ББК 22.144
Л55
УДК 512.62

Лидл Р., Нидеррайтер Г.

Л55 Конечные поля: В 2-х т. Т. 1. Пер. с англ. — М.: Мир, 1988. — 430 с.

ISBN 5-03-000065-8

Монографня известных математиков (Австралия, Австрия), отражающая многочисленные связи классического раздела алгебры — теории коиечных полей — с комбинаторикой, теорией кодироваиия, теорией автоматов. Изложение отличается простотой и ясностью, большим числом (около 600) примеров и упражнений, имеются комментарии исторического характера. Книга входит в известиую энциклопедию математики и ее приложенний (под ред. Дж.-К. Роты); ряд ее томов переведен в издательствах «Мир» и «Наука».

Русское издаиие выходнт в двух томах.

Для математиков-прикладиников, иижеиеров-исследователей, аспираитов и студеитов университетов.

Л $\frac{1702030000—273}{041\ (01)—88}$ 8—88, ч. 1 ББК 22.144

Редакция литературы по математическим наукам

ISBN 5-03-000065-8 (русск.)
ISBN 5-03-000064-X
ISBN 0-201-13519-1 (англ.)

© Cambridge University Press 1985
This book was originally published in the English language by Cambridge University Press of Cambridge, England.
© перевод иа русский язык, с дополиеииями, «Мир», 1988

От редактора перевода

Конечные поля стали изучаться в начале XIX в. Этому предшествовали исследования выдающихся математиков XVII и XVIII в. Но бесспорные заслуги в формировании этого понятия принадлежат Гауссу и Галуа. Длительное время конечные поля изучались и находили применение только в алгебре и теории чисел, однако в последние десятилетия грани соприкосновения теории конечных полей с разными областями математики и ее прикладными разделами существенно расширились. Теория чисел, теория полей, теория групп, алгебраическая геометрия, комбинаторика, теория кодирования — вот далеко не полный перечень разделов математики, с которыми эта теория успешно взаимодействует.

К настоящему времени по теории конечных полей и ее приложениям накопился значительный материал, который разбросан по многочисленным изданиям журнального типа, и вызывает удивление, что до недавних пор ни у нас, ни за рубежом не было монографии по теории конечных полей. Предлагаемая вниманию читателей книга Лидла и Нидеррайтера восполняет этот пробел.

Хочется отметить ряд ее несомненных достоинств. Книга написана простым и ясным языком, авторы избегают излишней формализации, текст сопровождается большим числом примеров и упражнений. В первой главе излагаются все необходимые сведения из алгебры и теории чисел, а последняя содержит таблицы индексов, логарифмов Якоби, неприводимых и примитивных многочленов. Исключительно ценными являются обширные комментарии, которыми оканчивается каждая глава. Они включают в себя исторические сведения и указывают связи рассматриваемых вопросов с другими разделами математики. В этих комментариях обсуждаются также различные подходы к излагаемому материалу. И наконец, книга содержит уникальную по полноте библиографию, занимающую около четверти ее объема и охватывающую практически все монографии и журнальные статьи по этой тематике вплоть до 1983 г.

Все это делает книгу доступной для широкого круга читателей и весьма ценным справочным пособием для всех специалистов, исследования которых связаны с конечными полями.

Она также может быть эффективно использована при подготовке студентов и аспирантов математических факультетов университетов и педвузов.

В процессе перевода в список литературы был добавлен ряд названий. Они помещены отдельным списком и отмечены звездочкой. Добавлено также несколько примечаний, которые либо имеют целью дополнить даваемую авторами историческую перспективу, либо носят характер уточнений.

Русское издание выходит в двух томах. Перевод первых шести глав выполнен В. И. Петровым, остальных — А. Е. Жуковым.

В. И. Нечаев

От редактора Энциклопедии

Математика состоит главным образом из фактов, которые можно представить и описать подобно любому явлению природы. Эти факты, сформулированные явно в виде теорем или скрытые внутри доказательств, составляют основную часть приложений математики и, вероятно, переживут все изменения математических вкусов и интересов.

Цель настоящей Энциклопедии — постараться осветить все области математики. Непременным требованием к автору является ясность изложения материала, доступность для неспециалистов, а также наличие подробной библиографии. Тома Энциклопедии объединяются в серии, которые соответствуют различным областям современной математики; порядок выхода книг в отдельных сериях не устанавливается. Число томов и серий будет по мере надобности пересматриваться.

Мы надеемся, что наше предприятие будет способствовать еще более широкому применению математики там, где без нее нельзя обойтись, и сделает возможным ее применение в тех областях, где она могла бы быть полезной, но куда еще не проникла ввиду недостатка информации.

Джан-Карло Рота

Предисловие редактора серии

В большинстве книг по современной алгебре конечным полям обычно уделяется лишь несколько страниц. Поэтому на первый взгляд может показаться удивительным появление целой книги, посвященной теории конечных полей, да еще вышедшей в серии «Энциклопедия математики и ее приложений». Однако читатель этой книги увидит, что ее авторы выполнили в высшей степени своевременную задачу, собрав воедино различные линии развития, обязанные своим возникновением данному предмету. В первую очередь следует отметить бурно развивающуюся теорию кодирования (которой в этой серии уже была посвящена монография Макэлайса). В настоящем издании теория кодирования трактуется в более широком контексте теории многочленов над конечными полями, и при этом устанавливается ее связь с линейными рекуррентными последовательностями и регистрами сдвига.

Что же касается «чистой» (т. е. теоретической) стороны, то имеется большая область теории чисел, которая наиболее естественно описывается в терминах конечных полей. Многое из изложенного здесь (например, тригонометрические суммы и уравнения над конечными полями) может служить образцом для более общего случая, и авторы продвигаются так далеко, как это только возможно при использовании лишь элементарных алгебраических методов. В результате книга может служить введением в указанную область.

Но конечные поля обладают такими свойствами, которые присущи далеко не всем алгебраическим объектам. Например, они (как, впрочем, и конечные булевы алгебры) функционально полны. Это значит, что любое отображение конечного поля в себя можно представить с помощью некоторого многочлена. Доказательство этого факта несложно (оно вытекает, например, из интерполяционной формулы Лагранжа), однако при отыскании многочленов, осуществляющих перестановки, возникает целый ряд практических проблем. Такие перестановочные многочлены используются в самых разных областях, и в данной книге излагаются методы их отыскания. Настоящее издание, вполне соответствуя своему назначению настольной книги для прикладников, содержит множество разнообразных алгоритмов

разложения многочленов на множители — как над большими, так и над малыми конечными полями.

Обширные комментарии в конце каждой главы дают интересную историческую перспективу, а исчерпывающая библиография делает данный выпуск Энциклопедии настоящим справочником по конечным полям.

П. М. Кон

Памеле и Герлинде

Предисловие

Теория конечных полей — это ветвь современной алгебры, ставшая за последние полвека весьма актуальной в связи с разнообразными приложениями, в том числе в комбинаторике, теории кодирования и математической теории переключательных схем. Начала теории восходят к XVII и XVIII в. и связаны с именами выдающихся математиков Пьера Ферма (1601—1665), Леонарда Эйлера (1707—1783), Жозефа-Луи Лагранжа (1730—1813) и Адриена-Мари Лежандра (1752—1833), которые внесли вклад в структурную теорию простых конечных полей. Что же касается общей теории конечных полей, то она началась с работ Карла-Фридриха Гаусса (1777—1855) и Эвариста Галуа (1811—1832), но привлекла внимание прикладников лишь в последние десятилетия, когда резко возросло значение дискретной математики.

В данной монографии, первой книге, целиком посвященной конечным полям, мы хотим представить оба аспекта этого предмета — как классический, так и прикладной. Таким образом, читатель найдет здесь не только вопросы, представляющие собой неотъемлемую сущность теории, но также и те результаты и технические приемы, которые важны главным образом в связи с их использованием в приложениях. Ввиду обширности предмета на выбор материала были наложены жесткие ограничения. Пытаясь сделать книгу по возможности замкнутой в себе, мы воздерживались от включения в нее результатов и методов, принадлежащих собственно алгебраической геометрии или теории полей алгебраических функций. Приложения описываются лишь в пределах, позволяющих обходиться без слишком больших отступлений. Для чтения книги требуются только знание основ линейной алгебры (в пределах первого курса) и некоторые элементарные познания из анализа. Предварительное знакомство с абстрактной алгеброй, безусловно, полезно, хотя все необходимые сведения приводятся в гл. 1.

Глава 2 занимает в книге центральное место в силу того, что знакомит с общей структурой конечных полей, а также с основными понятиями, используемыми во всей книге. Третья глава, посвященная теории многочленов, тесно связана с четвертой, рассматривающей алгоритмы разложения многочленов на мно-

жители, так что их целесообразно изучать вместе. Столь же тесно связаны гл. 5 и 6, касающиеся тригонометрических сумм. Главы 7 и 8 можно читать независимо друг от друга, они опираются в основном на вторую и третью главы. Приложения, представленные в девятой главе, базируются на материале из предшествующих глав. Глава 10 дополняет некоторые части гл. 2 и 3.

Каждая глава открывается кратким обзором ее содержания, поэтому приводить этот обзор в предисловии необязательно. Поскольку данная монография является частью энциклопедической серии, мы стремились дать как можно больше информации при заданном объеме, а это, в частности, привело к исключению некоторых громоздких доказательств. Чтобы не усложнять основной текст, мы вынесли библиографические ссылки в комментарии в конце каждой главы. Эти комментарии, кроме того, снабжают читателя обзором литературы и сводкой дальнейших результатов. В конце книги собрана воедино вся литература, которая упоминалась в комментариях.

Для повышения привлекательности данной монографии как учебного пособия мы поместили в подходящих местах текста разобранные примеры и снабдили каждую главу (кроме последней) списком упражнений. Упражнения эти весьма разнятся по сложности — от обычных задач до самостоятельных доказательств ключевых теорем. Они включают также материал, не охваченный основным текстом.

Что касается перекрестных ссылок, то мы перенумеровали все отдельные пункты основного текста последовательно по главам — независимо от того, определения ли это, теоремы, примеры и т. п. Таким образом, например, «определение 2.41» отсылает к п. 41 гл. 2 (который оказывается определением), а «замечание 6.28» отсылает к п. 28 гл. 6 (который оказывается замечанием). Аналогично «упражнение 5.31» отсылает к списку упражнений к гл. 5.

Нам доставляет огромное удовольствие выразить благодарность профессору Джану-Карло Роте за то, что он предложил нам написать эту книгу, и за его терпение в ожидании результатов наших усилий. Мы признательны за помощь госпоже Мелании Бартон, которая с большой тщательностью и умением отпечатала нашу рукопись, и, наконец, мы благодарим весь персонал издательства Addison-Wesley за высокий профессионализм при создании этой книги.

Р. Лидл, Г. Нидеррайтер

Глава 1

Алгебраические основы

Эта вводная глава содержит обзор некоторых основных алгебраических понятий, которые используются в книге. В элементарной алгебре применение арифметических операций (например, сложения и умножения) с заменой конкретных чисел символами обеспечивает возможность получения формул, которые при подстановке чисел вместо символов дают решение частных числовых задач. В современной алгебре уровень абстракции возрастает: от обычных операций над действительными числами переходят к общим операциям — процессам образования в некотором множестве общего вида из двух или более данных элементов некоторого нового элемента. При этом ставится цель изучить общие свойства всевозможных систем, состоящих из множества и некоторого числа заданных на нем и определенным образом взаимодействующих операций, например множества с двумя бинарными операциями, взаимодействующими подобно сложению и умножению действительных чисел.

Мы рассмотрим лишь самые основные определения и свойства алгебраических систем (т. е. множеств с одной или несколькими операциями на них), сознательно ограничив себя тем минимумом теории, который необходим для нашей основной цели — изучения конечных полей. При этом некоторые стандартные результаты мы сообщим без доказательства. В вопросе о множествах мы принимаем наивную точку зрения. Будем использовать следующие числовые множества: $\mathbb{N}$ — множество натуральных, $\mathbb{Z}$ — целых, $\mathbb{Q}$ — рациональных, $\mathbb{R}$ — действительных и $\mathbb{C}$ — комплексных чисел.

§ 1. Группы

Известны две операции на множестве $\mathbb{Z}$ целых чисел — сложение и умножение. Обобщим понятие операции на произвольное множество.

Пусть S — некоторое множество, и пусть $S \times S$ обозначает множество упорядоченных пар (s, t), где $s \in S$, $t \in S$. Тогда произвольное отображение из $S \times S$ в S мы будем называть (*бинарной*) *операцией* на множестве S. В этом определении мы

требуем, чтобы образ каждой пары $(s, t) \in S \times S$ был непременно элементом множества S — это так называемое *свойство замкнутости* операции. Под *алгебраической системой* или *алгебраической структурой* мы будем понимать некоторое множество S с одной или несколькими операциями на нем.

В элементарной арифметике мы имеем дело с двумя операциями — сложением и умножением, важным свойством которых является ассоциативность. Среди всевозможных алгебраических систем, имеющих одну ассоциативную операцию, самыми изученными и развитыми являются группы. Теория групп — один из старейших разделов абстрактной алгебры, который к тому же особенно богат приложениями.

1.1. Определение. *Группой* $(G, *)$ называется некоторое множество G с бинарной операцией $*$ на нем, для которых выполняются следующие три условия:

1. Операция $*$ *ассоциативна*, т. е. для любых $a, b, c \in G$

$$a * (b * c) = (a * b) * c.$$

2. В G существует *единичный элемент* (или *единица*) e, такой, что для любого $a \in G$

$$a * e = e * a = a.$$

3. Для каждого $a \in G$ существует *обратный элемент* $a^{-1} \in G$, такой, что

$$a * a^{-1} = a^{-1} * a = e.$$

Если группа удовлетворяет также следующему условию:

4. Для любых $a, b \in G$

$$a * b = b * a,$$

то она называется *абелевой* (или *коммутативной*).

Группу $(G, *)$ будем обозначать просто G. Легко показать, что единичный элемент e группы G, а также обратный элемент a^{-1} для каждого данного элемента $a \in G$ определяются однозначно указанными выше условиями. Далее, для всех $a, b \in G$ имеет место равенство $(a * b)^{-1} = b^{-1} * a^{-1}$. Для простоты мы часто для групповой операции будем использовать мультипликативное обозначение $\cdot$ (как для обычного умножения) и вместо $a * b$ писать $a \cdot b$ или просто ab (называя этот элемент *произведением* элементов a и b). Но необходимо подчеркнуть, что при этом мы отнюдь не предполагаем, что операция и в самом деле является обычным умножением. Иногда, однако, для групповой операции бывает удобно использовать аддитивную запись и писать $a + b$ вместо $a * b$ (называя этот элемент *суммой* элементов a и b), 0 вместо e (называя этот элемент *нулем*) и $-a$ вместо a^{-1}. Такие

(аддитивные) обозначения обычно резервируются для абелевых групп.

Закон ассоциативности гарантирует, что выражение вида $a_1a_2 \dots a_n$, где $a_i \in G$, $1 \leqslant i \leqslant n$, не содержит никакой двусмысленности, так как независимо от расстановки скобок это выражение всегда представляет один и тот же элемент группы G. Пусть $a \in G$ и $n \in \mathbb{N}$. Будем применять запись

$$a^n = aa \dots a \quad (n \text{ сомножителей } a)$$

и называть элемент a^n n-й *степенью* элемента a. Если же для групповой операции применяется аддитивное обозначение $+$, то вместо a^n будем писать

$$na = a + a + \cdots + a \quad (n \text{ слагаемых } a).$$

Используя обычные обозначения, мы получаем следующие правила:

Мультипликативные обозначения	*Аддитивные обозначения*
$a^{-n} = (a^{-1})^n$	$(-n)\,a = n\,(-a)$
$a^m a^n = a^{m+n}$	$ma + na = (m + n)\,a$
$(a^m)^n = a^{mn}$	$m\,(na) = (mn)\,a$

Для $n = 0 \in \mathbb{Z}$ полагаем $a^0 = e$ в мультипликативных обозначениях и $0a = 0$ в аддитивных (здесь второй нуль является единичным элементом группы G).

1.2. Примеры

(i) Пусть G — множество целых чисел с операцией $+$ (обычным сложением). Известно, что это ассоциативная операция и что сумма двух целых чисел — однозначно определенное целое число. Легко убедиться, что G — группа, в которой единичным элементом является нуль 0, а обратным для целого числа a — противоположное число $-a$. Эту группу обозначают через $\mathbb{Z}$.

(ii) Множество, состоящее из единственного элемента e с операцией $*$, определенной условием $e * e = e$, образует группу.

(iii) Пусть G — множество $\{0, 1, 2, 3, 4, 5\}$ остатков от деления целых чисел на 6, и для $a, b \in G$ пусть $a * b$ — остаток от деления на 6 обычной суммы чисел a и b. Существование единичного элемента и обратных здесь очевидно, но для установления ассоциативности операции $*$ требуются некоторые вычисления. Полученную группу можно непосредственно обобщить, заменив целое число 6 любым натуральным числом n. □

Интересный класс образуют группы, в которых каждый элемент является степенью некоторого фиксированного элемента

группы (при аддитивной записи говорят о кратном, а не о степени).

1.3. Определение. Мультипликативная группа G называется *циклической*, если в ней имеется такой элемент a, что каждый элемент $b \in G$ является степенью элемента a, т. е. существует целое число k, такое, что $b = a^k$. Этот элемент a называется *образующим* группы G. Для циклической группы G применяют обозначение $G = \langle a \rangle$.

Из определения сразу же следует, что каждая циклическая группа коммутативна. Заметим также, что циклическая группа может иметь не один образующий. Например, в аддитивной группе $\mathbb{Z}$ образующим является как 1, так и -1.

Рассматривая аддитивную группу остатков от деления целых чисел на $n \in \mathbb{N}$, обобщающую пример 1.2 (iii), нетрудно заметить, что используемый там тип операции приводит к отношению эквивалентности на множестве целых чисел. В общем случае *отношением эквивалентности* на множестве S называется подмножество R множества $S \times S$ упорядоченных пар (s, t), $s, t \in S$, обладающее следующими тремя свойствами:

(a) $(s, s) \in R$ для всех $s \in S$ (*рефлексивность*).
(b) Если $(s, t) \in R$, то $(t, s) \in R$ (*симметричность*).
(c) Если (s, t), $(t, u) \in R$, то $(s, u) \in R$ (*транзитивность*).

Элементы $s, t \in S$ называются *эквивалентными*, если $(s, t) \in R$. Наиболее простым примером отношения эквивалентности является равенство. Важно отметить, что любое отношение эквивалентности на множестве S вызывает некоторое *разбиение* этого множества, т. е. представление S в виде объединения его непустых попарно непересекающихся подмножеств. Собрав вместе все элементы множества S, эквивалентные некоторому фиксированному элементу $s \in S$, получим *класс эквивалентности* элемента s, обозначаемый символом

$$[s] = \{t \in S \mid (s, t) \in R\}.$$

Совокупность всех различных классов эквивалентности и дает требуемое разбиение множества S. Заметим, что $[s] = [t]$ в том и только том случае, когда s и t эквивалентны, т. е. $(s, t) \in R$. Пример 1.2 (iii) подводит к следующему понятию.

1.4. Определение. Пусть a и b — произвольные целые числа и n — натуральное число. Будем говорить, что a *сравнимо с* b *по модулю* n, и будем писать $a \equiv b \pmod{n}$, если разность $a - b$ делится на n, т. е. если $a = b + kn$ для некоторого целого числа k.

Легко проверяется, что сравнимость по модулю n является отношением эквивалентности на множестве $\mathbb{Z}$ целых чисел. Рефлексивность и симметричность его очевидны. Транзитивность

тоже проверяется несложно: если $a = b + kn$ и $b = c + ln$ для некоторых целых чисел k и l, то $a = c + (k + l)\,n$, так что из $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$ следует $a \equiv c \pmod{n}$.

Рассмотрим теперь классы эквивалентности, на которые отношение сравнимости по модулю n разбивает множество $\mathbb{Z}$ (они называются *классами вычетов по модулю n*). Ими являются множества

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\},$$
$$[1] = \{\ldots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \ldots\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$[n - 1] = \{\ldots, -n - 1, -1, n - 1, 2n - 1, 3n - 1, \ldots\}.$$

Мы можем определить на множестве $\{[0], [1], \ldots, [n-1]\}$ классов вычетов по модулю n некоторую бинарную операцию (которую мы снова обозначим знаком $+$, хотя она, конечно, не является обычным сложением), положив

$$[a] + [b] = [a + b], \tag{1.1}$$

где a и b — произвольные элементы соответствующих классов $[a]$ и $[b]$, а сумма $a + b$ справа является обычной суммой чисел a и b. Для того чтобы показать, что мы действительно определили некоторую операцию, т. е. что наше определение корректно, мы должны проверить, что класс вычетов $[a] + [b]$ однозначно определяется классами $[a]$ и $[b]$ и не зависит от выбора их представителей a и b. Доказательство этого мы оставляем читателю в качестве упражнения. Ассоциативность операции (1.1) следует из ассоциативности обычного сложения. Единичным элементом является $[0]$, а обратным элементом для $[a]$ будет $[-a]$. Итак, множество элементов $\{[0], [1], \ldots, [n-1]\}$ образует группу относительно операции $+$.

1.5. Определение. Группа, образованная множеством $\{[0], [1], \ldots, [n-1]\}$ классов вычетов по модулю n с операцией (1.1), называется *группой классов вычетов по модулю n* и обозначается $\mathbb{Z}_n$.

Группа $\mathbb{Z}_n$ является циклической группой с образующим элементом $[1]$, и эта группа имеет порядок n в соответствии со следующим определением.

1.6. Определение. Группа называется *конечной* (соответственно *бесконечной*), если она состоит из конечного (соответственно бесконечного) числа элементов. Число элементов конечной группы называется ее *порядком*. Для порядка конечной группы G будем использовать обозначение $|G|$.

Существует удобный способ задания конечной группы — в виде таблицы. Эта таблица, представляющая групповую операцию (она обычно называется *таблицей групповой операции*

или *таблицей Кэли* группы), строится так: ее строки и столбцы помечаются элементами группы и на пересечении строки, помеченной элементом a, и столбца, помеченного элементом b, ставится элемент ab.

1.7. Пример. Таблица Кэли группы $\mathbb{Z}_6$ имеет вид

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

□

Каждая группа содержит некоторые подмножества, которые сами образуют группу при той же групповой операции. Например, таким свойством обладает подмножество $\{[0], [2], [4]\}$ группы $\mathbb{Z}_6$.

1.8. Определение. Подмножество H группы G называется *подгруппой* этой группы, если H само образует группу относительно операции группы G. Подгруппы группы G, отличные от *тривиальных подгрупп* $\{e\}$ и G, называется ее *собственными подгруппами*.

Легко проверяется, что множество всех степеней произвольного элемента a группы G образует подгруппу этой группы.

1.9. Определение. Подгруппа группы G, состоящая из всех степеней элемента a этой группы, называется подгруппой, *порожденной элементом* a, и обозначается символом $\langle a\rangle$. Эта подгруппа, очевидно, циклическая. Если $\langle a\rangle$ — конечная подгруппа, то ее порядок называется *порядком* элемента a. В противном случае a называется элементом *бесконечного порядка*.

Таким образом, порядок элемента a равен наименьшему натуральному числу k, такому, что $a^k = e$. Нетрудно показать, что любое целое число m, обладающее тем свойством, что $a^m = e$, делится на k. Если S — некоторое непустое подмножество группы G, то подгруппа H группы G, состоящая из всех конечных произведений степеней элементов из S, называется подгруппой, *порожденной множеством* S, и обозначается символом $\langle S\rangle$, а S называется *множеством образующих* подгруппы H.

Для аддитивной группы $\mathbb{Z}$ целых чисел понятие сравнимости по модулю n (где n — натуральное число) тесно связано с подгруппой $\langle n\rangle$, порожденной элементом n, так как

$$a \equiv b \pmod{n} \Leftrightarrow a - b \in \langle n\rangle.$$

Таким образом, подгруппа $\langle n \rangle$ определяет отношение эквивалентности на множестве $\mathbb{Z}$. Эту ситуацию можно обобщить следующим образом.

1.10. Теорема. *Если H — подгруппа группы G, то отношение R_H на G, определяемое условием*

$$(a, b) \in R_H \Leftrightarrow a = bh \text{ для некоторого } h \in H,$$

является отношением эквивалентности.

Доказательство тривиально. Соответствующие отношению R_H классы эквивалентности называются *левыми смежными классами* группы G по подгруппе H и обозначаются

$$aH = \{ah \mid h \in H\}$$

(или $a + H = \{a + h \mid h \in H\}$, если G — аддитивная группа), где a — фиксированный элемент группы G. Аналогично определяется разбиение группы G на *правые смежные классы* по подгруппе H, которые имеют вид $Ha = \{ha \mid h \in H\}$. Если G — абелева группа, то ее левые смежные классы по подгруппе H совпадают с правыми.

1.11. Пример. Пусть $G = \mathbb{Z}_{12}$, и пусть H — подгруппа $\{[0], [3], [6], [9]\}$. Тогда различными (левыми) смежными классами G по H являются

$$\begin{aligned} [0] + H &= \{[0], [3], [6], [9]\}, \\ [1] + H &= \{[1], [4], [7], [10]\}, \\ [2] + H &= \{[2], [5], [8], [11]\}. \end{aligned}$$

□

1.12. Теорема. *Если H — конечная подгруппа группы G, то каждый (левый или правый) смежный класс группы G по подгруппе H содержит столько же элементов, сколько H.*

1.13. Определение. Если подгруппа H группы G такова, что множество смежных классов G по H конечно, то число этих смежных классов называется *индексом* подгруппы H в группе G и обозначается через $(G : H)$.

Так как левые смежные классы группы G по подгруппе H образуют разбиение этой группы, то из теоремы 1.12 вытекает следующий важный результат.

1.14. Теорема. *Порядок конечной группы G равен произведению порядка любой ее подгруппы H на индекс $(G : H)$ этой подгруппы в G. В частности, порядок любой подгруппы H группы G и ее индекс в G делят порядок группы G, и порядок любого элемента $a \in G$ делит порядок группы G.*

Подгруппы и порядки элементов для циклических групп описываются несложно. Относящиеся к этому факты мы суммируем в следующей теореме.

1.15. Теорема.
(i) *Каждая подгруппа циклической группы также является циклической.*
(ii) *В конечной циклической группе* $\langle a\rangle$ *порядка* m *элемент* a^k *порождает подгруппу порядка* $m/\text{НОД}(k, m)$ (где НОД (k, m) — *наибольший общий делитель чисел* k *и* m).
(iii) *Если* d *— положительный делитель порядка* m *конечной циклической группы* $\langle a\rangle$, *то* $\langle a\rangle$ *содержит единственную подгруппу индекса* d. *Для любого положительного делителя* l *числа* m *группа* $\langle a\rangle$ *содержит в точности одну подгруппу порядка* l.
(iv) *Пусть* l *— положительный делитель порядка конечной циклической группы* $\langle a\rangle$. *Тогда* $\langle a\rangle$ *содержит* $\varphi(l)$ *элементов порядка* l. (Здесь $\varphi(l)$ *— функция Эйлера*, указывающая число целых чисел k, $1 \leqslant k \leqslant l$, которые взаимно просты с l.)
(v) *Конечная циклическая группа* $\langle a\rangle$ *порядка* m *содержит* $\varphi(m)$ *образующих* (*т. е. таких элементов* a^r, *что* $\langle a^r\rangle = \langle a\rangle$). *Образующими являются те и только те степени* a^r *элемента* a, *для которых* НОД $(r, m) = 1$.

Доказательство. (i) Пусть H — подгруппа циклической группы $\langle a\rangle$, такая, что $H \neq \{e\}$. Если $a^n \in H$, то $a^{-n} \in H$; поэтому H содержит по крайней мере одну степень элемента a с положительным показателем. Пусть d — наименьший положительный показатель, для которого $a^d \in H$, и пусть $a^s \in H$. Деление s на d дает $s = qd + r$, $0 \leqslant r < d$, q, $r \in \mathbb{Z}$. Таким образом, $a^s (a^{-d})^q = a^r \in H$, что противоречит минимальности d, если $r \neq 0$. Поэтому показатели всех степеней элемента a, принадлежащих H, кратны d, так что $H = \langle a^d\rangle$.
(ii) Положим $d = \text{НОД}(k, m)$. Порядок группы $\langle a^k\rangle$ — наименьшее натуральное число n, такое, что $a^{kn} = e$. Последнее равенство справедливо тогда и только тогда, когда число m делит число kn, т. е. тогда и только тогда, когда m/d делит n. Наименьшее натуральное число n с таким свойством есть m/d.
(iii) Если d задано, то $\langle a^d\rangle$ является подгруппой порядка m/d группы $\langle a\rangle$ и потому имеет индекс d в $\langle a\rangle$ ввиду (ii). Если $\langle a^k\rangle$ — другая подгруппа индекса d группы $\langle a\rangle$, то ее порядок равен m/d, так что $d = \text{НОД}(k, m)$ в силу (ii). В частности, d делит k, так что $a^k \in \langle a^d\rangle$ и $\langle a^k\rangle$ является подгруппой группы $\langle a^d\rangle$. Но так как обе группы одного порядка, то они совпадают. Вторая часть вытекает из того факта, что подгруппами порядка l являются те и только те подгруппы, индексы которых равны m/l.
(iv) Пусть $|\langle a\rangle| = m$ и $m = dl$. В силу (ii) элемент a^k имеет порядок l в том и только том случае, если НОД $(k, m) = d$. Поэтому число элементов порядка l равно количеству целых чисел k, $1 \leqslant k \leqslant m$, для которых НОД $(k, m) = d$. Значит, $k = dh$, где $1 \leqslant h \leqslant l$, и тогда условие НОД $(k, m) = d$ эквива-

лентно условию НОД $(h, l) = 1$. Количество таких чисел h равно $\varphi(l)$.

(v) Образующими группы $\langle a\rangle$ являются те и только те элементы, порядки которых равны m, так что первая часть следует из (iv). Вторая же часть вытекает из (ii). □

При сравнении структуры двух групп весьма важную роль играют такие отображения одной группы в другую, которые сохраняют их операции.

1.16. Определение. Отображение $f\colon G \to H$ группы G в группу H называется *гомоморфизмом* группы G в H, если оно сохраняет операцию группы G. Это значит, что если $*$ и $\cdot$ — операции в группах G и H соответственно, то для всех $a, b \in G$ имеет место равенство $f(a * b) = f(a) \cdot f(b)$. Если, кроме того, f — отображение на H, то оно называется *эпиморфизмом* (или *гомоморфизмом «на»*), и в этом случае H называется *гомоморфным образом* группы G. Гомоморфизм группы G в G называется *эндоморфизмом* этой группы. Если f — взаимно однозначный гомоморфизм группы G на группу H, то он называется *изоморфизмом*, и в таком случае говорят, что группы G и H *изоморфны*. Изоморфизм группы G на G называется *автоморфизмом* этой группы.

В качестве примера рассмотрим отображение f аддитивной группы $\mathbb{Z}$ целых чисел на группу $\mathbb{Z}_n$ классов вычетов по модулю n, определяемое условием $f(a) = [a]$. Тогда

$$f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$$
$$\text{для } a, b \in \mathbb{Z},$$

так что f — гомоморфизм (точнее, эпиморфизм).

Если $f\colon G \to H$ — гомоморфизм и e — единичный элемент группы G, то из $ee = e$ следует $f(e) f(e) = f(e)$, так что $f(e) = e'$ — единичный элемент группы H. Из равенства $aa^{-1} = e$ получаем $f(a^{-1}) = (f(a))^{-1}$ для всех $a \in G$.

Автоморфизмы группы G представляют особый интерес, в частности, потому, что они сами образуют группу относительно обычной композиции [1]) отображений (это проверяется без труда). Важными примерами автоморфизмов группы G являются ее внутренние автоморфизмы. *Внутренний автоморфизм* f_a определяется для фиксированного элемента a группы G условием $f_a(b) = aba^{-1}$ для всех $b \in G$. Очевидно, что f_a — автоморфизм группы G, и все внутренние автоморфизмы группы G получаются, когда a пробегает все элементы группы G. Элементы b и aba^{-1} называются *сопряженными*, и если S — непустое подмножество

---

[1]) *Композицией* отображений $\varphi\colon B \to C$ и $\psi\colon A \to B$ называется отображение $f\colon A \to C$ (обозначаемое $f = \varphi \circ \psi$), которое определяется условием $f(a) = \varphi(\psi(a))$ для любого $a \in G$. — *Прим. перев.*

в G, то множество $aSa^{-1} = \{asa^{-1} \mid s \in S\}$ называется *сопряженным* с S. Таким образом, сопряженными с S множествами в группе G оказываются образы множества S при всевозможных внутренних автоморфизмах группы G и только они.

1.17. Определение. *Ядром* гомоморфизма $f\colon G \to H$ группы G в группу H называется множество

$$\operatorname{Ker} f = \{a \in G \mid f(a) = e'\},$$

где e' — единичный элемент группы H.

1.18. Пример. Для гомоморфизма $f : \mathbb{Z} \to \mathbb{Z}_n$, определенного условием $f(a) = [a]$, ядро $\operatorname{Ker} f$ состоит из всех $a \in \mathbb{Z}$, для которых $[a] = [0]$. Так как это условие выполняется для тех и только тех чисел a, которые делятся на n, то получаем, что $\operatorname{Ker} f = \langle n \rangle$ — подгруппа группы $\mathbb{Z}$, порожденная числом n. □

Легко проверить, что ядро $\operatorname{Ker} f$ гомоморфизма $f\colon G \to H$ всегда является подгруппой группы G. Более того, эта подгруппа $\operatorname{Ker} f$ обладает важным дополнительным свойством: для любых $a \in G$ и $b \in \operatorname{Ker} f$ имеет место включение $aba^{-1} \in \operatorname{Ker} f$. Это приводит нас к следующему важному понятию.

1.19. Определение. Подгруппа H группы G называется *нормальной подгруппой* (или *нормальным делителем*) этой группы, если $ghg^{-1} \in H$ для всех $g \in G$ и $h \in H$.

Ясно, что каждая подгруппа абелевой группы нормальна, поскольку в этом случае $ghg^{-1} = gg^{-1}h = eh = h$. Дадим два критерия нормальности подгруппы.

1.20. Теорема. (i) *Подгруппа H группы G нормальна тогда и только тогда, когда она совпадает со всеми своими сопряженными подгруппами, т. е. тогда и только тогда, когда подгруппа H инвариантна относительно всех внутренних автоморфизмов группы G.*

(ii) *Подгруппа H группы G нормальна тогда и только тогда, когда для любого элемента $a \in G$ левый смежный класс aH совпадает с правым смежным классом Ha.*

Важным свойством нормальной подгруппы является тот факт, что множество (левых) смежных классов по ней можно наделить групповой структурой.

1.21. Теорема. *Если H — нормальная подгруппа группы G, то множество (левых) смежных классов группы G по подгруппе H образует группу относительно операции*

$$(aH)\,(bH) = (ab)\,H.$$

1.22. Определение. Пусть H — нормальная подгруппа группы G. Тогда группа, образованная (левыми) смежными классами

группы G по подгруппе H с операцией, введенной в теореме 1.21, называется *факторгруппой* группы G по подгруппе H и обозначается через G/H.

Если факторгруппа G/H конечна, то ее порядок совпадает с индексом $(G : H)$ подгруппы H в G. Таким образом, из теоремы 1.14 получаем, что для конечной группы G

$$|G/H| = (G : H) = |G|/|H|.$$

Каждая нормальная подгруппа группы G естественным образом определяет некоторый гомоморфизм этой группы, причем верно и обратное утверждение.

1.23. Теорема (о гомоморфизме). *Пусть* $f\colon G \to G_1 = f(G)$ — *гомоморфизм группы* G *на группу* G_1. *Тогда ядро* $\operatorname{Ker} f$ *является нормальной подгруппой группы* G, *причем группа* G_1 *изоморфна факторгруппе* $G/\operatorname{Ker} f$. *Обратно, если* H — *нормальная подгруппа группы* G, *то отображение* $\psi\colon G \to G/H$, *определяемое условием* $\psi(a) = aH$ *для любого* $a \in G$, *является гомоморфизмом группы* G *на* G/H, *причем* $\operatorname{Ker} \psi = H$.

Выведем теперь для конечной группы одно важное соотношение для мощностей [1]) классов сопряженных элементов, которое понадобится в § 6 гл. 2.

1.24. Определение. Пусть S — непустое подмножество группы G. Его *нормализатором* в группе G называется множество

$$N(S) = \{a \in G \mid aSa^{-1} = S\}.$$

Если $S = \{b\}$, то $N(\{b\})$ будем называть *нормализатором элемента* b в G и обозначать $N(b)$.

1.25. Теорема. *Для любого непустого подмножества* S *группы* G *нормализатор* $N(S)$ *является подгруппой группы* G, *причем имеет место взаимно однозначное соответствие между левыми смежными классами группы* G *по подгруппе* $N(S)$ *и различными множествами* aSa^{-1}, *сопряженными с* S.

Доказательство. Очевидно, что $e \in N(S)$, и если $a, b \in N(S)$, то a^{-1} и ab тоже принадлежат $N(S)$, так что $N(S)$ — подгруппа группы G. Далее,

$$aSa^{-1} = bSb^{-1} \Leftrightarrow S = a^{-1}bSb^{-1}a = (a^{-1}b)\,S\,(a^{-1}b)^{-1} \Leftrightarrow$$
$$\Leftrightarrow a^{-1}b \in N(S) \Leftrightarrow b \in aN(S).$$

Таким образом, сопряженные с S множества aSa^{-1} и bSb^{-1} совпадают тогда и только тогда, когда элементы a и b принадлежат

[1]) *Мощностью* конечного множества называется число элементов этого множества. — *Прим. перев.*

одному и тому же левому смежному классу группы G по подгруппе $N(S)$. Отсюда следует вторая часть теоремы. □

Если собрать все элементы группы G, сопряженные с фиксированным элементом a, то получим множество, называемое *классом сопряженных с a элементов* группы G или *классом сопряженности* группы G, содержащим элемент a. Для некоторых элементов соответствующие им классы сопряженности состоят из единственного элемента (а именно из самого исходного элемента). Таким свойством обладают элементы центра группы и только они.

1.26. Определение. *Центром* группы G называется ее подмножество

$$C = \{c \in G \mid ca = ac \quad \text{для всех} \quad a \in G\}.$$

Без труда проверяется, что центр — нормальная подгруппа группы G. Очевидно, что группа G является абелевой тогда и только тогда, когда $C = G$. Несложный подсчет приводит к следующему важному равенству, которое иногда называют «*уравнением классов сопряженности*».

1.27. Теорема. *Пусть G — конечная группа с центром C. Тогда имеет место равенство*

$$|G| = |C| + \sum_{i=1}^{k} n_i,$$

где $n_1, \ldots, n_k$ — мощности классов сопряженности группы G, содержащих более одного элемента, так что $n_i \geqslant 2$, и при этом каждое число n_i делит порядок $|G|$ группы G, $1 \leqslant i \leqslant k$.

Доказательство. Поскольку отношение «a сопряжено с b» является отношением эквивалентности на G, то различные классы сопряженности группы G образуют разбиение множества G. Поэтому порядок $|G|$ группы G равен сумме мощностей различных классов сопряженности. Но имеется ровно $|C|$ классов сопряженности, состоящих из единственного элемента (они соответствуют элементам центра C), а мощности $n_1, \ldots, n_k$ остальных классов сопряженности превышают единицу. Отсюда и вытекает требуемое равенство. Для доказательства того, что каждое из чисел n_i делит $|G|$, достаточно заметить, что n_i — число элементов, сопряженных с некоторым элементом $a_i \in G$, и потому в силу теоремы 1.25 оно равно числу левых смежных классов группы G по подгруппе $N(a_i)$, а индекс нормализатора по теореме 1.14 делит порядок $|G|$ группы G. □

§ 2. Кольца и поля

В большинстве числовых систем, используемых в элементарной арифметике, имеется две различные бинарные операции:

сложение и умножение. Примерами могут служить целые, рациональные и действительные числа. Сейчас мы определим важный тип алгебраических структур, называемый кольцом, который обладает основными свойствами указанных числовых систем.

1.28. Определение. *Кольцом* $(R, +, \cdot)$ называется множество R с двумя бинарными операциями, обозначаемыми символами $+$ и $\cdot$, такими, что

1. R — абелева группа относительно операции $+$.
2. Операция $\cdot$ ассоциативна, т. е. для всех $a, b, c \in R$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

3. Выполняются *законы дистрибутивности*, т. е. для всех $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{и} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Следует обратить внимание на то, что операции $+$ и $\cdot$ не обязательно являются обычными сложением и умножением. Для краткости кольцо $(R, +, \cdot)$ будем обозначать одной буквой R. Единичный элемент аддитивной группы кольца R называется *нулевым элементом* (или *нулем*) кольца R и обозначается символом 0, а обратный к элементу a этой группы обозначается через $-a$. Вместо $a + (-b)$ пишут обычно $a - b$, а вместо $a \cdot b$ — просто ab. Из определения кольца получается общее свойство $a0 = 0a = 0$ для всех $a \in R$. Из этого в свою очередь следует, что $(-a)\, b = a\, (-b) = -ab$ для всех $a, b \in R$.

Простейшим примером кольца является, по-видимому, кольцо обычных целых чисел. Рассматривая его свойства, нетрудно обнаружить среди них такие, которыми не обладает произвольное кольцо. Таким образом, кольца допускают дальнейшую классификацию.

1.29. Определение.

(i) Кольцо называется *кольцом с единицей*, если оно имеет мультипликативную единицу, т. е. если существует такой элемент $e \in R$, что $ae = ea = a$ для любого $a \in R$.

(ii) Кольцо называется *коммутативным*, если операция $\cdot$ коммутативна.

(iii) Кольцо называется *целостным кольцом* (или *областью целостности*), если оно является коммутативным кольцом с единицей $e \neq 0$, в котором равенство $ab = 0$ влечет за собой $a = 0$ или $b = 0$.

(iv) Кольцо R называется *телом*, если $R \neq \{0\}$ и ненулевые элементы в R образуют группу относительно операции .

(v) Коммутативное тело называется *полем*.

Поскольку наша книга посвящена полям, то особое внимание мы обратим на определение этого понятия. Прежде всего

поле есть множество F, на котором заданы две операции, называемые *сложением* и *умножением* и которое содержит два выделенных элемента 0 и e, причем $0 \neq e$. Далее, поле F — абелева группа по сложению, единичным элементом которой является 0, а элементы из F, отличные от 0, образуют абелеву группу по умножению, единичным элементом которой является e. Две операции, сложение и умножение, связаны законом дистрибутивности $a(b + c) = ab + ac$. Второй закон дистрибутивности $(b + c)\, a = ba + ca$ выполняется автоматически в силу коммутативности умножения. Элемент 0 называется *нулевым элементом* (или просто *нулем*), а e — *единичным элементом* (или просто *единицей*) поля F. В дальнейшем для единицы, как правило, будем использовать символ 1.

Свойство, появляющееся в определении 1.29 (iii): равенство $ab = 0$ влечет за собой $a = 0$ или $b = 0$ — будем выражать словами «*отсутствуют делители нуля*». В частности, поле не имеет делителей нуля, так как если $ab = 0$ и $a \neq 0$, то умножение на a^{-1} дает $b = a^{-1}0 = 0$.

Проиллюстрируем понятие кольца следующими примерами.

1.30. Примеры

(i) Пусть R — абелева группа с групповой операцией $+$. Определим умножение условием $ab = 0$ для всех $a, b \in R$. Тогда R становится кольцом.

(ii) Целые числа образуют целостное кольцо, но не поле.

(iii) Четные числа образуют коммутативное кольцо без единицы.

(iv) Функции $f\colon \mathbb{R} \to \mathbb{R}$ образуют коммутативное кольцо с единицей, если сумма $f + g$ и произведение fg определяются условиями $(f + g)(x) = f(x) + g(x)$ и $(fg)(x) = f(x)\, g(x)$ для любых $x \in \mathbb{R}$.

(v) Множество всех (2×2)-матриц с элементами из $\mathbb{R}$ образует некоммутативное кольцо с единицей относительно операций сложения и умножения матриц. □

Выше мы видели, что поле, в частности, является целостным кольцом. Обратное, вообще говоря, неверно (см. пример 1.30 (ii)), однако верно в случае, когда указанное целостное кольцо состоит из конечного числа элементов (т. е. является *конечным* кольцом). *Порядком* конечного кольца называется число элементов этого кольца.

1.31. Теорема. *Каждое конечное целостное кольцо является полем.*

Доказательство. Пусть элементы конечного целостного кольца R суть $a_1, a_2, \ldots, a_n$. Для некоторого фиксированного ненулевого элемента $a \in R$ рассмотрим произведения $aa_1, aa_2, \ldots,$

aa_n. Они различны, так как если $aa_i = aa_j$, то $a(a_i - a_j) = 0$, и так как $a \neq 0$, то $a_i - a_j = 0$, т. е. $a_i = a_j$. Таким образом, каждый элемент в R имеет вид aa_i и, в частности, $e = aa_i$ для некоторого i, $1 \leqslant i \leqslant n$, где e — единица R. Поскольку кольцо R коммутативно, то также $a_i a = e$, так что элемент a_i является мультипликативным обратным к a. Таким образом, ненулевые элементы кольца R образуют абелеву группу, т. е. R — поле. □

1.32. Определение. Подмножество S кольца $(R, +, \cdot)$ называется *подкольцом* этого кольца, если оно замкнуто относительно операций $+$ и $\cdot$ и образует кольцо относительно этих операций.

1.33. Определение. Подмножество J кольца R называется (*двусторонним*) *идеалом* этого кольца, если оно является подкольцом кольца R и для всех $a \in J$ и $r \in R$ имеет место $ar \in J$ и $ra \in J$.

1.34. Примеры

(i) Пусть R — поле $\mathbb{Q}$ рациональных чисел. Тогда множество $\mathbb{Z}$ целых чисел является его подкольцом, но не идеалом, так как, например, $1 \in \mathbb{Z}$, $^1/_2 \in \mathbb{Q}$, но $^1/_2 \cdot 1 = {}^1/_2 \notin \mathbb{Z}$.

(ii) Пусть R — коммутативное кольцо, $a \in R$, и пусть $J = \{ra \mid r \in R\}$. Тогда J — идеал кольца R.

(iii) Пусть R — коммутативное кольцо. Тогда наименьшим идеалом, содержащим данный элемент $a \in R$, является идеал $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$. Если кольцо R имеет единицу, то $(a) = \{ra \mid r \in R\}$. □

1.35. Определение. Пусть R — коммутативное кольцо. Идеал J кольца R называется *главным*, если существует элемент $a \in R$, такой, что $J = (a)$. В этом случае J называют также главным идеалом, *порожденным элементом* a.

Так как идеалы являются нормальными подгруппами аддитивной группы кольца, то каждый идеал J кольца R определяет некоторое разбиение множества R на смежные классы по аддитивной подгруппе J, называемые *классами вычетов* кольца R *по модулю идеала* J. Класс вычетов кольца R по модулю J, содержащий элемент $a \in R$, будем обозначать через $[a] = a + J$, так как он состоит из всех элементов R вида $a + c$, где $c \in J$. Элементы a, $b \in R$, принадлежащие одному и тому же классу вычетов по модулю J (т. е. такие, что $a - b \in J$), будем называть *сравнимыми* по модулю J и записывать это так: $a \equiv b \pmod{J}$ (ср. с определением 1.4). Нетрудно проверить, что если $a \equiv b \pmod{J}$, то $a + r \equiv b + r \pmod{J}$, $ar \equiv br \pmod{J}$, $ra \equiv rb \pmod{J}$ и $na \equiv nb \pmod{J}$ для любых $r \in R$ и $n \in \mathbb{Z}$. Если, кроме того, $r \equiv s \pmod{J}$, то $a + r \equiv b + s \pmod{J}$ и $ar \equiv bs \pmod{J}$.

Прямой проверкой показывается, что множество классов вычетов кольца R по модулю идеала J образует кольцо относительно операций $+$ и $\cdot$, определяемых равенствами

$$(a + J) + (b + J) = (a + b) + J, \tag{1.2}$$

$$(a + J)(b + J) = ab + J. \tag{1.3}$$

1.36. Определение. Кольцо классов вычетов кольца R по модулю идеала J относительно операций (1.2) и (1.3) называется *факторкольцом* кольца R по идеалу J и обозначается через R/J.

1.37. Пример (факторкольцо $\mathbb{Z}/(n)$) [1]. Как и в случае группы (ср. с определением 1.5), обозначим класс вычетов по модулю n ($n \in \mathbb{N}$), содержащий число $a \in \mathbb{Z}$, через $[a]$; этот класс также может быть записан в виде $a + (n)$, где (n) — главный идеал, порожденный числом n. Элементами кольца $\mathbb{Z}/(n)$ являются

$$[0] = 0 + (n), \quad [1] = 1 + (n), \ldots, [n - 1] = n - 1 + (n). \quad \square$$

1.38. Теорема. *Факторкольцо $\mathbb{Z}/(p)$ кольца $\mathbb{Z}$ целых чисел по главному идеалу, порожденному простым числом p, является полем.*

Доказательство. В силу теоремы 1.31 достаточно показать, что $\mathbb{Z}/(p)$ является целостным кольцом. Ясно, что его единицей является $[1]$ и что равенство $[a][b] = [ab] = [0]$ выполняется в том и только том случае, когда $ab = kp$ для некоторого целого числа k. Но поскольку p — простое число, то оно делит произведение ab тогда и только тогда, когда оно делит по крайней мере один из сомножителей. Следовательно, либо $[a] = [0]$, либо $[b] = [0]$, так что кольцо $\mathbb{Z}/(p)$ не имеет делителей нуля $\square$

1.39. Пример. Пусть $p = 3$. Тогда факторкольцо $\mathbb{Z}/(p)$ состоит из трех элементов $[0]$, $[1]$ и $[2]$. Операции в этом кольце можно задать таблицами (сложения и умножения), аналогичными таблицам Кэли конечных групп (см. пример 1.7):

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Факторкольцо $\mathbb{Z}/(p)$ — наш первый пример *конечного поля*, т. е. поля, содержащего конечное число элементов. Общая теория таких полей будет развита позже.

Следует предостеречь читателя от ошибочного предположения, что при образовании факторкольца обязательно сохраняются все свойства исходного кольца. Так, например, свойство отсут-

[1] Кольца такого вида часто называют *кольцами вычетов*. — *Прим. перев.*

ствия делителей нуля при этом не всегда сохраняется, что видно на примере кольца $\mathbb{Z}/(n)$ при составном натуральном числе n.

Понятие гомоморфизма групп допускает очевидное обобщение на случай колец. Отображение $\varphi\colon R \to S$ кольца R в кольцо S называется *гомоморфизмом*, если для любых $a, b \in R$

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{и} \quad \varphi(ab) = \varphi(a)\,\varphi(b).$$

Таким образом, гомоморфизм $\varphi\colon R \to S$ сохраняет обе операции $+$ и $\cdot$ кольца R и индуцирует гомоморфизм аддитивной группы кольца R в аддитивную группу кольца S. Множество

$$\operatorname{Ker}\varphi = \{a \in R \mid \varphi(a) = 0 \in S\}$$

называется *ядром* гомоморфизма φ. Другие понятия, такие, как изоморфизм и т. п., аналогичны приведенным в определении 1.16. Имеет место также теорема о гомоморфизме, аналогичная теореме 1.23 для групп:

1.40. Теорема (о гомоморфизме колец). *Если φ — гомоморфизм кольца R на кольцо S, то* $\operatorname{Ker}\varphi$ *— идеал кольца R, причем кольцо S изоморфно факторкольцу $R/\operatorname{Ker}\varphi$. Обратно, если J — идеал кольца R, то отображение $\psi\colon R \to R/J$, определяемое условием $\psi(a) = a + J$ для всех $a \in R$, является гомоморфизмом кольца R на R/J с ядром J.*

Отображения могут быть использованы также для перенесения некоторой структуры с алгебраической системы на множество без структуры. Например, пусть R — кольцо, и пусть φ — взаимно однозначное отображение множества R на множество S; тогда с помощью отображения φ можно определить на S кольцевую структуру, которая превращает отображение φ в изоморфизм. Более подробно, пусть s_1 и s_2 — два элемента множества S, а r_1 и r_2 — элементы кольца R, однозначно определяемые условиями $\varphi(r_1) = s_1$ и $\varphi(r_2) = s_2$. Тогда, определив сумму $s_1 + s_2$ как $\varphi(r_1 + r_2)$ и произведение $s_1 s_2$ как $\varphi(r_1 r_2)$, обеспечим выполнение всех нужных свойств. Полученную на S структуру можно назвать кольцевой структурой, *индуцированной отображением* φ. При этом если кольцо R обладает какими-либо дополнительными свойствами, например является целостным кольцом или полем, то эти свойства наследуются и множеством S. Применим этот принцип для получения более удобного представления конечного поля $\mathbb{Z}/(p)$.

1.41. Определение. Для простого числа p обозначим через $\mathbb{F}_p$ множество $\{0, 1, \ldots, p-1\}$ целых чисел, и пусть отображение $\varphi\colon \mathbb{Z}/(p) \to \mathbb{F}_p$ определяется условием $\varphi([a]) = a$ для $a = 0, 1, \ldots, p-1$. Тогда множество $\mathbb{F}_p$ со структурой поля, индуцированной отображением φ, называется *полем Галуа порядка p* (часто оно обозначается также символом $GF(p)$).

В соответствии с ранее сказанным отображение $\varphi\colon \mathbb{Z}/(p) \to \mathbb{F}_p$ является изоморфизмом, так что $\varphi([a]+[b]) = \varphi([a]) + \varphi([b])$ и $\varphi([a][b]) = \varphi([a])\,\varphi([b])$. Нулем конечного поля $\mathbb{F}_p$ будет 0, а единицей является 1, и его структура совпадает со структурой поля $\mathbb{Z}/(p)$. Поэтому при вычислениях с элементами поля $\mathbb{F}_p$ применяется обычная арифметика целых чисел с приведением по модулю p.

1.42. Примеры

(i) Рассмотрим поле $\mathbb{Z}/(5)$, изоморфное полю Галуа $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, с изоморфизмом, задаваемым соответствием $[0] \to 0$, $[1] \to 1$, $[2] \to 2$, $[3] \to 3$, $[4] \to 4$. Таблицы операций $+$ и $\cdot$ поля $\mathbb{F}_5$ имеют вид

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(ii) Столь же прост и даже более важен пример конечного поля $\mathbb{F}_2$ второго порядка. Элементами этого поля являются 0 и 1, и таблицы операций имеют следующий вид:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

В таком контексте элементы 0 и 1 называются *бинарными элементами*.

Если b — произвольный ненулевой элемент кольца $\mathbb{Z}$ целых чисел, то его аддитивный порядок бесконечен, т. е. из $nb = 0$ следует $n = 0$. Однако в факторкольце $\mathbb{Z}/(p)$, где p — простое число, аддитивный порядок каждого ненулевого элемента b равен p, т. е. p — наименьшее натуральное число, для которого выполняется равенство $pb = 0$. Это свойство приводит к следующему важному понятию.

1.43. Определение. Пусть R — произвольное кольцо. Если существует такое натуральное число n, что для каждого $r \in R$ выполняется равенство $nr = 0$, то наименьшее из таких чисел n (скажем, n_0) называется *характеристикой* кольца R, а само R называется кольцом (*положительной*) *характеристики* n_0. Если же таких натуральных чисел n не существует, то R называется кольцом *характеристики* 0.

1.44. Теорема. *Если кольцо $R \neq \{0\}$ с единицей e и без делителей нуля имеет положительную характеристику n, то n — простое число.*

Доказательство. Поскольку кольцо R содержит ненулевой элемент, характеристика n этого кольца больше или равна 2. Если n — составное число, то $n = km$, где $k, m \in \mathbb{Z}$, $1 < k$, $m < n$. Тогда $0 = ne = (km)\,e = (ke)\,(me)$, так что либо $ke = 0$, либо $me = 0$ (поскольку в R нет делителей нуля). Значит, либо $kr = (ke)\,r = 0$ для всех $r \in R$, либо $mr = (me)\,r = 0$ для всех $r \in R$, что противоречит определению характеристики n. □

1.45. Следствие. *Характеристикой конечного поля является простое число.*

Доказательство. Учитывая теорему 1.44, достаточно показать, что любое конечное поле F имеет положительную характеристику. Рассмотрим в поле F элементы e, $2e$, $3e$, ..., кратные единице e. Так как F содержит конечное число различных элементов, то существуют натуральные числа k и m, $1 \leqslant k < m$, такие, что $ke = me$, так что $(m - k)\,e = 0$, и потому F имеет положительную характеристику. □

Конечное поле $\mathbb{Z}/(p)$ (т. е. $\mathbb{F}_p$), очевидно, имеет характеристику p, в то время как кольцо $\mathbb{Z}$ целых чисел и поле $\mathbb{Q}$ рациональных чисел имеют характеристику 0. Заметим, что в кольце R характеристики 2 имеет место равенство $2a = a + a = 0$, откуда следует, что $a = -a$ для всех $a \in R$. Полезно следующее свойство коммутативного кольца простой характеристики.

1.46. Теорема. *Пусть R — коммутативное кольцо простой характеристики p. Тогда*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{и} \quad (a - b)^{p^n} = a^{p^n} - b^{p^n}$$

для всех $a, b \in R$ и $n \in \mathbb{N}$.

Доказательство. Воспользуемся тем фактом, что для всех $k \in \mathbb{N}$, $1 \leqslant k \leqslant p - 1$,

$$\binom{p}{k} = \frac{p\,(p-1)\cdots(p-k+1)}{1\cdot 2\cdot \ldots \cdot k} \equiv 0 \pmod{p}.$$

Это следует из того, что биномиальный коэффициент $\binom{p}{k}$ — целое число и при этом сомножитель p в числителе не может сократиться. Поэтому по формуле бинома (см. упр. 1.8)

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p = a^p + b^p.$$

Теперь индукцией по n устанавливается первое тождество, а из него получаем

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n},$$

откуда следует второе тождество. □

Теперь выясним, каким должен быть идеал M коммутативного кольца R с единицей, чтобы факторкольцо R/M было целостным кольцом или полем. Для этого нам понадобятся некоторые понятия из теории колец.

Пусть R — коммутативное кольцо с единицей. Элемент $a \in R$ называется *делителем* элемента $b \in R$, если существует элемент $c \in R$, такой, что $ac = b$. Делители единицы называются *обратимыми элементами*. Элементы a и b из R называются *ассоциированными*, если существует обратимый элемент $\varepsilon \in R$, такой, что $a = b\varepsilon$. Элемент $c \in R$ называется *простым элементом* кольца R, если он не является обратимым элементом и не имеет других делителей, кроме ассоциированных с ним элементов или обратимых элементов. Идеал $P \neq R$ кольца R называется *простым идеалом*, если для $a, b \in R$ включение $ab \in P$ имеет место лишь в том случае, когда либо $a \in P$, либо $b \in P$. Идеал $M \neq R$ кольца R называется *максимальным идеалом*, если для любого идеала J кольца R включение $M \subseteq J$ влечет за собой $J = M$ или $J = R$. Наконец, кольцо R называется *кольцом главных идеалов*, если оно является целостным кольцом и каждый идеал J кольца R является главным, т. е. существует элемент $a \in R$, такой, что $J = (a) = \{ra \mid r \in R\}$.

1.47. Теорема. *Пусть R — коммутативное кольцо с единицей. Тогда*

(i) *Идеал M кольца R является максимальным тогда и только тогда, когда факторкольцо R/M является полем.*

(ii) *Идеал P кольца R является простым тогда и только тогда, когда факторкольцо R/P является целостным кольцом.*

(iii) *Каждый максимальный идеал кольца R является простым.*

(iv) *Если R — кольцо главных идеалов, то факторкольцо $R/(c)$ является полем в том и только том случае, когда c — простой элемент кольца R.*

Доказательство. (i) Пусть M — максимальный идеал кольца R. Тогда для $a \in R$, $a \notin M$, множество $J = \{ar + m \mid r \in R, m \in M\}$ является идеалом кольца R, содержащим M и отличным от M, так что $J = R$. В частности, существуют такие $r \in R$ и $m \in M$, что $ar + m = 1$, где 1 — мультипликативная единица кольца R. Это означает, что если $a + M \neq 0 + M$, т. е. класс вычетов $a + M$ является ненулевым элементом факторкольца R/M, то он обладает мультипликативным обратным, так как $(a + M)(r + M) = ar + M = (1 - m) + M = 1 + M$. Следо-

вательно, R/M — поле. Обратно, пусть R/M — поле, и пусть J — такой идеал кольца R, что $J \supseteq M$, $J \neq M$. Тогда для $a \in J$, $a \notin M$, класс вычетов $a + M$ имеет мультипликативный обратный, так что $(a + M)(r + M) = 1 + M$ для некоторого $r \in R$. Это означает, что $ar + m = 1$ для некоторого $m \in M$. Поскольку J — идеал, $1 \in J$, а значит, $(1) = R \subseteq J$, откуда $J = R$. Таким образом, M — максимальный идеал кольца R.

(ii) Пусть P — простой идеал кольца R. Тогда факторкольцо R/P является коммутативным кольцом с единицей $1 + P \neq 0 + P$. Пусть $(a + P)(b + P) = 0 + P$; тогда $ab \in P$. Так как P — простой идеал, то либо $a \in P$, либо $b \in P$, т. е. либо $a + P = 0 + P$, либо $b + P = 0 + P$. Таким образом, факторкольцо R/P не имеет делителей нуля и потому является целостным кольцом. Обратное получим сразу же, проведя указанные рассуждения в обратном порядке.

(iii) Это утверждение следует из (i) и (ii), так как каждое поле является целостным кольцом.

(iv) Пусть $c \in R$. Если c — обратимый элемент, то $(c) = R$ и факторкольцо $R/(c)$ состоит из единственного элемента, так что оно не может быть полем. Если c не обратимый и не простой элемент, то c обладает некоторым делителем $a \in R$, который не является ассоциированным с c и не является обратимым элементом. Заметим, что $a \neq 0$, так как если $a = 0$, то $c = 0$ и a был бы ассоциирован с c. Пусть $c = ab$, где $b \in R$. Мы утверждаем, что $a \notin (c)$. Действительно, в противном случае $a = cd = abd$, где $d \in R$, т. е. $a(1 - bd) = 0$. Так как $a \neq 0$, то $bd = 1$, значит, b — обратимый элемент, а это противоречит тому, что a не ассоциирован с c. Следовательно, $(c) \subseteq (a) \subseteq (R)$, где все включения собственные, так что факторкольцо $R/(c)$ не может быть полем ввиду (i). Итак, остается последний случай, когда c — простой элемент кольца R. Тогда $(c) \neq R$, так как c не является обратимым элементом. Далее, если $J \supseteq (c)$ — идеал кольца R, то $J = (a)$ для некоторого $a \in R$, поскольку R — кольцо главных идеалов. Следовательно, $c \in (a)$, так что a — делитель элемента c. Поэтому a — либо обратимый элемент, либо ассоциирован с c, так что либо $J = R$, либо $J = (c)$. Это показывает, что (c) — максимальный идеал кольца R. Отсюда следует в силу (i), что факторкольцо $R/(c)$ является полем. □

В качестве приложения этой теоремы рассмотрим случай $R = \mathbb{Z}$. Заметим, что $\mathbb{Z}$ — кольцо главных идеалов, так как в силу теоремы 1.15(i) любая аддитивная подгруппа $\mathbb{Z}$ порождается единственным элементом. Простое число p подходит под определение простого элемента, и, таким образом, из теоремы 1.47(iv) вытекает другое доказательство того известного факта, что факторкольцо $\mathbb{Z}/(p)$ является полем. Отсюда следует, что

(p) — максимальный и одновременно простой идеал кольца $\mathbb{Z}$. Для составного натурального числа n идеал (n) не является простым в $\mathbb{Z}$, и потому факторкольцо $\mathbb{Z}/(n)$ не является даже целостным кольцом. Другие приложения будут приведены в следующем параграфе, когда мы будем рассматривать факторкольца колец многочленов над полями.

§ 3. Многочлены

В элементарной алгебре рассматриваются выражения вида $a_0 + a_1x + \ldots + a_nx^n$, называемые многочленами (или полиномами). Здесь a_i называются коэффициентами многочлена и обычно являются действительными или комплексными числами, а x рассматривается как переменная, т. е., подставляя вместо x произвольное число α, получаем определенное число $a_0 + a_1\alpha + \ldots + a_n\alpha^n$, называемое *значением многочлена* при $x = \alpha$. Арифметика многочленов регулируется обычными правилами. Понятие многочлена и связанных с ним операций можно обобщить на формальную алгебраическую ситуацию следующим образом.

Пусть R — произвольное кольцо. *Многочленом* (или *полиномом*) над R называется выражение вида

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1x + \cdots + a_nx^n,$$

где n — неотрицательное целое число, коэффициенты a_i, $0 \leqslant i \leqslant n$, — элементы кольца R, а x — некоторый символ, не принадлежащий кольцу R, называемый *переменной* (или *неизвестной*) над R. В тех случаях, когда из контекста ясно, какая переменная имеется в виду, мы для обозначения многочлена $f(x)$ будем использовать символ f. Для удобства будем считать, что член a_ix^i с $a_i = 0$ не обязательно выписывать. В частности, выписанный выше многочлен $f(x)$ можно записать в эквивалентной форме $f(x) = a_0 + a_1x + \ldots + a_nx^n + 0x^{n+1} + \ldots + 0x^{n+h}$, где h — любое натуральное число. Поэтому при сравнении двух многочленов $f(x)$ и $g(x)$ над R можно предполагать, что оба они содержат одни и те же степени переменной x. Многочлены

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{и} \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

над R считаются равными тогда и только тогда, когда $a_i = b_i$ для $0 \leqslant i \leqslant n$. Определим *сумму* многочленов $f(x)$ и $g(x)$ равенством

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

а *произведение* многочленов

$$f(x) = \sum_{i=0}^{m} a_i x^i \quad \text{и} \quad g(x) = \sum_{j=0}^{n} b_j x^j$$

равенством

$$f(x)\,g(x) = \sum_{k=0}^{m+n} c_k x_k, \quad \text{где} \quad c_k = \sum_{\substack{i+j=k \\ 0 \leqslant i \leqslant m,\ 0 \leqslant j \leqslant n}} a_i b_j.$$

Легко видеть, что множество многочленов с такими операциями образует кольцо.

1.48. Определение. Кольцо, образованное многочленами над кольцом R с введенными выше операциями, называется *кольцом многочленов* над R и обозначается через $R[x]$.

Нулевым элементом кольца $R[x]$ является многочлен, все коэффициенты которого равны 0. Он называется *нулевым многочленом* и обозначается через 0. Из контекста всегда будет ясно, обозначает ли символ 0 нулевой элемент кольца R или нулевой многочлен.

1.49. Определение. Пусть $f(x) = \sum_{i=0}^{n} a_i x^i$ — многочлен над кольцом R, не являющийся нулевым. Значит, можно предположить, что $a_n \neq 0$. Тогда a_n называется *старшим коэффициентом* многочлена $f(x)$, a_0 — его *постоянным членом* и n — его *степенью* (последняя обозначается символом $n = \deg(f(x)) = \deg(f)$). Для удобства будем считать, что $\deg(0) = -\infty$. Многочлены степени $\leqslant 0$ называются *постоянными многочленами* (или *константами*). Если кольцо R имеет единицу 1 и если старший коэффициент многочлена $f(x)$ равен 1, то многочлен $f(x)$ называется *нормированным* (его называют также *приведенным* или *унитарным*).

Подсчет старших коэффициентов суммы и произведения двух многочленов приводит к следующему результату.

1.50. Теорема. *Пусть* $f, g \in R[x]$. *Тогда*

$$\deg(f+g) \leqslant \max(\deg(f), \deg(g)),$$

$$\deg(fg) \leqslant \deg(f) + \deg(g).$$

Если R *— целостное кольцо, то*

$$\deg(fg) = \deg(f) + \deg(g). \tag{1.4}$$

Если отождествить постоянные многочлены с элементами кольца R, то R можно рассматривать как подкольцо кольца $R[x]$. Некоторые свойства кольца R наследуются кольцом $R[x]$. В сле-

дующей теореме доказательство части (iii) опирается на равенство (1.4).

1.51. Теорема. *Пусть R — кольцо. Тогда*

(i) *$R[x]$ является коммутативным кольцом в том и только том случае, если кольцо R коммутативно.*

(ii) *$R[x]$ является кольцом с единицей тогда и только тогда, когда R — кольцо с единицей.*

(iii) *$R[x]$ является целостным кольцом тогда и только тогда, когда R — целостное кольцо.*

В последующих главах мы почти всегда будем иметь дело с многочленами над полями. Пусть F обозначает поле (не обязательно конечное). Понятие делимости применительно к кольцу $F[x]$ вводится следующим образом. Будем говорить, что многочлен $g \in F[x]$ *делит* многочлен $f \in F[x]$, если существует многочлен $h \in F[x]$, такой, что $f = gh$. В этом случае будем также говорить, что g — *делитель* многочлена f, а многочлен f *делится* на g (или *кратен* g). Обратимыми элементами в кольце $F[x]$ являются делители постоянного многочлена 1, а следовательно, ими являются все ненулевые постоянные многочлены и только они.

Как и в кольце целых чисел, в кольце многочленов над полем существует деление с остатком.

1.52. Теорема (алгоритм деления). *Пусть $g \neq 0$ — многочлен из $F[x]$, где F — поле. Тогда для каждого $f \in F[x]$ существуют такие многочлены q, $r \in F[x]$, что*

$$f = qg + r, \text{ где } \deg(r) < \deg(g).$$

1.53. Пример. Рассмотрим многочлены $f(x) = 2x^5 + x^4 + 4x + 3$ и $g(x) = 3x^2 + 1$ из кольца $\mathbb{F}_5[x]$. Вычислим многочлены q, $r \in \mathbb{F}_5[x]$ из теоремы 1.52, используя обычное *деление углом*:

$$\begin{array}{r|l}
2x^5 + x^4 + 4x + 3 & 3x^2 + 1 \\
\cline{2-2}
-\,(2x^5 + 4x^3) & 4x^3 + 2x^2 + 2x + 1 \\
\cline{1-1}
x^4 + x^3 + 4x + 3 & \\
-\,(x^4 + 2x^2) & \\
\cline{1-1}
x^3 + 3x^2 + 4x + 3 & \\
-\,(x^3 + 2x) & \\
\cline{1-1}
3x^2 + 2x + 3 & \\
-\,(3x^2 + 1) & \\
\cline{1-1}
2x + 2 &
\end{array}$$

Таким образом, $q(x) = 4x^3 + 2x^2 + 2x + 1$, $r(x) = 2x + 2$, и, очевидно, $\deg(r) < \deg(g)$. □

Тот факт, что кольцо $F[x]$ допускает алгоритм деления, приводит (стандартным рассуждением) к тому, что каждый идеал кольца $F[x]$ главный.

1.54. Теорема. *Кольцо $F[x]$ многочленов над полем F является кольцом главных идеалов. Другими словами, для каждого идеала $J \neq (0)$ кольца $F[x]$ найдется однозначно определенный нормированный многочлен $g \in F[x]$, такой, что $J = (g)$.*

Доказательство. Согласно теореме 1.51(iii), $F[x]$ является целостным кольцом. Пусть $J \neq (0)$ — идеал кольца $F[x]$. Пусть, далее, $h(x)$ — ненулевой многочлен наименьшей степени, содержащийся в J, b — старший коэффициент многочлена $h(x)$ и $g(x) = b^{-1}h(x)$. Тогда g — нормированный многочлен, содержащийся в J. Если f — произвольный многочлен из J, то, применяя алгоритм деления, найдем q, $r \in F[x]$, такие, что $f = qg + r$ и $\deg(r) < \deg(g) = \deg(h)$. Так как J — идеал, то $r = f - qg \in J$, и по определению h должно быть $r = 0$. Поэтому многочлен f делится на g, так что $J = (g)$. Если $g_1 \in F[x]$ — другой нормированный многочлен, такой, что $J = (g_1)$, то $g = c_1g_1$ и $g_1 = c_2g$, где $c_1, c_2 \in F[x]$. Отсюда $g = c_1c_2g$, так что $c_1c_2 = 1$, т. е. c_1 и c_2 — постоянные многочлены. Поскольку оба многочлена g и g_1 нормированы, то $g_1 = g$, и единственность g установлена. □

1.55. Теорема. *Пусть $f_1, \ldots, f_n$ — многочлены из $F[x]$, не все равные 0. Тогда существует однозначно определенный нормированный многочлен $d \in F[x]$, обладающий следующими свойствами:*

(i) *d делит каждый многочлен f_i, $1 \leqslant i \leqslant n$;*

(ii) *любой многочлен $g \in F[x]$, который делит каждый из многочленов f_i, $1 \leqslant i \leqslant n$, делит и многочлен d.*

Более того, многочлен d может быть представлен в виде

$$d = b_1f_1 + \ldots + b_nf_n, \quad \text{где} \quad b_1, \ldots, b_n \in F[x]. \qquad (1.5)$$

Доказательство. Множество J, состоящее из всех многочленов вида $c_1f_1 + \ldots + c_nf_n$, где $c_1, \ldots, c_n \in F[x]$, является, как легко убедиться, идеалом кольца $F[x]$. Поскольку не все f_i равны нулю, $J \neq (0)$, и по теореме 1.54 получаем, что $J = (d)$ для некоторого нормированного многочлена $d \in F[x]$. Свойство (i) и представление (1.5) сразу вытекают из определения многочлена d. Свойство (ii) следует из (1.5). Если d_1 — другой нормированный многочлен из $F[x]$, удовлетворяющий (i) и (ii), то из этих свойств получим, что многочлены d_1 и d делят друг друга, так что $(d) = (d_1)$. Поэтому в силу единственности, доказанной в теореме 1.54, $d_1 = d$. □

Нормированный многочлен d, появляющийся в теореме 1.55, называется *наибольшим общим делителем* многочленов $f_1, \ldots, f_n$ и обозначается НОД $(f_1, \ldots, f_n)$. Если НОД $(f_1, \ldots, f_n) = 1$, то

многочлены $f_1, \ldots, f_n$ называются *взаимно простыми*. Они называются *попарно взаимно простыми*, если НОД $(f_i, f_j) = 1$ для $1 \leqslant i < j \leqslant n$.

Наибольший общий делитель двух многочленов f и g из $F[x]$ можно найти при помощи *алгоритма Евклида*. Предположим без ограничения общности, что многочлен g отличен от нуля и не делит многочлен f. Тогда, применяя многократно алгоритм деления, получим

$$\begin{aligned}
f &= q_1 g + r_1, && 0 \leqslant \deg(r_1) < \deg(g),\\
g &= q_2 r_1 + r_2, && 0 \leqslant \deg(r_2) < \deg(r_1),\\
r_1 &= q_3 r_2 + r_3, && 0 \leqslant \deg(r_3) < \deg(r_2),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{s-2} &= q_s r_{s-1} + r_s, && 0 \leqslant \deg(r_s) < \deg(r_{s-1}),\\
r_{s-1} &= q_{s+1} r_s.
\end{aligned}$$

Здесь $q_1, \ldots, q_{s+1}$ и $r_1, \ldots, r_s$ — многочлены из $F[x]$. Так как степень $\deg(g)$ конечна, то процедура должна закончиться после конечного числа шагов. Если старший коэффициент последнего ненулевого остатка r_s равен b, то НОД $(f, g) = b^{-1} r_s$.

Для нахождения НОД $(f_1, \ldots, f_n)$ при $n > 2$ и при ненулевых многочленах f_i сначала определяют НОД (f_1, f_2), а затем последовательно находят, применяя алгоритм Евклида, НОД (НОД $(f_1, f_2), f_3)$ = НОД (f_1, f_2, f_3) и т. д.

1.56. Пример. Применяя алгоритм Евклида к многочленам $f(x) = 2x^6 + x^3 + x^2 + 2$ и $g(x) = x^4 + x^2 + 2x$ из $\mathbb{F}_3[x]$, получаем

$$\begin{aligned}
2x^6 + x^3 + x^2 + 2 &= (2x^2 + 1)(x^4 + x^2 + 2x) + x + 2,\\
x^4 + x^2 + 2x &= (x^3 + x^2 + 2x + 1)(x + 2) + 1,\\
x + 2 &= (x + 2)\,1.
\end{aligned}$$

Следовательно, НОД $(f, g) = 1$, т. е. многочлены f и g взаимно просты. □

Двойственным к понятию наибольшего общего делителя является понятие наименьшего общего кратного. Пусть $f_1, \ldots, f_n$ — ненулевые многочлены из $F[x]$. Тогда можно показать (см. упр. 1.25), что существует однозначно определенный нормированный многочлен $m \in F[x]$, обладающий следующими свойствами: (i) m делится на каждый многочлен f_i, $1 \leqslant i \leqslant n$; (ii) любой многочлен $g \in F[x]$, который делится на каждый из многочленов f_i, $1 \leqslant i \leqslant n$, делится на m. Многочлен m называется *наименьшим общим кратным* многочленов $f_1, \ldots, f_n$ и обозначается

НОК $(f_1, \ldots, f_n)$. Для двух ненулевых многочленов $f, g \in F[x]$ имеет место соотношение

$$a^{-1}fg = \text{НОД}(f, g)\,\text{НОК}(f, g), \tag{1.6}$$

где a — старший коэффициент произведения fg. Это соотношение легко сводит вычисление НОК (f, g) к вычислению НОД (f, g). Однако для трех и более многочленов прямого аналога формулы (1.6) не существует. В этом случае для нахождения наименьшего общего кратного применяется тождество

$$\text{НОК}(f_1, \ldots, f_n) = \text{НОК}(\text{НОК}(f_1, \ldots, f_{n-1}), f_n).$$

Простые элементы кольца $F[x]$ обычно называются *неприводимыми многочленами*. Ввиду особой важности этого понятия дадим еще одно его определение.

1.57. Определение. Многочлен $f \in F[x]$ называется *неприводимым* (точнее, неприводимым *над полем* F или *в кольце* $F[x]$), если он имеет положительную степень и равенство $f = gh$, $g, h \in F[x]$, может выполняться лишь в том случае, когда либо g, либо h является постоянным многочленом.

Короче говоря, многочлен положительной степени неприводим над F, если он допускает лишь тривиальные разложения на множители. Многочлен положительной степени из $F[x]$, не являющийся неприводимым над F, называется *приводимым над* F. Приводимость или неприводимость данного многочлена существенно зависит от того, над каким полем он рассматривается. Например, многочлен $x^2 - 2 \in \mathbb{Q}[x]$ неприводим над полем $\mathbb{Q}$ рациональных чисел, но приводим над полем $\mathbb{R}$ действительных чисел, так как $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Неприводимые многочлены играют важную роль в устройстве кольца $F[x]$, поскольку каждый многочлен из $F[x]$ может быть записан и притом единственным способом в виде произведения неприводимых многочленов. Для доказательства этого предложения нам понадобится следующий результат.

1.58. Лемма. *Если неприводимый многочлен f из $F[x]$ делит произведение $f_1 \ldots f_m$ многочленов из $F[x]$, то по крайней мере один из сомножителей f_j делится на f.*

Доказательство. Так как многочлен f делит произведение $f_1 \ldots f_m$, то в факторкольце $F[x]/(f)$ мы получаем равенство $(f_1 + (f)) \ldots (f_m + (f)) = 0 + (f)$. Поскольку на основании теоремы 1.47(iv) это факторкольцо является полем, то для некоторого j, $1 \leqslant j \leqslant m$, должно выполняться равенство $f_j + (f) = 0 + (f)$, а это означает, что многочлен f делит f_j. □

1.59. Теорема (об однозначном разложении на множители). *Каждый многочлен положительной степени $f \in F[x]$ (где F — поле) может быть представлен в виде произведения*

$$f = af_1^{e_1} \dots f_k^{e_k}, \tag{1.7}$$

где $a \in F$, $f_1, \dots, f_k$ — различные нормированные неприводимые многочлены из $F[x]$, а $e_1, \dots, e_k$ — натуральные числа. Более того, это разложение однозначно с точностью до порядка, в котором расположены сомножители.

Доказательство. Возможность представления любого непостоянного многочлена $f \in F[x]$ в виде (1.7) доказывается индукцией по степени многочлена f. Случай $\deg(f) = 1$ тривиален, так как любой многочлен первой степени неприводим над F. Предположим теперь, что требуемое разложение установлено для всех непостоянных многочленов из $F[x]$ степени $< n$. Если $\deg(f) = n$ и f неприводим над F, то $f = a(a^{-1}f)$, где a — старший коэффициент f, — требуемое представление, так как $a^{-1}f$ — нормированный неприводимый многочлен из $F[x]$. Если же f приводим, то он допускает разложение $f = gh$, где $g, h \in F[x]$, $1 \leqslant \deg(g) < n$, $1 \leqslant \deg(h) < n$. По предположению индукции можно g и h представить в виде (1.7), а следовательно, можно в таком виде представить и f.

Для доказательства единственности предположим, что f имеет два разложения вида (1.7):

$$f = af_1^{e_1} \dots f_k^{e_k} = bg_1^{d_1} \dots g_r^{d_r}. \tag{1.8}$$

Сравнение старших коэффициентов дает $a = b$. Далее, неприводимый многочлен f_1 из $F[x]$ делит правую часть равенства (1.8), и потому (ввиду леммы 1.58) он делит один из многочленов g_j, $1 \leqslant j \leqslant r$. Но многочлен g_j тоже неприводим в кольце $F[x]$, так что $g_j = cf_1$, где c — постоянный многочлен. Так как g_j и f_1 оба нормированы, то $g_j = f_1$. Таким образом, мы можем в равенстве (1.8) сократить f_1 и g_j и к полученному равенству применить тот же прием. После конечного числа таких шагов мы убедимся, что оба разложения в (1.8) совпадают с точностью до порядка сомножителей. □

Разложение (1.7) будем называть *каноническим разложением* многочлена f в кольце $F[x]$. Если поле F совпадает с полем $\mathbb{Q}$ рациональных чисел, то существует метод Кронекера, позволяющий найти каноническое разложение за конечное число шагов. Этот метод вкратце описан в упр. 1.30. Для многочленов над конечными полями алгоритмы разложения будут описаны в гл. 4.

Основным вопросом для многочленов из $F[x]$ является вопрос о том, приводим или неприводим данный многочлен над полем F.

Для наших целей особенно интересны многочлены, неприводимые над простым полем $\mathbb{F}_p$. Чтобы найти все неприводимые нормированные многочлены данной степени n над полем $\mathbb{F}_p$, можно сначала найти все приводимые нормированные многочлены степени n над этим полем, а затем исключить их из множества всех нормированных многочленов степени n над $\mathbb{F}_p$. Однако, если числа p или n велики, такой метод непригоден, и мы в § 2, 3 гл. 3 разовьем более мощные методы.

1.60. Пример. Найдем все неприводимые многочлены степени 4 над полем $\mathbb{F}_2$ (заметим, что каждый ненулевой многочлен из $\mathbb{F}_2[x]$ автоматически нормирован). Всего существует $2^4 = 16$ многочленов 4-й степени над $\mathbb{F}_2$. Такой многочлен приводим тогда и только тогда, когда он имеет делитель 1-й или 2-й степени. Найдем поэтому все произведения вида $(a_0 + a_1x + a_2x^2 + x^3)(b_0 + x)$ и $(a_0 + a_1x + x^2)(b_0 + b_1x + x^2)$, где $a_i, b_j \in \mathbb{F}_2$, — это и будут все приводимые многочлены 4-й степени из $\mathbb{F}_2[x]$. Исключив их из полного набора многочленов 4-й степени над $\mathbb{F}_2$, получим искомые неприводимые многочлены: $f_1(x) = x^4 + x + 1$, $f_2(x) = x^4 + x^3 + 1$ и $f_3(x) = x^4 + x^3 + x^2 + x + 1$. □

Поскольку именно неприводимые многочлены над полем F являются простыми элементами кольца $F[x]$, следующий результат (одна часть которого уже была использована в лемме 1.58) непосредственно вытекает из теорем 1.47(iv) и 1.54.

1.61. Теорема. *Пусть $f \in F[x]$. Для того чтобы факторкольцо $F[x]/(f)$ было полем, необходимо и достаточно, чтобы многочлен f был неприводим над полем F.*

С целью подготовки к следующему параграфу мы остановимся подробнее на строении факторкольца $F[x]/(f)$, где f — произвольный ненулевой многочлен из $F[x]$. Это факторкольцо состоит из классов вычетов $[g] = g + (f)$, где $g \in F[x]$, а операции вводятся формулами (1.2) и (1.3). Два класса вычетов $g + (f)$ и $h + (f)$ совпадают в том и только том случае, когда $g \equiv h \pmod f$, т. е. когда многочлен $g - h$ делится на f. Это равносильно требованию, чтобы g и h давали один и тот же остаток при делении на f. В классе вычетов $g + (f)$ содержится единственный многочлен $r \in F[x]$, для которого $\deg(r) < \deg(f)$; этот многочлен просто является остатком при делении g на f. Процесс перехода от g к r называется *приведением по модулю* f. Единственность многочлена r вытекает из того, что если существует многочлен $r_1 \in g + (f)$, такой, что $\deg(r_1) < \deg(f)$, то разность $r - r_1$ должна делиться на f, но поскольку $\deg(r - r_1) < \deg(f)$, то это возможно лишь при $r_1 = r$. Различные элементы, образующие факторкольцо $F[x]/(f)$, можно теперь описать явно: а именно это классы вычетов $r + (f)$, где r пробегает все многочлены из $F[x]$

степени, меньшей чем $\deg(f)$. Таким образом, если $F = \mathbb{F}_p$ и $\deg(f) = n \geqslant 0$, то число элементов факторкольца $\mathbb{F}_p[x]/(f)$ равно числу многочленов степени, меньшей n, в кольце $\mathbb{F}_p[x]$, т. е. p^n.

1.62. Примеры

(i) Пусть $f(x) = x \in \mathbb{F}_2[x]$. В этом случае $p^n = 2^1$ многочленов степени, меньшей 1, из $\mathbb{F}_2[x]$ определяют полный набор классов вычетов, составляющих факторкольцо $\mathbb{F}_2[x]/(x)$, так что это факторкольцо состоит из классов вычетов $[0]$ и $[1]$ и, следовательно, изоморфно полю $\mathbb{F}_2$.

(ii) Пусть $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. В этом случае факторкольцо $\mathbb{F}_2[x]/(f)$ состоит из $p^n = 2^2$ элементов $[0]$, $[1]$, $[x]$, $[x+1]$. Для построения таблиц сложения и умножения этого факторкольца нужно произвести требуемые операции над многочленами, определяющими соответствующие классы вычетов, а затем, если нужно, привести результаты по модулю f. Мы получаем следующие таблицы:

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

Из этих таблиц видно, что факторкольцо $\mathbb{F}_2[x]/(f)$ является полем (это следует также из неприводимости многочлена $f(x) = x^2 + x + 1$ над полем $\mathbb{F}_2$ на основании теоремы 1.61). Это наш первый пример конечного поля, число элементов которого не является простым числом.

(iii) Пусть $f(x) = x^2 + 2 \in \mathbb{F}_3[x]$. Тогда факторкольцо $\mathbb{F}_3[x]/(f)$ состоит из $p^n = 3^2$ классов вычетов $[0]$, $[1]$, $[2]$, $[x]$, $[x+1]$, $[x+2]$, $[2x]$, $[2x+1]$, $[2x+2]$. Таблицы операций факторкольца $\mathbb{F}_3[x]/(f)$ опять можно получить, производя соответствующие операции над определяющими классы вычетов многочленами с последующим приведением по модулю f (когда это нужно). Поскольку $\mathbb{F}_3[x]/(f)$ — коммутативное кольцо, достаточно найти лишь элементы таблиц операций, стоящие на главной диагонали и над нею.

+	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[0]	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[1]		[2]	[0]	[x+1]	[x+2]	[x]	[2x+1]	[2x+2]	[2x]
[2]			[1]	[x+2]	[x]	[x+1]	[2x+2]	[2x]	[2x+1]
[x]				[2x]	[2x+1]	[2x+2]	[0]	[1]	[2]
[x+1]					[2x+2]	[2x]	[1]	[2]	[0]
[x+2]						[2x+1]	[2]	[0]	[1]
[2x]							[x]	[x+1]	[x+2]
[2x+1]								[x+2]	[x]
[2x+2]									[x+1]

	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]		[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[2]			[1]	[2x]	[2x+2]	[2x+1]	[x]	[x+2]	[x+1]
[x]				[1]	[x+1]	[2x+1]	[2]	[x+2]	[2x+2]
[x+1]					[2x+2]	[0]	[2x+2]	[0]	[x+1]
[x+2]						[x+2]	[x+2]	[2x+1]	[0]
[2x]							[1]	[2x+1]	[x+1]
[2x+1]								[x+2]	[0]
[2x+2]									[2x+2]

Заметим, что факторкольцо $\mathbb{F}_3[x]/(f)$ не является полем (и даже не является целостным кольцом). Это соответствует и теореме 1.61, поскольку $f(x) = x^2 + 2 = (x+1)(x+2)$ приводим над $\mathbb{F}_3$. □

Пусть снова F — произвольное поле и $f(x) \in F[x]$. Тогда замена переменной x в многочлене $f(x)$ произвольным элементом поля F обращает этот многочлен в корректно определенный элемент поля F. Точнее, если $f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$ и $b \in F$, то, заменяя x на b, получаем элемент $f(b) = a_0 + a_1b + \ldots + a_nb^n \in F$. Будем его называть *значением многочлена $f(x)$ при $x = b$*. Если в кольце $F[x]$ имеется какое-либо (полиномиальное) равенство, то, заменяя в нем x произвольным фиксированным элементом $b \in F$, мы получаем равенство в поле F (*принцип подстановки*).

1.63. Определение. Элемент $b \in F$ называется *корнем* (или *нулем*) многочлена $f \in F[x]$, если $f(b) = 0$.

Следующая теорема устанавливает важную связь между корнями и делимостью.

1.64. Теорема. *Элемент $b \in F$ является корнем многочлена $f \in F[x]$ в том и только том случае, когда многочлен $x - b$ делит f.*

Доказательство. Применяя алгоритм деления (см. теорему 1.52), можно написать $f(x) = q(x)(x - b) + c$, где $q \in F[x]$, $c \in F$.

Подставляя элемент b вместо переменной x, получим $f(b) = c$, откуда $f(x) = q(x)(x - b) + f(b)$. Из этого равенства легко следует доказываемая теорема. □

1.65. Определение. Пусть $b \in F$ — корень многочлена $f \in F[x]$. *Кратностью* корня b называется такое натуральное число k, что $f(x)$ делится на $(x - b)^k$, но не делится на $(x - b)^{k+1}$. При $k = 1$ корень b называется *простым*, а при $k > 1$ — *кратным*.

1.66. Теорема. *Пусть* $f \in F(x)$ *и* $\deg(f) = n \geqslant 0$. *Если* $b_1, \ldots, b_m \in F$ *— различные корни многочлена* f *соответственно кратностей* $k_1, \ldots, k_m$, *то* f *делится на произведение* $(x - b_1)^{k_1} \ldots (x - b_m)^{k_m}$. *Следовательно,* $k_1 + \ldots + k_m \leqslant n$ *и многочлен* f *может иметь не более* n *различных корней в поле* F.

Доказательство. Заметим, что каждый многочлен $x - b_j$, $1 \leqslant j \leqslant m$, неприводим над F, так что $(x - b_j)^{k_j}$ входит в качестве сомножителя в каноническое разложение многочлена f. Таким образом, в это каноническое разложение входит произведение $(x - b_1)^{k_1} \ldots (x - b_m)^{k_m}$, и, следовательно, оно является делителем многочлена f. Сравнивая степени, получаем, что $k_1 + \ldots + k_m \leqslant n$, и неравенства $m \leqslant k_1 + \ldots + k_m \leqslant n$ доказывают последнее утверждение. □

1.67. Определение. *Производной* многочлена $f = f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in F[x]$ называется многочлен $f' = f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1} \in F[x]$.

1.68. Теорема. *Корень* $b \in F$ *многочлена* $f \in F[x]$ *является кратным тогда и только тогда, когда он одновременно является и корнем производной* f' *многочлена* f.

Существует связь между несуществованием корней и неприводимостью. Если f — неприводимый многочлен из $F[x]$ степени $\geqslant 2$, то, согласно теореме 1.64, он не имеет корней в поле F. Обратное справедливо для многочленов степеней 2 и 3, но вовсе не обязательно для многочленов более высокой степени.

1.69. Теорема. *Для неприводимости многочлена* $f \in F[x]$ *степени* 2 *или* 3 *в кольце* $F[x]$ *необходимо и достаточно, чтобы он не имел корней в поле* F.

Доказательство. Необходимость этого условия уже отмечалась выше. С другой стороны, если многочлен f не имеет корней в поле F, но приводим в кольце $F[x]$, то его можно записать в виде $f = gh$, где $g, h \in F[x]$ и $1 \leqslant \deg(g) \leqslant \deg(h)$. Но $\deg(g) + \deg(h) = \deg(f) \leqslant 3$, откуда $\deg(g) = 1$. Значит, $g(x) = ax + b$, где $a, b \in F$, $a \neq 0$. Но тогда элемент $-ba^{-1}$ является

корнем многочлена g, а значит, и многочлена f в F, что противоречит предположению. □

1.70. Пример. Пользуясь теоремой 1.69, можно найти неприводимые многочлены степеней 2 и 3 в кольце $\mathbb{F}_2[x]$, исключая из полной совокупности многочленов соответствующей степени, принадлежащих данному кольцу, те многочлены, которые имеют корни в поле $\mathbb{F}_2$. Этим путем легко убедиться, что в кольце $\mathbb{F}_2[x]$ имеется всего один неприводимый многочлен степени 2, а именно $f(x) = x^2 + x + 1$, и два неприводимых многочлена степени 3: $f_1(x) = x^3 + x + 1$ и $f_2(x) = x^3 + x^2 + 1$. □

В математическом анализе хорошо известен метод построения многочлена с действительными коэффициентами по его значениям в заданных точках. Этот метод применим и к многочленам над произвольным полем.

1.71. Теорема (интерполяционная формула Лагранжа). *Пусть $n \geqslant 0$, и пусть $a_0, a_1, \ldots, a_n$ — различные и $b_0, b_1, \ldots, b_n$ — произвольные элементы поля F. Тогда существует в точности один многочлен $f \in F[x]$ степени $\leqslant n$, такой, что $f(a_i) = b_i$ для $i = 0, 1, \ldots, n$. Этот многочлен имеет вид*

$$f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} (a_i - a_k)^{-1}(x - a_k).$$

Можно рассматривать также многочлены от нескольких переменных. Пусть R обозначает коммутативное кольцо с единицей, и пусть $x_1, \ldots, x_n$ — символы, которые выступают в качестве переменных. Образуем сначала кольцо многочленов $R[x_1]$, затем кольцо многочленов $R[x_1, x_2] = R[x_1][x_2]$ и т. д., пока не достигнем $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. Элементами кольца $R[x_1, \ldots, x_n]$ являются выражения вида

$$f = f(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$$

с коэффициентами $a_{i_1 \ldots i_n} \in R$, причем суммирование распространяется на конечное множество n-наборов $(i_1, \ldots, i_n)$ неотрицательных целых чисел и соблюдается соглашение $x_j^0 = 1$, $1 \leqslant j \leqslant n$. Такое выражение называется *многочленом от переменных* $x_1, \ldots, x_n$ над кольцом R. Два многочлена f и g из $R[x_1, \ldots, x_n]$ *равны* тогда и только тогда, когда равны все соответствующие коэффициенты. При этом предполагается, что переменные $x_1, \ldots, x_n$ коммутируют (т. е. перестановочны) друг с другом, так что, например, выражения $x_1x_2x_3x_4$ и $x_4x_1x_3x_2$ отождествляются.

1.72. Определение. Пусть многочлен $f \in R[x_1, \ldots, x_n]$ задан выражением

$$f(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}.$$

Если $a_{i_1 \ldots i_n} \neq 0$, то $a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ называется *членом* многочлена f, а $i_1 + \ldots + i_n$ — *степенью* этого члена. *Степень* многочлена $f \neq 0$ (обозначаемая через $\deg(f)$) определяется как наибольшая из степеней его членов. Для $f = 0$ полагается $\deg(f) = -\infty$. Если $f = 0$ или все члены f имеют одну и ту же степень, то многочлен f называется *однородным*.

Любой многочлен $f \in R[x_1, \ldots, x_n]$ можно записать в виде конечной суммы однородных многочленов. Степени многочленов из $R[x_1, \ldots, x_n]$ снова удовлетворяют неравенствам теоремы 1.50, а если R — целостное кольцо, то справедливо равенство (1.4), так что $R[x_1, \ldots, x_n]$ тоже является целостным кольцом. Если F — поле, то каждый многочлен положительной степени из $F[x_1, \ldots, x_n]$ снова может быть единственным образом представлен в виде произведения постоянного сомножителя и нормированных простых элементов кольца $F[x_1, \ldots, x_n]$ (где нормированность определяется подходящим образом). Однако здесь при $n \geqslant 2$ не существует аналога для алгоритма деления, и $F[x_1, \ldots, x_n]$ не является кольцом главных идеалов.

Важным классом многочленов от n переменных являются симметрические многочлены.

1.73. Определение. Многочлен $f \in R[x_1, \ldots, x_n]$ называется *симметрическим*, если для любой перестановки $i_1, \ldots, i_n$ целых чисел $1, \ldots, n$ выполняется равенство $f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n)$.

1.74. Пример. Пусть z — переменная над кольцом $R[x_1, \ldots, x_n]$, и пусть $g(z) = (z - x_1)(z - x_2) \ldots (z - x_n)$. Тогда

$$g(z) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n \sigma_n,$$

где

$$\sigma_k = \sigma_k(x_1, \ldots, x_n) = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} x_{i_1} \ldots x_{i_k} \quad (k = 1, 2, \ldots, n).$$

Таким образом,

$$\sigma_1 = x_1 + x_2 + \cdots + x_n,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \ldots + x_2x_n + \ldots + x_{n-1}x_n,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\sigma_n = x_1x_2 \ldots x_n.$$

Поскольку многочлен g остается неизменным при любой перестановке переменных $x_1, x_2, \ldots, x_n$, то все σ_k являются симметрическими многочленами от этих переменных и каждый из них однороден. Многочлен $\sigma_k = \sigma_k(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ называется *k-м элементарным симметрическим многочленом* от переменных $x_1, \ldots, x_n$ над R. Прилагательное «элементарные» применяется ввиду так называемой основной теоремы о симметрических многочленах, гласящей, что *для каждого симметрического многочлена $f \in R[x_1, \ldots, x_n]$ существует единственный многочлен $h \in R[x_1, \ldots, x_n]$, такой, что $f(x_1, \ldots, x_n) = h(\sigma_1, \ldots, \sigma_n)$.* □

1.75. Теорема (формула Ньютона). *Пусть $\sigma_1, \ldots, \sigma_n$ — элементарные симметрические многочлены от переменных $x_1, \ldots, x_n$ над кольцом R, и пусть $s_0 = n \in \mathbb{N}$ и $s_k = s_k(x_1, \ldots, x_n) = x_1^k + \ldots + x_n^k \in R[x_1, \ldots, x_n]$ при $k \geqslant 1$. Тогда для $k \geqslant 1$ справедлива формула*

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \cdots + (-1)^{m-1}s_{k-m+1}\sigma_{m-1} + \\ + (-1)^m \frac{m}{n} s_{k-m}\sigma_m = 0,$$

где $m = \min(k, n)$.

1.76. Теорема (формула Варинга). *При тех же обозначениях, что и в теореме 1.75, для $k \geqslant 1$ имеет место равенство*

$$s_k = \sum (-1)^{i_2+i_4+i_6+\ldots} \frac{(i_1 + i_2 + \ldots + i_n - 1)!\, k}{i_1!\, i_2! \ldots i_n!} \sigma_1^{i_1}\sigma_2^{i_2} \ldots \sigma_n^{i_n},$$

где суммирование распространяется на все n-наборы $(i_1, \ldots, i_n)$ неотрицательных целых чисел, удовлетворяющие условию $i_1 + 2i_2 + \ldots + ni_n = k$. Коэффициент при $\sigma_1^{i_1} \ldots \sigma_n^{i_n}$ всегда является целым числом.

§ 4. Расширения полей

Пусть F — поле. Подмножество K поля F, которое само является полем относительно операций поля F, называется его *подполем*. В этом случае поле F называется *расширением* поля K. Если $K \neq F$, будем K называть *собственным подполем* поля F.

Если K — подполе конечного поля $\mathbb{F}_p$ при простом p, то оно должно содержать элементы 0 и 1, а значит, и все другие элементы поля $\mathbb{F}_p$ в силу замкнутости поля K по сложению. Следовательно, поле $\mathbb{F}_p$ не имеет собственных подполей. Так мы приходим к следующему понятию.

1.77. Определение. Поле, не содержащее собственных подполей, называется *простым полем*.

Как показывает предыдущее рассуждение, любое поле порядка p при простом p — простое поле. Другим примером простого поля является поле $\mathbb{Q}$ рациональных чисел.

Пересечение любой непустой совокупности подполей данного поля F — снова подполе поля F. Пересечение *всех* подполей поля F называется *простым подполем* поля F. Очевидно, что оно является простым полем.

1.78. Теорема. *Простое подполе поля F изоморфно либо полю $\mathbb{F}_p$ при некотором простом числе p, либо полю $\mathbb{Q}$, и в соответствии с этим характеристикой поля F является либо p, либо 0.*

1.79. Определение. Пусть K — подполе поля F и M — любое подмножество поля F. Тогда поле $K(M)$ определим как пересечение всех подполей поля F, содержащих одновременно K и M; оно называется *расширением* поля K, *полученным присоединением элементов множества* M. В случае конечного множества $M = \{\theta_1, \ldots, \theta_n\}$ мы будем писать $K(M) = K(\theta_1, \ldots, \theta_n)$. Если M состоит из единственного элемента $\theta \in F$, то поле $L = K(\theta)$ называется *простым расширением* поля K, а θ — *образующим* (или *порождающим*) *элементом* простого расширения L поля K.

Очевидно, что $K(M)$ является наименьшим подполем поля F, содержащим одновременно K и M. Определим теперь один важный тип расширений.

1.80. Определение. Пусть K — некоторое подполе поля F и $\theta \in F$. Если θ удовлетворяет нетривиальному полиномиальному уравнению с коэффициентами из поля K, т. е. если $a_n\theta^n + \ldots + a_1\theta + a_0 = 0$, где элементы a_i лежат в K и не равны нулю одновременно, то элемент θ называется *алгебраическим* над K. Расширение L поля K называется *алгебраическим расширением* поля K, если каждый элемент поля L является алгебраическим над K.

Пусть элемент $\theta \in F$ является алгебраическим над K. Рассмотрим множество $J = \{f \in K[x] \mid f(\theta) = 0\}$. Легко проверить, что J — идеал кольца $K[x]$, причем $J \neq (0)$, так как θ — алгебраический элемент над K. Но в таком случае, согласно теореме 1.54, существует однозначно определенный нормированный многочлен $g \in K[x]$, такой, что J совпадает с главным идеалом (g). Важно заметить, что многочлен g неприводим в $K[x]$. Действительно, во-первых, g имеет положительную степень, так как он имеет корень θ, а во-вторых, если $g = h_1h_2$ в $K[x]$, где $1 \leqslant \deg(h_i) < \deg(g)$, $i = 1, 2$, то из $0 = g(\theta) = h_1(\theta)\,h_2(\theta)$ вытекает, что либо h_1, либо h_2 принадлежит идеалу J и, значит, делится на g, а это невозможно.

1.81. Определение. Если элемент θ поля F алгебраический над подполем K этого поля, то однозначно определенный нормированный

рованный многочлен $g \in K[x]$, порождающий идеал $J = \{f \in K[x] \mid f(\theta) = 0\}$ кольца $K[x]$, называется *минимальным многочленом* элемента θ над полем K. Под *степенью* элемента θ над полем K понимается степень его минимального многочлена g.

1.82. Теорема. *Если элемент θ поля F является алгебраическим над подполем K поля F, то его минимальный многочлен g над K обладает следующими свойствами:*

(i) *Многочлен g неприводим в кольце $K[x]$.*

(ii) *Для многочлена $f \in K[x]$ равенство $f(\theta) = 0$ выполняется в том и только том случае, когда многочлен g делит f.*

(iii) *Многочлен g является нормированным многочленом наименьшей степени в кольце $K[x]$, для которого θ является корнем.*

Доказательство. Свойство (i) уже установлено, а (ii) вытекает из определения g. Что касается (iii), то достаточно заметить, что любой нормированный многочлен из $K[x]$, для которого θ является корнем, кратен g и, значит, либо равен g, либо имеет степень, превышающую степень g. □

Отметим, что как минимальный многочлен алгебраического элемента θ, так и степень этого элемента зависят от того поля K, над которым рассматривается этот элемент, так что нельзя говорить о минимальном многочлене или о степени элемента θ, не указывая поля K (если, конечно, это не ясно из контекста).

Если L — расширение поля K, то L можно рассматривать как *векторное* (или *линейное*) *пространство* над полем K. Элементы поля L (т. е. «*векторы*») образуют по сложению абелеву группу. Кроме того, каждый «вектор» $\alpha \in L$ может быть умножен на «*скаляр*» $r \in K$, и при этом произведение $r\alpha$ снова принадлежит L (здесь $r\alpha$ — просто произведение в смысле операции поля L элементов r и α этого поля). Наконец, выполняются законы $r(\alpha + \beta) = r\alpha + r\beta$, $(r + s)\alpha = r\alpha + s\alpha$, $(rs)\alpha = r(s\alpha)$ и $1\alpha = \alpha$, где $r, s \in K$, $\alpha, \beta \in L$.

1.83. Определение. Пусть L — некоторое расширение поля K. Если L, рассматриваемое как векторное пространство над K, имеет конечную размерность, то L называется *конечным расширением* поля K. Размерность векторного пространства L над K называется *степенью* поля L над K и обозначается $[L : K]$.

1.84. Теорема. *Если L — конечное расширение поля K и M — конечное расширение поля L, то M — конечное расширение поля K, причем*

$$[M : K] = [M : L]\,[L : K].$$

Доказательство. Положим $[M : L] = m$, $[L : K] = n$, и пусть $\{\alpha_1, \ldots, \alpha_m\}$ — базис векторного пространства M над L и $\{\beta_1, \ldots, \beta_n\}$ — базис L над K. Тогда каждый элемент $\alpha \in M$ является

линейной комбинацией $\alpha = \gamma_1\alpha_1 + \ldots + \gamma_m\alpha_m$, где $\gamma_i \in L$, $1 \leqslant i \leqslant m$, и, записывая каждое γ_i через базисные элементы β_j, получим

$$\alpha = \sum_{i=1}^{m} \gamma_i\alpha_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} r_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij}\beta_j\alpha_i,$$

где коэффициенты r_{ij} лежат в K. Для доказательства теоремы теперь достаточно доказать линейную независимость mn элементов $\beta_j\alpha_i$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, над полем K. Допустим, что

$$\sum_{i=1}^{m} \sum_{j=1}^{n} s_{ij}\beta_j\alpha_i = 0$$

с коэффициентами s_{ij} из K. Тогда

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} s_{ij}\beta_j \right) \alpha_i = 0,$$

и из линейной независимости элементов $\alpha_1, \ldots, \alpha_m$ над L мы заключаем, что

$$\sum_{j=1}^{n} s_{ij}\beta_j = 0 \quad \text{для} \quad 1 \leqslant i \leqslant m.$$

Но так как элементы $\beta_1, \ldots, \beta_n$ линейно независимы над K, мы делаем вывод, что все s_{ij} равны 0. □

1.85. Теорема. *Каждое конечное расширение поля K является алгебраическим над K.*

Доказательство. Пусть L — конечное расширение поля K, $[L : K] = m$ и $\theta \in L$. Тогда $m + 1$ элементов $1, \theta, \ldots, \theta^m$ поля L являются линейно зависимыми над K, так что имеет место равенство $a_0 + a_1\theta + \cdots + a_m\theta^m = 0$ с коэффициентами $a_i \in K$, не равными нулю одновременно. Но это означает, что θ — алгебраический элемент над K. □

Изучим строение простого расширения $K(\theta)$ поля K, полученного присоединением к K некоторого алгебраического элемента. Пусть F — расширение поля K, и пусть $\theta \in F$ — алгебраический элемент над K. Оказывается, что $K(\theta)$ — конечное (а потому и алгебраическое) расширение поля K.

1.86. Теорема. *Пусть θ — элемент поля F, являющийся алгебраическим степени n над подполем K поля F, и пусть g — минимальный многочлен элемента θ над K. Тогда*

(i) *Простое расширение $K(\theta)$ изоморфно факторкольцу $K[x]/(g)$.*

(ii) $[K(\theta) : K] = n$ *и* $\{1, \theta, \ldots, \theta^{n-1}\}$ — *базис векторного*

пространства $K(\theta)$ *над полем* K.

(iii) *Каждый элемент* $\alpha \in K(\theta)$ *является алгебраическим над полем* K, *и его степень является делителем* n.

Доказательство. (i) Рассмотрим отображение τ: $K[x] \to K(\theta)$, определяемое условием $\tau(f) = f(\theta)$ для всех $f \in K[x]$. Очевидно, что τ является гомоморфизмом колец. Заметим, что $\operatorname{Ker}\tau = \{f \in K[x] \mid f(\theta) = 0\} = (g)$ в силу определения минимального многочлена. Пусть S — образ отображения τ, т. е. множество значений [1]) многочленов от x с коэффициентами из поля K при $x = \theta$. Тогда по теореме о гомоморфизме колец (теорема 1.40) получаем, что S изоморфно факторкольцу $K[x]/(g)$. Но в силу теорем 1.61 и 1.82(i) факторкольцо $K[x]/(g)$ является полем, а следовательно, S — поле. Но поскольку $K \subseteq S \subseteq K(\theta)$ и $\theta \in S$, по определению простого расширения $S = K(\theta)$ и (i) доказано.

(ii) Так как $S = K(\theta)$, то любой элемент $\alpha \in K(\theta)$ можно записать в виде $\alpha = f(\theta)$ для некоторого $f \in K[x]$. Применяя алгоритм деления, находим многочлены q и r из $K[x]$, такие, что $f = qg + r$, где $\deg(r) < \deg(g) = n$. Тогда $\alpha = f(\theta) = q(\theta) \cdot g(\theta) + r(\theta) = r(\theta)$, и потому α является линейной комбинацией элементов $1, \theta, \ldots, \theta^{n-1}$ с коэффициентами из K. С другой стороны, если для некоторых $a_i \in K$ имеет место равенство $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = 0$, то θ является корнем многочлена $h(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in K[x]$, и потому h в силу теоремы 1.82 (ii) кратен g. Но поскольку $\deg(h) < n = \deg(g)$, это возможно лишь при условии, что $h = 0$, т. е. что все a_i равны 0. Поэтому элементы $1, \theta, \ldots, \theta^{n-1}$ линейно независимы над K, что доказывает (ii).

(iii) Поле $K(\theta)$ является конечным расширением поля K ввиду (ii). Поэтому элемент $\alpha \in K(\theta)$ будет в силу теоремы 1.85 алгебраическим над K. Далее, $K(\alpha)$ — подполе поля $K(\theta)$. Если d — степень элемента α над K, то из (ii) и теоремы 1.84 следует, что $n = [K(\theta) : K] = [K(\theta) : K(\alpha)]\,[K(\alpha) : K]$, так что $d = [K(\alpha) : K]$ делит n. □

Таким образом, элементами простого алгебраического расширения $K(\theta)$ поля K являются значения многочленов от x с коэффициентами из поля K при $x = \theta$. При этом любой элемент поля $K(\theta)$ может быть однозначно представлен в виде $a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$, где $a_i \in K$, $0 \leqslant i \leqslant n-1$.

Как подчеркивалось выше, в теореме 1.86 предполагается, что поле K и элемент θ принадлежат некоторому большему полю F. Это необходимо для того, чтобы алгебраические выражения, содержащие θ, имели смысл. Но сейчас мы хотим построить простое

[1]) Многочлен над K можно рассматривать и как многочлен над F. — *Прим. перев.*

алгебраическое расширение ab ovo [1]), т. е. без ссылок на предварительно заданное большее поле. Идея этого построения содержится в п. (i) теоремы 1.86.

1.87. Теорема. *Пусть многочлен $f \in K[x]$ неприводим над полем K. Тогда существует простое алгебраическое расширение поля K, образующим элементом которого является некоторый корень многочлена f.*

Доказательство. Рассмотрим факторкольцо $L = K[x]/(f)$, которое по теореме 1.61 является полем. Элементами кольца L являются классы вычетов $[h] = h + (f)$, где $h \in K[x]$. Для каждого $a \in K$ мы можем построить класс вычетов $[a]$, определяемый постоянным многочленом a, и если $a, b \in K$ различны, то $[a] \neq [b]$, так как f имеет положительную степень. Отображение $a \mapsto [a]$ дает изоморфизм поля K на некоторое подполе K' поля L, так что поле K' можно отождествить с K. Другими словами, мы можем рассматривать поле L как расширение поля K. Для каждого многочлена $h(x) = a_0 + a_1x + \ldots + a_mx^m \in K[x]$ в соответствии с правилами действий с классами вычетов и учитывая отождествление $[a_i] = a_i$, получаем

$$[h] = [a_0 + a_1x + \ldots + a_mx^m] =$$
$$= [a_0] + [a_1][x] + \ldots + [a_m][x]^m = a_0 + a_1[x] + \ldots + a_m[x]^m$$

Таким образом, каждый элемент поля L может быть записан как многочлен от «переменной» $[x]$ с коэффициентами из K. Так как любое поле, одновременно содержащее K и $[x]$, должно содержать и каждый такой элемент $[h]$, то L является простым расширением поля K, получаемым присоединением элемента $[x]$. Если $f(x) = b_0 + b_1x + \ldots + b_nx^n$, то $f([x]) = b_0 + b_1[x] + \ldots + b_n[x]^n = [b_0 + b_1x + \ldots + b_nx^n] = [f] = [0]$, так что $[x]$ является корнем многочлена f и, следовательно, L есть простое алгебраическое расширение поля K. □

1.88. Пример. В качестве примера формального процесса присоединения корня, описанного в теореме 1.87, рассмотрим простое поле $\mathbb{F}_3$ и многочлен $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$, который неприводим над $\mathbb{F}_3$. Пусть $\theta = [x]$ — некоторый «корень» многочлена f, т. е. класс вычетов $x + (f)$ из факторкольца $L = \mathbb{F}_3[x]/(f)$. Другим корнем многочлена f в L является тогда $2\theta + 2$, поскольку $f(2\theta + 2) = (2\theta + 2)^2 + (2\theta + 2) + 2 = \theta^2 + \theta + 2 = 0$. Как следует из теоремы 1.86 (ii), простое алгебраическое расширение $L = \mathbb{F}_3(\theta)$ состоит из девяти элементов: $0, 1, 2, \theta, \theta + 1, \theta + 2, 2\theta, 2\theta + 1, 2\theta + 2$. Таблицы операций для L можно построить так же, как и в примере 1.62. □

[1]) ab ovo — дословно «от яйца» (лат.), т. е. с самого начала. — *Прим. перев.*

Заметим, что в рассмотренном примере мы могли бы вместо θ присоединить к полю $\mathbb{F}_3$ корень $2\theta + 2$ того же многочлена f и получили бы то же самое поле L. Эта ситуация обобщается следующим легко проверяемым результатом.

1.89. Теорема. *Пусть α и β — два корня многочлена $f \in K[x]$, который неприводим над полем K. Тогда простые расширения $K(\alpha)$ и $K(\beta)$ изоморфны, причем изоморфизм осуществляется отображением, переводящим элемент α в β и оставляющим неизменными элементы поля K.*

Теперь займемся такими расширениями поля K, которым принадлежат все корни некоторого заданного многочлена над K.

1.90. Определение. Пусть многочлен $f \in K[x]$ имеет положительную степень, и пусть F — некоторое расширение поля K. Тогда говорят, что многочлен f *вполне разлагается* (split) в поле F, если f можно записать в виде произведения линейных сомножителей из $F[x]$, т. е. существуют такие элементы $\alpha_1, \ldots, \alpha_n \in F$, что

$$f(x) = a(x - \alpha_1) \ldots (x - \alpha_n),$$

где a — старший коэффициент многочлена f. Поле F называется *полем разложения* многочлена f над полем K, если f вполне разлагается в поле F и, кроме того, $F = K(\alpha_1, \ldots, \alpha_n)$.

Ясно, что поле разложения F многочлена f над полем K является наименьшим из полей, содержащих одновременно K и все корни многочлена f, в следующем смысле: никакое собственное подполе поля F, являющееся расширением поля K, не может содержать всех корней многочлена f. Повторным применением процесса, описанного в теореме 1.87, можно получить первую часть следующего предложения. Вторая часть является обобщением теоремы 1.89.

1.91. Теорема (существование и единственность поля разложения). *Если K — некоторое поле и f — многочлен положительной степени из $K[x]$, то существует поле разложения многочлена f над K. Любые два поля разложения многочлена f над K изоморфны, и соответствующий изоморфизм оставляет неизменными элементы поля K и осуществляет некоторую перестановку корней многочлена f.*

Поскольку изоморфные поля можно отождествить, мы можем говорить о вполне определенном поле разложения многочлена f над полем K. Оно получается присоединением к полю K конечного числа алгебраических над K элементов, и потому (как можно показать на основании теорем 1.84 и 1.86 (ii)) поле разложения многочлена f над K является конечным расширением поля K.

Чтобы продемонстрировать полезность полей разложения, воспользуемся ими для решения следующей задачи: как выяснить,

имеет или нет данный многочлен кратные корни (см. определение 1.65)?

1.92. Определение. Пусть $f \in K[x]$ — некоторый многочлен степени $n \geqslant 2$, и пусть $f(x) = a_0(x - \alpha_1) \ldots (x - \alpha_n)$, где $\alpha_1, \ldots, \alpha_n$ — элементы поля разложения многочлена f над полем K. Тогда *дискриминант* $D(f)$ многочлена f определяется так:

$$D(f) = a_0^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Из определения $D(f)$ ясно, что многочлен f в том и только том случае имеет кратный корень, когда $D(f) = 0$. Заметим, что дискриминант $D(f)$, хоть он и определяется через элементы расширения поля K, на самом деле является элементом самого поля K. Для небольших n это можно показать простым подсчетом. Например, если $n = 2$ и $f(x) = ax^2 + bx + c = a(x - \alpha_1)(x - \alpha_2)$, то

$$D(f) = a^2(\alpha_1 - \alpha_2)^2 = a^2((\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2) = a^2(b^2a^{-2} - 4ca^{-1}),$$

откуда получается выражение, хорошо известное из теории квадратных уравнений:

$$D(ax^2 + bx + c) = b^2 - 4ac.$$

Если $n = 3$ и $f(x) = ax^3 + bx^2 + cx + d = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, то

$$D(f) = a^4(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2,$$

и несколько более сложный подсчет показывает, что

$$D(ax^3 + bx^2 + cx + d) = b^2c^2 - 4b^3d - 4ac^3 - 27a^2d^2 + 18\,abcd. \quad (1.9)$$

В общем случае рассмотрим сначала многочлен $s \in K[x_1, \ldots, x_n]$, заданный выражением

$$s(x_1, \ldots, x_n) = a_0^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2.$$

Тогда очевидно, что s — симметрический многочлен, и по основной теореме о таких многочленах (см. пример 1.74) его можно представить в виде некоторого многочлена от элементарных симметрических многочленов $\sigma_1, \ldots, \sigma_n$ с коэффициентами из поля K: $s = h(\sigma_1, \ldots, \sigma_n)$ для некоторого $h \in K[x_1, \ldots, x_n]$. Если

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = a_0(x - \alpha_1) \ldots (x - \alpha_n) \in K[x],$$

то из определения элементарных симметрических многочленов (см. снова пример 1.74) вытекает, что

$$\sigma_k(\alpha_1, \ldots, \alpha_n) = (-1)^k a_k a_0^{-1} \in K, \quad 1 \leqslant k \leqslant n.$$

Таким образом,

$$D(f) = s(\alpha_1, \ldots, \alpha_n) = h(\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots, \alpha_n)) =$$
$$= h\left(-a_1a_0^{-1}, \ldots, (-1)^n a_n a_0^{-1}\right) \in K.$$

Так как $D(f) \in K$, то возникает мысль, нельзя ли подсчитать дискриминант $D(f)$, не переходя к расширению поля K. Оказывается, это можно сделать, воспользовавшись понятием результанта. Заметим сначала, что если многочлен $f \in K[x]$ задан в виде $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, то мы не исключаем возможности равенства нулю коэффициента a_0, так что натуральное число n не обязательно является степенью многочлена f. В таком случае мы будем называть число n *формальной степенью* многочлена f; формальная степень n всегда не меньше настоящей степени $\deg(f)$.

1.93. Определение. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in K[x]$ и $g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m \in K[x]$ — два многочлена с формальными степенями n и m соответственно, $n, m \in \mathbb{N}$. Тогда *результант* $R(f, g)$ этих двух многочленов — это определитель

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_n & 0 & \ldots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_m & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_m & \ldots & & 0 \\ \vdots & & & & & & \vdots \\ 0 & \ldots & b_0 & b_1 & \ldots & & b_m \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \} m \text{ строк} \\ \\ \\ \\ \} n \text{ строк} \\ \\ \\ \end{matrix}$$

порядка $m + n$.

Если $\deg(f) = n$ (т. е. $a_0 \neq 0$) и $f(x) = a_0(x - \alpha_1) \ldots (x - \alpha_n)$ в поле разложения многочлена f над K, то $R(f, g)$ можно также задать формулой

$$R(f, g) = a_0^m \prod_{i=1}^{n} g(\alpha_i). \tag{1.10}$$

В этом случае очевидно, что равенство $R(f, g) = 0$ выполняется тогда и только тогда, когда многочлены f и g имеют общий корень (т. е. f и g имеют общий делитель положительной степени в кольце $K[x]$).

Теорема 1.68 наводит на мысль, что между дискриминантом $D(f)$ и результантом $R(f, f')$ имеется связь. Пусть $f \in K[x]$,

$\deg(f) = n \geqslant 2$ и старший коэффициент f равен a_0. Тогда и в самом деле имеет место равенство

$$D(f) = (-1)^{n(n-1)/2} a_0^{-1} R(f, f'), \tag{1.11}$$

где производная f' рассматривается как многочлен формальной степени $n - 1$. Последнее замечание требуется потому, что в случае поля K простой характеристики может оказаться, что $\deg(f') < n - 1$ и даже что $f' = 0$. Но в любом случае равенство (1.11) выполняется, так что дискриминант $D(f)$ можно найти, вычислив определитель порядка $2n - 1$ с элементами из поля K.

Комментарии

§ 1. Определения и теоремы этой главы можно найти почти в каждой из вводных книг по современной алгебре. Упомянем некоторые из них: Birkhoff, MacLane [1], Fraleigh [1], Herstein [4], Kochendörffer [1], Lang [4], Rédei [10], van der Waerden [2] (а также Калужнин [1*], Кострикин [1*], Курош [1*], Мальцина, Проскуряков [1*], Скорняков [1*], Сушкевич [1*], Фаддеев [1*]. — *Перев.*)

Существуют и другие эквивалентные определения группы. Например, группу можно определить как непустое множество G с ассоциативной бинарной операцией, такой, что для любых $a, b \in G$ уравнения $ax = b$ и $ya = b$ имеют решения в G. Важной иллюстрацией понятия группы может служить (наряду с приведенными выше примерами) группа матриц, т. е. множество матриц с элементами из некоторого поля, образующее группу относительно операции умножения матриц. Такие группы встретятся нам в гл. 8. Другие важные примеры можно найти в упомянутых руководствах (а также в книгах Hall [6], Каргаполов, Мерзляков [1*], Курош [2*], Шмидт [1*]. — *Перев.*)

Латинским квадратом называется квадратная таблица, в каждой строке и в каждом столбце которой ровно один раз встречается каждый элемент некоторого множества. Таким образом, таблица Кэли любой конечной группы является латинским квадратом. Однако не каждый латинский квадрат можно рассматривать как таблицу Кэли некоторой группы, так как не обязательно выполнен закон ассоциативности. Подробнее о латинских квадратах см. в § 4 гл. 9, а также в книге Dénes, Keedwell [1].

По поводу циклических групп можно легко доказать, что любая бесконечная циклическая группа изоморфна аддитивной группе $\mathbb{Z}$ целых чисел и любая циклическая группа порядка n изоморфна аддитивной группе $\mathbb{Z}_n$ вычетов по модулю n.

---

[1]) «Звездочкой» помечены работы, добавленные при переводе. — *Прим. ред.*

Стоит упомянуть определения некоторых алгебраических систем, которые даже проще, чем группы, так как для них выполняется лишь часть аксиом группы. Так, множество с бинарной операцией называется *группоидом*; если же дополнительно предполагается ассоциативность операции, то это *полугруппа*. Полугруппа с единичным элементом называется *моноидом*.

§ 2. Существуют разные определения кольца. Например, некоторые авторы опускают ассоциативность умножения, а структуру, введенную определением 1.28, называют *ассоциативным кольцом*. В определении целостного кольца иногда опускается требование существования мультипликативной единицы.

Первое абстрактное определение поля было дано Вебером (Weber [3]). Конечные простые поля $\mathbb{F}_p$, где p — простое число, были широко изучены еще Гауссом (Gauss [3]) в связи со сравнениями в кольце $\mathbb{Z}$ целых чисел по простому модулю.

Характеристика поля совпадает с характеристикой его простого подполя. Существуют поля простой характеристики, не являющиеся конечными. Примером может служить подходящее расширение поля $\mathbb{F}_p$, скажем, поле рациональных функций над $\mathbb{F}_p$ или алгебраическое замыкание поля $\mathbb{F}_p$ (ср. с комментариями к § 4).

Многие свойства целых чисел можно перенести на соответствующие главные идеалы в кольце $\mathbb{Z}$. Это обусловлено тем фактом, что целое число a делит целое число b в том и только том случае, если главный идеал (a) содержит главный идеал (b). Особый интерес представляют простые числа. Согласно обычному определению, простым называется целое число >1, которое не имеет нетривиальных делителей. Можно дать другое равносильное определение, назвав простым такое целое число >1, которое делит произведение целых чисел лишь тогда, когда оно делит один из сомножителей. Перефразируя для идеалов эти характеризации простого числа, мы соответственно приходим к определениям максимального и простого идеалов.

§ 3. При обычном определении многочлена как выражения вида $a_0 + a_1x + \ldots + a_nx^n$ обсуждения вопроса о связи коэффициентов a_i и переменной x обычно избегают. Однако существует способ дать совершенно безукоризненное определение многочлена как элемента кольца многочленов.

Чтобы дать такое определение, рассмотрим множество S всех бесконечных последовательностей вида

$$(a_0, a_1, \ldots, a_n, \ldots),$$

компонентами a_i которых являются элементы некоторого коммутативного кольца R с единицей 1, причем лишь конечное число компонент a_i может быть отлично от 0. Нетрудно убедиться, что

множество S образует коммутативное кольцо с единицей относительно следующих операций сложения и умножения:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$
$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, \ldots),$$

где $(n + 1)$-я компонента произведения равна $a_0b_n + a_1b_{n-1} + \ldots + a_nb_0$. Нулевым элементом кольца S является, очевидно, $(0, 0, \ldots)$, а единицей $(1, 0, 0, \ldots)$.

Множество P последовательностей вида $(a_0, 0, 0, \ldots)$, где лишь первая компонента может быть отличной от 0, образует подкольцо кольца S. Это подкольцо P и заданное кольцо R изоморфны, причем изоморфизм задается соответствием $(a_0, 0, 0, \ldots) \longmapsto a_0$. Поэтому мы отождествляем эти два кольца и пишем $(a_0, 0, 0, \ldots) = a_0$. Кольцо R, таким образом, можно рассматривать как подкольцо кольца S, а S — как расширение кольца R.

Обозначим теперь через x последовательность $(0, 1, 0, \ldots)$. Легко проверить, что

$$x^n = (0, \ldots, 0, 1, 0, \ldots) \quad \text{для} \quad n \geqslant 1,$$

где 1 является $(n + 1)$-й компонентой. Если, кроме того, положить $x^0 = (1, 0, 0, \ldots) = 1$, то для любой последовательности $(a_0, a_1, a_2, \ldots)$ из S

$$\begin{aligned}(a_0, a_1, a_2, \ldots) &= \\ &= (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + (0, 0, a_2, 0, \ldots) + \ldots = \\ &= (a_0, 0, 0, \ldots)(1, 0, 0, \ldots) + (a_1, 0, 0, \ldots)(0, 1, 0, \ldots) + \\ &\quad + (a_2, 0, 0, \ldots)(0, 0, 1, 0, \ldots) + \ldots = \\ &= (a_0, 0, 0, \ldots)\,1 + (a_1, 0, 0, \ldots)\,x + (a_2, 0, 0, \ldots)\,x^2 + \ldots = \\ &= a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = f(x).\end{aligned}$$

Таким образом, элементами кольца S являются многочлены $f(x) \in R[x]$, определяемые как бесконечные последовательности с конечным числом ненулевых компонент.

Мы снова обращаем внимание, что главным соображением в пользу такого определения многочлена $f(x)$ над R является прояснение связи между элементами из R и новым элементом x. Переход от кольца R к кольцу S многочленов над R называется *кольцевым присоединением* элемента x к кольцу R. Кольцо многочленов $R[x]$ можно считать также подкольцом кольца формальных степенных рядов над кольцом R (оно будет введено в гл. 8).

Рассматривая свойства кольца $\mathbb{Z}$ целых чисел и кольца $F[x]$ многочленов над некоторым полем F, нетрудно заметить некоторое сходство между ними. Действительно, оба типа колец относятся к одному и тому же классу — евклидовым кольцам. *Евклидово кольцо* — это коммутативное кольцо R, содержащее не менее

двух элементов и не имеющее делителей нуля, для которого существует отображение ν из множества ненулевых элементов кольца R в множество неотрицательных целых чисел со следующими двумя свойствами: (i) если $a, b \in R$, причем $ab \neq 0$, то $\nu(ab) \geqslant \nu(a)$; (ii) для $a, b \in R$, где $b \neq 0$, существуют элементы $q, r \in R$, такие, что $a = qb + r$, причем либо $r = 0$, либо $\nu(r) < \nu(b)$. Нетрудно заметить, что $\mathbb{Z}$ является евклидовым кольцом, где $\nu(n) = |n|$ для $n \in \mathbb{Z}$, а $F[x]$ является евклидовым кольцом, где $\nu(f) = \deg(f)$ для $f \in F[x]$. Справедлив такой общий результат: любое евклидово кольцо является кольцом главных идеалов.

Свойство, устанавливаемое теоремой 1.59, тоже сохраняется и при более общих предположениях. Введем следующее определение. Целостное кольцо, в котором выполняется теорема об однозначном разложении на простые сомножители, т. е. в котором каждый отличный от нуля элемент, не являющийся делителем единицы, может быть однозначно (с точностью до делителей единицы и до порядка сомножителей) представлен в виде произведения простых элементов, называется *факториальным кольцом* или кольцом *с однозначным разложением на простые сомножители*. Таким образом, коротко говоря, теорема 1.59 утверждает, что кольцо $F[x]$ многочленов над полем F является факториальным. Более того, любое кольцо главных идеалов тоже является факториальным. Китайская теорема об остатках (см. упр. 1.37) является частным случаем общего результата такого типа, доказанного в книге Ленга Lang [4, ch. 2].

Много фактов о многочленах от одной или нескольких переменных содержится в книгах Rédei [10] и van der Waerden [2] и в монографии повышенного типа о многочленах Lausch, Nöbauer [1].

§ 4. В этом параграфе основными являются теоремы 1.86 и 1.87. В сущности, можно сказать, что теорема 1.87 устанавливает один из наиболее фундаментальных результатов теории полей. Этот результат, принадлежащий Кронекеру (Kronecker [8]), гарантирует для любого непостоянного многочлена над полем F существование такого расширения поля F, в котором этот многочлен имеет корень. Более того, доказательство этой теоремы не просто дает обоснование факта существования указанного расширения — оно дает также метод построения требуемого расширения.

Можно классифицировать элементы расширения F поля K по их отношению к полю K. Если $\theta \in F$, то простое расширение $K(\theta)$ поля K либо изоморфно полю $K(x)$ рациональных фуикцнй над K (называемому также полем частных кольца $K[x]$), либо (в силу теоремы 1.86) изоморфно факторкольцу $K[x]/(g)$, где $g \in K[x]$ — некоторый неприводимый многочлен, для которого

элемент θ является корнем. В первом случае элемент θ называется *трансцендентным* над K, во втором, как нам уже известно, θ является алгебраическим над K. Расширение F поля K, которое не является алгебраическим, называется *трансцендентным*. Примеров трансцендентных элементов можно привести сколько угодно. Так, бóльшая часть действительных чисел (например, e, π, $2^{\sqrt{2}}$, ...) — это трансцендентные над полем рациональных чисел $\mathbb{Q}$ числа.

Поля разложения существуют не только для одного непостоянного многочлена над полем K, но и для любой совокупности таких многочленов. Поле разложения над K совокупности всех непостоянных многочленов из $K[x]$ называется *алгебраическим замыканием* $\overline{K}$ поля K. Это поле является алгебраическим расширением поля K со следующим дополнительным свойством: любой непостоянный многочлен из $\overline{K}[x]$ вполне разлагается в поле $\overline{K}$. Для случаев $K = \mathbb{Q}$ и $K = \mathbb{F}_p$ алгебраическое замыкание $\overline{K}$ служит примером алгебраического расширения поля K, которое не является конечным расширением этого поля.

Абстрактная теория расширений полей была развита в фундаментальной статье Steinitz [1]. Более ранние исследования в этом направлении проведены в работах Kneser [1], Kronecker [5], [8] и Weber [3].

Упражнения

1.1. Доказать, что единичный элемент группы определяется однозначно.

1.2. Пусть G — мультипликативная группа. Доказать, что непустое подмножество H группы G является подгруппой этой группы в том и только том случае, когда из $a, b \in H$ следует $ab^{-1} \in H$. Если H конечно, то указанное условие можно заменить таким: из $a, b \in H$ следует $ab \in H$.

1.3. Пусть a — элемент конечного порядка k мультипликативной группы G. Показать, что для $m \in Z$ равенство $a^m = e$ выполняется тогда и только тогда, когда k делит m.

1.4. Для $m \in \mathbb{N}$ функция Эйлера $\varphi(m)$ определяется как число натуральных чисел k, не превосходящих m, которые взаимно просты с m. Доказать следующие свойства этой функции (здесь $m, n, s \in \mathbb{N}$ и p — простое число):

(a) $\varphi(p^s) = p^s\left(1 - \frac{1}{p}\right)$;

(b) $\varphi(mn) = \varphi(m)\,\varphi(n)$, если НОД $(m, n) = 1$;

(c) $\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right)$, где $m = p_1^{e_1} \ldots p_r^{e_r}$ — разложение m на простые сомножители.

1.5. Найти $\varphi(490)$ и $\varphi(768)$.

1.6. Доказать следующее утверждение: если порядок группы равен p^s, где p — простое число, $s \in \mathbb{N}$, то порядок ее центра делится на p (использовать теорему 1.27 — уравнение классов сопряженности).

1.7. Доказать, что в кольце R для всех $a, b \in R$ имеет место равенство $(-a)(-b) = ab$.

1.8. Доказать, что в коммутативном кольце R для всех $a, b \in R$ и $n \in \mathbb{N}$ справедлива формула

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \ldots + \binom{n}{n-1} ab^{n-1} + b^n,$$

где $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$

(*формула бинома*).

1.9. Пусть $p \in Z$ — простое число. Для любого $a \in Z$, не делящегося на p, показать, что p делит число $a^{p-1} - 1$ (малая теорема Ферма).

1.10. Доказать, что для любого простого числа p имеет место сравнение $(p-1)! \equiv -1 \pmod p$ (теорема Вильсона).

1.11. Доказать, что если p — простое число, то $\binom{p-1}{j} \equiv (-1)^j \pmod p$ для $0 \leqslant j \leqslant p-1$, $j \in Z$.

1.12. Ферма высказал гипотезу, что для всех целых неотрицательных чисел n число $2^{2^n}+1$ является простым. Эйлер нашел противоречащий пример: число 641 делит $2^{32}+1$. Подтвердить это, используя сравнения.

1.13. Доказать, что если $m_1, \ldots, m_k$ — натуральные попарно взаимно простые числа, т. е. НОД $(m_i, m_j) = 1$ для $1 \leqslant i < j \leqslant k$, то для любых целых чисел $a_1, \ldots, a_k$ система сравнений $y \equiv a_i \pmod{m_i}$, $i = 1, \ldots, k$, имеет решение y, определенное однозначно по модулю $m = m_1 \ldots m_k$ (китайская теорема об остатках).

1.14. Решить систему сравнений $5x \equiv 20 \pmod 6$, $6x \equiv 6 \pmod 5$, $4x \equiv 5 \pmod{77}$.

1.15. Показать, что если R — коммутативное кольцо простой характеристики p, то при любых $a_1, \ldots, a_s \in R$

$$(a_1 + \ldots + a_s)^{p^n} = a_1^{p^n} + \ldots + a_s^{p^n}.$$

1.16. Вывести из результата упр. 1.11, что в коммутативном кольце R простой характеристики p для всех $a, b \in R$ имеет место равенство

$$(a-b)^{p-1} = \sum_{j=0}^{p-1} a^j b^{p-1-j}.$$

1.17. Пусть F — поле и $f \in F[x]$. Доказать, что совокупность многочленов $\{g(f(x)) \mid g \in F[x]\}$ совпадает с кольцом $F[x]$ тогда и только тогда, когда $\deg(f) = 1$.

1.18. Показать, что из равенства $p^2(x) - xq^2(x) = xr^2(x)$, где $p, q, r \in \mathbb{R}[x]$, следует, что $p = q = r = 0$.

1.19. Пусть F — поле и $f, g \in F[x]$. Показать, что главный идеал (f) содержится в главном идеале (g) тогда и только тогда, когда многочлен g делит f.

1.20. Доказать следующее предложение. Если F — поле и многочлены $f, g \in F[x]$ взаимно просты и не являются постоянными одновременно, то существуют многочлены $a, b \in F[x]$, такие, что $\deg(a) < \deg(g)$, $\deg(b) < \deg(f)$ и $af + bg = 1$.

1.21. Пусть для многочленов $f_1, \ldots, f_n \in F[x]$, где F — поле, НОД $(f_1, \ldots, f_n) = d$, так что $f_i = dg_i$, где $g_i \in F[x]$, $i = 1, \ldots, n$. Доказать, что многочлены $g_1, \ldots, g_n$ взаимно просты.

1.22. Доказать, что для многочленов $f_1, \ldots, f_n \in F[x]$, где F — поле и $n \geqslant 3$, справедливо соотношение

$$\text{НОД}(f_1, \ldots, f_n) = \text{НОД}(\text{НОД}(f_1, \ldots, f_{n-1}), f_n).$$

1.23. Пусть F — поле и $f, g, h \in F[x]$. Доказать, что если f делит gh и НОД $(f, g) = 1$, то f делит h.

1.24. Применяя алгоритм Евклида, найти НОД (f, g) для следующих многочленов f и g с коэффициентами из указанного поля F:

(a) $F = \mathbb{Q}$, $f(x) = x^7 + 2x^5 + 2x^2 - x + 2$, $g(x) = x^6 - 2x^5 - x^4 + x^2 + 2x + 3$;

(b) $F = \mathbb{F}_2$, $f(x) = x^7 + 1$, $g(x) = x^5 + x^3 + x + 1$;

(c) $F = \mathbb{F}_2$, $f(x) = x^5 + x + 1$, $g(x) = x^6 + x^5 + x^4 + 1$;

(d) $F = \mathbb{F}_3$, $f(x) = x^8 + 2x^5 + x^3 + x^2 + 1$, $g(x) = 2x^6 + x^5 + 2x^3 + 2x^2 + 2$.

1.25. Пусть $f_1, \ldots, f_n$ — ненулевые многочлены из $F[x]$, где F — поле. Доказать существование и единственность нормированного многочлена $m \in F[x]$ со свойствами наименьшего общего кратного многочленов $f_1, \ldots, f_n$. (*Указание.* Рассмотреть пересечение главных идеалов $(f_1) \cap \ldots \cap (f_n)$.)

1.26. Доказать соотношение (1.6).

1.27. Пусть F — поле и $f_1, \ldots, f_n \in F[x]$ — ненулевые попарно взаимно простые многочлены. Показать, что НОК $(f_1, \ldots, f_n) = a^{-1} f_1 \ldots f_n$, где a — старший коэффициент многочлена $f_1 \ldots f_n$.

1.28. Доказать, что для многочленов $f_1, \ldots, f_n \in F[x]$, где F — поле и $n \geqslant 3$, справедливо соотношение

$$\text{НОК}(f_1, \ldots, f_n) = \text{НОК}(\text{НОК}(f_1, \ldots, f_{n-1}), f_n).$$

1.29. Пусть F — поле, $f_1, \ldots, f_n \in F[x]$ — ненулевые многочлены и для каждого f_i, $1 \leqslant i \leqslant n$, задано каноническое разложение

$$f_i = a_i \prod p^{e_i(p)},$$

где $a_i \in F$, произведение распространяется на все неприводимые нормированные многочлены p из $F[x]$ и $e_i(p)$ — неотрицательные целые числа, причем для каждого i строгое неравенство $e_i(p) > 0$ выполняется лишь для конечного числа многочленов p. Для каждого p положим $m(p) = \min(e_1(p), \ldots, e_n(p))$, $M(p) = \max(e_1(p), \ldots, e_n(p))$. Доказать, что

$$\text{НОД}(f_1, \ldots, f_n) = \prod p^{m(p)}, \quad \text{НОК}(f_1, \ldots, f_n) = \prod p^{M(p)}.$$

1.30. Метод Кронекера нахождения делителей степени $\leqslant s$ непостоянного многочлена $f \in \mathbb{Q}[x]$ состоит в следующем.

(1) Можно считать, что $f \in \mathbb{Z}[x]$ (учитывая возможность умножения многочлена f на константу).

(2) Возьмем $s + 1$ различных чисел $a_0, \ldots, a_s \in \mathbb{Z}$, не являющихся корнями многочлена f, и для каждого i, $0 \leqslant i \leqslant s$, найдем все делители числа $f(a_i)$.

(3) Для каждого $(s+1)$-набора $(b_0, \ldots, b_s)$, где b_i — делитель числа $f(a_i)$, $0 \leqslant i \leqslant s$, найдем такой многочлен $g \in \mathbb{Q}[x]$, чтобы $\deg(g) \leqslant s$ и $g(a_i) = b_i$, $0 \leqslant i \leqslant s$ (например, используя интерполяционную формулу Лагранжа из теоремы 1.71).

(4) Выясним, какие из этих многочленов g являются делителями исходного многочлена f. Если $\deg(f) = n \geqslant 1$ и s — наибольшее целое число, не превосходящее $n/2$, то многочлен f неприводим в кольце $\mathbb{Q}[x]$ в том случае, когда указанный метод выявляет в качестве делителей f лишь постоянные многочлены g. В остальных случаях метод Кронекера обязательно приводит к нетривиальному разложению многочлена f.

Применяя затем тот же метод к полученным сомножителям и повторяя этот процесс, мы получим в конце концов каноническое разложение многочлена f в кольце $\mathbb{Q}[x]$.

Использовать указанную процедуру для нахождения канонического разложения многочлена

$$f(x) = \frac{1}{3}x^6 - \frac{5}{3}x^5 + 2x^4 - x^3 + 5x^2 - \frac{17}{3}x - 1 \in \mathbb{Q}[x].$$

1.31. Построить таблицы сложения и умножения для факторкольца $\mathbb{F}_2[x]/(x^3+x^2+x)$. Определить, будет ли это кольцо полем.

1.32. Пусть $[x+1]$ — класс вычетов многочлена $x+1$ в факторкольце $\mathbb{F}_2[x]/(x^4+1)$. Найти классы вычетов, составляющие главный идеал $([x+1])$ в указанном факторкольце.

1.33. Пусть F — поле и $a, b, g \in F[x]$, причем $g \neq 0$. Доказать, что сравнение $af \equiv b \pmod g$ имеет решение $f \in F[x]$ тогда и только тогда, когда НОД (a, g) делит многочлен b.

1.34. Решить сравнение $(x^2+1)f(x) \equiv 1 \pmod{(x^3+1)}$ в $\mathbb{F}_3[x]$, если это возможно.

1.35. Решить, если это возможно, сравнение

$$(x^4+x^3+x^2+1)f(x) \equiv x^2+1 \pmod{(x^3+1)}$$

в $\mathbb{F}_2[x]$.

1.36. Доказать, что факторкольцо $R[x]/(x^4+x^3+x+1)$ не может быть полем, каким бы ни было коммутативное кольцо R с единицей.

1.37. Доказать, что если F — поле, $g_1, \ldots, g_k$ — произвольные, а $f_1, \ldots, f_k$ — ненулевые попарно взаимно простые многочлены из $F[x]$, то система сравнений $h \equiv g_i \pmod{f_i}$, $i = 1, \ldots, k$, имеет единственное решение $h \in F[x]$ по модулю $f = f_1 \ldots f_k$ (китайская теорема об остатках для кольца $F[x]$).

1.38. Подсчитать $f(3)$ для многочлена

$$f(x) = x^{214} + 3x^{152} + 2x^{47} + 2 \in \mathbb{F}_5[x].$$

1.39. Пусть p — простое число, $a_0, \ldots, a_n \in Z$ и p не делит a_n. Показать, что сравнение $a_0 + a_1 y + \ldots + a_n y^n \equiv 0 \pmod p$ имеет не более n различных решений y по модулю p.

1.40. Доказать, что для простого числа $p > 2$ существует ровно два элемента $a \in \mathbb{F}_p$, таких, что $a^2 = 1$.

1.41. Показать, что многочлен $f \in Z[x]$, такой, что $f(0) \equiv f(1) \equiv 1 \pmod 2$, не может иметь корней в Z.

1.42. Пусть p — простое число и $f \in Z[x]$. Показать, что сравнение $f(a) \equiv 0 \pmod p$ выполняется для всех $a \in Z$ в том и только том случае, если $f(x) = (x^p - x)g(x) + ph(x)$ для некоторых $g, h \in Z[x]$.

1.43. Пусть p — простое число и c — элемент некоторого поля F. Показать, что многочлен $x^p - c$ тогда и только тогда неприводим над F, когда он не имеет корней в поле F.

1.44. Показать, что для многочлена f положительной степени над полем F следующие условия эквивалентны:

(a) многочлен f неприводим над F;

(b) главный идеал (f) кольца $F[x]$ является максимальным идеалом;

(c) главный идеал (f) кольца $F[x]$ является простым идеалом.

1.45. Доказать следующие свойства производной многочленов над полем F:

(a) $(f_1 + \ldots + f_m)' = f_1' + \ldots + f_m'$;

(b) $(fg)' = f'g + fg'$;

(c) $(f_1 \ldots f_m)' = \sum_{i=1}^{m} f_1 \ldots f_{i-1} f_i' f_{i+1} \ldots f_m$.

1.46. Пусть f — многочлен над полем F. Доказать, что если характеристика поля F равна 0, то $f' = 0$ тогда и только тогда, когда f — постоянный многочлен; если же F — поле простой характеристики p, то $f' = 0$ тогда и только тогда, когда $f(x) = g(x^p)$ для некоторого многочлена $g \in F[x]$.

1.47. Доказать теорему 1.68.

1.48. Доказать, что ненулевой многочлен f над полем F имеет кратные корни (из некоторого расширения поля F) тогда и только тогда, когда f и f' не взаимно просты.

1.49. Применить критерий, полученный в предыдущем упражнении, для выяснения вопроса, имеют ли следующие многочлены кратные корни:
(a) $f(x) = x^4 - 5x^3 + 6x^2 + 4x - 8 \in \mathbb{Q}[x]$;
(b) $f(x) = x^6 + x^5 + x^4 + x^3 + 1 \in \mathbb{F}_2[x]$.

1.50. n-я производная $f^{(n)}$ многочлена f над полем F определяется рекуррентно следующим образом: $f^{(0)} = f$, $f^{(n)} = (f^{(n-1)})'$ для $n \geqslant 1$. Доказать, что для $f, g \in F[x]$ имеет место соотношение

$$(fg)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} f^{(n-i)} g^{(i)}$$

(формула Лейбница).

1.51. Пусть F — некоторое поле и k — натуральное число (если F — поле простой характеристики p, то предполагается, что $k < p$). Доказать, что элемент $b \in F$ является корнем кратности k многочлена $f \in F[x]$ в том и только том случае, если $f^{(i)}(b) = 0$ для $0 \leqslant i \leqslant k-1$ и $f^{(k)}(b) \neq 0$.

1.52. Доказать, что интерполяционную формулу Лагранжа (см. теорему 1.71) можно записать также в следующем виде:

$$f(x) = \sum_{i=0}^{n} b_i (g'(a_i))^{-1} \frac{g(x)}{x - a_i}, \quad \text{где} \quad g(x) = \prod_{k=0}^{n} (x - a_k).$$

1.53. Найти многочлен $f \in \mathbb{F}_5[x]$, такой, что $f(0) = f(1) = f(4) = 1$, а $f(2) = f(3) = 3$.

1.54. Найти многочлен $f \in \mathbb{Q}[x]$ степени $\leqslant 3$, такой, что $f(-1) = -1$, $f(0) = 3$, $f(1) = 3$, $f(2) = 5$.

1.55. Выразить многочлен $s_5(x_1, x_2, x_3, x_4) = x_1^5 + x_2^5 + x_3^5 + x_4^5 \in \mathbb{F}_3[x_1, x_2, x_3, x_4]$ через элементарные симметрические многочлены от четырех переменных σ_1, σ_2, σ_3 и σ_4 (см. пример 1.74).

1.56. Доказать, что подмножество K поля F является его подполем тогда и только тогда, когда выполняются следующие условия:
(a) K содержит по крайней мере два элемента;
(b) если $a, b \in K$, то $a - b \in K$;
(c) если $a, b \in K$ и $b \neq 0$, то $ab^{-1} \in K$.

1.57. Доказать, что расширение L поля K является конечным расширением в том и только том случае, если L может быть получено из K присоединением конечного числа алгебраических над K элементов.

1.58. Доказать, что если θ — алгебраический элемент над полем L, где L — алгебраическое расширение поля K, то элемент θ является алгебраическим также над полем K. Это значит, что если F — алгебраическое расширение поля L, то F — в то же время и алгебраическое расширение поля K.

1.59. Доказать, что если L — расширение поля K и степень $[L : K]$ — простое число, то единственными полями F, удовлетворяющими условию $K \subseteq F \subseteq L$, являются $F = K$ и $F = L$.

1.60. Построить таблицы сложения и умножения для поля $L = \mathbb{F}_3(\theta)$ из примера 1.88.

1.61. Доказать неприводимость над $\mathbb{F}_2$ многочлена $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ и построить таблицы операций для простого расширения $\mathbb{F}_2(\theta)$, где θ — корень многочлена f.

1.62. Вычислить дискриминант $D(f)$ многочлена f и с его помощью выяснить, имеет или нет многочлен f кратные корни:
(a) $f(x) = 2x^3 - 3x^2 + x + 1 \in \mathbb{Q}[x]$;
(b) $f(x) = 2x^4 + x^3 + x^2 + 2x + 2 \in \mathbb{F}_3[x]$.

1.63. Вывести формулу (1.9) из (1.11).

1.64. Доказать, что многочлены f и g из $K[x]$ (K — поле) имеют общий корень (из некоторого расширения поля K) в том и только том случае, если f и g имеют общий делитель положительной степени из $K[x]$.

1.65. Найти общие корни многочленов $x^7 - 2x^4 - x^3 + 2$ и $x^5 - 3x^4 - x + 3$ из $\mathbb{Q}[x]$.

1.66. Доказать, что если f и g — многочлены из определения 1.93, то $R(f, g) = (-1)^{mn} R(g, f)$.

1.67. Пусть f и g — многочлены положительной степени над полем K, и пусть в поле разложения многочлена fg над K имеем $f(x) = a_0(x - \alpha_1) \ldots (x - \alpha_n)$, $a_0 \neq 0$, $g(x) = b_0(x - \beta_1) \ldots (x - \beta_m)$, $b_0 \neq 0$. Доказать, что

$$R(f, g) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j),$$

где в качестве формальных степеней многочленов f и g берутся соответственно их степени n и m.

1.68. Вычислить результант $R(f, g)$ двух данных многочленов f и g (при формальных степенях, совпадающих со степенями) и выяснить, имеют или нет эти многочлены общие корни:

(a) $f(x) = x^3 + x + 1$, $g(x) = 2x^5 + x^2 + 2 \in \mathbb{F}_3[x]$;

(b) $f(x) = x^4 + x^3 + 1$, $g(x) = x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]$.

1.69. Для многочлена $f \in K[x_1, \ldots, x_n]$ от $n \geqslant 2$ переменных над полем K *нулем* можно назвать такой n-набор $(\alpha_1, \ldots, \alpha_n)$ элементов α_i, принадлежащих некоторому расширению поля K, для которого $f(\alpha_1, \ldots, \alpha_n) = 0$. Пусть теперь $f, g \in K[x_1, \ldots, x_n]$ и переменная x_n фактически входит в многочлены f и g. Тогда оба этих многочлена можно рассматривать как многочлены $\bar{f}(x_n)$ и $\bar{g}(x_n)$ положительной степени от одной переменной x_n из кольца $K[x_1, \ldots, x_{n-1}][x_n]$. Результаит этих многочленов (при формальных степенях, совпадающих со степенями) $R(\bar{f}, \bar{g}) = R_{x_n}(f, g)$ тогда является многочленом от перемеиных $x_1, \ldots, x_{n-1}$. Показать, что многочлены f и g имеют общий нуль $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$ тогда и только тогда, когда $(n-1)$-набор $(\alpha_1, \ldots, \alpha_{n-1})$ является иулем результанта $R(\bar{f}, \bar{g})$.

1.70. Используя результат предыдущего упражнения, иайти общие иули многочленов $f(x, y) = x(y^2 - x)^2 + y^5$ и $g(x, y) = y^4 + y^2 - x^2$ из $\mathbb{Q}[x, y]$.

Глава 2

Строение конечных полей

Это наиболее важная глава, так как в ней излагаются основные свойства конечных полей и описываются методы построения конечных полей.

Наиболее известным примером конечного поля является поле классов вычетов по простому модулю, т. е. факторкольцо $\mathbb{Z}/(p)$, где p — простое число. Многие свойства этого поля сохраняются и для произвольных конечных полей.

В § 1 устанавливается, что порядком каждого конечного поля является некоторая степень простого числа и, наоборот, для каждой степени простого числа $q = p^n$, $n \in \mathbb{N}$, существует конечное поле, состоящее из q элементов. Более того, оказывается, что все конечные поля с одним и тем же числом элементов изоморфны друг другу и потому могут быть отождествлены.

В следующих двух параграфах даются сведения о корнях неприводимых многочленов, позволяющие рассматривать каждое конечное поле как поле разложения некоторого неприводимого многочлена над его простым подполем, а также о следах, нормах и базисах, определяемых конечным полем и его расширением.

В § 4 корни из единицы изучаются с точки зрения общей теории полей (это понадобится в § 6, а также в гл. 5). В § 5 указываются разные способы представления элементов конечного поля. И наконец, в § 6 даются два доказательства известной теоремы Веддербёрна о том, что каждое конечное тело является полем.

В последующих главах многие идеи и методы этой главы получат дальнейшее развитие.

§ 1. Характеризация конечных полей

В гл. 1 мы уже встретились с важным классом конечных полей, т. е. полей, состоящих из конечного числа элементов. А именно было установлено (теорема 1.38), что для каждого простого числа p факторкольцо $\mathbb{Z}/(p)$ является конечным полем, состоящим из p элементов, которое может быть отождествлено с полем Галуа $\mathbb{F}_p = GF(p)$ порядка p (см. определение 1.41).

Поле $\mathbb{F}_p$ играет важную роль в общей теории полей, так как, согласно теореме 1.78, каждое поле характеристики p должно содержать изоморфное $\mathbb{F}_p$ подполе и потому может рассматриваться как расширение поля $\mathbb{F}_p$. Это замечание играет основную роль в классификации конечных полей, поскольку характеристика каждого конечного поля является простым числом (следствие 1.45).

Установим прежде всего одно простое предложение о числе элементов конечного поля.

2.1. Лемма. *Пусть F — конечное поле, содержащее подполе K из q элементов. Тогда F состоит из q^m элементов, где $m = [F : K]$.*

Доказательство. Поле F можно рассматривать как векторное пространство над полем K. В силу конечности F это пространство конечномерно. Если $[F : K] = m$, то F имеет базис над полем K, состоящий из m элементов, скажем, $b_1, \ldots, b_m$. Таким образом, каждый элемент поля F может быть однозначно представлен в виде линейной комбинации $a_1b_1 + \ldots + a_mb_m$, где $a_1, \ldots, a_m \in K$. Так как каждый коэффициент a_i может принимать q значений, то поле F состоит в точности из q^m элементов. □

2.2. Теорема. *Пусть F — конечное поле. Тогда оно состоит из p^n элементов, где простое число p является характеристикой поля F, а натуральное число n является степенью поля F над его простым подполем.*

Доказательство. Так как поле F конечно, то его характеристика — некоторое простое число p (см. следствие 1.45). Поэтому простое подполе K поля F изоморфно $\mathbb{F}_p$, согласно теореме 1.78, и, значит, содержит p элементов. Остальное вытекает из леммы 2.1. □

Отправляясь от простых полей $\mathbb{F}_p$, мы можем строить другие конечные поля с помощью процесса присоединения корня, описанного в § 4 гл. 1. Если $f \in \mathbb{F}_p[x]$ — неприводимый многочлен степени n над $\mathbb{F}_p$, то, присоединяя к $\mathbb{F}_p$ корень этого многочлена, мы получим конечное поле из p^n элементов. Однако на этом этапе еще неясно, существует ли для каждого натурального числа n неприводимый многочлен степени n из $\mathbb{F}_p[x]$. Чтобы установить, что для каждого простого p и каждого натурального n существует конечное поле из p^n элементов, мы используем другой подход, подсказываемый следующей леммой.

2.3. Лемма. *Если F — конечное поле из q элементов, то каждый элемент $a \in F$ удовлетворяет равенству $a^q = a$.*

Доказательство. Для $a = 0$ равенство $a^q = a$ выполняется тривиально. Что же касается ненулевых элементов поля F, то

они образуют мультипликативную группу порядка $q-1$, так что для каждого ненулевого элемента $a \in F$ выполняется равенство $a^{q-1}=1$, умножение которого на a приводит к требуемому результату. □

2.4. Лемма. *Если F — конечное поле из q элементов и K — подполе поля F, то многочлен x^q-x из $K[x]$ вполне разлагается в $F[x]$ следующим образом:*

$$x^q-x=\prod_{a\in F}(x-a),$$

так что F является полем разложения многочлена x^q-x над полем K.

Доказательство. Многочлен x^q-x степени q имеет не более q различных корней в поле F. В силу леммы 2.3 нам известно q таких различных корней — ими являются все элементы поля F. Таким образом, данный многочлен разлагается в поле F указанным в формулировке образом и не может вполне разлагаться ни в каком меньшем поле. □

Теперь мы в состоянии доказать главную характеризационную теорему для конечных полей, основная идея которой содержится в лемме 2.4.

2.5. Теорема (существование и единственность конечных полей). *Для каждого простого числа p и каждого натурального числа n существует конечное поле из p^n элементов. Любое конечное поле из $q=p^n$ элементов изоморфно полю разложения многочлена x^q-x над полем $\mathbb{F}_p$.*

Доказательство. Существование. Для $q=p^n$ рассмотрим многочлен x^q-x из $\mathbb{F}_p[x]$, и пусть F будет его полем разложения над $\mathbb{F}_p$. Указанный многочлен имеет q различных корней в поле F, так как его производная является постоянным многочленом $qx^{q-1}-1=-1\neq 0$ из $\mathbb{F}_p[x]$ и в силу этого не может иметь общих корней с x^q-x (см. теорему 1.68). Положим $S=\{a\in F \mid a^q-a=0\}$. Тогда S является подполем поля F, так как (i) S содержит 0 и 1; (ii) если $a, b\in S$, то по теореме 1.46 $(a-b)^q=a^q-b^q=a-b$, а значит, $a-b\in S$; (iii) для $a, b\in S$, $b\neq 0$, имеем $(ab^{-1})^q=a^qb^{-q}=ab^{-1}$, так что $ab^{-1}\in S$. Но, с другой стороны, многочлен x^q-x должен вполне разлагаться в S, так как поле S содержит все его корни. Таким образом, $S=F$, а поскольку S состоит из q элементов, то F является конечным полем из q элементов.

Единственность. Пусть F — конечное поле из $q = p^n$ элементов. Тогда F имеет характеристику p (теорема 2.2) и потому содержит в качестве подполя поле $\mathbb{F}_p$. Из леммы 2.4 следует, что F является полем разложения многочлена $x^q - x$ над полем $\mathbb{F}_p$. Требуемый результат теперь вытекает из единственности (с точностью до изоморфизма) поля разложения (теорема 1.91). □

Доказанная в теореме 2.5 единственность позволяет говорить о вполне определенном конечном поле данного порядка q (т. е. о поле Галуа из q элементов). Будем обозначать его через $\mathbb{F}_q$, где под q понимается степень некоторого простого числа p, которое является характеристикой этого поля (теорема 2.2).

2.6. Теорема (критерий подполя). *Пусть $\mathbb{F}_q$ — конечное поле из $q = p^n$ элементов (p — простое число). Тогда каждое подполе поля $\mathbb{F}_q$ имеет порядок p^m, где m является положительным делителем числа n. Обратно, если m — положительный делитель числа n, то существует ровно одно подполе поля $\mathbb{F}_q$ из p^m элементов.*

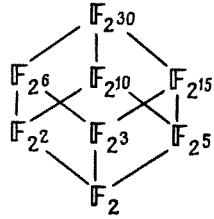
Доказательство. Ясно, что любое подполе K поля $\mathbb{F}_q$ должно иметь порядок p^m, где m — натуральное число, не превосходящее n. Из леммы 2.1 следует, что число $q = p^n$ должно быть степенью числа p^m, так что m обязательно делит число n.

Обратно, если m — положительный делитель числа n, то $p^m - 1$ делит число $p^n - 1$, так что многочлен $x^{p^m-1} - 1$ делит многочлен $x^{p^n-1} - 1$ в $\mathbb{F}_p[x]$. Следовательно, $x^{p^m} - x$ делит многочлен $x^{p^n} - x = x^q - x$ в $\mathbb{F}_p[x]$. Таким образом, каждый корень многочлена $x^{p^m} - x$ является корнем многочлена $x^q - x$ и, значит, принадлежит полю $\mathbb{F}_q$. Поэтому поле $\mathbb{F}_q$ должно содержать в качестве подполя поле разложения многочлена $x^{p^m} - x$ над $\mathbb{F}_p$, а из доказательства теоремы 2.5 мы видели, что такое поле разложения имеет порядок p^m. Если бы поле $\mathbb{F}_q$ содержало два различных подполя порядка p^m, то эти подполя содержали бы в совокупности больше чем p^m корней многочлена $x^{p^m} - x$ в поле $\mathbb{F}_q$, а это невозможно. □

Доказательство теоремы 2.6 показывает, что если m — положительный делитель числа n, то в поле $\mathbb{F}_{p^n}$ имеется единственное подполе порядка p^m, и это подполе состоит в точности из корней многочлена $x^{p^m} - x \in \mathbb{F}_p[x]$ в поле $\mathbb{F}_{p^n}$.

2.7. Пример. Подполя конечного поля $\mathbb{F}_{2^{30}}$ можно найти, составив список всех положительных делителей числа 30. Отно-

шения включения между этими подполями указаны в следующей диаграмме.



Согласно теореме 2.6, эти отношения включения равносильны отношениям делимости соответствующих делителей числа 30. □

Для конечного поля $\mathbb{F}_q$ мы будем через $\mathbb{F}_q^*$ обозначать мультипликативную группу его ненулевых элементов. Следующий результат устанавливает одно важное свойство этой группы.

2.8. Теорема. *Мультипликативная группа $\mathbb{F}_q^*$ ненулевых элементов произвольного конечного поля $\mathbb{F}_q$ циклическая.*

Доказательство. Можно предположить, что $q \geqslant 3$. Пусть $h = p_1^{r_1} \ldots p_m^{r_m}$ — разложение порядка $h = q - 1$ группы $\mathbb{F}_q^*$ на простые сомножители. Для каждого i, $1 \leqslant i \leqslant m$, многочлен $x^{h/p_i} - 1$ имеет не более h/p_i корней в поле $\mathbb{F}_q$. Поскольку $h/p_i < h$, то в поле $\mathbb{F}_q$ имеются ненулевые элементы, не являющиеся корнями этого многочлена. Пусть a_i — такой элемент; положим $b_i = a_i^{h/p_i^{r_i}}$. Тогда $b_i^{p_i^{r_i}} = 1$, откуда следует, что порядок элемента b_i является делителем числа $p_i^{r_i}$ и, значит, имеет вид $p_i^{s_i}$, где $0 \leqslant s_i \leqslant r_i$. С другой стороны,

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1,$$

так что порядок элемента b_i равен $p_i^{r_i}$. Покажем теперь, что элемент $b = b_1 b_2 \ldots b_m$ имеет порядок h. Допустим, что это не так и что порядок элемента b является собственным делителем числа h, а значит, делителем по крайней мере одного из m целых чисел h/p_i, $1 \leqslant i \leqslant m$, скажем h/p_1. Тогда

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \ldots b_m^{h/p_1}.$$

Теперь если $2 \leqslant i \leqslant m$, то $p_i^{r_i}$ делит число h/p_1, так что $b_i^{h/p_1} = 1$. Поэтому $b_1^{h/p_1} = 1$. Это означает, что порядок элемента b_1 должен делить число h/p_1, а это невозможно, так как он равен $p_1^{r_1}$. Итак, $\mathbb{F}_q^*$ — циклическая группа с образующим элементом b. □

2.9. Определение. Образующий элемент циклической группы $\mathbb{F}_q^*$ называется *примитивным элементом* поля $\mathbb{F}_q$.

Из теоремы 1.15 (v) следует, что поле $\mathbb{F}_q$ содержит $\varphi(q-1)$ примитивных элементов, где φ — функция Эйлера. Наличием в любом конечном поле примитивных элементов можно воспользоваться, например, для доказательства того факта, что каждое конечное поле является простым алгебраическим расширением своего простого подполя.

2.10. Теорема. *Пусть $\mathbb{F}_q$ — конечное поле и $\mathbb{F}_r$ — его конечное расширение. Тогда $\mathbb{F}_r$ является простым алгебраическим расширением поля $\mathbb{F}_q$, причем образующим элементом этого простого расширения может служить любой примитивный элемент поля $\mathbb{F}_r$.*

Доказательство. Пусть ζ — любой примитивный элемент поля $\mathbb{F}_r$. Тогда очевидно, что $\mathbb{F}_q(\zeta) \subseteq \mathbb{F}_r$. С другой стороны, поле $\mathbb{F}_q(\zeta)$ содержит 0 и все степени элемента ζ, а значит, все элементы поля $\mathbb{F}_r$. Следовательно, $\mathbb{F}_q(\zeta) = \mathbb{F}_r$.

2.11. Следствие. *Для каждого конечного поля $\mathbb{F}_q$ и каждого натурального числа n в кольце $\mathbb{F}_q[x]$ существует неприводимый многочлен степени n.*

Доказательство. Пусть $\mathbb{F}_r$ — расширение поля $\mathbb{F}_q$ порядка q^n, так что $[\mathbb{F}_r : \mathbb{F}_q] = n$. Согласно теореме 2.10, существует такой элемент $\zeta \in \mathbb{F}_r$, что $\mathbb{F}_r = \mathbb{F}_q(\zeta)$. Но тогда в соответствии с теоремами 1.82 (i) и 1.86 (ii) минимальный многочлен элемента ζ над $\mathbb{F}_q$ является неприводимым многочленом степени n в кольце $\mathbb{F}_q[x]$. □

§ 2. Корни неприводимых многочленов

В этом параграфе мы исследуем вопрос о множестве корней неприводимого многочлена над конечным полем.

2.12. Лемма. *Пусть $f \in \mathbb{F}_q[x]$ — неприводимый многочлен над конечным полем $\mathbb{F}_q$, и пусть α — корень этого многочлена в некотором расширении поля $\mathbb{F}_q$. Тогда для многочлена $h \in \mathbb{F}_q[x]$ равенство $h(\alpha) = 0$ выполняется в том и только том случае, если многочлен f делит h.*

Доказательство. Пусть a — старший коэффициент многочлена f. Положим $g(x) = a^{-1}f(x)$. Тогда g — нормированный неприводимый многочлен из $\mathbb{F}_q[x]$, причем $g(\alpha) = 0$, а значит, g — минимальный многочлен элемента α над $\mathbb{F}_q$ в смысле определения 1.81. Остальное вытекает из теоремы 1.82 (ii). □

2.13. Лемма. *Пусть $f \in \mathbb{F}_q[x]$ — неприводимый многочлен степени m над $\mathbb{F}_q$. Тогда $f(x)$ делит многочлен $x^{q^n} - x$ в том и только том случае, если число m делит n.*

Доказательство. Допустим, что многочлен $f(x)$ делит $x^{q^n} - x$. Пусть α — некоторый корень многочлена f в поле разложения этого многочлена над $\mathbb{F}_q$. Тогда $\alpha^{q^n} = \alpha$, так что $\alpha \in \mathbb{F}_{q^n}$. Значит, простое расширение $\mathbb{F}_q(\alpha)$ поля $\mathbb{F}_q$ является подполем поля $\mathbb{F}_{q^n}$. Но так как $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ и $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, то из теоремы 1.84 следует, что число m делит n.

Обратно, если m делит n, то из теоремы 2.6 следует, что поле $\mathbb{F}_{q^n}$ содержит $\mathbb{F}_{q^m}$ в качестве подполя. Если α — некоторый корень многочлена f в поле разложения этого многочлена над $\mathbb{F}_q$, то $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, так что $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Следовательно, $\alpha \in \mathbb{F}_{q^n}$, значит, $\alpha^{q^n} = \alpha$ и, таким образом, α — корень многочлена $x^{q^n} - x \in \mathbb{F}_q[x]$. Тогда в соответствии с леммой 2.12 мы заключаем, что $f(x)$ делит многочлен $x^{q^n} - x$. □

2.14. Теорема. *Если $f \in \mathbb{F}_q[x]$ — неприводимый многочлен степени m, то в поле $\mathbb{F}_{q^m}$ содержится любой корень α многочлена f. Более того, все корни многочлена f просты и ими являются m различных элементов α, α^q, α^{q^2}, ..., $\alpha^{q^{m-1}}$ поля $\mathbb{F}_{q^m}$.*

Доказательство. Пусть α — произвольный корень многочлена f в поле разложения этого многочлена над $\mathbb{F}_q$. Тогда $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, так что $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, и, в частности, $\alpha \in \mathbb{F}_{q^m}$. Покажем теперь, что если $\beta \in \mathbb{F}_{q^m}$ — какой-нибудь корень многочлена f, то β^q — тоже корень этого многочлена. Пусть f записан в виде $f(x) = a_m x^m + \ldots + a_1 x + a_0$, где $a_i \in \mathbb{F}_q$, $0 \leqslant i \leqslant m$. Применяя лемму 2.3 и теорему 1.46, получим

$$f(\beta^q) = a_m\beta^{q^m} + \ldots + a_1\beta^q + a_0 = a_m^q\beta^{q^m} + \ldots + a_1^q\beta^q + a_0^q = (a_m\beta^m + \ldots + a_1\beta + a_0)^q = f(\beta)^q = 0.$$

Поэтому элементы α, α^q, α^{q^2}, ..., $\alpha^{q^{m-1}}$ являются корнями многочлена f. Остается доказать, что эти элементы различны. Допустим обратное. Тогда $\alpha^{q^j} = \alpha^{q^k}$ для некоторых целых j и k, $0 \leqslant j < k \leqslant m - 1$. Возводя это равенство в степень q^{m-k}, получим

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

Из леммы 2.12 тогда следует, что многочлен $f(x)$ делит многочлен $x^{q^{m-k+j}} - x$, а по лемме 2.13 это возможно лишь в случае когда число m делит $m - k + j$. Но так как $0 < m - k + j < m$ то мы получаем противоречие. □

2.15. Следствие. *Если $f \in \mathbb{F}_q[x]$ — неприводимый многочлен степени m, то его полем разложения над полем $\mathbb{F}_q$ является $\mathbb{F}_{q^m}$.*

Доказательство. Из теоремы 2.14 следует, что многочлен f вполне разлагается в поле $\mathbb{F}_{q^m}$. При этом для некоторого корня α многочлена f имеем $\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha)$. Но из доказательства той же теоремы 2.14 видно, что $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. □

2.16. Следствие. *Поля разложения любых двух неприводимых многочленов одной и той же степени из кольца* $\mathbb{F}_q[x]$ *изоморфны.*

Введем более удобную терминологию для элементов, появляющихся в теореме 2.14, не зависящую от того, является элемент $\alpha \in \mathbb{F}_{q^m}$ корнем некоторого неприводимого многочлена степени m из $\mathbb{F}_q[x]$ или нет.

2.17. Определение. Пусть $\mathbb{F}_{q^m}$ — расширение поля $\mathbb{F}_q$, и пусть $\alpha \in \mathbb{F}_{q^m}$. Тогда элементы

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

называются *сопряженными* с элементом α относительно поля $\mathbb{F}_q$.

Сопряженные с $\alpha \in \mathbb{F}_{q^m}$ относительно поля $\mathbb{F}_q$ элементы различны тогда и только тогда, когда минимальный многочлен элемента α над $\mathbb{F}_q$ имеет степень m. Если же это не так, то степень d минимального многочлена элемента α является собственным делителем числа m, и тогда среди сопряженных с α относительно $\mathbb{F}_q$ элементов различными будут лишь элементы $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$, каждый из которых повторяется в ряду сопряженных m/d раз [1]).

2.18. Теорема. *Элементы, сопряженные с элементом* $\alpha \in \mathbb{F}_q^*$ *относительно любого подполя поля* $\mathbb{F}_q$, *имеют один и тот же порядок в группе* $\mathbb{F}_q^*$.

Доказательство. Так как, согласно теореме 2.8, $\mathbb{F}_q^*$ — циклическая группа, то этот результат следует из теоремы 1.15 (ii) и того, что каждая степень характеристики поля $\mathbb{F}_q$ взаимно проста с порядком $q - 1$ группы $\mathbb{F}_q^*$. □

2.19. Следствие. *Если* α — *примитивный элемент поля* $\mathbb{F}_q$, *то примитивными также будут и все сопряженные с ним относительно любого подполя поля* $\mathbb{F}_q$ *элементы.*

2.20. Пример. Пусть $\alpha \in \mathbb{F}_{16}$ — корень многочлена $f(x) = x^4 + x + 1$ из $\mathbb{F}_2[x]$. Тогда сопряженными с α относительно поля $\mathbb{F}_2$ будут элементы α, α^2, $\alpha^4 = \alpha + 1$ и $\alpha^8 = \alpha^2 + 1$, каждый из которых является примитивным элементом поля $\mathbb{F}_{16}$.

---

[1]) Последнее вытекает из того, что ввиду $\alpha^{q^m} = \alpha$ совокупность $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ инвариантна относительно возведения ее членов в степень q. — *Прим. перев.*

Сопряженными же с α относительно поля $\mathbb{F}_4$ являются лишь элементы α и $\alpha^4 = \alpha + 1$. □

Существует тесная связь между сопряженными элементами и автоморфизмами конечного поля. Пусть $\mathbb{F}_{q^m}$ — расширение поля $\mathbb{F}_q$. Назовем *автоморфизмом* σ поля $\mathbb{F}_{q^m}$ *над* $\mathbb{F}_q$ такой автоморфизм поля $\mathbb{F}_{q^m}$, который оставляет неподвижными элементы поля $\mathbb{F}_q$. Точнее говоря, σ — такое взаимно однозначное отображение из $\mathbb{F}_{q^m}$ на себя, что $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ и $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ для любых $\alpha, \beta \in \mathbb{F}_{q^m}$, и $\sigma(a) = a$ для любых $a \in \mathbb{F}_q$.

2.21. Теорема. *Различными автоморфизмами поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ являются отображения $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, определяемые условиями $\sigma_j(\alpha) = \alpha^{q^j}$, где $\alpha \in \mathbb{F}_{q^m}$, $0 \leqslant j \leqslant m - 1$, и только они.*

Доказательство. Для каждого отображения σ_j и любых $\alpha, \beta \in \mathbb{F}_{q^m}$ мы, очевидно, имеем $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ и $\sigma_j(\alpha + \beta) = \sigma_j(\alpha) + \sigma_j(\beta)$ ввиду теоремы 1.46, так что σ_j является эндоморфизмом поля $\mathbb{F}_{q^m}$. Кроме того, $\sigma_j(\alpha) = 0$ тогда и только тогда, когда $\alpha = 0$, так что σ_j — взаимно однозначное отображение. Но поскольку $\mathbb{F}_{q^m}$ — конечное множество, σ_j является эпиморфизмом, а следовательно, и автоморфизмом поля $\mathbb{F}_{q^m}$. Кроме того, по лемме 2.3 $\sigma_j(a) = a$ для всех $a \in \mathbb{F}_q$. Итак, каждое σ_j есть некоторый автоморфизм поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. При этом отображения $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ различны, так как они переводят фиксированный примитивный элемент поля $\mathbb{F}_{q^m}$ в разные элементы.

Предположим теперь, что σ — любой автоморфизм поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Пусть β — некоторый примитивный элемент поля $\mathbb{F}_{q^m}$ и $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in \mathbb{F}_q[x]$ — его минимальный многочлен над $\mathbb{F}_q$. Тогда

$$0 = \sigma(\beta^m + a_{m-1}\beta^{m-1} + \ldots + a_0) = \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \ldots + a_0,$$

так что элемент $\sigma(\beta) \in \mathbb{F}_{q^m}$ тоже является корнем многочлена f. Из теоремы 2.14 следует, что $\sigma(\beta) = \beta^{q^j}$ для некоторого j, $0 \leqslant j \leqslant m - 1$. Но так как σ — гомоморфизм, то тогда для любого $\alpha \in \mathbb{F}_{q^m}$ получаем $\sigma(\alpha) = \alpha^{q^j}$ (поскольку любой элемент $\alpha \neq 0$ представим степенью элемента β). □

На основании доказанной теоремы ясно, что сопряженные с данным элементом $\alpha \in \mathbb{F}_{q^m}$ относительно $\mathbb{F}_q$ элементы можно получить, действуя на α автоморфизмами поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Поскольку автоморфизмы поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ образуют группу относительно операции композиции отображений, то из теоремы 2.21 следует, что эта группа является циклической группой порядка m с образующим элементом σ_1.

§ 3. Следы, нормы и базисы

В этом параграфе мы снова будем рассматривать конечное расширение $F = \mathbb{F}_{q^m}$ конечного поля $K = \mathbb{F}_q$ как векторное пространство над K (см. гл. 1, § 4). Тогда размерность F над K равна m, и если $\{\alpha_1, \ldots, \alpha_m\}$ — базис векторного пространства F над полем K [1]), то каждый элемент $\alpha \in F$ однозначно представим в виде линейной комбинации

$$\alpha = c_1\alpha_1 + \cdots + c_m\alpha_m, \quad c_j \in K, \quad 1 \leqslant j \leqslant m.$$

Введем важную функцию из F в K, которая, как мы позже увидим, оказывается линейной функцией.

2.22. Определение. Пусть $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$ и $\alpha \in F$. Определим *след* $\mathrm{Tr}_{F/K}(\alpha)$ элемента α над K равенством

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}.$$

Если K — простое подполе поля F, то $\mathrm{Tr}_{F/K}(\alpha)$ называется *абсолютным следом* элемента α и обозначается просто $\mathrm{Tr}_F(\alpha)$.

Другими словами, след $\mathrm{Tr}_{F/K}(\alpha)$ элемента α над полем K есть сумма всех сопряженных с α относительно K элементов. Дадим еще одно определение следа. Пусть $f \in K[x]$ — минимальный многочлен элемента $\alpha \in F = \mathbb{F}_{q^m}$ над полем $K = \mathbb{F}_q$. Его степень d является делителем числа m. Назовем многочлен $g(x) = f(x)^{m/d}$ из $K[x]$ *характеристическим многочленом* элемента α над полем K. Согласно теореме 2.14, корнями многочлена f в поле F являются элементы α, α^q, ..., $\alpha^{q^{d-1}}$, поэтому, учитывая замечание, следующее за определением 2.17, получаем, что корнями многочлена g в поле F являются те и только те элементы, которые сопряжены с элементом α относительно поля K. Отсюда

$$g(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 = (x - \alpha)(x - \alpha^q) \ldots (x - \alpha^{q^{m-1}}), \tag{2.1}$$

и сравнение коэффициентов дает

$$\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1}. \tag{2.2}$$

В частности, получаем, что след $\mathrm{Tr}_{F/K}(\alpha)$ всегда является элементом поля K.

2.23. Теорема. *Пусть $K = \mathbb{F}_q$ и $F = \mathbb{F}_{q^m}$. Тогда функция следа $\mathrm{Tr}_{F/K}$ обладает следующими свойствами:*

(i) $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ *для всех* $\alpha, \beta \in F$;

(ii) $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$ *для всех* $c \in K$, $\alpha \in F$;

[1]) В дальнейшем мы будем часто называть его *базисом поля F над K*. — *Прим. перев.*

(iii) $\mathrm{Tr}_{F/K}$ *является линейным отображением из* F *на* K, *где* F *и* K *рассматриваются как векторные пространства над полем* K;

(iv) $\mathrm{Tr}_{F/K}(a) = ma$ *для всех* $a \in K$;

(v) $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ *для всех* $\alpha \in F$.

Доказательство. (i) Используя теорему 1.46 для $\alpha, \beta \in F$, получим

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q+\ldots+(\alpha+\beta)^{q^{m-1}} = \\ &= \alpha+\beta+\alpha^q+\beta^q+\ldots+\alpha^{q^{m-1}}+\beta^{q^{m-1}} = \\ &= \mathrm{Tr}_{F/K}(\alpha)+\mathrm{Tr}_{F/K}(\beta).\end{aligned}$$

(ii) Для $c \in K$ по лемме 2.3 $c^{q^j} = c$ для всех $j \geqslant 0$. Поэтому для $\alpha \in F$

$$\begin{aligned}\mathrm{Tr}_{F/K}(c\alpha) &= c\alpha + c^q\alpha^q + \ldots + c^{q^{m-1}}\alpha^{q^{m-1}} = \\ &= c\alpha + c\alpha^q + \ldots + c\alpha^{q^{m-1}} = c\mathrm{Tr}_{F/K}(\alpha).\end{aligned}$$

(iii) Из свойств (i) и (ii) с учетом того, что $\mathrm{Tr}_{F/K}(\alpha) \in K$ для всех $\alpha \in F$, получаем, что функция следа $\mathrm{Tr}_{F/K}$ является линейным отображением из F в K. Остается установить, что это отображение «на». Для этого ввиду (ii) достаточно доказать существование элемента $\alpha \in F$, такого, что $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. Ясно, что $\mathrm{Tr}_{F/K}(\alpha) = 0$ тогда и только тогда, когда α является корнем многочлена $x^{q^{m-1}} + \ldots + x^q + x \in K[x]$ в поле F. Но так как этот многочлен может иметь не более q^{m-1} корней в F, а поле F состоит из q^m элементов, то нужный нам элемент в F существует.

(iv) Это равенство непосредственно вытекает из определения функции следа и из леммы 2.3.

(v) Так как в силу леммы 2.3 для $\alpha \in F$ имеем $\alpha^{q^m} = \alpha$, то $\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^m} = \mathrm{Tr}_{F/K}(\alpha)$. □

Функция следа $\mathrm{Tr}_{F/K}$ не только сама является линейным отображением из F на K, но может служить для описания всех возможных линейных отображений из F в K (т. е., в иной терминологии, всех линейных функционалов на F). Это описание имеет то преимущество, что не зависит от выбора базиса.

2.24. Теорема. *Пусть* F *— конечное расширение конечного поля* K (*оба поля рассматриваются как векторные пространства над* K). *Тогда линейными отображениями из* F *в* K *являются отображения* L_β, $\beta \in F$, *определяемые условием* $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ *для всех* $\alpha \in F$, *и только они. При этом если* β *и* γ *— различные элементы поля* F, *то* $L_\beta \neq L_\gamma$.

Доказательство. Каждое отображение L_β в силу теоремы 2.23 (iii) является линейным отображением из F в K. При этом, если $\beta, \gamma \in F$, $\beta \neq \gamma$, то

$$L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) = \mathrm{Tr}_{F/K}((\beta - \gamma)\alpha) \neq 0$$

для подходящим образом выбранного элемента $\alpha \in F$, так как $\mathrm{Tr}_{F/K}$ отображает F на K; поэтому отображения L_β и L_γ различны. Если $K = \mathbb{F}_q$ и $F = \mathbb{F}_{q^m}$, то получим q^m различных линейных отображений L_β из F в K. С другой стороны, выбрав определенный базис $\{\alpha_1, \ldots, \alpha_m\}$ векторного пространства F над полем K, мы можем получить любое линейное отображение из F в K, отображая базисные элементы α_j, $j = 1, \ldots, m$, в произвольные элементы поля K. Это можно сделать q^m различными способами; следовательно, все линейные отображения из F в K исчерпываются отображениями L_β, $\beta \in F$. □

2.25. Теорема. *Пусть F — конечное расширение поля $K = \mathbb{F}_q$. Тогда для $\alpha \in F$ равенство $\mathrm{Tr}_{F/K}(\alpha) = 0$ выполняется в том и только том случае, если имеет место равенство $\alpha = \beta^q - \beta$ для некоторого элемента $\beta \in F$.*

Доказательство. Достаточность этого условия очевидна ввиду теоремы 2.23 (v). Для доказательства необходимости допустим, что $\alpha \in F = \mathbb{F}_{q^m}$ таково, что $\mathrm{Tr}_{F/K}(\alpha) = 0$, и β — корень многочлена $x^q - x - \alpha$ из некоторого расширения поля F. Тогда $\beta^q - \beta = \alpha$ и

$$\begin{aligned} 0 = \mathrm{Tr}_{F/K}(\alpha) &= \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} = \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \ldots + (\beta^q - \beta)^{q^{m-1}} = \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \ldots + (\beta^{q^m} - \beta^{q^{m-1}}) = \\ &= \beta^{q^m} - \beta, \end{aligned}$$

так что $\beta \in F$. □

Если рассматривается *двухэтажная башня* $K \subseteq F \subseteq E$ расширений полей, то композиция функций следа ведет себя очень просто.

2.26. Теорема (транзитивность следа). *Пусть K — конечное поле, F — конечное расширение поля K и E — конечное расширение поля F. Тогда для всех $\alpha \in E$ имеет место равенство*

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)).$$

Доказательство. Пусть $K = \mathbb{F}_q$, $[F : K] = m$ и $[E : F] = n$, так что $[E : K] = mn$ согласно теореме 1.84. Тогда для $\alpha \in E$

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) = \sum_{i=0}^{m-1} (\mathrm{Tr}_{E/F}(\alpha))^{q^i} =$$

$$= \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}} \right)^{q^i} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} =$$
$$= \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha). \qquad \square$$

Другая интересная функция из конечного поля в его подполе получается, если рассматривать произведения элементов, сопряженных с некоторым элементом поля относительно данного подполя.

2.27. Определение. Для $\alpha \in F = \mathbb{F}_{q^m}$ и $K = \mathbb{F}_q$ определим *норму* $\mathrm{N}_{F/K}(\alpha)$ элемента α над полем K равенством

$$\mathrm{N}_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdot \ldots \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}.$$

Сравнивая в равенстве (2.1) постоянные члены, получим выражение нормы $\mathrm{N}_{F/K}(\alpha)$ через свободный член характеристического многочлена элемента α над полем K:

$$\mathrm{N}_{F/K}(\alpha) = (-1)^m a_0. \tag{2.3}$$

В частности, получаем, что норма $\mathrm{N}_{F/K}(\alpha)$ всегда является элементом поля K.

2.28. Теорема. *Пусть* $K = \mathbb{F}_q$ *и* $F = \mathbb{F}_{q^m}$. *Тогда функция нормы* $\mathrm{N}_{F/K}$ *обладает следующими свойствами*:

(i) $\mathrm{N}_{F/K}(\alpha\beta) = \mathrm{N}_{F/K}(\alpha)\,\mathrm{N}_{F/K}(\beta)$ *для всех* $\alpha, \beta \in F$;
(ii) $\mathrm{N}_{F/K}$ *отображает* F на K *и* F^* *на* K^*;
(iii) $\mathrm{N}_{F/K}(a) = a^m$ *для всех* $a \in K$;
(iv) $\mathrm{N}_{F/K}(\alpha^q) = \mathrm{N}_{F/K}(\alpha)$ *для всех* $\alpha \in F$.

Доказательство. Свойство (i) вытекает непосредственно из определения нормы.

(ii) Мы уже отмечали, что функция $\mathrm{N}_{F/K}$ отображает F в K. Поскольку $\mathrm{N}_{F/K}(\alpha) = 0$ в том и только том случае, если $\alpha = 0$, то $\mathrm{N}_{F/K}$ отображает F^* в K^*. Свойство (i) означает, что отображение $\mathrm{N}_{F/K}$ является гомоморфизмом мультипликативной группы F^* в мультипликативную группу K^*. Так как элементами ядра гомоморфизма $\mathrm{N}_{F/K}$ являются корни многочлена $x^{(q^m-1)/(q-1)} - 1 \in K[x]$, принадлежащие полю F, и только они, то порядок d этого ядра удовлетворяет неравенству $d \leqslant (q^m - 1)/(q - 1)$. Согласно теореме 1.23, образ отображения $\mathrm{N}_{F/K}$ имеет порядок $(q^m - 1)/d \geqslant q - 1$. Значит, $\mathrm{N}_{F/K}$ отображает F^* на K^* и, следовательно, F на K.

(iii) Это свойство сразу вытекает из определения нормы и того факта, что все элементы, сопряженные с $a \in K$ относительно поля K, равны a.

(iv) Учитывая, что $N_{F/K}(\alpha) \in K$ для любого $\alpha \in F$, и применяя (i) и лемму 2.3, получим, что $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)^q = N_{F/K}(\alpha)$, и это доказывает (iv). □

2.29. Теорема (транзитивность нормы). *Пусть K — конечное поле, F — конечное расширение поля K и E — конечное расширение поля F. Тогда для всех $\alpha \in E$*

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha)).$$

Доказательство. В обозначениях теоремы 2.26 для $\alpha \in E$ получаем

$$\begin{aligned} N_{F/K}(N_{E/F}(\alpha)) &= N_{F/K}\left(\alpha^{(q^{mn}-1)/(q^m-1)}\right) = \\ &= \left(\alpha^{(q^{mn}-1)/(q^m-1)}\right)^{(q^m-1)/(q-1)} = \\ &= \alpha^{(q^{mn}-1)/(q-1)} = N_{E/K}(\alpha). \end{aligned}$$ □

Если $\{\alpha_1, \ldots, \alpha_m\}$ — базис конечного поля F над некоторым подполем K, то возникает вопрос о вычислении коэффициентов $c_j(\alpha) \in K$, $1 \leqslant j \leqslant m$, в однозначном представлении

$$\alpha = c_1(\alpha)\,\alpha_1 + \ldots + c_m(\alpha)\,\alpha_m \tag{2.4}$$

элемента $\alpha \in F$. Заметим, что $c_j\colon \alpha \mapsto c_j(\alpha)$ есть линейное отображение из F в K, и потому, согласно теореме 2.24, существует элемент $\beta_j \in F$, такой, что $c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha)$ для всех $\alpha \in F$. Полагая $\alpha = \alpha_i$, $1 \leqslant i \leqslant m$, мы видим, что след $\mathrm{Tr}_{F/K}(\beta_j\alpha_i)$ равен 0 при $i \neq j$ и 1 при $i = j$. Кроме того, $\{\beta_1, \ldots, \beta_m\}$ — тоже базис F над K, так как если

$$d_1\beta_1 + \ldots + d_m\beta_m = 0 \quad \text{при} \quad d_i \in K, \quad 1 \leqslant i \leqslant m,$$

то, умножая на фиксированное α_i и применяя функцию следа $\mathrm{Tr}_{F/K}$, получаем, что $d_i = 0$.

2.30. Определение. Пусть K — конечное поле и F — его конечное расширение. Тогда два базиса $\{\alpha_1, \ldots, \alpha_m\}$ и $\{\beta_1, \ldots, \beta_m\}$ поля F над K называются *дуальными*, если для $1 \leqslant i, j \leqslant m$

$$\mathrm{Tr}_{F/K}(\alpha_i\beta_j) = \begin{cases} 0 & \text{при} \quad i \neq j, \\ 1 & \text{при} \quad i = j. \end{cases}$$

Выше было показано, что для любого базиса $\{\alpha_1, \ldots, \alpha_m\}$ поля F над K существует некоторый дуальный базис $\{\beta_1, \ldots, \beta_m\}$. В действительности дуальный базис для базиса $\{\alpha_1, \ldots, \alpha_m\}$ определяется однозначно, так как из его определения видно, что коэффициенты $c_j(\alpha)$, $1 \leqslant j \leqslant m$, в (2.4) для всех $\alpha \in F$ задаются равенством $c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha)$, и по теореме 2.24 элемент $\beta_j \in F$ однозначно определяется линейным отображением c_j.

2.31. Пример. Пусть $\alpha \in \mathbb{F}_8$ — корень неприводимого многочлена $x^3 + x^2 + 1$ из $\mathbb{F}_2[x]$. Тогда $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ — базис поля $\mathbb{F}_8$ над $\mathbb{F}_2$. Легко проверить, что однозначно определенным дуальным к нему базисом снова будет $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$. Такой базис, который дуален к самому себе, называется *автодуальным*. Элемент $\alpha^5 \in \mathbb{F}_8$ можно однозначно представить в виде $\alpha^5 = c_1\alpha + c_2\alpha^2 + c_3(1 + \alpha + \alpha^2)$, где коэффициенты c_1, c_2, c_3 из $\mathbb{F}_2$ определяются равенствами

$$c_1 = \mathrm{Tr}_{\mathbb{F}_8}(\alpha \cdot \alpha^5) = 0,$$

$$c_2 = \mathrm{Tr}_{\mathbb{F}_8}(\alpha^2 \cdot \alpha^5) = 1,$$

$$c_3 = \mathrm{Tr}_{\mathbb{F}_8}((1 + \alpha + \alpha^2)\alpha^5) = 1,$$

так что $\alpha^5 = \alpha^2 + (1 + \alpha + \alpha^2)$. □

Различных базисов поля F над K существует довольно много (см. упр. 2.37), но имеется два особенно важных типа базисов. Один — это так называемый *полиномиальный* [1]) *базис* $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$, образованный степенями образующего элемента α поля F (как простого расширения поля K). В качестве α часто берется примитивный элемент поля F (см. теорему 2.10). Другим важным типом базиса является нормальный базис, определяемый некоторым подходящим образом выбранным элементом поля F.

2.32. Определение. Пусть $K = \mathbb{F}_q$ и $F = \mathbb{F}_{q^m}$. Тогда базис поля F над K вида $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$, состоящий из подходящим образом выбранного элемента $\alpha \in F$ и сопряженных с ним относительно поля K элементов, называется *нормальным базисом* поля F над K.

Базис $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ поля $\mathbb{F}_8$ над $\mathbb{F}_2$, рассмотренный в примере 2.31, является нормальным базисом поля $\mathbb{F}_8$ над $\mathbb{F}_2$, так как $1 + \alpha + \alpha^2 = \alpha^4$. Покажем, что нормальный базис существует всегда. Доказательство этого факта опирается на две леммы — одну о линейной независимости групповых гомоморфизмов определенного вида и другую о линейных отображениях.

2.33. Лемма (лемма Артина). *Пусть $\psi_1, \ldots, \psi_m$ — различные гомоморфизмы некоторой группы G в мультипликативную группу F^* произвольного поля F и $a_1, \ldots, a_m$ — элементы поля F, не все равные нулю. Тогда существует такой элемент g группы G, что*

$$a_1\psi_1(g) + \ldots + a_m\psi_m(g) \neq 0.$$

[1]) Этот термин связан с тем фактом, что каждый элемент $\beta \in F$ представляется в этом базисе значением при $x = \alpha$ некоторого многочлена $f_\beta(x) \in K[x]$ степени, не превышающей $m - 1$. — *Прим. перев.*

Доказательство. Применим индукцию по m. Случай $m = 1$ тривиален. Предположим, что $m > 1$ и что утверждение справедливо для любых $m - 1$ различных гомоморфизмов. Теперь возьмем указанные в лемме $\psi_1, \ldots, \psi_m$ и $a_1, \ldots, a_m$. Если $a_1 = 0$, то предположение индукции сразу приводит к нужному результату. Поэтому пусть $a_1 \neq 0$. Допустим, что имеет место равенство

$$a_1\psi_1(g) + \ldots + a_m\psi_m(g) = 0 \quad \text{для всех } g \in G, \tag{2.5}$$

Так как $\psi_1 \neq \psi_m$, то существует $h \in G$, такой, что $\psi_1(h) \neq \psi_m(h)$. Тогда, заменяя g на hg в (2.5), получим

$$a_1\psi_1(h)\psi_1(g) + \ldots + a_m\psi_m(h)\psi_m(g) = 0 \quad \text{для всех } g \in G.$$

Умножая на $\psi_m(h)^{-1}$, получим

$$b_1\psi_1(g) + \ldots + b_{m-1}\psi_{m-1}(g) + a_m\psi_m(g) = 0 \quad \text{для всех } g \in G,$$

где $b_i = a_i\psi_i(h)\psi_m(h)^{-1}$, $1 \leqslant i \leqslant m - 1$. Вычитая полученное равенство из (2.5), приходим к равенству

$$c_1\psi_1(g) + \ldots + c_{m-1}\psi_{m-1}(g) = 0 \quad \text{для всех } g \in G,$$

где $c_i = a_i - b_i$, $1 \leqslant i \leqslant m - 1$. Но $c_1 = a_1 - a_1\psi_1(h)\psi_m(h)^{-1} \neq 0$, так что получаем противоречие с предположением индукции. □

Напомним теперь некоторые понятия и факты из линейной алгебры. Пусть T — линейный оператор (линейное преобразование) в конечномерном векторном пространстве V над (произвольным) полем K. Будем говорить, что многочлен $f(x) = a_nx^n + \ldots + a_1x + a_0$ из кольца $K[x]$ *аннулирует* оператор T, если $a_nT^n + \ldots + a_1T + a_0I = O$, где I — тождественный, а O — нулевой операторы в пространстве V. Однозначно определенный нормированный многочлен наименьшей степени, обладающий таким свойством, называется *минимальным многочленом* оператора T. Он делит любой другой многочлен из $K[x]$, аннулирующий T. Известно, что минимальный многочлен оператора T делит *характеристический многочлен* $g(x)$ этого оператора (теорема Гамильтона—Кэли), который задается равенством $g(x) = \det(xI - T)$ [1]) и является нормированным многочленом степени, равной размерности пространства V. Вектор $\alpha \in V$ назовем *циклическим вектором* оператора T, если совокупность векторов $T^k\alpha$, $k = 0, 1, \ldots$,

[1]) *Определителем* $\det(T)$ линейного оператора T в конечномерном векторном пространстве V над полем K называется определитель матрицы A этого оператора в произвольном базисе. Если B — матрица оператора T в другом базисе, то $B = S^{-1}AS$ для некоторой невырожденной матрицы S, так что $\det(B) = \det(A)$. — *Прим. перев.*

порождает пространство V. Приведем известный результат из линейной алгебры.

2.34. Лемма. *Пусть T — линейный оператор в конечномерном векторном пространстве V. Оператор T обладает циклическим вектором в том и только том случае, если его характеристический многочлен совпадает с минимальным.*

2.35. Теорема (теорема о нормальном базисе). *Для каждого конечного поля K и каждого его конечного расширения F существует нормальный базис поля F над K.*

Доказательство. Пусть $K = \mathbb{F}_q$ и $F = \mathbb{F}_{q^m}$, $m \geqslant 2$. Из теоремы 2.21 и следующих за ней замечаний известно, что автоморфизмы поля F над K исчерпываются различными автоморфизмами ε, σ, σ^2, ..., σ^{m-1}, где ε — тождественный автоморфизм поля F, $\sigma(\alpha) = \alpha^q$ для любого $\alpha \in F$, а σ^j означает j-кратную композицию отображения σ с самим собой. Поскольку $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ и $\sigma(c\alpha) = \sigma(c)\,\sigma(\alpha) = c\sigma(\alpha)$ для α, $\beta \in F$ и $c \in K$, отображение σ можно также рассматривать как линейный оператор в векторном пространстве F над полем K. Так как $\sigma^m = \varepsilon$, то многочлен $x^m - 1 \in K[x]$ аннулирует оператор σ. Из леммы 2.33, примененной к операторам ε, σ, σ^2, ..., σ^{m-1}, рассматриваемым как эндоморфизмы группы F^*, следует, что в кольце $K[x]$ не существует ненулевых многочленов степени, меньшей m, которые аннулируют оператор σ. Следовательно, $x^m - 1$ — минимальный многочлен линейного оператора σ. Поскольку характеристический многочлен оператора σ является нормированным многочленом степени m, делящимся на минимальный многочлен этого оператора, то ясно, что характеристическим многочленом оператора σ тоже является $x^m - 1$. Поэтому в силу леммы 2.34 существует элемент $\alpha \in F$, такой, что элементы α, $\sigma(\alpha)$, $\sigma^2(\alpha)$, ... порождают пространство F. Отбрасывая повторяющиеся элементы, мы видим, что элементы α, $\sigma(\alpha)$, $\sigma^2(\alpha)$, ..., $\sigma^{m-1}(\alpha)$ порождают F и, следовательно, образуют базис F над K. Так как этот базис состоит из α и сопряженных с ним относительно поля K элементов, то он является нормальным базисом поля F над K. □

Другое доказательство теоремы о нормальном базисе будет дано в § 4 гл. 3. Оно использует так называемые линеаризованные многочлены.

Введем одно понятие, которое позволит нам решить вопрос, является ли данное множество элементов базисом некоторого расширения поля.

2.36. Определение. Пусть K — конечное поле и F — его расширение, имеющее степень m над K. Тогда *дискриминантом*

$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ элементов $\alpha_1, \ldots, \alpha_m \in F$ над K назовем следующий определитель порядка m:

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \ldots & \ldots & \ldots & \ldots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{vmatrix}.$$

Из определения следует, что дискриминант $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ всегда является элементом поля K. Теперь можно дать следующую простую характеризацию базиса.

2.37. Теорема. *Пусть K — конечное поле и F — его расширение степени m. Элементы $\{\alpha_1, \ldots, \alpha_m\}$ поля F образуют его базис над K в том и только том случае, если $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$.*

Доказательство. Пусть $\{\alpha_1, \ldots, \alpha_m\}$ — базис поля F над K. Докажем, что строки определителя $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ линейно независимы; это и будет означать, что $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$. Допустим, что

$$c_1\mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + c_2\mathrm{Tr}_{F/K}(\alpha_2\alpha_j) + \ldots + c_m\mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0$$
$$\text{для} \quad 1 \leqslant j \leqslant m,$$

где $c_1, \ldots, c_m \in K$. Тогда если $\beta = c_1\alpha_1 + \ldots + c_m\alpha_m$, то $\mathrm{Tr}_{F/K}(\beta\alpha_j) = 0$ для $1 \leqslant j \leqslant m$, и так как элементы $\alpha_1, \ldots, \alpha_m$ порождают пространство F, то это значит, что $\mathrm{Tr}_{F/K}(\beta\alpha) = 0$ для всех $\alpha \in F$. Но это возможно лишь при $\beta = 0$, т. е. $c_1\alpha_1 + \ldots + c_m\alpha_m = 0$, а это значит, что $c_1 = c_2 = \ldots = c_m = 0$.

Обратно, допустим, что $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ и $c_1\alpha_1 + \ldots + c_m\alpha_m = 0$ для некоторых $c_1, \ldots, c_m \in K$. Тогда

$$c_1\alpha_1\alpha_j + \ldots + c_m\alpha_m\alpha_j = 0 \quad \text{для } 1 \leqslant j \leqslant m$$

и, применяя функцию следа, получаем

$$c_1\mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + \ldots + c_m\mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \quad \text{для } 1 \leqslant j \leqslant m.$$

Но поскольку строки определителя $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ линейно независимы, $c_1 = \ldots = c_m = 0$. Поэтому элементы $\alpha_1, \ldots, \alpha_m$ линейно независимы над полем K. □

Имеется и другой определитель порядка m, служащий той же цели, что и дискриминант $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$. Но его элементами являются элементы расширения F поля $K = \mathbb{F}_q$. Для данных элементов $\alpha_1, \ldots, \alpha_m$ поля F пусть A будет $m \times m$-матрицей (a_{ij}), где $a_{ij} = \alpha_j^{q^{i-1}}$. Если через A^{T} обозначить матрицу, транспонированную к матрице A, то легко подсчитать, что в $m \times m$-матрице

$B = A^TA$ на пересечении i-й строки и j-го столбца стоит элемент $\mathrm{Tr}_{F/K}(\alpha_i\alpha_j)$. Поэтому, переходя к определителям, получаем

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \det(A)^2.$$

Таким образом, теперь из теоремы 2.37 вытекает следующий результат.

2.38. Следствие. *Элементы* $\{\alpha_1, \ldots, \alpha_m\}$ *поля* $\mathbb{F}_{q^m}$ *образуют базис этого поля над полем* $\mathbb{F}_q$ *тогда и только тогда, когда определитель*

$$\det(A) = \begin{vmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \ldots & \alpha_m^q \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \ldots & \alpha_m^{q^{m-1}} \end{vmatrix}$$

отличен от нуля.

С помощью полученного критерия нетрудно проверить, приводит или нет данный элемент к нормальному базису.

2.39. Теорема. *Для того чтобы степени* $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ *элемента* $\alpha \in \mathbb{F}_{q^m}$ *образовывали нормальный базис поля* $\mathbb{F}_{q^m}$ *над полем* $\mathbb{F}_q$, *необходимо и достаточно, чтобы многочлены* $x^m - 1$ *и* $\alpha x^{m-1} + \alpha^q x^{m-2} + \ldots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ *из кольца* $\mathbb{F}_{q^m}[x]$ *были взаимно простыми.*

Доказательство. При $\alpha_1 = \alpha$, $\alpha_2 = \alpha^q$, $\ldots$, $\alpha_m = \alpha^{q^{m-1}}$ определитель из следствия 2.38 принимает вид

$$\pm \begin{vmatrix} \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \ldots & \alpha^{q^{m-2}} \\ \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & \alpha & \ldots & \alpha^{q^{m-3}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & \alpha \end{vmatrix} \tag{2.6}$$

(после подходящей перестановки строк). Теперь рассмотрим результант $R(f, g)$ многочленов $f(x) = x^m - 1$ и $g(x) = \alpha x^{m-1} + \alpha^q x^{m-2} + \ldots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ с формальными степенями m и $m-1$ соответственно. Этот результант в соответствии с определением 1.93 является определителем порядка $2m-1$. Если в этом определителе прибавить $(m+1)$-й столбец к первому, $(m+2)$-й ко второму и т. д. и, наконец, $(2m-1)$-й столбец к $(m-1)$-му, то в результате получится определитель, равный произведению определителя диагональной матрицы порядка $m-1$

с элементами —1 по главной диагонали и определителя (2.6). Поэтому $R(f, g)$ с точностью до знака равен определителю (2.6). Утверждение теоремы вытекает теперь из следствия 2.38 и того факта, что $R(f, g) \neq 0$ тогда и только тогда, когда многочлены f и g взаимно просты. □

В связи со сказанным выше упомянем без доказательства еще один результат о нормальном базисе.

2.40. Теорема. *Для каждого конечного поля F существует нормальный базис этого поля над его простым подполем, который состоит из примитивных элементов поля F.*

§ 4. Корни из единицы и круговые многочлены

В этом параграфе мы исследуем поле разложения многочлена $x^n - 1$ над произвольным полем K, где n — натуральное число. Кроме того, мы получим обобщение понятия корня из единицы, хорошо известного для комплексных чисел.

2.41. Определение. Для натурального числа n поле разложения многочлена $x^n - 1$ над произвольным полем K называется *n-круговым* (или *n-циклотомическим*) *полем* над K и обозначается $K^{(n)}$. Корни многочлена $x^n - 1$ из поля $K^{(n)}$ называются *корнями n-й степени из единицы над K*; множество этих корней обозначим $E^{(n)}$.

В том частном случае, когда K — поле рациональных чисел, $K^{(n)}$ представляет собой некоторое подполе поля $\mathbb{C}$ комплексных чисел, а корни n-й степени из единицы имеют известную геометрическую интерпретацию: они являются вершинами правильного n-угольника, вписанного в единичную окружность с центром в начале координат, в комплексной плоскости.

Для наших целей наиболее важен случай конечного поля K. Однако основные свойства корней из единицы можно установить без ограничительного предположения о конечности поля K. Как показывает следующая теорема, структура множества $E^{(n)}$ определяется соотношением между числом n и характеристикой поля K. Говоря ниже о характеристике p поля K, мы не исключаем случая $p = 0$.

2.42. Теорема. *Пусть $n \in \mathbb{N}$ и K — поле характеристики p. Тогда*

(i) *Если p не делит n, то множество $E^{(n)}$ является циклической подгруппой порядка n мультипликативной группы поля $K^{(n)}$.*

(ii) *Если p делит n и $n = mp^e$, где m, $e \in \mathbb{N}$ и p не делит m, то $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ и корнями многочлена $x^n - 1$ в поле $K^{(n)}$ являются m элементов множества $E^{(m)}$, каждый из которых имеет кратность p^e.*

Доказательство. (i) Случай $n = 1$ тривиален. Для $n \geqslant 2$ многочлен $x^n - 1$ и его производная nx^{n-1} общих корней не имеют, так как nx^{n-1} имеет единственный корень 0 в поле $K^{(n)}$. Поэтому по теореме 1.68 многочлен $x^n - 1$ не может иметь кратных корней, так что множество $E^{(n)}$ состоит из n элементов. Далее, если ζ, $\eta \in E^{(n)}$, то $(\zeta\eta^{-1})^n = \zeta^n (\eta^n)^{-1} = 1$, так что $\zeta\eta^{-1} \in E^{(n)}$. Следовательно, $E^{(n)}$ — мультипликативная группа. Пусть $n = p_1^{e_1} \dots p_t^{e_t}$ — разложение числа n на простые сомножители. Тогда такое же рассуждение, как и при доказательстве теоремы 2.8, приводит к существованию для каждого i, $1 \leqslant i \leqslant t$, элемента $\alpha_i \in E^{(n)}$, который не является корнем многочлена $x^{n/p_i} - 1$, так что элемент $\beta_i = \alpha_i^{n/p_i^{e_i}}$ имеет порядок $p_i^{e_i}$, и, следовательно, $E^{(n)}$ — циклическая группа с образующим элементом $\beta = \beta_1 \dots \beta_t$.

(ii) Это утверждение сразу вытекает из (i) и равенств $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$. □

2.43. Определение. Пусть K — поле характеристики p и n — натуральное число, не делящееся на p. Тогда образующий элемент циклической группы $E^{(n)}$ называется *первообразным* (или *примитивным*) *корнем n-й степени из единицы над полем K*.

Из теоремы 1.15 (v) мы получаем, что если p не делит n, то существует ровно $\varphi(n)$ различных первообразных корней n-й степени из единицы над полем K. Если ζ — один из них, то все первообразные корни n-й степени из единицы над K имеют вид ζ^s, где $1 \leqslant s \leqslant n$, НОД $(s, n) = 1$. Большой интерес представляют многочлены, корнями которых являются все первообразные корни n-й степени из единицы над полем K и только они.

2.44. Определение. Пусть K — поле характеристики p, n — натуральное число, не делящееся на p, и ζ — первообразный корень n-й степени из единицы над K. Тогда многочлен

$$Q_n(x) = \prod_{\substack{s=1 \\ \text{НОД}(s,\, n) = 1}}^{n} (x - \zeta^s)$$

называется *n-круговым* (или *n-циклотомическим*) *многочленом* над полем K.

Ясно, что многочлен $Q_n(x)$ не зависит от выбора элемента ζ. Его степень равна $\varphi(n)$, а его коэффициенты, очевидно, принадлежат n-круговому полю над K. Однако несложное рассуждение показывает, что на самом деле они принадлежат простому подполю поля K. Будем ниже использовать символ $\prod_{d \mid n}$ для обозначения произведения, распространяющегося на все натуральные делители d натурального числа n

2.45. Теорема. *Пусть K — поле характеристики p и n — натуральное число, не делящееся на p. Тогда*

(i) $x^n - 1 = \prod_{d \mid n} Q_d(x)$;

(ii) *коэффициенты n-кругового многочлена $Q_n(x)$ принадлежат простому подполю поля K, если p — простое число, или кольцу $\mathbb{Z}$ целых чисел, если $p = 0$.*

Доказательство. (i) Каждый корень n-й степени из единицы над полем K является первообразным корнем d-й степени из единицы над K ровно для одного натурального делителя d числа n. А именно если ζ^s — произвольный корень n-й степени из единицы над K (где ζ — некоторый первообразный корень n-й степени из единицы над K), то указанное число d равно $n/\text{НОД}(s, n)$, т. е. d — порядок элемента ζ^s в группе $E^{(n)}$. Поскольку

$$x^n - 1 = \prod_{s=1}^{n} (x - \zeta^s),$$

формула в утверждении (i) получается собиранием тех множителей $(x - \zeta^s)$, для которых ζ^s является первообразным корнем d-й степени из единицы над K (для каждого положительного делителя d числа n).

(ii) Это утверждение доказывается индукцией по n. Отметим, что $Q_n(x)$ — нормированный многочлен. Для $n = 1$ имеем $Q_1(x) = x - 1$, и утверждение справедливо. Пусть теперь $n > 1$, и допустим, что утверждение справедливо для всех $Q_d(x)$, $1 \leqslant d < n$. Тогда ввиду (i) получаем, что $Q_n(x) = (x^n - 1)/f(x)$, где $f(x) = \prod_{d \mid n,\ d<n} Q_d(x)$. Из предположения индукции следует, что $f(x)$ — многочлен с коэффициентами из простого подполя поля K (при простом p) или из кольца $\mathbb{Z}$ (при $p = 0$). Применяя обычное деление углом многочлена $x^n - 1$ на $f(x)$, где $f(x)$ — нормированный многочлен, легко убеждаемся, что коэффициенты многочлена $Q_n(x)$ тоже принадлежат простому подполю поля K (при простом p) или кольцу $\mathbb{Z}$ (при $p = 0$). □

2.46. Пример. Пусть r — простое число и $k \in \mathbb{N}$. Тогда

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}},$$

так как по теореме 2.45 (i)

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{Q_1(x)\, Q_r(x) \cdots Q_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}.$$

Для $k = 1$ имеем просто $Q_r(x) = 1 + x + x^2 + \ldots + x^{r-1}$. □

Явное выражение для n-кругового многочлена, обобщающее формулу из примера 2.46, мы дадим в § 2 гл. 3. Для приложений

к конечным полям полезно знать некоторые свойства круговых полей.

2.47. Теорема. *Круговое поле $K^{(n)}$ является простым алгебраическим расширением поля K. Кроме того,*

(i) *Если $K = \mathbb{Q}$, то $[K^{(n)} : K] = \varphi(n)$, причем круговой многочлен Q_n неприводим над K (здесь φ — функция Эйлера).*

(ii) *Если $K = \mathbb{F}_q$ и НОД $(q, n) = 1$, то $[K^{(n)} : K] = d$, где d — наименьшее натуральное число, такое, что $q^d \equiv 1 \pmod{n}$. При этом круговой многочлен Q_n разлагается в произведение $\varphi(n)/d$ различных нормированных неприводимых многочленов из $K[x]$ одной и той же степени d и $K^{(n)}$ является полем разложения каждого из этих многочленов.*

Доказательство. Если существует первообразный корень n-й степени из единицы ζ над K, то ясно, что $K^{(n)} = K(\zeta)$. В противном случае K — поле простой характеристики p, делящей число n, и мы попадаем в ситуацию, описанную в теореме 2.42 (ii), и тогда $K^{(n)} = K^{(m)}$, где $n = mp^e$, НОД $(m, p) = 1$, так что снова $K^{(n)} = K(\zeta)$, поскольку существует первообразный корень m-й степени из единицы ζ над K.

Из остальных утверждений мы докажем лишь (ii) как случай, особенно важный для наших целей. Пусть η — первообразный корень n-й степени из единицы над $\mathbb{F}_q$. Тогда $\eta \in \mathbb{F}_{q^k}$ в том и только том случае, если $\eta^{q^k} = \eta$, а это равенство эквивалентно сравнению $q^k \equiv 1 \pmod{n}$. Наименьшее натуральное число k, для которого выполняется это сравнение, равно d, так что $\eta \in \mathbb{F}_{q^d}$, но η не принадлежит никакому собственному подполю поля $\mathbb{F}_{q^d}$. Поэтому минимальный многочлен элемента η над полем $K = \mathbb{F}_q$ имеет степень d, и так как η — произвольный корень многочлена Q_n, то требуемый результат установлен. □

2.48. Пример. Пусть $K = \mathbb{F}_{11}$ и $Q_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. В обозначениях теоремы 2.47 (ii) мы имеем $d = 2$. Действительно, разложение многочлена $Q_{12}(x)$ на неприводимые сомножители в кольце $\mathbb{F}_{11}[x]$ имеет вид $Q_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1)$. Круговым полем $K^{(12)}$ является $\mathbb{F}_{121}$.

Дальнейшую связь между круговыми и конечными полями устанавливает следующая теорема.

2.49. Теорема. *Конечное поле $\mathbb{F}_q$ является $(q-1)$-круговым полем над любым из своих подполей.*

Доказательство. Многочлен $x^{q-1} - 1$ вполне разлагается в поле $\mathbb{F}_q$, так как его корнями являются как раз все ненулевые элементы поля $\mathbb{F}_q$. С другой стороны, ясно, что этот многочлен не может вполне разлагаться ни в каком собственном подполе

поля $\mathbb{F}_q$. Следовательно, $\mathbb{F}_q$ является полем разложения многочлена $x^{q-1} - 1$ над любым из его подполей. □

Поскольку $\mathbb{F}_q^*$ — циклическая группа порядка $q - 1$ (согласно теореме 2.8), то для любого положительного делителя n числа $q - 1$ существует циклическая подгруппа $\{1, \alpha, \ldots, \alpha^{n-1}\}$ группы $\mathbb{F}_q^*$ порядка n (см. теорему 1.15 (iii)). Все элементы этой подгруппы являются корнями n-й степени из единицы над любым подполем поля $\mathbb{F}_q$, а ее образующий элемент α является первообразным корнем n-й степени из единицы над любым подполем поля $\mathbb{F}_q$.

Закончим параграф леммой, которая позже нам пригодится.

2.50. Лемма. *Пусть d — делитель натурального числа n, $1 \leqslant d < n$. Тогда n-круговой многочлен $Q_n(x)$ (если, конечно, он определен над рассматриваемым полем) делит многочлен $(x^n - 1)/(x^d - 1)$.*

Доказательство. Из теоремы 2.45 (i) мы знаем, что $Q_n(x)$ делит многочлен

$$x^n - 1 = (x^d - 1) \cdot \frac{x^n - 1}{x^d - 1}.$$

Поскольку d — собственный делитель числа n, то многочлены $Q_n(x)$ и $x^d - 1$ не имеют (согласно той же теореме) общих корней, и, следовательно, НОД $(Q_n(x), x^d - 1) = 1$, что доказывает наше утверждение. □

§ 5. Представление элементов конечных полей

В этом параграфе мы опишем три разных способа представления элементов конечного поля $\mathbb{F}_q$ из $q = p^n$ элементов, где p — характеристика $\mathbb{F}_q$.

Первый способ основан на принципах, изложенных в § 4 гл. 1 и в данной главе. Заметим, что в силу теоремы 2.10 поле $\mathbb{F}_q$ является простым алгебраическим расширением простого поля $\mathbb{F}_p$. Действительно, если f — неприводимый многочлен степени n из $\mathbb{F}_p[x]$, то по теореме 2.14 любой корень α этого многочлена принадлежит полю $\mathbb{F}_{p^n} = \mathbb{F}_q$, и потому $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Значит, ввиду теоремы 1.86 каждый элемент поля $\mathbb{F}_q$ можно однозначно представнть в виде значения некоторого многочлена от x над $\mathbb{F}_p$ степени, не превосходящей $n - 1$, при $x = \alpha$. Мы можем также рассматривать поле $\mathbb{F}_q$ как факторкольцо $\mathbb{F}_p[x]/(f)$.

2.51. Пример. Чтобы представить таким способом элементы поля $\mathbb{F}_9$, будем рассматривать $\mathbb{F}_9$ как простое алгебраическое расширение степени 2 поля $\mathbb{F}_3$, получаемое присоединением корня α неприводимого квадратного многочлена над $\mathbb{F}_3$, скажем $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Тогда $f(\alpha) = \alpha^2 + 1 = 0$ в $\mathbb{F}_9$, и девять элементов поля $\mathbb{F}_9$ можно задать в виде $a_0 + a_1\alpha$, где a_0,

$a_1 \in \mathbb{F}_3$. Точнее, $\mathbb{F}_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$. Таблицы операций для $\mathbb{F}_9$ можно построить так же, как и в примере 1.62, причем корень α играет здесь ту же роль, какую там играл класс вычетов $[x]$. □

Другую возможность представления элементов поля $\mathbb{F}_q$ дает применение теорем 2.47 и 2.49. Поскольку поле $\mathbb{F}_q$ является $(q-1)$-круговым полем над $\mathbb{F}_p$, мы можем построить его, найдя разложение $(q-1)$-кругового многочлена $Q_{q-1} \in \mathbb{F}_p[x]$ на неприводимые сомножители в $\mathbb{F}_p[x]$ (все они имеют одну и ту же степень). Любой корень каждого из этих многочленов тогда является первообразным корнем $(q-1)$-й степени из единицы над $\mathbb{F}_p$, а значит, и примитивным элементом поля $\mathbb{F}_q$. Таким образом, поле $\mathbb{F}_q$ состоит из нуля и степеней этого примитивного элемента.

2.52. **Пример.** Чтобы применить этот способ для построения поля $\mathbb{F}_9$, заметим, что $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$, т. е. поле $\mathbb{F}_9$ является 8-круговым полем над $\mathbb{F}_3$. Далее, следуя примеру 2.46, получаем, что $Q_8(x) = x^4 + 1 \in \mathbb{F}_3[x]$. Разложение многочлена Q_8 на неприводимые сомножители в $\mathbb{F}_3[x]$ выглядит так:

$$Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2).$$

Пусть ζ — корень многочлена $x^2 + x + 2$; тогда он является первообразным корнем 8-й степени из единицы над $\mathbb{F}_3$. Поскольку $\mathbb{F}_9 = \mathbb{F}_3(\zeta)$, то каждый ненулевой элемент поля $\mathbb{F}_9$ можно представить подходящей степенью элемента ζ, так что $\mathbb{F}_9 = \{0, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7, \zeta^8\}$ [1]). Мы можем свести ненулевые элементы поля $\mathbb{F}_9$ в так называемую *таблицу индексов*, в которой указывается значение степени ζ^i, соответствующее показателю i. Для установления связи с предыдущим представлением (пример 2.51) заметим, что корнем многочлена $x^2 + x + 2 \in \mathbb{F}_3[x]$ является элемент $\zeta = 1 + \alpha$, где $\alpha^2 + 1 = 0$ (т. е. α — корень многочлена $x^2 + 1$, как и в примере 2.51). Поэтому таблица индексов для поля $\mathbb{F}_9$ имеет следующий вид:

i	ζ^i	i	ζ^i
1	$1+\alpha$	5	$2+2\alpha$
2	2α	6	α
3	$1+2\alpha$	7	$2+\alpha$
4	2	8	1

[1]) Иногда при таком представлении элементов поля $\mathbb{F}_q$ (в виде нуля и степеней примитивного элемента ζ) для удобства вводят формальный символ $*$, такой, что $\zeta^* = 0$. Тогда произвольный элемент β поля $\mathbb{F}_q$ представляется в виде ζ^b, где b — либо символ $*$, либо вычет по модулю $q-1$. Это удобно для вычислений. — *Прим. перев.*

Из таблицы видно, что мы получаем, конечно, те же самые элементы, что и в примере 2.51, только в другом порядке. □

Третий способ представления элементов конечного поля $\mathbb{F}_q$ осуществляется с помощью матриц. Пусть $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$ — нормированный многочлен положительной степени n над некоторым полем (не обязательно конечным). Его *сопровождающей матрицей* называется следующая квадратная матрица порядка n:

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

Из линейной алгебры известно, что матрица A удовлетворяет уравнению $f(A) = O$, где $f(A)$ — «значение» многочлена $f(x)$ при $x = A$ (будем называть его многочленом от матрицы A), т. е.

$$a_0I + a_1A + \ldots + a_{n-1}A^{n-1} + A^n = O,$$

где I — единичная, а O — нулевая квадратные матрицы порядка n.

Таким образом, если A — сопровождающая матрица нормированного неприводимого многочлена f степени $n \in \mathbb{N}$ над простым конечным полем $\mathbb{F}_p$, то $f(A) = O$, и потому матрица A может играть роль «корня» многочлена f. Отсюда следует, что элементы поля $\mathbb{F}_{p^n}$ представляются всевозможными многочленами над $\mathbb{F}_p$ от матрицы A степеней, меньших n.

2.53. Пример. Как и в примере 2.51, пусть задан многочлен $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Сопровождающей матрицей этого многочлена является матрица

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

Следовательно, поле $\mathbb{F}_9$ можно представить так:

$$\mathbb{F}_9 = \{O,\ I,\ 2I,\ A,\ I + A,\ 2I + A,\ 2A,\ I + 2A,\ 2I + 2A\}.$$

Или, в явном виде,

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\quad 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},\quad A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix},$$

$$I+A=\begin{pmatrix}1&2\\1&1\end{pmatrix},\quad 2I+A=\begin{pmatrix}2&2\\1&2\end{pmatrix},\quad 2A=\begin{pmatrix}0&1\\2&0\end{pmatrix},$$
$$I+2A=\begin{pmatrix}1&1\\2&1\end{pmatrix},\quad 2I+2A=\begin{pmatrix}2&1\\2&2\end{pmatrix}.$$

Если поле $\mathbb{F}_9$ задано таким образом, то вычисления в этом поле проводятся по обычным правилам алгебры матриц. Например,

$$(2I+A)(I+2A)=\begin{pmatrix}2&2\\1&2\end{pmatrix}\begin{pmatrix}1&1\\2&1\end{pmatrix}=\begin{pmatrix}0&1\\2&0\end{pmatrix}=2A. \qquad \square$$

Аналогичным образом и метод, основанный на разложении кругового многочлена Q_{q-1} на неприводимые сомножители в $\mathbb{F}_p[x]$, можно приспособить для того, чтобы он давал представление элементов поля $\mathbb{F}_q$ матрицами.

2.54. Пример. Как и в примере 2.52, пусть $h(x)=x^2+x+2\in\mathbb{F}_3[x]$ — неприводимый делитель кругового многочлена $Q_8\in\mathbb{F}_3[x]$. Сопровождающей матрицей многочлена h является матрица

$$C=\begin{pmatrix}0&1\\1&2\end{pmatrix}.$$

Поле $\mathbb{F}_9$ может быть представлено следующим образом:

$$\mathbb{F}_9=\{O, C, C^2, C^3, C^4, C^5, C^6, C^7, C^8\},$$

где

$$O=\begin{pmatrix}0&0\\0&0\end{pmatrix},\quad C=\begin{pmatrix}0&1\\1&2\end{pmatrix},\quad C^2=\begin{pmatrix}1&2\\2&2\end{pmatrix},$$
$$C^3=\begin{pmatrix}2&2\\2&0\end{pmatrix},\quad C^4=\begin{pmatrix}2&0\\0&2\end{pmatrix},\quad C^5=\begin{pmatrix}0&2\\2&1\end{pmatrix},$$
$$C^6=\begin{pmatrix}2&1\\1&1\end{pmatrix},\quad C^7=\begin{pmatrix}1&1\\1&0\end{pmatrix},\quad C^8=\begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

Вычисления проводятся по правилам алгебры матриц. Например,

$$C^6+C=\begin{pmatrix}2&1\\1&1\end{pmatrix}+\begin{pmatrix}0&1\\1&2\end{pmatrix}=\begin{pmatrix}2&2\\2&0\end{pmatrix}=C^3. \qquad \square$$

§ 6. Теорема Веддербёрна [1])

Все результаты, полученные для конечных полей, справедливы также и для любых конечных тел в силу известной теоремы

[1]) Этот параграф может быть опущен без ущерба для понимания последующих глав.

Веддербёрна. Эта теорема утверждает, что если конечное кольцо обладает всеми свойствами поля, кроме коммутативности умножения (т. е. если это кольцо является телом), то умножение в нем должно также быть коммутативным. Мы приведем два доказательства этой важной теоремы. В первом из них, рассматривая какое-либо подполе конечного тела, мы установим сначала одно числовое соотношение, связывающее мультипликативную группу этого поля с мультипликативной группой всего тела. Используя затем это соотношение и некоторые сведения о круговых многочленах, мы придем к противоречию, если только исходное тело не совпадает с рассматриваемым полем. Прежде чем перейти к детальному доказательству теоремы Веддербёрна, отметим несколько общих соображений, которые мы будем использовать.

Пусть D — некоторое тело и F — его коммутативное подтело (будем в дальнейшем называть F *подполем* тела D). Тогда D можно рассматривать как (левое) векторное пространство над полем F (аналогичная ситуация для полей была рассмотрена в § 4 гл. 1). Если $F = \mathbb{F}_q$ и тело D имеет конечную размерность n над F, то D состоит из q^n элементов. Для мультипликативной группы ненулевых элементов тела D примем обозначение D^*.

Пусть G — некоторая группа и S — ее непустое подмножество. Выше было введено понятие нормализатора $N(b)$ элемента $b \in G$ в группе G (см. определение 1.24). Из теоремы 1.25 следует, что если G — конечная группа, то число элементов в классе сопряженных с b элементов группы G равно индексу $|G|/|N(b)|$ нормализатора $N(b)$ в группе G.

2.55. Теорема (теорема Веддербёрна). *Каждое конечное тело является полем.*

Первое доказательство. Пусть D — конечное тело и $Z = \{z \in D \mid zd = dz$ для любого $d \in D\}$ — его *центр*. Нетрудно проверить, что Z — поле. Тогда $Z = \mathbb{F}_q$, где q — некоторая степень простого числа. Так как тело D является векторным пространством над Z некоторой конечной размерности n, то D состоит из q^n элементов. Покажем, что $D = Z$, т. е. что $n = 1$.

Предположим противное, т. е. что $n > 1$. Пусть $a \in D$ и $N_a = \{b \in D \mid ab = ba\}$. Тогда N_a — тело, содержащее Z, и потому состоит из q^r элементов, где $1 \leqslant r \leqslant n$. Покажем, что число r делит n. Поскольку N_a^* — подгруппа группы D^*, то число $q^r - 1$ делит $q^n - 1$. Если $n = rm + t$, где $0 \leqslant t < r$, то $q^n - 1 = q^{rm}q^t - 1 = q^t(q^{rm} - 1) + (q^t - 1)$. Поскольку число $q^r - 1$ делит как $q^n - 1$, так и $q^{rm} - 1$, то оно делит также и $q^t - 1$. Но $q^t - 1 < q^r - 1$, а значит, $t = 0$. Отсюда получаем, что число r делит n.

Рассмотрим теперь уравнение классов сопряженности для группы D^* (см. теорему 1.27). Центром D^* является группа Z^*

порядка $q-1$. Если $a \in D^*$, то N_a^* — нормализатор элемента a в группе D^*. Поэтому любой класс сопряженности группы D^*, содержащий более одного элемента, состоит из $(q^n-1)/(q^r-1)$ элементов, где r — некоторый собственный делитель числа n, $1 \leqslant r < n$. Значит, уравнение классов сопряженности имеет вид

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{r_i} - 1}, \tag{2.7}$$

где $r_1, \ldots, r_k$ — собственные делители числа n (не обязательно различные), причем $1 \leqslant r_i < n$, $1 \leqslant i \leqslant k$.

Рассмотрим n-круговой многочлен Q_n над полем рациональных чисел. В силу теоремы 2.45 (ii) $Q_n(q)$ — целое число. Согласно лемме 2.50, число $Q_n(q)$ делит $(q^n-1)/(q^{r_i}-1)$ при любом i, $1 \leqslant i \leqslant k$. Поэтому из (2.7) получаем, что число $Q_n(q)$ делит $q-1$. Однако это приводит к противоречию. Действительно, по определению

$$Q_n(x) = \prod_{\substack{s=1 \\ \text{НОД}(s,\,n)=1}}^{n} (x - \zeta^s),$$

где комплексное число ζ является первообразным корнем n-й степени из единицы над полем $\mathbb{Q}$ рациональных чисел. Поэтому, переходя к модулю комплексного числа $Q_n(q)$, получаем

$$|Q_n(q)| = \prod_{\substack{s=1 \\ \text{НОД}(s,\,n)=1}}^{n} |q - \zeta^s| > \prod_{\substack{s=1 \\ \text{НОД}(s,\,n)=1}}^{n} (q-1) \geqslant q-1,$$

так как $n > 1$ и $q \geqslant 2$. Это неравенство несовместимо с утверждением, что $Q_n(q)$ делит $q-1$. Полученное противоречие означает, что $n = 1$, т. е. $D = Z$, что и доказывает теорему. □

Прежде чем приступить ко второму доказательству теоремы Веддербёрна, установим несколько вспомогательных результатов. Пусть D — конечное тело с центром Z, и пусть F — *максимальное подполе* тела D, т. е. F — такое подполе тела D, что единственным подполем этого тела, содержащим F, является само поле F. Тогда F является расширением поля Z. Действительно, если бы существовал элемент $z \in Z$, $z \notin F$, то, присоединяя z к F, мы получили бы подполе тела D, содержащее F в качестве собственного подполя, что противоречит максимальности F. Согласно теореме 2.10, $F = Z(\xi)$, где $\xi \in F^*$ — корень некоторого нормированного неприводимого многочлена $f \in Z[x]$.

Если рассматривать тело D как векторное пространство над полем F, то для каждого фиксированного элемента $a \in D$ равенство

$$T_a(d) = da \quad \text{для любого} \quad d \in D$$

определяет некоторый линейный оператор T_a в этом векторном пространстве. Рассмотрим теперь линейный оператор T_ξ. Если d — какой-нибудь собственный вектор этого оператора, то для некоторого $\lambda \in F^*$ (соответствующего собственного значения) будем иметь $T_\xi(d) = d\xi = \lambda d$, или $d\xi d^{-1} = \lambda$. Отсюда вытекает, что $dF^*d^{-1} = F^*$, т. е. элемент d принадлежит нормализатору $N(F^*)$ группы F^* в группе D^*. Обратно, если $d \in N(F^*)$, то $d\xi d^{-1} = \lambda$ для некоторого $\lambda \in F^*$, а это означает, что d — собственный вектор линейного оператора T_ξ. Таким образом, мы доказали следующий результат.

2.56. Лемма. *Элемент $d \in D^*$ является собственным вектором линейного оператора T_ξ в том и только том случае, когда он принадлежит нормализатору $N(F^*)$ группы F^* в группе D^*.*

Если λ — собственное значение, соответствующее собственному вектору d линейного оператора T_ξ, т. е. если $d\xi = \lambda d$, то

$$0 = df(\xi) = f(\lambda)\, d.$$

Это означает, что λ должно быть корнем многочлена f. Если d_0 — другой собственный вектор, соответствующий тому же собственному значению λ, то $d_0 d^{-1} \lambda d d_0^{-1} = \lambda$, так что элемент $b = d_0 d^{-1}$ коммутирует с λ, а следовательно, и с каждым элементом поля $F = Z(\lambda)$. Если через P обозначить множество значений многочленов из $F[x]$ при $x = b$, то легко проверить, что P образует конечное целостное кольцо, а значит (ввиду теоремы 1.31), P — конечное поле. Но поскольку P содержит F, то ввиду максимальности F имеем $P = F$. В частности, получим, что $b \in F$, а так как $d_0 = bd$, то заключаем, что собственному значению λ не может соответствовать двух и более линейно независимых собственных векторов. Теперь нам понадобится следующий результат из линейной алгебры.

2.57. Лемма. *Пусть T — линейный оператор в конечномерном векторном пространстве V над полем K. Для того чтобы пространство V имело базис, состоящий из собственных векторов оператора T, необходимо и достаточно, чтобы минимальный многочлен оператора T разлагался в поле K в произведение различных нормированных линейных сомножителей.*

Так как $f(\xi) = 0$, то многочлен f аннулирует оператор T_ξ. Кроме того, ввиду теоремы 2.14 f разлагается в поле F в произведение различных нормированных линейных сомножителей. Минимальный многочлен оператора T_ξ делит f, а следовательно, тоже разлагается в F в произведение различных нормированных линейных сомножителей. Поэтому по лемме 2.57 векторное пространство D над F имеет базис, состоящий из собственных векторов оператора T_ξ. Но выше было показано, что каждому собствен-

ному значению этого оператора может отвечать лишь одномерное собственное подпространство. Следовательно, размерность m векторного пространства D над F равна числу различных собственных значений оператора T_ξ. Пусть $\xi = \xi_1, \xi_2, \ldots, \xi_m$ — различные собственные значения линейного оператора T_ξ, а $1 = d_1, d_2, \ldots, d_m$ — соответствующие им собственные векторы, образующие базис векторного пространства D над F. Так как $N(F^*)$ как группа замкнуто относительно умножения, то в силу леммы 2.56 произведение $d_i d_j$ тоже является собственным вектором оператора T_ξ, соответствующим некоторому собственному значению ξ_k, так что $d_i d_j \xi = \xi_k d_i d_j$, а поскольку $d_j \xi = \xi_j d_j$, то отсюда получаем $d_i \xi_j = \xi_k d_i$, или $d_i \xi_j d_i^{-1} = \xi_k$. Это доказывает, что для любого i, $1 \leqslant i \leqslant m$, отображение, переводящее ξ_j в $d_i \xi_j d_i^{-1}$, переставляет собственные значения ξ_j между собой. Если ввести многочлен $g(x) = (x - \xi_1) \ldots (x - \xi_m)$, то сказанное выше означает, что его коэффициенты коммутируют с собственными векторами $d_1, \ldots, d_m$ оператора T_ξ. Так как коэффициенты многочлена g, очевидно, принадлежат полю F, а значит, коммутируют со всеми элементами этого поля, то они коммутируют также и со всеми элементами D, поскольку каждый такой элемент может быть представлен в виде линейной комбинации собственных векторов $d_1, \ldots, d_m$ с коэффициентами из F. Следовательно, коэффициенты многочлена g принадлежат центру Z тела D. Но $g(\xi) = 0$ [1]). Поэтому ввиду леммы 2.12 многочлен f делит g. С другой стороны, выше было установлено, что каждое собственное значение ξ_i оператора T_ξ является корнем многочлена f. Значит, $g = f$. Тем самым показано, что $[F : Z] = [Z(\xi) : Z] = \deg(f) = m$. Но число m в то же время является размерностью векторного пространства D над полем F, поэтому размерность D над полем Z равна m^2 (теорема 1.84). Поскольку эта размерность не зависит от поля F, мы заключаем, что каждое максимальное подполе тела D имеет одну и ту же степень над полем Z. Придадим этому результату следующую эквивалентную форму:

2.58. Лемма. *Все максимальные подполя тела D имеют один и тот же порядок.*

Второе доказательство теоремы 2.55. Пусть D — конечное тело, а Z, $F = Z(\xi)$ и $f \in Z[x]$ те же, что и раньше. Пусть E — произвольное максимальное подполе тела D. Тогда по лемме 2.58 поля E и F имеют один и тот же порядок, скажем q. В силу леммы

---

[1]) Так как $d_i g(\xi) d_i^{-1} = d_i \prod_{j=1}^{m} (\xi - \xi_j) d_i^{-1} = \prod_{j=1}^{m} (d_i \xi d_i^{-1} - d_i \xi_j d_i^{-1}) =$
$= \prod_{j=1}^{m} (\xi_i - \xi_{k_j}) = \prod_{j=1}^{m} (\xi_i - \xi_j) = 0$. — *Прим. перев.*

2.4 как E, так и F являются полями разложения многочлена $x^q - x$ над Z. На основании теоремы 1.91 существует изоморфизм поля F на E, оставляющий на месте элементы из Z. При этом изоморфизме образом элемента ξ является некоторый элемент $\eta \in E^*$, являющийся корнем многочлена f в поле E, так что $E = Z(\eta)$. Рассмотрим теперь линейный оператор T_η в векторном пространстве D над F. Так как $f(\eta) = 0$, то многочлен f аннулирует оператор T_η. Но поскольку f разлагается в поле F на линейные сомножители, существует такой корень $\lambda \in F$ многочлена f, который является собственным значением оператора T_η. Для соответствующего ему собственного вектора $d \in D$ мы получим тогда $d_\eta = \lambda d$. Отсюда ввиду того, что $F = Z(\lambda)$, получаем, что $E^* = d^{-1}F^*d$. Таким образом, E^* является сопряженной с F^* подгруппой группы D^*.

Для произвольного элемента $c \in D^*$ множество значений многочленов из $Z[x]$ при $x = c$ образует целостное кольцо, которое ввиду его конечности является полем (теорема 1.31). Поэтому каждый элемент группы D^* содержится в некотором подполе тела D, а значит, и в некотором максимальном подполе тела D. Выше мы доказали, что каждый элемент группы D^* принадлежит некоторой сопряженной с F^* подгруппе. Число различных сопряженных с F^* подгрупп группы D^* равно индексу нормализатора $N(F^*)$ в группе D^* (теорема 1.25), а так как $F^* \subset N(F^*)$, то оно не превосходит числа $|D^*|/|F^*|$. Поскольку каждая сопряженная с F^* подгруппа группы D^* содержит единицу тела D, то объединение всех сопряженных с F^* подгрупп содержит не более

$$\frac{|D^*|}{|F^*|}(|F^*| - 1) + 1 = |D^*| - \frac{|D^*|}{|F^*|} + 1$$

элементов. Но за исключением случая $D^* = F^*$ это число меньше $|D^*|$. Значит, $D = F$, т. е. тело D является полем. □

Комментарии

§ 1. Этой главой начинается собственно теория конечных полей. Большинство руководств по абстрактной алгебре посвящают конечным полям лишь несколько страниц. Наиболее обширные из таких разделов можно найти в книгах Albert [3], Berlekamp [4], Birkhoff, Bartee [1], Carmichael [4], Dornhoff, Hohn [1], Herstein [4], Lüneburg [2], Rédei [10], [11] и von Ammon, Tröndle [1]. Общая теория полей подробно изложена в книгах Browkin [2], Jacobson [2], Nagata [2] и Winter [1]. О конечных кольцах см. McDonald [1].

Понятие конечного поля в его общем значении (т. е. когда имеются в виду не только простые поля $\mathbb{F}_p$) впервые появляется в 1830 г. в статье Галуа (Galois [1]) в связи с решением сравнений

по модулю p (т. е. уравнений над полем $\mathbb{F}_p$) в подходящих расширениях поля $\mathbb{F}_p$. К этому времени многие свойства простых конечных полей $\mathbb{F}_p$ были уже установлены Ферма, Эйлером, Лагранжем, Лежандром и Гауссом (см. Gauss [1]). После исходной статьи Галуа изучение «высших сравнений», как тогда назывались уравнения над конечными полями, было продолжено в работах Schönemann [3], Serret [1] и Dedekind [1]. Начатки теории содержатся также в посмертно опубликованной работе Гаусса (Gauss [4]). Изложение этой ранней работы по конечным полям можно найти в сообщении Smith H. J. S. [1] и в работах Serret [2], Jordan C. [2] и Borel, Drach [1]. См. также заметку Niederreiter [14] о ранней истории предмета. О развитии теории конечных полей до 1915 г. см. книгу Dickson [40, ch. 8]. Впервые современная трактовка теории конечных полей появляется у Диксона (Dickson [7]).

Самыми важными результатами этой главы являются теоремы 2.5, 2.6 и 2.8. Существуют разные доказательства этих теорем, и их можно найти в упомянутых выше источниках. Заметим, что многие авторы используют для конечного поля (или поля Галуа) порядка q обозначение GF (q). Часть, касающаяся единственности, теоремы 2.5 впервые была доказана в общем виде Муром (Moore [1], [2]). Другое классическое доказательство теоремы 2.5 приводится в статье Dickson [6]. См. также Szele [1]. В связи с леммой 2.4 заметим, что простая формула для $\prod_{a \in F} (x - a^n)$ неявно содержится в работе Rados [5]; см. также относящиеся к этому статьи Beeger [1], Lubelski [1] и Ore [3].

Метод, использованный при доказательстве теоремы 2.8, можно применить и для доказательства следующего более общего утверждения: каждая конечная подгруппа мультипликативной группы поля циклична. Справедливо также обращение теоремы 2.8 (см. упр. 2.10). В статье Gilmer [1] найдены все конечные коммутативные кольца с единицей, в которых делители единицы образуют циклическую группу. В статье Čupona [1] конечные поля характеризуются свойствами порядков элементов мультипликативной группы данного поля.

Примитивные элементы конечного поля $\mathbb{F}_p$ при простом числе p рассматриваются также в элементарной теории чисел, где они носят название *первообразных корней по модулю p*. Задача нахождения первообразных корней по модулю p ставилась еще Гауссом (Gauss [1]); см. также Desmarest [1], Frolov [1], Jacobi [3], Schönheim [1], Stern [1] и Чебышёв [1]. Цассенхауз (Zassenhaus [4]) построил алгоритм для нахождения примитивных элементов любого конечного поля $\mathbb{F}_q$. О частном случае поля $\mathbb{F}_{p^2}$, где p — простое число Мерсенна, см. также Miller, Reed, Truong [1], Reed, Truong [1] и Reed, Truong, Miller [4].

Первая большая таблица первообразных корней была построена Якоби (Jacobi [3]) в 1839 г. Более подробно о таких таблицах см. в гл. 10. С примитивными элементами мы встретимся еще в связи с так называемыми примитивными многочленами (см. § 1 гл. 3).

Дэвенпорт (Davenport [6]) показал, что если простое число p достаточно велико, скажем $p > p_0(n)$, и θ — образующий элемент поля $\mathbb{F}_{p^n}$ как простого расширения поля $\mathbb{F}_p$, то в поле $\mathbb{F}_p$ найдется такой элемент a, что $\theta - a$ является примитивным элементом поля $\mathbb{F}_{p^n}$. С другой стороны, для данного $p > 2$ существуют расширение $\mathbb{F}_{p^n}$ и образующий элемент θ его как простого расширения поля $\mathbb{F}_p$, такие, что ни один из элементов $b\theta + c$, где $b, c \in \mathbb{F}_p$, не является примитивным элементом поля $\mathbb{F}_{p^n}$. Различные количественные улучшения и обобщения были получены в работах Carlitz [34], [41], Friedlander [1] и Schwarz [7]; см. также Giudici, Margaglio [2] для случая квадратичного расширения поля $\mathbb{F}_q$. Дэвенпорт и Льюис (Davenport, Lewis [3]) установили один результат о распределении примитивных элементов в конечных полях, обобщающий результат, полученный Бёрджессом (Burgess [2]) для простых полей $\mathbb{F}_p$. Позднее Бёрджесс (Burgess [7]) улучшил результат Дэвенпорта и Льюиса для полей $\mathbb{F}_{p^2}$, а Карацуба [6] распространил его на общие конечные поля. В статье Stevens H. [1] доказан один элементарный результат о распределении примитивных элементов. В работе Gerjets, Bergum [1] изучено распределение примитивных элементов в поле $\mathbb{F}_{p^2}$ с элементарной точки зрения. Простое доказательство существования примитивных элементов с абсолютным следом 1 в конечном поле $\mathbb{F}_q$ характеристики 2 получено в статье Moreno O. [2]. Из результата И. М. Виноградова (см. Виноградов И. М. [11]) следует, что для данных целых чисел a и b и всех достаточно больших простых чисел p существует целое число c, такое, что каждое из чисел c, $c + a$, $c + b$ является первообразным корнем по модулю p. Сегал [1] показал, что для данного целого числа $r \geqslant 2$ и всех достаточно больших простых чисел p существует такое целое число c, что каждое из чисел $c + 1$, $c + 2$, ..., $c + r$ является первообразным корнем по модулю p; этот результат был обобщен Карлицом (Carlitz [68]). См. также Johnsen [1], Szalay [1], [2], Vegh [1], [2], [3], [4], [5], [6] и Виноградов И. М. [8]. В работах Madden [1], Виноградов И. М. [5] и Сегал [1] изучается распределение примитивных элементов среди значений данного многочлена. Эрдёш (Erdös [1]) составил список нерешенных проблем и полученных результатов о первообразных корнях по модулю p. Для логарифма Якоби, определяемого с помощью примитивных элементов (см. упр. 2.8), в книге Jacobi [2] построены таблицы (для простых полей $\mathbb{F}_p$, $p \leqslant 103$); более удобные для вычислений таблицы приведены в работе Conway [1], см. также гл. 10, § 1 и таблицу B. В статье Gauss [1] дана формула для

суммы всех примитивных элементов простого поля $\mathbb{F}_p$, а в статье Stern [1] дана аналогичная формула для суммы всех элементов фиксированного порядка группы $\mathbb{F}_p^*$. В работе Forsyth [1] получена формула для суммы k-х степеней всех примитивных элементов поля $\mathbb{F}_p$; см. также Czarnota [1]. Шимичек (Szymiczek [1]) вывел формулу для суммы k-х степеней всех примитивных элементов произвольного конечного поля $\mathbb{F}_q$, и даже для суммы k-х степеней всех элементов фиксированного порядка группы $\mathbb{F}_q^*$.

В связи со следствием 2.11 заметим, что формула для числа нормированных неприводимых многочленов степени n в кольце $\mathbb{F}_q[x]$ будет получена в теореме 3.25. Это приведет к новому доказательству следствия 2.11 (см. замечания, следующие за примером 3.26).

§ 2. Важная теорема 2.14 была доказана Галуа (Galois [1]). Эта теорема выражает тот факт, что каждое конечное расширение $\mathbb{F}_{q^m}$ конечного поля $\mathbb{F}_q$ является *нормальным расширением*, т. е. оно обладает тем свойством, что каждый неприводимый многочлен из $\mathbb{F}_q[x]$, имеющий хотя бы один корень в поле $\mathbb{F}_{q^m}$, разлагается в этом поле на линейные сомножители. Справедлив и более общий результат: расширение произвольного поля K является конечным нормальным расширением в том и только том случае, если оно является полем разложения над K некоторого многочлена из $K[x]$. Теорема 2.14, кроме того, показывает, что любое конечное поле является *совершенным полем*, т. е. обладает следующим свойством: каждый неприводимый над этим полем многочлен имеет лишь простые корни. В соответствии с известной характеризацией совершенными являются поля характеристики 0 и те поля простой характеристики p, для которых корень p-й степени из любого элемента поля содержится в этом поле. Последнее условие непосредственно и легко проверяется для конечных полей (ср. с упр. 2.12).

Автоморфизм σ поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$, порождающий все автоморфизмы поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ (в соответствии с теоремой 2.21), называется *автоморфизмом Фробениуса* поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Группа автоморфизмов поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ носит также название *группы Галуа* поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$. Эта группа играет основную роль в теории Галуа. О теории Галуа см. Artin [8], Gaal [1], Jacobson [2], Lang [4, ch. 8], van der Waerden [2, ch. 8] (а также Постников М. М. [1*]. — *Перев.*), а о том частном ее случае, который рассматривается здесь, см. Dickson [10] и Scarpis [3]. В силу теоремы 2.21 группа Галуа поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ циклическая, и, следовательно, $\mathbb{F}_{q^m}$ — *циклическое* расширение поля $\mathbb{F}_q$.

Неприводимые многочлены над конечными полями будут рассматриваться и в гл. 3 (особенно в § 2, 3 и 5).

§ 3. Результаты теоремы 2.25 и упр. 2.33 являются частными случаями для следов и норм теоремы 90 Гильберта, справедливой

для любого конечного циклического расширения некоторого поля (Hilbert [2]). См. также упр. 2.30 и 2.31 о других доказательствах теоремы 2.25. Об обобщениях теоремы 90 Гильберта см. Albert [3, ch. 4], Bourbaki [1, ch. V, § 11], Jacobson [2] и Winter [1].

В связи с понятием автодуального базиса (см. пример 2.31) заметим, что в статье Seroussi, Lempel [1] показано, что поле $F = \mathbb{F}_{q^m}$ тогда и только тогда имеет автодуальный базис над $K = \mathbb{F}_q$, когда либо q четно, либо q и m оба нечетны. В той же статье доказано, что поле F всегда имеет *следоортогональный базис* над K, т. е. базис $\{\alpha_1, \ldots, \alpha_m\}$, такой, что $\mathrm{Tr}_{F/K}(\alpha_i\alpha_j) = 0$ для $i \neq j$. Для случая $q = 2$ эти результаты были установлены раньше в статье Lempel [2]. В книге MacWilliams, Sloane [2, ch. 4] показано, что поле $\mathbb{F}_{2^m}$ имеет автодуальный нормальный базис, если m нечетно. Для четного m это не всегда верно (см. упр. 2.41).

Доказательство леммы 2.34 приводится, например, в книге Hoffman, Kunze [1, ch. 7]; указанное пособие можно рекомендовать для справок и по другим вопросам линейной алгебры. Теорема 2.35 является частным случаем общей теоремы о нормальном базисе для конечных расширений Галуа (см. Albert [3, ch. 4], Berger, Reiner [1], Deuring [1], Jacobson [2], Rédei [10, ch. 11], Waterhouse [3]). Другое доказательство теоремы 2.35 вместе с формулой для числа различных нормальных базисов поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ будет приведено в гл. 3 (см. теорему 3.73 и следующее за ней замечание). Теорема о нормальном базисе для конечных полей была сформулирована Эйзенштейном (Eisenstein [6]) и частично доказана Шёнеманном (Schönemann [4]). Первое полное доказательство ее дал Гензель (Hensel [1]). См. также Krasner [2], где дается иной тип доказательства. Таблицы нормальных базисов и дуальных базисов к полиномиальным и нормальным базисам построил Конвей (Conway [1]) для полей характеристики 2; см. также гл. 10 (§ 1 и табл. B). О приложении теоремы о нормальном базисе к теории кодирования см. Camion [1].

Мур (Moore [3]) представил определитель из следствия 2.38 в виде $\prod\left(\sum_{j=1}^{m} b_j\alpha_j\right)$, где произведение берется по всем ненулевым m-наборам $(b_1, \ldots, b_m) \in \mathbb{F}_q^m$, для которых ненулевой элемент b_j с наибольшим индексом равен 1. См. также лемму 3.51, где эта формула доказывается проще. В статье Carlitz [85] доказано несколько аналогичных равенств для определителей. Прямое доказательство следствия 2.38, не использующее формулу Мура, было дано Диксоном (Dickson [2], [7, part 1, ch. 4]). Теорема 2.39 была в эквивалентной форме доказана Дэвенпортом (Davenport [9]). В этой же статье содержится доказательство теоремы

2.40. Для конечного поля F достаточно большого порядка этот результат раньше был уже установлен Карлицом (Carlitz [35]). Ленстра (Lenstra H. W. [1]) показал, что нормальный базис поля F, состоящий из примитивных элементов, существует над любым подполем этого поля. Если число m в теореме 2.39 является степенью характеристики поля $\mathbb{F}_q$, то утверждение теоремы выполняется при более слабом предположенин, а именно что след элемента α над $\mathbb{F}_q$ отличен от нуля; об этом случае см. также Perlis [1], Burde [5] и Childs, Orzech [1].

Эффективный алгоритм построения базисных векторов для всех подпространств заданной размерности некоторого векторного пространства над полем $\mathbb{F}_q$ получен в статье Calabi, Wilf [1]. Некоторые комбинаторные задачи для векторных пространств над конечным полем $\mathbb{F}_q$ были рассмотрены в работах Baum, Neuwirth [1], Bu [1], Constantin, Courteau [1], Jamison [1], Lee A. [1], Luh [1] и Wolfmann [1]. В статье Brawley, Hankins [1] дан перечень базисов векторного пространства, образованного $m \times n$-матрицами над $\mathbb{F}_q$, в соответствии с рангами базисных матриц.

§ 4. Явная формула для кругового многочлена будет указана в теореме 3.27. Результат теоремы 2.47 (i) был установлен впервые Кронекером (Kronecker [1]). Другие классические доказательства принадлежат Арндту (Arndt [1]), Дедекинду (Dedekind [2]) и Лебегу (Lebesgue [3]). Доказательства этой теоремы можно найти также в книгах Lang [4, ch. 8], Rédei [10, ch. 8] и van der Waerden [2, ch. 8]. Разложение круговых многочленов над простыми полями $\mathbb{F}_p$ рассматривалось Гауссом (Gauss [4]), Шёнеманном (Schönemann [3]) и Пелле (Pellet [5]) еще в XIX в. См. об этом также Ballieu [1], Chowla, Vijayaraghavan [1], Golomb [7], Guerrier [1], Lubelski [2], McLain, Edgar [1], Rèdei [10, ch. 8] и van de Vooren-van Veen [1]. Случай произвольного конечного поля $\mathbb{F}_q$ рассмотрен в статье Rautèr [2]. Из теоремы 2.47 (ii) и элементарной теории чисел следует, что круговой многочлен Q_n неприводим над полем $\mathbb{F}_q$ тогда и только тогда, когда q — первообразный корень по модулю n и n принимает значения 4, r^k или $2r^k$ при простом нечетном числе r и неотрицательном целом числе k. Подробнее о методах отыскания разложений круговых многочленов над конечными полями см. в гл. 4, особенно в примере 4.6. Упражнение 2.57 содержит список дальнейших свойств круговых многочленов.

В статьях Reed, Truong, Miller [1], [2] развиты эффективные методы вычисления корней некоторой степени из единицы в конечных полях специального вида; см. также Liu, Reed, Truong [1]. В работе Althaus, Leake [1] дана формула обращения матрицы Вандермонда, элементами которой являются корни из единицы, см. также Knuth [2, ch. 1].

§ 5. В дополнение к уже рассмотренным методам представления конечных полей заметим, что конечные поля можно рассматривать также как факторкольца кольца целых алгебраических чисел по простым идеалам, — этой точке зрения придавал особое значение Дедекинд (Dedekind [3]); см. также Burde [7] и Niederreiter [14]. Цассенхауз (Zassenhaus [4]) дал алгоритм построения конечных расширений поля $\mathbb{F}_q$, а Ю. П. Васильев в [1] рассматривает этот вопрос с точки зрения применения ЭВМ; см. также Chor [1]. О представлении элементов конечных полей матрицами см. Scognamiglio [1]. В этой связи интересны также работы Beard [1], [2], [3], [4] и Beard, McConnel [1]. Некоторые результаты о сопровождающей матрице многочлена, используемой в этом параграфе, можно найти в книге Hoffman, Kunze [1, ch. 7].

В статье Hohler [1] поле $\mathbb{F}_{p^2}$ строится на базе простого поля $\mathbb{F}_p$ способом, напоминающим построение комплексных чисел на базе действительных. Дальнейшие представления элементов конечных полей можно найти в работах Bartee, Schneider [1], Fadini [1], Mönnig [1], Neikirk [1]. Конечные поля, которые можно рассматривать как подполя факторкольца $\mathbb{Z}/(m)$, были охарактеризованы в статье Nymann [1]. В работе Raktoe [1] показано, как некоторые кольца, аналогичные кольцу многочленов над кольцом $\mathbb{Z}/(m)$, можно построить, исходя из конечных полей и колец многочленов над конечными полями.

§ 6. В 1905 г. Веддербёрн доказал, что каждое конечное тело является полем. Со времени исходной статьи Веддербёрна Wedderburn [1] было дано много других доказательств этого результата, и они допускают разветвленную классификацию в зависимости от используемого аппарата: теории чисел, теории групп, линейной алгебры, теории конечномерных алгебр или теории когомологий. В статье Веддербёрна приведено три доказательства этого результата. Первое, основанное на линейной алгебре и теории минимальных многочленов, однако, как заметил Артин (Artin [2]), оказалось ошибочным; см. Hinz [1], где это доказательство исправляется. Другие два доказательства основаны на следующей теоретико-числовой лемме: если n и b — такие целые числа $\geqslant 2$, что каждый простой делитель числа $b^n - 1$ делит число $b^m - 1$ при некотором m, $1 \leqslant m < n$, то либо $n = 2$ и $b + 1$ — степень двойки, либо $n = 6$ и $b = 2$ (см. Zsigmondy [1], Birkhoff, Vandiver [1], а также Artin [5]). Диксон в статье Dickson [8] дал свое доказательство теоремы Веддербёрна (использующее эту же лемму); при этом он отмечает, что Веддербёрн пришел к своим последним двум доказательствам после того, как познакомился с доказательством Диксона.

Первое из приводимых нами доказательств теоремы 2.55 принадлежит Витту (Witt [1]). Оно одно из самых коротких и изящных. В последней его части можно избежать использования ком-

плексных чисел, воспользовавшись методами элементарной теории чисел (см. Klobe [1] и Rogers K. [1]). Второе доказательство принадлежит Тейлору (Taylor D. E. [1]). Доказательство леммы 2.57 можно найти, например, в книге Hoffman, Kunze [1, ch. 6].

Многие доказательства теоремы Веддербёрна используют теорию групп. Так, доказательство Цассенхауза (Zassenhaus [2]) опирается на следующую лемму: любая конечная группа, в которой нормализатор каждой абелевой подгруппы совпадает с ее централизатором, является абелевой. По поводу других теоретико-групповых доказательств см. Brandis [1], Kaczynski [1] и Scott [1, ch. 14]. В книге Blanchard [1, ch. 4] дается доказательство, основанное на теории когомологий. В статье Herstein [2] использована комбинация теоретико-кольцевых и теоретико-групповых методов. Доказательство, использующее многочлены над телами, предложено Артином (Artin [2]).

Доказательства теоремы Веддербёрна, основанные на теории конечномерных алгебр и на результатах, аналогичных лемме 2.58, можно найти в работах Blanchard [1, ch. 3], Bourbaki [2, ch. VIII, § 11], Nagahara, Tominaga [1] и van der Waerden [3, ch. 14]. Интересный вариант доказательства приводится в статье Joly [5], где в решающем месте использована теорема Шевалле об уравнениях над конечными полями (см. следствие 6.6).

Другие доказательства и комментарии к истории теоремы Веддербёрна можно найти в работах Artin [4], Herstein [3, ch. 3], [4] и Rédei [10, ch. 8].

Известным обобщением теоремы Веддербёрна является следующий результат Джекобсона (см. Jacobson [1]): если в кольце R для каждого элемента $a \in R$ найдется натуральное число $n(a) > 1$, такое, что $a^{n(a)} = a$, то R является полем. Доказательство теоремы Джекобсона имеется также в работах Herstein [1], [2], [3, ch. 3], [4], Laffey [1], Nagahara, Tominaga [1], Rogers K. [2] и Wamsley [1]. В другом направлении теорема Веддербёрна была обобщена смягчением условия ассоциативности умножения в конечном теле (Albert [2], McCrimmon [1]). Характеризация конечных простых полей в классе почти-колец (near-rings) с единицей была дана в работах Clay, Malone [1] и Maxson [1].

[Кох (Koh [1*]) получил оценки для числа невырожденных квадратных матриц порядка n над произвольным конечным полем. В работе Calmet [1*] рассматриваются алгебраические алгоритмы в конечных полях (типа алгоритмов для разложения многочленов на множители, нахождения корней многочленов и т. п.). По тематике второй главы имеются еще следующие работы: Barker [1*], Cohen [2*], [3*], [4*], Coppersmith [1*], Coppersmith, Odlyzko, Schroeppel [1*], Gerth [1*], Hellman, Reyneri [1*], Katze, Rajwade [1*], [2*], Lempel, Seroussi, Winograd [1*], Lempel,

Seroussi, Ziv [1*], Mukhopadhyay [1*], Muskat, Williams [1*], Pei, Wang, Omura [1*], Zeitler [1*], Кисловская [1*], Курбатов [1*] и Сейтенов [1*]. — *Перев.*]

Упражнения

2.1 Доказать, что многочлен $x^2 + 1$ неприводим над полем $\mathbb{F}_{11}$, и показать непосредственно, что факторкольцо $\mathbb{F}_{11}[x]/(x^2 + 1)$ состоит из 121 элемента. Доказать также, что многочлен $x^2 + x + 4$ неприводим над полем $\mathbb{F}_{11}$, и показать, что факторкольца $\mathbb{F}_{11}[x]/(x^2 + 1)$ и $\mathbb{F}_{11}[x]/(x^2 + x + 4)$ изоморфны.

2.2. Показать, что для каждого конечного поля, кроме $\mathbb{F}_2$, сумма всех его элементов равна 0.

2.3. Пусть a, b — элементы поля $\mathbb{F}_{2^n}$ (n — нечетное число). Показать, что из равенства $a^2 + ab + b^2 = 0$ вытекает $a = b = 0$.

2.4. Найти все примитивные элементы поля $\mathbb{F}_7$.

2.5. Найти все примитивные элементы поля $\mathbb{F}_{17}$.

2.6. Найти все примитивные элементы поля $\mathbb{F}_9$.

2.7. Записать все элементы поля $\mathbb{F}_{25}$ в виде линейных комбинаций базисных элементов над полем $\mathbb{F}_5$. Затем найти какой-нибудь примитивный элемент β поля $\mathbb{F}_{25}$ и для каждого элемента $\alpha \in \mathbb{F}_{25}^*$ найти наименьшее целое неотрицательное число n, такое, что $\alpha = \beta^n$.

2.8. Если элементы мультипликативной группы $\mathbb{F}_q^*$ поля $\mathbb{F}_q$ представлены в виде степеней фиксированного примитивного элемента $b \in \mathbb{F}_q$, то сложение в поле $\mathbb{F}_q$ облегчается введением так называемого *логарифма Якоби* [1]) $L(n)$, определяемого равенством

$$1 + b^n = b^{L(n)},$$

где случай $b^n = -1$ исключается [2]). Показать, что тогда всюду, где L определен, справедливо равенство

$$b^m + b^n = b^{m + L(n-m)}.$$

Построить таблицу логарифмов Якоби для полей $\mathbb{F}_9$ и $\mathbb{F}_{17}$.

2.9. Доказать, что любая конечная подгруппа мультипликативной группы F^* произвольного поля F циклична.

2.10. Пусть F — поле. Доказать, что если его мультипликативная группа F^* циклична, то F — конечное поле.

2.11. Пусть F — конечное поле и F^* — его мультипликативная группа. Доказать, что множество $H \cup \{0\}$ для любой подгруппы H группы F^* будет подполем поля F в том и только том случае, если порядок группы F^* равен 1 или простому числу вида $2^p - 1$, где p — простое число.

2.12. Показать, что каждый элемент конечного поля $\mathbb{F}_q$ характеристики p имеет в этом поле один и только один корень p-й степени.

2.13. Показать, что если $\mathbb{F}_q$ — конечное поле нечетной характеристики, то элемент $a \in \mathbb{F}_q^*$ имеет в поле $\mathbb{F}_q$ квадратный корень тогда и только тогда, когда $a^{(q-1)/2} = 1$.

2.14. Доказать, что для данного натурального числа k элемент $a \in \mathbb{F}_q^*$ является k-й степенью некоторого элемента из поля $\mathbb{F}_q$ в том и только том случае, если $a^{(q-1)/d} = 1$, где $d = \text{НОД}(q - 1, k)$.

---

[1]) Некоторые авторы (например, Conway [1]) называют его логарифмом Зеха (Sech). — *Прим. перев.*

[2]) В соответствии с соглашением в подстрочном примечании к примеру 2.52 для такого n, что $b^n = -1$, полагается $L(n) = *$. — *Прим. перев.*

2.15. Доказать, что для любого $k \in \mathbb{N}$ каждый элемент поля $\mathbb{F}_q$ является k-й степенью некоторого элемента из этого поля в том и только том случае, если НОД $(q-1, k) = 1$.

2.16. Пусть $\mathbb{F}_q$ — конечное поле, k — положительный делитель числа $q-1$ и a — такой элемент поля F_q, что уравнение $x^k = a$ не имеет решений в $\mathbb{F}_q$. Доказать, что это уравнение имеет решение в поле $\mathbb{F}_{q^m}$, если число m делится на k, и что если k — простое число, то выполняется обратное утверждение.

2.17. Доказать, что для $f \in \mathbb{F}_q[x]$ верно равенство $[f(x)]^q = f(x^q)$.

2.18. Показать, что любой квадратный многочлен из $\mathbb{F}_q[x]$ разлагается над полем $\mathbb{F}_{q^2}$ на линейные множители.

2.19. Показать, что при $a \in \mathbb{F}_q$ и $n \in \mathbb{N}$ многочлен $x^{q^n} - x + na$ делится на $x^q - x + a$ в кольце $\mathbb{F}_q[x]$.

2.20. Найти все автоморфизмы конечного поля.

2.21. Пусть F — некоторое поле и отображение $\Psi\colon F \to F$ определяется условием $\Psi(a) = a^{-1}$ при $a \neq 0$ и $\Psi(a) = 0$ при $a = 0$. Доказать, что Ψ является автоморфизмом поля F тогда и только тогда, когда F состоит не более чем из четырех элементов.

2.22. Доказать, что натуральное число n делит число $\varphi(p^n - 1)$, где p — простое число, а φ — функция Эйлера. (*Указание.* Воспользоваться следствием 2.19).

2.23. Пусть $\mathbb{F}_q$ — конечное поле характеристики p. Доказать, что многочлен $f \in \mathbb{F}_q[x]$ обладает свойством $f'(x) = 0$ в том и только том случае, если f является p-й степенью некоторого многочлена из $\mathbb{F}_q[x]$.

2.24. Пусть F — конечное расширение конечного поля K, причем $[F : K] = m$, и пусть

$$f(x) = x^d + b_{d-1}x^{d-1} + \cdots + b_0 \in K[x]$$

— минимальный многочлен элемента $\alpha \in F$ над полем K. Доказать, что $\mathrm{Tr}_{F/K}(\alpha) = -(m/d)\, b_{d-1}$ и $\mathrm{N}_{F/K}(\alpha) = (-1)^m b_0^{m/d}$.

2.25. Пусть F — конечное расширение конечного поля K и $\alpha \in F$. Пусть, далее, отображение $L\colon \beta \in F \longmapsto \alpha\beta \in F$ является линейным оператором в поле F, рассматриваемом как векторное пространство над K. Доказать, что характеристический многочлен $g(x)$ элемента α над K совпадает с характеристическим многочленом линейного оператора L, т. е. $g(x) = \det(xI - L)$, где I — тождественный оператор.

2.26. Рассмотрим ту же ситуацию, что и в упр. 2.25. Доказать, что $\mathrm{Tr}_{F/K}(\alpha)$ совпадает со следом линейного оператора L (т. е. с суммой диагональных элементов соответствующей оператору матрицы в произвольном базисе), и $\mathrm{N}_{F/K}(\alpha) = \det(L)$.

2.27. Доказать свойства (i) и (ii) из теоремы 2.23, используя интерпретацию $\mathrm{Tr}_{F/K}(\alpha)$, полученную в упр. 2.26.

2.28. Доказать свойства (i) и (iii) из теоремы 2.28, используя интерпретацию $\mathrm{N}_{F/K}(\alpha)$, полученную в упр. 2.26.

2.29. Пусть F — конечное расширение конечного поля K характеристики p. Доказать, что для всех $\alpha \in F$ и $n \in \mathbb{N}$ имеет место равенство $\mathrm{Tr}_{F/K}(\alpha^{p^n}) = [\mathrm{Tr}_{F/K}(\alpha)]^{p^n}$.

2.30. Дать другое доказательство теоремы 2.25, рассматривая поле F как векторное пространство над полем K и показав, сравнивая размерности, что ядро линейного отображения $\mathrm{Tr}_{F/K}$ совпадает с множеством значений линей-

ного оператора L в векторном пространстве F над полем K, где $L(\beta) = \beta^q - \beta$ для всех $\beta \in F$.

2.31. Дать другое доказательство необходимости условия в теореме 2.25, показав, что если $\alpha, \gamma \in F$ таковы, что $\mathrm{Tr}_{F/K}(\alpha) = 0$ и $\mathrm{Tr}_{F/K}(\gamma) = -1$, и $\delta_j = \alpha + \alpha^q + \ldots + \alpha^{q^{j-1}}$, то элемент

$$\beta = \sum_{j=1}^{[F:K]} \delta_j \gamma^{q^j - 1}$$

удовлетворяет условию $\beta^q - \beta = \alpha$.

2.32. Пусть F — конечное расширение поля $K = \mathbb{F}_q$ и $\alpha = \beta^q - \beta$ для некоторого $\beta \in F$. Доказать, что равенство $\alpha = \gamma^q - \gamma$ выполняется для $\gamma \in F$ тогда и только тогда, когда $\beta - \gamma \in K$.

2.33. Пусть F — конечное расширение поля $K = \mathbb{F}_q$. Доказать, что для $\alpha \in F$ равенство $\mathrm{N}_{F/K}(\alpha) = 1$ выполняется в том и только том случае, если $\alpha = \beta^{q-1}$ для некоторого $\beta \in F^*$.

2.34. Доказать, что $\sum_{j=0}^{m-1} x^{q^j} - c = \prod (x - \alpha)$ для всех $c \in K = \mathbb{F}_q$, где произведение берется по всем $\alpha \in F = \mathbb{F}_{q^m}$, удовлетворяющим условию $\mathrm{Tr}_{F/K}(\alpha) = c$.

2.35. Доказать, что для любого $m \in \mathbb{N}$ имеет место равенство

$$x^{q^m} - x = \prod_{c \in \mathbb{F}_q} \left(\sum_{j=0}^{m-1} x^{q^j} - c \right).$$

2.36. Рассматривая поле $\mathbb{F}_{q^m}$ как векторное пространство над полем $\mathbb{F}_q$, доказать, что для каждого линейного оператора L в этом векторном пространстве существует однозначно определенный m-набор $(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ элементов из $\mathbb{F}_{q^m}$, который обладает свойством

$$L(\beta) = \alpha_0 \beta + \alpha_1 \beta^q + \cdots + \alpha_{m-1} \beta^{q^{m-1}}$$

для всех $\beta \in \mathbb{F}_{q^m}$.

2.37. Доказать, что если учитывать порядок элементов базиса, то число различных базисов поля $\mathbb{F}_{q^m}$ как векторного пространства над полем $\mathbb{F}_q$ равно

$$(q^m - 1)(q^m - q)(q^m - q^2) \ldots (q^m - q^{m-1}).$$

2.38. Доказать, что если $\{\alpha_1, \ldots, \alpha_m\}$ — базис поля $F = \mathbb{F}_{q^m}$ как векторного пространства над полем $K = \mathbb{F}_q$, то $\mathrm{Tr}_{F/K}(\alpha_i) \neq 0$ хотя бы для одного i, $1 \leqslant i \leqslant m$.

2.39. Доказать, что существует нормальный базис $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ поля $F = \mathbb{F}_{q^m}$ над $K = \mathbb{F}_q$, для которого $\mathrm{Tr}_{F/K}(\alpha) = 1$.

2.40. Пусть K — конечное поле, $F = K(\alpha)$ — его простое расширение степени n и $f \in K[x]$ — минимальный многочлен элемента α над K. Пусть, далее,

$$\frac{f(x)}{x - \alpha} = \beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} \in F[x] \quad \text{и} \quad \gamma = f'(\alpha).$$

Доказать, что дуальным к базису $\{1, \alpha, \ldots, \alpha^{n-1}\}$ поля F над K является базис $\{\beta_0 \gamma^{-1}, \beta_1 \gamma^{-1}, \ldots, \beta_{n-1} \gamma^{-1}\}$.

2.41. Показать, что существует автодуальный нормальный базис поля $\mathbb{F}^4$ над $\mathbb{F}_2$, но не существует автодуального нормального базиса поля $\mathbb{F}_{16}$ над $\mathbb{F}^2$ (определенне автодуального базиса см. в примере 2.31).

2.42. Построить автодуальный базис поля $\mathbb{F}_{16}$ над $\mathbb{F}_2$ (определение автодуального базиса см. в примере 2.31).

2.43. Доказать, что дуальный базнс к нормальному базису поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ снова является нормальным базисом.

2.44. Пусть F — расширение конечного поля K с базисом $\{\alpha_1, \ldots, \alpha_m\}$ над K. Пусть, далее, элементы $\beta_1, \ldots, \beta_m \in F$ таковы, что $\beta_i = \sum_{j=1}^{m} b_{ij}\alpha_j$ для $1 \leqslant i \leqslant m$, где $b_{ij} \in K$. Пусть, наконец, $B = (b_{ij})$ — квадратная матрица порядка m. Доказать, что

$$\Delta_{F/K}(\beta_1, \ldots, \beta_m) = [\det(B)]^2\, \Delta_{F/K}(\alpha_1, \ldots, \alpha_m).$$

2.45. Пусть $K = \mathbb{F}_q$ и $F = \mathbb{F}_{q^m}$. Доказать, что для любого $\alpha \in F$ имеет место равенство

$$\Delta_{F/K}(1, \alpha, \ldots, \alpha^{m-1}) = \prod_{0 \leqslant i < j \leqslant m-1} \left(\alpha^{q^i} - \alpha^{q^j}\right)^2.$$

2.46. Доказать, что для $\alpha \in F = \mathbb{F}_{q^m}$ с $m \geqslant 2$ и $K = \mathbb{F}_q$ дискриминант $\Delta_{F/K}(1, \alpha, \ldots, \alpha^{m-1})$ совпадает с дискриминантом характеристического многочлена элемента α над полем K (см. определение 1.92).

2.47. Найти первообразные корни 4-й и 8-й степеней из единицы в поле $\mathbb{F}_9$.

2.48. Найти первообразный корень 9-й степени из единицы в поле $\mathbb{F}_{19}$.

2.49. Пусть ζ — корень n-й степени из единицы над полем K. Доказать, что

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = \begin{cases} 0 & \text{при } \zeta \neq 1, \\ n & \text{при } \zeta = 1. \end{cases}$$

2.50. Для $n \geqslant 2$ пусть $\zeta_1, \ldots, \zeta_n$ — все (не обязательно различные) корни n-й степени из единицы над произвольным полем K. Доказать, что

$$\zeta_1^k + \cdots + \zeta_n^k = \begin{cases} 0 & \text{при } k = 1, 2, \ldots, n-1, \\ n & \text{при } k = 0. \end{cases}$$

2.51. Показать, что $K^{(2n)} = K^{(n)}$ для произвольного поля K и нечетного числа n.

2.52. Пусть K — произвольное поле. Доказать, что круговое поле $K^{(d)}$ является подполем поля $K^{(n)}$ для каждого положительиого делителя d числа $n \in \mathbb{N}$. Найти минимальный многочлен над полем $K^{(4)}$ такого корня из единицы, который может служить образующим элементом простого расширения $K^{(12)}$ над $K^{(4)}$.

2.53. Доказать, что если p — простое число, то $p - 1$ первообразных корней p-й степени из единицы над полем $\mathbb{Q}$ рацнональных чисел линейно независимы над $\mathbb{Q}$ н потому образуют базис поля $\mathbb{Q}^{(p)}$ над $\mathbb{Q}$.

2.54. Пусть K — произвольное поле и n — натуральное число, большее единицы. Доказать, что многочлен $x^{n-1} + x^{n-2} + \ldots + x + 1$ неприводим над K, лишь когда n — простое число.

2.55. Найти наименьшее простое число p, такое, что многочлен $x^{22} + x^{21} + \ldots + x + 1$ неприводнм над полем $\mathbb{F}_p$.

2.56. Найти десять наименьших простых чисел p, таких, что многочлен $x^{p-1} + x^{p-2} + \ldots + x + 1$ неприводим над полем $\mathbb{F}_2$.

2.57. Доказать следующие свойства круговых многочленов над любым полем, для которого они определены:

(a) $Q_{mp}(x) = Q_m(x^p)/Q_m(x)$, если p — простое число и натуральное число m не делится на p;

(b) $Q_{mp}(x) = Q_m(x^p)$ для всех натуральных чисел m, кратных простому числу p;

(c) $Q_{mp^k}(x) = Q_{mp}\left(x^{p^{k-1}}\right)$, если p — простое число и m, $k \in \mathbb{N}$;

(d) $Q_{2n}(x) = Q_n(-x)$, если $n \geqslant 3$ — нечетное число;

(e) $Q_n(0) = 1$, если $n \geqslant 2$;

(f) $Q_n\left(x^{-1}\right) x^{\varphi(n)} = Q_n(x)$, если $n \geqslant 2$;

(g) $Q_n(1) = \begin{cases} 0, \text{ если } n = 1, \\ p, \text{ если } n \text{ — степень простого числа } p, \\ 1, \text{ если } n \text{ имеет по крайней мере два различных простых делителя;} \end{cases}$

(h) $Q_n(-1) = \begin{cases} 0, \text{ если } n = 2, \\ -2, \text{ если } n = 1, \\ p, \text{ если } n \text{ — удвоенная степень простого числа } p, \\ 1 \text{ в остальных случаях.} \end{cases}$

2.58. Дать представление с помощью матриц для элементов поля $\mathbb{F}_8$, используя для этой цели непрнводимый многочлен $x^3 + x + 1$ над полем $\mathbb{F}_2$.

2.59. Пусть ζ — прнмитивный элемент поля $F = \mathbb{F}_{16}$, такой, что $\zeta^4 + \zeta + 1 = 0$. Для $k \geqslant 0$ запишем $\zeta^k = \sum_{l=0}^{3} a_{kl}\zeta^l$, где $a_{kl} \in \mathbb{F}_2$, и пусть $M_k = \left(m_{ij}^{(k)}\right)$ — квадратная матрица 4-го порядка с элементами $m_{ij}^{(k)} = a_{k+i-1,\, j-1}$. Показать, что 15 матриц M_k, $0 \leqslant k \leqslant 14$, и нулевая матрица 4-го порядка образуют поле (относительно операций сложения и умножения матриц над полем $\mathbb{F}_2$), которое изоморфно F. Доказать, что для $0 \leqslant k \leqslant 14$ след $\mathrm{Tr}_F(\zeta^k)$ равен следу матрицы M_k и совпадает с коэффициентом a_{k3}.

Глава 3

Многочлены над конечными полями

Теория многочленов над конечными полями важна как для исследования алгебраической структуры конечных полей, так и для многочисленных приложений. При этом особую роль играют неприводимые многочлены — простые элементы кольца многочленов над конечным полем. Они необходимы для построения самого́ конечного поля и для проведения вычислений с элементами этого поля.

В первом параграфе вводится понятие порядка многочлена. Важным фактом является связь между минимальными многочленами примитивных элементов конечного поля (так называемыми примитивными многочленами) и многочленами максимального возможного для данной степени порядка. В § 2 представлены результаты о неприводимых многочленах, не рассмотренные в предыдущих главах. Третий параграф посвящен конструктивным аспектам неприводимости, а также вопросу о нахождении минимального многочлена элемента из некоторого расширения поля.

В последних двух параграфах рассматриваются некоторые специальные классы многочленов. Линеаризованный многочлен характеризуется тем, что степень каждого его члена является некоторой степенью характеристики поля. Теория таких многочленов, интересная сама по себе, позволяет к тому же дать новое доказательство теоремы о нормальном базисе. Двучлены (биномы) и трехчлены, т. е. двучленные и трехчленные многочлены образуют другой класс, для которого тоже можно установить ряд особых свойств, представляющих значительный интерес. Следует напомнить, что в предыдущей главе было рассмотрено еще одно полезное семейство многочленов — а именно круговые многочлены (см. гл. 2, § 4). Некоторые дополнительные факты об этих многочленах приводятся далее в § 2.

§ 1. Порядки многочленов и примитивные многочлены

У каждого ненулевого многочлена f над конечным полем кроме его степени $\deg(f)$ имеется еще одна важная целочисленная характеристика — его порядок. Определение порядка многочлена основывается на следующем факте.

3.1. Лемма. *Если* $f \in \mathbb{F}_q[x]$ *— многочлен степени* $m \geqslant 1$, *удовлетворяющий условию* $f(0) \neq 0$, *то существует натуральное число* $e \leqslant q^m - 1$, *для которого двучлен* $x^e - 1$ *делится на многочлен* $f(x)$.

Доказательство. В факторкольце $\mathbb{F}_q[x]/(f)$ содержится $q^m - 1$ ненулевых элементов (т. е. классов вычетов по модулю идеала (f)). Поскольку каждый из q^m классов вычетов $x^j + (f)$, $j = 0, 1, \ldots, q^m - 1$, является ненулевым элементом этого фактор кольца, то должны существовать такие целые числа r и s, $0 \leqslant r < s \leqslant q^m - 1$ что $x^s \equiv x^r \pmod{(f(x))}$. А поскольку многочлен x взаимно прост с $f(x)$, то $x^{s-r} \equiv 1 \pmod{(f(x))}$. Это означает, что многочлен $x^{s-r} - 1$ делится на $f(x)$, где $0 < s - r \leqslant q^m - 1$. □

Так как многочлен $x - 1$ делится на любой ненулевой постоянный многочлен, то в следующее определение можно включить и постоянные многочлены.

3.2. Определение. Пусть $f \in \mathbb{F}_q[x]$ — ненулевой многочлен. Если $f(0) \neq 0$, то наименьшее натуральное число e, для которого многочлен $f(x)$ делит $x^e - 1$, называется *порядком* многочлена $f(x)$ и обозначается $\operatorname{ord}(f) = \operatorname{ord}(f(x))$. Если же $f(0) = 0$, то многочлен $f(x)$ однозначно представим в виде $f(x) = x^h g(x)$, где $h \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$ и $g(0) \neq 0$, и в этом случае порядок $\operatorname{ord}(f)$ многочлена f определяется как $\operatorname{ord}(g)$.

Порядок многочлена f иногда называют также *периодом* или *экспонентой* этого многочлена. Порядок неприводимого многочлена f допускает также следующую характеризацию.

3.3. Теорема. *Пусть* $f \in \mathbb{F}_q[x]$ *— неприводимый многочлен степени* m, *удовлетворяющий условию* $f(0) \neq 0$, *Порядок этого многочлена совпадает с порядком любого корня этого многочлена в мультипликативной группе* $\mathbb{F}_{q^m}^*$ *поля* $\mathbb{F}_{q^m}$.

Доказательство. На основании следствия 2.15 $\mathbb{F}_{q^m}$ является полем разложения многочлена f над полем $\mathbb{F}_q$. Все корни многочлена f имеют по теореме 2.18 один и тот же порядок в группе $\mathbb{F}_{q^m}^*$. Пусть $\alpha \in \mathbb{F}_{q^m}^*$ — какой-нибудь корень многочлена f. Тогда по лемме 2.12 равенство $\alpha^e = 1$ выполняется в том и только том случае, если многочлен $f(x)$ делит $x^e - 1$. Требуемый результат вытекает теперь из определений $\operatorname{ord}(f)$ и порядка элемента α в группе $\mathbb{F}_{q^m}^*$. □

3.4. Следствие. *Если* $f \in \mathbb{F}_q[x]$ *— неприводимый многочлен степени* m *над полем* $\mathbb{F}_q$, *то его порядок делит число* $q^m - 1$.

Доказательство. Если $f(x) = cx$, где $c \in \mathbb{F}_q^*$, то $\operatorname{ord}(f) = 1$ и результат тривиален. В противном же случае результат вытекает из теоремы 3.3 и того факта, что $\mathbb{F}_{q^m}^*$ — группа порядка $q^m - 1$.

Для приводимых многочленов утверждение следствия 3.4 не обязательно выполняется (см. пример 3.10). Существует еще одна интерпретация порядка многочлена f, при которой с многочленом f связывается некоторая квадратная матрица и $\operatorname{ord}(f)$ совпадает с порядком этой матрицы как элемента некоторой группы матриц (см. лемму 8.26).

С помощью теоремы 3.3 можно получить формулу для числа нормированных многочленов данной степени и данного порядка. Снова символом φ будем обозначать функцию Эйлера, введенную в теореме 1.15 (iv). Удобна следующая терминология: если n — натуральное и b — целое числа, причем НОД $(n, b) = 1$, то наименьшее натуральное число k, для которого $b^k \equiv 1 \pmod{n}$, называется *показателем, которому принадлежит число b по модулю n* (его называют также *мультипликативным порядком числа b по модулю n*).

3.5. Теорема. *Число нормированных неприводимых многочленов из $\mathbb{F}_q[x]$ степени m и порядка e равно $\varphi(e)/m$, если $e \geqslant 2$, а m — показатель, которому принадлежит число q по модулю e, равно 2, если $m = e = 1$, и равно 0 во всех остальных случаях. В частности, степень неприводимого многочлена из $\mathbb{F}_q[x]$ порядка e должна совпадать с показателем, которому принадлежит число q по модулю e.*

Доказательство. Пусть f — неприводимый многочлен из $\mathbb{F}_q[x]$, причем $f(0) \neq 0$. Тогда по теореме 3.3 $\operatorname{ord}(f) = e$ в том и только том случае, если все корни многочлена f являются первообразными корнями степени e из единицы над полем $\mathbb{F}_q$, т. е. если f делит круговой многочлен Q_e. По теореме 2.47 (ii) все нормированные неприводимые делители многочлена Q_e имеют одну и ту же степень, и этой степенью является наименьшее натуральное число m, для которого $q^m \equiv 1 \pmod{e}$. Число таких делителей равно $\varphi(e)/m$. Для $m = e = 1$ мы должны принять в расчет также нормированный неприводимый многочлен $f(x) = x$.

Значения порядков многочленов удобно представить в виде таблицы, по крайней мере для неприводимых многочленов (см. § 2 гл. 10). Так как каждый многочлен положительной степени можно записать в виде произведения неприводимых многочленов, то вычисление порядков многочленов значительно упрощается, если знать, как находить порядок степени неприводимого многочлена и произведения попарно взаимно простых многочленов. Последующий материал посвящен как раз этим вопросам.

3.6. Лемма. *Пусть c — натуральное число. Многочлен $f \in \mathbb{F}_q[x]$, удовлетворяющий условию $f(0) \neq 0$, делит двучлен $x^c - 1$ в том и только том случае, если $\operatorname{ord}(f)$ делит число c.*

Доказательство. Если число $e = \operatorname{ord}(f)$ делит c, то многочлен $f(x)$ делит $x^e - 1$, а $x^e - 1$ делит $x^c - 1$. Обратно, если многочлен $f(x)$ делит $x^c - 1$, то по определению порядка многочлена $c \geqslant e$, так что можно записать $c = me + r$, где $m \in \mathbb{N}$ и $0 \leqslant r < e$. Так как $x^c - 1 = (x^{me} - 1)\, x^r + (x^r - 1)$, то многочлен $f(x)$ делит $x^r - 1$ (поскольку делит остальные два члена предыдущего равенства), а это возможно лишь при $r = 0$. Значит, число e делит c.

3.7. Следствие. *Если e_1 и e_2 — натуральные числа, то наибольший общий делитель многочленов $x^{e_1} - 1$ и $x^{e_2} - 1$ в $\mathbb{F}_q[x]$ равен $x^d - 1$, где $d = \text{НОД}(e_1, e_2)$.*

Доказательство. Пусть $f(x)$ — нормированный наибольший общий делитель многочленов $x^{e_1} - 1$ и $x^{e_2} - 1$. Поскольку $x^d - 1$ — общий делитель этих многочленов, то $x^d - 1$ делит $f(x)$. С другой стороны, так как $f(x)$ делит и $x^{e_1} - 1$, и $x^{e_2} - 1$, то по лемме 3.6 порядок многочлена $f(x)$ делит как e_1, так и e_2. Следовательно, $\operatorname{ord}(f)$ делит d, а значит, согласно лемме 3.6, многочлен $f(x)$ делит $x^d - 1$. Объединяя полученные результаты, заключаем, что $f(x) = x^d - 1$. □

Так как при определении порядка многочлена не учитывается его сомножитель, равный степени переменной x, то нет необходимости рассматривать степени таких неприводимых многочленов $g(x)$, для которых $g(0) = 0$.

3.8. Теорема. *Пусть $n \in \mathbb{N}$ и $g(x)$ — неприводимый многочлен над конечным полем характеристики p, такой, что $g(0) \neq 0$. Тогда для многочлена вида $f = g^n$*

$$\operatorname{ord}(f) = \operatorname{ord}(g^n) = p^t \operatorname{ord}(g),$$

где t — наименьшее целое число, для которого $p^t \geqslant n$.

Доказательство. Положим $e = \operatorname{ord}(g)$ и $c = \operatorname{ord}(f)$. Учитывая, что делимость двучлена $x^c - 1$ на многочлен $f(x)$ влечет за собой делимость $x^c - 1$ на многочлен $g(x)$, получаем в силу леммы 3.6 что число e делит c. Далее, многочлен $g(x)$ делит $x^e - 1$; поэтому $f(x)$ делит $(x^e - 1)^n$, а значит, делит и $(x^e - 1)^{p^t} = x^{ep^t} - 1$. Таким образом, в силу леммы 3.6 число c делит ep^t. Учитывая доказанное ранее, получаем, что число c имеет вид $c = ep^s$, где $0 \leqslant s \leqslant t$. Заметим, что многочлен $x^e - 1$ имеет лишь простые корни, так как по следствию 3.4 число e не делится на p. Поэтому все корни многочлена $x^{ep^s} - 1 = (x^e - 1)^{p^s}$ имеют кратность p^s. Но так как многочлен $f(x) = (g(x))^n$ делит $x^{ep^s} - 1$, то, сравнивая кратности корней, получаем, что $p^s \geqslant n$, так что $s \geqslant t$. Таким образом, заключаем, что $s = t$ и $c = ep^t$. □

3.9. Теорема. *Пусть* $g_1, \ldots, g_k$ — *попарно взаимно простые ненулевые многочлены над полем* $\mathbb{F}_q$, *и пусть* $f = g_1 \ldots g_k$. *Тогда*

$$\operatorname{ord}(f) = \operatorname{ord}(g_1 \ldots g_k) = \text{НОК}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_k)).$$

Доказательство. Нетрудно видеть, что для доказательства теоремы достаточно рассмотреть лишь случай, когда $g_i(0) \neq 0$, $i = 1, \ldots, k$. Положим $e = \operatorname{ord}(f)$ и $e_i = \operatorname{ord}(g_i)$, $i = 1, \ldots, k$, и пусть $c = \text{НОК}(e_1, \ldots, e_k)$. Тогда каждый многочлен $g_i(x)$, $1 \leqslant i \leqslant k$, делит двучлен $x^{e_i} - 1$ и потому делит $x^c - 1$. В силу попарной взаимной простоты многочленов $g_1, \ldots, g_k$ получаем, что $f(x) = \prod_{i=1}^{k} g_i(x)$ делит $x^c - 1$. Учитывая лемму 3.6, мы видим, что число e делит c. С другой стороны, $f(x)$ делит $x^e - 1$ и, следовательно, каждый многочлен $g_i(x)$, $1 \leqslant i \leqslant k$, делит $x^e - 1$. Снова применяем лемму 3.6 и получаем, что каждое из чисел e_i, $1 \leqslant i \leqslant k$, делит e, а потому и c делит e. Это означает, что $c = e$.

В действительности, используя то же доказательство, можно показать, что порядок наименьшего общего кратного нескольких ненулевых многочленов равен наименьшему общему кратному порядков этих многочленов.

3.10. Пример. Найдем порядок многочлена $f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Каноническое разложение его над полем $\mathbb{F}_2$ имеет вид

$$f(x) = (x^2 + x + 1)^3 (x^4 + x + 1).$$

Так как $\operatorname{ord}(x^2 + x + 1) = 3$, то из теоремы 3.8 получаем, что $\operatorname{ord}((x^3 + x + 1)^3) = 12$. Далее, $\operatorname{ord}(x^4 + x + 1) = 15$, так что из теоремы 3.9 получаем, что $\operatorname{ord}(f) = \text{НОК}(12, 15) = 60$. Заметим, что $\operatorname{ord}(f)$ не делит число $2^{10} - 1 = 1023$; это показывает, что для приводимых многочленов следствие 3.4 не обязательно выполняется. □

На основании доказанного можно дать следующую общую формулу для порядка многочлена. При этом предполагается, что все рассматриваемые многочлены имеют положительную степень и ненулевой постоянный член.

3.11. Теорема. *Пусть* $\mathbb{F}_q$ — *конечное поле характеристики* p. *Если* $f = a f_1^{n_1} \ldots f_k^{n_k}$ — *каноническое разложение в кольце* $\mathbb{F}_q[x]$ *многочлена* $f(x) \in \mathbb{F}_q[x]$ *положительной степени, такого, что* $f(0) \neq 0$ (*т. е.* $a \in \mathbb{F}_q$, $n_1, \ldots, n_k \in \mathbb{N}$ *и* $f_1, \ldots, f_k$ — *различные нормированные неприводимые многочлены из* $\mathbb{F}_q[x]$, *отличные от* x), *то*

$$\operatorname{ord}(f) = \operatorname{ord}(a f_1^{n_1} \ldots f_k^{n_k}) = p^t \text{НОК}(\operatorname{ord}(f_1), \ldots, \operatorname{ord}(f_k)),$$

где t — наименьшее целое число, удовлетворяющее неравенству $p^t \geqslant \max\{n_1, \ldots, n_h\}$.

Один из *методов определения порядка* неприводимого многочлена f из $\mathbb{F}_q[x]$, удовлетворяющего условию $f(0) \neq 0$, основан на том факте, что порядок e многочлена f является наименьшим натуральным числом, удовлетворяющим сравнению

$$x^e \equiv 1 \pmod{f(x)}.$$

Кроме того, согласно следствию 3.4, число e делит $q^m - 1$, где m — степень многочлена f. Предполагая, что $q^m > 2$, будем исходить из разложения числа $q^m - 1$ на простые сомножители:

$$q^m - 1 = \prod_{j=1}^{s} p_j^{r_j}.$$

Для каждого j, $1 \leqslant j \leqslant s$, найдем вычеты одночленов $x^{(q^m-1)/p_j}$ по модулю $f(x)$ (т. е. остатки при их делении на $f(x)$). Обычно это делается перемножением подходящим образом выбранного набора вычетов по модулю $f(x)$ степеней x, x^q, x^{q^2}, ..., $x^{q^{m-1}}$ переменной x. При этом, если окажется, что $x^{(q^m-1)/p_j} \not\equiv 1 \pmod{f(x)}$, то число e делится на $p_j^{r_j}$, а если $x^{(q^m-1)/p_j} \equiv 1 \pmod{f(x)}$, то число e не делится на $p_j^{r_j}$. В последнем случае мы выясняем, будет ли число e делиться на $p_j^{r_j-1}$, $p_j^{r_j-2}$, ..., p_j, вычисляя соответственно вычеты по модулю $f(x)$ следующих степеней переменной x:

$$x^{(q^m-1)/p_j^2}, \; x^{(q^m-1)/p_j^3}, \; \ldots, \; x^{(q^m-1)/p_j^{r_j}}.$$

Такой подсчет проводится для каждого простого делителя p_j числа $q^m - 1$, и в итоге находится число $e = \operatorname{ord}(f)$.

Ключевым моментом указанного метода является разложение на простые сомножители натурального числа $q^m - 1$. Составлены обширные таблицы для полного разложения чисел такого вида, особенно для случая $q = 2$.

Существует связь между порядками некоторых многочленов, которые можно получать друг из друга простыми алгебраическими преобразованиями. Типичным примером может служить следующее преобразование.

3.12. Определение. Пусть дан многочлен

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$$

с $a_n \neq 0$. Тогда *возвратный* (или *двойственный*) к нему многочлен f^* определяется так:

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n.$$

3.13. Теорема. *Пусть f — ненулевой многочлен из $\mathbb{F}_q[x]$ и f^* — возвратный к нему многочлен. Тогда* $\operatorname{ord}(f^*) = \operatorname{ord}(f)$.

Доказательство. Сначала рассмотрим случай $f(0) \neq 0$. Тогда утверждение вытекает из того факта, что многочлен $f(x)$ делит $x^e - 1$ в том и только том случае, если многочлен $f^*(x)$ делит $x^e - 1$. Если же $f(0) = 0$, то запишем $f(x) = x^h g(x)$, где $h \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$ и $g(0) \neq 0$. Тогда из ранее доказанного и из определения порядка следует, что $\operatorname{ord}(f) = \operatorname{ord}(g) = \operatorname{ord}(g^*) = \operatorname{ord}(f^*)$, где последнее равенство вытекает из равенства $g^* = f^*$. □

Имеется также тесная взаимосвязь между порядками многочленов $f(x)$ и $f(-x)$. Поскольку для поля характеристики 2 имеем $f(-x) = f(x)$, то достаточно рассмотреть лишь поля нечетной характеристики.

3.14. Теорема. *Для нечетного q пусть $f \in \mathbb{F}_q[x]$ — многочлен положительной степени, такой, что $f(0) \neq 0$, и пусть e и E — соответственно порядки многочленов $f(x)$ и $f(-x)$. Тогда $E = e$, если e делится на 4, и $E = 2e$, если e нечетно. Если же $e = 2h$, где h нечетно, то $E = e/2$ в случае, когда все неприводимые делители многочлена f имеют четный порядок, и $E = e$ в противном случае.*

Доказательство. Так как $\operatorname{ord}(f) = e$, то многочлен $f(x)$ делит $x^{2e} - 1$, а значит, многочлен $f(-x)$ делит $(-x)^{2e} - 1 = x^{2e} - 1$. Поэтому число E делит $2e$ (согласно лемме 3.6). Аналогично показывается, что число e делит $2E$. Отсюда заключаем, что E может быть лишь одним из трех чисел: $2e$, e или $e/2$. Если число e делится на 4, то оба числа e и E четны. Поскольку $f(x)$ делит $x^e - 1$, $f(-x)$ делит $(-x)^e - 1 = x^e - 1$, так что E делит e. Аналогично показывается, что e делит E, значит, $E = e$. Если число e нечетно, то многочлен $f(-x)$ делит $(-x)^e - 1 = -x^e - 1$, а значит, делит $x^e + 1$. Но тогда $f(-x)$ не может делить $x^e - 1$ и потому выполняется равенство $E = 2e$.

Остается разобрать случай $e = 2h$, где h нечетно. Пусть многочлен f является степенью неприводимого многочлена из $\mathbb{F}_q[x]$. Тогда $f(x)$ делит произведение $(x^h - 1)(x^h + 1)$, но не делит $x^h - 1$, так как $\operatorname{ord}(f) = 2h$. Поскольку многочлены $x^h - 1$ и $x^h + 1$ взаимно просты, то $f(x)$ делит $x^h + 1$. Значит, $f(-x)$ делит многочлен $(-x)^h + 1 = -x^h + 1$, а следовательно, и $x^h - 1$. Это означает, что $E = e/2$. Заметим, что по теореме 3.8 многочлен, являющийся степенью неприводимого многочлена, имеет четный порядок в том и только том случае, если сам неприводимый многочлен имеет четный порядок (напоминаем, что характеристика поля $\mathbb{F}_q$ предполагается нечетной).

В общем случае пусть многочлен f имеет разложение $f = f_1 \dots f_k$, где $f_i = g_i^{b_i}$, $b_i \in \mathbb{N}$, $1 \leqslant i \leqslant k$, и $g_1, \dots, g_k$ — различные неприводимые многочлены из $\mathbb{F}_q[x]$. Поскольку многочлены $f_1, \dots, f_k$ попарно взаимно просты, то по теореме 3.9 имеем $2h = \text{НОК}(\text{ord}(f_1), \dots, \text{ord}(f_k))$. Это значит, что многочлены f_i можно так перенумеровать, чтобы $\text{ord}(f_i(x)) = 2h_i$ для $1 \leqslant i \leqslant j$ и $\text{ord}(f_i(x)) = h_i$ для $j+1 \leqslant i \leqslant k$, где все числа h_i нечетны и $\text{НОК}(h_1, \dots, h_k) = h$. На основании ранее доказанного имеем $\text{ord}(f_i(-x)) = h_i$ для $1 \leqslant i \leqslant j$ и $\text{ord}(f_i(-x)) = 2h_i$ для $j+1 \leqslant i \leqslant k$. Поэтому в силу теоремы 3.9 получаем

$$E = \text{НОК}(h_1, \dots, h_j, 2h_{j+1}, \dots, 2h_k),$$

так что $E = h = e/2$, если $j = k$, и $E = 2h = e$, если $j < k$. Это доказывает последнюю часть теоремы. □

Из леммы 3.1 и определения 3.2 вытекает, что порядок многочлена степени $m \geqslant 1$ над $\mathbb{F}_q$ не превосходит числа $q^m - 1$. Указанная граница достигается для важного класса многочленов, а именно для примитивных многочленов. Определение примитивного многочлена опирается на введенное в определении 2.9 понятие примитивного элемента.

3.15. Определение. Многочлен $f \in \mathbb{F}_q[x]$ степени $m \geqslant 1$ называется *примитивным многочленом* над полем $\mathbb{F}_q$, если он является минимальным многочленом над $\mathbb{F}_q$ некоторого примитивного элемента расширения $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$.

Таким образом, примитивный многочлен над $\mathbb{F}_q$ степени m — это нормированный многочлен, который неприводим над $\mathbb{F}_q$ и имеет корень $\alpha \in \mathbb{F}_{q^m}$, который является образующим мультипликативной группы $\mathbb{F}_{q^m}^*$ поля $\mathbb{F}_{q^m}$. Примитивные многочлены над $\mathbb{F}_q$ можно охарактеризовать еще так:

3.16. Теорема. *Многочлен $f \in \mathbb{F}_q[x]$ степени m является примитивным многочленом над $\mathbb{F}_q$ в том и только том случае, если он — нормированный многочлен, такой, что $f(0) \neq 0$ и $\text{ord}(f) = q^m - 1$.*

Доказательство. Если f — примитивный многочлен над $\mathbb{F}_q$, то он — нормированный многочлен, удовлетворяющий условию $f(0) \neq 0$. Поскольку f неприводим над $\mathbb{F}_q$, то из теоремы 3.3 и того факта, что его корнем является примитивный элемент расширения $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$, следует, что $\text{ord}(f) = q^m - 1$.

Обратно, из условия $\text{ord}(f) = q^m - 1$ следует, что $m \geqslant 1$. Далее, мы утверждаем, что многочлен f неприводим над $\mathbb{F}_q$. Допустим, что он приводим над $\mathbb{F}_q$. Тогда либо f является степенью некоторого неприводимого многочлена, либо он может быть представлен в виде произведения двух взаимно простых много-

членов положительной степени. В первом случае пусть $f = g^b$, где многочлен $g \in \mathbb{F}_q[x]$ неприводим над $\mathbb{F}_q$, $g(0) \neq 0$ и $b \geqslant 2$. Тогда в силу теоремы 3.8 порядок многочлена f должен делиться на характеристику поля $\mathbb{F}_q$, но $q^m - 1$ не делится на нее, и мы получаем противоречие. Во втором случае пусть $f = g_1 g_2$, где g_1 и g_2 — взаимно простые многочлены из $\mathbb{F}_q[x]$ положительных степеней m_1 и m_2 соответственно. Если $e_i = \operatorname{ord}(g_i)$, $i = 1, 2$, то по теореме 3.9 имеем $\operatorname{ord}(f) \leqslant e_1 e_2$. Кроме того, в силу леммы 3.1 $e_i \leqslant q^{m_i} - 1$, $i = 1, 2$, так что

$$\operatorname{ord}(f) \leqslant (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1+m_2} - 1 = q^m - 1,$$

и вновь приходим к противоречию. Следовательно, многочлен f неприводим над $\mathbb{F}_q$, и тогда из теоремы 3.3 и нормированности f мы заключаем, что f — примитивный многочлен над $\mathbb{F}_q$. □

Заметим, что требование $f(0) \neq 0$ понадобилось лишь, чтобы исключить случай неприводимого многочлена $f(x) = x$ при $q = 2$ и $m = 1$. Другая характеризация примитивных многочленов опирается на следующий вспомогательный результат.

3.17. Лемма. *Пусть $f \in \mathbb{F}_q[x]$ — многочлен положительной степени, удовлетворяющий условию $f(0) \neq 0$. Пусть r — наименьшее натуральное число, для которого степень x^r переменной x сравнима по модулю $f(x)$ с некоторым элементом из поля $\mathbb{F}_q$, т. е. $x^r \equiv a \pmod{f(x)}$, где элемент $a \in \mathbb{F}_q^*$ однозначно определен. Тогда $\operatorname{ord}(f) = hr$, где h — порядок элемента a в мультипликативной группе $\mathbb{F}_q^*$ поля $\mathbb{F}_q$.*

Доказательство. Положим $e = \operatorname{ord}(f)$. Так как $x^e \equiv 1 \pmod{f(x)}$, то мы получаем, что $e \geqslant r$. Поэтому можно написать $e = sr + t$, где $s \in \mathbb{N}$ и $0 \leqslant t < r$. Тогда

$$1 \equiv x^e \equiv x^{sr+t} \equiv a^s x^t \pmod{f(x)}, \qquad (3.1)$$

так что $x^t \equiv a^{-s} \pmod{f(x)}$, и потому в соответствии с определением числа r получаем, что $t = 0$. Из сравнения (3.1) тогда видно, что $a^s \equiv 1 \pmod{f(x)}$, т. е. $a^s = 1$, и потому $s \geqslant h$ и $e \geqslant hr$. С другой стороны, $x^{hr} \equiv a^h \equiv 1 \pmod{f(x)}$, так что $hr \geqslant e$. Значит, $e = hr$. □

3.18. Теорема. *Нормированный многочлен $f \in \mathbb{F}_q[x]$ степени $m \geqslant 1$ является примитивным многочленом над полем $\mathbb{F}_q$ в том и только том случае, если $(-1)^m f(0)$ — примитивный элемент поля $\mathbb{F}_q$ и наименьшим натуральным числом r, для которого степень x^r переменной x сравнима по модулю $f(x)$ с некоторым элементом поля $\mathbb{F}_q$, является*

$$r = \frac{q^m - 1}{q - 1}.$$

Если f — примитивный многочлен над $\mathbb{F}_q$, то имеет место сравнение

$$x^r \equiv (-1)^m f(0) \pmod{f(x)}.$$

Доказательство. Если многочлен f примитивен над $\mathbb{F}_q$, то f имеет корень $\alpha \in \mathbb{F}_{q^m}$, который является примитивным элементом поля $\mathbb{F}_{q^m}$. Вычислив норму $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ с помощью определения 2.27 и равенства (2.3) и замечая, что f — характеристический многочлен элемента α над полем $\mathbb{F}_q$, мы приходим к равенству

$$(-1)^m f(0) = \alpha^{(q^m-1)/(q-1)}. \tag{3.2}$$

Из него вытекает, что порядок элемента $(-1)^m f(0)$ в группе $\mathbb{F}_q^*$ равен $q-1$, т. е. $(-1)^m f(0)$ — примитивный элемент поля $\mathbb{F}_q$. Так как f — минимальный многочлен элемента α над полем $\mathbb{F}_q$, то из теоремы 1.82 (ii) и равенства (3.2) следует, что

$$x^{(q^m-1)/(q-1)} \equiv (-1)^m f(0) \pmod{f(x)},$$

так что $r \leqslant (q^m-1)/(q-1)$. Но из теоремы 3.16 и леммы 3.17 следует, что $q^m - 1 = \operatorname{ord}(f) \leqslant (q-1)r$, так что $r \geqslant (q^m - 1)/(q-1)$. Значит, $r = (q^m-1)/(q-1)$.

Обратно, допустим, что условия теоремы выполнены. Из равенства $r = (q^m-1)/(q-1)$ и леммы 3.17 тогда следует, что числа $\operatorname{ord}(f)$ и q взаимно просты. Из теоремы 3.11 в таком случае получаем, что многочлен f разлагается в произведение $f = f_1 \dots f_k$ различных нормированных неприводимых над $\mathbb{F}_q$ многочленов $f_1, \dots, f_k$. Если $m_i = \deg(f_i)$, то $\operatorname{ord}(f_i)$ делит $q^{m_i} - 1$, $1 \leqslant i \leqslant k$ (на основании следствия 3.4). Поскольку $q^{m_i} - 1$ делит число

$$d = (q^{m_1} - 1) \dots (q^{m_k} - 1)/(q-1)^{k-1},$$

то число $\operatorname{ord}(f_i)$ делит d, $1 \leqslant i \leqslant k$. Из леммы 3.6 следует, что $f_i(x)$ делит $x^d - 1$ для $1 \leqslant i \leqslant k$, так что многочлен $f(x)$ делит $x^d - 1$. Если $k \geqslant 2$, то

$$d < (q^{m_1+\dots+m_k} - 1)/(q-1) = (q^m-1)/(q-1) = r,$$

что противоречит определению числа r. Таким образом, $k = 1$ и многочлен f неприводим над $\mathbb{F}_q$. Если $\beta \in \mathbb{F}_{q^m}$ — корень многочлена f, то рассуждение, аналогичное приводящему к (3.2), приведет к тому, что $\beta^r = (-1)^m f(0)$, так что $x^r \equiv (-1)^m f(0) \pmod{f(x)}$. А поскольку порядок элемента $(-1)^m f(0)$ в группе $\mathbb{F}_q^*$ равен $q-1$, то из леммы 3.17 вытекает, что $\operatorname{ord}(f) = q^m - 1$, так что в соответствии с теоремой 3.16 f является примитивным многочленом над $\mathbb{F}_q$. □

3.19. Пример. Рассмотрим многочлен $f(x) = x^4 + x^3 + x^2 + 2x + 2 \in \mathbb{F}_3[x]$. Так как f неприводим над полем $\mathbb{F}_3$, то,

применяя метод, изложенный после теоремы 3.11, получим, что $\operatorname{ord}(f) = 3^4 - 1 = 80$. Следовательно, f — примитивный многочлен над $\mathbb{F}_3$ (по теореме 3.16). В соответствии с теоремой 3.18 $x^{40} \equiv 2 \pmod{f(x)}$. □

§ 2. Неприводимые многочлены

Напомним, что многочлен $f \in \mathbb{F}_q[x]$ *неприводим* над полем $\mathbb{F}_q$, если он имеет положительную степень и любое его разложение на множители в кольце $\mathbb{F}_q[x]$ обязательно содержит постоянный многочлен (см. определение 1.57). Простейшие свойства неприводимых многочленов были рассмотрены в § 2 гл. 2.

3.20. Теорема. *Для каждого конечного поля $\mathbb{F}_q$ и каждого $n \in \mathbb{N}$ произведение всех нормированных неприводимых многочленов над $\mathbb{F}_q$, степень которых делит n, равно $x^{q^n} - x$.*

Доказательство. По лемме 2.13 каноническое разложение многочлена $g(x) = x^{q^n} - x$ в кольце $\mathbb{F}_q[x]$ содержнт те и только те нормированные неприводимые многочлены над $\mathbb{F}_q$, степень которых делит число n. Так как $g'(x) = -1$, то из теоремы 1.68 вытекает, что многочлен g в его поле разложения над $\mathbb{F}_q$ не имеет кратных корней, так что каждый нормированный неприводимый многочлен над $\mathbb{F}_q$, степень которого делит n, встретится в каноническом разложении многочлена g в кольце $\mathbb{F}_q[x]$ ровно один раз. □

3.21. Следствие. *Если $N_q(d)$ — число нормированных неприводимых многочленов из $\mathbb{F}_q[x]$ степени d, то*

$$q^n = \sum_{d \mid n} dN_q(d) \text{ для всех } n \in \mathbb{N}, \tag{3.3}$$

где сумма берется по всем положительным делителям d числа n.

Доказательство. Тождество (3.3) получается из теоремы 3.20 сопоставлением степени многочлена $g(x) = x^{q^n} - x$ с полной степенью канонического разложения многочлена $g(x)$ на неприводимые сомножители. □

Используя элементарные сведения из теории чисел, мы можем получить из формулы (3.3) точную формулу для числа нормированных неприводимых многочленов фиксированной степени из кольца $\mathbb{F}_q[x]$. Для этого потребуется одна арифметическая функция, называемая функцией Мёбиуса, которая определяется так:

3.22. Определение. *Функцией Мёбиуса* называется функция μ на множестве $\mathbb{N}$, определяемая равенствами

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } n \text{ — произведение } k \text{ различных простых чисел,} \\ 0, & \text{если } n \text{ делится на квадрат некоторого простого числа.} \end{cases}$$

Когда в формуле (3.3) мы использовали символ суммирования $\sum_{d|n}$, это означало, что сумма распространяется на все положительные делители d числа $n \in \mathbb{N}$. Удобно использовать аналогичный символ и для произведения: $\prod_{d|n}$.

3.23. Лемма. *Для $n \in \mathbb{N}$ функция Мёбиуса удовлетворяет соотношению*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases}$$

Доказательство. Для $n > 1$ мы должны принимать во внимание лишь те положительные делители d числа n, для которых $\mu(d) \neq 0$, т. е. для которых или $d = 1$, или d является произведением различных простых чисел. Таким образом, если $p_1, \ldots, p_k$ — различные простые делители числа n, то

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leqslant i_1 < i_2 \leqslant k} \mu(p_{i_1} p_{i_2}) + \cdots$$
$$\cdots + \mu(p_1 \ldots p_k) =$$
$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k =$$
$$= [1 + (-1)]^k = 0.$$

Случай же $n = 1$ тривиален. □

3.24. Теорема (формула обращения Мёбиуса).

(i) Аддитивный вариант. *Пусть h и H — две функции из множества $\mathbb{N}$ натуральных чисел в некоторую абелеву группу G с аддитивной записью. Тогда равенство*

$$H(n) = \sum_{d|n} h(d) \quad \text{для всех } n \in \mathbb{N} \tag{3.4}$$

выполняется в том и только том случае, если выполняется равенство

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(n) H\left(\frac{n}{d}\right) \quad \text{для всех } n \in \mathbb{N}. \tag{3.5}$$

(ii) Мультипликативный вариант. *Пусть h и H — две функции из множества $\mathbb{N}$ натуральных чисел в некоторую абелеву группу G с мультипликативной записью. Тогда равенство*

$$H(n) = \prod_{d \mid n} h(d) \quad \text{для всех } n \in \mathbb{N} \tag{3.6}$$

выполняется в том и только том случае, если выполняется равенство

$$h(n) = \prod_{d \mid n} H(d)^{\mu(n/d)} = \prod_{d \mid n} H\left(\frac{n}{d}\right)^{\mu(d)} \quad \text{для всех } n \in \mathbb{N}. \tag{3.7}$$

Доказательство. Предполагая выполненным равенство (3.4) и используя лемму 3.23, получим

$$\sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu(d) \sum_{c \mid \frac{n}{d}} h(c) =$$

$$= \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} \mu(d) h(c) = \sum_{c \mid n} h(c) \sum_{d \mid \frac{n}{c}} \mu(d) = h(n)$$

для всех $n \in \mathbb{N}$. Обратное утверждение доказывается аналогично. Доказательство части (ii) сразу же получается из доказательства части (i) заменой сумм произведениями, а кратных — степенями. □

3.25. Теорема. *Число $N_q(n)$ нормированных неприводимых многочленов степени n в кольце $\mathbb{F}_q[x]$ задается формулой*

$$N_q(n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}.$$

Доказательство. Применим аддитивный вариант формулы обращения Мёбиуса к группе $G = \mathbb{Z}$ — аддитивной группе целых чисел. Пусть $h(n) = nN_q(n)$ и $H(n) = q^n$ для всех $n \in \mathbb{N}$. Тогда формула (3.4) справедлива ввиду равенства (3.3), и из (3.5) получаем требуемую формулу. □

3.26. Пример. Число нормированных неприводимых многочленов степени 20 в кольце $\mathbb{F}_q[x]$ равно

$$N_q(20) = \frac{1}{20}\left[\mu(1) q^{20} + \mu(2) q^{10} + \mu(4) q^5 + \mu(5) q^4 + \right.$$

$$\left. + \mu(10) q^2 + \mu(20) q\right] =$$

$$= \frac{1}{20}(q^{20} - q^{10} - q^4 + q^2). \qquad \square$$

Следует отметить, что из формулы теоремы 3.25 можно получить еще одно доказательство существования хотя бы одного неприводимого многочлена степени n в кольце $\mathbb{F}_q[x]$ для любого $n \in \mathbb{N}$ и любого конечного поля $\mathbb{F}_q$ (ср. со следствием 2.11). А именно, учитывая, что $\mu(1) = 1$ и $\mu(d) \geqslant -1$ для всех $d \in \mathbb{N}$, получаем

$$N_q(n) \geqslant \frac{1}{n}(q^n - q^{n-1} - q^{n-2} - \ldots - q) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q-1}\right) > 0.$$

В качестве другого применения формулы обращения Мёбиуса получим явную формулу для n-кругового многочлена $Q_n(x)$.

3.27. Теорема. *Для поля K характеристики p и натурального числа n, не делящегося на p, n-круговой многочлен $Q_n(x)$ над K задается формулой*

$$Q_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)} = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)}.$$

Доказательство. Применим мультипликативный вариант формулы обращения Мёбиуса к мультипликативной группе G ненулевых рациональных функций над полем K. Пусть $h(n) = Q_n(x)$ и $H(n) = x^n - 1$ для всех $n \in \mathbb{N}$. Тогда из теоремы 2.45 (i) вытекает справедливость формулы (3.6), а из (3.7) получаем требуемый результат. □

3.28. Пример. Для полей K, для которых определен круговой многочлен Q_{12}, получаем

$$\begin{aligned} Q_{12}(x) &= \prod_{d \mid 12} (x^{12/d} - 1)^{\mu(d)} = \\ &= (x^{12} - 1)^{\mu(1)} (x^6 - 1)^{\mu(2)} (x^4 - 1)^{\mu(3)} (x^3 - 1)^{\mu(4)} \cdot \\ &\qquad \cdot (x^2 - 1)^{\mu(6)} (x - 1)^{\mu(12)} = \\ &= \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 + 1. \end{aligned}$$

□

Явную формулу из теоремы 3.27 можно использовать для вывода основных свойств круговых многочленов (ср. с упр. 3.35).

В теореме 3.25 мы определили *число* нормированных неприводимых многочленов данной степени n в кольце $\mathbb{F}_q[x]$. Теперь получим формулу для *произведения* всех нормированных неприводимых многочленов данной степени n из кольца $\mathbb{F}_q[x]$.

3.29. Теорема. *Произведение $I(q, n; x)$ всех нормированных неприводимых многочленов степени n из кольца $\mathbb{F}_q[x]$ задается формулой*

$$I(q, n; x) = \prod_{d \mid n} (x^{q^d} - x)^{\mu(n/d)} = \prod_{d \mid n} (x^{q^{n/d}} - x)^{\mu(d)}.$$

Доказательство. Из теоремы 3.20 следует, что

$$x^{q^n} - x = \prod_{d \mid n} I(q, d; x).$$

Применяя теперь мультипликативный вариант формулы обращения Мёбиуса к мультипликативной группе G ненулевых рациональных функций над полем $\mathbb{F}_q$ и полагая $h(n) = I(q, n; x)$ и $H(n) = x^{q^n} - x$ для всех $n \in \mathbb{N}$, мы получим требуемую формулу. □

3.30. Пример. Для $q = 2$, $n = 4$ получаем

$$\begin{aligned} I(2, 4; x) &= (x^{16} - x)^{\mu(1)} (x^4 - x)^{\mu(2)} (x^2 - x)^{\mu(4)} = \\ &= \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} = \\ &= x^{12} + x^9 + x^6 + x^3 + 1. \end{aligned}$$ □

Все нормированные неприводимые многочлены степени n из $\mathbb{F}_q[x]$ можно найти, разлагая на множители многочлен $I(q, n; x)$. В этой связи было бы полезно представить $I(q, n; x)$ в частично разложенном виде. Это достигается с помощью следующей теоремы.

3.31. Теорема. *Пусть $I(q, n; x)$ то же, что и в теореме* 3.29. *Тогда для натурального числа $n > 1$ имеет место формула*

$$I(q, n; x) = \prod_m Q_m(x), \tag{3.8}$$

где $Q_m(x)$ есть m-круговой многочлен над $\mathbb{F}_q$ и произведение берется по всем натуральным делителям m числа $q^n - 1$, для которых n является показателем, которому принадлежит число q по модулю m.

Доказательство. Для $n > 1$ пусть S — множество элементов поля $\mathbb{F}_{q^n}$, которые имеют степень n над полем $\mathbb{F}_q$. Тогда каждый элемент $\alpha \in S$ имеет минимальный многочлен степени n над $\mathbb{F}_q$ и, таким образом, является корнем многочлена $I(q, n; x)$. С другой стороны, если β — корень многочлена $I(q, n; x)$, то он в то же время является корнем некоторого нормированного неприводимого многочлена степени n из $\mathbb{F}_q[x]$, а это значит, что $\beta \in S$. Поэтому

$$I(q, n; x) = \prod_{\alpha \in S} (x - \alpha).$$

Если $\alpha \in S$, то $\alpha \in \mathbb{F}_{q^n}^*$, и, значит, порядок элемента α в этой мультипликативной группе делит число $q^n - 1$. Заметим, что элемент $\gamma \in \mathbb{F}_{q^n}^*$ является элементом какого-нибудь собственного подполя $\mathbb{F}_{q^d}$ поля $\mathbb{F}_{q^n}$ в том и только том случае, если $\gamma^{q^d} = \gamma$,

т. е. если порядок элемента γ делит число $q^d - 1$. Поэтому порядок m элемента α из S должен быть таким, чтобы n было наименьшим натуральным числом, таким, что $q^n \equiv 1 \pmod{m}$, т. е. чтобы n было показателем, которому принадлежит q по модулю m. Для положительного делителя m числа $q^n - 1$ с таким свойством пусть S_m будет множеством элементов порядка m из S. Тогда S является объединением непересекающихся подмножеств S_m, так что можно написать

$$I(q, n; x) = \prod_{m} \prod_{\alpha \in S_m} (x - \alpha).$$

Множество S_m состоит из всех элементов группы $\mathbb{F}_{q^n}^*$, имеющих порядок m. Другими словами, S_m — множество первообразных корней m-й степени из единицы над $\mathbb{F}_q$. Тогда из определения круговых многочленов (см. определение 2.44) следует, что

$$\prod_{\alpha \in S_m} (x - \alpha) = Q_m(x),$$

и тем самым формула (3.8) установлена. □

3.32. Пример. Найдем все (нормированные) неприводимые многочлены степени 4 из кольца $\mathbb{F}_2[x]$. Из равенства (3.8) следует, что $I(2, 4; x) = Q_5(x) Q_{15}(x)$. На основании теоремы 2.47 (ii) круговой многочлен $Q_5(x) = x^4 + x^3 + x^2 + x + 1$ неприводим в $\mathbb{F}_2[x]$. По той же теореме круговой многочлен $Q_{15}(x)$ разлагается в произведение двух неприводимых многочленов из $\mathbb{F}_2[x]$ степени 4. Поскольку $Q_5(x + 1) = x^4 + x^3 + 1$ — неприводимый многочлен из $\mathbb{F}_2[x]$, этот многочлен должен делить $Q_{15}(x)$, так что

$$Q_{15}(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 = (x^4 + x^3 + 1)(x^4 + x + 1).$$

Поэтому неприводимыми многочленами степени 4 из $\mathbb{F}_2[x]$ являются $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$ и $x^4 + x + 1$ и только они. □

Неприводимые многочлены часто возникают как минимальные многочлены элементов какого-нибудь расширения поля. Минимальные многочлены были введены определением 1.81, а их основные свойства были установлены теоремой 1.82. Теперь применительно к конечным полям мы отметим наиболее полезные факты о минимальных многочленах.

3.33. Теорема. *Пусть α — некоторый элемент из расширения $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$, и пусть d — степень элемента α над $\mathbb{F}_q$, а $g \in \mathbb{F}_q[x]$ — минимальный многочлен элемента α над $\mathbb{F}_q$. Тогда*

(i) *Многочлен g неприводим над $\mathbb{F}_q$, и его степень d делит число m.*

(ii) *Многочлен* $f \in \mathbb{F}_q[x]$ *удовлетворяет условию* $f(\alpha) = 0$ *тогда и только тогда, когда многочлен* g *делит* f.

(iii) *Если* f *— нормированный неприводимый многочлен из* $\mathbb{F}_q[x]$, *такой, что* $f(\alpha) = 0$, *то* $f = g$.

(iv) $g(x)$ *делит многочлены* $x^{q^d} - x$ *и* $x^{q^m} - x$.

(v) *Корнями многочлена* $g(x)$ *являются элементы* α, α^q, ..., $\alpha^{q^{d-1}}$, *причем* $g(x)$ *— минимальный многочлен над* $\mathbb{F}_q$ *каждого из этих элементов.*

(vi) *Если* $\alpha \neq 0$, *то порядок многочлена* g *равен порядку элемента* α *в мультипликативной группе* $\mathbb{F}_{q^m}^*$ *поля* $\mathbb{F}_{q^m}$.

(vii) g *является примитивным многочленом над полем* $\mathbb{F}_q$ *тогда и только тогда, когда порядок элемента* α *в группе* $\mathbb{F}_{q^m}^*$ *равен* $q^d - 1$.

Доказательство. (i) Первая часть вытекает из теоремы 1.82 (i), а вторая — из теоремы 1.86.

(ii) Это утверждение следует из теоремы 1.82 (ii).

(iii) Это утверждение сразу вытекает из (ii).

(iv) Это утверждение следует из (i) и леммы 2.13.

(v) Первая часть утверждения вытекает из (i) и теоремы 2.14, а вторая — из (iii).

(vi) Так как $\alpha \in \mathbb{F}_{q^d}^*$, а $\mathbb{F}_{q^d}^*$ — подгруппа группы $\mathbb{F}_{q^m}^*$, то утверждение вытекает из теоремы 3.3.

(vii) Если g — примитивный элемент над $\mathbb{F}_q$, то $\operatorname{ord}(g) = q^d - 1$, так что порядок элемента α в группе $\mathbb{F}_{q^m}^*$ равен $q^d - 1$ в силу (vi). Обратно, если α — элемент порядка $q^d - 1$ в группе $\mathbb{F}_{q^m}^*$, а значит, и в $\mathbb{F}_{q^d}^*$, то α — примитивный элемент поля $\mathbb{F}_{q^d}$, а следовательно, g — примитивный многочлен над $\mathbb{F}_q$ согласно определению 3.15. □

§ 3. Построение неприводимых многочленов

Сначала мы опишем общий принцип получения новых неприводимых многочленов на основе известных. Этот метод опирается на один вспомогательный теоретико-числовой результат. Напомним, что если n — натуральное число и b — целое взаимно простое с n число, то наименьшее натуральное число k, такое, что

$$b^k \equiv 1 \pmod{n},$$

называется *показателем, которому принадлежит число* b *по модулю* n. Заметим, что этот показатель делит любое другое натуральное число h, такое, что $b^h \equiv 1 \pmod{n}$.

3.34. Лемма. *Пусть* $s \geqslant 2$ *и* $e \geqslant 2$ *— взаимно простые целые числа, и пусть* m *— показатель, которому принадлежит число* s

по модулю e. Пусть, далее, $t \geqslant 2$ — целое число, простые делители которого делят e, но не делят $(s^m - 1)/e$. Пусть, наконец, $s^m \equiv 1 \pmod 4$, когда t кратно четырем. Тогда показатель, которому принадлежит число s по модулю et, равен mt.

Доказательство. Применим индукцию по числу простых делителей числа t, считая каждый делитель с его кратностью. Сначала пусть t будет простым числом. Полагая $d = (s^m - 1)/e$, получим $s^m = 1 + de$, так что

$$s^{mt} = (1 + de)^t = \\ = 1 + \binom{t}{1} de + \binom{t}{2} d^2e^2 + \cdots + \binom{t}{t-1} d^{t-1}e^{t-1} + d^te^t.$$

В последнем выражении каждый член, кроме первого и последнего, делится на et в силу свойства биномиальных коэффициентов, указанного в доказательстве теоремы 1.46. Но и последний член тоже делится на et, так как t делит e. Поэтому $s^{mt} \equiv 1 \pmod{et}$, и, значит, показатель k, которому принадлежит число s по модулю et, делит mt. По определению показателя k $s^k \equiv 1 \pmod{et}$, так что $s^k \equiv 1 \pmod e$, а отсюда по определению числа m получаем, что k делится на m. Поскольку t — простое число, делящее e, то число k может быть равно лишь m или mt. Если $k = m$, то $s^m \equiv 1 \pmod{et}$, откуда $s^m - 1 = de \equiv 0 \pmod{et}$, и, следовательно, t должно делить d, что невозможно. Значит, остается единственная возможность $k = mt$.

Теперь предположим, что число t имеет по крайней мере два простых делителя, и запишем $t = rt_0$, где r — простой делитель числа t. По доказанному выше показатель, которому принадлежит число s по модулю er, равен mr. Если мы докажем, что каждый простой делитель числа t_0 делит er, но не делит $d_0 = (s^{mr} - 1)/er$, то из предположения индукции, примененного к t_0, получим, что показатель, которому принадлежит число s по модулю $ert_0 = et$, равен $mrt_0 = mt$. Пусть r_0 — простой делитель числа t_0. Поскольку каждый простой делитель числа t делит e, то, очевидно, r_0 делит er. Снова запишем $d = (s^m - 1)/e$. Имеем $s^{mr} - 1 = c(s^m - 1)$, где $c = s^{m(r-1)} + \ldots + s^m + 1$, так что $d_0 = c(s^m - 1)/er = cd/r$. Далее, так как $s^m \equiv 1 \pmod e$ и r делит e, то $s^m \equiv 1 \pmod r$, так что $c = \sum_{i=0}^{r-1} s^{mi} \equiv 0 \pmod r$. Таким образом, c/r — целое число. Поскольку число r_0 не делит d, то, чтобы доказать, что r_0 не делит $d_0 = cd/r$, достаточно показать, что r_0 не делит c/r. Заметим, что $s^m \equiv 1 \pmod{r_0}$, так что $c \equiv r \pmod{r_0}$. Если $r_0 \neq r$, то $c/r \equiv 1 \pmod{r_0}$, и, значит, r_0 не делит c/r. Теперь пусть $r_0 = r$. Тогда $s^m \equiv 1 + br \pmod{r^2}$ для некоторого $b \in \mathbb{Z}$,

откуда $s^{mj} \equiv (1 + br)^j \equiv 1 + jbr \pmod{r^2}$ для всех $j \geqslant 0$, и, таким образом,

$$c \equiv r + br \sum_{j=0}^{r-1} j \equiv r + br \frac{r(r-1)}{2} \pmod{r^2}.$$

Это значит, что

$$\frac{c}{r} \equiv 1 + b \frac{r(r-1)}{2} \pmod{r}.$$

Если r нечетно, то $c/r \equiv 1 \pmod{r}$, так что $r_0 = r$ не делит c/r. Остается рассмотреть лишь случай $r_0 = r = 2$. Тогда t кратно четырем, и, значит, $s^m \equiv 1 \pmod 4$ по предположению. Так как в этом случае $c = s^m + 1$, то мы получаем $c \equiv 2 \pmod 4$, а следовательно, $c/r = c/2 \equiv 1 \pmod 2$. Это вновь означает, что r_0 не делит c/r. □

3.35. Теорема. *Пусть $f_1(x), \ldots, f_N(x)$ — все различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$ степени m и порядка e, и пусть $t \geqslant 2$ — некоторое целое число, простые делители которого делят e, но не делят $(q^m - 1)/e$. Пусть, наконец, $q^m \equiv 1 \pmod 4$, если t кратно четырем. Тогда $f_1(x^t), \ldots, f_N(x^t)$ представляют собой все различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$ степени mt и порядка et.*

Доказательство. Из условия теоремы следует, что $e \geqslant 2$. В соответствии с теоремой 3.5 нормированный неприводимый многочлен степени m и порядка $e \geqslant 2$ в кольце $\mathbb{F}_q[x]$ существует лишь тогда, когда m является показателем, которому принадлежит число q по модулю e, и в таком случае $N = \varphi(e)/m$. По лемме 3.34 показатель, которому принадлежит число q по модулю et, равен mt, и так как из формулы, указанной в упр. 1.4 (c), вытекает, что $\varphi(et)/mt = \varphi(e)/m$, то число нормированных неприводимых многочленов степени mt и порядка et в кольце $\mathbb{F}_q[x]$ тоже равно N. Поэтому остается показать, что каждый из многочленов $f_j(x^t)$, $1 \leqslant j \leqslant N$, неприводим в $\mathbb{F}_q[x]$ и имеет порядок et. Так как корни каждого многочлена $f_j(x)$ являются первообразными корнями степени e из единицы над $\mathbb{F}_q$ (по теореме 3.3) то $f_j(x)$ делит круговой многочлен $Q_e(x)$ над $\mathbb{F}_q$. Но тогда многочлен $f_j(x^t)$ делит $Q_e(x^t)$, и повторное использование свойства, указанного в упр. 2.57(b), приводит к равенству $Q_e(x^t) = Q_{et}(x)$. Таким образом, многочлен $f_j(x^t)$ делит $Q_{et}(x)$. По теореме 2.47(ii) степень каждого неприводимого делителя многочлена $Q_{et}(x)$ в $\mathbb{F}_q[x]$ равна показателю, которому принадлежит q по модулю et. Этот показатель равен mt. Так как многочлен $f_j(x^t)$ имеет степень mt, то он неприводим в кольце $\mathbb{F}_q[x]$. Кроме того, поскольку $f_j(x^t)$ делит $Q_{et}(x)$, то порядок многочлена $f_j(x^t)$ равен et. □

3.36. Пример. Неприводимыми многочленами степени 4 и порядка 15 в кольце $\mathbb{F}_2[x]$ являются $x^4 + x + 1$ и $x^4 + x^3 + 1$. Поэтому по теореме 3.35 неприводимыми многочленами в $\mathbb{F}_2[x]$ степени 12 и порядка 45 являются $x^{12} + x^3 + 1$ и $x^{12} + x^9 + 1$. А неприводимыми многочленами в $\mathbb{F}_2[x]$ степени 60 и порядка 225 являются $x^{60} + x^{15} + 1$ и $x^{60} + x^{45} + 1$. Неприводимыми многочленами в $\mathbb{F}_2[x]$ степени 100 и порядка 375 являются $x^{100} + x^{25} + 1$ и $x^{100} + x^{75} + 1$. □

Случай $t \equiv 0 \pmod 4$ и $q^m \equiv 3 \pmod 4$ не охватывается теоремой 3.35. Здесь должно быть $q \equiv 3 \pmod 4$ и нечетное m. Результат, относящийся к этому случаю, сложнее, чем теорема 3.35.

3.37. Теорема. *Пусть $f_1(x), \ldots, f_N(x)$ — все различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$ нечетной степени m и порядка e. Пусть $q = 2^a u - 1$ и $t = 2^b v$, где a и $b \geqslant 2$ — целые, a и, v — нечетные числа и при этом все простые делители числа t делят e, но не делят $(q^m - 1)/e$. Пусть k — наименьшее из чисел a и b. Тогда каждый из многочленов $f_j(x^t)$ разлагается в произведение 2^{k-1} нормированных неприводимых многочленов $g_{ij}(x)$ из $\mathbb{F}_q[x]$ степени $mt2^{1-k}$. Указанными $2^{k-1}N$ многочленами $g_{ij}(x)$ исчерпываются все различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$ степени $mt2^{1-k}$ и порядка et.*

Доказательство. Если $v \geqslant 3$, то из теоремы 3.35 следует, что $f_1(x^v), \ldots, f_N(x^v)$ — все различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$ нечетной степени mv и порядка ev. Таким образом, мы сводим вопрос к рассмотрению лишь одного случая $t = 2^b$.

Итак, пусть $t = 2^b$. Заметим, что здесь точно так же, как и в доказательстве теоремы 3.35, устанавливается, что m — показатель, которому принадлежит число q по модулю e, $N = \varphi(e)/m$ и каждый многочлен $f_j(x^t)$ делит $Q_{et}(x)$. По теореме 2.47 (ii) круговой многочлен $Q_{et}(x)$ разлагается в произведение различных нормированных неприводимых многочленов из $\mathbb{F}_q[x]$ степени d, где d — показатель, которому принадлежит число q по модулю et. Так как $q^d \equiv 1 \pmod{et}$, то $q^d \equiv 1 \pmod e$ и, значит, m делит d. Рассмотрим сначала случай $a \geqslant b$. Тогда $q^{2m} - 1 = (q^m - 1)(q^m + 1)$, и первый сомножитель делится на e, а второй делится на t, поскольку из $q \equiv -1 \pmod{2^a}$ следует $q \equiv -1 \pmod t$, так что $q^m \equiv (-1)^m \equiv -1 \pmod t$. Таким образом, $q^{2m} \equiv 1 \pmod{et}$, поэтому число d может быть равно только m или $2m$. Если $d = m$, то $q^m \equiv 1 \pmod{et}$, откуда $q^m \equiv 1 \pmod t$, что невозможно. Таким образом, $d = 2m = m2^{b-k+1}$, так как в этом случае $k = b$.

Теперь рассмотрим случай $a < b$. Индукцией по h доказываем, что для всех $h \in \mathbb{N}$

$$q^{m2^h} \equiv 1 + w2^{a+h} \pmod{2^{a+h+1}}, \tag{3.9}$$

где w — нечетное число. Для $h = 1$ получаем

$$q^{2m} = (2^a u - 1)^{2m} =$$

$$= 1 - 2^{a+1}um + \sum_{n=2}^{2m} \binom{2m}{n} (-1)^{2m-n} 2^{na} u^n \equiv$$

$$\equiv 1 + w2^{a+1} \pmod{2^{a+2}},$$

где $w = -um$. Если (3.9) выполнено для некоторого $h \in \mathbb{N}$, то для некоторого $c \in \mathbb{Z}$

$$q^{m2^h} = 1 + w2^{a+h} + c2^{a+h+1}.$$

Это значит, что

$$q^{m2^{h+1}} = (1 + w2^{a+h} + c2^{a+h+1})^2 \equiv 1 + w2^{a+h+1} \pmod{2^{a+h+2}},$$

и, таким образом, доказательство формулы (3.9) завершено. Полагая в (3.9) $h = b - a + 1$, получим, что $q^{m2^{b-a+1}} \equiv 1 \pmod{2^{b+1}}$. Кроме того, из $q^m \equiv 1 \pmod{e}$ следует $q^{m2^{b-a+1}} \equiv 1 \pmod{e}$ и, значит, $q^{m2^{b-a+1}} \equiv 1 \pmod{L}$, где $L = \text{НОК}(2^{b+1}, e)$. Здесь число e четно, поскольку все простые делители числа t делят e, однако $e \not\equiv 0 \pmod 4$, так как $q^m \equiv 1 \pmod{e}$ и $q^m \equiv 3 \pmod 4$. Поэтому $L = e2^b = et$, и, значит, $q^{m2^{b-a+1}} \equiv 1 \pmod{et}$. С другой стороны, полагая в (3.9) $h = b - a$, получаем

$$q^{m2^{b-a}} \equiv 1 + w2^b \not\equiv 1 \pmod{2^{b+1}},$$

откуда вытекает, что $q^{m2^{b-a}} \not\equiv 1 \pmod{et}$. Следовательно, мы должны иметь $d = m2^{b-a+1} = m2^{b-k+1}$, поскольку в этом случае $k = a$. Поэтому формула $d = m2^{b-k+1} = mt2^{1-k}$ справедлива в обоих случаях.

Так как круговой многочлен $Q_{et}(x)$ разлагается в произведение различных нормированных неприводимых многочленов из $\mathbb{F}_q[x]$ степени $mt2^{1-k}$, то и каждый многочлен $f_j(x^t)$ разлагается в произведение таких многочленов. Сравнивая степени, получаем, что число таких сомножителей равно 2^{k-1}. Поскольку каждый из указанных неприводимых сомножителей $g_{ij}(x)$ многочлена $f_j(x^t)$ делит $Q_{et}(x)$, то каждый многочлен $g_{ij}(x)$ имеет порядок et. Многочлены $g_{ij}(x)$ с различными наборами индексов (i, j), $1 \leqslant i \leqslant 2^{k-1}$, $1 \leqslant j \leqslant N$, различны, так как в противном случае один такой многочлен, скажем $g(x)$, делил бы многочлены $f_{j_1}(x^t)$ и $f_{j_2}(x^t)$,

где $j_1 \neq j_2$, и тогда для любого корня β многочлена $g(x)$ степень β^t была бы общим корнем многочленов $f_{j_1}(x)$ и $f_{j_2}(x)$, что невозможно. По теореме 3.5 число нормированных неприводимых многочленов степени $mt2^{1-k}$ и порядка et в кольце $\mathbb{F}_q[x]$ равно $\varphi(et)/mt2^{1-k} = 2^{k-1}\varphi(et)/mt = 2^{k-1}\varphi(e)/m = 2^{k-1}N$, и, следовательно, многочленами $g_{ij}(x)$ исчерпываются все такие многочлены. □

Теперь мы покажем, как из данного неприводимого многочлена порядка e получить все неприводимые многочлены, порядки которых делят e. Поскольку в их число обязательно войдет неприводимый многочлен $g(x) = x$, то мы будем рассматривать лишь те неприводимые многочлены g, для которых $g(0) \neq 0$. Пусть f — нормированный неприводимый многочлен из $\mathbb{F}_q[x]$ степени m и порядка e, такой, что $f(0) \neq 0$. Пусть $\alpha \in \mathbb{F}_{q^m}$ — некоторый корень многочлена f, и для каждого $t \in \mathbb{N}$ пусть $g_t \in \mathbb{F}_q[x]$ — минимальный многочлен элемента α^t над $\mathbb{F}_q$. Пусть $T = \{t_1, \ldots, t_n\}$ — множество натуральных чисел, таких, что для каждого $t \in \mathbb{N}$ существует однозначно определенный индекс i, $1 \leqslant i \leqslant n$ такой, что $t \equiv t_i q^b \pmod{e}$ для некоторого целого числа $b \geqslant 0$. Такое множество T можно, например, построить следующим образом. Положим $t_1 = 1$, и, когда уже построены $t_1, \ldots, t_{j-1}$, пусть t_j будет наименьшим натуральным числом, для которого $t_j \not\equiv t_i q^b \pmod{e}$ при $1 \leqslant i < j$ и всех целых $b \geqslant 0$. Эта процедура закончится через конечное число шагов.

При введенных выше обозначениях получаем следующий общий результат.

3.38. Теорема. *Многочленами $g_{t_1}, \ldots, g_{t_n}$ исчерпываются все различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$, порядки которых делят число e, а постоянные члены отличны от нуля.*

Доказательство. Каждый многочлен g_{t_i} по определению нормирован и неприводим в кольце $\mathbb{F}_q[x]$ и удовлетворяет условию $g_{t_i}(0) \neq 0$. Кроме того, раз многочлен g_{t_i} имеет корень α^{t_i}, порядок которого в группе $\mathbb{F}_{q^m}^*$ делит порядок элемента α, то из теоремы 3.3 следует, что $\operatorname{ord}(g_{t_i})$ делит e.

Пусть g — произвольный нормированный неприводимый многочлен из $\mathbb{F}_q[x]$ порядка d, делящего e, такой, что $g(0) \neq 0$. Если β — какой-нибудь корень многочлена g, то из равенства $\beta^d = 1$ следует, что $\beta^e = 1$, так что β — корень степени e из единицы над $\mathbb{F}_q$. Так как α — первообразный корень степени e из единицы над $\mathbb{F}_q$, то из теоремы 2.42 (i) получаем, что $\beta = \alpha^t$ для некоторого $t \in \mathbb{N}$. Тогда из определения множества T следует, что $t \equiv$

$\equiv t_i q^b \pmod e$ при некотором целом i, $1 \leqslant i \leqslant n$, и целом $b \geqslant 0$. Поэтому $\beta = \alpha^t = (\alpha^{t_i})^{q^b}$, так что β — корень многочлена g_{t_i} (согласно теореме 2.14). А поскольку g — минимальный многочлен элемента β над $\mathbb{F}_q$, из теоремы 3.33 (iii) следует, что $g = g_{t_i}$.

Остается показать, что многочлены g_{t_i}, $1 \leqslant i \leqslant n$, различны. Допустим, что $g_{t_i} = g_{t_j}$ при $i \neq j$. Тогда α^{t_i} и α^{t_j} — корни многочлена g_{t_i}, так что $\alpha^{t_j} = (\alpha^{t_i})^{q^b}$ для некоторого $b \geqslant 0$. Отсюда следует, что $t_j \equiv t_i q^b \pmod e$, но так как, кроме того, $t_j \equiv t_j q^0 \pmod e$, то мы получаем противоречие с определением множества T. □

Минимальный многочлен g_t элемента $\alpha^t \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$ обычно вычисляют с помощью характеристического многочлена f_t этого элемента над $\mathbb{F}_q$. Из рассуждения, следующего за определением 2.22, мы знаем, что $f_t = g_t^r$, где $r = m/k$ и k — степень многочлена g_t. Поскольку многочлен g_t неприводим в кольце $\mathbb{F}_q[x]$, число k является показателем, которому принадлежит q по модулю $d = \operatorname{ord}(g_t)$; поэтому число d равно порядку элемента α^t в группе $\mathbb{F}_{q^m}^*$, а этот порядок по теореме 1.15 (ii) равен $e/\text{НОД}(t, e)$. Значит, число d, а также k и r можно легко определить.

Для вычисления характеристического многочлена f_t элемента $\alpha^t \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$ существует несколько способов. Один из них основан на использовании связи между многочленом f_t и исходным многочленом f.

3.39. Теорема. *Пусть f — нормированный неприводимый многочлен степени m из $\mathbb{F}_q[x]$. Пусть $\alpha \in \mathbb{F}_{q^m}$ — какой-либо корень этого многочлена, и для $t \in \mathbb{N}$ пусть f_t — характеристический многочлен элемента $\alpha^t \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Тогда*

$$f_t(x^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega_j x),$$

где $\omega_1, \ldots, \omega_t$ — корни степени t из единицы над $\mathbb{F}_q$ с учетом их кратности.

Доказательство. Пусть $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ — все корни многочлена f. Тогда $\alpha_1^t, \ldots, \alpha_m^t$ — корни многочлена f_t с учетом их кратности. Поэтому

$$f_t(x^t) = \prod_{i=1}^{m} (x^t - \alpha_i^t) = \prod_{i=1}^{m} \prod_{j=1}^{t} (x - \alpha_i \omega_j) =$$
$$= \prod_{i=1}^{m} \prod_{j=1}^{t} \omega_j (\omega_j^{-1} x - \alpha_i).$$

Сравнивая коэффициенты в равенстве

$$x^t - 1 = \prod_{j=1}^{t} (x - \omega_j),$$

получаем, что $\prod_{j=1}^{t} \omega_j = (-1)^{t+1}$, так что

$$f_t(x^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} \prod_{i=1}^{m} (\omega_j^{-1} x - \alpha_i) =$$

$$= (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega_j^{-1} x) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega_j x),$$

поскольку $\omega_1^{-1}, \ldots, \omega_t^{-1}$ пробегают в точности все корни степени t из единицы над $\mathbb{F}_q$. □

3.40. Пример. Рассмотрим неприводимый многочлен $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Чтобы вычислить f_3, заметим, что корни третьей степени из единицы над $\mathbb{F}_2$ суть 1, ω и ω^2, где ω — корень многочлена $x^2 + x + 1$, принадлежащий полю $\mathbb{F}_4$. Тогда

$$f_3(x^3) = (-1)^{16} f(x) f(\omega x) f(\omega^2 x) =$$

$$= (x^4 + x + 1)(\omega x^4 + \omega x + 1)(\omega^2 x^4 + \omega^2 x + 1) =$$

$$= x^{12} + x^9 + x^6 + x^3 + 1,$$

так что $f_3(x) = x^4 + x^3 + x^2 + x + 1$. □

Другой способ отыскания характеристического многочлена f_t элемента α^t базируется на теории матриц. Пусть $f(x) = x^m - a_{m-1} x^{m-1} - \ldots - a_1 x - a_0$, и пусть A — *сопровождающая матрица* многочлена f, определяемая как $m \times m$-матрица вида

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \ldots & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \ldots & 1 & a_{m-1} \end{pmatrix}.$$

Тогда f является *характеристическим многочленом матрицы* A в смысле линейной алгебры, т. е. $f(x) = \det(xI - A)$, где I — единичная $m \times m$-матрица над $\mathbb{F}_q$. Для каждого $t \in \mathbb{N}$ многочлен f_t является характеристическим многочленом для t-й степени A^t матрицы A. Так, вычисляя степени матрицы A, можно получить многочлены f_t.

3.41. Пример. Интересно выяснить, какие из многочленов f_t являются неприводимыми в кольце $\mathbb{F}_q[x]$. Из рассуждения,

предшествующего теореме 3.39, сразу следует, что характеристический многочлен f_t элемента $\alpha^t \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$ будет неприводим в $\mathbb{F}_q[x]$ тогда и только тогда, когда он совпадает с минимальным многочленом g_t элемента α^t над $\mathbb{F}_q$, т. е. когда $\deg(g_t) = m$, а для этого необходимо и достаточно, чтобы m было показателем, которому принадлежит q по модулю $d = e/\text{НОД}(t, e)$. Рассмотрим, например, случай $q = 2$, $m = 6$, $e = 63$. Так как показатель, которому принадлежит число q по модулю какого-нибудь делителя числа e, должен быть делителем числа m, то кроме m возможны лишь показатели $k = 1, 2, 3$. Для них $q^k - 1 = 1, 3, 7$, так что сравнения $q^k \equiv 1 \pmod d$ выполняются лишь при $d = 1, 3, 7$. Таким образом, многочлен f_t приводим в кольце $\mathbb{F}_2[x]$ как раз в случаях, когда НОД $(t, 63) = 9, 21, 63$. Поскольку достаточно рассмотреть лишь значения t, удовлетворяющие условию $1 \leqslant t \leqslant 63$, то получаем, что многочлен f_t неприводим в кольце $\mathbb{F}_2[x]$ для всех значений t из указанного интервала, за исключением $t = 9, 18, 21, 27, 36, 42, 45, 54, 63$. □

На практике неприводимые многочлены часто появляются как минимальные многочлены элементов какого-нибудь расширения исходного поля. Если в проведенном выше рассуждении в качестве f взять примитивный многочлен над $\mathbb{F}_q$, т. е. считать, что $e = q^m - 1$, то степени элемента α будут пробегать все ненулевые элементы поля $\mathbb{F}_{q^m}$. Поэтому описанный выше метод можно применять для вычисления минимальных многочленов над $\mathbb{F}_q$ всех элементов мультипликативной группы $\mathbb{F}_{q^m}^*$ поля $\mathbb{F}_{q^m}$.

Прямой *метод нахождения минимальных многочленов* состоит в следующем. Пусть θ — образующий элемент поля $\mathbb{F}_{q^m}$ как простого расширения поля $\mathbb{F}_q$, так что $\{1, \theta, \ldots, \theta^{m-1}\}$ — базис $\mathbb{F}_{q^m}$ как векторного пространства над $\mathbb{F}_q$. Чтобы найти минимальный многочлен g элемента $\beta \in \mathbb{F}_{q^m}^*$ над $\mathbb{F}_q$, выразим степени $\beta^0, \beta^1, \ldots, \beta^m$ через базисные элементы. Пусть для $1 \leqslant i \leqslant m + 1$

$$\beta^{i-1} = \sum_{j=1}^{m} b_{ij}\theta^{j-1}.$$

Запишем многочлен g в виде $g(x) = c_m x^m + \ldots + c_1 x + c_0$. Нам нужно, чтобы g был нормированным многочленом наименьшей степени, удовлетворяющим условию $g(\beta) = 0$. Это условие $g(\beta) = c_m\beta^m + \ldots + c_1\beta + c_0 = 0$ приводит к однородной системе линейных уравнений

$$\sum_{i=1}^{m+1} c_{i-1}b_{ij} = 0, \quad j = 1, 2, \ldots, m, \tag{3.10}$$

с неизвестными $c_0, c_1, \ldots, c_m$. Пусть B — матрица коэффициентов этой системы, т. е. некоторая $(m + 1) \times m$-матрица $B = (b_{ij})$,

и пусть ее ранг равен r. Тогда размерность пространства решений системы (3.10) равна $s = m + 1 - r$, и поскольку $1 \leqslant r \leqslant m$, то $1 \leqslant s \leqslant m$. Поэтому мы можем произвольно задать значения для s из $m + 1$ неизвестных $c_0, c_1, \ldots, c_m$, и тогда остальные неизвестные определятся однозначно. Если $s = 1$, мы положим $c_m = 1$, а если $s > 1$, то положим $c_{m-1} = \ldots = c_{m-s+2} = 0$, а $c_{m-s+1} = 1$.

3.42. Пример. Пусть $\theta \in \mathbb{F}_{64}$ — корень неприводимого многочлена $x^6 + x + 1 \in \mathbb{F}_2[x]$. Тогда для элемента $\beta = \theta^3 + \theta^4$ получаем

$$\begin{aligned}
\beta^0 &= 1, \\
\beta^1 &= \theta^3 + \theta^4, \\
\beta^2 &= 1 + \theta + \theta^2 + \theta^3, \\
\beta^3 &= \theta + \theta^2 + \theta^3, \\
\beta^4 &= \theta + \theta^2 + \theta^4, \\
\beta^5 &= 1 + \theta^3 + \theta^4, \\
\beta^6 &= 1 + \theta + \theta^2 + \theta^4,
\end{aligned}$$

Поэтому матрица B имеет вид

$$B = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0
\end{pmatrix},$$

и ее ранг r равен 3. Значит, $s = m + 1 - r = 4$, и мы полагаем $c_3 = 1$, $c_6 = c_5 = c_4 = 0$. Остальные коэффициенты определяем из системы (3.10) и получаем $c_2 = 1$, $c_1 = 0$, $c_0 = 1$. Следовательно, минимальный многочлен элемента β над $\mathbb{F}_2$ равен $g(x) = x^3 + x^2 + 1$. □

Еще один *метод нахождения минимальных многочленов* основан на теореме 3.33 (v). Если требуется найти минимальный многочлен g элемента $\beta \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$, то мы вычисляем степени β, β^q, β^{q^2}, ..., пока не получим наименьшее натуральное число d, для которого $\beta^{q^d} = \beta$. Это целое число d является степенью многочлена g, а сам этот многочлен задается формулой

$$g(x) = (x - \beta)(x - \beta^q) \ldots (x - \beta^{q^{d-1}}).$$

Элементы β, β^q, β^{q^2}, ..., $\beta^{q^{d-1}}$ являются различными сопряженными с β элементами относительно поля $\mathbb{F}_q$, а g — минимальный многочлен над $\mathbb{F}_q$ любого из этих элементов.

3.43. Пример. Найдем минимальные многочлены над $\mathbb{F}_2$ для всех элементов поля $\mathbb{F}_{16}$. Пусть $\theta \in \mathbb{F}_{16}$ — корень примитивного многочлена $x^4 + x + 1$ над $\mathbb{F}_2$, так что каждый ненулевой элемент из поля $\mathbb{F}_{16}$ можно представить некоторой степенью элемента θ. Для поля $\mathbb{F}_{16}$ получаем следующую таблицу индексов:

i	θ^i	i	θ^i
0	1	8	$1+\theta^2$
1	θ	9	$\theta+\theta^3$
2	θ^2	10	$1+\theta+\theta^2$
3	θ^3	11	$\theta+\theta^2+\theta^3$
4	$1+\theta$	12	$1+\theta+\theta^2+\theta^3$
5	$\theta+\theta^2$	13	$1+\theta^2+\theta^3$
6	$\theta^2+\theta^3$	14	$1+\theta^3$
7	$1+\theta+\theta^3$		

Ниже указываются минимальные многочлены элементов β поля $\mathbb{F}_{16}$ над полем $\mathbb{F}_2$:

$\beta = 0$: $g_1(x) = x$.

$\beta = 1$: $g_2(x) = x + 1$.

$\beta = \theta$: различными сопряженными с θ элементами относительно $\mathbb{F}_2$ являются θ, θ^2, θ^4, θ^8, и минимальный многочлен каждого из них равен

$$g_3(x) = (x-\theta)(x-\theta^2)(x-\theta^4)(x-\theta^8) = x^4 + x + 1.$$

$\beta = \theta^3$: различными сопряженными с θ^3 элементами относительно $\mathbb{F}_2$ являются θ^3, θ^6, θ^{12}, $\theta^{24} = \theta^9$, и минимальным многочленом каждого из них является

$$g_4(x) = (x-\theta^3)(x-\theta^6)(x-\theta^9)(x-\theta^{12}) = x^4 + x^3 + x^2 + x + 1.$$

$\beta = \theta^5$: так как $\beta^4 = \beta$, то различными сопряженными с θ^5 относительно $\mathbb{F}_2$ элементами являются θ^5, θ^{10}, и соответствующий минимальный многочлен равен

$$g_5(x) = (x-\theta^5)(x-\theta^{10}) = x^2 + x + 1.$$

$\beta = \theta^7$: различными сопряженными с θ^7 элементами относительно $\mathbb{F}_2$ являются θ^7, θ^{14}, $\theta^{28} = \theta^{13}$, $\theta^{56} = \theta^{11}$, и соответствующий минимальный многочлен равен

$$g_6(x) = (x-\theta^7)(x-\theta^{11})(x-\theta^{13})(x-\theta^{14}) = x^4 + x^3 + 1.$$

Указанные элементы вместе с их сопряженными относительно $\mathbb{F}_2$ составляют поле $\mathbb{F}_{16}$. □

Важной проблемой является *нахождение примитивных многочленов*. Один из подходов основан на том факте, что произведение всех примитивных многочленов степени m над $\mathbb{F}_q$ равно круговому многочлену Q_e, где $e = q^m - 1$ (см. теорему 2.47 (ii) и упр. 3.42). Поэтому все примитивные многочлены над $\mathbb{F}_q$ степени m можно найти, применяя один из алгоритмов разложения (см. гл. 4) к круговому многочлену Q_e.

Другой метод опирается на построение какого-либо примитивного элемента поля $\mathbb{F}_{q^m}$, для которого затем описанными выше способами вычисляется его минимальный многочлен над $\mathbb{F}_q$ (этот многочлен и является примитивным). Для нахождения примитивного элемента поля $\mathbb{F}_{q^m}$ берут порядок $q^m - 1$ этого элемента в группе $\mathbb{F}_{q^m}^*$ и разлагают его на множители: $q^m - 1 = h_1 \dots h_k$, где натуральные числа $h_1, \dots, h_k$ попарно взаимно просты. Если для каждого h_i, $1 \leqslant i \leqslant k$, можно найти элемент $\alpha_i \in \mathbb{F}_{q^m}^*$ порядка h_i, то произведение $\alpha = \alpha_1 \dots \alpha_k$ имеет порядок $q^m - 1$ и, следовательно, является примитивным элементом поля $\mathbb{F}_{q^m}$.

3.44. Пример. Найдем примитивный многочлен степени 4 над полем $\mathbb{F}_3$. Поскольку $3^4 - 1 = 16 \cdot 5$, мы предварительно построим два элемента группы $\mathbb{F}_{81}^*$ соответственно порядков 16 и 5. Элементы порядка 16 являются корнями кругового многочлена $Q_{16}(x) = x^8 + 1 \in \mathbb{F}_3[x]$. Так как показатель, которому принадлежит число 3 по модулю 16, равен 4, то Q_{16} разлагается на два нормированных неприводимых многочлена степени 4 из $\mathbb{F}_3[x]$. Далее

$$x^8 + 1 = (x^4 - 1)^2 - x^4 = (x^4 - 1 + x^2)(x^4 - 1 - x^2),$$

так что многочлен $f(x) = x^4 - x^2 - 1$ неприводим над $\mathbb{F}_3$, и $\mathbb{F}_{81} = \mathbb{F}_3(\theta)$ для некоторого корня θ многочлена f. Кроме того θ — элемент порядка 16 группы $\mathbb{F}_{81}^*$. Чтобы найти элемент α порядка 5, запишем его в виде

$$\alpha = a + b\theta + c\theta^2 + d\theta^3$$

с неопределенными коэффициентами a, b, c и d из $\mathbb{F}_3$. Так как $\alpha^{10} = 1$, то

$$\begin{aligned} 1 = \alpha^9\alpha &= (a + b\theta^9 + c\theta^{18} + d\theta^{27})(a + b\theta + c\theta^2 + d\theta^3) = \\ &= (a - b\theta + c\theta^2 - d\theta^3)(a + b\theta + c\theta^2 + d\theta^3) = \\ &= (a + c\theta^2)^2 - (b\theta + d\theta^3)^2 = \\ &= a^2 + (2ac - b^2)\theta^2 + (c^2 - 2bd)\theta^4 - d^2\theta^6 = \\ &= a^2 + c^2 - d^2 + bd + (c^2 + d^2 - b^2 - ac + bd)\theta^2. \end{aligned}$$

Сравнение коэффициентов дает

$$a^2 + c^2 - d^2 + bd = 1, \quad c^2 + d^2 - b^2 - ac + bd = 0,$$

Полагая $a = d = 0$, получим $b^2 = c^2 = 1$. Беря $b = c = 1$, легко находим, что элемент $\alpha = \theta + \theta^2$ имеет порядок 5. Следовательно, элемент $\zeta = \theta\alpha = \theta^2 + \theta^3$ имеет порядок 80 и, таким образом, является примитивным элементом поля $\mathbb{F}_{81}$. Минимальный многочлен g элемента ζ над $\mathbb{F}_3$ равен

$$\begin{aligned} g(x) &= (x - \zeta)(x - \zeta^3)(x - \zeta^9)(x - \zeta^{27}) = \\ &= (x - \theta^2 - \theta^3)(x - 1 + \theta + \theta^2)(x - \theta^2 + \theta^3)(x - \\ &\quad - 1 - \theta + \theta^2) = \\ &= x^4 + x^3 + x^2 - x - 1, \end{aligned}$$

и мы, таким образом, получили примитивный многочлен степени 4 над полем $\mathbb{F}_3$. □

3.45. Пример. Найдем примитивный многочлен степени 6 над $\mathbb{F}_2$. Поскольку $2^6 - 1 = 9 \cdot 7$, то сначала построим два элемента группы $\mathbb{F}_{64}^*$ порядков 9 и 7 соответственно. Показатель, которому принадлежит 2 по модулю 9, равен 6, так что круговой многочлен $Q_9(x) = x^6 + x^3 + 1$ неприводим над $\mathbb{F}_2$. Корень θ этого многочлена имеет порядок 9 в группе $\mathbb{F}_{64}^*$, причем $\mathbb{F}_{64} = \mathbb{F}_2(\theta)$. Элемент $\alpha \in \mathbb{F}_{64}^*$ порядка 7 удовлетворяет равенству $\alpha^8 = \alpha$, так что, записав $\alpha = \sum_{i=0}^{5} a_i\theta^i$ с коэффициентами $a_i \in \mathbb{F}_2$, $0 \leqslant i \leqslant 5$, получаем

$$\begin{aligned} \alpha = \sum_{i=0}^{5} a_i\theta^i = \alpha^8 = \left(\sum_{i=0}^{5} a_i\theta^i\right)^8 = \sum_{i=0}^{5} a_i\theta^{8i} = \\ = a_0 + a_1\theta^8 + a_2\theta^7 + a_3\theta^6 + a_4\theta^5 + a_5\theta^4 = \\ = (a_0 + a_3) + a_2\theta + a_1\theta^2 + a_3\theta^3 + (a_2 + a_5)\,\theta^4 + \\ + (a_1 + a_4)\,\theta^5, \end{aligned}$$

и сравнение коэффициентов дает $a_3 = 0$, $a_1 = a_2$, $a_4 = a_2 + a_5$. Выбирая $a_0 = a_3 = a_4 = 0$, $a_1 = a_2 = a_5 = 1$, получим, что $\alpha = \theta + \theta^2 + \theta^5$ является элементом порядка 7. Таким образом, $\zeta = \alpha\theta = 1 + \theta^2$ является примитивным элементом поля $\mathbb{F}_{64}$. Его степени равны $\zeta^2 = 1 + \theta^4$, $\zeta^3 = \theta^2 + \theta^3 + \theta^4$, $\zeta^4 = 1 + \theta^2 + \theta^5$, $\zeta^5 = 1 + \theta + \theta^5$, $\zeta^6 = 1 + \theta^2 + \theta^3 + \theta^4 + \theta^5$. Применяя тот же метод, что и в примере 3.42, найдем минимальный многочлен $g(x) = x^6 + x^4 + x^3 + x + 1$ элемента ζ над $\mathbb{F}_2$, который, таким образом, является примитивным многочленом над $\mathbb{F}_2$ степени 6. □

Если примитивный многочлен g над $\mathbb{F}_q$ степени m известен, то все остальные примитивные многочлены над $\mathbb{F}_q$ той же степени

можно получить, рассматривая некоторый корень θ многочлена g в поле $\mathbb{F}_{q^m}$ и находя минимальные многочлены над $\mathbb{F}_q$ для всех элементов вида θ^t, где t пробегает все натуральные взаимно простые с $q^m - 1$ числа, не превосходящие $q^m - 1$. Вычисление этих минимальных многочленов можно осуществить методами, описанными выше в этом параграфе.

Полезно выяснить, остается ли данный неприводимый над $\mathbb{F}_q$ многочлен неприводимым и над заданным конечным расширением этого поля $\mathbb{F}_{q^m}$. Следующие результаты относятся к этому вопросу.

3.46. Теорема. *Пусть f — неприводимый многочлен над $\mathbb{F}_q$ степени n и $k \in \mathbb{N}$. Тогда в кольце $\mathbb{F}_{q^k}[x]$ многочлен f разлагается на d неприводимых сомножителей одной и той же степени n/d, где $d = \text{НОД}(k, n)$.*

Доказательство. Так как случай $f(0) = 0$ тривиален, мы можем предположить, что $f(0) \neq 0$. Пусть g — неприводимый делитель многочлена f из $\mathbb{F}_{q^k}[x]$. Если $\operatorname{ord}(f) = e$, то, согласно теореме 3.3, также и $\operatorname{ord}(g) = e$ ввиду того, что корни многочлена g являются в то же время и корнями f. По теореме 3.5 показатель, которому принадлежит q по модулю e, равен n, и степень многочлена g равна показателю, которому принадлежит q^k по модулю e. Степени q^j, $j = 0, 1, \ldots$, рассматриваемые по модулю e, образуют циклическую группу порядка n. Таким образом, из теоремы 1.15 (ii) вытекает, что показатель, которому принадлежит q^k по модулю e, равен n/d, а значит, и степень многочлена g равна n/d. □

3.47. Следствие. *Неприводимый над полем $\mathbb{F}_q$ многочлен степени n остается неприводимым над расширением $\mathbb{F}_{q^k}$ этого поля в том и только том случае, если числа n и k взаимно просты.*

Доказательство. Это непосредственно вытекает из теоремы 3.46. □

3.48. Пример. Будем рассматривать примитивный многочлен $g(x) = x^6 + x^4 + x^3 + x + 1$ над $\mathbb{F}_2$ из примера 3.45 как многочлен над полем $\mathbb{F}_{16}$. Тогда в обозначениях теоремы 3.46 мы имеем $n = 6$, $k = 4$, и, значит, $d = 2$. Поэтому многочлен g разлагается в кольце $\mathbb{F}_{16}[x]$ на два неприводимых кубических сомножителя. Примем обозначения из примера 3.45, и пусть g_1 — тот неприводимый сомножитель многочлена g, корнем которого является $\zeta = 1 + \theta^2$. Другими корнями многочлена g_1 должны быть сопряженные с ζ относительно $\mathbb{F}_{16}$ элементы ζ^{16} и $\zeta^{256} = \zeta^4$. Так как эти элементы сопряжены с ζ также и относительно поля $\mathbb{F}_4$, то многочлен g_1 фактически принадлежит кольцу $\mathbb{F}_4[x]$. Далее, элемент $\beta = \zeta^{21}$ является первообразным куби-

ческим корнем из единицы над $\mathbb{F}_2$, так что $\mathbb{F}_4 = \{0, 1, \beta, \beta^2\}$. Получаем

$$g_1(x) = (x - \zeta)(x - \zeta^4)(x - \zeta^{16}) = \\ = x^3 + (\zeta + \zeta^4 + \zeta^{16}) x^2 + (\zeta^5 + \zeta^{17} + \zeta^{20}) x + \zeta^{21}.$$

Поскольку $\zeta^4 = 1 + \theta^2 + \theta^5$ и $\zeta^{16} = 1 + \theta^5$, то $\zeta + \zeta^4 + \zeta^{16} = 1$. Аналогично находим, что $\zeta^5 + \zeta^{17} + \zeta^{20} = 1$. Следовательно,

$$g_1(x) = x^3 + x^2 + x + \beta.$$

Деля многочлен g на g_1, находим второй неприводимый сомножитель g_2 многочлена g и получаем в итоге

$$g(x) = (x^3 + x^2 + x + \beta)(x^3 + x^2 + x + \beta^2)$$

— разложение многочлена g на неприводимые сомножители в $\mathbb{F}_4[x]$, а значит, и в $\mathbb{F}_{16}[x]$. Найденные неприводимые сомножители многочлена g являются примитивными многочленами над полем $\mathbb{F}_4$, но не над полем $\mathbb{F}_{16}$. На основании следствия 3.47 многочлен g над некоторыми другими расширениями поля $\mathbb{F}_2$ (например, над $\mathbb{F}_{32}$ или $\mathbb{F}_{128}$) остается неприводимым. □

§ 4. Линеаризованные многочлены

Специальный класс многочленов, вводимый в этом параграфе, весьма важен как для теории, так и для приложений. Интересной особенностью этих многочленов является структура множества их корней, которая облегчает их нахождение. В дальнейшем будем понимать под q, как обычно, некоторую степень простого числа.

3.49. Определение. Многочлен вида

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

с коэффициентами из некоторого расширения $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$ называется *q-многочленом* над $\mathbb{F}_{q^m}$.

Если число q раз и навсегда зафиксировано или ясно из контекста, то $L(x)$ также принято называть *линеаризованным многочленом*. Этот термин объясняется следующим свойством таких многочлеиов. Если F — произвольное расширение поля $\mathbb{F}_{q^m}$ и $L(x)$ — линеаризованный многочлен (т. е. q-многочлен) над F_{q^m}, то

$$L(\beta + \gamma) = L(\beta) + L(\gamma) \quad \text{для любых } \beta, \gamma \in F, \tag{3.11}$$

$$L(c\beta) = cL(\beta) \quad \text{для любых, } c \in \mathbb{F}_q, \beta \in F. \tag{3.12}$$

Равенство (3.11) вытекает из теоремы 1.46, а (3.12) — из того что $c^{q^i} = c$ для $c \in \mathbb{F}_q$ и $i \geqslant 0$. Таким образом, если поле F рассматривать как векторное пространство над полем $\mathbb{F}_q$, то линеаризованный многочлен $L(x)$ индуцирует в этом пространстве некоторый линейный оператор.

Следующий результат характеризует особенность множества корней линеаризованного многочлена.

3.50. Теорема. *Пусть $L(x)$ — ненулевой q-многочлен над $\mathbb{F}_{q^m}$, и пусть расширение $\mathbb{F}_{q^s}$ поля $\mathbb{F}_{q^m}$ содержит все корни этого многочлена. Тогда каждый корень многочлена $L(x)$ имеет одну и ту же кратность, равную либо единице, либо некоторой степени числа q; при этом если поле $\mathbb{F}_{q^s}$ рассматривать как векторное пространство над полем $\mathbb{F}_q$, то указанные корни образуют некоторое подпространство этого пространства.*

Доказательство. Из (3.11) и (3.12) следует, что любая линейная комбинация корней многочлена $L(x)$ с коэффициентами из поля $\mathbb{F}_q$ снова является корнем этого многочлена, так что корни многочлена L образуют векторное пространство (подпространство пространства $\mathbb{F}_{q^s}$). Если

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i},$$

то $L'(x) = \alpha_0$, так что многочлен $L(x)$ имеет при $\alpha_0 \neq 0$ лишь простые корни. Если же $\alpha_0 = \alpha_1 = \ldots = \alpha_{k-1} = 0$, но $\alpha_k \neq 0$ при некотором $k \geqslant 1$, то, поскольку

$$L(x) = \sum_{i=k}^{n} \alpha_i x^{q^i} = \sum_{i=k}^{n} \alpha_i^{q^{mk}} x^{q^i} = \left(\sum_{i=k}^{n} \alpha_i^{q^{(m-1)k}} x^{q^{i-k}} \right)^{q^k},$$

мы видим, что L является q^k-й степенью некоторого линеаризованного многочлена, имеющего простые корни. В таком случае каждый корень многочлена $L(x)$ имеет кратность q^k. □

Имеет место частичное обращение теоремы 3.50, которое дается теоремой 3.52. Оно опирается на следующее свойство определителей, обобщающее следствие 2.38.

3.51. Лемма. *Пусть $\beta_1, \beta_2, \ldots, \beta_n$ — элементы поля $\mathbb{F}_{q^m}$. Тогда*

$$\begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \ldots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \ldots & \beta_2^{q^{n-1}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_n & \beta_n^q & \beta_n^{q^2} & \ldots & \beta_n^{q^{n-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1, \ldots, c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{i=1}^{j} c_i \beta_i \right), \tag{3.13}$$

так что этот определитель отличен от нуля в том и только том случае, если элементы $\beta_1, \beta_2, \ldots, \beta_n$ *линейно независимы над полем* $\mathbb{F}_q$.

Доказательство. Пусть D_n — определитель из левой части равенства (3.13). Докажем это равенство индукцией по n. Заметим, что при $n = 1$ формула тривиальна, если пустое произведение в правой ее части интерпретировать как 1. Теперь допустим, что формула (3.13) доказана для некоторого $n \geqslant 1$. Рассмотрим многочлен

$$D(x) = \begin{vmatrix} \beta_1 & \beta_1^q & \ldots & \beta_1^{q^{n-1}} & \beta_1^{q^n} \\ \beta_2 & \beta_2^q & \ldots & \beta_2^{q^{n-1}} & \beta_2^{q^n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_n & \beta_n^q & \ldots & \beta_n^{q^{n-1}} & \beta_n^{q^n} \\ x & x^q & \ldots & x^{q^{n-1}} & x^{q^n} \end{vmatrix}.$$

Разлагая этот определитель по последней строке, получим

$$D(x) = D_n x^{q^n} + \sum_{i=0}^{n-1} \alpha_i x^{q^i},$$

где $\alpha_i \in \mathbb{F}_{q^m}$, $0 \leqslant i \leqslant n-1$. Предположим сначала, что элементы $\beta_1, \beta_2, \ldots, \beta_n$ линейно независимы над $\mathbb{F}_q$. Тогда $D(\beta_k) = 0$ при $1 \leqslant k \leqslant n$, и так как $D(x)$ является q-многочленом над $\mathbb{F}_{q^m}$, то все линейные комбинации $c_1\beta_1 + c_2\beta_2 + \ldots + c_n\beta_n$, где $c_k \in \mathbb{F}_q$, $1 \leqslant k \leqslant n$, являются корнями многочлена $D(x)$. Таким образом, $D(x)$ имеет q^n различных корней, и мы получаем разложение

$$D(x) = D_n \prod_{c_1, \ldots, c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right). \tag{3.14}$$

Если же $\beta_1, \beta_2, \ldots, \beta_n$ линейно зависимы над $\mathbb{F}_q$, то по предположению индукции $D_n = 0$ и $\sum_{k=1}^{n} b_k \beta_k = 0$ для некоторых $b_1, \ldots, b_n$ из поля $\mathbb{F}_q$, не равных нулю одновременно. Отсюда следует, что

$$\sum_{k=1}^{n} b_k \beta_k^{q^j} = \left(\sum_{k=1}^{n} b_k \beta_k \right)^{q^j} = 0 \quad \text{для} \quad j = 0, 1, \ldots, n,$$

так что первые n строк определителя, представляющего многочлен $D(x)$, линейно зависимы над $\mathbb{F}_q$. Поэтому $D(x) = 0$, и равенство (3.14) выполняется в любом случае. Отсюда получаем

$$D_{n+1} = D(\beta_{n+1}) = D_n \prod_{c_1, \ldots, c_n \in \mathbb{F}_q} \left(\beta_{n+1} - \sum_{k=1}^{n} c_k \beta_k \right),$$

что и доказывает формулу (3.13). □

3.52. Теорема. *Пусть U — произвольное подпространство векторного пространства $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$. Тогда для каждого неотрицательного целого числа k многочлен*

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k}$$

является q-многочленом над полем $\mathbb{F}_{q^m}$.

Доказательство. Поскольку в результате возведения q-многочлена над полем $\mathbb{F}_{q^m}$ в q^k-ю степень снова получаем q-многочлен над $\mathbb{F}_{q^m}$, то достаточно рассмотреть лишь случай $k = 0$. Пусть $\{\beta_1, \ldots, \beta_n\}$ — базис векторного пространства U над $\mathbb{F}_q$. Тогда определитель D_n левой части равенства (3.13) отличен от нуля по лемме 3.51; поэтому

$$L(x) = \prod_{\beta \in U} (x - \beta) =$$

$$= \prod_{c_1, \ldots, c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right) = D_n^{-1} D(x),$$

ввиду (3.14), а это уже доказывает, что $L(x)$ является q-многочленом над полем $\mathbb{F}_{q^m}$. □

Установленные нами свойства линеаризованных многочленов приводят к следующему *методу нахождения корней* таких многочленов. Пусть

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

— некоторый q-многочлен над полем $\mathbb{F}_{q^m}$ и требуется найти все его корни в некотором конечном расширении F поля $\mathbb{F}_{q^m}$. Как уже отмечалось выше, отображение $L\colon \beta \in F \longmapsto L(\beta) \in F$ является линейным оператором в векторном пространстве F над полем $\mathbb{F}_q$. Поэтому L можно представить некоторой матрицей над полем $\mathbb{F}_q$. Пусть $\{\beta_1, \ldots, \beta_s\}$ — базис F над полем $\mathbb{F}_q$; тогда каждый элемент $\beta \in F$ можно задать в виде линейной комбинации

$$\beta = \sum_{j=1}^{s} c_j \beta_j, \quad \text{где} \quad c_j \in \mathbb{F}_q \quad \text{для} \quad 1 \leqslant j \leqslant s,$$

и, значит,

$$L(\beta) = \sum_{j=1}^{s} c_j L(\beta_j).$$

Теперь пусть

$$L(\beta_j) = \sum_{k=1}^{s} b_{jk}\beta_k \quad \text{для} \quad 1 \leqslant i \leqslant s,$$

где $b_{jk} \in \mathbb{F}_q$ для $1 \leqslant j, k \leqslant s$, и пусть $B = (b_{jk})$ — квадратная матрица порядка s над $\mathbb{F}_q$. Тогда

$$L(\beta) = \sum_{k=1}^{s} d_k\beta_k,$$

где коэффициенты d_k определяются условием

$$(c_1, \ldots, c_s)\, B = (d_1, \ldots, d_s).$$

В частности, уравнение $L(\beta) = 0$ эквивалентно условию

$$(c_1, \ldots, c_r)\, B = (0, \ldots, 0). \tag{3.15}$$

Это однородная система из s линейных уравнений относительно s неизвестных $c_1, \ldots, c_s$. Если ранг матрицы B равен r, то система (3.15) имеет q^{s-r} линейно независимых решений — векторов $(c_1, \ldots, c_s)$. Каждое решение $(c_1, \ldots, c_s)$ соответствует некоторому корню

$$\beta = \sum_{j=1}^{s} c_j\beta_j$$

q-многочлена $L(x)$ в поле F. Таким образом, задача нахождения корней линеаризованного многочлена L, лежащих в поле F, сводится к более легкой задаче решения однородной системы линейных уравнений.

3.53. Пример. Рассмотрим линеаризованный многочлен $L(x) = x^9 - x^3 - \alpha x \in \mathbb{F}_9[x]$, где α — корень примитивного многочлена $x^2 + x - 1$ над полем $\mathbb{F}_3$. Для нахождения корней многочлена $L(x)$ в поле $\mathbb{F}_{81}$ рассмотрим базис $\{1, \zeta, \zeta^2, \zeta^3\}$ поля $\mathbb{F}_{81}$ как векторного пространства над полем $\mathbb{F}_3$, где ζ — корень примитивного многочлена $x^4 + x^3 + x^2 - x - 1$ над $\mathbb{F}_3$ (ср. с примером 3.44). Учитывая, что порядками элементов α и ζ в мультипликативной группе $\mathbb{F}_{81}^*$ являются соответственно числа 8 и 80, получаем равенство вида $\alpha = \zeta^{10j}$, где j принимает значения 1, 3, 5 или 7; но поскольку $\zeta^{20} + \zeta^{10} - 1 = 0$, то мы можем взять $\alpha = \zeta^{10} = -1 + \zeta + \zeta^2 - \zeta^3$. Затем находим

$$\begin{aligned}
L(1) &= -\alpha = 1 - \zeta - \zeta^2 + \zeta^3,\\
L(\zeta) &= \zeta^9 - \zeta^3 - \alpha\zeta = -\zeta - \zeta^2 - \zeta^3,\\
L(\zeta^2) &= \zeta^{18} - \zeta^6 - \alpha\zeta^2 = -1 + \zeta^3,\\
L(\zeta^3) &= \zeta^{27} - \zeta^9 - \alpha\zeta^3 = 1 - \zeta^3,
\end{aligned}$$

и, следовательно, получаем, что

$$B = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & -1 & -1 & -1 \\ -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \end{pmatrix}.$$

Однородная система линейных уравнений (3.15) имеет два линейно независимых решения, например (0, 0, 1, 1) и (—1, 1, 0, 1). Любое решение этой системы получается как линейная комбинация указанных двух векторов с коэффициентами из поля $\mathbb{F}_3$. Следовательно, корнями многочлена $L(x)$ в поле $\mathbb{F}_{81}$ являются элементы $\theta_1 = 0$, $\theta_2 = \zeta^2 + \zeta^3$, $\theta_3 = -\zeta^2 - \zeta^3$, $\theta_4 = -1 + \zeta + \zeta^3$, $\theta_5 = 1 - \zeta - \zeta^3$, $\theta_6 = -1 + \zeta + \zeta^2 - \zeta^3$, $\theta_7 = 1 - \zeta - \zeta^2 + \zeta^3$, $\theta_8 = 1 - \zeta + \zeta^2$, $\theta_9 = -1 + \zeta - \zeta^2$. □

Этот метод нахождения корней можно применять и для более общего класса многочленов, а именно для так называемых аффинных многочленов.

3.54. Определение. Многочлен вида $A(x) = L(x) - \alpha$, где $L(x)$ есть q-многочлен над полем $\mathbb{F}_{q^m}$, а $\alpha \in \mathbb{F}_{q^m}$, называется *аффинным q-многочленом* над $\mathbb{F}_{q^m}$.

Элемент β из некоторого конечного расширения F поля $\mathbb{F}_{q^m}$ является корнем многочлена $A(x)$ в том и только том случае, если $L(\beta) = \alpha$. В обозначениях формулы (3.15) равенство $L(\beta) = \alpha$ эквивалентно равенству

$$(c_1, \ldots, c_s)\, B = (d_1, \ldots, d_s), \tag{3.16}$$

где $\alpha = \sum_{k=1}^{s} d_k \beta_k$. Система (3.16) линейных уравнений разрешима относительно $c_1, \ldots, c_s$, и каждый ее вектор-решение $(c_1, \ldots, c_s)$ соответствует некоторому корню $\beta = \sum_{j=1}^{s} c_j \beta_j$ многочлена $A(x)$, лежащему в поле F.

Сравнительная легкость отыскания корней аффинных многочленов подсказывает следующий *метод нахождения корней* произвольного многочлена $f(x)$ положительной степени над $\mathbb{F}_{q^m}$ в некотором расширении F поля $\mathbb{F}_{q^m}$. Сначала находим какой-нибудь ненулевой аффинный q-многочлен $A(x)$ над $\mathbb{F}_{q^m}$, который делится на $f(x)$; он называется *аффинным кратным* многочлена $f(x)$. Затем описанным выше способом получаем все корни многочлена $A(x)$ из F. Поскольку среди этих корней находятся и корни многочлена $f(x)$ из F, то достаточно подсчитать значения $f(\beta)$ для всех корней $\beta \in F$ многочлена $A(x)$, и мы выделим все корни многочлена $f(x)$ в поле F.

Остается выяснить лишь, как находить аффинное кратное $A(x)$ многочлена $f(x)$. Существует следующий способ. Пусть $n \geqslant 1$ — степень многочлена $f(x)$. Для каждого $i = 0, 1, \ldots, n-1$ вычисляем однозначно определенный многочлен $r_i(x)$ степени $\leqslant n-1$, удовлетворяющий условию $x^{q^i} \equiv r_i(x) \pmod{f(x)}$. Затем находим такие элементы $\alpha_i \in \mathbb{F}_{q^m}$, не все равные нулю, чтобы линейная комбинация $\sum_{i=0}^{n-1} \alpha_i r_i(x)$ была постоянным многочленом. С этой целью приравниваем нулю $n-1$ коэффициентов при положительных степенях x^j, $1 \leqslant j \leqslant n-1$, переменной x. Так мы получаем однородную систему из $n-1$ линейных уравнений относительно n неизвестных $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$. Такая система всегда имеет нетривиальное решение. Зафиксировав некоторое нетривиальное решение $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ этой системы уравнений, мы получаем $\sum_{i=0}^{n-1} \alpha_i r_i(x) = \alpha$ для некоторого $\alpha \in \mathbb{F}_{q^m}$. Это означает, что

$$\sum_{i=0}^{n-1} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n-1} \alpha_i r_i(x) \equiv \alpha \pmod{f(x)},$$

так что

$$A(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha$$

есть ненулевой аффинный q-многочлен над $\mathbb{F}_{q^m}$, делящийся на $f(x)$. Ясно, что этот многочлен $A(x)$ можно выбрать нормированным.

3.55. Пример. Пусть $f(x) = x^4 + \theta^2 x^3 + \theta x^2 + x + \theta \in \mathbb{F}_4[x]$, где θ — некоторый корень многочлена $x^2 + x + 1 \in \mathbb{F}_2[x]$. Требуется найти корни многочлена $f(x)$, лежащие в поле $\mathbb{F}_{64}$. Сначала найдем какое-нибудь аффинное кратное $A(x)$ многочлена $f(x)$, применяя описанный выше метод при $q = 2$. По модулю $f(x)$ имеем $x \equiv x = r_0(x)$, $x^2 \equiv x^2 = r_1(x)$, $x^4 \equiv \theta^2 x^3 + \theta x^2 + x + \theta = r_2(x)$, $x^8 \equiv \theta x^3 + \theta x^2 + x + \theta = r_3(x)$. Условие, состоящее в том, что линейная комбинация $\alpha_0 r_0(x) + \alpha_1 r_1(x) + \alpha_2 r_2(x) + \alpha_3 r_3(x)$ с коэффициентами $\alpha_i \in \mathbb{F}_4$ должна быть постоянным многочленом, приводит к следующей однородной системе линейных уравнений относительно коэффициентов $\alpha_0, \alpha_1, \alpha_2, \alpha_3$:

$$\begin{aligned} \alpha_0 + \alpha_2 + \alpha_3 &= 0, \\ \alpha_1 + \theta\alpha_2 + \theta\alpha_3 &= 0, \\ \theta^2\alpha_2 + \theta\alpha_3 &= 0. \end{aligned}$$

Выберем $\alpha_3 = 1$, и тогда получим $\alpha_2 = \theta^2$, $\alpha_1 = \theta^2$, $\alpha_0 = \theta$. Таким образом, искомым постоянным многочленом является

$$\alpha = \alpha_0 r_0(x) + \alpha_1 r_1(x) + \alpha_2 r_2(x) + \alpha_3 r_3(x) = \theta^2,$$

и, значит,

$$A(x) = \alpha_3 x^8 + \alpha_2 x^4 + \alpha_1 x^2 + \alpha_0 x - \alpha = \\ = x^8 + \theta^2 x^4 + \theta^2 x^2 + \theta x + \theta^2.$$

Теперь подсчитаем корни аффинного 2-многочлена $A(x)$ в поле $\mathbb{F}_{64}$. Это значит, что для 2-многочлена

$$L(x) = x^8 + \theta^2 x^4 + \theta^2 x^2 + \theta x$$

над $\mathbb{F}_4$ мы должны решить уравнение $L(x) = \theta^2$. Пусть ζ — какой-нибудь корень примитивного многочлена $x^6 + x + 1$ над $\mathbb{F}_2$. Тогда $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ — базис поля $\mathbb{F}_{64}$ над $\mathbb{F}_2$. Так как θ — произвольный первообразный корень третьей степени из единицы над $\mathbb{F}_2$, то можно взять

$$\theta = \zeta^{21} = 1 + \zeta + \zeta^3 + \zeta^4 + \zeta^5.$$

Пользуясь тем, что $\theta^2 = \theta + 1 = \zeta + \zeta^3 + \zeta^4 + \zeta^5$, получим

$$\begin{aligned} L(1) &= \zeta + \zeta^3 + \zeta^4 + \zeta^5, \\ L(\zeta) &= \zeta + \zeta^2 + \zeta^5, \\ L(\zeta^2) &= \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5, \\ L(\zeta^3) &= \zeta + \zeta^3 + \zeta^4, \\ L(\zeta^4) &= \zeta^5, \\ L(\zeta^5) &= \zeta^2 + \zeta^3 + \zeta^4. \end{aligned}$$

Таким образом, матрица B из (3.16) имеет вид

$$B = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Из указанного выше представления элемента $\alpha = \theta^2$ получаем, что вектор $(d_1, \ldots, d_6)$ из (3.16) равен $(0, 1, 0, 1, 1, 1)$. Теперь нетрудно найти общее решение системы (3.16):

$$(1, 0, 0, 0, 0, 0) + a_1(0, 1, 1, 1, 0, 0) + \\ + a_2(1, 1, 1, 0, 1, 0) + a_3(1, 1, 0, 0, 0, 1),$$

где a_1, a_2, a_3 — произвольные коэффициенты из поля $\mathbb{F}_2$. Итак, корнями аффинного многочлена $A(x)$ в поле $\mathbb{F}_{64}$ являются $\eta_1 = 1$,

$\eta_2 = \zeta + \zeta^5$, $\eta_3 = \zeta + \zeta^2 + \zeta^4$, $\eta_4 = 1 + \zeta^2 + \zeta^4 + \zeta^5$, $\eta_5 = 1 + \zeta + \zeta^2 + \zeta^3$, $\eta_6 = \zeta^2 + \zeta^3 + \zeta^5$, $\eta_7 = \zeta^3 + \zeta^4$, $\eta_8 = 1 + \zeta + \zeta^3 + \zeta^4 + \zeta^5 = 0$. Вычисляя значения $f(\eta_j)$ для $j = 1, \ldots, 8$, получаем окончательно, что корнями многочлена $f(x)$ в поле $\mathbb{F}_{64}$ являются элементы η_3, η_5, η_7 и η_8. □

Рассмотренный метод отыскания корней аффинного многочлена свидетельствует, в частности, о том, что эти корни образуют в векторном пространстве некоторое *аффинное подпространство* (или *линейное многообразие*), т. е. сдвинутое на некоторый вектор подпространство этого векторного пространства. Но это можно получить также и из других соображений вместе с утверждением, касающимся кратности.

3.56. Теорема. *Пусть $A(x)$ — аффинный q-многочлен положительной степени над полем $\mathbb{F}_{q^m}$, и пусть расширение $\mathbb{F}_{q^s}$ поля $\mathbb{F}_{q^m}$ содержит все корни многочлена $A(x)$. Тогда все корни многочлена $A(x)$ имеют одну и ту же кратность, равную единице или некоторой степени числа q. При этом корни многочлена $A(x)$ образуют некоторое аффинное подпространство векторного пространства $\mathbb{F}_{q^s}$ над полем $\mathbb{F}_q$.*

Доказательство. Результат о кратности доказывается так же, как и в теореме 3.50. Теперь пусть $A(x) = L(x) - \alpha$, где $L(x)$ — некоторый q-многочлен над $\mathbb{F}_{q^m}$ и $\alpha \in \mathbb{F}_{q^m}$, и пусть $\beta \in \mathbb{F}_{q^s}$ — некоторый корень многочлена $A(x)$. Тогда элемент $\gamma \in \mathbb{F}_{q^s}$ будет корнем многочлена $A(x)$ в том и только том случае, когда $L(\gamma) = \alpha = L(\beta)$, т. е. тогда и только тогда, когда $L(\gamma - \beta) = 0$. Последнее означает, что $\gamma \in \beta + U$, где U — подпространство пространства $\mathbb{F}_{q^s}$ над $\mathbb{F}_q$, состоящее из всех корней многочлена $L(x)$. Таким образом, корни многочлена $A(x)$ образуют аффинное подпространство векторного пространства $\mathbb{F}_{q^s}$. □

3.57. Теорема. *Пусть T — аффинное подпространство поля $\mathbb{F}_{q^m}$, рассматриваемого как векторное пространство над полем $\mathbb{F}_q$. Тогда для каждого неотрицательного целого числа k многочлен*

$$A(x) = \prod_{\gamma \in T} (x - \gamma)^{q^k}$$

является аффинным q-многочленом над $\mathbb{F}_{q^m}$.

Доказательство. Пусть $T = \eta + U$, где U — подпространство векторного пространства $\mathbb{F}_{q^m}$ и $\eta \in \mathbb{F}_{q^m}$. Тогда

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k}$$

— некоторый q-многочлен над $\mathbb{F}_{q^m}$ (согласно теореме 3.52). Далее,

$$A(x) = \prod_{\gamma \in T} (x - \gamma)^{q^k} = \prod_{\beta \in U} (x - \eta - \beta)^{q^k} = L(x - \eta),$$

и $L(x - \eta)$, как легко видеть, является аффинным q-многочленом над полем $\mathbb{F}_{q^m}$. □

Обычное произведение линеаризованных многочленов не обязательно является линеаризованным многочленом. Однако композиция $L_1(L_2(x))$ двух q-многочленов $L_1(x)$ и $L_2(x)$ над полем $\mathbb{F}_{q^m}$ снова является q-многочленом. Вместо слова «композиция» будем использовать выражение «символическое произведение». Итак, мы определим *символическое умножение* равенством

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

Если рассматриваются лишь q-многочлены над полем $\mathbb{F}_q$, то без труда проверяется, что символическое умножение коммутативно, ассоциативно и дистрибутивно (по отношению к обычному сложению). На самом деле множество q-многочленов над $\mathbb{F}_q$ образует целостное кольцо относительно операций символического умножения и обычного сложения. Но операцию символического умножения можно связать и с обычной арифметикой многочленов с помощью следующего понятия.

3.58. Определение. Многочлены

$$l(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{и} \quad L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

над полем $\mathbb{F}_{q^m}$ называются *q-ассоциированными* друг с другом. При этом $l(x)$ называется просто *q-ассоциированным* с $L(x)$ многочленом, а $L(x)$ — *линеаризованным q-ассоциированным с $l(x)$* многочленом.

3.59. Лемма. *Пусть q-ассоциированными с q-многочленами $L_1(x)$ и $L_2(x)$ над полем $\mathbb{F}_q$ являются соответственно многочлены $l_1(x)$ и $l_2(x)$. Тогда многочлены $l(x) = l_1(x)\, l_2(x)$ и $L(x) = L_1(x) \otimes L_2(x)$ являются q-ассоциированными друг с другом.*

Доказательство. Равенства

$$l(x) = \sum_i a_i x^i = \sum_j b_j x^j \sum_k c_k x^k = l_1(x)\, l_2(x)$$

и

$$L(x) = \sum_i a_i x^{q^i} = \sum_j b_j \Big(\sum_k c_k x^{q^k} \Big)^{q^j} = \sum_j b_j \sum_k c_k x^{q^j + k} =$$

$$= L_1(x) \otimes L_2(x)$$

верны тогда и только тогда, когда в том и другом для каждого i

$$a_i = \sum_{j+k=i} b_j c_k. \qquad \square$$

Если $L_1(x)$ и $L(x)$ являются q-многочленами над $\mathbb{F}_q$, то будем говорить, что многочлен $L_1(x)$ *символически делит* $L(x)$ (или что $L(x)$ *символически делится* на $L_1(x)$), если $L(x) = L_1(x) \otimes L_2(x)$ для некоторого q-многочлена $L_2(x)$ над $\mathbb{F}_q$. Из леммы 3.59 тогда сразу вытекает следующий критерий символической делимости.

3.60. Следствие. *Пусть q-ассоциированными с q-многочленами $L_1(x)$ и $L(x)$ над $\mathbb{F}_q$ являются многочлены $l_1(x)$ и $l(x)$ соответственно. Тогда многочлен $L_1(x)$ символически делит $L(x)$ в том и только том случае, если многочлен $l_1(x)$ делит $l(x)$.*

3.61. Пример. Пусть q-многочлен $L(x)$ над $\mathbb{F}_q$ символически делит многочлен $x^{q^m} - x$, где $m \in \mathbb{N}$. Это значит, что существует такой q-многочлен $L_1(x)$ над $\mathbb{F}_q$, что

$$x^{q^m} - x = L(x) \otimes L_1(x) = L_1(x) \otimes L(x) = L_1(L(x)). \qquad (3.17)$$

Этот факт можно использовать так. Пусть α — фиксированный элемент из поля $\mathbb{F}_{q^m}$. Тогда аффинный многочлен $L(x) - \alpha$ имеет по крайней мере один корень в поле $\mathbb{F}_{q^m}$ в том и только том случае, когда $L_1(\alpha) = 0$, а если $L_1(\alpha) = 0$, то на самом деле все корни многочлена $L(x) - \alpha$ принадлежат полю $\mathbb{F}_{q^m}$. Действительно, если $\beta \in \mathbb{F}_{q^m}$ — некоторый корень многочлена $L(x) - \alpha$, то $L(\beta) = \alpha$, и, подставляя β вместо x в (3.17), получим $L_1(\alpha) = \beta^{q^m} - \beta = 0$. Обратно, если $L_1(\alpha) = 0$ и γ — произвольный корень многочлена $L(x) - \alpha$ в некотором расширении поля $\mathbb{F}_{q^m}$, то $L(\gamma) = \alpha$, и, подставляя γ вместо x в (3.17), получим $\gamma^{q^m} - \gamma = L_1(\alpha) = 0$, так что $\gamma \in \mathbb{F}_{q^m}$. Чтобы найти многочлен $L_1(x)$, сначала находят q-ассоциированный с $L(x)$ многочлен $l(x)$, а затем, полагая $l_1(x) = (x^m - 1)/l(x)$, переходят к линеаризованному q-ассоциированному с $l_1(x)$ многочлену $L_1(x)$. Доказанное предложение в качестве частного случая содержит теорему 2.25. Действительно, если взять в качестве $L(x)$ многочлен $x^q - x$, то оказывается, что $L_1(x) = x + x^q + x^{q^2} + \ldots + x^{q^{m-1}}$. $\square$

Замечателен следующий факт: несмотря на серьезное различие между операциями символического и обычного умножения, понятия делимости для линеаризованных многочленов, основанные на этих разных операциях, оказываются эквивалентными.

3.62. Теорема. *Пусть q-ассоциированными с q-многочленами $L_1(x)$ и $L(x)$ являются многочлены $l_1(x)$ и $l(x)$ соответственно. Тогда следующие свойства эквивалентны:*

(i) *многочлен $L_1(x)$ символически делит $L(x)$;*

(ii) *многочлен* $L_1(x)$ *делит* $L(x)$ *в обычном смысле*;
(iii) *многочлен* $l_1(x)$ *делит* $l(x)$.

Доказательство. Так как эквивалентность (i) и (iii) была установлена следствием 3.60, то достаточно доказать эквивалентность (i) и (ii). Если многочлен $L_1(x)$ символически делит $L(x)$, то

$$L(x) = L_1(x) \otimes L_2(x) = L_2(x) \otimes L_1(x) = L_2(L_1(x))$$

для некоторого q-многочлена $L_2(x)$ над $\mathbb{F}_q$. Пусть

$$L_2(x) = \sum_{i=0}^{n} a_i x^{q^i},$$

тогда

$$L(x) = a_0 L_1(x) + a_1 L_1(x)^q + \cdots + a_n L_1(x)^{q^n},$$

так что $L(x)$ делит $L(x)$ и в обычном смысле. Обратно, допустим, что многочлен $L_1(x)$ делит $L(x)$ в обычном смысле. Тогда можно считать многочлен $L_1(x)$ ненулевым. Применяя алгоритм деления, запишем $l(x) = k(x)\, l_1(x) + r(x)$, где $\deg(r) < \deg(l_1)$, и переходя к линеаризованным q-ассоциированным многочленам (обозначаемым соответствующими большими буквами), получим равенство $L(x) = K(x) \otimes L_1(x) + R(x)$. Согласно уже доказанному, $L_1(x)$ делит символическое произведение $K(x) \otimes L_1(x)$ в обычном смысле, а следовательно, $L_1(x)$ делит и $R(x)$ в обычном смысле. Но так как $\deg(R) < \deg(L_1)$, то $R(x)$ должен быть нулевым многочленом, а это доказывает, что многочлен $L_1(x)$ символически делит $L(x)$. □

Полученный результат можно использовать для установления интересной взаимосвязи между неприводимыми многочленами и неприводимыми делителями линеаризованных q-ассоциированных с ними многочленов.

3.63. Теорема. *Пусть для неприводимого многочлена* $f(x)$ *из* $\mathbb{F}_q[x]$ *линеаризованным* q*-ассоциированным с ним многочленом является* $F(x)$. *Тогда степень каждого неприводимого делителя многочлена* $F(x)/x$ *в* $\mathbb{F}_q[x]$ *равна порядку многочлена* $f(x)$.

Доказательство. Так как случай $f(0) = 0$ тривиален, то будем предполагать, что $f(0) \neq 0$. Положим $e = \operatorname{ord}(f)$, и пусть $h(x) \in \mathbb{F}_q[x]$ — некоторый неприводимый делитель многочлена $F(x)/x$ и $d = \deg(h)$. Тогда многочлен $f(x)$ делит $x^e - 1$, а следовательно (ввиду теоремы 3.62), многочлен $F(x)$ делит $x^{q^e} - x$. Значит, и многочлен $h(x)$ делит $x^{q^e} - x$, а потому в силу теоремы 3.20 число d делит e.

С другой стороны, применяя алгоритм деления, можем написать $x^d - 1 = g(x) f(x) + r(x)$, где $g(x)$, $r(x) \in \mathbb{F}_q[x]$ и

$\deg(r) < \deg(f)$. Переходя к линеаризованным q-ассоциированным с данными многочленам (обозначаемым большими буквами), получим равенство

$$x^{q^d} - x = G(x) \otimes F(x) + R(x),$$

и так как $h(x)$ делит оба многочлена $x^{q^d} - x$ и $G(x) \otimes F(x)$, то $h(x)$ делит и многочлен $R(x)$. Если $r(x)$ — ненулевой многочлен, то он взаимно прост с $f(x)$ ввиду неприводимости последнего, поэтому (см. теорему 1.55) существуют такие многочлены $s(x)$ и $k(x)$ из $\mathbb{F}_q[x]$, что

$$s(x)\, r(x) + k(x)\, f(x) = 1.$$

Обращаясь к линеаризованным q-ассоциированным многочленам, получим соответствующее равенство

$$S(x) \otimes R(x) + K(x) \otimes F(x) = x.$$

Поскольку $h(x)$ делит многочлены $R(x)$ и $F(x)$, то $h(x)$ должен делить и многочлен x, что невозможно. Следовательно, $r(x)$ — нулевой многочлен, так что многочлен $f(x)$ делит $x^d - 1$, и поэтому (по лемме 3.6) число e делит d. Итак, мы доказали, что $d = e$. □

Будем говорить, что q-многочлен $L(x)$ степени, большей 1, над полем $\mathbb{F}_q$ *символически неприводим* над $\mathbb{F}_q$, если в любом его символическом разложении на множители $L(x) = L_1(x) \otimes L_2(x)$, где $L_1(x)$ и $L_2(x)$ суть q-многочлены над $\mathbb{F}_q$, по крайней мере один из сомножителей имеет степень 1. Символически неприводимый многочлен в обычном смысле всегда приводим, так как любой линеаризованный многочлен степени, большей 1, имеет нетривиальный сомножитель x. Применяя лемму 3.59, сразу получаем, что q-многочлен $L(x)$ символически неприводим над $\mathbb{F}_q$ в том и только том случае, когда q-ассоциированный с ним многочлен $l(x)$ неприводим над $\mathbb{F}_q$.

Каждый q-многочлен $L(x)$ степени, большей 1, над $\mathbb{F}_q$ можно *символически разложить* в символическое произведение символически неприводимых многочленов над $\mathbb{F}_q$, причем это разложение по существу однозначно (в том смысле, что все другие такие символические разложения получаются из него перестановкой сомножителей и умножением сомножителей на ненулевые элементы поля $\mathbb{F}_q$). Используя соответствие между линеаризованными многочленами и многочленами, q-ассоциированными с ними, нетрудно видеть, что символическое разложение q-многочлена $L(x)$ над $\mathbb{F}_q$ можно получить, найдя сначала каноническое разложение в $\mathbb{F}_q[x]$ q-ассоциированного с ним многочлена $l(x)$ и затем переходя к соответствующему равенству для линеаризованных q-ассоциированных многочленов.

3.64. Пример. Рассмотрим 2-многочлен $L(x) = x^{16} + x^8 + x^2 + x$ над полем $\mathbb{F}_2$; 2-ассоциированный с ним многочлен $l(x) = x^4 + x^3 + x + 1$ имеет следующее каноническое разложение: $l(x) = (x^2 + x + 1)(x + 1)^2$ в $\mathbb{F}_2[x]$. Поэтому символическим разложением 2-многочлена $L(x)$ на символически неприводимые 2-многочлены над $\mathbb{F}_2$ является

$$L(x) = (x^4 + x^2 + x) \otimes (x^2 + x) \otimes (x^2 + x). \qquad \square$$

Для двух и более q-многочленов над $\mathbb{F}_q$, не равных нулю одновременно, можно определить их *наибольший общий символический делитель* как нормированный q-многочлен над $\mathbb{F}_q$ наивысшей степени, который символически делит все эти многочлены. Чтобы сравнить это понятие с понятием обычного наибольшего общего делителя этих многочленов, заметим сначала, что корнями наибольшего общего делителя заданных q-многочленов являются общие корни всех этих многочленов. Поскольку пересечение подпространств векторного пространства снова является подпространством, то корни наибольшего общего делителя образуют подпространство некоторого расширения $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$ (рассматриваемого как векторное пространство над полем $\mathbb{F}_q$). Далее, применяя к данным q-многочленам первую часть теоремы 3.50, получаем, что все корни наибольшего общего делителя имеют одну и ту же кратность, равную либо единице, либо некоторой степени числа q. Поэтому из теоремы 3.52 следует, что наибольший общий делитель данных q-многочленов сам является q-многочленом. Но тогда из теоремы 3.62 вытекает, что *наибольший общий делитель и наибольший общий символический делитель совпадают*. Эффективным способом нахождения наибольшего общего (символического) делителя данных q-многочленов над $\mathbb{F}_q$ является переход к q-ассоциированным с ними многочленам и нахождение их наибольшего общего делителя; тогда линеаризованный q-ассоциированный с ним многочлен и будет наибольшим общим (символическим) делителем данных q-многочленов.

Согласно теореме 3.50, корни ненулевого q-многочлена над $\mathbb{F}_q$ образуют векторное пространство над $\mathbb{F}_q$. Эти корни обладают еще одним дополнительным свойством: q-е степени этих корней снова являются корнями [1]). Конечномерное векторное пространство M над полем $\mathbb{F}_q$, содержащееся в некотором расширении поля $\mathbb{F}_q$ и обладающее дополнительным свойством, что q-я степень каждого элемента из M снова принадлежит M, назовем *q-модулем*. На основе этого понятия можно установить следующий критерий.

---

[1]) Если $L(x)$ есть q-многочлен над $\mathbb{F}_q$, то $L(x)^q = L(x^q)$, так что если β — корень L, то $L(\beta^q) = 0$. — *Прим. перев.*

3.65. Теорема. *Нормированный многочлен $L(x)$ тогда и только тогда является q-многочленом над полем $\mathbb{F}_q$, когда все его корни имеют одну и ту же кратность, равную единице или некоторой степени числа q, и эти корни образуют q-модуль.*

Доказательство. Необходимость условия вытекает из теоремы 3.50 и сделанных выше замечаний. С другой стороны, из условия теоремы на основании теоремы 3.52 следует, что многочлен $L(x)$ является q-многочленом над некоторым расширением поля $\mathbb{F}_q$. Пусть M — множество корней многочлена $L(x)$. Из условия теоремы получаем, что

$$L(x) = \prod_{\beta \in M} (x - \beta)^{q^k}$$

для некоторого неотрицательного целого числа k. Поскольку M является q-модулем, то $M = \{\beta^q \mid \beta \in M\}$. Отсюда получаем

$$L(x)^q = \prod_{\beta \in M} (x^q - \beta^q)^{q^k} = \prod_{\beta \in M} (x^q - \beta)^{q^k} = L(x^q).$$

Если

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i},$$

то

$$\sum_{i=0}^{n} \alpha_i^q x^{q^{i+1}} = L(x)^q = L(x^q) = \sum_{i=0}^{n} \alpha_i x^{q^{i+1}},$$

так что $\alpha_i^q = \alpha_i$ для $0 \leqslant i \leqslant n$, т. е. $\alpha_i \in \mathbb{F}_q$. Поэтому $L(x)$ является q-многочленом над $\mathbb{F}_q$.

Любой q-многочлен степени q над $\mathbb{F}_q$, очевидно, символически неприводим над $\mathbb{F}_q$. Для q-многочленов степени $>q$ над полем $\mathbb{F}_q$ понятие q-модуля можно использовать для характеризации символически неприводимых многочленов.

3.66. Теорема. *q-многочлен $L(x)$ степени $>q$ над полем $\mathbb{F}_q$ символически неприводим над $\mathbb{F}_q$ тогда и только тогда, когда он имеет простые корни и эти корни образуют q-модуль M, не содержащий других q-модулей, кроме $\{0\}$ и самого M.*

Доказательство. Допустим, что многочлен $L(x)$ символически неприводим над $\mathbb{F}_q$. Если бы он имел кратные корни, то в соответствии с теоремой 3.65 его можно было бы записать в виде $L(x) = L_1(x)^q$, где $L_1(x)$ — некоторый q-многочлен над $\mathbb{F}_q$ степени, большей 1. Но тогда $L(x) = x^q \otimes L_1(x)$, что противоречит символической неприводимости $L(x)$. Таким образом, $L(x)$ имеет лишь

простые корни. Пусть теперь N — некоторый q-модуль, содержащийся в M. Тогда из теоремы 3.65 получаем, что $L_2(x) = \prod_{\beta \in N} (x - \beta)$ — некоторый q-многочлен над $\mathbb{F}_q$. Поскольку многочлен $L_2(x)$ делит $L(x)$ в обычном смысле, то, согласно теореме 3.62, он и символически делит $L(x)$. Но так как многочлен $L(x)$ символически неприводим над $\mathbb{F}_q$, то степень $\deg(L_2)$ должна быть равна либо 1, либо $\deg(L)$, а это означает, что q-модуль N либо совпадает с $\{0\}$, либо с M.

Чтобы доказать достаточность условия теоремы, предположим, что $L(x) = L_1(x) \otimes L_2(x)$ — символическое разложение $L(x)$, где $L_1(x)$ и $L_2(x)$ — некоторые q-многочлены над $\mathbb{F}_q$. Тогда многочлен $L_1(x)$ символически делит $L(x)$, а значит, согласно теореме 3.62, он делит $L(x)$ и в обычном смысле. Следовательно, корни многочлена $L_1(x)$ просты и q-модуль N, образованный этими корнями, содержится в M. Поэтому N совпадает либо с $\{0\}$, либо с M, $\deg(L_1)$ равна либо 1, либо $\deg(L)$. Значит, один из многочленов $L_1(x)$ или $L_2(x)$ имеет степень 1, а это означает, что многочлен $L(x)$ символически неприводим над $\mathbb{F}_q$. □

3.67. Определение. Пусть $L(x)$ — ненулевой q-многочлен над полем $\mathbb{F}_{q^m}$. Корень ζ этого многочлена называется *q-первообразным корнем над* $\mathbb{F}_{q^m}$, если он не является корнем никакого ненулевого q-многочлена над $\mathbb{F}_{q^m}$ более низкой степени.

К этому понятию можно подойти также с другой точки зрения. Пусть $g(x)$ — минимальный многочлен элемента ζ над полем $\mathbb{F}_{q^m}$. Нетрудно видеть, что ζ является q-первообразным корнем многочлена $L(x)$ над $\mathbb{F}_{q^m}$ тогда и только тогда, когда многочлен $g(x)$ делит $L(x)$, но не делит никакого ненулевого q-многочлена более низкой степени.

Для заданного элемента ζ из какого-либо конечного расширения поля $\mathbb{F}_{q^m}$ всегда можно найти ненулевой q-многочлен над $\mathbb{F}_{q^m}$, для которого ζ является q-первообразным корнем над $\mathbb{F}_{q^m}$. Чтобы убедиться в этом, мы поступим так же, как и при построении аффинного кратного. Пусть $g(x)$ — минимальный многочлен элемента ζ над $\mathbb{F}_{q^m}$, и пусть $\deg(g) = n$. Найдем для каждого $i = 0, 1, \ldots, n$ однозначно определенный многочлен $r_i(x)$ степени $\deg(r_i) \leqslant n - 1$, такой что $x^{q^i} \equiv r_i(x) \pmod{g(x)}$. Затем найдем элементы $\alpha_i \in \mathbb{F}_{q^m}$, не равные нулю одновременно, для которых $\sum_{i=0}^{n} \alpha_i r_i(x) = 0$. С этой целью приравняем нулю коэффициенты при всех степенях x^j, $0 \leqslant j \leqslant n - 1$, и получим n условий, представляющих собой однородную систему из n линейных уравнений относительно $n + 1$ неизвестных

$\alpha_0, \alpha_1, \ldots, \alpha_n$. Такая система всегда имеет нетривиальное решение, и для любого такого решения $(\alpha_0, \alpha_1, \ldots, \alpha_n)$

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n} \alpha_i r_i(x) \equiv 0 \pmod{g(x)},$$

а это значит, что $L(x)$ — ненулевой q-многочлен над $\mathbb{F}_{q^m}$, делящийся на $g(x)$. Выбрав α_i так, чтобы многочлен $L(x)$ оказался нормированным многочленом наименьшей возможной степени, мы убедимся, что ζ является q-первообразным корнем многочлена $L(x)$ над $\mathbb{F}_{q^m}$. Легко видеть, что этот нормированный q-многочлен $L(x)$ над $\mathbb{F}_{q^m}$ наименьшей положительной степени, который делится на $g(x)$, определяется однозначно; он называется *минимальным q-многочленом* элемента ζ над $\mathbb{F}_{q^m}$.

3.68. Теорема. *Пусть ζ — элемент из некоторого конечного расширения поля $\mathbb{F}_{q^m}$, и пусть $M(x)$ — его минимальный q-многочлен над $\mathbb{F}_{q^m}$. Для того чтобы элемент ζ был корнем q-многочлена $K(x)$ над $\mathbb{F}_{q^m}$, необходимо и достаточно, чтобы $K(x) = L(x) \otimes M(x)$ для некоторого q-многочлена $L(x)$ над $\mathbb{F}_{q^m}$. В частности, при $m = 1$ это означает, что элемент ζ является корнем q-многочлена $K(x)$ над $\mathbb{F}_{q^m}$ в том и только том случае, если $K(x)$ символически делится на $M(x)$.*

Доказательство. Если $K(x) = L(x) \otimes M(x) = L(M(x))$, то сразу получаем, что $K(\zeta) = 0$. Обратно, пусть

$$M(x) = \sum_{j=0}^{t} \gamma_j x^{q^j}, \quad \text{где} \quad \gamma_t = 1, \quad \gamma_j \in \mathbb{F}_{q^m},$$

и допустим, что элемент ζ является корнем q-многочлена

$$K(x) = \sum_{k=0}^{r} \alpha_k x^{q^k}, \quad \text{где} \quad r \geqslant t, \quad \alpha_k \in \mathbb{F}_{q^m}.$$

Полагая $s = r - t$ и $\gamma_j = 0$ для $j < 0$, рассмотрим систему из $s + 1$ линейных уравнений относительно $s + 1$ неизвестных $\beta_0, \beta_1, \ldots, \beta_s$:

$$\begin{aligned}
\beta_0 + \gamma_{t-1}^{q}\beta_1 + \gamma_{t-2}^{q^2}\beta_2 + \cdots + \gamma_{t-s}^{q^s}\beta_s &= \alpha_t,\\
\beta_1 + \gamma_{t-1}^{q}\beta_2 + \cdots + \gamma_{t-s+1}^{q^s}\beta_s &= \alpha_{t+1},\\
&\cdots\cdots\cdots\cdots\\
\beta_{s-1} + \gamma_{t-1}^{q^s}\beta_s &= \alpha_{r-1},\\
\beta_s &= \alpha_r.
\end{aligned}$$

Ясно, что эта система имеет единственное решение $(\beta_0, \beta_1, \ldots, \beta_s)$, где $\beta_i \in \mathbb{F}_{q^m}$, $0 \leqslant i \leqslant s$. Введем многочлены

$$L(x) = \sum_{i=0}^{s} \beta_i x^{q^i} \quad \text{и} \quad R(x) = K(x) - L(M(x)).$$

Имеем

$$\begin{aligned} R(x) &= \sum_{k=0}^{r} \alpha_k x^{q^k} - \sum_{i=0}^{s} \beta_i \left(\sum_{j=0}^{t} \gamma_j x^{q^j} \right)^{q^i} = \\ &= \sum_{k=0}^{r} \alpha_k x^{q^k} - \sum_{i=0}^{s} \beta_i \sum_{j=0}^{t} \gamma_j^{q^i} x^{q^{i+j}} = \\ &= \sum_{k=0}^{r} \alpha_k x^{q^k} - \sum_{k=0}^{r} \left(\sum_{i=0}^{s} \gamma_{k-i}^{q^i} \beta_i \right) x^{q^k} = \\ &= \sum_{k=0}^{r} \left(\alpha_k - \sum_{i=0}^{s} \gamma_{k-i}^{q^i} \beta_i \right) x^{q^k}. \end{aligned}$$

В силу выбора элементов β_i многочлен $R(x)$ имеет степень $< q^t$. Но так как $R(\zeta) = K(\zeta) - L(M(\zeta)) = 0$, то из определения многочлена $M(x)$ вытекает, что $R(x)$ — нулевой многочлен. Следовательно, $K(x) = L(M(x)) = L(x) \otimes M(x)$. □

Обозначим теперь через N_L число q-первообразных над $\mathbb{F}_q$ корней ненулевого q-многочлена $L(x)$ над $\mathbb{F}_q$. Рассмотрим задачу нахождения N_L. Если q-многочлен $L(x)$ имеет кратные корни, то по теореме 3.65 можно написать $L(x) = L_1(x)^q$, где $L_1(x)$ — некоторый q-многочлен над $\mathbb{F}_q$. Так как каждый корень многочлена $L(x)$ является в то же время и корнем многочлена $L_1(x)$, то $N_L = 0$. Таким образом, можно предположить, что многочлен $L(x)$ имеет лишь простые корни. Если $\deg(L(x)) = 1$, то, очевидно, $N_L = 1$. Если же $L(x)$ — многочлен степени $q^n > 1$ и, кроме того, нормирован (это предположение не ограничивает общности), то пусть

$$L(x) = \underbrace{L_1(x) \otimes \ldots \otimes L_1(x)}_{e_1} \otimes \ldots \otimes \underbrace{L_r(x) \otimes \ldots \otimes L_r(x)}_{e_r}$$

— символическое разложение $L(x)$ в символическое произведение различных нормированных символически неприводимых q-многочленов $L_1(x), \ldots, L_r(x)$ над $\mathbb{F}_q$. Мы получим число N_L, вычитая из полного числа q^n корней многочлена $L(x)$ число таких корней этого многочлена, которые в то же время являются корнями каких-либо ненулевых q-многочленов над $\mathbb{F}_q$ степени, меньшей чем q^n. Если ζ — один из таких корней многочлена $L(x)$ и $M(x)$ — его минимальный q-многочлен над $\mathbb{F}_q$, то $\deg(M(x)) < q^n$, так что по теореме 3.68 многочлен $M(x)$ символически делит

$L(x)$. Отсюда следует, что $M(x)$ символически делит один из таких многочленов $K_i(x)$, $1 \leqslant i \leqslant r$, который получается из символического разложения $L(x)$ исключением одного символического сомножителя $L_i(x)$, и тогда, согласно теореме 3.68, $K_i(\zeta) = 0$. Поскольку каждый корень многочлена $K_i(x)$ является в то же время и корнем многочлена $L(x)$, мы видим, что число N_L получается вычитанием из q^n числа элементов ζ, которые являются корнями каких-либо многочленов $K_i(x)$. Если степень многочлена $L_i(x)$ равна q^{n_i}, то степень (а значит, и число корней) многочлена $K_i(x)$ равна q^{n-n_i}. Если при $s < r$ индексы $i_1, \ldots, i_s$ различны, $1 \leqslant i_j \leqslant r$, то число общих корней многочленов $K_{i_1}(x), \ldots, K_{i_s}(x)$ равно степени их наибольшего общего делителя, которая совпадает со степенью их наибольшего общего символического делителя (см. рассуждение после примера 3.64). Используя символические разложения, находим, что эта степень равна

$$q^{n-n_{i_1}-\ldots-n_{i_s}}.$$

Применяя теперь комбинаторный принцип включения-исключения, получаем окончательно, что

$$N_L = q^n - \sum_{i=1}^{r} q^{n-n_i} + \sum_{1 \leqslant i < j \leqslant r} q^{n-n_i-n_j} - \ldots + (-1)^r q^{n-n_1-\ldots-n_r} =$$
$$= q^n (1 - q^{-n_1}) \ldots (1 - q^{-n_r}).$$

Это выражение можно интерпретировать и иначе. Пусть $l(x)$ есть q-ассоциированный с $L(x)$ многочлен. Тогда

$$l(x) = l_1(x)^{e_1} \ldots l_r(x)^{e_r}$$

— каноническое разложение многочлена $l(x)$ в кольце $\mathbb{F}_q[x]$, где $l_i(x)$ есть q-ассоциированный с $L_i(x)$ многочлен, $1 \leqslant i \leqslant r$. Определим аналог функции Эйлера φ (см. упр. 1.4) для ненулевого многочлена $f(x) \in \mathbb{F}_q[x]$, обозначая через $\Phi_q(f(x)) = \Phi_q(f)$ число взаимно простых с $f(x)$ многочленов степени, меньшей $\deg(f)$, из $\mathbb{F}_q[x]$. Тогда из следующего результата вытекает, что $N_L = \Phi_q(l(x))$.

3.69. Лемма. *Функция $\Phi_q(f)$, определенная выше для ненулевых многочленов $f \in \mathbb{F}_q[x]$, обладает следующими свойствами:*

(i) $\Phi_q(f) = 1$, *если* $\deg(f) = 0$;

(ii) $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$, *если* НОД$(f, g) = 1$;

(iii) *если* $\deg(f) = n > 1$, *то*

$$\Phi_q(f) = q^n (1 - q^{-n_1}) \ldots (1 - q^{-n_r}),$$

где $n_1, \ldots, n_r$ — степени различных нормированных неприводимых сомножителей из канонического разложения многочлена f в $\mathbb{F}_q[x]$.

Доказательство. Свойство (i) тривиально. Перейдем к свойству (ii). Положим $\Phi_q(f) = s$ и $\Phi_q(g) = t$, и пусть $f_1, \ldots, f_s$ (соответственно $g_1, \ldots, g_t$) — все многочлены из $\mathbb{F}_q[x]$, взаимно простые с f (соответственно с g), степени которых меньше $\deg(f)$ (соответственно $\deg(g)$). Если $h \in \mathbb{F}_q[x]$ — многочлен степени, меньшей чем $\deg(fg)$, взаимно простой с произведением fg, то он взаимно прост также и с каждым из многочленов f и g. Поэтому найдутся однозначно определенные числа i и j, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant t$, такие, что $h \equiv f_i \pmod f$ и $h \equiv g_j \pmod g$. С другой стороны, согласно китайской теореме об остатках для кольца $\mathbb{F}_q[x]$ (см. упр. 1.37), для каждой упорядоченной пары (i, j), $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant t$, существует однозначно определенный многочлен $h(x) \in \mathbb{F}_q[x]$ степени $\deg(h) < \deg(fg)$, обладающий свойством $h \equiv f_i \pmod f$, $h \equiv g_j \pmod g$. Отсюда следует, что $h(x)$ взаимно прост с каждым из многочленов $f(x)$ и $g(x)$, а значит, и с их произведением $f(x)\,g(x)$. Поэтому существует взаимно однозначное соответствие между st упорядоченными парами (i, j) и многочленами $h(x) \in \mathbb{F}_q[x]$, такими, что $\deg(h) < \deg(fg)$ и НОД $(h, fg) = 1$. Следовательно, $\Phi_q(fg) = st = \Phi_q(f)\,\Phi_q(g)$.

Для натурального числа e и неприводимого многочлена $b \in \mathbb{F}_q[x]$ степени m число $\Phi_q(b^e)$ можно подсчитать непосредственно. Если многочлен $h \in \mathbb{F}_q[x]$ степени, меньшей чем $\deg(b^e) = me$, не взаимно прост с b^e, то он делится на b и потому имеет вид $h = bg$, где $\deg(g) < em - m$. Такой многочлен g в $\mathbb{F}_q[x]$ можно выбрать q^{em-m} различными способами. Отсюда вытекает, что $\Phi_q(b^e) = q^{em} - q^{em-m} = q^{em}(1 - q^{-m})$. Свойство (iii) теперь следует из (ii). □

3.70. Теорема. *Пусть $L(x)$ — ненулевой q-многочлен над $\mathbb{F}_q$ и $l(x)$ есть q-ассоциированный с ним многочлен. Тогда число N_L q-первообразных над $\mathbb{F}_q$ корней многочлена $L(x)$ равно 0, если $L(x)$ имеет кратные корни, и равно $\Phi_q(l(x))$, если $L(x)$ имеет простые корни.*

Доказательство. Утверждение теоремы вытекает из леммы 3.69 и предшествующего ей рассуждения. □

3.71. Следствие. *Каждый ненулевой q-многочлен над $\mathbb{F}_q$ с простыми корнями имеет хотя бы один q-первообразный над $\mathbb{F}_q$ корень.*

Выше было введено понятие q-модуля. Полученные результаты о q-первообразных корнях можно использовать для построения особого типа базиса для q-модуля.

3.72. Теорема. *Для q-модуля M размерности $m \geqslant 1$ над $\mathbb{F}_q$ существует такой элемент $\zeta \in M$, что $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ — базис M над $\mathbb{F}_q$.*

Доказательство. Согласно теореме 3.65, $L(x) = \prod_{\beta \in M} (x - \beta)$ является q-многочленом над $\mathbb{F}_q$. В силу следствия 3.71 этот многочлен имеет q-первообразный корень ζ над $\mathbb{F}_q$. Поэтому ζ, ζ^q, ζ^{q^2}, ..., $\zeta^{q^{m-1}}$ являются элементами q-модуля M. Если бы они были линейно зависимыми над $\mathbb{F}_q$, то элемент ζ был бы корнем некоторого ненулевого q-многочлена над $\mathbb{F}_q$ степени $< \deg(L(x)) = q^m$, что противоречит определению q-первообразного над $\mathbb{F}_q$ корня многочлена $L(x)$. Поэтому указанные выше m элементов линейно независимы над $\mathbb{F}_q$ и, следовательно, образуют базис q-модуля M над $\mathbb{F}_q$. □

3.73. Теорема. *В поле $\mathbb{F}_{q^m}$ имеется ровно $\Phi_q(x^m - 1)$ различных элементов ζ, для которых $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ является базисом $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$.*

Доказательство. Так как поле $\mathbb{F}_{q^m}$ можно рассматривать как q-модуль, то доказательство получается применением теоремы 3.72. Здесь в силу леммы 2.4

$$L(x) = \prod_{\beta \in \mathbb{F}_{q^m}} (x - \beta) = x^{q^m} - x,$$

и каждому q-первообразному над $\mathbb{F}_q$ корню ζ многочлена $L(x)$ соответствует базис указанного вида. С другой стороны, если элемент $\zeta \in \mathbb{F}_{q^m}$ не является q-первообразным над $\mathbb{F}_q$ корнем многочлена $L(x)$, то элементы ζ, ζ^q, ζ^{q^2}, ..., $\zeta^{q^{m-1}}$ линейно зависимы над $\mathbb{F}_q$ и, следовательно, не образуют базис в $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Значит, число элементов $\zeta \in \mathbb{F}_{q^m}$, для которых $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ является базисом $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$, совпадает с числом q-первообразных корней над $\mathbb{F}_q$ многочлена $L(x)$, которое в силу теоремы 3.70 равно $\Phi_q(x^m - 1)$. □

Этот результат придает определенную законченность теореме о нормальном базисе (ср. с определением 2.32 и теоремой 2.35). Поскольку каждый из элементов ζ, ζ^q, ζ^{q^2}, ..., $\zeta^{q^{m-1}}$ порождает один и тот же нормальный базис $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$, то число различных нормальных базисов $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ равно $(1/m)\,\Phi_q(x^m - 1)$.

3.74. Пример. Подсчитаем число различных нормальных базисов поля $\mathbb{F}_{64}$ над $\mathbb{F}_2$. Так как $64 = 2^6$, то это число равно $(1/6)\,\Phi_2(x^6 - 1)$. Из канонического разложения многочлена $x^6 - 1$ в кольце $\mathbb{F}_2[x]$

$$x^6 - 1 = (x + 1)^2 (x^2 + x + 1)^2$$

и леммы 3.69 (iii) получаем, что

$$\Phi_2(x^6 - 1) = 2^6 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{4}\right) = 24.$$

Следовательно, существуют четыре различных нормальных базиса $\mathbb{F}_{64}$ над $\mathbb{F}_2$. □

§ 5. Двучлены и трехчлены

Двучленом (*биномом*) называется многочлен, состоящий из двух ненулевых членов, одним из которых является постоянный член. Неприводимость двучлена можно охарактеризовать в явном виде. Для этого достаточно рассмотреть лишь нормированные нелинейные двучлены.

3.75. Теорема. *Для натурального числа $t \geqslant 2$ и $a \in \mathbb{F}_q^*$ двучлен $x^t - a$ неприводим над полем $\mathbb{F}_q$ тогда и только тогда, когда выполнены следующие два условия:*

(i) *каждый простой делитель числа t делит порядок e элемента a в группе $\mathbb{F}_q^*$, но не делит число $(q-1)/e$;*

(ii) *если t кратно четырем, то $q \equiv 1 \pmod 4$.*

Доказательство. Пусть условия (i) и (ii) выполнены. Тогда на основании теоремы 3.35 из неприводимости в $\mathbb{F}_q[x]$ линейного многочлена $f(x) = x - a$ порядка e следует неприводимость многочлена $f(x^t) = x^t - a$ в $\mathbb{F}_q[x]$.

Допустим, что условие (i) нарушено. Тогда существует простой делитель r числа t, который либо делит число $(q-1)/e$, либо не делит число e. В первом случае $(q-1)/e = rs$ для некоторого $s \in \mathbb{N}$. Подгруппа группы $\mathbb{F}_q^*$, состоящая из r-х степеней элементов этой группы, имеет порядок $(q-1)/r = es$ и потому содержит подгруппу порядка e группы $\mathbb{F}_q^*$, которая порождается элементом a. Это, в частности, означает, что $a = b^r$ для некоторого $b \in \mathbb{F}_q^*$, а отсюда следует, что двучлен $x^t - a = x^{t_1 r} - b^r$ имеет нетривиальный делитель $x^{t_1} - b$. Остается случай, когда простой делитель r числа t не делит ни $(q-1)/e$, ни e, а значит, не делит и числа $q-1$. В таком случае существует такое натуральное число r_1, что $r_1 r \equiv 1 \pmod{(q-1)}$, и, следовательно, двучлен $x^t - a = x^{t_1 r} - a^{r_1 r}$ имеет делитель $x^{t_1} - a^{r_1}$.

Теперь допустим, что условие (i) выполнено, но (ii) нарушено. Тогда $t = 4t_2$ для некоторого $t_2 \in \mathbb{N}$ и $q \not\equiv 1 \pmod 4$. Но из (i) следует, что число e четно, а так как e делит $q-1$, то q должно быть нечетным. Значит, $q \equiv 3 \pmod 4$, и из теоремы 3.37 следует, что многочлен $x^t - a$ приводим в кольце $\mathbb{F}_q[x]$. Но это можно доказать и непосредственно. Заметим сначала, что из условий на e и q следует, что $e \equiv 2 \pmod 4$. Более того, $a^{e/2} = -1$, так что $x^t - a = x^t + a^{(e/2)+1} = x^t + a^d$, где $d = (e/2) + 1$ четно. Далее,

$$a^d = 4(2^{-1}a^{d/2})^2 = 4(2^{-1}a^{d/2})^{q+1} = 4c^4,$$

где $c = (2^{-1}a^{d/2})^{(q+1)/4}$, а это приводит к разложению

$$x^t - a = x^{4t_2} + 4c^4 =$$

$$= (x^{2t_2} + 2cx^{t_2} + 2c^2)(x^{2t_2} - 2cx^{t_2} + 2c^2). \quad \square$$

Если $q \equiv 3 \pmod 4$, то мы можем записать q в виде $q = 2^A u - 1$, где $A \geqslant 2$ и u нечетно. Допустим, что условие (i) из теоремы 3.75 выполнено и число t делится на 2^A. Запишем $t = Bv$, где $B = 2^{A-1}$ и v четно. Тогда число k из теоремы 3.37 равно A и при $f(x) = x - a$ многочлен $f(x^t) = x^t - a$ разлагается в произведение B нормированных неприводимых многочленов из $\mathbb{F}_q[x]$ степени $t/B = v$. Эти неприводимые многочлены можно найти в явном виде. Заметим, что, как и в последней части доказательства теоремы 3.75, число $d = (e/2) + 1$ четно. Поскольку НОД $(2B, q - 1) = 2$, то существует число $r \in \mathbb{N}$, такое, что $2Br \equiv d \pmod{(q-1)}$. Полагая $b = a^r \in \mathbb{F}_q$, мы получим следующее каноническое разложение.

3.76. Теорема. *Пусть a — отличный от нуля элемент конечного поля $\mathbb{F}_q$, $q = 2^A u - 1$, где A — целое число, $A \geqslant 2$, и u нечетно. Пусть e — порядок элемента a в группе $\mathbb{F}_q^*$ и для натурального числа t, кратного $2^A = 2B$, выполнено условие* (i) *теоремы* 3.75. *Тогда двучлен $x^t - a$ разлагается в произведение B нормированных неприводимых сомножителей степени $v = t/B$:*

$$x^t - a = \prod_{j=1}^{B} (x^v - bc_j x^{v/2} - b^2),$$

где $b = a^r$, $2Br \equiv e/2 + 1 \pmod{(q-1)}$, а элементы $c_1, \ldots, c_B$ — корни многочлена

$$F(x) = \sum_{i=0}^{B/2} \frac{(B-i-1)!\,B}{i!\,(B-2i)!} x^{B-2i} \in \mathbb{F}_q[x],$$

при этом все c_j лежат в $\mathbb{F}_q$, $1 \leqslant j \leqslant B$.

Доказательство. Для ненулевого элемента γ из некоторого расширения поля $\mathbb{F}_q$

$$(x - \gamma)(x + \gamma^{-1}) = x^2 - \beta x - 1, \quad \text{где } \beta = \gamma - \gamma^{-1}.$$

Применяя утверждение и обозначения формулы Варинга (см. теорему 1.76), получаем

$$s_B(x_1, x_2) = x_1^B + x_2^B =$$

$$= \sum_{\substack{i_1+2i_2=B \\ i_1>0,\ i_2>0}} (-1)^{i_2} \frac{(i_1+i_2-1)!\,B}{i_1!\,i_2!} \sigma_1(x_1, x_2)^{i_1} \sigma_2(x_1, x_2)^{i_2} =$$

$$= \sum_{i_2=0}^{B/2} (-1)^{i_2} \frac{(B-i_2-1)!\,B}{(B-2i_2)!\,i_2!} (x_1+x_2)^{B-2i_2} (x_1x_2)^{i_2}.$$

Полагая $x_1 = \gamma$, $x_2 = -\gamma^{-1}$, получаем

$$\gamma^B + \gamma^{-B} = \sum_{i=0}^{B/2} (-1)^i \frac{(B-i-1)!\,B}{i!\,(B-2i)!} \beta^{B-2i} (-1)^i = F(\beta).$$

Если c_j — корень многочлена $F(x)$ из некоторого расширения поля $\mathbb{F}_q$ и γ_j — корень квадратного трехчлена $x^2 - c_j x - 1$ из некоторого расширения поля $\mathbb{F}_q$, то $\gamma_j - \gamma_j^{-1} = c_j$, так что $\gamma_j^B + \gamma_j^{-B} = F(c_j) = 0$, поэтому $\gamma_j^{2B} = -1$. Так как $q+1 = 2Bu$, где u нечетно, то $\gamma_j^{q+1} = (-1)^u = -1$, откуда $\gamma_j^q = -\gamma_j^{-1}$. Тогда

$$c_j^q = (\gamma_j - \gamma_j^{-1})^q = \gamma_j^q - \gamma_j^{-q} = -\gamma_j^{-1} + \gamma_j = c_j,$$

так что $c_j \in \mathbb{F}_q$.

Так как $F(x)$ — нормированный многочлен, то

$$F(x) = \prod_{j=1}^{B} (x - c_j),$$

откуда

$$\gamma^B + \gamma^{-B} = F(\beta) = \prod_{j=1}^{B} (\beta - c_j) = \prod_{j=1}^{B} (\gamma - \gamma^{-1} - c_j).$$

Это означает, что

$$\gamma^{2B} + 1 = \prod_{j=1}^{B} (\gamma^2 - c_j\gamma - 1).$$

Поскольку это равенство справедливо для любого элемента γ из любого расширения поля $\mathbb{F}_q$ (в том числе и для $\gamma = 0$), мы получаем полиномиальное равенство

$$x^{2B} + 1 = \prod_{j=1}^{B} (x^2 - c_j x - 1).$$

Подставляя в него $b^{-1}x^{v/2}$ вместо x и умножая на b^{2B}, получаем (полагая $d = (e/2) + 1$) разложение многочлена

$$x^{Bv} + b^{2B} = x^t + a^{2Br} = x^t + a^d = x^t - a$$

(ср. с заключительной частью доказательства теоремы 3.75). Полученные сомножители неприводимы в $\mathbb{F}_q[x]$, поскольку нам уже известно, что на основании теоремы 3.37 каноническое разложение двучлена $x^t - a$ содержит B неприводимых многочленов из $\mathbb{F}_q[x]$ степени v (см. рассуждение, предшествующее теореме 3.76). □

3.77. **Пример.** Разложим двучлен $x^{24} - 3$ в кольце $\mathbb{F}_7[x]$. Здесь $q = 2^3 - 1$, так что $A = 3$, $B = 4$ и $v = 6$. Кроме того, элемент $a = 3$ имеет в группе $\mathbb{F}_7^*$ порядок $e = 6$, так что условие (i) теоремы 3.75 выполнено и можно применить теорему 3.76. Имеем $d = 4$ и, решая сравнение $8r \equiv 4 \pmod 6$, получаем $r = 2$. Поэтому $b = a^2 = 2$. Далее, многочлен $F(x) = x^4 + 4x^2 + 2$ имеет в поле $\mathbb{F}_7$ корни ± 1 и ± 3. Таким образом, получаем каноническое разложение многочлена $x^{24} - 3$ в кольце $\mathbb{F}_7[x]$:

$$x^{24} - 3 = (x^6 - 2x^3 - 4)(x^6 + 2x^3 - 4)(x^6 - x^3 - 4)(x^6 + x^3 - 4). \quad \square$$

Трехчленом называется многочлен из трех ненулевых членов, одним из которых является постоянный член. Сначала мы рассмотрим такие трехчлены, которые являются аффинными миогочленами.

3.78. **Теорема.** *Пусть a — ненулевой элемент конечного поля $\mathbb{F}_q$ характеристики p. Трехчлен $x^p - x - a$ неприводим в $\mathbb{F}_q[x]$ тогда и только тогда, когда он не имеет корней в поле $\mathbb{F}_q$.*

Доказательство. Если β — какой-либо корень многочлена $x^p - x - a$ в некотором расширении поля $\mathbb{F}_q$, то, согласно доказательству теоремы 3.56, множеством корней многочлена $x^p - x - a$ является $\beta + U$, где U — множество корней линеаризованного многочлена (p-многочлена) $x^p - x$. Но нам известно, что $U = \mathbb{F}_p$, так что

$$x^p - x - a = \prod_{b \in \mathbb{F}_p} (x - \beta - b).$$

Допустим теперь, что трехчлен $x^p - x - a$ имеет делитель $g \in \mathbb{F}_q[x]$, где $1 \leqslant r = \deg(g) < p$ и g — нормированный многочлен. Тогда

$$g(x) = \prod_{i=1}^{r} (x - \beta - b_i)$$

для некоторых $b_i \in \mathbb{F}_p$. Сравнивая коэффициенты при x^{r-1}, получаем, что $r\beta + b_1 + \ldots + b_r$ — элемент из поля $\mathbb{F}_q$. Поскольку число r как элемент поля $\mathbb{F}_q$ имеет мультипликативный обратный элемент в этом поле, то $\beta \in \mathbb{F}_q$. Итак, мы показали, что если трехчлен $x^p - x - a$ нетривиально разлагается в кольце $\mathbb{F}_q[x]$, то он имеет корень в поле $\mathbb{F}_q$. Обратное же утверждение тривиально.

3.79. **Следствие.** *В обозначениях теоремы* 3.78 *трехчлен $x^p - x - a$ неприводим в кольце $\mathbb{F}_q[x]$ тогда и только тогда, когда* $\mathrm{Tr}_{\mathbb{F}_q}(a) \neq 0$.

Доказательство. По теореме 2.25 многочлен $x^p - x - a$ тогда и только тогда имеет корень в поле $\mathbb{F}_q$, когда абсолютный след $\mathrm{Tr}_{\mathbb{F}_q}(a)$ равен нулю. Остальное вытекает из теоремы 3.78. □

Поскольку для любого $b \in \mathbb{F}_q^*$ многочлен $f(x)$ неприводим над полем $\mathbb{F}_q$ тогда и только тогда, когда неприводим над $\mathbb{F}_q$ многочлен $f(bx)$, то приведенный выше критерий сохраняет силу также и для трехчленов вида $b^p x^p - bx - a$.

Что же касается более общих трехчленов подобного вида, степенью которых является не характеристика p исходного поля, а некоторая ее степень p^n, $n > 1$, то найденные выше критерии для них уже недействительны. Однако в этом случае может быть установлена следующая формула разложения.

3.80. Теорема. *Пусть $\mathbb{F}_q = F$ — конечное поле и $\mathbb{F}_r = K$ — его собственное подполе. Если $a \in \mathbb{F}_r = K$, то трехчлен $x^q - x - a$ имеет следующее разложение в кольце $\mathbb{F}_q[x]$:*

$$x^q - x - a = \prod_{j=1}^{q/r} (x^r - x - \beta_j), \tag{3.18}$$

где β_j — различные элементы поля $\mathbb{F}_q$, для которых $\mathrm{Tr}_{F/K}(\beta_j) = a$.

Доказательство. Пусть $\beta_j \in \mathbb{F}_q$ — элемент, указанный в теореме, и пусть γ — корень трехчлена $x^r - x - \beta_i$ из некоторого расширения поля $\mathbb{F}_q$. Тогда $\gamma^r - \gamma = \beta_j$, так что

$$a = \mathrm{Tr}_{F/K}(\beta_j) = \mathrm{Tr}_{F/K}(\gamma^r - \gamma) =$$
$$= (\gamma^r - \gamma) + (\gamma^r - \gamma)^r + (\gamma^r - \gamma)^{r^2} + \ldots + (\gamma^r - \gamma)^{q/r} = \gamma^q - \gamma,$$

т. е. элемент γ является корнем трехчлена $x^q - x - a$. Поскольку многочлен $x^r - x - \beta_j$ имеет лишь простые корни, то $x^r - x - \beta_j$ делит трехчлен $x^q - x - a$. А так как все трехчлены $x^r - x - \beta_j$, $j = 1, \ldots, q/r$, попарно взаимно просты, то их произведение делит многочлен $x^q - x - a$. Сравнение степеней и старших коэффициентов многочленов в обеих частях формулы (3.18) показывает, что эти многочлены совпадают. □

3.81. Пример. Пусть $x^9 - x - 1$ — трехчлен из $\mathbb{F}_9[x]$. Рассматривая поле $\mathbb{F}_9$ как $\mathbb{F}_3(\alpha)$, где α — корень неприводимого многочлена $x^2 - x - 1 \in \mathbb{F}_3[x]$, получим, что элементами поля $\mathbb{F}_9$, имеющими абсолютный след, равный 1, являются элементы -1, α и $1 - \alpha$. Поэтому формула (3.18) приводит к следующему разложению:

$$x^9 - x - 1 = (x^3 - x + 1)(x^3 - x - \alpha)(x^3 - x - 1 + \alpha).$$

Так как все три сомножителя неприводимы в кольце $\mathbb{F}_9[x]$, то мы одновременно получили и каноническое разложение трехчлена $x^9 - x - 1$ в $\mathbb{F}_9[x]$. □

Наши познания о неприводимых трехчленах можно теперь применить для того, чтобы, исходя из данных неприводимых многочленов, строить новые.

3.82. **Теорема.** *Пусть* $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ — *неприводимый многочлен над полем* $\mathbb{F}_q$ *характеристики* p, *и пусть* $b \in \mathbb{F}_q$. *Многочлен* $f(x^p - x - b)$ *неприводим над полем* $\mathbb{F}_q$ *тогда и только тогда, когда абсолютный след* $\mathrm{Tr}_{\mathbb{F}_q}(mb - a_{m-1})$ *отличен от нуля.*

Доказательство. Допустим, что $\mathrm{Tr}_{\mathbb{F}_q}(mb - a_{m-1}) \neq 0$. Положим $K = \mathbb{F}_q$, и пусть F — поле разложения многочлена f над K. Если $\alpha \in F$ — корень многочлена f, то на основании теоремы 2.14 все возможные корни данного многочлена — это различные элементы α, α^q, α^{q^2}, ..., $\alpha^{q^{m-1}}$; при этом $F = K(\alpha)$. Кроме того, $\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1}$, согласно (2.2), и, применяя теорему 2.26, получаем, что

$$\mathrm{Tr}_F(\alpha + b) = \mathrm{Tr}_K(\mathrm{Tr}_{F/K}(\alpha + b)) = \mathrm{Tr}_K(-a_{m-1} + mb) \neq 0.$$

На основании следствия 3.79 трехчлен $x^p - x - (\alpha + b)$ неприводим над полем F. Поэтому $[F(\beta) : F] = p$, где β — корень трехчлена $x^p - x - (\alpha + b)$. Из теоремы 1.84 получаем, что

$$[F(\beta) : K] = [F(\beta) : F]\,[F : K] = pm.$$

Далее, так как $\alpha = \beta^p - \beta - b$, то $\alpha \in K(\beta)$ и $K(\beta) = K(\alpha, \beta) = F(\beta)$. Это значит, что $[K(\beta) : K] = pm$, и минимальный многочлен элемента β над K имеет степень pm. Но ввиду того что $f(\beta^p - \beta - b) = f(\alpha) = 0$, элемент β является корнем нормированного многочлена $f(x^p - x - b) \in K[x]$ степени pm. Из теоремы 3.33 (ii) следует, что $f(x^p - x - b)$ — минимальный многочлен элемента β над полем K, и потому по теореме 3.33 (i) он неприводим над полем $K = \mathbb{F}_q$.

Если же $\mathrm{Tr}_{\mathbb{F}_q}(mb - a_{m-1}) = 0$, то трехчлен $x^p - x - (\alpha + b)$ приводим над полем F, так что $[F(\beta) : F] < p$ для любого корня β трехчлена $x^p - x - (\alpha + b)$. Такое же рассуждение, как и выше, показывает, что β является корнем многочлена $f(x^p - x - b)$ и при этом $[F(\beta) : K] < pm$, откуда вытекает приводимость многочлена $f(x^p - x - b)$ над полем $K = \mathbb{F}_q$. □

Для некоторых типов приводимых трехчленов можно установить вид их канонических разложений. Условия следующей теоремы включают в себя требование неприводимости некоторого двучлена — вопрос, решаемый теоремой 3.75.

3.83. **Теорема.** *Пусть задан трехчлен* $f(x) = x^r - ax - b \in \mathbb{F}_q[x]$, *степень* $r > 2$ *которого является степенью характеристики поля* $\mathbb{F}_q$, *и пусть двучлен* $x^{r-1} - a$ *неприводим над* $\mathbb{F}_q$.

Тогда трехчлен $f(x)$ является произведением некоторого линейного многочлена и неприводимого над $\mathbb{F}_q$ многочлена степени $r-1$.

Доказательство. Так как $f'(x) = -a \neq 0$, то трехчлен $f(x)$ имеет лишь простые корни. Если p — характеристика поля $\mathbb{F}_q$, то $f(x)$ является аффинным p-многочленом над $\mathbb{F}_q$. Поэтому на основании теоремы 3.56 разность γ двух различных корней трехчлена $f(x)$ является корнем p-многочлена $x^r - ax$, а значит, и корнем двучлена $x^{r-1} - a$. Ввиду неприводимости этого двучлена и условия $r-1 > 1$ мы получаем, что элемент γ не принадлежит полю $\mathbb{F}_q$, так что существует корень α трехчлена $f(x)$, не являющийся элементом поля $\mathbb{F}_q$. Тогда $\alpha^q \neq \alpha$, причем α^q тоже является корнем $f(x)$, поэтому, согласно сказанному выше, разность $\alpha^q - \alpha$ является корнем неприводимого двучлена $x^{r-1} - a$ над $\mathbb{F}_q$, так что $[\mathbb{F}_q(\alpha^q - \alpha) : \mathbb{F}_q] = r-1$. Ввиду того что $\mathbb{F}_q(\alpha^q - \alpha) \subseteq \mathbb{F}_q(\alpha)$, степень $m = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ кратна числу $r-1$. С другой стороны, α — корень многочлена $f(x)$ степени r, так что $m \leqslant r$. Но поскольку $r > 2$, то для m остается единственная возможность, а именно $m = r-1$. Таким образом, минимальным многочленом элемента α над $\mathbb{F}_q$ является некоторый неприводимый многочлен над $\mathbb{F}_q$ степени $r-1$, делящий трехчлен $f(x)$. Отсюда сразу вытекает утверждение теоремы. □

Для частного случая простых конечных полей можно среди трехчленов определенного вида выделить примитивные многочлены.

3.84. Теорема. *Для простого числа p трехчлен $x^p - x - a \in \mathbb{F}_p[x]$ в том и только том случае является примитивным многочленом над $\mathbb{F}_p$, если a — примитивный элемент поля $\mathbb{F}_p$ и при этом* $\operatorname{ord}(x^p - x - 1) = (p^p - 1)/(p-1)$.

Доказательство. Допустим сначала, что $f(x) = x^p - x - a$ — примитивный многочлен над $\mathbb{F}_p$. Тогда по теореме 3.18 элемент a является примитивным элементом поля $\mathbb{F}_p$. Если β — корень многочлена $g(x) = x^p - x - 1$ из некоторого расширения поля $\mathbb{F}_p$, то

$$0 = ag(\beta) = a(\beta^p - \beta - 1) = a^p\beta^p - a\beta - a = f(a\beta),$$

так что элемент $\alpha = a\beta$ является корнем неприводимого трехчлена $f(x)$ и, следовательно, примитивным элементом поля $\mathbb{F}_{p^p}$. Поэтому $\beta^r \neq 1$ для $0 < r < (p^p - 1)/(p-1)$, так как в противном случае мы получили бы $\alpha^{r(p-1)} = 1$ для $0 < r(p-1) < p^p - 1$, что противоречит примитивности элемента α в поле $\mathbb{F}_{p^p}$. С другой стороны, согласно следствию 3.79, трехчлен $g(x)$ неприводим над $\mathbb{F}_p$, так что

$$g(x) = x^p - x - 1 = (x-\beta)(x-\beta^p)\dots(x-\beta^{p^{p-1}}).$$

Сравнение постоянных членов приводит к равенству $\beta^{(p^p-1)/(p-1)} = 1$, откуда по теореме 3.3 следует, что порядок многочлена $g(x) = x^p - x - 1$ равен $(p^p - 1)/(p - 1)$.

Обратно, если выполнены условия теоремы, то элементы α и β имеют в мультипликативной группе $\mathbb{F}_{p^p}^*$ порядки $p - 1$ и $(p^p - 1)/(p - 1)$ соответственно. Далее,

$$\begin{aligned}(p^p - 1)/(p - 1) &= 1 + p + p^2 + \ldots + p^{p-1} \equiv \\ &\equiv 1 + 1 + 1 + \ldots + 1 \equiv \\ &\equiv p \equiv 1 \pmod{(p - 1)},\end{aligned}$$

так что числа $p - 1$ и $(p^p - 1)/(p - 1)$ взаимно просты. Поэтому элемент $\alpha = a\beta$ имеет порядок $(p - 1)\cdot(p^p - 1)/(p - 1) = p^p - 1$ в группе $\mathbb{F}_{p^p}^*$. Следовательно, α — примитивный элемент поля $\mathbb{F}_{p^p}$, а значит, $f(x)$ — примитивный многочлен над $\mathbb{F}_p$. □

3.85. **Пример.** Для $p = 5$ мы имеем $(p^p - 1)/(p - 1) = 781 = 11\cdot 71$. Из доказательства теоремы 3.84 следует, что $x^{781} \equiv 1 \pmod{(x^5 - x - 1)}$, и так как $x^{11} \not\equiv 1 \pmod{(x^5 - x - 1)}$ и $x^{71} \not\equiv 1 \pmod{(x^5 - x - 1)}$, то получаем, что $\operatorname{ord}(x^5 - x - 1) = 781$. Далее, числа 2 и 3 являются примитивными элементами поля $\mathbb{F}_5$, поэтому, согласно теореме 3.84, трехчлены $x^5 - x - 2$ и $x^5 - x - 3$ являются примитивными многочленами над полем $\mathbb{F}_5$. □

Нетрудно видеть, что квадратный трехчлен $x^2 + x + a$ над полем $\mathbb{F}_q$ нечетной характеристики является неприводимым в кольце $\mathbb{F}_q[x]$ в том и только том случае, если элемент a не представим в виде $a = 4^{-1} - b^2$ ни для какого $b \in \mathbb{F}_q$. Следовательно, существует $(q - 1)/2$ различных выборов элемента $a \in \mathbb{F}_q$, для которых квадратный трехчлен $x^2 + x + a$ неприводим над $\mathbb{F}_q$. И вообще число элементов $a \in \mathbb{F}_q$, для которых трехчлен $x^n + x + a$ неприводим над $\mathbb{F}_q$, как правило, асимптотически равно q/n согласно следующему результату.

3.86. **Теорема.** *Пусть характеристика p конечного поля $\mathbb{F}_q$ не делит числа $2n(n - 1)$, где $n \in \mathbb{N}$, $n \geqslant 2$, и пусть число элементов $a \in \mathbb{F}_q$, для которых трехчлен $x^n + x + a$ неприводим над $\mathbb{F}_q$, равно $T_n(q)$. Тогда существует константа B_n, зависящая лишь от n, такая, что*

$$\left| T_n(q) - \frac{q}{n} \right| \leqslant B_n \sqrt{q}.$$

Доказательство этой теоремы, опирающееся на тонкое исследование некоторых групп Галуа, мы опускаем.

В определении 1.92 было введено понятие дискриминанта многочлена. Ниже устанавливается точная формула для дискриминанта трехчлена.

3.87. Теорема. *Дискриминант трехчлена* $x^n + ax^k + b \in \mathbb{F}_q[x]$, *где* $n > k \geqslant 1$, *выражается формулой*

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} \cdot [n^N b^{N-K} - (-1)^N (n-k)^{N-K} k^K a^N]^d,$$

где $d = \text{НОД}(n, k)$, $N = n/d$, $K = k/d$.

Комментарии

§ 1. Разнообразный материал о многочленах над конечными полями можно найти в монографиях Albert [3, ch. 5] и Berlekamp [4], а также в вышедших совсем недавно книгах Blake, Mullin [1], MacWilliams, Sloane [2] и McDonald [1]. Результаты, содержащиеся в этих книгах, имеют отношение ко всем параграфам этой главы. Дальнейшие результаты о многочленах и некоторые дополнительные ссылки на материал, выходящий за рамки нашей книги, будут приведены в конце комментариев к § 5.

Основные результаты, содержащиеся в лемме 3.1 и следствии 3.4, были доказаны еще Гауссом (Gauss [4]). Изучение порядка многочлена было продолжено Серре (Serret [3]) и Пелле (Pellet [1]), в последней статье можно найти теорему 3.5; см. также Bachmann [4, ch. 7] и Dickson [7, part I, ch. 3]. О теоремах 3.8 и 3.9 см., например, Ward [5]. Простой метод определения $\text{ord}(f)$ для неприводимого над простым полем $\mathbb{F}_p$ многочлена f степени m в случае, когда $(p^m - 1)/(p - 1)$ — простое число, предложен Гараковым в [2]. Как уже отмечалось в основном тексте, порядок многочлена (см. определение 3.2) иногда называют также периодом (Berlekamp [4]) или экспонентой (Albert [3], Dickson [7]) этого многочлена. Понятие порядка многочлена от нескольких переменных было введено Лонгом (Long [1], [2]). Для многочлена $f(x)$ над $\mathbb{F}_q$, удовлетворяющего условию $f(0) \neq 0$, наименьшее натуральное число e, такое, что $f(x)$ делит двучлен $x^e - c$ при некотором $c \in \mathbb{F}_q$, называется *приведенным порядком* этого многочлена; его называют еще *интегральным порядком* (Bose, Chowla, Rao [1]) или *субэкспонентой* (Hirschfeld [4], [5]) многочлена $f(x)$. Связь между порядком и приведенным порядком неприводимого многочлена неявно указана в статье Ward [6]; ср. также с леммой 3.17.

Таблицы неприводимых многочленов и их порядков имеются, например, в следующих работах: Chang, Godwin [1], Golomb [4, ch. 3], Marsh [1] и McEliece [3] (см. также гл. 10 этой книги). Ключевым моментом при отыскании порядков неприводимых многочленов является разложение на множители чисел вида $q^m - 1$. Укажем некоторые источники, где можно найти такие разложения. Классические таблицы таких разложений имеются в работах Cunningham, Woodall [1], Cunningham [1] и Kraïtchik [1].

В статьях Lehmer D. H. [4], [5] развит эффективный метод решета для делителей чисел вида $q^m - 1$, а в статьях Lehmer D. H. [1], [2], [3], [7], [10] — различные методы для проверки на простоту и разложения на множители чисел такого вида; см. также Kraïtchik [2] и Miller J. C. P. [1]. В статье Brillhart, Selfridge [1] дается список полных разложений чисел вида $2^m - 1$, а в работе Brillhart, Lehmer, Selfridge [1] приводятся дальнейшие сведения о разложении чисел такого вида. Обзор различных методов разложения дается в работах Knuth [3, ch. 4] и Williams H. C. [2].

В связи с определением 3.12 отметим интересный класс *самовозвратных многочленов*, т. е. таких многочленов f, для которых $f^* = f$ (см. также упр. 3.13—3.15, 3.24 и 3.93). В статье Levine, Brawley [1] определяется число нормированных неприводимых самовозвратных многочленов данной степени (равной 2 или 4), а в статье Carlitz [105] та же задача решается для многочленов любой четной степени. По поводу дальнейших результатов о самовозвратных многочленах см. также Fredman [1], Golomb [5], Hong, Bossen [1], Miller R. L. [1] и Варшамов, Гараков [1]. В работах Knee, Goldman [1] и Levine, Brawley [1] изучаются *квазисамовозвратные многочлены*, т. е. такие многочлены, для которых $f^* = \pm f$. В статье Albert [5] свойство двух неприводимых многочленов одинаковой степени над $\mathbb{F}_2$ быть возвратными друг к другу описывается при помощи многочленов, корнями которых являются произведения корней исходных многочленов. В связи с теоремой 3.14 см. Chang, Godwin [1]. В статье MacWilliams, Odlyzko [1] связь между разложением многочлена и разложением возвратного к нему многочлена использована для опровержения гипотезы о корреляции конечных последовательностей из поля $\mathbb{F}_2$.

Примитивные многочлены называются еще *индексирующими* (indexing) *многочленами* (см. Alanen, Knuth [2] и Sugimoto [1]). Конечно, такие многочлены тесно связаны с примитивными элементами конечных полей. Ватсон (Watson E. J. [1]) приводит список, где указано по одному примитивному многочлену над $\mathbb{F}_2$ для всех степеней $n \leqslant 100$, а в статье Stahnke [1] — для всех степеней $n \leqslant 168$. В статье Sugimoto [1] приводится таблица примитивных многочленов над простыми полями $\mathbb{F}_p$ для $3 \leqslant p \leqslant 47$. Списки примитивных многочленов имеются также в следующих источниках: Alanen, Knuth [1], [2], Bussey [1], [2], Marsh [1], Peterson, Weldon [1], а также в гл. 10 настоящей книги. В статье Bose, Chowla, Rao [1], [2] дается характеризация примитивных многочленов степеней 2 и 3. Карлиц (Carlitz [96]) показал, что над полем $\mathbb{F}_q$ существует в точности один примитивный многочлен степени n лишь в случаях, когда $q = 2$, $n \leqslant 2$ или $q = 3$, $n = 1$. В статьях Beard [5] и Beard, West [1]

продолжено изучение примитивных элементов и примитивных многочленов, начатое Карлицом (Carlitz [35]). В работе Bilharz [1] доказан для примитивных многочленов аналог гипотезы Артина (Artin [1]) о первообразных корнях при определенном предположении о местонахождении нулей конгруэнц-дзета-функций (см. об этих функциях комментарии к § 4 гл. 6). Это предположение было доказано Дэвенпортом (Davenport [7]) и в более сильной форме А. Вейлем (Weil [1], (2], [3]). В статье Brown, Zassenhaus [1] изучается относительная частота простых чисел p, для которых заданный неприводимый над полем рациональных чисел $\mathbb{Q}$ многочлен с целыми коэффициентами будет примитивным многочленом по модулю p. Мирончиков [1] доказал связанный с теоремой 3.16 результат о том, что многочлен $f \in \mathbb{F}_2[x]$ неприводим над $\mathbb{F}_2$, если $\deg(f) = 2m$ и $\operatorname{ord}(f) = 2^m + 1$, где m четно. В работе Agou [12] получена характеризация неприводимых многочленов заданного порядка, а значит, в частности, и примитивных многочленов. Теорема 3.18 доказана в работе Alanen, Knuth [2] для конечных простых полей. В статьях Hirschfeld [4], [5] изучались *подпримитивные многочлены*, т. е. такие многочлены над полем $\mathbb{F}_q$ некоторой степени m, которые имеют приведенный порядок $(q^m - 1)/(q - 1)$. В соответствии с теоремой 3.18 каждый примитивный многочлен над $\mathbb{F}_q$ является также подпримнтивным.

§ 2. Первое крупное исследование о неприводимых многочленах и неприводимых делителях многочленов от одной переменной над полем $\mathbb{F}_q$ было проведено Диксоном (Dickson [7]), который опирался на ранние работы Jordan C. [2], Pallet [7] и Serret [2], [4]. Теорема 3.25 была доказана еще Гауссом (Gauss [4]) для случая конечных простых полей; см. также Dedekind [1] и Schönemann [3]. Доказательства этой теоремы можно найти также в следующих источниках: Albert [3, ch. 5], Bachmann [4, ch. 7], Berlekamp [4, ch. 3], Dickson [7, part I, ch. 2], Jeger [1], Serret [3], Simmons [1] и van de Vooren-van Veen [1]. Общая теория функций Мёбиуса и обращения Мёбиуса была развита Рота (Rota [1]). Некоторые общие принципы, лежащие в основе подсчета числа неприводимых многочленов, были указаны Фредманом (Fredman [1]). Ленской [1] и Вильямс (Williams K. S. [11]) получили асимптотические формулы для числа нормированных неприводимых многочленов над $\mathbb{F}_q$ степени $\leqslant n$ и степени n соответственно. Об абстрактной точке зрения на такие формулы см. Knopfmacher [1], [2]. Карлиц (Carlitz [40]) обобщил результат Диксона (Dickson [29]), дав асимптотическую формулу для числа неприводимых многочленов над $\mathbb{F}_q$ с некоторыми заранее заданными коэффициентами; см. также Cohen S. D. [7], Dress [1], Hayes [2], Uchiyama [1], [4], Williams K. S. [15] и Варшамов [3], [5]. В статьях Levine, Brawley [1], Carlitz [105] и Fredman [1] изучается число нормированных неприводимых

самовозвратных многочленов фиксированной степени. Фредман (Fredman [1]) обсуждает также подсчет числа неприводимых многочленов других типов. В работе Golomb [6] установлено взаимно однозначное соответствие между неприводимыми многочленами степени n над полем $\mathbb{F}_q$ и непериодическими ожерельями из n бусинок q разных цветов и тем самым определено число таких ожерелий. См. также статью Miller R. L. [1] о других вычислительных задачах.

В связи с теоремой 3.27 напомним, что ссылки на работы о круговых многочленах собраны в комментариях к § 4 гл. 2.

Формула для $I(q, n; x)$ в теореме 3.29 по существу принадлежит Дедекинду (Dedekind [1]); см. также Serret [2], [4], [5], Dickson [3], [7, part, I, ch. 2], Bachmann [4, ch. 7] и Albert [3, ch. 5]. Карлиц (Carlitz [3]) доказал формулы для наименьшего общего кратного (см. также Walker [1]) и для произведения всех нормированных многочленов над $\mathbb{F}_q$ фиксированной степени (см. также Willims K. S. [26]). Последнюю формулу можно применить также при вычислении произведений характеристических многочленов для некоторых классов матриц над $\mathbb{F}_q$ (см. Carlitz [104]).

Таблицы неприводимых многочленов можно найти в следующих источниках: Alanen, Knuth [1], [2], Bussey [1], [2], Chang, Godwin [1], Church [1], Golomb [4, ch. 3], Marsh [1], Mossige [1], Peterson, Weldon [1], Гараков [3] и в гл. 10 настоящей книги. В работе Conway [1] приведены фрагменты более полных таблиц для конечных полей порядков $p^n \leqslant 1024$ (p — простое число, $n \geqslant 2$), в которых для каждого элемента такого поля указываются его характеристический и минимальный многочлены над каждым собственным подполем; см. также гл. 10 (§ 1 и таблицу B) этой книги.

Неприводимые кубические многочлены были подробно изучены в следующих работах: Cailler [1], Carlitz [103], Dickson [9], [29], Mirimanoff [1], Williams K. S. [32] и Гельфанд [1], [2]. О неприводимых многочленах четвертой степени см. Albert [3, ch. 5], Carlitz [73], [103], Dickson [9], Leonard, Williams [1] и Skolem [4]. Серре (Serret [4], [5]) и Диксон (Dickson [3], [7, part I, ch. 3]) охарактеризовали такие неприводимые многочлены, степени которых являются степенями характеристики основного конечного поля. В статье Golomb, Lempel [1] изучаются неприводимые многочлены, задаваемые рекуррентными соотношениями второго порядка. О неприводимых двучленах и трехчленах см. § 5 и комментарии к нему. Агу в статьях Agou [1], [3] показал, что нормированный многочлен $f(x)$ над $\mathbb{F}_q$ степени $n \geqslant 1$ неприводим над $\mathbb{F}_q$ тогда и только тогда, когда он делит коэффициенты следующего многочлена от y:

$$(y - x)(y - x^q) \ldots (y - x^{q^{n-1}}) - f(y);$$

в работе Agou [3] он дает аналогичный критерий того, чтобы данный нормированный многочлен был степенью неприводимого многочлена. В работе того же автора Agou [9] найден критерий неприводимости над $\mathbb{F}_q$ многочлена $f(g(x))$, где $f, g \in \mathbb{F}_q[x]$ — нормированные многочлены, причем $f(x)$ неприводим над $\mathbb{F}_q$. Этот критерий он использует в статьях Agou [9], [13], [15], [16] для характеризации неприводимых многочленов некоторых специальных типов, таких, как $f(x^{p^r} - ax)$, $f(x^p - x - b)$ и др. Подобные неприводимые композиции изучаются также в § 5 этой главы и в статьях Cohen S. D. [2], [10], Long [3], [4] и Ore [6]. О композициях вида $f(x^t)$ см. § 3.

Действие группы аффинных преобразований на множестве всех неприводимых многочленов над $\mathbb{F}_q$ рассматривалось в работе Dodunekov [1], а действие группы дробно-линейных преобразований с коэффициентами из простого поля $\mathbb{F}_p$ на множестве неприводимых многочленов данной степени над $\mathbb{F}_p$ изучалось в статьях Brahana [1], [2] и Hanneken [1], [2], [3], [4], [5]. Действие той же группы при $p = 2$ на множестве корней неприводимых над $\mathbb{F}_2$ многочленов рассматривается в работе Golomb [5].

Корнблюм (Kornblum [1]) доказал для кольца $\mathbb{F}_q[x]$ аналог теоремы Дирихле о простых числах в арифметической прогрессии, а именно он показал, что если g и h — ненулевые взаимно простые многочлены из $\mathbb{F}_q[x]$, то существует бесконечно много нормированных неприводимых многочленов $f(x)$ над $\mathbb{F}_q$, сравнимых по модулю $h(x)$ с $g(x)$, даже при дополнительном предположении, что их степени $\deg(f)$ принадлежат заданной арифметической прогрессии. В статьях Artin [1], Cohen S. D. [7], Hayes [2], Johnsen [2] и Rhin [3] получены количественные уточнения этого результата. Дэвенпорт (Davenport [6]) применил результат Корнблюма для изучения примитивных элементов.

Карлиц (Carlitz [15], [95], [99]) рассматривал распределение неприводимых многочленов от нескольких переменных; эта работа продолжена статьями Cohen S. D. [1], [3] и Fredman [2]. В статье Prabhu, Bose [1] предлагается способ оценки числа неприводимых многочленов в кольце $\mathbb{F}_q[x_1, \ldots, x_n]$ с заранее заданными степенями по каждой переменной x_i. Карлиц (Carlitz [12]) назвал многочлен от нескольких переменных *факторизуемым*, если его можно разложить в произведение линейных сомножителей над некоторым конечным расширением поля $\mathbb{F}_q$. В этой же работе найдено число факторизуемых многочленов и число неприводимых факторизуемых многочленов данной степени над $\mathbb{F}_q$. Факторизуемые многочлены изучались также в работах Agou [7], Carlitz [15], Long [1], [2], [5] и Williams K. S. [14]. Об абсолютно неприводимых многочленах от нескольких переменных см. § 4 гл. 6.

§ 3. Теоремы 3.35 и 3.37 для конечных простых полей доказаны Серре (Serret [2]); см. также Albert [3, ch. 5] и Dickson [7, part I, ch. 3]. Прямой метод получения неприводимых многочленов данной степени и данного порядка исследовался Голомбом (Golomb [8]). Теоремы 3.38 и 3.39 были доказаны в статье Daykin [6]. Эта статья содержит и другие результаты о характеристических многочленах f_t для степеней α^t элемента $\alpha \in \mathbb{F}_q$. Для случая примитивного элемента α алгоритм вычисления характеристических многочленов f_t был описан в работе Alanen, Knuth [2]. Голомб (Golomb [6]) дал алгоритм нахождения минимального многочлена для степени α^t элемента α по минимальному многочлену самого элемента α над $\mathbb{F}_2$; см. также Gordon [1]. В случае когда минимальный многочлен элемента α над $\mathbb{F}_2$ является трехчленом, см. также Bajoga [1] и Bajoga, Walbesser [1]. Алгоритмы для нахождения минимальных многочленов обсуждаются также в книгах Berlekamp [4, ch. 4] и MacWilliams, Sloane [2, ch. 4]. Таблицы характеристических и минимальных многочленов см. в работе Conway [1]; ср. также с § 1 гл. 10.

Критерии неприводимости для многочленов вида $f(x^t)$ установлены в статьях Agou [9], [10], [11], Butler [2], Cohen S. D. [2], Pellet [7], Petterson [3] и Serret [2], [3]. Связь между порядками многочленов $f(x^t)$ и $f(x)$ изучается в работах Berlekamp [4, ch. 6] и Варшамов, Ананиашвили [1].

Другие классические методы построения неприводимых и примитивных многочленов можно найти в работах Albert [3, ch. 5], Dickson [3], [7, part I, ch. 3], Pellet [4], [5] и Serret [2]. Алгоритм построения всех неприводимых многочленов над конечным простым полем был предложен в статьях Popovici [1], [2]. В работах Rabin [1] и Calmet, Loss [1] описаны вероятностные алгоритмы для построения неприводимых многочленов. Варшамов и Антонян [1] описали метод построения новых неприводимых многочленов над полем $\mathbb{F}_2$, исходя из данного неприводимого многочлена; см. также Варшамов [2]. В статьях Swift [1] и Варшамов [4] показывается, как строить неприводимые многочлены над $\mathbb{F}_2$, исходя из примитивных многочленов. В последней статье содержится также теоретико-матричный метод построения всех неприводимых многочленов, степени которых делят n, исходя из некоторого неприводимого многочлена степени n. В работах Lempel [1] и Swift [1] описываются методы нахождения примитивных многочленов над полем $\mathbb{F}_2$, а Варшамов и Гамкрелидзе [1] указывают аналогичные конструктивные методы для случая произвольного конечного простого поля $\mathbb{F}_p$. В статье Alanen, Knuth [2] приведены алгоритмы для построения новых примитивных многочленов над $\mathbb{F}_p$, исходя из одного такого многочлена.

Теорема 3.46 была доказана Пелле (Pellet [1]) для конечных простых полей и Диксоном (Dickson [7, part I, ch. 3]) для произвольных конечных полей; см. также Agou [4].

§ 4. Многие результаты этого параграфа восходят к фундаментальным статьям Ope (Ore [4], [5], [6], [7]). Некоторые из результатов Ope предвидел Релла (Rella [1]). В статье Ore [4] изучаются p-многочлены над произвольными полями характеристики p. Теория линеаризованных многочленов над конечными полями была широко развита в работе Ore [5], там же обобщаются некоторые результаты из статьи Dickson [3] и исследуется операция символического умножения. В статье Ore [6] изучение этих вопросов продолжено, в ней дается также важное уточнение теоремы о нормальном базисе (см. теоремы 3.72 и 3.73). Та же техника применяется Артином (Artin [3]) для доказательства теоремы о нормальном базисе для некоторых бесконечных полей характеристики p. Дальнейшие ссылки, связанные с теоремой о нормальном базисе, см. в комментариях к § 3 гл. 2. Формула из леммы 3.51 установлена Муром (Moore [3]). Ее простое доказательство указано Диксоном (Dickson [30]).

Линеаризованные многочлены изучались также в работах Carcanague [1], [2], Carlitz [21] и Vaughan T. P. [1]. Частные классы линеаризованных многочленов появляются у Карлица (Carlitz [7], [17], [20], [34], [35]). В статье Daykin [5] рассматриваются аффинные многочлены и выясняются степени и число их неприводимых делителей. Метод отыскания корней многочленов на основе их аффинных кратных изложен в работе Berlekamp, Rumsey, Solomon [1]. В работах Carlitz [21], [91], Ore [7], Silva [1] и Vaughan T. P. [1] исследуются связи между линеаризованными многочленами и циркулянтными матрицами. О векторных пространствах и линейных отображениях над конечными полями см. Brawley, Carlitz, Vaughan [1], Burde [2], [5], Pele [1], Rella [1], Ulbrich [1] и Vaughan T. P. [1], [2]. Питерсон (Peterson [2]) применил результаты Пеле (Pele [1]) в теории кодирования. В статье Jamison [1] линеаризованные многочлены используются в задаче о покрытии векторного пространства над $\mathbb{F}_q$ аффинными подпространствами. В работе Segre, Bartocci [1] линеаризованные многочлены над $\mathbb{F}_2$ применяются к конечным проективным геометриям. Изложение теории линеаризованных и аффинных многочленов можно найти в книгах Berlekamp [4, ch. 11], MacWilliams, Sloane [2, ch. 4], McDonald [1, ch. 2] и Rédei [10, ch. 8]. Линеаризованные многочлены над более общими полями характеристики p изучались в работах Artin [3], Crampton, Whaples [1], Krasner [1] и Whaples [1].

Теорема 3.63 доказана Ope (Ore [6]); см. также Zierler [2]. Для частного случая, когда $f(x)$ является примитивным многочленом над $\mathbb{F}_q$ (и тогда многочлен $F(x)/x$ неприводим над $\mathbb{F}_q$),

этот результат получен в статье Marsh, Gleason [1]. Дальнейшие результаты в этом направлении можно найти в работах Dickson [30], Mills [3] и Варшамов [2], [3], [5].

Формула для $\Phi_q(f)$ из леммы 3.69 (iii) была получена Дедекиндом (Dedekind [1]) для простого числа q и Митчеллом (Mitchell O. H. [1]) для общего случая. Дальнейшие результаты о $\Phi_q(f)$ имеются у Карлица (Carlitz [26], [28]). Групповая структура множества многочленов, подсчитываемых числом Φ_q, была исследована в статьях Claasen [1], [2]; см. также Smits [1]. В работе Cohen S. D. [4] рассматривается аналог функции $\Phi_q(f)$ для многочленов от нескольких переменных. В статье Kühne [3] получена формула для числа нормированных многочленов данной степени $d < \deg(f)$, которые взаимно просты с данным многочленом $f \in \mathbb{F}_p[x]$.

§ 5. Теорема 3.75 по существу была доказана Серре (Serret [2]) для конечных простых полей. Дальнейшие характеризации неприводимых двучленов можно найти в работах Albert [3, ch 5], Capelli [1], [2], [3], Dickson [7, part I, ch. 3], Lowe, Zelinsky [1], Rédei [10, ch. 11] и Schwarz [4]. Разложение в теореме 3.76 получено тоже Серре (Serret [2]); см. также Albert [3, ch. 5] и Dickson [7, part I, ch. 3]. В статье Shiva, Allard [1] рассмотрен один способ разложения двучлена $x^{2^k-1}+1$ над полем $\mathbb{F}_2$. Разложение двучлена $x^{q-1}-a$ над полем $\mathbb{F}_q$ рассматривается в работе Dickson [30]; см. также Agou [14]. Шварц (Schwarz [7]) получил формулу для числа нормированных неприводимых делителей фиксированной степени данного двучлена, а Редеи (Rédei [9]) указал ее короткое доказательство; см. также Agou [10], Butler [2] и Schwarz [4]. В статье Gay, Vélez [1] доказана формула для степени поля разложения неприводимого двучлена над произвольным полем (ранее она была установлена Дарби (Darbi [1]) лишь для полей характеристики 0). В работе Agou [4] изучается разложение неприводимого над $\mathbb{F}_q$ двучлена в некотором расширении поля $\mathbb{F}_q$. Таблицы разложений двучленов вида x^n-1 даются в статьях Beard, West [2] и McEliece [3]. Разложение многочленов более общего внда $g(x)^t-a$ над конечными простыми полями рассматривается в работах Ore [2] и Petterson [3]. Приложения разложений двучленов можно найти в статьях Agou [10], Berlekamp [2] и Vaughan T. P. [1].

Теорема 3.78 и следствие 3.79 были впервые доказаны Пелле (Pellet [1]). Неприводимость трехчлена x^p-x-a над $\mathbb{F}_p$ при условии, что $a \in \mathbb{F}_p^*$, была установлена еще Серре (Serret [2], [3]). См. об этом также Dickson [3], [7, part I, ch. 3] и Albert 2, ch. 5]. Теорема 3.80 доказана Диксоном (Dickson [3], [7, part I, ch. 3]), но для частного случая $a=0$ она была установлена еще Матье (Mathieu [1]). Теорема 3.82 в общем виде была

доказана Варшамовым [3], [5]; см. также Agou [9]. Случай $b = 0$ привлек внимание гораздо раньше. Соответствующий результат (в случае $b = 0$) для простых конечных полей был сформулирован Пелле в работе Pellet [1] и доказан им в статье Pellet [9]. Многочлены вида $f(x^p - x)$ над $\mathbb{F}_p$, где степенью многочлена f является степень числа p, были изучены Серре (Serret [4], [5]). Случай $b = 0$ для произвольных конечных полей рассмотрели Диксон (Dickson [7, part I, ch. 3]) и Альберт (Albert [3, ch. 5]). Изучались также и более общие типы многочленов, такие, как $f(x^{p^r} - ax)$, $f(x^{p^{2r}} - ax^{p^r} - bx)$ и другие; см. например, работы Agou [9], [13], [14], [15], [16], [17], [18], [19], [20], Cohen S. D. [10], Long [2], [3], [4], [5], Long, Vaughan [1], [2] и Оге [6]. Теорема 3.83 обобщает результаты Диксона (Dickson [30]) и Альберта (Albert [3, ch. 5]). См. Schwarz [12] о дальнейших результатах в этом направлении. Вопрос о числе корней трехчлена $x^r - ax - b \in \mathbb{F}_q[x]$, где r — степень характеристики поля $\mathbb{F}_q$, изучался в статьях Liang [1], Segre [10] и Vilanova [1]. Теорема 3.84 получена Диксоном (Dickson [7, part I, ch. 3]).

Човла (Chowla S. [17]) высказал предположение, что для фиксированного натурального числа $n \geqslant 2$ число неприводимых над $\mathbb{F}_p$ многочленов вида $x^n + x + a \in \mathbb{F}_p[x]$ асимптотически равно p/n при $p \to \infty$. Он доказал это для случая $n = 3$. Этот случай рассмотрен также в статье Carlitz [103]. Леонард (Leonard [1]) обобщил это доказательство на случай $n = 4$ (см., кроме того, Leonard [3]), а в работе Leonard [2] он доказал ослабленную форму гипотезы Човлы для $n = 5$. В статье Williams K. S. [13] гипотеза Човлы доказана для $n \leqslant 5$. Общее доказательство гипотезы Човлы (и нашей теоремы 3.86) получено Коэном (Cohen S. D. [5]) и Ри (Ree [1]). Коэн (Cohen S. D. [5]) доказал даже более общий асимптотический результат о числе неприводимых многочленов вида $f(x) + ag(x)$ с заданными $f, g \in \mathbb{F}_q[x]$ и изменяющимся $a \in \mathbb{F}_q$. См. также Cohen S. D. [6], Hayes [6], Leonard [5]. Дальнейшие результаты о трехчленах вида $x^n + x + a$ над простым конечным полем $\mathbb{F}_q$ имеются в работах Mortimer, Williams [1], Sato, Yorinaga [1], Uchiyama [8] и Williams K. S. [13]. В статье Cazacu, Simovici, [1] дается алгоритм построения неприводимых трехчленов вида $ax^n + x + 1$ над конечными полями характеристики 2. Доказательства теоремы 3.87 имеются в работах Berlekamp [4, ch. 6] и Swan [1].

Таблицы неприводимых трехчленов над полем $\mathbb{F}_2$ имеются в следующих источниках: Golomb [4, ch. 5], Golomb, Welch, Hales [1], Zierler [7] и Zierler, Brillhart [1], [2]. В статье Fredricksen, Wisniewski [1] рассматриваются специальные классы неприводимых трехчленов над $\mathbb{F}_2$. Примитивные трехчлены над $\mathbb{F}_2$ приводятся в статьях Rodemich, Rumsey [1], Zierler [6] и Zier-

ler, Brillhart [1], [2]. Различные результаты о порядках трехчленов над $\mathbb{F}_2$ и таблицы этих порядков имеются в работах Golomb [4, ch. 5], Golomb, Welch, Hales [1], Young [1], Zierler [8] и Аракелов, Тененгольц [1]. В статьях Bajoga [1] и Bajoga, Walbesser [1] изучаются элементы поля характеристики 2, минимальные многочлены которых над $\mathbb{F}_2$ являются трехчленами. Списки некоторых неприводимых трехчленов вида $x^n + x + a$ над простым конечным полем имеются в статье Mortimer, Williams [1].

Таблицы разложения трехчленов на множители имеются в следующих работах: Beard, West [3], Golomb [4, ch. 5], Golomb, Welch, Hales [1], Zierler [7] и Zierler, Brillhart [1], [2]. Голомб (Golomb [4, ch. 5]) выдвинул гипотезу, что степень каждого неприводимого делителя трехчлена $x^{2r+1} + x^{r-1} + 1$, где $r = 2^n$, над полем $\mathbb{F}_2$ делит число $6n$. Эта гипотеза была доказана в статье Mills, Zierler [1], причем даже в более сильной форме (а именно что каждая такая степень делит или $2n$, или $3n$, но не n), а затем обобщена Карлицом (Carlitz [112]) на случай произвольного конечного поля. Миллс (Mills [3]) доказал, что степень каждого неприводимого делителя трехчлена $x^{r+1} + x + 1$, где $r = q^n$, над полем $\mathbb{F}_q$ делит число $3n$. Многие другие результаты подобного типа можно найти в работах Golomb [4, ch. 5] и Marsh Mills, Ward, Rumsey, Welch [1]. Вопрос о разложении трехчлена $x^4 + ax^2 + b$ над конечными простыми полями рассматривается в статьях Carlitz [73], [103].

Теперь мы дадим обзор тех вопросов о многочленах, которые не были упомянуты в данной главе. Существует обширная литература об обобщениях классических вопросов теории чисел на случай кольца многочленов $\mathbb{F}_q[x]$. Проблема представления многочлена в виде суммы неприводимых многочленов (обобщенная форма *проблемы Гольдбаха* для $\mathbb{F}_q[x]$) рассматривается в статьях Car [2], Cherly [2], Hayes [1], [4] и Webb [1]. Представление многочленов в виде суммы двух неприводимых многочленов и некоторого квадрата изучалось в работе Car [6]; см. также Webb [1]. Проблема представления многочлена в виде суммы степеней многочленов (*проблема Варинга для* $\mathbb{F}_q[x]$) рассматривается в статьях Car [1], [3], [4], Joly [1], Kubota R. M. [1], Matthews K. R. [1], Paley [2] и Webb [2], [3]. Особенно интенсивно изучался частный случай этой проблемы, касающийся представления многочлена в виде суммы квадратов; см. Carlitz [5], [8], [13], [19], [26], [27], [116], Carlitz, Cohen [2], Cohen E. [1], [2], Joly [2], Leahey [1], Stevens, Kuty [1], Verner [1], [2] и Webb [2]. О представлениях квадратичными формами см. Carlitz [54] и Carlitz, Cohen [3], а об одновременных представлениях квадратичными и линейными формами см. Carlitz [94]. Суммы

степеней с полиномиальными коэффициентами рассматривались в статьях Carlitz, Cohen [1] и Cohen E. [3], [4]. О более общих формах см. Carlitz [32] и Cohen E. [4], [6]. Проблемы аддитивной теории чисел в кольце $\mathbb{F}_q[x]$ рассматривались в работах Carlitz [48] и Cherly [1], [2], [3].

Функции Φ_q (см. лемму 3.69) и μ_q (см. упр. 3.75) являются частными примерами арифметических функций на множестве $\mathbb{F}_q[x]$. Такого рода функции систематически изучались Карлицом (Carlitz [1], [2], [3], [26], [28], [30], [36]); что же касается функции Φ_q, то она рассматривалась еще Дедекиндом (Dedekind [1]). Аналог функции Φ_q для многочленов от нескольких переменных был изучен Коэном (Cohen S. D. [4]). Дальнейшие результаты об арифметических функциях получены в работах Carlitz [6], [14], [19], [20], Carlitz, Cohen [1], [2], Cohen E. [3], [6], Cohen S. D. [3], [4], Dress [1], Rhin [3], Shader [1], [4] и Silva [2]. Об абстрактном подходе см. Knopfmacher [1], [2]. Аналог для кольца $\mathbb{F}_q[x]$ понятия совершенного числа изучался в статьях Beard [6], Beard, Bullock, Harbin [1], Beard, Doyle, Mandelberg [1], Beard, Harbin [1] и Beard, O'Connell, West [1]. О сумме делителей многочлена над $\mathbb{F}_2$ см. Canaday [1]. В статье Johnsen [2] изучаются методы решета в кольце $\mathbb{F}_q[x]$. Связь между арифметикой в $\mathbb{F}_q[x]$ и современной алгебраической геометрией появляется в работе Goss [3]. Квадратичный закон взаимности для нормированных неприводимых многочленов над простым конечным полем $\mathbb{F}_p$ доказал Дедекинд (Dedekind [1]), другое его доказательство дал Артин (Artin [1]); см. также Vaidyanathaswamy [1]. Высший закон взаимности для неприводимых многочленов над произвольным конечным полем $\mathbb{F}_q$ был установлен Кюне (Kühne [1]) и еще раз доказан Шмидтом (Schmidt F. K. [2]) и Карлицом (Carlitz [1], [2], [4]); см. также Ore [6], Pocklington [2], Schwarz [2] и Whiteman [1]. Полиномиальные сравнения изучались в работах Carlitz [7], [8], [9], [10], [11], [17], Cohen E. [5], Rao K. N. [1], [2], [3], Shader [2], [3] и Ленской [2].

Карлиц (Carlitz [7]) начал изучение функции $\psi_m(t) = \prod(t - f(x))$, где произведение берется по всем многочленам $f(x)$ над $\mathbb{F}_q$ степени, меньшей чем m. Это изучение было продолжено работами Carlitz [10], [19], [20], [31] и Wagner [1]. О приложениях таких функций см. Bundschuh [2], Carlitz [119], Geijsel [1], Wade [1], [2], [3] и Wagner [2], [3]. В статье Carlitz [18] вводятся полиномиальные аналоги круговых многочленов, а в статье Carlitz [23] — аналоги многочленов Бернулли для конечных полей. Теорема типа теоремы фон Штаудта для таких многочленов была доказана Карлицом (Carlitz [24]), она обобщает его же результаты из статей Carlitz [16], [22]; см. также Carlitz [25], Dickey, Kairies, Shank [1], Goss [1], [2] и Herget [1], [2].

В работе Carlitz [31] показано, что многочлены $f \in \mathbb{F}_q[x]$, обладающие для всех $a \in \mathbb{F}_q$ свойством $f(x+a) = f(x)$, имеют вид $f(x) = \sum_k c_k (x^q - x)^k$, где $c_k \in \mathbb{F}_q$; см. также Dodunekov [2]. Обобщения на случай нескольких переменных представлены в статье Carlitz [119]. В статье Mullen [13] для фиксированных $a \in \mathbb{F}_q^*$ и $b \in \mathbb{F}_q$ дается характеризация многочленов $f \in \mathbb{F}_q[x]$, обладающих свойством $f(bx+a) = bf(x) + a$; случай $b = 1$ уже рассматривался раньше в работе Wells [6]. Вагнер (Wagner [2]) на кольце $\mathbb{F}_q[x]$ определяет такие линейные операторы L, что $L(f+g) \equiv L(f) \pmod{g}$ для всех $f, g \in \mathbb{F}_q[x]$.

В статье Shehadeh [1] определяется наибольшее возможное число последовательных нулей или единиц и их распределение среди коэффициентов некоторых многочленов над $\mathbb{F}_2$, таких, как многочлен $(x^n - 1)/f(x)$, где $f(x)$ — примитивный многочлен над $\mathbb{F}_2$ степени k и $n = 2^k - 1$.

Понятие равномерного распределения для последовательностей многочленов над конечными полями было введено в статье Hodges [23]. Дальнейшие работы на эту тему: Dijksma [1], [2], [3], [4], Hodges [26], [27], Kuipers [2], Kuipers, Scheelbeek [1], Meijer, Dijksma [1] и Webb [4]. Равномерное распределение в поле рядов Лорана $\sum_{i=-\infty}^{m} c_i x^i$ над $\mathbb{F}_q$ было введено Карлицом (Carlitz [33]) и далее изучалось в работах de Mathan [1], [2], [3], Dijksma [2], [3], [4], Hodges [27], Kuipers [1], Long, Webb [1], Meijer, Dijksma [1], Rhin [1], [2], [3] и Webb [4]. Изложение этих результатов можно найти в книге Kuipers, Niederreiter [1, ch. 5]. Близкие результаты по диофантовым приближениям в поле рядов Лорана над конечным полем $\mathbb{F}_q$ содержатся в статьях Bateman, Duquette [1], Carlitz [32], [33], Deshouillers [1], [2], [3], Dubois, Paysan-Le Roux [1], Grandet-Hugot [1], [2] и Houndonougbo [2].

В работе Kustaanheimo, Qvist [1] построен аналог комплексного анализа для кольца $\mathbb{F}_q[x]$ (авторы вводят подходящее понятие производной и доказывают, в частности, аналог условий Коши—Римана).

Степанов [3*] предложил новый подход к выводу асимптотической формулы для количества неприводимых многочленов фиксированной степени над $\mathbb{F}_q$, часть коэффициентов которых задана. Метод демонстрируется на примере многочленов четвертой степени с двумя фиксированными коэффициентами. В статье Варшамова [1*] дается алгоритм построения неприводимого многочлена данной степени над $\mathbb{F}_q$, имеющий полиномиальную сложность. Неприводимость некоторых трехчленов специального вида исследована в работе Agou [2*]. Шпарлинский [4*] доказал, что

при фиксированном n и достаточно большом простом числе p существует примитивный по модулю p многочлен степени n и высоты $H(f) = O(p^{n/(n+1)+\varepsilon})$. Этот результат при $n = 1$ переходит в известные оценки И. М. Виноградова [8] для наименьшего первообразного корня по модулю p. Кроме того, там показывается, что существуют примитивные многочлены, содержащие лишь $n/2 + O(1)$ ненулевых коэффициентов. В работе Car [3*] получены верхние и нижние оценки для количества многочленов степени N над $\mathbb{F}_q$, имеющих делитель степени n. Митькин [3*] получил нижние оценки для количества различных значений многочлена над простым полем $\mathbb{F}_p$, уточняющие результаты Морделла (Mordell [16]). Бурке (Burke [1*])ввел понятие плотности множества многочленов над конечным полем и получил для него аналоги соответствующих результатов, касающихся плотности множеств целых чисел. Свойства плотности множеств многочленов изучались также в работах Car [1*], [2*], [4*], [8*], [9*]. Эффингер (Effinger [1*]) исследовал аналог проблемы Гольдбаха для многочленов степени $\leqslant 6$.

По тематике третьей главы имеются также следующие работы: Agou [1*], [3*], Beard, Sue [1*], Car [6*], [7*], Claasen [1*], Hellegouarch [1*], Hensley [1*], Kaltofen [2*], Kaminski [1*], Kashiwagi, Moriuchi [1*], Kashiwagi, Uchimura [1*], Smits [1*], [2*], Варшамов [1*], Варшамов, Кожевников [1*], Кюрегян [2*], Маренич [1*] и Мурзаев [1*]. — *Перев.*]

Упражнения

3.1. Найти порядок многочлена $(x^2 + x + 1)^5 (x^3 + x + 1)$ над полем $\mathbb{F}_2$.

3.2. Найти порядок многочлена $x^7 - x^6 + x^4 - x^2 + x$ над полем $\mathbb{F}_3$.

3.3. Найти $\operatorname{ord}(f)$ для всех нормированных неприводимых многочленов f степени 3 из $\mathbb{F}_3[x]$.

3.4. Доказать, что многочлен $x^8 + x^7 + x^3 + x + 1$ неприводим над полем $\mathbb{F}_2$, и найти его порядок.

3.5. Пусть $f \in \mathbb{F}_q[x]$ — многочлен степени $m \geqslant 1$, удовлетворяющий условию $f(0) \neq 0$, и пусть корни $\alpha_1, \ldots, \alpha_m$ этого многочлена из его поля разложения над $\mathbb{F}_q$ просты. Доказать, что $\operatorname{ord}(f)$ равен наименьшему натуральному числу e, такому, что $\alpha_i^e = 1$ для $1 \leqslant i \leqslant m$.

3.6. Доказать, что $\operatorname{ord}(Q_e) = e$ для всех чисел e, для которых определен круговой многочлен $Q_e \in \mathbb{F}_q[x]$.

3.7. Пусть многочлен f неприводим над полем $\mathbb{F}_q$, причем $f(0) \neq 0$, и пусть e — натуральное число, взаимно простое с q. Доказать, что $\operatorname{ord}(f) = e$ тогда и только тогда, когда f делит круговой многочлен Q_e.

3.8. Пусть $f \in \mathbb{F}_q[x]$ — тот же многочлен, что и в упр. 3.5, и пусть $b \in \mathbb{N}$. Найти общую формулу, устанавливающую связь между $\operatorname{ord}(f^b)$ и $\operatorname{ord}(f)$.

3.9. Пусть $\mathbb{F}_q$ — конечное поле характеристики p, и пусть $f \in \mathbb{F}_q[x]$ — многочлен положительной степени, такой, что $f(0) \neq 0$. Доказать, что $\operatorname{ord}(f(x^p)) = p \operatorname{ord}(f(x))$.

3.10. Пусть f — неприводимый многочлен из $\mathbb{F}_q[x]$, такой, что $f(0) \neq 0$, и пусть $\operatorname{ord}(f) = e$ и r — простое число, не делящее q. Доказать, что

(i) если r делит e, то каждый неприводимый делитель многочлена $f(x^r)$ в $\mathbb{F}_q[x]$ имеет порядок er;

(ii) если r не делит e, то один из неприводимых делителей многочлена $f(x^r)$ в $\mathbb{F}_q[x]$ имеет порядок e, а остальные — порядок er.

3.11. Используя упр. 3.10, доказать, что если $f \in \mathbb{F}_q[x]$ — многочлен положительной степени, $f(0) \neq 0$ и r — простое число, не делящее q, то $\operatorname{ord}(f(x^r)) = r \cdot \operatorname{ord}(f(x))$.

3.12. Доказать, что возвратный многочлен (см. определение 3.12) к неприводимому многочлену f над $\mathbb{F}_q$, такому, что $f(0) \neq 0$, тоже неприводим над $\mathbb{F}_q$.

3.13. Ненулевой многочлен $f \in \mathbb{F}_q[x]$ называется *самовозвратным*, если $f^* = f$. Доказать, что если для неприводимых над $\mathbb{F}_q$ многочленов g и h многочлен $f = gh$ самовозвратен, то либо (i) $h^* = ag$, где $a \in \mathbb{F}_q^*$, либо (ii) $g^* = bg$, $h^* = bh$, где $b = \pm 1$.

3.14. Доказать, что если f — самовозвратный неприводимый многочлен из $\mathbb{F}_q[x]$ степени $m > 1$, то m должно быть четным числом.

3.15. Доказать, что если f — самовозвратный неприводимый многочлен из $\mathbb{F}_q[x]$ степени >1 и порядка e, то каждый неприводимый многочлен из $\mathbb{F}_q[x]$ степени $d > 1$, порядок которого делит e, самовозвратен.

3.16. Показать, что многочлен $x^6 + x^5 + x^2 + x + 1$ примитивен над полем $\mathbb{F}_2$.

3.17. Показать, что многочлен $x^8 + x^6 + x^5 + x + 1$ примитивен над полем $\mathbb{F}_2$.

3.18. Показать, что многочлен $x^5 - x + 1$ примитивен над полем $\mathbb{F}_3$.

3.19. Пусть $f \in \mathbb{F}_q[x]$ — нормированный многочлен степени $m \geqslant 1$. Доказать, что f примитивен над $\mathbb{F}_q$ тогда и только тогда, когда он является неприводимым делителем над $\mathbb{F}_q$ кругового многочлена $Q_d = \mathbb{F}_q[x]$, где $d = q^m - 1$.

3.20. Найти число примитивных многочленов степени m над полем $\mathbb{F}_q$.

3.21. Пусть натуральное число m не является простым. Доказать, что не каждый нормированный неприводимый многочлен над полем $\mathbb{F}_q$ степени m является примитивным многочленом над $\mathbb{F}_q$.

3.22. Пусть m — простое число. Доказать, что все нормированные неприводимые многочлены над полем $\mathbb{F}_q$ степени m примитивны над $\mathbb{F}_q$ в том и только том случае, если $q = 2$ и число $2^m - 1$ простое.

3.23. Пусть f — примитивный многочлен над полем $\mathbb{F}_q$. Доказать, что $f(0)^{-1} f^*$ — тоже примитивный многочлен над $\mathbb{F}_q$.

3.24. Доказать, что самовозвратными (см. упр. 3.13) примитивными многочленами над $\mathbb{F}_2$ являются лишь многочлены $x + 1$ и $x^2 + x + 1$, а над $\mathbb{F}_3$ — лишь многочлен $x + 1$.

3.25. Доказать, что если многочлен $f(x)$ неприводим в кольце $\mathbb{F}_q[x]$, то многочлен $f(ax + b)$ тоже неприводим в $\mathbb{F}_q[x]$ для любых $a, b \in \mathbb{F}_q$, $a \neq 0$.

3.26. Доказать, что $N_q(n) \leqslant (1/n)(q^n - q)$, причем равенство имеет место тогда и только тогда, когда n — простое число ($N_q(n)$ — число нормированных неприводимых многочленов степени n в $\mathbb{F}_q[x]$).

3.27. Доказать, что

$$N_q(n) \geqslant \frac{1}{n} q^n - \frac{q}{n(q-1)} (q^{n/2} - 1).$$

3.28. Дать строгое доказательство того, что из (3.5) вытекает (3.4).

3.29. Доказать, что функция Мёбиуса μ для всех натуральных взаимно простых чисел m и n удовлетворяет условию $\mu(mn) = \mu(m)\mu(n)$.

3.30. Доказать, что для всех натуральных чисел n имеет место равенство

$$\sum_{d \mid n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}.$$

3.31. Доказать, что для каждого четного целого числа $n \geqslant 2$

$$\sum_{d \mid n} \mu(d)\, \varphi(d) = 0.$$

3.32. Доказать равенство $\sum_{d \mid n} |\mu(d)| = 2^k$, где k — число различных простых делителей натурального числа n.

3.33. Доказать, что число $N_q(n)$ из упр. 3.26 делится на eq, если $n \geqslant 2$, e — некоторый делитель числа $q - 1$ и НОД $(eq, n) = 1$.

3.34. Применяя явную формулу из теоремы 3.27, найти круговые многочлены Q_{12} и Q_{30}.

3.35. Применяя явную формулу из теоремы 3.27, доказать свойства (a)—(f) кругового многочлена из упр. 2.57.

3.36. Доказать, что круговой многочлен Q_n неприводим над полем $\mathbb{F}_q$ при условии, что НОД $(q, n) = 1$, в том и только том случае, когда показатель, которому принадлежит q по модулю n, равен $\varphi(n)$.

3.37. Пусть круговой многочлен Q_n неприводим над полем $\mathbb{F}_2$. Доказать, что n должно быть либо простым числом, сравнимым с ± 3 по модулю 8, либо степенью такого числа. Показать также, что это условие не является достаточным.

3.38. Доказать, что круговой многочлен Q_{15} неприводим над каждым конечным полем, над которым он определен.

3.39. Пусть $n \in \mathbb{N}$. Доказать такое утверждение: для того чтобы существовало целое число b, взаимно простое с n и принадлежащее по модулю n показателю $\varphi(n)$, необходимо и достаточно, чтобы n было одним из чисел 1, 2, 4, p^r или $2p^r$, где p — нечетное простое число и $r \in \mathbb{N}$.

3.40. Теорема Дирихле о простых числах в арифметической прогрессии утверждает, что любая целочисленная арифметическая прогрессия b, $b + n$, ..., ..., $b + kn$, ..., где $b \in Z$, $n \in \mathbb{N}$ и НОД $(b, n) = 1$, содержит бесконечно много простых чисел.

Применить эту теорему для доказательства следующего предложения: если для натурального числа n существует конечное поле $\mathbb{F}_q$, такое, что НОД $(q, n) = 1$ и круговой многочлен Q_n неприводим над $\mathbb{F}_q$, то число n может принимать лишь следующие значения: 1, 2, 4, p^r или $2p^r$, где p — нечетное простое число и $r \in \mathbb{N}$.

3.41. Доказать, что круговые многочлены Q_{19} и Q_{27} над полем $\mathbb{F}_2$ имеют одну и ту же степень и неприводимы над $\mathbb{F}_2$.

3.42. Пусть $\mathbb{F}_q$ — конечное поле, $e > 1$, НОД $(e, q) = 1$ и m — показатель, которому принадлежит число q по модулю e. Доказать, что произведение всех нормированных неприводимых многочленов степени m и порядка e из $\mathbb{F}_q[x]$ является круговым многочленом Q_e над $\mathbb{F}_q$.

3.43. Найти разложение многочлена $x^{32} - x$ на неприводимые сомножители в кольце $\mathbb{F}_2[x]$.

3.44. Вычислить многочлен $I(2, 6; x)$ по формуле из теоремы 3.29.

3.45. Вычислить многочлен $I(2, 6; x)$ по формуле из теоремы 3.31.

3.46. Доказать, что

$$I(q, n; x) = \prod_{d \mid n} \left(x^{q^d} - 1\right)^{\mu(n/d)} \quad \text{для } n > 1.$$

3.47. Доказать, что над конечным полем нечетного порядка q многочлен

$$\frac{1}{2}\left(1 + x^{(q+1)/2} + (1 - x)^{(q+1)/2}\right)$$

является квадратом некоторого многочлена.

3.48. Найти в кольце $\mathbb{F}_2[x]$ все неприводимые многочлены степени 6 и порядка 21, а также степени 294 и порядка 1029.

3.49. Найти в кольце $\mathbb{F}_3[x]$ все нормированные неприводимые многочлены степени 3 и порядка 26, а также степени 6 и порядка 104.

3.50. Тем же способом, что и в примере 3.41, выяснить, какие из многочленов f_t неприводимы в кольце $\mathbb{F}_q[x]$ для случая $q = 5$, $m = 4$, $e = 78$.

3.51. В обозначениях примера 3.41 доказать, что если t — такое простое число, что $t - 1$ делит число $m - 1$, то многочлен f_t неприводим в кольце $\mathbb{F}_2[x]$.

3.52. В обозначениях примера 3.41 для данного неприводимого многочлена $f(x) = x^3 - x^2 + x + 1$ над полем $\mathbb{F}_3$ найти матричным способом многочлены f_2 и f_5.

3.53. Найти многочлены f_2 и f_5 из предыдущего упражнения с помощью теоремы 3.39.

3.54. Представить все элементы группы $\mathbb{F}_{29}^*$ через корень примитивного многочлена $x^3 - x + 1$ над $\mathbb{F}_3$ и найти минимальные многочлены над $\mathbb{F}_3$ для всех элементов поля $\mathbb{F}_{27}$.

3.55. Пусть $\theta \in \mathbb{F}_{64}$ — корень неприводимого многочлена $x^6 + x + 1 \in \mathbb{F}_2[x]$. Найти минимальный многочлен элемента $\beta = 1 + \theta^2 + \theta^3$ над полем $\mathbb{F}_2$.

3.56. Пусть $\theta \in \mathbb{F}_{64}$ — корень неприводимого многочлена $x^6 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$. Найти минимальный многочлен элемента $\beta = 1 + \theta + \theta^5$ над полем $\mathbb{F}_2$.

3.57. Найти все примитивные многочлены степени 2 над полем $\mathbb{F}_3$.

3.58. Найти все примитивные многочлены степени 2 над полем $\mathbb{F}_4$.

3.59. Найти примитивный многочлен степени 3 над полем $\mathbb{F}_5$.

3.60. Разложить многочлен $g \in \mathbb{F}_3[x]$ из примера 3.44 в кольце $\mathbb{F}_9[x]$ для получения примитивных многочленов над полем $\mathbb{F}_9$.

3.61. Разложить многочлен $g \in \mathbb{F}_2[x]$ из примера 3.45 в кольце $\mathbb{F}_8[x]$ для получения примитивных многочленов над полем $\mathbb{F}_8$.

3.62. Найти корни следующих линеаризованных многочленов из полей разложения этих многочленов:

(a) $L(x) = x^8 + x^4 + x^2 + x \in \mathbb{F}_2[x]$;
(b) $L(x) = x^9 + x \in \mathbb{F}_3[x]$.

3.63. Найти корни следующих многочленов в указанных полях, предварительно определив их аффинные кратные:

(a) $f(x) = x^7 + x^6 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ в $\mathbb{F}_{32}$;
(b) $f(x) = x^4 + \theta x^3 - x^2 - (\theta + 1)x + 1 - \theta \in \mathbb{F}_9[x]$ в $\mathbb{F}_{729}$, где θ — корень многочлена $x^2 - x - 1 \in \mathbb{F}_3[x]$.

3.64. Доказать, что для каждого многочлена f положительной степени над полем $\mathbb{F}_{q^m}$ существует ненулевой q-многочлен над $\mathbb{F}_{q^m}$, который делится на f.

3.65. Доказать, что наибольший общий делитель двух или более ненулевых q-многочленов над полем $\mathbb{F}_{q^m}$ снова является q-многочленом, но их наименьшее общее кратное не обязательно является q-многочленом.

3.66. Найти наибольший общий делитель двух линеаризованных многочленов:

(a) $L_1(x) = x^{64} + x^{16} + x^8 + x^4 + x^2 + x \in \mathbb{F}_2[x]$,
$L_2(x) = x^{32} + x^8 + x^2 + x \in \mathbb{F}_2[x]$;
(b) $L_1(x) = x^{243} - x^{81} - x^9 + x^3 + x \in \mathbb{F}_3[x]$,
$L_2(x) = x^{81} + x \in \mathbb{F}_3[x]$.

3.67. Найти символическое разложение следующих линеаризованных многочленов на символически неприводимые сомножители над указанными простыми полями:

(a) $L(x) = x^{32} + x^{16} + x^8 + x^4 + x^2 + x \in \mathbb{F}_2[x]$;
(b) $L(x) = x^{81} - x^9 - x^3 - x \in \mathbb{F}_3[x]$.

3.68. Доказать, что q-многочлен $L_1(x)$ над полем $\mathbb{F}_{q^m}$ делит q-многочлен $L(x)$ над $\mathbb{F}_{q^m}$ в том и только том случае, если $L(x) = L_2(x) \otimes L_1(x)$ для некоторого q-многочлена $L_2(x)$ над $\mathbb{F}_{q^m}$.

3.69. Доказать, что наибольший общий делитель двух или более аффинных q-многочленов над полем $\mathbb{F}_{q^m}$, не равных нулю одновременно, является аффинным q-многочленом.

3.70. Пусть $A_1(x) = L_1(x) - \alpha_1$ и $A_2(x) = L_2(x) - \alpha_2$ — два аффинных q-многочлена над полем $\mathbb{F}_{q^m}$. Доказать, что если $A_1(x)$ делит $A_2(x)$, то q-многочлен $L_1(x)$ делит q-многочлен $L_2(x)$.

3.71. Пусть $f(x) \in \mathbb{F}_q[x]$ — неприводимый многочлен, такой, что $f(0) \neq 0$, и пусть $F(x)$ — линеаризованный q-ассоциированный с ним многочлен. Доказать, что многочлен $F(x)/x$ неприводим в кольце $\mathbb{F}_q[x]$ тогда и только тогда, когда $f(x)$ является примитивным многочленом над $\mathbb{F}_q$ или отличается от такого многочлена ненулевым постоянным множителем.

3.72. Пусть ζ — элемент из конечного расширения поля $\mathbb{F}_{q^m}$. Доказать, что ζ является корнем q-многочлена $K(x)$ над $\mathbb{F}_{q^m}$ тогда и только тогда, когда $K(x)$ делится на минимальный q-многочлен элемента ζ над $\mathbb{F}_{q^m}$.

3.73. Доказать, что для ненулевого многочлена $f \in \mathbb{F}_q[x]$

$$\sum \Phi_q(g) = q^{\deg(f)},$$

где сумма распространяется на все нормированные делители $g \in \mathbb{F}_q[x]$ многочлена f, а функция Φ_q введена перед леммой 3.69.

3.74. Для ненулевого многочлена $f \in \mathbb{F}_q[x]$ и многочлена $g \in \mathbb{F}_q[x]$, удовлетворяющих условию НОД $(f, g) = 1$, доказать, что $g^k \equiv 1 \pmod f$, где $k = \Phi_q(f)$.

3.75. Определим функцию μ_q на множестве S ненулевых многочленов f из кольца $\mathbb{F}_q[x]$ следующим образом: $\mu_q(f) = 1$, если $\deg(f) = 0$; $\mu_q(f) = 0$, если f имеет хотя бы один кратный корень; $\mu_q(f) = (-1)^k$, если $\deg(f) \geqslant 1$, f имеет лишь простые корни и k — число неприводимых сомножителей в каноническом разложении многочлена f в кольце $\mathbb{F}_q[x]$. Доказать следующие свойства:

(a) $\sum \mu_q(g) = \begin{cases} 1, & \text{если } \deg(f) = 0, \\ 0, & \text{если } \deg(f) \geqslant 1; \end{cases}$

(b) $\mu_q(fg) = \mu_q(f)\,\mu_q(g)$ для всех $f, g \in S$, таких, что НОД $(f, g) = 1$;

(c) $\sum q^{\deg(g)} \mu_q(f/g) = \Phi_q(f)$ для всех $f \in S$;

(d) если ψ — отображение из S в аддитивную абелеву группу G, обладающее свойством $\psi(cf) = \psi(f)$ для всех $c \in \mathbb{F}_q^*$ и $f \in S$, и $\Psi(f) = \sum \psi(g)$ для всех $f \in S$, то $\psi(f) = \sum \mu_q(f/g)\,\Psi(g) = \sum \mu_q(g)\,\Psi(f/g)$ для всех $f \in S$.

Здесь $\sum$ обозначает сумму, распространенную на все нормированные делители $g \in \mathbb{F}_q[x]$ многочлена f.

3.76. Доказать, что число различных нормальных базисов поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ равно

$$\frac{1}{m} \prod_{d \mid m} (q^{\varphi(d)} - 1)$$

при условии, что НОД $(m, q) = 1$ и показатель, которому принадлежит число q по модулю m, равен $\varphi(m)$.

3.77. Определение автодуального базиса было дано в примере 2.31. Показать, что при нечетном числе m автодуальный базис поля $\mathbb{F}_{2^m}$ над $\mathbb{F}_2$ существует. (*Указание.* Показать предварительно, что число различных нормальных базисов поля $\mathbb{F}_{2^m}$ над $\mathbb{F}_2$ нечетно, если нечетно число m.)

3.78. Доказать, что если r — простое число и $a \in \mathbb{F}_q$, то либо двучлен $x^r - a$ неприводим в кольце $\mathbb{F}_q[x]$, либо он имеет корень в поле $\mathbb{F}_q$.

3.79. Доказать, что если r — нечетное простое число, $n \in \mathbb{N}$ и $a \in \mathbb{F}_q$, то многочлен $x^{r^n} - a$ неприводим в кольце $\mathbb{F}_q[x]$ тогда и только тогда, когда элемент a не является r-й степенью элемента из $\mathbb{F}_q$.

3.80. Найти каноническое разложение над указанными простыми полями следующих двучленов:

(a) $f(x) = x^8 + 1 \in \mathbb{F}_3[x]$;

(b) $f(x) = x^{27} - 4 \in \mathbb{F}_{19}[x]$;

(c) $f(x) = x^{88} - 10 \in \mathbb{F}_{23}[x]$.

3.81. Доказать, что в условиях теоремы 3.76 корни введенного там многочлена $F(x)$ просты.

3.82. Доказать, что результант двух двучленов $x^m - a$ и $x^n - b$ в кольце $\mathbb{F}_q[x]$ задается выражением $(-1)^m (b^{m/d} - a^{n/d})^d$, где $d = \text{НОД}(m, n)$. Здесь m и n рассматриваются как формальные степени этих двучленов (ср. с определением 1.93).

3.83. Пусть b — ненулевой элемент из простого поля $\mathbb{F}_p$. Доказать, что трехчлен $x^p - x - b$ неприводим в кольце $\mathbb{F}_{p^n}[x]$ тогда и только тогда, когда n не делится на p.

3.84. Доказать, что любой трехчлен вида $x^q - ax - b \in \mathbb{F}_q[x]$ при $a \neq 1$ имеет корень в поле $\mathbb{F}_q$.

3.85. Доказать такое предложение: если трехчлен $x^p - x - a$ неприводим над полем $\mathbb{F}_q$ характеристики p и β — корень этого трехчлена в некотором расширении поля $\mathbb{F}_q$, то трехчлен $x^p - x - a\beta^{p-1}$ неприводим над полем $\mathbb{F}_q(\beta)$.

3.86. Доказать следующее предложение: если $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ — неприводимый многочлен над полем $\mathbb{F}_q$ характеристики p и b — такой элемент из $\mathbb{F}_q$, что $\text{Tr}_{\mathbb{F}_q}(mb - a_{m-1}) = 0$, то многочлен $f(x^p - x - b)$ разлагается в произведение p неприводимых сомножителей над $\mathbb{F}_q$ степени m.

3.87. Доказать, что если m и p — различные простые числа и число p по модулю m принадлежит показателю $m - 1$, то многочлен $\sum_{i=0}^{m-1} (x^p - x)^i$ неприводим над полем $\mathbb{F}_p$.

3.88. Найти каноническое разложение над указанными полями следующих многочленов:

(a) $f(x) = x^8 - \alpha x - 1 \in \mathbb{F}_{64}[x]$, где α удовлетворяет равенству $\alpha^3 = \alpha + 1$;

(b) $f(x) = x^9 - \alpha x + \alpha \in \mathbb{F}_9[x]$, где α удовлетворяет равенству $\alpha^2 = \alpha + 1$.

3.89. Пусть $A(x) = L(x) - \alpha \in \mathbb{F}_q[x]$ — аффинный p-многочлен степени $r > 2$ и $L(x)$ — такой p-многочлен над $\mathbb{F}_q$, что многочлен $L(x)/x$ неприводим над полем $\mathbb{F}_q$. Доказать, что $A(x)$ является произведением линейного многочлена и неприводимого многочлена над $\mathbb{F}_q$ степени $r - 1$.

3.90. Доказать, что трехчлен $x^n + ax^k + b \in \mathbb{F}_q[x]$, $n > k \geqslant 1$, при четном числе q имеет кратные корни в том и только том случае, если оба числа n и k тоже четны.

3.91. Доказать, что степень каждого неприводимого делителя трехчлена $x^{2^n} + x + 1$ в кольце $\mathbb{F}_2[x]$ делит число $2n$.

3.92. Доказать, что степень каждого неприводимого делителя трехчлена $x^{2^n+1} + x + 1$ в кольце $\mathbb{F}_2[x]$ делит число $3n$.

3.93. Доказать, что если $f \in \mathbb{F}_2[x]$ — самовозвратный многочлен (см. упр. 3.13) положительной степени, то он делит некоторый трехчлен из $\mathbb{F}_2[x]$ лишь в том случае, если $\text{ord}(f)$ делится на 3. Доказать также, что обратное утверждение справедливо, если многочлен f неприводим над полем $\mathbb{F}_2$.

3.94. Доказать, что если $d \in \mathbb{N}$ — нечетное число, то круговой многочлен $Q_d \in \mathbb{F}_2[x]$ делит некоторый трехчлен из $\mathbb{F}_2[x]$ тогда и только тогда, когда d кратно трем.

3.95. Пусть $f(x) = x^n + ax^k + b \in \mathbb{F}_q[x]$, $n > k \geqslant 1$, и пусть число $m \in \mathbb{N}$ кратно $\operatorname{ord}(f)$. Доказать, что $f(x)$ делит трехчлен $g(x) = x^{m-k} + b^{-1}x^{n-k} + ab^{-1}$.

3.96. Доказать, что трехчлен $x^{2n} + x^n + 1$ неприводим над полем $\mathbb{F}_2$ тогда и только тогда, когда $n = 3^k$ для некоторого целого неотрицательного числа k.

3.97. Доказать, что трехчлен $x^{4n} + x^n + 1$ неприводим над полем $\mathbb{F}_2$ тогда и только тогда, когда $n = 3^k 5^m$ для некоторых целых неотрицательных чисел k и m.

Глава 4

Разложение многочленов на множители

Любой непостоянный многочлен над заданным полем можно разложить в произведение неприводимых многочленов. Если рассматриваемое поле конечно, то для фактического вычисления неприводимых сомножителей данного многочлена положительной степени над этим полем существуют весьма эффективные алгоритмы.

Наличие таких алгоритмов для многочленов над конечными полями особенно важно для теории кодирования и для изучения линейных рекуррентных соотношений в конечных полях. Но и вне области конечных полей в алгебре и теории чисел имеется много вычислительных задач, которые так или иначе связаны с разложением многочленов над конечными полями. В этой связи можно упомянуть, например, разложение на множители многочленов над кольцом целых чисел, отыскание разложений простых рациональных чисел в полях алгебраических чисел, вычисление группы Галуа некоторого уравнения над полем рациональных чисел и построение расширений полей.

Здесь будет изложено несколько алгоритмов разложения многочленов над конечными полями. Выбор конкретного алгоритма обычно зависит от того, «малым» или «большим» является данное конечное поле. В § 1 мы опишем те алгоритмы, которые более удобны для «малых» полей, а в § 2 — те, которые лучше работают для «больших» конечных полей. Некоторые из этих алгоритмов сводят проблему разложения многочленов к задаче отыскания корней некоторых других многочленов. Поэтому в § 3 вопрос об отыскании корней многочленов рассматривается с вычислительной точки зрения.

§ 1. Разложение многочленов над малыми конечными полями

Для любого многочлена $f \in \mathbb{F}_q[x]$ положительной степени существует каноническое разложение в кольце $\mathbb{F}_q[x]$ (теорема 1.59). При построении алгоритма такого разложения, очевидно, достаточно ограничиться рассмотрением лишь нормирован-

ных многочленов. Таким образом, нашей целью является представление нормированного многочлена $f \in \mathbb{F}_q[x]$ положительной степени в виде произведения

$$f = f_1^{e_1} \dots f_k^{e_k}, \tag{4.1}$$

где $f_1, \dots, f_k$ — различные нормированные неприводимые делители многочлена f в кольце $\mathbb{F}_q[x]$, а $e_1, \dots, e_k$ — натуральные числа.

Прежде всего мы упростим свою задачу, показав, что указанную проблему можно свести к проблеме разложения многочлена *без кратных* неприводимых *сомножителей*, т. е. такого многочлена f, для которого в каноническом разложении (4.1) все показатели $e_1, \dots, e_k$ равны единице (это равносильно отсутствию у многочлена f кратных корней). Для этого мы сначала найдем, применяя алгоритм Евклида, многочлен

$$d(x) = \text{НОД}(f(x), f'(x))$$

— наибольший общий делитель многочлена f и его производной f'.

Если $d(x) = 1$, то в силу теоремы 1.68 многочлен $f(x)$ не имеет кратных сомножителей [1]). Рассмотрим случай, когда $d(x) = f(x)$. Тогда, очевидно, должно быть $f'(x) = 0$, а это значит, что $f(x) = g(x)^p$ для некоторого многочлена $g(x) \in \mathbb{F}_q[x]$, где p — характеристика поля $\mathbb{F}_q$. Указанную процедуру редукции можно, если это необходимо, повторить применительно к многочлену $g(x)$ и т. д., пока не получим представление $f(x) = h(x)^{p^s}$, где $h'(x) \neq 0$.

Если же многочлен $d(x)$ отличен от 1 и от $f(x)$, то он является нетривиальным делителем многочлена $f(x)$, и в этом случае многочлен $f(x)/d(x)$ не имеет кратных неприводимых сомножителей. Мы придем к разложению $f(x)$, разложив по отдельности многочлены меньшей степени $d(x)$ и $f(x)/d(x)$. В случае если многочлен $d(x)$ все еще имеет кратные множители, мы для него повторяем указанный процесс редукции.

Применив этот процесс нужное число раз, мы сведем исходную проблему к задаче разложения некоторого числа многочленов, не имеющих кратных неприводимых сомножителей. Канонические разложения этих многочленов сразу же приведут к каноническому разложению исходного многочлена. Эти соображения позволяют нам сосредоточить свое внимание на многочленах, не имеющих кратных неприводимых сомножителей. Следующая теорема является основной.

---

[1]) Речь идет о каноническом разложении. — *Прим. перев.*

4.1. Теорема. *Если* $f \in \mathbb{F}_q[x]$ *— нормированный многочлен положительной степени и многочлен* $h \in \mathbb{F}_q[x]$ *удовлетворяет условию* $h^q \equiv h \pmod f$, *то*

$$f(x) = \prod_{c \in \mathbb{F}_q} \text{НОД}(f(x),\ h(x) - c). \tag{4.2}$$

Доказательство. Каждый наибольший общий делитель из правой части равенства (4.2) делит многочлен $f(x)$. Поскольку многочлены $h(x) - c$, $c \in \mathbb{F}_q$, попарно взаимно просты, то взаимно простыми являются и их наибольшие общие делители с $f(x)$, т. е. сомножители правой части (4.2), и, следовательно, правая часть равенства (4.2) делит многочлен $f(x)$. С другой стороны, многочлен $f(x)$ делит разность

$$h(x)^q - h(x) = \prod_{c \in \mathbb{F}_q} (h(x) - c),\ .$$

и, значит, $f(x)$ делит правую часть равенства (4.2). Итак, обе части (4.2) являются нормированными многочленами, каждый из которых делит другой, и, значит, они должны совпадать. □

Вообще говоря, формула (4.2) не дает полного разложения многочлена f, поскольку многочлен НОД $(f(x), h(x) - c)$ может оказаться приводимым в кольце $\mathbb{F}_q[x]$. Если же $h(x) \equiv c \pmod{f(x)}$ для некоторого $c \in \mathbb{F}_q$, теорема 4.1 вообще приводит к тривиальному разложению $f(x)$ и потому бесполезна. Если многочлен $h(x)$ таков, что теорема 4.1 приводит к нетривиальному разложению многочлена $f(x)$, он называется *f-разлагающим многочленом*. Любой многочлен $h \in \mathbb{F}_q[x]$, обладающий свойствами $h^q \equiv h \pmod f$ и $0 < \deg(h) < \deg(f)$, очевидно, является f-разлагающим. Чтобы на основе теоремы 4.1 получить алгоритмы разложения, мы должны найти способы построения f-разлагающих многочленов. Но уже на этом этапе ясно, что, поскольку разложение, основанное на формуле (4.2), связано с вычислением q наибольших общих делителей, то прямое применение этой формулы возможно лишь для малых конечных полей $\mathbb{F}_q$ (т. е. для небольших значений q).

Первый способ построения f-разлагающих многочленов использует китайскую теорему об остатках для многочленов (см. упр. 1.37). Допустим, что многочлен f не имеет кратных сомножителей, так что $f = f_1 \dots f_k$ — произведение различных нормированных неприводимых многочленов над полем $\mathbb{F}_q$. Тогда для любого k-набора $(c_1, \dots, c_k)$ элементов поля $\mathbb{F}_q$, согласно китайской теореме об остатках, существует единственный многочлен $h \in \mathbb{F}_q[x]$, такой, что $h(x) \equiv c_i \pmod{f_i(x)}$, $1 \leqslant i \leqslant k$, и $\deg(h) < \deg(f)$. Этот многочлен удовлетворяет условию

$$h(x)^q \equiv c_i^q \equiv c_i \equiv h(x) \pmod{f_i(x)}, \quad i = 1, \dots, k,$$

и потому

$$h^q \equiv h (\mathrm{mod}\, f), \quad \deg(h) < \deg(f). \tag{4.3}$$

С другой стороны, если многочлен h является решением сравнения (4.3), то из равенства

$$h(x)^q - h(x) = \prod_{c \in \mathbb{F}_q} (h(x) - c)$$

в силу попарной взаимной простоты сомножителей правой части следует, что каждый неприводимый делитель многочлена f должен делить один и только один из многочленов $h(x) - c$. Таким образом, каждое решение $h(x)$, $\deg(h) < \deg(f)$, сравнения (4.3) удовлетворяет системе сравнений $h(x) \equiv c_i (\mathrm{mod}\, f_i(x))$, $i = 1, \ldots, k$, для некоторого k-набора $(c_1, \ldots, c_k)$ элементов поля $\mathbb{F}_q$. Следовательно, сравнение (4.3) имеет ровно q^k решений.

Чтобы найти эти решения, сведем сравнение (4.3) к системе линейных уравнений. Полагая $\deg(f) = n$ и вычисляя x^{iq} по модулю $f(x)$, построим $n \times n$-матрицу $B = (b_{ij})$, $0 \leqslant i, j \leqslant n - 1$. А именно

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j (\mathrm{mod}\, f(x)), \quad i = 0, 1, \ldots, n-1. \tag{4.4}$$

Тогда многочлен $h(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in \mathbb{F}_q[x]$ будет решением сравнения (4.3) в том и только том случае, когда $(a_0, a_1, \ldots, a_{n-1})$ является решением системы линейных уравнений (записанной в матричной форме)

$$(a_0, a_1, \ldots, a_{n-1}) B = (a_0, a_1, \ldots, a_{n-1}). \tag{4.5}$$

Это следует из того факта, что равенство (4.5) выполняется тогда и только тогда, когда

$$h(x) = \sum_{j=0}^{n-1} a_j x^j = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i b_{ij} x^j \equiv$$
$$\equiv \sum_{i=0}^{n-1} a_i x^{iq} \equiv h(x)^q (\mathrm{mod}\, f(x)).$$

Систему (4.5) можно записать в следующей эквивалентной форме:

$$(a_0, a_1, \ldots, a_{n-1})(B - I) = (0, 0, \ldots, 0), \tag{4.6}$$

где I — единичная $n \times n$-матрица над $\mathbb{F}_q$. Согласно доказанному выше, однородная система (4.6) имеет q^k решений. Это означает, что *размерность пространства решений* [1]) *этой системы равна* k,

[1]) Это пространство называют также *аннулируемым пространством* или *нуль-пространством* матрицы $B - I$. — *Прим. перев.*

т. е. числу различных нормированных неприводимых делителей многочлена f, а *ранг матрицы* $B-I$ *равен* $n-k$.

Поскольку постоянный многочлен $h_1(x)=1$ всегда является решением сравнения (4.3), то соответствующий ему вектор $(1, 0, \ldots, 0)$ всегда является решением системы (4.6), в чем можно убедиться также и прямой подстановкой. Кроме того, найдутся еще непостоянные многочлены $h_2(x), \ldots, h_k(x)$ со степенями, не превосходящими $n-1$, такие, что соответствующие им и многочлену $h_1(x)$ векторы образуют базис пространства решений однородной системы (4.6). Поскольку все многочлены $h_2(x), \ldots, h_k(x)$ непостоянны и удовлетворяют сравнению (4.3), то они являются f-разлагающими многочленами.

При таком подходе важную роль играет отыскание ранга r матрицы $B-I$. Как было отмечено выше, $r=n-k$; поэтому, найдя ранг r, мы тем самым находим *число* $k=n-r$ *различных нормированных неприводимых делителей многочлена* f. А это позволяет судить о том, до каких пор нужно продолжать процедуру разложения.

Ранг матрицы $B-I$ обычно определяется приведением этой матрицы к ступенчатому виду с помощью элементарных преобразований ее строк и столбцов. Однако, поскольку мы хотим в то же время решить систему (4.6), целесообразно применять лишь преобразования столбцов, поскольку пространство решений этой однородной системы инвариантно относительно таких преобразований. Итак, мы допускаем следующие элементарные операции: перемена местами двух столбцов матрицы $B-I$, умножение любого ее столбца на ненулевой элемент поля $\mathbb{F}_q$ и прибавление к любому ее столбцу другого столбца, умноженного на любой элемент из $\mathbb{F}_q$. Ранг r матрицы $B-I$ — это число ненулевых столбцов полученной матрицы ступенчатого вида.

Вычислив r, мы найдем число $k=n-r$. Если $k=1$, то мы заключаем, что f — неприводимый многочлен над $\mathbb{F}_q$, и процедура на этом заканчивается. В этом случае единственными решениями сравнения (4.3) являются постоянные многочлены, и пространство решений системы (4.6) состоит лишь из векторов вида $(c, 0, \ldots, 0)$, где $c \in \mathbb{F}_q$. Если же $k \geqslant 2$, то мы берем f-разлагающий базисный многочлен $h_2(x)$ и находим наибольшие общие делители НОД $(f(x), h_2(x)-c)$ для всех $c \in \mathbb{F}_q$. В результате получим некоторое нетривиальное разложение многочлена $f(x)$, даваемое формулой (4.2). Если использование многочлена $h_2(x)$ еще не приводит к разложению многочлена f на k сомножителей, то переходим к следующему f-разлагающему базисному многочлену $h_3(x)$ и находим НОД $(g(x), h_3(x)-c)$ для всех $c \in \mathbb{F}_q$ и всех нетривиальных делителей $g(x)$ многочлена $f(x)$, найденных по формуле (4.2) на первом этапе. Эта процедура продолжается до тех пор,

пока мы не получим все k неприводимых сомножителей многочлена $f(x)$.

Описанный процесс должен в конечном счете привести к нахождению всех неприводимых делителей многочлена $f(x)$. Действительно, если рассмотреть два различных нормированных неприводимых делителя многочлена $f(x)$, например $f_1(x)$ и $f_2(x)$, то рассуждение, следующее за сравнением (4.3), показывает, что для каждого j, $1 \leqslant j \leqslant k$, существуют элементы c_{j1} и c_{j2} из поля $\mathbb{F}_q$, такие, что выполняются сравнения $h_j(x) \equiv c_{j1} \pmod{f_1(x)}$, $h_j(x) \equiv c_{j2} \pmod{f_2(x)}$. Допустим, что $c_{j1} = c_{j2}$ для всех j, $1 \leqslant j \leqslant k$. Тогда, учитывая, что любое решение $h(x)$ сравнения (4.3) является линейной комбинацией базисных многочленов $h_1(x), \ldots, h_k(x)$ с коэффициентами из $\mathbb{F}_q$, получаем, что для любого такого решения $h(x)$ существует элемент $c \in \mathbb{F}_q$, такой, что $h(x) \equiv c \pmod{f_1(x)}$, $h(x) \equiv c \pmod{f_2(x)}$. Но рассуждение, которое привело к сравнению (4.3), показывает, что существует, в частности, и такое решение $h(x)$ сравнения (4.3), что $h(x) \equiv 0 \pmod{f_1(x)}$ и $h(x) \equiv 1 \pmod{f_2(x)}$. Полученное противоречие доказывает, что $c_{j1} \neq c_{j2}$ для некоторого j, $1 \leqslant j \leqslant k$ (точнее, для некоторого j, $2 \leqslant j \leqslant k$, поскольку $h_1(x) = 1$). Поэтому многочлен $h_j(x) - c_{j1}$ будет делиться на $f_1(x)$, но не на $f_2(x)$. Отсюда следует, что любые два различных нормированных неприводимых делителя многочлена $f(x)$ обязательно «отделимы» друг от друга (в указанном смысле) некоторым базисным многочленом $h_j(x)$.

Этот алгоритм разложения многочлена f, основанный на нахождении f-разлагающих многочленов (путем решения системы (4.6) линейных уравнений) носит название *алгоритма Берлекэмпа*.

4.2. Пример. Разложим многочлен $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ над полем $\mathbb{F}_2$, применяя алгоритм Берлекэмпа. Так как НОД $(f(x), f'(x)) = 1$, то многочлен $f(x)$ не имеет кратных сомножителей. Нам требуется найти вычеты одночленов x^{iq} по модулю $f(x)$ для $q = 2$ и $i = 0, 1, \ldots, 7$. Это приводит к следующим сравнениям по модулю $f(x)$:

$$
\begin{aligned}
x^0 &\equiv 1, \\
x^2 &\equiv x^2, \\
x^4 &\equiv x^4, \\
x^6 &\equiv x^6, \\
x^8 &\equiv 1 + x^3 + x^4 + x^6, \\
x^{10} &\equiv 1 + x^2 + x^3 + x^4 + x^5, \\
x^{12} &\equiv x^2 + x^4 + x^5 + x^6 + x^7, \\
x^{14} &\equiv 1 + x + x^3 + x^4 + x^5.
\end{aligned}
$$

Поэтому 8×8-матрица B имеет вид

$$B=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0\\1&0&0&1&1&0&1&0\\1&0&1&1&1&1&0&0\\0&0&1&0&1&1&1&1\\1&1&0&1&1&1&0&0\end{pmatrix},$$

а матрица $B-I$ имеет вид

$$B-I=\begin{pmatrix}0&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0\\0&0&1&0&1&0&0&0\\0&0&0&1&0&0&1&0\\1&0&0&1&0&0&1&0\\1&0&1&1&1&0&0&0\\0&0&1&0&1&1&0&1\\1&1&0&1&1&1&0&1\end{pmatrix}.$$

Несложные вычисления показывают, что матрица $B-I$ имеет ранг 6 и векторы $(1, 0, 0, 0, 0, 0, 0, 0)$ и $(0, 1, 1, 0, 0, 1, 1, 1)$ образуют базис пространства решений однородной системы (4.6), соответствующей матрице $B-I$. Этим векторам соответствуют многочлены $h_1(x)=1$ и $h_2(x)=x+x^2+x^5+x^6+x^7$. Вычисляя при помощи алгоритма Евклида НОД $(f(x), h_2(x)-c)$ для элементов $c\in\mathbb{F}_2$, получаем, что НОД $(f(x), h_2(x))=x^6+x^5+x^4+x+1$, НОД $(f(x), h_2(x)-1)=x^2+x+1$. В итоге получаем следующее каноническое разложение многочлена $f(x)$:

$$f(x)=(x^6+x^5+x^4+x+1)(x^2+x+1). \qquad \square$$

Другой метод получения f-разлагающих многочленов связан с построением некоторого семейства многочленов, в котором имеется по крайней мере один f-разлагающий многочлен. Пусть снова f обозначает произвольный нормированный многочлен степени $n>1$, не имеющий кратных сомножителей, и пусть $f=f_1\dots f_k$ — его каноническое разложение в кольце $\mathbb{F}_q[x]$, причем $\deg(f_j)=n_j$ для $1\leqslant j\leqslant k$. Если N — наименьшее натуральное число, такое, что $x^{q^N}\equiv x \pmod{f(x)}$, то из теоремы 3.20 получаем, что $N=\text{НОК}(n_1, \dots, n_k)$, при этом также нетрудно видеть, что N — степень поля разложения F многочлена f над $\mathbb{F}_q$. Рассмотрим многочлен $T\in\mathbb{F}_q[x]$ вида $T(x)=x+x^q+x^{q^2}+\dots+x^{q^{N-1}}$.

Положим $T_i(x) = T(x^i)$ для $i \in \mathbb{N}$. Следующий результат показывает, что в рассматриваемом случае (когда многочлен $f(x)$ приводим в кольце $\mathbb{F}_q[x]$ и не имеет кратных сомножителей) среди многочленов $T_i(x)$, $1 \leqslant i \leqslant n$, найдется хотя бы один f-разлагающий многочлен.

4.3. Теорема. *Пусть многочлен без кратных сомножителей $f \in \mathbb{F}_q[x]$ приводим в $\mathbb{F}_q[x]$. Тогда (во введенных выше обозначениях) по крайней мере один из многочленов T_i, $1 \leqslant i \leqslant n-1$, является f-разлагающим многочленом.*

Доказательство. Учитывая сравнения $x^{q^N} \equiv x \pmod{f(x)}$, мы видим, что каждый из многочленов T_i удовлетворяет условию $T_i^q \equiv T_i \pmod f$. Допустим теперь, что для всех многочленов T_i, $1 \leqslant i \leqslant n-1$, разложение многочлена f, даваемое формулой (4.2), тривиально (при $h = T_i$). Это означает, что существуют элементы $c_1, \ldots, c_{n-1} \in \mathbb{F}_q$, такие, что $T_i(x) \equiv c_i \pmod{f(x)}$ для $i = 1, \ldots, n-1$. Рассматривая $c_0 = N$ как элемент поля $\mathbb{F}_q$, получаем сравнения $T(x^i) \equiv c_i \pmod{f(x)}$, $i = 0, 1, \ldots, n-1$. Для любого многочлена

$$g(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q[x]$$

степени меньше n мы имеем тогда

$$T(g(x)) = T\left(\sum_{i=0}^{n-1} a_i x^i\right) = \sum_{i=0}^{n-1} a_i T(x^i) \equiv \sum_{i=0}^{n-1} a_i c_i \pmod{f(x)}.$$

Полагая

$$c(g) = \sum_{i=0}^{n-1} a_i c_i \in \mathbb{F}_q,$$

получим

$$T(g(x)) \equiv c(g) \pmod{f_j(x)}, \quad j = 1, \ldots, k. \tag{4.7}$$

Так как $N = \text{НОК}(n_1, \ldots, n_k)$, то по крайней мере одно из целых чисел N/n_j, скажем N/n_1, не делится [1]) на характеристику поля $\mathbb{F}_q$. Пусть θ_1 — корень многочлена f_1 из поля разложения F_1 этого многочлена над $\mathbb{F}_q$. В силу теоремы 2.23 (iii) существует [2]) многочлен $g_1 \in \mathbb{F}_q[x]$, такой, что $\deg(g_1) < \deg(f_1)$ и

$$\mathrm{Tr}_{F_1/\mathbb{F}_q}(g_1(\theta_1)) = 1. \tag{4.8}$$

---

[1]) Так как НОД $\left(\frac{N}{n_1}, \ldots, \frac{N}{n_k}\right) = 1$. — *Прим. перев.*

[2]) Учитывая, что $F_1 = \mathbb{F}_q(\theta_1)$. — *Прим. перев.*

Ввиду того что $k \geqslant 2$ (по предположению), мы можем применить китайскую теорему об остатках и получить такой многочлен $g \in \mathbb{F}_q[x]$ степени меньше n, что

$$g \equiv g_1 \pmod{f_1}, \quad g \equiv 0 \pmod{f_2}. \tag{4.9}$$

Из (4.8) и (4.9) следует, что

$$\mathrm{Tr}_{F_1/\mathbb{F}_q}(g(\theta_1)) = 1,$$

так что из теорем 2.23(iv) и 2.26 получаем равенство

$$\mathrm{Tr}_{F/\mathbb{F}_q}(g(\theta_1)) = N/n_1,$$

где F — поле разложения многочлена f над $\mathbb{F}_q$. Из определений следа и элемента θ_1 вытекает, что

$$T(g(x)) \equiv N/n_1 \pmod{f_1(x)}.$$

Однако второе сравнение в (4.9) приводит к сравнению $T(g(x)) \equiv 0 \pmod{f_2(x)}$, и, поскольку число N/n_1 как элемент поля $\mathbb{F}_q$ отлично от нуля, мы получаем противоречие с (4.7). Это противоречие означает, что по крайней мере один из многочленов T_i, $1 \leqslant i \leqslant n-1$, является f-разлагающим. □

4.4. **Пример.** Разложим многочлен

$$f(x) = x^{17} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x + 1 \in \mathbb{F}_2[x],$$

Поскольку НОД $(f(x), f'(x)) = x^{10} + x^8 + 1$, то многочлен $f_0(x) = f(x)/\text{НОД}(f(x), f'(x)) = x^7 + x^5 + x^4 + x + 1$ не имеет кратных сомножителей. Разложим $f_0(x)$ описанным выше методом, найдя f_0-разлагающий многочлен. Для этого будем приводить по модулю $f_0(x)$ степени x, x^2, x^4, x^8, ..., пока не найдем наименьшего натурального числа N, такого, что $x^{2^N} \equiv x \pmod{f_0(x)}$. Для упрощения записи условимся многочлен $\sum_{i=0}^{n-1} a_i x^i$ обозначать n-набором (вектором) $(a_0, a_1, \ldots, a_{n-1})$ из его коэффициентов; в частности, $f_0(x) = (1, 1, 0, 0, 1, 1, 0, 1)$. Подсчет нужных степеней переменной x по модулю $f_0(x)$ упрощается, если заметить, что квадрат многочлена $(a_0, a_1, \ldots, a_6)$ по модулю $f_0(x)$ совпадает (в векторной записи) с произведением вектора $(a_0, a_1, \ldots, a_6)$ на квадратную матрицу порядка 7, образованную четными степенями переменной x, а именно x^0, x^2, ..., x^{12}, приведениыми по модулю $f_0(x)$. Эта матрица получается из правых частей следующих сравнений (по модулю $f_0(x)$):

$$x^0 \equiv (1, 0, 0, 0, 0, 0, 0),$$
$$x^2 \equiv (0, 0, 1, 0, 0, 0, 0);$$

$$x^4 \equiv (0, 0, 0, 0, 1, 0, 0),$$
$$x^6 \equiv (0, 0, 0, 0, 0, 0, 1),$$
$$x^8 \equiv (0, 1, 1, 0, 0, 1, 1),$$
$$x^{10} \equiv (1, 0, 1, 1, 0, 0, 1),$$
$$x^{12} \equiv (0, 1, 0, 0, 1, 0, 1).$$

Произведя теперь с помощью этой матрицы последовательные возведения в квадрат, получим (по модулю $f_0(x)$)

$$x \equiv (0, 1, 0, 0, 0, 0, 0),$$
$$x^2 \equiv (0, 0, 1, 0, 0, 0, 0),$$
$$x^4 \equiv (0, 0, 0, 0, 1, 0, 0),$$
$$x^8 \equiv (0, 1, 1, 0, 0, 1, 1),$$
$$x^{16} \equiv (1, 1, 0, 1, 0, 0, 0),$$
$$x^{32} \equiv (1, 0, 1, 0, 0, 0, 1),$$
$$x^{64} \equiv (1, 1, 0, 0, 0, 0, 1),$$
$$x^{128} \equiv (1, 1, 1, 0, 1, 0, 1),$$
$$x^{256} \equiv (1, 0, 0, 0, 0, 1, 0),$$
$$x^{512} \equiv (0, 0, 1, 1, 0, 0, 1),$$
$$x^{1024} \equiv (0, 1, 0, 0, 0, 0, 0).$$

Таким образом, $N = 10$ и многочлен T имеет вид

$$T(x) = T_1(x) = \sum_{j=0}^{9} x^{2^j} \equiv (1, 1, 1, 0, 0, 0, 1) \pmod{f_0(x)}.$$

Поскольку многочлен $T_1(x)$ не сравним с константой по модулю $f_0(x)$, то он является f_0-разлагающим многочленом. Находим НОД $(f_0(x), T_1(x) - c)$ для значений $c = 0$ и $c = 1$:

$$\text{НОД}(f_0(x), T_1(x)) = \text{НОД}((1, 1, 0, 0, 1, 1, 0, 1), (1, 1, 1, 0, 0, 0, 1)) = x^5 + x^4 + x^3 + x^2 + 1,$$

$$\text{НОД}(f_0(x), T_1(x) - 1) = \text{НОД}((1, 1, 0, 0, 1, 1, 0, 1), (0, 1, 1, 0, 0, 0, 1)) = x^2 + x + 1,$$

и по формуле (4.2) получаем

$$f_0(x) = (x^5 + x^4 + x^3 + x^2 + 1)(x^2 + x + 1).$$

Второй сомножитель, очевидно, неприводим в $\mathbb{F}_2[x]$. Поскольку число $N = 10$ является наименьшим общим кратным степеней

неприводимых делителей многочлена $f_0(x)$, а любое нетривиальное разложение первого сомножителя привело бы к значению N, отличному от 10, то первый сомножитель тоже неприводим в $\mathbb{F}_2(x)$.

Теперь остается разложить многочлен НОД $(f(x), f'(x)) = x^{10} + x^8 + 1$. Нетрудно заметить, что $x^{10} + x^8 + 1 = (x^5 + x^4 + 1)^2$, причем многочлен $x^5 + x^4 + 1$ делится на неприводимый делитель x^2+x+1 многочлена $f_0(x)$, так что $x^5 + x^4 + 1 = (x^3 + x + 1)(x^2 + x + 1)$, где многочлен $x^3 + x + 1$ тоже неприводим над $\mathbb{F}_2[x]$. Окончательно получим такое каноническое разложение многочлена $f(x)$ в $\mathbb{F}_2[x]$:

$$f(x) = (x^5 + x^4 + x^3 + x^2 + 1)(x^3 + x + 1)^2 (x^2 + x + 1)^3. \square$$

Следует, однако, заметить, что, вообще говоря, f-разлагающие многочлены вида T_i могут не привести к полному разложению многочлена f, поскольку они неспособны отделить те неприводимые делители f_j многочлена f, для которых число N/n_j делится на характеристику поля $\mathbb{F}_q$. В таком случае обычно сначала с помощью f-разлагающего многочлена T_i находят частичное нетривиальное разложение многочлена f, а потом ищут новые T_i для каждого из полученных сомножителей. Так в конечном счете получают полное разложение многочлена f.

Но существует модификация изложенного метода, когда вместо многочленов T_i строятся связанные с ними многочлены R_i, которые способны отделить все неприводимые сомножители многочлена f сразу. Предположим (без ограничения общности), что $f(0) \neq 0$. Пусть $\operatorname{ord}(f(x)) = e$, так что $f(x)$ делит двучлен $x^e - 1$. Поскольку многочлен $f(x)$ не имеет кратных сомножителей, то на основании следствия 3.4 и теоремы 3.9 числа e и q взаимно просты. Пусть i — целое неотрицательное число; обозначим через m_i наименьшее натуральное число, удовлетворяющее сравнению

$$x^{iq^{m_i}} \equiv x^i \pmod{f(x)}. \tag{4.10}$$

Пусть теперь

$$R_i(x) = x^i + x^{iq} + x^{iq^2} + \cdots + x^{iq^{m_i-1}}$$

— многочлен над $\mathbb{F}_q$. Поскольку сравнение (4.10) эквивалентно сравнению

$$iq^{m_i} \equiv i \pmod{e}, \tag{4.11}$$

которое в свою очередь эквивалентно сравнению $q^{m_i} \equiv 1 \pmod{(e/\text{НОД}(e, i))}$, то отсюда следует, что число m_i является показателем, которому принадлежит число q по модулю $e/\text{НОД}(e,$

i). Сравнивая определения многочленов T_i и R_i, легко устанавливаем [1]), что

$$T_i(x) \equiv \frac{N}{m_i} R_i(x) \pmod{f(x)}.$$

Ясно, что для всех i справедливо сравнение $R_i^q \equiv R_i \pmod f$, так что многочлены R_i можно использовать вместо h в формуле (4.2). Покажем теперь, что многочлены R_i обладают указанным выше свойством.

4.5. Теорема. *Пусть приводимый над полем $\mathbb{F}_q$ нормированный многочлен f не имеет кратных сомножителей, и пусть $f(0) \neq 0$ и $\operatorname{ord}(f) = e$. Тогда, используя вместо $h(x)$ в формуле* (4.2) *многочлены* $R_i(x) = x^i + x^{iq} + x^{iq^2} + \ldots + x^{iq^{m_i-1}}$, $1 \leqslant i \leqslant e-1$, *где числа m_i определяются условием* (4.10), *можно отделить все неприводимые сомножители многочлена f.*

Доказательство. Пусть $h(x) = \sum_{i=0}^{e-1} a_i x^i \in \mathbb{F}_q[x]$ — решение сравнения $h(x)^q \equiv h(x) \pmod{(x^e - 1)}$. Если рассматривать индексы коэффициентов a_i как вычеты по $\bmod e$, то ввиду взаимной простоты чисел q и e получаем сравнение $h(x) \equiv \sum_{i=0}^{e-1} a_{iq} x^{iq} \pmod{(x^e - 1)}$, так как при $i = 0, 1, \ldots, e-1$ числа iq пробегают полную систему вычетов по $\bmod e$. А поскольку $h(x)^q = \sum_{i=0}^{e-1} a_i x^{iq}$, то

$$\sum_{i=0}^{e-1} a_i x^{iq} \equiv \sum_{i=0}^{e-1} a_{iq} x^{iq} \pmod{(x^e - 1)}.$$

Рассматривая здесь показатели как вычеты по модулю e, мы видим, что соответствующие коэффициенты равны. Значит, $a_i = a_{iq}$ для всех i, так что для всех i выполняются равенства $a_i = a_{iq} = a_{iq^2} = \ldots$. Поскольку m_i — наименьшее натуральное число, для которого имеет место сравнение (4.11), то

$$h(x) \equiv \sum_{i \in J} a_i R_i(x) \pmod{(x^e - 1)},$$

где множество J содержит по одному представителю от каждого класса эквивалентности при следующем определении отношения эквивалентности $\sim$: для $i_1, i_2 \in \mathbb{Z}$ считаем, что $i_1 \sim i_2$ тогда и

---

[1]) Так как $R_i(x)^{q^{m_i}} = \sum_{j=0}^{m_i-1} x^{iq^j + m_i} = \sum_{j=0}^{m_i-1} \left(x^{iq^{m_i}}\right)^{q^j} \equiv \sum_{j=1}^{m_i-1} x^{iq^j} \equiv R_i(x) \pmod{f(x)}$. — *Прим. перев.*

только тогда, когда имеет место сравнение $i_1 \equiv i_2 q^t \pmod{e}$ для некоторого $t \geqslant 0$. Таким образом, для подходящих элементов [1]) $b_i \in \mathbb{F}_q$

$$h(x) \equiv \sum_{i=0}^{e-1} b_i R_i(x) \pmod{(x^e - 1)}. \tag{4.12}$$

Пусть теперь $f_1(x)$ и $f_2(x)$ — два различных нормированных неприводимых делителя многочлена $f(x)$ (а следовательно, и двучлена $x^e - 1$). Согласно рассуждению, которое привело к сравнению (4.3), существует такое решение $h(x) \in \mathbb{F}_q[x]$ сравнения $h(x)^q \equiv h(x) \pmod{(x^e - 1)}$, что $\deg(h(x)) < e$ и при этом

$$h(x) \equiv 0 \pmod{f_1(x)}, \quad h(x) \equiv 1 \pmod{f_2(x)}. \tag{4.13}$$

Поскольку $R_i^q \equiv R_i \pmod{f}$, то из рассуждения, следующего за сравнением (4.3), вытекает существование таких элементов c_{i1}, $c_{i2} \in \mathbb{F}_q$, что $R_i(x) \equiv c_{i1} \pmod{f_1(x)}$ и $R_i(x) \equiv c_{i2} \pmod{f_2(x)}$ для всех i, $0 \leqslant i \leqslant e-1$. Если для всех этих i имеет место равенство $c_{i1} = c_{i2}$, то из (4.12) следует, что для некоторого $c \in \mathbb{F}_q$ имеют место сравнения $h(x) \equiv c \pmod{f_1(x)}$, $h(x) \equiv c \pmod{f_2(x)}$, но это противоречит сравнениям (4.13). Поэтому должно быть $c_{i1} \neq c_{i2}$ для некоторого i, $0 \leqslant i \leqslant e-1$ (точнее, для некоторого i, $1 \leqslant i \leqslant e-1$, так как $R_0(x) = 1$). В таком случае многочлен $R_i(x) - c_{i1}$ будет делиться на $f_1(x)$, но не на $f_2(x)$. Следовательно, используя этот многочлен $R_i(x)$ вместо $h(x)$ в формуле (4.2), мы отделим $f_1(x)$ от $f_2(x)$. □

Из доказательства теоремы 4.5 видно, что все неприводимые делители многочлена f могут быть отделены многочленами R_i, где i пробегает ненулевые элементы множества J. Однако для нахождения множества J требуется знать порядок e многочлена f; прямой же подсчет числа e (т. е. без использования канонического разложения многочлена f), как правило, чересчур громоздок.

Такая проблема не возникает в следующих двух частных случаях — двучлена $f(x) = x^e - 1$ и e-кругового многочлена $f(x) = Q_e(x)$, поскольку в обоих этих случаях, очевидно, $\operatorname{ord}(x^e - 1) = \operatorname{ord}(Q_e(x)) = e$. Оказывается, что многочлены R_i очень удобны для разложения таких двучленов и круговых многочленов.

4.6. **Пример.** Найдем каноническое разложение кругового многочлена $Q_{52}(x)$ в кольце $\mathbb{F}_3[x]$. Согласно теореме 3.27,

$$Q_{52}(x) = \frac{(x^{52}-1)(x^2-1)}{(x^{26}-1)(x^4-1)} =$$
$$= x^{24} - x^{22} + x^{20} - x^{18} + x^{16} - x^{14} + x^{12} -$$
$$- x^{10} + x^8 - x^6 + x^4 - x^2 + 1.$$

[1]) Здесь $b_i = a_i$, если $i \in J$, и $b_i = 0$, если $i \notin J$. — *Прим. перев.*

Рассмотрим теперь многочлен $R_1(x) = x + x^3 + x^9 + x^{27} + x^{81} + x^{243}$. Ввиду того [1]), что $x^{26} \equiv -1 \pmod{Q_{52}(x)}$, получаем, что $R_1(x) \equiv 0 \pmod{Q_{52}(x)}$, так что R_1 не является Q_{52}-разлагающим многочленом. Переходим к следующему многочлену $R_2(x) = x^2 + x^6 + x^{18}$. Для него получаем

$$\begin{aligned}
\text{НОД}\,(Q_{52}(x),\ R_2(x)) &= x^6 - x^2 + 1,\\
\text{НОД}\,(Q_{52}(x),\ R_2(x) + 1) &= x^6 + x^4 - x^2 + 1,\\
\text{НОД}\,(Q_{52}(x),\ R_2(x) - 1) &= x^{12} + x^{10} - x^8 + x^6 + x^4 + x^2 + 1 = \\
&= g(x),
\end{aligned}$$

так что из формулы (4.2) следует равенство

$$Q_{52}(x) = (x^6 - x^2 + 1)(x^6 + x^4 - x^2 + 1)\, g(x).$$

Согласно теореме 2.47 (ii), круговой многочлен $Q_{52}(x)$ в кольце $\mathbb{F}_3[x]$ разлагается в произведение четырех неприводимых сомножителей степени 6. Так что остается только разложить многочлен $g(x)$. Поскольку $R_3(x) = x^3 + x^9 + x^{27} + x^{81} + x^{243} + x^{729} \equiv 0 \pmod{Q_{52}(x)}$, переходим к следующему многочлену $R_4(x) = x^4 + x^{12} + x^{36}$. Заметив, что $x^{12} \equiv -x^{10} + x^8 - x^8 - x^4 - x^2 - 1 \pmod{g(x)}$ и $x^{36} \equiv -x^{10} \pmod{g(x)}$, получим, что

$$R_4(x) \equiv x^{10} + x^8 - x^6 - x^2 - 1 \pmod{g(x)}.$$

Поэтому

$$\begin{aligned}
\text{НОД}\,(g(x),\ R_4(x)) &= \text{НОД}\,(g(x),\ x^{10} + x^8 - x^6 - x^2 - 1) = 1,\\
\text{НОД}\,(g(x),\ R_4(x) + 1) &= \text{НОД}\,(g(x),\ x^{10} + x^8 - x^6 - x^2) = \\
&= x^6 - x^4 + x^2 + 1,\\
\text{НОД}\,(g(x),\ R_4(x) - 1) &= \text{НОД}\,(g(x),\ x^{10} + x^8 - x^6 - x^2 + 1) = \\
&= x^6 - x^4 + 1.
\end{aligned}$$

Таким образом, искомое каноническое разложение многочлена $Q_{52}(x)$ имеет вид

$$Q_{52}(x) = $$
$$= (x^6 - x^2 + 1)(x^6 + x^4 - x^2 + 1)(x^6 - x^4 + x^2 + 1)(x^6 - x^4 + 1).$$

□

§ 2. Разложение многочленов над большими конечными полями

Если $\mathbb{F}_q$ — большое конечное поле, т. е. число q велико, то практическое применение методов предыдущего параграфа становится затруднительным. Хоть мы и можем, затратив определен-

[1]) Так как $x^{26} + 1 = (x^{52} - 1)/(x^{26} - 1)$ содержит все первообразные корни 52-й степени из 1. — *Прим. перев.*

ные усилия, найти f-разлагающий многочлен, однако прямое использование основной формулы (4.2) становится уже нереальным, так как оно требует подсчета q наибольших общих делителей. Поэтому для того, чтобы сделать возможным использование f-разлагающих многочленов и для больших конечных полей, необходимо изыскать пути сокращения числа элементов $c \in \mathbb{F}_q$, для которых в формуле (4.2) нужно подсчитывать наибольшие общие делители. Заметим, что в контексте, связанном с разложением многочленов, мы будем считать порядок q конечного поля $\mathbb{F}_q$ «большим», если он существенно больше степени разлагаемого многочлена.

Пусть снова f — произвольный нормированный многочлен степени n из кольца $\mathbb{F}_q[x]$, разлагающийся в произведение k различных нормированных неприводимых сомножителей над полем $\mathbb{F}_q$. Допустим, что многочлен $h \in \mathbb{F}_q[x]$ удовлетворяет условиям $h^q \equiv h \pmod f$ и $0 < \deg(h) < n$, так что он является f-разлагающим многочленом. Поскольку различные наибольшие общие делители из правой части формулы (4.2) взаимно просты, то ясно, что не более k из них могут быть отличны от 1. Задача состоит в том, как a priori охарактеризовать те элементы $c \in \mathbb{F}_q$, для которых НОД $(f(x), h(x) - c) \neq 1$.

Одну из таких характеризаций можно получить, применяя теорию результантов (см. определение 1.93 и последующие замечания). Пусть $R(f(x), h(x) - c)$ — результант многочленов $f(x)$ и $h(x) - c$, где в качестве формальных степеней берутся степени этих многочленов. Тогда НОД $(f(x), h(x) - c) \neq 1$ в том и только том случае, если $R(f(x), h(x) - c) = 0$. Так мы приходим к рассмотрению функции

$$F(y) = R(f(x), h(x) - y),$$

которая, очевидно, является многочленом степени, не большей n, относительно переменной y (учитывая представление результанта в виде определителя). Ясно, что НОД $(f(x), h(x) - c) \neq 1$ в том и только том случае, если элемент c является корнем многочлена $F(y)$ из поля $\mathbb{F}_q$.

Многочлен $F(y)$ можно найти непосредственно из его определения; для этого потребуется вычислить определитель порядка не более чем $2n - 1$, элементами которого являются либо элементы из поля $\mathbb{F}_q$, либо линейные многочлены от y с коэффициентами из $\mathbb{F}_q$. Однако во многих случаях предпочтительнее другой способ, состоящий в следующем. Выберем $n + 1$ различных элементов $c_0, c_1, \ldots, c_n$ из $\mathbb{F}_q$ и подсчитаем результанты $r_i = R(f(x), h(x) - c_i)$, $i = 0, 1, \ldots, n$. Тогда тот единственный многочлен $F(y)$ степени не превосходящей n, для которого $F(c_i) = r_i$, $i = 0, 1, \ldots, n$, можно получить с помощью интерполяционной формулы

Лагранжа (см. теорему 1.71). Этот метод имеет еще то преимущество, что если какие-либо элементы r_i равны нулю, то мы автоматически получаем корни многочлена $F(y)$ из поля $\mathbb{F}_q$. Во всяком случае вопрос о выделении тех элементов $c \in \mathbb{F}_q$, для которых НОД $(f(x), h(x) - c) \neq 1$, теперь сводится к вопросу нахождения корней некоторого многочлена в поле $\mathbb{F}_q$. Вычислительный аппарат для решения этой проблемы будет развит в следующем параграфе.

4.7. Пример. Разложим многочлен $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7$ над полем $\mathbb{F}_{23}$. Так как НОД $(f(x), f'(x)) = 1$, то многочлен $f(x)$ не имеет кратных сомножителей. Применяя алгоритм Берлекэмпа, найдем степени x^{23i} по модулю $f(x)$ для $i = 0, 1, \ldots, 5$. Это приводит к 6×6-матрице

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & -1 & 8 & -3 & -10 \\ -10 & 10 & 10 & 0 & 1 & -9 \\ 0 & 7 & 9 & -8 & 10 & -11 \\ 11 & 0 & -4 & 7 & 7 & 2 \\ -3 & 0 & -10 & 9 & 2 & -9 \end{pmatrix},$$

так что матрица $B - I$ имеет вид

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & -1 & -1 & 8 & -3 & -10 \\ -10 & 10 & 9 & 0 & 1 & -9 \\ 0 & 7 & 9 & -9 & 10 & -11 \\ 11 & 0 & -4 & 7 & 6 & 2 \\ -3 & 0 & -10 & 9 & 2 & -10 \end{pmatrix}.$$

Приведение этой матрицы элементарными преобразованиями столбцов к ступенчатому виду показывает, что ранг r матрицы $B - I$ равен 3, так что многочлен f имеет $k = 6 - r = 3$ различных нормированных неприводимых сомножителей над полем $\mathbb{F}_{23}$. Базис пространства решений однородной системы (4.6), соответствующий матрице $B - I$, задается векторами $h_1 = (1, 0, 0, 0, 0, 0)$, $h_2 = (0, 4, 2, 1, 0, 0)$ и $h_3 = (0, -2, 9, 0, 1, 1)$, которые соответствуют многочленам $h_1(x) = 1$, $h_2(x) = x^3 + 2x^2 + 4x$ и $h_3(x) = x^5 +$

$+ x^4 + 9x^2 - 2x$. Возьмем теперь f-разлагающий многочлен $h_2(x)$ и рассмотрим многочлен от y

$$F(y) = R(f(x), h_2(x) - y) =$$

$$= \begin{vmatrix} 1 & -3 & 5 & -9 & -5 & 6 & 7 & 0 & 0 \\ 0 & 1 & -3 & 5 & -9 & -5 & 6 & 7 & 0 \\ 0 & 0 & 1 & -3 & 5 & -9 & -5 & 6 & 7 \\ 1 & 2 & 4 & -y & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 4 & -y & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 4 & -y & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 & -y & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 4 & -y & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & -y \end{vmatrix}.$$

Этот определитель можно вычислить непосредственно, и мы получим $F(y) = y^6 + 4y^5 + 3y^4 - 7y^3 + 10y^2 + 11y + 7$. Поскольку многочлен f имеет три различных нормированных неприводимых сомножителя в кольце $\mathbb{F}_{23}[x]$, то, как отмечалось выше, многочлен $F(y)$ может иметь не более трех корней в поле $\mathbb{F}_{23}$. Применяя либо один из методов, рассматриваемых в следующем параграфе, либо метод проб и ошибок, находим эти корни, равные соответственно 2, -3 и 6. Далее,

$$\text{НОД}(f(x), h_2(x) - 2) = x^2 - x + 7,$$
$$\text{НОД}(f(x), h_2(x) + 3) = x - 4,$$
$$\text{НОД}(f(x), h_2(x) - 6) = x^3 + 2x^2 + 4x - 6,$$

так что каноническим разложением многочлена $f(x)$ в кольце $\mathbb{F}_{23}[x]$ является

$$f(x) = (x - 4)(x^2 - x + 7)(x^3 + 2x^2 + 4x - 6). \qquad \square$$

Другой метод характеризации тех элементов c поля $\mathbb{F}_q$, для которых нужно подсчитывать НОД $(f(x), h(x) - c)$ в формуле (4.2), основан на следующих соображениях. Пусть сохранены те же обозначения, что и выше, и пусть C обозначает множество всех тех $c \in \mathbb{F}_q$, для которых НОД $(f(x), h(x) - c) \neq 1$. Тогда из (4.2) следует, что

$$f(x) = \prod_{c \in C} \text{НОД}(f(x), h(x) - c), \tag{4.14}$$

так что многочлен $f(x)$ делит произведение $\prod_{c \in C} (h(x) - c)$. Введем в рассмотрение многочлен

$$G(y) = \prod_{c \in C} (y - c).$$

Тогда многочлен $f(x)$ делит $G(h(x))$, и многочлен $G(y)$ можно охарактеризовать следующим образом.

4.8. Теорема. *Среди всех многочленов $g \in \mathbb{F}_q[y]$, таких, что $f(x)$ делит $g(h(x))$, многочлен $G(y)$ однозначно определяется тем, что это нормированный многочлен наименьшей степени.*

Доказательство. Мы уже показали, что нормированный многочлен $G(y)$ обладает тем свойством, что $f(x)$ делит $G(h(x))$. Легко видеть, что многочлены $g \in \mathbb{F}_q[y]$, такие, что $f(x)$ делит $g(h(x))$, образуют ненулевой идеал кольца $\mathbb{F}_q[y]$. По теореме 1.54 этот идеал является главным идеалом, порожденным некоторым однозначно определенным нормированным многочленом $G_0 \in \mathbb{F}_q[y]$. Это значит, что многочлен $G_0(y)$ делит $G(y)$, так что

$$G_0(y) = \prod_{c \in C_1} (y - c)$$

для некоторого подмножества C_1 множества C. Следовательно, $f(x)$ делит $G_0(h(x)) = \prod_{c \in C_1} (h(x) - c)$, и, значит,

$$f(x) = \prod_{c \in C_1} \text{НОД}(f(x),\ h(x) - c).$$

Сравнение с (4.14) показывает, что $C_1 = C$. Поэтому $G_0(y) = G(y)$, и теорема доказана. □

Этот результат можно использовать следующим образом. Пусть m — число элементов множества C. Тогда запишем

$$G(y) = \prod_{c \in C} (y - c) = \sum_{j=0}^{m} b_j y^j$$

с коэффициентами $b_j \in \mathbb{F}_q$. Поскольку $f(x)$ делит $G(h(x))$, то мы получаем

$$\sum_{j=0}^{m} b_j h(x)^j \equiv 0 \pmod{f(x)}.$$

Так как $b_m = 1$, то это сравнение можно рассматривать как нетривиальное соотношение линейной зависимости над полем $\mathbb{F}_q$, связывающее вычеты по модулю $f(x)$ многочленов 1, $h(x)$, $h(x)^2$, ..., $h(x)^m$. Согласно теореме 4.8, если произвести нормирование так, чтобы $b_m = 1$, то такое соотношение линейной зависимости определяется однозначно; поэтому вычеты по модулю $f(x)$ многочленов 1, $h(x)$, $h(x)^2$, ..., $h(x)^{m-1}$ линейно независимы над $\mathbb{F}_q$. Ограничение $m \leqslant k$ (где k определено в начале параграфа) вытекает из (4.14).

Поэтому многочлен G можно найти, если приводить по модулю $f(x)$ степени многочлена $h(x)$: 1, $h(x)$, $h(x)^2$, ..., пока не найдем

ту наименьшую степень $h(x)^m$ этого многочлена, которая линейно зависит (над полем $\mathbb{F}_q$) от предыдущих степеней. Коэффициенты этого первого соотношения линейной зависимости в нормированной форме (т. е. с коэффициентом 1 при $h(x)^m$) и являются коэффициентами многочлена G. При этом мы знаем, что для нахождения этого соотношения линейной зависимости требуется рассмотреть лишь степени многочлена $h(x)$ не выше k-й, где число k можно получить из алгоритма Берлекэмпа. Элементами множества C являются корни многочлена G, лежащие в поле $\mathbb{F}_q$, и только они. Этот метод, сводящий проблему нахождения элементов множества C к задаче отыскания корней некоторого многочлена в поле $\mathbb{F}_q$, носит название *алгоритма Цассенхауза.*

4.9. Пример. Рассмотрим снова тот же многочлен $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7 \in \mathbb{F}_{23}[x]$, что и в примере 4.7. С помощью алгоритма Берлекэмпа мы уже нашли число его неприводимых сомножителей k, равное 3, и f-разлагающий многочлен $h(x) = x^3 + 2x^2 + 4x \in \mathbb{F}_{23}[x]$. Применим теперь алгоритм Цассенхауза для нахождения множества C тех элементов $c \in \mathbb{F}_{23}$, для которых НОД $(f(x), h(x) - c) \neq 1$. Мы имеем

$$h(x) \equiv x^3 + 2x^2 + 4x \pmod{f(x)},$$
$$h(x)^2 \equiv 7x^5 + 7x^4 + 2x^3 - 2x^2 - 6x - 7 \pmod{f(x)},$$

так что ясно, что $h(x)^2$ не зависит линейно от 1 и $h(x)$. Поскольку число m элементов множества C не превосходит $k = 3$, то степень $h(x)^3$ должна быть наименьшей степенью многочлена $h(x)$, которая линейно зависит от предыдущих степеней. Имеем

$$h(x)^3 \equiv -11x^5 - 11x^4 - x^3 - 9x^2 - 5x - 2 \pmod{f(x)},$$

и искомая линейная зависимость такова:

$$h(x)^3 - 5h(x)^2 + 11h(x) - 10 \equiv 0 \pmod{f(x)},$$

следовательно, $G(y) = y^3 - 5y^2 + 11y - 10$. Теперь, применяя либо методы следующего параграфа, либо метод проб и ошибок, находим, что корнями многочлена G в поле $\mathbb{F}_{23}$ являются элементы 2, -3 и 6. Каноническое разложение многочлена f в $\mathbb{F}_{23}[x]$ находится так же, как в последней части примера 4.7. □

Приведем еще один метод, который основан на применении матриц из многочленов. Хоть его схема более сложна, но зато он представляет больший теоретический интерес. Под *матрицей из многочленов* мы будем понимать матрицу, элементами которой являются многочлены из кольца $\mathbb{F}_q[x]$.

4.10. Определение. Квадратную матрицу из многочленов будем называть *невырожденной*, если ее определителем является ненулевой многочлен, и *унимодулярной*, если ее определителем является ненулевой элемент поля $\mathbb{F}_q$.

4.11. Определение. Квадратные матрицы из многочленов P и Q будем называть *эквивалентными*, если существуют такие унимодулярная матрица из многочленов U и невырожденная матрица E с элементами из поля $\mathbb{F}_q$, что $P = UQE$.

Легко проверить, что введенное нами понятие эквивалентности матриц из многочленов действительно является отношением эквивалентности в том смысле, что оно рефлексивно, симметрично и транзитивно.

Мы видели в § 1, что существуют многочлены $h_2, \ldots, h_k \in \mathbb{F}_q[x]$, $0 < \deg(h_i) < \deg(f)$, $i = 2, \ldots, k$, которые вместе с $h_1(x) = 1$ являются линейно независимыми над полем $\mathbb{F}_q$ решениями сравнения $h^q \equiv h \pmod f$. Ясно, что многочлены h_i можно выбрать нормированными. Следующая теорема является основополагающей.

4.12. Теорема. *Пусть $f = f_1 \ldots f_k$, где $f_1, \ldots, f_k$ — различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$, и пусть $h_2, \ldots, h_k \in \mathbb{F}_q[x]$ — нормированные многочлены степени $<\deg(f)$, которые вместе с $h_1 = 1$ являются линейно независимыми над полем $\mathbb{F}_q$ решениями сравнения $h^q \equiv h \pmod f$. Тогда диагональная матрица из многочленов*

$$D = \begin{pmatrix} f_1 & 0 & \ldots & 0 \\ 0 & f_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & f_k \end{pmatrix}$$

эквивалентна матрице из многочленов

$$A = \begin{pmatrix} f & 0 & 0 & \ldots & 0 \\ h_2 & -1 & 0 & \ldots & 0 \\ h_3 & 0 & -1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ h_k & 0 & 0 & \ldots & -1 \end{pmatrix}.$$

Доказательство. Из рассуждения, следующего из (4.3), вытекает, что существуют элементы $e_{ij} \in \mathbb{F}_q$, такие, что $h_i(x) \equiv e_{ij} \pmod{f_j(x)}$, $1 \leqslant i, j \leqslant k$. Обозначим $k \times k$-матрицу (e_{ij}) через E. Покажем, что матрица E невырожденна. Если бы это было не так, то существовали бы такие элементы $d_1, \ldots, d_k \in \mathbb{F}_q$, не все равные нулю, что

$$\sum_{i=1}^{k} d_i e_{ij} = 0, \quad j = 1, \ldots, k.$$

Это означало бы, что

$$\sum_{i=1}^{k} d_i h_i \equiv 0 \pmod{f_j}, \quad j = 1, \ldots, k,$$

откуда следовало бы, что $\sum_{i=1}^{k} d_i h_i \equiv 0 \pmod{f}$. Но так как $\deg(h_i) < \deg(f)$ для всех i, $1 \leqslant i \leqslant k$, то на самом деле мы получили бы равенство $\sum_{i=1}^{k} d_i h_i = 0$, которое противоречит линейной независимости многочленов $h_1, \ldots, h_k$.

Теперь заметим, что AE является невырожденной матрицей из многочленов, так как $\det(AE) = (-1)^{k-1} f \det(E)$. Поэтому мы можем написать $D = (D(AE)^{-1})AE$, и теорема будет доказана, как только мы покажем, что $U = D(AE)^{-1}$ является унимодулярной матрицей из многочленов.

Пусть $AE = (b_{ij})$, где $b_{ij} \in \mathbb{F}_q[x]$. Тогда, так как $h_1 = 1$, то $b_{1j} = fe_{1j} = f \equiv 0 \pmod{f_j}$ для $1 \leqslant j \leqslant k$, а для $2 \leqslant i \leqslant k$ имеем $b_{ij} = h_i e_{1j} - e_{ij} = h_j - e_{ij} \equiv 0 \pmod{f_j}$ при $1 \leqslant j \leqslant k$, так что

$$b_{ij} \equiv 0 \pmod{f_j} \quad \text{для всех} \quad 1 \leqslant i, j \leqslant k. \tag{4.15}$$

Далее,

$$(AE)^{-1} = \frac{1}{\det(AE)}(B_{ij})_{1 \leqslant i, j \leqslant k} = \frac{(-1)^{k-1}}{\det(E) f}(B_{ij})_{1 \leqslant i, j \leqslant k},$$

где B_{ji} — алгебраическое дополнение элемента b_{ij} матрицы AE, так что

$$U = D(AE)^{-1} = \frac{(-1)^{k-1}}{\det(E) f}(f_i B_{ij})_{1 \leqslant i, j \leqslant k}.$$

Из (4.15) следует, что $B_{ij} \equiv 0 \pmod{f/f_i}$, поэтому $f_i B_{ij}$ делится на f, и каждый элемент матрицы U является многочленом над полем $\mathbb{F}_q$. Кроме того,

$$\det(U) = \frac{\det(D)}{\det(AE)} = \frac{(-1)^{k-1}}{\det(E)},$$

т. е. $\det(U)$ — ненулевой элемент поля $\mathbb{F}_q$. Значит, U — унимодулярная матрица из многочленов. □

Теорема 4.12 обеспечивает теоретическую возможность нахождения неприводимых делителей многочлена f путем приведения матрицы A к диагональному виду. Сама же матрица A (число k и многочлены $h_2, \ldots, h_k$ из ее первого столбца) относительно легко строится с помощью алгоритма Берлекэмпа. Однако алгоритм, с помощью которого производится диагонализация матрицы A, довольно сложен.

Алгоритм диагонализации основан на применении следующих *элементарных преобразований*: (i) перестановки любой пары строк (столбцов) матрицы; (ii) умножения любой строки (столбца) на любой элемент группы $\mathbb{F}_q^*$; (iii) умножения любой строки (столбца) на произвольный элемент поля $\mathbb{F}_q$ и прибавления результата к любой другой строке (столбцу).

Элементарные преобразования для строк можно осуществить умножением исходной матрицы слева на подходящим образом выбранную унимодулярную матрицу из многочленов, тогда как элементарные преобразования для столбцов можно осуществить умножением исходной матрицы справа на подходящим образом выбранную невырожденную матрицу с элементами из $\mathbb{F}_q$. Поэтому новая матрица, получаемая применением любого элементарного преобразования, всегда эквивалентна исходной матрице.

Можно показать, что матрица A эквивалентна такой матрице R из многочленов, что для каждой ее строки степень диагонального элемента больше степеней остальных элементов строки. Такую матрицу R можно получить из A, произведя не более $(2\Delta + k - 1) \cdot (k - 1)$ элементарных преобразований, где $\Delta = \deg(h_2) + \ldots + \deg(h_k)$.

Заметим, что диагональные элементы матрицы R можно переставлять, производя соответствующую перестановку строк и столбцов. Таким образом мы можем получить матрицу S, которая, обладая всеми свойствами матрицы R, обладает следующим дополнительным свойством: $\deg(s_{ii}) \geqslant \deg(s_{jj})$ для $1 \leqslant i < j \leqslant k$, где s_{ii} — диагональные элементы матрицы S. Кроме того, умножением строк матрицы S на подходящие элементы из $\mathbb{F}_q^*$ можно добиться, чтобы многочлены s_{ii} были нормированными. Матрицу S из многочленов, обладающую всеми этими свойствами, будем называть *нормализованной матрицей*.

Диагональные элементы матрицы D из теоремы 4.12 тоже можно переставить так, чтобы выполнялись неравенства $\deg(f_i) \geqslant \deg(f_j)$ для $1 \leqslant i < j \leqslant k$. В результате мы получим эквивалентную матрицу, которую тоже обозначим D и которая будет диагональной и нормализованной. Можно показать, что из эквивалентности нормализованных матриц S и D вытекает, что $\deg(s_{ii}) = \deg(f_i)$ для всех i, $1 \leqslant i \leqslant k$. Отсюда следует, что степени различных неприводимых делителей многочлена f совпадают со степенями диагональных элементов матрицы S. Более того, если натуральное число d является степенью некоторого диагонального элемента (многочлена) s_{ii} матрицы S и если $S^{(d)}$ — квадратная подматрица матрицы S, главная диагональ которой состоит как раз из всех тех многочленов s_{ii}, степени которых равны d, то можно показать, что определитель матрицы $S^{(d)}$ равен определителю соответствующей подматрицы $D^{(d)}$ матрицы D. Поэтому $\det(S^{(d)}) = g_d$, где g_d

есть произведение всех многочленов f_i степени d. Таким образом мы приходим к частичному разложению многочлена f:

$$f = \prod_d g_d, \tag{4.16}$$

где произведение берется по всем натуральным числам d, являющимся степенями неприводимых делителей f_i многочлена f.

В итоге матрица S позволяет получить следующие сведения о нормированных неприводимых сомножителях f_i многочлена f: узнать степени этих сомножителей, число всех сомножителей данной степени и произведение всех сомножителей данной степени. Поэтому если степени всех сомножителей f_i различны, а это значит, что различны степени всех диагональных элементов (многочленов) s_{ii} матрицы S, то разложение (4.16) уже является каноническим разложением f в $\mathbb{F}_q[x]$.

Но если разложение (4.16) еще не является каноническим разложением многочлена f, то мы можем продолжить его несколькими путями. Например, можно применить один из рассмотренных ранее методов для разложения многочленов g_d. А можно продолжать алгоритм диагонализации с тем, чтобы в итоге получить диагональную матрицу D, эквивалентную нормализованной матрице S.

Выберем второй путь и будем считать, что матрица D имеет нормализованный вид. К упомянутым выше свойствам матрицы S можно добавить еще одно, а именно что каждая ее подматрица $S^{(d)}$ эквивалентна соответствующей подматрице $D^{(d)}$ матрицы D. Поэтому достаточно диагонализировать каждую такую подматрицу $S^{(d)}$ отдельно. В силу эквивалентности матриц $S^{(d)}$ и $D^{(d)}$ найдутся такие унимодулярная матрица из многочленов U и невырожденная матрица E с элементами из поля $\mathbb{F}_q$, что $S^{(d)} = UD^{(d)}E$. Мы можем тогда записать

$$S^{(d)} = S_0^{(d)} + S_1^{(d)}x + \cdots + S_d^{(d)}x^d,$$
$$U = U_0 + U_1x + \cdots + U_mx^m,$$
$$D^{(d)} = D_0^{(d)} + D_1^{(d)}x + \cdots + D_d^{(d)}x^d,$$

где $S_r^{(d)}$, $D_r^{(d)}$ и U_t, $0 \leqslant r \leqslant d$, $0 \leqslant t \leqslant m$, — матрицы с элементами из поля $\mathbb{F}_q$, $U_m \neq 0$ и $S_d^{(d)} = D_d^{(d)} = I$ — единичные матрицы соответствующего порядка. Сравнение матричных коэффициентов при высших степенях переменной x в обеих частях равенства $S^{(d)} = UD^{(d)}E$ дает $I = U_mIE$, так что $m = 0$. Поэтому $U = U_0 = E^{-1}$ и $S^{(d)} = E^{-1}D^{(d)}E$.

Сравнивая матричные коэффициенты при одинаковых степенях переменной x в последнем равенстве, получаем $S_r^{(d)} = E^{-1}D^{(d)}E$ для всех r, $0 \leqslant r \leqslant d$. Следовательно, матрицы $S_r^{(d)}$ и $D_r^{(d)}$ имеют

одинаковые характеристические многочлены, а значит, и одинаковые собственные значения; кроме того, поскольку $D_r^{(d)}$ — диагональная матрица, то ее собственные значения совпадают с ее диагональными элементами. Поэтому эти диагональные элементы можно найти как корни характеристического многочлена матрицы $S_r^{(d)}$, причем все они должны принадлежать полю $\mathbb{F}_q$. Таким образом, мы снова, как и в предыдущих способах, сводим проблему разложения многочлена f к задаче отыскания корней некоторых многочленов в поле $\mathbb{F}_q$.

Частичное разложение (4.16) можно получить также совсем другим способом. Расширим определение многочленов g_d, обозначая через g_i, $i \geqslant 1$, произведение всех нормированных неприводимых многочленов степени i из $\mathbb{F}_q[x]$, которые делят многочлен f. В частности, $g_i(x) = 1$ в том случае, если многочлен f не имеет в кольце $\mathbb{F}_q[x]$ неприводимых делителей степени i. Тогда мы можем написать

$$f = \prod_{i \geqslant 1} g_i.$$

Ясно, что нужно рассматривать лишь те значения i, которые не превосходят $\deg(f)$. Будем теперь, исходя из равенств

$$r_0(x) = x, \quad F_0(x) = f(x),$$

последовательно находить многочлены $r_0(x)$, $r_1(x)$, ..., а также $F_0(x)$, $F_1(x)$, ... и $d_1(x)$, $d_2(x)$, ..., используя для $i \geqslant 1$ следующие рекуррентные соотношения:

$$r_i(x) \equiv r_{i-1}(x)^q \pmod{F_{i-1}(x)}, \quad \deg(r_i) < \deg(F_{i-1}),$$
$$d_i(x) = \text{НОД}(F_{i-1}(x),\ r_i(x) - x),$$
$$F_i(x) = F_{i-1}(x)/d_i(x).$$

Этот процесс заканчивается, когда $d_i(x) = F_{i-1}(x)$.

4.13. Теорема. *В обозначениях, введенных выше, для всех $i \geqslant 1$ имеет место равенство $d_i(x) = g_i(x)$.*

Доказательство. Учитывая делимость многочлена F_{i-1} на F_i, прямой индукцией получаем, что

$$r_i(x) \equiv x^{q^i} \pmod{F_{i-1}(x)} \quad \text{для всех} \quad i \geqslant 1. \tag{4.17}$$

Докажем теперь при помощи индукции, что

$$F_{i-1} = \prod_{j \geqslant i} g_j \quad \text{и} \quad d_i = g_i \quad \text{для всех} \quad i \geqslant 1. \tag{4.18}$$

При $i = 1$ первое равенство выполняется, поскольку $F_0 = f$. Что касается второго равенства, то в силу (4.17)

$$d_1(x) = \text{НОД}(F_0(x),\ r_1(x) - x) = \text{НОД}(f(x),\ x^q - x),$$

и поскольку двучлен $x^q - x$ равен произведению всех нормированных линейных многочленов из кольца $\mathbb{F}_q[x]$, то многочлен d_1 является произведением всех нормированных линейных многочленов из $\mathbb{F}_q[x]$, которые делят f, так что $d_1 = g_1$. Теперь предположим, что равенства (4.18) выполняются для некоторого $i \geqslant 1$. Тогда

$$F_i = F_{i-1}/d_i = F_{i-1}/g_i = \prod_{j \geqslant i+1} g_j, \tag{4.19}$$

так что первое равенство из (4.18) доказано для $i+1$. Кроме того, из (4.17) получаем

$$d_{i+1}(x) = \text{НОД}(F_i(x),\ r_{i+1}(x) - x) = \text{НОД}(F_i(x),\ x^{q^{i+1}} - x).$$

В силу теоремы 3.20 двучлен $x^{q^{i+1}} - x$ является произведением всех нормированных неприводимых многочленов из $\mathbb{F}_q[x]$, степени которых делят число $i+1$. Поэтому многочлен d_{i+1} является произведением всех нормированных неприводимых многочленов из $\mathbb{F}_q[x]$, которые делят F_i и степени которых делят $i+1$. Из (4.19) тогда следует, что $d_{i+1} = g_{i+1}$. □

В изложенном алгоритме самым сложным шагом (с вычислительной точки зрения) является нахождение многочлена r_i путем приведения многочлена r_{i-1}^q по модулю F_{i-1}. Общая техника сокращения вычислительной работы при этом основана на предварительном нахождении вычетов по модулю F_{i-1} многочленов r_{i-1}, r_{i-1}^2, r_{i-1}^4, ..., $r_{i-1}^{2^e}$ (где 2^e — наибольшая степень двойки, не превосходящая q) последовательным возведением в квадрат и приведением по модулю F_{i-1} с последующим перемножением того набора полученных вычетов, который дает нужную нам степень r_{i-1}^q многочлена r_{i-1} по модулю F_{i-1}. Например, чтобы получить вычет степени r_{i-1}^{23} по модулю F_{i-1}, нужно перемножить вычеты степеней r_{i-1}^{16}, r_{i-1}^4, r_{i-1}^2 и r_{i-1} по модулю F_{i-1}.

Однако вместо техники повторных возведений в квадрат мы могли бы для нахождения многочлена $r_i(x)$ по известному $r_{i-1}(x)$ использовать матрицу B из алгоритма Берлекэмпа (см. § 1). Пусть $n = \deg(f)$ и

$$r_{i-1}(x) = \sum_{j=0}^{n-1} r_{i-1}^{(j)} x^j.$$

Определим вектор $(s_i^{(0)}, s_i^{(1)}, \ldots, s_i^{(n-1)}) \in \mathbb{F}_q^n$ матричным равенством

$$(s_i^{(0)}, s_i^{(1)}, \ldots, s_i^{(n-1)}) = (r_{i-1}^{(0)}, r_{i-1}^{(1)}, \ldots, r_{i-1}^{(n-1)})\, B, \tag{4.20}$$

где B — матрица порядка n из (4.5). Если ввести многочлен

$$s_i(x) = \sum_{j=0}^{n-1} s_i^{(j)} x^j, \tag{4.21}$$

то получим, что $r_{i-1}(x)^q \equiv s_i(x) \pmod{f(x)}$, откуда $r_{i-1}(x)^q \equiv s_i(x) \pmod{F_{i-1}(x)}$, так что

$$r_i(x) \equiv s_i(x) \pmod{F_{i-1}(x)}.$$

Поэтому если известна матрица B, то на каждом шаге i мы, зная многочлен $r_{i-1}(x)$, можем найти многочлен $r_i(x)$ приведением по модулю $F_{i-1}(x)$ многочленов $s_i(x)$, получаемых из (4.20) и (4.21).

4.14. Пример. Рассмотрим тот же многочлен $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7 \in \mathbb{F}_{23}[x]$, что и в примере 4.7. Тогда матрица B имеет вид

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & -1 & 8 & -3 & -10 \\ -10 & 10 & 10 & 0 & 1 & -9 \\ 0 & 7 & 9 & -8 & 10 & -11 \\ 11 & 0 & -4 & 7 & 7 & 2 \\ -3 & 0 & -10 & 9 & 2 & -9 \end{pmatrix}.$$

Начнем алгоритм с $r_0(x) = x$ и $F_0(x) = f(x)$. Из (4.20) и (4.21) получаем многочлен $s_1(x) = -10x^5 - 3x^4 + 8x^3 - x^2 + 5$, и, приводя его по модулю $F_0(x)$, находим $r_1(x) = s_1(x)$. Согласно теореме 4.13, имеем $g_1(x) = d_1(x) = \text{НОД}(F_0(x), r_1(x) - x) = x - 4$. Кроме того, $F_1(x) = F_0(x)/d_1(x) = x^5 + x^4 + 9x^3 + 4x^2 + 11x + 4$.

На втором шаге мы вновь применяем (4.20) и (4.21) для нахождения многочлена $s_2(x) = 5x^5 - 8x^4 + 9x^3 - 10x^2 - 11$, и приведением его по модулю $F_1(x)$ получаем $r_2(x) = 10x^4 + 10x^3 - 7x^2 - 9x - 8$. Согласно теореме 4.13, $g_2(x) = d_2(x) = \text{НОД}(F_1(x), r_2(x) - x) = x^2 - x + 7$. Кроме того, $F_2(x) = F_1(x)/d_2(x) = x^3 + 2x^2 + 4x - 6$. Но, согласно первой части (4.18), все неприводимые делители многочлена $F_2(x)$ имеют степени не менее 3, поэтому многочлен $F_2(x)$ сам должен быть неприводимым в кольце $\mathbb{F}_{23}[x]$, так что $g_3(x) = F_2(x)$. Таким образом, мы получаем частичное разложение

$$f(x) = (x - 4)(x^2 - x + 7)(x^3 + 2x^2 + 4x - 6),$$

которое в данном случае уже оказывается каноническим разложением многочлена $f(x)$ в кольце $\mathbb{F}_{23}[x]$. □

§ 3. Вычисление корней многочленов

В предыдущих параграфах мы видели, что проблему канонического разложения некоторого многочлена над конечным полем часто можно свести к задаче нахождения корней в этом поле некоторого вспомогательного многочлена. Но вычисление корней многочлена, безусловно, представляет и самостоятельный интерес.

Вообще говоря, мы ставим следующую задачу. Пусть задан многочлен $f \in \mathbb{F}_r[x]$; требуется найти его корни в некотором расширении $\mathbb{F}_q$ поля $\mathbb{F}_r$. Однако достаточно рассмотреть ситуацию, когда нужно найти корни многочлена $f \in \mathbb{F}_q[x]$ положительной степени, лежащие в самом $\mathbb{F}_q$, так как многочлен над подполем всегда можно рассматривать как многочлен над всем полем.

Ясно, что каждый алгоритм разложения многочлена f в кольце $\mathbb{F}_q[x]$, в частности, является и алгоритмом нахождения его корней в поле $\mathbb{F}_q$, так как эти корни определяются линейными сомножителями канонического разложения f в кольце $\mathbb{F}_q[x]$. Поэтому алгоритмы, рассмотренные в предыдущих параграфах этой главы, можно использовать также и для нахождения корней. Однако эти алгоритмы чаще всего являются не самым эффективным способом вычисления корней многочлена, когда ставится именно такая задача. Поэтому мы рассмотрим методы, более приспособленные для этой цели.

В качестве исходного шага полезно выделить ту часть многочлена f, которая содержит все его корни в поле $\mathbb{F}_q$. Это достигается вычислением НОД $(f(x), x^q - x)$. Ввиду того что двучлен $x^q - x$ является произведением всех нормированных линейных многочленов кольца $\mathbb{F}_q[x]$, указанный наибольший общий делитель равен произведению всех тех нормированных линейных многочленов над $\mathbb{F}_q$, которые делят f; поэтому его корнями являются те и только те корни многочлена f, которые принадлежат полю $\mathbb{F}_q$. Учитывая это, можно без ограничения общности предполагать, что все корни многочлена, для которого мы намерены найти корни в поле $\mathbb{F}_q$, принадлежат полю $\mathbb{F}_q$ и притом различны, т. е. что f является произведением различных линейных нормированных многочленов из $\mathbb{F}_q[x]$.

Один полезный метод нахождения корней многочленов мы уже рассмотрели в § 4 гл. 3; он был основан на определении аффинного кратного для данного многочлена. Этот метод мы проиллюстрировали примером 3.55.

Переходя к другим методам, рассмотрим сначала случай простого поля $\mathbb{F}_p$. Как уже было отмечено, достаточно рассмотреть лишь многочлены вида

$$f(x) = \prod_{i=1}^{n} (x - c_i),$$

где $c_1, \ldots, c_n$ — различные элементы поля $\mathbb{F}_p$. Если число p мало, то найти корни многочлена f можно просто методом проб и ошибок, т. е. простым вычислением всех значений $f(0), f(1), \ldots, f(p-1)$.

Если же число p велико, то можно применить следующий прием. Пусть $b \in \mathbb{F}_p$, где p нечетно. Рассмотрим равенство

$$f(x-b) = \prod_{i=1}^{n} (x - (b + c_i)).$$

Заметим, что многочлен $f(x-b)$ делит двучлен $x^p - x = x(x^{(p-1)/2} + 1)(x^{(p-1)/2} - 1)$. Если при этом x является делителем многочлена $f(x-b)$, то $f(-b) = 0$, и нами найден один из корней многочлена f. Если же x не является делителем $f(x-b)$, то

$$f(x-b) = \text{НОД}(f(x-b), x^{(p-1)/2} + 1)\,\text{НОД}(f(x-b), x^{(p-1)/2} - 1). \quad (4.22)$$

Равенство (4.22) мы теперь используем следующим образом. Приведем степень $x^{(p-1)/2}$ по модулю $f(x-b)$ (например, применяя технику последовательного возведения в квадрат, рассмотренную вслед за теоремой 4.13). Если $x^{(p-1)/2} \not\equiv \pm 1 \pmod{f(x-b)}$, то равенство (4.22) даст нетривиальное частичное разложение многочлена $f(x-b)$. Заменяя x на $x+b$, мы получим нетривиальное частичное разложение многочлена $f(x)$. В довольно редком случае, когда $x^{(p-1)/2} \equiv \pm 1 \pmod{f(x-b)}$, можно использовать другое значение b. Таким образом, изменяя по мере необходимости выбор элемента b, мы можем найти либо некоторый корень многочлена f, либо его нетривиальное частичное разложение. Продолжая тот же процесс для полученных делителей многочлена f, мы в конечном счете получим все корни этого многочлена. Здесь можно было бы заметить, что описанный алгоритм отыскания корней многочлена носит не детерминистический, а вероятностный характер, так как зависит от случайного выбора соответствующего элемента b.

4.15. Пример. Найдем корни многочлена $f(x) = x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2 \in \mathbb{F}_{17}[x]$, содержащиеся в поле $\mathbb{F}_{17}$. Такими корнями являются корни в этом поле многочлена $g(x) = \text{НОД}(f(x), x^{17} - x)$ и только они. С помощью алгоритма Евклида находим, что $g(x) = x^4 + 6x^3 - 5x^2 + 7x - 2$. Для отыскания корней многочлена $g(x)$ воспользуемся алгоритмом, описанным выше. Возьмем сначала $b = 0$; прямое вычисление показывает, что $x^{(p-1)/2} = x^8 \equiv 1 \pmod{g(x)}$, так что значение $b = 0$ не приводит к нетривиальному частичному разложению многочлена $g(x)$. Возьмем теперь $b = 1$; тогда $g(x-1) = x^4 + 2x^3 - 3x - 2$ и $x^8 \equiv -4x^3 - 7x^2 + 8x - 5 \pmod{g(x-1)}$,

и мы приходим к нетривиальному частичному разложению многочлена $g(x-1)$. Имеем

$$\text{НОД}(g(x-1), x^8+1) = \text{НОД}(x^4+2x^3-3x-2, -4x^3-7x^2+8x-4) = x^2-7x+4,$$

$$\text{НОД}(g(x-1), x^8-1) = \text{НОД}(x^4+2x^3-3x-2, -4x^3-7x^2+8x-6) = x^2-8x+8,$$

так что из равенства (4.22) получаем разложение

$$g(x-1) = (x^2-7x+4)(x^2-8x+8),$$

которое после замены x на $x+1$ приводит к следующему частичному разложению для $g(x)$:

$$g(x) = (x^2-5x-2)(x^2-6x+1) = g_1(x)\,g_2(x).$$

Чтобы разложить многочлены $g_1(x)$ и $g_2(x)$, возьмем $b=2$. Тогда $g_1(x-2) = x^2+8x-5$ и $x^8 \equiv -8x+2 \pmod{g_1(x-2)}$. Далее,

$$\text{НОД}(g_1(x-2), x^8+1) = \text{НОД}(x^2+8x-5, -8x+3) = x+6;$$

деление углом дает $g_1(x-2) = (x+6)(x+2)$, откуда получаем

$$g_1(x) = (x+8)(x+4).$$

Обращаясь к $g_2(x)$, получаем, что $g_2(x-2) = x^2+7x = x(x+7)$, так что -2 — корень многочлена $g_2(x)$. Отсюда следует, что

$$g_2(x) = (x+2)(x-8).$$

В итоге получаем следующее разложение $g(x)$ на линейные множители: $g(x) = (x+8)(x+4)(x+2)(x-8)$. Поэтому корнями многочлена $g(x)$ (а значит, и многочлена $f(x)$) в поле $\mathbb{F}_{17}$ являются элементы -8, -4, -2 и 8. □

Теперь мы построим алгоритм нахождения корней для случая, когда конечное поле $\mathbb{F}_q$ велико, но его характеристика p мала. Как и выше, достаточно рассмотреть случай, когда

$$f(x) = \prod_{i=1}^{n} (x-\gamma_i),$$

где $\gamma_1, \ldots, \gamma_n$ — различные элементы поля $\mathbb{F}_q$. Считая, что $q = p^m$, положим

$$S(x) = \sum_{j=0}^{m-1} x^{p^j}.$$

Напомним, что для любого элемента $\gamma \in \mathbb{F}_q$ его абсолютный след $S(\gamma) = \mathrm{Tr}_{\mathbb{F}_q}(\gamma)$ принадлежит простому подполю $\mathbb{F}_p$ (см. определение 2.22). В силу теоремы 2.23(iii), уравнение $S(\gamma) = c$ имеет p^{m-1} решений $\gamma \in \mathbb{F}_q$ для каждого $c \in \mathbb{F}_p$, так что мы приходим к равенству

$$x^q - x = \prod_{c \in \mathbb{F}_p} (S(x) - c). \tag{4.23}$$

Поскольку многочлен $f(x)$ делит $x^q - x$, мы получаем, что

$$\prod_{c \in \mathbb{F}_p} (S(x) - c) \equiv 0 \pmod{f(x)},$$

откуда

$$f(x) = \prod_{c \in \mathbb{F}_p} \mathrm{НОД}(f(x),\ S(x) - c). \tag{4.24}$$

Этот метод приводит к частичному разложению многочлена $f(x)$, и при этом требуется вычислить всего p наибольших общих делителей. Поэтому если p мало, то указанный метод, безусловно, пригоден.

Может, однако, случиться, что разложение (4.24) тривиально (так будет, если $S(x) \equiv c \pmod{f(x)}$ для некоторого $c \in \mathbb{F}_p$). В таком случае следует использовать другие вспомогательные многочлены, связанные с $S(x)$. Пусть β — образующий элемент поля $\mathbb{F}_q$ над $\mathbb{F}_p$, так что $\{1, \beta, \beta^2, \ldots, \beta^{m-1}\}$ — базис $\mathbb{F}_q$ над $\mathbb{F}_p$. Подставляя $\beta^j x$, $0 \leqslant j \leqslant m-1$, вместо x в (4.23), получаем

$$(\beta^j)^q x^q - \beta^j x = \prod_{c \in \mathbb{F}_p} (S(\beta^j x) - c).$$

Так как $(\beta^j)^q = \beta^j$, то

$$x^q - x = \beta^{-j} \prod_{c \in \mathbb{F}_p} (S(\beta^j x) - c).$$

Это приводит к следующему обобщению разложения (4.24):

$$f(x) = \prod_{c \in \mathbb{F}_p} \mathrm{НОД}(f(x),\ S(\beta^j x) - c) \quad \text{для любого } j,$$
$$0 \leqslant j \leqslant m-1. \tag{4.25}$$

Покажем теперь, что если $n = \deg(f) \geqslant 2$, то существует по крайней мере одно значение j, $0 \leqslant j \leqslant m-1$, для которого частичное разложение (4.25) нетривиально. Предположим противное, т. е. что все частичные разложения вида (4.25) тривиальны. Тогда для каждого j, $0 \leqslant j \leqslant m-1$, существует такой элемент $c_j \in \mathbb{F}_p$, что

$$S(\beta^j x) \equiv c_j \pmod{f(x)}.$$

В частности, для (различных!) корней γ_1 и γ_2 многочлена f получаем

$$S(\beta^j\gamma_1) = S(\beta^j\gamma_2) = c_j \quad \text{для всех} \quad j,\ 0 \leqslant j \leqslant m-1.$$

В силу линейности следа это означает, что

$$\mathrm{Tr}_{\mathbb{F}_q}((\gamma_1 - \gamma_2)\beta^j) = 0 \quad \text{для всех} \quad j,\ 0 \leqslant j \leqslant m-1,$$

так что

$$\mathrm{Tr}_{\mathbb{F}_q}((\gamma_1 - \gamma_2)\alpha) = 0 \quad \text{для всех} \quad \alpha \in \mathbb{F}_q.$$

Применяя вторую часть теоремы 2.24, мы тогда заключаем, что $\gamma_1 - \gamma_2 = 0$, получая противоречие. Таким образом, по крайней мере для одного значения j, $0 \leqslant j \leqslant m-1$, частичное разложение (4.25) нетривиально.

Образующий элемент β поля $\mathbb{F}_q$ над $\mathbb{F}_p$, используемый в разложении (4.25), можно выбрать как корень какого-либо заданного неприводимого многочлена степени m из кольца $\mathbb{F}_p[x]$. Получив нетривиальное разложение вида (4.25), мы затем тот же метод применяем к найденным нетривиальным сомножителям многочлена f, используя другое значение j. Рассуждение, приведенное выше, показывает также, что, перебирая разные значения j в (4.25), мы в конечном счете можем найти все корни многочлена f.

Пример 4.16. Рассмотрим поле $\mathbb{F}_{64} = \mathbb{F}_2(\beta)$, где β — некоторый корень неприводимого многочлена $x^6 + x + 1$ из $\mathbb{F}_2[x]$, и пусть

$$f(x) = x^4 + (\beta^5 + \beta^4 + \beta^3 + \beta^2)x^3 + (\beta^5 + \beta^4 + \beta^2 + \beta + 1)x^2 + (\beta^4 + \beta^3 + \beta)x + (\beta^3 + \beta) \in \mathbb{F}_{64}[x].$$

Используя сравнение

$$x^6 \equiv (\beta^5 + \beta + 1)x^3 + (\beta^4 + \beta^3 + \beta^2)x^2 + (\beta^5 + \beta^3 + \beta^2 + 1)x + (\beta^5 + \beta^4 + \beta^2 + 1) \pmod{f(x)},$$

получим последовательным возведением в квадрат следующие сравнения по модулю $f(x)$:

$$\begin{aligned}
x &\equiv x,\\
x^2 &\equiv x^2,\\
x^4 &\equiv (\beta^5+\beta^4+\beta^3+\beta^2)x^3 + (\beta^5+\beta^4+\beta^2+\beta+1)x^2 + (\beta^4+\beta^3+\beta)x + (\beta^3+\beta),\\
x^8 &\equiv (\beta^4+\beta^3+\beta^2)x^3 + (\beta^5+\beta+1)x^2 + (\beta^5+\beta+1)x + (\beta^5+\beta^4),\\
x^{16} &\equiv (\beta^5+\beta^3+\beta)x^3 + (\beta^3+\beta)x^2 + \beta^5 x + (\beta^4+\beta^3+\beta^2+\beta+1),\\
x^{32} &\equiv (\beta^5+\beta^2+1)x^3 + (\beta^5+\beta^4+\beta^3+\beta^2+\beta+1)x^2 + (\beta^4+\beta^2)x + (\beta^5+\beta^3),\\
x^{64} &\equiv x.
\end{aligned}$$

Таким образом, многочлен $f(x)$ делит двучлен $x^{64} - x$ и, следовательно, имеет четыре различных корня в поле $\mathbb{F}_{64}$. Рассмотрим

теперь многочлен $S(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{32}$. Из приведенных выше сравнений получаем, что

$$S(x) \equiv (\beta^5 + \beta^3 + \beta^2 + \beta + 1)\, x^3 + \beta^5 x^2 + (\beta^3 + \beta^2)\, x + (\beta^3 + \beta^2 + 1) \pmod{f(x)},$$

так что

$$\text{НОД}(f(x),\ S(x)) = \text{НОД}(f(x),\ (\beta^5 + \beta^3 + \beta^2 + \beta + 1)\, x^3 + \beta^5 x^2 + (\beta^3 + \beta^2)\, x + (\beta^3 + \beta^2 + 1)) =$$
$$= x^3 + (\beta^4 + \beta^3 + \beta^2)\, x^2 + (\beta^5 + \beta^2 + 1)\, x + (\beta^3 + \beta^2) = g(x)$$

и

$$\text{НОД}(f(x),\ S(x) - 1) = \text{НОД}(f(x),\ (\beta^5 + \beta^3 + \beta^2 + \beta + 1)\, x^3 + \beta^5 x^2 + (\beta^3 + \beta^2)\, x + (\beta^3 + \beta^2) =$$
$$= x + \beta^5.$$

Поэтому из (4.24) получаем

$$f(x) = g(x)\,(x + \beta^5). \tag{4.26}$$

Чтобы найти корни многочлена $g(x)$, мы теперь применим разложение (4.25) с $j = 1$. Поскольку

$$S(\beta x) = \beta x + \beta^2 x^2 + \beta^4 x^4 + \beta^8 x^8 + \beta^{16} x^{16} + \beta^{32} x^{32} =$$
$$= \beta x + \beta^2 x^2 + \beta^4 x^4 + (\beta^3 + \beta^2)\, x^8 + (\beta^4 + \beta + 1)\, x^{16} + (\beta^3 + 1)\, x^{32},$$

то из полученных выше сравнений вытекает, что

$$S(\beta x) \equiv (\beta^2 + 1)\, x^3 + (\beta^3 + \beta + 1)\, x^2 + (\beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta + 1)\, x + (\beta^4 + \beta^2 + \beta) \pmod{f(x)}.$$

Так как многочлен $g(x)$ делит $f(x)$, то это сравнение выполняется также и по модулю $g(x)$, поэтому

$$S(\beta x) \equiv (\beta^2 + 1)\, x^3 + (\beta^3 + \beta + 1)\, x^2 + (\beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta + 1)\, x + (\beta^4 + \beta^2 + \beta) \equiv$$
$$\equiv (\beta^5 + \beta^2)\, x^2 + \beta^3 x + (\beta^5 + \beta^3 + \beta) \pmod{g(x)}.$$

Таким образом,

$$\text{НОД}(g(x),\ S(\beta x)) = \text{НОД}(g(x),\ (\beta^5 + \beta^2)\, x^2 + \beta^3 x + (\beta^5 + \beta^3 + \beta)) =$$
$$= x^2 + (\beta^3 + 1)\, x + (\beta^4 + \beta^3 + \beta^2 + \beta) = h(x)$$

и

$$\text{НОД}(g(x),\ S(\beta x) - 1) = \text{НОД}(g(x),\ (\beta^5 + \beta^2)\, x^2 + \beta^3 x + (\beta^5 + \beta^3 + \beta + 1)) =$$
$$= x + (\beta^4 + \beta^2 + 1).$$

Поэтому для $j = 1$ из (4.25) получаем, что

$$g(x) = h(x)(x + (\beta^4 + \beta^2 + 1)). \tag{4.27}$$

Чтобы найти корни многочлена $h(x)$, снова применим разложение (4.25), но возьмем $j = 2$. Поскольку

$$\begin{aligned} S(\beta^2 x) &= \beta^2 x + \beta^4 x^2 + \beta^8 x^4 + \beta^{16} x^8 + \beta^{32} x^{16} + \beta^{64} x^{32} = \\ &= \beta^2 x + \beta^4 x^2 + (\beta^3 + \beta^2) x^4 + (\beta^4 + \beta + 1) x^8 + \\ &\quad + (\beta^3 + 1) x^{16} + \beta x^{32}, \end{aligned}$$

то такой же подсчет, как и для $S(\beta x)$, дает

$$S(\beta^2 x) \equiv (\beta^5 + \beta^2 + 1) x + (\beta^5 + \beta^3 + \beta^2) \pmod{h(x)}.$$

Поэтому

$$\begin{aligned} \text{НОД}(h(x), S(\beta^2 x)) &= \text{НОД}(h(x), (\beta^5 + \beta^2 + 1) x + \beta^5 + \\ &\quad + \beta^3 + \beta^2) = \\ &= x + (\beta + 1), \\ \text{НОД}(h(x), S(\beta^2 x) - 1) &= \text{НОД}(h(x), (\beta^5 + \beta^2 + 1) x + \\ &\quad + \beta^5 + \beta^3 + \beta^2 + 1) = \\ &= x + (\beta^3 + \beta), \end{aligned}$$

так что из (4.25) для $j = 2$ мы получаем

$$h(x) = (x + \beta + 1)(x + \beta^3 + \beta). \tag{4.28}$$

Объединяя (4.26), (4.27) и (4.28), получаем следующее разложение многочлена f:

$$f(x) = (x + \beta + 1)(x + \beta^3 + \beta)(x + \beta^4 + \beta^2 + 1)(x + \beta^5),$$

так что корнями многочлена $f(x)$ в поле $\mathbb{F}_{64}$ являются элементы $\beta + 1$, $\beta^3 + \beta$, $\beta^4 + \beta^2 + 1$ и β^5. □

И наконец, мы рассмотрим проблему отыскания корней многочлена для случая большого конечного поля $\mathbb{F}_q$ с большой характеристикой p. Как уже говорилось раньше, достаточно выяснить, как находить корни многочленов вида

$$f(x) = \prod_{i=1}^{n} (x - \gamma_i)$$

с различными элементами $\gamma_1, \ldots, \gamma_n \in \mathbb{F}_q$. Для выяснения вопроса, будет ли данный многочлен $f(x)$ иметь такой вид, достаточно лишь проверить выполнение сравнения $x^q \equiv x \pmod{f(x)}$ (ср. с первой частью примера 4.16). Мы можем предположить, что q — наименьшая степень характеристики p, для которой выполняется

это сравнение. Многочлен $f(x)$ зададим стандартным представлением

$$f(x) = \sum_{j=0}^{n} \alpha_j x^j,$$

где $\alpha_j \in \mathbb{F}_q$ для $0 \leqslant j < n$ и $\alpha_n = 1$.

Нашей первой целью будет отыскание какого-нибудь нетривиального делителя многочлена $f(x)$. Чтобы исключить тривиальный случай, предположим, что $n \geqslant 2$. Считая, что $q = p^m$, рассмотрим многочлены

$$f_k(x) = \sum_{j=0}^{n} \alpha_j^{p^k} x^j, \quad k = 0, 1, \ldots, m-1, \tag{4.29}$$

так что $f_0(x) = f(x)$ и $f_k(x)$ — нормированный многочлен над $\mathbb{F}_q$ для каждого k, $0 \leqslant k \leqslant m-1$. Нетрудно видеть, что для всех i, $1 \leqslant i \leqslant n$, и k, $0 \leqslant k \leqslant m-1$,

$$f_k(\gamma_i^{p^k}) = \sum_{j=0}^{n} \alpha_j^{p^k} \gamma_i^{jp^k} = \left(\sum_{j=0}^{n} \alpha_j \gamma_i^j \right)^{p^k} = 0,$$

так что

$$f_k(x) = \prod_{i=1}^{n} (x - \gamma_i^{p^k}), \quad k = 0, 1, \ldots, m-1.$$

Построим теперь многочлен

$$F(x) = \prod_{k=0}^{m-1} f_k(x). \tag{4.30}$$

Это многочлен над полем $\mathbb{F}_p$, так как

$$F(x) = \prod_{k=0}^{m-1} \prod_{i=1}^{n} (x - \gamma_i^{p^k}) = \prod_{i=1}^{n} \prod_{k=0}^{m-1} (x - \gamma_i^{p^k}) = \prod_{i=1}^{n} F_i(x)^{m/d_i},$$

где $F_i(x)$ — минимальный многочлен элемента γ_i над полем $\mathbb{F}_p$, а d_i — его степень (ср. с материалом, предшествующим теореме 2.23). Поэтому многочлены $F_i(x)$ являются неприводимыми сомножителями многочлена $F(x)$ в кольце $\mathbb{F}_p[x]$, но некоторые из них, вообще говоря, могут совпадать между собой. Значит, каноническое разложение многочлена $F(x)$ в кольце $\mathbb{F}_p[x]$ имеет вид

$$F(x) = G_1(x) \ldots G_r(x), \tag{4.31}$$

где $G_t(x)$, $1 \leqslant t \leqslant r$, — степени различных неприводимых многочленов $F_i(x)$. Это каноническое разложение может быть получено с помощью одного из алгоритмов, изложенных в § 2 этой главы.

Поскольку многочлен $f(x) = f_0(x)$ делит $F(x)$, то из (4.31) следует, что

$$f(x) = \prod_{t=1}^{r} \text{НОД}(f(x),\ G_t(x)). \tag{4.32}$$

Формула (4.32), как правило, дает нетривиальное частичное разложение многочлена $f(x)$. Тривиальным оно является в том и только том случае, когда НОД $(f(x), G_t(x)) = f(x)$ для какого-нибудь t, $1 \leqslant t \leqslant r$, что эквивалентно условию $r = 1$ [1]), и тогда $f(x)$ делит $F_1(x)$. Сравнение степеней показывает [2]), что $n \leqslant d_1 = m$. Кроме того, корни многочлена $f(x)$ в этом случае все сопряжены относительно поля $\mathbb{F}_p$. Таким образом, мы можем записать (изменив, если нужно, нумерацию корней многочлена $f(x)$)

$$\gamma_i = \gamma_1^{p^{b_i}}, \quad 1 \leqslant i \leqslant n, \quad \text{где } 0 = b_1 < b_2 < \ldots < b_n < m.$$

Положим $b_{n+1} = m$ и $d = \min\limits_{1 \leqslant i \leqslant n} (b_{i+1} - b_i)$. Ясно, что $d \leqslant m/n$. Могут встретиться следующие две возможности:

(A) $b_{i+1} - b_i > d$ для некоторого i, $1 \leqslant i \leqslant n$;

(B) $b_{i+1} - b_i = d$ для всех i, $1 \leqslant i \leqslant n$.

В случае (A) заметим, что множеством корней многочлена $f(x)$ является

$$\left\{\gamma_1^{p^{b_1}},\ \gamma_1^{p^{b_2}},\ \ldots,\ \gamma_1^{p^{b_n}}\right\},$$

а множеством корней многочлена $f_d(x)$ является

$$\left\{\gamma_1^{p^{b_1+d}},\ \gamma_1^{p^{b_2+d}},\ \ldots,\ \gamma_1^{p^{b_n+d}}\right\}.$$

Из условия (A) следует, что эти два множества корней не совпадают. Но, с другой стороны, поскольку $b_{i+1} - b_i = d$ для некоторого i, $1 \leqslant i \leqslant n$, эти два множества корней содержат общий элемент. Таким образом, многочлен НОД $(f(x), f_d(x))$ отличен как от $f(x)$, так и от 1. Следовательно, НОД $(f(x), f_d(x))$ является нетривиальным делителем многочлена $f(x)$. Нетрудно видеть также, что в этом случае $d < m/n$.

В случае (B) сравнение множеств корней многочленов $f(x)$ и $f_d(x)$ показывает, что $f(x) = f_d(x)$, так что НОД $(f(x), f_k(x)) = 1$ для всех $k = 1, \ldots, d-1$. Кроме того, $d = m/n$, так что число n делит m, и, значит, $b_i = d(i-1)$ для $i = 1, \ldots, n$. Отсюда следуют равенства, $\gamma_i = \gamma_1^{p^{d(i-1)}}$, $i = 1, 2, \ldots, n$,

[1]) Так как если $G_t(x) = F_i(x)^{k_i}$, то F_i является минимальным многочленом каждого корня γ_j многочлена f. — *Прим. перев.*

[2]) Так как F_1 содержит все γ_j, $1 \leqslant j \leqslant n$. Если бы было $d_1 < m$, то все γ_j принадлежали бы $\mathbb{F}_{p^{d_1}}$, что противоречит выбору $q = p^m$. — *Прим. перев.*

т. е. элементами γ_i являются элементы, сопряженные с γ_1 относительно поля $\mathbb{F}_{p^d}$, и только они. Следовательно, $f(x)$ является минимальным многочленом элемента γ_1 над $\mathbb{F}_{p^d}$ и, значит, неприводим над $\mathbb{F}_{p^d}$.

Поэтому в соответствии со случаями (A) и (B) мы получаем следующие две возможности:

(A) Многочлен НОД $(f(x), f_k(x))$ для некоторого k, $1 \leqslant k < m/n$, является нетривиальным делителем многочлена $f(x)$.

(B) НОД $(f(x), f_k(x)) = 1$ для всех $k = 1, \ldots, d-1$, где $d = m/n \in \mathbb{N}$, и $f(x) = f_d(x)$ — минимальный многочлен элемента γ_1 над полем $\mathbb{F}_{p^d}$.

Следовательно, в случае (A) наша цель отыскания нетривиального делителя многочлена $f(x)$ достигнута.

В случае же (B) еще требуется дополнительное исследование. Пусть β снова обозначает образующий элемент поля $\mathbb{F}_q$ над $\mathbb{F}_p$. Тогда $\mathbb{F}_{p^d}(\beta) = \mathbb{F}_q = \mathbb{F}_{p^m}$, так что элемент β имеет степень $m/d = n$ над полем $\mathbb{F}_{p^d}$. В частности, это означает, что $\beta^j \notin \mathbb{F}_{p^d}$ для всех j, $1 \leqslant j \leqslant n-1$. Пусть теперь коэффициенты α_j многочлена $f(x)$ таковы, что $\alpha_{j_0} \neq 0$ для некоторого j_0, $1 \leqslant j_0 \leqslant n-1$. Рассмотрим многочлен

$$\bar{f}(x) = \beta^{-n} f(\beta x), \tag{4.33}$$

который является нормированным многочленом степени n над $\mathbb{F}_q$. Так как $\beta^{n-j_0} \notin \mathbb{F}_{p^d}$, а $\alpha_{j_0} \in \mathbb{F}_{p^d}^*$, то, значит, коэффициент при x^{j_0} в многочлене $\bar{f}(x)$ не принадлежит полю $\mathbb{F}_{p^d}$. Поэтому $\bar{f}(x)$ не является многочленом над полем $\mathbb{F}_{p^d}$, и, следовательно, если указанную выше процедуру применить к многочлену $\bar{f}(x)$, то случай (B) не может встретиться, и мы получим некоторый нетривиальный делитель многочлена $\bar{f}(x)$. А поскольку $f(x) = \beta^n \bar{f}(\beta^{-1}x)$, то каждому нетривиальному делителю многочлена $\bar{f}(x)$ соответствует некоторый нетривиальный делитель многочлена $f(x)$.

Остается рассмотреть последнюю возможность: когда имеет место случай (B) и коэффициенты α_j многочлена $f(x)$ равны нулю для всех j, $1 \leqslant j \leqslant n-1$. Это означает, что $f(x)$ является двучленом $x^n + \alpha_0 \in \mathbb{F}_{p^d}[x]$. Здесь n не может делиться на p, так как в противном случае мы имели бы $f(x) = \left(x^{n/p} + \alpha_0^{p^{d-1}}\right)^p$, что противоречит неприводимости многочлена $f(x)$ над полем $\mathbb{F}_{p^d}$. Положим в этом случае

$$\bar{f}(x) = \beta^{-n} f(\beta x + 1), \tag{4.34}$$

и тогда из того, что $\beta^{-1} \notin \mathbb{F}_{p^d}$, сразу вытекает, что коэффициент при x^{n-1} в многочлене $\bar{f}(x)$ не принадлежит полю $\mathbb{F}_{p^d}$. Следова-

тельно, если описанную выше процедуру применить к многочлену $\bar{f}(x)$, то не может встретиться случай (B), и мы получим некоторое нетривиальное разложение многочлена $f(x)$. Но поскольку $f(x) = \beta^n \bar{f}(\beta^{-1}(x-1))$, каждому нетривиальному разложению многочлена $\bar{f}(x)$ соответствует некоторое нетривиальное разложение многочлена $f(x)$.

Итак, применяя этот алгоритм отыскания корней многочлена $f(x)$, мы должны поступать следующим образом. Сначала построим многочлены $f_k(x)$ по формуле (4.29) и многочлен $F(x) \in \mathbb{F}_p[x]$ по формуле (4.30). Затем, применяя алгоритм разложения из § 2, находим каноническое разложение (4.31) многочлена $F(x)$ в кольце $\mathbb{F}_p[x]$; это приводит к частичному разложению (4.32) многочлена $f(x)$. Если это разложение оказывается тривиальным, мы находим многочлены НОД $(f(x), f_k(x))$ для всех k, $1 \leqslant k < m/n$. Если и это не приводит к нетривиальному разложению многочлена $f(x)$, мы заменяем многочлен $f(x)$ многочленом $\bar{f}(x)$ из формул (4.34) или (4.33) в соответствии с тем, является $f(x)$ двучленом или нет. Как показано выше, применение того же алгоритма к $\bar{f}(x)$ уже обязательно приводит к нетривиальному разложению многочлена $\bar{f}(x)$, а следовательно, и многочлена $f(x)$. Как только нетривиальные делители многочлена $f(x)$ найдены, процедура повторяется с заменой многочлена $f(x)$ полученными его нетривиальными делителями, и так продолжается до полного разложения многочлена $f(x)$ на линейные сомножители, которые, согласно теореме 1.64, и определяют корни этого многочлена.

Комментарии

§ 1. Алгоритм разложения, основанный на матрице B (алгоритм Берлекэмпа), был впервые изложен в статье Berlekamp [3] и воспроизведен в книге Berlekamp [4, ch. 6]. Возможность использования матрицы B из этого алгоритма для определения числа нормированных неприводимых сомножителей многочлена f была замечена еще раньше. В статье Petr [1] показано, что если все неприводимые сомножители многочлена f различны (т. е. в разложении (4.1) $e_1 = \ldots = e_k = 1$), то характеристический многочлен $\det(xI - B)$ матрицы B равен произведению двучленов $(x^{n_1} - 1) \ldots (x^{n_k} - 1)$, где $n_i = \deg(f_i)$, $i = 1, \ldots, k$. Общий случай был исследован Шварцом, показавшим в статье Schwarz [1], что $\det(xI - B) = x^m (x^{n_1} - 1) \ldots (x^{n_k} - 1)$, где $m = \sum_{i=1}^{k} n_i (e_i - 1)$; см. также Schwarz [11]. Результат, состоящий в том, что ранг матрицы $B - I$ равен $n - k$, установлен Батлером (Butler [1]); другое его доказательство дано Шварцом (Schwarz [11]). В статье Willett [5] число k интерпретируется как размерность

векторного пространства линейных рекуррентных последовательностей (см. гл. 8). Алгоритм Берлекэмпа излагается в следующих работах: Childs [1, part II, ch. 12], Collins [3], Knuth [3, ch. 4], Lidl, Pilz [1, ch. 7], Mignotte [3] и Zimmer [2, ch. 2].

Алгоритмы, основанные на многочленах T_i (см. теорему 4.3) и R_i (см. теорему 4.5), построены Макэлайсом (McEliece [2]). В его же работе McEleice [3] приводятся таблицы разложения двучленов $x^n - 1$, полученные применением этих алгоритмов. Изложение этих и других алгоритмов разложения можно найти также в работах Collins [3], Knuth [3, ch. 4], Lidl, Wiesenbauer [1, ch. 2], Mignotte [3] и Zimmer [2, ch. 2].

Матрицу B можно также использовать для определения числа σ_d различных нормированных неприводимых делителей степени d $(1 \leqslant d \leqslant n)$ многочлена f. Шварц (Schwarz [11]) показал, что числа σ_d удовлетворяют следующей системе линейных уравнений:

$$\sum_{d=1}^{n} \text{НОД}\,(j,\ d)\ \sigma_d = n - h_j, \quad j = 1, 2, \ldots, n,$$

где h_j — ранг матрицы $B^j - I$. Частные случаи такой системы рассматривались раньше в статьях Rédei [9] и Schwarz [4], [7]. С помощью этой системы в статье Gunji, Arnon [1] был построен алгоритм для определения чисел σ_d. В статье Schwarz [13] для числа σ_d получено следующее сравнение по модулю характеристики ρ поля $\mathbb{F}_q$:

$$d\sigma_d \equiv \sum_{t \mid d} \mu\,(d/t)\ \text{Tr}\,(B^t) \pmod{p},$$

где μ — функция Мёбиуса, $\text{Tr}\,(B^t)$ — след матрицы B^t, а сумма распространяется на все положительные делители t числа d. Частный случай этого сравнения для $d = 1$ был получен еще в статье Schwarz [3]. В этой последней статье содержатся и другие сравнения по модулю p для чисел σ_d, выраженные с помощью $n \times n$-матрицы $A = (a_{ij})$, где $a_{ij} = s_{i+j}$ и s_r обозначает сумму r-х степеней корней многочлена f. В статье Schwarz [14] были получены формулы, выражающие числа σ_d через ранги матриц, связанных с матрицей A. В работе Horáková, Schwarz [1] приводятся формулы, выражающие числа σ_d через ранги циркулянтных матриц, образованных коэффициентами многочлена f; по этому поводу см. также Ward [10]. Связи между свойствами многочлена f и соответствующей ему матрицы B были исследованы также в работах Chen, Li [1] и T'u [1]. Упомянем еще об использовании матрицы B в общем алгоритме разложения Кемпферта (Kempfert [1]) и в полученных Симсом (Sims [1]) условиях, при которых коммутативная конечномерная алгебра над конечным полем $\mathbb{F}_q$ является полем.

Отметим следующий полезный результат о числе неприводимых сомножителей многочлена. Пусть над полем $\mathbb{F}_q$ нечетной характеристики задан многочлен f степени $n \geqslant 2$ с дискриминантом $D \neq 0$ (см. определение 1.92) и k — число его нормированных неприводимых сомножителей; тогда $\eta(D) = (-1)^{n-k}$, где η — квадратичный характер поля $\mathbb{F}_q$ (см. пример 5.10). Впервые это показал (для простых полей) Пелле (Pellet [2]), а затем в общем виде доказал Штикельбергер (Stickelberger [2]); в литературе этот результат известен как *теорема четности* Штикельбергера. Доказательство этого результата можно также найти в следующих работах: Berlekamp [4, ch. 6], Carlitz [67], Childs [1, part III, ch. 15], Dalen [1], Hensel [2], Lubelski [2], Rédei [6], [10, ch. 11], Schwarz [3], Segre [10], Skolem [5], Swan [1] и Вороной [2], а один частный случай этой теоремы был рассмотрен в статье Dickson [9]. Различные варианты теоремы четности Штикельбергера для случая поля $\mathbb{F}_q$ характеристики 2 даются в работах Stickelberger [2], Carlitz [44], Segre [10] и Berlekamp [4, ch. 6], [10]. Еще Пелле (Pellet [2]) заметил, что теорему четности Штикельбергера можно применить для доказательства квадратичного закона взаимности (см. теорему 5.17); см. также работы Berlekamp [4, ch. 6], Childs [1, part III, ch. 16], Mirimanoff, Hensel [1], Rédei [10, ch. 11] и Swan [1].

Мы уже встречались с разложениями многочленов из некоторых специальных классов. Так, в § 4 гл. 2 рассматривались круговые многочлены, в § 4 гл. 3 — линеаризованные и аффинные многочлены и в § 5 гл. 3 — двучлены и трехчлены. По вопросу о числе корней многочлена (а значит, и о числе его линейных сомножителей) мы отсылаем читателя к § 1 гл. 6. Таблицы разложений многочленов и списки неприводимых многочленов представлены в гл. 10.

Вопрос о разложимости многочленов четвертой степени изучался в работах Carlitz [70], [73], Giudici, Margaglio [1], Leonard [3], Leonard, Williams [1], Skolem [4] и Гребенюк [1]. Разложимость многочленов вида $f(x^t)$ для неприводимых многочленов f рассматривалась в статьях Agou [10], [11], Butler [2] и Pellet [1]. Результаты о степенях делителей многочленов вида $g(x)^t - a$, полученные Ope (Ore [2]), были обобщены в статьях Petterson [1], [2], [3], где изучались многочлены вида $f(g(x)^t)$ для неприводимых многочленов f и им подобные композиции. Разложения многочленов вида $f(L(x))$, где f — неприводимый, а L — линеаризованный многочлены, изучались в работах Agou [4], [19], [20], Long [3], [4], Long, Vaughan [1], [2] и Варшамов [3], [5]; аналогичные вопросы для многочленов от нескольких переменных рассматривались в статьях Carlitz, Long [1] и Long [5]. В статье Daykin [3] находятся степени и число неприводи-

мых сомножителей многочлена вида $(cx + d)\, x^{q^m} - (ax + b)$ над полем $\mathbb{F}_q$. В работе Williams K. S. [25] получено разложение так называемых многочленов Диксона (см. § 2 гл. 7), а в статье Сергеева [1] — разложение многочленов близкого к ним вида. Некоторые результаты о разложении многочленов Эйлера и Бернулли над конечным простым полем получены в статье Brillhart [1]. В работе Golomb, Lempel [1] изучалось разложение многочленов, задаваемых рекуррентным соотношением второго порядка. Фейт и Рис (Feit, Rees [1]) получили критерий разложимости многочлена $f \in \mathbb{F}_q[x]$ на линейные сомножители над $\mathbb{F}_q$ в терминах сумм степеней корней многочлена f. Более ранние результаты в этом направлении можно найти в статьях Schönemann [2], Thouvenot, Châtelet [1] и Шатуновский [1]. В статье Craven, Csordas [1] охарактеризованы такие последовательности (c_n), $n = 0, 1, \ldots$, что если конечное поле $\mathbb{F}_q$ является полем разложения для многочлена $\sum a_n x^n$, то оно является полем разложения и для многочлена $\sum c_n a_n x^n$.

Коэн (Cohen S. D. [5], [6]) изучал, как распределяются различные типы разложения среди многочленов вида $f(x) + ag(x)$ при заданных $f, g \in \mathbb{F}_q[x]$ и изменяющемся $a \in \mathbb{F}_q$ (см. об этом также Leonard [5]). Кроме того, Коэн (Cohen S. D. [7]) изучал также распределение типов разложения в классах вычетов по модулю некоторого заданного многочлена и в множествах многочленов фиксированной степени, некоторые коэффициенты которых заранее заданы. Вильямс (Williams K. S. [11]) получил асимптотическую формулу для числа $N(q, d, s, e)$ нормированных многочленов данной степени d над полем $\mathbb{F}_q$, имеющих ровно s различных неприводимых нормированных делителей степени e над $\mathbb{F}_q$. В статьях Car [5], [7] и Cohen S. D. [3] приводятся асимптотические формулы для числа нормированных многочленов заданной степени над $\mathbb{F}_q$, имеющих определенные типы разложения; о случае, когда степень многочленов ограничена данным натуральным числом, см. статью Gogia, Luthar [1]. В работе Zsigmondy [2] найдено число нормированных многочленов данной степени n над простым полем $\mathbb{F}_p$, имеющих заданное число различных корней в поле $\mathbb{F}_p$, и для каждого d, $1 \leqslant d \leqslant n$, подсчитано также число нормированных многочленов степени n над $\mathbb{F}_p$, не имеющих неприводимых делителей степени d.

При фактическом осуществлении какого-либо алгоритма разложения многочлена приходится выполнять различные операции в рассматриваемом конечном поле. Например, чтобы сделать нормированным многочлен f, требуется вычислить мультипликативный обратный элемент для старшего коэффициента этого многочлена. Для эффективного выполнения в конечных полях арифметических действий были изобретены различные методы. Так, в работах Collins [1], Davida [1], Schönhage [1] и Willett

[6] рассматривается вопрос о вычислении мультипликативных обратных элементов. Эффективные методы умножения элементов поля разработаны в статьях Fiduccia, Zalcstein [1] и Winograd [1], [2]; см. также Bini, Capovani [1]. Алгоритмы для вычисления некоторых первообразных корней из единицы представлены в работах Liu, Reed, Truong [1] и Reed, Truong, Miller [1], [2]. В статье Pohlig, Hellman [1] построен быстрый алгоритм для вычисления показателя r в равенстве $b^r = a$ при заданных a, $b \in \in \mathbb{F}_q^*$, где b — примитивный элемент поля $\mathbb{F}_q$; об этом см. также работы Herlestam, Johannesson [1], Pollard [3] и Zierler [9], а также гл. 10, § 1 и табл. А настоящей книги. Обзор по арифметическим алгоритмам для конечного поля $\mathbb{F}_q$ дается в работе Mignotte [3]. Реализация арифметики конечных полей на переключательных схемах рассматривалась в следующих работах: Bartee, Schneider [1], Berlekamp [4, ch. 2], Gill [2, ch. 6], MacWilliams, Sloane [2, ch. 3], Peterson, Weldon [1, ch. 7], Redinbo [1], Tanaka, Kasahara, Tezuka, Kasahara [1] и Willett [6]; о реализации ее на ЭВМ см. Calmet, Loos [2].

Полезным вычислительным изобретением является *дискретное преобразование Фурье* для конечного поля $\mathbb{F}_q$, введенное Поллардом (Pollard [1]). Пусть b — некоторый элемент порядка d мультипликативной группы поля $\mathbb{F}_q$. Тогда конечная последовательность $a_0, a_1, \ldots, a_{d-1}$ элементов поля $\mathbb{F}_q$ может быть преобразована в конечную последовательность

$$A_i = \sum_{j=0}^{d-1} a_j b^{ij}, \quad i = 0, 1, \ldots, d-1.$$

При этом обратное преобразование задается формулой

$$a_j = d^{-1} \sum_{i=0}^{d-1} A_i b^{-ij}, \quad j = 0, 1, \ldots, d-1.$$

Эти преобразования называются дискретными преобразованиями Фурье. Оба они допускают быстрое вычисление, и при этом работают методы, аналогичные применяемым в теории быстрых преобразований Фурье в обычном комплексном аиализе. Дискретное преобразование Фурье встречается в теории кодирования под названием многочлена Мэттсона—Соломона (см. Mattson, Solomon [1] и MacWilliams, Sloane [2, ch. 8]). Поллард (Pollard [1]) показал, как можно использовать дискретные преобразования Фурье для выполнения арифметических действий в поле $\mathbb{F}_q$. Дальнейшие результаты о дискретном преобразовании Фурье и его приложениях можно найти в работах Agarwal, Burrus [1], Blahut [1], Fateman [1], Golomb, Reed, Truong [1], Liu, Reed, Truong [1], [2], McClellan, Rader [1], Nussbaumer [1, ch. 8],

Pollard [2], Preparata, Sarwate [1], Redinbo [1], Reed, Scholtz, Truong, Welch [1], Reed, Truong [1], [2], [3], Reed, Truong, Welch [1], Rice [1] и Sarwate [1], [2].

Осуществление какого-либо алгоритма разложения зависит также от действий с многочленами. Эффективные методы перемножения двух многочленов над конечным полем $\mathbb{F}_q$ предлагаются в работах Borodin, Munro [1], Rice [2], Schönhage [2] и Бассалыго [1]; см. также Fateman [1] и Pollard [1]. О вычислении наибольшего общего делителя и об алгоритме Евклида для многочленов от одной или нескольких переменных см. работы Agou [2], [5], Barnett [1], Blankinship [1], Bose N. K. [1], Brown W. S. [1], Collins [3], Dickson [33], Emre, Hüseyin [1], Knuth [3, ch. 4], Maroulas, Barnett [1], McEliece, Shearer [1], Moses [1] и Vogt, Bose [1]. Дальнейшие результаты об арифметике многочленов можно найти в статьях Bhanu Murthy, Sampath [1], Lal [1], Михайлюк [1], [2] и Мурзаев [1]. Полезные сведения о полиномиальных операциях над конечными полями можно найти в следующих книгах: Aho, Hopcroft, Ullman [1], Berlekamp [4, ch. 2], Birkhoff, Bartee [1, ch. 11], Borodin, Munro [1], Gill [2, ch. 6], Knuth [3, ch. 4] и Peterson, Weldon [1, ch. 7]).

§ 2. Алгоритм разложения, основанный на использовании результантов, восходит к одному утверждению из первого издания книги Кнута Knuth [3, ch. 4]. Вычисление полиномиальных результантов методом интерполяции предложено Коллинзом (Collins [2]). Алгоритм Цассенхауза был описан в статье Zassenhaus [5]. Алгоритм разложения с помощью диагонализации матриц из многочленов был предложен Берлекэмпом (Berlekamp [6]). Алгоритм, основанный на теореме 4.13, взят из статьи Golomb, Welch, Hales [1]; см. также Agou [8] и Knuth [3, ch. 4]. О вероятностном алгоритме в этой связи см. Cantor, Zassenhaus [1].

В работах Zassenhaus [4], Kempfert [1] и Knuth [3, ch. 4] рассматривается алгоритм, состоящий в последовательном вычислении для данного многочлена $f \in \mathbb{F}_q[x]$ степени $n \geqslant 2$ без кратных сомножителей многочленов вида $d_i(x) = \text{НОД}(f(x), x^{q^i} - x)$ для $i = 1, 2, \ldots, \lfloor n/2 \rfloor$. Если все d_i равны 1, то многочлен f неприводим над полем $\mathbb{F}_q$. Если же $j \leqslant \lfloor n/2 \rfloor$ — наименьший индекс, для которого $d_j \neq 1$, то многочлен f приводим над $\mathbb{F}_q$ и d_j является произведением всех его неприводимых сомножителей степени j. Другие алгоритмы разложения можно найти в работах Arwin [2], Beard [5], Camion [2], [3], Rabin [1], Ананиашвили, Варшамов, Горовой, Пархоменко [1], Варшамов, Остиану [1] и Дынькин, Агаронов [1]. Сравнительное изучение эффективности различных алгоритмов разложения многочленов предпринято в статье Moenck [1]. Методы определения степени поля разложения многочлена над простым конечным полем рас-

сматриваются в статьях Speiser [1] и Wegner [4]; случай произвольного конечного поля изучается в статьях Mignotte [1], [2], [4].

Эффективные алгоритмы разложения многочленов над конечными простыми полями могут служить хорошим инструментом также и для разложения многочленов над кольцом Z целых чисел. Здесь основной является следующая идея: сначала надо разложить данный многочлен $f \in Z[x]$ по модулю надлежащим образом выбранного простого числа p, а затем отсюда получить разложение этого многочлена над кольцом Z. Берлекэмп (Berlekamp [6], [7]) и Кнут (Knuth [3, ch. 4]) предлагают с этой целью выбрать некий априорный максимум B_0 абсолютных величин для всех коэффициентов любых возможных делителей многочлена f над Z, а затем взять простое число $p > 2B_0$, учитывая, что все делители многочлена f над кольцом Z целых чисел обязательно встретятся среди найденных делителей этого многочлена по модулю p. Относительно значений числа B_0 см. работы Childs [1, part II, ch. 13], Knuth [3, ch. 4], Mignotte [4], Zassenhaus [5] и Zimmer [2, ch. 2]. Цассенхауз в статьях Zassenhaus [5], [6], [7] рассматривает p-адическую процедуру, в которой, исходя из разложения многочлена f по модулю какого-либо меньшего простого числа p, затем с помощью одной конструктивной версии леммы Гензеля получается разложение f по модулю некоторой степени p^k, большей $2B_0$. Из дальнейших работ на эту тему см. Kempfert [1], Lenstra, Lenstra, Lovász [1] и Lloyd [1], [2]; см. также Childs [1, part II, ch. 13]. Обзоры по методам разложения многочленов над кольцом Z целых чисел имеются в работах Collins [3], Knuth [3, ch. 4] и Zimmer [2, ch. 2]. Однако следует заметить, что многочлен $f \in Z[x]$ может быть неприводимым над полем рациональных чисел и в то же время приводимым по модулю p для всех простых чисел p. Пример такого многочлена был указан еще Гильбертом (Hilbert [1]). Особенно простой пример такого многочлена, а именно $f(x) = x^4 + 1$, предложил Шварц (Schwarz [4]). Другие примеры имеются в работах Lee M. A. [1] и Pólya, Szegö [1, sec. VIII, problem 129]). Существуют также многочлены над Z, не имеющие линейных делителей над полем рациональных чисел, но имеющие хотя бы один линейный делитель по модулю p для каждого простого числа p (см., например, Hasse [1], Skolem [3] и van der Waerden [1]).

Алгоритмы разложения для многочленов над полями алгебраических чисел были построены в статьях Lenstra A. K. [1] и Weinberger, Rothschild [1]. Методы разложения многочленов от нескольких переменных над полем рациональных чисел или над полями алгебраических чисел получены в работах Collins [3], Moses [1], Musser [1], Viry [1], [2], Wang P. S. [1], [2], Wang, Rothschild [1] и Weinberger, Rothschild [1].

Дальнейшие результаты о матрицах из многочленов можно найти в следующих источниках: Albert [3, ch. 3], Hoffman, Kunze [1, ch. 7], Krishnamurthy [1], Maroulas, Barnett [1] и Гантмахер [1, гл. 6].

§ 3. Методы, излагаемые в этом параграфе, развиты в работе Берлекэмпа (Berlekamp [6]). Некоторые усовершенствования получены в статье Moenck [1] для случая простого поля $\mathbb{F}_p$, когда число $p-1$ делится на большую степень двойки. Описанный в § 4 гл. 3 алгоритм нахождения корней многочлена на основе рассмотрения его аффинных кратных получен в работе Berlekamp, Rumsey, Solomon [1]; см. также монографию Berlekamp [4, ch. 11]. Другой метод нахождения корней многочленов для конечных полей большой характеристики приводится в статье Rabin [1]; см. также Cantor, Zassenhaus [1]. Реализация этих алгоритмов на ЭВМ рассматривается в статье Calmet, Loos [2]. В статьях Fray, Gilmer [1] и Mann [6] изучается теоретический вопрос о разрешимости в радикалах полиномиального уравнения над $\mathbb{F}_q$. В последней из этих работ приводится также выражение для корней неприводимого над полем $\mathbb{F}_q$ многочлена f, степень которого не делится на характеристику этого поля, через корни из единицы над $\mathbb{F}_q$ и многочлены от коэффициентов f. В статье Prešić [1] для многочлена f с корнями в поле $\mathbb{F}_q$ указывается весьма сложная формула, выражающая эти корни через примитивный элемент поля $\mathbb{F}_q$. В статье Rados [4] приводится явное выражение для многочлена НОД $(f(x), x^{p-1}-1)$, где p — простое число.

Особые приемы были развиты для нахождения корней многочленов небольшой степени. Даже задача определения корней квадратного уравнения $x^2 - a \in \mathbb{F}_p[x]$, где p — простое число, становится нетривиальной, если число p велико. Некоторые методы встречаются еще у Гаусса (Gauss [1, ch. 6]); см. также Adleman, Manders, Miller [1], Chang [1], Cipolla [1], [2], Lehmer D. H. [10], Pocklington [1], Schönheim [1], Shanks [2], Smith H. J. S. [1], Tamarkine, Friedmann [1], Tonelli [1], Uspensky, Heaslet [1, ch. 10] и Vandiver [2]. Методы отыскания корней квадратных многочленов над конечными полями характеристики 2 приводятся в работах Berlekamp [4, ch. 6] и Berlekamp, Rumsey, Solomon [1]. О многочленах третьей и четвертой степени см. следующие работы: Arnoux [1, ch. 9], Arwin [1], Cailler [1], Cauchy [3], Cordone [1], Dickson [31], Escott [1], Hirschfeld [5, ch. 1], Mignosi [1], Mirimanoff [1], Oltramare [1], Sansone [1], [2], [3], [4], [5], Scarpis [1], Segre [10], Williams, Zarnke [1], Гребенюк [2], Иванов [1] и Матвеева [1]. О многочленах пятой степени см. работы Arwin [2] и Горбов и Шмидт [1]. Особые методы вычисления корней для многочленов малой степени возникают также в связи с алгоритмами декодирования в алге-

браической теории кодирования; см., например, статьи Chien, Cunningham [1], Polkinghorn [1] и Блох [1]. Точные формулы для корней двучленов над простыми конечными полями можно найти в работах Cipolla [4], Dickson [40, ch. 7], Furquim de Almeida [1], Lindgren [1] и Scorza [1]. Эффективный алгоритм для нахождения корней двучленов над простым конечным полем развит в статье Adleman, Manders, Miller [1]; относительно случая произвольного конечного поля см. Mignotte [5]. В статье Williams H. C. [1] рассматривается случай двучленов простой степени над простым полем $\mathbb{F}_p$.

Условия, при которых все корни многочлена из кольца $\mathbb{F}_q[x]$ принадлежат полю $\mathbb{F}_q$, найдены в работе Feit, Rees [1]. Частный случай, когда число q простое, рассматривался в следующих работах: Schönemann [2], Thouvenot, Châtelet [1] и Шатуновский [1]. В статье Mignotte [4] представлен быстрый алгоритм, с помощью которого можно проверить, все ли корни многочлена $f \in \mathbb{F}_q[x]$ принадлежат полю $\mathbb{F}_q$. В работах Cipolla [5] и Mignosi [2] приводятся формулы для корней многочлена $f \in \mathbb{F}_q[x]$ в случае, когда все эти корни принадлежат полю $\mathbb{F}_q$. Редеи (Rédei [11, ch. 5]) указал многочлены вида $f(x) = x^q + a_k x^k + a_{k-1}x^{k-1} + \ldots + a_0 \in \mathbb{F}_q[x]$, где $k \leqslant (q+1)/2$, у которых все корни принадлежат полю $\mathbb{F}_q$; см. также статью Rédei [7] о более ранних результатах в этом направлении. В статье Gerst, Brillhart [1] изучены условия, при которых многочлен $f \in \mathbb{Z}[x]$ разлагается на различные линейные сомножители по модулю p, для многих простых чисел p; близкий пример приводится в статье Lubelski [3].

За результатами о числе корней многочлена в заданном конечном поле мы отсылаем читателя к § 1 гл. 6 и комментариям к этому параграфу.

[Григорьев [1*], Ленстра (Lenstra [2*]) и Ван дер Газен и Калтофен (van der Gathen, Kaltofen [1*]) построили алгоритмы разложения на множители многочленов степени n от r переменных над произвольным конечным полем $\mathbb{F}_q$. При этом в работах первых двух авторов строится детерминированный алгоритм, имеющий сложность, ограниченную многочленом от n^r и q, а в последней работе — вероятностный алгоритм, имеющий сложность, ограниченную многочленом от n^r и $\ln q$.

По тематике четвертой главы имеются также следующие работы: Calmet, Loos [1*], Lenstra [1*], Smeets [1*], Кюрегян [1*] и Мурзаев [2*]. — *Перев.*]

Упражнения

4.1. Разложить многочлен $x^{12} + x^7 + x^5 + x^4 + x^3 + x^2 + 1$ над полем $\mathbb{F}_2$ с помощью алгоритма Берлекэмпа.

4.2. Разложить многочлен $x^7 + x^6 + x^5 - x^3 + x^2 - x - 1$ над полем $\mathbb{F}_3$ с помощью алгоритма Берлекэмпа.

4.3. Пусть $\mathbb{F}_4 = \mathbb{F}_2(\theta)$; разложить многочлен $x^5 + \theta x^4 + x^3 + (1+\theta)x + \theta$ над полем $\mathbb{F}_4$ с помощью алгоритма Берлекэмпа.

4.4. Применить алгоритм Берлекэмпа для доказательства неприводимости многочлена $x^6 - x^3 - x - 1$ в кольце $\mathbb{F}_3[x]$.

4.5. Применить алгоритм Берлекэмпа для определения числа различных нормированных неприводимых делителей многочлена $x^4 + 1$ в кольце $\mathbb{F}_p[x]$ для всех нечетных простых чисел p.

4.6. Использовать многочлены T_i из теоремы 4.3 для разложения многочлена $x^5 + x^4 + 1$ над полем $\mathbb{F}_2$.

4.7. Найти поле разложения многочлена $x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$ над полем $\mathbb{F}_2$.

4.8. Найти поле разложения многочлена $x^6 - x^4 - x^2 - x + 1$ над полем $\mathbb{F}_3$.

4.9. Использовать многочлены R_i из теоремы 4.5 для разложения многочлена из упр. 4.1 над полем $\mathbb{F}_2$.

4.10. Найти каноническое разложение многочлена $x^8 + x^6 + x^4 + x^3 + 1$ в кольце $\mathbb{F}_2[x]$, используя многочлены R_i.

4.11. Найти каноническое разложение кругового многочлена $Q_{31}(x)$ в кольце $\mathbb{F}_2[x]$.

4.12. Разложить многочлен $f(x) = x^8 + x^3 + 1$ над полем $\mathbb{F}_2$ и вычислить ord $(f(x))$.

4.13. Разложить многочлен $f(x) = x^9 + x^8 + x^7 + x^4 + x^3 + x + 1$ над полем $\mathbb{F}_2$ и вычислить ord $(f(x))$.

4.14. Дать подробное доказательство того, что если f — ненулевой многочлен над некоторым полем и $d = \text{НОД}(f, f')$, то многочлен f/d не имеет кратных неприводимых сомножителей. (*Замечание.* Считать ненулевые постоянные многочлены многочленами без кратных сомножителей.)

4.15. Пусть f — нормированный многочлен положительной степени с целыми коэффициентами, не имеющий кратных сомножителей. Доказать, что существует лишь конечное число простых чисел p, таких, что f, рассматриваемый как многочлен над полем $\mathbb{F}_p$, имеет кратные сомножители.

4.16. Определить число нормированных многочленов из $\mathbb{F}_q[x]$ степени $n \geqslant 1$, не имеющих кратных неприводимых сомножителей.

4.17. Пусть f — нормированный многочлен над полем $\mathbb{F}_q$, и пусть $g_1, \ldots, g_r$ — ненулевые многочлены над $\mathbb{F}_q$, которые попарно взаимно просты. Доказать, что если f делит произведение $g_1 \ldots g_r$, то $f = \prod_{i=1}^{r} \text{НОД}(f, g_i)$.

4.18. Используя алгоритм Берлекэмпа, доказать следующий частный случай теоремы 3.75: если $a \in \mathbb{F}_q^*$ и t — простой делитель числа $q-1$, то двучлен $x^t - a$ неприводим в кольце $\mathbb{F}_q[x]$ тогда и только тогда, когда $a^{(q-1)/t} \neq 1$.

4.19. Пусть f — неприводимый многочлен степени n из $\mathbb{F}_q[x]$ и $n \times n$-матрица $B = (b_{ij})$ определена условием (4.4). Доказать, что характеристический многочлен $\det(xI - B)$ матрицы B равен $x^n - 1$.

4.20. Пусть многочлен f равен произведению k различных нормированных неприводимых многочленов $f_1, \ldots, f_k$ из $\mathbb{F}_q[x]$ степеней $n_1, \ldots, n_k$ соответственно. Положим $\deg(f) = n = n_1 + \ldots + n_k$ и определим $n \times n$-матрицу $B = (b_{ij})$ условием (4.4). Доказать, что характеристический многочлен $\det(xI - B)$ матрицы B равен произведению $\left(x^{n_1} - 1\right) \ldots \left(x^{n_k} - 1\right)$.

4.21. В обозначениях теоремы 4.3 доказать, что многочлены T_i не отделяют тех неприводимых сомножителей f_i многочлена f, для которых число N/n_j делится на характеристику поля $\mathbb{F}_q$.

4.22. Пусть $f \in \mathbb{F}_q[x]$ — нормированный многочлен степени $n \geqslant 1$. Определим многочлен от двух переменных $h \in \mathbb{F}_q[x, y]$ равенством

$$h(x, y) = (y - x)\left(y - x^q\right)\left(y - x^{q^2}\right) \ldots \left(y - x^{q^{n-1}}\right) - f(y)$$

и представим его в виде

$$h(x, y) = s_{n-1}(x) y^{n-1} + \cdots + s_1(x) y + s_0(x).$$

Доказать, что многочлен f тогда и только тогда неприводим над полем $\mathbb{F}_q$, когда f делит каждый из многочленов s_j, $0 \leqslant j \leqslant n-1$.

4.23. Применить критерий из предыдущего упражнения для доказательства приводимости многочлена $x^7 + x^6 + x^3 + x^2 + 1$ над полем $\mathbb{F}_2$.

4.24. Доказать, что квадратный многочлен $f(x) = x^2 + bx + c$ неприводим над полем $\mathbb{F}_q$ тогда и только тогда, когда он делит трехчлен $x^q + x + b$.

4.25. Пусть f — неприводимый многочлен степени m из $\mathbb{F}_q[x]$ и λ — его корень в поле $\mathbb{F}_{q^m}$. Доказать, что если g и h — ненулевые многочлены из $\mathbb{F}_q[x]$, то многочлен $h(x)^m f(g(x)/h(x))$ неприводим в $\mathbb{F}_q[x]$ тогда и только тогда, когда многочлен $g(x) - \lambda h(x)$ неприводим в кольце $\mathbb{F}_{q^m}[x]$.

4.26. Применить метод, использованный в примере 4.7, для разложения многочлена $x^4 + 3x^3 + 4x^2 + 2x - 1$ над полем $\mathbb{F}_{13}$.

4.27. Применить метод, использованный в примере 4.7, для разложения многочлена $x^3 - 6x^2 - 8x - 8$ над полем $\mathbb{F}_{19}$.

4.28. Применить алгоритм Цассенхауза для разложения многочлена $x^4 + 3x^3 + 4x^2 + 2x - 1$ над полем $\mathbb{F}_{13}$.

4.29. Применить алгоритм Цассенхауза для разложения многочлена $x^3 - 6x^2 - 8x - 8$ над полем $\mathbb{F}_{19}$.

4.30. Применить алгоритм Цассенхауза для разложения многочлена $x^5 + 3x^4 + 2x^3 - 6x^2 + 5$ над полем $\mathbb{F}_{17}$.

4.31. Разложить многочлен $x^4 - 7x^3 + 4x^2 + 2x + 4$ над полем $\mathbb{F}_{17}$.

4.32. Разложить многочлен $x^4 - 3x^3 + 4x^2 - 6x - 8$ над полем $\mathbb{F}_{19}$.

4.33. Дать подробное доказательство того, что эквивалентность квадратных матриц из многочленов, введенная в определении 4.11, рефлексивна, симметрична и транзитивна.

4.34. Применить метод, использованный в примере 4.14, для разложения многочлена $x^3 - 6x^2 - 8x - 8$ над полем $\mathbb{F}_{19}$.

4.35. Применить метод, использованный в примере 4.14, для разложения многочлена $x^5 + 3x^4 + 2x^3 - 6x^2 + 5$ над полем $\mathbb{F}_{17}$.

4.36. Применить метод, использованный в примере 4.14, для получения частичного разложения многочлена $x^7 - 2x^6 - 4x^4 + 3x^3 - 5x^2 + 3x + 5$ над полем $\mathbb{F}_{11}$ и завершить разложение другим методом.

4.37. Найти корни многочлена $f(x) = x^5 - x^4 + 2x^3 + x^2 - x - 2 \in \mathbb{F}_3[x]$, содержащиеся в поле $\mathbb{F}_3$.

4.38. Найти корни многочлена $f(x) = x^5 + 6x^4 + 2x^3 - 6x^2 - 5x + 5 \in \mathbb{F}_{13}[x]$, содержащиеся в поле $\mathbb{F}_{13}$.

4.39. Доказать, что все корни многочлена $f(x) = x^3 + 8x^2 + 6x - 7 \in \mathbb{F}_{19}[x]$ содержатся в поле $\mathbb{F}_{19}$, и найти их.

4.40. Пусть $\mathbb{F}_{32} = \mathbb{F}_2(\beta)$, где β — корень неприводимого многочлена $x^5 + x^2 + 1$ над полем $\mathbb{F}_2$. Доказать, что все корни многочлена $f(x) = x^3 + (\beta^4 + \beta^3 + 1)x^2 + \beta^2 x + (\beta^4 + \beta^3 + \beta + 1) \in \mathbb{F}_{32}[x]$ содержатся в поле $\mathbb{F}_{32}$, и найти их.

4.41. Пусть $\mathbb{F}_{27} = \mathbb{F}_3(\beta)$, где β — корень неприводимого многочлена $x^3 - x + 1$ над полем $\mathbb{F}_3$. Доказать, что все корни многочлена $f(x) = x^3 + x^2 - (\beta^2 - \beta + 1)x + (\beta^2 - 1) \in \mathbb{F}_{27}[x]$ лежат в поле $\mathbb{F}_{27}$, и найти их.

4.42. Пусть $\mathbb{F}_{169} = \mathbb{F}_{13}(\beta)$, где β — корень неприводимого многочлена $x^2 - x - 1$ над полем $\mathbb{F}_{13}$. Найти корни многочлена $f(x) = x^2 + (3\beta + 1)x + (\beta + 5) \in \mathbb{F}_{169}[x]$, содержащиеся в поле $\mathbb{F}_{169}$.

4.43. Пусть $f \in \mathbb{F}_p[x]$ и $b \in \mathbb{F}_p$, где p — простое нечетное число. Доказать, что если $f(x - b)$ — квадратный многочлен с постоянным членом $c \neq 0$, то разложение (4.22) является нетривиальным в том и только том случае, если c не является квадратом какого-нибудь элемента из поля $\mathbb{F}_p$.

4.44. Пусть β — образующий элемент поля $F = \mathbb{F}_{2^m}$ над $\mathbb{F}_2$. Доказать следующие утверждения:

(a) Существует число k, $0 \leqslant k \leqslant m-1$, такое, что $\mathrm{Tr}_F(\beta^k) = 1$.

(b) Для каждого $i = 0, 1, \ldots, m-1$ существует элемент $\alpha_i \in F$, такой, что

$$\alpha_i^2 + \alpha_i = \begin{cases} \beta^i, & \text{если } \mathrm{Tr}_F(\beta^i) = 0, \\ \beta^i + \beta^k, & \text{если } \mathrm{Tr}_F(\beta^i) = 1, \end{cases}$$

где число k определено условием (a).

(c) Если $\gamma = \sum_{i=0}^{m-1} c_i \beta^i$, $c_i \in \mathbb{F}_2$, и $\mathrm{Tr}_F(\gamma) = 0$, то корнями многочлена $x^2 + x + \gamma$ являются элементы $\sum_{i=0}^{m-1} c_i \alpha_i$ и $1 + \sum_{i=0}^{m-1} c_i \alpha_i$.

Глава 5

Тригонометрические суммы

В теории чисел тригонометрические (или экспоненциальные) суммы являются важным инструментом для решения различных проблем, связанных с целыми числами, которые часто не поддаются решению другими методами. Такие суммы можно рассматривать и в теории конечных полей, причем и здесь они оказываются весьма полезными — например, при исследовании вопроса о числе решений уравнений над конечными полями (см. гл. 6), а также в различных приложениях конечных полей.

При использовании тригонометрических сумм в теории конечных полей главную роль играет некоторая специальная группа гомоморфизмов, называемых характерами. Нужно различать два типа характеров — аддитивные и мультипликативные — в зависимости от того, с аддитивной или мультипликативной группами данного конечного поля связаны упомянутые гомоморфизмы. Тригонометрические суммы образуются из значений одного или нескольких характеров, при этом возможно сочетание их с некоторыми функциональными величинами. Когда суммируются значения какого-то одного характера, то мы будем говорить о *сумме значений характера*.

В первом параграфе мы получим основные соотношения для характеров, сначала рассматривая произвольную конечную абелеву группу, а затем переходя к конечным полям. В § 2 будут изучаться суммы Гаусса, бесспорно являющиеся самым важным типом тригонометрических сумм для конечных полей, поскольку они связывают аддитивную и мультипликативную структуры конечного поля. Они возникают также во многих вопросах алгебры и теории чисел. С суммами Гаусса тесно связаны суммы Якоби, изучаемые в третьем параграфе. Эти суммы особенно важны для приложений к уравнениям над конечными полями (см. гл. 6).

Суммы значений характеров с полиномиальными аргументами (иногда называемые суммами Вейля) изучаются в § 4. Исследование проводится сугубо элементарными средствами, т. е. без привлечения алгебраической геометрии. Однако этот «элементарный» подход доведен до достаточной степени совершенства, так что оказывается возможным получить все основные оценки для сумм Вейля. Рассмотрение указанных сумм значений характеров идет

в тесной связи с детальным изучением некоторых типов уравнений над конечными полями. Поэтому некоторые возникающие «свободные концы» удастся связать лишь в гл. 6, где будут изучены соответствующие уравнения.

В § 5 мы рассмотрим суммы значений характеров специального вида, представляющие интерес для теории чисел, а именно суммы Клостермана и суммы Якобсталя. В связи с одним результатом о суммах значений квадратичных характеров в этом же параграфе рассматриваются разложения в непрерывные дроби рациональных функций над конечными полями.

§ 1. Характеры

Пусть G — произвольная конечная мультипликативная абелева группа порядка $|G|$ с единичным элементом 1_G. *Характером* χ группы G называется гомоморфизм из G в мультипликативную группу U комплексных чисел, по модулю равных 1, т. е. такое отображение χ: $G \to U$, что $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ для всех $g_1, g_2 \in G$. Поскольку $\chi(1_G) = \chi(1_G)\chi(1_G)$, то должно быть $\chi(1_G) = 1$. Далее, для каждого элемента $g \in G$

$$(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1,$$

так что значениями характера χ являются корни степени $|G|$ из единицы. Заметим также, что $\chi(g)\overline{\chi(g^{-1})} = \chi(gg^{-1}) = \chi(1_G) = 1$, так что $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$ для каждого элемента $g \in G$ (здесь черта означает комплексное сопряжение).

Среди характеров группы G имеется *тривиальный* характер χ_0, определяемый условием $\chi_0(g) = 1$ для всех $g \in G$; все остальные характеры группы G называются *нетривиальными*. Каждому характеру χ группы G соответствует *сопряженный* характер $\bar{\chi}$, определяемый условием $\bar{\chi}(g) = \overline{\chi(g)}$ для всех $g \in G$. Для данного конечного множества характеров $\chi_1, \ldots, \chi_n$ группы G можно образовать их *произведение* $\chi_1 \ldots \chi_n$, полагая $(\chi_1 \ldots \chi_n)(g) = \chi_1(g) \ldots \chi_n(g)$ для всех $g \in G$. Если $\chi_1 = \ldots = \chi_n = \chi$, то произведение $\chi_1 \ldots \chi_n$ будем обозначать χ^n и называть n-й *степенью* характера χ. Очевидно, что множество $\hat{G}$ всех характеров группы G образует абелеву группу относительно введенного умножения характеров. А так как значениями характеров могут быть лишь корни степени $|G|$ из единицы, то группа $\hat{G}$ конечна.

Прежде чем перейти к установлению основных свойств характеров произвольной конечной абелевой группы G, рассмотрим один важный частный случай, когда G — конечная циклическая группа.

5.1. Пример. Пусть G — конечная циклическая группа порядка n, и пусть g — ее образующий элемент. Легко убедиться,

что для произвольного фиксированного целого числа j, $0 \leqslant j \leqslant n-1$, функция

$$\chi_j(g^k) = e^{2\pi ijk/n} = \cos 2\pi jk/n + i \sin 2\pi jk/n, \quad k = 0, 1, \ldots, n-1,$$

где i — мнимая единица, определяет некоторый характер группы G. С другой стороны, если χ — произвольный характер группы G, то $\chi(g)$ является некоторым корнем n-й степени из единицы, скажем $\chi(g) = e^{2\pi ij/n}$ для некоторого j, $0 \leqslant j \leqslant n-1$, и, значит, $\chi = \chi_j$. Поэтому группа характеров $\hat{G}$ циклической группы $G = \langle g \rangle$ состоит из характеров $\chi_0, \chi_1, \ldots, \chi_{n-1}$. □

5.2. Теорема. *Пусть H — некоторая подгруппа конечной абелевой группы G, и пусть ψ — характер группы H. Тогда ψ можно продолжить до некоторого характера группы G, т. е. существует такой характер χ группы G, что $\chi(h) = \psi(h)$ для всех $h \in H$.*

Доказательство. Можно считать H собственной подгруппой группы G. Выберем такой элемент $a \in G$, что $a \notin H$, и пусть H_1 — подгруппа группы G, порожденная множеством $H \cup \{a\}$. Пусть m — наименьшее натуральное число, для которого $a^m \in H$. Тогда каждый элемент $g \in H_1$ может быть однозначно представлен в виде $g = a^j h$, где $0 \leqslant j < m$ и $h \in H$. Определим на группе H_1 функцию ψ_1 условием $\psi_1(g) = \omega^j \psi(h)$, где ω — фиксированное комплексное число, удовлетворяющее равенству $\omega^m = \psi(a^m)$. Покажем, что функция ψ_1 является характером группы H_1. Пусть $g_1 = a^k h_1$, где $0 \leqslant k < m$, $h_1 \in H$, т. е. g_1 — еще один элемент группы H_1. Если $j + k < m$, то $\psi_1(gg_1) = \omega^{j+k}\psi(hh_1) = \psi_1(g)\psi_1(g_1)$. Если же $j + k \geqslant m$, то $gg_1 = a^{j+k-m}(a^m hh_1)$, так что

$$\psi_1(gg_1) = \omega^{j+k-m}\psi(a^m hh_1) = \omega^{j+k-m}\psi(a^m)\psi(hh_1) = \omega^{j+k}\psi(hh_1) = \psi_1(g)\psi_1(g_1).$$

Очевидно, что $\psi_1(h) = \psi(h)$ для всех $h \in H$. Поэтому если $H_1 = G$, то теорема доказана. В противном же случае мы продолжим эту процедуру, пока через конечное число шагов не получим продолжение характера ψ до группы G. □

5.3. Следствие. *Для любых двух различных элементов $g_1, g_2 \in G$ существует характер χ группы G, такой, что $\chi(g_1) \neq \chi(g_2)$.*

Доказательство. Достаточно показать, что для элемента $h = g_1 g_2^{-1} \neq 1_G$ существует характер χ группы G, такой, что $\chi(h) \neq 1$. Но это вытекает из примера 5.1 и теоремы 5.2, если через H обозначить циклическую подгруппу группы G, порожденную элементом h.

5.4. Теорема. *Если* χ *— нетривиальный характер конечной абелевой группы* G, *то*

$$\sum_{g \in G} \chi(g) = 0. \tag{5.1}$$

Если $g \in G$, *причем* $g \neq 1_G$, *то*

$$\sum_{\chi \in G^\wedge} \chi(g) = 0. \tag{5.2}$$

Доказательство. Поскольку χ — нетривиальный характер группы G, то существует элемент $h \in G$, такой, что $\chi(h) \neq 1$. Поэтому

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g),$$

так как если элемент g пробегает группу G, то и произведение hg пробегает группу G. Таким образом, мы получаем равенство

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0,$$

откуда следует (5.1).

Что касается второй части, то заметим, что функция $\hat{g}$, определенная равенством $\hat{g}(\chi) = \chi(g)$ для всех $\chi \in G^\wedge$, является характером конечной абелевой группы $G^\wedge$. Этот характер нетривиален, так как ввиду следствия 5.3 существует характер $\chi \in G^\wedge$, такой, что $\chi(g) \neq \chi(1_G) = 1$. Поэтому из равенства (5.1), примененного к группе $G^\wedge$, получаем

$$\sum_{\chi \in G^\wedge} \chi(g) = \sum_{\chi \in G^\wedge} \hat{g}(\chi) = 0. \qquad \square$$

5.5. Теорема. *Число характеров конечной абелевой группы* G *равно* $|G|$.

Доказательство. Это следует из того, что

$$|G^\wedge| = \sum_{g \in G} \sum_{\chi \in G^\wedge} \chi(g) = \sum_{\chi \in G^\wedge} \sum_{g \in G} \chi(g) = |G|,$$

где в первом равенстве использовано (5.2) и тот факт, что $\chi(1_G) = 1$, а в последнем — (5.1) и тот факт, что $\chi_0(g) = 1$. $\square$

Утверждения теорем 5.4 и 5.5 можно объединить в следующие *соотношения ортогональности для характеров*. Пусть χ и ψ — характеры группы G. Тогда

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)} = \begin{cases} 0, & \text{если } \chi \neq \psi, \\ 1, & \text{если } \chi = \psi. \end{cases} \tag{5.3}$$

Первая часть получается применением (5.1) к характеру $\chi\bar{\psi}$, вторая часть тривиальна.

Кроме того, если g и h — элементы группы G, то

$$\frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(g)\overline{\chi(h)}=\begin{cases}0, & \text{если } g\neq h,\\ 1, & \text{если } g=h.\end{cases} \tag{5.4}$$

Здесь первая часть получается применением (5.2) к элементу gh^{-1}, а вторая часть вытекает из теоремы 5.5.

Теорию характеров часто применяют, чтобы получить выражение для числа решений какого-либо уравнения в конечной абелевой группе G. Так, пусть f — произвольное отображение декартовой степени $G^n = G\times\ldots\times G$ (n сомножителей) группы G в G. Тогда на основании (5.4) для фиксированного элемента $h\in G$ число $N(h)$ n-наборов $(g_1, \ldots, g_n)\in G^n$, для которых $f(g_1, \ldots, g_n) = h$, определяется равенством

$$N(h)=\frac{1}{|G|}\sum_{g_1\in G}\ldots\sum_{g_n\in G}\sum_{\chi\in G^\wedge}\chi(f(g_1,\ \ldots,\ g_n))\overline{\chi(h)}. \tag{5.5}$$

Характер χ группы G может быть нетривиальным на группе G, но *аннулировать* при этом какую-либо подгруппу H группы G (в том смысле, что $\chi(h) = 1$ для всех $h\in H$). Множество характеров группы G, аннулирующих данную подгруппу H, называется *аннулятором* подгруппы H в группе характеров $G^\wedge$ группы G.

5.6. Теорема. *Пусть H — подгруппа конечной абелевой группы G. Тогда аннулятор этой подгруппы в группе характеров $G^\wedge$ является подгруппой группы $G^\wedge$ порядка $|G|/|H|$.*

Доказательство. Обозначим аннулятор подгруппы H в группе характеров $G^\wedge$ через A. Из определения аннулятора сразу следует, что A — подгруппа группы $G^\wedge$. Пусть $\chi\in A$; тогда легко видеть, что равенство $\mu(gH) = \chi(g)$ для $g\in G$ задает характер μ факторгруппы G/H. Обратно, если μ — некоторый характер группы G/H, то легко видеть, что равенство $\chi(g) = \mu(gH)$ для $g\in G$ определяет некоторый характер χ группы G, аннулирующий подгруппу H. При этом различные элементы из A соответствуют различным характерам факторгруппы G/H. Поэтому между элементами подгруппы A и элементами группы характеров $(G/H)^\wedge$ факторгруппы G/H существует взаимно однозначное соответствие, так что порядок подгруппы A группы $G^\wedge$ равен порядку группы $(G/H)^\wedge$, который равен $|G/H| = |G|/|H|$ согласно теореме 5.5. □

Переходя к конечному полю $\mathbb{F}_q$, сразу заметим, что в нем имеется две очень важные конечные абелевы группы, а именно аддитивная и мультипликативная группы этого поля. Поэтому

необходимо проводить четкое различие между характерами, соответствующими этим двум группам. В обоих случаях мы приведем явные формулы для характеров.

Рассмотрим сначала *аддитивную группу* поля $\mathbb{F}_q$. Пусть p — характеристика конечного поля $\mathbb{F}_q$; тогда простым полем, содержащимся в $\mathbb{F}_q$, является $\mathbb{F}_p$, которое мы отождествляем с факторкольцом $\mathbb{Z}/(p)$. Пусть $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ — функция абсолютного следа из $\mathbb{F}_q$ в $\mathbb{F}_p$ (см. определение 2.22). Тогда функция χ_1, определенная равенством

$$\chi_1(c) = e^{2\pi i \operatorname{Tr}(c)/p} \quad \text{для всех} \quad c \in \mathbb{F}_q, \tag{5.6}$$

является характером аддитивной группы поля $\mathbb{F}_q$, так как для любых $c_1, c_2 \in \mathbb{F}_q$ мы имеем $\mathrm{Tr}(c_1 + c_2) = \mathrm{Tr}(c_1) + \mathrm{Tr}(c_2)$, так что $\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2)$. Вместо того чтобы говорить «характер аддитивной группы поля $\mathbb{F}_q$», будем в дальнейшем употреблять термин *аддитивный характер поля* $\mathbb{F}_q$. При этом характер, определенный равенством (5.6), мы будем называть *каноническим аддитивным характером поля* $\mathbb{F}_q$. Любой аддитивный характер поля $\mathbb{F}_q$ можно выразить через канонический характер χ_1.

5.7. Теорема. *Пусть $\mathbb{F}_q$ — конечное поле и $b \in \mathbb{F}_q$. Тогда функция χ_b, определенная равенством $\chi_b(c) = \chi_1(bc)$ для всех $c \in \mathbb{F}_q$, является аддитивным характером поля $\mathbb{F}_q$. При этом каждый аддитивный характер поля $\mathbb{F}_q$ совпадает с характером χ_b для некоторого $b \in \mathbb{F}_q$.*

Доказательство. Для $c_1, c_2 \in \mathbb{F}_q$

$$\chi_b(c_1 + c_2) = \chi_1(bc_1 + bc_2) = \chi_1(bc_1)\chi_1(bc_2) = \chi_b(c_1)\chi_b(c_2),$$

и первая часть установлена.

Поскольку, согласно теореме 2.23 (iii), функция Tr отображает поле $\mathbb{F}_q$ на $\mathbb{F}_p$, то χ_1 — нетривиальный характер. Поэтому для $a, b \in \mathbb{F}_q$, $a \neq b$, найдется элемент $c \in \mathbb{F}_q$, такой, что

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a-b)c) \neq 1,$$

так что χ_a и χ_b — различные характеры. Поэтому когда элемент b пробегает поле $\mathbb{F}_q$, мы получаем q различных аддитивных характеров χ_b. С другой стороны, согласно теореме 5.5, существует ровно q аддитивных характеров поля $\mathbb{F}_q$, так что этим списком исчерпываются все аддитивные характеры поля $\mathbb{F}_q$. □

Полагая $b = 0$ в теореме 5.7, мы получаем тривиальный характер χ_0, обладающий свойством $\chi_0(c) = 1$ для всех $c \in \mathbb{F}_q$.

Пусть E — конечное расширение поля $\mathbb{F}_q$, χ_1 — канонический аддитивный характер поля $\mathbb{F}_q$ и μ_1 — канонический аддитивный характер поля E, определенный по аналогии с (5.6), где функция

Tr, естественно, заменяется функцией абсолютного следа Tr_E из E в $\mathbb{F}_p$. Нетрудно видеть, что характеры χ_1 и μ_1 связаны следующим равенством:

$$\chi_1(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)) = \mu_1(\beta) \quad \text{для всех} \quad \beta \in E, \tag{5.7}$$

где $\mathrm{Tr}_{E/\mathbb{F}_q}$ — функция следа из E в $\mathbb{F}_q$. Это вытекает из транзитивности функции следа (см. теорему 2.26):

$$\mathrm{Tr}_E(\beta) = \mathrm{Tr}(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)) \quad \text{для всех} \quad \beta \in E.$$

Характеры *мультипликативной группы* $\mathbb{F}_q^*$ поля $\mathbb{F}_q$ называются *мультипликативными характерами поля* $\mathbb{F}_q$. Поскольку $\mathbb{F}_q^*$ — циклическая группа порядка $q-1$ (см. теорему 2.8), то ее характеры легко найти.

5.8. Теорема. *Пусть g — некоторый фиксированный примитивный элемент поля $\mathbb{F}_q$. Тогда для каждого j, $0 \leqslant j \leqslant q-2$, функция ψ_j, определенная равенством*

$$\psi_j(g^k) = e^{2\pi i jk/(q-1)} \quad \text{для всех} \quad k,\ 0 \leqslant k \leqslant q-2,$$

определяет некоторый мультипликативный характер поля $\mathbb{F}_q$. При этом каждый мультипликативный характер поля $\mathbb{F}_q$ совпадает с характером ψ_j для некоторого j, $0 \leqslant j \leqslant q-2$.

Доказательство. Утверждение теоремы сразу вытекает из примера 5.1. □

Независимо от выбора примитивного элемента g в теореме 5.8 характер ψ_0 всегда является тривиальным мультипликативным характером, т. е. обладает свойством $\psi_0(c) = 1$ для всех $c \in \mathbb{F}_q^*$.

5.9. Следствие. *Группа мультипликативных характеров конечного поля $\mathbb{F}_q$ является циклической группой порядка $q-1$ с единичным элементом ψ_0.*

Доказательство. Каждый характер ψ_j из теоремы 5.8, для которого индекс j взаимно прост с числом $q-1$, является образующим элементом группы $(\mathbb{F}_q^*)\hat{}$ мультипликативных характеров поля $\mathbb{F}_q$. □

5.10. Пример. Пусть $\mathbb{F}_q$ — поле нечетной характеристики, и пусть на его мультипликативной группе $\mathbb{F}_q^*$ задана действительнозначная функция η, такая, что $\eta(c) = 1$ для элементов c, являющихся квадратами некоторых элементов группы $\mathbb{F}_q^*$, и $\eta(c) = -1$ для всех остальных элементов $c \in \mathbb{F}_q^*$. Легко проверить, что η является мультипликативным характером поля $\mathbb{F}_q$. Он совпадает с характером ψ_j из теоремы 5.8 при $j = (q-1)/2$. Характер η аннулирует подгруппу группы $\mathbb{F}_q^*$, состоящую из квадратов эле-

ментов этой группы, и, согласно теореме 5.6, он является единственным нетривиальным характером группы $\mathbb{F}_q^*$, обладающим таким свойством. Этот однозначно определенный характер η называется *квадратичным характером* поля $\mathbb{F}_q$. Если q — простое нечетное число, то с помощью квадратичного характера можно определить *символ Лежандра* $\left(\frac{c}{q}\right)$ из элементарной теории чисел, полагая $\left(\frac{c}{q}\right) = \eta(c)$, где $c \in \mathbb{F}_q^*$. □

Соотношения ортогональности (5.3) и (5.4), примененные к аддитивным или мультипликативным характерам поля $\mathbb{F}_q$, приводят к некоторым фундаментальным тождествам. Рассмотрим сначала случай аддитивных характеров, для которых мы будем использовать те же обозначения, что и в теореме 5.7. Тогда для аддитивных характеров χ_a и χ_b мы имеем

$$\sum_{c \in \mathbb{F}_q} \chi_a(c)\,\overline{\chi_b(c)} = \begin{cases} 0, & \text{если } a \neq b, \\ q, & \text{если } a = b. \end{cases} \tag{5.8}$$

В частности,

$$\sum_{c \in \mathbb{F}_q} \chi_a(c) = 0, \quad \text{если } a \neq 0. \tag{5.9}$$

Далее, для элементов $c,\ d \in \mathbb{F}_q$

$$\sum_{b \in \mathbb{F}_q} \chi_b(c)\,\overline{\chi_b(d)} = \begin{cases} 0, & \text{если } c \neq d, \\ q, & \text{если } c = d. \end{cases} \tag{5.10}$$

Аналогично для мультипликативных характеров ψ и τ поля $\mathbb{F}_q$ имеет место соотношение

$$\sum_{c \in \mathbb{F}_q^*} \psi(c)\,\overline{\tau(c)} = \begin{cases} 0, & \text{если } \psi \neq \tau, \\ q-1, & \text{если } \psi = \tau. \end{cases} \tag{5.11}$$

В частности,

$$\sum_{c \in \mathbb{F}_q^*} \psi(c) = 0, \quad \text{если } \psi \neq \psi_0. \tag{5.12}$$

Если $c,\ d \in \mathbb{F}_q^*$, то

$$\sum_{\psi} \psi(c)\,\overline{\psi(d)} = \begin{cases} 0, & \text{если } c \neq d, \\ q-1, & \text{если } c = d, \end{cases} \tag{5.13}$$

где сумма берется по всем мультипликативным характерам ψ поля $\mathbb{F}_q$.

§ 2. Суммы Гаусса

Пусть ψ — мультипликативный, а χ — аддитивный характеры поля $\mathbb{F}_q$. Тогда *сумма Гаусса* [1]) для поля $\mathbb{F}_q$ определяется следующим равенством:

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c).$$

Абсолютная величина суммы Гаусса $G(\psi, \chi)$, очевидно, не превышает числа $q-1$, но, как правило, гораздо меньше, что вытекает из следующей теоремы. Снова через ψ_0 будем обозначать тривиальный мультипликативный характер, а через χ_0 — тривиальный аддитивный характер поля $\mathbb{F}_q$.

5.11. Теорема. *Пусть ψ — некоторый мультипликативный, а χ — аддитивный характеры поля $\mathbb{F}_q$. Тогда сумма Гаусса $G(\psi, \chi)$ удовлетворяет следующему соотношению:*

$$G(\psi, \chi) = \begin{cases} q-1, & \text{если } \psi = \psi_0, \ \chi = \chi_0, \\ -1, & \text{если } \psi = \psi_0, \ \chi \neq \chi_0, \\ 0, & \text{если } \psi \neq \psi_0, \ \chi = \chi_0. \end{cases} \tag{5.14}$$

Если же $\psi \neq \psi_0$ и $\chi \neq \chi_0$, то

$$|G(\psi, \chi)| = q^{1/2}. \tag{5.15}$$

Доказательство. Первый случай из (5.14) тривиален, третий сразу вытекает из (5.12), а во втором случае, согласно (5.9),

$$G(\psi_0, \chi) = \sum_{c \in \mathbb{F}_q^*} \chi(c) = \sum_{c \in \mathbb{F}_q} \chi(c) - \chi(0) = -1.$$

Если же $\psi \neq \psi_0$ и $\chi \neq \chi_0$, то

$$\begin{aligned} |G(\psi, \chi)|^2 &= \overline{G(\psi, \chi)}\, G(\psi, \chi) = \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \overline{\psi(c)}\,\overline{\chi(c)}\,\psi(c_1)\chi(c_1) = \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \psi(c^{-1}c_1)\chi(c_1 - c). \end{aligned}$$

[1]) Суммы подобного вида иазывают *тригонометрическими* (или *экспоненциальными*), поскольку входящие в иих характеры являются экспонеицииальиыми (или тригонометрическими) функциями, как это видно из примера 5.1, равеиства (5.6) и теорем 5.7 и 5.8. — *Прим. перев.*

Введем новую переменную d, полагая во внутренней сумме $c^{-1}c_1 = d$; тогда

$$|G(\psi, \chi)|^2 = \sum_{c\in\mathbb{F}_q^*} \sum_{d\in\mathbb{F}_q^*} \psi(d)\chi(c(d-1)) =$$
$$= \sum_{d\in\mathbb{F}_q^*} \psi(d)\Big(\sum_{c\in\mathbb{F}_q} \chi(c(d-1)) - \chi(0)\Big) =$$
$$= \sum_{d\in\mathbb{F}_q^*} \psi(d) \sum_{c\in\mathbb{F}_q} \chi(c(d-1)),$$

где в последнем равенстве использовано соотношение (5.12). Внутренняя сумма ввиду (5.9) принимает значение q при $d = 1$ и значение 0 при $d \neq 1$. Поэтому $|G(\psi, \chi)|^2 = \psi(1)\, q = q$, и тем самым равенство (5.15) установлено. □

Изучая поведение сумм Гаусса при различных преобразованиях аддитивных или мультипликативных характеров, можно получнть некоторые полезные тождества.

5.12. Теорема. *Суммы Гаусса для конечного поля $\mathbb{F}_q$ удовлетворяют следующим условиям:*

(i) $G(\psi, \chi_{ab}) = \overline{\psi(a)}\, G(\psi, \chi_b)$ *для* $a\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q$;

(ii) $G(\psi, \bar{\chi}) = \psi(-1)\, \overline{G(\psi, \chi)}$;

(iii) $G(\bar{\psi}, \chi) = \psi(-1)\, \overline{G(\psi, \chi)}$;

(iv) $G(\psi, \chi)\, G(\bar{\psi}, \chi) = \psi(-1)\, q$ *для* $\psi \neq \psi_0$, $\chi \neq \chi_0$;

(v) $G(\psi^p, \chi_b) = G(\psi, \chi_{\sigma(b)})$ *для* $b\in\mathbb{F}_q$, *где* p *— характеристика поля* $\mathbb{F}_q$ *и* $\sigma(b) = b^p$.

Доказательство. (i) Согласно определению из теоремы 5.7, $\chi_{ab}(c) = \chi_1(abc) = \chi_b(ac)$ для любого $c \in \mathbb{F}_q$. Поэтому

$$G(\psi, \chi_{ab}) = \sum_{c\in\mathbb{F}_q^*} \psi(c)\chi_{ab}(c) = \sum_{c\in\mathbb{F}_q^*} \psi(c)\chi_b(ac).$$

Введем теперь новую переменную d, полагая $d = ac$. Тогда

$$G(\psi, \chi_{ab}) = \sum_{d\in\mathbb{F}_q^*} \psi(a^{-1}d)\chi_b(d) =$$
$$= \psi(a^{-1}) \sum_{d\in\mathbb{F}_q^*} \psi(d)\chi_b(d) = \overline{\psi(a)}\, G(\psi, \chi_b).$$

(ii) Согласно теореме 5.7, $\chi = \chi_b$ для подходящим образом выбранного элемента $b \in \mathbb{F}_q$ и $\bar{\chi}(c) = \chi_b(-c) = \chi_{-b}(c)$ для любого $c \in \mathbb{F}_q$. Поэтому, используя (i) при $a = -1$ и замечая, что $\psi(-1) = \pm 1$, получаем

$$G(\psi, \bar{\chi}) = G(\psi, \chi_{-b}) = \overline{\psi(-1)}\, G(\psi, \chi_b) = \psi(-1)\, G(\psi, \chi).$$

(iii) Из (ii) вытекает, что $G(\bar{\psi}, \chi) = \bar{\psi}(-1)\, G(\bar{\psi}, \bar{\chi}) = \psi(-1)\, \overline{G(\psi, \chi)}$.

(iv) Комбинируя (iii) и (5.15), получаем, что

$$G(\psi, \chi)\, G(\bar{\psi}, \chi) = \psi(-1)\, G(\psi, \chi)\, \overline{G(\psi, \chi)} = \psi(-1) \cdot |G(\psi, \chi)|^2 = \psi(-1)\, q.$$

(v) На основании теоремы 2.23 (v) $\mathrm{Tr}(a) = \mathrm{Tr}(a^p)$ для $a \in \mathbb{F}_q$, поэтому согласно (5.6), $\chi_1(a) = \chi_1(a^p)$. Таким образом, для любого $c \in \mathbb{F}_q$ получаем

$$\chi_b(c) = \chi_1(bc) = \chi_1(b^p c^p) = \chi_{\sigma(b)}(c^p),$$

а потому

$$G(\psi^p, \chi_b) = \sum_{c \in \mathbb{F}_q^*} \psi^p(c)\, \chi_b(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c^p)\, \chi_{\sigma(b)}(c^p).$$

Но когда c пробегает группу $\mathbb{F}_q^*$, c^p тоже пробегает $\mathbb{F}_q^*$, так что отсюда вытекает требуемый результат. □

5.13. Замечание. В связи с доказанными свойствами сумм Гаусса представляет интерес значение $\psi(-1)$. Очевидно, что $\psi(-1) = \pm 1$. Пусть m — *порядок характера* ψ в группе мультипликативных характеров поля $\mathbb{F}_q$, т. е. m — наименьшее натуральное число, обладающее свойством $\psi^m = \psi_0$. Тогда m делит число $q - 1$, так как $\psi^{q-1} = \psi_0$. Поскольку значениями характера ψ являются корни m-й степени из единицы, то значение -1 может получиться лишь в случае четного числа m. Если g — примитивный элемент поля $\mathbb{F}_q$, то $\psi(g) = \zeta$, где ζ — первообразный корень m-й степени из единицы. Если m четно (и, значит, q нечетно), то в силу примитивности g $\psi(-1) = \psi(g^{(q-1)/2}) = \zeta^{(q-1)/2}$. Полученное число равно -1 в том и только том случае, когда $(q-1)/2 \equiv m/2 \pmod{m}$, т. е. когда $(q-1)/m \equiv 1 \pmod 2$. Поэтому $\psi(-1) = -1$ тогда и только тогда, когда m четно, а $(q-1)/m$ нечетно. Во всех же остальных случаях мы имеем $\psi(-1) = 1$. □

Суммы Гаусса возникают в самых разных областях. Рассмотрим такой пример. Пусть ψ — мультипликативный характер поля $\mathbb{F}_q$; тогда, применяя (5.10), можно написать

$$\psi(c) = \frac{1}{q} \sum_{d \in \mathbb{F}_q^*} \psi(d) \sum_{b \in \mathbb{F}_q} \chi_b(c)\, \overline{\chi_b(d)} =$$

$$= \frac{1}{q} \sum_{b \in \mathbb{F}_q} \chi_b(c) \sum_{d \in \mathbb{F}} \psi(d)\, \bar{\chi}_b(d)$$

для каждого $c \in \mathbb{F}_q^*$. Поэтому

$$\psi(c) = \frac{1}{q} \sum_{\chi} G(\psi, \bar{\chi}) \chi(c) \quad \text{для всех} \quad c \in \mathbb{F}_q^*, \tag{5.16}$$

где сумма берется по всем аддитивным характерам χ поля $\mathbb{F}_q$. Это тождество можно рассматривать как разложенне Фурье мультипликативного характера ψ по аддитивным характерам поля $\mathbb{F}_q$, коэффициентами Фурье которого являются суммы Гаусса.

Аналогично если χ — аддитивный характер поля $\mathbb{F}_q$, то, применяя (5.13), можем написать

$$\chi(c) = \frac{1}{q-1} \sum_{d \in \mathbb{F}_q^*} \chi(d) \sum_{\psi} \psi(c) \overline{\psi(d)} =$$

$$= \frac{1}{q-1} \sum_{\psi} \psi(c) \sum_{d \in \mathbb{F}_q^*} \bar{\psi}(d) \chi(d) \quad \text{для всех} \quad c \in \mathbb{F}_q^*.$$

Таким образом, получаем

$$\chi(c) = \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \psi(c) \quad \text{для всех} \quad c \in \mathbb{F}_q^*, \tag{5.17}$$

где сумма берется по всем мультипликативным характерам ψ поля $\mathbb{F}_q$. Это тождество опять можно рассматривать как разложение Фурье ограничения аддитивного характера χ поля $\mathbb{F}_q$ на $\mathbb{F}_q^*$ по мультипликативным характерам этого поля, причем коэффициентами Фурье снова являются суммы Гаусса. Таким образом, для конечных полей суммы Гаусса служат инструментом для перехода от аддитивной структуры к мультипликативной и обратно.

Прежде чем устанавливать дальнейшие свойства сумм Гаусса, мы изложим один полезный принцип общего характера. Пусть Φ — множество всех нормированных многочленов над полем $\mathbb{F}_q$ и λ — некоторая комплекснозначная функция, определенная на Φ, которая является *мультипликативной* в следующем смысле:

$$\lambda(gh) = \lambda(g) \lambda(h) \quad \text{для всех} \quad g, h \in \Phi, \tag{5.18}$$

и, кроме того, удовлетворяет условиям

$$\lambda(1) = 1 \quad \text{и} \quad |\lambda(g)| \leqslant 1 \quad \text{для всех} \quad g \in \Phi.$$

Обозначим через Φ_k подмножество множества Φ, состоящее из многочленов степени k, и рассмотрим степенной ряд

$$L(z) = \sum_{k=0}^{\infty} \left(\sum_{g \in \Phi_k} \lambda(g) \right) z^k \tag{5.19}$$

в комплексной области. Поскольку множество Φ_k содержит q^k многочленов, коэффициенты при z^k по абсолютной величине не превосходят q^k, так что указанный степенной ряд сходится абсолютно при $|z| < q^{-1}$. В силу (5.18) и учитывая единственность разложения на множители в кольце $\mathbb{F}_q[x]$, мы можем написать

$$L(z) = \sum_{g \in \Phi} \lambda(g) z^{\deg(g)} =$$

$$= \prod_f (1 + \lambda(f) z^{\deg(f)} + \lambda(f^2) z^{\deg(f^2)} + \dots) =$$

$$= \prod_f (1 + \lambda(f) z^{\deg(f)} + (\lambda(f))^2 z^{2\deg(f)} + \dots),$$

где произведение берется по всем нормированным неприводимым многочленам f из $\mathbb{F}_q[x]$. Это означает, что

$$L(z) = \prod_f (1 - \lambda(f) z^{\deg(f)})^{-1}.$$

Теперь применим логарифмическое дифференцирование и результат умножим на z. Получим

$$z \frac{d \log L(z)}{dz} = \sum_f \frac{\lambda(f) \deg(f) z^{\deg(f)}}{1 - \lambda(f) z^{\deg(f)}}.$$

Разлагая $(1 - \lambda(f) z^{\deg(f)})^{-1}$ в геометрический ряд, получаем

$$z \frac{d \log L(z)}{dz} = \sum_f \lambda(f) \deg(f) z^{\deg(f)} \cdot$$

$$\cdot (1 + \lambda(f) z^{\deg(f)} + \lambda(f)^2 z^{2\deg(f)} + \dots) =$$

$$= \sum_f \deg(f) (\lambda(f) z^{\deg(f)} + \lambda(f)^2 z^{2\deg(f)} +$$

$$+ \lambda(f^3) z^{3\deg(f)} + \dots),$$

и, собирая одинаковые степени z, приходим к равенству

$$z \frac{d \log L(z)}{dz} = \sum_{s=1}^{\infty} L_s z^s, \tag{5.20}$$

где

$$L_s = \sum_f \deg(f) \lambda(f)^{s/\deg(f)}; \tag{5.21}$$

здесь сумма берется по всем нормированным неприводимым многочленам f из $\mathbb{F}_q[x]$, степень $\deg(f)$ которых делит s.

Теперь предположим, что существует такое натуральное число t, что

$$\sum_{g \in \Phi_k} \lambda(g) = 0 \quad \text{для всех} \quad k > t. \tag{5.22}$$

Тогда, согласно (5.19), $L(z)$ является комплексным многочленом степени, не превосходящей t, с постоянным членом, равным единице, так что его можно записать в виде

$$L(z) = (1 - \omega_1 z)(1 - \omega_2 z) \dots (1 - \omega_t z), \tag{5.23}$$

где $\omega_1, \omega_2, \dots, \omega_t$ — некоторые комплексные числа. Это означает, что

$$\begin{aligned} z\frac{d \log L(z)}{dz} &= -\sum_{m=1}^{t} \frac{\omega_m z}{1 - \omega_m z} = \\ &= -\sum_{m=1}^{t} \omega_m z \sum_{j=0}^{\infty} \omega_m^j z^j = \\ &= -\sum_{j=0}^{\infty} \left(\sum_{m=1}^{t} \omega_m^{j+1} \right) z^{j+1} = -\sum_{s=1}^{\infty} \left(\sum_{m=1}^{t} \omega_m^s \right) z^s, \end{aligned}$$

и, сравнивая с (5.20), получаем, что

$$L_s = -\omega_1^s - \omega_2^s - \dots - \omega_t^s \quad \text{для всех} \quad s \in \mathbb{N}. \tag{5.24}$$

В качестве приложения этого принципа, выражаемого равенством (5.24), установим одно важное предложение. Пусть χ — аддитивный, а ψ — мультипликативный характеры поля $\mathbb{F}_q$, и пусть E — некоторое конечное расшнрение поля $\mathbb{F}_q$. Тогда характеры χ и ψ можно «поднять» до поля E, полагая $\chi'(\beta) = \chi\left(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)\right)$ для любого $\beta \in E$ и $\psi'(\beta) = \psi\left(N_{E/\mathbb{F}_q}(\beta)\right)$ для любого $\beta \in E^*$. Из аддитивности следа и мультипликативности нормы вытекает, что χ' — аддитивный, а ψ' — мультнпликативный характеры поля E (будем называть их *поднятиями* до E характеров χ и ψ соответственно). Следующая теорема устанавливает важное соотношение между суммой Гаусса $G(\psi, \chi)$ в поле $\mathbb{F}_q$ и суммой Гаусса $G(\psi', \chi')$ в поле E.

5.14. Теорема (теорема Дэвенпорта—Хассе). *Пусть χ — аддитивный, а ψ — мультипликативный характеры поля $\mathbb{F}_q$, не являющиеся одновременно тривиальными, и пусть E — конечное расширение поля $\mathbb{F}_q$, причем $[E : \mathbb{F}_q] = s$. Если χ' и ψ' — поднятия до поля E характеров χ и ψ поля $\mathbb{F}_q$ соответственно, то имеет место равенство*

$$G(\psi', \chi') = (-1)^{s-1} G(\psi, \chi)^s.$$

Доказательство. Для удобства распространим определение мультипликативного характера ψ на все поле $\mathbb{F}_q$, полагая $\psi(0) = 0$. Воспользуемся обозначениями из рассуждения, приводящего к равенству (5.24); в частности, пусть Φ снова обозначает миоже-

ство всех нормированных многочленов над $\mathbb{F}_q$. Определим на этом множестве комплекснозначную функцию λ, полагая $\lambda(1) = 1$ и $\lambda(g) = \psi(c_k)\chi(c_1)$ для любого непостоянного многочлена $g \in \Phi$, представленного в виде $g(x) = x^k - c_1x^{k-1} + \ldots + (-1)^k c_k$. Тогда для функции λ легко проверяется свойство мультипликативности (5.18). Напомнив, что Φ_k обозначает множество многочленов из Φ степени k, разобьем теперь для каждого $k > 1$ множество Φ_k на подмножества, соответствующие фиксированным значениям коэффициентов c_1 и c_k многочленов $g \in \Phi_k$. Так как мощность такого подмножества, соответствующего паре (c_1, c_k), равна q^{k-2}, то

$$\sum_{g \in \Phi_k} \lambda(g) = q^{k-2} \sum_{c_1, c_k \in \mathbb{F}_q} \psi(c_k)\chi(c_1) =$$

$$= q^{k-2}\left(\sum_{c \in \mathbb{F}_q^*} \psi(c)\right)\left(\sum_{c \in \mathbb{F}_q} \chi(c)\right).$$

А ввиду того что по крайней мере один из характеров χ или ψ нетривиален, либо из (5.9), либо из (5.12) получаем, что

$$\sum_{g \in \Phi_k} \lambda(g) = 0 \quad \text{для всех} \quad k > 1.$$

Поэтому равенства (5.22) выполняются при значении $t = 1$. Кроме того, поскольку Φ_1 состоит из многочленов вида $x - c$, где $c \in \mathbb{F}_q$, то

$$\sum_{g \in \Phi_1} \lambda(g) = \sum_{c \in \mathbb{F}_q} \psi(c)\chi(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c) = G(\psi, \chi).$$

Таким образом, из (5.19) получаем, что $L(z) = 1 + G(\psi, \chi)z$, так что, согласно (5.23), $\omega_1 = -G(\psi, \chi)$. Теперь рассмотрим коэффициент L_s степенного ряда (5.20), соответствующий указанному в теореме числу s. В силу (5.21) и ввиду мультипликативности функции λ он должен иметь вид

$$L_s = \sum_f \deg(f)\lambda(f)^{s/\deg(f)} =$$

$$= \sum_f{}^* \deg(f)\lambda(f^{s/\deg(f)}),$$

где сумма берется по всем нормированным неприводимым многочленам f из $\mathbb{F}_q[x]$, степень $\deg(f)$ которых делит s, а звездочка означает, что при этом исключается многочлен $f(x) = x$. Поскольку $[E : \mathbb{F}_q] = s$, то (по теореме 2.14) каждый из этих многочленов f имеет $\deg(f)$ ненулевых различных корней в поле E, и характеристическим многочленом над $\mathbb{F}_q$ каждого корня β многочлена f служит многочлен $f(x)^{s/\deg(f)}$. Пусть

$$f(x)^{s/\deg(f)} = x^s - c_1x^{s-1} + \cdots + (-1)^s c_s;$$

тогда $c_1 = \mathrm{Tr}_{E/\mathbb{F}_q}(\beta)$ и $c_s = N_{E/\mathbb{F}_q}(\beta)$ согласно (2.2) и (2.3). Поэтому

$$\lambda(f^{s/\deg(f)}) = \psi(c_s)\chi(c_1) = \psi(N_{E/\mathbb{F}_q}(\beta))\chi(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)) = \\ = \psi'(\beta)\chi'(\beta),$$

так что

$$L_s = \sum_f{}^{*} \deg(f)\lambda(f^{s/\deg(f)}) = \sum_f{}^{*} \sum_{\substack{\beta \in E \\ f(\beta)=0}} \psi'(\beta)\chi'(\beta).$$

Когда f пробегает все нормированные неприводимые многочлены из $\mathbb{F}_q[x]$ (кроме $f(x) = x$), степени которых делят s, элемент β пробегает в точностн все элементы мультиплнкатнвной группы E^* поля E. Поэтому

$$L_s = \sum_{\beta \in E^*} \psi'(\beta)\chi'(\beta) = G(\psi', \chi'),$$

и, применяя равенство (5.24), получаем

$$G(\psi', \chi') = -(-G(\psi, \chi))^s,$$

что и завершает доказательство теоремы. □

Для некоторых частных характеров соответствующие им суммы Гаусса удается вычислить в явном виде. Так, мы установим еще несколько формул помимо тех тривиальных, список которых приведен в (5.14). Хорошо известна формула, получаемая для квадратичного характера η, определенного в примере 5.10.

5.15. Теорема. *Пусть p — простое нечетное число, $s \in \mathbb{N}$ и $\mathbb{F}_q$ — конечное поле порядка $q = p^s$. Если η — квадратичный, а χ_1 — канонический аддитивный характеры поля $\mathbb{F}_q$, то*

$$G(\eta, \chi_1) = \begin{cases} (-1)^{s-1} q^{1/2}, & \text{если } p \equiv 1 \pmod 4, \\ (-1)^{s-1} i^s q^{1/2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Доказательство. Применяя теорему 5.12 (iv) и учитывая, что $\bar{\eta} = \eta$, получим $G(\eta, \chi_1)^2 = \eta(-1)q$, а поскольку в силу замечания 5.13 $\eta(-1) = 1$ при $q \equiv 1 \pmod 4$ и $\eta(-1) = -1$ при $q \equiv 3 \pmod 4$, то

$$G(\eta, \chi_1) = \begin{cases} \pm q^{1/2}, & \text{если } q \equiv 1 \pmod 4, \\ \pm iq^{1/2}, & \text{если } q \equiv 3 \pmod 4. \end{cases} \tag{5.25}$$

Главная сложность состоит в определении правильного знака.

Рассмотрим сначала случай $s = 1$. Пусть V — множество всех комплекснозначных функцнй, определенных на множестве $\mathbb{F}_p^*$; оно представляет собой $(p-1)$-мерное векторное пространство над полем комплексных чисел. Базис этого пространства

можно, например, построить из *характеристических функций* f_1, f_2, ..., f_{p-1} элементов группы $\mathbb{F}_p^*$, которые определяются условиями $f_j(c) = 1$, если $c = j$, и $f_j(c) = 0$, если $c \neq j$, $j = 1, 2, \ldots$ ..., $p - 1$. Из соотношения ортогональности (5.11) легко вытекает, что мультипликативные характеры ψ_0, ψ_1, ..., ψ_{p-2} поля $\mathbb{F}_p$, определенные в теореме 5.8, ввиду их линейной независимости над $\mathbb{F}_p$ тоже образуют базис пространства V. Пусть $\zeta = e^{2\pi i/p}$; определим линейный оператор T на пространстве V, задавая Th для $h \in V$ равенством

$$(Th)(c) = \sum_{k=1}^{p-1} \zeta^{ck} h(k) \quad \text{для} \quad c = 1, 2, \ldots, p-1. \tag{5.26}$$

Учитывая, что, согласно (5.6) и теореме 5.7, $\zeta^{ck} = \chi_c(k)$, получаем из теоремы 5.12 (i), что для каждого мультипликативного характера ψ поля $\mathbb{F}_p$ справедливо равенство $T\psi = G(\psi, \chi_1)\bar{\psi}$. Поскольку равенство $\bar{\psi} = \psi$ имеет место лишь для тривиального и квадратичного характеров, то матрица оператора T в базисе ψ_0, ψ_1, ..., ψ_{p-2} имеет два диагональных ненулевых элемента, а именно $G(\psi_0, \chi_1) = -1$ (ввиду (5.14)) и $G(\eta, \chi_1)$, и, кроме того, семейство диагональных блоков вида

$$\begin{pmatrix} 0 & G(\bar{\psi}, \chi_1) \\ G(\psi, \chi_1) & 0 \end{pmatrix},$$

соответствующих каждой паре ψ, $\bar{\psi}$ сопряженных характеров (отличных от тривиального и квадратичного). При подсчете определителя этой матрицы мы от каждого такого блока на основании теоремы 5.12 (iv) получаем сомножитель

$$-G(\psi, \chi_1)\, G(\bar{\psi}, \chi_1) = -\psi(-1)\, p.$$

Таким образом,

$$\det(T) = -G(\eta, \chi_1)\,(-p)^{(p-3)/2} \prod_{j=1}^{(p-3)/2} \psi_j(-1). \tag{5.27}$$

Далее, так как $\psi_j(-1) = \psi_1^j(-1) = (-1)^j$, то

$$\prod_{j=1}^{(p-3)/2} \psi_j(-1) = (-1)^{1+2+\cdots+(p-3)/2} = (-1)^{(p-1)\,(p-3)/8}. \tag{5.28}$$

Кроме того, поскольку

$$i^{(p-1)^2/4} = \begin{cases} 1, & \text{если} \quad p \equiv 1 \pmod 4, \\ i, & \text{если} \quad p \equiv 3 \pmod 4, \end{cases}$$

получаем из (5.25), что

$$G(\eta, \chi_1) = \pm i^{(p-1)^2/4} p^{1/2}. \tag{5.29}$$

Учитывая равенства (5.27), (5.28) и (5.29), получаем, что

$$\det(T) = \pm(-1)^{(p-1)/2}\, i^{(p-1)^2/4}\,(-1)^{(p-1)\ (p-3)/8}\, p^{(p-2)/2} =$$
$$= \pm(-1)^{(p-1)/2}\, i^{(p-1)^2/4+(p-1)\ (p-3)/4} p^{(p-2)/2},$$

т. е.

$$\det(T) = \pm(-1)^{(p-1)/2}\, i^{(p-1)\ (p-2)/2} p^{(p-2)/2}. \tag{5.30}$$

Теперь мы вычислим определитель $\det(T)$, задавая матрицу оператора T в базисе $f_1, f_2, \ldots, f_{p-1}$. Из (5.26) находим, что

$$\det(T) = \det((\zeta^{jk})_{1\leqslant j,\ k\leqslant p-1}) = \det((\zeta^j \zeta^{j\ (k-1)})_{1\leqslant j,\ k\leqslant p-1}) =$$
$$= \zeta^{1+2+\cdots+(p-1)} \det((\zeta^{j\ (k-1)})_{1\leqslant j,\ k\leqslant p-1}) =$$
$$= \det((\zeta^{j\ (k-1)})_{1\leqslant j,\ k\leqslant p-1}),$$

т. е. $\det(T)$ является определителем Вандермонда. Поэтому

$$\det(T) = \prod_{1\leqslant m<n\leqslant p-1} (\zeta^n - \zeta^m).$$

При $\delta = e^{\pi i/p}$ мы получаем

$$\det(T) = \prod_{1\leqslant m<n\leqslant p-1} (\delta^{2n} - \delta^{2m}) =$$
$$= \prod_{1\leqslant m<n\leqslant p-1} \delta^{n+m}(\delta^{n-m} - \delta^{-(n-m)}) =$$
$$= \prod_{1\leqslant m<n\leqslant p-1} \delta^{n+m} \prod_{1\leqslant m<n\leqslant p-1} \left(2i \sin\frac{\pi(n-m)}{p}\right).$$

Так как

$$\sum_{1\leqslant m<n\leqslant p-1} (n+m) = \sum_{n=2}^{p-1}\sum_{m=1}^{n-1} (n+m) =$$
$$= \frac{3}{2}\sum_{n=2}^{p-1} n(n-1) = \frac{3}{2}\sum_{n=1}^{p-2}(n^2+n) =$$
$$= \frac{3}{2}\left(\frac{(p-2)(p-1)(2p-3)}{6} + \frac{(p-2)(p-1)}{2}\right) =$$
$$= \frac{p(p-1)(p-2)}{2},$$

го первое произведение равно

$$\delta^{p\ (p-1)\ (p-2)/2} = (-1)^{(p-1)\ (p-2)/2} = ((-1)^{(p-2)\ (p-1)/2} = (-1)^{(p-1)/2}.$$

Кроме того,

$$A = \prod_{1\leqslant m<n\leqslant p-1} \left(2\sin\frac{\pi(n-m)}{p}\right) > 0,$$

так что

$$\det(T) = (-1)^{(p-1)/2}\, i^{(p-1)(p-2)/2} A, \quad \text{где} \quad A > 0.$$

Сравнивая это выражение с (5.30), мы видим, что в равенстве (5.29) всегда следует брать знак $+$. Это доказывает теорему для случая $s = 1$.

Общий случай сразу получается из теоремы 5.14 ввиду того, что канонический аддитивный характер поля $\mathbb{F}_p$ поднимается до канонического аддитивного характера поля $\mathbb{F}_q$ (по формуле (5.7)), а квадратичный характер поля $\mathbb{F}_p$ поднимается до квадратичного характера поля $\mathbb{F}_q$. □

Учитывая формулы (5.14) и теорему 5.12) (i), можно вывести формулу, аналогичную указанной в теореме 5.15, для суммы Гаусса $G(\eta, \chi)$ с любым аддитивным характером χ поля $\mathbb{F}_q$.

Получим теперь формулу для другого частного типа сумм Гаусса, применимую для более широкого класса мультипликативных характеров, но требующую некоторого ограничения на основное поле. Будем использовать понятие порядка мультипликативного характера, введенное в замечании 5.13.

5.16. Теорема (теорема Штикельбергера). *Пусть χ_1 — канонический аддитивный характер поля $\mathbb{F}_{q^2}$, где q — некоторая степень простого числа, и пусть ψ — нетривиальный мультипликативный характер того же поля, причем порядок m этого характера делит число $q+1$. Тогда*

$$G(\psi, \chi_1) = \begin{cases} q, & \text{если } m \text{ нечетно или } \dfrac{q+1}{m} \text{ четно;} \\ -q, & \text{если } m \text{ четно, а } \dfrac{q+1}{m} \text{ нечетно.} \end{cases}$$

Доказательство. Положим $E = \mathbb{F}_{q^2}$ и $F = \mathbb{F}_q$. Пусть γ — примитивный элемент поля E, и пусть $g = \gamma^{q+1}$. Тогда $g^{q-1} = 1$, так что $g \in F$; более того, g является примитивным элементом поля F. Каждый элемент $\alpha \in E^*$ можно записать в виде $\alpha = g^j \gamma^k$, где $0 \leqslant j < q-1$ и $0 \leqslant k < q+1$. Так как $\psi(g) = \psi^{q+1}(\gamma) = 1$, то

$$\begin{aligned} G(\psi, \chi_1) &= \sum_{j=0}^{q-2} \sum_{k=0}^{q} \psi(g^j \gamma^k)\, \chi_1(g^j \gamma^k) = \\ &= \sum_{k=0}^{q} \psi^k(\gamma) \sum_{j=0}^{q-2} \chi_1(g^j \gamma^k) = \\ &= \sum_{k=0}^{q} \psi^k(\gamma) \sum_{b \in F^*} \chi_1(b\gamma^k). \end{aligned} \tag{5.31}$$

Если τ_1 — канонический аддитивный характер поля F, то, согласно (5.7), $\chi_1(b\gamma^k) = \tau_1(\mathrm{Tr}_{E/F}(b\gamma^k))$. Поэтому, учитывая теорему 2.23 (ii) и (5.9), получаем

$$\sum_{b\in F^*}\chi_1(b\gamma^k) = \sum_{b\in F^*}\tau_1(b\,\mathrm{Tr}_{E/F}(\gamma^k)) = \begin{cases} -1, & \text{если } \mathrm{Tr}_{E/F}(\gamma^k)\neq 0,\\ q-1, & \text{если } \mathrm{Tr}_{E/F}(\gamma^k)=0. \end{cases} \tag{5.32}$$

Поскольку по определению следа $\mathrm{Tr}_{E/F}(\gamma^k) = \gamma^k + \gamma^{kq}$, то

$$\mathrm{Tr}_{E/F}(\gamma^k) = 0 \text{ тогда и только тогда, когда } \gamma^{k(q-1)} = -1. \tag{5.33}$$

Если число q нечетно, то последнее условие эквивалентно равенству $k = (q+1)/2$, и тогда из (5.32) получаем

$$\sum_{b\in F^*}\chi_1(b\gamma^k) = \begin{cases} -1 & \text{при } 0\leqslant k<q+1,\ k\neq\frac{q+1}{2},\\ q-1 & \text{при } k=\frac{q+1}{2}. \end{cases}$$

Поэтому из (5.31) следует, что

$$G(\psi,\chi_1) = -\sum_{\substack{k=0\\ k\neq(q+1)/2}}^{q}\psi^k(\gamma) + (q-1)\psi^{(q+1)/2}(\gamma) = -\sum_{k=0}^{q}\psi^k(\gamma) + q\psi^{(q+1)/2}(\gamma) = q\psi^{(q+1)/2}(\gamma),$$

так как $\psi(\gamma)\neq 1$ и $\psi^{q+1}(\gamma) = 1$. Далее, поскольку m — порядок характера ψ, то значение $\psi^{(q+1)/2}(\gamma) = -1$ может получиться лишь при четном m и нечетном $(q+1)/m$ (так как тогда $\psi^{(q+1)/2}(\gamma) = (\psi^{m/2}(\gamma))^{(q+1)/m} = (-1)^{(q+1)/m} = -1$. — *Перев.*). Во всех же остальных случаях $\psi^{(q+1)/2}(\gamma) = 1$. Поэтому для нечетного числа q получим

$$G(\psi,\chi_1) = \begin{cases} q, & \text{если } m \text{ нечетно или } \frac{q+1}{m} \text{ четно},\\ -q, & \text{если } m \text{ четно и } \frac{q+1}{m} \text{ нечетно}. \end{cases} \tag{5.34}$$

Если же число q четно, то равенство $\gamma^{k(q-1)} = -1$ в (5.33) эквивалентно равенству $\gamma^{k(q-1)} = 1$, и единственным числом k, $0\leqslant k<q+1$, удовлетворяющим ему, является $k = 0$. Поэтому из (5.32) получим, что

$$\sum_{b\in F^*}\chi_1(b\gamma^k) = \begin{cases} -1 & \text{при } 1\leqslant k\leqslant q,\\ q-1 & \text{при } k=0, \end{cases}$$

а тогда из (5.31) вытекает, что

$$G(\psi, \chi_1) = -\sum_{k=1}^{q} \psi^k(\gamma) + q - 1 = -\sum_{k=0}^{q} \psi^k(\gamma) + q = q.$$

Объединяя это с (5.34), получаем искомый результат. □

В заключение покажем, как можно использовать суммы Гаусса для получения одного классического результата теории чисел, а именно *квадратичного закона взаимности*. Напомним (см. пример 5.10), что если p — нечетное простое число и η — квадратичный характер поля $\mathbb{F}_p$, то для $c \not\equiv 0 \pmod p$ символ Лежандра $\left(\frac{c}{p}\right)$ определяется равенством $\left(\frac{c}{p}\right) = \eta(c)$.

5.17. **Теорема** (квадратичный закон взаимности). *Для любых различных нечетных простых чисел p и r имеет место равенство*

$$\left(\frac{p}{r}\right)\left(\frac{r}{p}\right) = (-1)^{(p-1)(r-1)/4}.$$

Доказательство. Пусть η — квадратичный и χ_1 — канонический аддитивный характеры поля $\mathbb{F}_p$; положим $G = G(\eta, \chi_1)$. Из (5.25) вытекает, что $G^2 = (-1)^{(p-1)/2} p = \tilde{p}$, так что

$$G^r = (G^2)^{(r-1)/2} G = \tilde{p}^{(r-1)/2} G. \tag{5.35}$$

Пусть R — кольцо *целых алгебраических чисел*, т. е. R состоит из всех комплексных чисел, являющихся корнями иормированных многочленов с целыми коэффициентами. Поскольку значения (как аддитивных, так и мультипликативных) характеров конечных полей являются комплексными корнями из единицы, а каждый такой корень является целым алгебраическим числом, то значения сумм Гаусса являются целыми алгебраическими числами. В частности, $G \in R$. Обозначим через (r) главный идеал кольца R, порожденный числом r. Тогда факторкольцо $R/(r)$ имеет характеристику r, и применеиие теоремы 1.46 дает

$$G^r = \left(\sum_{c \in \mathbb{F}_p^*} \eta(c)\chi_1(c)\right)^r \equiv \sum_{c \in \mathbb{F}_p^*} \eta^r(c)\chi_1^r(c) \pmod{(r)}.$$

Далее,

$$\sum_{c \in \mathbb{F}_p^*} \eta^r(c)\chi_1^r(c) = \sum_{c \in \mathbb{F}_p^*} \eta(c)\chi_r(c) = G(\eta, \chi_r) = \eta(r)\, G,$$

где в последнем равеистве использована теорема 5.12 (i), так что

$$G^r \equiv \eta(r)\, G \pmod{(r)}.$$

Объединяя это с (5.35), получаем

$$\tilde{p}^{(r-1)/2}G \equiv \eta(r)\, G \pmod{(r)};$$

умножение на G приводит к сравнению

$$\tilde{p}^{(r-1)/2}\tilde{p} \equiv \eta(r)\, \tilde{p} \pmod{(r)},$$

так как $G^2 = \tilde{p}$. Поскольку обе части последнего сравнения фактически являются элементами кольца $\mathbb{Z}$ целых чисел, мы получаем сравнение в этом кольце:

$$\tilde{p}^{(r-1)/2}\tilde{p} \equiv \eta(r)\, \tilde{p} \pmod{r}.$$

Поскольку число $\tilde{p}$ взаимно просто с r, то отсюда получаем сравнение

$$\tilde{p}^{(r-1)/2} \equiv \eta(r) \pmod{r}.$$

Далее, умножая на $p^{(r-1)/2}$, получаем в силу равенства $\tilde{p} = (-1)^{(p-1)/2}p$ и сравнения $p^{r-1} \equiv 1 \pmod{r}$ (см. упр. 1.9), что

$$(-1)^{(p-1)\,(r-1)/4} \equiv p^{(r-1)/2}\eta(r) \pmod{r}. \tag{5.36}$$

Поскольку $p^{(r-1)/2} \equiv \pm 1 \pmod{r}$ и знак $+$ имеет место тогда и только тогда, когда число p сравнимо по модулю r с некоторым квадратом, то

$$p^{(r-1)/2} \equiv \left(\frac{p}{r}\right) \pmod{r},$$

Так как $\eta(r) = \left(\frac{r}{p}\right)$, то из (5.36) получаем

$$(-1)^{(p-1)\,(r-1)/4} \equiv \left(\frac{p}{r}\right)\left(\frac{r}{p}\right) \pmod{r}.$$

Но целые числа, стоящие в разных частях этого сравнения, могут быть лишь ± 1, поэтому ввиду того, что $r \geqslant 3$, сравнение выполняется лишь тогда, когда эти числа совпадают. □

§ 3. Суммы Якоби

Если λ — мультипликативный характер конечного поля $\mathbb{F}_q$, то он определен для всех ненулевых элементов этого поля. Однако полезно распространить его определение на все поле $\mathbb{F}_q$, положив $\lambda(0) = 1$, если λ — тривиальный характер, и $\lambda(0) = 0$, если λ — нетривиальный характер. При таком доопределении

$$\sum_{c \in \mathbb{F}_q} \lambda(c) = \begin{cases} q, & \text{если } \lambda \text{ тривиален,} \\ 0, & \text{если } \lambda \text{ нетривиален.} \end{cases} \tag{5.37}$$

Кроме того, теперь условие $\lambda(a_1, a_2) = \lambda(a_1)\lambda(a_2)$ выполняется для всех $a_1, a_2 \in \mathbb{F}_q$.

Пусть заданы k мультипликативных характеров $\lambda_1, \ldots, \lambda_k$ поля $\mathbb{F}_q$, и пусть зафиксирован некоторый элемент $a \in \mathbb{F}_q$. Определим сумму

$$J_a(\lambda_1, \ldots, \lambda_k) = \sum_{c_1+\cdots+c_k=a} \lambda_1(c_1) \ldots \lambda_k(c_k),$$

где суммирование ведется по всем k-наборам $(c_1, \ldots, c_k)$ элементов поля $\mathbb{F}_q$, таким, что $c_1 + \ldots + c_k = a$. Таким образом, эта сумма содержит q^{k-1} членов.

Если $a \neq 0$, то мы можем положить $c_1 = ab_1, \ldots, c_k = ab_k$. Тогда $b_1 + \ldots + b_k = 1$, и мы получаем

$$\begin{aligned} J_a(\lambda_1, \ldots, \lambda_k) &= \sum_{b_1+\cdots+b_k=1} \lambda_1(ab_1) \ldots \lambda_k(ab_k) = \\ &= \lambda_1(a) \ldots \lambda_k(a) \sum_{b_1+\cdots+b_k=1} \lambda_1(b_1) \ldots \lambda_k(b_k) = \\ &= (\lambda_1 \ldots \lambda_k)(a) J_1(\lambda_1, \ldots, \lambda_k). \end{aligned} \tag{5.38}$$

В силу этого простого соотношения достаточно рассмотреть лишь две суммы: $J_0(\lambda_1, \ldots, \lambda_k)$ и $J_1(\lambda_1, \ldots, \lambda_k)$. Вторая из них более важна для приложений, поэтому мы для нее будем использовать более простое обозначение.

5.18. Определение. Пусть заданы k мультипликативных характеров $\lambda_1, \ldots, \lambda_k$ поля $\mathbb{F}_q$. Тогда *суммой Якоби* для них называется сумма

$$J(\lambda_1, \ldots, \lambda_k) = \sum_{c_1+\cdots+c_k=1} \lambda_1(c_1) \ldots \lambda_k(c_k),$$

где суммирование ведется по всем k-наборам $(c_1, \ldots, c_k)$ элементов поля $\mathbb{F}_q$, таким, что $c_1 + \ldots + c_k = 1$.

Если $k = 1$, то $J(\lambda_1) = \lambda_1(1) = 1$ для любого мультипликативного характера λ_1 поля $\mathbb{F}_q$. Поэтому суммы Якоби представляют интерес лишь для $k \geqslant 2$. Из определения сразу вытекает, что значение $J(\lambda_1, \ldots, \lambda_k)$ не зависит от порядка, в котором выписаны характеры λ_i. То же справедливо и для $J_0(\lambda_1, \ldots, \lambda_k)$.

Сумма Якоби $J(\lambda_1, \ldots, \lambda_k)$, а также и сумма $J_0(\lambda_1, \ldots, \lambda_k)$ легко вычисляются, если некоторые из характеров λ_i тривиальны.

5.19. Теорема. *Если все мультипликативные характеры* $\lambda_1, \ldots, \lambda_k$ *поля* $\mathbb{F}_q$ *тривиальны, то*

$$J(\lambda_1, \ldots, \lambda_k) = J_0(\lambda_1, \ldots, \lambda_k) = q^{k-1}. \tag{5.39}$$

Если же некоторые (но не все) из характеров λ_i *тривиальны, то*

$$J(\lambda_1, \ldots, \lambda_k) = J_0(\lambda_1, \ldots, \lambda_k) = 0. \tag{5.40}$$

Доказательство. Равенства (5.39) очевидны, так как в обоих случаях мы имеем сумму q^{k-1} членов, каждый из которых равен 1. Для доказательства (5.40) предположим, что характеры выписаны в таком порядке, что $\lambda_1, \ldots, \lambda_h$ нетривиальны, а $\lambda_{h+1}, \ldots, \lambda_k$ тривиальны, где $1 \leqslant h \leqslant k-1$. Тогда

$$J(\lambda_1, \ldots, \lambda_k) = \sum_{c_1+\cdots+c_k=1} \lambda_1(c_1) \ldots \lambda_k(c_k) = \sum_{c_1+\cdots+c_h=1} \lambda_1(c_1) \ldots \lambda_h(c_h).$$

Для фиксированных элементов $c_1, \ldots, c_h \in \mathbb{F}_q$ существует q^{k-h-1} решений $(c_{h+1}, \ldots, c_k)$ уравнения $c_{h+1} + \ldots + c_k = 1 - c_1 - \ldots - c_h$. Поэтому

$$J(\lambda_1, \ldots, \lambda_k) = q^{k-h-1} \sum_{c_1, \ldots, c_h \in \mathbb{F}_q} \lambda_1(c_1) \ldots \lambda_h(c_h) = q^{k-h-1} \left(\sum_{c_1 \in \mathbb{F}_q} \lambda_1(c_1)\right) \ldots \left(\sum_{c_h \in \mathbb{F}_q} \lambda_h(c_h)\right) = 0,$$

где последнее равенство вытекает из (5.37). Аналогичное рассуждение показывает, что и $J_0(\lambda_1, \ldots, \lambda_k) = 0$. □

Для исследования случая, когда все характеры λ_i нетривиальны, нам понадобится один результат, связывающий сумму $J_0(\lambda_1, \ldots, \lambda_k)$ с суммами Якоби.

5.20. Теорема. *Пусть $\lambda_1, \ldots, \lambda_k$ — мультипликативные характеры поля $\mathbb{F}_q$, причем характер λ_k нетривиален. Если при этом характер $\lambda_1 \ldots \lambda_k$ тоже нетривиален, то*

$$J_0(\lambda_1, \ldots, \lambda_k) = 0, \tag{5.41}$$

если же характер $\lambda_1 \ldots \lambda_k$ тривиален, то

$$J_0(\lambda_1, \ldots, \lambda_k) = \lambda_k(-1)(q-1) J(\lambda_1, \ldots, \lambda_{k-1}). \tag{5.42}$$

Доказательство. Так как случай $k = 1$ тривиален, то можно считать, что $k \geqslant 2$. Тогда

$$J_0(\lambda_1, \ldots, \lambda_k) = \sum_{a \in \mathbb{F}_q} \left(\sum_{c_1+\cdots+c_{k-1}=-a} \lambda_1(c_1) \ldots \lambda_{k-1}(c_{k-1})\right) \lambda_k(a) = \sum_{a \in \mathbb{F}_q} J_{-a}(\lambda_1, \ldots, \lambda_{k-1}) \lambda_k(a).$$

Поскольку (в силу нетривиальности λ_k) $\lambda_k(0) = 0$, то, применяя (5.38), получаем

$$J_0(\lambda_1, \ldots, \lambda_k) = \sum_{a \in \mathbb{F}_q^*} J_{-a}(\lambda_1, \ldots, \lambda_{k-1}) \lambda_k(a) =$$

$$= J(\lambda_1, \ldots, \lambda_{k-1}) \sum_{a \in \mathbb{F}_q^*} (\lambda_1 \ldots \lambda_{k-1})(-a)\lambda_k(a) =$$

$$= (\lambda_1 \ldots \lambda_{k-1})(-1) J(\lambda_1, \ldots, \lambda_{k-1}) \cdot$$

$$\cdot \sum_{a \in \mathbb{F}_q^*} (\lambda_1 \ldots \lambda_{k-1}\lambda_k)(a).$$

Теперь если характер $\lambda_1 \ldots \lambda_k$ нетривиален, то в силу (5.12) последняя сумма равна нулю и равенство (5.41) доказано. Если же характер $\lambda_1 \ldots \lambda_k$ тривиален, то последняя сумма равна $q - 1$. Равенство (5.42) тогда вытекает из следующих равенств: $(\lambda_1 \ldots \ldots \lambda_{k-1})(-1) = \bar{\lambda}_k(-1) = \lambda_k(-1)$; последнее из них обусловлено действительностью числа $\lambda_k(-1)$, поскольку $\lambda_k(-1)^2 = \lambda_k(1) = 1$. □

В случае когда все характеры λ_i нетривиальны, существует важная связь между суммами Якоби и суммами Гаусса, которая позволит нам вычислить абсолютные величины сумм Якоби.

5.21. Теорема. *Пусть $\lambda_1, \ldots, \lambda_k$ — нетривиальные мультипликативные, а χ — нетривиальный аддитивный характеры поля $\mathbb{F}_q$. Тогда если характер $\lambda_1 \ldots \lambda_k$ нетривиален, то*

$$J(\lambda_1, \ldots, \lambda_k) = \frac{G(\lambda_1, \chi) \ldots G(\lambda_k, \chi)}{G(\lambda_1 \ldots \lambda_k, \chi)}; \tag{5.43}$$

если же характер $\lambda_1 \ldots \lambda_k$ тривиален, то

$$J(\lambda_1, \ldots, \lambda_k) = -\lambda_k(-1) J(\lambda_1, \ldots, \lambda_{k-1}) =$$

$$= -\frac{1}{q} G(\lambda_1, \chi) \ldots G(\lambda_k, \chi). \tag{5.44}$$

Доказательство. Ввиду нетривиальности каждого характера λ имеем $\lambda_i(0) = 0$, так что

$$G(\lambda_i, \chi) = \sum_{c_i \in \mathbb{F}_q} \lambda_i(c_i)\chi(c_i).$$

Поэтому

$$G(\lambda_1, \chi) \ldots G(\lambda_k, \chi) = \left(\sum_{c_1 \in \mathbb{F}_q} \lambda_1(c_1)\chi(c_1)\right) \ldots \left(\sum_{c_k \in \mathbb{F}_q} \bar{\lambda}_k(c_k)\chi(c_k)\right) =$$

$$= \sum_{c_1, \ldots, c_k \in \mathbb{F}_q} \lambda_1(c_1) \ldots \lambda_k(c_k)\chi(c_1 + \ldots + c_k) =$$

$$= \sum_{a \in \mathbb{F}_q} \chi(a) \sum_{c_1 + \cdots + c_k = a} \lambda_1(c_1) \ldots \lambda_k(c_k) =$$

$$= \sum_{a \in \mathbb{F}_q} \chi(a) J_a(\lambda_1, \ldots, \lambda_k).$$

Если характер $\lambda_1 \dots \lambda_k$ нетривиален, то в силу (5.41) $J_0(\lambda_1, \dots, \lambda_k) = 0$, и на основании (5.38) получаем

$$G(\lambda_1, \chi) \dots G(\lambda_k, \chi) = J(\lambda_1, \dots, \lambda_k) \sum_{a \in \mathbb{F}_q^*} (\lambda_1 \dots \lambda_k)(a)\chi(a) =$$

$$= J(\lambda_1, \dots, \lambda_k) G(\lambda_1 \dots \lambda_k, \chi).$$

Здесь $G(\lambda_1 \dots \lambda_k, \chi) \neq 0$ в силу (5.15), поскольку характер $\lambda_1 \dots \lambda_k$ нетривиален, и тем самым равенство (5.43) доказано.

Если же характер $\lambda_1 \dots \lambda_k$ тривиален, то ввиду (5.38) имеем $J_a(\lambda_1, \dots, \lambda_k) = J(\lambda_1, \dots, \lambda_k)$ для всех $a \in \mathbb{F}_q^*$, и поэтому

$$J_0(\lambda_1, \dots, \lambda_k) + (q-1) J(\lambda_1, \dots, \lambda_k) = \sum_{a \in \mathbb{F}_q} J_a(\lambda_1, \dots, \lambda_k) =$$

$$= \sum_{c_1, \dots, c_k \in \mathbb{F}_q} \lambda_1(c_1) \dots \lambda_k(c_k) =$$

$$= \left(\sum_{c_1 \in \mathbb{F}_q} \lambda_1(c_1)\right) \dots \left(\sum_{c_k \in \mathbb{F}_q} \lambda_k(c_k)\right) = 0,$$

где в последнем равенстве использовано (5.37). Отсюда, применяя (5.42), получаем первое равенство из (5.44). Кроме того, ввиду нетривиальности характера $\lambda_1 \dots \lambda_{k-1}$ мы можем применить (5.43) и получим

$$\lambda_k(-1) J(\lambda_1, \dots, \lambda_{k-1}) = \frac{\lambda_k(-1) G(\lambda_1, \chi) \dots G(\lambda_{k-1}, \chi)}{G(\lambda_1 \dots \lambda_{k-1}, \chi)} =$$

$$= \frac{\lambda_k(-1) G(\lambda_1, \chi) \dots G(\lambda_{k-1}, \chi) G(\lambda_k, \chi)}{G(\bar{\lambda}_k, \chi) G(\lambda_k, \chi)} =$$

$$= \frac{1}{q} G(\lambda_1, \chi) \dots G(\lambda_k, \chi),$$

используя на последнем шаге теорему 5.12 (iv). Таким образом, доказано и второе равенство из (5.44). □

5.22. Теорема. *Пусть $\lambda_1, \dots, \lambda_k$ — нетривиальные мультипликативные характеры поля $\mathbb{F}_q$. Тогда если характер $\lambda_1 \dots \lambda_k$ нетривиален, то*

$$|J(\lambda_1, \dots, \lambda_k)| = q^{(k-1)/2}; \tag{5.45}$$

если же характер $\lambda_1 \dots \lambda_k$ тривиален, то

$$|J(\lambda_1, \dots, \lambda_k)| = q^{(k-2)/2}. \tag{5.46}$$

Доказательство. Равенство (5.45) вытекает из (5.15) и (5.43), а равенство (5.46) — из (5.15) и (5.44). □

5.23. Следствие. *Если $\lambda_1, \dots, \lambda_k$ — нетривиальные мультипликативные характерны поля $\mathbb{F}_q$ и характер $\lambda_1 \dots \lambda_k$ тривиален, то*

$$|J_0(\lambda_1, \dots, \lambda_k)| = (q-1) q^{(k-2)/2}.$$

Доказательство. Утверждение вытекает из (5.42) и (5.45). □

5.24. **Пример.** Дадим еще одно доказательство квадратичного закона взаимности (см. теорему 5.17), применяя свойства сумм Якоби. Пусть p и r — различные простые нечетные числа, η — квадратичный характер, а χ_1 — канонический аддитивный характер поля $\mathbb{F}_p$ и $G = G(\eta, \chi_1)$. Определим сумму Якоби J для поля $\mathbb{F}_p$ равенством

$$J = \underbrace{J(\eta, \ldots, \eta)}_{r} = \sum_{c_1+\cdots+c_r=1} \eta(c_1) \ldots \eta(c_r).$$

Поскольку η^{r+1} — тривиальный характер, то из второго равенства (5.44) получаем

$$G^{r+1} = \eta(-1)\, pJ = \tilde{p}J, \quad \text{где} \quad \tilde{p} = (-1)^{(p-1)/2} p.$$

С другой стороны, $G^2 = \tilde{p}$ (из доказательства теоремы 5.17), так что

$$G^{r+1} = (G^2)^{(r+1)/2} = \tilde{p}^{(r+1)/2}.$$

Сравнивая, получаем, что

$$J = \tilde{p}^{(r-1)/2}. \tag{5.47}$$

Теперь рассмотрим члены суммы J. Поскольку характер η принимает лишь значения 0 и ± 1, то каждый член суммы J является целым числом. Если $c_1 = \ldots = c_r = c$, то c должно быть равно $r^{-1} \in \mathbb{F}_p$, и соответствующий r-набору $(c, \ldots, c)$ член суммы J имеет значение $\eta^r(r^{-1}) = \eta(r^{-1}) = \eta(r)$. Если же элементы c_i не все равны между собой, то существует r различных r-наборов, получаемых из $(c_1, \ldots, c_r)$ циклическими перестановками. Соответствующие им члены суммы J должны совпадать, и, таким образом, сумма этих r членов будет сравнима с нулем по модулю r. Разбивая сумму J на такие группы слагаемых, мы получим, что $J \equiv \eta(r) \pmod{r}$. Вместе с (5.47) это дает

$$\tilde{p}^{(r-1)/2} \equiv \eta(r) \pmod{r}.$$

Завершение доказательства проводится так же, как и в теореме 5.17. □

5.25. **Пример.** Докажем с помощью сумм Якоби, что каждое простое нечетное число p, которое сравнимо с 1 по модулю 4, представимо в виде суммы квадратов двух целых чисел. Поскольку 4 делит число $p - 1$, то из следствия 5.9 вытекает существование мультипликативного характера λ поля $\mathbb{F}_p$, имеющего порядок 4 (определение порядка мультипликативного характера см. в замечании 5.13). Тогда λ может принимать лишь значения 0, ± 1 и $\pm i$, поэтому ясно, что для квадратичного характера $\eta = \lambda^2$

$$J(\lambda, \eta) = \sum_{c_1+c_2=1} \lambda(c_1)\, \eta(c_2) = A + Bi,$$

где A и B — некоторые целые числа. На основании (5.45)

$$p = |J(\lambda, \eta)|^2 = A^2 + B^2,$$

и утверждение доказано.

Заметим, что простое нечетное число p, сравнимое с 3 по модулю 4, нельзя записать в виде суммы двух квадратов целых чисел, так как квадрат целого числа сравним по модулю 4 либо с 0, либо с 1; поэтому $A^2 + B^2$ никогда не может быть сравнимо с 3 по модулю 4. Что же касается единственного простого числа, не рассмотренного выше, а именно $p = 2$, то оно, очевидно, является суммой двух квадратов целых чисел, поскольку $2 = 1^2 + 1^2$. □

Существует аналог теоремы 5.14 для сумм Якоби. Будем снова употреблять понятие поднятия характеров, введенное перед теоремой 5.14.

5.26. Теорема. *Пусть* $\lambda_1, \ldots, \lambda_k$ — *мультипликативные характеры поля* $\mathbb{F}_q$, *не все из которых тривиальны. Если* $\lambda_1', \ldots, \lambda_k'$ — *соответственно поднятия характеров* $\lambda_1, \ldots, \lambda_k$ *до конечного расширения* E *поля* $\mathbb{F}_q$, *где* $[E : \mathbb{F}_q] = s$, *то*

$$J(\lambda_1', \ldots, \lambda_k') = (-1)^{(s-1)(k-1)} J(\lambda_1, \ldots, \lambda_k)^s. \qquad (5.48)$$

Доказательство. Заметим, что поднимая тривиальный характер, получаем снова тривиальный характер, а поднимая нетривиальный, получаем нетривиальный. Поэтому если какой-либо из характеров λ_i тривиален, то обе части равенства (5.48) равны нулю, согласно (5.40). Если все характеры $\lambda_1, \ldots, \lambda_k$ нетривиальны и характер $\lambda_1 \ldots \lambda_k$ тоже нетривиален, то для некоторого нетривиального аддитивного характера χ поля $\mathbb{F}_q$ из (5.43) и теоремы 5.14 следует, что

$$J(\lambda_1', \ldots, \lambda_k') = \frac{G(\lambda_1', \chi') \ldots G(\lambda_k', \chi')}{G(\lambda_1' \ldots \lambda_k', \chi')} =$$

$$= \frac{(-1)^{s-1} G(\lambda_1, \chi)^s \ldots (-1)^{s-1} G(\lambda_k, \chi)^s}{(-1)^{s-1} G(\lambda_1 \ldots \lambda_k, \chi)^s} =$$

$$= (-1)^{(s-1)(k-1)} J(\lambda_1, \ldots, \lambda_k)^s.$$

Если же все характеры λ_i нетривиальны, но характер $\lambda_1 \ldots \lambda_k$ тривиален, то из (5.44) и теоремы 5.14 вытекает, что

$$J(\lambda_1', \ldots, \lambda_k') = -\frac{1}{q^s} G(\lambda_1', \chi') \ldots G(\lambda_k', \chi') =$$

$$= -\frac{1}{q^s} (-1)^{(s-1)k} G(\lambda_1, \chi)^s \ldots G(\lambda_k, \chi)^s =$$

$$= (-1)^{(s-1)\,k}(-1)^{-(s-1)}\left(-\frac{1}{q}G(\lambda_1, \chi)\ldots G(\lambda_k, \chi)\right)^s =$$
$$= (-1)^{(s-1)\,(k-1)}J(\lambda_1, \ldots, \lambda_k)^s. \quad \square$$

Для случая $k = 2$, который часто встречается в приложениях сумм Якоби, можно установить несколько результатов, представляющих особый интерес. Мы снова будем употреблять понятие порядка мультипликативного характера, введенное в замечании 5.13.

5.27. **Теорема.** *Пусть λ — мультипликативный характер поля $\mathbb{F}_q$, имеющий порядок $m \geqslant 2$, и пусть χ — нетривиальный аддитивный характер того же поля. Тогда*

$$G(\lambda, \chi)^m = \lambda(-1)\,qJ(\lambda, \lambda)\,J(\lambda, \lambda^2)\ldots J(\lambda, \lambda^{m-2}). \quad (5.49)$$

Доказательство. Сначала допустим, что $m \geqslant 3$. Тогда из (5.43) получим

$$\frac{G(\lambda, \chi)\,G(\lambda^j, \chi)}{G(\lambda^{j+1}, \chi)} = J(\lambda, \lambda^j) \quad \text{для} \quad 1 \leqslant j \leqslant m-2.$$

Перемножая между собой все эти $m-2$ равеиств, получим

$$\frac{G(\lambda, \chi)^{m-1}}{G(\lambda^{m-1}, \chi)} = J(\lambda, \lambda)\,J(\lambda, \lambda^2)\ldots J(\lambda, \lambda^{m-2}). \quad (5.50)$$

Так как λ^m — тривиальный характер, то $\lambda^{m-1} = \bar{\lambda}$, откуда в силу теоремы 5.12 (iv)

$$G(\lambda, \chi)\,G(\lambda^{m-1}, \chi) = \lambda(-1)\,q. \quad (5.51)$$

Перемножая равенства (5.50) и (5.51), получаем требуемый результат. Если же $m = 2$, то пустое произведение сумм Якоби в правой части интерпретируется как 1, и тогда результат содержится в равенстве (5.51). $\square$

Другой результат для $k = 2$ приводит к замечательному соотношению между суммами Гаусса. Для аддитивных характеров будем употреблять обозначения, введенные в теореме 5.7.

5.28. **Теорема** (соотношение Дэвенпорта—Хассе). *Пусть λ и ψ — мультипликативные характеры поля $\mathbb{F}_q$, причем λ имеет порядок $m \geqslant 2$, а характер ψ^m нетривиален, и пусть χ_b — нетривиальный аддитивный характер того же поля. Тогда*

$$\frac{G(\psi, \chi_b)^m}{G(\psi^m, \chi_{mb})} = \prod_{j=1}^{m-1} J(\psi, \lambda^j).$$

5.29. Следствие. *Пусть выполнены условия теоремы* 5.28. *Тогда для нечетного* m *имеет место равенство*

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = q^{(m-1)/2} G(\psi^m, \chi_{mb}), \tag{5.52}$$

а для четного m *имеет место равенство*

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = (-1)^{(q-1)(m-2)/8} q^{(m-2)/2} G(\eta, \chi_b) G(\psi^m, \chi_{mb}), \tag{5.53}$$

где η *— квадратичный характер поля* $\mathbb{F}_q$.

Прежде всего мы выведем указанное следствие из теоремы 5.28. Заметим сначала, что каждый характер $\psi\lambda^j$, $0 \leqslant j \leqslant m-1$, нетривиален, так как в противном случае характер $(\psi\lambda^j)^m = \psi^m\lambda^{jm} = \psi^m$ был бы тривиален, что противоречит предположению. Поэтому мы можем применить к равенству из теоремы 5.28 соотношение (5.43), и это дает

$$\frac{G(\psi, \chi_b)^m}{G(\psi^m, \chi_{mb})} = G(\psi, \chi_b)^{m-1} \prod_{j=1}^{m-1} \frac{G(\lambda^j, \chi_b)}{G(\psi\lambda^j, \chi_b)}.$$

Переупорядочение членов приводит к следующему равенству:

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = G(\psi^m, \chi_{mb}) \prod_{j=1}^{m-1} G(\lambda^j, \chi_b). \tag{5.54}$$

Если m — нечетное число, то

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = \prod_{j=1}^{(m-1)/2} G(\lambda^j, \chi_b) G(\lambda^{m-j}, \chi_b),$$

и так как λ^m — тривиальный характер, то $\lambda^{m-j} = \bar{\lambda}^j$, поэтому, применяя теорему 5.12 (iv), получаем

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = q^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \lambda^j(-1).$$

Согласно замечанию 5.13, $\lambda(-1) = 1$, поэтому

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = q^{(m-1)/2}.$$

С учетом (5.54) это дает (5.52).

Если же число m четно, то, вновь применяя теорему 5.12 (iv), получаем

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = G(\lambda^{m/2}, \chi_b) \prod_{j=1}^{(m-2)/2} G(\lambda^j, \chi_b) G(\lambda^{m-j}, \chi_b) =$$

$$= G(\eta, \chi_b) \prod_{j=1}^{(m-2)/2} G(\lambda^j, \chi_b) G(\overline{\lambda^j}, \chi_b) =$$

$$= q^{(m-2)/2} G(\eta, \chi_b) \prod_{j=1}^{(m-2)/2} \lambda^j(-1).$$

Из замечания 5.13 следует, что $\lambda(-1) = 1$, если число $(q-1)/m$ четно, и $\lambda(-1) = -1$, если $(q-1)/m$ нечетно; поэтому $\lambda(-1) = (-1)^{(q-1)/m}$. Таким образом,

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = q^{(m-2)/2} G(\eta, \chi_b) \prod_{j=2}^{(m-2)/2} (-1)^{j(q-1)/m} =$$

$$= q^{(m-2)/2} G(\eta, \chi_b) (-1)^{(q-1)(m-2)/8},$$

и вместе с (5.54) это дает (5.53). □

Известные доказательства теоремы 5.28 основаны на теории алгебраических чисел или на теории конечных расширений поля рациональных функций над полем $\mathbb{F}_q$ (называемых *полями алгебраических функций* над $\mathbb{F}_q$). Но для некоторых частных случаев удается дать и элементарное доказательство, например для случая, когда ψ — квадратичный характер или когда число m является степенью числа 2. Приведем эти доказательства.

Рассмотрим сначала случай, когда ψ совпадает с квадратичным характером η поля $\mathbb{F}_q$. В этом случае оба числа m и q должны быть нечетными. Мы докажем равенство из теоремы 5.28, если убедимся в справедливости эквивалентного ему равенства (5.52). Преобразуем левую часть равенства (5.52):

$$\prod_{j=0}^{m-1} G(\eta\lambda^j, \chi_b) = G(\eta, \chi_b) \prod_{j=1}^{(m-1)/2} G(\eta\lambda^j, \chi_b) G(\eta\lambda^{m-j}, \chi_b) =$$

$$= G(\eta, \chi_b) \prod_{j=1}^{(m-1)/2} G(\eta\lambda^j, \chi_b) G(\overline{\eta\lambda^j}, \chi_b) =$$

$$= G(\eta, \chi_b) q^{(m-1)/2} \prod_{j=1}^{(m-1)/2} (\eta\lambda^j)(-1)$$

согласно теореме 5.12 (iv). Поскольку в силу замечания 5.13 $\lambda(-1) = 1$ и $\eta(-1) = (-1)^{(q-1)/2}$, то

$$\prod_{j=0}^{m-1} G(\eta\lambda^j, \chi_b) = q^{(m-1)/2} (-1)^{(q-1)(m-1)/4} G(\eta, \chi_b).$$

Для правой части равенства (5.52) получаем [1])

$$q^{(m-1)/2} G(\eta^m, \chi_{mb}) = q^{(m-1)/2} G(\eta, \chi_{mb}) = q^{(m-1)/2} \eta(m) G(\eta, \chi_b),$$

[1]) Под m как элементом поля $\mathbb{F}_q$ понимается вычет по модулю p, принадлежащий простому подполю $\mathbb{F}_p$ поля $\mathbb{F}_q$. — *Прим. перев.*

согласно теореме 5.12 (i), так что остается показать, что

$$\eta(m) = (-1)^{(q-1)(m-1)/4}. \tag{5.55}$$

Пусть p — характеристика поля $\mathbb{F}_q$ и $q = p^s$. Так как квадратичный характер η поля $\mathbb{F}_q$ можно получить подиятием (в смысле теоремы 5.14) квадратичного характера η_p поля $\mathbb{F}_p$, то

$$\eta(m) = \eta_p\left(N_{\mathbb{F}_q/\mathbb{F}_p}(m)\right) = \eta_p(m^s).$$

Пусть $m = r_1 \dots r_t$, где r_i — простые нечетные числа (не обязательно различные), которые отличны от p (поскольку m делит число $q - 1$). Тогда

$$\eta(m) = [\eta_p(r_1) \dots \eta_p(r_t)]^s = \left[\left(\frac{r_1}{p}\right) \dots \left(\frac{r_t}{p}\right)\right]^s,$$

так как η_p задается символом Лежандра (см. пример 5.10). Из квадратичного закона взаимности (теорема 5.17) получаем

$$\eta(m) = \left[\left(\frac{p}{r_1}\right)(-1)^{(p-1)(r_1-1)/4} \dots \left(\frac{p}{r_t}\right)(-1)^{(p-1)(r_t-1)/4}\right]^s =$$

$$= \left(\frac{q}{r_1}\right) \dots \left(\frac{q}{r_t}\right)[(-1)^{us}]^{(p-1)/2},$$

где

$$u = \frac{r_1 - 1}{2} + \dots + \frac{r_t - 1}{2}$$

и для квадратичного характера η_{r_i} поля $\mathbb{F}_{r_i}$

$$\left(\frac{p}{r_i}\right)^s = \eta_{r_i}(p)^s = \eta_{r_i}(p^s) = \left(\frac{q}{r_i}\right).$$

Заметим, что

$$\frac{q-1}{p-1} = p^{s-1} + p^{s-2} + \dots + p + 1 \equiv s \pmod 2.$$

Кроме того, для двух нечетных чисел v и w

$$\frac{vw-1}{2} - \frac{v-1}{2} - \frac{w-1}{2} = \frac{(v-1)(w-1)}{2} \equiv 0 \pmod 2,$$

так что

$$\frac{v-1}{2} + \frac{w-1}{2} \equiv \frac{vw-1}{2} \pmod 2.$$

Применяя это повторно, получаем

$$u = \frac{r_1 - 1}{2} + \dots + \frac{r_t - 1}{2} \equiv \frac{r_1 \dots r_t - 1}{2} \equiv \frac{m-1}{2} \pmod 2.$$

Это приводит к сравнению

$$us \equiv \frac{m-1}{2} \cdot \frac{q-1}{p-1} \pmod 2,$$

и отсюда получаем

$$\eta(m) = \left(\frac{q}{r_1}\right) \dots \left(\frac{q}{r_t}\right) (-1)^{(q-1)\ (m-1)/4}.$$

Но

$$\left(\frac{q}{r_i}\right) = 1 \quad \text{для} \quad i = 1, \dots, t,$$

так как из $q \equiv 1 \pmod m$ следует $q \equiv 1 \pmod{r_i}$. Таким образом, равенство (5.55), а значит, и соотношение Дэвенпорта—Хассе для указанного частного случая установлены.

Теперь докажем соотношение Дэвенпорта—Хассе для случая, когда число m является степенью числа 2. Если $m = 2$, то λ совпадает с квадратичным характером η поля $\mathbb{F}_q$, и число q нечетно. Из (5.43) и теоремы 5.12 (i) получаем

$$\begin{aligned}\frac{G(\psi, \chi_b)^2}{G(\psi^2, \chi_{2b})} &= \frac{G(\psi, \chi_b)^2}{\bar{\psi}(4)\, G(\psi^2, \chi_b)} = \\ &= \psi(4)\, J(\psi, \psi) = \psi(4) \sum_{c_1 + c_2 = 1} \psi(c_1)\, \psi(c_2) = \\ &= \psi(4) \sum_{c \in \mathbb{F}_q} \psi(c - c^2).\end{aligned}$$

Для фиксированиого элемента $d \in \mathbb{F}_q$ уравнение $x - x^2 = d$ имеет или два решения в поле $\mathbb{F}_q$ (если $1 - 4d$ является квадратом некоторого элемента из $\mathbb{F}_q^*$), или одно решение в $\mathbb{F}_q$ (если $1 - 4d = 0$), или вообще не имеет решений в $\mathbb{F}_q$ (если $1 - 4d$ не является квадратом какого-либо элемеита из $\mathbb{F}_q$). Отсюда получаем, что число решений уравнения $x - x^2 = d$ в поле $\mathbb{F}_q$ задается выражением $1 + \eta(1 - 4d)$. Следовательно,

$$\begin{aligned}\frac{G(\psi, \chi_b)^2}{G(\psi^2, \chi_{2b})} &= \psi(4) \sum_{d \in \mathbb{F}_q} (1 + \eta(1 - 4d))\, \psi(d) = \\ &= \psi(4) \sum_{d \in \mathbb{F}_q} \psi(d) + \sum_{d \in \mathbb{F}_q} \psi(4d)\, \eta(1 - 4d) = \\ &= J(\psi, \eta),\end{aligned}$$

где на последнем шаге использовано равенство (5.37). Таким образом, для случая $m = 2$ соотношение Дэвенпорта—Хассе доказано.

Теперь пусть число $m \geqslant 4$ является степенью числа 2, и предположим, что соотношение Дэвенпорта—Хассе в форме (5.53) уже доказано для всех меньших степеней двойки. Воспользовавшись этим соотношением для степени числа 2, равной $m/2$, получим

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = \prod_{j=0}^{(m/2)-1} G(\psi\lambda^{2j}, \chi_b) \prod_{j=0}^{(m/2)-1} G(\psi\lambda\lambda^{2j}, \chi_b) =$$

$$= (-1)^{(q-1)\,(m-4)/16}\, q^{(m-4)/4} G(\eta, \chi_b)\, G(\psi^{m/2}, \chi_{(m/2)\,b}) \cdot$$
$$\cdot (-1)^{(q-1)\,(m-4)/16}\, q^{(m-4)/4} G(\eta, \chi_b)\, G(\psi^{m/2}\eta, \chi_{(m/2)\,b}) =$$
$$= q^{(m-4)/2} G(\eta, \chi_b)^2\, G(\psi^{m/2}, \chi_{(m/2)\,b})\, G(\psi^{m/2}\eta, \chi_{(m/2)\,b}).$$

Так как, согласно теореме 5.12 (iv), $G(\eta, \chi_b)^2 = \eta(-1)\, q$ и в силу замечания 5.13 $\eta(-1) = (-1)^{(q-1)/2}$, то

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = (-1)^{(q-1)/2}\, q^{(m-2)/2} G(\psi^{m/2}, \chi_{(m/2)\,b})\, G(\psi^{m/2}\eta, \chi_{(m/2)\,b}).$$

Пользуясь равенством (5.53) при $m = 2$, получаем

$$G(\psi^{m/2}, \chi_{(m/2)\,b})\, G(\psi^{m/2}\eta, \chi_{(m/2)\,b}) = G(\eta, \chi_{(m/2)\,b})\, G(\psi^m, \chi_{mb}),$$

а применение теоремы 5.12 (i) дает [1])

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = (-1)^{(q-1)/2}\, q^{(m-2)/2} \eta\left(\frac{m}{2}\right) G(\eta, \chi_b)\, G(\psi^m, \chi_{mb}). \tag{5.56}$$

Сначала найдем $\eta(2)$. Так как $q^2 \equiv 1 \pmod 8$, то существует элемент $\gamma \in \mathbb{F}_{q^2}^*$ порядка 8. Тогда $\gamma^4 = -1$, откуда $(\gamma + \gamma^{-1})^2 = \gamma^{-2}(\gamma^4 + 1) + 2 = 2$. Следовательно, 2 является квадратом некоторого элемента поля $\mathbb{F}_q$ в том и только том случае, если $\gamma + \gamma^{-1} \in \mathbb{F}_q$, т. е. если $(\gamma + \gamma^{-1})^q = \gamma + \gamma^{-1}$. Последнее условие эквивалентно равенству $\gamma^q + \gamma^{-q} = \gamma + \gamma^{-1}$, а значит, и равенству $(\gamma^{q+1} - 1)(\gamma^{q-1} - 1) = 0$. А это означает, что либо $\gamma^{q+1} = 1$, либо $\gamma^{q-1} = 1$. Но поскольку элемент γ имеет порядок 8, мы получаем, что $\eta(2) = 1$ тогда и только тогда, когда $q \equiv \pm 1 \pmod 8$. В остальных случаях $\eta(2) = -1$.

Чтобы найти $\eta(m/2)$, заметим, что если $m \geqslant 8$, то должно быть [2]) $q \equiv 1 \pmod 8$, т. е. $\eta(m/2) = 1$. Если же $m = 4$, то $q \equiv 1 \pmod 4$, так что либо $\eta(2) = 1$ (если $q \equiv 1 \pmod 8$), либо $\eta(2) = -1$ (если $q \equiv 5 \pmod 8$). В любом случае можно написать, что

$$\eta\left(\frac{m}{2}\right) = (-1)^{(q-1)\,(m-6)/8}.$$

А отсюда и из (5.56) вытекает справедливость равенства (5.53). Таким образом, соотношение Дэвенпорта—Хассе установлено для случая, когда число m является степенью числа 2.

---

[1]) $m/2$ рассматривается как элемент поля $\mathbb{F}_q$. — *Прим. перев.*

[2]) Порядок $m = 2^s$, $s \geqslant 3$, мультипликативного характера λ поля $\mathbb{F}_q$ должен делить число $q - 1$, согласно теореме 5.5. — *Прим. перев.*

§ 4. Суммы значений характеров с полиномиальными аргументами

Пусть χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, и пусть задан многочлен $f \in \mathbb{F}_q[x]$ положительной степени. Рассмотрим сумму вида

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)),$$

которую называют иногда *суммой Вейля*. Задача точного вычисления таких сумм очень сложна. Поэтому обычно ограничиваются оценкой абсолютной величины такой суммы.

Но для некоторых частных случаев удается провести исследование этих сумм элементарным образом. Например, если f — линейный многочлен, то из (5.9) легко получить, что такая сумма равна нулю. Исследование случая, когда f является двучленом, опирается на следующее соотношение между суммами Гаусса, представляющее и самостоятельный интерес.

5.30. Теорема. *Пусть n — натуральное число, χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$ и λ — мультипликативный характер того же поля, имеющий порядок $d = \text{НОД}(n, q-1)$. Тогда*

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = \chi(b) \sum_{j=1}^{d-1} \bar{\lambda}^j(a) G(\lambda^j, \chi)$$

для всех a, $b \in \mathbb{F}_q$, $a \neq 0$.

Доказательство. Пусть τ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, определенный условием $\tau(c) = \chi(ac)$ для $c \in \mathbb{F}_q$. Тогда

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = \chi(b) \sum_{c \in \mathbb{F}_q} \chi(ac^n) = \chi(b) \sum_{c \in \mathbb{F}_q} \tau(c^n). \quad (5.57)$$

Согласно (5.17),

$$\tau(c^n) = \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \tau) \psi(c^n) \quad \text{для} \quad c \in \mathbb{F}_q^*,$$

где сумма берется по всем мультипликативным характерам поля $\mathbb{F}_q$. Таким образом,

$$\sum_{c \in \mathbb{F}_q} \tau(c^n) = \tau(0) + \sum_{c \in \mathbb{F}_q^*} \tau(c^n) = 1 + \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \tau) \sum_{c \in \mathbb{F}_q^*} \psi^n(c).$$

Внутренняя сумма в последнем выражении в силу (5.12) либо равна $q-1$ (если ψ^n — тривиальный характер), либо равна 0 (если характер ψ^n нетривиален). Характер же ψ^n тривиален тогда

и только тогда, когда порядок характера ψ делит число d. Поскольку характер $\bar{\lambda}$ имеет порядок d, то все характеры ψ, порядки которых делят число d, должны иметь вид $\psi = \bar{\lambda}^j$, $j = 0, 1, \ldots, d-1$. Поэтому, учитывая (5.14), получаем

$$\sum_{c \in \mathbb{F}_q} \tau(c^n) = 1 + \sum_{j=0}^{d-1} G(\lambda^j, \tau) = \sum_{j=1}^{d-1} G(\lambda^j, \tau).$$

Отсюда на основании (5.57) и теоремы 5.12 (i) вытекает искомый результат. □

5.31. Следствие. *Если χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$ и* НОД $(n, q-1) = 1$, *то*

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = 0$$

для любых $a, b \in \mathbb{F}_q$, $a \neq 0$.

5.32. Теорема. *Пусть χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, $n \in \mathbb{N}$ и $d =$* НОД $(n, q-1)$. *Тогда*

$$\left| \sum_{c \in \mathbb{F}_q} \chi(ac^n + b) \right| \leqslant (d-1) q^{1/2}$$

для любых $a, b \in \mathbb{F}_q$, $a \neq 0$.

Доказательство. Утверждение сразу вытекает из теоремы 5.30 и равенства (5.15). □

Особенно простой вид принимает теорема 5.30 для $n = 2$ и нечетного q. Этим можно воспользоваться при подсчете сумм характеров для любых квадратных многочленов над полем нечетной характеристики.

5.33. Теорема. *Пусть χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, где q нечетно, и пусть $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$, $a_2 \neq 0$. Тогда*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \chi\left(a_0 - a_1^2 (4a_2)^{-1}\right) \eta(a_2) G(\eta, \chi),$$

где η — квадратичный характер поля $\mathbb{F}_q$.

Доказательство. Для $c \in \mathbb{F}_q$

$$f(c) = a_2c^2 + a_1c + a_0 = a_2\left[c + a_1 (2a_2)^{-1}\right]^2 + a_0 - a_1^2 (4a_2)^{-1}.$$

Таким образом, полагая $c_1 = c + a_1 (2a_2)^{-1}$, $b = a_0 - a_1^2 (4a_2)^{-1}$ и применяя теорему 5.30, получим, что

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \sum_{c_1 \in \mathbb{F}_q} \chi\left(a_2c_1^2 + b\right) = \chi(b) \eta(a_2) G(\eta, \chi).$$ □

Суммы значений характеров подобного вида можно вычислить в явном виде также для случая, когда f является аффинным p-многочленом над полем $\mathbb{F}_q$ (см. определение 3.54).

5.34. Теорема. *Пусть конечное поле $\mathbb{F}_q$ имеет характеристику p и*

$$f(x) = a_r x^{p^r} + a_{r-1}x^{p^{r-1}} + \cdots + a_1 x^p + a_0 x + a$$

— некоторый аффинный p-многочлен над $\mathbb{F}_q$. Тогда для любого нетривиального аддитивного характера χ_b, $b \in \mathbb{F}_q^*$, поля $\mathbb{F}_q$, (в обозначениях теоремы 5.7) имеет место соотношение

$$\sum_{c \in \mathbb{F}_q} \chi_b(f(c)) =$$

$$= \begin{cases} \chi_b(a)\, q, & \text{если } ba_r + b^p a_{r-1}^p + \cdots + b^{p^{r-1}} a_1^{p^{r-1}} + b^{p^r} a_0^{p^r} = 0, \\ 0 & \text{в противном случае} \end{cases}$$

Доказательство. Имеем

$$\sum_{c \in \mathbb{F}_q} \chi_b(f(c)) = \chi_b(a) \sum_{c \in \mathbb{F}_q} \chi_1(L(c)),$$

где

$$L(x) = ba_r x^{p^r} + ba_{r-1}x^{p^{r-1}} + \cdots + ba_1 x^p + ba_0 x$$

есть p-многочлен над полем $\mathbb{F}_q$. Если мы положим $\tau(c) = \chi_1(L(c))$ для всех $c \in \mathbb{F}_q$, то из (3.11) следует, что τ — аддитивный характер поля $\mathbb{F}_q$. Таким образом,

$$\sum_{c \in \mathbb{F}_q} \chi_1(L(c)) = \sum_{c \in \mathbb{F}_q} \tau(c) = \begin{cases} q, & \text{если } \tau \text{ тривиален,} \\ 0 & \text{в противном случае.} \end{cases}$$

Остается охарактеризовать те p-миогочлены $L(x)$, для которых характер τ тривиален. Пусть $q = p^s$, а Tr — функция абсолютного следа из $\mathbb{F}_q$ в $\mathbb{F}_p$. Тогда в соответствии с определением (5.6) характер τ тривиален тогда и только тогда, когда

$$\mathrm{Tr}(L(c)) = \sum_{j=0}^{s-1} L(c)^{p^j} = 0 \quad \text{для всех } c \in \mathbb{F}_q.$$

Указанные равенства выполияются в том и только том случае, когда имеет место полииомиальное сравнение

$$\sum_{j=0}^{s-1} L(x)^{p^j} \equiv 0 \pmod{(x^q - x)}. \tag{5.58}$$

Далее,

$$\sum_{j=0}^{s-1} L(x)^{p^j} = \sum_{j=0}^{s-1} \left(\sum_{i=0}^{r} ba_i x^{p^i} \right)^{p^j} = \sum_{j=0}^{s-1} \sum_{i=0}^{r} b^{p^j} a_i^{p^j} x^{p^{i+j}},$$

и поскольку при $m \equiv n \pmod{s}$ выполняется равенство $c^{p^m} = c^{p^n}$ для всех $c \in \mathbb{F}_q$, а также имеет место сравнение $x^{p^m} \equiv x^{p^n} \pmod{(x^q - x)}$, то

$$\sum_{j=0}^{s-1} L(x)^{p^j} \equiv \sum_{k=0}^{s-1} \left(\sum_{i=0}^{r} b^{p^{k-i}} a_i^{p^{k-i}} \right) x^{p^k} \pmod{(x^q - x)}.$$

Таким образом, сравнение (5.58) выполняется тогда и только тогда, когда

$$\sum_{i=0}^{r} b^{p^{k-i}} a_i^{p^{k-i}} = 0 \quad \text{для} \quad k = 0, 1, \ldots, s-1.$$

А это равенство выполняется тогда и только тогда, когда

$$\sum_{i=0}^{r} b^{p^{r-i}} a_i^{p^{r-i}} = \left(\sum_{i=0}^{r} b^{p^{k-i}} a_i^{p^{k-i}} \right)^{p^{r-k}} = 0,$$

что и завершает доказательство. □

Теорема 5.34 содержит, в частности (при $p = 2$, $r = 1$), формулу для вычисления сумм значений характеров того же вида, что и в теореме 5.33, но для случая, который там не рассматривался, а именно для четного q.

5.35. Следствие. *Пусть* $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$, *где* q *четно, и пусть* χ_b, $b \in \mathbb{F}_q^*$, — *нетривиальный аддитивный характер поля* $\mathbb{F}_q$. *Тогда*

$$\sum_{c \in \mathbb{F}_q} \chi_b(f(c)) = \begin{cases} \chi_b(a_0)q, & \text{если } a_2 = ba_1^2, \\ 0 & \text{в противном случае,} \end{cases}$$

Обратимся теперь к общему методу получения оценок для сумм значений характеров с полиномиальными аргументами. Так как случай линейного многочлена тривиален, то можно считать, что степень многочлена не ниже двух. Следующий результат является основным. Напомним, что поднятие $\chi^{(s)}$ аддитивного характера χ поля $\mathbb{F}_q$ до расширения $E = \mathbb{F}_{q^s}$ этого поля вводится при помощи соотношения $\chi^{(s)}(\beta) = \chi(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta))$ для $\beta \in E$.

5.36. Теорема. *Пусть* $f \in \mathbb{F}_q[x]$ — *многочлен степени* $n \geqslant 2$, *причем* НОД $(n, q) = 1$, *и пусть* χ — *нетривиальный аддитивный характер поля* $\mathbb{F}_q$. *Тогда существуют такие комплексные числа* $\omega_1, \ldots, \omega_{n-1}$, *зависящие только от* f *и* χ, *что для любого натурального числа* s *имеет место равенство*

$$\sum_{\gamma \in \mathbb{F}_{q^s}} \chi^{(s)}(f(\gamma)) = -\omega_1^s - \cdots - \omega_{n-1}^s.$$

Доказательство. Пусть $f(x) = b_n x^n + \ldots + b_1 x + b_0$, где $b_n \neq 0$. Для фиксированного натурального числа $k \geqslant 1$ тогда

$$f(x_1) + \ldots + f(x_k) = b_n s_n(x_1, \ldots, x_k) + \ldots + b_1 s_1(x_1, \ldots, x_k) + k b_0, \tag{5.59}$$

где

$$s_j(x_1, \ldots, x_k) = x_1^j + \ldots + x_k^j, \quad 1 \leqslant j \leqslant n,$$

Для $1 \leqslant r \leqslant k$ пусть $\sigma_r = \sigma_r(x_1, \ldots, x_k)$ есть r-й элементарный симметрический многочлен от переменных $x_1, \ldots, x_r$ над полем $\mathbb{F}_q$ (см. пример 1.74). Тогда для $j \geqslant 1$ мы получим, используя формулу Варинга (см. теорему 1.76), равенство

$$s_j(x_1, \ldots, x_k) = \sum (-1)^{i_2+i_4+i_6+\ldots} \frac{(i_1+i_2+\cdots+i_k-1)!\, j}{i_1!\, i_2! \ldots i_k!} \sigma_1^{i_1} \sigma_2^{i_2} \ldots \sigma_k^{i_k},$$

где суммирование ведется по всем k-наборам $(i_1, \ldots, i_k)$ неотрицательных целых чисел, таких, что $i_1 + 2i_2 + \ldots + k i_k = j$. Для $j = 1$ мы имеем $s_1(x_1, \ldots, x_k) = \sigma_1$. Для $2 \leqslant j \leqslant k$ существует одно решение уравнения $i_1 + 2i_2 + \ldots + k i_k = j$, в котором $i_j = 1$, а все остальные i_r равны 0; слагаемое, соответствующее этому решению, равно $(-1)^{j-1} j\sigma_j$. Для остальных решений уравнения $i_1 + 2i_2 + \ldots + k i_k = j$ обязательно $i_j = i_{j+1} = \ldots = i_k = 0$, так что соответствующие им слагаемые могут содержать лишь симметрические многочлены $\sigma_1, \sigma_2, \ldots, \sigma_{j-1}$. Поэтому

$$s_1(x_1, \ldots, x_k) = \sigma_1,$$

$$s_j(x_1, \ldots, x_k) = (-1)^{j-1} j\sigma_j + G_j(\sigma_1, \ldots, \sigma_{j-1}) \quad \text{при} \quad 2 \leqslant j \leqslant k,$$

$$s_j(x_1, \ldots, x_k) = H_j(\sigma_1, \ldots, \sigma_k) \quad \text{при} \quad j > k,$$

где G_j — многочлен от $j-1$ переменных, а H_j — многочлен от k переменных над $\mathbb{F}_q$. Из (5.59) тогда получаем, что

$$f(x_1) + \cdots + f(x_k) = \begin{cases} (-1)^{n-1} n b_n \sigma_n + G(\sigma_1, \ldots, \sigma_{n-1}) & \text{при } k \geqslant n, \\ H(\sigma_1, \ldots, \sigma_k) & \text{при } 1 \leqslant k \leqslant n-1, \end{cases} \tag{5.60}$$

где G — многочлен от $n-1$ переменных, а H — многочлен от k переменных над $\mathbb{F}_q$.

Определим теперь функцию λ из множества Φ всех нормированных многочленов над полем $\mathbb{F}_q$ в множество комплексных чисел с модулем, равным единице, следующим образом. Положим $\lambda(1) = 1$. Далее, если многочлен g принадлежит подмножеству Φ_k множества Φ, состоящему из многочленов степени $k \geqslant 1$, и разложение этого многочлена в поле его разложения над $\mathbb{F}_q$ имеет вид $g(x) = (x - \alpha_1) \ldots (x - \alpha_k)$, то положим

$$\lambda(g) = \chi(f(\alpha_1) + \ldots + f(\alpha_k)).$$

Заметим, что поскольку $\sigma_r(\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_q$, $1 \leqslant r \leqslant k$, то из (5.60) следует, что $f(\alpha_1) + \ldots + f(\alpha_k) \in \mathbb{F}_q$. Взяв другой многочлен h из Φ, для которого $h(x) = (x - \beta_1) \ldots (x - \beta_m)$, получим

$$\begin{aligned}\lambda(gh) &= \chi(f(\alpha_1) + \ldots + f(\alpha_k) + f(\beta_1) + \ldots + f(\beta_m)) = \\ &= \chi(f(\alpha_1) + \ldots + f(\alpha_k))\,\chi(f(\beta_1) + \ldots + f(\beta_m)) = \\ &= \lambda(g)\,\lambda(h),\end{aligned}$$

так что условие (5.18) мультипликативности функции λ выполняется. Рассмотрим теперь сумму

$$\sum_{g \in \Phi_k} \lambda(g)$$

для фиксированного $k \geqslant n$. Для многочлена

$$g(x) = x^k + \sum_{r=1}^{k} (-1)^r a_r x^{k-r} = (x - \alpha_1) \ldots (x - \alpha_k) \in \Phi_k$$

мы имеем $\sigma_r(\alpha_1, \ldots, \alpha_k) = a_r$, $r = 1, \ldots, k$, так что из (5.60) следует, что

$$f(\alpha_1) + \ldots + f(\alpha_k) = (-1)^{n-1} n b_n a_n + G(a_1, \ldots, a_{n-1}).$$

Поскольку НОД $(n, q) = 1$, то $b = (-1)^{n-1} n b_n \neq 0$, а значит,

$$\begin{aligned}\sum_{g \in \Phi_k} \lambda(g) &= \sum_{a_1, \ldots, a_k \in \mathbb{F}_q} \chi(b a_n + G(a_1, \ldots, a_{n-1})) = \\ &= q^{k-n} \sum_{a_1, \ldots, a_n \in \mathbb{F}_q} \chi(b a_n)\,\chi(G(a_1, \ldots, a_{n-1})) = \\ &= q^{k-n} \Big(\sum_{a_n \in \mathbb{F}_q} \chi(b a_n)\Big)\Big(\sum_{a_1, \ldots, a_{n-1} \in \mathbb{F}_q} \chi(G(a_1, \ldots, a_{n-1}))\Big) = 0\end{aligned}$$

согласно (5.9). Таким образом, условие (5.22) выполняется при $t = n - 1$. Поэтому из (5.24) следует существование комплексных чисел $\omega_1, \ldots, \omega_{n-1}$, таких, что

$$L_s = -\sum_{j=1}^{n-1} \omega_j^s, \quad s = 1, 2, \ldots, \tag{5.61}$$

где L_s введено условием (5.20).

Вычислим теперь L_s по формуле (5.21). Согласно этой формуле,

$$L_s = \sum_g \deg(g)\,\lambda(g^{s/\deg(g)}),$$

где суммирование ведется по всем нормированным неприводимым многочленам g из $\mathbb{F}_q[x]$, степени $\deg(g)$ которых делят число s. Для такого многочлена g пусть $\gamma \in E = \mathbb{F}_{q^s}$ — некоторый его

корень. Тогда многочлен $g^{s/\deg(g)}$ является характеристическим многочленом элемента γ над $\mathbb{F}_q$, так что в силу (2.1)

$$g(x)^{s/\deg(g)} = (x-\gamma)(x-\gamma^q)(x-\gamma^{q^2})\ \dots\ (x-\gamma^{q^{s-1}}),$$

откуда следует, что

$$\lambda(g^{s/\deg(g)}) = \chi(f(\gamma)+f(\gamma^q)+\dots+f(\gamma^{q^{s-1}})).$$

Последнее выражение, очевидно, не изменится, если элемент γ заменить любым из различных сопряженных с ним элементов γ^q, γ^{q^2}, ..., $\gamma^{q^{\deg(g)-1}}$; поэтому можно написать

$$\deg(g)\lambda(g^{s/\deg(g)}) = \sum_{\substack{\gamma\in E\\ g(\gamma)=0}} \chi(f(\gamma)+f(\gamma^q)+\dots+f(\gamma^{q^{s-1}}))$$

и

$$L_s = \sum_g \sum_{\substack{\gamma\in E\\ g(\gamma)=0}} \chi(f(\gamma)+f(\gamma^q)+\dots+f(\gamma^{q^{s-1}})) =$$
$$= \sum_{\gamma\in E} \chi(f(\gamma)+f(\gamma^q)+\dots+f(\gamma^{q^{s-1}})).$$

Но поскольку

$$\chi(f(\gamma)+f(\gamma^q)+\dots+f(\gamma^{q^{s-1}})) = \chi(f(\gamma)+f(\gamma)^q+\dots+f(\gamma)^{q^{s-1}}) =$$
$$= \chi(\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma))) = \chi^{(s)}(f(\gamma)),$$

то

$$L_s = \sum_{\gamma\in E} \chi^{(s)}(f(\gamma)),$$

и утверждение теоремы теперь вытекает из (5.61). □

5.37. Теорема. *Все комплексные числа* $\omega_1, \dots, \omega_{n-1}$ *из теоремы* 5.36 *по модулю равны* $q^{1/2}$.

Первоначально теорема 5.37 была установлена глубокими методами алгебраической геометрии. Более элементарное доказательство было получено с использованием теории уравнений над конечными полями. В следующей главе мы докажем более слабое утвержденне, а именно что $|\omega_j| \leqslant q^{1/2}$, $j = 1, \dots, n-1$ (см. теорему 6.60), которое вполне достаточно для приложений к оценке сумм значенний характеров.

5.38. Теорема (теорема Вейля). *Пусть* $f \in \mathbb{F}_q[x]$ — *многочлен степени* $n \geqslant 1$, *причем* НОД $(n, q) = 1$, *и пусть* χ — *нетривиальный аддитивный характер поля* $\mathbb{F}_q$. *Тогда*

$$\left|\sum_{c\in\mathbb{F}_q} \chi(f(c))\right| \leqslant (n-1)q^{1/2}.$$

Доказательство. Случай $n = 1$ тривиален. При $n \geqslant 2$ можно применить теорему 5.36. Получим

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = -\omega_1 - \cdots - \omega_{n-1}.$$

Используя теорему 5.37 или более простое утверждение, что $|\omega_j| \leqslant q^{1/2}$, $j = 1, \ldots, n-1$ (теорему 6.60), мы получаем требуемое неравенство. □

Чтобы гарантировать выполнение теоремы Вейля, на многочлен f приходится наложить определенное ограничение. Заметим, что если НОД $(n, q) > 1$, т. е. если степень $\deg(f)$ многочлена f делится на характеристику p поля $\mathbb{F}_q$, то могут возникнуть определенные осложнения. Рассмотрим, например, случай, когда $f(x) = x^p - x$ и $\chi = \chi_1$ — канонический аддитивный характер поля $\mathbb{F}_q$, определенный условием (5.6). Тогда в силу свойства функции абсолютного следа, полученного в теореме 2.23 (v), $\chi_1(f(c)) = 1$ для всех $c \in \mathbb{F}_q$, так что оценка в теореме Вейля неверна при $q \geqslant p^2$. В более общем случае аналогичная ситуация возникает, когда многочлен f имеет вид $f = g^p - g + b$, где $g \in \mathbb{F}_q[x]$ и $b \in \mathbb{F}_q$. Однако если f имеет вид, отличный от приведенного, то оценка в теореме Вейля для такого многочлена f сохраняет силу, даже если его степень делится на характеристику p поля $\mathbb{F}_q$ (см. комментарии).

Применяя аналогичную технику, мы можем исследовать и суммы мультипликативных характеров. При этом снова целесообразно расширить область определения мультипликативного характера ψ поля $\mathbb{F}_q$ до всего этого поля, положив $\psi(0) = 0$ для нетривиального и $\psi(0) = 1$ для тривиального характера ψ. Кроме того, следует заметить, что любой мультипликативный характер ψ поля $\mathbb{F}_q$ можно поднять до расширения $E = \mathbb{F}_{q^s}$ поля $\mathbb{F}_q$, воспользовавшись формулой $\psi^{(s)}(\beta) = \psi(N_{E/\mathbb{F}_q}(\beta))$ для $\beta \in E$.

5.39. Теорема. *Пусть ψ — мультипликативный характер порядка $m > 1$ поля $\mathbb{F}_q$, и пусть $f \in \mathbb{F}_q[x]$ — нормированный многочлен положительной степени, который не является m-й степенью какого-либо многочлена. Пусть d — число различных корней многочлена f в его поле разложения над $\mathbb{F}_q$, причем $d \geqslant 2$. Тогда существуют такие комплексные числа $\omega_1, \ldots, \omega_{d-1}$, зависящие лишь от f и ψ, что для любого натурального числа s имеет место равенство:*

$$\sum_{\gamma \in \mathbb{F}_{q^s}} \psi^{(s)}(f(\gamma)) = -\omega_1^s - \ldots - \omega_{d-1}^s.$$

Доказательство. Мы пойдем тем же путем, что и при доказательстве теоремы 5.36. Определим функцию λ из множества Φ

всех нормированных многочленов над полем $\mathbb{F}_q$ в множество комплексных чисел с модулем, не превосходящим 1, положив сначала $\lambda(1) = 1$. Обозначив через Φ_k подмножество множества Φ, состоящее из многочленов степени k, рассмотрим для многочлена $g \in \Phi_k$, $k \geqslant 1$, результант $R(g, f)$ при формальных степенях, совпадающих со степенями g и f (см. определение 1.93). Тогда $R(g, f) \in \mathbb{F}_q$, и мы положим $\lambda(g) = \psi(R(g, f))$. Если разложение многочлена g в его поле разложения над $\mathbb{F}_q$ имеет вид $g(x) = (x - \alpha_1) \dots (x - \alpha_k)$, то, согласно формуле (1.10), $R(g, f) = f(\alpha_1) \dots f(\alpha_k)$, так что можно написать

$$\lambda(g) = \psi(f(\alpha_1) \dots f(\alpha_k)).$$

Тогда условие мультипликативности функции (5.18), очевидно, выполняется. Пусть

$$f = f_1^{e_1} \dots f_r^{e_r}$$

— каноническое разложение многочлена f в $\mathbb{F}_q[x]$, где $f_1, \dots, f_r$ — различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$. Согласно упр. 1.66, $R(g, f) = (-1)^{kn} R(f, g)$, где $n = \deg(f)$. Вновь применяя формулу (1.10), получим

$$R(g, f) = (-1)^{kn} R(f_1, g)^{e_1} \dots R(f_r, g)^{e_r}. \tag{5.62}$$

Пусть $d_i = \deg(f_i)$ для $1 \leqslant i \leqslant r$, E_i — расширение поля $\mathbb{F}_q$, такое, что $[E_i : \mathbb{F}_q] = d_i$, и β_i — некоторый фиксированный корень многочлена f_i в E_i. Тогда все корни многочлена f_i задаются сопряженными с β_i относительно поля $\mathbb{F}_q$ элементами, так что

$$R(f_i, g) = g(\beta_i) g\left(\beta_i^q\right) \dots g\left(\beta_i^{q^{d_i-1}}\right) = \mathrm{N}_{E_i/\mathbb{F}_q}(g(\beta_i)), \quad 1 \leqslant i \leqslant r.$$

С учетом (5.62) мы получим

$$\lambda(g) = \psi\left((-1)^{kn}\right) \psi^{e_1}\left(\mathrm{N}_{E_1/\mathbb{F}_q}(g(\beta_1))\right) \dots \psi^{e_r}\left(\mathrm{N}_{E_r/\mathbb{F}_q}(g(\beta_r))\right) =$$
$$= \varepsilon_k \tau_1(g(\beta_1)) \dots \tau_r(g(\beta_r)), \tag{5.63}$$

где $\varepsilon_k = \psi\left((-1)^{kn}\right)$ и для $1 \leqslant i \leqslant r$ τ_i — поднятие мультипликативного характера ψ^{e_i} до поля E_i. Так как по предположению многочлен f не является m-й степенью другого многочлена, то по крайней мере одно из чисел e_i не кратно m; значит, по крайней мере один из характеров ψ^{e_i}, а следовательно, и характер τ_i нетривиальны. Рассмотрим теперь сумму

$$\sum_{g \in \Phi_k} \lambda(g)$$

для $k \geqslant d$. Заметим, что $d = d_1 + \ldots + d_r$. Пусть отображение S: $\Phi_k \to E_1 \times \ldots \times E_r$ определено условием

$$S(g) = (g(\beta_1), \ldots, g(\beta_r)) \quad \text{для} \quad g \in \Phi_k.$$

Пусть задан r-набор $(\nu_1, \ldots, \nu_r) \in E_1 \times \ldots \times E_r$. Каждый элемент ν_i, $1 \leqslant i \leqslant r$, можно представить в виде $\nu_i = h_i(\beta_i)$, где $h_i \in \mathbb{F}_q[x]$. Равенство $S(g) = (\nu_1, \ldots, \nu_r)$ выполняется тогда и только тогда, когда многочлен g является решением системы сравнений

$$g \equiv h_i \pmod{f_i}, \quad i = 1, \ldots, r.$$

На основаиии китайской теоремы об остатках (см. упр. 1.37) эта система сравнений имеет единственное решение $G \in \mathbb{F}_q[x]$ степени $\deg(G) < d_1 + \ldots + d_r = d$. В таком случае все решения $g \in \Phi_k$ этой системы имеют вид $g = Ff_1 \ldots f_r + G$, где F — произвольный нормированный многочлен над $\mathbb{F}_q$ степени $k - d$. Поскольку существует ровно q^{k-d} возможностей выбора этого многочлена F, то существует в точности q^{k-d} таких многочленов $g \in \Phi_k$, что $S(g) = (g(\beta_1), \ldots, g(\beta_r)) = (\nu_1, \ldots, \nu_r)$. Используя этот факт и равенство (5.36), получаем, что

$$\sum_{g \in \Phi_k} \lambda(g) = \varepsilon_k q^{k-d} \sum_{\substack{\nu_1, \ldots, \nu_r \\ \nu_i \in E_i}} \tau_1(\nu_1) \ldots \tau_r(\nu_r) =$$

$$= \varepsilon_k q^{k-d} \left(\sum_{\nu_1 \in E_1} \tau_1(\nu_1) \right) \ldots \left(\sum_{\nu_r \in E_r} \tau_r(\nu_r) \right) = 0,$$

так как хотя бы один из характеров τ_i нетривиален (как было отмечено ранее). Таким образом, условие (5.22) выполнено при $t = d - 1$. Поэтому из (5.24) следует, что существуют комплексные числа $\omega_1, \ldots, \omega_{d-1}$, такие, что

$$L_s = -\sum_{j=1}^{d-1} \omega_j^s, \quad s = 1, 2, \ldots .$$

Теперь подсчитаем L_s по формуле (5.21), используя тот же прием, что и при доказательстве теоремы 5.36. При $E = \mathbb{F}_{q^s}$ получаем

$$L_s = \sum_{\gamma \in E} \psi\left(f(\gamma) f(\gamma^q) \ldots f(\gamma^{q^{s-1}})\right),$$

и поскольку

$$\psi\left(f(\gamma) f(\gamma^q) \ldots f(\gamma^{q^{s-1}})\right) = \psi\left(f(\gamma) f(\gamma)^q \ldots f(\gamma)^{q^{s-1}}\right) =$$

$$= \psi\left(\mathrm{N}_{E/\mathbb{F}_q}(f(\gamma))\right) = \psi^{(s)}(f(\gamma)),$$

то можно написать

$$L_s = \sum_{\gamma \in E} \psi^{(s)}(f(\gamma)),$$

что и завершает доказательство. □

5.40. Теорема. *Все комплексные числа* $\omega_1, \ldots, \omega_{d-1}$ *из теоремы* 5.39 *по модулю равны* $q^{1/2}$.

Замечания, сделанные после теоремы 5.37, справедливы также и по отношению к теореме 5.40. В частности, элементарное доказательство более слабого утверждения, а именно что $|\omega_j| \leqslant q^{1/2}$, $j = 1, \ldots, d-1$, будет дано в следующей главе (см. теорему 6.56).

5.41. Теорема. *Пусть* ψ *— мультипликативный характер поля* $\mathbb{F}_q$, *имеющий порядок* $m > 1$, *и пусть* $f \in \mathbb{F}_q[x]$ *— нормированный многочлен положительной степени, не являющийся* m*-й степенью другого многочлена. Если* d *— число различных корней многочлена* f *в его поле разложения над* $\mathbb{F}_q$, *то для каждого* $a \in \mathbb{F}_q$ *выполняется неравенство*

$$\left| \sum_{c \in \mathbb{F}_q} \psi(af(c)) \right| \leqslant (d-1) q^{1/2}.$$

Доказательство. Случай $d = 1$ легко проверяется, так что можно предположить, что $d \geqslant 2$. Тогда, применяя теорему 5.39, получаем

$$\sum_{c \in \mathbb{F}_q} \psi(af(c)) = \psi(a) \sum_{c \in \mathbb{F}_q} \psi(f(c)) = -\psi(a)(\omega_1 + \ldots + \omega_{d-1}).$$

Теперь, используя либо теорему 5.40, либо ее ослабленную форму $|\omega_j| \leqslant q^{1/2}$, $j = 1, \ldots, d-1$ (теорему 6.56), мы получаем требуемое неравенство. □

В случае, который не покрывается теоремой 5.41 (а именно когда многочлен f является m-й степенью некоторого другого многочлена), приведенная в этой теореме оценка не всегда справедлива. Например, если $f = g^m$ и многочлен $g \in \mathbb{F}_q[x]$ не имеет корней в поле $\mathbb{F}_q$, то $\psi(f(c)) = \psi^m(g(c)) = 1$ для всех $c \in \mathbb{F}_q$, так как ψ^m — тривиальный характер, и поэтому оценка в теореме 5.41, вообще говоря, неверна (левая часть равна q).

Случай, когда ψ — квадратичный характер, будет подробно рассмотрен в следующем параграфе.

§ 5. Дальнейшие результаты о суммах значений характеров

Сначала рассмотрим один тип сумм значений характеров, который допускает исследование методами предыдущего параграфа и представляет интерес для теории чисел.

5.42. Определение. Пусть χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, и пусть $a, b \in \mathbb{F}_q$. Сумма вида

$$K(\chi; a, b) = \sum_{c \in \mathbb{F}_q^*} \chi(ac + bc^{-1})$$

называется *суммой Клостермана*.

Случаи, когда $ab = 0$, тривиальны. Если $a = b = 0$, то $K(\chi; a, b) = q - 1$, а если лишь одно из чисел a или b равно 0, то $K(\chi; a, b) = -1$. Вообще заметим, что сумма Клостермана всегда принимает действительные значения, так как если $K = K(\chi; a, b)$ и $\overline{K}$ — его комплексно-сопряженное, то

$$\overline{K} = \sum_{c \in \mathbb{F}_q^*} \chi(-ac - bc^{-1}) = \sum_{c \in \mathbb{F}_q^*} \chi(a(-c) + b(-c)^{-1}) = K,$$

поскольку элемент $-c$ при этом тоже пробегает все множество $\mathbb{F}_q^*$.

Как и в § 4, мы через $\chi^{(s)}$ будем обозначать поднятие аддитивного характера χ до расширения $\mathbb{F}_{q^s}$ поля $\mathbb{F}_q$.

5.43. Теорема. *Пусть χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$ и $a, b \in \mathbb{F}_q$, причем $ab \neq 0$. Тогда существуют такие числа ω_1 и ω_2, зависящие лишь от χ, a и b (которые либо оба действительные, либо комплексно-сопряженные), что для каждого натурального числа s выполняется равенство*

$$K(\chi^{(s)}; a, b) = \sum_{\gamma \in \mathbb{F}_{q^s}^*} \chi^{(s)}(a\gamma + b\gamma^{-1}) = -\omega_1^s - \omega_2^s.$$

Доказательство. Метод доказательства тот же, что и для теорем 5.36 и 5.39. Определим функцию λ из множества Φ всех нормированных многочленов в множество комплексных чисел, модуль которых не превосходит единицы, следующим образом. Как и раньше, через Φ_k обозначим подмножество Φ, состоящее из многочленов степени k. Положим $\lambda(1) = 1$. Далее, если многочлен $g \in \Phi_k$, $k \geqslant 1$, имеет вид

$$g(x) = \sum_{r=0}^{k} (-1)^r c_r x^{k-r}, \quad c_0 = 1,$$

то положим $\lambda(g) = 0$, если $c_k = 0$, и

$$\lambda(g) = \chi(ac_1 + bc_{k-1}c_k^{-1}), \quad \text{если } c_k \neq 0.$$

Легко проверить, что $\lambda(gh) = \lambda(g)\lambda(h)$ для всех $g, h \in \Phi$. Для $k \geqslant 3$

$$\sum_{g \in \Phi_k} \lambda(g) = \sum_{c_1, c_{k-1} \in \mathbb{F}_q} \sum_{c_k \in \mathbb{F}_q^*} \chi\left(ac_1 + bc_{k-1}c_k^{-1}\right) =$$

$$= q^{k-3}\left(\sum_{c_1 \in \mathbb{F}_q} \chi(ac_1)\right) \sum_{c_{k-1} \in \mathbb{F}_q} \sum_{c_k \in \mathbb{F}_q^*} \chi\left(bc_{k-1}c_k^{-1}\right) = 0,$$

так что условие (5.22) выполнено при $t = 2$. Из (5.19) получаем

$$L(z) = 1 + \left(\sum_{g \in \Phi_1} \lambda(g)\right) z + \left(\sum_{g \in \Phi_2} \lambda(g)\right) z^2.$$

При $K = K(\chi; a, b)$ имеем

$$\sum_{g \in \Phi_1} \lambda(g) = \sum_{c \in \mathbb{F}_q^*} \chi(ac + bc^{-1}) = K.$$

Кроме того,

$$\sum_{g \in \Phi_2} \lambda(g) = \sum_{c_2 \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q} \chi\left(c_1\left(a + bc_2^{-1}\right)\right) = q,$$

так как внутренняя сумма равна q при $c_2 = -a^{-1}b$ и равна 0 в остальных случаях. Таким образом, $L(z) = 1 + Kz + qz^2 = (1 - \omega_1 z)(1 - \omega_2 z)$, где ω_1 и ω_2 либо оба действительные числа, либо комплексно-сопряженные, так как многочлен $L(z)$ имеет действительные коэффициенты. Согласно (5.24),

$$L_s = -\omega_1^s - \omega_2^s \quad \text{для всех } s = 1, 2, \ldots. \tag{5.64}$$

Остается оценить L_s. Из (5.21) мы получаем

$$L_s = \sum_g \deg(g)\lambda\left(g^{s/\deg(g)}\right) = \sum_g{}^* \deg(g)\lambda\left(g^{s/\deg(g)}\right),$$

где сумма берется по всем нормированным неприводимым многочленам g из $\mathbb{F}_q[x]$, степень которых делит число s, а звездочка означает, что из области суммирования исключается многочлен $g(x) = x$. Каждый такой многочлен g имеет $\deg(g)$ различных ненулевых корней в поле $E = \mathbb{F}_{q^s}$, и характеристическим многочленом любого корня γ многочлена g будет многочлен

$$g(x)^{s/\deg(g)} = (x - \gamma)(x - \gamma^q) \ldots \left(x - \gamma^{q^{s-1}}\right).$$

Пусть, скажем,

$$g(x)^{s/\deg(g)} = x^s - c_1 x^{s-1} + \ldots + (-1)^{s-1} c_{s-1}(x) + (-1)^s c_s.$$

Тогда $c_1 = \mathrm{Tr}_{E/\mathbb{F}_q}(\gamma)$, $c_s = \gamma\gamma^q \ldots \gamma^{q^{s-1}}$ и

$$c_{s-1}c_s^{-1} = \gamma^{-1} + \gamma^{-q} + \ldots + \gamma^{-q^{s-1}} = \mathrm{Tr}_{E/\mathbb{F}_q}\left(\gamma^{-1}\right).$$

Поэтому

$$\lambda(g^{s/\deg(g)}) = \chi\left(a\,\mathrm{Tr}_{E/\mathbb{F}_q}(\gamma) + b\,\mathrm{Tr}_{E/\mathbb{F}_q}(\gamma^{-1})\right) = \chi^{(s)}(a\gamma + b\gamma^{-1}),$$

так что

$$L_s = \sum_g{}^{*} \deg(g)\,\lambda(g^{s/\deg(g)}) = \sum_g{}^{*} \sum_{\substack{\gamma \in E \\ g(\gamma)=0}} \chi^{(s)}(a\gamma + b\gamma^{-1}).$$

Если многочлен g пробегает указанную выше область суммнрования, то элемент γ пробегает в точности все элементы множества E^*. Таким образом,

$$L_s = \sum_{\gamma \in E^*} \chi^{(s)}(a\gamma + b\gamma^{-1}) = K(\chi^{(s)};\ a,\ b),$$

и требуемый результат вытекает из (5.64). □

5.44. Теорема. *Числа* ω_1 *и* ω_2 *из теоремы* 5.43 *удовлетворяют условию* $|\omega_1| = |\omega_2| = q^{1/2}$.

Элементарное доказательство теоремы 5.44, использующее теорию уравнеиий над конечными полями, дается в примере 6.63 для нечетного q.

5.45. Теорема. *Если* χ — *нетривиальный аддитивный характер поля* $\mathbb{F}_q$ *и один из элементов* $a,\ b \in \mathbb{F}_q$ *не равен нулю, то сумма Клостермана* $K(\chi;\ a,\ b)$ *удовлетворяет неравенству*

$$|K(\chi;\ a,\ b)| \leqslant 2q^{1/2}.$$

Доказательство. В силу замечания, следующего за определением 5.42, результат тривиален, если одно из чисел a или b равно нулю. Если же $ab \neq 0$, то из теоремы 5.43 получаем $K(\chi;\ a,\ b) = -\omega_1 - \omega_2$, так что требуемое неравенство вытекает из теоремы 5.44. □

Теорему 5.43 можно использовать для доказательства редукционной формулы, связывающей «поднятую» сумму Клостермана $K(\chi^{(s)};\ a,\ b)$ для расширения $\mathbb{F}_{q^s}$ поля $\mathbb{F}_q$, определяемую в этой теореме, с суммой Клостермана $K(\chi;\ a,\ b)$ для основного поля $\mathbb{F}_q$.

5.46. Теорема. *Пусть* χ — *нетривиальный аддитивный характер поля* $\mathbb{F}_q$, *и пусть* $a,\ b \in \mathbb{F}_q$, *причем* $ab \neq 0$, *и* $K = K(\chi;\ a,\ b)$. *Тогда для любого натурального числа* s *имеет место равенство*

$$K(\chi^{(s)};\ a,\ b) = \sum_{j=0}^{\lfloor s/2 \rfloor} (-1)^{s-j-1} \frac{s}{s-j} \binom{s-j}{j} q^j K^{s-2j},$$

где $\lfloor s/2 \rfloor$ — *наибольшее целое число, не превосходящее* $s/2$.

Доказательство. Симметрический многочлен $x_1^s + x_2^s$ можно выразить через элементарные симметрические многочлены $x_1 + x_2$ и x_1x_2 с помощью формулы Варинга (см. теорему 1.76). Это дает

$$x_1^s + x_2^s = \sum_{i_1+2i_2=s} (-1)^{i_2} \frac{(i_1+i_2-1)!\,s}{i_1!\,i_2!} (x_1+x_2)^{i_1} (x_1x_2)^{i_2},$$

где i_1 и i_2 — неотрицательные целые числа. Полагая $i_1 = s - 2j$ и $i_2 = j$, получим

$$x_1^s + x_2^s = \sum_{j=0}^{\lfloor s/2 \rfloor} (-1)^j \frac{s}{s-j} \binom{s-j}{j} (x_1+x_2)^{s-2j} (x_1x_2)^j.$$

Теперь применим теорему 5.43 и подставим в полученное выше равенство $x_1 = \omega_1$ и $x_2 = \omega_2$. Заметим, что $\omega_1^s + \omega_2^s = -K(\chi^{(s)}; a, b)$ и $\omega_1 + \omega_2 = -K$, а также что $\omega_1\omega_2 = q$ в силу равенства $1 + Kz + qz^2 = (1 - \omega_1 z)(1 - \omega_2 z)$, устаиовленного при доказательстве теоремы 5.43. Отсюда сразу вытекает требуемая формула. □

Для суммы Клостермана $K^{(s)} = K(\chi^{(s)}; a, b)$ можно вывести также рекуррентное соотношение. Из соотношения

$$\omega_1^s + \omega_2^s = (\omega_1^{s-1} + \omega_2^{s-1})(\omega_1 + \omega_2) - (\omega_1^{s-2} + \omega_2^{s-2})\omega_1\omega_2$$

и теоремы 5.43 сразу вытекает, что

$$K^{(s)} = -K^{(s-1)}K - K^{(s-2)}q \quad \text{для } s \geqslant 2,$$

где мы полагаем $K^{(0)} = -2$ и $K^{(1)} = K = K(\chi; a, b)$.

Если число q нечетно, то нетривиальные суммы Клостермана можно связать с квадратичным характером η поля $\mathbb{F}_q$. Мы сиова для удобства полагаем $\eta(0) = 0$.

5.47. Теорема. *Если χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$ нечетной характеристики и $a, b \in \mathbb{F}_q$ — элементы, не равные нулю одновременно, то сумма Клостермана $K(\chi; a, b)$ представима в следующем виде:*

$$K(\chi; a, b) = \sum_{c \in \mathbb{F}_q} \chi(c)\,\eta(c^2 - 4ab),$$

где η — квадратичный характер поля $\mathbb{F}_q$.

Доказательство. Если одно из чисел a или b равно нулю, то $K(\chi; a, b) = -1$, что, как нетрудно убедиться, совпадает со значением правой части равеиства из формулнровки теоремы. Если же $ab \neq 0$, то можно написать

$$K(\chi; a, b) = \sum_{c \in \mathbb{F}_q^*} \chi(ac + bc^{-1}) = \sum_{d \in \mathbb{F}_q} \chi(d)\,N(d),$$

где $N(d)$ — число элементов $c \in \mathbb{F}_q^*$, для которых $ac + bc^{-1} = d$. Последнее уравнение эквивалентно квадратному уравнению $ac^2 - dc + b = 0$. Следовательно, $N(d)$ принимает значения 2, 1 или 0 в зависимости от того, принимает ли квадратичный характер $\eta(d^2 - 4ab)$ значения 1, 0 или -1 соответственно. Другими словами, $N(d) = 1 + \eta(d^2 - 4ab)$. Отсюда вытекает, что

$$K(\chi; a, b) = \sum_{d \in \mathbb{F}_q} \chi(d)(1 + \eta(d^2 - 4ab)) =$$
$$= \sum_{d \in \mathbb{F}_q} \chi(d) + \sum_{d \in \mathbb{F}_q} \chi(d)\eta(d^2 - 4ab) =$$
$$= \sum_{d \in \mathbb{F}_q} \chi(d)\eta(d^2 - 4ab),$$

где на последнем шаге использовано равенство (5.9). □

Теперь мы перейдем к рассмотрению сумм, содержащих только квадратичный характер η поля $\mathbb{F}_q$, где q нечетно, и имеющих полиномиальные аргументы, т. е. сумм вида

$$\sum_{c \in \mathbb{F}_q} \eta(f(c)), \tag{5.65}$$

где $f \in \mathbb{F}_q[x]$. Случай линейного многочлена f тривиален, а для квадратного многочлена f можно установить еще одну явную формулу.

5.48. Теорема. *Пусть над полем $\mathbb{F}_q$ нечетной характеристики задан квадратный многочлен $f(x) = a_2x^2 + a_1x + a_0$, где $a_2 \neq 0$. Если η — квадратичный характер поля $\mathbb{F}_q$ и $d = a_1^2 - 4a_0a_2$, то справедлива формула*

$$\sum_{c \in \mathbb{F}_q} \eta(f(c)) = \begin{cases} -\eta(a_2), & \text{если } d \neq 0, \\ (q-1)\eta(a_2), & \text{если } d = 0. \end{cases}$$

Доказательство. Умножая сумму $\sum_{c \in \mathbb{F}_q} \eta(f(c))$ на $\eta(4a_2^2) = 1$, получаем

$$\sum_{c \in \mathbb{F}_q} \eta(f(c)) = \eta(a_2) \sum_{c \in \mathbb{F}_q} \eta(4a_2^2c^2 + 4a_1a_2c + 4a_0a_2) =$$
$$= \eta(a_2) \sum_{c \in \mathbb{F}_q} \eta((2a_2c + a_1)^2 - d) = \eta(a_2) \sum_{b \in \mathbb{F}_q} \eta(b^2 - d). \tag{5.66}$$

Для случая $d = 0$ результат получается сразу. Для $d \neq 0$ можно написать

$$\sum_{b \in \mathbb{F}_q} \eta(b^2 - d) = -q + \sum_{b \in \mathbb{F}_q} (1 + \eta(b^2 - d)),$$

и так как величина $1 + \eta(b^2 - d)$ равна числу элементов $c \in \mathbb{F}_q$, таких, что $c^2 = b^2 - d$, то

$$\sum_{b \in \mathbb{F}_q} \eta(b^2 - d) = -q + S(d), \tag{5.67}$$

где $S(d)$ — число упорядоченных пар (b, c), таких, что $b, c \in \mathbb{F}_q$ и $b^2 - c^2 = d$. Чтобы решить последнее уравнение, положим $b + c = u$, $b - c = v$ и заметим, что между упорядоченными парами (b, c) и (u, v) существует взаимно однозначное соответствие, поскольку q нечетно. Таким образом, $S(d)$ равно числу упорядоченных пар (u, v), где $u, v \in \mathbb{F}_q$ и $uv = d$; отсюда видно, что $S(d) = q - 1$. С учетом (5.66) и (5.67) это дает требуемую формулу. □

5.49. Определение. Пусть η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики, $a \in \mathbb{F}_q^*$ и n — натуральное число. Сумма вида

$$H_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^{n+1} + ac) = \sum_{c \in \mathbb{F}_q} \eta(c)\,\eta(c^n + a)$$

называется *суммой Якобсталя*.

Из теоремы 5.48 вытекает, что $H_1(a) = -1$ для всех $a \in \mathbb{F}_q^*$. Вместе с суммой Якобсталя $H_n(a)$ можно рассмотреть сходную сумму

$$I_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^n + a), \tag{5.68}$$

которая связана с $H_n(a)$ следующим образом.

5.50. Теорема. *Для всех элементов $a \in \mathbb{F}_q^*$, где q нечетно, и натуральных чисел n выполняется тождество*

$$I_{2n}(a) = I_n(a) + H_n(a).$$

Доказательство. Имеем

$$I_{2n}(a) = \sum_{c \in \mathbb{F}_q} \eta(c^{2n} + a) = \sum_{d \in \mathbb{F}_q} N(d)\,\eta(d^n + a),$$

где $N(d)$ — число элементов $c \in \mathbb{F}_q$, таких, что $c^2 = d$. Но $N(d) = 1 + \eta(d)$, так что

$$I_{2n}(a) = \sum_{d \in \mathbb{F}_q} (1 + \eta(d))\,\eta(d^n + a) = I_n(a) + H_n(a). \qquad \square$$

Суммы $I_n(a)$ легко подсчитываются для $n = 1$ и $n = 2$. Получаем $I_1(a) = 0$ и $I_2(a) = -1$ для всех $a \in \mathbb{F}_q^*$, где второе равенство вытекает либо из теоремы 5.48, либо из теоремы 5.50. В общем же случае суммы $I_n(a)$ можно выражать через суммы Якоби.

5.51. Теорема. *Пусть $\mathbb{F}_q$ — поле нечетной характеристики. Тогда для всех $a \in \mathbb{F}_q^*$ и всех натуральных чисел n выполняется равенство*

$$I_n(a) = \eta(a) \sum_{j=1}^{d-1} \lambda^j(-a) J(\lambda^j, \eta),$$

где λ — некоторый мультипликативный характер порядка $d =$ = НОД $(n, q-1)$ поля $\mathbb{F}_q$, а η — квадратичный характер этого поля.

Доказательство. Сумму $I_n(a)$ можно представить в следующем виде:

$$I_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^n + a) = \sum_{b \in \mathbb{F}_q} \eta(b + a) M(b), \tag{5.69}$$

где $M(b)$ — число элементов $c \in \mathbb{F}_q$, таких, что $c^n = b$. Для $b \neq 0$, используя (5.13), получим

$$M(b) = \frac{1}{q-1} \sum_{c \in \mathbb{F}_q^*} \sum_{\psi} \psi(c^n) \bar{\psi}(b) = \frac{1}{q-1} \sum_{\psi} \bar{\psi}(b) \sum_{c \in \mathbb{F}_q^*} \psi^n(c).$$

Согласно (5.12), внутренняя сумма в последнем выраженни равна $q-1$, если характер ψ^n тривиален, и равна 0, если ψ^n нетривиален. Но рассуждение из доказательства теоремы 5.30 показывает, что характер ψ^n тривиален тогда и только тогда, когда $\psi = \bar{\lambda}^j$, $j = 0, 1, \ldots, d-1$. Поэтому

$$M(b) = \sum_{j=0}^{d-1} \lambda^j(b), \tag{5.70}$$

и так как $M(0) = 1$, то равенство (5.70) выполняется также и для $b = 0$. Объединяя (5.69) и (5.70) и применяя (5.38), получаем

$$I_n(a) = \sum_{b \in \mathbb{F}_q} \eta(b + a) \sum_{j=0}^{d-1} \lambda^j(b) = \eta(-1) \sum_{j=0}^{d-1} \sum_{b \in \mathbb{F}_q} \lambda^j(b) \eta(-b - a) =$$

$$= \eta(-1) \sum_{j=0}^{d-1} J_{-a}(\lambda^j, \eta) = \eta(-1) \sum_{j=0}^{d-1} (\lambda^j \eta)(-a) J(\lambda^j, \eta) =$$

$$= \eta(a) \sum_{j=0}^{d-1} \lambda^j(-a) J(\lambda^j, \eta).$$

На основании (5.40) член, соответствующий $j = 0$, можно опустить. □

5.52. Теорема. *Пусть $\mathbb{F}_q$ — поле нечетной характеристики, $a \in \mathbb{F}_q^*$ и $n \in \mathbb{N}$. Тогда сумма Якобсталя $H_n(a)$ равна нулю,*

если наибольшая степень числа 2, делящая число $q-1$, делит также n. В противном случае имеет место равенство.

$$H_n(a) = \eta(a)\lambda(-1)\sum_{j=0}^{d-1}\lambda^{2j+1}(a)J(\lambda^{2j+1}, \eta),$$

где $d = \text{НОД}(n, q-1)$, λ — некоторый мультипликативный характер порядка $2d$ поля $\mathbb{F}_q$, η — квадратичный характер этого поля и J — сумма Якоби.

Доказательство. По теореме 5.50 имеем $H_n(a) = I_{2n}(a) - I_n(a)$. Если наибольшая степень числа 2, делящая $q-1$, делит также n, то $\text{НОД}(2n, q-1) = \text{НОД}(n, q-1)$, и из теоремы 5.51 следует, что $H_n(a) = 0$. В противном же случае $\text{НОД}(2n, q-1) = 2d$, так что из теоремы 5.51 получаем

$$I_{2n}(a) = \eta(a)\sum_{j=1}^{2d-1}\lambda^j(-a)J(\lambda^j, \eta).$$

Поскольку характер λ^2 имеет порядок d, та же теорема 5.51 показывает, что

$$I_n(a) = \eta(a)\sum_{j=1}^{d-1}\lambda^{2j}(-a)J(\lambda^{2j}, \eta).$$

Это означает, что

$$H_n(a) = \eta(a)\sum_{j=0}^{d-1}\lambda^{2j+1}(-a)J(\lambda^{2j+1}, \eta) =$$
$$= \eta(a)\lambda(-1)\sum_{j=0}^{d-1}\lambda^{2j+1}(a)J(\lambda^{2j+1}, \eta). \qquad \square$$

Из этих результатов и теоремы 5.22 получаются следующие оценки:

$$|I_n(a)| \leqslant (d-1)q^{1/2}, \quad |H_n(a)| \leqslant dq^{1/2},$$

которые не хуже полученных из теоремы 5.41.

5.53. **Пример.** В примере 5.25 мы показали, что каждое простое число p, сравнимое с 1 по модулю 4, можно представить в виде $p = A^2 + B^2$, где A и B — целые числа. Легко видеть, что одно из этих целых чисел, скажем A, должно быть нечетным, а другое должно быть четным. Поскольку знак A можно выбрать произвольным, то можно считать, что $A \equiv -1 \pmod 4$. Покажем теперь, что это число A можно найти непосредственно, используя подходящим образом взятые суммы Якобсталя.

Пусть λ — мультипликативный характер порядка 4 поля $\mathbb{F}_p$. Тогда из равенства $\lambda^3 = \bar{\lambda}$ и теоремы 5.52 следует, что

$$H_2(1) = \lambda(-1)(J(\lambda, \eta) + J(\lambda^3, \eta)) = \lambda(-1)(J(\lambda, \eta) + \overline{J(\lambda, \eta)}) =$$
$$= 2\lambda(-1)\operatorname{Re} J(\lambda, \eta),$$

где $\operatorname{Re} J(\lambda, \eta) = \pm(1/2) H_2(1)$. С другой стороны, в примере 5.25 мы видели, что $p = (\operatorname{Re} J(\lambda, \eta))^2 + (\operatorname{Im} J(\lambda, \eta))^2$. Теперь покажем, что $(1/2) H_2(1) \equiv -1 \pmod 4$. Так как, согласно замечанию 5.13, $\eta(-1) = 1$ для $p \equiv 1 \pmod 4$, то мы можем написать

$$H_2(1) = \sum_{c=1}^{p-1} \eta(c)\,\eta(c^2+1) =$$
$$= \sum_{c=1}^{(p-1)/2} \eta(c)\,\eta(c^2+1) + \sum_{c=1}^{(p-1)/2} \eta(-c)\,\eta(c^2+1) =$$
$$= 2 \sum_{c=1}^{(p-1)/2} \eta(c)\,\eta(c^2+1),$$

так что

$$\frac{1}{2} H_2(1) = \sum_{c=1}^{(p-1)/2} \eta(c)\,\eta(c^2+1). \tag{5.71}$$

Из теоремы 5.48 получаем

$$-1 = \sum_{c=0}^{p-1} \eta(c^2+1) = 1 + 2 \sum_{c=1}^{(p-1)/2} \eta(c^2+1),$$

откуда

$$-1 = \sum_{c=1}^{(p-1)/2} \eta(c^2+1). \tag{5.72}$$

Вычитая (5.72) из (5.71), получим

$$\frac{1}{2} H_2(1) + 1 = \sum_{c=1}^{(p-1)/2} (\eta(c) - 1)\,\eta(c^2+1).$$

Для $1 \leqslant c \leqslant (p-1)/2$

$$(\eta(c) - 1)(\eta(c^2+1) - 1) \equiv 0 \pmod 4, \quad \text{если } \eta(c^2+1) \neq 0,$$

так как оба сомножителя слева четны. Таким образом,

$$(\eta(c) - 1)\,\eta(c^2+1) \equiv \eta(c) - 1 \pmod 4, \quad \text{если } \eta(c^2+1) \neq 0.$$

Случай $\eta(c^2+1) = 0$ имеет место тогда и только тогда, когда $c^2 \equiv -1 \pmod p$, а это сравнение имеет единственное решение c_1, $1 \leqslant c_1 \leqslant (p-1)/2$. Следовательно,

$$\frac{1}{2} H_2(1) + 1 \equiv \sum_{\substack{c=1 \\ c \neq c_1}}^{(p-1)/2} (\eta(c) - 1) \equiv \sum_{c=1}^{(p-1)/2} (\eta(c) - 1) - (\eta(c_1) - 1) \equiv$$
$$\equiv \sum_{c=1}^{(p-1)/2} \eta(c) + \frac{3-p}{2} - \eta(c_1) \pmod 4.$$

Кроме того,

$$0 = \sum_{c=1}^{p-1} \eta(c) = 2 \sum_{c=1}^{(p-1)/2} \eta(c)$$

и $\eta(c_1) = \lambda^2(c_1) = \lambda(c_1^2) = \lambda(-1)$, так что

$$\frac{1}{2} H_2(1) + 1 \equiv \frac{3-p}{2} - \lambda(-1) \pmod 4.$$

Теперь из замечания 5.13 следует, что

$$\lambda(-1) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 8, \\ -1, & \text{если } p \equiv 5 \pmod 8, \end{cases}$$

причем

$$\frac{3-p}{2} \equiv \begin{cases} 1 \pmod 4, & \text{если } p \equiv 1 \pmod 8, \\ -1 \pmod 4, & \text{если } p \equiv 5 \pmod 8, \end{cases}$$

так что $(1/2) H_2(1) + 1 \equiv 0 \pmod 4$ и $(1/2) H_2(1) \equiv -1 \pmod 4$. Значит, $A = (1/2) H_2(1)$.

Можно показать, что при нормировании $A \equiv -1 \pmod 4$ целое число A определяется однозначно. Допустим, что $p = A^2 + B^2 = C^2 + D^2$, где A и C нечетны, а B и D четны. Если $h, k \in \mathbb{Z}$ таковы, что $A \equiv hB \pmod p$, $C \equiv kD \pmod p$, то из $A^2 + B^2 \equiv C^2 + D^2 \equiv 0 \pmod p$ следует, что $h^2 + 1 \equiv k^2 + 1 \equiv 0 \pmod p$, откуда $C \equiv \pm hD \pmod p$. Таким образом, можно написать $C = \pm C_1$, где $C_1 \equiv hD \pmod p$. Тогда в равенстве

$$p^2 = (A^2 + B^2)(C_1^2 + D^2) = (AC_1 + BD)^2 + (AD - BC_1)^2$$

числа в скобках справа кратны p. Деля обе части на p^2, мы получаем выражение, представляющее единицу в виде суммы двух квадратов целых чисел. Это возможно лишь в случае, когда $1 = (\pm 1)^2 + 0^2$. Таким образом, $AD - BC_1 = 0$, и так как НОД $(A, B) =$ НОД $(C_1, D) = 1$, то $A = \pm C_1$, откуда $A = \pm C$. Если, кроме того, $A \equiv C \equiv -1 \pmod 4$, то $A = C$; таким образом, число A однозначно определено.

Выше мы показали, что этим единственным целым числом A является $(1/2) H_2(1)$, и тогда целое число B определяется однозначно с точностью до знака. Используя то же рассуждение, что и в начале этого примера, нетрудно показать, что в качестве числа B можно взять $(1/2) H_2(a)$, где a — такой элемент поля $\mathbb{F}_p$, что $\eta(a) = -1$. □

Существует замечательная связь между суммами значений квадратичного характера η и *алгоритмом разложения в непрерывные дроби* для *рациональных функций* над полем $\mathbb{F}_q$ (т. е. для дробей вида f/g, где $f, g \in \mathbb{F}_q[x]$, $g \neq 0$). Нам понадобятся лишь элементарные сведения из теории таких непрерывных дробей,

которая совершенно аналогична классической теории непрерывных дробей для рациональных чисел. Алгоритм разложения рациональной функции в непрерывную дробь является по существу алгоритмом Евклида, рассмотренным нами в § 3 гл. 1. Мы слегка изменим обозначения с учетом потребностей настоящего момента.

Пусть r_0 и r_1 — два произвольных многочлена из кольца $\mathbb{F}_q[x]$, причем $r_1 \neq 0$. Применяя алгоритм Евклида, можно написать $r_0 = A_0 r_1 + r_2$, $r_1 = A_1 r_2 + r_3$ и вообще

$$r_i = A_i r_{i+1} + r_{i+2} \quad \text{для} \quad i = 0, 1, \ldots, s, \tag{5.73}$$

где $0 \leqslant \deg(r_{i+1}) < \deg(r_i)$ для $i = 1, \ldots, s$, и $r_{s+2} = 0$. Здесь A_0, $A_1, \ldots, A_s$ — некоторые многочлены над полем $\mathbb{F}_q$, причем $A_1, \ldots, A_s$ обязательно имеют положительные степени. Из равенств (5.73) получаем

$$\frac{r_i}{r_{i+1}} = A_i + \frac{1}{r_{i+1}/r_{i+2}} \quad \text{для} \quad i = 0, 1, \ldots, s-1,$$

и $r_s/r_{s+1} = A_s$. Отсюда следует, что

$$\frac{r_0}{r_1} = A_0 + \frac{1}{r_1/r_2},$$

$$\frac{r_0}{r_1} = A_0 + \cfrac{1}{A_1 + \cfrac{1}{r_2/r_3}},$$

и, продолжая таким образом, в конце концов получим

$$\frac{r_0}{r_1} = A_0 + \cfrac{1}{A_1 + \cfrac{1}{A_2 + \ddots + \cfrac{1}{A_s}}} = [A_0, A_1, A_2, \ldots, A_s],$$

где символ в правой части — это сокращенное обозначение разложения в непрерывную дробь, даваемого средним членом равенства. Удобный способ вычисления рациональной функции, представленной непрерывной дробью, основан на следующей рекуррентной процедуре. Определим многочлены P_i и Q_i, $i = -1, 0, \ldots, s$, условиями

$$P_{-1} = 1, \quad P_0 = A_0, \quad P_i = A_i P_{i-1} + P_{i-2} \quad \text{для} \quad i = 1, \ldots, s, \tag{5.74}$$

$$Q_{-1} = 0, \quad Q_0 = 1, \quad Q_i = A_i Q_{i-1} + Q_{i-2} \quad \text{для} \quad i = 1, \ldots, s. \tag{5.75}$$

Ясно, что $\deg(P_{i-1}) < \deg(P_i)$ для $i = 1, \ldots, s$ и $\deg(Q_{i-1}) < \deg(Q_i)$ для $i = 0, 1, \ldots, s$. Следствия 5.55 и 5.58 ниже показывают, что P_i и Q_i являются соответственно числителем и знаменателем (несократимой) рациональной функции, представленной

непрерывной дробью $[A_0, A_1, \ldots, A_i]$; будем P_i/Q_i называть *приведенной формой* непрерывной дроби $[A_0, A_1, \ldots, A_i]$. Полезно распространить определение степени на множество всех рациональных функций, полагая *степенью* рациональной функции $\rho = f/g$ число $\deg(\rho) = \deg(f) - \deg(g)$. При этом условливаются, что $\deg(0) = -\infty$ и $-\infty - n = -\infty$ для любого $n \in \mathbb{Z}$.

5.54. Лемма. *Для любой рациональной функции ρ неотрицательной степени имеет место равенство*

$$[A_0, A_1, \ldots, A_{i-1}, \rho] = \frac{\rho P_{i-1} + P_{i-2}}{\rho Q_{i-1} + Q_{i-2}} \quad \text{для } i = 1, \ldots, s+1.$$

Доказательство. Применим индукцию по i. Для $i = 1$ обе части равны $A_0 + \rho^{-1}$. Если утверждение выполняется для некоторого i, $1 \leqslant i < s+1$, то, поскольку $A_i + \rho^{-1}$ — рациональная функция положительной степени, получим, используя предположение индукции и равенства (5.74) и (5.75),

$$[A_0, A_1, \ldots, A_i, \rho] = [A_0, A_1, \ldots, A_{i-1}, A_i + \rho^{-1}] =$$
$$= \frac{(A_i + \rho^{-1}) P_{i-1} + P_{i-2}}{(A_i + \rho^{-1}) Q_{i-1} + Q_{i-2}} = \frac{P_i + \rho^{-1} P_{i-1}}{Q_i + \rho^{-1} Q_{i-1}} = \frac{\rho P_i + P_{i-1}}{\rho Q_i + Q_{i-1}}. \quad \square$$

5.55. Следствие. *Для любого i, $0 \leqslant i \leqslant s$, имеет место равенство*

$$[A_0, A_1, \ldots, A_i] = \frac{P_i}{Q_i}.$$

Доказательство. Утверждение тривиально для $i = 0$. Для $1 \leqslant i \leqslant s$ положим в лемме 5.54 $\rho = A_i$ и используем (5.74) и (5.75). $\square$

5.56. Лемма. *Для любого i, $0 \leqslant i \leqslant s$, имеет место равенство*

$$\frac{r_0}{r_1} = \frac{P_i + \beta_i P_{i-1}}{Q_i + \beta_i Q_{i-1}},$$

где $\beta_i = r_{i+2}/r_{i+1}$ — рациональная функция отрицательной степени.

Доказательство. Доказываем по индукции. Для $i = 0$

$$\frac{P_0 + \beta_0 P_{-1}}{Q_0 + \beta_0 Q_{-1}} = A_0 + \beta_0 = A_0 + \frac{r_2}{r_1} = \frac{A_0 r_1 + r_2}{r_1} = \frac{r_0}{r_1},$$

где на последнем шаге использовано равенство (5.73). Предполагая доказываемое равенство выполненным для некоторого i, $0 \leqslant i < s$, получаем, в силу (5.74) и (5.75)

$$\frac{P_{i+1} + \beta_{i+1} P_i}{Q_{i+1} + \beta_{i+1} Q_i} = \frac{(A_{i+1} + \beta_{i+1}) P_i + P_{i-1}}{(A_{i+1} + \beta_{i+1}) Q_i + Q_{i-1}},$$

а из (5.73) следует, что $\beta_i^{-1} = A_{i+1} + \beta_{i+1}$. Таким образом,

$$\frac{P_{i+1} + \beta_{i+1}P_i}{Q_{i+1} + \beta_{i+1}Q_i} = \frac{\beta_i^{-1}P_i + P_{i-1}}{\beta_i^{-1}Q_i + Q_{i-1}} = \frac{P_i + \beta_i P_{i-1}}{Q_i + \beta_i Q_{i-1}} = \frac{r_0}{r_1}$$

согласно предположению индукции. Это завершает доказательство. □

5.57. Лемма. *Для любого* i, $0 \leqslant i \leqslant s$, *имеет место равенство*

$$P_iQ_{i-1} - P_{i-1}Q_i = (-1)^{i-1}.$$

Доказательство. Доказываем по индукции. Для $i = 0$ имеем $P_0Q_{-1} - P_{-1}Q_0 = -1$. Допустим, что равенство справедливо для некоторого i, $0 \leqslant i < s$. Тогда, используя (5.74) и (5.75), получим

$$P_{i+1}Q_i - P_iQ_{i+1} = (A_{i+1}P_i + P_{i-1})Q_i - P_i(A_{i+1}Q_i + Q_{i-1}) =$$
$$= -(P_iQ_{i-1} - P_{i-1}Q_i) = (-1)^i$$

согласно предположению индукции. □

5.58. Следствие. *Для любого* i, $0 \leqslant i \leqslant s$, *имеет место равенство* НОД $(P_i, Q_i) = 1$.

Доказательство. Если для $0 \leqslant i \leqslant s$ положить $d_i = $ НОД (P_i, Q_i), то из леммы 5.57 получаем, что многочлен d_i делит $(-1)^{i-1}$, так что $d_i = 1$. □

Теперь мы можем рассмотреть приложения непрерывных дробей к изучению сумм значений квадратичных характеров с полиномиальными аргументами. Пусть $f \in \mathbb{F}_q[x]$ — многочлен положительной степени, не имеющий корней в поле $\mathbb{F}_q$ нечетной характеристики, и пусть $G(x) = x^q - x$. Положим $F(x) = f(x)^{(q-1)/2}$ и рассмотрим разложение в непрерывные дроби следующих двух рациональных функций над $\mathbb{F}_q$:

$$\frac{F(x) - 1}{G(x)} = [A_0, A_1, \ldots, A_s] \tag{5.76}$$

и

$$\frac{F(x) + 1}{G(x)} = [a_0, a_1, \ldots, a_t]. \tag{5.77}$$

Ясно, что $A_0 = a_0$. Определим n_f как наибольшее целое число m, такое, что $A_i = a_i$ для $i = 0, 1, \ldots, m$. Равенства $n_f = s = t$ не могут выполняться, так как в таком случае указанные рациональные функции совпадали бы. Следующий результат, однако, показывает, что представляющие их непрерывные дроби весьма близки.

5.59. Лемма. *При указанных выше условиях имеет место одна из двух возможностей: либо* $n_f = s = t - 1$, *либо* $n_f = t = s - 1$.

Доказательство. Определим P_i и Q_i условиями (5.74) и (5.75) и аналогично определим p_i и q_i, используя a_j вместо A_j в (5.74) и (5.75). Согласно следствиям 5.55 и 5.58, рациональные функции P_s/Q_s и p_t/q_t соответственно являются приведенными формами рациональных функций $(F(x) - 1)/G(x)$ и $(F(x) + 1)/G(x)$, заданных разложениями (5.76) и (5.77), так что

$$Q_s(x) = \frac{b_1 G(x)}{\text{НОД}(F(x) - 1,\ G(x))}, \quad p_t(x) = \frac{b_2 G(x)}{\text{НОД}(F(x) + 1,\ G(x))}, \tag{5.78}$$

где $b_1,\ b_2 \in \mathbb{F}_q^*$. Каждый элемент $c \in \mathbb{F}_q$ является простым корнем многочлена $G(x)$, и других корней $G(x)$ не имеет. С другой стороны, для каждого $c \in \mathbb{F}_q$ по предположению $f(c) \neq 0$, так что $f(c)^{q-1} = 1$, и, следовательно, многочлен $G(x)$ делит $f(x)^{q-1} - 1 = (F(x) - 1)(F(x) + 1)$. Значит,

$$\text{НОД}(F(x) - 1,\ G(x)) \cdot \text{НОД}(F(x) + 1,\ G(x)) = G(x),$$

и из (5.78) вытекает, что

$$Q_s(x)\, q_t(x) = bG(x), \quad \text{где } q = b_1 b_2 \in \mathbb{F}_s^*. \tag{5.79}$$

Пусть $n_f = n$, и предположим, что $n < s$ и $n < t$. Согласно лемме 5.56,

$$\frac{F(x) - 1}{G(x)} = \frac{P_{n+1} + \beta_{n+1} P_n}{Q_{n+1} + \beta_{n+1} Q_n}, \quad \frac{F(x) + 1}{G(x)} = \frac{p_{n+1} + \gamma_{n+1} p_n}{q_{n+1} + \gamma_{n+1} q_n}$$

с рациональными функциями β_{n+1} и γ_{n+1} отрицательной степени. Вычитая первое равенство из второго, получим

$$\frac{2}{G(x)} = \frac{N}{(Q_{n+1} + \beta_{n+1} Q_n)(q_{n+1} + \gamma_{n+1} q_n)}, \tag{5.80}$$

где числитель N имеет вид

$$N = p_{n+1}Q_{n+1} - P_{n+1}q_{n+1} + \beta_{n+1}(p_{n+1}Q_n - P_n q_{n+1}) + \\ + \gamma_{n+1}(p_n Q_{n+1} - P_{n+1} q_n) + \beta_{n+1}\gamma_{n+1}(p_n Q_n - P_n q_n).$$

Из определения числа n вытекает, что $P_i = p_i$ и $Q_i = q_i$ для $i = -1,\ 0,\ \ldots,\ n$. Следовательно, $p_{n+1}Q_n - P_n q_{n+1} = (-1)^n$ и $p_n Q_{n+1} - P_{n+1} q_n = (-1)^{n+1}$ в силу леммы 5.57, а $p_n Q_n - P_n q_n = 0$. Кроме того, простой подсчет с использованием (5.74), (5.75) и леммы 5.57 показывает, что

$$p_{n+1}Q_{n+1} - P_{n+1}q_{n+1} = (-1)^n (A_{n+1} - a_{n+1}).$$

Таким образом, мы получаем

$$N = (-1)^n (A_{n+1} - a_{n+1} + \beta_{n+1} - \gamma_{n+1}).$$

Поскольку из определения числа n следует, что $A_{n+1} \neq a_{n+1}$, то $\deg(N) \geqslant 0$. Сравнение степеней в равенстве (5.80) дает с учетом неравенства $n+1 \leqslant \min\{s, t\}$ и (5.79), что

$$q \leqslant \deg(G) + \deg(N) = \deg(Q_{n+1}) + \deg(q_{n+1}) \leqslant \\ \leqslant \deg(Q_s) + \deg(q_t) = q.$$

Таким образом, здесь всюду должен стоять знак равенства. Поэтому $\deg(N) = 0$ и, следовательно, $\deg(A_{n+1}) = \deg(a_{n+1})$. Тогда мы получаем из (5.75), что $\deg(Q_{n+1}) = \deg(q_{n+1}) = q/2$, а это противоречит предположению о нечетности числа q.

Таким образом, либо $n = s$, либо $n = t$. Допустим, что $n = s$. Тогда $t > 3$, и мы можем написать

$$\frac{F(x)-1}{G(x)} = \frac{P_s}{Q_s}, \qquad \frac{F(x)+1}{G(x)} = \frac{p_{s+1}+\gamma_{s+1}p_s}{q_{s+1}+\gamma_{s+1}q_s}.$$

Снова вычитая первое равенство из второго, получим в силу леммы 5.57

$$\frac{2}{G(x)} = \frac{(-1)^s}{Q_s(q_{s+1}+\gamma_{s+1}q_s)},$$

и сравнение степеней дает

$$q = \deg(Q_s) + \deg(q_{s+1}) \leqslant \deg(Q_s) + \deg(q_t) = q$$

согласно (5.79). Значит, $\deg(q_{s+1}) = \deg(q_t)$, откуда $s+1 = t$, так как степень $\deg(q_i)$ возрастает с i. Аналогично предположение $n = t$ приводит к тому, что $t+1 = s$. □

После этих приготовлений мы можем теперь без труда вывести формулу для сумм значений квадратичного характера η поля $\mathbb{F}_q$ нечетной характеристики, аргументом которого является многочлен $f \in \mathbb{F}_q[x]$. Точный вид этой формулы зависит от того, какой из двух случаев леммы 5.59 имеет место.

5.60. Теорема. *Пусть η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики, и пусть $f \in \mathbb{F}_q[x]$ — многочлен положительной степени, не имеющий корней в поле $\mathbb{F}_q$. Тогда*

$$\sum_{c \in \mathbb{F}_q} \eta(f(c)) = \begin{cases} \deg(a_t), & \text{если } n_f = s, \\ -\deg(A_s), & \text{если } n_f = t, \end{cases}$$

где многочлены A_s и a_t получаются соответственно из (5.76) *и* (5.77).

Доказательство. Обозначим через $N(1)$ (соответственно $N(-1)$) число элементов $c \in \mathbb{F}_q$, таких, что $\eta(f(c))$ равно 1 (соответственно -1). Тогда

$$\sum_{c \in \mathbb{F}_q} \eta(f(c)) = N(1) - N(-1). \tag{5.81}$$

Так как $\eta(f(c))=1$ тогда и только тогда, когда $F(c) = f(c)^{(q-1)/2} = 1$, то $N(1)$ равно степени многочлена НОД $(F(x) - 1, G(x))$, так что $N(1) = q - \deg(Q_s)$ в силу первого из равенств (5.78). Аналогично $N(-1) = q - \deg(q_t)$. Если в лемме 5.59 имеет место случай $n_f = t = s - 1$, то $q_t = Q_t = Q_{s-1}$ и $N(1) - N(-1) = -\deg(Q_s) + \deg(Q_{s-1}) = -\deg(A_s)$ согласно (5.75). В случае же $n_f = s = t - 1$ получаем $N(1) - N(-1) = \deg(q_t) - \deg(q_{t-1}) = \deg(a_t)$. Результат вытекает теперь из (5.81). □

Заметим, что утверждения леммы 5.59 и теоремы 5.60 теряют силу, если многочлен f имеет корни в поле $\mathbb{F}_q$. Рассмотрим, например, случай $f(x) = x$. В этом случае сумма значений характера равна нулю, поскольку $\sum_{c\in\mathbb{F}_q} \eta(c) = \sum_{c\in\mathbb{F}_q^*} \eta(c) = 0$. С другой стороны,

$$\frac{F(x)-1}{G(x)} = [0,\ x^{(q+1)/2} + x], \qquad \frac{F(x)+1}{G(x)} = [0,\ x^{(q+1)/2} - x],$$

так что $s = t = 1$ и $\deg(A_s) = \deg(a_t) = (q+1)/2$.

Комментарии

§ 1. Характеры конечных абелевых групп подробно изучаются, например, в книге Холла (Hall [6, ch. 13]) [1]). Факт, состоящий в том, что конечная абелева группа имеет столько же характеров, сколько и элементов (см. теорему 5.5), был впервые доказан Вебером (Weber [2]). Нетрудно доказать, что группа характеров $\hat{G}$ группы G изоморфна самой группе G (см. упр. 5.5). Особые свойства квадратичных характеров поля $\mathbb{F}_{p^2}$ при простом нечетном числе p были установлены в работах Giudici [1], [2] и Hardman, Jordan [1]. В статье Cartier [1] изучаются квадратичные характеры произвольного конечного поля $\mathbb{F}_q$ и квадратичные характеры групп невырожденных матриц над $\mathbb{F}_q$. Пеллегрино (Pellegrino [2]) изучал, как ведет себя квадратичный характер поля $\mathbb{F}_q$ при дробно-линейных преобразованиях этого поля. Карлиц (Carlitz [27]) получил аддитивные характеры факторкольца $\mathbb{F}_q[x]/(f)$. Общие обзоры по тригонометрическим суммам см. в книгах Hua [12] и Katz [4] [2]).

§ 2. Суммы Гаусса для конечных простых полей были использованы еще в работе Лагранжа (Lagrange [4]) о решении алгебраических уравнений (в старой литературе эти суммы часто назы-

[1]) См. также Шмидт [I*, гл. 9. 10]. — *Прим. перев.*

[2]) А также Виноградов [2*] и Виноградов, Карацуба [1*]. — *Прим. перев.*

ваются «резольвентами» и «циклотомическими резольвентами»). Гаусс также упоминал о них и доказал формулу (5.15) в своих «Арифметических исследованиях» (Gauss [1, sec. VIII]); он же установил некоторые из свойств, приведенных в теореме 5.12 (Gauss [2], [5]). Доказательства элементарных результатов о суммах Гаусса имеются в классических работах Коши (Cauchy [2], [4]), Эйзенштейна (Eisenstein [1]), Якоби (Jacobi [1], [2]), Куммера (Kummer [3], [4], [5], [6]) и Лебега (Lebesgue [2]). Обзор этих ранних результатов можно найти в работах Bachmann [1], [2], Dickson, Mitchell, Vandiver, Wahlin [1, sec. 19] и Smith H. J. S. [1]. Суммы Гаусса для конечных полей общего вида первым рассмотрел Штикельбергер (Stickelberger [1]). Интересные замечания исторического характера имеются в работах Berndt, Evans [4] и Weil [11]. Современные толкования разных вопросов теории гауссовых сумм даются в работах Apostol [2], Gras [1], Hasse [15], Ireland, Rosen [1], Joly [5], Lang [3], [5] и Schmidt W. M. [3].

Теорема 5.14 доказана в статье Davenport, Hasse [1]. Наше доказательство — это по существу доказательство Вейля (Weil [6]), где с учетом работ Ireland, Rosen [1, ch. 11] и McEliece, Rumsey [1] сделаны некоторые упрощения. Другие доказательства этой теоремы можно найти в книгах Lang [5, ch. 1] и Schmidt W. M. [3, ch. 2]; особенно элементарны доказательства, приводимые в работах Schmid [1] и Степанов [14]. Более общий результат получен Делинем (Deligne [4]) применением когомологических методов. См. также статью Hayes [3], в которой доказывается аналог теоремы Дэвенпорта — Хассе о суммах Гаусса для факторкольца $\mathbb{F}_q[x]/(f)$.

Выражение для квадратичной суммы Гаусса из теоремы 5.15 было впервые найдено Гауссом (Gauss [2]) для случая $s = 1$. С тех пор появилось множество различных доказательств этой теоремы. Приведенное в нашей книге доказательство, взятое из статьи Waterhouse [2] и основанное на идеях Шура (Schur [3]), имеет то преимущество, что использует по возможности лишь алгебраические соображения. В доказательстве Шура применяется матрица $(e^{2\pi ijk/m})_{1\leqslant j,\, k\leqslant m}$, которая в дальнейшем изучалась в статьях Carlitz [80], где были найдены ее собственные значения, и McClellan, Parks [1] и Morton [1], где были определены ее собственные векторы. Другой подход к вычислению квадратичных сумм Гаусса с использованием теории матриц был предложен Карлицом (Carlitz [74]). См. также работы Bressoud [1], Carlitz [106], Cauchy [5], Kronecker [2], Mordell [12] и Shanks [1], где даются в основном алгебраические доказательства; аналитические доказательства используются в работах Bambah, Chowla [1], Dirichlet [1], Estermann [2], Karamata, Tomić [1]

Kronecker [9], Landau [3], Mordell [1] и Weber [6], а также в некоторых других. Во многих из этих работ вычисляется сумма

$$\sum_{n=0}^{p-1} e^{2\pi i n^2/p},$$

которая, как нетрудно убедиться, совпадает с квадратичной суммой Гаусса для простого поля $\mathbb{F}_p$. С другими доказательствами можно познакомиться в книгах Apostol [2, ch. 8], Chowla S. [16, ch. 2], Davenport [8, ch. 2], Landau [5, ch. 4], Lang [3, ch. 4] и Боревич, Шафаревич [1, гл. 5]. В статье Berndt, Evans [4] дается исчерпывающий разбор техники, применяемой при вычислении квадратичных сумм Гаусса. В связи с теоремой 5.15 интересен следующий результат Човлы (Chowla S. [13], [14]) и Морделла (Mordell [13]) (см. также Narkiewicz [1, ch. 6]): если p — простое нечетное число и ψ — мультипликативный характер поля $\mathbb{F}_p$, то число $G(\psi, \chi_1)\, p^{-1/2}$ является корнем из единицы лишь в том случае, когда ψ — квадратичный характер. Обобщения этого результата на произвольные конечные поля получены в статьях Evans [1] и Yokoyama [1]. См. также работы Evans [8] и Stickelberger [1] по поводу близких результатов.

В статье Carlitz [81] показано, что сумма вида $B = \sum_{n=1}^{p-1} c_n e^{2\pi i n/p}$ при простом нечетном числе p и $c_n = \pm 1$ удовлетворяет равенству $|B| = p^{1/2}$ лишь в случае, когда B — квадратичная сумма Гаусса для поля $\mathbb{F}_p$. Другая характеризация квадратичных сумм Гаусса среди сумм вида B дается в работах Rédei [7], [11, ch. 6]. В статье Cavior [3] отмечается, что если в сумме B коэффициенты c_n — произвольные целые числа и выполнено условие $|B| = p^{1/2}$, то сумма B тесно связана с квадратичной суммой Гаусса.

Теорема 5.16 принадлежит Штикельбергеру (Stickelberger [1]). Ее доказательство приводится также в статьях Carlitz [71] и Baumert, McEliece [1], при этом последняя содержит также вычисления некоторых других сумм Гаусса специального вида. Подобные же формулы можно найти также в работах Berndt, Evans [1], [2], [4], Evans [1], Ishimura [1], McEliece [5] и Myerson [5], однако некоторые из этих формул содержат неточности.

Квадратичный закон взаимности (теорема 5.17) был установлен Гауссом (Gauss [1]), который дал несколько его доказательств (см. также Gauss [2], [4]). Одно из них основано на суммах Гаусса (Gauss [2]); см. также Cauchy [2], Eisenstein [3], Hasse [15, ch. 8] и Ireland, Rosen [1, ch. 6]. Некоторые рассуждения в доказательстве теоремы 5.17 существенно упрощаются, если использовать суммы Гаусса со значениями из конечных полей; см. упр. 5.26 и 5.27, а также работы Burde [6], Hausner [1],

Holzer [1, § 18, 19], Ireland, Rosen [1, ch. 7], Kloosterman [6], Serre [1, ch. 1] и Zassenhaus [3]. Другой метод доказательства квадратичного закона взаимности с помощью конечных полей связан с разложением многочлена $(x^r - 1)/(x - 1)$ над простым полем $\mathbb{F}_p$. Эта идея восходит к посмертно опубликованной работе Гаусса (Gauss [4]) и позднее неоднократно использовалась фактически в эквивалентных формах другими авторами (см. Pellet [2], Mirimanoff, Hensel [1] и Swan [1]). Этот тип доказательства воспроизведен также в книгах Bachmann [4, ch. 7], Berlekamp [4, ch. 6], Childs [1, part III, ch. 16] и Rédei [10, ch. 11]. Другие доказательства, использующие конечные поля, можно найти в статьях Agou [6], Brewer [1], Chowla S. [18], Furquim de Almeida [2], Lebesgue [4], Pellet [9], Skolem [6] и Решетуха [2]; см. также пример 5.24 в § 3. Систематический обзор различной техники, используемой для доказательства квадратичного закона взаимности, можно найти в работе Pieper [1]. В книге Bachmann [4, ch. 6] представлена история различных доказательств. Интересны также доказательства квадратичного закона взаимности в недавно опубликованных статьях Brown E. [1] и Frame [1].

Суммы Гаусса используются также при доказательстве высших законов взаимности; см. Eisenstein [2] относительно кубичного случая и Eisenstein [4] относительно биквадратичного случая. Доказательство Эйзенштейна кубичного закона взаимности воспроизводится в книгах Bachmann [1, ch. 14] и Ireland, Rosen [1, ch. 9]; см. также Bachmann [1, ch. 13] по поводу биквадратичного случая. Доказательство Джоули (Joly [4]) кубичного закона взаимности тоже связано с суммами Гаусса. При этом использование сумм Гаусса со значениями из конечного поля вновь приводит к упрощениям (см. Burde [6], [9] относительно кубичного и биквадратичного случаев соответственно). Доказательство кубичного закона взаимности, основанное на конечных полях, приводится также в статье Skolem [6]. Суммы Гаусса используются, кроме того, в законе взаимности, принадлежащем Вестерну (Western [1]) и в так называемых рациональных законах взаимности, рассмотренных в статьях Evans [9], Leonard, Williams [6] и Williams K. S. [34]. Об оценке роли сумм Гаусса в законах взаимности см. Weil [11].

Интересные соображения об общих законах взаимности приведены в книге Hasse [16] и обзорной статье Wyman [1]. Другой тип законов взаимности, связанных с конечными полями, рассматривал Дедекинд (Dedekind [1]), который установил квадратичный закон взаимности для нормированных неприводимых многочленов над конечными простыми полями; см. также Artin [1] и Vaidyanathaswamy [1]. Высший закон взаимности этого типа для произвольных конечных полей был получен Кюне (Kühne [1]) и затем переоткрыт Шмидтом (Schmidt F. K. [2])

и Карлицом (Carlitz [1], [2]); см. также Carlitz [4], Ore [6], Pocklington [2], Schwarz [2] и Whiteman [1].

Большое количество работ о суммах Гаусса с кубичными характерами появилось в связи с давней гипотезой Куммера. Куммер (Kummer [2]) на основании вычислений, проделанных в статье Kummer [1], выдвинул гипотезу, что для мультипликативного характера ψ порядка 3 простого поля $\mathbb{F}_p$, где $p \equiv 1 \pmod 3$, числа попаданий величины $G(\psi, \chi_1)\, p^{-1/2}$ в три подмножества единичной окружности

$$I_1 = \left\{e^{\pi i t} \,\middle|\, |t| \leqslant \frac{1}{3}\right\}, \quad I_2 = \left\{e^{\pi i t} \,\middle|\, \frac{1}{3} < |t| \leqslant \frac{2}{3}\right\},$$

$$I_3 = \left\{e^{\pi i t} \,\middle|\, \frac{2}{3} < |t| \leqslant 1\right\}$$

стремятся к отношению 3 : 2 : 1 при $p \to \infty$. Однако более основательная вычислительная работа, проделанная многими авторами (например, von Neumann, Goldstine [1], Beyer [1], Lehmer E. [5], Cassels [2], Fröberg [1]), склоняла к выводу, что предельное отношение ближе к 1 : 1 : 1. Теоретические результаты Морено (Moreno C. J. [1]) и Паттерсона (Patterson S. J. [3]) также указывали на это. Наконец, Хит-Браун и Паттерсон (Heath-Brown, Patterson [1]) преуспели в доказательстве гораздо более сильного утверждения, а именно что значения $G(\psi, \chi_1)\, p^{-1/2}$ распределены равномерно на единичной окружности, когда число p пробегает все простые числа, сравнимые с единицей по модулю 3. Это доказательство построено на более ранних работах Куботы (Kubota T. [5], [6]) и Паттерсона (Patterson S. J. [1], [2]). См. также Deligne [5], где результаты Паттерсона рассматриваются с другой точки зрения. Более ранняя попытка А. И. Виноградова [1] опровергнуть гипотезу Куммера оказалась неудачной. Мэтьюз (Matthews C. R. [1]) доказал формулу, высказанную ранее Касселсом (Cassels [3], [4], [5]) в качестве гипотезы, согласно которой значение кубичной суммы Гаусса над простым полем $\mathbb{F}_p$ равно

$$G(\psi, \chi_1) = J(\psi, \psi)\, H(\psi)\, p^{1/3},$$

где $J(\psi, \psi)$ — сумма Якоби (см. § 3), а $H(\psi)$ — произведение значений $\mathfrak{p}$-функции Вейерштрасса. Простой алгоритм для вычисления этого выражения предложен в статье McGettrick [1]. О дальнейших результатах по кубичным суммам Гаусса см. Hasse [15, ch. 20], Krätzel [1], Loxton [1], [2], [3] и Решетуха [1], а также обзорную статью Berndt, Evans [4].

Мэтьюз (Matthews C. R. [2]) доказал справедливость формул, предложенных Локстоном (Loxton [2], [3]) и Мак-Гетриком (McGettrick [2]) в качестве гипотез и дающих значения биквадратичных сумм Гаусса $G(\psi, \chi_1)$ над простым полем $\mathbb{F}_p$. Распределе-

ние величины $G(\psi, \chi_1)\, p^{-1/2}$ на единичной окружности исследовали Хассе (Hasse [15, ch. 20]), Кубота (Kubota T. [4]), Лемер (Lehmer E. [5]) и Ямамото (Yamamoto [1]), а затем Паттерсон (Patterson S. J. [4]) показал, что эти значения равномерно распределены на единичной окружности, когда p пробегает все простые числа, сравнимые с 1 по модулю 4 и что аналогичная теорема справедлива для сумм Гаусса любого высшего порядка. Дальнейшие результаты о биквадратичных суммах Гаусса можно найти в работах Berndt, Evans [4], Hasse [15, ch. 20], Krätzel [1] и Kubota T. [4]. Другого типа результат о равнораспределенности для сумм Гаусса установил Смит (Smith R. A. [3], [4]), который показал, что если ψ пробегает все нетривиальные мультипликативные характеры простого поля $\mathbb{F}_p$, то распределение $p-2$ величин $G(\psi, \chi_1)\, p^{-1/2}$ на единичной окружности стремится к равномерному распределению, когда $p \to \infty$ (см. также Katz [4, ch. 1]).

При доказательстве теоремы 5.17 мы отмечали, что значения сумм Гаусса являются целыми алгебраическими числами. Поэтому представляет интерес разложение на множители такого значения (точнее главного идеала, порожденного таким значением) в кольце целых соответствующего поля алгебраических чисел. Это было осуществлено в важной статье Штикельбергера (Stickelberger [1]). Некоторые результаты этой статьи излагаются в работах Gras [1], Joly [5], Lang [3, ch. 4], [5, ch. 1]. В статье Fröhlich [2] предлагается другой метод доказательства. Штикельбергер в той же статье (Stickelberger [1]) получил некоторые сравнения для значений сумм Гаусса; см. также Dwork [2] и Gras [1].

Результатом, представляющим большой теоретический интерес, является формула Гросса и Коблица (Gross, Koblitz [1]), выражающая значение суммы Гаусса в виде некоторого произведения значений p-адической гамма-функции; см. также Boyarsky [1], Koblitz [3, ch. 3] и Lang [6, ch. 15].

Интересное мультипликативное соотношение между суммами Гаусса, впервые установленное Якоби (Jacobi [2]), представлено следствием 5.29. Предположение Хассе (Hasse [15, p. 465]) о том, что соотношения, выводимые из теоремы 5.12 (iv)) и следствия 5.29, порождают все возможные мультипликативные соотношения между суммами Гаусса, было опровергнуто Ямамото (Yamamoto [2]); см. также Yamamoto [4]. Другие тождества, содержащие произведения сумм Гаусса, можно найти в работах Boyarsky [1], Evans [7], Grant [1] и Helversen-Pasotto [1], [2], [3], [4].

Суммы Гаусса возникают также и во многих других разделах математики. Так, в теории чисел весьма эффективно используются суммы Гаусса для факторкольца $\mathbb{Z}/(m)$ (m может быть

и составным числом). Они определяются с помощью какого-нибудь аддитивного характера кольца $\mathbb{Z}/(m)$ и некоторого характера группы делителей единицы этого кольца. Развитая теория таких сумм представлена в книге Hasse [15, ch. 20]. Такие суммы рассматриваются также и в других источниках, например в книгах Apostol [2, ch. 8], Ayoub [1, ch. 5], Lang [3, ch. 4], [5, ch. 3] и Narkiewicz [1, ch. 6]. Квадратичные суммы Гаусса такого вида удовлетворяют закону взаимности, который был сформулирован Коши (Cauchy [5]) и доказан Шааром (Schaar [1]) и Кронекером (Kronecker [3]); см. также Bochner [1], Landsberg [2] и Lerch [1]. Обобщения этого закона взаимности можно найти в работах Berndt [1], Berndt, Evans [4], Guinand [1] и Siegel [3]. Другие соотношения между квадратичными суммами Гаусса для кольца $\mathbb{Z}/(m)$ и близкими к ним суммами приводятся в статьях Carlitz [107], Chowla S. [1], [2] и Menon [1]. Суммы Гаусса для кольца $\mathbb{Z}/(m)$ с ограниченной областью суммирования рассматриваются в статьях Berndt, Evans [3] и Lehmer D. H. [11].

Суммы Гаусса для полей алгебраических чисел были введены Гекке (Hecke [1]). Об этой теории см. Hasse [10], Hecke [4, ch. 8] и Narkiewicz [1, ch. 6]. Дальнейшие результаты, в частности, о законах взаимности для квадратичных сумм Гаусса этого типа можно найти в работах Barner [2], Hecke [2], [3], Kloosterman [3], Kubota T. [1], Kunert [1], Mordell [3], Shiratani [1] и Siegel [3]. Гауссовы суммы Гекке были затем обобщены Хассе (Hasse [12], [13]), который рассмотрел так называемые гауссовы суммы Галуа; см. также Kubota T. [1], [2], Lakkis [1], [2], [3] и более ранние работы Fröhlich, Taylor [1], Martinet [1] и Taylor M. J. [1], [2]. Еще один тип сумм Гаусса для полей алгебраических чисел был рассмотрен в работе Kubota T. [3].

В статьях Carlitz [27] и Hayes [3] были рассмотрены суммы Гаусса для факторколец вида $\mathbb{F}_q[x]/(f)$, а Шмид (Schmid [2]) ввел суммы Гаусса для колец векторов Витта над конечными полями. В статье Schmid, Teichmüller [1] рассматриваются суммы Гаусса еще для одного класса колец, построенного с помощью конечных полей. Кондо (Kondo [1]) изучал суммы Гаусса для колец матриц над конечными полями, а квадратичные суммы Гаусса для таких колец рассматривались в статьях Porter [16], [17]. Общая теория гауссовых сумм для конечных колец была развита Лампрехтом (Lamprecht [1], [2], [3]); см. также Kutzko [1]. Суммы Гаусса для так называемых квадратичных характеров конечных абелевых групп изучались Шпрингером (Springer [3]). Ссылки на литературу по обобщениям сумм Гаусса см. в работе Berndt, Evans [4].

Суммы Гаусса находят много приложений в теории конечных полей, теории чисел и комбинаторике. О применении сумм Гаусса для определения числа решений некоторых уравнений над конеч-

ными полями см. гл. 6. Суммы Гаусса можно использовать для получения унитарных представлений степени p для группы характеров группы $\mathbb{F}_p^*$ (см. Burde [1]). В статье Yamada [1] изложено одно приложение сумм Гаусса к кривым $y^p - y = x^{p^a} - 1$ над простым полем $\mathbb{F}_p$. Морено (Moreno O. [1]) использовал суммы Гаусса для определения числа элементов поля $\mathbb{F}_{2^m}$ с абсолютным следом 0 и с заданным степенным характером. Значение сумм Гаусса в доказательстве законов взаимности было отмечено выше. Упомянем также следующие теоретико-числовые вопросы, где используются суммы Гаусса: критерий того, является ли данный элемент вычетом (квадратичным или более высокой степени) (Ankeny [3], Evans [6], Hasse [14], Hayashi [2], Muskat [1], [3], Whiteman [8], Williams K. S. [31]), проблема Варинга (Ayoub [1, ch. 4], Barrucand [1], Hardy, Littlewood [2], [3], Landau [2, ch. 6], Vaughan R. C. [1, ch. 4]) [1]), проверка на простоту (Lenstra H. W. [2]), L-функции Дирихле и функциональные уравнения для них (Apostol [1], Ayoub [1, app. B], Chowla S. [16, ch. 1], Hasse [11, ch. 1], Lang [5, ch. 3]), функциональные уравнения для рядов Дирихле, соответствующих модулярным формам (Shimura [1, ch. 3]), абелевы числовые поля (Gras [1], Leopoldt [1]) и формулы для числа классов (Bergström [1], Hasse [9]). Суммы Гаусса возникают в теории разностных множеств (Berndt, Chowla [1], Berndt, Evans [1], Evans [4], [10], Menon [2], Muskat, Whiteman [1], Yamamoto [3]) и в связи с распределением весов в циклических кодах (Baumert, McEliece [1], McEliece [5], McEliece, Rumsey [1], Niederreiter [8]). С помощью сумм Гаусса в статье Auslander, Tolimieri [1] получено интересное соотношение для конечных преобразований Фурье. Суммы Гаусса появляются также в функциональных уравнениях для дзета-функций, соответствующих некоторым представлениям группы $GL(n, \mathbb{F}_q)$ невырожденных $n \times n$-матриц над конечным полем $\mathbb{F}_q$ (см. Springer [2]).

§ 3. Суммы Якоби $J(\lambda_1, \ldots, \lambda_k)$ для конечных простых полей и при $k = 2$ упоминаются Якоби (Jacobi [1]) в его письме Гауссу. Первыми публикациями, где они обсуждаются, являются статьи Коши (Cauchy [2]) и Якоби (Jacobi [2]), и, что окончательно запутывает вопрос о приоритете, они встречаются также в посмертно опубликованной работе Гаусса Gauss [5]. Указанные источники наряду со статьями Cauchy [4], Eisenstein [1] и Lebesgue [2] содержат уже все основные свойства таких сумм. По поводу этих ранних работ см. также Bachmann [1], Dickson, Mitchell, Vandiver, Wahlin [1, § 19], Smith H. J. S. [1] и Weil [11]. Эквивалентные суммам Якоби тригонометрические суммы для произвольных конечных полей при $k = 2$ были введены Кум-

[1]) См. также Виноградов [1*]. — *Прим. перев.*

мером (Kummer [6]). Новый этап изучения этих сумм начался со статьи Штикельбергера (Stickelberger [1]). Суммы Якоби для произвольного $k \geqslant 2$, кажется, появляются впервые в статьях Вейля (Weil [6]) и Вандивера (Vandiver [16]). Доказательства основных свойств сумм Якоби общего вида можно найти как в этих двух работах, так и в статье Faircloth, Vandiver [1]. Эти свойства сумм Якоби излагаются в книгах Hasse [15] и Ireland, Rosen [1], а также в статье Joly [5].

Мы уже говорили в § 2 о теореме 5.14, доказанной Дэвенпортом и Хассе (Davenport, Hasse [1]). Аналогом этой теоремы для сумм Якоби является теорема 5.26, которая была доказана гораздо раньше Митчеллом (Mitchell H. H. [1]). Теорема 5.28 доказана в статье Davenport, Hasse [1], однако следствие 5.29 появилось (для случая простых конечных полей) еще в статье Якоби (Jacobi [2]); о доказательстве теоремы 5.28 см. также Gras [1] и Lang [5, ch. 2]. Элементарные доказательства теоремы 5.28 имеются в работах Berndt, Evans [1] и Hasse [15, ch. 20] (для случая квадратичного характера) и в статье Berndt, Evans [2] (для случая, когда m — степень двойки). В работах Berndt, Evans [2] и Gras [1] показано также, что задача нахождения элементарного доказательства теоремы 5.28 может быть сведена к случаю, когда m — простое чнсло.

Попытки вычисления сумм Якоби при $k = 2$ для характеров малых порядков предпринимались многими авторами, нередко в связи с циклотомией. Но во многих случаях еще остаются неясности. Упомянем работы Berndt, Evans [2], Dickson [46], Evans [2], [3], Ireland, Rosen [1], Ishimura [1], Lehmer E. [7], [8], Muskat, Zee [1], Tanner [1], [3] и Zee [1], [2]; наиболее подробны работы Berndt, Evans [1] и Muskat [6]. Содержит сведения по этому вопросу и обзорная статья Berndt, Evans [4]. Интересен результат, полученный Эвансом (Evans [1]): если λ — мультипликативный характер порядка $k > 2$ простого поля $\mathbb{F}_p$, то ни одна из степеней суммы Якоби $J(\lambda, \ldots, \lambda)^n$, где n — ненулевое целое число, не может быть действительным числом, если число аргументов суммы Якоби превышает 1. Этот результат улучшает полученный ранее результат Ёкоямы (Yokoyama [1]).

Если λ — мультипликативный характер порядка m произвольного конечного поля $\mathbb{F}_q$, то сумма Якоби $J(\lambda^r, \lambda^s)$, очевидно, является целым алгебраическим числом из m-кругового поля $\mathbb{Q}^{(m)}$ над полем $\mathbb{Q}$ рациональных чисел. Задача нахождения разложения главного идеала, порожденного этим целым алгебраическим числом в кольце целых кругового поля $\mathbb{Q}^{(m)}$, в этом случае проще, чем в случае сумм Гаусса. Она была решена Куммером для случая простого числа m в статьях Kummer [3], [6] и для составного m в статье Kummer [7]. Современное изложение этих результатов см. также в книге Lang [5, ch. 1] Сравнения для сумм Якоби

были получены Кронекером (Kronecker [6]) и Шверингом (Schwering [1]); см. также Parnami, Agrawal, Rajwade [2].

Как и суммы Гаусса, суммы Якоби рассматриваются и в других разделах математики и ее приложений. Важность сумм Якоби для полей алгебраических чисел стала очевидной после того, как Вейль (Weil [7], [10]) показал, что из них получаются так называемые характеры Гекке (или гроссенхарактеры) абелевых расширений поля $\mathbb{Q}$ рациональных чисел; см также Deligne [4] и Lang [5, ch. 1]. Делинь (Deligne [4]) дает когомологическую интерпретацию сумм Якоби; см. также Katz [5]. В статье Fröhlich [1] рассматриваются так называемые якобиевы суммы Галуа и их разложение. Холл (Hall [7]) определил суммы Якоби для групповых колец над круговыми полями. Общую теорию сумм Якоби для конечных колец развил Лампрехт (Lamprecht [3]); см. также Kutzko [1]. Оно (Ono [8]) ввел суммы Якоби для конечных абелевых групп.

В примерах 5.24 и 5.25 указаны два теоретико-числовых приложения сумм Якоби. Существует и множество других приложений. Так, на суммах Якоби можно основать доказательство кубичного закона взаимности (Ireland, Rosen [1, ch. 9], Joly [4], Weil [11]), биквадратичного закона взаимности (Bachmann [1, ch. 13]), а также высших законов взаимности (Evans [9], Leonard, Williams [6], Western [1], Williams K. S. [34]). Суммы Якоби можно использовать для установления критерия того, является ли данный элемент вычетом (см. Berndt, Evans [1], Evans [6], Hasse [14], Leonard, Mortimer, Williams [1], Muskat [2], [3], [5], Western [2], Whiteman [8]). С помощью сумм Якоби можно получить результаты, аналогичные примеру 5.25; богатым источником таких результатов являются работы Berndt, Evans [1], [2]; см. также Ireland, Rosen [1, ch. 8] и Leonard, Williams [2]. Приложения сумм Якоби к проверке на простоту получены в статьях Adleman [1], Adleman, Pomerance, Rumely [1] и Cohen, Lenstra [1]. В статьях Carlitz [76] и Lehmer D. H. [9] суммы Якоби применяются для изучения матрицы $(\psi(i-j))_{1\leqslant i,\, j\leqslant p-1}$, где ψ — мультипликативный характер простого поля $\mathbb{F}_p$. Ивасава (Iwasawa [1]) связал суммы Якоби с числами классов круговых полей.

Что же касается приложений сумм Якоби в теории конечных полей, то отметим, что они не только тесно связаны с суммами Гаусса, но появляются также и при изучении других тригонометрических сумм; см., например, теоремы 5.51 и 5.52, а также статьи Berndt, Evans [1], [2], Leonard, Williams [4], Singh, Rajwade [1] и Whiteman [14]. Приложения их к уравнениям над конечными полями будут рассмотрены в гл. 6. Отметим здесь лишь тесную связь между суммами Якоби и так называемыми циклотомическими числами. Если b — примитивный элемент

поля $\mathbb{F}_q$ и e — заданный натуральный делитель числа $q-1$, то *циклотомическим числом* $(h, k)_e$ порядка e называется число упорядоченных пар (s, t), удовлетворяющих равенству

$$b^{es+h}+1=b^{et+k}, \quad 0 \leqslant s, t<(q-1)/e.$$

Связь между циклотомическими числами и суммами Якоби была замечена еще Куммером (Kummer [4], [6]). Большинство исследователей этой связи ограничились лишь случаем простого числа q; см., например, Hall [7], Mitchell H. H. [1], Myerson [5], Parnami, Agrawal, Rajwade [3] и Storer [2], [4]. Общий случай рассмотрен в статьях Vandiver [14], [17]. О связи между циклотомическими числами и суммами Якоби см. также работы Bachmann [1, ch. 15], Baumert, Fredricksen [1], Berndt, Evans [1], Bruck [2], Dickson [26], [44], [46], Evans, Hill [1], Leonard, Williams [5], Muskat [4], [6], [7], Muskat, Whiteman [1], Schwering [1], Storer [1], Whiteman [5], [9], [10], [11], [14] (см., кроме того, комментарии к § 3 гл. 6 об оценке циклотомических чисел и об их связи с уравнениями над конечными полями). Некоторые из приведенных работ имеют отношение также к теории разностных множеств. О приложениях сумм Якоби к этой теории см. Baumert, Fredricksen [1], Berndt, Evans [1], Menon [2], Muskat, Whiteman [1], Storer [1], Whiteman [10], [11] и Yamamoto [3].

§ 4. Суммы значений характеров из теоремы 5.30, которые в силу этой теоремы тесно связаны с суммами Гаусса, иногда тоже называют суммами Гаусса. Их элементарная оценка, приводимая в теореме 5.32, получена Харди и Литтлвудом (Hardy, Littlewood [3]) для простых конечных полей, а для произвольных конечных полей — в эквивалентной форме — Хуа и Вандивером (Hua, Vandiver [1]); см. также Schmidt W. M. [3, ch. 2]. Некоторые улучшения удается получить, если брать числа n из определенного множества (см. Митькин [5]). Эти суммы для небольших значений n удается вычислить; см. Berndt, Evans [1], [2], а также обзорную статью Berndt, Evans [4]. Значения этой суммы для $n=2$ приводятся в теореме 5.33 и следствии 5.35. Аналогичные суммы значений характеров с произвольным n встречаются в аналитической теории чисел в связи с *проблемой Варинга* о представлении натуральных чисел суммами n-х степеней; см. Ayoub [1, ch. 4], Barrucand [1], Hardy, Littlewood [2], [3], Kloosterman [4], Landau [2, ch. 6] и Vaughan R. C. [1, ch. 2, 4] [1]). Теорема 5.34 доказана Карлицом (Carlitz [120]).

Теоремы 5.38 и 5.41 были получены Вейлем (Weil [5]) на основе его доказательства гипотезы Римана для кривых над конечными полями. В связи с этим вопросом см. комментарии к § 4 гл. 6.

[1]) См. также Виноградов [1*]. — *Прим. перев.*

Как отмечалось в рассуждении, следующем за теоремой 5.38, условия, наложенные на многочлен f в этой теореме, могут быть ослаблены. Действительно, Карлиц и Утияма (Carlitz, Uchiyama [1]) показали, что для справедливости теоремы достаточно, чтобы многочлен f нельзя было представить в виде $g^p - g + b$, где $g \in \mathbb{F}_q[x]$, $b \in \mathbb{F}_q$ и p — характеристика поля $\mathbb{F}_q$. Для многочленов же f такого вида полученная в теореме оценка не обязательно верна (см. снова рассуждение, следующее за этой теоремой). Завершение нашего доказательства теоремы 5.38 в § 4 гл. 6 покажет, что это связано с нахождением хороших оценок для числа решений уравнения $y^q - y = f(x)$ в расширении поля $\mathbb{F}_q$. Элементарный метод установления таких оценок принадлежит Степанову[1]) [3], [5]; его упрощения получены Шмидтом (Schmidt W. M. [3, ch. 2]) и Митькиным [1]. Связь между такими оценками и теоремой 5.38 разъясняется также Шмидтом (Schmidt W. M. [3, ch. 2]) и Постниковым [1]. Оценка, аналогичная полученной в теореме 5.38, приводилась в качестве гипотезы в статьях Hasse [5] и Mordell [6]. Ранее полученные оценки для простых конечных полей имели вместо показателя 1/2 сначала показатель $1-2^{1-n}+\varepsilon$ для любого $\varepsilon > 0$ (см. Hardy, Littlewood [1] и, с небольшим улучшением, Kamke [1]), а затем $1 - 1/n$ (Mordell [4] и, с небольшим улучшением, Davenport [4]). Как общая оценка теорема 5.38 является наилучшей из возможных согласно результату Шмидта (Schmidt W. M. [3, ch. 2]). Другие нижние границы для абсолютных величин таких сумм значений характеров получены в следующих работах: Anderson, Stiffler [1], Tietäväinen [2], Карацуба [5], Книжнерман, Соколинский [1], Коробов, Митькин [1] и Митькин [3]. В статье Cavior [3] определено число многочленов над простым полем $\mathbb{F}_p$, для которых соответствующая сумма равна по абсолютной величине числу $p^{1/2}$. Одони (Odoni [1]) получил один результат о статистическом распределении величины $\left|\sum_{c \in \mathbb{F}_q} \chi(f(c))\right| q^{-1/2}$.

В статьях Davenport, Heilbronn [1], Акулиничев [1], Виноградов И. М. [5] и Карацуба [5] рассматривался случай $f(x) = ax^n + bx$, $a, b \in \mathbb{F}_p^*$, $2 \leqslant n \leqslant p-1$, причем в последней из названных работ показано, что

$$\left|\sum_{c \in \mathbb{F}_p} \chi(f(c))\right| \leqslant (n-1)^{1/4} p^{3/4}$$

для нетривиального аддитивного характера χ простого поля $\mathbb{F}_p$. Эта оценка при $n > 1 + p^{1/3}$ лучше, чем в теореме 5.38. Частные случаи $n = 3$ и $n = 4$ рассматривались Карлицом (Carlitz [122], [124]) и Морделлом (Mordell [28], [29]) соответственно. В статье

[1]) См. комментарии к § 4 гл. 6. — *Прим. перев.*

Birch [2] изучалось усредненное поведение таких сумм при $n = 3$, когда a и b пробегают простое поле $\mathbb{F}_p$. Для случая $f(x) = ax^{p+1} + bx \in \mathbb{F}_q[x]$, где $a \neq 0$ и p — характеристика поля $\mathbb{F}_q$, такие суммы значений характера оценивались Карлицом (Carlitz [124], [125]). Элементарное доказательство отмеченного выше результата Карлица и Утиямы было получено Вильямсом (Williams K. S. [27]) для случая, когда число q четно и $\deg(f) \leqslant 6$.

Аналоги сумм значений характера из теоремы 5.38 изучались также для факторколец $\mathbb{Z}/(m)$; см., например, статьи Chen J. R. [1], Hua [1], [3], [6], [7], [9, ch. 1], [12] и Карацуба [4]; недавние уточнения см. в работах Chen J. R. [2], Körner, Stähle [1], Loxton, Smith [1], Smith R. A. [6], Нечаев [7], Нечаев, Топунов [1] и Стечкин [1].

Завершение нашего доказательства теоремы 5.41 в § 4 гл. 6 покажет, что содержащаяся в ней оценка зависит от нахождения хороших оценок для числа решений уравнения $y^m = f(x)$ в расширениях поля $\mathbb{F}_q$. Элементарный метод нахождения таких оценок принадлежит Степанову [2], [7] и Шмидту (Schmidt W. M. [1], [3]); ср. с комментариями к § 4 гл. 6 Менее точные оценки для сумм значений характера из теоремы 5.41 ранее были установлены в статье Davenport [7], а для некоторых частных случаев — в работах Davenport [1], [2], [3] и Виноградов И. М. [11]. Оценка из теоремы 5.41 является наилучшей возможной общей оценкой (см. Schmidt W. M. [3, ch. 2]). Случай, когда f является трехчленом, был рассмотрен в статье Ono [7]. Относительно результатов о сумме из теоремы 5.41 для случая, когда ψ — квадратичный характер, см. также § 5 и примечания к нему. Некоторыми авторами изучались так называемые *гибридные суммы*, т. е. суммы вида

$$\sum_{c \in \mathbb{F}_q} \psi(f(c))\,\chi(g(c)),$$

где $f, g \in \mathbb{F}_q[x]$, ψ — нетривиальный мультипликативный, а χ — нетривиальный аддитивный характеры поля $\mathbb{F}_q$. Оказывается, что такие суммы (если исключить тривиальные случаи) также имеют порядок роста не более $q^{1/2}$; см. Schmidt W. M. [3, ch. 2] и Перельмутер [1], [2]. Подобные суммы рассматривал также Вильямс (Williams K. S. [20]).

Интенсивному изучению подверглись суммы значений таких характеров, аргументами которых являются многочлены от нескольких переменных. Для случая двух переменных пусть $f \in \mathbb{F}_q[x, y]$ — многочлен степени $n \geqslant 2$, который невырожден в том смысле, что нельзя с помощью невырожденного линейного преобразования переменных перевести его в многочлен от одной переменной. Для случая нетривиального аддитивного характера χ

поля $\mathbb{F}_q$ в статьях Hua, Min [2], [3] установлена граница для суммы значений этого характера

$$\sum_{c,\, d \in \mathbb{F}_q} \chi(f(c, d)),$$

имеющая порядок $q^{2-(2/n)}$, и тем самым существенно улучшена полученная раньше оценка Камке (Kamke [1]). Для случая $n = 3$ Хуа и Мин (Hua, Min [2], [3]) получили еще лучшую границу — порядка $q^{5/4}$; см. также работу Davenport, Lewis [1], где приведен тот же результат. Наилучший возможный порядок q для случая $n = 3$ получен в статье Bombieri, Davenport [1], но для некоторых специальных кубических многочленов это было показано ранее Морделлом (Mordell [11], [18]). Суммы значений характеров с кубическими многочленами от двух переменных рассматривались также Карлицом (Carlitz [122]). Некоторые простейшие гибридные двойные суммы, т. е. двойные суммы, содержащие и аддитивный, и мультипликативный характеры, были изучены в статьях Chowla S. [21] и Chowla, Smith [1]. Дэвенпорт и Льюис (Davenport, Lewis [1]) получили оценку для суммы

$$\sum_{c_1,\, c_2,\, c_3 \in \mathbb{F}_q} \chi(f(c_1, c_2, c_3))$$

наилучшего возможного порядка q^2 в случае, когда χ — тот же характер, что и выше, а f — кубический многочлен над $\mathbb{F}_q$ от трех переменных, который невырожден, т. е. не может быть переведен в многочлен от меньшего числа переменных никаким невырожденным линейным преобразованием переменных; см. также Mordell [15] о некоторых частных случаях.

Для произвольной суммы вида

$$S(f) = \sum_{c_1, \ldots, c_r \in \mathbb{F}_q} \chi(f(c_1, \ldots, c_r)),$$

где $f \in \mathbb{F}_q[x_1, \ldots, x_r]$, Бомбьери (Bombieri [3], [4]) доказал аналог теоремы 5.36. Аналогичный результат для мультипликативного характера установлен Перельмутером [3]. Нетривиальные оценки для сумм $S(f)$ были получены в статьях Min [2] и Uchiyama [7], но настоящим достижением явилась фундаментальная статья Делиня (Deligne [3]), где была подтверждена гипотеза Вейля для случая алгебраических многообразий над конечными полями (ср. с комментариями к § 4 гл. 6). Из работы Делиня вытекает, что если степень n многочлена f не делится на характеристику p конечного поля $\mathbb{F}_q$ и однородная часть степени n многочлена f в некотором смысле невырожденна, то

$$|S(f)| \leqslant (n-1)^r q^{r/2}$$

(см. Deligne [3], [6], Katz [4, ch. 5], Serre [3]), — справедливость этого результата предугадал Бомбьери (Bombieri [4]). Делинь (Deligne [4]) обобщил упоминавшийся выше результат Карлица и Утиямы следующим образом: если многочлен $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ произвольной степени n нельзя представить в виде $g^p - g + b$, где $g \in \mathbb{F}_q[x_1, \ldots, x_r]$, $b \in \mathbb{F}_q$, то

$$|S(f)| \leqslant (n-1)\, q^{r-(1/2)}.$$

Подробное исследование сумм $S(f)$ проводится в книге Katz [4]. Легко показать, что средний порядок роста абсолютной величины $|S(f)|$ равен $q^{r/2}$ (см. Carlitz [47]). Оценки для многочленов f специального вида были даны раньше, чем появилась упомянутая работа Делиня; см. Davenport, Lewis [1] для случая кубического многочлена f, Mordell [14] для случая

$$f(x_1, \ldots, x_r) = a_1 x_1^{h_1} + \ldots + a_r x_r^{h_r} + b x_1^{k_1} \ldots x_r^{k_r},$$

Mordell [24] для случаев

$$f(x_1, \ldots, x_r) = (a_1 x_1 + \ldots + a_r x_r)\, x_1^{m_1} \ldots x_r^{m_r}$$

и

$$f(x_1, \ldots, x_r) = g(x_1^2, \ldots, x_r^2),$$

где g — квадратный многочлен, и Ono [2] для случая, когда многочлен f является полуинвариантом некоторой связной алгебраической группы. Если f — квадратичная форма, то суммы $S(f)$ можно вычислить в явном виде (см. упр. 6.27—6.30). О когомологических интерпретациях суммы $S(f)$ см. Katz [4, ch. 3] и Springer [4]. Общий подход к этим суммам был осуществлен в статье Ono [1]. Относительно сумм с мультипликативными характерами и гибридных сумм, содержащих многочлены от нескольких переменных, см. работы Davenport, Lewis [1], Katz [4], Serre [3] и Перельмутер [11], [12]. Суммы вида $S(f)$ над факторкольцом $\mathbb{Z}/(m)$ рассматривались в следующих статьях: Loxton, Smith [2], Архипов, Карацуба и Чубариков [1] и Чубариков [1] [1]).

Суммы, аналогичные рассмотренной выше сумме $S(f)$, но в которых r-наборы $(c_1, \ldots, c_r) \in \mathbb{F}_q^r$ принадлежат какой-либо кривой или многообразию из $\mathbb{F}_q^r$, были впервые рассмотрены Бомбьери (Bombieri [4]); см. также статьи Adolphson, Sperber [1], Bombieri [7], Chalk, Smith [1], Hooley [4], [5], [6], Laumon [1], Milne [2], Serre [3], Smith R. A. [2], Williams K. S. [6] и Перельмутер [9], а также детальный разбор в книге Katz [4].

Так называемые *неполные суммы* тоже возникают при ограничении на область суммирования, а именно когда суммирование

[1]) См. также Чубариков [1*], [2*], [3*]. — *Прим. перев.*

производится лишь по некоторым «интервалам» или «ящикам». Неполные суммы в основном рассматривались для простых полей. Относительно неполных сумм вида $\sum_{c=N+1}^{N+H} \chi(f(c))$, где χ — нетривиальный аддитивный характер простого поля $\mathbb{F}_p$ или кольца $\mathbb{Z}/(m)$, а f — многочлен, см. работы Davenport, Heilbronn [1], Hua [11], [12, § 14], Карацуба [3], [7], Коробов [2], [3], [4], [5] и Лебедев [1]. О случае, когда f — многочлен от r переменных и суммирование ведется по всем r-наборам $(c_1, \ldots, c_r) \in \mathbb{Z}^r$, где $a_i \leqslant c_i \leqslant b_i$ для $1 \leqslant i \leqslant r$, см. Mordell [22] и Serre [3].

Для неполных сумм с нетривиальными мультипликативными характерами ψ простого поля $\mathbb{F}_p$ существует классическое неравенство И. М. Виноградова [1] и Пойи (Pólya [1]) (см. также Schur [2]):

$$\left|\sum_{c=1}^{H} \psi(c)\right| < p^{1/2} \log p.$$

Небольшие улучшения постоянного множителя были затем получены Ландау (Landau [1]) и И. М. Виноградовым [12]; см. также Whyburn [2]. Тот факт, что порядком роста левой части может быть число $p^{1/2} \log\log p$, был доказан Човлой (Chowla S. [3]) с использованием расширенной гипотезы Римана и затем в статье Bateman, Chowla, Erdös [1] (без использования недоказанных предположений); этим был улучшен результат из статьи Paley [1] для кольца $\mathbb{Z}/(m)$. Верхняя граница указанного порядка роста была установлена Монтгомери и Воном (Montgomery, Vaughan [1]) в предположении, что выполняется гипотеза Римана для L-функций Дирихле. О приложениях неравенства Виноградова — Пойи в теории чисел см. Hua [12, § 14]. Соколовский [1] показал, что для любого мультипликативного характера ψ простого конечного поля $\mathbb{F}_p$, $p > 2$, существует число $N \in \mathbb{N}$, такое, что

$$\left|\sum_{c=N+1}^{N+(p-1)/2} \psi(c)\right| \geqslant \frac{1}{2}(p - 1/p)^{1/2};$$

это улучшает результат из статьи Sárközy [1]. Обобщение неравенства Виноградова — Пойи на случай произвольных конечных полей $\mathbb{F}_q$, $q = p^n$, было получено Дэвенпортом и Льюисом (Davenport, Lewis [3]), показавшими, что если ψ — нетривиальный мультипликативный характер поля $\mathbb{F}_q$, то

$$\left|\sum_{c \in B} \psi(c)\right| < q^{1/2}(1 + \log p)^n,$$

где B — «ящик», состоящий из элементов $c = c_1\alpha_1 + \ldots + c_n\alpha_n$, удовлетворяющих условиям $0 \leqslant N_j < c_j \leqslant N_j + H_j < p$ для

$1 \leqslant j \leqslant n$ (где $\{\alpha_1, \ldots, \alpha_n\}$ — базис поля $\mathbb{F}_q$ над простым подполем $\mathbb{F}_p$, а N_j и H_j — заданные целые неотрицательные числа). Оценки неполных сумм с мультипликативными характерами, зависящие от числа H слагаемых, были впервые получены Бёрджессом (Burgess [1]) для квадратичного характера простого поля $\mathbb{F}_p$, а затем Вангом (Wang Y. [1], [2]) и Бёрджессом (Burgess [2], [3], [5]) для произвольных нетривиальных мультипликативных характеров простого поля $\mathbb{F}_p$. Эти результаты имеют следующий вид: для любого $\varepsilon > 0$ существует число $\delta > 0$, такое, что для простого числа $p > p_0(\varepsilon)$ и целого числа $H > p^{(1/4)+\varepsilon}$ справедлива оценка

$$\left| \sum_{c=N+1}^{N+H} \psi(c) \right| < Hp^{-\delta}$$

для любых нетривиальных характеров ψ поля $\mathbb{F}_p$ и любых целых чисел N (см. Burgess [2]). Аналог неравенства типа неравенства Бёрджесса — Ванга для произвольного конечного поля $\mathbb{F}_q$ был доказан впервые Дэвенпортом и Льюисом (Davenport, Lewis [3]); дальнейшее его усиление получено в статьях Burgess [7], Friedlander [3] и Jordan J. H. [3] (для частного случая $q = p^2$) и в статьях Burgess [10], Friedlander [2] и Карацуба [6], [8] для общего случая [1]). Распределение значений неполной суммы $\sum_{c=N+1}^{N+H} \eta(c)$, где η — квадратичный характер простого поля $\mathbb{F}_p$, изучалось в статьях Davenport, Erdös [1], Montgomery [2], Wolke [1] и Усольцев [1]. Неполные суммы вида $\sum_{c=N+1}^{N+H} \psi(f(c))$, где ψ — нетривиальный мультипликативный характер простого поля $\mathbb{F}_p$ и $f \in \mathbb{F}_p[x]$, рассматривались в работах Burgess [6], Виноградов И. М. [4] и Сегал [1]. Нижние границы для абсолютных величин таких сумм при $\psi = \eta$ были найдены Карацубой [9], Митькиным [3] и Степановым [11]. Неполные кратные суммы для простого поля $\mathbb{F}_p$ с мультипликативными характерами изучались в статьях Burgess [8], [9] для случая бинарных квадратичных форм и в статье Gillett [1] для случая произвольных многочленов от нескольких переменных.

§ 5. Суммы Клостермана впервые появились в работе Kloosterman [1] в связи с представлением целых чисел квадратичной формой. В этой работе содержится также оценка нетривиальных сумм Клостермана для конечных простых полей $\mathbb{F}_p$, имеющая порядок $p^{3/4}$ (см. также Estermann [1] и Salié [1]). Улучшенная граница порядка $p^{2/3}$ была получена в статьях Davenport [4]

[1]) Бёрджесс [10] и Фридлендер [2] повторили результат Карацубы [6], [8]. Метод также заимствован у Карацубы. — *Прим. перев.*

и Salié [2]. Хассе (Hasse [5]) заметил, что оценка, указанная в теореме 5.45, вытекает из гипотезы Римана для кривых над конечными полями. Справедливость этой гипотезы была установлена Вейлем (Weil [1], [2], [3]), который затем доказал в статье Weil [5] и упомянутую выше оценку для сумм Клостермана. Доказательство Вейля теоремы 5.45 было упрощено Карлицом и Утиямой (Carlitz, Uchiyama [1]), которые к тому же рассмотрели случай четного числа q, не изученный Вейлем. Два доказательства теоремы 5.45 можно найти в книге Шмидта (Schmidt W. M. [3, ch. 2]); они существенно опираются на метод Степанова [4], [5].

Теорема 5.46 доказана в статье Carlitz [111]. Применяя многочлены Диксона, определенные равенством (7.6) (см. гл. 7), можно переписать формулу из теоремы 5.46 в виде

$$K(\chi^{(s)};\ a,\ b) = -g_s(-K,\ q) = (-1)^{s-1} g_s(K,\ q).$$

Равенство в теореме 5.47 является частным случаем формулы преобразования из статьи Jacobsthal [1]. Доказательства теоремы 5.47 можно найти также в работах Davenport [4], Salié [1], Schmidt W. M. [3, ch. 2] и Williams K. S. [16]. Различные равенства для сумм Клостермана, а также сумм из произведений сумм Клостермана содержатся в статьях Davenport [4], Lehmer, Lehmer [1], [3], Salié [1] и Whiteman [5]; см. также Kutzko [1], где предлагается иной подход. Некоторые из этих равенств связаны с суммами Якобсталя. Карлиц (Carlitz [109]) изучил некоторые элементарные свойства сумм Клостермана для поля $\mathbb{F}_q$ характеристики 2.

Поскольку уже само появление сумм Клостермана было связано с квадратичными формами, вряд ли следует удивляться тому, что их можно использовать для изучения тригонометрических сумм, содержащих квадратичные формы (см. Carlitz [45], [46], [109], Chowla S. [20], Виноградов И. М. [4], Малышев [2]). Результат работы Carlitz [46] был обобщен в работах Carlitz [72] и Hodges [16]. В статье Dwork [11] суммы Клостермана рассматриваются с точки зрения p-адических когомологий.

Рассматриваются также суммы Клостермана для факторколец $\mathbb{Z}/(m)$. Оценка для таких сумм, основанная на оценке Вейля, была получена в статье Hooley [1]; см. также Estermann [3], [4]. В статье Salié [1] получено точное значение для сумм Клостермана в случае $m = p^k$, где p — простое число и $k \geqslant 2$; см. также Whiteman [2], Williams K. S. [19], [28] и Малышев [3, гл. 2]. Клостерман (Kloosterman [2]) сделал важное наблюдение, что суммы Клостермана для кольца $\mathbb{Z}/(m)$ появляются в связи с коэффициентами Фурье модулярных форм. Эта замечательная связь в дальнейшем широко использовалась; см., например, работы Bruggeman [1], Deshouillers, Iwaniec [1], Iwaniec [1],

Parson [1], Petersson [1], Rademacher [1], [2], Selberg [2], Кузнецов Н. В. [1], Линник [2], Малышев [4] и Проскурина [1], [2]. Дальнейшие результаты о суммах Клостермана для факторкольца $\mathbb{Z}/(m)$ можно найти в работах Hooley [2], Kloosterman [1], [2], Salié [1], Selberg [1], Smith R. A. [5] и Малышев [3, гл. 2]. Андрухаев [2] изучал суммы Клостермана для факторколец кольца целых гауссовых чисел. Неполные суммы Клостермана изучались Клостерманом (Kloosterman [1], [2]) и Радемахером (Rademacher [1]); см. также Hooley [3, ch. 2].

Обобщенные суммы Клостермана, определяемые в упр. 5.83, были введены Дэвенпортом (Davenport [4]). Для случая квадратичного характера ψ такую сумму называют также *суммой Салье*, так как Салье (Salié [1]) впервые доказал для нее формулы, приведенные в упр. 5.84 и 5.85 для простых конечных полей. Доказательства формул для сумм Салье можно найти также в работах Lehmer D. H. [6], Mordell [26], [28], [30], Williams K. S. [16], [21], [22] и Малышев [3, гл. 2]. Суммы Салье играют важную роль в изучении функции разбиения (см. Lehmer D. H. [6]). Оценка типа Вейля для обобщенных сумм Клостермана была получена Човлой (Chowla S. [22]) для случая, когда ψ не является квадратичным характером. Обобщенные суммы Клостермана появляются также в статьях Carlitz [46], Hodges [16], Kloosterman [5] и Виноградов И. М. [5] и (в близкой форме) в работах Knopp [1], Rohrbach [1], Андрухаев [1] и Малышев [1], [3, гл. 2], [4]. О дальнейших обобщениях сумм Клостермана, связанных с теорией модулярных форм, см. Bruggeman [1], Deshouillers, Iwaniec [1], Rankin [1, ch. 5], Selberg [2] и Проскурин [1], [3]. Другое важное обобщение сумм Клостермана для конечных полей возникает при рассмотрении сумм вида $\sum \chi(R(c))$, где R — рациональная функция над полем $\mathbb{F}_q$ и суммирование ведется по всем элементам $c \in \mathbb{F}_q$, для которых определено значение $R(c)$; см. Bombieri [4], Елистратов [7], Перельмутер [1], [2], [9] и Степанов [5]. Гибридные суммы с рациональными функциями изучались в статьях Mordell [27] и Перельмутер [1], [2], [9]; такие же и даже более общего вида суммы появляются в статье Williams K. S. [20].

Кратные суммы Клостермана (или *гиперсуммы Клостермана*) были введены Морделлом (Mordell [14]). В нетривиальном случае они имеют вид

$$K_r = \sum_{c_1, \ldots, c_r \in \mathbb{F}_q^*} \chi(a_1c_1 + \ldots + a_rc_r + bc_1^{-1} \ldots c_r^{-1}),$$

где χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, а $a_1, \ldots, a_r, b \in \mathbb{F}_q^*$. В статье Mordell [14] доказана оценка $|K_r| \leqslant q^{(r+1)/2}$ для случая, когда q — простое число; см. также Carlitz [100]

и Smith R. A. [4]; некоторые улучшения для частных случаев получены в работах Carlitz [100], [108]. Окончательная оценка

$$|K_r| \leqslant (r+1)\, q^{r/2}$$

установлена Делинем (Deligne [4]). Это, безусловно, является прямым обобщением теоремы 5.45. В работах Katz [4, ch. 2, 5] и Serre [3] обсуждаются предпосылки доказательства Делиня. Бомбьери (Bombieri [7]) получил границу того же порядка роста (относительно q), использовав лишь предварительные результаты из статьи Делиня Deligne [4]. О дальнейших результатах по кратным суммам Клостермана см. работы Carlitz [100], [113], Kutzko [1], Lehmer, Lehmer [4], McEliece, Rumsey [1] и Sperber [2]. Кратные суммы Клостермана для факторколец $\mathbb{Z}/(m)$ были рассмотрены в статьях Carlitz [98], Smith R. A. [3], [4], [5] и Weinstein [1]. О гибридных кратных суммах Клостермана см. Deligne [4], Katz [4, ch. 5] и Mordell [26], [31]. Кратные тригонометрические суммы с другими рациональными функциями рассматривались в работах Carlitz [113], Katz [4, ch. 5], Lehmer, Lehmer [1], Mordell [10], [27], [28], [31] и Sperber [1], [3]. Суммы Клостермана для невырожденных матриц над конечными полями рассмотрены в статье Hodges [6], для кососимметрических матриц — в статьях Hodges [8], [25], для симметрических и эрмитовых матриц — в статьях Hodges [3], [10], [17].

Теорема 5.48 была доказана Якобсталем (Jacobsthal [1], [2]) для конечных простых полей. О приложениях формулы из этой теоремы см. Hall [8, ch. 14] и Lehmer D. H. [8]. Суммы $H_n(a)$ и $I_n(a)$ были впервые изучены Якобсталем (Jacobsthal [1], [2]) — главным образом, для случаев $n = 1$ и $n = 2$. Различные тождества, связывающие эти суммы, были получены в работах Berndt, Evans [1], Lehmer E. [4], von Schrutka [1], Whiteman [6] и Постников и Степанов [1]. Суммы Якобсталя вычислялись для небольших значений n, часто одинаковым по существу способом, а именно путем определения числа решений уравнений $y^2 = x^n + a$ в поле $\mathbb{F}_q$; так, для нетривиального случая, когда $n = 4$, $a = 1$ и q — простое число, это было проделано еще Гауссом (Gauss [3]). О дальнейших результатах см. работы Brewer [2], Chowla S. [6], Davenport, Hasse [1], Evans [2], [3], Hasse [15, ch. 10], Hudson, Williams [1], Ireland, Rosen [1, ch. 11], Lehmer E. [1], [4], [7], Leonard, Williams [7], Morlaye [2], Rajwade [3], [8], Singh, Rajwade [1], Whiteman [3], [6], Williams K. S. [30] и Андрианов [1], причем особенное внимание следует обратить на работы Berndt, Evans [1], [2], которые содержат полную информацию по данному вопросу. Некоторые сравнения по модулю p для значений сумм Якобсталя для простого поля $\mathbb{F}_p$ были установлены в работах Lehmer E. [6], Nashier, Rajwade [1] и Whiteman [6]. Якобсталь (Jacobsthal [1]) доказал для случая

простого поля $\mathbb{F}_p$ неравенство $|H_2(a)| < 2p^{1/2}$, а Човла (Chowla S. [11]) показал, что в нем как постоянный множитель, так и показатель являются наилучшими возможными. Нижняя граница для числа $\max_{a \in \mathbb{F}_q^*} |H_n(a)|$ была установлена Постниковым и Степановым [1]. Нижние границы для абсолютных величин сумм Якобсталя можно также получить из нижних границ более общих сумм значений характеров с полиномиальными аргументами (см. комментарии к § 4). Для простых полей $\mathbb{F}_p$ Карацуба [9] показал, что равенство $I_n(a) = p$ возможно для $a \in \mathbb{F}_p^*$, а Постников и Степанов [1] показали, что равенство $H_n(a) = p - 1$ возможно для $a \in \mathbb{F}_p^*$, в обоих случаях при условии, что n имеет порядок роста $p/\log p$.

Теоремы 5.51 и 5.52 показывают, что суммы Якобсталя тесно связаны с другими классическими тригонометрическими суммами, например такими, как суммы Якоби; см. также Berndt, Evans [1], Lehmer E. [7] и Singh, Rajwade [1]. Связь между суммами Якобсталя и так называемыми суммами Бревера рассматривается в статьях Berndt, Evans [2], Giudici, Muskat, Robinson [1], Robinson S. F. [1] и Whiteman [13], [14], [15]. *Обобщенные суммы Якобсталя*, т. е. суммы вида

$$\sum_{c \in \mathbb{F}_p} \lambda(c)\psi(c^n + a),$$

где λ и ψ — нетривиальные мультипликативные характеры простого поля — $\mathbb{F}_p$, рассматривались в статье Walum [1]. Двойные суммы Якобсталя появляются в статье Lehmer, Lehmer [1].

Применение сумм Якобсталя, описанное в примере 5.53, содержится в статье Jacobsthal [2]. Доказательства того же результата имеются в работах Berndt, Evans [1], Burde [4], Chowla S. [16, ch. 4], Hasse [15, ch. 10] и Whiteman [3], [6]. Целые числа A и B из примера 5.53 появляются также в работах Bachmann [1, ch. 10], Chowla S. [16, ch. 5] и Whiteman [6]. Другие приложения сумм Якобсталя к квадратичным разбиениям простых чисел имеются в работах Berndt, Evans [1], [2], Chowla S. [5], [6], Hasse [15, ch. 10], Lehmer E. [4], Nashier, Rajwade [1], Rajwade [3], Rosenberg [1], von Schrutka [1], Whiteman [3], [6] и Williams K. S. [29], [30]. Близкие к суммам Якобсталя суммы тоже полезны для нахождения квадратичных разбиений простых чисел; см. Berndt, Evans [2], Brewer [2], [3] и Whiteman [4], [13]. Связь между суммами Якобсталя и циклотомией исследуется в статьях Giudici, Muskat, Robinson [1], Rajwade [3] и Whiteman [3], [6], [14], а приложение сумм Якобсталя для выяснения вопроса о том, будет ли данный элемент вычетом, встречается в статье Leonard, Mortimer, Williams [1]. Карлиц (Carlitz [50]) применил суммы Якобсталя для нахождения числа ре-

шений некоторых полиномиальных уравнений с числом переменных, бо́льшим двух. Андрианов [1] установил связь между значением I_3 (1) для простого поля $\mathbb{F}_p$ и числом представлений числа p в виде некоторой квадратичной формы от четырех переменных; см. также статью Фоменко [1], где получен близкий результат.

Теорема 5.60 доказана Дэвенпортом (Davenport [10]). Лежащая в ее основе теория непрерывных дробей была развита еще Артином (Artin [1]); о дальнейших результатах по непрерывным дробям см. также de Mathan [3]. В статьях Baum, Sweet [1], [2] установлены важные результаты о непрерывных дробях над полем $\mathbb{F}_2$ при частичных дробях малой степени. В статье Houndonougbo [1] изучается длина разложений рациональных функций в непрерывную дробь. Приложения алгоритма разложения в непрерывные дроби к теории кодирования рассматриваются в работах Mills [4], Reed, Scholtz, Truong, Welch [1], Reed, Truong [4], Reed, Truong, Miller [3], Welch, Scholtz [1] и Гоппа [1]. Специального вида непрерывные дроби для элементов поля $\mathbb{F}_q$ изучаются в статье Borho [1].

Среди тригонометрических сумм, содержащих квадратичный характер η, большое внимание уделяется так называемым суммам Бревера. Рассмотрим многочлен Диксона $g_k(x, a)$ (см. (7.6)) над конечным полем $\mathbb{F}_q$ нечетной характеристики, где $a \in \mathbb{F}_q^*$, и образуем *сумму Бревера*:

$$\Lambda_k(a) = \sum_{c \in \mathbb{F}_q} \eta(g_k(c, a)).$$

Для частного случая $a = 1$ такие суммы были введены в статье Brewer [2], а для общего — в статье Brewer [3]. Оказывается, что $\Lambda_k(a) = 0$, если НОД $(k, q^2 - 1) = 1$ (см. Chowla P. [2], а также следствие 7.17). Значения сумм Бревера при малых значениях k можно найти в статьях Berndt, Evans [2], Brewer [2], [3], Giudici, Muskat, Robinson [1], Leonard, Williams [4], Rajwade [7], Robinson S. F. [1], Whiteman [13], [14], [15] и Williams K. S. [35], причем статья Berndt, Evans [2] является особенно обильным источником таких результатов. В этих статьях можно также проследить связь сумм Бревера с квадратичными разбиениями простых чисел и с циклотомией. Суммы Бревера связаны также с *суммами Эйзенштейна*, определяемыми в упр. 5.68, которые были впервые введены в статье Eisenstein [5]; см. также Berndt, Evans [2], Giudici, Muskat, Robinson [1] и Whiteman [15] о связи между этими двумя типами сумм значений характеров.

Для сумм с квадратичным характером и произвольными полиномиальными аргументами Коробов [6] и Митькин [2] установили оценки, которые в некоторых случаях даже лучше оценок Вейля из теоремы 5.41. Нижние оценки для абсолютных величин таких сумм были найдены Книжнерманом и Соколинским [1]

и Митькиным [3], а для соответствующих неполных сумм — Степановым [11]. Привлекает внимание случай, когда многочлен является произведением различных нормированных линейных сомножителей — в связи с распределением квадратичных вычетов; см., например, Burde [4], Davenport [1], Hasse [15, ch. 10], Hopf [1], Yamauchi [1] и Виноградов И. М. [10]. Относительно сумм значений квадратичных характеров с другими специальными многочленами см. работы Birch [2], Chowla S. [19], Davenport [3], Olson [1], Опо [3], Rajwade, Parnami [1], Rosenberg [1], Salié [3], Williams [36], [37], [38], Абдуллаев [1], [2], Абдуллаев, Коган [1], Тушкина [1] и Фоменко [1]. Перельмутер [10], [11], [12] дает оценки для кратных сумм с квадратичным характером.

Связь между суммами значений квадратичных характеров и распределением квадратичных вычетов и невычетов по модулю p (или, более общо, квадратов и неквадратов в поле $\mathbb{F}_q$) отражена в упр. 5.63 и 5.64. По этому вопросу мы отсылаем также к работам Bergum, Jordan [1], Burde [4], Davenport [1], [3], Giudici [1], Hardman, Jordan [1], Hasse [4], [15, ch. 10], Horf [1], Johnsen [1], Katz [4, ch. 1], Koutský [1], Pellegrino [1], Rocci [1], Schmidt W. M. [3, ch. 3], von Grosschmid [1], Аладов [1] и Виноградов И. М. [4]. В теории чисел широко изучались и другие типы задач о распределении квадратичных вычетов и невычетов; см., например, работы Ankeny [1], Brauer A. [2], Burgess [1], Davenport, Erdös [1], Dörge [1], Elliott [2], Hua [12, § 14], Hudson R. H. [2], [3], [5], Perron [1], Salié [3], Виноградов И. М. [3], Гельфонд и Линник [1, гл. 9] и Усольцев [1]. О геометрическом подходе см. Raber [1] и Ralston [1]. В связи с вопросами, затронутыми в упр. 5.65 и 5.66, см. работы Burde [1], [3], [7], Davenport [2], [7], Jänichen [1], Koutský [2], Виноградов И. М. [6], [11], Мороз [1] и Сегал [1]. Брауэр (Brauer A. [1], [3]) доказал, что если заданы целые числа m, $h \geqslant 2$ и комплексный корень m-й степени из единицы ε, то для достаточно больших простых чисел p, сравнимых с 1 по модулю m, и для любого мультипликативного характера ψ порядка m поля $\mathbb{F}_p$ найдется элемент $c \in \mathbb{F}_p$, для которого $\psi(c+i) = \varepsilon$ при всех $i = 0, 1, \ldots, h-1$. О близких результатах по распределению значений мультипликативных характеров, а также по распределению степеней по модулю p или степеней в конечных полях см. работы Bierstedt, Mills [1], Brauer A. [4], [5], Brillhart, Lehmer, Lehmer [1], Burgess [4], [6], [10], [11], Chowla, Chowla [2], Dunton [2], Elliott [1], [3], [4], [5], Graham [1], Hua [12, § 14], Hudson R. H. [1], [4], [5], [6], Jordan J. H. [1], [2], [4], [5], Lehmer, Lehmer [2], Lehmer, Lehmer, Mills [1], Lehmer, Lehmer, Mills, Selfridge [1], Metsänkylä [1], Mills [2], Montgomery [1, ch. 13], Norton [2], [3], [4], [5], [6], Rabung, Jordan [1], Singh [1], [5], Stephens [2], Stevens H. [1], Stevens, Kuty [1], Wang Y.

[3], Whyburn [1], Бухштаб [1], Виноградов И. М. [2], [3], [7], [9] и Гельфонд, Линник [1, гл. 9]. Комбинаторные свойства подгруппы группы $\mathbb{F}_q^*$, состоящей из m-х степеней, рассматриваются в работах Cameron, Hall, van Lint, Springer, van Tilborg [1], Evans [5], Muskat, Street [1] и Street, Whitehead [1].

Тригонометрические суммы, аргументами которых являются линейные рекуррентные последовательности, рассматриваются в § 7 гл. 8.

[В работе Naranjani [1*], продолжающей аналогичные исследования Бёрджесса (Burgess [6]), изучается распределение степенных невычетов по простому модулю в полиномиальных последовательностях. В работах Hinz [1*], [2*], [3*], [4*] изучается распределение примитивных элементов по модулю простого идеала в поле алгебраических чисел. Распределение последовательных квадратичных вычетов и невычетов исследовалось Хадсоном (Hudson [1*], [2*]). Распределение значений символа Лежандра в конечном поле исследовалось в работе Guerra, Ughi [1*]. Коэн (Cohen [2*], [3*], [4*]) исследовал вопрос о распределении примитивных элементов и степенных вычетов, а также пар последовательных примитивных элементов (т. е. отличающихся на 1) среди значений многочлена над конечным полем. В работе Loxton, Vaughan [1*] получена оценка рациональной тригонометрической суммы с многочленом $\sum_{k=1}^{q} e^{2\pi i f(k)/q} = O(q^{1-1/(e+1)})$, где e — максимальная кратность комплексных корней многочлена $f'(x)$, и тем самым доказана гипотеза, высказанная в работе Loxton, Smith [1]. Стечкин [1*] получил оценку суммы Гаусса

$$\left|\sum_{k=1}^{q} e^{2\pi i a k^n/q}\right| \leqslant \exp\left(c\,[n/\varphi(n)]^2\right) q^{1-1/n},$$

где $\varphi(n)$ — функция Эйлера, $c > 0$ — абсолютная постоянная и НОД $(a, q) = 1$. Митькин [2*] получил уточнение оценки Хуа Ло-гена [12] для рациональных тригонометрических сумм, которые близки к полным суммам. Шмидт (Schmidt W. M. [1*], [2*]) подробно исследовал тригонометрические суммы с кубическими многочленами. Степановым в работах [1*], [2*], [4*] получены новые оценки кратных тригонометрических сумм на алгебраических многообразиях, обобщающие полученные ранее оценки Бомбьери (Bombieri [4]) и Перельмутера [9] на случай составного знаменателя тригонометрической суммы. В работе Heath-Brown [1*] показано, что аналог оценки Делиня (Deligne [3]) для рациональных тригонометрических сумм со знаменателем p^2 может быть получен на основе довольно элементарных соображений. В работе В. Шмидта (Schmidt W. M. [3*]) получена

оценка кратной тригонометрической суммы с многочленом и с простым знаменателем для случаев, не охватываемых оценкой Делиня (Deligne [3]). Одони (Odoni [1*], [2*]) перенес статистический подход, примененный им ранее к суммам Вейля (см. Odoni [1]) на случай других сумм.

По тематике пятой главы имеются также следующие работы: Bremser [1*], Cohen [1*], Cohen, Lenstra [1*], Exponentialsummen (Kloosterman'sche Summen), Goldfeld, Sarnak [1*], Hudson, Williams [1*], Monzingo [1*], Ozeki [1*], Sivaramakrishan, Vijayan [1*], Tietäväinen [1*], Архипов, Карацуба, Чубариков [1*], [2*], Архипов, Чубариков [1*], Бронштейн [1*], Голубева [1*], Глазунов [1*], Елистратов [1*], [2*] Карацуба [1*], [2*], [4*], [5*], [6*], [7*], [8*], [9*], Кузнецов [1*], [2*], [3*], Митькин [4*], Перельмутер [1*], [2*], Постников [1*], Постникова [1*] и Чубариков [1*], [2*], [3*]. — *Перев.*]

Упражнения

5.1. Пусть G — конечная абелева группа, H — ее собственная подгруппа и $g \in G$, $g \notin H$. Доказать, что существует характер χ группы G, который аннулирует H, но для которого $\chi(g) \neq 1$.

5.2. Пусть H — подгруппа конечной абелевой группы G. Доказать, что аннулятор A подгруппы H в группе характеров $G\hat{}$ группы G изоморфен факторгруппе G/H и что факторгруппа $G\hat{}/A$ изоморфна подгруппе H.

5.3. Пусть G — конечная абелева группа и $m \in \mathbb{N}$. Доказать, что элемент $g \in G$ является m-й степенью некоторого элемента группы G в том и только том случае, если $\chi(g) = 1$ для всех характеров χ группы G, для которых χ^m — тривиальный характер.

5.4. Пусть $G_1, \ldots, G_k$ — конечные абелевы группы. Определим умножение k-наборов $(g_1, \ldots, g_k)$ и $(h_1, \ldots, h_k)$, где $g_i, h_i \in G_i$ для $1 \leqslant i \leqslant k$, равенством

$$(g_1, \ldots, g_k)(h_1, \ldots, h_k) = (g_1h_1, \ldots, g_kh_k).$$

Показать, что относительно этой операции множество всех таких k-наборов является конечной абелевой группой (она называется *прямым произведением* групп $G_1, \ldots, G_k$ и обозначается $G_1 \otimes \ldots \otimes G_k$). Доказать затем, что соответствующая группа характеров $(G_1 \otimes \ldots \otimes G_k)\hat{}$ изоморфна прямому произведению $G_1\hat{} \otimes \ldots \otimes G_k\hat{}$.

5.5. Применив структурную теорему о конечных абелевых группах, которая в своей простейшей форме утверждает, что каждая такая группа изоморфна прямому произведению некоторых конечных циклических групп, доказать, что группа характеров $G\hat{}$ конечной абелевой группы G изоморфна G.

5.6. Показать, что если χ_a — аддитивный характер конечного поля $\mathbb{F}_q$ (в обозначениях теоремы 5.7), то $\chi_a\chi_b = \chi_{a+b}$ для всех $a, b \in \mathbb{F}_q$. Показать таким способом, без использования упр. 5.5, что группа аддитивных характеров поля $\mathbb{F}_q$ изоморфна аддитивной группе этого поля.

5.7. Пусть χ_1 — канонический аддитивный характер конечного поля $\mathbb{F}_q$ характеристики p. Доказать, что $\chi_1(c^{p^j}) = \chi_1(c)$ для всех $c \in \mathbb{F}_q$ и $j \in \mathbb{N}$.

5.8. Пусть ψ— мультипликативный характер порядка m конечного поля $\mathbb{F}_q s$, где $m, s \in \mathbb{N}$. Доказать, что ограниченне характера ψ на поле $\mathbb{F}_q$ является мультипликативным характером порядка $m/\text{НОД}(m, (q^s - 1)/(q - 1))$ поля $\mathbb{F}_q$.

5.9. В обозначениях упр. 5.8 доказать, что ограничение характера ψ на $\mathbb{F}_q$ является тривиальным характером поля $\mathbb{F}_q$ в том и только том случае, когда m делит число $(q^s-1)/(q-1)$.

5.10. Пусть ψ — мультипликативный характер поля $\mathbb{F}_q$, и пусть ψ' — его поднятие до расширения $\mathbb{F}_{q^s}$ поля $\mathbb{F}_q$ (определение поднятия характера см. в рассуждении, предшествующем теореме 5.14). Доказать, что $\psi'(c)=\psi^s(c)$ для любого $c\in\mathbb{F}_q^*$.

5.11. Доказать, что мультипликативный характер τ поля $\mathbb{F}_{q^s}$ совпадает с поднятием ψ' некоторого мультипликативного характера поля $\mathbb{F}_q$ тогда и только тогда, когда τ^{q-1} — тривиальный характер.

5.12. Пусть $m\in\mathbb{N}$, $q\equiv 1 \pmod m$ и ψ пробегает множество всех мультипликативных характеров поля $\mathbb{F}_q$, порядки которых делят m. Доказать, что при этом соответствующее поднятие ψ' до расширения $\mathbb{F}_{q^s}$ поля $\mathbb{F}_q$ пробегает множество всех мультипликативных характеров поля $\mathbb{F}_{q^s}$, порядки которых делят m.

5.13. Доказать, что аддитивный характер χ конечного расширения E поля $\mathbb{F}_q$ совпадает с поднятием некоторого характера поля $\mathbb{F}_q$ тогда и только тогда, когда он имеет вид $\chi=\mu_b$ для некоторого $b\in\mathbb{F}_q$, где μ_1 — канонический аддитивный характер поля E (определение характера μ_b см. в теореме 5.7).

5.14. Пусть $\mathbb{F}_q$ — конечное поле. Доказать, что если $c\in\mathbb{F}_q^*$, то

$$\sum_{d\mid(q-1)}\frac{\mu(d)}{\varphi(d)}\sum_{\psi^{(d)}}\psi^{(d)}(c)=\begin{cases}\dfrac{q-1}{\varphi(q-1)}, & \text{если } c \text{ — примитивный элемент } \mathbb{F}_q,\\ 0 & \text{в противном случае,}\end{cases}$$

где во внешней сумме d пробегает все положительные делители числа $q-1$, а во внутренней $\psi^{(d)}$ пробегает $\varphi(d)$ мультипликативных характеров порядка d поля $\mathbb{F}_q$. Здесь μ обозначает функцию Мёбиуса (см. определение 3.22), а φ — функцию Эйлера (см. теорему 1.15 (iv)).

5.15. Показать, что $\eta(2)=(-1)^{(q^2-1)/8}$, где η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики (определение η см. в примере 5.10).

5.16. Пусть $\mathbb{F}_q$ — конечное поле характеристики p и $r\in\mathbb{N}$. Доказать, что в обозначениях теоремы 5.7 для любого мультипликативного характера ψ поля $\mathbb{F}_q$ и любого $b\in\mathbb{F}_q$ имеет место равенство $G(\psi^{p^r},\chi_b)=G(\psi,\chi_{\rho(b)})$, где $\rho(b)=b^{p^r}$. Здесь G — сумма Гаусса.

5.17. Доказать, что для любого мультипликативного характера ψ поля $\mathbb{F}_q$ справедливо равенство

$$\sum_{\chi}G(\psi,\chi)=0,$$

где χ пробегает множество всех аддитивных характеров поля $\mathbb{F}_q$.

5.18. Доказать, что для любого аддитивного характера χ поля $\mathbb{F}_q$ справедливо равенство

$$\sum_{\psi}G(\psi,\chi)=(q-1)\chi(1),$$

где ψ пробегает множество всех мультипликативных характеров поля $\mathbb{F}_q$.

5.19. Пусть $s \in \mathbb{N}$, $q = p^s$, где p — простое нечетное число, и η — квадратичный характер поля $\mathbb{F}_q$. Доказать, что если χ_b $(b \in \mathbb{F}_q)$ — аддитивный характер поля $\mathbb{F}_q$, определенный в теореме 5.7, то справедливо равенство

$$G(\eta, \chi_b) = \eta(b)(-1)^{(q+1)/2} i^{s(p^2+2p+5)/4} q^{1/2}.$$

5.20. Доказать, что если η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики, то в обозначениях теоремы 5.7 справедливо равенство

$$G(\eta, \chi_a) G(\eta, \chi_b) = \eta(-ab) q \quad \text{для любых } a, b \in \mathbb{F}_q^*.$$

5.21. Применить квадратичный закон взаимности (см. теорему 5.17) для вычисления символов Лежандра $\left(\frac{13}{59}\right)$ и $\left(\frac{7}{61}\right)$. Определение символа Лежандра дается в примере 5.10.

5.22. Найти все простые числа p, для которых $\left(\frac{-3}{p}\right) = 1$.

5.23. Найти все степени q простых нечетных чисел, для которых квадратичный характер η поля $\mathbb{F}_q$ удовлетворяет условию $\eta(3) = 1$.

5.24. Доказать, что квадратный многочлен $x^2 + ax + b$ над полем $\mathbb{F}_q$ нечетной характеристики неприводим тогда и только тогда, когда $\eta(a^2 - 4b) = -1$, где η — квадратичный характер поля $\mathbb{F}_q$.

5.25. Выяснить, будет ли квадратный многочлен $x^2 + 12x + 41$ неприводимым в кольце $\mathbb{F}_{227}[x]$.

5.26. Пусть p и r — различные нечетные простые числа и s — такое натуральное число, что $r^s \equiv 1 \pmod{p}$. Определим для целого числа k и элемента ζ порядка p группы $\mathbb{F}_{r^s}^*$ элемент $G_k \in \mathbb{F}_{r^s}$ равенством

$$G_k = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \zeta^{kc},$$

где $\left(\frac{c}{p}\right)$ — символ Лежандра. Доказать следующие свойства: (i) $G_k = \left(\frac{k}{p}\right) G_1$; (ii) $G_1^2 = (-1)^{(p-1)/2} p$, где правая часть равенства рассматривается как элемент поля $\mathbb{F}_r$.

5.27. Использовать результат упр. 5.26 для доказательства квадратичного закона взаимности (теоремы 5.17).

5.28. Пусть $\lambda_1, \ldots, \lambda_k$ — мультипликативные характеры поля $\mathbb{F}_q$. Доказать, что если характер λ_k нетривиален, а характер $\lambda_1 \ldots \lambda_k$ тривиален, то справедливо равенство

$$J(\lambda_1, \ldots, \lambda_k) = -\lambda_k(-1) J(\lambda_1, \ldots, \lambda_{k-1}).$$

Здесь J — сумма Якоби.

5.29. Пусть $\lambda_1, \ldots, \lambda_k$ — мультипликативные характеры поля $\mathbb{F}_q$. Доказать, что если хотя бы один из характеров λ_i нетривиален, $1 \leqslant i \leqslant k$, то

$$\sum_{a \in \mathbb{F}_q} J_a(\lambda_1, \ldots, \lambda_k) = 0.$$

5.30. Пусть $\lambda_1, \ldots, \lambda_k$ — заданные мультипликатнвные характеры поля $\mathbb{F}_q$. Доказать, что имеет место равенство

$$\sum_{\lambda} J(\lambda, \lambda_1, \ldots, \lambda_k) = (q-1) J_0(\lambda_1, \ldots, \lambda_k) + J(\lambda_1, \ldots, \lambda_k),$$

где сумма распространяется на все мультипликативные характеры λ поля $\mathbb{F}_q$.

5.31. Пусть χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$ и a, b_1, ..., $b_k \in \mathbb{F}_q$. Доказать, что

$$\sum_{c_1+\ldots+c_k=a} \chi(b_1c_1+\cdots+b_kc_k) = \begin{cases} \chi(ab_1)\,q^{k-1}, & \text{если } b_1=\ldots=b_k, \\ 0 & \text{в противном случае.} \end{cases}$$

5.32. Используя соотношение (5.16) и результат упр. 5.31, дать другое доказательство формулы из теоремы 5.21, выражающей сумму Якоби $J(\lambda_1, \ldots, \lambda_k)$ через суммы Гаусса. (*Указание.* Показать сначала, что при стандартном соглашении относительно $\psi(0)$ (т. е. $\psi(0)$ равно 0 для нетривиального и равно 1 для тривиального характера ψ) равенство (5.16) выполняется для $c=0$ и нетривиального характера ψ.)

5.33. Использовать (5.16) и результат упр. 5.31 для доказательства следующего утверждения. Пусть $\lambda_1, \ldots, \lambda_k$ — мультипликативные характеры поля $\mathbb{F}_q$, причем $\lambda_1, \ldots, \lambda_k$ нетривиальны, а $\lambda_1 \ldots \lambda_k$ тривиален. Тогда для любого нетривиального аддитивного характера χ поля $\mathbb{F}_q$ справедливо равенство

$$J_0(\lambda_1, \ldots, \lambda_k) = \left(1-\frac{1}{q}\right) G(\lambda_1, \chi) \ldots G(\lambda_k, \chi).$$

5.34. Доказать, что если $\lambda_1, \ldots, \lambda_k$ — нетривиальные мультипликативные, а χ — нетривиальный аддитивный характеры поля $\mathbb{F}_q$, то справедливо равенство

$$J(\lambda_1, \ldots, \lambda_k) = \frac{1}{q} G(\lambda_1, \chi) \ldots G(\lambda_k, \chi) G(\overline{\lambda_1 \ldots \lambda_k}, \bar{\chi}).$$

5.35. Доказать, что если λ_1, λ_2, λ_3, $\lambda_1\lambda_2$ и $\lambda_1\lambda_3$ — нетривиальные мультипликативные характеры поля $\mathbb{F}_q$, то

$$J(\lambda_1, \lambda_2) J(\lambda_1\lambda_2, \lambda_3) = J(\lambda_1, \lambda_3) J(\lambda_1\lambda_3, \lambda_2).$$

5.36. Пусть $\lambda_1, \ldots, \lambda_k$ — нетривиальные мультипликативные характеры поля $\mathbb{F}_q$ и $1 \leqslant h < k$. Доказать, что если характер $\lambda_1 \ldots \lambda_h$ нетривиален, то

$$J(\lambda_1, \ldots, \lambda_k) = J(\lambda_1, \ldots, \lambda_h) J(\lambda_1 \ldots \lambda_h, \lambda_{h+1}, \ldots, \lambda_k).$$

5.37. Пусть $k \geqslant 3$ и $\lambda_1, \ldots, \lambda_k$ — мультипликативные характеры поля $\mathbb{F}_q$, причем λ_1 и λ_k нетривиальны, а $\lambda_1 \ldots \lambda_k$ тривиален. Доказать, что

$$J(\lambda_1, \ldots, \lambda_{k-1}) = (\lambda_2 \ldots \lambda_{k-1})(-1) J(\lambda_2, \ldots, \lambda_k).$$

5.38. Пусть ψ — мультипликативный характер порядка $m \geqslant 2$ поля $\mathbb{F}_q$, а χ — нетривиальный аддитивный характер этого поля. Доказать, что

$$G(\psi, \chi)^k = \begin{cases} -qJ(\psi, \ldots, \psi), & \text{если } m \text{ делит } k, \\ G(\psi^k, \chi) J(\psi, \ldots, \psi) & \text{в противном случае,} \end{cases}$$

где суммы Якоби зависят от k характеров ψ.

5.39. Доказать, что сумма Якоби $J(\eta, \ldots, \eta)$, зависящая от k квадратичных характеров η поля $\mathbb{F}_q$ нечетной характеристики, задается формулой

$$J(\eta, \ldots, \eta) = \begin{cases} (-1)^{(k(q-1)+4)/4} q^{(k-2)/2} & \text{при четном } k, \\ (-1)^{(k-1)(q-1)/4} q^{(k-1)/2} & \text{при нечетном } k. \end{cases}$$

5.40. Доказать, что если λ — мультиплнкативный характер нечетного порядка $m \geqslant 3$ поля $\mathbb{F}_q$, то справедливо равенство

$$J(\lambda, \lambda^2, \ldots, \lambda^{m-1}) = -q^{(m-3)/2}.$$

5.41. Пусть λ — мультипликативный характер порядка 3 поля $\mathbb{F}_q$ и χ — нетривиальный аддитивный характер того же поля. Доказать, что

$$G(\lambda, \chi)^3 = qJ(\lambda, \lambda).$$

5.42. Доказать, что если η и ψ — мультипликативные характеры порядков 2 и 3 соответственно поля $\mathbb{F}_{q^2}$ и $q \equiv -1 \pmod 6$, то $J(\eta, \psi) = q$. (*Указание.* Применить теорему 5.16.)

5.43. Доказать, что если ψ — нетривиальный мультипликативный, а η — квадратичный характеры поля $\mathbb{F}_q$ нечетной характеристики, то $J(\psi, \eta) = \psi(4)\, J(\psi, \psi)$.

5.44. Пусть η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики, а ψ — такой мультипликативный характер этого поля, что характер ψ^4 нетривиален. Доказать равенство

$$J(\psi^2, \eta) = \psi(4)\, J(\psi, \psi\eta),$$

воспользовавшись теоремой 5.28.

5.45. Доказать, что если характеры ψ и η те же, что и в упр. 5.44, то $J(\psi, \psi\eta) = \psi(4)\, J(\psi^2, \psi^2)$.

5.46. Доказать, что если η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики и ψ — мультипликативный характер порядка не менее 3 этого же поля, то справедливо равенство

$$\psi(16)\, J(\psi, \psi) = \eta(-1)\, J(\bar{\psi}\eta, \bar{\psi}\eta).$$

5.47. Доказать, что если характеры ψ и η те же, что и в упр. 5.46, то $J(\psi, \bar{\psi}\eta) = \psi(-4)\, J(\psi, \psi)$.

5.48. Пусть ψ — мультипликативный характер порядка 4 поля $\mathbb{F}_q$, где $q \equiv 1 \pmod 4$, и η — квадратичный характер этого поля. Доказать, что $J(\psi, \psi) = \psi(-1)\, J(\psi, \eta)$.

5.49. Пусть λ — мультипликативный характер порядка 3 поля $\mathbb{F}_q$, где $q \equiv 1 \pmod 3$. Доказать, что $J(\lambda, \lambda) = A + B\omega$, где $A, B \in Z$, $A \equiv -1 \pmod 3$, $B \equiv 0 \pmod 3$ и ω — комплексный первообразный корень третьей степени из единицы. (*Указание.* Применить теорему 5.27 и использовать сравнения в кольце целых алгебраических чисел.)

5.50. Пусть λ — мультипликативный характер порядка 4 простого поля $\mathbb{F}_q$, где $p \equiv 1 \pmod 4$. Доказать, что $J(\lambda, \lambda) = A + Bi$, где A и B — целые числа, такие, что $A^2 + B^2 = p$, причем $A \equiv -1 \pmod 4$.

5.51. Доказать, что каждое простое число p вида $p \equiv 1 \pmod 3$ можно представить в виде $p = A^2 - AB + B^2$, где $A, B \in Z$.

5.52. Для тех же мультипликативных характеров λ и ψ, что и в теореме 5.28, доказать, что если число m нечетно, то соотношение Дэвенпорта—Хассе (см. теорему 5.28) эквивалентно равенству

$$J(\psi, \psi\lambda, \ldots, \psi\lambda^{m-1}) = \bar{\psi}(m^m)\, q^{(m-1)/2}.$$

5.53. Пусть χ — аддитивный характер поля $\mathbb{F}_q$, а ψ — мультипликативный характер порядка m этого поля. Доказать, что

$$G(\psi, \chi)^m = A_0 + A_1\zeta + \cdots + A_{m-1}\zeta^{m-1},$$

где $A_0, A_1, \ldots, A_{m-1} \in Z$, а ζ — комплексный первообразный корень m-й степени из единицы.

5.54. Доказать, что если $a, b \in \mathbb{F}_q$, $a \neq b$, и ψ — нетривиальный мультипликативный характер поля $\mathbb{F}_q$, то

$$\sum_{c \in \mathbb{F}_q} \psi(c + a)\, \bar{\psi}(c + b) = -1.$$

5.55. Пусть ψ — нетривиальный мультипликативный характер поля $\mathbb{F}_q$, и пусть S — произвольное подмножество в $\mathbb{F}_q$, состоящее из h элементов. Доказать, что

$$\sum_{c \in \mathbb{F}_q} \left| \sum_{a \in S} \psi(c+a) \right|^2 = h(q-h).$$

5.56. Пусть λ_1, λ_2, λ_3 — нетривиальные мультипликативные характеры поля $\mathbb{F}_q$ и $a_1, a_2 \in \mathbb{F}_q$, $a_1 \neq a_2$. Доказать, что

$$\sum_{b \in \mathbb{F}_q} \left| \sum_{c \in \mathbb{F}_q} \lambda_1(c+a_1)\lambda_2(c+a_2)\lambda_3(c+b) \right|^2 = \begin{cases} q^2-3q, & \text{если } \lambda_1\lambda_2 \text{ — нетривиальный характер,} \\ q^2-2q-1, & \text{если } \lambda_1\lambda_2 \text{ — тривиальный характер.} \end{cases}$$

5.57. Пусть ψ — мультипликативный характер порядка $m > 1$ поля $\mathbb{F}_q$ и $a \in \mathbb{F}_q$. Доказать, что

$$\sum_{c \in \mathbb{F}_q} \psi(ac^n) = \begin{cases} (q-1)\psi(a), & \text{если } m \text{ делит } n, \\ 0 & \text{в противном случае.} \end{cases}$$

5.58. Пусть $n \in \mathbb{N}$, $a, b \in \mathbb{F}_q^*$ и ψ — нетривиальный мультиплнкативный характер поля $\mathbb{F}_q$. Доказать, что

$$\sum_{c \in \mathbb{F}_q} \psi(ac^n + b) = \psi(b) \sum_{j=1}^{d-1} \bar{\lambda}^j(a)\, \lambda^j(-b)\, J(\lambda^j, \psi),$$

где λ — мультипликативный характер поля $\mathbb{F}_q$, имеющий порядок $d = \text{НОД}(n, q-1)$.

5.59. Доказать, что если η — квадратичный характер поля $\mathbb{F}_q$, $q \equiv 3 \pmod 4$ и $f \in \mathbb{F}_q[x]$ — нечетный многочлен (т. е. $f(-x) = -f(x)$), то $\sum_{c \in \mathbb{F}_q} \eta(f(c)) = 0$.

5.60. Пусть $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$, где q нечетно, и $a_2 \neq 0$. Доказать, что если ψ — мультипликативный характер порядка не менее 3 поля $\mathbb{F}_q$, а η — квадратичный характер этого поля, то

$$\sum_{c \in \mathbb{F}_q} \psi(f(c)) = \bar{\psi}(4a_2)\psi(-d)\eta(d)J(\psi, \eta),$$

где $d = a_1^2 - 4a_0a_2$.

5.61. Доказать, что для p-многочлена

$$L(x) = a_rx^{p^r} + a_{r-1}x^{p^{r-1}} + \cdots + a_1x^p + a_0x$$

над полем $\mathbb{F}_q$ характеристики p условие $a_r + a_{r-1}^p + \ldots + a_1^{p^{r-1}} + a_0^{p^r} = 0$ (см. теорему 5.34) выполняется в том и только том случае, когда $L(x) = M(x)^p$ — $M(x)$ для некоторого p-многочлена $M(x)$ над $\mathbb{F}_q$.

5.62. В связи с теоремой 5.39 доказать следующий результат. Пусть $m \in \mathbb{N}$ и $f \in \mathbb{F}_q[x]$ — нормированный многочлен положительной степени, являющийся m-й степенью какого-либо многочлена (над некоторым расширением поля $\mathbb{F}_q$). Тогда существует нормированный многочлен $g \in \mathbb{F}_q[x]$, такой, что $f = g^m$.

5.63. Пусть $a_1, \ldots, a_k$ — различные k элемеитов поля $\mathbb{F}_q$ нечетной характеристики, и пусть $\varepsilon_1, \ldots, \varepsilon_k$ — заданные k целых чисел, каждое из которых равно 1 или -1. Пусть $N(\varepsilon_1, \ldots, \varepsilon_k)$ обозначает число элементов $c \in \mathbb{F}_q$, таких,

что $\eta(c+a_j)=\varepsilon_j$ для $1\leqslant j\leqslant k$, где η — квадратичный характер поля $\mathbb{F}_q$. Доказать, что

$$N(\varepsilon_1, \ldots, \varepsilon_k)=\frac{1}{2^k}\sum_{c\in\mathbb{F}_q}[1+\varepsilon_1\eta(c+a_1)]\ldots[1+\varepsilon_k\eta(c+a_k)]-A,$$

где $0\leqslant A\leqslant k/2$.

5.64. Доказать неравенство

$$\left|N(\varepsilon_1, \ldots, \varepsilon_k)-\frac{q}{2^k}\right|\leqslant\left(\frac{k-2}{2}+\frac{1}{2^k}\right)q^{1/2}+\frac{k}{2},$$

используя упр. 5.63 и оценки для сумм значений характеров.

5.65. Пусть ψ — мультипликативный характер порядка $m\geqslant 2$ поля $\mathbb{F}_q$, $a_1, \ldots, a_k$ — различные k элементов этого поля и $\varepsilon_1, \ldots, \varepsilon_k$ — заданные k комплексных корней m-й степени из единицы. Пусть $N(\varepsilon_1, \ldots, \varepsilon_k)$ обозначает число элементов $c\in\mathbb{F}_q$, удовлетворяющих условию $\psi(c+a_j)=\varepsilon_j$ для $1\leqslant j\leqslant k$. Доказать, что

$$N(\varepsilon_1, \ldots, \varepsilon_k)=\frac{1}{m^k}\sum_{c\in\mathbb{F}_q}\prod_{j=1}^{k}\{1+\varepsilon_j^{-1}\psi(c+a_j)+\varepsilon_j^{-2}\psi^2(c+a_j)+\ldots$$

$$\ldots+\varepsilon_j^{-m+1}\psi^{m-1}(c+a_j)\}-A,$$

где $0\leqslant A\leqslant k/m$.

5.66. Доказать неравенство

$$\left|N(\varepsilon_1, \ldots, \varepsilon_k)-\frac{q}{m^k}\right|\leqslant\left(k-1-\frac{k}{m}+\frac{1}{m^k}\right)q^{1/2}+\frac{k}{m},$$

используя упр. 5.65 и оценки для сумм значений характеров.

5.67. Пусть m и k — заданные натуральные числа. Доказать существование такого действительного числа $q_0(m, k)$, что для любого числа q, являющегося степенью простого числа и удовлетворяющего неравенству $q\geqslant q_0(m, k)$, и для любых элементов $a_1, \ldots, a_k$ из поля $\mathbb{F}_q$ найдется такой элемент $c\in\mathbb{F}_q$, что каждый из элементов $c+a_1, \ldots, c+a_k$ является m-й степенью некоторого элемента из $\mathbb{F}_q^*$.

5.68. Пусть ψ — некоторый мультипликативный характер поля $\mathbb{F}_{p^2}$, где p — нечетное простое число, а $\gamma\in\mathbb{F}_{p^2}^*$ — элемент порядка $2(p-1)$. Определим *сумму Эйзенштейна* $E(\psi)$ равенством

$$E(\psi)=\sum_{c\in\mathbb{F}_p}\psi(1+c\gamma).$$

Доказать, что $E(\psi)$ не зависит от выбора элемента γ.

5.69. Доказать, что сумму Эйзенштейна (см. предыдущее упражнение) можно также задать равенством

$$E(\psi)=\frac{p\psi(2)\,G(\tilde{\psi}^*, \chi_1)}{G(\tilde{\psi}, \mu_1)},$$

где χ_1 и μ_1 — канонические аддитивные характеры полей $\mathbb{F}_p$ и $\mathbb{F}_{p^2}$ соответственно, а $\tilde{\psi}^*$ — ограничение характера $\tilde{\psi}$ на $\mathbb{F}_p^*$. (*Указание.* Использовать соотношение

(5.16) и свойства сумм Гаусса.) Для случая же, когда ψ^* — нетривиальный характер, доказать, что $E(\psi)$ можно записать также в виде

$$E(\psi) = \frac{\psi(2)\, G(\psi, \mu_1)}{G(\psi^*, \chi_1)}.$$

5.70. Для элемента a конечного поля $\mathbb{F}_q$ и мультипликативного характера ψ поля $\mathbb{F}_{q^s}$, где $s \in \mathbb{N}$, определим *обобщенную сумму Эйзенштейна* $E_s(\psi; a)$ равенством

$$E_s(\psi; a) = \sum_{\mathrm{Tr}(\alpha)=a} \psi(\alpha),$$

где суммирование распространяется на все элементы $\alpha \in \mathbb{F}_{q^s}$, для которых $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = a$. Доказать, что сумма Эйзенштейна является также и обобщенной суммой Эйзенштейна, так как $E(\psi) = E_2(\psi; 2)$.

5.71. Пусть T_0 — множество всех элемеитов $\alpha \in \mathbb{F}_{q^s}$, для которых $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = 0$. Доказать, что множество B элементов $\beta \in \mathbb{F}_{q^s}$, обладающих свойством $\alpha\beta \in T_0$ для всех $\alpha \in T_0$, совпадает с полем $\mathbb{F}_q$.

5.72. Доказать, что обобщенную сумму Эйзенштейна $E_s(\psi; a)$ можно также задать равенством

$$E_s(\psi; a) = \frac{q^{s-1}\psi(a)\, G(\bar{\psi}^*, \chi_1)}{G(\bar{\psi}, \mu_1)},$$

где χ_1 и μ_1 — канонические аддитивные характеры полей $\mathbb{F}_q$ и $\mathbb{F}_{q^s}$ соответственно, а $\bar{\psi}^*$ — ограничение характера $\bar{\psi}$ на $\mathbb{F}_q^*$. (*Указание.* Использовать соотношение (5.16), упр. 5.71 и свойства сумм Гаусса.) Для случая же, когда ψ^* — нетривиальный характер, доказать, что $E_s(\psi; a)$ можно записать также в виде

$$E_s(\psi; a) = \frac{\psi(a)\, G(\psi, \mu_1)}{G(\psi^*, \chi_1)}.$$

5.73. Доказать равенства

$$E_s(\psi^p; a) = E_s(\psi; a^p), \qquad E_s(\psi^q; a) = E_s(\psi; a),$$

где p — характеристика соответствующих полей $\mathbb{F}_q$ и $\mathbb{F}_{q^s}$.

5.74. Доказать, что если $a \in \mathbb{F}_q^*$ и ψ— нетривиальный мультиплнкативный характер поля $\mathbb{F}_{q^2}$, порядок m которого делит число $q+1$, то имеет место равенство

$$E_2(\psi; a) = (-1)^{(mq-q-1)/m}.$$

(*Указание.* Применить теорему 5.16 Штикельбергера.)

5.75. Пусть ψ — мультиплнкативный характер поля $\mathbb{F}_{q^s}$ и ψ^* — его ограничение на $\mathbb{F}_q^*$. Доказать, что если характер ψ^* нетривиален и $a \in \mathbb{F}_q^*$, то $|E_s(\psi; a)| = q^{(s-1)/2}$. (*Указание.* Воспользоваться результатом упр. 5.9.)

5.76. Доказать следующее свойство суммы Эйзенштейна: если ограничение ψ^* мультипликативного характера ψ поля $\mathbb{F}_{p^2}$ на $\mathbb{F}_p^*$ является нетривиальным характером, то

$$\frac{E(\psi)^2}{E(\psi^2)} = \frac{J(\psi, \psi)}{J(\psi^*, \psi^*)}.$$

5.77. Доказать следующее свойство обобщенной суммы Эйзенштейна: если ограничения $\psi_1^*, \ldots, \psi_k^*$ мультипликативных характеров $\psi_1, \ldots, \psi_k$ поля $\mathbb{F}_{q^s}$ на $\mathbb{F}_q^*$ нетривиальны, то для любого $a \in \mathbb{F}_q^*$ справедливо равенство

$$\frac{E_s(\psi_1; a) \ldots E_s(\psi_k; a)}{E_s(\psi_1 \ldots \psi_k; a)} = \frac{J(\psi_1, \ldots, \psi_k)}{J(\psi_1^*, \ldots, \psi_k^*)}.$$

5.78. Доказать, что если ограничение ψ^* на $\mathbb{F}_p^*$ мультипликативного характера ψ поля $\mathbb{F}_{p^2}$ является нетривиальным характером, то $E(\psi^{p+1}) = -J(\psi^*, \eta_p)$, где η_p — квадратичный характер поля $\mathbb{F}_p$.

5.79. Доказать, что суммы Клостермана (см. определение 5.42) обладают свойством $K(\chi; a, b) = K(\chi; b, a)$ для всех $a, b \in \mathbb{F}_q$.

5.80. Доказать, что если $a, b \in \mathbb{F}_q$ и хотя бы один из элементов a и b не равен нулю, то $K(\chi; a, b) = K(\chi; ab, 1) = K(\chi; 1, ab)$.

5.81. В обозначениях теоремы 5.43 доказать, что

$$K(\chi; a, b)^4 + K(\chi^{(4)}; a, b) + 4qK(\chi^{(2)}; a, b) = 6q^2 \quad \text{для } a, b \in \mathbb{F}_q^*.$$

5.82. Пусть $\mathbb{F}_q$ — поле нечетной характеристики, f и g — квадратные многочлены над $\mathbb{F}_q$ и χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$. Выразить сумму $\sum_c \chi(f(c) g(c)^{-1})$ через суммы Клостермана (здесь c пробегает все элементы поля $\mathbb{F}_q$, для которых $g(c) \neq 0$).

5.83. Пусть ψ — мультипликативный, а χ — аддитивный характеры поля $\mathbb{F}_q$ и $a, b \in \mathbb{F}_q$. Определим *обобщенную сумму Клостермана* равенством

$$K(\psi, \chi; a, b) = \sum_{c \in \mathbb{F}_q^*} \psi(c) \chi(ac + bc^{-1}).$$

Доказать, что если $ab = 0$, то такая сумма сводится к сумме Гаусса в следующем смысле:

$$K(\psi, \chi; a, b) = \begin{cases} \psi(b) G(\bar{\psi}, \chi), & \text{если } a = 0, b \neq 0, \\ \bar{\psi}(a) G(\psi, \chi), & \text{если } a \neq 0, b = 0, \\ G(\psi, \chi_0), & \text{если } a = b = 0. \end{cases}$$

5.84. Доказать, что если η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики и $a, b \in \mathbb{F}_q$, причем $\eta(ab) = -1$, то $K(\eta, \chi; a, b) = 0$ для любого аддитивного характера χ поля $\mathbb{F}_q$.

5.85. Доказать, что если η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики и $a, b \in \mathbb{F}_q$, причем $ab = d^2$ для некоторого $d \in \mathbb{F}_q^*$, то для каждого аддитивного характера χ поля $\mathbb{F}_q$ имеет место равенство

$$K(\eta, \chi; a, b) = \eta(b) G(\eta, \chi)(\chi(2d) + \chi(-2d)).$$

(*Указание.* Использовать соотношение (5.16) и теорему 5.47.)

5.86. Доказать, что если χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$ нечетной характеристики, η — квадратичный характер, а ψ — мультипликативный характер порядка не менее 3 того же поля, то для $a, b \in \mathbb{F}_q$, $b \neq 0$, имеет место равенство

$$K(\psi, \chi; a, b) = \frac{\psi(4b) G(\eta, \chi)}{G(\bar{\psi}\eta, \chi)} \sum_{c \in \mathbb{F}_q} \chi(c) (\bar{\psi}\eta)(c^2 - 4ab).$$

5.87. Показать непосредственно, что $H_1(a) = H_1(1)$ для любого $a \in \mathbb{F}_q^*$, где q нечетно и $H_1(a)$ — сумма Якобсталя (см. определение 5.49). Вычислить

затем сумму $\sum_{a \in \mathbb{F}_q^*} H_1(a)$ и, таким образом, получить другое доказательство того факта, что $H_1(a) = -1$ для любого $a \in \mathbb{F}_q^*$.

5.88. Пусть $n \in \mathbb{N}$ — нечетное число и η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики. Доказать, что для любого $a \in \mathbb{F}_q^*$ имеет место равенство

$$H_n(a) = \eta(a) I_n(a^{-1}) - 1,$$

где $H_n(a)$ — сумма Якобсталя, а $I_n(a)$ определяется равенством (5.68). (*Замечание.* Это снова доказывает, что $H_1(a) = -1$ для любого $a \in \mathbb{F}_q^*$.)

5.89. Доказать, что для нечетного $n \in \mathbb{N}$ и любого $a \in \mathbb{F}_q^*$, где q нечетно, имеет место равенство

$$I_{2n}(a) = \eta(a) H_n(a^{-1}) + H_n(a) + \eta(a).$$

5.90. Доказать, что если $a \in \mathbb{F}_q^*$, где $q \equiv 3 \pmod 4$, то $I_4(a) = -1$.

5.91. Пусть p — такое простое число, что $p \equiv 1 \pmod 4$. Доказать, что

$$I_4(-1) = \begin{cases} -1 + 2A, & \text{если } p \equiv 1 \pmod 8, \\ -1 - 2A, & \text{если } p \equiv 5 \pmod 8, \end{cases}$$

где A определяется условиями $p = A^2 + B^2$, $A, B \in \mathbb{Z}$, $A \equiv 3 \pmod 4$.

5.92. Найти разложения в непрерывные дроби (см. рассуждение перед леммой 5.54) рациональной функции $(x^5 + x^3 + x^2 + x)/(x^6 + x^5 + x^4 + x^3 + 1)$ над полем $\mathbb{F}_2$ и рациональной функции $(x^6 - x^5 - x^4 + x^3 - x^2 - 1)/(x^5 - x^3 - x^2 + 1)$ над полем $\mathbb{F}_3$.

5.93. Доказать, что если многочлены P_i и Q_i определены равенствами (5.74) и (5.75) соответственно, то справедливы равенства

$$P_i Q_{i-2} - P_{i-2} Q_i = (-1)^i A_i, \quad i = 1, \ldots, s.$$

5.94. Доказать, что

$$\deg\left(\frac{r_0}{r_1} - \frac{P_i}{Q_i}\right) = -\deg(Q_i Q_{i+1}), \quad i = 0, 1, \ldots, s-1,$$

где P_i и Q_i определены равенствами (5.74) и (5.75) соответственно.

5.95. Доказать, что рациональные функции P_i/Q_i, где P_i и Q_i определены равенствами (5.74) и (5.75), наилучшим образом приближают рациональную функцию r_0/r_1 в том смысле, что если f/g — такая рациональная функция над полем $\mathbb{F}_q$, что для некоторого i, $0 \leqslant i \leqslant s-1$, имеет место неравенство

$$\deg\left(\frac{r_0}{r_1} - \frac{f}{g}\right) < \deg\left(\frac{r_0}{r_1} - \frac{P_i}{Q_i}\right),$$

то $\deg(g) \geqslant \deg(Q_{i+1})$.

Глава 6

Уравнения над конечными полями

Мы рассмотрим здесь полиномиальные уравнения вида $f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n)$, где $f_1, f_2 \in \mathbb{F}_q[x_1, \ldots, x_n]$. Под числом решений такого уравнения в множестве $\mathbb{F}_q^n$ мы будем понимать число различных n-наборов $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, для которых $f_1(c_1, \ldots, c_n) = f_2(c_1, \ldots, c_n)$. Указанное уравнение часто представляют в следующей эквивалентной форме: $f(x_1, \ldots, x_n) = 0$, где $f = f_1 - f_2$. В некоторых частных случаях удается указать точные формулы для числа решений, но в общем случае приходится удовлетвориться оценками. Далее мы встретимся с примерами результатов каждого типа.

В первом параграфе приводятся некоторые классические теоремы о числе решений полиномиальных уравнений, такие, как теоремы Кёнига—Радоша, Шевалле и Варнинга. Здесь устанавливаются также элементарные верхние границы для числа решений и некоторые результаты об ожидаемом числе решений.

Второй и третий параграфы посвящены специальным классам уравнений, а именно квадратичным и диагональным уравнениям соответственно. Оказывается, что очень полезным инструментом при изучении этих уравнений являются тригонометрические суммы. Для квадратичных уравнений важную роль в облегчении нахождения числа решений играет теория приведения квадратичных форм к диагональному виду.

В четвертом параграфе будет продемонстрирована зависимость между оценками для числа решений некоторых уравнений и оценками для сумм значений характеров. Изучение уравнений вида $y^m = f(x)$ и $y^q - y = f(x)$ приводит к завершению доказательства важных неравенств для сумм значений характеров, рассмотренных в § 4 гл. 5 (см. теоремы 5.38 и 5.41). Методы, применяемые для исследования указанных уравнений, довольно сложны, но элементарны в том смысле, что не связаны с алгебраической геометрией и не требуют глубокого знания теории полей алгебраических функций.

§ 1. Элементарные результаты о числе решений

Мы начнем с простейшего случая, а именно с полиномиального уравнения от одной переменной. Пусть $f \in \mathbb{F}_q[x]$ — многочлен положительной степени от одной переменной. Рассмотрим

уравнение $f(x) = 0$. Решениями этого уравнения в поле $\mathbb{F}_q$ являются все различные корни многочлена f, лежащие в этом поле, и только они. Как мы видели в § 3 гл. 4, многочлен НОД $(f(x), x^q - x)$ является делителем многочлена f, все корни которого просты, причем это в точности все различные корни многочлена f, лежащие в $\mathbb{F}_q$. Поэтому число решений уравнения $f(x) = 0$ в поле $\mathbb{F}_q$ равно степени многочлена НОД $(f(x), x^q - x)$. Что же касается фактического отыскания этих решений, то мы отсылаем читателя к § 3 гл. 4.

Для определения числа решений уравнения $f(x) = 0$ в поле $\mathbb{F}_q$ можно также использовать теорию матриц. Поскольку вопрос о том, является ли нуль решением этого уравнения, выясняется тривиально, то достаточно рассмотреть лишь ненулевые решения этого уравнения. Этими решениями являются корни многочлена НОД $(f(x), x^{q-1} - 1)$ (все они различны и принадлежат полю $\mathbb{F}_q$). Поэтому мы без ограничения общности можем считать, что $\deg(f) \leqslant q - 1$. Кроме того, поскольку $b^{q-1} = 1$ для любого элемента $b \in \mathbb{F}_q^*$, то ненулевые решения уравнения

$$f(x) = a_0 + a_1 x + \cdots + a_{q-2}x^{q-2} + a_{q-1}x^{q-1} = 0$$

в поле $\mathbb{F}_q$ совпадают с ненулевыми решениями уравнения

$$(a_0 + a_{q-1}) + a_1 x + \cdots + a_{q-2}x^{q-2} = 0$$

в поле $\mathbb{F}_q$. Таким образом, можно даже предположить (без ограничения общности), что $\deg(f) \leqslant q - 2$.

Рассмотрим теперь многочлен

$$f(x) = a_0 + a_1 x + \cdots + a_{q-2}x^{q-2} \in \mathbb{F}_q[x].$$

Сопоставим с этим многочленом следующую квадратичную матрицу порядка $q - 1$:

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \ldots & a_{q-2} & a_0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{q-2} & a_0 & \ldots & a_{q-4} & a_{q-3} \end{pmatrix}. \tag{6.1}$$

Такая матрица называется *левой циркулянтной* матрицей; в ней каждая строка получается из расположенной над нею циклическим сдвигом на один элемент влево.

6.1. Теорема (теорема Кёнига—Радоша). *Пусть*

$$f(x) = a_0 + a_1 x + \cdots + a_{q-2}x^{q-2} \in \mathbb{F}_q[x].$$

Тогда число ненулевых решений уравнения $f(x) = 0$ *в поле* $\mathbb{F}_q$ *равно* $q - 1 - r$, *где* r — *ранг матрицы* A, *заданной формулой* (6.1).

Доказательство. Пусть $b_1, \ldots, b_{q-1}$ — различные элементы группы $\mathbb{F}_q^*$; образуем из них матрицу Вандермонда

$$B = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ b_1 & b_2 & \ldots & b_{q-1} \\ b_1^2 & b_2^2 & \ldots & b_{q-1}^2 \\ \ldots & \ldots & \ldots & \ldots \\ b_1^{q-2} & b_2^{q-2} & \ldots & b_{q-1}^{q-2} \end{pmatrix}.$$

Учитывая, что $b^{q-1} = 1$ для каждого $b \in \mathbb{F}_q^*$, получим

$$AB = \begin{pmatrix} f(b_1) & f(b_2) & \ldots & f(b_{q-1}) \\ b_1^{-1} f(b_1) & b_2^{-1} f(b_2) & \ldots & b_{q-1}^{-1} f(b_{q-1}) \\ b_1^{-2} f(b_1) & b_2^{-2} f(b_2) & \ldots & b_{q-1}^{-2} f(b_{q-1}) \\ \ldots & \ldots & \ldots & \ldots \\ b_1^{-(q-2)} f(b_1) & b_2^{-(q-2)} f(b_2) & \ldots & b_{q-1}^{-(q-2)} f(b_{q-1}) \end{pmatrix}.$$

Если N — число ненулевых решений уравнения $f(x) = 0$ в поле $\mathbb{F}_q$, то можно считать, что, во-первых, $N \leqslant q - 2$ (случай $N = q - 1$ возникает лишь если A — нулевая матрица с $r = 0$) и, во-вторых, что элементы упорядочены таким образом, что $f(b_i) \neq 0$ для $1 \leqslant i \leqslant q - 1 - N$ и $f(b_i) = 0$ для $q - N \leqslant i \leqslant q - 1$. Тогда элементы в последних N столбцах матрицы AB все равны 0. Следовательно, ранг матрицы AB не превосходит числа $q - 1 - N$. С другой стороны, главный минор порядка $q - 1 - N$ матрицы AB равен

$$f(b_1) \ldots f(b_{q-1-N}) \begin{vmatrix} 1 & 1 & \ldots & 1 \\ b_1^{-1} & b_2^{-1} & \ldots & b_{q-1-N}^{-1} \\ b_1^{-2} & b_2^{-2} & \ldots & b_{q-1-N}^{-2} \\ \ldots & \ldots & \ldots & \ldots \\ b_1^{-(q-2-N)} & b_2^{-(q-2-N)} & \ldots & b_{q-1-N}^{-(q-2-N)} \end{vmatrix},$$

и потому он отличен от нуля (поскольку выписанный определитель Вандермонда образован различными элементами $b_1^{-1}, \ldots, b_{q-1-N}^{-1}$). Следовательно, ранг матрицы AB равен $q - 1 - N$. Но матрица B невырожденна ввиду того, что все элементы $b_1, \ldots, b_{q-1}$ различны. Поэтому матрицы AB и A имеют один и тот же ранг. Итак, мы получаем, что $r = q - 1 - N$, или $N = q - 1 - r$. □

6.2. Пример. Пусть $f(x) = 3 + x - 3x^2 + 2x^3 \in \mathbb{F}_7[x]$. Тогда соответствующая матрица A имеет вид

$$A = \begin{pmatrix} 3 & 1 & -3 & 2 & 0 & 0 \\ 1 & -3 & 2 & 0 & 0 & 3 \\ -3 & 2 & 0 & 0 & 3 & 1 \\ 2 & 0 & 0 & 3 & 1 & -3 \\ 0 & 0 & 3 & 1 & -3 & 2 \\ 0 & 3 & 1 & -3 & 2 & 0 \end{pmatrix};$$

ее ранг r равен 6. Таким образом, по теореме Кёнига—Радоша уравнение $f(x) = 0$ не имеет ненулевых решений в поле $\mathbb{F}_7$. А поскольку и нуль, очевидно, тоже не является решением этого уравнения, то уравнение $f(x) = 0$ вообще не имеет решений в поле $\mathbb{F}_7$. Другими словами, многочлен $f(x)$ неприводим над полем $\mathbb{F}_7$.

Перейдем теперь к многочленам от нескольких переменных. Некоторые элементарные результаты о числе решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ удается установить для случая, когда число n переменных больше степени многочлена f (степень многочлена от нескольких переменных вводится определением 1.72).

6.3. Лемма. *Пусть k — целое неотрицательное число. Тогда*

$$\sum_{c \in \mathbb{F}_q} c^k = \begin{cases} 0, & \text{если } k = 0 \text{ или } k \text{ не делится на } q-1, \\ -1, & \text{если } k > 0 \text{ и } k \text{ делится на } q-1. \end{cases}$$

Доказательство. При $k = 0$ применяем стандартное соглашение $0^0 = 1$; тогда утверждение тривиально $\left(\sum\limits_{c \in \mathbb{F}_q} c^0 = q = 0\right)$. Если $k \in \mathbb{N}$ и k делится на $q-1$, то для любого $c \in \mathbb{F}_q^*$ имеем $c^k = 1$, так что $\sum\limits_{c \in \mathbb{F}_q} c^k = \sum\limits_{c \in \mathbb{F}_q^*} c^k = q - 1 = -1$. Наконец, при $k \in \mathbb{N}$, не делящемся на $q-1$, выберем в поле $\mathbb{F}_q$ примитивный элемент b. Тогда, применяя формулу суммы геометрической прогрессии, получаем

$$\sum_{c \in \mathbb{F}_q} c^k = \sum_{c \in \mathbb{F}_q^*} c^k = \sum_{j=0}^{q-2} b^{jk} = \sum_{j=0}^{q-2} (b^k)^j = \frac{b^{(q-1)k} - 1}{b^k - 1} = 0. \quad \square$$

6.4. Лемма. *Пусть $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — многочлен степени, меньшей чем $n(q-1)$. Тогда*

$$\sum_{c_1, \ldots, c_n \in \mathbb{F}_q} f(c_1, \ldots, c_n) = 0.$$

Доказательство. Учитывая линейность, это равенство достаточно доказать для одночлена $x_1^{k_1} \dots x_n^{k_n}$, где $k_1 + \dots + k_n < n(q-1)$. Из указанного неравенства вытекает существование такого j, $1 \leqslant j \leqslant n$, что $0 \leqslant k_j < q-1$. Поэтому

$$\sum_{c_1, \dots, c_n \in \mathbb{F}_q} c_1^{k_1} \dots c_n^{k_n} = \left(\sum_{c_1 \in \mathbb{F}_q} c_1^{k_1}\right) \dots \left(\sum_{c_n \in \mathbb{F}_q} c_n^{k_n}\right) = 0$$

в силу леммы 6.3. □

6.5. Теорема (теорема Варнинга). *Пусть* $f \in \mathbb{F}_q[x_1, \dots, x_n]$ — *многочлен от* n *переменных степени, меньшей чем* n. *Тогда число решений уравнения* $f(x_1, \dots, x_n) = 0$ *в* $\mathbb{F}_q^n$ *делится на характеристику* p *поля* $\mathbb{F}_q$.

Доказательство. Рассмотрим многочлен $F = 1 - f^{q-1}$, который обладает тем свойством, что $F(c_1, \dots, c_n) = 1$, если $f(c_1, \dots, c_n) = 0$, и $F(c_1, \dots, c_n) = 0$, если $f(c_1, \dots, c_n) \neq 0$. Тогда

$$\sum_{c_1, \dots, c_n \in \mathbb{F}_q} F(c_1, \dots, c_n) = N, \tag{6.2}$$

где N — число решений уравнения $f(x_1, \dots, x_n) = 0$ в $\mathbb{F}_q^n$. С другой стороны, из условия $\deg(f) < n$ следует, что $\deg(F) < n(q-1)$, поэтому из леммы 6.4 вытекает, что сумма в (6.2) равна нулю. Следовательно, число N, рассматриваемое как элемент поля $\mathbb{F}_q$, равно 0, а это и означает, что N делится на p. □

6.6. Следствие (теорема Шевалле). *Пусть* $f \in \mathbb{F}_q[x_1, \dots, x_n]$ — *многочлен степени, меньшей чем* n, *причем* $f(0, \dots, 0) = 0$. *Тогда уравнение* $f(x_1, \dots, x_n) = 0$ *имеет хотя бы одно нетривиальное решение в* $\mathbb{F}_q^n$, *т. е. существует такой* n-*набор* $(c_1, \dots, c_n) \in \mathbb{F}_q^n$, $(c_1, \dots, c_n) \neq (0, \dots, 0)$, *что* $f(c_1, \dots, c_n) = 0$.

Доказательство. Из условия $f(0, \dots, 0) = 0$ следует, что число N решений рассматриваемого уравнения удовлетворяет неравенству $N \geqslant 1$. Применяя теперь теорему 6.5, получаем, что $N \geqslant p \geqslant 2$. □

Заметим, что условие $\deg(f) < n$ в теореме 6.5 и следствии 6.6 является наилучшим возможным. Сейчас мы построим такой многочлен степени n от n переменных, для которого утверждения теорем Варнинга и Шевалле не выполняются.

6.7. Пример. Пусть $n \in \mathbb{N}$, и пусть $\{\alpha_1, \dots, \alpha_n\}$ — базис поля $E = \mathbb{F}_{q^n}$ (как векторного пространства) над $\mathbb{F}_q$. Положим

$$f(x_1, \dots, x_n) = \prod_{j=0}^{n-1} (\alpha_1^{q^j} x_1 + \dots + \alpha_n^{q^j} x_n).$$

Так как элементы $\alpha_i^{q^j}$, $j = 0, 1, \ldots, n-1$, сопряжены с α_i относительно $\mathbb{F}_q$ (см. определение 2.17), то коэффициенты многочлена f принадлежат полю $\mathbb{F}_q$. Ясно, что $\deg(f) = n$. Для произвольного n-набора $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ положим $\gamma = c_1\alpha_1 + \ldots + c_n\alpha_n \in E$. Тогда

$$f(c_1, \ldots, c_n) = \prod_{j=0}^{n-1} (\alpha_1^{q^j} c_1 + \cdots + \alpha_n^{q^j} c_n) =$$

$$= \prod_{j=0}^{n-1} (c_1\alpha_1 + \cdots + c_n\alpha_n)^{q^j} = \prod_{j=0}^{n-1} \gamma^{q^j} = N_{E/\mathbb{F}_q}(\gamma).$$

Таким образом, равенство $f(c_1, \ldots, c_n) = 0$ эквивалентно равенству $N_{E/\mathbb{F}_q}(\gamma) = 0$; последнее же имеет место лишь для элемента $\gamma = 0$, т. е. при $c_1 = \ldots = c_n = 0$. Это значит, что уравнение $f(x_1, \ldots, x_n) = 0$ имеет единственное решение $(0, \ldots, 0)$ в $\mathbb{F}_q^n$. Отсюда следует, что для многочлена f не выполняются ни утверждение теоремы 6.5, ни утверждение следствия 6.6. □

Теорему Варнинга и теорему Шевалле нетрудно распространить и на системы уравнений.

6.8. Теорема. *Пусть* $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ — *такие многочлены от* n *переменных, что* $\deg(f_1) + \ldots + \deg(f_m) < n$. *Тогда число* n*-наборов* $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, *для которых* $f_i(c_1, \ldots, c_n) = 0$ *при всех* i, $1 \leqslant i \leqslant m$, *делится на характеристику* p *поля* $\mathbb{F}_q$.

Доказательство. Положим

$$F = (1 - f_1^{q-1}) \ldots (1 - f_m^{q-1})$$

и проведем для этого многочлена F то же самое доказательство, что и в теореме 6.5. □

6.9. Следствие. *Пусть* $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ — *такие многочлены от* n *переменных, что* $f_i(0, \ldots, 0) = 0$ *для всех* i, $1 \leqslant i \leqslant m$, *и* $\deg(f_1) + \ldots + \deg(f_m) < n$. *Тогда существует ненулевой* n*-набор* $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, *такой, что* $f_i(c_1, \ldots, c_n) = 0$ *для всех* i, $1 \leqslant i \leqslant m$.

В теореме 6.11 мы покажем, что если в условиях теоремы 6.8 соответствующая система уравнений имеет по крайней мере одно решение, то она имеет гораздо больше решений. Предварительно введем некоторые обозначения и понятия. Пусть S — множество таких n-наборов $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, что $f_i(c_1, \ldots, c_n) = 0$ для всех i, $1 \leqslant i \leqslant m$. Будем через $|T|$ обозначать мощность (т. е. число элементов) конечного множества T, так что, например, $|S|$ — число решений в $\mathbb{F}_q^n$ системы уравнений

$f_i(x_1, \ldots, x_n) = 0$, $i = 1, \ldots, m$. Напомним (см. § 4 гл. 3) понятие *аффинного подпространства* векторного пространства, под которым мы понимаем сдвиг некоторого подпространства этого векторного пространства. Под *размерностью* аффинного подпространства по определению понимается размерность соответствующего подпространства. Два аффинных подпространства назовем *параллельными*, если они получаются сдвигами одного и того же подпространства.

6.10. Лемма. *Пусть выполнены условия теоремы* 6.8. *Если* W_1 *и* W_2 *— два параллельных аффинных подпространства размерности* $d = \deg(f_1) + \ldots + \deg(f_m)$ *векторного пространства* $\mathbb{F}_q^n$ *над полем* $\mathbb{F}_q$ *характеристики* p, *то*

$$|W_1 \cap S| \equiv |W_2 \cap S| \pmod{p}.$$

Доказательство. Случай $W_1 = W_2$ тривиален, так что можно предположить, что $W_1 \neq W_2$. Произведя соответствующим образом подобранное невырожденное линейное преобразование (которое не может изменить степени многочленов f_i), мы можем добиться, чтобы аффинные подпространства W_1 и W_2 определялись условиями

$$W_1 = \{(c_1, \ldots, c_n) \in \mathbb{F}_q^n \mid c_1 = c_2 = \cdots = c_{n-d} = 0\},$$
$$W_2 = \{(c_1, \ldots, c_n) \in \mathbb{F}_q^n \mid c_1 = 1,\ c_2 = \cdots = c_{n-d} = 0\}.$$

Рассмотрим многочлен

$$G(x_1, \ldots, x_n) =$$
$$= (-1)^{n-d}\left(x_1^{q-2} + \cdots + x_1 + 1\right)\left(x_2^{q-1} - 1\right) \ldots \left(x_{n-d}^{q-1} - 1\right)$$

степени $(n - d)(q - 1) - 1$. Этот многочлен G принимает значение -1 на аффинном подпространстве W_1, значение 1 на W_2 и значение 0 во всех остальных точках пространства $\mathbb{F}_q^n$. Теперь положим

$$H = \left(1 - f_1^{q-1}\right) \ldots \left(1 - f_m^{q-1}\right) G.$$

Для многочлена H имеем

$$\deg(H) = d(q - 1) + (n - d)(q - 1) - 1 =$$
$$= n(q - 1) - 1 < n(q - 1),$$

при этом H принимает значение -1 на множестве $W_1 \cap S$, значение 1 на $W_2 \cap S$ и значение 0 в остальных точках. Таким образом,

$$\sum_{c_1, \ldots, c_n \in \mathbb{F}_q} H(c_1, \ldots, c_n) = |W_2 \cap S| - |W_1 \cap S|.$$

С другой стороны, на основании леммы 6.4 эта сумма равна нулю. Отсюда вытекает требуемый результат. □

6.11. Теорема. *Пусть* $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ — *такие многочлены, что* $d = \deg(f_1) + \ldots + \deg(f_m) < n$. *Если имеется хотя бы один* n*-набор* $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, *такой, что* $f_i(c_1, \ldots, c_n) = 0$ *для всех* i, $1 \leqslant i \leqslant m$, *то число* N *таких* n*-наборов удовлетворяет неравенству* $N \geqslant q^{n-d}$.

Доказательство. Рассмотрим два случая. В первом случае предположим, что существует хотя бы одно аффинное подпространство W_1 размерности d векторного пространства $\mathbb{F}_q^n$ над полем $\mathbb{F}_q$ характеристики p, для которого $|W_1 \cap S| \not\equiv 0 \pmod{p}$. В таком случае из леммы 6.10 мы получаем, что $|W_2 \cap S| \not\equiv 0 \pmod{p}$ для каждого аффинного подпространства W_2, параллельного W_1, так что $|W_2 \cap S| \geqslant 1$. Представим теперь множество S решений в $\mathbb{F}_q^n$ системы уравнений $f_i(x_1, \ldots, x_n) = 0$, $i = 1, \ldots, m$, в виде объединения попарно непересекающихся множеств: $S = \bigcup_W (W \cap S)$, где W пробегает все q^{n-d} различных аффинных подпространств, параллельных W_1 (включая соответствующее векторное подпространство). Тогда

$$N = |S| = \sum_W |W \cap S| \geqslant q^{n-d}.$$

Осталось рассмотреть случай, когда $|W \cap S| \equiv 0 \pmod{p}$ для всех аффинных подпространств W размерности d векторного пространства $\mathbb{F}_q^n$. Так как по предположению $N = |S| \geqslant 1$, то существует натуральное число k, $1 \leqslant k \leqslant d$, такое, что для каждого аффинного подпространства V размерности k имеет место сравнение $|V \cap S| \equiv 0 \pmod{p}$, однако существует некоторое аффинное подпространство U размерности $k-1$, для которого $|U \cap S| \not\equiv 0 \pmod{p}$. Зафиксируем одно из таких аффинных подпространств U. Рассмотрим теперь все аффинные подпространства V размерности k, содержащие U. Число таких V равно [1])

$$\frac{q^n - q^{k-1}}{q^k - q^{k-1}} = \frac{q^{n-k+1} - 1}{q - 1} = q^{n-k} + \cdots + q + 1.$$

Для каждого такого аффинного подпространства V рассмотрим теоретико-множественную разность $V \setminus U$. Имеем

$$|(V \setminus U) \cap S| = |V \cap S| - |U \cap S| \not\equiv 0 \pmod{p},$$

[1]) Каждая точка $\alpha \in \mathbb{F}_q^n \setminus U$ однозначно определяет такое V, причем все $q^k - q^{k-1}$ точек из $V \setminus U$ определяют V. — *Прим. перев.*

откуда следует, что $|(V \setminus U) \cap S| \geqslant 1$. Поскольку множество U и все разности $V \setminus U$ образуют разбиение множества $\mathbb{F}_q^n$, то

$$N = |S| = |U \cap S| + \sum_V |(V \setminus U) \cap S| \geqslant$$

$$\geqslant q^{n-k} + \cdots + q + 2 > q^{n-d},$$

так как $k \leqslant d$. □

6.12. Пример. Неравенство $N \geqslant q^{n-d}$ из теоремы 6.11 опять является наилучшим из возможных (даже для $m = 1$) в том смысле, что для любых натуральных чисел d и n, $d < n$, существует такой многочлен $f_1 \in \mathbb{F}_q[x_1, \ldots, x_n]$ степени d, что уравнение $f_1(x_1, \ldots, x_n) = 0$ имеет ровно q^{n-d} решений в $\mathbb{F}_q^n$. Пусть многочлен $g \in \mathbb{F}_q[x_1, \ldots, x_d]$ определен так же, как многочлен f из примера 6.7, но число n заменено на d. Тогда положим $f_1(x_1, \ldots, x_n) = g(x_1, \ldots, x_d)$, так что переменные $x_{d+1}, \ldots, x_n$ не входят явно в f_1. Теперь тем же способом, что и в примере 6.7, можно показать, что $f_1(c_1, \ldots, c_n) = 0$ в том и только том случае, если $c_1 = \ldots = c_d = 0$. Поскольку при этом $c_{d+1}, \ldots, c_n$ могут быть любыми элементами поля $\mathbb{F}_q$, то уравнение $f_1(x_1, \ldots, x_n) = 0$ имеет ровно q^{n-d} решений в $\mathbb{F}_q^n$. □

Нетрудно также найти некоторые элементарные *верхние границы* для числа решений уравнения $f(x_1, \ldots, x_n) = 0$. Следующий результат можно рассматривать как обобщение известной теоремы о том, что многочлен от одной переменной степени $d \geqslant 0$ имеет не более d корней (ср. с теоремой 1.66).

6.13. Теорема. *Пусть $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — многочлен степени $d \geqslant 0$. Тогда уравнение $f(x_1, \ldots, x_n) = 0$ имеет не более dq^{n-1} решений в $\mathbb{F}_q^n$.*

Доказательство. Если $d = 0$, то многочлен f является ненулевой константой, и результат тривиален. Если $d = 1$, то уравнение

$$f(x_1, \ldots, x_n) = a_1x_1 + \cdots + a_nx_n + b = 0$$

имеет q^{n-1} решений в $\mathbb{F}_q^n$, так как по крайней мере один из коэффициентов a_i отличен от 0, так что соответствующая переменная x_i однозначно определяется значениями остальных переменных (которые можно задавать произвольно). Результат, очевидно, верен и для $n = 1$.

Таким образом, теорема верна в случае, когда $d \leqslant 1$ или $n = 1$. Далее будем продолжать двойной индукцией. Пусть $n > 1$, $d > 1$ и результат справедлив для ненулевых многочленов не более чем от n переменных степени, меньшей чем d, а также для ненулевых многочленов менее чем от n переменных степени, ие

превосходящей d. Докажем, что результат справедлив для произвольного многочлена $f(x_1, \ldots, x_n)$ от n переменных степени d. Рассмотрим два случая.

Случай 1. Многочлен $f(x_1, \ldots, x_n)$ делится на $x_1 - c$ при некотором $c \in \mathbb{F}_q$. Тогда

$$f(x_1, \ldots, x_n) = (x_1 - c)\, g(x_1, \ldots, x_n),$$

где g — ненулевой многочлен степени, равной $d - 1$. Используя предположение индукции и элементарный подсчет, легко показать, что число N решенй уравнения $f(x_1, \ldots, x_n) = 0$, лежащих в $\mathbb{F}_q^n$, не превосходит числа $q^{n-1} + (d-1)\, q^{n-1} = dq^{n-1}$.

Случай 2. Пусть многочлен $f_1(x_1, \ldots, x_n)$ не делится на $x_1 - c$ ни при каком $c \in \mathbb{F}_q$. Тогда $f(c, x_2, \ldots, x_n)$ — ненулевой многочлен от $n-1$ переменных степени, не превосходящей d, для любого $c \in \mathbb{F}_q$. По предположению индукции уравнение $f(c, x_2, \ldots, x_n) = 0$ имеет не более dq^{n-2} решений в $\mathbb{F}_q^{n-1}$. Но поскольку существует q различных выборов элемента $c \in \mathbb{F}_q$, то число N решений уравнения $f(x_1, \ldots, x_n) = 0$ из $\mathbb{F}_q^n$ не превышает $q \cdot dq^{n-2} = dq^{n-1}$. □

6.14. Пример. Верхняя граница dq^{n-1}, полученная в теореме 6.13, может представлять интерес лишь в случае, когда $d \leqslant q$. В этом случае граница может действительно достигаться. Рассмотрим, например, многочлен

$$f(x_1, \ldots, x_n) = (x_1 - c_1)(x_1 - c_2) \ldots (x_1 - c_d),$$

где $c_1, c_2, \ldots, c_d$ — различные элементы поля $\mathbb{F}_q$. Степень многочлена f равна d, и легко видеть, что уравнение $f(x_1, \ldots, x_n) = 0$ имеет ровно dq^{n-1} решений в $\mathbb{F}_q^n$. □

В соответствии с определением 1.72 многочлен f называется *однородным многочленом* (или *формой*), если все его члены имеют одну и ту же степень. Для такого многочлена положительной степени уравнение $f(x_1, \ldots, x_n) = 0$ всегда имеет тривиальное решение $(0, \ldots, 0)$. Рассматривая нетривиальные решения (если они имеются), можно для однородных многочленов получить небольшое снижение верхней границы, найденной в теореме 6.13.

6.15. Теорема. *Пусть* $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — *однородный многочлен степени* $d \geqslant 1$. *Тогда уравнение* $f(x_1, \ldots, x_n) = 0$ *имеет не более* $d(q^{n-1} - 1)$ *нетривиальных решений в* $\mathbb{F}_q^n$.

Доказательство. Если либо $d = 1$, либо $n = 1$, то результат очевиден. Продолжим доказательство двойной индукцией, как и при доказательстве теоремы 6.13. Допустим, что $n > 1$, $d > 1$ и что результат верен как для непостоянных однородных многочленов не более чем от n переменных степени, меньшей чем d,

так и для непостоянных однородных многочленов менее чем от n переменных степени, не превышающей d. Возьмем однородный многочлен $f(x_1, \ldots, x_n)$ степени d от n переменных и рассмотрим два случая.

Случай 1. Пусть многочлен $f(x_1, \ldots, x_n)$ делится на x_1. Тогда

$$f(x_1, \ldots, x_n) = x_1 \cdot g(x_1, \ldots, x_n),$$

где g — непостоянный однородный многочлен степени, равной $d-1$. Используя предположение индукции и элементарный подсчет, легко обнаружить, что число нетривиальных решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ не превосходит числа

$$(q^{n-1}-1) + (d-1)(q^{n-1}-1) = d(q^{n-1}-1).$$

Случай 2. Многочлен $f(x_1, \ldots, x_n)$ не делится на x_1. Тогда $f(c, x_2, \ldots, x_n)$ является многочленом от $n-1$ переменных степени d для любого $c \in \mathbb{F}_q^*$, так что по теореме 6.13 уравнение $f(x_1, \ldots, x_n) = 0$ имеет не более $(q-1)dq^{n-2}$ решений $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, для которых $c_1 \neq 0$. Кроме того, $f(0, x_2, \ldots, x_n)$ является однородным многочленом степени d от $n-1$ переменных, так что из предположения индукции вытекает, что уравнение $f(x_1, \ldots, x_n) = 0$ имеет не более $d(q^{n-2}-1)$ нетривиальных решений вида $(0, c_2, \ldots, c_n) \in \mathbb{F}_q^n$. В итоге число нетривиальных решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ не превышает числа

$$(q-1)dq^{n-2} + d(q^{n-2}-1) = d(q^{n-1}-1). \qquad \square$$

Исследуем теперь вопрос о *среднем числе решений* полиномиального уравнения. Для натурального числа d пусть Ω_d — множество всех многочленов $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, степень которых не превосходит d. Пусть $\omega(d)$ — число n-наборов $(i_1, \ldots, i_n)$ неотрицательных целых чисел, для которых $i_1 + \ldots + i_n \leqslant d$. Тогда мощность $|\Omega_d|$ множества Ω_d равна $q^{\omega(d)}$. Для $f \in \Omega_d$ обозначим через $N(f)$ число решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$.

6.16. Теорема. *В обозначениях, введенных выше, имеет место равенство*

$$\frac{1}{|\Omega_d|} \sum_{f \in \Omega_d} N(f) = q^{n-1}.$$

Другими словами, среднее число решений в $\mathbb{F}_q^n$ уравнения $f(x_1, \ldots, x_n) = 0$ (где f — многочлен положительной степени $\leqslant d$ от n переменных над полем $\mathbb{F}_q$) равно q^{n-1}.

Доказательство. Можно написать

$$\sum_{f\in\Omega_d} N(f) = \sum_{f\in\Omega_d} \sum_{\substack{(c_1,\ \ldots,\ c_n)\in\mathbb{F}_q^n \\ f(c_1,\ \ldots,\ c_n)=0}} 1 = \sum_{(c_1,\ \ldots,\ c_n)\in\mathbb{F}_q^n} \sum_{\substack{f\in\Omega_d \\ f(c_1,\ \ldots,\ c_n)=0}} 1.$$

Для n-набора $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ все многочлены степени $\leqslant d$

$$f(x_1, \ldots, x_n) = \sum a_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n} \in \Omega_d,$$

обладающие свойством $f(c_1, \ldots, c_n) = 0$, можно получить, выбирая произвольно коэффициенты $a_{i_1, \ldots, i_n}$, $0 < i_1 + \ldots + i_n \leqslant d$, а затем определяя свободный член $a_{0, \ldots, 0}$ так, чтобы $f(c_1, \ldots, c_n) = 0$. Таким образом, число многочленов $f \in \Omega_d$, удовлетворяющих условию $f(c_1, \ldots, c_n) = 0$, равно $q^{\omega(d)-1}$. Поэтому

$$\sum_{f\in\Omega_d} N(f) = q^n q^{\omega(d)-1} = |\Omega_d| q^{n-1},$$

и искомый результат установлен. □

Полиномиальное уравнение от n переменных имеет, таким образом, в среднем q^{n-1} решений в $\mathbb{F}_q^n$. Найдем теперь среднее квадратичное отклонение от найденного среднего значения.

6.17. Теорема. *В обозначениях, введенных выше, имеет место равенство*

$$\frac{1}{|\Omega_d|} \sum_{f\in\Omega_d} (N(f) - q^{n-1})^2 = q^{n-1} - q^{n-2}.$$

Другими словами, среднее квадратичное отклонение от среднего значения q^{n-1} числа решений в $\mathbb{F}_q^n$ уравнения $f(x_1, \ldots, x_n) = 0$ (где f — многочлен положительной степени $\leqslant d$ от n переменных над полем $\mathbb{F}_q$) равно $q^{n-1} - q^{n-2}$.

Доказательство. Вводя обозначения $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ и $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, можно написать

$$\sum_{f\in\Omega_d} N(f)^2 = \sum_{f\in\Omega_d} \left(\sum_{\substack{\mathbf{c}\in\mathbb{F}_q^n \\ f(\mathbf{c})=0}} 1 \right)^2 = \sum_{f\in\Omega_d} \sum_{\substack{\mathbf{b}\in\mathbb{F}_q^n \\ f(\mathbf{b})=0}} \sum_{\substack{\mathbf{c}\in\mathbb{F}_q^n \\ f(\mathbf{c})=0}} 1 =$$

$$= \sum_{\mathbf{b},\ \mathbf{c}\in\mathbb{F}_q^n} \sum_{\substack{f\in\Omega_d \\ f(\mathbf{b})=f(\mathbf{c})=0}} 1.$$

Если $\mathbf{b} = \mathbf{c}$, то из доказательства теоремы 6.16 мы видели, что внутренняя сумма принимает значение $q^{\omega(d)-1}$; если же $\mathbf{b} \neq \mathbf{c}$, то равенства $f(\mathbf{b}) = f(\mathbf{c}) = 0$ приводят к системе из двух линейных уравнений ранга 2 относительно коэффициентов много-

члена f. Указанная система имеет $q^{\omega(d)-2}$ решений. Отсюда следует, что

$$\sum_{f\in\Omega_d} N(f)^2 = \sum_{c\in\mathbb{F}_q^n} |\Omega_d| q^{-1} + \sum_{\substack{b,\ c\in\mathbb{F}_q^n \\ b\neq c}} |\Omega_d| q^{-2} =$$

$$= q^n |\Omega_d| q^{-1} + q^n(q^n-1)\,|\Omega_d| q^{-2} =$$

$$= |\Omega_d|\,(q^{2n-2} + q^{n-1} - q^{n-2}).$$

Применяя полученное равенство и теорему 6.16, получаем

$$\sum_{f\in\Omega_d} (N(f) - q^{n-1})^2 = \sum_{f\in\Omega_d} N(f)^2 - 2q^{n-1}\sum_{f\in\Omega_d} N(f) + q^{2n-2}\sum_{f\in\Omega_d} 1 =$$

$$= |\Omega_d|\,(q^{2n-2} + q^{n-1} - q^{n-2}) -$$

$$- 2q^{n-1}|\Omega_d| q^{n-1} + q^{2n-2}|\Omega_d| =$$

$$= |\Omega_d|\,(q^{n-1} - q^{n-2}),$$

и тем самым результат установлен. □

Таким образом, среднее значение квадратичного отклонения $(N(f) - q^{n-1})^2$ равно $q^{n-1} - q^{n-2}$. Можно поэтому ожидать, что в большинстве случаев величина $|N(f) - q^{n-1}|$ имеет порядок $q^{(n-1)/2}$. В последующих параграфах мы встретимся с примерами, подтверждающими такое предположение.

§ 2. Квадратичные формы

Квадратичной формой (от n переменных) над полем $\mathbb{F}_q$ называется однородный многочлен f степени 2 из кольца $\mathbb{F}_q[x_1, \ldots, x_n]$ или нулевой многочлен. Если число q нечетно (а этот случай представляет особый интерес), то смешанные члены $b_{ij}x_ix_j$ $(1 \leqslant i < j \leqslant n)$ можно представить в виде $\frac{1}{2} b_{ij}x_ix_j + \frac{1}{2} b_{ij}x_jx_i$, что приводит к представлению

$$f(x_1, \ldots, x_n) = \sum_{i,\,j=1}^{n} a_{ij}x_ix_j, \quad \text{где} \quad a_{ij} = a_{ji},$$

для любой квадратичной формы f над $\mathbb{F}_q$. Тогда мы сопоставляем с f квадратную матрицу порядка n

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}.$$

Матрица A называется *матрицей коэффициентов* квадратичной формы f (или просто *матрицей квадратичной формы* f). Если транспонированную к матрице M матрицу обозначить символом M^{T}, то в данном случае окажется, что $A^{\mathrm{T}} = A$, т. е. матрица A симметрическая. Если через $\mathbf{x}$ обозначить вектор-столбец из переменных $x_1, \ldots, x_n$, то легко видеть, что квадратичная форма f представляется в виде матрицы $\mathbf{x}^{\mathrm{T}}A\mathbf{x}$ (т. е. $f(\mathbf{x}^{\mathrm{T}}) = \mathbf{x}^{\mathrm{T}}A\mathbf{x}$).

6.18. Пример. Рассмотрим квадратичную форму $f(x_1, x_2) = 2x_1^2 + x_1x_2 + x_2^2$ от двух переменных (так называемую *бинарную квадратичную форму*) над полем $\mathbb{F}_5$. Матрица коэффициентов квадратичной формы f равна

$$A = \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}$$

и

$$\mathbf{x}^{\mathrm{T}}A\mathbf{x} = (x_1,\ x_2)\begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 2x_1^2 + x_1x_2 + x_2^2 = f(x_1,\ x_2). \quad \square$$

Если f — квадратичная форма над полем $\mathbb{F}_q$ и $b \in \mathbb{F}_q$, то для числа решений уравнения $f(x_1, \ldots, x_n) = b$ в $\mathbb{F}_q^n$ удается установить явную формулу. Для получения этой формулы мы сначала с помощью линейного преобразования переменных приведем квадратичную форму f к простейшему виду. Линейное преобразование переменных зададим матричным равенством $\mathbf{x} = C\mathbf{y}$, где C — квадратная матрица порядка n над $\mathbb{F}_q$, и $\mathbf{y}$ — вектор-столбец из новых переменных $y_1, \ldots, y_n$. Если матрица C невырожденна, то соответствующее линейное преобразование тоже называется *невырожденным*.

6.19. Определение. Две квадратичные формы f и g над произвольным фиксированным конечным полем $\mathbb{F}_q$ называются *эквивалентными*, если f может быть переведена в g с помощью невырожденного линейного преобразования переменных.

Нетрудно убедиться в том, что эквивалентность квадратичных форм действительно задает отношение эквивалентности (т. е. обладает свойствами рефлексивности, симметричности и транзитивности). Кроме того, если квадратичные формы f и g эквивалентны, то для любого элемента $b \in \mathbb{F}_q$ уравнения $f(x_1, \ldots, x_n) = b$ и $g(x_1, \ldots, x_n) = b$ имеют одно и то же число решений в $\mathbb{F}_q^n$ (ввиду того, что матрицу C можно использовать для задания взаимно однозначного соответствия между векторами-решениями этих двух уравнений). При нечетном числе q матрицы коэффициентов A и B двух эквивалентных квадратичных форм f и g над $\mathbb{F}_q$ связаны соотношением $B = C^{\mathrm{T}}AC$, где невырожденная

матрица C задает соответствующее линейное преобразование переменных (так как $f(\mathbf{x}^\tau) = \mathbf{x}^\tau A\mathbf{x} = (C\mathbf{y})^\tau A\,(C\mathbf{y}) = \mathbf{y}^\tau (C^\tau AC)\,\mathbf{y} = \mathbf{y}^\tau B\mathbf{y} = g(\mathbf{y}^\tau)$).

Сначала мы изучим подробнее случай, когда число q нечетно (т. е. поле $\mathbb{F}_q$ имеет характеристику $p > 2$). Покажем, что каждая квадратичная форма над $\mathbb{F}_q$ эквивалентна некоторой *диагональной квадратичной форме* $a_1x_1^2 + \ldots + a_nx_n^2$ над $\mathbb{F}_q$. Будем пользоваться следующей терминологией: квадратичная форма f над полем $\mathbb{F}_q$ *представляет* элемент $a \in \mathbb{F}_q$, если уравнение $f(x_1, \ldots, x_n) = a$ имеет хотя бы одно решение в $\mathbb{F}_q^n$.

6.20. Лемма. *Если q нечетно и квадратичная форма от n переменных $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ при $n \geqslant 2$ представляет элемент $a \in \mathbb{F}_q^*$, то f эквивалентна квадратичной форме $ax_1^2 + g(x_2, \ldots, x_n)$, где g — некоторая квадратичная форма над $\mathbb{F}_q$ от $n - 1$ переменных.*

Доказательство. По предположению существует n-набор $\mathbf{c}^\tau = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, для которого $f(c_1, \ldots, c_n) = a$. Поскольку $a \neq 0$, то не все c_i равны 0, поэтому можно найти невырожденную $n \times n$-матрицу C над $\mathbb{F}_q$, первый столбец которой состоит из элементов $c_1, \ldots, c_n$ (т. е. равен $\mathbf{c}$). Если применить к квадратичной форме f линейное преобразование переменных, задаваемое матрицей C, то получим квадратичную форму от новых переменных $y_1, \ldots, y_n$, у которой коэффициент при y_1^2 равен $f(c_1, \ldots, c_n) = a$ (так как в матрице $B = C^\tau AC = (b_{ij})$ элемент b_{11} равен $\mathbf{c}^\tau A\mathbf{c} = f(\mathbf{c}^\tau) = a$). Это значит, что f эквивалентна квадратичной форме вида

$$ay_1^2 + 2b_2y_1y_2 + \cdots + 2b_ny_1y_n + h(y_2, \ldots, y_n) = \\ = a(y_1 + b_2a^{-1}y_2 + \cdots + b_na^{-1}y_n)^2 + g(y_2, \ldots, y_n)$$

для подходящим образом подобранных элементов $b_2, \ldots, b_n \in \mathbb{F}_q$ и квадратичных форм h и g над $\mathbb{F}_q$. Невырожденное линейное преобразование

$$x_1 = y_1 + b_2a^{-1}y_2 + \cdots + b_na^{-1}y_n, \quad x_2 = y_2, \ \ldots, \ x_n = y_n$$

приводит тогда к квадратичной форме требуемого вида. □

6.21. Теорема. *Каждая квадратичная форма над полем $\mathbb{F}_q$, где q нечетно, эквивалентна некоторой диагональной квадратичной форме.*

Доказательство. Применим индукцию по числу n переменных. Если $n = 1$, то квадратичная форма $f(x_1) = a_{11}x_1^2$ уже диагональна. Пусть теперь $n \geqslant 2$, и предположим, что утверждение теоремы справедливо для квадратичной формы от $n - 1$ переменных. Пусть $f(x_1, \ldots, x_n)$ — квадратичная форма от n переменных.

Теорема верна, если f — нулевой многочлен. Если же $f \neq 0$, то либо f имеет некоторый коэффициент $a_{ii} \neq 0$ и тогда она представляет элемент a_{ii}, либо все a_{ii} равны 0, $i = 1, \ldots, n$, но найдется такая пара (i, j), $1 \leqslant i < j \leqslant n$, что $a_{ij} = a_{ji} \neq 0$, и тогда f представляет элемент $2a_{ij} \neq 0$, так как при $c_i = c_j = 1$, $c_k = 0$ для всех $k \neq i, j$ получаем $f(c_1, \ldots, c_n) = 2a_{ij}$. В любом случае f представляет некоторый элемент $a_1 \in \mathbb{F}_q^*$, так что f эквивалентна квадратичной форме $a_1x_1^2 + g(x_2, \ldots, x_n)$ согласно лемме 6.20. По предположению индукции g эквивалентна некоторой диагональной квадратичной форме $a_2x_2^2 + \ldots + a_nx_n^2$, так что f эквивалентна диагональной квадратичной форме $a_1x_1^2 + \ldots + a_nx_n^2$. □

Если квадратичная форма $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ эквивалентна диагональной квадратичной форме $a_1x_1^2 + \ldots + a_nx_n^2$, то может оказаться, что некоторые из коэффициентов a_i равны нулю. Поскольку умножение какой-либо матрицы на невырожденную матрицу не изменяет ранга исходной матрицы, то матрицы коэффициентов эквивалентных матриц имеют один и тот же ранг. В частности, число ненулевых коэффициентов a_i в полученной выше диагональной квадратичной форме совпадает с рангом матрицы A коэффициентов исходной квадратичной формы f. Если матрица A имеет ранг, равный ее порядку n, то квадратичная форма f называется *невырожденной*. Назовем *определителем* (*детерминантом*) $\det(f)$ *квадратичной формы* f определитель матрицы ее коэффициентов. Тогда для невырожденности квадратичной формы f необходимо и достаточно, чтобы $\det(f) \neq 0$.

Отметим одно полезное соотношение. Если квадратичные формы f и g эквивалентны, причем f переводится в g с помощью невырожденного линейного преобразования переменных с матрицей C, то из равенства $B = C^TAC$, связывающего матрицы коэффициентов A и B квадратичных форм f и g соответственно, сразу вытекает равенство

$$\det(g) = \det(f) \det(C)^2. \tag{6.3}$$

Для ненулевой квадратичной формы $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ эквивалентная ей диагональная квадратичная форма может быть записана без ограничения общности в следующем виде: $a_1x_1^2 + \ldots + a_kx_k^2$, где $1 \leqslant k \leqslant n$ и все a_i, $i = 1, \ldots, k$, отличны от нуля. Поскольку для любого $b \in \mathbb{F}_q$ число решений уравнения $a_1x_1^2 + \ldots + a_kx_k^2 = b$, лежащих в $\mathbb{F}_q^n$, является увеличенным в q^{n-k} раз числом решений того же уравнения в $\mathbb{F}_q^k$, то в дальнейшем достаточно изучить лишь случай $k = n$, т. е. случай невырожденной квадратичной формы.

В дальнейшем исследовании весьма полезными окажутся вводимая ниже функция и некоторые ее простейшие свойства.

6.22. Определение. Пусть $\mathbb{F}_q$ — произвольное конечное поле. Определим целочисленную функцию $v(x)$ на $\mathbb{F}_q$ условием

$$v(b) = \begin{cases} -1, & \text{если } b \in \mathbb{F}_q^*, \\ q-1, & \text{если } b = 0. \end{cases}$$

6.23. Лемма. *Для любого конечного поля $\mathbb{F}_q$ справедливо равенство*

$$\sum_{c \in \mathbb{F}_q} v(c) = 0, \tag{6.4}$$

и для любого $b \in \mathbb{F}_q$ имеет место соотношение

$$\sum_{c_1+\cdots+c_m=b} v(c_1) \ldots v(c_k) = \begin{cases} 0, & \text{если } 1 \leqslant k < m, \\ v(b)\, q^{m-1}, & \text{если } k = m, \end{cases} \tag{6.5}$$

где сумма распространяется на все $c_1, \ldots, c_m \in \mathbb{F}_q$, такие, что $c_1 + \ldots + c_m = b$.

Доказательство. Равенство (6.4) тривиально. Далее, для любого k, $1 \leqslant k < m$,

$$\sum_{c_1+\cdots+c_m=b} v(c_1) \ldots v(c_k) =$$

$$= \sum_{c_1, \ldots, c_k \in \mathbb{F}} v(c_1) \ldots v(c_k) \sum_{c_{k+1}+\ldots+c_m=b-c_1-\ldots-c_k} 1 =$$

$$= q^{m-k-1} \sum_{c_1, \ldots, c_k \in \mathbb{F}_q} v(c_1) \ldots v(c_k) =$$

$$= q^{m-k-1} \left(\sum_{c_1 \in \mathbb{F}_q} v(c_1) \right) \ldots \left(\sum_{c_k \in \mathbb{F}_q} v(c_k) \right) = 0$$

согласно (6.4). Если же $k = m$ в (6.5), то применим индукцию по m. Случай $m = 1$ тривиален; допустим, что формула верна для некоторого $m \geqslant 1$. Тогда в силу первой (доказанной) частн (6.5)

$$\sum_{c_1+\ldots+c_m+c_{m+1}=b} v(c_1) \ldots v(c_m) v(c_{m+1}) =$$

$$= \sum_{c_1+\ldots+c_m+c_{m+1}=b} v(c_1) \ldots v(c_m) [v(c_{m+1}) + 1] =$$

$$= \sum_{c_1, \ldots, c_m \in \mathbb{F}_q} v(c_1) \ldots v(c_m) [v(b - c_1 - \cdots - c_m) + 1] =$$

$$= q \sum_{c_1+\ldots+c_m=b} v(c_1) \ldots v(c_m).$$

Справедливость последнего шага вытекает из того, что выражение в квадратных скобках равно нулю, если $c_1 + \ldots + c_m \neq b$, и равно q, если $c_1 + \ldots + c_m = b$. Остальное вытекает из предположения индукции. □

В дальнейшем мы часто будем использовать обозначение $N(\ldots)$ для числа решений уравнения, указанного в скобках, лежащих в декартовой степени основного конечного поля, учитывая лишь те переменные, которые на самом деле входят в уравнение. Так, $N\left(a_1x_1^2 + a_2x_2^2 = b\right)$ обозначает число решений указанного уравнения в $\mathbb{F}_q^2$.

Теперь продолжим изучение квадратичной формы f над полем $\mathbb{F}_q$ при нечетном q. Как мы видели, достаточно найти число решений $N(f(x_1, \ldots, x_n) = b)$ уравнения, указанного в скобках, для невырожденной квадратичной формы f. При этом будем различать случаи четного и нечетного n. Рассмотрим сначала одно уравнение специального вида.

6.24. Лемма. *Пусть η — квадратичный характер поля $\mathbb{F}_q$ нечетной характеристики, $b \in \mathbb{F}_q$ и $a_1, a_2 \in \mathbb{F}_q^*$. Тогда*

$$N\left(a_1x_1^2 + a_2x_2^2 = b\right) = q + v(b)\,\eta(-a_1a_2).$$

Доказательство. Считая c_1 и c_2 элементами поля $\mathbb{F}_q$, получим, используя (5.37), соотношение

$$\begin{aligned} N\left(a_1x_1^2 + a_2x_2^2 = b\right) &= \sum_{c_1+c_2=b} N\left(a_1x_1^2 = c_1\right) N\left(a_2x_2^2 = c_2\right) = \\ &= \sum_{c_1+c_2=b} \left[1 + \eta\left(c_1a_1^{-1}\right)\right]\left[1 + \eta\left(c_2a_2^{-1}\right)\right] = \\ &= q + \eta(a_1) \sum_{c_1 \in \mathbb{F}_q} \eta(c_1) + \eta(a_2) \sum_{c_2 \in \mathbb{F}_q} \eta(c_2) + \\ &\quad + \eta(a_1a_2) \sum_{c_1+c_2=b} \eta(c_1c_2) = \\ &= q + \eta(a_1a_2) \sum_{c \in \mathbb{F}_q} \eta(bc - c^2). \end{aligned}$$

Теперь на основании теоремы 5.48 последняя сумма равна $v(b) \cdot \eta(-1)$, и, таким образом, результат доказан. □

6.25. Замечание. Полученный выше результат показывает, в частности, что уравнение $a_1x_1^2 + a_2x_2^2 = b$ всегда имеет хотя бы одно решение в $\mathbb{F}_q^2$. Но это можно было бы установить и следующим несложным рассуждением. Рассмотрим множества $S = \{a_1c_1^2 \mid c_1 \in \mathbb{F}_q\}$ и $T = \{b - a_2c_2^2 \mid c_2 \in \mathbb{F}_q\}$ при нечетном q;

их мощности $|S|$ и $|T|$ равны $(q+1)/2$. Поскольку $|S|+|T|>q$, то S и T должны иметь хотя бы один общий элемент, например c. Тогда $c=a_1c_1^2=b-a_2c_2^2$ для некоторых $c_1,\ c_2\in\mathbb{F}_q$. Это значит, что $a_1c_1^2+a_2c_2^2=b$. Ввиду того что при четном q каждый элемент поля $\mathbb{F}_q$ является квадратом некоторого элемента этого поля, замечание тривиально выполняется и для случая четного q. □

6.26. Теорема. *Пусть f — невырожденная квадратичная форма от четного числа n переменных над полем $\mathbb{F}_q$, где q нечетно. Тогда для любого $b\in\mathbb{F}_q$ число решений уравнения $f(x_1,\ldots,x_n)=b$ в $\mathbb{F}_q^n$ равно*

$$q^{n-1}+v(b)\,q^{(n-2)/2}\eta\left((-1)^{n/2}\Delta\right),$$

где η — квадратичный характер поля $\mathbb{F}_q$ и $\Delta=\det(f)$.

Доказательство. Пусть $a_1x_1^2+\ldots+a_nx_n^2$ — диагональная квадратичная форма, эквивалентная f. Поскольку эквивалентным квадратичным формам f и g соответствует одно и то же значение $\eta(\Delta)$ в силу (6.3), а также одно и то же число решений уравнений $f(x_1,\ldots,x_n)=a$ и $g(x_1,\ldots,x_n)=a$ в $\mathbb{F}_q^n$ для любого $a\in\mathbb{F}_q$, то утверждение достаточно доказать для уравнения $a_1x_1^2+\ldots+a_nx_n^2=b$, где все a_i отличны от 0. Для $m=n/2$ и $c_1,\ldots,c_m\in\mathbb{F}_q$ из леммы 6.24 и соотношения (6.5) получаем

$$\begin{aligned}
&N\left(a_1x_1^2+\cdots+a_nx_n^2=b\right)=\\
&=\sum_{c_1+\ldots+c_m=b}N\left(a_1x_1^2+a_2x_2^2=c_1\right)\ \ldots\ N\left(a_{n-1}x_{n-1}^2+a_nx_n^2=c_m\right)=\\
&=\sum_{c_1+\ldots+c_m=b}\left[q+v(c_1)\,\eta(-a_1a_2)\right]\ \ldots\ \left[q+v(c_m)\,\eta(-a_{n-1}a_n)\right]=\\
&=q^{m-1}q^m+\eta\left((-1)^m a_1\ \ldots\ a_n\right)\sum_{c_1+\ldots+c_m=b}v(c_1)\ \ldots\ v(c_m)=\\
&=q^{n-1}+v(b)\,q^{(n-2)/2}\eta\left((-1)^{n/2}a_1\ \ldots\ a_n\right).
\end{aligned}$$

□

6.27. Теорема. *Пусть f — невырожденная квадратичная форма от нечетного числа n переменных над полем $\mathbb{F}_q$, где q нечетно. Тогда для $b\in\mathbb{F}_q$ число решений уравнения $f(x_1,\ldots,x_n)=b$ в $\mathbb{F}_q^n$ равно*

$$q^{n-1}+q^{(n-1)/2}\eta\left((-1)^{(n-1)/2}\,b\Delta\right),$$

где η — квадратичный характер поля $\mathbb{F}_q$ и $\Delta=\det(f)$.

Доказательство. Как и в теореме 6.26, указанную формулу достаточно установить для уравнения $a_1x_1^2+\ldots+a_nx_n^2=b$, где

все a_i отличны от 0. Формула справедлива для $n = 1$. Для $n \geqslant 3$ применим теорему 6.26 и получим при $c_1, c_2 \in \mathbb{F}_q$

$$N\left(a_1x_1^2 + \dots + a_nx_n^2 = b\right) =$$

$$= \sum_{c_1+c_2=b} N\left(a_1x_1^2 = c_1\right) N\left(a_2x_2^2 + \dots + a_nx_n^2 = c_2\right) =$$

$$= \sum_{c_1+c_2=b} [1 + \eta(c_1a_1)] \cdot$$

$$\cdot [q^{n-2} + v(c_2)\, q^{(n-3)/2} \eta\left((-1)^{(n-1)/2}\, a_2 \dots a_n\right)] =$$

$$= q^{n-1} + q^{n-2}\eta(a_1) \sum_{c_1 \in \mathbb{F}_q} \eta(c_1) +$$

$$+ q^{(n-3)/2}\eta\left((-1)^{(n-1)/2} a_2 \dots a_n\right) \sum_{c_2 \in \mathbb{F}_q} v(c_2) +$$

$$+ q^{(n-3)/2}\eta\left((-1)^{(n-1)/2} a_1 \dots a_n\right) \sum_{c_1+c_2=b} \eta(c_1)\, v(c_2) =$$

$$= q^{n-1} + q^{(n-3)/2}\eta\left((-1)^{(n-1)/2} a_1 \dots a_n\right) \sum_{c \in \mathbb{F}_q} \eta(c)\, v(b-c),$$

где на последнем шаге мы воспользовались формулами (5.37) и (6.4). Теперь получаем

$$\sum_{c \in \mathbb{F}_q} \eta(c)\, v(b-c) = \sum_{c \in \mathbb{F}_q} \eta(c)\, [v(b-c) + 1] = q\eta(b),$$

и результат доказан. □

Дадим теперь еще одно доказательство теорем 6.26 и 6.27, использующее метод доказательства леммы 6.24 и свойства сумм Якоби. Как и раньше, достаточно рассмотреть уравнение $a_1x_1^2 + \dots + a_nx_n^2 = b$, где все a_i отличны от 0. Обозначим через ψ_0 тривиальный мультипликативный характер поля $\mathbb{F}_q$, и пусть $\psi_1 = \eta$ и $N = N\left(a_1x_1^2 + \dots + a_nx_n^2 = b\right)$. Тогда для $c_1, \dots, c_n \in \mathbb{F}_q$

$$N = \sum_{c_1+\dots+c_n=b} N\left(a_1x_1^2 = c_1\right) \dots N\left(a_nx_n^2 = c_n\right) =$$

$$= \sum_{c_1+\dots+c_n=b} \left[1 + \psi_1\left(c_1a_1^{-1}\right)\right] \dots \left[1 + \psi_1\left(c_na_n^{-1}\right)\right] = \cdot$$

$$= \sum_{c_1+\dots+c_n=b} [\psi_0(c_1a_1) + \psi_1(c_1a_1)] \dots [\psi_0(c_na_n) + \psi_1(c_na_n)] =$$

$$= \sum_{c_1+\ldots+c_n=b} \sum_{i_1, \ldots, i_n=0}^{1} \psi_{i_1}(c_1 a_1) \ldots \psi_{i_n}(c_n a_n) =$$

$$= \sum_{i_1, \ldots, i_n=0}^{1} \psi_{i_1}(a_1) \ldots \psi_{i_n}(a_n) \sum_{c_1+\ldots+c_n=0} \psi_{i_1}(c_1) \ldots \psi_{i_n}(c_n) =$$

$$= \sum_{i_1, \ldots, i_n=0}^{1} \psi_{i_1}(a_1) \ldots \psi_{i_n}(a_n) J_b(\psi_{i_1}, \ldots, \psi_{i_n}).$$

В силу (5.38), (5.39) и (5.40) в этой сумме остаются лишь два члена, а именно те, которые соответствуют n-наборам $(i_1, \ldots, i_n)$, равным $(0, \ldots, 0)$ и $(1, \ldots, 1)$, так что

$$N = q^{n-1} + \eta(a_1 \ldots a_n) J_b(\eta, \ldots, \eta), \tag{6.6}$$

где в сумму Якоби входит n экземпляров η.

Для $b \neq 0$, применяя (5.38), получим

$$N = q^{n-1} + \eta(a_1 \ldots a_n) \eta^n(b) J(\eta, \ldots, \eta). \tag{6.7}$$

Если n четно, то можно применить (5.44) и теорему 5.12 (iv), и тогда для произвольного нетривиального аддитивного характера χ поля $\mathbb{F}_q$ получаем

$$J(\eta, \ldots, \eta) = -\frac{1}{q} G(\eta, \chi)^n = -\frac{1}{q} [G(\eta, \chi)^2]^{n/2} =$$

$$= -\frac{1}{q} [\eta(-1) q]^{n/2} = -q^{(n-2)/2} \eta((-1)^{n/2}).$$

Теперь из (6.7) следует равенство

$$N = q^{n-1} - q^{(n-2)/2} \eta((-1)^{n/2} a_1 \ldots a_n),$$

что согласуется с теоремой 6.26 при $b \neq 0$. Если же n нечетно, то из (5.43) и теоремы 5.12 (iv) получим

$$J(\eta, \ldots, \eta) = G(\eta, \chi)^{n-1} = [G(\eta, \chi)^2]^{(n-1)/2} = [\eta(-1) q]^{(n-1)/2} =$$

$$= q^{(n-1)/2} \eta((-1)^{(n-1)/2}), \tag{6.8}$$

так что из (6.7) вытекает

$$N = q^{n-1} + q^{(n-1)/2} \eta((-1)^{(n-1)/2} b a_1 \ldots a_n),$$

что согласуется с теоремой 6.27.

Теперь рассмотрим случай $b = 0$. Если n четно, то можно применить (5.42), и тогда получим

$$J_0(\eta, \ldots, \eta) = (q - 1) \eta(-1) J(\eta, \ldots, \eta),$$

где в последнюю сумму Якоби входит $n-1$ экземпляров η. Таким образом, согласно (6.8),

$$J_0(\eta, \ldots, \eta) = (q-1)\,q^{(n-2)/2}\eta\left((-1)^{n/2}\right),$$

и из (6.6) получаем равенство

$$N = q^{n-1} + (q-1)\,q^{(n-2)/2}\eta\left((-1)^{n/2}a_1 \ldots a_n\right),$$

что согласуется с теоремой 6.26. Если же n нечетно, то, согласно (5.41), $J_0(\eta, \ldots, \eta) = 0$; поэтому из (6.6) следует, что $N = q^{n-1}$, и это согласуется с теоремой 6.27. □

6.28. Замечание. При нечетном числе q мы можем также найти число решений в $\mathbb{F}_q^n$ уравнения $h(x_1, \ldots, x_n) = b$, где $b \in \mathbb{F}_q$ и h — многочлен над $\mathbb{F}_q$ степени 2 (но не обязательно квадратичная форма). Можно написать $h = f + g$, где f — квадратичная форма и $\deg(g) \leqslant 1$. Применив невырожденное линейное преобразование, переводящее f в диагональную квадратичную форму, получим уравнение

$$a_1x_1^2 + \cdots + a_kx_k^2 + b_1x_1 + \cdots + b_nx_n = b \quad (1 \leqslant k \leqslant n, \text{ все } a_i \neq 0),$$

которое имеет то же число решений, что и исходное уравнение. Если $k < n$, то без ограничения общности можно предположить, что $b_n \neq 0$. Тогда число решений этого уравнения равно q^{n-1}, так как переменным $x_1, \ldots, x_{n-1}$ можно придать произвольные значения из $\mathbb{F}_q$ и по ним однозначно определить значение x_n. Если же $k = n$, то невырожденное линейное преобразование $x_i = y_i - b_i(2a_i)^{-1}$, $i = 1, \ldots, n$, приводит к уравнению $a_1y_1^2 + \ldots + a_ny_n^2 = c$ для некоторого $c \in \mathbb{F}_q$, не изменяя числа решений. Теперь число решений указывается теоремами 6.26 и 6.27. □

Перейдем теперь к случаю четного q, т. е. к случаю, когда основным является конечное поле $\mathbb{F}_q$ характеристики 2. Рассмотрим тот же вопрос о числе $N(f(x_1, \ldots, x_n) = b)$ решений в $\mathbb{F}_q^n$ уравнения $f(x_1, \ldots, x_n) = b$, где f — квадратичная форма над $\mathbb{F}_q$ от n переменных и $b \in \mathbb{F}_q$. Будем применять ту же стратегию, что и раньше, а именно приведем сначала f к эквивалентной квадратичной форме простейшего вида. Квадратичную форму f от n переменных над полем характеристики 2 назовем *невырожденной*, если f не эквивалентна никакой квадратичной форме от меньшего, чем n, числа переменных (если такое определение применить к случаю нечетного q, то мы придем к тому же понятию невырожденности, что и раньше). Снова достаточно изучить лишь случай невырожденной квадратичной формы.

6.29. Лемма. *Невырожденная квадратичная форма $f(x_1, \ldots, x_n)$ от $n \geqslant 3$ переменных над полем $\mathbb{F}_q$ при четном q эквивалентна $x_1x_2 + g(x_3, \ldots, x_n)$, где g — невырожденная квадратичная форма над $\mathbb{F}_q$ от $n-2$ переменных.*

Доказательство. Покажем сначала, что квадратичная форма f эквивалентна некоторой квадратичной форме, в которой коэффициент при x_1^2 равен 0. Запишем

$$f(x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j. \tag{6.9}$$

Если какой-нибудь коэффициент a_{ii} равен 0, то изменяя нумерацию переменных, полагаем $a_{11} = 0$. Поэтому можно предположить, что все a_{ii} отличны от 0. Если при этом все a_{ij} равны 0 для $i < j$, то

$$f(x_1, \ldots, x_n) = a_{11}x_1^2 + \cdots + a_{nn}x_n^2 = (a_{11}^{q/2}x_1 + \cdots + a_{nn}^{q/2}x_n)^2,$$

но это означает, что f эквивалентна квадратичной форме от одной переменной, что противоречит невырожденности f. Поэтому найдется $a_{ij} \neq 0$, $i < j$, и, изменяя соответствующим образом нумерацию переменных, можно считать, что $a_{23} \neq 0$. Выделяя теперь члены f, содержащие x_2, можно написать

$$f(x_1, \ldots, x_n) = a_{22}x_2^2 + x_2(a_{12}x_1 + a_{23}x_3 + \cdots + a_{2n}x_n) + \\ + g_1(x_1, x_3, \ldots, x_n),$$

и затем, применив невырожденное линейное преобразование переменных

$$x_3 = a_{23}^{-1}(a_{12}y_1 + y_3 + a_{24}y_4 + \cdots + a_{2n}y_n),$$
$$x_i = y_i \quad \text{для} \quad i \neq 3,$$

перейти к эквивалентной квадратичной форме

$$a_{22}y_2^2 + y_2y_3 + g_2(y_1, y_3, \ldots, y_n).$$

Пусть b_{11} обозначает теперь коэффициент при y_1^2 в g_2; тогда, применив невырожденное линейное преобразование переменных

$$y_2 = (a_{22}^{-1}b_{11})^{q/2}z_1 + z_2,$$
$$y_i = z_i \quad \text{для} \quad i \neq 2,$$

получим эквивалентную квадратичную форму, в которой коэффициент при z_1^2 окажется равным 0.

Теперь пусть квадратичная форма f задана равенством (6.9), причем $a_{11} = 0$. Поскольку f невырожденна, все a_{1j} не могут быть равными нулю, так что можно предположить, что $a_{12} \neq 0$. Тогда невырожденное линейное преобразование переменных

$$x_2 = a_{12}^{-1}(y_2 + a_{13}y_3 + \cdots + a_{1n}y_n),$$
$$x_i = y_i \quad \text{для} \quad i \neq 2$$

переводит f в квадратичную форму вида

$$y_1y_2 + \sum_{2 \leqslant i \leqslant j \leqslant n} c_{ij}y_iy_j,$$

которая в свою очередь с помощью невырожденного линейного преобразования переменных

$$y_1 = z_1 + c_{22}z_2 + \ldots + c_{2n}z_n,$$
$$y_i = z_i \quad \text{для} \quad i \neq 1$$

переводится в квадратичную форму $z_1z_2 + g(z_3, \ldots, z_n)$, где g, очевидно, — невырожденная квадратичная форма. □

6.30. Теорема. *Пусть $f(x_1, \ldots, x_n)$ — невырожденная квадратичная форма от n переменных над конечным полем $\mathbb{F}_q$ характеристики 2. Если число n нечетно, то f эквивалентна квадратичной форме*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2.$$

Если же n четно, то f эквивалентна либо квадратичной форме

$$x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n,$$

либо квадратичной форме

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2,$$

где $a \in \mathbb{F}_q$, причем $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$.

Доказательство. Если n нечетно, то, применяя индукцию по n и теорему 6.29, легко показать, что f эквивалентна квадратичной форме вида $x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + ax_n^2$, где $a \in \mathbb{F}_q^*$. Заменяя теперь x_n на $a^{-q/2}x_n$, получаем требуемую квадратичную форму.

Если же n четно, то, применяя индукцию по n и лемму 6.29, можно показать, что f эквивалентна квадратичной форме вида

$$x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + bx_{n-1}^2 + cx_{n-1}x_n + dx_n^2,$$

где $b, c, d \in \mathbb{F}_q$. В силу невырожденности f элемент c должен быть отличен от 0, иначе равенство

$$bx_{n-1}^2 + dx_n^2 = (b^{q/2}x_{n-1} + d^{q/2}x_n)^2$$

позволило бы привести f к эквивалентной квадратичной форме от меньшего, чем n, числа переменных. Если $b = 0$, то квадратичная форма

$$cx_{n-1}x_n + dx_n^2 = (cx_{n-1} + dx_n)\,x_n$$

эквивалентна $x_{n-1}x_n$, и мы приходим к требуемому виду. Если же $b \neq 0$, то, заменяя x_{n-1} на $b^{-q/2}x_{n-1}$ и x_n на $b^{q/2}c^{-1}x_n$, получаем,

что квадратичная форма $bx_{n-1}^2 + cx_{n-1}x_n + dx_n^2$ эквивалентна $x_{n-1}^2 + x_{n-1}x_n + ax_n^2$ для некоторого $a \in \mathbb{F}_q$. Если при этом многочлен $x^2 + x + a$ приводим в кольце $\mathbb{F}_q[x]$, то

$$x^2 + x + a = (x + c_1)(x + c_2)$$

для некоторых $c_1, c_2 \in \mathbb{F}_q$, откуда

$$x_{n-1}^2 + x_{n-1}x_n + ax_n^2 = (x_{n-1} + c_1x_n)(x_{n-1} + c_2x_n),$$

что эквивалентно квадратичной форме $x_{n-1}x_n$. Если же многочлен $x^2 + x + a$ неприводим в $\mathbb{F}_q[x]$, то на основании следствия 3.79 получаем, что $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$, и результат полностью установлен. □

Ввиду инвариантности числа $N(f(x_1, \ldots, x_n) = b)$ относительно перехода к эквивалентной f квадратичной форме можно теперь сосредоточить внимание на квадратичных формах тех специальных типов, которые указаны в теореме 6.30. При этом мы снова воспользуемся функцией $v(x)$, введенной определением 6.22.

6.31. Лемма. *Пусть* $a \in \mathbb{F}_q$, *где* q *четно, причем* $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$, *и* $b \in \mathbb{F}_q$. *Тогда*

$$N(x_1^2 + x_1x_2 + ax_2^2 = b) = q - v(b).$$

Доказательство. Так как в силу следствия 3.79 многочлен $x^2 + x + a$ неприводим в кольце $\mathbb{F}_q[x]$, то

$$x^2 + x + a = (x + \alpha)(x + \alpha^q),$$

где $\alpha \in \mathbb{F}_{q^2}$, $\alpha \notin \mathbb{F}_q$, так что

$$f(x_1, x_2) = x_1^2 + x_1x_2 + ax_2^2 = (x_1 + \alpha x_2)(x_1 + \alpha^q x_2).$$

Поэтому для произвольной упорядоченной пары $(c_1, c_2) \in \mathbb{F}_q^2$ получаем

$$f(c_1, c_2) = (c_1 + \alpha c_2)(c_1 + \alpha^q c_2) = (c_1 + \alpha c_2)(c_1 + \alpha c_2)^q = (c_1 + \alpha c_2)^{q+1}.$$

Ввиду того что $\{1, \alpha\}$ — базис поля $\mathbb{F}_{q^2}$ (как векторного пространства) над полем $\mathbb{F}_q$, то между упорядоченными парами $(c_1, c_2) \in \mathbb{F}_q^2$ и элементами $\gamma = c_1 + \alpha c_2 \in \mathbb{F}_{q^2}$ можно установить взаимно однозначное соответствие. Поэтому число $N(f(x_1, x_2) = b)$ совпадает с числом элементов $\gamma \in \mathbb{F}_{q^2}$, для которых $\gamma^{q+1} = b$. При $b = 0$ получаем

$$N(f(x_1, x_2) = 0) = 1 = q - v(0).$$

Если же $b \neq 0$, то поскольку $\mathbb{F}_{q^2}^*$ — циклическая группа порядка $q^2 - 1$ и $b^{(q^2-1)/(q+1)} = b^{q-1} = 1$, существует $q + 1$ элементов $\gamma \in \mathbb{F}_{q^2}$, таких, что $\gamma^{q+1} = b$. Это означает, что $N(f(x_1, x_2) = b) = q + 1 = q - v(b)$. □

6.32. Теорема. *Пусть* $\mathbb{F}_q$ *— конечное поле характеристики* 2, *и пусть* $b \in \mathbb{F}_q$. *Тогда для нечетного числа* n *число решений уравнения*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2 = b$$

в $\mathbb{F}_q^n$ *равно* q^{n-1}. *Для четного* n *число решений уравнения*

$$x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n = b$$

в $\mathbb{F}_q^n$ *равно* $q^{n-1} + v(b)\, q^{(n-2)/2}$. *Для четного* n *и* $a \in \mathbb{F}_q$, *удовлетворяющего условию* $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$, *число решений уравнения*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = b$$

в $\mathbb{F}_q^n$ *равно* $q^{n-1} - v(b)\, q^{(n-2)/2}$.

Доказательство. Так как уравнение $x^2 = c$ имеет единственное решение (в силу теоремы 2.21) в поле $\mathbb{F}_q$ характеристики 2 для любого $c \in \mathbb{F}_q$, то для нечетного n получаем

$$N\left(x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2 = b\right) = q^{n-1},$$

поскольку для произвольно заданных значений переменных $x_1, \ldots, x_{n-1}$ значение переменной x_n, удовлетворяющее уравнению в скобках, определяется однозначно.

Теперь заметим, что число $N(x_1x_2 = b)$ равно $q - 1$ при $b \neq 0$ и $2q - 1$ при $b = 0$, так что в обоих случаях справедливо равенство $N(x_1x_2 = b) = q + v(b)$. Поэтому для четного n, скажем $n = 2m$, мы получим при $c_1, \ldots, c_m \in \mathbb{F}_q$

$$\begin{aligned} N(x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n = b) &= \\ &= \sum_{c_1+\cdots+c_m=b} N(x_1x_2 = c_1) \ldots N(x_{n-1}x_n = c_m) = \\ &= \sum_{c_1+\cdots+c_m=b} [q + v(c_1)] \ldots [q + v(c_m)] = \\ &= q^{m-1}q^m + \sum_{c_1+\cdots+c_m=b} v(c_1) \ldots v(c_m) = q^{n-1} + v(b)\, q^{(n-2)/2}, \end{aligned}$$

где мы воспользовались формулой (6.5).

Осталось рассмотреть уравнение последнего типа. В этом случае указанная в теореме формула числа решений в силу леммы 6.31 справедлива для $n = 2$. Если же $n \geqslant 4$, то, используя

результат предыдущего случая и лемму 6.31, получаем (при $c_1, c_2 \in \mathbb{F}_q$)

$$N\left(x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = b\right) =$$
$$= \sum_{c_1+c_2=b} N\left(x_1x_2 + \cdots + x_{n-3}x_{n-2} = c_1\right) \times$$
$$\times N\left(x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = c_2\right) =$$
$$= \sum_{c_1+c_2=b} \left[q^{n-3} + v(c_1)\, q^{(n-4)/2}\right]\left[q - v(c_2)\right] =$$
$$= q^{n-1} + q^{(n-2)/2} \sum_{c_1 \in \mathbb{F}_q} v(c_1) -$$
$$- q^{n-3} \sum_{c_2 \in \mathbb{F}_q} v(c_2) - q^{(n-4)/2} \cdot \sum_{c_1+c_2=b} v(c_1)\, v(c_2) =$$
$$= q^{n-1} - v(b)\, q^{(n-2)/2},$$

где на последнем шаге мы воспользовались формулами (6.4) и (6.5). □

§ 3. Диагональные уравнения

В предыдущем параграфе мы пришли к изучению уравнений, содержащих диагональные квадратичные формы. Такие уравнения являются частным случаем общего семейства так называемых диагональных уравнений. *Диагональным уравнением* (над конечным полем $\mathbb{F}_q$) называется уравнение вида

$$a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b, \tag{6.10}$$

где $k_1, \ldots, k_n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{F}_q^*$ и $b \in \mathbb{F}_q$.

Число решений

$$N = N\left(a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = b\right)$$

уравнения (6.10) в $\mathbb{F}_q^n$ можно выразить через суммы Якоби. Если $c_1, \ldots, c_n \in \mathbb{F}_q$, то

$$N = \sum_{c_1+\cdots+c_n=b} N\left(a_1x_1^{k_1} = c_1\right) \ldots N\left(a_nx_n^{k_n} = c_n\right) =$$
$$= \sum_{c_1+\cdots+c_n=b} N\left(x_1^{k_1} = a_1^{-1}c_1\right) \ldots N\left(x_n^{k_n} = a_n^{-1}c_n\right).$$

Из (5.70) получаем

$$N\left(x^k = c\right) = \sum_{j=0}^{d-1} \lambda^j(c),$$

где λ — мультипликативный характер порядка $d = \text{НОД}(k, q-1)$ поля $\mathbb{F}_q$. Для $i = 1, \ldots, n$ пусть $d_i = \text{НОД}(k_i, q-1)$ и λ_i — мультипликативный характер порядка d_i поля $\mathbb{F}_q$. Тогда

$$N = \sum_{c_1+\cdots+c_n=b} \left(\sum_{j_1=0}^{d_1-1} \lambda_1^{j_1}(a_1^{-1}c_1)\right)\cdots\left(\sum_{j_n=0}^{d_n-1} \lambda_n^{j_n}(a_n^{-1}c_n)\right) =$$

$$= \sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \lambda_1^{j_1}(a_1^{-1}) \ldots \lambda_n^{j_n}(a_n^{-1}) \sum_{c_1+\cdots+c_n=b} \lambda_1^{j_1}(c_1)\ldots\lambda_n^{j_n}(c_n) =$$

$$= \sum_{j_1=0}^{d_1-1} \cdots \sum_{j_n=0}^{d_n-1} \bar{\lambda}_1^{j_1}(a_1)\ldots\bar{\lambda}_n^{j_n}(a_n) J_b(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}).$$

Если $(j_1, \ldots, j_n) = (0, \ldots, 0)$, то $J_b(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}) = q^{n-1}$ согласно (5.38) и (5.39). Если некоторые (но не все) j_i равны 0, то $J_b(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}) = 0$ согласно (5.38) и (5.40). Поэтому

$$N = q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \bar{\lambda}_1^{j_1}(a_1)\ldots\bar{\lambda}_n^{j_n}(a_n) J_b(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}). \quad (6.11)$$

Рассмотрим теперь два случая $b = 0$ и $b \neq 0$. Если $b = 0$, то из (5.41) вытекает, что если характер $\lambda_1^{j_1} \ldots \lambda_n^{j_n}$ нетривиален, то $J_0(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}) = 0$. Поэтому мы приходим к следующему результату.

6.33. Теорема. *Число N решений в $\mathbb{F}_q^n$ диагонального уравнения $a_1x_1^{k_1} + \ldots + a_nx_n^{k_n} = 0$ задается формулой*

$$N = q^{n-1} + \sum_{(j_1, \ldots, j_n)\in T} \bar{\lambda}_1^{j_1}(a_1)\ldots\bar{\lambda}_n^{j_n}(a_n) J_0(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}),$$

где λ_i — мультипликативный характер порядка $d_i = \text{НОД}(k_i, q-1)$ поля $\mathbb{F}_q$, $1 \leqslant i \leqslant n$, и T — множество всех n-наборов $(j_1, \ldots, j_n) \in \mathbb{Z}^n$, где $1 \leqslant j_i \leqslant d_i - 1$, $1 \leqslant i \leqslant n$, таких, что $\lambda_1^{j_1} \ldots \lambda_n^{j_n}$ — тривиальный характер поля $\mathbb{F}_q$.

Если же $b \neq 0$, то, применяя (5.38), получим, что

$$J_b(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}) = (\lambda_1^{j_1}\ldots\lambda_n^{j_n})(b)\, J(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}).$$

Это приводит к следующему результату.

6.34. Теорема. *Если $b \in \mathbb{F}_q^*$, то число N решений в $\mathbb{F}_q^n$ диагонального уравнения $a_1x_1^{k_1} + \ldots + a_nx_n^{k_n} = b$ задается формулой*

$$N = q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \lambda_1^{j_1}(ba_1^{-1})\ldots\lambda_n^{j_n}(ba_n^{-1}) J(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n}),$$

где λ_i *— мультипликативный характер порядка* $d_i = \text{НОД}\,(k_i, q-1)$ *поля* $\mathbb{F}_q$.

6.35. Замечание. Выведенные выше формулы показывают, что число N зависит не непосредственно от показателей k_i, а лишь от наибольших общих делителей $d_i = \text{НОД}\,(k_i, q-1)$. Можно поэтому считать без ограничения общности, что в уравнении (6.10) показателями k_i являются делители числа $q-1$. □

Из теорем 6.33 и 6.34 нетрудно получить оценки для числа N. Пусть $d_1, \ldots, d_n$ — натуральные числа, и пусть $M(d_1, \ldots, d_n)$ — число n-наборов $(j_1, \ldots, j_n) \in Z^n$, таких, что $1 \leqslant j_i \leqslant d_i - 1$ при $1 \leqslant i \leqslant n$ и $(j_1/d_1) + \ldots + (j_n/d_n) \in Z$.

6.36. Теорема. *Число* N *решений в* $\mathbb{F}_q^n$ *диагонального уравнения* $a_1x_1^{k_1} + \ldots + a_nx_n^{k_n} = 0$ *удовлетворяет неравенству*

$$|N - q^{n-1}| \leqslant M(d_1, \ldots, d_n)(q-1)q^{(n-2)/2},$$

где $d_i = \text{НОД}\,(k_i, q-1)$, $1 \leqslant i \leqslant n$.

Доказательство. Из следствия 5.23 и теоремы 6.33 вытекает (в обозначениях этой теоремы), что

$$|N - q^{n-1}| \leqslant |T|(q-1)q^{(n-2)/2}.$$

Группа мультипликативных характеров поля $\mathbb{F}_q$, согласно следствию 5.9, циклична. Пусть λ — образующий элемент этой группы. В теореме 6.33 можно взять $\lambda_i = \lambda^{(q-1)/d_i}$, $i = 1, \ldots, n$. Тогда произведение

$$\lambda_1^{j_1} \ldots \lambda_n^{j_n} = \lambda^{(j_1(q-1)/d_1) + \cdots + (j_n(q-1)/d_n)}$$

будет тривиальным характером в том и только том случае, если $(j_1/d_1) + \ldots + (j_n/d_n) \in Z$, так что $|T| = M(d_1, \ldots, d_n)$. □

6.37. Теорема. *Пусть* $b \in \mathbb{F}_q^*$. *Тогда число* N *решений в* $\mathbb{F}_q^n$ *диагонального уравнения* $a_1x_1^{k_1} + \ldots + a_nx_n^{k_n} = b$ *удовлетворяет неравенству*

$$|N - q^{n-1}| \leqslant$$

$$\leqslant [(d_1 - 1)\ldots(d_n - 1) - (1 - q^{-1/2})M(d_1, \ldots, d_n)]q^{(n-1)/2},$$

где $d_i = \text{НОД}\,(k_i, q-1)$, $1 \leqslant i \leqslant n$.

Доказательство. Из теорем 5.22 и 6.34 следует, что

$$|N - q^{n-1}| \leqslant [(d_1 - 1)\ldots(d_n - 1) - |T|]q^{(n-1)/2} + |T|q^{(n-2)/2} =$$
$$= [(d_1 - 1)\ldots(d_n - 1) - (1 - q^{-1/2})|T|]q^{(n-1)/2}.$$

Остается только напомнить, что $|T| = M(d_1, \ldots, d_n)$ на основании доказательства теоремы 6.36. □

Ясно, что $M(d_1, \ldots, d_n) \leqslant (d_1 - 1) \ldots (d_n - 1)$. Число $M(d_1, \ldots, d_n)$ может равняться нулю, например, если одно из чисел d_i взаимно просто со всеми остальными. Чтобы это доказать, предположим для определенности, что НОД $(d_1, d_i) = 1$ при всех $i = 2, \ldots, n$. Если для некоторого n-набора $(j_1, \ldots, j_n) \in Z^n$, где $1 \leqslant j_i \leqslant d_i - 1$ для $1 \leqslant i \leqslant n$, имеем $(j_1/d_1) + \ldots + (j_n/d_n) = m \in Z$, то $j_1 d_2 \ldots d_n + j d_1 = m d_1 \ldots d_n$ для некоторого $j \in Z$, поэтому $j_1 d_2 \ldots d_n \equiv 0 \pmod{d_1}$. Но НОД $(d_1, d_2 \ldots d_n) = 1$, значит, $j_1 \equiv 0 \pmod{d_1}$, что невозможно. Из теоремы 6.36 видно, что если $M(d_1, \ldots, d_n) = 0$, то $N = q^{n-1}$.

Общую формулу для $M(d_1, \ldots, d_n)$ можно получить следующим образом. Положим $D = \text{НОК}\ (d_1, \ldots, d_n)$ и $e(t) = e^{2\pi i t}$, где $t \in \mathbb{R}$; заметим, что

$$\frac{1}{D} \sum_{h=0}^{D-1} e\left(h\left(\frac{j_1}{d_1} + \cdots + \frac{j_n}{d_n}\right)\right) = \begin{cases} 1, & \text{если } \frac{j_1}{d_1} + \cdots + \frac{j_n}{d_n} \in Z, \\ 0 & \text{в противном случае.} \end{cases}$$

Поэтому

$$M(d_1, \ldots, d_n) = \sum_{j_1=1}^{d_1-1} \ldots \sum_{j_n=1}^{d_n-1} \frac{1}{D} \sum_{h=0}^{D-1} e\left(h\left(\frac{j_1}{d_1} + \cdots + \frac{j_n}{d_n}\right)\right) =$$

$$= \frac{1}{D} \sum_{h=0}^{D-1} \left(\sum_{j_1=1}^{d_1-1} e\left(j_1 \frac{h}{d_1}\right)\right) \ldots \left(\sum_{j_n=1}^{d_n-1} e\left(j_n \frac{h}{d_n}\right)\right) =$$

$$= \frac{1}{D} \sum_{h=0}^{D-1} \left(\sum_{j_1=0}^{d_1-1} e\left(j_1 \frac{h}{d_1}\right) - 1\right) \ldots \left(\sum_{j_n=0}^{d_n-1} e\left(j_n \frac{h}{d_n}\right) - 1\right) =$$

$$= \frac{1}{D} \sum_{h=0}^{D-1} \Bigg[(-1)^n + \Bigg.$$

$$\Bigg. + \sum_{r=1}^{n} (-1)^{n-r} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant n} \prod_{s=1}^{r} \left(\sum_{j_{i_s}=0}^{d_{i_s}-1} e\left(j_{i_s} \frac{h}{d_{i_s}}\right)\right) \Bigg].$$

Поскольку для $d \in \mathbb{N}$ имеет место соотношение

$$\sum_{j=0}^{d-1} e\left(j \frac{h}{d}\right) = \begin{cases} d, & \text{если } h \equiv 0 \pmod{d}, \\ 0 & \text{в противном случае,} \end{cases}$$

то произведение в последнем выражении для $M(d_1, \ldots, d_n)$ равно $d_{i_1} \ldots d_{i_r}$, если h делится на НОК $(d_{i_1}, \ldots, d_{i_r}) = \Delta_{i_1 \ldots i_r}$ и равно 0 в противном случае. Поэтому

$$M(d_1, \ldots, d_n) =$$

$$= (-1)^n + \frac{1}{D} \sum_{h=0}^{D-1} \sum_{r=1}^{n} (-1)^{n-r} \sum_{\substack{1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant n \\ h \equiv 0 \pmod{\Delta_{i_1 \ldots i_r}}}} d_{i_1} \ldots d_{i_r} =$$

$$= (-1)^n + \frac{1}{D} \sum_{r=1}^{n} (-1)^{n-r} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant n} d_{i_1} \ldots d_{i_r} \sum_{\substack{h=0 \\ h \equiv 0 \pmod{\Delta_{i_1 \ldots i_r}}}}^{D-1} 1.$$

Самая внутренняя сумма равна $D/\text{НОК}(d_{i_1}, \ldots, d_{i_r})$, так что

$$M(d_1, \ldots, d_n) = (-1)^n + \sum_{r=1}^{n} (-1)^{n-r} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant n} \frac{d_{i_1} \ldots d_{i_r}}{\Delta_{i_1 \ldots i_r}}. \quad (6.12)$$

Теперь мы укажем *еще один подход* к оценке числа $N = N(a_1 x_1^{k_1} + \ldots + a x_n^{k_n} = b)$ решений диагонального уравнения (6.10) в $\mathbb{F}_q^n$, опирающийся на суммы Гаусса. Согласно (5.5),

$$N = \frac{1}{q} \sum_{c_1, \ldots, c_n \in \mathbb{F}_q} \sum_{\chi} \chi(a_1 c_1^{k_1} + \cdots + a_n c_n^{k_n}) \bar{\chi}(b),$$

где во внутренней сумме χ пробегает все аддитивные характеры поля $\mathbb{F}_q$. Меняя порядок суммирования и отделяя часть, соответствующую тривиальному характеру χ_0, получим

$$N = \frac{1}{q} \sum_{\chi} \bar{\chi}(b) \sum_{c_1, \ldots, c_n \in \mathbb{F}_q} \chi(a_1 c_1^{k_1}) \ldots \chi(a_n c_n^{k_n}) =$$

$$= q^{n-1} + \frac{1}{q} \sum_{\chi \neq \chi_0} \bar{\chi}(b) \left(\sum_{c_1 \in \mathbb{F}_q} \chi(a_1 c_1^{k_1}) \right) \ldots \left(\sum_{c_n \in \mathbb{F}_q} \chi(a_n c_n^{k_n}) \right).$$

Применяя теперь теорему 5.30, получим

$$N = q^{n-1} + \frac{1}{q} \sum_{\chi \neq \chi_0} \bar{\chi}(b) \left(\sum_{j_1=1}^{d_1-1} \bar{\lambda}_1^{j_1}(a_1) G(\lambda_1^{j_1}, \chi) \right) \ldots$$

$$\ldots \left(\sum_{j_n=1}^{d_n-1} \bar{\lambda}_n^{j_n}(a_n) G(\lambda_n^{j_n}, \chi) \right) = q^{n-1} + \frac{1}{q} \sum_{j_1=1}^{d_1-1} \ldots$$

$$\ldots \sum_{j_n=1}^{d_n-1} \bar{\lambda}_1^{j_1}(a_1) \ldots \bar{\lambda}_n^{j_n}(a_n) \sum_{\chi \neq \chi_0} \bar{\chi}(b) G(\lambda_1^{j_1}, \chi) \ldots G(\lambda_n^{j_n}, \chi),$$

где λ_i, как и раньше, обозначает мультипликативный характер порядка $d_i = \text{НОД}(k_i, q-1)$ поля $\mathbb{F}_q$. Для внутренней суммы, используя обозначения из теоремы 5.7 и применяя теорему 5.12 (i), получим

$$\sum_{\chi \neq \chi_0} \bar{\chi}(b) G(\lambda_1^{j_1}, \chi) \ldots G(\lambda_n^{j_n}, \chi) =$$

$$= \sum_{a \in \mathbb{F}_q^*} \bar{\chi}_a(b) G(\lambda_1^{j_1}, \chi_a) \ldots G(\lambda_n^{j_n}, \chi_a) =$$

$$= G(\lambda_1^{j_1}, \chi_1) \ldots G(\lambda_n^{j_n}, \chi_1) \sum_{a \in \mathbb{F}_q^*} \bar{\chi}_b(a) \bar{\lambda}_1^{j_1}(a) \ldots \bar{\lambda}_n^{j_n}(a) =$$

$$= G(\lambda_1^{j_1}, \chi_1) \ldots G(\lambda_n^{j_n}, \chi_1) G(\bar{\lambda}_1^{j_1} \ldots \bar{\lambda}_n^{j_n}, \bar{\chi}_b),$$

так что

$$N = q^{n-1} + \frac{1}{q} \sum_{j_1=1}^{d_1-1} \ldots \sum_{j_n=1}^{d_n-1} G(\lambda_1^{j_1}, \chi_{a_1}) \ldots G(\lambda_n^{j_n}, \chi_{a_n}) G(\bar{\lambda}_1^{j_1} \ldots \bar{\lambda}_n^{j_n}, \bar{\chi}_b). \tag{6.13}$$

Для случая $b = 0$ можно применить (5.14); тогда

$$N = q^{n-1} + \left(1 - \frac{1}{q}\right) \sum_{(j_1, \ldots, j_n) \in T} G(\lambda_1^{j_1}, \chi_{a_1}) \ldots G(\lambda_n^{j_n}, \chi_{a_n}), \tag{6.14}$$

где T — то же множество, что и в теореме 6.33. Полученную в той теореме формулу теперь можно вывести из (6.14), используя теорему 5.12 (i) и формулы (5.42) и (5.44). Для случая $b \neq 0$ формулу (6.13) можно преобразовать в формулу из теоремы 6.34 применением теоремы 5.12 (i) и результата упр. 5.34.

Диагональное уравнение (6.10) можно рассматривать также как уравнение над некоторым конечным расширением поля $\mathbb{F}_q$,

а не над самим $\mathbb{F}_q$, как было до сих пор. Пусть $E = \mathbb{F}_{q^s}$, где $s \in \mathbb{N}$, — некоторое расширение поля $\mathbb{F}_q$; обозначим через N_s число решений в E^n диагонального уравнения (6.10). Попытаемся найти зависимость N_s от s в предположении, что все показатели k_i делят число $q-1$.

Для случая $b = 0$ можно получить значение N_s из (6.14). Если μ_1 — канонический аддитивный характер поля E, то каждый характер χ_{a_i} в (6.14) должен быть заменен на μ_{a_i}. Но для $a \in \mathbb{F}_q$ мы, согласно (5.7), имеем $\mu_a(\beta) = \chi_a\left(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)\right)$ при всех $\beta \in E$, так что $\mu_a = (\chi_a)'$, где $(\chi_a)'$ — характер, получаемый поднятием характера χ_a поля $\mathbb{F}_q$ до E (ср. с рассуждением, предшествующим теореме 5.14). Кроме того, каждый характер λ_i порядка k_i в (6.14) должен быть заменен мультипликативным характером порядка k_i поля E. Но поскольку функция нормы (см. определение 2.27) отображает E^* на $\mathbb{F}_q^*$ (по теореме 2.28 (ii)), то (надо учесть формулу $(\lambda_i)'(\beta) = \lambda_i\left(N_{E/\mathbb{F}_q}(\beta)\right)$, $\beta \in E^*$) поднятый характер $(\lambda_i)'$ имеет тот же порядок, что и λ_i, и, таким образом, характер λ_i в (6.14) можно заменить на $(\lambda_i)'$. Поэтому, применяя (6.14) и теорему 5.14, получаем

$$N_s = q^{s(n-1)} + \left(1 - \frac{1}{q^s}\right) \sum_{(j_1, \ldots, j_n) \in T} G\left(\left(\lambda_1^{j_1}\right)', (\chi_{a_1})'\right) \ldots$$

$$\ldots G\left(\left(\lambda_n^{j_n}\right)', (\chi_{a_n})'\right) =$$

$$= q^{s(n-1)} + (-1)^{n(s-1)}\left(1 - \frac{1}{q^s}\right) \sum_{(j_1, \ldots, j_n) \in T} G\left(\lambda_1^{j_1}, \chi_{a_1}\right)^s \ldots$$

$$\ldots G\left(\lambda_n^{j_n}, \chi_{a_n}\right)^s =$$

$$= (q^{n-1})^s + (-1)^n \sum_{(j_1, \ldots, j_n) \in T} \left((-1)^n G\left(\lambda_1^{j_1}, \chi_{a_1}\right) \ldots G\left(\lambda_n^{j_n}, \chi_{a_n}\right)\right)^s -$$

$$- (-1)^n \sum_{(j_1, \ldots, j_n) \in T} \left(\frac{1}{q}(-1)^n G\left(\lambda_1^{j_1}, \chi_{a_1}\right) \ldots G\left(\lambda_n^{j_n}, \chi_{a_n}\right)\right)^s.$$

Таким образом, эта сумма имеет вид

$$N_s = \nu_1^s + \ldots + \nu_t^s - \omega_1^s - \ldots - \omega_u^s, \tag{6.15}$$

где алгебраические числа $\nu_1, \ldots, \nu_t$, $\omega_1, \ldots, \omega_u$ не зависят от s и удовлетворяют условиям $|\nu_h| = q^{m_h/2}$ и $|\omega_j| = q^{n_j/2}$ для некоторых $m_h, n_j \in \mathbb{Z}$.

Для $b \neq 0$ значение N_s можно получить из (6.13). Те же рассуждения, что и выше, приводят к формуле

$$N_s = q^{s(n-1)} + \frac{1}{q^s} \sum_{j_1=1}^{k_1-1} \dots \sum_{j_n=1}^{k_n-1} G\left(\left(\lambda_1^{j_1}\right)', (\chi_{a_1})'\right) \dots G\left(\left(\lambda_n^{j_n}\right)', (\chi_{a_n})'\right) \times$$

$$\times G\left(\left(\bar{\lambda}_1^{j_1} \dots \bar{\lambda}_n^{j_n}\right)', (\bar{\chi}_b)'\right) =$$

$$= q^{s(n-1)} + \frac{1}{q^s} (-1)^{(n+1)(s-1)} \sum_{j_1=1}^{k_1-1} \dots \sum_{j_n=1}^{k_n-1} G\left(\lambda_1^{j_1}, \chi_{a_1}\right)^s \dots$$

$$\dots G\left(\lambda_n^{j_n}, \chi_{a_n}\right)^s G\left(\bar{\lambda}_1^{j_1} \dots \bar{\lambda}_n^{j_n}, \bar{\chi}_b\right)^s =$$

$$= (q^{n-1})^s + (-1)^{n+1} \sum_{j_1=1}^{k_1-1} \dots$$

$$\dots \sum_{j_n=1}^{k_n-1} \left(\frac{1}{q}(-1)^{n+1} G\left(\lambda_1^{j_1}, \chi_{a_1}\right) \dots G\left(\lambda_n^{j_n}, \chi_{a_n}\right) \times\right.$$

$$\left. \times G\left(\bar{\lambda}_1^{j_1} \dots \bar{\lambda}_n^{j_n}, \chi_b\right)\right)^s,$$

которая снова имеет вид (6.15).

Оценки, полученные в теоремах 6.36 и 6.37, можно использовать для доказательства существования решений диагональных уравнений (по крайней мере при достаточно больших q).

6.38. Пример. Пусть k — заданное натуральное число. Покажем, что для каждого конечного поля $\mathbb{F}_q$ с достаточно большим q, скажем

$$q > \frac{1}{4}\left[(k-1)(k-2) + \sqrt{k(k-1)(k^2-5k+8)}\right]^2,$$

каждый элемент $b \in \mathbb{F}_q$ может быть представлен в виде суммы двух k-х степеней элементов этого поля. Поскольку случай $b = 0$ тривиален, рассмотрим случай $b \neq 0$, и пусть N — число решений уравнения $x_1^k + x_2^k = b$ в $\mathbb{F}_q^2$. При $d = \text{НОД}(k, q-1)$ из теоремы 6.37 следует, что

$$|N - d| \leqslant \left[(d-1)^2 - (1 - q^{-1/2}) M(d, d)\right] q^{1/2}.$$

Теперь $M(d, d) = d - 1$ (согласно (6.12) или исходя из определения числа M), поэтому с учетом того, что $d \leqslant k$, получаем

$$|N - q| \leqslant \left[(d-1)^2 - (1 - q^{-1/2})(d-1)\right] q^{1/2} =$$

$$= (d-1)(d-2) q^{1/2} + d - 1 \leqslant$$

$$\leqslant (k-1)(k-2) q^{1/2} + k - 1,$$

и, в частности,

$$N \geqslant q - (k-1)(k-2)\, q^{1/2} - k + 1.$$

Теперь для достижения нашей цели достаточно лишь найти число $u_0 \in \mathbb{R}$, такое, чтобы при $q \geqslant u_0$ правая часть этого неравенства была положительна. В качестве u_0 можно, например, взять $u_0 = t_0^2$, где t_0 — наибольший из корней квадратного многочлена $t^2 - (k-1)(k-2)\, t - k + 1$. Относительно случая $k = 2$ см. также замечание 6.25. □

Некоторые сведения о числе решений диагональных уравнений могут быть получены и без использования тригонометрических сумм (в дальнейшем мы приведем несколько таких примеров). При таком подходе часто используются арифметические свойства полиномиальных коэффициентов; эти свойства можно вывести из приводимой ниже леммы 6.39. В качестве побочного продукта этого вспомогательного результата мы получим утверждение, что все полиномиальные коэффициенты являются целыми числами (что можно было бы доказать также комбинаторным путем). Для простого числа p обозначим через $E_p(r)$ наибольший целый показатель j, такой, что p^j делит число $r \in \mathbb{N}$. Через $\lfloor t \rfloor$ будем обозначать наибольшее целое число, не превосходящее числа $t \in \mathbb{R}$.

6.39. Лемма. *Для каждого целого неотрицательного числа m и каждого простого числа p имеет место формула*

$$E_p(m!) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor = \frac{m-s}{p-1},$$

где s — сумма коэффициентов p-ичного разложения числа m.

Доказательство. Если $p^i \geqslant m$, то $\lfloor m/p^i \rfloor = 0$, так что указанный в формуле ряд содержит не более конечного числа ненулевых членов. Первое равенство справедливо для $0! = 1$. Для натурального числа h

$$\left\lfloor \frac{h}{p^i} \right\rfloor - \left\lfloor \frac{h-1}{p^i} \right\rfloor = \begin{cases} 1, & \text{если } p^i \text{ делит } h, \\ 0 & \text{в противном случае.} \end{cases}$$

Отсюда для $m \geqslant 1$ получаем

$$E_p(m!) = E_p(1 \cdot 2 \ldots m) = \sum_{h=1}^{m} E_p(h) = \sum_{h=1}^{m} \sum_{i=1}^{\infty} \left(\left\lfloor \frac{h}{p^i} \right\rfloor - \left\lfloor \frac{h-1}{p^i} \right\rfloor \right) =$$

$$= \sum_{i=1}^{\infty} \sum_{h=1}^{m} \left(\left\lfloor \frac{h}{p^i} \right\rfloor - \left\lfloor \frac{h-1}{p^i} \right\rfloor \right) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor.$$

Для доказательства второго равенства представим число m в p-ичной системе: $m = b_u p^u + b_{u-1} p^{u-1} + \ldots + b_0$, где $0 \leqslant b_i < p$ для $0 \leqslant i \leqslant u$. Тогда

$$\left\lfloor \frac{m}{p} \right\rfloor = b_u p^{u-1} + b_{u-1} p^{u-2} + \cdots + b_2 p + b_1,$$
$$\left\lfloor \frac{m}{p^2} \right\rfloor = b_u p^{u-2} + b_{u-1} p^{u-3} + \cdots + b_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\left\lfloor \frac{m}{p^u} \right\rfloor = b_u$$

и $\lfloor m/p^i \rfloor = 0$ для $i > u$. Складывая эти равенства, получим

$$\sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor = b_u \frac{p^u - 1}{p-1} + b_{u-1} \frac{p^{u-1} - 1}{p-1} + \cdots + b_1 =$$
$$= \frac{1}{p-1} (b_u p^u + b_{u-1} p^{u-1} + \cdots + b_1 p + b_0 -$$
$$- b_u - b_{u-1} - \cdots - b_1 - b_0) =$$
$$= \frac{m-s}{p-1}. \qquad \square$$

6.40. Следствие. *Если m_0, m_1, ..., m_n — неотрицательные целые числа и $m = m_0 + m_1 + \ldots + m_n$, то полиномиальный коэффициент*

$$\frac{m!}{m_0!\, m_1! \ldots m_n!}$$

является целым числом.

Доказательство. Достаточно показать, что для каждого простого числа p его степень, делящая знаменатель, делит и числитель. Применяя неравенство

$$\lfloor t_0 + t_1 + \cdots + t_n \rfloor \geqslant \lfloor t_0 \rfloor + \lfloor t_1 \rfloor + \cdots + \lfloor t_n \rfloor$$

для $t_0, t_1, \ldots, t_n \in \mathbb{R}$

и лемму 6.39, действительно получаем

$$E_p(m!) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor \geqslant \sum_{i=1}^{\infty} \left(\left\lfloor \frac{m_0}{p^i} \right\rfloor + \left\lfloor \frac{m_1}{p^i} \right\rfloor + \cdots + \left\lfloor \frac{m_n}{p^i} \right\rfloor \right) =$$
$$= E_p(m_0!) + E_p(m_1!) + \cdots + E_p(m_n!) =$$
$$= E_p(m_0!\, m_1! \ldots m_n!). \qquad \square$$

6.41. Теорема. *Число решений в $\mathbb{F}_q^n$ диагонального уравнения* (6.10) *делится на характеристику p поля $\mathbb{F}_q$ при условии, что*

$$\frac{1}{d_1}+\cdots+\frac{1}{d_n}>1, \tag{6.16}$$

где $d_i = \text{НОД}\,(k_i,\ q-1)$ *для* $i = 1, \ldots, n$.

Доказательство. Пусть N — число решений уравнения (6.10), и пусть $\overline{N}$ — то же число N, но рассматриваемое как элемент поля $\mathbb{F}_q$. Положим

$$G(x_1, \ldots, x_n) = a_0 + a_1x_1^{k_1} + \cdots + a_nx_n^{k_n}, \quad \text{где} \quad a_0 = -b.$$

Так как N является также числом решений уравнения $G(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$, то

$$\begin{aligned}
\overline{N} &= \sum_{c_1,\ \ldots,\ c_n\in\mathbb{F}_q} (1 - G(c_1, \ldots, c_n)^{q-1}) = \\
&= -\sum_{c_1,\ \ldots,\ c_n\in\mathbb{F}_q} G(c_1, \ldots, c_n)^{q-1} = \\
&= -\sum_{c_1,\ \ldots,\ c_n\in\mathbb{F}_q} \left(a_0 + a_1c_1^{k_1} + \cdots + a_nc_n^{k_n}\right)^{q-1} = \\
&= -\sum_{c_1,\ \ldots,\ c_n\in\mathbb{F}_q} \sum_{\substack{h_0,\ h_1,\ \ldots,\ h_n\geqslant 0\\ h_0+h_1+\cdots+h_n=q-1}} \frac{(q-1)!}{h_0!\ h_1!\ \ldots\ h_n!}\, a_0^{h_0}a_1^{h_1}\ldots a_n^{h_n}c_1^{k_1h_1}\ldots \\
&\quad \ldots c_n^{k_nh_n} = \\
&= -\sum_{\substack{h_0,\ h_1,\ \ldots,\ h_n\geqslant 0\\ h_0+h_1+\cdots+h_n=q-1}} \frac{(q-1)!}{h_0!\ h_1!\ \ldots\ h_n!}\, a_0^{h_0}a_1^{h_1}\ldots \\
&\quad \ldots a_n^{h_n}\left(\sum_{c_1\in\mathbb{F}_q} c_1^{k_1h_1}\right)\ldots\left(\sum_{c_n\in\mathbb{F}_q} c_n^{k_nh_n}\right).
\end{aligned}$$

В силу леммы 6.3 во внимание следует принимать лишь те члены внешней суммы, в которых h_i положительны и k_ih_i делятся на $q-1$ для всех i, $1 \leqslant i \leqslant n$. Но последнее условие эквивалентно делимости h_i на $(q-1)/d_i$. Поэтому

$$\overline{N} = (-1)^{n+1} \sum_{(h_0,\ h_1,\ \ldots,\ h_n)\in H} \frac{(q-1)!}{h_0!\ h_1!\ \ldots\ h_n!}\, a_0^{h_0}a_1^{h_1}\ldots a_n^{h_n}, \tag{6.17}$$

где через H обозначено множество $(n+1)$-наборов $(h_0, h_1, \ldots, h_n)$ целых чисел, для которых $h_0 + h_1 + \ldots + h_n = q-1$, $h_0 \geqslant 0$

и для каждого i, $1 \leqslant i \leqslant n$, число h_i является положительным кратным числа $(q-1)/d_i$.

Теперь допустим, что выполняется неравенство (6.16). Тогда если $(h_0, h_1, \ldots, h_n) \in H$, то $h_i \geqslant (q-1)/d_i$ для всех i, $1 \leqslant i \leqslant n$, так что

$$h_0 + h_1 + \cdots + h_n \geqslant \frac{q-1}{d_1} + \cdots + \frac{q-1}{d_n} > q-1,$$

а это невозможно. Таким образом, множество H пусто, так что $\overline{N} = 0$ на основании (6.17), а это означает, что число N делится на p. □

Если $k_1 = \ldots = k_n = d$ и d — делитель числа $q-1$, то из (6.16) получаем неравенство $n > d$, и мы приходим к частному случаю теоремы 6.5.

6.42. Теорема. *Пусть p — характеристика поля $\mathbb{F}_q$, $k_1, \ldots, k_n$ — заданные натуральные числа, $a_1, \ldots, a_n \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$ и числа $d_i = \text{НОД}(k_i, q-1)$ делят $p-1$ для $i = 1, \ldots, n$, причем*

$$\frac{1}{d_1} + \cdots + \frac{1}{d_n} = 1.$$

Тогда диагональное уравнение (6.10) *с показателями степени $k_1, \ldots, k_n$ имеет хотя бы одно решение в $\mathbb{F}_q^n$.*

Доказательство. Применим (6.17) и заметим, что при условии $(1/d_1) + \ldots + (1/d_n) = 1$ множество H состоит из единственного $(n+1)$-набора $(0, h_1, \ldots, h_n)$, где $h_i = (q-1)/d_i$ для $1 \leqslant i \leqslant n$. Поэтому

$$\overline{N} = (-1)^{n+1} \frac{(q-1)!}{h_1! \ldots h_n!} a_1^{h_1} \ldots a_n^{h_n}.$$

Так как $q = p^r$ для некоторого $r \in \mathbb{N}$, то

$$q - 1 = (p-1)\, p^{r-1} + (p-1)\, p^{r-2} + \ldots + (p-1)$$

есть представление числа $q-1$ в p-ичной системе, так что

$$E_p((q-1)!) = \frac{q-1-r(p-1)}{p-1} = \frac{q-1}{p-1} - r$$

согласно лемме 6.39. Поскольку числа d_i делят $p-1$, то представление числа $h_i = (q-1)/d_i$ в p-ичной системе имеет вид

$$h_i = \frac{p-1}{d_i} p^{r-1} + \frac{p-1}{d_i} p^{r-2} + \cdots + \frac{p-1}{d_i},$$

так что

$$E_p(h_i!) = \frac{h_i - r(p-1)/d_i}{p-1} = \frac{h_i}{p-1} - \frac{r}{d_i}.$$

Из равенства $(1/d_1) + \ldots + (1/d_n) = 1$ тогда следует, что

$$E_p(h_1!) + \cdots + E_p(h_n!) = E_p((q-1)!),$$

а это означает, что число $(q-1)!/h_1! \ldots h_n!$ не делится на p. Но поскольку все a_i отличны от 0, то это значит, что $\bar{N} \neq 0$, а следовательно, $N > 0$. □

В некоторых случаях этот метод удается применить и к уравнениям, не являющимся диагональными. Если в следующей теореме многочлен g является постоянным, то соответствующий результат будет следствием теоремы 6.42.

6.43. Теорема. *Пусть p — характеристика поля $\mathbb{F}_q$, k — положительный делитель числа $p-1$ и $a_1, \ldots, a_k \in \mathbb{F}_q^*$. Если $g \in \mathbb{F}_q[x_1, \ldots, x_k]$ — многочлен степени, меньшей чем k, то уравнение*

$$a_1 x_1^k + \cdots + a_k x_k^k = g(x_1, \ldots, x_k)$$

имеет по крайней мере одно решение в $\mathbb{F}_q^k$.

Доказательство. Поступим так же, как при доказательстве теоремы 6.41, используя те же обозначения и функцию G вида

$$G(x_1, \ldots, x_k) = a_1 x_1^k + \cdots + a_k x_k^k - g(x_1, \ldots, x_k).$$

Тогда

$$\bar{N} = -\sum_{c_1, \ldots, c_k \in \mathbb{F}_q} (a_1 c_1^k + \cdots + a_k c_k^k - g(c_1, \ldots, c_k))^{q-1} =$$

$$= -\sum_{c_1, \ldots, c_k \in \mathbb{F}_q} \sum_{\substack{h_0, h_1, \ldots, h_k \geqslant 0 \\ h_0 + h_1 + \cdots + h_k = q-1}} \frac{(q-1)!}{h_0!\, h_1! \ldots h_k!} (-g(c_1, \ldots, c_k))^{h_0} \times$$

$$\times a_1^{h_1} \ldots a_k^{h_k} c_1^{kh_1} \ldots c_k^{kh_k} =$$

$$= -\sum_{\substack{h_0, h_1, \ldots, h_k \geqslant 0 \\ h_0 + h_1 + \cdots + h_k = q-1}} \frac{(q-1)!}{h_0!\, h_1! \ldots h_k!} (-1)^{h_0} a_1^{h_1} \ldots a_k^{h_k} \times$$

$$\times \sum_{c_1, \ldots, c_k \in \mathbb{F}_q} g(c_1, \ldots, c_k)^{h_0} c_1^{kh_1} \ldots c_k^{kh_k}.$$

Если $h_0 > 0$, то

$$h_0 \deg(g) + kh_1 + \ldots + kh_k < k(h_0 + h_1 + \ldots + h_k) = k(q-1),$$

и из леммы 6.4 следует, что внутренняя сумма равна 0, так что в нашей сумме остаются лишь члены, соответствующие $h_0 = 0$:

$$\overline{N} = -\sum_{\substack{h_1, \ldots, h_k \geqslant 0 \\ h_1 + \cdots + h_k = q-1}} \frac{(q-1)!}{h_1! \ldots h_k!} a_1^{h_1} \ldots a_k^{h_k} \left(\sum_{c_1 \in \mathbb{F}_q} c_1^{kh_1} \right) \ldots \left(\sum_{c_k \in \mathbb{F}_q} c_k^{kh_k} \right).$$

Согласно лемме 6.3, ненулевой член может получиться лишь в том случае, если для каждого i, $1 \leqslant i \leqslant k$, натуральное число h_i делится на $h = (q-1)/k$. Поскольку $h_1 + \ldots + h_k = q - 1$, то это возможно лишь в случае $h_1 = \ldots = h_k = h$. Таким образом,

$$\overline{N} = (-1)^{k+1} \frac{(q-1)!}{h!^k} (a_1 \ldots a_k)^h.$$

Как и в доказательстве теоремы 6.42, показываем, что число $(q-1)!/h!^k$ не делится на p. Это означает, что $\overline{N} \neq 0$, а значит, $N > 0$. □

6.44. Следствие. *Если k — положительный делитель числа $p - 1$, где p — простое число, и $f_1(x_1), \ldots, f_k(x_k)$ — многочлены степени k над конечным полем $\mathbb{F}_q$ характеристики p, то уравнение*

$$f_1(x_1) + \ldots + f_k(x_k) = 0$$

имеет по крайней мере одно решение в $\mathbb{F}_q^k$.

§ 4. Метод Степанова—Шмидта

Рассмотрим специальные типы уравнений вида $F(x, y) = 0$, где $F \in \mathbb{F}_q[x, y]$, для которых удается установить нетривиальные результаты о числе решений «элементарными» методами, т. е. методами, не связанными с алгебраической геометрией или с широким использованием полей алгебраических функций. Нашей основной целью будет доказательство ряда результатов, необходимых для оценки некоторых сумм значений характеров из § 4 гл. 5 (см. теоремы 5.38 и 5.41).

Первым типом уравнений, который мы рассмотрим, будут уравнения вида $y^m = f(x)$. Следующий результат служит исходной точкой для исследования вопроса о числе решений таких уравнений.

6.45. Лемма. *Пусть $\mathbb{F}_q$ — конечное поле, $f \in \mathbb{F}_q[x]$, m — положительный делитель числа $q - 1$ и $g = f^{(q-1)/m}$. Тогда число N решений уравнения $y^m = f(x)$, лежащих в $\mathbb{F}_q^2$, задается формулой*

$$N = |T_0| + m|T_1|,$$

где T_0 *— множество корней многочлена* $f(x)$ *в поле* $\mathbb{F}_q$, *а* T_1 *— множество корней многочлена* $g(x) - 1$ *в* $\mathbb{F}_q$. *Кроме того,* $|T_0| + |T_1| + |T_2| = q$, *где* T_2 *— множество корней многочлена* $g(x)^{m-1} + g(x)^{m-2} + \ldots + g(x) + 1$ *в* $\mathbb{F}_q$.

Доказательство. Будем различать решения $(x = c_1,\ y = c_2)$ уравнения $y^m = f(x)$, у которых $c_2 = 0$ и у которых $c_2 \neq 0$. Число решений вида $(c_1,\ 0)$ в точности равно T_0. Если же $c_2 \neq 0$, то для решения $(c_1,\ c_2)$ имеем $f(c_1) \neq 0$, и поскольку мультипликативная группа $\mathbb{F}_q^*$ поля $\mathbb{F}_q$ циклична (см. теорему 2.8), то $f(c_1)$ является m-й степенью некоторого элемента из $\mathbb{F}_q^*$ в том и только том случае, когда $g(c_1) = f(c_1)^{(q-1)/m} = 1$. При этом если $g(c_1) = 1$, то существует ровно m элементов $c_2 \in \mathbb{F}_q^*$, таких, что $c_2^m = f(c_1)$. Отсюда следует, что $N = |T_0| + m|T_1|$.

Легко убедиться в том, что множества T_0, T_1 и T_2 попарно не пересекаются. С другой стороны, для каждого элемента $c \in \mathbb{F}_q$, очевидно, выполняется равенство

$$0 = f(c)^q - f(c) = f(c)(g(c) - 1)(g(c)^{m-1} + g(c)^{m-2} + \cdots + g(c) + 1).$$

Отсюда вытекает, что каждый элемент поля $\mathbb{F}_q$ принадлежит одному из трех указанных множеств. Следовательно, $|T_0| + |T_1| + |T_2| = q$. □

Ключевым пунктом элементарного метода Степанова и Шмидта является построение некоторого вспомогательного многочлена, кратными корнями которого являются заранее заданные элементы. Доказываемая ниже лемма гарантирует, что такой вспомогательный многочлен является ненулевым. Будем применять следующие терминологию и обозначения. Пусть K — произвольное поле. Многочлен положительной степени $F \in K[x, y]$ назовем *абсолютно неприводимым* (над K), если он неприводим (т. е. не допускает нетривиального разложения) над любым алгебраическим расширением поля K. Через $K(x)$ будем обозначать *поле рациональных функций* над K, т. е. поле, состоящее из дробей вида f/g, $f,\ g \in K[x]$, $g \neq 0$.

6.46. Лемма. *Пусть* $f \in \mathbb{F}_q[x]$ *— такой многочлен степени* $k \geqslant 1$ *и* $m \geqslant 2$ *— такой делитель числа* $q - 1$, *что многочлен* $y^m - f(x)$ *абсолютно неприводим. Положим* $g = f^{(q-1)/m}$, *и пусть* $h_1, h_2, \ldots, h_{m-1}$ *— многочлены вида*

$$h_i(x) = \sum_{j=0}^{u} e_{ij}(x) x^{qj}, \quad 0 \leqslant i \leqslant m - 1,$$

где $e_{ij} \in \mathbb{F}_q[x]$ *и* $\deg(e_{ij}) \leqslant q/m - k$. *Тогда если*

$$h_0 + h_1 g + \ldots + h_{m-1} g^{m-1} = 0, \tag{6.18}$$

то все многочлены e_{ij} *нулевые.*

Доказательство. Сначала установим справедливость леммы при дополнительном предположении, что $f(0) \neq 0$. Положим

$$A(y; h_0, \ldots, h_{m-1}) = h_0 + h_1 y + \cdots + h_{m-1} y^{m-1}.$$

Тогда многочлен

$$B(y_1, \ldots, y_m) = \prod_{i=1}^{m} A(y_i; h_0, \ldots, h_{m-1})$$

является симметрическим многочленом от переменных $y_1, \ldots, y_m$. По основной лемме о симметрических многочленах (см. пример 1.74) многочлен $B(y_1, \ldots, y_m)$ можно выразить в виде многочлена от элементарных симметрических многочленов $\sigma_1(y_1, \ldots, y_m), \ldots, \sigma_m(y_1, \ldots, y_m)$. Пусть $\zeta_1 = 1, \zeta_2, \ldots, \zeta_m$ — корни m-й степени из единицы в поле $\mathbb{F}_q$; положим $y_i = \zeta_i y$, $1 \leqslant i \leqslant m$. Из равенства $x^m - 1 = (x - \zeta_1) \ldots (x - \zeta_m)$ получаем, что $\sigma_i(\zeta_1 y, \ldots, \zeta_m y) = 0$ для всех i, $1 \leqslant i \leqslant m - 1$, и $\sigma_m(\zeta_1 y, \ldots, \zeta_m y) = -y^m$. Поэтому $B(\zeta_1 y, \ldots, \zeta_m y)$ является многочленом от y^m; обозначим его $G(y^m)$. Сравнивая степени y, получаем

$$m \deg(G) = \deg(B(\zeta_1 y, \ldots, \zeta_m y)) \leqslant m(m-1)$$

(здесь $\deg(G)$ — степень G как многочлена от y^m). Отсюда следует, что $\deg(G) \leqslant m - 1$. Поэтому можно написать

$$\prod_{i=1}^{m} A(\zeta_i y; h_0, \ldots, h_{m-1}) = \sum_{i=0}^{m-1} C_i(h_0, \ldots, h_{m-1}) y^{mi}, \tag{6.19}$$

где каждый C_i (как многочлен от $h_0, \ldots, h_{m-1}$) имеет степень, не превосходящую m. Поскольку $A(\zeta_1 g; h_0, \ldots, h_{m-1}) = 0$ в силу (6.18) и $g^m = f^{q-1}$, из (6.19) вытекает, что

$$\sum_{i=0}^{m-1} C_i(h_0, \ldots, h_{m-1}) f^{(q-1)i} = 0.$$

Умножая это равенство на f^{m-1}, получим

$$\sum_{i=0}^{m-1} C_i(h_0, \ldots, h_{m-1}) f^{qi} f^{m-1-i} = 0.$$

Рассматривая последнее равенство по модулю x^q и замечая, что $h_i(x) \equiv e_{i0}(x) \pmod{x^q}$, $f(x)^q \equiv f(0) \pmod{x^q}$, получаем

$$\sum_{i=0}^{m-1} C_i(e_{00}(x), \ldots, e_{m-1,0}(x)) f(0)^i f(x)^{m-1-i} \equiv 0 \pmod{x^q}.$$

Но поскольку степень по x левой части не превосходит числа $m(q/m-k)+(m-1)k<q$, то

$$\sum_{i=0}^{m-1} C_i(e_{00}, \ldots, e_{m-1,0}) f(0)^i f^{m-1-i} = 0,$$

откуда

$$\sum_{i=0}^{m-1} C_i(e_{00}, \ldots, e_{m-1,0}) \left(\frac{f(0)}{f}\right)^i = 0. \tag{6.20}$$

В подходящем алгебраическом расширении поля $\mathbb{F}_q$ существует элемент α, такой, что $\alpha^m = f(0)$. Тогда $(\alpha y)^m - f(x) = f(0) \cdot (y^m - f(0)^{-1} f(x))$, так что многочлен $y^m - f(0)^{-1} f(x)$ абсолютно неприводим (ввиду абсолютной неприводимости $y^m - f(x)$). Далее, многочлен $y^m - f(0)^{-1} f(x)$ (как многочлен от y над полем $\mathbb{F}_q(x)$) имеет в некотором расширении поля $\mathbb{F}_q(x)$ корень Y. Из (6.20) получаем

$$\sum_{i=0}^{m-1} C_i(e_{00}, \ldots, e_{m-1,0}) Y^{-mi} = 0.$$

Поэтому из (6.19) следует, что

$$\prod_{i=1}^{m} A(\zeta_i Y^{-1}; e_{00}, \ldots, e_{m-1,0}) = 0.$$

Таким образом, $A(\zeta_i Y^{-1}; e_{00}, \ldots, e_{m-1,0}) = 0$ для некоторого i, $0 \leqslant i \leqslant m-1$, и после умножения на Y^{m-1} получаем для этого i равенство

$$e_{00} Y^{m-1} + \zeta_i e_{10} Y^{m-2} + \cdots + \zeta_i^{m-1} e_{m-1,0} = 0.$$

Но Y имеет степень m над полем $\mathbb{F}_q(x)$, так как многочлен $y^m - f(0)^{-1} f(x)$ абсолютно неприводим, поэтому все многочлены $e_{00}, e_{10}, \ldots, e_{m-1,0}$ нулевые. Значит, мы можем разделить (6.18) на x^q и с помощью такого же рассуждения доказать, что $e_{01} = e_{11} = \ldots = e_{m-1,1} = 0$. Продолжая таким же образом, получим, что все e_{ij} — нулевые многочлены.

Остается показать, что общий случай можно свести к случаю $f(0) \neq 0$. Если $k \geqslant q$, то $\deg(e_{ij}) < 0$ (по предположению), так что $e_{ij} = 0$. Поэтому можно считать, что $k < q$, так что существует некоторый элемент $c \in \mathbb{F}_q$, для которого $f(c) \neq 0$. Положим $f_1(x) = f(x+c)$ и $g_1(x) = g(x+c)$; тогда многочлен $y^m - f_1(x)$, очевидно, абсолютно неприводим, и в силу (6.18)

$$h_0(x+c) + h_1(x+c) g_1(x) + \cdots + h_{m-1}(x+c) g_1(x)^{m-1} = 0,$$

где многочлены $h_i(x+c)$ снова имеют требуемый вид (но с другими многочленами $e_{ij}(x)$). Так как $f_1(0) \neq 0$, то установленный

выше результат приводит к равенству нулю всех многочленов e_{ij}, так что все $h_i(x+c)$ равны 0, откуда следует, что все многочлены h_i нулевые, а значит, и все исходные многочлены e_{ij} равны нулю. □

При построении вспомогательного многочлена с заданными кратными корнями нам понадобится удобный метод определения кратности корней. Для поля характеристики 0 это успешно осуществляется при помощи производных, однако для поля простой характеристики p метод производных можно применять лишь в ограниченных пределах (ср. упр. 1.51). Например, у многочлена x^p все производные в точке 0 обращаются в нуль, тогда как 0 является корнем всего лишь кратности p. Поэтому мы введем усовершенствованные производные, так называемые гиперпроизводные, которые окажутся более полезными.

Пусть K — произвольное поле. Для целого неотрицательного числа n и многочлена $f(x) = \sum_{j=0}^{d} a_j x^j \in K[x]$ определим *n-ю гиперпроизводную* $E^{(n)}(f)$ равенством

$$E^{(n)}(f) = E^{(n)}\left(\sum_{j=0}^{d} a_j x^j\right) = \sum_{j=0}^{d} \binom{j}{n} a_j x^{j-n}.$$

Здесь мы применяем стандартное соглашение о биномиальных коэффициентах, а именно считаем, что $\binom{j}{n} = 0$ при $n > j$; это гарантирует, что n-я гиперпроизводная является многочленом над полем K. Если поле K имеет характеристику 0, то

$$E^{(n)}(f) = \frac{1}{n!} f^{(n)} \quad \text{для всех } f \in K[x].$$

Ясно, что $E^{(n)}$ является линейным оператором в том смысле, что $E^{(n)}(cf) = cE^{(n)}(f)$ и $E^{(n)}(f_1 + f_2) = E^{(n)}(f_1) + E^{(n)}(f_2)$ для всех $c \in K$ и $f, f_1, f_2 \in K[x]$. Установим теперь некоторые формулы для гиперпроизводных, которые нам понадобятся в дальнейшем.

6.47. Лемма. *Если $f_1, \ldots, f_t \in K[x]$, где K — произвольное поле, то*

$$E^{(n)}(f_1, \ldots, f_t) = \sum_{\substack{n_1, \ldots, n_t \geqslant 0 \\ n_1 + \ldots + n_t = n}} E^{(n_1)}(f_1) \ldots E^{(n_t)}(f_t). \quad (6.21)$$

Доказательство. Ввиду линейности $E^{(n)}$ достаточно доказать эту формулу для одночленов. Нетрудно видеть, что для многочле-

нов $f_j(x) = x^{k_j}$, $j = 1, \ldots, t$, равенство (6.21) эквивалентно равенству

$$\binom{k_1 + \ldots + k_t}{n} = \sum_{\substack{n_1, \ldots, n_t \geqslant 0 \\ n_1 + \ldots + n_t = n}} \binom{k_1}{n_1} \ldots \binom{k_t}{n_t};$$

последнее легко доказывается сравнением коэффициентов при x^n в обеих частях равенства

$$(x+1)^{k_1 + \ldots + k_t} = (x+1)^{k_1} \ldots (x+1)^{k_t}. \qquad \square$$

6.48. Следствие. *Если* $c \in K$, *то*

$$E^{(n)}((x-c)^t) = \binom{t}{n}(x-c)^{t-n}.$$

Доказательство. Применим к многочленам $f_i(x) = x - c$, $1 \leqslant i \leqslant t$, лемму 6.47. Так как $E^{(1)}(x-c) = 1$ и $E^{(n)}(x-c) = 0$ для $n \geqslant 2$, то в сумме (6.21) останутся лишь те члены, для которых все n_i принимают лишь значения 0 или 1. Число таких членов равно $\binom{t}{n}$, а каждый член равен $(x-c)^{t-n}$. $\square$

6.49. Следствие. *Если* $0 \leqslant n \leqslant t$ *и* $f, w \in K[x]$, *где* K — *произвольное поле, то*

$$E^{(n)}(wf^t) = w_1 f^{t-n},$$

где $w_1 \in K[x]$ *и* $\deg(w_1) \leqslant \deg(w) + n(\deg(f) - 1)$.

Доказательство. Применяя (6.21), получим

$$E^{(n)}(wf^t) = \sum_{\substack{n_0, n_1, \ldots, n_t \geqslant 0 \\ n_0 + n_1 + \ldots + n_t = n}} E^{(n_0)}(w) E^{(n_1)}(f) \ldots E^{(n_t)}(f).$$

Здесь в правой части каждый член делится на f^{t-n}, так как не менее $t - n$ из чисел $n_1, \ldots, n_t$ равны нулю. Поэтому $E^{(n)}(wf^t) = w_1 f^{t-n}$ для некоторого $w_1 \in K[x]$. Кроме того,

$$\begin{aligned} \deg(w_1) &= \deg(E^{(n)}(wf^t)) - (t-n)\deg(f) \leqslant \\ &\leqslant \deg(w) + t\deg(f) - n - (t-n)\deg(f) = \\ &= \deg(w) + n(\deg(f) - 1). \end{aligned} \qquad \square$$

6.50. Следствие. *Пусть* K — *поле простой характеристики* p, *и пусть задан многочлен вида* $h(x) = v(x, x^{p^s})$, *где* $v(x, y) \in K[x, y]$ *и* $s \in \mathbb{N}$. *Тогда* n-*я гиперпроизводная* $E^{(n)}(h)$ *многочлена* $h(x)$ *для* $0 \leqslant n < p^s$ *равна* n-*й частной производной многочлена* $v(x, y)$ *по* x *с последующей подстановкой* $y = x^{p^s}$.

Доказательство. Ввиду линейности $E^{(n)}$ достаточно рассмотреть лишь случай, когда $v(x, y) = x^j y^k$. Заметим сначала, что при $0 < n < p^s$ биномиальный коэффициент

$$\binom{p^s}{n} = \frac{p^s}{n}\binom{p^s-1}{n-1}$$

делится на p. Таким образом,

$$E^{(n)}(x^{p^s}) = \binom{p^s}{n} x^{p^s-n} = 0$$

в поле характеристики p. Поэтому, применяя лемму 6.47 с многочленами $f_1(x) = x^j$, $f_2(x) = \ldots = f_{k+1}(x) = x^{p^s}$, получим

$$E^{(n)}(h) = \binom{j}{n} x^{j-n} x^{kp^s}.$$

Такой же результат получится, если вычислить n-ю частную производную многочлена $v(x, y)$ по x и затем произвести подстановку $y = x^{p^s}$. □

Следующий результат показывает, что гиперпроизводные являются подходящим инструментом для определения кратности корней.

6.51. Лемма. *Пусть f — многочлен над произвольным полем K. Если элемент $c \in K$ является общим корнем гиперпроизводных $E^{(n)}(f)$ для $n = 0, 1, \ldots, M-1$, то этот элемент является корнем многочлена f кратности не менее M.*

Доказательство. Пусть $f(x) = a_0 + a_1(x-c) + \ldots + a_d(x-c)^d$. Из следствия 6.48 получаем

$$E^{(n)}(f(x)) = a_n + \binom{n+1}{n} a_{n+1}(x-c) + \ldots + \binom{d}{n} a_d (x-c)^{d-n}.$$

Подставляя $x = c$, получим $a_n = 0$ для $n = 0, 1, \ldots, M-1$, так что степень $(x-c)^M$ делит $f(x)$. Остальное вытекает из определения 1.65. □

Теперь мы в состоянии доказать основную лемму, в которой строится нужный нам вспомогательный многочлен.

6.52. Лемма. *Пусть $f \in \mathbb{F}_q[x]$ — такой многочлен степени $k \geqslant 1$ и $m \geqslant 2$ — такой делитель числа $q-1$, что многочлен $y^m - f(x)$ абсолютно неприводим. Пусть, далее, $g = f^{(q-1)/m}$, $B \in \mathbb{F}_q[x]$ — некоторый заданный многочлен степени r, $1 \leqslant r < m$, и T — множество таких элементов $c \in \mathbb{F}_q$, для которых либо $f(c) = 0$, либо $B(g(c)) = 0$. Пусть, наконец, M — такое натуральное число, что $M \geqslant k+1$ и $(M+3)^2 \leqslant 2q/m$. Тогда существует ненулевой многочлен $h \in \mathbb{F}_q[x]$, такой, что*

каждый элемент $c \in T$ *является его корнем кратности не менее* M, *и при этом*

$$\deg(h) < \frac{r}{m} qM + 4qk.$$

Доказательство. Будем искать нужный нам многочлен в следующем виде:

$$h(x) = f(x)^M \sum_{i=0}^{m-1} \sum_{j=0}^{u} e_{ij}(x)\, g(x)^i\, x^{qj}, \tag{6.22}$$

где e_{ij} — многочлены с коэффициентами из $\mathbb{F}_q$, которые надо определить, причем должно выполняться неравенство $\deg(e_{ij}) \leqslant q/m - k$, и где

$$u = \left\lfloor \frac{r}{m}(M + k + 1) \right\rfloor. \tag{6.23}$$

Найдем n-е гиперпроизводные многочлена h для $n = 0, 1, \ldots, M - 1$. Заметим сначала, что поскольку g является степенью многочлена f, то по следствию 6.49

$$E^{(n)}(f^M e_{ij} g^i) = f^{M-n} e_{ijn} g^i,$$

где

$$\deg(e_{ijn}) \leqslant \deg(e_{ij}) + n(k-1) \leqslant$$

$$\leqslant \frac{q}{m} - k + n(k-1) \leqslant \frac{q}{m} + n(k-1) - 1. \tag{6.24}$$

Можно считать, что $h(x) = v(x, x^q)$, где

$$v(x, y) = \sum_{i=0}^{m-1} \sum_{j=0}^{u} f(x)^M e_{ij}(x)\, g(x)^i\, y^j,$$

и так как $M \leqslant q$, то можно применить следствие 6.50 для $0 \leqslant n \leqslant M - 1$. Получим

$$E^{(n)}(h(x)) = f(x)^{M-n} \sum_{i=0}^{m-1} \sum_{j=0}^{u} e_{ijn}(x)\, g(x)^i\, x^{qj}. \tag{6.25}$$

Пусть $B(x) = b_0 + b_1 x + \ldots + b_{r-1} x^{r-1} - x^r$, где $b_i \in \mathbb{F}_q$. Если элемент $c \in \mathbb{F}_q$ удовлетворяет равенству $B(c) = 0$, то

$$c^r = b_0 + b_1 c + \ldots + b_{r-1} c^{r-1},$$

и тогда для любого $i \geqslant 0$ степень c^i представима [1]) линейной

[1]) При $i < r$ это очевидно, при $i = r + 1$ имеем $c^i = c \cdot c^r = c \sum_{i=0}^{r-1} b_i c^i = \sum_{i=0}^{r-2} b_i c^{i+1} + b_{r-1} \sum_{i=0}^{r-1} b_i c^i$ и т. д. — *Прим. перев.*

комбинацией степеней $1, c, \ldots, c^{r-1}$ с коэффициентами из $\mathbb{F}_q$:

$$c^i = \sum_{t=0}^{r-1} b_{ti} c^t.$$

Поэтому для элемента $c \in \mathbb{F}_q$, удовлетворяющего равенству $B(g(c)) = 0$, выполняется равенство

$$g(c)^i = \sum_{t=0}^{r-1} b_{ti} g(c)^t \quad \text{для } i \geqslant 0.$$

Подставляя в (6.25) вместо x такое значение c и учитывая, что $c^q = c$, получим

$$(E^{(n)}(h))(c) = f(c)^{M-n} \sum_{i=0}^{m-1} \sum_{j=0}^{u} e_{ijn}(c)\, g(c)^i c^j =$$

$$= f(c)^{M-n} \sum_{t=0}^{r-1} s_{tn}(c)\, g(c)^t,$$

где

$$s_{tn}(x) = \sum_{i=0}^{m-1} \sum_{j=0}^{u} b_{ti} e_{ijn}(x)\, x^j.$$

Чтобы получить равенство $(E^{(n)}(h))(c) = 0$, $n = 0, 1, \ldots, M-1$, для всех элементов $c \in \mathbb{F}_q$, удовлетворяющих равенству $B(g(c)) = 0$, надо приравнять нулю все многочлены s_{tn}, $0 \leqslant t \leqslant r-1$, $0 \leqslant n \leqslant M-1$. Из (6.24) следует, что

$$\deg(s_{tn}) \leqslant \frac{q}{m} + n(k-1) - 1 + u.$$

Поэтому если S обозначает суммарное число коэффициентов всех многочленов s_{tn}, $0 \leqslant t \leqslant r-1$, $0 \leqslant n \leqslant M-1$, то

$$S \leqslant r \sum_{n=0}^{M-1} \left(\frac{q}{m} + n(k-1) + u\right) =$$

$$= rM\left(\frac{q}{m} + u\right) + \frac{1}{2} r(k-1) M(M-1) \leqslant$$

$$\leqslant \frac{rq}{m} M + rM \frac{r}{m}(M + k + 1) + \frac{1}{2} r(k-1) M^2$$

ввиду (6.23). Учитывая, что $r < m$, получаем неравенство

$$S < \frac{rq}{m} M + \frac{1}{2} rM^2(k+1) + rM(k+1). \qquad (6.26)$$

Пусть A — суммарное число возможных коэффициентов всех многочленов e_{ij}, $0 \leqslant i \leqslant m-1$, $0 \leqslant j \leqslant u$. Тогда в силу (6.23)

$$A \geqslant \left(\frac{q}{m} - k\right) m(u+1) \geqslant (q - km)\frac{r}{m}(M+k+1) =$$

$$= \frac{rq}{m} M + \frac{rq}{m}(k+1) - rk(M+k+1).$$

Так как $M \geqslant k+1$, то

$$A \geqslant \frac{rq}{m} M + \frac{rq}{m}(k+1) - 2rkM. \tag{6.27}$$

Условие, состоящее в равенстве нулю всех многочленов s_{tn}, приводит к системе из S однородных линейных уравнений от A коэффициентов многочленов e_{ij}. Если $S < A$, то такая система обязательно имеет нетривиальное решение, а значит, найдутся многочлены e_{ij}, не равные нулю одновременно. Но в силу неравенств (6.26) и (6.27) неравенство $S < A$ будет обязательно выполняться, если выполняется неравенство

$$\frac{1}{2} rM^2(k+1) + rM(k+1) \leqslant \frac{rq}{m}(k+1) - 2rkM,$$

а для этого достаточно выполнения неравенства

$$\frac{1}{2} M^2(k+1) + 3(k+1)M \leqslant \frac{q}{m}(k+1),$$

которое эквивалентно неравенству

$$M^2 + 6M \leqslant \frac{2q}{m}.$$

Последнее же заведомо выполняется в силу предположения, что $(M+3)^2 \leqslant 2q/m$.

Выбрав, как указано, многочлены e_{ij}, мы построим многочлен h по формуле (6.22). Этот многочлен отличен от нулевого, поскольку в противном случае в силу леммы 6.46 мы получили бы, что все e_{ij} равны 0, а это исключено. По построению многочлена h и в силу леммы 6.51, каждый элемент $c \in \mathbb{F}_q$, такой, что $B(g(c)) = 0$, является корнем кратности не менее M многочлена h. Поскольку h имеет сомножитель f^M, то каждый элемент $c \in T$ является корнем кратности не менее M многочлена h. Кроме того, из (6.22) и (6.23) следует, что

$$\deg(h) \leqslant kM + \frac{q}{m} - k + (m-1)\frac{q-1}{m} k + qu <$$

$$< kM + \frac{q}{m} + qk + \frac{qr}{m}(M+k+1) <$$

$$< kq^{1/2} + \frac{r}{m} qM + q\left(\frac{1}{m} + 2k + 1\right) < \frac{r}{m} qM + 4kq.$$

□

Теперь мы установим предварительную оценку для числа решений уравнения $y^m = f(x)$, которая справедлива для достаточно больших значений q. Позднее этот результат будет улучшен в двух направлениях, а именно будут ослаблены условия и уточнена оценка (см. теорему 6.57).

6.53. Теорема. *Пусть $f \in \mathbb{F}_q[x]$ — такой многочлен степени $k \geqslant 1$ и $m \geqslant 2$ — такой делитель числа $q-1$, что многочлен $y^m - f(x)$ абсолютно неприводим. Тогда если выполняется неравенство $q \geqslant 100mk^2$, то число N решений уравнения $y^m = f(x)$ в $\mathbb{F}_q^2$ удовлетворяет неравенству*

$$|N - q| < 4km^{3/2}q^{1/2}.$$

Доказательство. Пусть h — многочлен, построенный в лемме 6.52. Так как $h \neq 0$, то из теоремы 1.66 следует, что (в обозначениях леммы 6.52) $M|T| \leqslant \deg(h)$, и оценка степени $\deg(h)$ в лемме 6.52 дает

$$|T| < \frac{r}{m}q + \frac{4k}{M}q.$$

Теперь возьмем $M = \lfloor (2q/m)^{1/2} \rfloor - 3$. Поскольку $q \geqslant 100mk^2$, то

$$M \geqslant \left(\frac{2q}{m}\right)^{1/2} - 4 \geqslant \left(\frac{q}{m}\right)^{1/2} \geqslant k+1,$$

так что число M удовлетворяет всем условиям леммы 6.52. Учитывая, что $M \geqslant (q/m)^{1/2}$, получим

$$|T| < \frac{r}{m}q + 4km^{1/2}q^{1/2}. \tag{6.28}$$

Сначала возьмем в лемме 6.52 $B(x) = x - 1$. Тогда $r = 1$, и в обозначениях леммы 6.45 $|T| = |T_0| + |T_1|$, так что из (6.28) следует неравенство

$$|T_0| + |T_1| < \frac{q}{m} + 4km^{1/2}q^{1/2}.$$

Таким образом,

$$N = |T_0| + m|T_1| \leqslant m(|T_0| + |T_1|) < q + 4km^{3/2}q^{1/2}. \tag{6.29}$$

Теперь возьмем $B(x) = x^{m-1} + x^{m-2} + \ldots + x + 1$. Тогда окажется, что $r = m - 1$ и $|T| = |T_0| + |T_2|$, так что из (6.28) получаем

$$|T_0| + |T_2| < \frac{m-1}{m}q + 4km^{1/2}q^{1/2}.$$

Вновь применяя лемму 6.45, приходим к соотношению

$$|T_1| = q - |T_0| - |T_2| > \frac{q}{m} - 4km^{1/2}q^{1/2},$$

так что

$$N \geqslant m|T_1| > q - 4km^{3/2}q^{1/2},$$

и, учитывая (6.29), мы получаем требуемый результат. □

Условие абсолютной неприводимости многочлена $y^m - f(x)$ можно задать в более удобном виде согласно следующему общему критерию.

6.54. Лемма. *Пусть K — произвольное поле, $f \in K[x]$ — многочлен положительной степени и $m \in \mathbb{N}$. Пусть*

$$f(x) = a(x - \alpha_1)^{e_1} \dots (x - \alpha_d)^{e_d}$$

— разложение многочлена f в его поле разложения над K, где $a \in K$ и $\alpha_1, \dots, \alpha_d$ — различные корни многочлена f. Для того чтобы многочлен $y^m - f(x)$ был абсолютно неприводимым, необходимо и достаточно, чтобы НОД $(m, e_1, \dots, e_d) = 1$.

Доказательство. Покажем, что многочлен $y^m - f(x)$ не будет абсолютно неприводимым в том и только том случае, когда НОД $(m, e_1, \dots, e_d) > 1$. Допустим, что этот многочлен приводим над некоторым алгебраическим расширением L поля K, причем можно предположить без ограничения общности, что в поле L многочлен $y^m - 1$ вполне разложим, т. е. $y^m - 1 = (y - \zeta_1) \dots (y - \zeta_m)$. Тогда

$$y^m - f(x) = F(x, y)\, G(x, y),$$

где $F, G \in L[x, y]$, $\deg(F) > 0$, $\deg(G) > 0$. Теперь рассмотрим $y^m - f(x)$ как многочлен от y над полем рациональных функций $L(x)$. Если Y — корень этого многочлена в его поле разложения над $L(x)$, то

$$y^m - f(x) = (y - \zeta_1 Y) \dots (y - \zeta_m Y).$$

В силу единственности разложения для некоторого ненулевого элемента α из L получим

$$F(x, y) = \alpha (y - \zeta_{j_1} Y) \dots (y - \zeta_{j_n} Y),$$

где $j_1, \dots, j_n \in \{1, \dots, m\}$, $1 \leqslant n < m$. Рассматривая обе части этого равенства как многочлены от y и сравнивая постоянные члены, получаем

$$(-1)^n \alpha \zeta_{j_1} \dots \zeta_{j_n} Y^n \in L[x],$$

а значит, $Y^n \in L[x]$. Пусть w — наименьшее натуральное число, для которого $Y^w \in L(x)$. Тогда $w \leqslant n < m$, и каждое $u \in \mathbb{N}$, такое, что $Y^u \in L(x)$, делится на w. В частности, число m делится на w, так как $Y^m = f \in L(x)$. Полагая $t = m/w > 1$ и $Y^w = g/h$ при $g, h \in L[x]$, $h \neq 0$, получаем, что $f = (g/h)^t$, откуда $fh^t = g^t$. Сравнивая кратности корней α_i, $1 \leqslant i \leqslant d$,

в обеих частях этого равенства, мы видим, что t делит каждое из чисел e_i. Поэтому t делит НОД $(m, e_1, \ldots, e_d)$, так что НОД $(m, e_1, \ldots, e_d) > 1$.

Пусть теперь, наоборот, $e = $ НОД $(m, e_1, \ldots, e_d) > 1$ и K_1 — поле разложения многочлена f над K. В подходящем конечном расширении поля K_1 существует элемент β, такой, что $\beta^e = a$. Положим $s = m/e$ и

$$f_1(x) = \beta (x - \alpha_1)^{e_1/e} \ldots (x - \alpha_d)^{e_d/e}.$$

Тогда

$$y^m - f(x) = (y^s)^e - (f_1(x))^e =$$

$$= (y^s - f_1(x))(y^{s(e-1)} + y^{s(e-2)} f_1(x) + \ldots + f_1(x)^{e-1}),$$

так что $y^m - f(x)$ не является абсолютно неприводимым многочленом. □

6.55. Лемма. *Пусть* $\omega_1, \ldots, \omega_n$ — *комплексные числа и* $B > 0$, $C > 0$ — *такие константы, что*

$$|\omega_1^s + \ldots + \omega_n^s| \leqslant CB^s \quad \text{для всех } s \in \mathbb{N}. \tag{6.30}$$

Тогда $|\omega_j| \leqslant B$ *для* $j = 1, \ldots, n$.

Доказательство. Пусть z — комплексная переменная. Для достаточно малых значений $|z|$

$$\log(1 - \omega_j z) = -\sum_{s=1}^{\infty} \frac{1}{s} \omega_j^s z^s, \quad j = 1, \ldots, n,$$

так что

$$\log((1 - \omega_1 z) \ldots (1 - \omega_n z)) = -\sum_{s=1}^{\infty} \frac{1}{s} (\omega_1^s + \ldots + \omega_n^s) z^s. \tag{6.31}$$

Ввиду (6.30) ряд в правой части (6.31) сходится для $|z| < B^{-1}$. Поэтому функция в левой части (6.31) аналитическая в круге $|z| < B^{-1}$. Таким образом, $1 - \omega_j z \neq 0$ при $|z| < B^{-1}$ и, следовательно, $|\omega_j| \leqslant B$ для $j = 1, \ldots, n$. □

Теперь мы можем доказать первый главный результат, который обосновывает одно утверждение, высказанное в § 4 гл. 5.

6.56. Теорема. *Комплексные числа* $\omega_1, \ldots, \omega_{d-1}$ *из теоремы* 5.39 *удовлетворяют неравенству* $|\omega_j| \leqslant q^{1/2}$ *для* $j = 1, \ldots, d - 1$.

Доказательство. Предполагая, что выполняются условия теоремы 5.39, и используя ее обозначения, положим $k = \deg(f)$

Выберем $r \in \mathbb{N}$ так, чтобы $q^r \geqslant 100mk^2$ и многочлен f вполне разлагался в поле $\mathbb{F}_{q^r}$:

$$f(x) = (x - \alpha_1)^{e_1} \ldots (x - \alpha_d)^{e_d},$$

где $\alpha_1, \ldots, \alpha_d$ — различные корни этого многочлена. Поскольку f не является m-й степенью какого-нибудь другого многочлена, то число $e = \text{НОД}(m, e_1, \ldots, e_d)$ является собственным делителем числа m. Пусть

$$g(x) = (x - \alpha_1)^{e_1/e} \ldots (x - \alpha_d)^{e_d/e} \in \mathbb{F}_{q^r}[x],$$

так что $f = g^e$. Зафиксируем число $s \in \mathbb{N}$ и положим $E = \mathbb{F}_{q^{rs}}$, $\lambda = \psi^{(rs)}$, $\tau = \lambda^e$. Тогда мультипликативный характер λ поля E имеет порядок m, а τ имеет порядок $n = m/e > 1$, так что

$$\sum_{\gamma \in E} \lambda(f(\gamma)) = \sum_{\gamma \in E} \lambda(g(\gamma)^e) = \sum_{\gamma \in E} \tau(g(\gamma)). \tag{6.32}$$

Пусть комплексное число ρ является первообразным корнем n-й степени из единицы, и пусть для $i = 0, 1, \ldots, n-1$ множество U_i состоит из всех $\alpha \in E$, таких, что $\tau(\alpha) = \rho^i$. Для фиксированного $\zeta \in U_1$ имеем $\alpha \in U_i$ тогда и только тогда, когда $\alpha\zeta^{-i} \in U_0$, что в свою очередь эквивалентно условию $\alpha\zeta^{-i} = \beta^n$ для некоторого $\beta \in E^*$. Пусть A_i — число элементов $\gamma \in E$, для которых $g(\gamma) \in U_i$, т. е. $\zeta^{-i} g(\gamma) = \beta^n$ для некоторого $\beta \in E^*$. Пусть B_i — число решений уравнения $y^n = \zeta^{-i} g(x)$ в E^2 с ненулевым значением координаты y. Тогда $A_i = B_i/n$. Пусть N_i — полное число решений уравнения $y^n = \zeta^{-i} g(x)$ в E^2. Так как

$$\text{НОД}(n, e_1/e, \ldots, e_d/e) = \text{НОД}(m/e, e_1/e, \ldots, e_d/e) = 1,$$

то в силу леммы 6.54 многочлен $y^n - \zeta^{-i} g(x)$ абсолютно неприводим. Кроме того, m делит число $q - 1$, так что n делит число $q^{rs} - 1$, и можно применить теорему 6.53, из которой получаем

$$|N_i - q^{rs}| < 4\frac{k}{e} n^{3/2} q^{rs/2} \quad \text{для } 0 \leqslant i \leqslant n-1.$$

Поскольку $|B_i - N_i| \leqslant k/e$,

$$|B_i - q^{rs}| \leqslant 5\frac{k}{e} n^{3/2} q^{rs/2} \quad \text{для } 0 \leqslant i \leqslant n-1,$$

Запишем

$$A_i = \frac{1}{n} q^{rs} + R_i;$$

тогда

$$|R_i| \leqslant 5\frac{k}{e} n^{1/2} q^{rs/2} \quad \text{для } 0 \leqslant i \leqslant n-1.$$

Из (6.32) получаем

$$\left|\sum_{\gamma\in E}\lambda(f(\gamma))\right| = \left|\sum_{\gamma\in E}\tau(g(\gamma))\right| = \left|\sum_{i=0}^{n-1}A_i\rho^i\right| = \left|\sum_{i=0}^{n-1}\left(\frac{1}{n}q^{rs}+R_i\right)\rho^i\right| =$$

$$= \left|\sum_{i=0}^{n-1}R_i\rho^i\right| \leqslant \sum_{i=0}^{n-1}|R_i| \leqslant 5\,\frac{k}{e}\,n^{3/2}q^{rs/2}.$$

Из теоремы 5.39 следует, что

$$\left|\omega_1^{rs}+\ldots+\omega_{d-1}^{rs}\right| \leqslant 5\,\frac{k}{e}\,n^{3/2}q^{rs\ 2}.$$

Поскольку это выполняется для любого $s\in\mathbb{N}$, то из леммы 6.55 получаем, что $|\omega_j^r| \leqslant q^{r/2}$, так что $|\omega_j| \leqslant q^{1/2}$ для всех j, $1 \leqslant j \leqslant d-1$. □

Оценка для сумм значений характеров в теореме 5.41 теперь полностью доказана. Эту оценку можно использовать для уточнения теоремы 6.53.

6.57. Теорема. *Пусть $m\in\mathbb{N}$ и $f\in\mathbb{F}_q[x]$ — такой многочлен положительной степени, что многочлен $y^t - f(x)$, где $t =$ НОД $(m, q-1)$, абсолютно неприводим. Тогда число N решений уравнения $y^m = f(x)$ в $\mathbb{F}_q^2$ удовлетворяет неравенству*

$$|N-q| \leqslant (t-1)(d-1)q^{1/2}.$$

где d — число различных корней многочлена f из его поля разложения над $\mathbb{F}_q$.

Доказательство. В силу (5.70)

$$N = \sum_{c\in\mathbb{F}_q} N(y^m = f(c)) = \sum_{c\in\mathbb{F}_q}\sum_{j=0}^{t-1}\lambda^j(f(c)) = q + \sum_{j=1}^{t-1}\sum_{c\in\mathbb{F}_q}\lambda^j(f(c)),$$

где λ — мультипликативный характер порядка t поля $\mathbb{F}_q$. Если $t=1$, то результат тривиален, так что можно считать, что $t>1$. Пусть

$$f(x) = af_1(x) = a(x-\alpha_1)^{e_1}\ \ldots\ (x-\alpha_d)^{e_d},$$

где $a\in\mathbb{F}_q$ и $\alpha_1, \ldots, \alpha_d$ — различные корни многочлена f. Поскольку многочлен $y^t - f(x)$ абсолютно неприводим, то по лемме 6.54 НОД $(t, e_1, \ldots, e_d) = 1$. Для $1 \leqslant j \leqslant t-1$ характер λ^j имеет порядок $r_j > 1$, где r_j делит t, так что f_1 не может быть r_j-й степенью некоторого многочлена. Поэтому в силу теоремы 5.41 получаем, что

$$|N-q| = \left|\sum_{j=1}^{t-1}\sum_{c\in\mathbb{F}_q}\lambda^j(af_1(c))\right| \leqslant (t-1)(d-1)q^{1/2}.$$ □

Для завершения доказательства теоремы 5.38 нам нужно теперь изучить уравнение вида $y^q - y = f(x)$ над конечными расширениями поля $\mathbb{F}_q$, которое связано с распределением следов значений многочлена f. Ключевым пунктом здесь снова является построение подходящего вспомогательного многочлена. Введем следующее обозначение. Если заданы многочлен f над некоторым конечным полем $\mathbb{F}_q$, элемент b этого поля и конечное расширение E поля $\mathbb{F}_q$, то через $T(b)$ обозначим множество таких элементов $\gamma \in E$, что $\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma)) = b$.

6.58. Лемма. *Пусть заданы многочлен $f \in \mathbb{F}_q[x]$ положительной степени, причем* НОД $(\deg(f), q) = 1$, *расширение $E = \mathbb{F}_{q^s}$ поля $\mathbb{F}_q$, где $s \geqslant 3$, и элемент $b \in \mathbb{F}_q$. Пусть M — такое натуральное число, кратное q, что $0 < M \deg(f) \leqslant q^{s-k-1}$, где $k = \lfloor s/2 \rfloor$. Тогда существует такой ненулевой многочлен $h \in \mathbb{F}_q[x]$, что каждый элемент $\gamma \in T(b)$ является корнем кратности не менее M этого многочлена, и при этом*

$$\deg(h) < Mq^{s-1} + q^s \deg(f).$$

Доказательство. Положим $g = f^{q^k} + f^{q^{k+1}} + \ldots + f^{q^{s-1}}$, $m = \deg(f)$, и пусть m_0 — меньшее из чисел m и q. Будем искать многочлен h в виде

$$h(x) = \sum_{i=0}^{q-1} \sum_{j=0}^{u} e_{ij}(x)\, g(x)^i\, x^{iq^s}, \tag{6.33}$$

где $u = M/q$ и e_{ij} — многочлены над $\mathbb{F}_q$, которые требуется определить, причем $\deg(e_{ij}) < m_0 q^{s-2}$. Поскольку

$$g(x) = f(x^{q^k}) + f(x^{q^{k+1}}) + \ldots + f(x^{q^{s-1}}),$$

мы можем написать, что $h(x) = v(x, x^{q^k})$, где

$$v(x, y) = \sum_{i=0}^{q-1} \sum_{j=0}^{u} e_{ij}(x) \left(f(y) + f(y^q) + \ldots + f(y^{q^{s-k+1}})\right)^i y^{iq^{s-k}}.$$

Ввиду того что $s \leqslant 2k + 1$, получаем, что $M \leqslant q^{s-k-1} \leqslant q^k$, так что можно применить следствие 6.50 для всех n, $0 \leqslant n \leqslant M - 1$. Тогда

$$E^{(n)}(h(x)) = \sum_{i=0}^{q-1} \sum_{j=0}^{u} e_{ijn}(x)\, g(x)^i\, x^{iq^s}, \quad 0 \leqslant n \leqslant M - 1,$$

где $e_{ijn}(x) = E^{(n)}(e_{ij}(x))$. Если $\gamma \in T(b)$, то $b = \mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma)) = G(\gamma) + g(\gamma)$, где $G = f + f^q + \ldots + f^{q^{k-1}}$. Учитывая также, что $\gamma^{q^s} = \gamma$, получим

$$(E^{(n)}(h))(\gamma) = \sum_{i=0}^{q-1} \sum_{j=0}^{u} e_{ijn}(\gamma)\, (b - G(\gamma))^i\, \gamma^j = r_n(\gamma),$$

где

$$r_n(x) = \sum_{i=0}^{q-1} \sum_{j=0}^{u} e_{ijn}(x)(b - G(x))^i x^j, \quad 0 \leqslant n \leqslant M - 1.$$

Для того чтобы гарантировать, что каждый элемент $\gamma \in T(b)$ является корнем многочлена h кратности не менее M, достаточно в силу леммы 6.51, чтобы были нулевыми все многочлены r_n, $0 \leqslant n \leqslant M - 1$. Поскольку $u = M/q \leqslant q^{k-1}$, то

$$\deg(r_n) < m_0 q^{s-2} + m(q-1)q^{k-1} + u \leqslant$$
$$\leqslant m_0 q^{s-2} + m(q-1)q^{k-1} + q^{k-1} \leqslant m_0 q^{s-2} + mq^k,$$

и, если $n \geqslant 1$, то $\deg(r_n) < m_0 q^{s-2} + mq^k - 1$. Таким образом, если через S обозначить суммарное число коэффициентов всех многочленов r_n, $0 \leqslant n \leqslant M - 1$, то

$$S < M(m_0 q^{s-2} + mq^k) \leqslant M m_0 q^{s-2} + q^{s-1}. \tag{6.34}$$

Суммарное же число A возможных коэффициентов всех многочленов e_{ij}, $0 \leqslant i \leqslant q - 1$, $0 \leqslant j \leqslant u$, удовлетворяет неравенству

$$A = q(u+1)m_0 q^{s-2} = M m_0 q^{s-2} + m_0 q^{s-1} \geqslant M m_0 q^{s-2} + q^{s-1}. \tag{6.35}$$

Условие, что все многочлены r_n равны 0, приводит к системе из S однородных линейных уравнений от A неизвестных коэффициентов многочленов e_{ij}. Учитывая (6.34) и (6.35), получаем неравенство $S < A$, означающее, что существует нетривиальное решение этой системы; это решение определяет многочлены e_{ij}, не все равные нулю.

Определив таким образом многочлены e_{ij}, мы определим многочлен h по формуле (6.33). Тогда, беря $u = M/q$ и $m_0 \leqslant m$, получим, что

$$\deg(h) < m_0 q^{s-2} + m(q-1)q^{s-1} + uq^s < Mq^{s-1} + mq^s.$$

Остается лишь проверить, что $h \neq 0$. Это вытекает из того, что ненулевые слагаемые

$$d_{ij}(x) = e_{ij}(x)\, g(x)^i\, x^{jq^s}$$

многочлена h имеют различные степени. Действительно,

$$\deg(d_{ij}) = \deg(e_{ij}) + imq^{s-1} + jq^s,$$

так что для $d_{ij} \neq 0$

$$q^{s-1}(im + jq) \leqslant \deg(d_{ij}) < q^{s-1} + q^{s-1}(im + jq),$$

поскольку $\deg(e_{ij}) < m_0 q^{s-2} \leqslant q^{s-1}$. Поэтому для того, чтобы доказать, что степени ненулевых многочленов d_{ij} различны, достаточно показать, что если $(i, j) \neq (i', j')$, где $0 \leqslant i, i' \leqslant q - 1$, $0 \leqslant j, j' \leqslant u$, то $im + iq \neq i'm + j'q$. Допустим, что

$im + jq = i'm + j'q$. Тогда $im \equiv i'm \pmod q$, и так как по предположению НОД $(m, q) = 1$, то $i \equiv i' \pmod q$, откуда следует, что $i = i'$ и $j = j'$, а это невозможно. □

На основе леммы 6.58 мы можем теперь найти предварительную оценку числа $N(b) = |T(b)|$, т. е. числа элементов $\gamma \in E$, удовлетворяющих условию $\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma)) = b$. Позднее этот результат будет улучшен (см. теорему 6.61). Но и той оценки, которую мы сейчас получим, будет вполне достаточно для доказательства нашего второго главного результата, приводимого ниже в теореме 6.60.

6.59. Теорема. *Пусть* $f \in \mathbb{F}_q[x]$ — *многочлен степени* $n \geqslant 1$, *причем* НОД $(n, q) = 1$. *Тогда для любого конечного расширения* $E = \mathbb{F}_{q^s}$ *поля* $\mathbb{F}_q$ *число* $N(b)$ *элементов* $\gamma \in E$, *для которых* $\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma)) = b$, *удовлетворяет неравенству*

$$|N(b) - q^{s-1}| < 2n^2 q^{(s/2)+4} \quad \text{для любых } b \in \mathbb{F}_q. \tag{6.36}$$

Доказательство. Если $q^s < n^2 q^4$, то тривиальная оценка $0 \leqslant N(b) \leqslant q^s$ показывает, что неравенство (6.36) выполняется. Таким образом, можно считать, что $q^s \geqslant n^2 q^4$. Если $k = \lfloor s/2 \rfloor$, как в лемме 6.58 (где $\lfloor t \rfloor$ — наибольшее целое, не превосходящее t), то

$$q^{s-k-2} \geqslant q^{(s-4)/2} \geqslant n,$$

так что чнсло

$$M = \left\lfloor \frac{1}{n} q^{s-k-2} \right\rfloor q$$

является положительным кратным числа q. Ясно, что $Mn \leqslant q^{s-k-1}$, так что все условия леммы 6.58 выполнены. Для многочлена $h \neq 0$, построенного в этой лемме, по теореме 1.66 выполняется неравенство $N(b)\, M \leqslant \deg(h)$, и оценка степенн $\deg(h)$, указанная в лемме 6.58, дает

$$N(b) < q^{s-1} + \frac{nq^s}{M}.$$

Так как

$$M \geqslant \frac{1}{2n} q^{s-k-1},$$

то

$$N(b) < q^{s-1} + 2n^2 q^{k+1} \quad \text{для всех } b \in \mathbb{F}_q.$$

Поэтому

$$N(b) = q^s - \sum_{\substack{c \in \mathbb{F}_q \\ c \neq b}} N(c) > q^s - (q-1)\, q^{s-1} - 2(q-1)\, n^2 q^{k+1} >$$

$$> q^{s-1} - 2n^2 q^{k+2},$$

так что в итоге

$$|N(b) - q^{s-1}| < 2n^2q^{k+2} \leqslant 2n^2q^{(s/2)+2},$$

откуда вытекает неравенство (6.36).

6.60. Теорема. *Комплексные числа* $\omega_1, \ldots, \omega_{n-1}$ *из теоремы* 5.36 *удовлетворяют неравенствам* $|\omega_j| \leqslant q^{1/2}$ *для* $j = 1, \ldots, n-1$.

Доказательство. Будем предполагать выполненными условия теоремы 5.36. Тогда в обозначениях этой теоремы при $E = \mathbb{F}_{q^s}$

$$\sum_{\gamma \in E} \chi^{(s)}(f(\gamma)) = \sum_{\gamma \in E} \chi\left(\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma))\right) = \sum_{b \in \mathbb{F}_q} N(b)\chi(b).$$

Если положить $N(b) = q^{s-1} + R(b)$, то ввиду (6.36) $|R(b)| < 2n^2q^{(s/2)+4}$, так что, применяя (5.9), имеем

$$\left|\sum_{\gamma \in E} \chi^{(s)}(f(\gamma))\right| = \left|\sum_{b \in \mathbb{F}_q} (q^{s-1} + R(b))\chi(b)\right| = \left|\sum_{b \in \mathbb{F}_q} R(b)\chi(b)\right| \leqslant$$
$$\leqslant \sum_{b \in \mathbb{F}_q} |R(b)| \leqslant 2n^2q^{(s/2)+5}.$$

Из теоремы 5.36 следует, что

$$|\omega_1^s + \ldots + \omega_{n-1}^s| \leqslant 2n^2q^5q^{s/2} \quad \text{для всех } s \in \mathbb{N},$$

поэтому, учитывая лемму 6.55, получаем $|\omega_j| \leqslant q^{1/2}$ для $j = 1, \ldots, n-1$. □

Оценка для суммы значений характеров из теоремы 5.38 полностью доказана. Эту оценку теперь можно использовать для уточнения теоремы 6.59.

6.61. Теорема. *Пусть* $f \in \mathbb{F}_q[x]$ — *многочлен степени* $n \geqslant 1$, *причем* НОД$(n, q) = 1$. *Тогда для* $b \in \mathbb{F}_q$ *число* $N(b)$ *элементов* $\gamma \in E = \mathbb{F}_{q^s}$, *для которых* $\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma)) = b$, *удовлетворяет неравенству*

$$|N(b) - q^{s-1}| \leqslant \left(1 - \frac{1}{q}\right)(n-1)q^{s/2}.$$

Доказательство. На основании (5.10)

$$N(b) = \frac{1}{q} \sum_{\gamma \in E} \sum_{\chi} \chi\left(\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma))\right) \bar{\chi}(b),$$

где внутренняя сумма берется по всем аддитивным характерам χ поля $\mathbb{F}_q$. Меняя порядок суммирования и выделяя часть, соответствующую тривиальному характеру χ_0, получим

$$N(b) = q^{s-1} + \frac{1}{q} \sum_{\chi \neq \chi_0} \bar{\chi}(b) \sum_{\gamma \in E} \chi^{(s)}(f(\gamma)),$$

откуда, согласно теореме 5.38,

$$|N(b)-q^{s-1}|\leqslant\frac{1}{q}\sum_{\chi\neq\chi_0}\left|\sum_{\gamma\in E}\chi^{(s)}(f(\gamma))\right|\leqslant\left(1-\frac{1}{q}\right)(n-1)\,q^{s/2},$$

так как ввиду $\chi\neq\chi_0$ поднятие $\chi^{(s)}$ характера χ нетривиально. □

6.62. Следствие. *Пусть* $f\in\mathbb{F}_q[x]$ *— многочлен степени* $n\geqslant 1$, *причем* НОД $(n, q)=1$, *и пусть* $E=\mathbb{F}_{q^s}$, *где* $s\in\mathbb{N}$. *Тогда число* N *решений уравнения* $y^q-y=f(x)$ *в* E^2 *удовлетворяет неравенству*

$$|N-q^s|\leqslant(q-1)(n-1)\,q^{s/2}.$$

Доказательство. Согласно теореме 2.25, для фиксированного элемента $\gamma\in E$ равенство $\beta^q-\beta=f(\gamma)$ выполняется при некотором $\beta\in E$ в том и только том случае, когда $\mathrm{Tr}_{E/\mathbb{F}_q}(f(\gamma))=0$. Кроме того, если для элемента $\gamma\in E$ найдется такое $\beta_0\in E$, что выполняется равенство $\beta_0^q-\beta_0=f(\gamma)$, то существует в общей сложности q элементов $\beta\in E$, удовлетворяющих условию $\beta^q-\beta=f(\gamma)$, причем все они имеют вид $\beta=\beta_0+c$, где $c\in\mathbb{F}_q$. Таким образом, $N=qN(0)$. Остальное вытекает из теоремы 6.61. □

6.63. Пример. В качестве дальнейшего приложения метода, рассмотренного в этом параграфе, мы приведем доказательство теоремы 5.44 для нечетного q. Будем использовать обозначения из теоремы 5.43, и пусть $E=\mathbb{F}_{q^s}$. Тогда

$$K(\chi^{(s)};\,a,\,b)=\sum_{\gamma\in E^*}\chi\left(\mathrm{Tr}_{E/\mathbb{F}_q}(a\gamma+b\gamma^{-1})\right)=\sum_{c\in\mathbb{F}_q}M(c)\,\chi(c),\quad(6.37)$$

где $M(c)$ — число элементов $\gamma\in E^*$, таких, что $\mathrm{Tr}_{E/\mathbb{F}_q}(a\gamma+b\gamma^{-1})=c$. Если β_0 — фиксированный элемент поля E, удовлетворяющий равенству $\mathrm{Tr}_{E/\mathbb{F}_q}(\beta_0)=c$, то, согласно теореме 2.25, равенство $\mathrm{Tr}_{E/\mathbb{F}_q}(a\gamma+b\gamma^{-1})=c$ выполняется в том и только том случае, когда $a\gamma+b\gamma^{-1}=\beta^q-\beta+\beta_0$ для некоторого $\beta\in E$, а это эквивалентно условию $a\gamma^2-(\beta^q-\beta+\beta_0)\gamma+b=0$. Пусть N — число решений уравнения $ay^2-(x^q-x+\beta_0)y+b=0$ в E^2. Тогда из доказательства следствия 6.62 можно получить, что $N=qM(c)$. При нечетном q очевидные выкладки показывают, что N является также числом решений [1]) уравнения $y^2=(x^q-x+\beta_0)^2-4ab=f(x)$ в E^2. Так как $f'(x)=-2(x^q-x+\beta_0)$, то многочлен f имеет лишь

[1]) Так как уравнения $y^2=f(x_0)$ и $ay^2-(x_0^q-x_0+\beta_0)y+b=0$ для $x_0\in E$ имеют в поле E по одному решению, если $f(x_0)=0$, по два, если $f(x_0)$ — квадрат некоторого элемента из E^*, и ни одного, если $f(x_0)$ не является квадратом в поле E. — *Прим. перев.*

простые корни (в силу теоремы 1.68, поскольку $ab \neq 0$). Отсюда следует, что многочлен $y^2 - f(x)$ абсолютно неприводим согласно лемме 6.54. Поэтому из теоремы 6.57 получаем

$$|N - q^s| \leqslant (2q - 1)\, q^{s/2}.$$

Таким образом, если записать $M(c) = q^{s-1} + R(c)$ и вспомнить, что $M(c) = N/q$, то получим, что $|R(c)| \leqslant 2q^{s/2}$. Вместе с (6.37) и (5.9) это дает

$$|K(\chi^{(s)}; a, b)| = \left|\sum_{c \in \mathbb{F}_q} (q^{s-1} + R(c))\,\chi(c)\right| = \left|\sum_{c \in \mathbb{F}_q} R(c)\,\chi(c)\right| \leqslant$$
$$\leqslant \sum_{c \in \mathbb{F}_q} |R(c)| \leqslant 2q \cdot q^{s/2},$$

так что по теореме 5.43

$$|\omega_1^s + \omega_2^s| \leqslant 2q \cdot q^{s/2}.$$

Поскольку это неравенство выполняется для всех $s = 1, 2, \ldots$, из леммы 6.55 получаем, что $|\omega_j| \leqslant q^{1/2}$ для $j = 1, 2$. Более того, в доказательстве теоремы 5.43 мы установили равенство

$$L(z) = 1 + Kz + qz^2 = (1 - \omega_1 z)(1 - \omega_2 z),$$

из которого, в частности, вытекает, что $\omega_1 \omega_2 = q$. Таким образом, $|\omega_1| = |\omega_2| = q^{1/2}$. □

Комментарии

§ 1. Первый важный результат о числе решений уравнений над конечными полями принадлежит Лагранжу (Lagrange [2]); он состоит в том, что многочлен от одной переменной степени $n \geqslant 0$ над простым полем $\mathbb{F}_p$ имеет не более n корней. Это предложение справедливо, разумеется, для любого поля (см. теорему 1.66). Условия, при которых все n корней принадлежат основному полю $\mathbb{F}_q$, получены Фейтом и Рисом (Feit, Rees [1]); см. также Schönemann [2], Thouvenot, Châtelet [1] и Шатуновский [1] для случая, когда q — простое число, а также комментарии к § 3 гл. 4. В статьях Mignosi [5], [6] изучаются такие элементы $b \in \mathbb{F}_q$, для которых многочлен $f(x) + b \in \mathbb{F}_q[x]$ имеет $\deg(f)$ различных ненулевых корней в $\mathbb{F}_q$.

Теорема 6.1 доказана Кёнигом, а первое опубликованное изложение появилось в статье Raussnitz [1]. Вскоре ее доказательства были получены Гегенбауэром (Gegenbauer [1]), Кронекером (Kronecker [7]) и Радошом (Rados [1]). Доказательства этой теоремы можно также найти в работах Gegenbauer [6], [7] и Rédei [10, ch. 8], а также Tazawa [1] для частного случая. Близкий результат, использующий вместо ранга циркулянтной матрицы сумму всех ее главных миноров фиксированного порядка,

установлен в статье Rédei, Turàn [1]. Как обобщение теоремы Кёнига—Радоша можно рассматривать формулы, полученные в работах Horàkovà, Schwarz [1] и Schwarz [14], которые выражают число нормированных неприводимых делителей данной степени некоторого многочлена через ранги соответствующих матриц. В работах Raussnitz [1], Segre [3], [4] и Vaughan T. P. [1] показано, что через ранг циркулянтной матрицы можно выразить также число таких решений уравнения $f(x) = 0$, $f \in \mathbb{F}_q[x]$, которые являются m-ми степенями элементов из $\mathbb{F}_q^*$. Гегенбауэр (Gegenbauer [4]) получил аналогичное выражение для числа общих ненулевых корней двух многочленов. Вопрос же о существовании общих корней двух многочленов можно решить с помощью теории результантов (см. § 4 гл. 1); в связи с этим см. также Rados [3] и Vogt, Bose [1]. Гегенбауэр (Gegenbauer [2]) использовал результанты в формулах для числа общих ненулевых корней двух многочленов, а также для числа различных ненулевых корней одного многочлена над простым полем $\mathbb{F}_p$; см. также Ore [1]. Другие типы формул для числа решений полиномиального уравнения $f(x) = 0$ в конечном простом поле см. в статьях Bellman [1] и Cazacu [1]. Оре (Ore [7]) указал оценку для числа решений в поле $\mathbb{F}_p$ уравнения $a_0 + a_1x + \ldots + a_{p-2}x^{p-2} = 0$, коэффициенты которого удовлетворяют некоторому линейному рекуррентному соотношению.

Для $f \in \mathbb{F}_q[x]$ число N решений уравнения $f(x) = 0$ в поле $\mathbb{F}_q$ можно определить по модулю характеристики p поля $\mathbb{F}_q$ с помощью следующего простого закона, найденного Лебегом (Lebesgue [1]):

$$N \equiv \sum_{c \in \mathbb{F}_q} [1 - f(c)^{q-1}] \pmod{p}.$$

Этот прием был затем развит в работах Cipolla [3], Dickson [19] и Hurwitz [1]. Другой подход был применен Шварцом (Schwarz [3]), который показал, что если f — нормированный многочлен без кратных сомножителей, то $N \equiv \mathrm{Tr}(B) \pmod{p}$, где $\mathrm{Tr}(B)$ обозначает след матрицы $B = (b_{ij})$, определенной выражением (4.4). Этот метод обобщен в статье Шварца Schwarz [13]; см. также комментарии к § 1 гл. 4. Сравнение по модулю p для числа N получено также в статье Mignosi [7]. Сравнения по модулю p для числа общих корней конечного множества многочленов, которые не являются корнями никакого многочлена из другого конечного множества многочленов, можно найти в статье Mignosi [3].

Много результатов о числе решений уравнения $f(x) = 0$ получено для различных специальных классов многочленов f. Так, о кубических многочленах f и многочленах f четвертой степени см. работы Bose, Chowla, Rao [3], Carlitz [103], Cazacu,

Simovici [1], Cordone [1], Dickson [40, ch. 8], Leonard [3], [4], Mirimanoff [1], Oltramare [1], Rédei [5], [6], [10, ch. 11], Schwarz [3], Segre [10], Skolem [1], [2], [4], Thouvenot [1], Thouvenot, Châtelet [1], Вороной [1, гл. 1], [2] и Гребенюк [2]. Особенно простым является случай, когда f — двучлен; для произвольного конечного поля $\mathbb{F}_q$ он был рассмотрен Дедекиндом (Dedekind [1]), но для простых конечных полей он привлек внимание исследователей значительно раньше (см. обширную библиографию в книге Dickson [40, ch. 7]). Относительно трехчленов см. Leonard [2], Liang [1], Segre [10] и Vilanova [1]. О линеаризованных и аффинных многочленах f см. Berlekamp [4, ch. 11], Liang [1], Segre [10] и Vilanova [1]. Карлиц (Carlitz [118]) доказал, что для $q > k_1 > k_2 > \ldots > k_s \geqslant 1$ существуют элементы $a_1, \ldots, a_s \in \mathbb{F}_q$, такие, что многочлен $a_1x^{k_1} + \ldots + a_sx^{k_s} + 1$ имеет по крайней мере s различных корней в поле $\mathbb{F}_q$. Леонард (Leonard [1]) получил с помощью доказательства из работы Birch, Swinnerton-Dyer [1] асимптотическую формулу для числа элементов $b \in \mathbb{F}_q$, таких, что многочлен $f(x) + b$ имеет заранее заданное число корней в поле $\mathbb{F}_q$, в предположении, что f является многочленом определенного вида. В статье Whiteman [4] устанавливается зависимость между квадратичным разбиением простого числа p и числом решений квадратного и кубического уравнений над полем $\mathbb{F}_p$. Методы отыскания корней многочленов рассматриваются в § 3 гл. 4.

Следствия 6.6 и 6.9 принадлежат Шевалле (Chevalley [1]), тогда как усиления, содержащиеся в теоремах 6.5, 6.8 и 6.11, были вслед за тем установлены Варнингом (Warning [1]). Результат следствия 6.6 был сформулирован Диксоном в статье Dickson [28] и доказан там для однородных многочленов не выше третьей степени, а в статье Dickson [32] — для любых однородных многочленов над полем $\mathbb{F}_2$. Доказательство теорем Шевалле—Варнинга можно найти также в следующих источниках: Ax [1], Greenberg [1, ch. 2], Ireland, Rosen [1, ch. 10], Joly [5], Schmidt W. M. [3, ch. 4], Serre [1, ch. 1] и Боревич, Шафаревич [1, гл.1]. Другое доказательство леммы 6.3 см. в работах Dickson [2], [7, part I, ch. 4]; об аналогичной кратной сумме см. Williams W. L. G. [5], а об аналоге суммы степеней для квадратных матриц см. Brawley, Carlitz, Levine [1]. Теорему Шевалле можно использовать для доказательства теоремы Веддербёрна (теорема 2.55); см. Joly [5] и McCrimmon [1]. По поводу других ее приложений см. статьи Ax [2], Ax, Kochen [1], Carlitz [32] и Львов [1]. Результаты типа теорем Шевалле—Варнинга для систем уравнений имеются также в статье Segre [7]. В статье Carlitz [65] показано, что если $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — однородный многочлен степени n и число N решений уравнения $f(x_1, \ldots$

..., $x_n) = 0$ не делится на характеристику p поля $\mathbb{F}_q$, то для каждого многочлена $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ степени, меньшей n, уравнение $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ имеет по крайней мере одно решение в $\mathbb{F}_q^n$. Если же N делится на p и при этом $g(0, 0, \ldots, 0) = 0$, то число решений уравнения $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ в $\mathbb{F}_q^n$ делится на p, и этот результат можно распространить на системы аналогичных уравнений (см. Carlitz [87]). О близких к этому результатах для случая $\deg(f) = n$ см. также Terjanian [1] и Joly [5]. В статье Frattini [2] найдено условие, при котором однородному уравнению удовлетворяют значения переменных, отличные друг от друга и от нуля. Результаты Брауэра (Brauer R. [1]) о системах однородных уравнений над произвольными полями можно рассматривать как обобщение следствия 6.9. Другое обобщение следствия 6.9 для однородных многочленов получено в статье Fulton W. [1] о многообразиях над конечными полями. Теоремы Шевалле—Варнинга для кольца $Z/(p^k)$ установлены в работах Browkin [1] и Schanuel [1].

Важным усилением теоремы 6.5 является теорема Акса (Ax [1]), состоящая в том, что если $f \in \mathbb{F}_q[x_1, \ldots x_n]$ — многочлен степени $\deg(f) = d < n$ и b — наибольшее целое число, которое меньше n/d, то число решений уравнения $f(x_1, \ldots, x_n) = 0$ делится на q^b; доказательство этого результата имеется также в статье Joly [5]. Обобщение указанного результата на случай системы уравнений получено Катцом (Katz [1]). Близкий результат содержится в статье Delsarte, McEliece [1]. О приложениях теоремы Акса см. Carlitz [110].

Однородные многочлены f, построенные в примере 6.7, называются *норменными формами;* они были введены Диксоном (Dickson [16], [28]). Карлиц (Carlitz [78]) исправил доказательство Диксона (Dickson [16]) и показал, что если для нечетного $q \geqslant 13$ однородный многочлен $f \in \mathbb{F}_q[x_1, x_2, x_3]$ третьей степени обращается в нуль на $\mathbb{F}_q^3$ лишь в точке (0, 0, 0), то он должен быть норменной формой. Системы уравнений, состоящие из норменных форм, были изучены Карлицом (Carlitz [87]). Норменные формы представляют собой частный случай так называемых факторизуемых многочленов (см. Carlitz [12] и комментарии к § 2 гл. 3). В статье Terjanian [1] доказано, что если $f \in \mathbb{F}_q[x_1, \ldots$ $\ldots, x_n]$ — многочлен степени n, обращающийся в нуль на q^n лишь в точке (0, ..., 0), то для каждого многочлена $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ степени, меньшей n, существует хотя бы одно решение уравнения $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$, лежащее в $\mathbb{F}_q^n$; см. также Joly [5].

Теорема 6.13 доказана Ope (Ore [1]); см. также Schmidt W. M. [3, ch. 4] и Боревич, Шафаревич [1, гл. 1]. В работе Schmidt W. M. [3] имеются также теоремы 6.15, 6.16 и 6.17. Тот факт, что для ненулевого многочлена $f \in \mathbb{F}_q[x_1, \ldots, x_n]$

число решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ не превышает q^{n-1}, был отмечен в статьях Min [2] и Lang, Weil [1], а для конечных простых полей также в работе Hua [9, ch. 2]. Обобщения теоремы 6.13 на случай системы уравнений можно найти в работах Chalk, Williams [1] и Schmidt W. M. [3, ch. 4].

Теоремы типа теоремы Кёнига—Радоша для полиномиальных уравнений от нескольких переменных и для систем таких уравнений были установлены в работах Gegenbauer [5], Rados [2] и Segre [4], [5], [7]. Сравнения по модулю характеристики поля $\mathbb{F}_q$ для числа решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ можно получить очевидным обобщением закона Лебега, упоминавшегося выше; см. Lebesgue [1], Hurwitz [1], Dickson [19] и Segre [3], [4]. Элементарный подход к числу решений указанного уравнения был использован в статье Cazacu [2]. Вандивер (Vandiver [3]) получил выражение для числа решений уравнения $f(x_1, \ldots, x_n) = 0$ через значения переменных x_i, являющиеся m_i-ми степенями в группе $\mathbb{F}_q^*$ для $1 \leqslant i \leqslant n$. Редеи (Rédei [3]) показал, что уравнение $f(x_1, \ldots, x_n) = 0$ в том и только том случае не имеет решений в $\mathbb{F}_q^n$, если многочлен $f^{q-1} - 1$ является линейной комбинацией многочленов от одной переменной вида $x_i^q - x_i$, $1 \leqslant i \leqslant n$, с коэффициентами из кольца $\mathbb{F}_q[x_1, \ldots, x_n]$. Робинсон (Robinson A. [1, ch. 2]) доказал, что если система полиномиальных уравнений от нескольких переменных над кольцом $\mathbb{Z}$ такова, что она имеет не более m решений в каждом расширении поля $\mathbb{Q}$, то для всех достаточно больших простых чисел p система уравнений, получаемая из исходной приведением коэффициентов по модулю p, имеет не более m решений в каждом расширении поля $\mathbb{F}_p$; см. также Gilmer, Mott [1].

Множество элементарных результатов доказано для частных типов уравнений от нескольких переменных. Об уравнениях, содержащих однородные многочлены с непересекающимися множествами переменных см. Carlitz [62] и Segre [10], а о частном случае факторизуемых многочленов см. Carlitz [58] и Williams K. S. [14]. Карлиц (Carlitz [39]) показал, что число решений уравнения $x_1^{m_1} \ldots x_n^{m_n} = f(y_1, \ldots, y_r)$, где $m_1, \ldots, m_n \in \mathbb{N}$ — взаимно простые числа, можно выразить через число решений уравнения $f = b$, $b \in \mathbb{F}_q$; обобщения этого результата см. в статьях Porter [9] и van Meter [2], [3]. Уравнения и системы уравнений, содержащие элементарные симметрические многочлены, рассматривались в работах Aberth [1], Carlitz [64], Fine [1], Mordell [7], Rêdei [11, ch. 6], Schwarz [15], Sedlàcek [1] и Аванесов [1]. Уравнение $f(x)(y - z) + f(y)(z - x) + f(z)(x - y) = 0$ с многочленом $f \in \mathbb{F}_q[x]$ изучалось в статье Ceccherini, Hirschfeld [1]. Определенное внимание привлекли

так называемые *мультилинейные уравнения*. *k-линейным уравнением* называется уравнение вида

$$a_1 x_{11} \ldots x_{1k} + a_2 x_{21} \ldots x_{2k} + \ldots + a_n x_{n1} \ldots x_{nk} = a$$

от kn переменных x_{ij}, где $a_1, \ldots, a_n, a \in \mathbb{F}_q$. О таких уравнениях и системах уравнений см. Carlitz [56], Cohen E. [8], Hodges [2], Joly [5], Porter [4], [5], [6] и van Meter [2]. Обобщения на случай, когда допускаются более высокие степени переменных x_{ij}, можно найти в статьях Carlitz [39], Porter [7], [9], [11] и van Meter [1], [2], [3]. О дальнейших элементарных результатах по частным типам систем уравнений см. работы Corson [1], Klein [1], [2], Mignosi [4], Serge, Bartocci [1] и Бабаев, Исмоилов [1]. Число решений уравнения $\det (x_{ij})_{1 \leqslant i,\ j \leqslant n} = a$ было получено в работах Jordan C. [7] и Fine, Niven [1]; см. также Carlitz [58], [67] об аналогичных уравнениях.

В статьях Ax [2], [3] и Fried, Sacerdote [1] рассматриваются алгоритмы, позволяющие выяснить, будет ли данная система уравнений от нескольких переменных разрешима не в одном конечном поле, а в целом семействе конечных полей. О матричных уравнениях над конечными полями см. комментарии к § 2, а об уравнениях, для которых неизвестными являются многочлены над конечными полями, см. комментарии к гл. 3. Некоторые функциональные уравнения над конечными полями изучаются в работах Dickey, Kairies, Shank [1], Dunn, Lidl [1], Herget [1] и Lüneburg, Plaumann [1].

§ 2. Уравнения над конечными полями, содержащие квадратичные формы, рассматривались еще Лагранжем (Lagrange [3]), который показал, что уравнение $x^2 + by^2 = c$, где $b, c \in \mathbb{F}_p^*$ при простом числе p, всегда разрешимо в $\mathbb{F}_p^2$. Это было необходимым шагом при доказательстве его известной теоремы о том, что каждое натуральное число может быть представлено в виде суммы четырех квадратов целых чисел. Простое доказательство разрешимости этого уравнения в замечании 6.25 принадлежит Коши (Cauchy [1]), который нашел его, исходя из общего комбинаторного принципа, переоткрытого впоследствии Дэвенпортом (Davenport [5]). То же самое доказательство применил Диксон (Dikson [43]). Вебер (Weber [5, § 64]) показал, что каждый элемент конечного поля можно представить в виде суммы двух квадратов. Формулы для числа решений уравнения $x^2 + by^2 = c$ в $\mathbb{F}_p^2$ приводятся в работах Hermite [1], Libri [1], Lebesgue [1] и Schönemann [1]. Более свежие результаты об этом уравнении см. в статьях Singh [2], [3] и Somer [1]. Решения уравнения $ax^2 + by^2 = c$ в $\mathbb{F}_p^2$ с малыми значениями x и y были исследованы в статьях Mordell [9], Smith R. A. [1] и Williams K. S. [12].

Вопрос о том, какие решения уравнения $x^2 + y^2 = z^2$ являются квадратичными вычетами, был изучен в статье Burde [8].

Лебег (Lebesgue [1]) установил формулу для числа решений уравнения $x_1^2 + \ldots + x_n^2 = b$ в $\mathbb{F}_p^n$, а для произвольных диагональных квадратичных форм над $\mathbb{F}_p$ это было впервые сделано Жорданом (Jordan C. [1]); см. также Jordan C. [2, § 197—200] и Lebesgue [5]. Теорема 6.21 для простого поля $\mathbb{F}_p$, $p > 2$, была доказана Жорданом (Jordan C. [5], [6]); он же нашел число решений уравнения $f = 0$, где f — произвольная квадратичная форма над таким полем. Обобщение указанной теоремы на случай произвольного конечного поля нечетной характеристики было осуществлено Диксоном в статье Dickson [4]; в этой статье можно также найти теорему 6.30. О тех же результатах с иными доказательствами см. также работы Bachmann [3, part II, ch. 7], Berlekamp [4, ch. 16], Cohen E. [13], Dickson [7, part. I, ch. 4; part II, ch. 7, 8], Hull [1], Ireland, Rosen [1, ch. 8], Joly [5], Nagata [1] и Schmidt W. M. [3, ch. 4]. Метод, указанный в замечании 6.28 для произвольных многочленов степени 2 над полем $\mathbb{F}_q$, не пригоден для четного числа q, но число решений можно найти и для этого случая (см. Carlitz [109]). Кантор (Kantor [1]) определил число различных значений, представимых квадратичными формами над простым полем $\mathbb{F}_p$, $p > 2$.

Системы уравнений $f_i(x_1, \ldots, x_n) = b_i \in \mathbb{F}_q$, $i = 1, \ldots, k$, с квадратичными формами $f_1, \ldots, f_k$ над $\mathbb{F}_q$ изучались в статьях Birch, Lewis [2], Birch, Lewis, Murphy [1], Carlitz [56], Lewis, Schuur [1], Mordell [8], Nordon [1], [2], [3], Weil [8] и Демьянов [2]. О системах, содержащих как квадратичные, так и линейные уравнения, см. Carlitz [101], [102], Cohen E. [10], [11], [12], Fulton J. D. [9], Jung [1], [2], O'Connor [1], O'Connor, Pall [1] и Tietäväinen [3]. В статьях Carlitz [101] и Tietäväinen [3] доказано предположение Коэна (Cohen E. [11]) о том, что система уравнений над полем $\mathbb{F}_q$ нечетной характеристики, состоящая из уравнения $f(x_1, \ldots, x_n) = b$, где f — некоторая невырожденная квадратичная форма, и системы из t линейных уравнений от переменных x_i полного ранга, всегда разрешима в $\mathbb{F}_q^n$, если $n \geqslant 2t + 2$, но при $n = 2t + 1$ существуют такие системы, которые не имеют решений в $\mathbb{F}_q^n$. Карлиц получил также аналогичный результат для поля характеристики 2 (Carlitz [101]). Системы уравнений, содержащие квадратичные и билинейные формы, рассматривались в статьях Carlitz [56] и Porter [1], [2], [3], [6], [15].

Карлиц (Carlitz [39], [43], [52], [63]) изучал уравнения вида $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$, где f — квадратный многочлен, а g — многочлен некоторого специального вида. Случай, когда $n = 3$ или 4 и $g(x_1, \ldots, x_n) = ax_1 \ldots x_n + b$, $a, b \in \mathbb{F}_q$,

рассматривался в статьях Carlitz [50], [52], [75] и Rosati [1]. В работе Carlitz [43] рассматривалось уравнение $f_1f_2 + \cdots + f_{2n-1}f_{2n} = b$, где f_i — квадратичные формы, не содержащие общих переменных. Другой частный тип уравнений, содержащих квадратичные формы, рассмотрен Карлицом (см. Carlitz [47]). О кубичных формах и формах четвертой степени см. работы Campbell [1], [3], [8], [10], Carlitz [64], Cicchese [1], [2], [3], [4], Davenport, Lewis [1], [4], [6], de Groote [1], [2], Lewis [1], Lewis, Schuur [1], Mordell [5], [21], Segre [10] и Манин [4, гл. 4], а также комментарии к § 3 и 4.

Содержащие квадратичные формы суммы значений характеров из упр. 6.27—6.30 можно рассматривать как обобщения квадратичных сумм Гаусса (ср. с. § 2 гл. 5). Впервые они были вычислены для конечных простых полей, а также для кольца $Z/(m)$ Жорданом (Jordan C. [4]) и Вебером (Weber [1]). О дальнейших результатах см. работы Bachmann [3, part II, ch. 7], Braun [1], Callahan, Smith [1], Carlitz [59], [109], Fulton J. D. [9], Smith R. A. [4]. Линник [2] и Малышев [2], [3, гл. 1]. О близких суммах значений характеров см. работы Carlitz [45], [46], [109], [113], Ono [4], Porter [16], [17], Springer [3] и ссылки на литературу в статье Berndt, Evans [4] по обобщениям сумм Гаусса.

Обширная теория приведения и теория инвариантов для квадратичных форм над конечными полями были развиты Диксоном в статьях Dickson [11], [12], [13], [18], [22], [24]. Аналогичные результаты для систем квадратичных форм были установлены Диксоном в статьях. Dickson [20], [22], [27]. Эти теории были распространены на формы высшей степени в работах Dickson [15], [24], [29], [30], [34], [36], [37], [38], [39]. Итог этим исследованиям был подведен в книгах Dickson [35] и [42, ch. 19]. О продолжении этих работ см., например, статьи Glenn [1], Hazlett [1], [2], [3], [4], Wiley [1], Williams W. L. G. [1], [2], [3], [4] и обзор в книге Rutherford [1]. Более поздние исследования инвариантов форм над конечными полями содержатся в работах Almkvist [1], Campbell [9], [11] и Carlitz [47], [53], [59]. Нужно отметить, что понятие инварианта для таких форм встречается еще у Гурвица (Hurwitz [1]). Основная теорема 6.21 справедлива, разумеется, для любого поля характеристики, отличной от 2, так как ее доказательство не использует конечности основного поля; см. также Боревич, Шафаревич [1, алгебраическое дополнение]. Теория квадратичных форм над произвольными полями характеристики 2 более сложна. Основными работами по этому вопросу являются статьи Albert [1] и Arf [1], причем в последней введен один важный инвариант. Об упрощенном подходе к инварианту Арфа см. Dieudonné [1], Dye [1], Klingenberg, Witt [1], Springer [1], Tietze [1] и Witt [2].

Жмудь [1] нашел соотношение, связывающее инвариант Арфа с обобщенными суммами Гаусса. В статье Meyer [1] представлен обзор результатов Диксона и Арфа с позиций их приложений к конечным полям. О квадратичных формах над конечными полями характеристики 2 см. также Campbell [2], [4], [5], [6], [7], а о кубических формах над полем $\mathbb{F}_2$ см. T'u [2]. В статье Pless [2] рассмотрены билинейные формы над полями характеристики 2. О квадратичных формах над кольцом $\mathbb{F}_q[x]$ см. работы Byers [1] и Carlitz [69].

Приложения квадратичных и билинейных форм над конечными полями к теории кодирования рассматриваются в статьях Cameron, Seidel [1], Delsarte P. [3], Delsarte, Goethals [2], Goethals [1], Lempel, Winograd [1] и Snapper [1]. О приложениях к конечным геометриям см., например, работы Artin [7, ch. 3], Cordes [1], [2], Dai, Feng [1], [2], Feng, Dai [1], [2], Snapper [1] и Козел, Шаклеина [1]. О приложениях к алгебрам над конечными полями см., например, Ono [5], [6]. Каплан (Kaplan [1]) доказал закон взаимности (см. теорему 5.17), рассматривая число решений сравнения $x_1^2 + \ldots + x_r^2 \equiv r \pmod{p}$.

Теорему 6.21 можно интерпретировать и следующим образом: каждая симметрическая матрица A над полем $\mathbb{F}_q$ при нечетном q подобна некоторой диагональной матрице D (в том смысле, что $D = C^{\mathrm{T}}AC$ для некоторой невырожденной матрицы C над $\mathbb{F}_q$); ср. с работами Newman [1, ch. 4) и Mateos Mateos [1]. Близкие результаты о подобии, ортогональном подобии и т. п. имеются в работах Albert [1], Porter [8], [13], Porter, Adams [1], Porter, Hanson [1], [2]. В силу связи между квадратичными формами и их матрицами коэффициентов над полем $\mathbb{F}_q$ при нечетном q число линейных преобразований, переводящих квадратичую форму с матрицей коэффициентов A в эквивалентную квадратичиую форму с матрицей коэффициентов B, совпадает с числом невырожденных матриц X, таких, что $X^{\mathrm{T}}AX = B$. Это число было определено Зигелем (Siegel [1]) и Карлицом (Carlitz [54]); для четного q число решений X матричного уравнения $X^{\mathrm{T}}AX = B$ для симметрических матриц A и B было получено в статьях Feng, Dai [1], [2] и Fulton J. D. [5], [7]; о случае $B = 0$ см. Buckhiester [2]. Случай матрицы X фиксированного (но не обязательно полного) ранга рассмотрен в статье Hodges [21]. *Кососимметрическая матрица* A определяется условием $A^{\mathrm{T}} = -A$. Матричное уравнение $X^{\mathrm{T}}AX = B$ с заданными кососимметрическими матрицами A и B рассматривалось в статьях Carlitz [51] и Hodges [22]. Такое же матричное уравнение с другими типами матриц A и B рассматривалось в статьях Buckhiester [2], [3], [4], [5], [6]. Об уравнении $X^{\mathrm{T}}X = 0$ см. Carlitz [114] и Perkins [1], [2]. В работе Hodges [9] рассматриваются матричные уравнения

$X^TA + A^TX = B$ для симметрической матрицы B и $X^TA - A^TX = B$ для кососимметрической матрицы B.

Матричное уравнение

$$X_n^T \dots X_1^T A X_1 \dots X_n = B$$

с различными неизвестными матрицами $X_1, \dots, X_n$ и заданными матрицами A и B, которые либо обе симметрические, либо обе кососимметрические, изучалось в статьях Mousouris, Porter [1], Porter, Riveland [1] и Riveland, Porter [1], [2]. Портер (Porter [12], [22]) обобщил матричные уравнения из статьи Hodges [9] на случай нескольких неизвестных матриц. В работах Hodges [1], [4] определено число решений матричного уравнения $X_1 + \dots + X_n = A$, где X_i — либо симметрическая, либо кососимметрическая матрица, см. также Porter, Mousouris [5]. Системы матричных уравнений, содержащие симметрические и кососимметрические матрицы, изучались в статьях Hodges [17], [25].

Для матрицы A над полем $\mathbb{F}_{q^2}$ определим матрицу A^*, применяя к элементам матрицы A автоморфизм Фробениуса поля $\mathbb{F}_{q^2}$ над $\mathbb{F}_q$ (т. е. заменяя каждый элемент α элементом α^q) и затем транспонируя полученную матрицу. Матрица A называется *эрмитовой*, если $A^* = A$. Матричное уравнение $X^*AX = B$, где A и B — эрмитовы матрицы, изучалось в работах Carlitz, Hodges [1], Fulton J. D. [6], Hodges [24] и Wan, Yang [1], [2]; оно связано с эрмитовыми формами (см. Albert [1], Dickson [1]). Более общее уравнение

$$X_n^* \dots X_1^* A X_1 \dots X_n = B$$

с неизвестными матрицами $X_1, \dots, X_n$ и заданными эрмитовыми матрицами A и B рассматривалось в статье Mousouris, Porter [2]. В работе Hodges [9] изучается уравнение $X^*A + A^*X = B$ с эрмитовой матрицей B, а в статье Porter [20] — его обобщение на случай нескольких неизвестных матриц. Системы матричных уравнений, содержащие эрмитовы матрицы, встречаются в статье Hodges [25]. Приложения эрмитовых форм к конечным геометриям подробно изучены в статье Segre [11].

Матричное уравнение $AX = B$ рассматривалось в работах Hodges [5], Porter [21] и Porter, Mousouris [2]. О несколько более общем уравнении $AXC = B$ см. в статьях Hodges [19], Porter, Mousouris [2]. Работы Hodges [2], [18] посвящены матричному уравнеиию $XAY = B$ с неизвестными матрицами X и Y. Дальнейшие обобщения можно найти в статьях Dalla, Porter [1], Porter [10] и Porter, Mousouris [1], где изучается уравнение $AX_1 \dots X_n = B$, а также Dalla, Porter [2], Porter [14] и Porter, Mousouris [1], где изучается уравнение $X_1 \dots X_n A Y_1 \dots Y_m = B$. В последней статье имеются также результаты об уравнении $AX_1 \dots X_n C = B$. В статье Porter, Mousouris [3]

рассматривается матричное уравнение $AX_1 \ldots X_n = BY_1 \ldots Y_m$. Об уравнении $XA + CY = B$ и его обобщениях на случай большего числа неизвестных см. Hodges [28], [29], Plesken [1], Porter [19] и Porter, Mousouris [4]. Об уравнении $A_1X_1 + \ldots + A_nX_n = B$ и его обобщении см. Porter [18] и Hodges [30] соответственно.

Многие работы посвящены так называемым *инволютивным матрицам*, т. е. таким матрицам A, для которых $A^2 = I$, где I — единичная матрица. Число инволютивных матриц порядка n над полем $\mathbb{F}_q$ определено Ходжесом (Hodges [12]); см. также Brawley [2]. Различные перечислительные задачи для специальных классов инволютивных матриц решались в работах Brawley, Levine [2], Fulton J. D. [1], [2] и Perkins, Fulton [1]. Вопрос о числе решений некоторых уравнений от инволютивных матриц рассматривался в статьях Fulton J. D. [3], [4] и Lewine, Brawley [1]. Об инволютивных матрицах над кольцом $Z/(m)$ см. Brawley, Gamble [1]. Матричное уравнение вида $f(X) = 0$, где f — заданный многочлен над полем $\mathbb{F}_q$, изучалось в статье Hodges [11]; см. также Brawley, Mullen [1]. Ходжес (Hodges [14]) определил число решений системы матричных уравнений $a_1X + b_1Y = c_1I$, $a_2X^2 + b_2Y^2 = c_2I$, где $a_1, a_2, b_1, b_2 \in \mathbb{F}_q^*$, $c_1, c_2 \in \mathbb{F}_q$.

Число $n \times n$-матриц над простым полем $\mathbb{F}_p$, имеющих заданное значение определителя, было подсчитано Жорданом (Jordan C. [7]) и Файном и Нивеном (Fine, Niven [1]). Уравнения в определителях, содержащие неизвестные матрицы, изучались в статьях Carlitz [51], [55], [60] и Hodges [13], [20]. В комментариях к § 1 гл. 8 мы еще встретимся с результатами о числе матриц некоторых типов, например заданного размера или ранга.

§ 3. Интерес к диагональным уравнениям (отличным от линейных и квадратичных) возник из теории циклотомии, где рассматривались уравнения вида $ax^k + by^k = 1$. Эта теория восходит к Гауссу; в статье Gauss [1] рассматривается случай такого уравнения с $k = 3$, а в статье Gauss [3] — с $k = 4$. О других ранних результатах для этих случаев см. также Libri [2] и Lebesgue [1]. Связь такого уравнения для произвольного k с циклотомическими числами (см. комментарии к § 3 гл. 5) и суммами Гаусса и Якоби была подробно изучена Куммером (Kummer [4], [5], [6]). Классическое изложение этих результатов дал Бахман (Bachmann [1]); о более поздних результатах см. Storer [1]. Математики прошлого века (кроме ранее упомянутых см. также Carey [1], Pellet [8], Pepin [1] и Schwering [1]) рассматривали лишь простые конечные поля $\mathbb{F}_p$. Обобщение результатов Куммера на случай произвольного конечного поля $\mathbb{F}_q$ было получено Митчеллом (Mitchell H. H. [1], [2]). Интерес к циклотомии был возрожден важными результатами Диксона (Dickson

[44], [45], [46], [47]). Вычисления циклотомических чисел низкого порядка, начатые статьями Диксона, были продолжены в работах Baumert, Fredricksen [1], Berndt, Evans [1], Bruck [2], Evans, Hill [1], Leonard, Williams [3], [5], Muskat [4], [6], [7], Muskat, Whiteman [1], Parnami, Agrawal, Rajwade [3], Storer [2], Wells, Muskat [1] и Whiteman [9], [10], [11]. О дальнейших результатах по циклотомическим числам, таких, например, как, соотношения между ними, см. работы Baumert, Mills, Ward [1], Hall [7], Hull [1], Kutzko [1], Myerson [5], Rédei [8], Storer [3], [4], Vandiver [9], [11], [12], [14], [15], [17], [19], [20], [21], [22], Venkatarayudu [1] и Whiteman [3], [5], [6], [14].

Уравнение $ax^k + bx^k = c$ рассматривалось также и независимо от теории циклотомии. Сколем (Skolem [3]) показал, что для каждого простого числа $p \neq 7$ уравнение $ax^3 + by^3 = c$ при заданных $a, b, c \in \mathbb{F}_p^*$ имеет решение в $\mathbb{F}_p^2$; см. также Dunton [1] и Nagell [1]. О случае $k = 3$ кроме уже упоминавшихся работ Гаусса, Либри и Лебега см. также Cohen E. [9], Ireland, Rosen [1, ch. 8], Pepin [1], Singh [4] и Vaidyanathaswamy [2]. О случае $k = 4$ см. Parnami, Agrawal, Rajwade [1]. Результаты, относящиеся к случаю произвольного k, имеются в работах Chowla I. [1], [3], Chowla S. [12], Ireland, Rosen [1, ch. 8], Small [1], [2], [3] и Vandiver [3], [4], [13]. О связи уравнения $x^k + y^k = 1$ над простым полем $\mathbb{F}_p$ с проблемой раскрашивания графа см. Greenwood, Gleason [1].

Более общее уравнение $ax^{k_1} + by^{k_2} = c$ было впервые рассмотрено в статьях Pellet [3] и Piuma [1]. О дальнейших результатах см. Chowla I. [2], Davenport, Hasse [1], Hua, Vandiver [3], Mordell [5], Vandiver [5], [6], [9], [12], [14], [15], [17], [18], [19], [20], [21], [22], [23], [25], Whiteman [5] и Williams K. S. [23]. Таблицы решений для таких уравнений построены в работах Lehmer, Vandiver [1], Pearson, Vandiver [1], Selfridge, Nicol, Vandiver [1] и Vandiver [24]. В случае когда одно из чисел k_i равно 2, мы приходим к эллиптическим или гиперэллиптическим уравнениям (ср. с комментариями к § 4). Об аналогичном трехчленном уравнении см. Albert [4].

Уравнение вида $ax^k + by^k + cz^k = d$ (чаще всего с $a = b = 1$, $c = \pm 1$, $d = 0$) широко изучалось в связи с последней теоремой Ферма. Ранние результаты о существовании нетривиальных решений (т. е. решений с $x, y, z \neq 0$) этого уравнения над конечными простыми полями для $d = 0$ получены в статьях Cornacchia [1], Dickson [25], [26], Hurwitz [2], Mantel [2], Pellat [8], Pepin [1], Schur [1] и Wendt [1]. Списки случаев, когда возможно лишь тривиальное решение, приведены в статьях Cornacchia [1] и Dickson [14], [17], [21]. Обзоры этих результатов можно найти в следующих монографиях: Bachmann [6], Dickson [41,

ch. 26], Mordell [2] и Ribenboim [2, ch. 12]. См. также детальное исследование в книге Klösgen [1]. В статье Ankeny, Erdös [1] указано условие, при котором уравнение $x^k + y^k + z^k = 0$ имеет в $\mathbb{F}_p^3$ лишь тривиальные решения, а в статьях Vandiver [6], [10] изучается уравнение $ax^k + by^k + cz^k = 0$ над произвольными конечными полями. Диксон (Dickson [48]) использовал циклотомию для получения результатов о числе решений уравнения $ax^k + by^k + cz^k = d$ над простым полем $\mathbb{F}_p$. Уравнение вида $ax^3 + by^3 + cz^3 = d$ изучалось в статьях Chowla, Cowles, Cowles [1], [2], [3], [4], Cohen E. [7], [9], Lewis [2], Schupfer [1] и Selmer [1]. Об уравнении $x^4 + y^4 - z^4 = 0$ над полем $\mathbb{F}_p$ см. Dickson [26]. Уравнение $x^k + y^k + z^k = 0$ над полем $\mathbb{F}_{q^6}$, где $k = q + 1$ или $k = q^5 + 1$, рассматривалось в статье Ennola [1]. В работах Segre [11] и Hirschfeld [1] определяется число решений уравнения $x^{q+1} + y^{q+1} + z^{q+1} = 0$ над полями $\mathbb{F}_{q^2}$ и $\mathbb{F}_{q^4}$. Связи между диагональными уравнениями над конечными полями и диофантовыми уравнениями типа рассмотренного в последней теореме Ферма широко исследовались Вандивером (Vandiver [1], [3], [4], [13], [18], [21], [23]); см. также Khadzhiivanov, Nenov [1] по поводу недавних результатов.

Подход к диагональному уравнению (6.10), основанный на тригонометрических суммах, применялся еще Пелле (Pellet [6]) для случая, когда $b = 0$ и все k_i равны друг другу. Метод, описанный для общего случая в § 3, был разработан приблизительно в одно и то же время в статьях Furtado Gomide [1], Hua, Vandiver [1], [2] и Weil [6]. О дальнейших результатах, связанных с применением тригонометрических сумм к уравнению (6.10), см. Ankeny [2], Faircloth [1], [2], Faircloth, Vandiver [2], Hua, Vandiver [4], Ireland, Rosen [1, ch. 8, 10], Joly [3], [5], Mordell [23, ch. 6], Pearson, Vandiver [1], Schmidt W. M. [3, ch. 4], Whiteman [7] и Боревич, Шафаревич [1, гл. 1]. Равенство (6.15) выражает тот факт, что дзета-функция гиперповерхности, определенной уравнением (6.10), удовлетворяет предположениям Вейля (см. Weil [6]); ср. также Ireland, Rosen [1, ch. 11] и комментарии к § 4. О результатах, аналогичных теоремам 6.16 и 6.17, но когда среднее берется по уравнениям (6.10) с фиксированными значениями $k_1, \ldots, k_n$ и изменяющимися коэффициентами $a_1, \ldots, a_n$, см. Carlitz, Corson [1], [2] и Schmidt W. M. [3, ch. 4]. Оценки для числа решений уравнения (6.10) можно получить также и без использования тригонометрических сумм; см. Mordell [5] и Schmidt W. M. [3, ch. 4]. Асимптотическая формула для числа решений уравнения (6.10) была получена Карлицом (Carlitz [34]). Вандивер (Vandiver [7]) построил алгоритм для нахождения решений этого уравнения. Гегенбауэр (Gegenbauer [5]) рассматривал уравнение (6.10) над простым полем $\mathbb{F}_p$, $p > 2$, для случаев, когда числа k_i принимают значе-

ния 1, 2 или $(p-1)/2$. Результаты, касающиеся распределения решений уравнения (6.10) над простым полем $\mathbb{F}_p$, получены в статьях Chalk [1], Tietäväinen [7] и Williams K. S. [23]. Оценка числа решений уравнения (6.10) при условии, что некоторые переменные x_i имеют заранее заданные порядки в группе $\mathbb{F}_q^*$, получена Карлицом (Carlitz [37], [57]).

Тот частный случай уравнения (6.10), когда все показатели k_i совпадают, привлек внимание главным образом в связи с проблемой Варинга представления чисел суммами данного числа k-х степеней. Рекуррентные формулы для числа решений такого уравнения были получены Лебегом (Lebesgue [1]) и Халлом (Hull [1]). Сегре (Segre [10], [11]) при изучении таких уравнений применял геометрический подход. О дальнейших результатах см. Dickson [46], [47], [48], Hull [1], Myerson [2], [3], Williams K. S. [17] и Демьянов [1]. Случай, когда все k_i равны 3, рассмотрен в статьях Chowla, Cowles, Cowles [1], Myerson [1], Segre [10] и Williams K. S. [1], о случае, когда все k_i равны 4, см. Myerson [1] и Segre [10], когда все k_i равны 5, см. Hayashi [1] и Segre [10] и, когда все $k_i = 7$, см. Segre [10]. Случай, когда уравнение (6.10) рассматривается над полем $\mathbb{F}_{q^2}$ и общее значение всех k_i является делителем числа $q+1$, рассмотрен Карлицом (Carlitz [71]). О связи с проблемой Варинга см. Hardy, Littlewood [3], [4], а также Ayoub [1, ch. 4], Ellison [1], Hua [9, ch. 8], Huston [1], Kloosterman [4], Landau [2, part VI], [4], Siegel [2] и Vaughan R. C. [1, ch. 2].

Результат, полученный в примере 6.38, по существу принадлежит Смоллу (Small [2]). Согласно замечанию 6.25, каждый элемент поля $\mathbb{F}_q$ можно представить как сумму двух квадратов. За исключением случаев $q = 4$ и 7, каждый элемент поля $\mathbb{F}_q$ можно представить также в виде суммы двух кубов; см. Skolem [3] и Nagell [1] для случая простого q и Singh [4] для общего случая. Существуют примеры, когда некоторые элементы поля $\mathbb{F}_q$ не могут быть представлены в виде суммы какого бы то ни было числа k-х степеней, поскольку все суммы k-х степеней могут содержаться в каком-либо собственном подполе поля $\mathbb{F}_q$. Так, если $q = p^e$, где p — простое число, то необходимым и достаточным условием представимости каждого элемента $\mathbb{F}_q$ в виде суммы k-х степеней является отсутствие у числа k делителей вида $(q-1)/(p^d-1)$, где d — собственный делитель числа e или 1. Это было доказано в статье Tornheim [1] для простого числа k и в статье Bhaskaran [1] для произвольного натурального числа k; см. также Anderson [1] и Joly [1], [5]. *Проблема Варинга* состоит в нахождении наименьшего числа $g(k, p)$ из натуральных чисел n, таких, что любой элемент поля $\mathbb{F}_p$ можно представить в виде суммы из n k-х степеней. Эта проблема становится тривиальной, если $d = \text{НОД}(k, p-1) \geqslant (p-1)/2$. Для $d < (p-$

— 1)/2 Харди и Литтлвуд (Hardy, Littlewood [4]) показали, что $g(k, p) \leqslant k$; см. также Chowla, Mann, Straus [1], Dickson [47], Joly [5], Landau [2, part VI] и Tornheim [1] о близких к этому результатах. Первая оценка вида $g(k, p) = O(k^c)$ с показателем $c < 1$ была получена в работе Chowla I. [4]. В статье Dodson [2] эта оценка улучшена до показателя $c = 7/8$, в работе Tietäväinen [13] получено $c = 3/5 + \varepsilon$ для любого $\varepsilon > 0$, и, наконец, в статье Dodson, Tietäväinen [1] показано, что в предположении $d < (p - 1)/2$ всегда выполняется оценка $g(k, p) = O(k^{1/2} (\log k)^2)$. Последняя оценка является наилучшей возможной в том смысле, что в той же самой статье построено бесконечное семейство натуральных чисел k, таких, что $g(k, p) \geqslant (\sqrt{3k} - 1)/2$ для некоторого p, удовлетворяющего неравенству $d < (p - 1)/2$. Другие результаты о числе $g(k, p)$ см. в работах Bovey [4] и Small [1], [3]. Аналогичный вопрос для произвольных полей $\mathbb{F}_q$ рассматривается в статьях Schwarz [5], Stemmler [1], Tietäväinen [6] и Tornheim [1]. Случай более общих колец рассмотрен в статьях Chinburg [1] и Joly [1]. В работе Odlyzko, Stanley [1] оценивается число подмножеств группы $\mathbb{F}_p^*$, для которых сумма k-х степеней элементов равна заданному элементу поля $\mathbb{F}_p$.

Условия, при которых диагональное уравнение $a_1 x_1^k + \ldots + a_n x_n^k = b$ с данными коэффициентами $a_i \in \mathbb{F}_q^*$ имеет решение в $\mathbb{F}_q^n$ для любого $b \in \mathbb{F}_q$, были получены в работах Landau [2, part VI], Dickson [47], Rédei [3] и Chowla, Mann, Straus [1] для простого q и в работах Schwarz [6], [8], [9], [10] и Tietäväinen [9] для общего случая. При $b = 0$ возникает вопрос о нетривиальной разрешимости этого уравнения. Из следствия 6.6 вытекает, что нетривиальное решение (т. е. для которого не все x_i равны 0) существует, если $n > k$. Небольшие усиления этого результата получены в статьях Dickson [47] (см. также Davenport, Lewis [5], Dočev, Dimitrov [1] и Joly [5]), Cray [1], Lewis [3] и Tietäväinen [9]. Обозначим через $G(k, p)$ наименьшее из натуральных чисел n, таких, что уравнение $a_1 x_1^k + \ldots + a_n x_n^k = 0$ имеет нетривиальное решение в $\mathbb{F}_p^n$ для любых $a_1, \ldots, a_n \in \mathbb{F}_p$. Важным достижением стал результат С. Човлы (Chowla S. [9], [15]), который показал, что для любого $\varepsilon > 0$ выполняется неравенство $G(k, p) < (2 + \varepsilon) \log_2 k$ для достаточно больших простых чисел k. Аналогичный результат был установлен в статьях Chowla, Shimura [1] и Tietäväinen [1], [2] для всех достаточно больших нечетных чисел k. Верхняя граница для чисел $G(k, p)$ порядка $\log_2 k$ была установлена Човлой (Chowla S. [8], [10]) при условии, что элемент —1 является k-й степенью в поле $\mathbb{F}_p$; этот результат был обобщен на случай произвольного поля $\mathbb{F}_q$ в работах Tietäväinen [1], [2] и Heisler

[2]. В статье Tietäväinen [11] установлен наилучший возможный результат, а именно $G(k, p) < (1 + \varepsilon) \log_2 k$ для всех достаточно больших нечетных чисел k. В статье Dodson [2] показано, что $G(k, p) < k^{(2/3)+\varepsilon}$ для всех достаточно больших четных чисел k, не делящихся на $p - 1$, а в статье Tietäväinen [16] показатель улучшен до $1/2 + \varepsilon$. Аналогичные исследования для кольца $Z/(p^r)$ были проведены в статьях Bovey [1], [2], [3], Chowla S. [15], Chowla, Shimura [1], Davenport, Lewis [5], Dodson [1], [3], [4], Hardy, Littlewood [4], Hua [9, ch. 8], Huston [1], Norton [1] и Tietäväinen [12] [1]). Примеры, когда уравнение $a_1x_1^k + \ldots + a_nx_n^k = 0$ над полем $\mathbb{F}_p$ не имеет решения $(c_1, \ldots, c_n) \in \mathbb{F}_p^n$, где все c_i отличны от 0, можно найти в работах Gegenbauer [3] и Vandiver [8]. Нижние границы для числа элементов поля $\mathbb{F}_q$, представимых в виде суммы $a_1x_1^k + \ldots + a_nx_n^k$, получены в статье Chowla, Mann, Straus [1] (см. также Mann [3, ch. 2]) для простого числа q и в статье Diderrich, Mann [1] для произвольного поля $\mathbb{F}_q$. В статьях Lehmer E. [2] и Kaplan [1] результаты о числе решений уравнения $x_1^k + \ldots + x_n^k = b$ в $\mathbb{F}_p^n$ используются для исследования вопроса о вычетах и изучения законов взаимности; см. также Williams K. S. [33]. В статье Hodges [15] рассматривается уравнение в определителях вида $a_1 \det(X_1)^k + \ldots + a_n \det(X_n)^k = b$, где $X_1, \ldots, X_n$ — неизвестные матрицы одного и того же порядка над полем $\mathbb{F}_q$.

Теоремы 6.41 и 6.42 установлены в статьях Morlaye [1] и Joly [5]. Метод их доказательства восходит к Лебегу (Lebesgue [1]), который установил некоторые сравнения по модулю p для числа решений диагональных уравнений над простым полем $\mathbb{F}_p$. Дальнейшие результаты этого типа получены в статьях Joly [3], [5] и Morlaye [1]. Теорема 6.43 доказана Карлицом (Carlitz [65]), который обобщил результат Шварца (Schwarz [6]), полученный для случая, когда g — константа. Следствие 6.44 тоже было установлено Карлицом (Carlitz [65]). Уравнения вида $f(x_1) + \ldots + f(x_n) = b \in \mathbb{F}_p$ с произвольным многочленом f над $\mathbb{F}_p$ рассматривались еще Диксоном (Dickson [47]); см. также Hua [2] и Hua, Min [1]. Случай кубического многочлена f более подробно изучался в работах Ghent [1] и Hua [4], [5], [8]. Уравнения вида $f_1(x_1) + \ldots + f_n(x_n) = b \in \mathbb{F}_q$ с произвольными многочленами $f_1, \ldots, f_n$ над $\mathbb{F}_q$ рассматривались в работах Carlitz [43], Carlitz, Lewis, Mills, Straus [1] и Tietäväinen [1], [2], [6], [7], а в работах Carlitz, Corson [1], [2] рассматривался даже более общий случай, когда f_i являются многочленами

[1]) См. также Карацуба [3*], где выясняются условия разрешимости в кольце $Z/(p^r)$ уравнения $x_1^k + \ldots + x_n^k = a$. — *Прим. перев.*

от непересекающихся множеств переменных. Случай, когда f_i — некоторые рациональные функции, появляется в статьях Carlitz [43] и Brenner, Carlitz [1].

Системы двух диагональных уравнений исследовались в работах Corson [1], Davenport, Lewis [6], [7], Markovič [1], Spackman [1] и Tietäväinen [8]. Более общие системы диагональных уравнений были рассмотрены в статьях Akhtar [1], Carlitz, Wells [1], Davenport, Lewis [8], Hua [9, ch. 11], [10], Min [1], Rédei [7], Spackman [1], [2], Tietäväinen [1], [2], [6], Wells [2], Карацуба [1], [2], Коробов [3], [7] и Линник [1]. В статье Tietäväinen [6] показано, что система уравнений $\sum_{j=1}^{n} a_{ij}x_j^k = 0$, $i = 1, \ldots, t$, над полем $\mathbb{F}_q$ имеет нетривиальное решение в $\mathbb{F}_q^n$ для нечетного числа $d = \text{НОД}(k, q-1) > 1$, если $n \geqslant 2t(1 + \log_2(d-1))$. В статье Spackman [2] получены результаты о распределении решений и о существовании «малых» решений для систем диагональных уравнений. В статьях Tietäväinen [1], [2], [6] рассматривались системы уравнений вида $\sum_{j=1}^{n} f_{ij}(x_j) = 0$, $i = 1, \ldots, t$, где f_{ij} — многочлены над полем $\mathbb{F}_q$, обладающие свойством $f_{ij}(0) = 0$, и получены условия существования нетривиального решения. Такие же системы над кольцом вычетов $\mathbb{Z}/(p^r)$ рассматривались в работе van der Corput [1]. О результате, полученном в упр. 6.72, и его обобщениях см. статьи Carlitz, Wells [1] и Wells [2].

§ 4. Метод, описываемый в этом параграфе, развит С. А. Степановым [1]), а усовершенствован и упрощен В. Шмидтом. Он представляет собой успешную попытку доказать элементарным путем результаты А. Вейля, который для той же цели использовал изощренную технику алгебраической геометрии. Этот метод был впервые применен в статье Степанова [1], где был доказан результат типа теоремы 6.53 для уравнения $y^2 = f(x)$ над простым полем $\mathbb{F}_p$ с многочленом f нечетной степени (см. также Елистратов [6] о более позднем результате того же типа). Затем

---

[1]) Как сообщил С. А. Степанов, говоря об истоках этого метода, нужно отметить: 1) результат Н. С. Аладова [1] (1896 г.) о числе решений сравнения $y^2 \equiv x(x+1) \pmod p$, полученный применением метода Лагранжа; 2) работу Ю. И. Манина [1] (1956 г.), в которой элементарным путем, моделирующим более ранний и очень сложный метод Хассе—Вейля, получена оценка $|N_p - p| < 2p^{1/2}$ для числа N_p решений сравнения $y^2 \equiv x^3 + ax + b \pmod p$ и 3) элементарное доказательство А. Г. Постникова (1967 г.) оценки $|N_p - p| \leqslant (p+3)/2$ для такого числа N_p. Для получения этого результата Постников рассмотрел многочлен $g(x) = 2f(x)\left(1 \pm (f(x))^{(p-1)/2}\right) + (x^p - x)f'(x)$, где $f(x) = x^3 + ax + b$, и доказал, что каждый корень многочлена $F(x) = 1 \pm (f(x))^{(p-1)/2}$ по модулю p является кратным корнем многочлена $g(x)$. — *Прим. перев.*

для того же уравнения Степановым был получен результат теоремы 6.57 (см. Степанов [6]). В его статье [2] указанный метод прилагается к более общему уравнению $y^m = f(x)$ над $\mathbb{F}_p$, где НОД $(\deg(f), m) = 1$. К уравнениям вида $y^q - y = f(x)$ этот метод впервые был приложен в статьях Степанова [3], [5]. Другой элементарный метод решения этих уравнений был предложен Митькиным [1]. Оба указанных типа уравнений являются частными случаями уравнения

$$f(x, y) = y^m + a_1(x)\, y^{m-1} + \cdots + a_m(x) = 0, \quad a_i(x) \in \mathbb{F}_p[x].$$

В предположении, что многочлен $f(x, y)$ неприводим над основным полем $\mathbb{F}_p$, степень $\deg(a_m) = k$ взаимно проста с m и $\deg(a_i) < ik/m$, $1 \leqslant i \leqslant m-1$, Степанов в работах [7], [8] получил следующую оценку для числа N решений уравнения $f(x, y) = 0$ в $\mathbb{F}_p^2$: $|N - p| \leqslant Cp^{1/2}$, где константа C зависит лишь от k и m; см. также Степанов [10]. Шмидт (Schmidt W. M. [1]) показал, что указанные условия на многочлен $f(x, y)$ влекут за собой его абсолютную неприводимость; он обобщил результат Степанова на случай произвольного поля $\mathbb{F}_q$, показав, что для абсолютно неприводимого многочлена $f(x, y)$ число N решений уравнения $f(x, y) = 0$ в $\mathbb{F}_q^2$ удовлетворяет неравенству $|N - q| \leqslant Cq^{1/2}$, где константа C зависит лишь от степени многочлена f; см. также Schmidt W. M. [3, ch. 3]. Изложение метода Степанова можно найти в его работах [9], [10], [12], [13]; весьма подробно этот метод разбирается также в монографии Шмидта Schmidt W. M. [3].

Еще до результата Степанова нетривиальные оценки числа решений уравнения $y^m = f(x)$ элементарными средствами были получены Морделлом (Mordell [5]). Из оценок сумм значений характеров, полученных Дэвенпортом (Davenport [1], [2], [3], [7]), тоже получаются аналогичные результаты; см., кроме того, замечания ниже об эллиптических и гиперэллиптических уравнениях. Идея использования гиперпроизводных $E^{(n)}$ для исследования функций над полями ненулевой характеристики принадлежит Хассе (Hasse [7]), а также Тейхмюллеру (Teichmüller [1]), который доказал основные свойства этих гиперпроизводных. Другое доказательство леммы 6.55 (основаниое на диофантовых приближениях) см. в книге Lang [1, ch. 5]; ср. также с упр. 6.68 и 6.69.

Подход с позиции алгебраической геометрии к уравнению $f(x, y) = 0$ состоит в том, что это уравнение рассматривается как определяющее некоторую кривую в аффинном или проективном пространстве над полем $\mathbb{F}_q$. Если многочлен $f \in \mathbb{F}_q[x, y]$ абсолютно неприводим и N_1 — число $\mathbb{F}_q$-рациональных точек на проективной кривой (т. е. точек в однородных координатах,

координатные отношения которых принадлежат полю $\mathbb{F}_q$), то справедлива оценка

$$| N_1 - q - 1 | \leqslant 2gq^{1/2},$$

где g — род данной кривой. Этот результат был сформулирован Вейлем в работах Weil [1], [2] и подробно им доказан в статье Weil [3]. В статье Lang, Weil [1] было отмечено, что коэффициент $2g$ в приведенном неравенстве нельзя в общем случае заменить меньшим. Учитывая неравенство $2g \leqslant (d-1)(d-2)$, где $d = \deg(f)$ (см., например, Artin [9, ch. 16]), для числа N решений уравнения $f(x, y) = 0$ в $\mathbb{F}_q^2$ (т. е. для числа «конечных» точек на соответствующей проективной кривой) получаем оценку

$$| N - q | \leqslant (d-1)(d-2)\, q^{1/2} + d^2.$$

На такую оценку, однако, нельзя рассчитывать, если многочлен f не является абсолютно неприводимым (см. упр. 6.64 и 6.65). Покажем, как эти оценки связаны с так называемой гипотезой Римана для кривых над конечными полями. Для $s \in \mathbb{N}$ обозначим через N_s число $\mathbb{F}_{q^s}$-рациональных точек на проективной кривой, задаваемой уравнением $f(x, y) = 0$. Определим *дзета-функцию* этой кривой равенством

$$Z(t) = \exp\left(\sum_{s=1}^{\infty} (N_s/s)\, t^s \right),$$

где ряд сходится при $| t | < q^{-1}$ (это легко проверить с помощью тривиальной оценки $N_s \leqslant dq^s$). Вейль установил, что на самом деле $Z(t)$ — рациональная функция вида

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)},$$

где $L(t)$ — многочлен степени $2g$ с целыми коэффициентами и свободным членом 1. Если записать

$$L(t) = \prod_{j=1}^{2g} (1 - \omega_j t),$$

то ω_j будут целыми алгебраическими числами. *Гипотеза Римана* (доказанная Вейлем) состоит в том, что $| \omega_j | = q^{1/2}$ для всех $j = 1, \ldots, 2g$. Рассуждение, аналогичное тому, которое привело к формуле (5.24), показывает, что

$$N_s = q^s + 1 - \sum_{j=1}^{2g} \omega_j^s \quad \text{для каждого } s \in \mathbb{N},$$

а отсюда, учитывая гипотезу Римана, получаем, в частности, указанную выше оценку для N_1. Кроме того, дзета-функция удов-

летворяет некоторому функциональному уравнению, из которого следует, что числа ω_j можно разбить на пары комплексно-сопряженных.

Вслед за упомянутыми статьями Вейля появились и другие доказательства гипотезы Римана для кривых над конечными полями. Так, в статье Mattuck, Tate [1] решающее место доказательства Вейля было выведено из теоремы Римана—Роха; см. аналогичное доказательство в статье Grothendieck [1]. Теорема Римана—Роха используется также в доказательстве Бомбьери (Bombieri [5]), которое в остальных отношениях элементарно; см. также Bombieri [6]. Другие доказательства, а также обзоры результатов Вейля можно найти в следующих источниках: Deuring [3], Joly [5], Lang [1, ch. 6], Monsky [1] и Swinnerton-Dyer [3]. В статье Bombieri [1] показано, что число N_s асимптотически равно q^s при $s \to \infty$, при этом используется гораздо более простая техника; см. также Andrews [1] и Chowla, Hasse [1]. Пименов [1] изучил распределение чисел $N_s - (q^s + 1)$ для кривых рода $g > 1$. Исследование нулей дзета-функции $Z(t)$ было предпринято Елистратовым [4], [5]. В статье Armitage [2] была отмечена связь между гипотезой Римана для кривых и геометрией чисел над полями рядов Лорана характеристики p. Уточнения верхней границы для числа N_1 были получены в статьях Ihara [1] и Манин [5].

Формально иной подход к уравнению $f(x, y) = 0$ базируется на изучении расширения поля $\mathbb{F}_q(x)$ рациональных функций над полем $\mathbb{F}_q$, определяемого этим уравнением, т. е. на изучении соответствующего поля алгебраических функций. Такая точка зрения позволила Артину, Дэвенпорту и Хассе (см. Artin [1], Davenport, Hasse [1] и Hasse [2], [4], [8]) доказать гипотезу Римана для некоторых частных случаев даже раньше Вейля. При таком подходе определяется некоторая функция ζ (называемая конгруэнц-дзета-функцией) по аналогии с дзета-функцией Дедекинда для полей алгебраических чисел. Конгруэнц-дзета-функция, однако, связана с дзета-функцией Z для соответствующей кривой равенством $\zeta(u) = Z(q^{-u})$. Гипотеза Римана равносильна утверждению, что действительные части всех нулей конгруэнц-дзета-функции ζ равны $1/2$. Это совершенно аналогично до сих пор не доказанной гипотезе Римана в классической аналитической теории чисел, с той лишь небольшой разницей, что конгруэнц-дзета-функция не имеет тривиальных нулей. Конгруэнц-дзета-функция была введена Артином (Artin [1]) для случая квадратичного расширения поля $\mathbb{F}_p(x)$ и Шмидтом (Schmidt F. K. [2], [3]) для общего случая. Шмидт (Schmidt F. K. [3]) доказал, что конгруэнц-дзета-функция ζ удовлетворяет функциональному уравнению $F(u) = F(1 - u)$, где $F(u) = q^{(g-1)u}\zeta(u)$ и g — род кривой. Хассе (Hasse [3]) установил, что если θ — максимум

действительных частей нулей функции ζ, то для введенного выше числа N_1 справедлива оценка

$$| N_1 - q - 1 | \leqslant 2gq^{\theta},$$

а также что $1/2 \leqslant \theta < 1$, если $g > 0$. Верхняя граница для θ была улучшена Дэвенпортом (Davenport [7]) еще до того, как Вейль показал, что $\theta = 1/2$. Связь между гипотезой Римана для конгруэнц-дзета-функции ζ и точными оценками некоторых сумм значений характеров была отмечена Хассе (Hasse [5]). Доказательства гипотезы Римана, использующие теорию полей алгебраических функций, были получены (после Вейля) в работах Igusa [1] и Roquette [1], [2]; см. также Eichler [1, ch. 5] и Hasse [18]. Об общей теории конгруэнц-дзета-функций (или дзета-функций для полей алгебраических функций над $\mathbb{F}_q$) см. также книгу Deuring [4, ch. 3]. Нижняя граница для рода g, зависящая от степени соответствующего поля алгебраических функций над полем $\mathbb{F}_q(x)$, была установлена в статье Armitage [1]. Что касается теории полей алгебраических функций над конечными полями, то ее зачатки появляются еще у Кюне (Kühne [2]). Своего полного развития эта теория достигла в работах Artin [1], Schmidt F. K. [1], Sengenhorst [1] и Rauter [1], [2], что и привело к отмеченным выше результатам.

Важным частным случаем рассмотренной выше проблемы является случай *эллиптических уравнений (эллиптических кривых, полей эллиптических функций)* над конечным полем $\mathbb{F}_q$. Этот случай выделяется условием $g = 1$ и приводится при нечетном q к виду $y^2 = f(x)$, где степень многочлена $f \in \mathbb{F}_q[x]$ равна 3 или 4 и его дискриминант отличен от 0. Именно для этого случая Хассе дал доказательство гипотезы Римана, аннонсировав его в работах Hasse [4], [6] и приведя подробное доказательство в статье Hasse [8]. В частности, он показал, что число N решений в $\mathbb{F}_q^2$ указанного уравнения удовлетворяет неравенству

$$| N - q + \eta(a) | < 2q^{1/2},$$

где η — квадратичный характер поля $\mathbb{F}_q$ и a — коэффициент при x^4 многочлена $f(x)$. В статьях Artin [1] и Hasse [2] гипотеза Римана была доказана для некоторых частных полей эллиптических функций; см. также Hasse [17]. Более слабые оценки для N были получены в статье Mordell [5]. Элементарное доказательство приведенной выше оценки для N было дано Маниным [1] для случая простого числа q и $\deg(f) = 3$; см. также Zimmer [1], Гельфонд, Линник [1, гл. 10] и Елистратов [3]. Рациональность дзета-функции эллиптической кривой можно установить довольно просто (см., например, Robert [1, ch. 4]).

История эллиптических уравнений восходит к Гауссу (Gauss [3]), который рассмотрел уравнение $y^2 = ax^4 + b$ над полем $\mathbb{F}_p$.

В последней записи своего дневника Гаусс поставил вопрос об определении числа решений уравнения $x^2y^2 + x^2 + y^2 = 1$ в $\mathbb{F}_p^2$. Эта задача впервые была решена в статье Herglotz [1], но позднее было замечено, что указанное уравнение легко преобразуется в уравнение $y^2 = 1 - x^4$; см., например, Ireland, Rosen [1, ch. 11]. Особое внимание привлекли эллиптические уравнения $y^2 = ax^3 + b$ и $y^2 = ax^4 + b$; см. Davenport, Hasse [1], Frattini [1], Hasse [15, ch. 10], Joly [5], Lehmer E. [4], Neumann O. [1], Rajwade [2], [3] и Singh, Rajwade [1]. Случай $y^2 = ax^3 + bx$ рассматривается в работах Davenport, Hasse [1], Hasse [15, ch. 10], Joly [5], Lehmer E. [4], Morlaye [2], Rajwade [4] и Singh, Rajwade [1] [1]). Некоторые другие частные случаи эллиптического уравнения с кубическим многочленом f рассмотрены в статьях Baldisserri [1], Olson [1], Rajwade [1], [9], Rajwade, Parnami [1], Williams K. S. [38], Абдуллаев [1], [2] и Тушкина [1]. Ввиду очевидного тождества

$$N = \sum_{c \in \mathbb{F}_q} (1 + \eta(f(c)))$$

для числа N решений уравнения $y^2 = f(x)$ в $\mathbb{F}_q^2$ нахождение числа N равносильно вычислению сумм значений характеров, содержащих квадратичный характер η. В соответствии с этим мы отсылаем читателя также к § 5 гл. 5 и соответствующим комментариям. Вопрос об условиях положительности числа N был рассмотрен в статьях Châtelet [1], [2], Frattini [1] и Schmidt F. K. [3]; см. также Joly [5]. В статье Groote, Hirschfeld [1] определены возможные значения числа N для случая эллиптических кубических кривых над полями $\mathbb{F}_q$, $q \leqslant 13$. В статье Birch [2] изучается поведение величины N для уравнения $y^2 = x^3 - ax - b$ над простым конечным полем $\mathbb{F}_p$, когда a и b пробегают это поле. Ёсида (Yoshida [1]) рассмотрел все эллиптические кривые над полем $\mathbb{F}_{p^m}$ и нашел предельное распределение чисел N при $m \to \infty$ для фиксированного простого числа p; обобщение этого результата см. в статье Deligne [6]. Некоторые результаты о поведении числа N, когда эллиптические кривые пробегают определенное семейство, можно найти в статье Milne [2]. По поводу поведения числа N решений сравнения $y^2 \equiv x^3 - Ax - B \pmod p$ при фиксированных $A, B \in \mathbb{Z}$ и изменяющемся простом p Тейтом (Tate [1]), а также Бёрчем и Свиннертоном-Дайером (Birch, Swinnerton-Dyer [2]) были выдвинуты важные гипотезы; о гипотезе Тейта см. также Swinnerton-Dyer [1] и Tate [2], а кроме того, Yamamoto, Naganuma, Doi [1]. Множество $\mathbb{F}_q$-рациональных точек на некоторой эллиптической кривой можно наделить

[1]) См. также Постникова [1*]. — *Прим. перев.*

групповой структурой; см., например, Bedocchi [1] и Borosh, Moreno, Porta [1], [2], где установлены некоторые свойства этой группы. В статье Bedocchi [2] изучаются классы изоморфизмов эллиптических кривых над $\mathbb{F}_q$. Важные результаты по общей теории полей эллиптических функций содержатся в работах Deuring [2] и Waterhouse [1]. Обзоры по теории эллиптических уравнений имеются в работах Cassels [1] и Zimmer [2, ch. 11].

Уравнение вида $y^2 = f(x)$ над полем $\mathbb{F}_q$ нечетной характеристики с произвольным многочленом f называется *гиперэллиптическим уравнением*. Мы не будем здесь касаться отмеченных выше результатов об эллиптических уравнениях. Общая теория гиперэллиптических уравнений впервые была развита Артином (Artin [1]), который сформулировал также гипотезу Римана для этого класса уравнений и показал, что в случае простого числа q и $\deg(f) \geqslant 3$ имеет место неравенство $1/2 \leqslant \theta < 1$, где θ — максимум действительных частей нулей конгруэнц-дзета-функции. Морделл для некоторых частных случаев гиперэллиптических уравнений получил нетривиальные оценки числа N их решений (Mordell [5]). Ввиду указанной выше связи между числом N и суммами значений характеров, содержащими квадратичный характер η, результаты Дэвенпорта (Davenport [1], [3]) о таких суммах значений характеров тоже приводят к определенным оценкам для числа N. Непосредственно вслед за этими результатами Дэвенпортом и Хассе (Davenport, Hasse [1] была доказана гипотеза Римана для уравнения $y^2 = ax^m + b$ над полем $\mathbb{F}_q$ в случае, когда m делит число $q - 1$. Элементарный метод Степанова [1], [6] для гиперэллиптических уравнений был до некоторой степени усовершенствован Коробовым [6], Митькиным [2] и Старком (Stark [1]), что позволяет в определенных случаях внести небольшие улучшения в теорему 6.57. Возможное усиление для случая $y^2 = x^m + ax + b$ отмечено в статье Ono [7]. Число решений некоторых специальных гиперэллиптических уравнений было подсчитано в статьях Lehmer E. [4] и Rajwade [3], [5], [6], [8]. См. также материал § 5 гл. 5 о сумме значений характеров $\sum_{c \in \mathbb{F}_q} \eta(f(c))$ и комментарии к этому параграфу. В статье Митькина [4] изучалась разрешимость гиперэллиптических уравнений над простым полем $\mathbb{F}_p$. В статье Davenport, Lewis [2] изучался «дефект» $N(b) - p$, когда элемент b пробегает поле $\mathbb{F}_p$; здесь $N(b)$ обозначает число решений уравнения $y^2 = f(x) + b$ в $\mathbb{F}_p^2$, где $f \in \mathbb{F}_p[x]$ — фиксированный многочлен. В статье Stephens [1] доказана гипотеза из работы Chowla, Chowla [1] о существовании малых решений (относительно x) уравнения $y^2 = (x + a_1) \ldots (x + a_n)$ над $\mathbb{F}_p$ при различных $a_1, \ldots, a_n \in \mathbb{F}_p$. Один частный случай был элементарными средствами разобран

в статье Singh [6]. В работе Segre [4] рассматривается система из двух гиперэллиптических уравнений.

Что касается других частных случаев общего уравнения $f(x, y) = 0$, то одним из них являются уравнения вида $y^m = f(x)$. Еще до Вейля такое уравнение рассматривалось в статьях Davenport [2], [7], Davenport, Hasse [1] и Mordell [5]. См. также недавнюю работу Ono [8], в которой проводится элементарный разбор еще одного случая. В статье Davenport, Lewis [2], упоминавшейся в предыдущем абзаце, «дефект» $N(b) - p$ рассматривался также для уравнения $y^3 = f(x) + b$ над простым полем $\mathbb{F}_p$, когда степень многочлена f равна 3 или 4. Елистратовым [1], [2] был развит элементарный подход к гипотезе Римана для уравнения $y^3 = f(x)$, $\deg(f) = 3$. Частный случай уравнения вида $y^p - y = f(x)$ появляется в статьях Davenport, Hasse [1] и Yamada [1]. В статье Carlitz [125] определяется число решений уравнения $y^p - y = ax^{p+1} + bx$ в $\mathbb{F}_q^2$. Степанов в работе [4] доказал теорему 5.45 о суммах Клостермана, применив свой элементарный метод к уравнению $y^p - y = ax + 1/x$; ср. также с примером 6.63 и работой Schmidt W. M. [3, ch. 2]. Морделл (Mordell [25]) охарактеризовал квадратные и кубические многочлены $f \in \mathbb{F}_p[x, y]$ с помощью свойства, что если одна из переменных принимает заранее заданное значение из $\mathbb{F}_p$, то получающееся уравнение имеет по крайней мере одно решение в $\mathbb{F}_p$. Гоппа в работе [2] применил теорию кривых над конечными полями для построения кодов; см. также Manin [5].

Первый имеющий важное значение общий результат об уравнениях $f(x_1, \ldots, x_n) = 0$ для $n \geqslant 3$ и системах таких уравнений был получен Ленгом и Вейлем (Lang, Weil [1]); его удобнее сформулировать в терминах проективных многообразий. Если V — некоторое абсолютно неприводимое многообразие в n-мерном проективном пространстве над конечным полем $\mathbb{F}_q$ размерности r и степени d, то число N_1 $\mathbb{F}_q$-рациональных точек многообразия V удовлетворяет неравенству

$$|N_1 - q^r| \leqslant (d-1)(d-2)q^{r-(1/2)} + A(n, r, d)q^{r-1},$$

где постоянная $A(n, r, d)$ зависит лишь от указанных параметров. Несколько более слабый результат примерно одновременно был установлен Нисневичем [1]. Для случая кривой ($r = 1$) отсюда легко получается указанная ранее оценка Вейля. Замечания по поводу результата Ленга и Вейля можно найти в статье Segre [9]. Для случая гиперповерхности ($r = n - 1$) следующая нижняя оценка была установлена Шмидтом (Schmidt W. M. [2]) применением метода Степанова: если $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — абсолютно

неприводимый многочлен степени d, то число N решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ удовлетворяет неравенству

$$N > q^{n-1} - (d-1)(d-2)\,q^{n-(3/2)} - 6d^2q^{n-2}$$

при достаточно большом числе q. Подробнее о применении оценки Ленга — Вейля к гиперповерхностям см. в книге Schmidt W. M. [3, ch. 5]. Случай произвольной размерности рассматривается в статьях Joly [5] и Schmidt W. M. [3, ch. 6]. Оценки Ленга — Вейля для специальных классов многообразий были получены в работах Carlitz, Wells [1] и Wells [2].

В статье Birch, Lewis [1] с помощью оценки Ленга — Вейля показывается, что если многочлен $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ абсолютно неприводим и однороден, то уравнение $f(x_1, \ldots, x_n) = 0$ имеет более $(1/2)\,q^{n-1}$ невырожденных решений в $\mathbb{F}_q^n$ при достаточно большом числе q (*вырожденным* называется такое решение в $\mathbb{F}_q^n$, для которого все частные производные функции f равны нулю). Дальнейшие результаты о невырожденных решениях таких уравнений можно найти в статье Lewis, Schuur [1], в частности для случая кубического многочлена f. Этот случай рассмотрен также в статьях Birch, Lewis [1] и Watson G. L. [1]. Конечные множества однородных многочленов одной и той же степени $d > 1$, любая нетривиальная линейная комбинация которых имеет лишь одну вырожденную точку, а именно $(0, \ldots, 0)$, были построены Карлицом (Carlitz [66]). Однородные многочлены f над $\mathbb{F}_q$ небольшой степени, для которых уравнение $f(x_1, \ldots, x_n) = 0$ имеет лишь вырожденные решения в $\mathbb{F}_q^n$, были охарактеризованы Льюисом (Lewis [1]). Формулы для числа точек многообразия определенных типов были получены в работах Corson [1], Swinnerton-Dyer [2] и Манин [2]; см. также Манин [4, гл. 4]. Оценки числа решений системы уравнений $f(x_1) = f(x_2) = \ldots = f(x_r)$, где $f \in \mathbb{F}_q[x]$, при различных значениях x_i были получены в статьях Birch, Swinnerton-Dyer [1] и Williams K. S. [24].

Теорию дзета-функций, имеющую такое значение для вопроса о числе решений уравнений, можно обобщить и на многообразия. Пусть V — многообразие, определенное в n-мерном аффинном или проективном пространстве над конечным полем $\mathbb{F}_q$, и пусть N_s — число точек из $\mathbb{F}_{q^s}^n$ (соответственно число $\mathbb{F}_{q^s}$-рациональных точек в случае проективного пространства), принадлежащих многообразию V. Определим *дзета-функцию* на многообразии V равенством

$$Z(V; t) = \exp\left(\sum_{s=1}^{\infty} (N_s/s)\,t^s\right),$$

где ряд сходится при $|t| < q^{-n}$. Вейль (Weil [6]) сформулировал некоторые предположения об этой дзета-функции, в частности, что $Z(V; t)$ является рациональной функцией от переменной t, что она удовлетворяет некоторому функциональному уравнению и что ее нули и полюсы имеют некоторые заранее заданные абсолютные величины. Рациональность дзета-функции $Z(V; t)$ была доказана Дворком (Dwork [2]) с помощью p-адической техники; см. также работу Dwork [1], где устанавливаются подготовительные результаты. Позднее Гротендик (Grothendieck [2]) доказал тот же результат средствами алгебраической геометрии. О рациональности дзета-функции $Z(V; t)$ см. также работы Bruhat [1], Dwork [9], Joly [5], Koblitz [2, ch. 5], [4], Milne [1, ch. 6], Monsky [1] и Reich [1]. Метод Дворка был обобщен в статье Kiefe [1], и с его помощью было доказано, что логарифмическая производная от дзета-функции не только на многообразии, но и на более общем множестве V является рациональной функцией. Тот факт, что дзета-функция гиперповерхности, определяемой диагональным уравнением, является рациональной функцией, был отмечен еще Вейлем (Weil [6]); ср. также с (6.15) и с примером 6.49, а также с разбором этого случая в книге Ireland, Rosen [1, ch. 11]. Для некоторых других частных случаев предположение Вейля о рациональности дзета-функции $Z(V; t)$ было доказано еще до Дворка в работах Carlitz [42], [56], Delsarte J. [1], Furtado Gomide [1], Sampson, Washnitzer [1] и Weil [8].

Если V — невырожденное абсолютно неприводимое проективное многообразие размерности r, то Вейль (Weil [6]) высказал, далее, предположение, что рациональная функция $Z(V; t)$ имеет вид

$$Z(V; t) = \frac{P_1(t) P_3(t) \dots P_{2r-1}(t)}{P_0(t) P_2(t) \dots P_{2r}(t)},$$

где каждое P_h — многочлен с целыми коэффициентами и постоянным членом 1. Более того, $P_0(t) = 1 - t$, $P_{2r}(t) = 1 - q^r t$ и

$$P_h(t) = \prod_{i=1}^{B_h} (1 - \alpha_{hi} t) \quad \text{для} \quad 0 \leqslant h \leqslant 2r,$$

где α_{hi} — целое алгебраическое число, для которого $|\alpha_{hi}| = q^{h/2}$. Он предположил также, что степень B_h многочлена P_h можно интерпретировать как число Бетти. Указанный вид дзета-функции $Z(V; t)$ ведет к следующему представлению числа N_s $\mathbb{F}_{q^s}$-рациональных точек на V, справедливому для любого натурального числа s:

$$N_s = \sum_{h=0}^{2r} (-1)^h \sum_{i=1}^{B_h} \alpha_{hi}^s.$$

Критический разбор предположений Вейля с различных точек зрения был проделан в следующих работах: Deuring [3], Joly [5], Kleiman [1], Mazur B. [1], Milne [1, ch. 6], Monsky [1], Swinnerton-Dyer [3] и Tate [1]. Первая брешь была пробита Дворком (Dwork [3], [5], [8]), который установил для случая гиперпространств указанные выше разложение функции $Z(V; t)$ и интерпретацию чисел B_h, а также показал, что эта функция удовлетворяет функциональному уравнению

$$Z\left(V; \frac{1}{q^r t}\right) = \pm q^{rk/2} t^k Z(V; t), \quad k = \sum_{h=0}^{2r} (-1)^h B_h,$$

о чем тоже говорилось в предположениях Вейля; см. также Dwork [6], [7], Ireland [1] и Monsky [1]. Предположения же Вейля о коэффициентах многочленов P_h и об абсолютных величинах чисел α_{hi} (так называемая *гипотеза Римана — Вейля*) до сих пор остаются недоказанными. Указанные результаты Дворка для гиперповерхностей были распространены на общий случай Гротендиком (Grothendieck [2], [3]). Другие доказательства были даны в статьях Lubkin [1], [2], а в статье Lubkin [3] было показано, что многочлены $P_h(q^{-h/2}t)$, $0 \leqslant h \leqslant 2r$, являются квазисамовозвратными. Гипотеза Римана — Вейля была доказана для некоторых кубических гиперповерхностей в статьях Bombieri, Swinnerton-Dyer [1] (см. также Bombieri [2]) и Перельмутер [5], для некоторых гиперповерхностей четвертой степени в статьях Deligne [1] и Dwork [10], для абелевых многообразий в статьях Weil [3], [4] и для некоторых других типов многообразий в статьях Deligne [1], [2], Harder [1], Weil [9], Исковских [2] и Манин [3]. И наконец, общая гипотеза Римана — Вейля была доказана Делинем (Deligne [3]), который также отметил вытекающую из нее оценку для числа точек на многообразии. В работе Katz [3] дается великолепный разбор основных частей доказательства Делиня; краткое изложение его можно найти в статье Serre [2]. См. обобщения этой теории в работах Deligne [6] и Lubkin [4], [5].

Для некоторых полиномиальных уравнений с числом переменных $n \geqslant 3$ можно гораздо более элементарными средствами получить оценки для числа решений, которые ничуть не уступают оценкам, полученным с использованием гипотезы Римана — Вейля. Так, помимо очевидных примеров линейных, квадратных и диагональных уравнений можно указать результаты Дэвенпорта и Льюиса (Davenport, Lewis [4]) и Морделла (Mordell [11], [17], [20], [21]), которые дают оценку $N = p^2 + O(p)$ для числа решений ряда кубических уравнений $f(x, y, z) = 0$ над полем $\mathbb{F}_p$. В статье Davenport, Lewis [4] получена оценка того же типа для почти всех (за некоторыми тривиальными исключениями) урав-

нений вида $z^m = F(x, y) + b$ над простым полем $\mathbb{F}_p$, где F — однородный многочлен и $b \in \mathbb{F}_p^*$. В статье Mordell [7] получена оценка $N = p^{n-1} + O(p^{(n-1)/2})$ для полиномиальных уравнений от $n \leqslant 4$ переменных над полем $\mathbb{F}_p$, образованных линейными комбинациями элементарных симметрических многочленов. В статье Mordell [14] получена оценка $N = p^{n-1} + O(p^{n/2})$ для уравнений, близких к диагональным, над полем $\mathbb{F}_p$ с любым числом n переменных. Перельмутер и Постников [1] рассмотрели уравнение вида $f_0(y) + f_1(y) x_1^{k_1} + \ldots + f_n(y) x_n^{k_n} = 0$ над простым полем $\mathbb{F}_p$ и показали, что при определенных условиях на $f_0, f_1, \ldots, f_n$ имеет место оценка $N = p^n + O(p^{n/2})$; см. обобщенне этого результата в книге Schmidt W. M. [3, ch. 4].

Оценки Ленга — Вейля и Делиня для числа точек на многообразиях можно использовать для установления некоторых результатов о распределении решений уравнения $f(x_1, \ldots, x_n) = 0$ или системы таких уравнений (см. Chalk, Williams [1], Myerson [4], Smith R. A. [2] и Williams K. S. [18]). Об общем принципе, лежащем в основе доказательств таких результатов см. Mordell [22] и Chalk [2].

Дальнейшие результаты о дзета-функциях многообразий можно найти в следующих источниках: об абелевых многообразиях см. Shimura, Taniyama [2, ch. 4] и Waterhouse, Milne [1]; о случае кубических поверхностей см. Swinnerton-Dyer [2] и Манин [4, гл. 4]; о гиперповерхностях уравнений $y^2 = f(x_1, \ldots, x_n)$ и $y^p - y = f(x_1, \ldots, x_n)$ над $\mathbb{F}_p$ см. Перельмутер [4]; о гиперповерхностях уравнения $y^p - y = f_0(x) + f_1(x) x_1^{k_1} + \ldots + f_n(x) x_n^{k_n}$ над $\mathbb{F}_q$ см. Кузнецов В. Н. [1]; см. также Bayer, Neukirch [1], Dwork [4], [10], Schneider [1], Swinnerton-Dyer [1] и Taniyama [1]. Полезные сведения из теории дзета-функций можно найти в работах Mazur B. [1] и Thomas [1]. Кац (Katz [2]) и Коблиц (Koblitz [1]) изучали поведение дзета-функции на семействе многообразий. В статье Curtis [1] обнаружена связь между дзета-функциями многообразий и теорией характеров некоторых конечных групп. В статье Spackman [1] дается элементарное доказательство предположений Вейля для многообразий, определяемых парой диагональных уравнений. В статье Haris [1] отмечена связь между результатами Дворка, касающимися предположений Вейля, и абстрактными формулами Пуассона. Ленг (Lang [2]) изучает связь между точками на многообразиях над конечными полями и точками на многообразиях над полями алгебраических чнсел. Дальнейшую информацию об абсолютно неприводимых многочленах можно найти в работах Fredman [2], Schmidt W. M. [3, ch. 5] и Williams K. S. [3].

Теория дзета-функций многообразий может быть расширена до теории L-функций. Эти функции играют ту же роль для оценки

сумм значений характеров, какую играют дзета-функции для оценки числа точек на многообразиях. Пусть V — аффинное или проективное многообразие над полем $\mathbb{F}_q$, и пусть $\chi^{(s)}$ — канонический аддитивный характер расширения $\mathbb{F}_{q^s}$ поля $\mathbb{F}_q$. Определим сумму значений этого характера

$$C_s = C_s(V, f) = \sum \chi^{(s)}(f(Q_s)),$$

где Q_s пробегает все точки многообразия V с координатами из $\mathbb{F}_{q^s}$ (соответственно $\mathbb{F}_{q^s}$-рациональные точки многообразия V в проективном случае), а f — регулярная функция на V, так что $f(Q_s) \in \mathbb{F}_{q^s}$ для всех точек Q_s, например, f — многочлен над $\mathbb{F}_q$. Соответствующую *L-функцию* определим равенством

$$L(V, f; t) = \exp\left(\sum_{s=1}^{\infty} (C_s/s)\, t^s\right).$$

Тот факт, что L-функции тоже являются рациональными функциями, был впервые доказан Гротендиком (Grothendieck [2], [3]); см. также Bombieri [3], [4], Dwork [9], Hooley [6] и Перельмутер [6]. При подходящих ограничениях на V и f снова можно сформулировать предположения Вейля. Некоторые из них, например касающиеся функционального уравнения и разложения L-функций, доказаны Гротендиком (Grothendieck [2], [3]); по поводу случая L-функций, связанных с полями алгебраических функций над $\mathbb{F}_q$, см. Weissinger [1]. Аналог гипотезы Римана — Вейля был доказан лишь с помощью результатов Делиня (Deligne [3], [4], [6]). Обзор результатов Делиня имеется в статьях Katz [4] и Serre [3]. Дальнейшие результаты по L-функциям можно найти в работах Adolphson, Sperber [1], Bombieri [7], Hooley [6], Laumon [1] и Sperber [1], [3]. Аналогичную теорию можно развить также и с помощью мультипликативных (а не аддитивных) характеров, а также для гибридных тригонометрических сумм (см. Katz [4], Serre [3] и Перельмутер [3]). Значение этих результатов для оценки тригонометрических сумм обсуждалось в комментариях к § 4 и 5 гл. 5.

[Различные диофантовы уравнения в конечных полях рассматривались в работах Orzech [1*], Small [1*] и Snapper [1*]. Спэкман (Spackman [1*]) получил рекуррентное соотношение для последовательностей, связанных с числом решений некоторых диагональных уравнений, и усилил результаты, полученные в работе Myerson [4]. Хеллесет (Helleseth [1*]) установил связь между одной задачей теории кодирования и проблемой Варинга в конечном поле. Стор и Волох (Stohr, Voloch [1*]) получили новое доказательство оценки Вейля (Weil A. [2]) для числа рациональных точек на кривой методом, аналогичным методу

Степанова [9], [10], а также получили некоторое ее уточнение. Мазур [1*] вывел асимптотическую формулу для числа решений системы сравнений

$$\sum_{k=1}^{p-1} \varepsilon_k k^{\nu} \equiv a_{\nu} \pmod{p}, \quad \nu = 1, \ldots, n \quad (\varepsilon_k \in \{0, 1\}, \quad k = 1, \ldots, p-1).$$

где p — простое и n — натуральное число. Одлыжко и Стэили (Odlyzko, Stanley [1]) рассмотрели только последнее уравнение этой системы и получили для него более точные результаты. Шпарлинский [3*] другим методом получил аналогичное уточнение для исходной системы. Конягин [1*] дал неулучшаемую оценку с асимптотически точным значением константы для числа решений полиномиального сравнения n-й степени. При этом он использовал результаты Стечкина [1] и Нечаева [7]. Хаксли (Huxley [1*]) получил уточнение аналогичной оценки Нагеля (Nagell [1*]) для числа решений сравнения с многочленом, имеющим ненулевой дискриминант.

К этому же кругу вопросов относится проблема Артина о локальном представлении нуля формой. Пусть $p \geqslant 2$ — простое число, $\mathbb{Q}_p$ — поле p-адических чисел, $F(x_1, \ldots, x_n)$ — форма степени n от k переменных над $\mathbb{Q}_p$. Если уравнение $F(x_1, \ldots, x_n) = 0$, $x_j \in \mathbb{Q}_p$, $j = 1, \ldots, k$, имеет ненулевое решение, то говорят, что форма F нетривиально представляет нуль. Гипотеза Артина была доказана при $n = 2$ Минковским и Хассе, при $n = 3$ — Демьяновым [1*] и Льюисом (Lewis [1*]). Кроме того, Ершов [1], а также Акс и Коген (Ax, Kochen [1]) в 1965 г. доказали, что при заданном n для всех p, за исключением конечного числа, гипотеза Артина верна. А в 1966 г. гипотеза Артина была опровергнута в работе Terjanian [1*], где доказано, что для нетривиального представления нуля формой над Q_p необходимо $k \geqslant n^{\log_4 20}$, в том же году это утверждение было усилено Бровкиным (Browkin [1*]) до $k \geqslant n^{3-\varepsilon}$, $\varepsilon > 0$. В 1981 г. Архипов и Карацуба [1*] (см. также [2*], [3*]) доказали, что необходимо условие $k \geqslant \exp(n/(\log n)^{1+\varepsilon})$, $\varepsilon > 0$, т. е. для выполнения гипотезы Артина требуется почти экспоненциальный рост числа переменных. Аналогичная гипотеза для системы форм была также опровергнута Архиповым [1*], [2*], который доказал, что в этом случае k должно расти экспоненциально, именно как 2^n. См. также Боревич, Шафаревич [1].

По тематике шестой главы кроме отмеченных выше имеются еще работы: Browkin [2*], Cheng [1*], Grytczyk, Tropak [1*] и Григорьев [1*]. — *Перев.*]

Упражнения

6.1. Найти число решений уравнения $x^5 + 2x^4 + x^2 + 1 = 0$ в поле $\mathbb{F}_5$.

6.2. Найти число решений уравнения $x^6 - 3x^5 - x^4 + x^3 - x = 0$ в поле $\mathbb{F}_7$.

6.3. Пусть $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — многочлен степени, меньшей чем n, и пусть $(c_{i1}, \ldots, c_{in})$, $i = 1, \ldots, N$, — решения уравнения $f(x_1, \ldots, x_n) = 0$, лежащие в $\mathbb{F}_q^n$. Доказать, что

$$\sum_{i=1}^{N} c_{ij}^k = 0 \quad \text{для любых } j \text{ и } k,\ 1 \leqslant j \leqslant n,\ 0 \leqslant k \leqslant q-2,$$

6.4. Многочлен $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ степени n называется *норменным многочленом*, если единственным решением уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ является $(0, \ldots, 0)$. (Объяснение такого определения содержится в примере 6.7.) Доказать, что если f — норменный многочлен и $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ — произвольный многочлен степени, меньшей чем n, то уравнение $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ имеет по крайней мере одно решение в $\mathbb{F}_q^n$.

6.5. Построить норменный многочлен степени 3 в кольце $\mathbb{F}_2[x_1, x_2, x_3]$.

6.6. Доказать, что если однородный многочлен $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ степени $d \geqslant 1$ делится на некоторую переменную x_i, то число решений уравнения $f(x_1, \ldots, x_n) = 0$ в $\mathbb{F}_q^n$ не превышает числа $dq^{n-1} - (d-1)q^{n-2}$.

6.7. Доказать, что число $\omega(d)$, определенное перед теоремой 6.16, совпадает с биномиальным коэффициентом $\binom{n+d}{d}$.

6.8. Найти диагональную квадратичную форму, эквивалентную форме $x_1x_2 + 2x_1x_3 - x_2x_3 \in \mathbb{F}_5[x_1, x_2, x_3]$.

6.9. Найти диагональную квадратичную форму, эквивалентную форме $2x_1^2 - 5x_2^2 + 3x_3^2 + x_1x_2 - 4x_1x_3 - 3x_2x_3 \in \mathbb{F}_{11}[x_1, x_2, x_3]$.

6.10. Найти число решений уравнения $3x_1^2 + x_2^2 - 2x_1x_2 + x_1x_3 + 3x_2x_3 = 2$ в $\mathbb{F}_7^3$.

6.11. Найти число решений уравнения $2x_1^2 - x_2^2 + x_3^2 - x_1x_2 - 2x_1x_3 = 2$ в $\mathbb{F}_5^3$.

6.12. Найти число решений уравнения $x_1^2 - x_2^2 + 2x_3^2 - x_1x_4 - x_2x_3 + 2x_2x_4 = 0$ в $\mathbb{F}_5^4$.

6.13. Найти число решений уравнения $x_1^2 + x_3^2 + x_5^2 - x_1x_2 - x_2x_3 + x_2x_4 + x_4x_5 = -1$ в $\mathbb{F}_3^5$.

6.14. Найти число решений уравнения $x_1^2 + 2x_2^2 - 2x_3^2 - 2x_1x_2 + x_1x_3 + 2x_2x_3 = 1$ в $\mathbb{F}_{25}^3$.

6.15. Найти число решений уравнения $x_1^2 - x_2^2 - x_3^2 + x_1x_2 + 2x_2x_3 - x_1 + 2x_3 = 0$ в $\mathbb{F}_5^3$.

6.16. Найти число решений уравнения $x_2^2 - x_3^2 + x_4^2 - x_1x_2 - x_1x_3 + x_1x_4 + x_3x_4 + x_2 + x_4 = 1$ в $\mathbb{F}_3^4$.

6.17. Найти число решений уравнения $x_1^2 + x_2^2 + x_1x_2 + x_1x_3 = 1$ в $\mathbb{F}_4^3$.

6.18. Найти число решений уравнения $x_1^2 + x_2^2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4 = 1$ в $\mathbb{F}_8^4$.

6.19. Найти число решений уравнения $\theta^2x_2^2 + \theta x_4^2 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 = 0$ в $\mathbb{F}_4^4$, где элемент $\theta \in \mathbb{F}_4$ удовлетворяет равенству $\theta^2 = \theta + 1$.

6.20. Найти число решений уравнения $(\theta^2 + \theta)x_2^2 + x_3^2 + \theta x_4^2 + \theta^2x_1x_2 + \theta x_1x_4 + \theta x_2x_3 + (\theta + 1)x_2x_4 = 0$ в $\mathbb{F}_8^4$, где элемент $\theta \in \mathbb{F}_8$ удовлетворяет равенству $\theta^3 = \theta^2 + 1$.

6.21. Доказать лемму 6.24 тем же способом, который применялся для доказательства леммы 6.31.

6.22. Доказать, что если f — квадратичная форма от $n \geqslant 3$ переменных над полем $\mathbb{F}_q$, то уравнение $f(x_1, \ldots, x_n) = 0$ имеет в $\mathbb{F}_q^n$ хотя бы одно нетривиальное решение. Доказать также, что условие $n \geqslant 3$ не может быть заменено условием $n \geqslant 2$.

6.23. Пусть $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — ненулевая квадратичная форма и $b \in \mathbb{F}_q$. Доказать, что уравнение $f(x_1, \ldots, x_n) = b$ имеет решение в $\mathbb{F}_q^n$, если (i) q четно

или (ii) q иечетио и ранг матрицы коэффициентов квадратичной формы f ие меньше 2.

6.24. Доказать, что две иевырожденные квадратичные формы $f, g \in \mathbb{F}_q[x_1, \ldots, x_n]$ при иечетном q эквивалентны тогда и только тогда, когда $\eta(\det(f)) = \eta(\det(g))$, где η — квадратичный характер поля $\mathbb{F}_q$. (*Указание.* Использовать лемму 6.20 и упр. 6.23).

6.25. Пусть $\mathbb{F}_q$ — коиечное поле иечетной характеристики. Доказать, что все иевырождеиные квадратичные формы $f \in \mathbb{F}_q[x_1, x_2]$, для которых уравиеиие $f(x_1, x_2) = 0$ имеет иетривиальиое решение в $\mathbb{F}_q^2$, эквивалеитны друг другу.

6.26. Пусть $\mathbb{F}_q$ — коиечное поле нечетной характеристики. Доказать, что каждая невырожденная квадратичная форма $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ при иечетном n эквивалентна квадратичной форме $x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + ax_n^2$ для иекоторого $a \in \mathbb{F}_q^*$, а при четном n эквивалентна квадратичной форме $x_1x_2 + x_3x_4 + \ldots + x_{n-3}x_{n-2} + x_{n-1}^2 + ax_n^2$ для иекоторого $a \in \mathbb{F}_q^*$.

6.27. Пусть f — невырожденная квадратичная форма над полем $\mathbb{F}_q$ нечетной характеристики от четного числа n переменных и пусть $\det(f) = \Delta$. Доказать, что для каждого нетривиального аддитивного характера χ поля $\mathbb{F}_q$ справедливо равенство

$$\sum_{c_1, \ldots, c_n \in \mathbb{F}_q} \chi(f(c_1, \ldots, c_n)) = q^{n/2}\eta((-1)^{n/2}\Delta),$$

где η — квадратичный характер поля $\mathbb{F}_q$.

6.28. Пусть условия те же, что и в упр. 6.27, только число n иечетно. Доказать, что

$$\sum_{c_1, \ldots, c_n \in \mathbb{F}_q} \chi(f(c_1, \ldots, c_n)) = q^{(n-1)/2}\eta((-1)^{(n-1)/2}\Delta)\,G(\eta, \chi),$$

где G — сумма Гаусса.

6.29. Пусть f — невырожденная квадратичная форма от нечетного числа n переменных над полем $\mathbb{F}_q$ характеристики 2. Доказать, что для каждого иетривиального аддитивного характера χ поля $\mathbb{F}_q$ справедливо равенство

$$\sum_{c_1, \ldots, c_q \in \mathbb{F}_q} \chi(f(c_1, \ldots, c_n)) = 0.$$

6.30. Пусть f — иевырожденная квадратичная форма от четного числа n переменных над полем $\mathbb{F}_q$ характеристики 2. Доказать, что если χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, то имеет место соотношение

$$\sum_{c_1, \ldots, c_n \in \mathbb{F}_q} \chi(f(c_1, \ldots, c_n)) = \varepsilon q^{n/2},$$

в котором ε принимает значение 1, если f эквивалентна квадратичной форме $x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$, и значение -1, если f эквивалентна квадратичной форме $x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2$ для некоторого $a \in \mathbb{F}_q$, такого, что $\mathrm{Tr}_{\mathbb{F}_q}(a) = 1$.

6.31. Пусть $a_0, b_0 \in \mathbb{F}_q$, где q нечетно, и пусть $a_1, \ldots, a_n \in \mathbb{F}_q^*$, $b_1, \ldots, b_n \in \mathbb{F}_q$, где $b_i \neq 0$ хотя бы для одного i, $1 \leqslant i \leqslant n$. Обозначим через N число решений в $\mathbb{F}_q^n$ системы уравиеиий

$$\begin{cases} a_1x_1^2 + \cdots + a_nx_n^2 = a_0, \\ b_1x_1 + \cdots + b_nx_n = b_0. \end{cases}$$

Положим $a = a_1 \dots a_n$, $b = b_1^2 a_1^{-1} + \dots + b_n^2 a_n^{-1}$ и $c = b_0^2 - a_0 b$. Доказать, что если $b \neq 0$ и $c = 0$, то

$$N = \begin{cases} q^{n-2}, & \text{если } n \text{ четно,} \\ q^{n-2} + q^{(n-3)/2}(q-1)\,\eta\left((-1)^{(n-1)/2} ab\right), & \text{если } n \text{ нечетно,} \end{cases}$$

где η — квадратичный характер поля $\mathbb{F}_q$.

6.32. Пусть N — число, определенное в упр. 6.31. Доказать, что если $b \neq 0$ и $c \neq 0$, то

$$N = \begin{cases} q^{n-2} + q^{(n-2)/2}\,\eta\left((-1)^{n/2} ac\right), & \text{если } n \text{ четно,} \\ q^{n-2} - q^{(n-3)/2}\,\eta\left((-1)^{(n-1)/2} ab\right), & \text{если } n \text{ нечетно.} \end{cases}$$

6.33. Пусть N то же, что и в упр. 6.31. Доказать, что если $b = c = 0$, то

$$N = \begin{cases} q^{n-2} + v(a_0)\, q^{(n-2)/2}\,\eta\left((-1)^{n/2} a\right), & \text{если } n \text{ четно,} \\ q^{n-2} + q^{(n-1)/2}\,\eta\left((-1)^{(n-1)/2} a_0 a\right), & \text{если } n \text{ нечетно,} \end{cases}$$

где v — функция, введенная определеннем 6.22.

6.34. Пусть N то же, что и в упр. 6.31. Доказать, что если $b = 0$ и $c \neq 0$, то $N = q^{n-2}$.

6.35. Пусть $\mathbb{F}_q$ — конечное поле нечетной характеристики, $a_0, b_0 \in \mathbb{F}_q$ и $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{F}_q^*$. Обозначим через N число решений в $\mathbb{F}_q^{2n}$ системы уравнений

$$\begin{cases} a_1 x_1^2 + \dots + a_n x_n^2 = a_0, \\ b_1 x_1 y_1 + \dots + b_n x_n y_n = b_0. \end{cases}$$

Положим $a = a_1 \dots a_n$. Доказать, что

$$N = \begin{cases} q^{2n-2} + (v(a_0)+1)\, v(b_0)\, q^{n-2} + \\ \quad + v(a_0)\, q^{(3n-4)/2}\,\eta\left((-1)^{n/2} a\right), & \text{если } n \text{ четно,} \\ q^{2n-1} + (v(a_0)+1)\, v(b_0)\, q^{n-2} + \\ \quad + q^{(3n-3)/2}\,\eta\left((-1)^{(n-1)/2} a_0 a\right), & \text{если } n \text{ нечетно,} \end{cases}$$

где η — квадратичный характер поля $\mathbb{F}_q$, а v — функция, введенная определеннем 6.22.

6.36. Пусть $b_1, \dots, b_n$ — различные элементы конечного поля $\mathbb{F}_q$ и $a, b \in \mathbb{F}_q$. Доказать, что число N решений в $\mathbb{F}_q^{2n}$ системы уравнений

$$\begin{cases} x_1 y_1 + \dots + x_n y_n = a, \\ b_1 x_1 y_1 + \dots + b_n x_n y_n = b \end{cases}$$

задается формулой

$$N = q^{2n-2} + q^{n-2}(q-1) \sum_{i=1}^{n} v(b - ab_i) + \\ + q^{n-2}(v(a)\, v(b) + v(a) + v(b)),$$

где v — функция, введенная определением 6.22.

6.37. Пусть $\mathbb{F}_q$ — конечное поле нечетной характеристики, $e \in \mathbb{F}_q$, и a, b, c, $d \in \mathbb{F}_q^*$. Доказать, что число N решений уравнения $ax_1^2 + bx_2^2 + cx_3^2 = 2dx_1x_2x_3 + e$ в $\mathbb{F}_q^3$ задается формулой

$$N = q^2 + 1 + q\,[\eta(a) + \eta(b) + \eta(c) + \eta(e)]\,\eta(d^2e - abc),$$

где η — квадратичный характер поля $\mathbb{F}_q$.

6.38. Пусть b — элемент конечного поля $\mathbb{F}_q$, $a_1, \ldots, a_m \in \mathbb{F}_q^*$ и $n = km$, где k, $m \in \mathbb{N}$. Доказать, что число N решений k-линейного уравнения

$$a_1x_1 \ldots x_k + a_2x_{k+1} \ldots x_{2k} + \cdots + a_mx_{n-k+1} \ldots x_n = b$$

в $\mathbb{F}_q^n$ задается формулой

$$N = q^{n-1} + v(b)\,q^{m-1}[q^{k-1} - (q-1)^{k-1}]^m,$$

где функция v вводнтся определением 6.22.

6.39. Доказать, что уравнение $x_1^3 + x_2^4 + x_3^9 = 0$ имеет q^2 решений в $\mathbb{F}_q^3$.

6.40. Доказать, что уравнение $x_1^{15} + x_2^{12} + x_3^6 + x_4^8 = 0$ имеет 1331 решение в $\mathbb{F}_{11}^4$.

6.41. Доказать непосредственно, что если НОД $(k_i, q-1) = 1$ для некоторого i, то днагональное уравнение (6.10) имеет q^{n-1} решений в $\mathbb{F}_q^n$.

6.42. Доказать, что для простого числа p, такого, что $p \equiv 1 \pmod 4$, число N решений уравнения $x_1^2 + x_2^4 = 1$ в $\mathbb{F}_p^2$ задается формулой

$$N = \begin{cases} p - 1 + 2A, & \text{если } p \equiv 1 \pmod 8, \\ p - 1 - 2A, & \text{если } p \equiv 5 \pmod 8, \end{cases}$$

где A — однозначно определенное целое число, удовлетворяющее условиям $A \equiv -1 \pmod 4$, $p = A^2 + B^2$ для некоторого $B \in Z$.

6.43. Доказать, что для $q \equiv 1 \pmod 6$ и $b \in \mathbb{F}_q^*$ число N решений уравнения $x_1^2 + x_2^3 = b$ в $\mathbb{F}_q^2$ задается формулой

$$N = q + 2\eta(b)\,\mathrm{Re}\,[\lambda(b)\,J(\eta, \lambda)],$$

где η — квадратичный характер поля $\mathbb{F}_q$, λ — мультипликативный характер этого поля порядка 3, а J — сумма Якоби.

6.44. Доказать, что для $q \equiv 1 \pmod 4$ и $b \in \mathbb{F}_q^*$ число N решений уравнения $x_1^4 + x_2^4 = b$ в $\mathbb{F}_q^2$ определяется формулой

$$N = \begin{cases} q - 3 + 2\,\mathrm{Re}\,[(2\bar{\psi}(b) + \eta(b))\,J(\eta, \psi)], & \text{если } q \equiv 1 \pmod 8, \\ q + 1 + 2\,\mathrm{Re}\,[(2\bar{\psi}(b) - \eta(b))\,J(\eta, \psi)], & \text{если } q \equiv 5 \pmod 8, \end{cases}$$

где η — квадратичный характер поля $\mathbb{F}_q$, а ψ — мультипликативный характер порядка 5 этого поля.

6.45. Пусть $\mathbb{F}_q$ — конечное поле характеристики p, $q = p^e$ и k — заданное натуральное число. Доказать, что каждый элемент поля $\mathbb{F}_q$ представим в внде суммы k-х степеней элементов этого поля в том и только том случае, если k не делится на число $(p^e - 1)/(p^d - 1)$, каким бы ни был делитель d числа e, $1 \leqslant d < e$.

6.46. Вывести нз результата упр. 6.45, что при $q > (k-1)^2$ каждый элемент поля $\mathbb{F}_q$ может быть представлен в виде суммы k-х степеней элементов этого поля.

6.47. Для целого числа $s > 1$ пусть $\beta \in E = \mathbb{F}_{q^s}$, $\beta \notin \mathbb{F}_q$. Доказать, что уравненне

$$a_1 x_1^{(q^s-1)/(q-1)} + \ldots + a_n x_n^{(q^s-1)/(q-1)} = \beta,$$

где $a_1, \ldots, a_n$ — элементы поля $\mathbb{F}_q$, не имеет решений в E^n.

6.48. Доказать, что прн $d_1 = \ldots = d_n = d$ нмеет место равенство

$$M(d_1, \ldots, d_n) = \frac{d-1}{d}[(d-1)^{n-1} - (-1)^{n-1}],$$

где $M(d_1, \ldots, d_n)$ обозначает число n-наборов $(j_1, \ldots, j_n) \in Z^n$, такнх, что $1 \leqslant j_i \leqslant d_i - 1$ для $1 \leqslant i \leqslant n$ и $(j_1/d_1) + \ldots + (j_n/d_n) \in Z$.

6.49. Доказать, что еслн число N_s определено равенством (6.15) н z — комплексная переменная, то функцня

$$\zeta(z) = \exp\left(\sum_{s=1}^{\infty} (N_s/s)\, z^s\right)$$

является рацнональной. Здесь

$$\exp(z) = \sum_{k=0}^{\infty} (1/k!)\, z^k$$

— показательная функция.

6.50. Доказать, что если N_s, $s = 1, 2, \ldots,$ — такие комплексные числа, что функцня

$$\zeta(z) = \exp\left(\sum_{s=1}^{\infty} (N_s/s)\, z^s\right)$$

рациональна, то эти числа N_s представимы формулой тнпа (6.15).

6.51. Пусть $\mathbb{F}_q$ — конечное поле нечетной характернстнкн, $b \in \mathbb{F}_q$ н $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ — невырожденная квадратнчная форма. Найтн число N_s решений уравнения $f(x_1, \ldots, x_n) = b$ в $\mathbb{F}_{q^s}^n$, где $s \in \mathbb{N}$, н провернть, что это число представнмо в виде (6.15).

6.52. Для числа N_s, определенного в упр. 6.51, найтн явное выражение функции

$$\zeta(z) = \exp\left(\sum_{s=1}^{\infty} (N_s/s)\, z^s\right)$$

в виде рациональной функции от z.

6.53. Пусть $a_1, \ldots, a_n, b \in \mathbb{F}_q$ и $N(a_1, \ldots, a_n, b)$ обозначает число решений уравнения $a_1 x_1^{k_1} + \ldots + a_n x_n^{k_n} = b$ в $\mathbb{F}_q^n$, где $k_1, \ldots, k_n$ — фнксированные натуральные числа. Доказать, что среднее значенне величины $N(a_1, \ldots, a_n, b)$ равно q^{n-1}, т. е. что

$$\frac{1}{q^{n+1}} \sum_{a_1, \ldots, a_n, b \in \mathbb{F}_q} N(a_1, \ldots a_n, b) = q^{n-1}.$$

6.54. В обозначеннях упр. 6.53 доказать, что

$$\sum_{a_1, \ldots, a_n, b \in \mathbb{F}_q} (N(a_1, \ldots, a_n, b) - q^{n-1})^2 \leqslant q^{2n-1}(q-1)\, d_1 \ldots d_n,$$

где $d_i = \text{НОД}(k_i, q-1)$ для $1 \leqslant i \leqslant n$.

6.55. Доказать, что число решений уравнения $x_1^2 + x_2^3 + x_3^5 = -2$ в $\mathbb{F}_q^3$ является положительным кратным характеристики поля $\mathbb{F}_q$.

6.56. Пусть p — характеристика поля $\mathbb{F}_q$ и число $d = \text{НОД}(k, q-1)$ делит $p-1$. Доказать, что диагональное уравнение $a_1x_1^k + \ldots + a_dx_d^k = b$ имеет решение в $\mathbb{F}_q^d$ для любых $b \in \mathbb{F}_q$ и $a_1, \ldots, a_d \in \mathbb{F}_q^*$.

6.57. Пусть p — характеристика поля $\mathbb{F}_q$, k — положительный делитель числа $p-1$ и $f \in \mathbb{F}_q[x_1, \ldots, x_k]$ — однородный многочлен степени k. Предполагая, что число решений уравнения $f(x_1, \ldots, x_k) = 0$ в $\mathbb{F}_q^k$ не делится на p, доказать, что для любого многочлена $g \in \mathbb{F}_q[x_1, \ldots, x_k]$ степени, меньшей k, уравнение $f(x_1, \ldots, x_k) = g(x_1, \ldots, x_k)$ имеет по крайней мере одно решение в $\mathbb{F}_q^k$.

6.58. Пусть p — характеристика поля $\mathbb{F}_q$, k — положительный делитель числа $p-1$ и $g \in \mathbb{F}_q[x_1, \ldots, x_k]$ — многочлен степени, меньшей k. Доказать, что уравнение $x_1 \ldots x_k = g(x_1, \ldots, x_k)$ имеет хотя бы одно решение в $\mathbb{F}_q^k$.

6.59. В условиях упр. 6.58 доказать, что уравнение $a_1x_1^k + \ldots + a_kx_k^k + ax_1 \ldots x_k = g(x_1, \ldots, x_k)$ имеет хотя бы одно решение в $\mathbb{F}_q^k$, если $a \in \mathbb{F}_q^*$, $a_1, \ldots, a_k \in \mathbb{F}_q$ и по крайней мере один из элементов a_i, $1 \leqslant i \leqslant k$, равен нулю.

6.60. Для биномиальных коэффициентов $\binom{n}{j}$, $0 \leqslant j \leqslant n$, доказать, что

$$E_p\left(\binom{n}{j}\right) = \frac{1}{p-1}(s_j + s_{n-j} - s_n),$$

где p — простое число, $E_p(r)$ — наибольший из показателей j, для которых p^j делит число $r \in \mathbb{N}$, а s_m — сумма коэффициентов p-ичного разложения числа m.

6.61. Вывести из результата упр. 6.60, что если $n = p^k$, $k \in \mathbb{N}$ и $1 \leqslant j \leqslant n$, то

$$E_p\left(\binom{n}{j}\right) = k - E_p(j).$$

6.62. Доказать, что если p — простое число, то равенство $E_p\left(\binom{n}{j}\right) = 0$ выполняется для всех j, $1 \leqslant j \leqslant n$, в том и только том случае, если число n имеет вид $n = mp^t - 1$, где $1 \leqslant m < p$ и $t \geqslant 0$.

6.63. Доказать, что натуральное число k удовлетворяет условию $\text{НОД}\left(\binom{n}{k}, k\right) = 1$ для всех n, $k \leqslant n < 2k$, в том и только том случае, если $k = p^t$ для некоторого простого числа p и $t \geqslant 0$.

6.64. Доказать, что если $\mathbb{F}_q$ — поле нечетной характеристики и $k \in \mathbb{N}$, то уравнение $y^2 = x^{2k}$ имеет $2q-1$ решений в $\mathbb{F}_q^2$. (*Указание.* Воспользоваться тем, что многочлен $y^2 - x^{2k}$ не является абсолютно неприводимым).

6.65. Доказать, что для поля $\mathbb{F}_q$, где $q \equiv 3 \pmod 8$, уравнение $y^2 = 2x^4 + 4x^2 + 2$ не имеет решений в $\mathbb{F}_q^2$. (*Указание.* Воспользоваться тем, что многочлен $y^2 - 2x^4 - 4x^2 - 2$ является неприводимым, но не абсолютно неприводимым над $\mathbb{F}_q$.)

6.66. Доказать, что если $m \in \mathbb{N}$ и $f \in \mathbb{F}_q[x]$ — такой многочлен степени $k \geqslant 1$, что $\text{НОД}(m, k) = 1$, то многочлен $y^m - f(x)$ абсолютно неприводим.

6.67. Обобщить теорему 6.57 следующим образом. Пусть $m \in \mathbb{N}$, $f \in \mathbb{F}_q[x]$ — многочлен положительной степени, и пусть

$$f(x) = a(x-\alpha_1)^{e_1} \dots (x-\alpha_d)^{e_d}$$

— разложение многочлена f в его поле разложения над $\mathbb{F}_q$, где $\alpha_1, \dots, \alpha_d$ — различные корни f. Положим $t = \text{НОД}(m, q-1)$ и $D = \text{НОД}(t, e_1, \dots, e_d)$, и пусть r — число корней α_i, принадлежащих полю $\mathbb{F}_q$. Тогда число N решений уравнения $y^m = f(x)$ в $\mathbb{F}_q^2$ удовлетворяет неравенству

$$|N - Dq + (D-1)r| \leqslant (t-D)(d-1)q^{1/2},$$

если элемент a является D-й степенью некоторого элемента из $\mathbb{F}_q^*$, и $N = r$ в противном случае.

6.68. Теорема Дирихле об одновременной аппроксимации утверждает, что для произвольных действительных чисел $t_1, \dots, t_n$ существует такой $(n+1)$-набор $(s, m_1, \dots, m_n) \in \mathbb{Z}^{n+1}$ с произвольно большим числом $s > 0$, что для всех i, $1 \leqslant i \leqslant n$, выполняется неравенство $|t_i - (m_i/s)| < s^{-(n+1)/n}$. Применить эту теорему для доказательства следующего утверждения: если $\omega_1, \dots, \omega_n$ — комплексные числа, то для любого $\varepsilon > 0$ существует бесконечно много натуральных чисел s, таких, что

$$\operatorname{Re}\left(\omega_1^s + \dots + \omega_n^s\right) \geqslant (1-\varepsilon)\left(|\omega_1|^s + \dots + |\omega_n|^s\right).$$

6.69. Дать другое доказательство леммы 6.55, использовав результат упр. 6.68.

6.70. В условиях теоремы 5.36 доказать, используя теорему 5.37, что для каждого $\varepsilon > 0$ существует бесконечно много натуральных чисел s, таких, что

$$\left|\sum_{\gamma \in \mathbb{F}_{q^s}} \chi^{(s)}(f(\gamma))\right| \geqslant (1-\varepsilon)(n-1)q^{s/2}.$$

6.71. В условиях теоремы 5.39 доказать, используя теорему 5.40, что для каждого $\varepsilon > 0$ существует бесконечно много натуральных чисел s, таких, что

$$\left|\sum_{\gamma \in \mathbb{F}_{q^s}} \psi^{(s)}(f(\gamma))\right| \geqslant (1-\varepsilon)(d-1)q^{s/2}.$$

6.72. Пусть $\mathbb{F}_q$ — конечное поле, $a_1, a_2, b_1, b_2 \in \mathbb{F}_q^*$, причем $a_1 b_2 \neq a_2 b_1$, и m, m_1, m_2 — натуральные числа. Доказать, что число N решений в $\mathbb{F}_q^3$ системы уравнений

$$\begin{cases} x_1^{m_1} = a_1 + b_1 x_3^m, \\ x_2^{m_2} = a_2 + b_2 x_3^m \end{cases}$$

удовлетворяет неравенству $|N - q| \leqslant Cq^{1/2}$, где C — некоторая константа, не зависящая от q.

6.73. Доказать, что если χ_1 — канонический аддитивный характер поля $\mathbb{F}_q$, где $q = 2^s$, то сумма Клостермана $K(\chi_1; 1, 1)$ задается формулой

$$K(\chi_1; 1, 1) = -\frac{1}{q}\left[(-1 + i\sqrt{7})^s + (-1 - i\sqrt{7})^s\right].$$

Вывести отсюда, что $|K(\chi_1; 1, 1)| \leqslant 2q^{1/2}$.

6.74. Доказать, что если E — коиечное расширение поля $\mathbb{F}_q$, то число N элементов $\gamma \in E^*$, таких, что $\mathrm{Tr}_{E/\mathbb{F}_q}(\gamma) = \mathrm{Tr}_{E/\mathbb{F}_q}(\gamma^{-1}) = 0$, задается формулой

$$N = \frac{1}{q^2} \sum_{a,\ b \in \mathbb{F}_q} K(\mu_1;\ a,\ b),$$

где μ_1 — канонический аддитивный характер поля E и K — сумма Клостермана.

6.75. Доказать, что если $E = \mathbb{F}_q$, где $q = 2^s$, то число N элементов $\gamma \in E^*$, таких, что $\mathrm{Tr}_E(\gamma) = \mathrm{Tr}_E(\gamma^{-1}) = 0$, задается формулой

$$N = \frac{1}{4}\left[q - 3 - \frac{1}{q}(-1 + i\sqrt{7})^s - \frac{1}{q}(-1 - i\sqrt{7})^s\right].$$

6.76. В условиях теоремы 5.43 доказать, используя теорему 5.44, что для каждого $\varepsilon > 0$ существует бескоиечио миого иатуральных чисел s, таких, что

$$|K(\chi^{(s)};\ a,\ b)| \geqslant (2 - \varepsilon)\, q^{s/2}.$$

ББК 22.144
Л55
УДК 512.62

Лидл Р., Нидеррайтер Г.

Л55 Конечные поля: В 2-х т. Т. 2. Пер. с англ. — М.: Мир, 1988. — 822 с.

ISBN 5-03-000066-6

Монография известиых математиков (Австралия, Австрия), отражающая многочисленные связи классического раздела алгебры — теории конечных полей — с комбиниторикой, теорией кодирования, теорией автоматов. Изложение отличается простотой и ясностью, большим числом (около 600) примеров и упражнений, имеются замечания исторического характера. Книга входит в известную энциклопедию математики и ее приложений (под редакцией Дж.-К. Роты); ряд ее томов переведен в издательствах «Мир» и «Наука».

Русское издание выходит в двух томах.

Для математиков-прикладников, инженеров-исследователей, аспирантов и студентов университетов.

Л $\frac{1702030000-274}{041\,(01)-88}$ 8—88, ч. 1 **ББК 22.144**

Редакция литературы по математическим наукам

ISBN 5-03-000066-6 (русск.)
ISBN 5-03-000064-X
ISBN 0-201-13519-1 (англ.)

© Cambridge University Press 1985
This book originally published in the English language by Cambridge University Press of Cambridge, England
© перевод на русский язык, с дополнениями, «Мир», 1988

Глава 7

Перестановочные многочлены

Задача этой главы — дать обзор результатов о перестановочных многочленах, т. е. таких многочленах, для которых соответствующие полиномиальные функции являются перестановками множества элементов данного конечного поля $\mathbb{F}_q$. Многочлены такого вида существуют для любого $\mathbb{F}_q$, так как любое отображение поля $\mathbb{F}_q$ в себя можно задать с помощью некоторого многочлена.

С перестановочными многочленами связан ряд естественных вопросов. Во-первых, само выяснение того, является данный многочлен перестановочным или нет, представляет собой нетривиальную задачу. Критерии, полученные в § 1, могут эту задачу упростить. Однако общие условия для того, чтобы многочлен был перестановочным, оказываются достаточно сложными. Поэтому большой интерес представляют полученные в § 2 результаты о некоторых типах перестановочных многочленов.

Перестановочные многочлены индуцируют перестановки элементов конечного поля $\mathbb{F}_q$ и, следовательно, соответствуют элементам симметрической группы S_q — группы всех подстановок на множестве из q элементов. Таким образом, если нам дан класс перестановочных многочленов поля $\mathbb{F}_q$, замкнутый относительно операции композиции (или композиции с последующим приведением по модулю $x^q - x$), то мы можем поставить вопрос, какая подгруппа группы S_q представлена этим классом. § 3 посвящен исследованию такого рода задач.

Связь между перестановочными и исключительными многочленами исследуется в § 4. При этом существенно применяется теория уравнений над конечными полями.

Понятие перестановочного многочлена обобщается в § 5 путем перехода к рассмотрению многочленов от нескольких переменных. Так как отдельные многочлены от $n \geqslant 2$ переменных не могут индуцировать отображения векторного пространства $\mathbb{F}_q^n$ в себя, то здесь теряется связь многочленов с перестановками. Чтобы восстановить эту связь, необходимо рассматривать системы многочленов. Это приводит к понятию ортогональной системы многочленов. Далее в этом параграфе изучаются основные свойства перестановочных многочленов от нескольких переменных, а также ортогональных систем.

§ 1. Критерии перестановочности многочленов

Многочлен $f \in \mathbb{F}_q[x]$ называется *перестановочным многочленом* поля $\mathbb{F}_q$, если соответствующая ему полиномиальная функция $f: \mathbb{F}_q \to \mathbb{F}_q$, отображающая элемент $c \in \mathbb{F}_q$ в элемент $f(c) \in \mathbb{F}_q$, является перестановкой элементов поля $\mathbb{F}_q$. Очевидно, что если f является перестановочным многочленом поля $\mathbb{F}_q$, то для каждого $a \in \mathbb{F}_q$ уравнение $f(x) = a$ имеет ровно одно решение в поле $\mathbb{F}_q$. Ввиду конечности поля $\mathbb{F}_q$ перестановочные многочлены над ним могут быть определены и другими способами.

7.1. Лемма. *Многочлен $f \in \mathbb{F}_q[x]$ является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда выполняется одно из следующих условий:*

(i) *функция $f: c \mapsto f(c)$, $c \in \mathbb{F}_q$, является отображением «на»;*

(ii) *функция $f: c \mapsto f(c)$, $c \in \mathbb{F}_q$, является взаимно однозначным отображением;*

(iii) *для любого $a \in \mathbb{F}_q$ уравнение $f(x) = a$ имеет решение в поле $\mathbb{F}_q$;*

(iv) *для любого $a \in \mathbb{F}_q$ уравнение $f(x) = a$ имеет ровно одно решение в поле $\mathbb{F}_q$.*

Если $\varphi: \mathbb{F}_q \to \mathbb{F}_q$ — произвольная функция, отображающая $\mathbb{F}_q$ в $\mathbb{F}_q$, то существует единственный многочлен $g \in \mathbb{F}_q[x]$, $\deg(g) < q$, являющийся представлением отображения φ в том смысле, что $g(c) = \varphi(c)$ для всех $c \in \mathbb{F}_q$. Многочлен g можно найти, вычислив соответствующий интерполяционный многочлен Лагранжа (см. теорему 1.71), или с помощью формулы

$$g(x) = \sum_{c \in \mathbb{F}_q} \varphi(c)\,(1 - (x - c)^{q-1}). \tag{7.1}$$

Если отображение φ задано в виде полиномиальной функции, например $\varphi: c \mapsto f(c)$, $c \in \mathbb{F}_q$, для некоторого $f \in \mathbb{F}_q[x]$, то искомый многочлен g может быть получен из многочлена f приведением последнего по модулю $x^q - x$ [1]) согласно следующему результату:

7.2. Лемма. *Если f, $g \in \mathbb{F}_q[x]$, то $f(c) = g(c)$ для всех $c \in \mathbb{F}_q$ в том и только том случае, когда $f(x) \equiv g(x) \pmod{(x^q - x)}$.*

Доказательство. Согласно алгоритму деления многочленов, мы можем записать $f(x) - g(x) = h(x)(x^q - x) + r(x)$, где h, $r \in \mathbb{F}_q[x]$ и $\deg(r) < q$. Тогда $f(c) = g(c)$ для всех $c \in \mathbb{F}_q$ в том и только том случае, если $r(c) = 0$ для всех $c \in \mathbb{F}_q$; последнее эквивалентно тому, что $r = 0$. □

---

[1]) Результат приведения многочлена f по модулю $x^q - x$ (см. определение на стр. 40) обозначается через $f \pmod{(x^q - x)}$. — *Прим. перев.*

Установим теперь один полезный критерий того, что данный многочлен является перестановочным. Нам потребуется следующая лемма.

7.3. **Лемма.** *Пусть* $a_0, a_1, \ldots, a_{q-1}$ — *элементы поля* $\mathbb{F}_q$. *Тогда следующие два условия эквивалентны*:

(i) $a_0, a_1, \ldots, a_{q-1}$ *все различны*;

(ii) $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 \text{ для } t = 0, 1, \ldots, q-2, \\ -1 \text{ для } t = q-1. \end{cases}$

Доказательство. Для фиксированного i, такого, что $0 \leqslant i \leqslant q-1$, рассмотрим многочлен

$$g_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j.$$

Тогда, полагая $0^0 = 1$, получаем, что $g_i(a_i) = 1$ и $g_i(b) = 0$ для всех $b \in \mathbb{F}_q$, $b \neq a_i$. Следовательно, многочлен

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = -\sum_{j=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-j} \right) x^j$$

отображает каждый элемент поля $\mathbb{F}_q$ в 1 тогда и только тогда, когда $\{a_0, a_1, \ldots, a_{q-1}\} = \mathbb{F}_q$. Так как $\deg(g) < q$, из леммы 7.2 следует, что многочлен g отображает каждый элемент поля $\mathbb{F}_q$ в 1 тогда и только тогда, когда $g(x) = 1$, что эквивалентно условию (ii). □

7.4. **Теорема** (критерий Эрмита). *Пусть* p — *характеристика поля* $\mathbb{F}_q$. *Тогда многочлен* $f \in \mathbb{F}_q[x]$ *является перестановочным многочленом поля* $\mathbb{F}_q$ *в том и только том случае, если выполняются следующие два условия*:

(i) *многочлен* f *имеет ровно один корень в* $\mathbb{F}_q$;

(ii) *для каждого целого* t, *такого, что* $1 \leqslant t \leqslant q-2$ *и* $t \not\equiv 0 \pmod{p}$, *результат приведения многочлена* $f(x)^t$ *по модулю* $x^q - x$ *имеет степень* $d \leqslant q-2$.

Доказательство. Пусть f — перестановочный многочлен поля $\mathbb{F}_q$. Тогда необходимость условия (i) очевидна. Приводя многочлен $f(x)^t$ по модулю $x^q - x$, получаем некоторый многочлен $\sum_{j=0}^{q-1} b_j^{(t)} x^j$, где $b_{q-1}^{(t)} = -\sum_{c \in \mathbb{F}_q} f(c)^t$ по (7.1). По лемме 7.3 $b_{q-1}^{(t)} = 0$ для всех $t = 1, 2, \ldots, q-2$, откуда следует условие (ii).

Обратно, пусть выполняются условия (i) и (ii). Тогда из условия (i) следует, что $\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = -1$, в то время как из условия

(ii) получаем, что $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ для всех t, $t \not\equiv 0 \pmod{p}$, $1 \leqslant t \leqslant q-2$. Из равенства

$$\sum_{c\in\mathbb{F}_q} f(c)^{tp^j} = \left(\sum_{c\in\mathbb{F}_q} f(c)^t\right)^{p^j}$$

получаем, что $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ для всех $1 \leqslant t \leqslant q-2$; в то же время для $t = 0$ это равенство очевидно. Тогда из леммы 7.3 следует, что f является перестановочным многочленом поля $\mathbb{F}_q$. □

7.5. Следствие. *Если число $d > 1$ является делителем числа $q-1$, то над полем $\mathbb{F}_q$ не существует перестановочного многочлена степени d.*

Доказательство. Если $f \in \mathbb{F}_q[x]$ и $\deg f = d$, то $\deg\left(f^{(q-1)/d}\right) = q-1$, и тогда для $t = (q-1)/d$ условие (ii) теоремы 7.4 не выполняется. □

Из доказательства теоремы 7.4 очевидно, что если многочлен $f \in \mathbb{F}_q[x]$ является перестановочным многочленом поля $\mathbb{F}_q$, то условие (ii) теоремы 7.4 выполняется и без ограничения $t \not\equiv 0 \pmod{p}$. Условие же (i) может быть заменено другими, например, как в следующей теореме.

7.6. Теорема. *Пусть поле $\mathbb{F}_q$ имеет характеристику p. Тогда многочлен $f \in \mathbb{F}_q[x]$ является перестановочным многочленом поля $\mathbb{F}_q$ в том и только том случае, если выполняются следующие два условия:*

(i) *многочлен $f(x)^{q-1} \pmod{(x^q - x)}$ имеет степень $q-1$;*

(ii) *для любого целого t, где $1 \leqslant t \leqslant q-2$ и $t \not\equiv 0 \pmod{p}$, многочлен $f(x)^t \pmod{(x^q - x)}$ имеет степень $d \leqslant q-2$.*

Доказательство. Необходимость условия (ii) следует из теоремы 7.4. В обозначениях, используемых при доказательстве этой теоремы, получаем, что

$$b_{q-1}^{(q-1)} = -\sum_{c\in\mathbb{F}_q} f(c)^{q-1}.$$

Тогда если f — перестановочный многочлен поля $\mathbb{F}_q$, то $b_{q-1}^{(q-1)} = 1$, и, таким образом, условие (i) выполняется.

Обратно, пусть условия (i) и (ii) выполняются. Тогда, как и в доказательстве теоремы 7.4, из условия (ii) следует, что $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ для всех $0 \leqslant t \leqslant q-2$, в то время как из условия

(i) вытекает, что $\sum_{c \in \mathbb{F}_q} f(c)^{q-1} \neq 0$. Таким образом, многочлен

$$g(x) = -\sum_{j=0}^{q-1} \left(\sum_{c \in \mathbb{F}_q} f(c)^{q-1-j} \right) x^j$$

является ненулевым и постоянным. Если бы многочлен f не являлся перестановочным многочленом поля $\mathbb{F}_q$, то, рассуждая аналогично тому, как мы рассуждали при доказательстве леммы 7.3, можно было бы показать, что $g(b) = 0$ для некоторого $b \in \mathbb{F}_q$, что невозможно. □

Еще один критерий того, что данный многочлен является перестановочным многочленом, можно получить, используя понятие аддитивного характера конечного поля (см. § 1 гл. 5).

7.7. Теорема. *Многочлен $f \in \mathbb{F}_q[x]$ является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = 0 \tag{7.2}$$

для любого нетривиального аддитивного характера χ поля $\mathbb{F}_q$.

Доказательство. Если f — перестановочный многочлен поля $\mathbb{F}_q$, а χ — нетривиальный аддитивный характер этого поля, то по формуле (5.9)

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \sum_{c \in \mathbb{F}_q} \chi(c) = 0.$$

Обратно, если через χ_0 обозначить тривиальный аддитивный характер поля $\mathbb{F}_q$ и считать, что равенство (7.2) выполняется для всех $\chi \neq \chi_0$, то для любого $a \in \mathbb{F}_q$ число N решений уравнения $f(x) = a$ в поле $\mathbb{F}_q$ определяется в силу (5.10) равенством

$$N = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \sum_{\chi} \chi(f(c)) \overline{\chi(a)} = 1 + \frac{1}{q} \sum_{\chi \neq \chi_0} \overline{\chi(a)} \sum_{c \in \mathbb{F}_q} \chi(f(c)) = 1.$$

Следовательно, многочлен f является перестановочным многочленом поля $\mathbb{F}_q$. □

§ 2. Примеры перестановочных многочленов

Несколько простых примеров перестановочных многочленов можно получить с помощью следующих элементарных результатов.

7.8. Теорема. (i) *Каждый линейный многочлен над полем $\mathbb{F}_q$ является перестановочным многочленом поля $\mathbb{F}_q$.*

(ii) *Одночлен x^n является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда* НОД $(n, q-1) = 1$.

Доказательство. (i) очевидно. (ii) Одночлен x^n является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда отображение $f\colon c \mapsto c^n$, $c \in \mathbb{F}_q$, является отображением «на», а это имеет место тогда и только тогда, когда НОД $(n, q-1) = 1$ (надо использовать теорему 1.15 (ii)). □

7.9. Теорема. *Пусть $\mathbb{F}_q$ — поле характеристики p. Тогда p-многочлен*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$$

является перестановочным многочленом поля $\mathbb{F}_q$ в том и только том случае, если многочлен $L(x)$ имеет в поле $\mathbb{F}_q$ единственный корень, равный 0.

Доказательство. Из рассуждений, приведенных после определения 3.49, следует, что функция $L\colon c \mapsto L(c)$, $c \in \mathbb{F}_q$, является линейным оператором в $\mathbb{F}_q$ (рассматриваемом как векторное пространство над полем $\mathbb{F}_p$). Тогда отображение L является взаимно однозначным в том и только том случае, если многочлен $L(x)$ имеет в поле $\mathbb{F}_q$ единственный корень, равный 0. □

Другие примеры перестановочных многочленов можно получить из приведенных выше результатов, если воспользоваться тем, что множество перестановочных многочленов замкнуто относительно операции композиции (т. е. если $f(x)$ и $g(x)$ — перестановочные многочлены поля $\mathbb{F}_q$, то $f(g(x))$ также является перестановочным многочленом поля $\mathbb{F}_q$). Получаемый при этом класс перестановочных многочленов описывается следующей теоремой.

7.10. Теорема. *Пусть $\mathbb{F}_q$ — конечное поле, $r \in \mathbb{N}$, НОД $(r, q-1) = 1$, и пусть s — положительный делитель числа $q-1$. Пусть, далее, $g(x) \in \mathbb{F}_q[x]$ — такой многочлен над полем $\mathbb{F}_q$, что многочлен $g(x^s)$ не имеет ненулевых корней в поле $\mathbb{F}_q$. Тогда многочлен $f(x) = x^r (g(x^s))^{(q-1)/s}$ является перестановочным многочленом поля $\mathbb{F}_q$.*

Доказательство. Покажем, что многочлен $f(x)$ удовлетворяет условиям теоремы 7.4. Условие (i) выполняется очевидным образом. Чтобы доказать (ii), возьмем $t \in \mathbb{Z}$, $1 \leqslant t \leqslant q-2$, и предположим сначала, что t не делится на s. Заметим, что $f(x)^t$ представляет собой сумму членов, показатели степени которых имеют вид $rt + ms$, где $m \in \mathbb{Z}$, $m \geqslant 0$. Так как НОД $(r, s) = 1$, эти показатели степени не делятся на s и, следовательно, не делятся на $q-1$. Тогда степень многочлена $f(x)^t \pmod{x^q - x}$ не превышает $q-2$. Если t делится на s, скажем $t = ks$, где $k \in \mathbb{N}$, то

$$f(x)^t = x^{rt} (g(x^s))^{(q-1)k}.$$

Если положить $h(x) = x^{rt}$, то, так как $g(c^s) \neq 0$ для всех $c \in \mathbb{F}_q^*$, мы получаем, что $f(c)^t = h(c)$; кроме того, $f(0)^t = h(0)$. Тогда по лемме 7.2 $f(x)^t \equiv x^{rt} \pmod{(x^q - x)}$, и так как rt не делится на $q - 1$, многочлен $f(x)^t \pmod{(x^q - x)}$ является многочленом степени, не большей чем $q - 2$. □

Из замечания, сделанного после теоремы 7.9, следует, в частности, что если $f \in \mathbb{F}_q[x]$ — перестановочный многочлен поля $\mathbb{F}_q$ и $b, c, d \in \mathbb{F}_q$, $c \neq 0$, то $f_1(x) = cf(x + b) + d$ также является перестановочным многочленом поля $\mathbb{F}_q$. Выбирая соответствующим образом константы b, c, d, можно получить многочлен $f_1(x)$ в *нормализованной форме*. Последнее означает, что $f_1(x)$ является нормированным многочленом и при этом $f_1(0) = 0$ и, если степень n многочлена $f_1(x)$ не делится на характеристику поля $\mathbb{F}_q$, то коэффициент при x^{n-1} равен 0. Таким образом, можно ограничиться изучением нормализованных перестановочных многочленов. Пользуясь критерием Эрмита, можно получить все нормализованные перестановочные многочлены произвольной фиксированной степени. Полный список таких многочленов степени не выше 5 приводится в табл. 7.1.

Таблица 7.1

Нормализованные перестановочные многочлены поля $\mathbb{F}_q$		q
x		q любое
x^2		$q \equiv 0 \pmod 2$
x^3		$q \not\equiv 1 \pmod 3$
$x^3 - ax$	(a — не квадрат)	$q \equiv 0 \pmod 3$
$x^4 \pm 3x$		$q = 7$
$x^4 + a_1x^2 + a_2x$	(если он имеет в $\mathbb{F}_q$ единственный корень, равный 0)	$q \equiv 0 \pmod 2$
x^5		$q \not\equiv 1 \pmod 5$
$x^5 - ax$	(a не является четвертой степенью)	$q \equiv 0 \pmod 5$
$x^5 + ax$	($a^2 = 2$)	$q = 9$
$x^5 \pm 2x^2$		$q = 7$
$x^5 + ax^3 \pm x^2 + 3a^2x$	(a — не квадрат)	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$	(a — произвольный элемент)	$q \equiv \pm 2 \pmod 5$
$x^5 + ax^3 + 3a^2x$	(a — не квадрат)	$q = 13$
$x^5 - 2ax^3 + a^2x$	(a — не квадрат)	$q \equiv 0 \pmod 5$

Для нечетных q мы можем охарактеризовать перестановочные многочлены поля $\mathbb{F}_q$ вида $x^{(q+1)/2} + ax$. Для этого обозначим через η квадратичный характер поля $\mathbb{F}_q$, удовлетворяющий стандартному условию $\eta(0) = 0$.

7.11. Теорема. *Для нечетного q многочлен $x^{(q+1)/2} + ax \in \mathbb{F}_q[x]$ является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда $\eta(a^2 - 1) = 1$.*

Доказательство. Пусть $f(x) = x^{(q+1)/2} + ax$. Покажем, что соответствующее отображение f не является взаимно однозначным тогда и только тогда, когда $\eta(a^2 - 1) \neq 1$. Если для некоторого $c \in \mathbb{F}_q^*$ выполняется равенство $f(c) = f(0) = 0$, то $a = -c^{(q-1)/2}$ и, следовательно, $\eta(a^2 - 1) = 0$. Если найдутся элементы $b, c \in \mathbb{F}_q^*$, $b \neq c$, для которых $f(b) = f(c) \neq 0$, то

$$bc^{-1} = (a + c^{(q-1)/2})(a + b^{(q-1)/2})^{-1}.$$

Если $\eta(b) = \eta(c)$, то $b^{(q-1)/2} = c^{(q-1)/2}$ и, следовательно, $b = c$, что противоречит выбору $b \neq c$. Таким образом, $\eta(b) \neq \eta(c)$. Не теряя общности, можно считать, что $\eta(b) = -1$, $\eta(c) = 1$. Тогда $b^{(q-1)/2} = -1$, $c^{(q-1)/2} = 1$, откуда

$$-1 = \eta(bc^{-1}) = \eta((a+1)(a-1)^{-1}) = \\ = \eta((a+1)(a-1)) = \eta(a^2 - 1).$$

Обратно, предположим, что $\eta(a^2 - 1) \neq 1$, тогда или $a^2 - 1 = 0$, или $\eta(a^2 - 1) = -1$. В первом случае получаем, что $a = \pm 1$, а тогда найдется такой элемент $c \in \mathbb{F}_q^*$, для которого $c^{(q-1)/2} = -a$. Отсюда следует, что $f(c) = f(0)$. Если же $\eta(a^2 - 1) = -1$, положим $b = (a+1)(a-1)^{-1}$. Тогда $\eta(b) = -1$, и, таким образом, $b^{(q-1)/2} = -1$, а следовательно,

$$f(b) = (a + b^{(q-1)/2})\, b = (a-1)\, b = a + 1 = f(1),$$

где $b \neq 1$. В обоих случаях f не является взаимно однозначным отображением. □

7.12. Замечание. Покажем, что $\eta(a^2 - 1) = 1$ тогда и только тогда, когда

$$a = (c^2 + 1)(c^2 - 1)^{-1}$$

для некоторого элемента $c \in \mathbb{F}_q^*$, $c^2 \neq 1$. В самом деле, если $\eta(a^2 - 1) = 1$, то $a^2 - 1 = b^2$ для некоторого $b \in \mathbb{F}_q^*$. Отсюда, если $c = (a+1)\, b^{-1}$, мы получаем, что $c \neq 0$, $c^2 \neq 1$ и

$$(c^2 + 1)(c^2 - 1)^{-1} = [(a+1)^2 + b^2][(a+1)^2 - b^2]^{-1} = a.$$

Обратно, если $a = (c^2 + 1)(c^2 - 1)^{-1}$, $c \in \mathbb{F}_q^*$, $c^2 \neq 1$, то $a^2 - 1 = 4c^2 (c^2 - 1)^{-2}$ и, следовательно, $\eta(a^2 - 1) = 1$. □

7.13. Теорема. *Если $a \in \mathbb{F}_q^*$, где q нечетно, то многочлен $x^{(q+1)/2} + ax$ не является перестановочным многочленом ни для какого поля $\mathbb{F}_{q^r}$ с $r > 1$.*

Доказательство. Если r четно, то результат вытекает из следствия 7.5. Если r нечетно, то, полагая $m = (q-1)/2$, получаем, что $q^r \equiv -1 \pmod{(m+1)}$, т. е. что $q^r = k(m+1) + m$ для некоторого $k \in \mathbb{N}$. Заметим, что из соотношения $k(m+1) \equiv m+1 \pmod{q}$ и того, что НОД $(m+1, q) = 1$, следует, что $k \equiv 1 \pmod{q}$. В силу теоремы 7.4 достаточно показать, что многочлен

$$(x^{m+1} + ax)^{k+m-1},$$

приведенный по модулю $x^{q^r} - x$, имеет степень $q^r - 1$. В самом деле,

$$(x^{m+1} + ax)^{k+m-1} = \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{(m+1)(k+m-j-1)+j} =$$

$$= \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{q^r+m^2-m-1-jm}.$$

Для $j \geqslant m$ соответствующие показатели степени переменной x не превосходят $q^r - 2$. Как нетрудно заметить, при $j \leqslant m-2$ соответствующие показатели степени x не меньше, чем q^r, но и не больше, чем $2q^r - 3$. Таким образом, после приведения этих членов по модулю $x^{q^r} - x$ мы получим одночлены степени, не превосходящей $q^r - 2$. Остается член, соответствующий $j = m-1$ и равный

$$\binom{k+m-1}{m-1} a^{m-1} x^{q^r-1}.$$

В этом случае достаточно показать, что указанный выше биномиальный коэффициент не делится на характеристику p поля $\mathbb{F}_q$. Если через s_n обозначить сумму цифр в p-ичном представлении числа n, то из соотношений $k \equiv 1 \pmod{q}$, $m < q$ и $m \not\equiv 0 \pmod{p}$ следует, что $s_{k+m-1} = s_{m-1} + s_k$, и тогда по лемме 6.39 получаем, что

$$E_p\left(\binom{k+m-1}{m-1}\right) = \frac{1}{p-1}(s_{m-1} + s_k - s_{k+m-1}) = 0,$$

откуда следует утверждение теоремы. □

Теорема 7.13 наводит на мысль о том, что многочлены над полем $\mathbb{F}_q$, являющиеся перестановочными для *всех* конечных расширений поля $\mathbb{F}_q$, встречаются, по-видимому, достаточно редко. На самом деле многочлены с таким свойством имеют очень специальный вид, и их можно полностью описать.

7.14. Теорема. *Многочлен $f(x) \in \mathbb{F}_q[x]$ является перестановочным многочленом для всех конечных расширений поля $\mathbb{F}_q$ тогда и только тогда, когда его можно представить в виде $f(x) = ax^{p^h} + b$, где $a \neq 0$, p — характеристика поля $\mathbb{F}_q$, а h — некоторое неотрицательное целое число.*

Доказательство. Достаточность непосредственно следует из теоремы 7.8 и замечания к теореме 7.9. Для того чтобы доказать необходимость, заметим сначала, что если f — перестановочный многочлен поля $\mathbb{F}_q$, то для любого $c \in \mathbb{F}_q$ уравнение $f(x) = c$ имеет единственное решение $d \in \mathbb{F}_q$. Тогда

$$f(x) - c = (x - d)^k g(x),$$

где $k \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$ и либо $\deg(g) = 0$, либо g является произведением неприводимых многочленов $g_i \in \mathbb{F}_q[x]$, $\deg(g_i) \geqslant 2$. Если для некоторого i число r делится на $\deg(g_i)$, то g_i имеет корень в $\mathbb{F}_{q^r}$ и, следовательно, f не является перестановочным многочленом поля $\mathbb{F}_{q^r}$. Таким образом, должно выполняться равенство

$$f(x) - c = a(x - d)^k, \quad a \neq 0, \tag{7.3}$$

т. е. для любого $c \in \mathbb{F}_q$ найдется элемент $d \in \mathbb{F}_q$, зависящий от c, такой, что выполняется (7.3). Беря $c = 0$ и $c = 1$, получаем

$$a(x - d_0)^k - a(x - d_1)^k = 1.$$

Заменяя x на $x + d_1$, приходим к равенству

$$a(x + d_1 - d_0)^k - ax^k = 1.$$

Применяя формулу бинома, получаем

$$\binom{k}{j} \equiv 0 \pmod{p}, \quad 0 < j < k. \tag{7.4}$$

Число k удовлетворяет неравенствам $p^h \leqslant k < p^{h+1}$ для некоторого $h \in \mathbb{Z}$, $h \geqslant 0$. Если $k \neq p^h$, то, полагая $j = p^h$, из леммы 6.39 получаем

$$E_p\left(\binom{k}{j}\right) = \frac{1}{p-1}(s_j + s_{k-j} - s_k) = 0,$$

где s_n обозначает сумму цифр в p-ичном представлении числа n. Так как последнее соотношение находится в противоречии с (7.4), получаем, что $k = p^h$. Утверждение теоремы следует теперь из формулы (7.3). □

7.15. Следствие. *Если многочлен $f(x) \in \mathbb{F}_q[x]$ нельзя представить в виде $ax^{p^h} + b$, то существует бесконечно много расширений $\mathbb{F}_{q^r}$ поля $\mathbb{F}_q$, таких, что $f(x)$ не является перестановочным многочленом поля $\mathbb{F}_{q^r}$.*

Доказательство. Если f не является перестановочным многочленом поля $\mathbb{F}_q$, то он не может быть перестановочным многочленом ни для какого поля вида $\mathbb{F}_{q^r}$, $r \in \mathbb{N}$. Если же f — перестановочный многочлен поля $\mathbb{F}_q$, то доказываемый результат можно извлечь из доказательства теоремы 7.14. □

Введем теперь специальный класс многочленов, называемых многочленами Диксона. Они обладают некоторыми интересными свойствами и являются новыми примерами перестановочных многочленов. Пусть x_1, x_2 — переменные и $k \in \mathbb{N}$. Тогда, как мы видели при доказательстве теоремы 5.46, из формулы Варинга следует, что

$$x_1^k + x_2^k = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-x_1x_2)^j (x_1 + x_2)^{k-2j}. \tag{7.5}$$

Это равенство выполняется для любого коммутативного кольца R с единицей. Если $a \in R$, то определим *многочлен Диксона* $g_k(x, a)$ над кольцом R формулой

$$g_k(x, a) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}. \tag{7.6}$$

Если перейти к полю комплексных чисел, то определенные выше многочлены оказываются самым тесным образом связанными с хорошо известными многочленами Чебышёва первого рода $T_k(x) = \cos(k \arccos x)$. В самом деле, если мы в (7.5) положим $x_1 = e^{i\theta}$, $x_2 = e^{-i\theta}$, то из (7.6) вытекает, что $2\cos k\theta = g_k(2\cos\theta, 1)$ и, следовательно,

$$g_k(2x, 1) = 2T_k(x). \tag{7.7}$$

В силу этой связи многочлены Диксона иногда тоже называют *многочленами Чебышёва*. Тождество (7.7) можно использовать для определения многочленов Чебышёва первого рода $T_k(x)$ над любым конечным полем характеристики, отличной от 2.

Рассмотрим многочлен Диксона $g_k(x, a)$ над полем F. Тогда в поле рациональных функций над F справедливо равенство

$$g_k\left(y + \frac{a}{y}, a\right) = y^k + \frac{a^k}{y^k}, \tag{7.8}$$

которое получается из (7.5) в результате подстановки $x_1 = y$, $x_2 = a/y$. Из определения многочленов Диксона также следует формула

$$g_k(x, ab^2) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j b^k b^{-(k-2j)} x^{k-2j} = b^k g_k(b^{-1}x, a), \tag{7.9}$$

которая справедлива для любых $a, b \in F$, $b \neq 0$. Следовательно, если $F = \mathbb{F}_q$, где q четно, то любой многочлен Диксона $g_k(x, a)$, $a \in \mathbb{F}_q^*$, может быть выражен через $g_k(x, 1)$. Если же $F = \mathbb{F}_q$, где q нечетно, то каждый многочлен Диксона $g_k(x, a)$, $a \in \mathbb{F}_q^*$, можно выразить как через $g_k(x, 1)$, так и через $g_k(x, c)$, где c — произвольный фиксированный элемент поля $\mathbb{F}_q$, не являющийся квадратом. Для нечетного q в соответствии с формулой (7.7) многочлены Диксона $g_k(x, a)$ можно также выразить через многочлены Чебышёва первого рода $T_k(x)$. В самом деле, если элемент $\beta \in \mathbb{F}_{q^2}$ таков, что $\beta^2 = a$, то из (7.7) и (7.9) следует, что

$$g_k(x, a) = \beta^k g_k(\beta^{-1}x, 1) = 2\beta^k T_k((2\beta)^{-1}x).$$

Как правило, случай $a = 0$ не представляет большого интереса в силу того, что $g_k(x, 0) = x^k$.

7.16. Теорема. *Многочлен Диксона $g_k(x, a)$, $a \in \mathbb{F}_q^*$, является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда* НОД $(k, q^2 - 1) = 1$.

Доказательство. Предположим, что для некоторых $b, c \in \mathbb{F}_q$ выполняется равенство $g_k(b, a) = g_k(c, a)$. В этом случае мы можем найти такие $\beta, \gamma \in \mathbb{F}_{q^2}^*$, что $\beta + \alpha\beta^{-1} = b$, $\gamma + a\gamma^{-1} = c$. Тогда из (7.8) вытекает равенство $\beta^k + a^k\beta^{-k} = \gamma^k + a^k\gamma^{-k}$; следовательно, $(\beta^k - \gamma^k)(\beta^k\gamma^k - a^k) = 0$, откуда $\beta^k = \gamma^k$ или $\beta^k = (a\gamma^{-1})^k$. Если теперь НОД $(k, q^2 - 1) = 1$, то по теореме 7.8 (ii) многочлен x^k является перестановочным многочленом поля $\mathbb{F}_{q^2}$. При этом $\beta = \gamma$ или $\beta = a\gamma^{-1}$. В обоих случаях получаем, что $b = c$, т. е. что $g_k(x, a)$ — перестановочный многочлен поля $\mathbb{F}_q$.

Предположим теперь, что НОД $(k, q^2 - 1) = d > 1$. Если d четно, то q нечетно, а k четно. Из (7.6) следует, что $g_k(x, a)$ содержит только четные степени x, поэтому $g_k(c, a) = g_k(-c, a)$ для всех $c \in \mathbb{F}_q^*$, $c \neq -c$. Следовательно, $g_k(x, a)$ не является перестановочным многочленом поля $\mathbb{F}_q$. Если d нечетно, то существует нечетное простое число r, делящее d. Тогда r делит k, и, значит, или $q - 1$, или $q + 1$ делится на r. Рассмотрим эти два случая по отдельности. В первом случае уравнение $x^r = 1$ имеет r решений в поле $\mathbb{F}_q$, т. е. существует элемент $b \in \mathbb{F}_q$, $b \neq 1, a$, для которого $b^r = 1$. Тогда $b^k = 1$ и из (7.8) следует, что

$$g_k(b + ab^{-1}, a) = 1 + a^k = g_k(1 + a, a).$$

Так как из равенства $b + ab^{-1} = 1 + a$ вытекает, что или $b = 1$, или $b = a$, то мы получаем соотношение $b + ab^{-1} \neq 1 + a$. Следовательно, $g_k(x, a)$ не является перестановочным многочленом поля $\mathbb{F}_q$. Во втором случае пусть $\gamma \in \mathbb{F}_{q^2}$ — решение уравнения $x^{q+1} = a$. Так как уравнение $x^r = 1$ имеет r решений в поле $\mathbb{F}_{q^2}$, то найдется элемент $\beta \in \mathbb{F}_{q^2}$, $\beta \neq 1$, $a\gamma^{-2}$, удовлетворяющий

равенству $\beta^r = 1$. Кроме того, $\beta^{q+1} = 1$ и $\beta^k = 1$. Значит, в силу (7.8)

$$g_k(\gamma + a\gamma^{-1}, a) = g_k(\beta\gamma + a(\beta\gamma)^{-1}, a).$$

Далее, справедливы соотношения $\gamma + a\gamma^{-1} = \gamma + \gamma^q \in \mathbb{F}_q$ и $\beta\gamma + a(\beta\gamma)^{-1} = \beta\gamma + (\beta\gamma)^q \in \mathbb{F}_q$, а также $\beta\gamma + a(\beta\gamma)^{-1} \neq \gamma + a\gamma^{-1}$, поскольку иначе $\beta = 1$ или $\beta = a\gamma^{-2}$. Таким образом, $g_k(x, a)$ опять не является перестановочным многочленом поля $\mathbb{F}_q$. □

7.17. **Следствие.** *Если* $a \in \mathbb{F}_q^*$ *и* НОД $(k, q^2 - 1) = 1$, *то*

$$\sum_{c \in \mathbb{F}_q} \chi(g_k(c, a)) = 0$$

для любого нетривиального аддитивного или мультипликативного характера χ *поля* $\mathbb{F}_q$.

Доказательство. Так как по теореме 7.16 многочлен $g_k(x, a)$ является перестановочным многочленом поля $\mathbb{F}_q$, то

$$\sum_{c \in \mathbb{F}_q} \chi(g_k(c, a)) = \sum_{c \in \mathbb{F}_q} \chi(c),$$

и тогда этот результат следует из формулы (5.9) или из (5.37). □

Суммы значений характеров, появляющиеся в следствии 7.17, в случае, когда χ — квадратичный характер поля $\mathbb{F}_q$, q нечетно, а $k \in \mathbb{N}$ — произвольное число, подробно изучались и получили название *сумм Бревера* (см. также комментарии к § 5 гл. 5).

В последнем параграфе настоящей главы мы рассмотрим многочлены Диксона от нескольких переменных, являющиеся обобщением многочленов вида (7.6)

§ 3. Группы перестановочных многочленов

Перестановочные многочлены поля $\mathbb{F}_q$, имеющие степень, меньшую чем q, можно комбинировать друг с другом с помощью операции *композиции* и последующего приведения по модулю $x^q - x$. Будем для удобства записывать эту операцию в виде

$$\langle g(x) \rangle \langle f(x) \rangle = \langle h(x) \rangle,$$

понимая под этим, что $f(g(x)) \equiv h(x) \pmod{(x^q - x)}$. Множество перестановочных многочленов поля $\mathbb{F}_q$, имеющих степень, меньшую чем q, образует группу относительно указанной выше операции. Эта группа изоморфна симметрической группе S_q, т. е. группе всех перестановок на множестве из q элементов. Таким образом, симметрическую группу S_q и ее подгруппы можно представлять в виде групп перестановочных многочленов.

7.18. Теорема. *Если $q > 2$, то многочлен x^{q-2} вместе со всеми линейными многочленами над полем $\mathbb{F}_q$ порождает группу S_q.*

Доказательство. Заметим, во-первых, что в силу теоремы 7.8 все указанные многочлены являются перестановочными многочленами поля $\mathbb{F}_q$. Известно, что каждую перестановку элементов множества $\mathbb{F}_q$ можно разложить в произведение транспозиций. На самом деле достаточно рассматривать лишь транспозиции вида $(0\ a)$, $a \in \mathbb{F}_q^*$, так как любую транспозицию $(b\ c) \in S_q$ можно представить в виде $(b\ c) = (0\ b)\,(0\ c)\,(0\ b)$. С другой стороны, многочлен

$$f_a(x) = -a^2[((x-a)^{q-2} + a^{-1})^{q-2} - a]^{q-2}$$

является представлением транспозиции $(0\ a)$ и при этом является композицией линейных многочленов и многочлена x^{q-2}. □

Выбор указанных в теореме многочленов в качестве образующих элементов группы S_q основывается на том, что они являются достаточно простыми по форме многочленами. Из выражения для $f_a(x)$ становится очевидным, что простая форма записи многочлена и простота соответствующей перестановки — понятия не эквивалентные.

7.19. Теорема. *Если $q > 2$, а c — фиксированный примитивный элемент поля $\mathbb{F}_q$, то симметрическая группа S_q порождается многочленами cx, $x + 1$ и x^{q-2}.*

Доказательство. Пусть $a,\ b \in \mathbb{F}_q^*$; тогда $a = c^s$, $b = c^t$, где s и t — некоторые натуральные числа, $s > t \geqslant 1$. Утверждение теоремы следует теперь из равенств

$$\langle ax\rangle = \langle c^s x\rangle = \langle cx\rangle^s, \quad \langle ax + b\rangle = \langle cx\rangle^{s-t}\langle x + 1\rangle\langle cx\rangle^t$$

и теоремы 7.18. □

Развивая дальше этот подход, мы можем найти образующие элементы знакопеременной группы A_q, которая является подгруппой группы S_q, образованной всеми четными перестановками. Далее будем называть перестановочный многочлен поля $\mathbb{F}_q$ *четным*, если соответствующая ему перестановка элементов $\mathbb{F}_q$ является четной.

7.20. Лемма. *Пусть $a \in \mathbb{F}_q$, где $q > 2$. Тогда многочлены $x + a$ и $(x^{q-2} + a)^{q-2}$ всегда являются четными перестановочными многочленами, а многочлен ax является четным перестановочным многочленом тогда и только тогда, когда элемент a является квадратом некоторого элемента из $\mathbb{F}_q^*$. Кроме того, многочлен x^{q-2} является четным перестановочным многочленом тогда и только тогда, когда $q \equiv 3 \pmod 4$.*

Доказательство. Перестановка, соответствующая многочлену $x + a$, разлагается на p^{e-1} циклов длины p, где $q = p^e$, а p — характеристика поля $\mathbb{F}_q$. Тогда если либо p нечетно, либо $q = 2^e$ и $e > 1$, то многочлен $x + a$ является четным перестановочным многочленом. Так как

$$\langle (x^{q-2} + a)^{q-2} \rangle = \langle x^{q-2} \rangle \langle x + a \rangle \langle x^{q-2} \rangle,$$

то многочлен $(x^{q-2} + a)^{q-2}$ является четным перестановочным многочленом. Далее, многочлен ax индуцирует перестановку элементов поля $\mathbb{F}_q$ тогда и только тогда, когда $a \neq 0$; в этом случае $\langle ax \rangle = \langle cx \rangle^s$, где c — примитивный элемент поля $\mathbb{F}_q$, а $a = c^s$. Перестановка, соответствующая многочлену cx, является циклом длины $q - 1$. Тогда условие четности многочлена ax следует из сказанного выше и того, что каждый элемент поля $\mathbb{F}_{2^e}$ является квадратом.

Если взять многочлен x^{q-2} и рассмотреть соответствующую перестановку, то ее можно разложить на непересекающиеся транспозиции, содержащие все элементы поля $\mathbb{F}_q$, кроме 0, 1 и -1. Таким образом, эта перестановка разлагается на $(q - 3)/2$ транспозиций, если q нечетно, и на $(q - 2)/2$, если q четно. □

Определим теперь следующие классы перестановочных многочленов поля $\mathbb{F}_q$ для $q > 2$:

$$L_q = \{ax + b \mid a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q\},$$
$$AL_q = \{a^2x + b \mid a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q\},$$
$$Q_q = \{(x^{q-2} + a)^{q-2} \mid a \in \mathbb{F}_q\}.$$

Каждое из этих множеств образует группу относительно операции композиции многочленов с последующим приведением по модулю $x^q - x$. Эти группы имеют следующие порядки: $|L_q| = q(q - 1)$, $|AL_q| = q(q - 1)/2$ для нечетных q, $|AL_q| = q(q - 1)$ для четных q и $|Q_q| = q$. Группа Q_q изоморфна аддитивной группе поля $\mathbb{F}_q$. Нетрудно доказать следующую теорему.

7.21. Теорема. *Пусть $q > 2$, и пусть c — фиксированный примитивный элемент поля $\mathbb{F}_q$. Тогда*

(i) *группа L_q порождается многочленами cx и $x + 1$;*

(ii) *группа AL_q порождается многочленами c^2x и $x + 1$;*

(iii) *знакопеременная группа A_q порождается своими подгруппами AL_q и Q_q;*

(iv) *знакопеременная группа A_q порождается многочленами c^2x, $x + 1$ и $(x^{q-2} + 1)^{q-2}$.*

Если дан класс перестановочных многочленов поля $\mathbb{F}_q$, замкнутый относительно операции композиции, то можно задаться вопросом, какую подгруппу симметрической группы S_q представ-

ляет данный класс. Сначала изучим множество $P(a)$ (a — фиксированный элемент поля $\mathbb{F}_q$) всех многочленов Диксона $g_k(x, a)$, которые являются перестановочными многочленами поля $\mathbb{F}_q$. Тогда

$$P(0) = \{g_k(x, 0) \mid k \in \mathbb{N},\ \text{НОД}(k, q-1) = 1\},$$
$$P(a) = \{g_k(x, a) \mid k \in \mathbb{N},\ \text{НОД}(k, q^2-1) = 1\} \text{ для } a \neq 0.$$

7.22. Теорема. *Множество $P(a)$ замкнуто относительно операции композиции многочленов тогда и только тогда, когда $a = 0$, 1 или -1.*

Доказательство. Если $a \in \mathbb{F}_q$, $k,\ m \in \mathbb{N}$, то

$$g_k\left(g_m\left(y + \frac{a}{y},\ a\right),\ a^m\right) = g_k\left(y^m + \frac{a^m}{y^m},\ a^m\right) =$$
$$= y^{km} + \frac{a^{km}}{y^{km}} = g_{km}\left(y + \frac{a}{y},\ a\right)$$

по (7.8), а тогда

$$g_{km}(x, a) = g_k(g_m(x, a), a^m). \tag{7.10}$$

Когда $a \neq 0$ и $P(a)$ замкнуто относительно операции композиции многочленов, то $g_k(g_m(x, a), a) \in P(a)$, если НОД $(k, q^2-1) =$ $=$ НОД $(m, q^2-1) = 1$. Таким образом, $g_k(g_m(x, a), a) =$ $= g_{km}(x, a)$, и в силу (7.10)

$$g_k(g_m(x, a), a^m) = g_k(g_m(x, a), a).$$

Так как многочлен $g_m(x, a)$ не является постоянным, то

$$g_k(x, a^m) = g_k(x, a).$$

Сравнивая коэффициенты при x^{k-2} для всех $k > 1$, получаем, что $a^m = a$ для всех m, удовлетворяющих соотношению НОД $(m, q^2-1) = 1$. Следовательно, $a^{-1} = a$, откуда вытекает, что $a = \pm 1$.

Обратно, если $a = 0$, 1 или -1, то в силу (7.10) множество $P(a)$ замкнуто относительно операции композиции многочленов. □

Таким образом, в трех случаях, когда $a = 1$, $a = -1$ и $a = 0$, множество $G(a)$ всех перестановок элементов $\mathbb{F}_q$, представимых с помощью многочленов из $P(a)$, является абелевой подгруппой симметрической группы S_q. Изучим теперь строение группы $G(a)$.

Пусть $a = \pm 1$. Для любого $c \in \mathbb{F}_q$ можно найти такой элемент $\gamma \in \mathbb{F}_{q^2}^*$, что $c = \gamma + a\gamma^{-1}$. Тогда для $k \equiv m \pmod{q^2-1}$ из (7.8) получаем

$$g_k(c, a) = g_k(\gamma + a\gamma^{-1}, a) = \gamma^k + a^k\gamma^{-k} = \gamma^m + a^m\gamma^{-m} =$$
$$= g_m(\gamma + a\gamma^{-1}, a) + g_m(c, a).$$

Следовательно, если НОД $(k, q^2 - 1) = 1$, то $g_k(x, a)$ и $g_m(x, a)$ индуцируют одну и ту же перестановку элементов поля $\mathbb{F}_q$. Таким образом, если каждому классу вычетов числа k по модулю $q^2 - 1$ сопоставить перестановку элементов поля $\mathbb{F}_q$, индуцированную многочленом $g_k(x, a)$, то мы получим эпиморфизм $R(q^2 - 1)$ на группу $G(a)$, где $R(q^2 - 1)$ — приведенная группа классов вычетов по модулю $q^2 - 1$, или, иначе говоря, группа обратимых элементов кольца $\mathbb{Z}/(q^2 - 1)$. Теперь в силу теоремы 1.23 достаточно найти ядро $K(a)$ этого эпиморфизма.

Если $k \in K(a)$, то $g_k(c, a) = c$ для всех $c \in \mathbb{F}_q$. Тогда если элемент γ такой же, как и выше, то $\gamma^k + a^k\gamma^{-k} = \gamma + a\gamma^{-1}$. Так как $a^k = a$, то $\gamma^k + a\gamma^{-k} = \gamma + a\gamma^{-1}$, следовательно, либо $\gamma^k = \gamma$, либо $\gamma^k = a\gamma^{-1}$ и, таким образом,

$$\text{либо } \gamma^{k-1} = 1, \text{ либо } \gamma^{k+1} = a$$

$$\text{для всех } \gamma \in \mathbb{F}_{q^2}^*, \text{ таких, что } \gamma + a\gamma^{-1} \in \mathbb{F}_q. \quad (7.11)$$

Это же условие оказывается достаточным для того, чтобы $k \in K(a)$. Теперь $\gamma + a\gamma^{-1} \in \mathbb{F}_q$ тогда и только тогда, когда $(\gamma + a\gamma^{-1})^q = \gamma + a\gamma^{-1}$, а последнее эквивалентно тому, что $\gamma^{q-1} = 1$ или $\gamma^{q+1} = a$. Пусть $a = 1$, и пусть ζ — примитивный элемент поля $\mathbb{F}_{q^2}$. Тогда или $\gamma = \zeta^{m(q+1)}$, или $\gamma = \zeta^{n(q-1)}$, где $m, n \in \mathbb{Z}$. Таким образом, из (7.11) следует, что $k \in K(a)$ тогда и только тогда, когда k является решением одной из следующих четырех систем сравнений:

$$\begin{cases} k \equiv 1 \pmod{(q-1)}, \\ k \equiv 1 \pmod{(q+1)}, \end{cases} \qquad \begin{cases} k \equiv 1 \pmod{(q-1)}, \\ k \equiv -1 \pmod{(q+1)}, \end{cases}$$

$$\begin{cases} k \equiv -1 \pmod{(q-1)}, \\ k \equiv 1 \pmod{(q+1)}, \end{cases} \qquad \begin{cases} k \equiv -1 \pmod{(q-1)}, \\ k \equiv -1 \pmod{(q+1)}. \end{cases}$$

Решая эти системы по модулю $q^2 - 1$, получаем, что

$$K(1) = \{1, q, -q, -1\} \text{ для четного } q$$

и

$$K(1) = \{1, q, -q, -1, 1 + (q^2 - 1)/2, q + (q^2 - 1)/2, -q + (q^2 - 1)/2, -1 + (q^2 - 1)/2\} \text{ для нечетного } q$$

Случай $a = -1$ исследуется аналогичным образом, и в этом случае получаем, что

$$K(-1) = \{1, q\} \text{ при } q \equiv 3 \pmod 4$$

и

$$K(-1) = \{1, q, 1 + (q^2 - 1)/2, q + (q^2 - 1)/2\} \text{ при } q \equiv (1 \pmod 4).$$

Полученные результаты можно сформулнровать в виде следующей теоремы:

7.23. Теорема. *Если* $a = \pm 1$, *то группа* $G(a)$ *изоморфна факторгруппе* $R(q^2-1)/K(a)$, *где* $K(a)$ *определено выше. При этом* $|K(1)| = 2$ *для* $q = 2$, $|K(1)| = 4$ *для четных* $q > 2$, $|K(1)| = 4$ *для* $q = 3$, $|K(1)| = 8$ *для нечетных* $q > 3$, $|K(-1)| = 2$, *если* $q \equiv 3 \pmod 4$, *и* $|K(-1)| = 4$, *если* $q \equiv 1 \pmod 4$. *Группа* $G(0)$ *изоморфна* $R(q-1)$ *— группе обратимых элементов кольца вычетов по модулю* $q - 1$.

Приведем еще один интересный класс перестановочных многочленов. Пусть $\mathbb{F}_{q^r}$ — расширение поля $\mathbb{F}_q$. Рассмотрим линеаризованные многочлены $L(x)$ вида

$$L(x) = \sum_{s=0}^{r-1} \alpha_s x^{q^s} \in \mathbb{F}_{q^r}[x]. \tag{7.12}$$

По теореме 7.9 многочлен $L(x)$ является перестановочным многочленом поля $\mathbb{F}_{q^r}$ тогда и только тогда, когда он имеет в $\mathbb{F}_{q^r}$ единственный корень, равный 0, т. е. тогда и только тогда, когда линейный оператор, индуцированный многочленом $L(x)$, в поле $\mathbb{F}_{q^r}$, рассматриваемом как векторное пространство над полем $\mathbb{F}_q$, является невырожденным. В свою очередь этот линейный оператор является невырожденным тогда и только тогда, когда для любого набора элементов $\beta_0, \beta_1, \ldots, \beta_{r-1} \in \mathbb{F}_{q^r}$, линейно независимых над полем $\mathbb{F}_q$, элементы $\gamma_0 = L(\beta_0)$, $\gamma_1 = L(\beta_1)$, ..., $\gamma_{r-1} = L(\beta_{r-1})$ также линейно независимы над полем $\mathbb{F}_q$. Теперь из (7.12) получаем

$$\gamma_i^{q^j} = \sum_{s=0}^{r-1} \alpha_s^{q^j} \beta_i^{q^{s+j}}, \quad 0 \leqslant i,\ j \leqslant r-1.$$

Пользуясь равенством $\beta_i^{q^r} = \beta_i$ и полагая $\alpha_t = \alpha_s$ для $t \equiv s \pmod r$, получаем

$$\gamma_i^{q^j} = \sum_{s=0}^{r-1} \beta_i^{q^s} \alpha_{s-j}^{q^j}.$$

Если Δ_1 и Δ_2 — определители вида (3.13), образованные соответственно элементами $\beta_0, \beta_1, \ldots, \beta_{r-1}$ и $\gamma_0, \gamma_1, \ldots, \gamma_{r-1}$, то

$$\Delta_2 = \Delta_1 \det(A),$$

где A — следующая матрица размера $r \times r$:

$$A = \begin{pmatrix} \alpha_0 & \alpha_{r-1}^q & \alpha_{r-2}^{q^2} & \ldots & \alpha_1^{q^{r-1}} \\ \alpha_1 & \alpha_0^q & \alpha_{r-1}^{q^2} & \ldots & \alpha_2^{q^{r-1}} \\ \alpha_2 & \alpha_1^q & \alpha_0^{q^2} & \ldots & \alpha_3^{q^{r-1}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{r-1} & \alpha_{r-2}^q & \alpha_{r-3}^{q^2} & \ldots & \alpha_0^{q^{r-1}} \end{pmatrix}.$$

В силу леммы 3.51 многочлен $L(x)$ является перестановочным многочленом поля $\mathbb{F}_{q^r}$ тогда и только тогда, когда $\det'(A) \neq 0$.

Множество многочленов вида (7.12), являющихся перестановочными многочленами поля $\mathbb{F}_{q^r}$, образует группу относительно операции композиции многочленов с последующим приведением по модулю $x^{q^r} - x$. Эта группа известна как *группа Бетти — Матье*. Приведем без доказательства следующую теорему.

7.24. **Теорема.** *Группа Бетти — Матье изоморфна общей линейной группе $GL(r, \mathbb{F}_q)$, образованной невырожденными $r \times r$-матрицами над полем $\mathbb{F}_q$ относительно операции умножения матриц.*

§ 4. Исключительные многочлены

При изучении перестановочных многочленов можно воспользоваться некоторыми геометрическими идеями. Преимущество, которое мы получаем от такого подхода, состоит в том, что появляется возможность применять очень сильную теорему Ленга — Вейля (см. комментарии к гл. 6), которая дает оценку для числа рациональных точек на абсолютно неприводимой кривой, заданной над конечным полем.

Пусть дан многочлен $f \in \mathbb{F}_q[x]$ степени $d \geqslant 1$; образуем многочлен от двух переменных

$$\Phi(x, y) = \frac{f(x) - f(y)}{x - y},$$

имеющий степень $d - 1$. Пусть $E \times E$ — прямое произведение двух экземпляров алгебраического расширения E поля $\mathbb{F}_q$. Определим *алгебраическую кривую* C_φ над полем $\mathbb{F}_q$ как подмножество множества $E \times E$ вида

$$C_\varphi = \{(a, b) \in E \times E \mid \varphi(a, b) = 0\},$$

где $\varphi \in \mathbb{F}_q[x, y]$ — ненулевой многочлен от двух переменных над полем $\mathbb{F}_q$. Точка (a, b), лежащая на кривой C_φ, называется *рациональной точкой*, если элементы a и b принадлежат $\mathbb{F}_q$. Разумеется, число рациональных точек на кривой всегда конечно, так как множество $\mathbb{F}_q \times \mathbb{F}_q$ само конечно. Используя введенные выше обозначения, получаем, что *многочлен $f(x)$ является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда C_Φ не содержит рациональных точек, лежащих вне прямой $y = x$.*

Напомним, что для любого поля K элементы кольца $K[x, y]$ единственным образом разлагаются на неприводимые многочлены и что многочлен положительной степени из $K[x, y]$ называется *абсолютно неприводимым*, если он неприводим над любым алгебраическим расширением поля K.

7.25. Определение. Многочлен $f(x) \in \mathbb{F}_q[x]$ степени $d \geqslant 2$ называется *исключительным многочленом* над полем $\mathbb{F}_q$, если ни один неприводимый делитель многочлена

$$\Phi(x, y) = \frac{f(x) - f(y)}{x - y} \in \mathbb{F}_q[x, y]$$

не является абсолютно неприводимым.

Иными словами, многочлен $f(x)$ является исключительным многочленом над полем $\mathbb{F}_q$, если каждый неприводимый делитель многочлена $\Phi(x, y) \in \mathbb{F}_q[x, y]$ допускает нетривиальное разложение на множители над некоторым алгебраическим расширением поля $\mathbb{F}_q$.

Следующая теорема устанавливает связь между перестановочными и исключительными многочленами. Отметим сначала (без доказательства), что любой исключительный многочлен является «почти перестановочным» многочленом в следующем смысле.

7.26. Лемма. *Пусть $f(x) \in \mathbb{F}_q[x]$ является исключительным многочленом над полем $\mathbb{F}_q$ степени d, и пусть через $V(f)$ обозначено число различных элементов в множестве $\{f(c) \mid c \in \mathbb{F}_q\}$ значений, которые может принимать этот многочлен. Тогда $V(f) \geqslant q - A(d)$, где $A(d)$ — константа, зависящая только от степени d многочлена $f(x)$.*

7.27. Теорема. *Пусть $\mathbb{F}_q$ — поле характеристики p, а $f(x)$ — исключительный многочлен над полем $\mathbb{F}_q$ степени d, причем $p \geqslant B(d)$, где $B(d)$ — некоторая константа, зависящая только от d. Тогда многочлен $f(x)$ является перестановочным многочленом поля $\mathbb{F}_q$.*

Доказательство. Используя обозначения леммы 7.26, можно представить $V(f)$ в виде $V(f) = q - w$, где $0 \leqslant w \leqslant A(d)$. Для доказательства теоремы достаточно показать, что $w = 0$. Допустим, что $w \geqslant 1$, и покажем, что в этом случае мы приходим к противоречию.

Пусть различными элементами в множестве значений, которые принимает $f(x)$, будут элементы $b_1, b_2, \ldots, b_{q-w}$, и пусть оставшиеся элементы поля $\mathbb{F}_q$ — это $c_1, c_2, \ldots, c_w$. Для $i = 1, 2, \ldots, q - w$ обозначим через m_i число решений уравнения $f(x) = b_i$ в поле $\mathbb{F}_q$; тогда $\sum_{i=1}^{q-w} m_i = q$. Кроме того, $m_i \geqslant 1$ для любого $i = 1, 2, \ldots, q - w$, а значит,

$$m_i \leqslant w + 1 \quad (i = 1, 2, \ldots, q - w). \tag{7.13}$$

В то же время для $t = 1, 2, \ldots, w$ получаем

$$\sum_{c \in \mathbb{F}_q} f(c)^t = \sum_{i=1}^{q-w} m_i b_i^t.$$

Если $p \geqslant B(d)$, где $B(d) = dA(d) + 2$, то справедливы соотношения $q - 2 \geqslant p - 2 \geqslant dA(d) \geqslant dw$, а тогда для всех $t = 1, 2, \ldots, w$ можно записать

$$f(x)^t = a_0^{(t)} + a_1^{(t)}x + \cdots + a_{q-2}^{(t)}x^{q-2}.$$

В силу леммы 7.3

$$\sum_{c \in \mathbb{F}_q} f(c)^t = \sum_{j=0}^{q-2} a_j^{(t)} \sum_{c \in \mathbb{F}_q} c^j = 0.$$

Таким образом,

$$\sum_{i=1}^{q-w} m_i b_i^t = 0 \quad (t = 1, 2, \ldots, w). \tag{7.14}$$

Положим $m = \max(m_1, \ldots, m_{q-w})$; тогда из (7.13) получаем, что $1 \leqslant m \leqslant w + 1$. Если через s_j, $1 \leqslant j \leqslant m$, обозначить число таких m_i, для которых $m_i = j$, то $s_1 + \ldots + s_m = q - w$ и

$$\sum_{j=1}^{m} (j-1)s_j = \sum_{i=1}^{q-w} m_i - \sum_{j=1}^{m} s_j = q - (q-w) = w. \tag{7.15}$$

Перенумеруем элементы $b_1, \ldots, b_{q-w}$ таким образом, что $m_1 = \ldots = m_{s_1} = 1$, $m_{s_1+1} = \ldots = m_{s_1+s_2} = 2$, $\ldots$, $m_{s_1+\ldots+s_{m-1}+1} = \ldots = m_{s_1+\ldots+s_m} = m$, тогда формула (7.14) принимает вид

$$A_t = \sum_{j=1}^{m} j \sum_{i=s_1+\cdots+s_{j-1}+1}^{s_1+\cdots+s_j} b_i^t = 0 \quad (t = 1, 2, \ldots, w).$$

Отсюда вытекает, что

$$\sum_{k=1}^{w} c_k^t = \sum_{k=1}^{w} c_k^t + A_t = \sum_{c \in \mathbb{F}_q} c^t + \sum_{j=1}^{m} (j-1) \sum_{i=s_1+\cdots+s_{j-1}+1}^{s_1+\cdots+s_j} b_i^t.$$

Так как $1 \leqslant t \leqslant w \leqslant dA(d) \leqslant q - 2$, то $\sum_{c \in \mathbb{F}_q} c^t = 0$, и, следовательно,

$$\sum_{k=1}^{w} c_k^t = \sum_{j=2}^{m} (j-1) \sum_{i=s_1+\cdots+s_{j-1}+1}^{s_1+\cdots+s_j} b_i^t. \tag{7.16}$$

Рассмотрим далее два многочлена

$$g(x) = \prod_{k=1}^{w} (x - c_k), \quad h(x) = \prod_{j=2}^{m} \prod_{i=1}^{s_j} \left(x - b_{s_1+\cdots+s_{j-1}+i}\right)^{j-1}.$$

Из (7.15) вытекает, что $\deg(g) = w$, $\deg(h) = w$. Обозначим через g_r и h_r, $0 \leqslant r \leqslant w$, коэффициенты при x^{w-r} соответственно в $g(x)$ и $h(x)$. Пусть G_t и H_t, $1 \leqslant t \leqslant w$, обозначают суммы t-х

степеней всех корней многочленов $g(x)$ и $h(x)$ соответственно. Тогда из (7.16) получаем, что $G_t = H_t$ для всех $1 \leqslant t \leqslant w$. Из формулы Ньютона (см. теорему 1.75) следует, что

$$\sum_{i=0}^{t-1} G_{t-i} g_i + t g_t = 0 \quad (1 \leqslant t \leqslant w). \tag{7.17}$$

Так как $p \geqslant dA(d) + 2 > A(d) \geqslant w$, то коэффициент при g_t в (7.17) отличен от 0. Значит, систему из w уравнений (7.17) можно однозначно разрешить относительно $g_1, \ldots, g_w$ и выразить их через $G_1, \ldots, G_w$, а именно $g_1 = -G_1$, $g_2 = (G_1^2 - G_2)/2$ и т. д. Аналогично получаем, что $h_1 = -H_1$, $h_2 = (H_1^2 - H_2)/2$ и т. д., а так как $G_t = H_t$ для всех $1 \leqslant t \leqslant w$, то отсюда вытекает, что $g_r = h_r$ для всех $0 \leqslant r \leqslant w$. Таким образом, $g(x) = h(x)$, и множество $\{c_1, \ldots, c_w\}$ должно с точностью до порядка элементов совпадать с множеством $\{b_{s_1+1}, \ldots, b_{q-w}\}$. Это, однако, невозможно, так как по определению элементы b_i отличны от c_k. Тем самым мы пришли к противоречию, что и завершает доказательство теоремы. □

Предыдущая теорема показывает, что в конечном поле достаточно большой характеристики свойство многочлена быть исключительным является *достаточным* для того, чтобы он был перестановочным многочленом. Определим теперь, при каких предположениях свойство многочлена быть исключительным является также и *необходимым* условием для того, чтобы этот многочлен был перестановочным.

Утверждение, обратное к теореме 7.27, становится справедливым при некоторых дополнительных условиях, которые можно получить из теоремы Ленга — Вейля. Переформулируем эту теорему следующим образом. Пусть через N обозначено число рациональных точек на кривой C_φ, где $\varphi \in \mathbb{F}_q[x, y]$ — абсолютно неприводимый многочлен, $\deg(\varphi) = d$. Тогда по теореме Ленга — Вейля (см. примечания к § 4 гл. 6) справедливо неравенство

$$|N - q| \leqslant (d-1)(d-2) q^{1/2} + C(d), \tag{7.18}$$

где $C(d)$ — некоторая константа, зависящая только от d. Для наших целей нам понадобится более слабое утверждение, вытекающее из (7.18).

7.28. Лемма. *Существует последовательность $k_1, k_2, \ldots$ целых положительных чисел, обладающих следующим свойством: если $\varphi \in \mathbb{F}_q[x, y]$ — абсолютно неприводимый многочлен и $q \geqslant k_d$, где $d = \deg(\varphi)$, то либо C_φ содержит некоторую рациональную точку (a, b), $a \neq b$, либо многочлен φ имеет вид $c(y - x)$ для некоторого $c \in \mathbb{F}_q$.*

Доказательство. Для каждого $d \in \mathbb{N}$ выберем число k_d таким образом, чтобы выполнялось неравенство

$$q - (d-1)(d-2)q^{1/2} - C(d) > d$$

для всех $q \geqslant k_d$. Тогда если φ — абсолютно неприводимый многочлен степени d от двух переменных над полем $\mathbb{F}_q$, где $q \geqslant k_d$, то из (7.18) следует, что C_φ содержит по меньшей мере $d+1$ рациональных точек. Если многочлен φ отличен от $c(y-x)$, то из его неприводимости следует, что он не делится на $y-x$ и, следовательно, $\varphi(x, x)$ не является нулевым многочленом. Таким образом, кривая C_φ пересекает прямую $y = x$ не более чем в d рациональных точках. Следовательно, C_φ содержит хотя бы одну рациональную точку (a, b), где $a \neq b$. □

Чтобы доказать следующую теорему, воспользуемся приведенными в начале этого параграфа понятиями алгебраических кривых и их рациональных точек, а также их связью с перестановочными многочленами.

7.29. **Теорема.** *Существует последовательность целых положительных чисел $k_1, k_2, \ldots$, такая, что для любого конечного поля $\mathbb{F}_q$ порядка $q \geqslant k_n$, такого, что* НОД $(n, q) = 1$, *справедливо следующее утверждение: если $f(x) \in \mathbb{F}_q[x]$ — перестановочный многочлен поля $\mathbb{F}_q$,* $\deg(f(x)) = n \geqslant 2$, *то он является исключительным многочленом над полем $\mathbb{F}_q$.*

Доказательство. Очевидно, что в лемме 7.28 числа $k_1, k_2, \ldots$ можно выбрать таким образом, что последовательность $k_1, k_2, \ldots$ будет неубывающей, т. е. $k_1 \leqslant k_2 \leqslant \ldots$. Пусть числа k_n выбраны указанным образом, и пусть $f(x) \in \mathbb{F}_q[x]$ — перестановочный многочлен поля $\mathbb{F}_q$, удовлетворяющий условиям нашей теоремы. Если

$$\Phi(x, y) = (f(x) - f(y))/(x-y) \in \mathbb{F}_q[x, y],$$

то алгебраическая кривая C_Φ не имеет рациональных точек, не лежащих на прямой $y = x$. Предположим теперь, что многочлен $f(x)$ не является исключительным многочленом. Тогда многочлен $\Phi(x, y)$ имеет абсолютно неприводимый делитель $g(x, y) \in \mathbb{F}_q[x, y]$. Если $g(x, y) = c(y-x)$, $c \in \mathbb{F}_q$, то для некоторого $h(x, y) \in \mathbb{F}_q[x, y]$ выполняется равенство $f(y) - f(x) = (y-x)^2 h(x, y)$. Тогда

$$f'(y) = 2(y-x)h(x, y) + (y-x)^2(\partial h(x, y)/\partial y),$$

и, таким образом, $f'(x) = 0$, а это противоречит тому, что НОД $(n, q) = 1$. Следовательно, многочлен $g(x, y)$ отличен от $c(y-x)$. Если $d = \deg(g)$, то $q \geqslant k_n \geqslant k_d$, а тогда из леммы 7.28 вытекает, что $g(a, b) = 0$ для некоторой пары $(a, b) \in \mathbb{F}_q^2$, $a \neq b$. Отсюда получаем, что $\Phi(a, b) = 0$ и тем самым приходим к противоречию. □

Если НОД $(n, q) > 1$, т. е. если характеристика p поля $\mathbb{F}_q$ делит n, то утверждение теоремы 7.29 не всегда остается справедливым. Так, например, x^p является перестановочным многочленом поля $\mathbb{F}_q$, однако равенство $(x^p - y^p)/(x - y) = (x - y)^{p-1}$ показывает, что x^p не является исключительным многочленом над полем $\mathbb{F}_q$.

Если объединить теоремы 7.27 и 7.29, то можно получить следующее описание перестановочных многочленов в случае конечных полей с достаточно большой характеристикой.

7.30. Следствие. *Для любого целого $n \geqslant 2$ найдется константа K_n, такая, что для любого конечного поля $\mathbb{F}_q$ характеристики $p \geqslant K_n$ выполняется следующее утверждение: многочлен $f(x) \in \mathbb{F}_q[x]$ степени n является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда он является исключительным многочленом над полем $\mathbb{F}_q$.*

Следующий результат, который в конечном счете тоже вытекает из теоремы Ленга — Вейля, помогает выяснить, в каком случае для данного конечного поля не существует перестановочных многочленов данной степени n.

7.31. Теорема. *Существует последовательность целых положительных чисел $k_1, k_2, \ldots$, обладающих следующим свойством: каково бы ни было натуральное число n, если $\mathbb{F}_q$ — конечное поле порядка $q \geqslant k_n$, НОД $(n, q) = 1$ и $\mathbb{F}_q$ содержит корень n-й степени из единицы $\zeta \neq 1$, то не существует перестановочных многочленов поля $\mathbb{F}_q$, имеющих степень n.*

Доказательство. Пусть $f \in \mathbb{F}_q[x]$ — произвольный многочлен степени n; положим

$$\Phi(x, y) = (f(x) - f(y))/(x - y).$$

Разлагая многочлен Φ на неприводимые сомножители сначала в $\mathbb{F}_q[x, y]$, а затем над подходящими последовательными алгебраическими расширениями поля $\mathbb{F}_q$, получаем в итоге некоторое алгебраическое расширение E поля $\mathbb{F}_q$ и разложение над E

$$\Phi = a_n g_1 \ldots g_r, \tag{7.19}$$

где a_n — старший коэффициент многочлена $f(x)$, а каждый сомножитель $g_i \in E[x, y]$ является нормированным по x и при этом абсолютно неприводимым. Пусть h_i, $1 \leqslant i \leqslant r$, — однородная часть наивысшей степени многочлена g_i. Тогда

$$\frac{x^n - y^n}{x - y} = h_1 \ldots h_r,$$

так как левая часть этого равенства является однородной частью наивысшей степени многочлена $a_n^{-1}\Phi$. Кроме того,

$$\frac{x^n - y^n}{x - y} = (x - \zeta_1 y) \dots (x - \zeta_{n-1} y),$$

где $\zeta_1, \dots, \zeta_{n-1}$ — отличные от 1 корни n-й степени из 1 в поле $\mathbb{F}_q$, которые все различны в силу теоремы 2.42 (i). Отсюда следует, что многочлен $x - \zeta y \in \mathbb{F}_q[x, y]$ делит в точности один из сомножителей h_i. Пусть для определенности это будет h_1.

Пусть σ — автоморфизм кольца $E[x, y]$, задаваемый формулой

$$\sigma\left(\sum_{i,k} \alpha_{ik} x^i y^k\right) = \sum_{i,k} \alpha_{ik}^q x^i y^k.$$

Применим σ к (7.19) и заметим, что $\sigma(\Phi) = \Phi$ и $\sigma(a_n) = a_n$, так как $\Phi \in \mathbb{F}_q[x, y]$ и $a_n \in \mathbb{F}_q$. Следовательно, в силу единственности разложения (7.19) σ переставляет многочлены g_i, так что $\sigma(g_1) = g_m$ для некоторого m, $1 \leqslant m \leqslant r$, а отсюда следует, что $\sigma(h_1) = h_m$. Так как многочлен $x - \zeta y$ делит h_1, то он делит и $h_m = \sigma(h_1)$, поскольку $\sigma(x - \zeta y) = x - \zeta y$. Отсюда вытекает, что $m = 1$, т. е. что $\sigma(g_1) = g_1$. Значит, все коэффициенты многочлена g_1 лежат в $\mathbb{F}_q$ и, таким образом, g_1 абсолютно неприводим над полем $\mathbb{F}_q$.

Вновь в лемме 7.28 числа $k_1, k_2, \dots$ выберем таким образом, чтобы они образовывали неубывающую последовательность $k_1 \leqslant k_2 \leqslant \dots$. Пусть $d = \deg(g_1)$ и $q \geqslant k_n \geqslant k_d$. Так как h_1 делится на $x - \zeta y$ и $\zeta \neq 1$, многочлен g_1 не может иметь вид $g_1 = c(y - x)$, $c \in \mathbb{F}_q$. Тогда из леммы 7.28 вытекает, что $g_1(a, b) = 0$ для некоторой пары $(a, b) \in \mathbb{F}_q^2$, $a \neq b$. Отсюда и из формулы (7.19) получаем, что $\Phi(a, b) = 0$. Следовательно, многочлен $f(x)$ не может быть перестановочным многочленом поля $\mathbb{F}_q$. □

7.32. **Следствие.** *Пусть $\mathbb{F}_q$ — конечное поле и $n \in \mathbb{N}$ — четное число. Если $q \geqslant k_n$ и* НОД $(n, q) = 1$, *то не существует перестановочных многочленов поля $\mathbb{F}_q$, имеющих степень n.*

Доказательство. Положим в теореме 7.31 $\zeta = -1$. □

Так как мультипликативная группа поля $\mathbb{F}_q$ является циклической группой порядка $q - 1$, то $\mathbb{F}_q$ содержит отличный от 1 корень n-й степени из единицы ζ тогда и только тогда, когда НОД $(n, q - 1) > 1$. Таким образом, из теоремы 7.31 вытекает следующий критерий.

7.33. **Следствие.** *Пусть $n \in \mathbb{N}$. Если $q \geqslant k_n$ и* НОД $(n, q) = 1$, *то перестановочные многочлены поля $\mathbb{F}_q$, имеющие степень n, существуют тогда и только тогда, когда* НОД $(n, q - 1) = 1$.

Доказательство. Необходимость следует из приведенных выше рассуждений и теоремы 7.31. С другой стороны, если НОД $(n, q-1)=1$, то из теоремы 7.8 (ii) следует, что x^n является перестановочным многочленом поля $\mathbb{F}_q$, причем $\deg(x^n)=n$. □

§ 5. Перестановочные многочлены от нескольких переменных

Пусть $n \geqslant 1$, и пусть $\mathbb{F}_q[x_1, \ldots, x_n]$ — кольцо многочленов от n переменных над полем $\mathbb{F}_q$. Через $\mathbb{F}_q^n$ обозначим прямое произведение n экземпляров поля $\mathbb{F}_q$. Перестановочный многочлен от n переменных над полем $\mathbb{F}_q$ естественно определить как такой многочлен $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, для которого число решений уравнения $f(x_1, \ldots, x_n)=a$ в $\mathbb{F}_q^n$ одно и то же для всех значений $a \in \mathbb{F}_q$. Если обозначить это число решений через N, то должно выполняться равенство $N=q^{n-1}$. Действительно, $|\mathbb{F}_q^n| = q^n = \sum_{a \in \mathbb{F}_q} N = qN$. Таким образом, мы приходим к следующему определению.

7.34. Определение. Многочлен $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ называется *перестановочным многочленом от n переменных* над полем $\mathbb{F}_q$, если для любого $a \in \mathbb{F}_q$ уравнение $f(x_1, \ldots, x_n)=a$ имеет ровно q^{n-1} решений в $\mathbb{F}_q^n$.

В случае $n>1$ мы не можем сказать, что перестановочный многочлен $f(x_1, \ldots, x_n)$ над полем $\mathbb{F}_q$ индуцирует перестановку элементов множества $\mathbb{F}_q^n$ ввиду того, что соответствующее отображение не является отображением $\mathbb{F}_q^n$ в себя. Однако следующее определение позволяет рассматривать отображения из $\mathbb{F}_q^n$ в $\mathbb{F}_q^m$, которые индуцируются системами многочленов от нескольких переменных.

7.35. Определение. Система многочленов

$$f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n], \quad 1 \leqslant m \leqslant n,$$

называется *ортогональной* над полем $\mathbb{F}_q$, если для каждого набора $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$ система уравнений

$$f_1(x_1, \ldots, x_n)=a_1, \ \ldots, \ f_m(x_1, \ldots, x_n)=a_m$$

имеет ровно q^{n-m} решений в $\mathbb{F}_q^n$.

В частном случае, когда $m=n$, это означает, что ортогональная система многочленов $f_1, \ldots, f_n$ индуцирует перестановку элементов множества $\mathbb{F}_q^n$. Применяя терминологию из определения 7.35 к одному многочлену, мы можем сказать, что многочлен f является перестановочным, если он сам по себе образует орто-

гональную систему. Из определения 7.35 непосредственно следует, что любая непустая подсистема ортогональной системы многочленов сама является ортогональной. В частности, *любой многочлен, входящий в ортогональную систему, является перестановочным многочленом.* С другой стороны, следующая теорема показывает, что каждую ортогональную систему из m многочленов от n переменных, где $m < n$, можно дополнить до ортогональной системы, содержащей большее число многочленов. Для этого, во-первых, заметим, что каждое отображение $\tau\colon \mathbb{F}_q^n \to \mathbb{F}_q$ можно представить с помощью некоторого многочлена $g(x_1, \ldots, x_n)$ над полем $\mathbb{F}_q$, который по каждой переменной имеет степень, меньшую q. Этот многочлен задается следующей формулой:

$$g(x_1, \ldots, x_n) = \sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} \tau(c_1, \ldots, c_n)(1 - (x_1 - c_1)^{q-1}) \ldots (1 - (x_n - c_n)^{q-1}). \tag{7.20}$$

Нетрудно проверить, что $g(c_1, \ldots, c_n) = \tau(c_1, \ldots, c_n)$ для всех наборов $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$.

7.36. **Теорема.** *Для любой ортогональной системы многочленов $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, $1 \leqslant m < n$, над полем $\mathbb{F}_q$ и любого натурального числа r, $1 \leqslant r \leqslant n - m$, найдутся многочлены $f_{m+1}, \ldots, f_{m+r} \in \mathbb{F}_q[x_1, \ldots, x_n]$, такие, что $f_1, \ldots, f_{m+r}$ образуют ортогональную систему над полем $\mathbb{F}_q$.*

Доказательство. Достаточно доказать теорему для $r = 1$. Если $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$, то положим

$$S(a_1, \ldots, a_m) = \{(c_1, \ldots, c_n) \in \mathbb{F}_q^n \mid f_i(c_1, \ldots, c_n) = a_i,\ 1 \leqslant i \leqslant m\}.$$

По предположению каждое множество $S(a_1, \ldots, a_m)$ содержит ровно q^{n-m} элементов. Теперь каждое множество $S(a_1, \ldots, a_m)$ разобьем произвольным образом на q попарно непересекающихся подмножеств $S(a_1, \ldots, a_m, a)$, $a \in \mathbb{F}_q$, каждое из которых содержит q^{n-m-1} элементов. Построим отображение $\tau\colon \mathbb{F}_q^n \to \mathbb{F}_q$ следующим образом. Так как каждый набор $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ принадлежит лишь одному множеству $S(a_1, \ldots, a_m, a)$, положим $\tau(c_1, \ldots, c_n) = a$. В силу (7.20) отображение τ можно задать с помощью многочлена $f_{m+1}(x_1, \ldots, x_n)$ над полем $\mathbb{F}_q$. Этот многочлен и является искомым. □

Необходимое и достаточное условие для того, чтобы система многочленов была ортогональной, можно получить с помощью характеров. Воспользуемся обозначениями для аддитивных характеров, введенными в теореме 5.7.

7.37. Теорема. *Система многочленов* $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, $1 \leqslant m \leqslant n$, *является ортогональной системой над полем* $\mathbb{F}_q$ *тогда и только тогда, когда*

$$\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} \chi_{b_1}(f_1(c_1, \ldots, c_n)) \ldots \chi_{b_m}(f_m(c_1, \ldots, c_n)) = 0$$

для любых аддитивных характеров $\chi_{b_1}, \ldots, \chi_{b_m}$ *поля* $\mathbb{F}_q$, *где* $(b_1, \ldots, b_m) \neq (0, \ldots, 0)$.

Доказательство. Для любого набора $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$ обозначим через $N(a_1, \ldots, a_m)$ число решений системы уравнений

$$f_1(x_1, \ldots, x_n) = a_1, \ \ldots, \ f_m(x_1, \ldots, x_n) = a_m$$

в $\mathbb{F}_q^n$. Если система многочленов $f_1, \ldots, f_m$ ортогональна над $\mathbb{F}_q$, то из (5.9) следует, что

$$\begin{aligned}
&\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} \chi_{b_1}(f_1(c_1, \ldots, c_n)) \ldots \chi_{b_m}(f_m(c_1, \ldots, c_n)) = \\
&= \sum_{(a_1, \ldots, a_m) \in \mathbb{F}_q^m} N(a_1, \ldots, a_m) \chi_{b_1}(a_1) \ldots \chi_{b_m}(a_m) = \\
&= q^{n-m} \left(\sum_{a_1 \in \mathbb{F}_q} \chi_{b_1}(a_1) \right) \ldots \left(\sum_{a_m \in \mathbb{F}_q} \chi_{b_m}(a_m) \right) = 0
\end{aligned}$$

при условии, что хотя бы один элемент b_i отличен от 0.

Обратно, если выполняются условия теоремы, то для любого набора $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$ из (5.10) получаем

$$\begin{aligned}
N(a_1, \ldots, a_m) = \frac{1}{q^m} &\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} \left(\sum_{b_1 \in \mathbb{F}_q} \chi_{b_1}(f_1(c_1, \ldots, c_n)) \overline{\chi_{b_1}(a_1)} \right) \ldots \\
&\ldots \left(\sum_{b_m \in \mathbb{F}_q} \chi_{b_m}(f_m(c_1, \ldots, c_n)) \overline{\chi_{b_m}(a_m)} \right) = \\
&= \frac{1}{q^m} \sum_{(b_1, \ldots, b_m) \in \mathbb{F}_q^m} \bar{\chi}_{b_1}(a_1) \ldots \bar{\chi}_{b_m}(a_m) \cdot \\
&\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} \chi_{b_1}(f_1(c_1, \ldots, c_n)) \ldots \chi_{b_m}(f_m(c_1, \ldots, c_n)) = \\
&= \frac{1}{q^m} \cdot q^n = q^{n-m}.
\end{aligned}$$

□

7.38. Следствие. *Многочлен $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ является перестановочным многочленом над полем $\mathbb{F}_q$ тогда и только тогда, когда*

$$\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} \chi(b(c_1, \ldots, c_n)) = 0$$

для любого нетривиального аддитивного характера χ поля $\mathbb{F}_q$.

7.39. Следствие. *Система многочленов $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, $1 \leqslant m \leqslant n$, является ортогональной системой над полем $\mathbb{F}_q$ тогда и только тогда, когда для любого набора $(b_1, \ldots, b_m) \in \mathbb{F}_q^m$, удовлетворяющего условию $(b_1, \ldots, b_m) \neq (0, \ldots, 0)$, многочлен $b_1 f_1 + \ldots + b_m f_m$ является перестановочным многочленом над полем $\mathbb{F}_q$.*

Доказательство. Утверждение вытекает из теоремы 7.37, следствия 7.38 и того, что $\chi_b(c) = \chi_1(bc)$ для любых $b, c \in \mathbb{F}_q$. □

Пусть $(x_1^q - x_1, \ldots, x_n^q - x_n)$ — идеал в кольце $\mathbb{F}_q[x_1, \ldots, x_n]$, состоящий из всех многочленов вида

$$g_1(x_1, \ldots, x_n)(x_1^q - x_1) + \cdots + g_n(x_1, \ldots, x_n)(x_n^q - x_n),$$

где $g_1, \ldots, g_n \in \mathbb{F}_q[x_1, \ldots, x_n]$. Тогда лемму 7.2 можно обобщить следующим образом.

7.40. Лемма. (i) *Для любого многочлена $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ найдется единственный многочлен $g \in \mathbb{F}_q[x_1, \ldots, x_n]$, имеющий по каждой переменной степень, меньшую чем q, и такой, что для любого набора $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ выполняется равенство $f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$.*

(ii) *Если $f, g \in \mathbb{F}_q[x_1, \ldots, x_n]$, то равенство $f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$ выполняется для всех наборов $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ тогда и только тогда, когда $f \equiv g \pmod{(x_1^q - x_1, \ldots, x_n^q - x_n)}$.*

(iii) *Для любого многочлена $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ найдется единственный многочлен $g \in \mathbb{F}_q[x_1, \ldots, x_n]$, имеющий по каждой переменной степень, меньшую чем q, и удовлетворяющий соотношению $f \equiv g \pmod{(x_1^q - x_1, \ldots, x_n^q - x_n)}$.*

Доказательство. (i) Существование многочлена g следует из (7.20). Для доказательства единственности достаточно показать, что если многочлен $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ имеет по каждой переменной степень, меньшую чем q, и $g(c_1, \ldots, c_n) = 0$ для всех наборов $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, то g является нулевым многочленом. Доказательство проведем индукцией по n. Заметим, во-первых, что случай $n = 1$ следует из леммы 7.2. Пусть $n \geqslant 2$, и предположим, что утверждение доказано для всех многочленов от $n - 1$

переменных. Если многочлен $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ является многочленом указанного вида, то мы можем записать

$$g(x_1, \ldots, x_n) = h_0(x_2, \ldots, x_n) + \\ + h_1(x_2, \ldots, x_n)x_1 + \cdots + h_{q-1}(x_2, \ldots, x_n)x_1^{q-1},$$

где каждый из многочленов h_j имеет по каждой из переменных $x_2, \ldots, x_n$ степень, меньшую чем q. Пусть зафиксирован набор $(c_2, \ldots, c_n) \in \mathbb{F}_q^{n-1}$. Из соотношения $g(c, c_2, \ldots, c_n) = 0$, которое должно выполняться для всех $c \in \mathbb{F}_q$, мы получаем систему из q однородных линейных уравнений относительно $h_j(c_2, \ldots, c_n)$, $0 \leqslant j \leqslant q-1$. Определителем этой системы является отличный от нуля определитель Вандермонда. Отсюда следует, что $h_j(c_2, \ldots, c_n) = 0$ для всех $0 \leqslant j \leqslant q-1$, а в силу того, что набор $(c_2, \ldots, c_n) \in \mathbb{F}_q^{n-1}$ выбран произвольно, по предположению индукции получаем, что все h_j равны 0 и, следовательно, $g = 0$.

(ii) Пусть $J = (x_1^q - x_1, \ldots, x_n^q - x_n)$. Если $f \equiv g \pmod{J}$, то очевидно, что $f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$ для всех наборов $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$. Обратно, пусть $f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$ для всех $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$. Соотношение $x_1^k \equiv x_i^m \pmod{J}$, $1 \leqslant i \leqslant n$, $k > m \geqslant 1$, которое выполняется тогда, когда $k \equiv m \pmod{(q-1)}$, позволяет получить многочлены f_1, g_1. Эти многочлены по каждой из переменных имеют степень, меньшую чем q, и удовлетворяют соотношениям $f \equiv f_1 \pmod{J}$, $g \equiv g_1 \pmod{J}$. Тогда

$$f_1(c_1, \ldots, c_n) = f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n) = g_1(c_1, \ldots, c_n)$$

для всех наборов $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$. Теперь из п. (i) следует, что $f_1 = g_1$ и, значит, $f \equiv g \pmod{J}$.

(iii) Этот пункт следует из пп. (i) и (ii). □

Однозначно определенный многочлен g из леммы 7.40 (iii) называется *результатом приведения* многочлена f по модулю идеала J и обозначается $f \pmod{(x_1^q - x_1, \ldots, x_n^q - x_n)}$. Теперь мы можем следующим образом обобщить теорему 7.6.

7.41. Теорема. *Пусть p — характеристика поля $\mathbb{F}_q$. Тогда система многочленов $f_1, \ldots, f_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ является ортогональной системой над полем $\mathbb{F}_q$ тогда и только тогда, когда выполняются следующие два условия:*

(i) *в многочлене*

$$f_1^{q-1} \ldots f_n^{q-1} \pmod{(x_1^q - x_1, \ldots, x_n^q - x_n)}$$

коэффициент при $x_1^{q-1} \ldots x_n^{q-1}$ не равен 0;

(ii) *в многочлене*

$$f_1^{t_1} \dots f_n^{t_n} \pmod{(x_1^q - x_1, \dots, x_n^q - x_n)}$$

коэффициент при $x_1^{q-1} \dots x_n^{q-1}$ *равен* 0, *если* $t_1, \dots, t_n$ — *целые числа, удовлетворяющие условиям* $0 \leqslant t_i \leqslant q-1$, $1 \leqslant i \leqslant n$, *не все* t_i *равны* $q-1$ *и хотя бы одно* t_i *не сравнимо с* 0 *по модулю* p.

Доказательство. Пусть многочлены $f_1, \dots, f_n$ образуют ортогональную систему над полем $\mathbb{F}_q$, и пусть $t_1, \dots, t_n \in Z$ — такие числа, что $0 \leqslant t_i \leqslant q-1$ для $1 \leqslant i \leqslant n$. Если через g обозначить многочлен

$$f_1^{t_1} \dots f_n^{t_n} \pmod{(x_1^q - x_1, \dots, x_n^q - x_n)},$$

то в силу леммы 7.40 и формулы (7.20) многочлен $g(x_1, \dots, x_n$ имеет вид

$$g(x_1, \dots, x_n) = \sum_{(c_1, \dots, c_n) \in \mathbb{F}_q^n} (f_1^{t_1} \dots f_n^{t_n})(c_1, \dots, c_n) \cdot \\ \cdot (1 - (x_1 - c_1)^{q-1}) \dots (1 - (x_n - c_n)^{q-1}).$$

Тогда коэффициент при $x_1^{q-1} \dots x_n^{q-1}$ в многочлене g равняется

$$(-1)^n \sum_{(c_1, \dots, c_n) \in \mathbb{F}_q^n} (f_1^{t_1} \dots f_n^{t_n})(c_1, \dots, c_n) = \\ = (-1)^n \sum_{(c_1, \dots, c_n) \in \mathbb{F}_q^n} f_1(c_1, \dots, c_n)^{t_1} \dots f_n(c_1, \dots, c_n)^{t_n} = \\ = (-1)^n \sum_{(a_1, \dots, a_n) \in \mathbb{F}_q^n} a_1^{t_1} \dots a_n^{t_n} = \\ = (-1)^n \left(\sum_{a_1 \in \mathbb{F}_q} a_1^{t_1} \right) \dots \left(\sum_{a_n \in \mathbb{F}_q} a_n^{t_n} \right).$$

Условия (i) и (ii) следуют теперь из леммы 7.3.

Обратно, пусть выполнены условия (i) и (ii). Тогда в силу проведенных выше вычислений из (i) следует, что

$$\sum_{(c_1, \dots, c_n) \in \mathbb{F}_q^n} (f_1^{q-1} \dots f_n^{q-1})(c_1, \dots, c_n) \neq 0, \qquad (7.21)$$

а из (ii) вытекает, что

$$\sum_{(c_1, \dots, c_n) \in \mathbb{F}_q^n} (f_1^{t_1} \dots f_n^{t_n})(c_1, \dots, c_n) = 0$$

для $t_1, \ldots, t_n$ из условия (ii). Используя равенство

$$\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} f(c_1, \ldots, c_n)^{tp^j} = \left(\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} f(c_1, \ldots, c_n)^t \right)^{p^j},$$

получаем, что

$$\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} (f_1^{t_1} \ldots f_n^{t_n})(c_1, \ldots, c_n) = 0 \qquad (7.22)$$

для $t_1, \ldots, t_n \in Z$, таких, что $0 \leqslant t_i \leqslant q-1$ при $1 \leqslant i \leqslant n$, не все t_i равны $q-1$ и не все t_i равны 0. Равенство (7.22) тривиально выполняется для $t_1 = \ldots = t_n = 0$. Для того чтобы показать, что многочлены $f_1, \ldots, f_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ образуют ортогональную систему над полем $\mathbb{F}_q$, достаточно показать, что $N(a_1, \ldots, a_n) \neq 0$ для любого набора $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$, где через $N(a_1, \ldots, a_n)$ обозначено число решений системы уравнений

$$f_1(x_1, \ldots, x_n) = a_1, \ \ldots, \ f_n(x_1, \ldots, x_n) = a_n$$

в $\mathbb{F}_q^n$. Покажем, что если $N(a_1, \ldots, a_n)$ рассматривать как элемент поля $\mathbb{F}_q$, то он отличен от 0. В самом деле, в силу (7.21) и (7.22)

$$N(a_1, \ldots, a_n) = (-1)^n \sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} \prod_{i=1}^{n} [(f_i(c_1, \ldots, c_n) - a_i)^{q-1} - 1] =$$

$$= (-1)^n \sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} [f_1^{q-1} \ldots f_n^{q-1} +$$

$$+ \sum_{\substack{t_1, \ldots, t_n = 0 \\ \text{не все } t_i = q-1}}^{q-1} b_{t_1 \ldots t_n} f_1^{t_1} \ldots f_n^{t_n}](c_1, \ldots, c_n) =$$

$$= (-1)^n \sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} (f_1^{q-1} \ldots f_n^{q-1})(c_1, \ldots, c_n) \neq 0. \ \square$$

Результат, получаемый в следующей теореме, может быть использован для построения новых перестановочных многочленов на основе уже известных.

7.42. Теорема. *Пусть многочлен* $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ *имеет вид*

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_m) + h(x_{m+1}, \ldots, x_n), \quad 1 \leqslant m < n.$$

Если хотя бы один из многочленов g *или* h *является перестановочным многочленом над полем* $\mathbb{F}_q$, *то и* f *является перестановочным*

многочленом над полем $\mathbb{F}_q$. *Если же* q — *простое число, то верно и обратное утверждение.*

Доказательство. Если $a \in \mathbb{F}_q$, то обозначим через $N(a)$ число решений уравнения $f(x_1, \ldots, x_n) = a$ в $\mathbb{F}_q^n$, а через $L(a)$ и $M(a)$ обозначим соответственно число решений уравнений $g(x_1, \ldots, x_m) = a$ и $h(x_{m+1}, \ldots, x_n) = a$. Тогда

$$N(a) = \sum_{a_1+a_2=a} L(a_1) M(a_2). \tag{7.23}$$

Предположим для определенности, что g является перестановочным многочленом над полем $\mathbb{F}_q$. В этом случае для всех $a \in \mathbb{F}_q$ справедливо равенство $L(a) = q^{m-1}$, и тогда из (7.23) следует, что

$$N(a) = q^{m-1} \sum_{a_2 \in \mathbb{F}_q} M(a_2) = q^{m-1} q^{n-m} = q^{n-1}.$$

Последнее означает, что $f(x_1, \ldots, x_n)$ является перестановочным многочленом над полем $\mathbb{F}_q$.

Пусть p — простое число, а $f(x_1, \ldots, x_n)$ — перестановочный многочлен над полем $\mathbb{F}_p$. Мы хотим показать, что в этом случае или g, или h является перестановочным многочленом над полем $\mathbb{F}_p$. Из (7.23) получаем, что

$$\sum_{a_1+a_2=a} L(a_1) M(a_2) = p^{n-1} \quad \text{для любого элемента } a \in \mathbb{F}_p.$$

Если выписать эти равенства для значений $a = -1, 0, 1, \ldots, p-2$, то получится система линейных уравнений относительно $M(p-1), M(p-2), \ldots, M(0)$. Пусть матрица этой системы имеет вид $(d_{ij})_{1 \leqslant i,j \leqslant p}$, $d_{ij} = L(i+j-2)$, где $i+j-2$ берется по модулю p. Пусть $D = \det(d_{ij})$. Если $D \neq 0$, то система имеет единственное решение, а именно $M(p-1) = M(p-2) = \ldots = M(0) = p^{n-m-1}$. Отсюда следует, что h является перестановочным многочленом над полем $\mathbb{F}_p$. Предположим, что $D = 0$. Воспользуемся тем фактом, что $D = \pm R$, где R — результант двух многочленов $G(x) = x^p - 1$ и $H(x) = L(0) x^{p-1} + L(1) x^{p-2} + \ldots + L(p-1)$ над полем рациональных чисел. Тогда $G(x)$ и $H(x)$ имеют общий корень в некотором расширении поля рациональных чисел. Но $G(x) = (x-1) Q_p(x)$, где $Q_p(x)$ — неприводимый p-круговой многочлен (см. теорему 2.47 (i)), а $H(1) = p^m \neq 0$. Следовательно, $Q_p(x)$ делит $H(x)$, т. е. $H(x) = L(0) Q_p(x)$. Приравнивая соответствующие коэффициенты, получаем $L(a) = L(0) = p^{m-1}$ для всех $a \in \mathbb{F}_p$; отсюда следует, что g является перестановочным многочленом над полем $\mathbb{F}_p$. □

7.43. Теорема. *Если* q — *степень простого числа (но не простое число), то для любого натурального* m, $1 \leqslant m < n$, *найдутся такие многочлены* $g(x_1, \ldots, x_m)$ *и* $h(x_{m+1}, \ldots, x_n)$ *над по-*

лем $\mathbb{F}_q$, *что* $g(x_1, \ldots, x_m) + h(x_{m+1}, \ldots, x_n)$ *является перестановочным многочленом над полем* $\mathbb{F}_q$, *но при этом ни* g, *ни* h *не являются перестановочными многочленами над* $\mathbb{F}_q$.

Доказательство. По условию теоремы $q = p^e$, где p — простое число, а $e > 1$. Порядок аддитивной факторгруппы $\mathbb{F}_q/\mathbb{F}_p$ равен $r = p^{e-1}$. Построим систему элементов $a_1, \ldots, a_r \in \mathbb{F}_q$, выбирая в качестве a_i представителей из всех смежных классов. Пусть L и M имеют тот же смысл, что и в теореме 7.42. В силу (7.20) существуют многочлены $g(x_1, \ldots, x_m)$ и $h(x_{m+1}, \ldots, x_n)$ над полем $\mathbb{F}_q$, такие, что $L(a_j) = (1/r)\, q^m$ для $1 \leqslant j \leqslant r$, $L(c) = 0$ для всех остальных элементов $c \in \mathbb{F}_q$ и $M(0) = M(1) = \ldots = M(p-1) = (1/p)\, q^{n-m}$, а $M(d) = 0$ для всех остальных элементов $d \in \mathbb{F}_q$. Ни $g(x_1, \ldots, x_m)$, ни $h(x_{m+1}, \ldots, x_n)$ не являются перестановочными многочленами над полем $\mathbb{F}_q$. Однако $g + h$ — перестановочный многочлен над $\mathbb{F}_q$. Действительно, любой элемент $a \in \mathbb{F}_q$ можно единственным образом представить в виде $a = a_j + b$, где $1 \leqslant j \leqslant r$ и $b \in \mathbb{F}_p$. Отсюда следует, что общее число решений уравнения

$$g(x_1, \ldots, x_m) + h(x_{m+1}, \ldots, x_n) = a = a_j + b$$

в $\mathbb{F}_q^n$ равняется

$$\left(\frac{1}{r} q^m\right)\left(\frac{1}{p} q^{n-m}\right) = q^{n-1}. \qquad \square$$

Следующая теорема устанавливает полезное взаимно однозначное соответствие между ортогональными системами над полем $\mathbb{F}_q$, образованными m многочленами от $n = mk$ переменных, и перестановочными многочленами от k переменных над полем $\mathbb{F}_{q^m}$.

7.44. Теорема. *Если* n, m, k — *натуральные числа, связанные соотношением* $n = mk$, *то существует взаимно однозначное соответствие между ортогональными системами над полем* $\mathbb{F}_q$, *которые состоят из* m *многочленов над полем* $\mathbb{F}_q$, *имеющих по каждой из* n *переменных степень, меньшую чем* q, *и перестановочными многочленами над полем* $\mathbb{F}_{q^m}$, *имеющими по каждой из* k *переменных степень, меньшую чем* q^m.

Доказательство. Пусть $\{\omega_1, \ldots, \omega_m\}$ — базис векторного пространства $E = \mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$. Каждый набор $(\gamma_1, \ldots, \gamma_k) \in E^k$ однозначно определяет набор $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ по формуле

$$\gamma_i = c_{(i-1)m+1}\omega_1 + c_{(i-1)m+2}\omega_2 + \cdots + c_{im}\omega_m, \quad 1 \leqslant i \leqslant k.$$

Пусть многочлены $f_1, \ldots, f_m$ имеют по каждой из n переменных степень, меньшую чем q, и образуют при этом ортогональную систему над полем $\mathbb{F}_q$. В силу (7.20) и леммы 7.40 найдется един-

ственный многочлен g над полем E, имеющий по каждой из своих k переменных степень, меньшую чем q^m, и такой, что

$$g(\gamma_1, \ldots, \gamma_k) = f_1(c_1, \ldots, c_n)\omega_1 + \cdots + f_m(c_1, \ldots, c_n)\omega_m \quad (7.24)$$

для всех наборов $(\gamma_1, \ldots, \gamma_k) \in E^k$. Тогда g является перестановочным многочленом над полем E. Действительно, для любого $\alpha = a_1\omega_1 + \ldots + a_m\omega_m \in E$, где $a_1, \ldots, a_m \in \mathbb{F}_q$, равенство $g(\gamma_1, \ldots, \gamma_k) = \alpha$ выполняется тогда и только тогда, когда $f_j(c_1, \ldots, c_n) = a_j$, где $1 \leqslant j \leqslant m$. Таким образом, имеется $q^{n-m} = (q^m)^{k-1}$ решений вида $(\gamma_1, \ldots, \gamma_k)$. С другой стороны, если g — данный перестановочный многочлен над полем E, имеющий по каждой из своих k переменных степень, меньшую чем q^m, то ортогональная система многочленов $f_1, \ldots, f_m$ над полем $\mathbb{F}_q$ рассматриваемого типа может быть однозначно восстановлена с помощью многочленов над полем $\mathbb{F}_q$, имеющих по каждой из своих переменных степень, меньшую чем q. Это многочлены $f_1, \ldots, f_m$ из формулы (7.24), которые представляют собой координатные функции относительно базиса $\{\omega_1, \ldots, \omega_m\}$. □

В частном случае $m = n$ мы получаем такое простое следствие из доказанной выше теоремы:

7.45. Следствие. *Существует взаимно однозначное соответствие между ортогональными системами над полем $\mathbb{F}_q$, которые состоят из n многочленов над полем $\mathbb{F}_q$, имеющих по каждой из n своих переменных степень, меньшую чем q, и перестановочными многочленами от одной переменной над полем $\mathbb{F}_{q^n}$, имеющими степень, меньшую чем q^n.*

Нетривиальные примеры ортогональных систем можно получить с помощью следующего обобщения многочленов Диксона (см. § 2). Для $n \in \mathbb{N}$, $a \in \mathbb{F}_q$ и $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ рассмотрим многочлен

$$r(c_1, \ldots, c_n, z) = z^{n+1} - c_1 z^n + c_2 z^{n-1} + \cdots$$
$$\cdots + (-1)^n c_n z + (-1)^{n+1} a \quad (7.25)$$

от переменной z над полем $\mathbb{F}_q$. Этот многочлен имеет $n+1$ не обязательно различных корней $\beta_1, \ldots, \beta_{n+1}$ в подходящем расширении поля $\mathbb{F}_q$. Пусть теперь $k \in \mathbb{N}$; положим

$$r_k(c_1, \ldots c_n, z) = (z - \beta_1^k) \ldots (z - \beta_{n+1}^k).$$

Тогда

$$r_k(c_1, \ldots, c_n, z) =$$
$$= z^{n+1} - \sigma_1(\beta_1^k, \ldots, \beta_{n+1}^k) z^n + \cdots + (-1)^{n+1} \sigma_{n+1}(\beta_1^k, \ldots, \beta_{n+1}^k),$$

где σ_i есть i-й элементарный симметрический многочлен от $n+1$ переменных (ср. с примером 1.74). Так как $\sigma_i(u_1^k, \ldots, u_{n+1}^k)$

является симметрическим многочленом от переменных $u_1, \ldots, u_{n+1}$, то существуют многочлены $g_k^{(1)}, \ldots, g_k^{(n+1)}$ от $n+1$ переменных над Z, такие, что

$$\sigma_i(u_1^k, \ldots u_{n+1}^k) = g_k^{(i)}(\sigma_1(u_1, \ldots, u_{n+1}), \ldots, \sigma_{n+1}(u_1, \ldots, u_{n+1})),$$
$$1 \leqslant i \leqslant n+1.$$

Учитывая, что $\beta_1, \ldots, \beta_{n+1}$ — корни многочлена (7.25), получаем

$$\sigma_i(\beta_1, \ldots, \beta_{n+1}) = c_i \quad \text{для} \quad 1 \leqslant i \leqslant n,$$
$$\sigma_{n+1}(\beta_1, \ldots, \beta_{n+1}) = \beta_1 \ldots \beta_{n+1} = a,$$

так что

$$\sigma_i(\beta_1^k, \ldots, \beta_{n+1}^k) = g_k^{(i)}(c_1, \ldots, c_n, a) \quad \text{для} \quad 1 \leqslant i \leqslant n+1.$$

Подставляя полученные выражения в $r_k(c_1, \ldots, c_n, z)$, получаем

$$r_k(c_1, \ldots, c_n, z) = z^{n+1} - g_k^{(1)}(c_1, \ldots, c_n, a)\, z^n + \cdots$$
$$\cdots + (-1)^n g_k^{(n)}(c_1, \ldots, c_n, a)\, z + (-1)^{n+1} a^k.$$

Многочлены

$$g_k^{(i)}(x_1, \ldots, x_n, a), \quad 1 \leqslant i \leqslant n,$$

являются многочленами от $x_1, \ldots, x_n, a$ над Z и, таким образом, являются многочленами над полем $\mathbb{F}_q$ от переменных $x_1, \ldots, x_n$. Последние многочлены называются *многочленами Диксона от n переменных* над полем $\mathbb{F}_q$. Это определение можно сделать содержательным для любого коммутативного кольца R с единицей. Выберем $a \in R$. Если $n = 1$, то многочлен $g_k^{(1)}(x_1, a)$ совпадает с многочленом Диксона от одной переменной, определенным формулой (7.6).

Явное выражение для многочленов $g_k^{(1)}(x_1, \ldots, x_n, a)$ можно получить из формулы Варинга (см. теорему 1.76). Например, для $n = 2$ получаем

$$g_k^{(1)}(x, y, a) =$$
$$= \sum_{\substack{i=0 \\ 2i+3j \leqslant k}}^{\lfloor k/2 \rfloor} \sum_{j=0}^{\lfloor k/3 \rfloor} \frac{k(-1)^i}{k-i-2j} \binom{k-i-2j}{i+j} \binom{i+j}{i} a^j x^{k-2i-3j} y^i.$$

Через $g_k(a)$ обозначим систему, состоящую из многочленов $g_k^{(1)}(x_1, \ldots, x_n, a), \ldots, g_k^{(n)}(x_1, \ldots, x_n, a)$. Справедливо следующее обобщение теорем 7.16 и 7.8 (ii).

7.46. Теорема. *Если $a \in \mathbb{F}_q^*$, то система $g_k(a)$ является ортогональной системой многочленов над полем $\mathbb{F}_q$ тогда и только тогда, когда* НОД $(k, q^s - 1) = 1$ *для всех* $s = 1, 2, \ldots, n+1$.

Система $g_k(0)$ *ортогональна над* $\mathbb{F}_q$ *тогда и только тогда, когда* НОД $(k, q^s - 1) = 1$ *для всех* $s = 1, 2, \ldots, n$.

Как было установлено выше, каждый многочлен, входящий в ортогональную систему $g_k(a)$, является перестановочным многочленом от n переменных над полем $\mathbb{F}_q$. Другой класс перестановочных многочленов от нескольких переменных можно получить, рассматривая линейные и квадратичные многочлены. Заметим, во-первых, что свойство быть перестановочным многочленом над полем $\mathbb{F}_q$ инвариантно относительно любых преобразований переменных вида

$$x_i = \sum_{j=1}^{n} a_{ij} y_j + b_i, \quad 1 \leqslant i \leqslant n, \tag{7.26}$$

где $a_{ij}, b_j \in \mathbb{F}_q$, $1 \leqslant i, j \leqslant n$, а матрица (a_{ij}) невырожденна. Назовем два многочлена от n переменных над полем $\mathbb{F}_q$ *эквивалентными*, если один из них может быть преобразован в другой с помощью преобразований переменных вида (7.26).

7.47. **Теорема.** *Пусть* $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, *причем* $\deg(f) \leqslant 2$ *и* $n \geqslant 2$. *Если* q *нечетно, то* f *является перестановочным многочленом над полем* $\mathbb{F}_q$ *тогда и только тогда, когда он эквивалентен многочлену вида* $g(x_1, \ldots, x_{n-1}) + x_n$ *для некоторого* $g \in \mathbb{F}_q[x_1, \ldots, x_{n-1}]$. *Если же* q *четно, то* f *является перестановочным многочленом над полем* $\mathbb{F}_q$ *тогда и только тогда, когда он эквивалентен или многочлену вида* $g(x_1, \ldots, x_{n-1}) + x_n$, *или многочлену вида* $g(x_1, \ldots, x_{n-1}) + x_n^2$, *где* $g(x_1, \ldots, x_{n-1})$ — *некоторый многочлен из* $\mathbb{F}_q[x_1, \ldots, x_{n-1}]$.

Пусть q нечетно, $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ и $\deg(f) \leqslant 2$, и пусть A — матрица коэффициентов квадратичной формы, соответствующей многочлену f (см. § 2 гл. 6). Пусть A' — расширенная матрица, образованная матрицей A и еще одним столбцом, содержащим коэффициенты линейных членов. Тогда из теоремы 7.47 легко следует, что f является перестановочным многочленом над полем $\mathbb{F}_q$ в том и только том случае, если $\operatorname{rg}(A') > \operatorname{rg}(A)$.

Комментарии

§ 1. Изучение перестановочных многочленов как таковых было начато в работе Эрмита (Hermite [2]), где рассматривался случай конечных простых полей. Отдельные результаты из числа первых в этом направлении можно также обнаружить в работах Jordan C. [2], Serret [2]. Перестановочные многочлены произвольного конечного поля впервые изучались в работе Диксона Dickson [2]. Основные результаты, полученные в этой работе, можно также найти в моиографии Dickson [7, part I, ch. 5].

История развития этой области до 1922 г. освещена в книге Dickson [42, ch. 18]. Результаты современных исследований по перестановочным многочленам представлены в книге Lausch, Nöbauer [1, ch. 4].

Тот факт, что любую функцию из $\mathbb{F}_q$ в $\mathbb{F}_q$ можно представить с помощью многочлена над полем $\mathbb{F}_q$, был впервые отмечен Эрмитом (Hermite [2]) для простого q (см. также Weber [4, sec. 180], Zsigmondy [3]) и Диксоном (Dickson [2]) для произвольного q. В той же работе Диксон показал, что условие $\deg(g) < q$ позволяет однозначно определить многочлен g, представляющий данную функцию. Различные методы получения многочлена g в явном виде обсуждались в работах Bernstein [2], Gill, Jacob [1], Székely, Mureşan [1], Wesselkamper [1]. В работах Zsigmondy [3], Dickson [2] и Carlitz [86] было отмечено, что перестановочные многочлены поля $\mathbb{F}_q$ можно получать, применяя интерполяционную формулу к функциям, осуществляющим перестановки элементов множества $\mathbb{F}_q$. Полиномиальные представления для функций из $\mathbb{F}_p$ в себя, принимающих лишь значения 0 и 1, рассматривались в статьях Carlitz [123] и Cazacu [1]. Весселькампер (Wesselkamper [2], [3]) изучал аналогичные представления для функций, определенных на подмножествах поля $\mathbb{F}_q$.

Конечные поля являются полиномиально полными в смысле следующего определения: кольцо R называется *полиномиально полным*, если любая функция из R в себя может быть представлена многочленом над R. Кемпнер (Kempner [1]) показал, что среди колец вычетов $Z/(m)$ полиномиально полными являются только конечные простые поля (см. также Bernstein [2]). В работе Rédei, Szele [1] доказан более общий результат, а именно что среди ненулевых коммутативных колец полиномиально полными являются только конечные поля, а Хайслер (Heisler [1]) доказал тот же результат, но без требования коммутативности. Общее обсуждение полиномиально полных алгебраических структур можно найти в книге Lausch, Nöbauer [1, ch. 1]. Пользуясь более общим понятием многочлена над кольцом R, Броули и Карлиц (Brawley, Carlitz [2]) показали, что каждую функцию из R в себя можно представить таким многочленом тогда и только тогда, когда R является тривиальным кольцом порядка 1 либо 2 (т. е. когда $ab = 0$ для $a, b \in R$) или когда R является кольцом $n \times n$-матриц над конечным полем $\mathbb{F}_q$ для некоторого $n \in \mathbb{N}$. Полиномиальные функции над кольцами последнего типа изучались также в статье Brawley [5].

Некоторое внимание уделялось изучению функций, отображающих кольцо $R_m = Z/(m)$ в себя. Если m — составное число, то, согласно отмеченному выше результату Кемпнера (Kempner [1]), не всякую такую функцию можно представить многочленом над кольцом R_m. Критерии для существования такого представления

получены в работах Kempner [1], Rédei, Szele [1], [2], Carlitz [97]. Множество P_m всех функций из кольца R_m в себя, которые могут быть представлены многочленами над R_m, само является кольцом относительно обычных операций сложения и умножения функций. Простое применение теоремы о гомоморфизме колец показывает, что кольцо P_m изоморфно факторкольцу $R_m[x]/I_m$, где $I_m = \{f \in R_m[x] \mid f(a) = 0$ для всех $a \in R_m\}$. Многочлены, содержащиеся в идеале I_m, называются *вычетными многочленами по модулю m*. Различные свойства этих многочленов изучались в работах Aizenberg, Semion, Citkin [1], Kempner [1], Litzinger [1], Niven, Warren [1], Rédei, Szele [1], Singmaster [1]. Дальнейшие результаты, касающиеся полиномиальных функций над R_m, можно найти в работах Keller, Olson [1], Nöbauer [1], Rédei, Szele [2]. Свойства вычетных многочленов над произвольными кольцами рассматривались в книге Lausch, Nöbauer [1, ch. 3].

Одно из утверждений леммы 7.3, а именно что из условия (i) следует условие (ii), уже содержалось в лемме 6.3. Обратное утверждение, даже в более сильной форме, можно найти в работе Carlitz, Lutz [1]. Критерий, сформулированный в теореме 7.4, для конечных простых полей был получен в по существу эквивалентной форме в работе Эрмита Hermite [2]; для случая произвольных полей он был получен Диксоном в работе Dickson [2]. В работе Rogers L. J. [2] отмечено, что в случае простого числа q условие (ii) необходимо проверять лишь для $1 \leqslant t \leqslant (q-1)/2$, однако при составном q это не так (см. Dickson [7, sec. 96]). Критерий Эрмита в явной форме, выраженный через коэффициенты многочлена f, для простых полей $\mathbb{F}_p$ приводится в работе London, Ziegler [1]. Следствие 7.5 было получено Диксоном для простого числа q в работе Dickson [1], а для общего случая — в работе Dickson [2]. Доказательство достаточности в теореме 7.6 можно найти в статье Carlitz, Lutz [1]. Другие критерии того, чтобы многочлен был перестановочным многочленом, содержатся в работах de Polignac [1], Raussnitz [1], Vaughan T. P. [1].

По вопросу приложений перестановочных многочленов конечных полей к конечным проективным геометриям мы отсылаем читателя к § 3 гл. 9 и комментарням к этому же параграфу. В работе Levine, Brawley [2] показано, как перестановочные многочлены конечных полей можно использовать для построения криптографических систем.

Перестановочные многочлены колец вычетов $Z/(m)$ рассматривались в работах Nöbauer [1], [2], [4], [8] (см. также Cavior [5], Keller, Olson [1], Niven [2], Zane [1]). Теорию перестановочных многочленов над некоторыми обобщениями колец вычетов можно найти в книге Lausch, Nöbauer [1, ch. 4]. В работе Brawley, Carlitz, Levine [2] (см. также Matthews R. [1]),

а также в статье Brawley [4] изучались такие многочлены над $\mathbb{F}_q$, которые индуцируют перестановки в кольце $n \times n$-матриц над полем $\mathbb{F}_q$, а в работе Brawley [3] рассматривался более общий случай, когда поле $\mathbb{F}_q$ заменяется произвольным коммутативным кольцом с единицей. Човла (Chowla P. [1]) и Корзатт (Corzatt [1]) исследовали многочлены, индуцирующие перестановки множеств целых чисел. Рациональные функции, индуцирующие перестановки элементов поля $\mathbb{F}_q$, рассматривались в работах Rédei [4], Carlitz [86], Cohen S. D. [5], [6], [9], Gwehenberger [1], Nöbauer [8], [11]. Последний автор рассматривал также случай кольца вычетов $\mathbb{Z}/(m)$.

Перестановочные многочлены поля $\mathbb{F}_q$ характеризуются свойством $V(f) = q$, где $V(f)$ — мощность множества $\{f(c) \mid c \in \mathbb{F}_q\}$, т. е. множества значений, которые может принимать данный многочлен $f(x) \in \mathbb{F}_q[x]$ на всех элементах поля $\mathbb{F}_q$. Величина $V(f)$ изучалась и для произвольных многочленов $f(x) \in \mathbb{F}_q[x]$. Для многочленов малых степеней можно получить точные формулы, выражающие величину $V(f)$; случаи линейных и квадратичных многочленов являются совсем простыми, формулы для кубических многочленов и многочленов четвертой степени специального вида можно найти в работах von Sterneck [1] и Kantor [1]. Човла поставил задачу получить оценки для величин $V(f)$ (Chowla S. [7]). Бёрч и Свиннертон-Дайер в работе Birch, Swinnerton-Dyer [1] получили следующий замечательный результат: если $f(x) \in \mathbb{F}_q[x]$ — многочлен степени $n \geqslant 1$, который является «общим» многочленом (в том смысле, что группа Галуа уравнения $f(x) = y$ над полем $\overline{\mathbb{F}}_q(y)$, где $\overline{\mathbb{F}}_q$ — алгебраическое замыкание поля $\mathbb{F}_q$, является симметрической группой S_n), то

$$V(f) = q \sum_{j=1}^{n} \frac{(-1)^{j-1}}{j!} + O(q^{1/2}),$$

причем остаточный член зависит только от величины n. Для $n = 4$ результат аналогичного типа упоминается в работе Chowla S. [7], а его элементарное доказательство можно найти в работе McCann, Williams [2]. Несколько раньше Бёрча и Свиннертона-Дайера Утияма (Uchiyama [2]) доказал следующий более слабый результат: если $n \geqslant 4$ и многочлен $[f(x) - f(y)]/(x - y)$ является абсолютно неприводимым, то $V(f) > q/2$ при условии, что характеристика поля $\mathbb{F}_q$ достаточно велика. Вильямс (Williams K. S. [4]) оценил число «общих» многочленов над полем $\mathbb{F}_q$ фиксированной степени n и получил точные формулы для малых n. Результаты о среднем значении величины $V(f)$, когда f пробегает все нормированные многочлены фиксированной степени n над полем $\mathbb{F}_q$, удовлетворяющие условию $f(0) = 0$, можно найти в работах Carlitz [61], Uchiyama [3], [6]; см. также Carlitz, Uchiyama

[1], Williams K. S. [4]. Случай, когда фиксированы коэффициенты при более высоких степенях переменной в многочлене $f(x)$, исследовался в работах Uchiyama [5] и Cohen S. D. [8]. Указанный выше результат Бёрча и Свиннертона-Дайера был распространен Коэном (Cohen S. D. [5]) на случай рациональных функций. Если $f \in \mathbb{F}_q[x]$ и $\deg(f) = n \geqslant 1$, то из того, что уравнение $f(x) = d \in \mathbb{F}_q$ может иметь в $\mathbb{F}_q$ не более n решений, легко вытекает, что $V(f) \geqslant \lfloor (q-1)/n \rfloor + 1$. В статье Carlitz, Lewis, Mills, Straus [1] показано, что если $V(f) = \lfloor (q-1)/n \rfloor + 1 \geqslant 3$, а n строго меньше характеристики поля $\mathbb{F}_q$, то $q \equiv 1 \pmod{n}$, и f имеет вид $f(x) = a(x-b)^n + c$, где $a, b, c \in \mathbb{F}_q$. Дальнейшие обобщения этого результата можно найти в работах Mills [1], Mordell [16] и Williams K. S. [5].

Число значений многочлена $f(x) \in \mathbb{F}_p[x]$, которые встречаются в множествах вида $\{1, 2, \ldots, h\}$, $1 \leqslant h < p$, изучалось в статье McCann, Williams [1] в случае, когда $f(x)$ — кубический многочлен, и в статье Williams K. S. [5] в случае, когда многочлен $[f(x) - f(y)]/(x-y)$ не имеет нелинейных абсолютно неприводимых делителей. Коэн (Cohen S. D. [7]) оценил среднее число значений многочлена $f \in \mathbb{F}_q[x]$, содержащихся в тех или иных подмножествах поля $\mathbb{F}_q$. Полученные им результаты усиливают и обобщают более ранний результат Вильямса (Williams K. S. [15]). В случае когда $f \in \mathbb{F}_p[x]$ — кубический многочлен, который не является перестановочным многочленом поля $\mathbb{F}_p$, Морделл в работе Mordell [19] получил оценку для наименьшего неотрицательного вычета k по модулю p, не встречающегося в качестве значений многочлена f, а Бомбьери и Дэвенпорт (Bombieri, Davenport [1]) нашли аналогичную оценку для общего случая. В работе Tietäväinen [5] указанная общая оценка улучшается: а именно показано, что $k < C(n)\, p^{1/2}$, где константа $C(n)$ зависит только от $n = \deg(f)$. Для случая $n = 4$ результат Бомбьери и Дэвенпорта был также получен Хадсоном (Hudson M. [1]) и Вильямсом (Williams K. S. [2]). Морделл в работе Mordell [19] также показал, что если f — многочлен положительной степени над простым полем $\mathbb{F}_p$, то минимальный неотрицательный вычет l по модулю p, встречающийся среди множества значений многочлена f, удовлетворяет неравенству $l \leqslant np^{1/2} \log p$. Аналогичный результат для случая произвольного поля $\mathbb{F}_q$ был получен в работе Cavior [4], а затем улучшен в статье Tietäväinen [4]. Другие результаты, касающиеся распределения элементов, входящих в множество значений многочлена f, можно найти в работах Mazur L. E. [1], McCann, Williams [2], Tietäväinen [7], Williams K. S. [6], [8] и Перельмутер [8].

Связь между двумя многочленами над полем $\mathbb{F}_p$, имеющими одинаковую степень и совпадающие множества значений, исследовалась в работе Williams K. S. [10] для случая квадратичных

многочленов и в работе McCann, Williams [3] для случая кубических многочленов. Связь между многочленами и рациональными функциями, для которых заданы соотношения между множествами их значений, исследовалась в работах Cohen S. D. [6], [9] и Fried [1], [5]. Диксон в работе Dickson [23] положил начало изучению таких многочленов над полем $\mathbb{F}_q$ нечетной характеристики, для которых множество принимаемых ими значений состоит из одних квадратов, отличных от нуля, а Карлиц (Carlitz [29]) показал, что если такие многочлены f удовлетворяют условию $\deg(f) = n$ и $q > (n-1)^2$, то $f = g^2$ для некоторого $g \in \mathbb{F}_q[x]$. Дальнейшие исследования в этом направлении, а также некоторые приложения можно найти в работах Carlitz [77], [89], Rédei [2], Birch, Lewis [2]. Результат, аналогичный результату работы Carlitz [29] и касающийся многочленов над полем $\mathbb{F}_q$, значения которых являются отличными от нуля d-ми степенями при $q \equiv 1 \pmod{d}$, был получен в работе Carlitz [38]. В работе Ribenboim [1] изучались аналогичные многочлены над полями алгебраических функций с элементами конечного поля в качестве констант. Редеи в книге Rédei [11, ch. 1] описал многочлены над полем $\mathbb{F}_q$ со значениями из некоторого подполя поля $\mathbb{F}_q$. В статье Tanner [2] рассматривались такие многочлены над простым полем нечетной характеристики, что $f(c) = \pm 1$ для всех $c \in \mathbb{F}_p^*$.

§ 2. Теорему 7.8 можно найти, например, в монографии Диксона Dickson [7, part I, ch. 5]. Цикловая структура отображений, задаваемых одночленами, изучалась в работе Ahmad [1]. Теорема 7.9 встречается в работе Mathieu [1]. Другие критерии для того, чтобы линеаризованные многочлены являлись перестановочными многочленами, приводятся в § 3 настоящей главы и в упр. 7.13 (см. также работу Carlitz [93]). В статье Раупе [1] ставится задача определить все такие 2-многочлены $L(x)$ над полем $\mathbb{F}_q$ характеристики 2, что как $L(x)$, так и $L(x)/x$ являются перестановочными многочленами поля $\mathbb{F}_q$. Теорема 7.10 доказана Роджерсом (Rogers L. J. [1]) для случая конечного простого поля и Диксоном (Dickson [2]) для случая произвольного конечного поля $\mathbb{F}_q$. Другие результаты о перестановочных многочленах указанного типа и родственных им многочленах можно найти в работах Ahmad [2], Dickson [7, part I, ch. 5], Fillmore [1], Nöbauer [8], Wells [1], [3]. Таблица нормализованных перестановочных многочленов над $\mathbb{F}_q$ степени не выше 5 взята из книги Dickson [7, part I, ch. 5]. Классификация таких перестановочных многочленов, а также нормализованных перестановочных многочленов степени 6 для поля $\mathbb{F}_q$ нечетной характеристики проводится в работе Dickson [2]. Для случая простого числа q эти результаты были получены еще в работе Dickson [1]. Другой подход к анализу случая, указанного в 12-й строке табл. 7.1, для простых q

приводится в статье Chowla S. [23]. Классификация некоторых типов перестановочных многочленов степеней 7 и 8 проведена соответственно в работах Dickson [2] и Cavior [1]. Перестановочные многочлены поля $\mathbb{F}_q$ для $q = 5$ приведены в работе Betti [1], для $q = 7$ — в работах Hermite [2], Brioschi [1], [3], Rogers L. J. [1], Dickson [2], а для других малых значений q — в работах Brioschi [1] и Dickson [1], [7, part I, ch. 5].

Теорема 7.11 получена в работе Niederreiter, Robinson [2]. Доказательство достаточности в этой теореме с условием $\eta(a^2 - 1) = 1$, замененным его эквивалентной формой из замечания 7.12, было получено ранее в работе Carlitz [83]. Простая форма этого условия приводится в упр. 7.9. Исследования перестановочных многочленов поля $\mathbb{F}_q$ вида $x^{m+1} + ax$, где m — делитель числа $q - 1$, а также некоторых других аналогичных многочленов можно найти в работах Carlitz [83], [93], Carlitz, Wells [1], Lausch, Nöbauer [1, ch. 4], Niederreiter, Robinson [2], см. также упр. 7.11. Теоремы 7.13 и 7.14 получены Карлицом (Carlitz [93]). В статьях Brioschi [1] и Grandi [2] изучались перестановочные многочлены поля $\mathbb{F}_p$ вида $x^{p-1-s} + ax^{(p-1-2s)/2}$. Вопрос о том, когда многочлен вида $x^{p-s} + ax^{(p-s+1)/2} + bx$ может быть перестановочным многочленом простого поля $\mathbb{F}_p$, исследовался в статьях Brioschi [2] и Grandi [1]. Другие частные случаи многочленов изучались в работах Carlitz [88] и Grandi [2].

Многочлены Диксона были введены в работе Dickson [2], см. также монографию Dickson [7, part I, ch. 5]. Теорема 7.16 получена в работе Nöbauer [10]. Ослабленный вариант этого критерия установил ранее Диксон (Dickson [2]). Другое доказательство достаточности приводится в статье Williams K. S. [25] Следствие 7.17 было отмечено Човлой в работе Chowla P. [2] Информацию о суммах Бревера можно найти в примечаниях к § 5 гл. 5 настоящей книги. Многочлены Диксона можно вычислять с помощью простой рекуррентной процедуры (см. упр. 7.15). Дальнейшие результаты, связанные с многочленами Диксона, содержатся в работах Dickson [2], [7, part I, ch. 5], Lausch, Nöbauer [1, ch. 4], Williams K. S. [25]. Многочлены Диксона как перестановочные многочлены кольца $Z/(m)$ изучаются в статьях Lausch, Müller, Nöbauer [1], Müller [1], Nöbauer [8], [12]. Взаимосвязь между рациональными перестановочными функциями (см. Rédei [4]) и многочленами Диксона была установлена Карлицом в работе Carlitz [86]. В статьях Carlitz [79] и Rosenberger [1] указаны некоторые приложения многочленов Чебышёва. Общую информацию о многочленах Чебышёва можно найти в книге Rivlin [1].

Значение многочленов Диксона особенно возрастает в связи с известной гипотезой Шура (Schur [4]) о том, что любой многочлен $f \in Z[x]$, являющийся перестановочным многочленом про-

стого поля $\mathbb{F}_p$ (т. е. рассматриваемый по модулю простого p) для бесконечного множества простых чисел p, может быть представлен в виде композиции двучлена $ax^n + b$ и многочлена Диксона. Шур в своей работе Schur [4] рассмотрел случай, когда $\deg(f)$ является простым числом, улучшив тем самым результат Диксона из работы Dickson [2]. В работе Wegner [1] исследовался случай, когда $\deg(f)$ является или произведением двух нечетных простых чисел, или степенью нечетного простого числа. Курбатов [3] исследовал случай, когда $\deg(f)$ является или произведением не более чем четырех нечетных простых чисел, или произведением степеней двух нечетных простых чисел. В другой своей работе [1] он показал, что если число $n = p_1 \dots p_k$, где p_i — различные нечетные простые числа и ни одно из p_i не может быть представлено как линейная комбинация с неотрицательными целочисленными коэффициентами остальных чисел p_i, то гипотеза Шура справедлива для случая $\deg(f) = n$. И наконец, справедливость гипотезы Шура была полностью доказана в работе Fried [2], где также был установлен аналогичный результат для многочленов над полями алгебраических чисел. Более того, в этой работе было показано, что если многочлен $f \in \mathbb{Q}[x]$ является композицией двучлена $ax^n + b$ и многочлена Диксона и если степень $\deg(f)$ взаимно проста с числом 6, то многочлен f является перестановочным многочленом поля $\mathbb{F}_p$ для бесконечного множества простых чисел p (см. также упр. 7.34). Близкими по тематике являются также работы Schur [4], Wegner [3], Fried [4], [5], Niederreiter, Lo [1] и Курбатов [2]. Если R — коммутативное кольцо с единицей и $f \in R[x]$, то множество всех (простых) идеалов J кольца R, таких, что f, рассматриваемый по модулю J, является перестановочным многочленом факторкольца R/J, называется (*простым*) *перестановочным спектром* многочлена f. Эти понятия были впервые рассмотрены для случая $R = \mathbb{Z}$ в работах Nöbauer [8], [9], а в общем случае в книге Lausch, Nöbauer [1, ch. 4]. Дополнительные замечания для случая $R = \mathbb{Z}$ можно найти в работе Narkiewicz [2]. Детальное исследование случая, когда R является кольцом целых в поле алгебраических чисел, было проведено Нидеррайтером и Ло в работе Niederreiter, Lo [1].

Карлиц в работе Carlitz [82] рассмотрел перестановочные многочлены поля $\mathbb{F}_q$ нечетной характеристики p, удовлетворяющие дополнительным условиям

$$(f(a) - f(b))^{(q-1)/2} = (a - b)^{(q-1)/2}, \quad a, b \in \mathbb{F}_q,$$

и показал, что если $\deg(f) < q$, то $f(x) = cx^{p^j} + d$, где $c \neq 0$ — ненулевой квадрат в поле $\mathbb{F}_q$, а d — произвольный элемент этого поля (см. также работу Goldberg [1]). Обобщение на случай многочленов от нескольких переменных приводится в работе Carlitz

[84]. Макконнел (McConnel [1]) обобщил результаты Карлица из работы Carlitz [82] в другом направлении и доказал результат, который можно сформулировать следующим образом: если G — собственная подгруппа группы $\mathbb{F}_q^*$, то многочлен $f \in \mathbb{F}_q[x]$, $\deg(f) < q$, удовлетворяет соотношению

$$(a-b)^{-1}(f(a)-f(b)) \in G \cdot \text{ для любых } a,\ b \in \mathbb{F}_q,\ a \neq b,$$

тогда и только тогда, когда f можно представить в виде $f(x) = cx^{p^j} + d$, где $c \in G$, $d \in \mathbb{F}_q$ и $p^j \equiv 1 \pmod m$, а m является индексом подгруппы G в группе $\mathbb{F}_q^*$. Другие доказательства этого результата приводятся в работе Bruen [1] для случая простого q и в работе Bruen, Levinger [1] для общего случая. В работах McConnel [1]—[3] эти результаты обобщаются на случай многочленов от нескольких переменных. В статье Grundhöfer [1] описываются все многочлены $f \in \mathbb{F}_q[x]$, которые удовлетворяют соотношению

$$(a-b)(f(a)-f(b)) \in G, \quad a,\ b \in \mathbb{F}_q,\ a \neq b.$$

В работе Glazek [1] изучались перестановочные многочлены поля $\mathbb{F}_q$, коммутирующие со всеми автоморфизмами этого поля.

Если оба многочлена $f(x)$ и $f(x)+x$ являются перестановочными многочленами поля $\mathbb{F}_q$, то $f(x)$ называется *вполне перестановочным многочленом* поля $\mathbb{F}_q$. Это понятие впервые было введено в статье Niederreiter, Robinson [1] и было детально изучено в работе Niederreiter, Robinson [2]. Човла и Цассенхаус (Chowla, Zassenhaus [1]) выдвинули следующую гипотезу: если $f(x) \in \mathbb{Z}[x]$, $\deg(f) \geqslant 2$, p — достаточно большое простое число и многочлен $f(x)$, рассматриваемый по модулю p, является перестановочным многочленом поля $\mathbb{F}_p$, то многочлен $f(x)+ax$ ни при каком $a \in \mathbb{F}_p^*$ не является перестановочным многочленом поля $\mathbb{F}_p$. В этой же работе выдвинута еще одна гипотеза: если $f \in \mathbb{Z}[x]$, $\deg(f) \geqslant 2$, p — достаточно большое простое число и миогочлен $f(x)$, рассматриваемый по модулю p, не является перестановочным многочленом поля $\mathbb{F}_p$, то найдется элемент $c \in \mathbb{F}_p$, такой, что многочлен $f(x)+c$ является неприводимым над полем $\mathbb{F}_p$.

§ 3. Теорема 7.18 была получена Карлицом в работе Carlitz [49]. Для случаев $q = 5$ и $q = 7$ этот результат был получен раньше соответственно в статьях Betti [1] и Dickson [2]. Аналог теоремы 7.18, связанный с транспозициями в произвольных полях, приводится в работе Carlitz [90]. С теоремой 7.18 также связано понятие *квазиперестановочного многочлена* (crude permutation polynomial) (см. Carlitz [93], а также упр. 7.22—7.24). Теоремы 7.19 и 7.21 получены в статье Wells [4]. Результат упр. 7.19 можно найти в работе Fryer [1]. Образующие групп S_{q+1} и A_{q+1}, выраженные через рациональные функции над полем $\mathbb{F}_q$, приведены в работе Wells [4]. Подгруппы группы S_p, p — простое

число, порожденные некоторыми перестановочными многочленами поля $\mathbb{F}_p$, изучались в статье Fryer [2].

Теоремы 7.22 и 7.23 получены в работе Nöbauer [10]. Группа $G(1)$ исследовалась также в книге Lausch, Nöbauer [1, ch. 4]. В статье Hule, Müller [1] охарактеризованы группы $G(a)$, являющиеся циклическими. Группы, аналогичные группам $G(a)$, но связанные с кольцами вычетов $Z/(m)$, изучались в работах Nöbauer [2] (в случае $a = 0$) и Lausch, Müller, Nöbauer [1], Müller [1], Nöbauer [12] (в случае $a = \pm 1$). Обобщения на случай нескольких переменных см. в примечаниях к § 5.

Группа Бетти—Матье впервые появляется в работах Betti [2], [3] и Mathieu [1]. Затем эта группа была исследована Диксоном (Dickson [2], [5], [7, part I, ch. 5]). Им же в работе Dickson [2] получен следующий критерий: для того чтобы $L(x)$ являлся перестановочным многочленом поля $\mathbb{F}_{q^r}$, необходимо и достаточно, чтобы $\det A \neq 0$. В этой же работе установлено взаимно однозначное соответствие между элементами группы Бетти—Матье и группы $GL(r, \mathbb{F}_q)$. Тот факт, что эти две группы изоморфны (теорема 7.24), впервые установлен в работе Bottema [1] (см. также Carlitz [91]). Изоморфизм между алгеброй линеаризированных многочленов вида (7.12) и алгеброй $r \times r$-матриц над полем $\mathbb{F}_q$ установлен в статьях Brawley, Carlitz, Vaughan [1] и Vaughan T. P. [1]. Ограничение этого результата на группу обратимых элементов снова приводит к теореме 7.24. В упомянутой выше работе Brawley, Carlitz, Vaughan [1] также изучалась группа перестановочных многочленов, для которых коэффициенты α_s в (7.12) берутся из данного подполя конечного поля $\mathbb{F}_{q^r}$.

Группы перестановочных многочленов, образуемые многочленами из теоремы 7.10, а также связанными с ними многочленами, изучались в работе Ahmad [2], Fillmore [1], Lausch, Nöbauer [1, ch. 4], Wells [1], [3]. В работе Carlitz, Hayes [1] изучалась группа всех перестановочных многочленов поля $\mathbb{F}_{q^r}$ с коэффициентами из поля $\mathbb{F}_q$; Мэттьюз (Matthews R. [3]) перенес эти результаты на случай многочленов от нескольких переменных. Нидеррайтер и Робинсон (Niederreiter, Robinson [2]) показали, что перестановочные многочлены поля $\mathbb{F}_q$, q нечетно, вида $ax^{(q+1)/2} + bx$ образуют группу относительно композиции по модулю $x^q - x$. Результаты упр. 7.20 и 7.21 (а также аналогичные результаты, показывающие, что большинство перестановок, которые перемещают лишь очень малое число элементов поля $\mathbb{F}_q$, представляются многочленами степени $q - 2$) можно найти в работе Wells [5]. Другие группы перестановочных многочленов кольца $Z/(m)$, помимо упомянутых выше, изучались в статьях Nöbauer [1], [4].

Из свойства (7.10) следует, что многочлены Диксона $g_k(x, a)$ с $a = 1$ коммутируют относительно операции композиции так же,

как и многочлены с $a = 0$. Этот результат породил многочисленную литературу, посвященную изучению многочленов f, g над полем F, удовлетворяющих условию $f(g(x)) = g(f(x))$. Классическими работами в этой области являются работы Fatou [1], Julia [1], Ritt [2], в которых изучается случай, когда F является полем комплексных чисел. Важным является понятие V-*цепи*, означающее последовательность многочленов над полем F, не являющихся постоянными и коммутирующих друг с другом, в которой содержатся многочлены всех положительных степеней. В статье Block, Thielman [1] описаны все V-цепи над полем $F = \mathbb{R}$. Якобсталь (Jacobsthal [3]) показал, что с точностью до естественной эквивалентности все V-цепи над полем F характеристики 0 — это V-цепи, образованные многочленами Диксона с $a = 0$ или $a = 1$. Аналогичный результат для произвольного поля F получен в работе Kautschitsch [1] (см. также Lausch, Nöbauer [1, ch. 4], Lidl [7]). Многочлены над полем $\mathbb{F}_q$, коммутирующие с данным линейным многочленом, описаны в работе Mullen [13]; случай нормированных линейных многочленов был изучен ранее в статье Wells [6]. Другие результаты о многочленах, коммутирующих с данным многочленом, можно найти в работах Bertram [1], Boyce [1], Kautschitsch [2]. Класс рациональных функций над полем $\mathbb{F}_q$, коммутирующих относительно операции композиции, появляется в статье Rédei [4].

Разложение многочленов на неразложимые многочлены (относительно операции композиции) и исследование свойств такого разложения проводились в статье Ritt [1] для случая многочленов над полем $\mathbb{C}$. Обобщение на случай полей характеристики 0 было сделано в работах Engstrom [3], Levi [1] (см. также Fried, MacRae [1], Dorey, Whaples [1], Lausch, Nöbauer [1, ch. 4]). Некоторые результаты для полей ненулевой характеристики содержатся также в работе Fried, MacRae [1]. Случай алгебраически замкнутого поля изучался в статьях Fried [3] и Клячко [1]. Здесь снова важную роль играют многочлены Диксона. С этой тематикой также связаны работы Bremner, Morton [1], Crampton, Whaples [1], Dorey, Whaples [1], Lausch, Nöbauer [1, ch. 3], Nöbauer [7]. Операция композиции многочленов по модулю $x^q - x$ была использована в работах Carlitz [47], Cavior [2], Mullen [1], [3], [5] при определении отношений эквивалентности для многочленов по модулю $x^q - x$ над полем $\mathbb{F}_q$.

§ 4. Исключительные многочлены были введены Дэвенпортом и Льюисом в работе Davenport, Lewis [2]. В этой же работе была выдвинута гипотеза о взаимосвязи этих многочленов с перестановочными многочленами. В статье MacCluer [1] доказано, что если $f \in \mathbb{F}_q[x]$ — исключительный многочлен и $\deg(f) < 2p$, где p — характеристика поля $\mathbb{F}_q$, то f является перестановочным многочленом поля $\mathbb{F}_q$. Коэн в работе Cohen S. D. [5] показал,

что этот результат остается справедливым и без ограничений на степень многочлена f, а также доказал аналогичный результат для рациональных функций над полем $\mathbb{F}_q$. Ослабленный вариант теоремы 7.27 может быть получен более элементарными методами; в приводимом доказательстве теоремы 7.27 мы следуем работе Williams K. S. [9]. Лемма 7.26 была получена тем же автором в работе Williams K. S. [5]. Теорема 7.29 для случая поля $\mathbb{F}_p$, p простое, была доказана Дэвенпортом и Льюисом (Davenport, Lewis [2]). С небольшими изменениями этот же результат содержится в работах Bombieri, Davenport [1] и Tietäväinen [5]. Вильямс (Williams K. S. [5]) заменил условие, что f является перестановочным многочленом поля $\mathbb{F}_p$, условием $V(f) = p + O(1)$. Теорема 7.29 в общем случае была доказана в работе Hayes [5], в этой же работе была получена теорема 7.31. Более сильный вариант теоремы 7.29, справедливый также и для рациональных функций над полем $\mathbb{F}_q$, был получен в работе Cohen S. D. [5]. Известной задачей в этой области является вопрос о том, остается ли следствие 7.32 справедливым, если условие НОД $(n, q) = 1$ заменить условием НОД $(2, q) = 1$. Если величина n является степенью числа 2, то ответ, безусловно, положительный. Единственными другими случаями, для которых опубликовано решение этой задачи, являются случаи $n = 6$ (Dickson [2]) и $n = 10$ (Hayes [5]); обсуждение вопросов, связанных с этой задачей, можно найти в работе Lidl [7].

В работе Fried [5] проведена классификация исключительных многочленов и рациональных функций над конечными полями. Вильямс (Williams K. S. [24]) выразил число абсолютно неприводимых делителей многочлена $[f(x) - f(y)]/(x - y)$ для достаточно большого q через число пар $(a, b) \in \mathbb{F}_q^2$, $a \neq b$, для которых $f(a) = f(b)$. Он же в работе Williams K. S. [25] для случая, когда f является многочленом Диксона, получил разложение многочлена $[f(x) - f(y)]/(x - y)$ над алгебраическим замыканием поля $\mathbb{F}_q$, откуда, в частности, можно вывести условие, при котором многочлен Диксона является перестановочным многочленом поля $\mathbb{F}_q$. Дальнейшие замечания об исключительных многочленах можно найти в работе Davenport, Lewis [2]. Вильямс (Williams K. S. [5]) назвал многочлен f *экстремальным многочленом индекса* k, если $[f(x) - f(y)]/(x - y)$ не имеет абсолютно неприводимых делителей, кроме k линейных делителей, и показал, что $V(f) = p/(k + 1) + O(1)$ для таких $f \in \mathbb{F}_p[x]$ при достаточно большом p. Частичное обращение этого утверждения было доказано ранее в работе Mordell [16]. Все эти результаты были улучшены и обобщены Коэном (Cohen S. D. [5]).

§ 5. Тот факт, что каждое отображение из $\mathbb{F}_q^n$ в $\mathbb{F}_q$ можно представить многочленом от n переменных над полем $\mathbb{F}_q$, имеющим

по каждой из переменной степень, меньшую чем q, для случая простого q был доказан Вебером (Weber [5, sec. 77]). Единственность такого представления (также для случая простого q) была доказана Гурвицом (Hurwitz [1]). В общем случае как представимость, так и единственность такого представления (см. формулу (7.20) и лемму 7.40) были установлены Диксоном (Dickson [24]). Результаты, связанные с теоремой единственности, содержатся в работе Mather [1]. Анализ взаимосвязи между отображениями и многочленами можно также найти в работе Joly [5]. Удобные методы для вычисления полиномиального представления данного отображения можно найти в работе Bernstein, Debely [1], а также в более поздних работах Benjauthrit, Reed [1], [2], Pradhan [1], Takahashi [1], Thayse [1], Yin [1]. В статьях Varnum [1] и Lehti [1] для этих же целей предложены матричные методы. Вычислительная сложность подобных интерполяционных процедур, а также сложность вычисления значений многочленов была исследована в работе Strassen [1], [2]; частный случай элементарных симметрических многочленов изучался Михайлюком [1], [2]. Выражения для характеристических функций подмножеств из $\mathbb{F}_p^n$ приводятся в работах Cazacu [2], [3] (см. также Rosenberg [3]). В статье Pizzarello [1] приводится критерий того, что многочлен от нескольких переменных над полем $\mathbb{F}_q$ является нулевым многочленом над некоторым конечным расширением поля $\mathbb{F}_q$. Отображения, определенные на подмножествах множества $\mathbb{F}_p^n$, исследовались в работах Bernstein [2], Bernstein, Debely [1]. Отображения из $(\mathbb{Z}/(m))^n$ в $\mathbb{Z}/(m)$, а также их представления многочленами изучались в работах Bernstein [1], Bernstein, Debely [1], Carlitz [97], Kempner [2], Rosenberg [2]. Полиномиальные отображения подобного типа, являющиеся нулем по некоторому модулю, были исследованы в работах Kempner [2], Lausch, Nöbauer [1, ch. 3], Litzinger [1], Nöbauer [3]. В статье Nöbauer [5] показано, что все коммутативные кольца R с единицей, для которых любое отображение из R^n в R может быть представлено многочленом из $R[x]$, являются конечными полями. Это обобщает результат из работы Redei, Szele [1], полученный для $n = 1$ (см. также Ceccherini [1]). Броули и Карлиц (Brawley, Carlitz [2]), пользуясь обобщением понятия многочлена, показали, что если R — ненулевое кольцо, а $n \geqslant 2$, то любое отображение из R^n в R можно представить одним из таких «многочленов» от n переменных над кольцом R тогда и только тогда, когда R является кольцом матриц над некоторым конечным полем. Возможность представления симметричных функций от счетного числа переменных многочленами над полем $\mathbb{F}_q$ от счетного числа переменных изучалась в статье Metropolis, Nicoletti, Rota [1].

Перестановочные многочлены от нескольких переменных и ортогональные системы впервые в явном виде появились в работах Карлица (Carlitz [47], [59]). Изучение этих понятий было затем продолжено в статье Nöbauer [6]. Ортогональные системы с $n = 2$ и простым q изучались Курбатовым и Старковым [1]. Ортогональные системы с $m = n$ называются также *перестановочными полиномиальными векторами*, так как они индуцируют перестановки элементов множества $\mathbb{F}_q^n$. Теорема 7.36 принадлежит Карлицу (Carlitz [59]); доказательство, приводимое нами, следует работе Niederreiter [2]. Теорема 7.37 также была получена Карлицом (Carlitz [47]), а следствие 7.39 принадлежит Нидеррайтеру (Niederreiter [2]). Другие критерии того, что система ортогональна, можно найти в упр. 7.47 или в работе Niederreiter [2]; критерии для перестановочных многочленов содержатся в работе Mullen [2]. В случае конечных простых полей можно привести специальный критерий перестановочности многочленов (см. упр. 7.32 и работу Niederreiter [3]). Теорема 7.41 является улучшением одного результата Лидла и Нидеррайтера (Lidl, Niederreiter [1]). Первая часть теоремы 7.42 получена в работе Nöbauer [6]; вторая часть для случая $m = 1$, $n = 2$ была доказана в работе Lidl [1], а для общего случая — в работе Lidl, Niederreiter [1]. Последняя содержит также доказательство теоремы 7.43. Теорема 7.44 доказана Нидеррайтером (Niederreiter [2]); следствие 7.45 принадлежит Карлицу (Carlitz [47]), а в случае $n = 2$ и простого q оно было также получено Курбатовым и Старковым [1]. Эти результаты позволяют перечислить все ортогональные системы, образованные многочленами над полем $\mathbb{F}_q$, имеющими по каждой из переменных степень, меньшую чем q. Это было сделано в статьях Carlitz [59], Niederreiter [2]. В работе Fried [4] теорема из статьи McCluer [1] перенесена на перестановочные полиномиальные векторы, причем показано, что мы получаем перестановочный полиномиальный вектор в случае, если система многочленов является в некотором смысле «исключительной». Формулы для выражения перестановок элементов множества $\mathbb{F}_q^n$ через перестановочные полиномиальные векторы приводятся в статье Lidl [2]. Перестановочные многочлены и перестановочные полиномиальные векторы над кольцами $\mathbb{Z}/(m)$ изучались в работах Lidl [3], Nöbauer [3], [6]; случай колец более общего вида рассматривался в книге Lausch, Nöbauer [1, ch. 4]. Аналогичные вопросы для рациональных функций от нескольких переменных рассматривались в работе Lidl [3].

Многочлены Диксона (или многочлены Чебышёва) от нескольких переменных были введены в работе Lidl, Wells [1]; там же была доказана теорема 7.46. Явные формулы, а также производящие функции и рекуррентные формулы для многочленов Дик-

сона от нескольких переменных можно найти в работах Eier, Lidl [1], Lidl [8], Lidl, Wells [1]. Ортогональные системы $g_k(a)$ из теоремы 7.46 замкнуты относительно операции композиции тогда и только тогда, когда $a = 0$, $a = 1$ или $a = -1$. Этот результат доказан Лидлом и Уэллсом (Lidl, Wells [1]) и обобщает теорему 7.22. Теоретико-групповые исследования, аналогичные теореме 7.23, содержатся в статьях Lidl [4], [6], Lidl, Müller [1], Matthews R. [1]. Для случая $n = 2$ системы $g_k(a)$, для которых якобиан отличен от нуля во всех точках пространства $\mathbb{F}_q^2$, были охарактеризованы в работе Lidl [5]; Мэттьюз (Matthews R. [2]) проделал то же самое для случая произвольного n. Предположение Лидла и Уэллса (Lidl, Wells [1]), в соответствии с которым многочлены Диксона от нескольких переменных играют ту же роль, которую играют многочлены Диксона от одной переменной в гипотезе Шура (Schur [4]) (см. примечания к § 2), было опровергнуто в статье Fried [4]. Системы многочленов Диксона от нескольких переменных изучались также в работе Matthews R. [2].

Теорема 7.47 получена Ниддеррайтером (Niederreiter [1]). В случае нечетного q этот же результат был независимо получен Лидлом (Lidl [1]). Аналогичный критерий, сформулированный в терминах рангов матрицы квадратичной формы и расширенной матрицы, можно найти в работе Niederreiter [3]. Муллен (Mullen [7], [8], [10]) изучал *локальные перестановочные многочлены* над полем $\mathbb{F}_q$ от $n \geqslant 2$ переменных, удовлетворяющие следующему условию: если зафиксировать любые значения из $\mathbb{F}_q$ для любых $n - 1$ переменных, то получающийся при этом многочлен от одной переменной является перестановочным многочленом поля $\mathbb{F}_q$. Системы образующих для групп перестановочных полиномиальных векторов относительно операции композиции были получены в работах Lidl [2] и Lidl, Niederreiter [1]. Мэттьюз (Matthews R. [3]) изучал группу перестановочных полиномиальных векторов над полем $\mathbb{F}_{q^r}$ с коэффициентами из $\mathbb{F}_q$. Приложение ортогональных систем над полем $\mathbb{F}_p$ к изучению силовских p-подгрупп симметрических групп S_{p^n} появляется у Калужнина [1]. Гудстейн (Goodstein [1]) показал, как с помощью операции композиции получить все многочлены от нескольких переменных над полем $\mathbb{F}_q$.

Теория соответствий и допустимых многочленов, приводимая в упр. 7.26—7.31, была развита Карлицом в работах Carlitz [115], [117], [121]. Понятие смежного класса для системы многочленов (см. упр. 7.49) появляется в работе Niederreiter [2]. Классы эквивалентности для многочленов и систем многочленов из $\mathbb{F}_q[x_1, \ldots, x_n]$, рассматриваемых по модулю идеала $(x_1^q - x_1, \ldots, x_n^q - x_n)$, изучались Карлицом в работах Carlitz [47, [59], [110] (см. также Cavior [6], Mullen [1], [2], [3], [9]). Аналогичные

понятия для матриц над конечными полями рассматривались в работах Brawley, Mullen [1], Chao [1], Mullen [4], [6], [11], [12].

Множества значений, принимаемых многочленами от нескольких переменных, стали предметом специального исследования. Кантор (Kantor [1]) получил формулу для числа значений, принимаемых произвольной квадратичной формой над полем $\mathbb{F}_p$, где p — нечетное простое число. В статье Williams K. S. [3] получено достаточное условие для того, чтобы множество значений многочлена над полем $\mathbb{F}_q$ совпадало с $\mathbb{F}_q$. Асимптотические результаты о распределении значений многочленов над конечными простыми полями были получены в работах Tietäväinen [10], Williams K. S. [7]. Частный случай элементарных симметрических многочленов был подробно изучен в работах Aberth [1], Akhtar [1], Fine [1]. Другие результаты, связанные с элементарными симметрическими многочленами, можно найти в работе Birch [1]. Нижние границы для числа значений, принимаемых диагональными формами, были получены в работах Chowla, Mann, Straus [1] (см. также Mann [3, ch. 2]) и Diderrich, Mann [1]. Диксон (Dickson [23], [28]) изучал однородные многочлены, множества значений которых содержат только квадраты или только кубы. Некоторые частные результаты о множествах значений, принимаемых системами многочленов, можно найти в работах Rédei [1], Rédei, Weinert [1] и Перельмутер [7]. Вопросы, связанные с множествами значений, принимаемых многочленами, имеют также непосредственную связь с вопросами решения уравнений в конечных полях (см. гл. 6).

[По тематике гл. 7 имеются также работы Nöbauer [1*], [2*].— *Перев.*]

Упражнения

7.1. Пусть $b \in \mathbb{F}_q$ — фиксированный элемент поля. Положим

$$f_b(x) = 1 - \sum_{i=0}^{q-1} b^{q-1-i} x^i.$$

Показать, что $f_b(a) = 0$, если $a \in \mathbb{F}_q$, $a \neq b$ и $f_b(b) = 1$. Пользуясь формулой (7.1), показать, что $\binom{q-1}{i} \equiv (-1)^i \pmod p$, где $0 \leqslant i \leqslant q-1$, а p — характеристика поля $\mathbb{F}_q$. (*Замечание.* Приведенное выше сравнение для биномиальных коэффициентов можно также вывести из равенства $(x-1)^{q-1} = (x^q-1)/(x-1)$.)

7.2. Доказать, что если q — простое число, то в условии (ii) теоремы 7.4 достаточно рассматривать целые t, заключенные в пределах $1 \leqslant t \leqslant (q-1)/2$. Привести пример, показывающий, что в случае, если $q = p^e$, $e > 1$, это не так.

7.3. Пусть $q = km + 1$, $k, m \in \mathbb{N}$. Показать, что многочлен x^{m+1} является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда НОД $(m+1, k) = 1$.

7.4. Доказать, что многочлен вида $x^{p^i} - ax^{p^k}$ над конечным полем $\mathbb{F}_q$ характеристики p является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда элемент a не является $(p^i - p^k)$-й степенью никакого элемента из $\mathbb{F}_q^*$.

7.5. Пусть p — характеристика поля $\mathbb{F}_q$, $r \in \mathbb{N}$, d — положительный делитель числа $p^r - 1$ и $a \in \mathbb{F}_q$. Показать, что многочлен вида $x(x^d - a)^{(p^r-1)/d}$ является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда элемент a не является d-й степенью никакого элемента из $\mathbb{F}_q^*$.

7.6. Пусть $a \in \mathbb{F}_q$, q нечетно, $r \in \mathbb{N}$ и НОД $(r, q-1) = 1$. Доказать, что многочлен вида $x^r(x^{(q-1)/2} - a)^2$ является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда $a \neq \pm 1$.

7.7. Найти все перестановочные многочлены поля $\mathbb{F}_7$ вида $x^r(x^3 - a)^2$, где $r \in \mathbb{N}$, $a \in \mathbb{F}_7$.

7.8. Показать, что многочлен $5x^5 + 5ax^3 + a^2x$ является перестановочным многочленом поля $\mathbb{F}_q$, если $q \equiv \pm 2 \pmod 5$, а a — произвольный элемент поля $\mathbb{F}_q$.

7.9. Показать, что многочлен $x^{(q+1)/2} + ax \in \mathbb{F}_q[x]$ является перестановочным многочленом поля $\mathbb{F}_q$ нечетной характеристики тогда и только тогда, когда $a = 2^{-1}(c + c^{-1})$, где c — некоторый элемент из $\mathbb{F}_q^*$, $c^2 \neq 1$.

7.10. Найти наименьшее число M, такое, что для любого конечного поля $\mathbb{F}_q$, где q нечетно и $q \geqslant M$, найдется такой элемент $a \in \mathbb{F}_q^*$, что многочлен вида $x^{(q+1)/2} + ax$ является перестановочным многочленом поля $\mathbb{F}_q$.

7.11. Пусть $m > 1$ — делитель числа $q - 1$. Доказать, что

$$x^{(q+m-1)/m} + ax \in \mathbb{F}_q[x]$$

является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда $(-a)^m \neq 1$ и

$$[(a + c^i)(a + c^j)^{-1}]^{(q-1)/m} \neq c^{j-i} \quad \text{для всех } 0 \leqslant i < j < m,$$

где c — фиксированный первообразный корень m-й степени из единицы в поле $\mathbb{F}_q$.

7.12. Пусть $q = p^e$, где p — нечетное простое число, а $m = (q-1)/2$. Доказать, что НОД $\left(\binom{m}{t}, p\right) = 1$ тогда и только тогда, когда $t = b_0 + b_1 p + \ldots + b_{e-1}p^{e-1}$, где $0 \leqslant b_i \leqslant (p-1)/2$, а $0 \leqslant i \leqslant e - 1$.

7.13. Пусть

$$f(x) = \sum_{i=0}^{n-1} c_i x^{q^i} \in \mathbb{F}_q[x].$$

Показать, что $f(x)$ является перестановочным многочленом поля $\mathbb{F}_{q^n}$ тогда и только тогда, когда

$$\text{НОД}\left(\sum_{i=0}^{n-1} c_i x^i,\ x^n - 1\right) = 1.$$

7.14. Доказать, что если характеристика поля отлична от 2, то многочлен Диксона $g_k(x, a)$ можно формально представить в виде

$$g_k(x, a) = \left(\frac{x + \sqrt{x^2 - 4a}}{2}\right)^k + \left(\frac{x - \sqrt{x^2 - 4a}}{2}\right)^k.$$

7.15. Показать что многочлены Диксона удовлетворяют следующим равенствам:

$$g_1(x, a) = x, \quad g_2(x, a) = x^2 - 2a,$$
$$g_{k+1}(x, a) = xg_k(x, a) - ag_{k-1}(x, a) \quad \text{для} \quad k \geqslant 2.$$

7.16. Показать, что многочлены Диксона удовлетворяют соотношению $g_k(ax, a^2) = a^k g_k(x, 1)$.

7.17. Пользуясь обозначениями теоремы 5.46, показать, что суммы Клостермана удовлетворяют равенству

$$K(\chi^{(s)}; a, b) = -g_s(-K, q),$$

где $g_s(x, q)$ — многочлены Диксона над полем действительных чисел.

7.18. Доказать, что знакопеременная группа A_q порождается своими подгруппами AL_q и Q_q (см. § 3 настоящей главы).

7.19. Пусть p — нечетное простое число. Доказать, что знакопеременная группа A_p порождается перестановками, соответствующими многочленам $x + 1$ и mx^{p-2}, где m — любой ненулевой элемент поля $\mathbb{F}_p$, являющийся квадратом, если $p \equiv 3 \pmod 4$, и любой элемент поля $\mathbb{F}_p$, не являющийся квадратом, если $p \equiv 1 \pmod 4$. В противном случае эти перестановки порождают всю симметрическую группу S_p.

7.20. Показать, что если $q > 2$, то любую транспозицию элементов поля $\mathbb{F}_q$ можно единственным образом представить с помощью многочлена степени $q - 2$.

7.21. Доказать следующие утверждения: (i) если $q \equiv 2 \pmod 3$, $q > 2$, то любой 3-цикл на $\mathbb{F}_q$ можно единственным образом представить с помощью многочлена степени $q - 2$; (ii) если $q \equiv 1 \pmod 3$, то все 3-циклы на $\mathbb{F}_q$ (кроме $2q(q-1)/3$ штук) можно представить с помощью многочленов степени $q - 2$.

7.22. Для конечного поля $\mathbb{F}_q$, $q > 2$, определим *квазиперестановочный многочлен* поля $\mathbb{F}_q$ как многочлен, являющийся композицией конечного числа многочленов над $\mathbb{F}_q$, которые или являются линейнымн многочленами, или равняются x^{q-2}. Доказать, что квазиперестановочный многочлен над полем $\mathbb{F}_q$ является перестановочным многочленом расширения $\mathbb{F}_{q^r}$ тогда и только тогда, когда НОД $(2^r - 1, q - 2) = 1$.

7.23. Пусть f — квазиперестановочный многочлен поля $\mathbb{F}_q$, $q > 4$. Доказать, что существует бесконечно много расширений $\mathbb{F}_{q^r}$ поля $\mathbb{F}_q$, для которых f является перестановочным многочленом, и бесконечно много расширений того же поля, для которых f не является перестановочным многочленом.

7.24. Показать, что квазиперестановочный многочлен поля $\mathbb{F}_q$, приведенный по модулю $x^q - x$, не обязательно является квазиперестановочным. Кроме того, показать, что различные квазиперестановочные многочлены после приведения по модулю $x^q - x$ могут совпадать.

7.25. Доказать, что группа $G(1)$ является гомоморфным образом группы $G(-1)$, где группы $G(a)$ определены в теореме 7.23.

7.26. Под *соответствием* Γ в поле $\mathbb{F}_q$ мы понимаем пару разбиений $A_0, A_1, \ldots, A_k$ и $B_0, B_1, \ldots, B_k$ поля $\mathbb{F}_q$, где $A_i \neq \varnothing$, $B_i \neq \varnothing$, $1 \leqslant i \leqslant k$. Целое число k называется *рангом соответствия* Γ. Многочлен $h \in \mathbb{F}_q[x, y]$ называется *допустимым* для Γ, если $h(a, b) = 0$ при $(a, b) \in A_i \times B_i$ для некоторого i, $1 \leqslant i \leqslant k$, и $h(a, b) \neq 0$ в остальных случаях. Доказать, что допустимый многочлен для Γ вида $h(x, y) = f(x) - g(y)$ существует тогда и только тогда, когда $k \neq q - 1$ или $k = q - 1$ и при этом или $A_0 = \varnothing$, или $B_0 = \varnothing$. Доказать, что если $k = q - 1$, $A_0 \neq \varnothing$, $B_0 \neq \varnothing$, то допустимый многочлен для Γ имеет вид

$$h(x, y) = (1 - f(x)^{q-1})(1 - g(y)^{q-1}) + (f(x) - g(y))^{q-1},$$

где f и g — некоторые многочлены над полем $\mathbb{F}_q$.

7.27. Многочлен $h \in \mathbb{F}_q[x, y]$ называется *допустимым*, если он является допустимым для некоторого соответствия в поле $\mathbb{F}_q$. Два допустимых многочлена называются *эквивалентными*, если они являются допустимыми для одного и того же соответствия. Доказать следующие утверждения:

(i) два допустимых многочлена $h_1(x, y)$ и $h_2(x, y)$ являются эквивалентными тогда и только тогда, когда

$$h_1(x, y)^{q-1} \equiv h_2(x, y)^{q-1} \pmod{(x^q - x, y^q - y)};$$

(ii) число классов эквивалентности допустимых многочленов равно числу соответствий.

7.28. Доказать, что если многочлены $h_1(x, y)$ и $h_2(x, y)$ являются допустимыми для некоторого соответствия Γ, то $h(x, y) = h_1(x, y)\, h_2(x, y)$ тоже является допустимым многочленом для этого соответствия.

7.29. Доказать, что если многочлен $h(x, y) = g(x - y)$ является допустимым для некоторого соответствия Γ в поле $\mathbb{F}_q$ и число различных корней многочлена g в поле $\mathbb{F}_q$ равняется целому числу $m > 0$, то m делит q, а ранг соответствия Γ равняется q/m.

7.30. Пусть $f(x)$ и $g(y)$ — многочлены над полем $\mathbb{F}_q$. Доказать, что многочлен $h(x, y) = f(x)\, g(y)$ является допустимым многочленом в каждом поле $\mathbb{F}_{q^r}$, $r = 1, 2, \ldots$, тогда и только тогда, когда хотя бы один из многочленов f или g является постоянным.

7.31. Пусть $f_1(x), f_2(x), g_1(y), g_2(y)$ — многочлены над полем $\mathbb{F}_q$. Доказать, что многочлен $h(x, y) = f_1(x)\, g_1(y) + f_2(x)\, g_2(y)$ является допустимым в поле $\mathbb{F}_{q^r}$, $r = 1, 2, \ldots$, тогда и только тогда, когда НОД $(f_1, f_2) =$ НОД $(g_1, g_2) = 1$.

7.32. Пусть $f \in \mathbb{Z}[x_1, \ldots, x_n]$, а p — простое число. Назовем f *перестановочным многочленом по модулю* p, если он, рассматриваемый как многочлен над полем $\mathbb{F}_p$, является перестановочным многочленом над полем $\mathbb{F}_p$. Доказать, что f является перестановочным многочленом по модулю p тогда и только тогда, когда каждое из сравнений

$$f(x_1, \ldots, x_n) \equiv a \pmod{p}, \quad a = 0, 1, \ldots, p - 1,$$

имеет хотя бы одно решение и

$$\sum_{a_1, \ldots, a_n = 0}^{p-1} f(a_1, \ldots, a_n)^{t p^{n-2}} \equiv 0 \pmod{p^{n-1}}$$

для всех $t = 1, 2, \ldots, p - 1$.

7.33. Доказать, что многочлен $ax^n + b \in \mathbb{Z}[x]$, $a \neq 0$, является перестановочным многочленом по модулю p для бесконечного множества простых чисел p тогда и только тогда, когда n нечетно.

7.34. Пусть $g_k(x, a)$ — многочлен Диксона над кольцом $\mathbb{Z}$, причем $a \neq 0$. Показать, что $g_k(x, a)$ является перестановочным многочленом по модулю p для бесконечного множества простых чисел p тогда и только тогда, когда НОД $(k, 6) = 1$.

7.35. Доказать, что многочлен $f \in \mathbb{Z}[x]$ является перестановочным многочленом по модулю p для всех простых чисел p тогда и только тогда, когда f — линейный многочлен со старшим коэффициентом, равным ± 1.

7.36. Пусть $1 \leqslant m < n$. Доказать, что многочлен $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ является перестановочным многочленом над полем $\mathbb{F}_q$ тогда и только тогда, когда он, рассматриваемый как элемент кольца $\mathbb{F}_q[x_1, \ldots, x_n]$, также является перестановочным многочленом над тем же полем.

7.37. Доказать первую часть теоремы 7.42, используя теорию характеров.

7.38. Пусть $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ — перестановочный многочлен над полем $\mathbb{F}_q$, и пусть $g \in \mathbb{F}_q[x_{m+1}, \ldots, x_n]$, где $1 \leqslant m < n$. Показать, что многочлен

$$h(x_1, \ldots, x_n) = f(x_1, \ldots, x_m)\, g(x_{m+1}, \ldots, x_n)$$

является перестановочным многочленом над полем $\mathbb{F}_q$ тогда и только тогда, когда уравнение $g(x_{m+1}, \ldots, x_n) = 0$ не имеет решений в $\mathbb{F}_q^{n-m}$.

7.39. Доказать, что многочлен

$$a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} \in \mathbb{F}_q[x_1, \ldots, x_n]$$

является перестановочным многочленом над полем $\mathbb{F}_q$, если для некоторого i, $1 \leqslant i \leqslant n$, выполняются соотношения $a_i \neq 0$ и НОД $(k_i, q-1) = 1$.

7.40. Показать, что если $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ является перестановочным миогочленом над полем $\mathbb{F}_q$, то перестановочными многочленами над этим полем являются и все многочлены вида $bf + c$, где $b \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$.

7.41. Показать, что если $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ является перестановочным многочленом над полем $\mathbb{F}_q$, то для всех $k \in \mathbb{N}$, удовлетворяющих условию НОД $(k, q-1) = 1$, многочлены f^k также являются перестановочными многочленами над полем $\mathbb{F}_q$.

7.42. Пользуясь обозначениями, введеннымн после теоремы 7.47, доказать, что миогочлен $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ является перестановочным многочленом над полем $\mathbb{F}_q$ тогда и только тогда, когда $\operatorname{rg}(A') > \operatorname{rg}(A)$.

7.43. Пусть $f, g \in \mathbb{F}_q[x_1, \ldots, x_{n-1}]$, и пусть число решений уравнеиия $f(x_1, \ldots, x_{n-1}) = 0$ в $\mathbb{F}_q^{n-1}$ не делится на q. Пусть многочлен $h \in \mathbb{F}_q[x_1, \ldots, x_n]$ таков, что $h(c_1, \ldots, c_{n-1}, x_n)$ при любом выборе элементов $c_1, \ldots, c_{n-1} \in \mathbb{F}_q$ является перестановочным многочленом от одной переменной x_n поля $\mathbb{F}_q$. Показать, что тогда многочлен

$$s(x_1, \ldots, x_n) = h(x_1, \ldots, x_n) f(x_1, \ldots, x_{n-1}) + g(x_1, \ldots, x_{n-1})$$

не является перестановочным многочленом над полем $\mathbb{F}_q$.

7.44. Пусть $f \in \mathbb{F}_q[x_1, \ldots, x_{n-1}]$ и при этом число решений уравнения $f(x_1, \ldots, x_{n-1}) = 0$ в $\mathbb{F}_q^{n-1}$ делится на q, а многочлен h такой же, как в упр. 7.43. Показать, что существует многочлен $g \in \mathbb{F}_q[x_1, \ldots, x_{n-1}]$, такой, что

$$s(x_1, \ldots, x_n) = h(x_1, \ldots, x_n) f(x_1, \ldots, x_{n-1}) + g(x_1, \ldots, x_{n-1})$$

является перестановочным многочленом над полем $\mathbb{F}_q$.

7.45. Показать, что многочлен Диксона $g_k^{(2)}(x, y, a)$ задается формулой

$$g_k^{(2)}(x, y, a) = \sum_{\substack{i=0 \\ 2i+3j \leqslant k}}^{\lfloor k/2 \rfloor} \sum_{j=0}^{\lceil k/3 \rceil} \frac{k(-1)^i}{k-i-2j} \binom{k-i-2j}{i+j} \binom{i+j}{i} a^{i+2j} x^i y^{k-2i-3j}.$$

7.46. Доказать обобщение теоремы 7.23 для многочленов Диксона от двух переменных.

7.47. Доказать, что система многочленов $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, $1 \leqslant m \leqslant n$, является ортогональной над полем $\mathbb{F}_q$ тогда и только тогда, когда для всех перестановочных многочленов $g(y_1, \ldots, y_m)$ от m переменных над полем $\mathbb{F}_q$ многочлен

$$g(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$$

является перестановочным многочленом от n переменных над полем $\mathbb{F}_q$.

7.48. Доказать, что для любой системы многочленов $f_1, \ldots, f_{n+1} \in \mathbb{F}_q[x_1, \ldots, x_n]$ найдутся такие элементы $b_1, \ldots, b_{n+1} \in \mathbb{F}_q$, не все равные 0, что $b_1 f_1 + \ldots + b_{n+1} f_{n+1}$ не является перестановочным многочленом над полем $\mathbb{F}_q$.

7.49. *Смежным классом относительно системы многочленов* $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, $1 \leqslant m \leqslant n$, называется непустое подмножество пространства $\mathbb{F}_q^n$, элементы которого отображаются данной системой многочленов в единственный элемент пространства $\mathbb{F}_q^m$. Пусть $\{f_1, \ldots, f_m\}$ является ортогональной системой над полем $\mathbb{F}_q$. Доказать, что для многочлена $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ следующие два условия эквивалентны: (i) многочлен g является перестановочным многочленом над полем $\mathbb{F}_q$, причем все смежные классы относительно системы $\{f_1, \ldots, f_m\}$ совпадают со смежными классами относительно многочлена g; (ii) $g \equiv h(f_1, \ldots, f_m) \left(\mathrm{mod}\left(x_1^q - x_1, \ldots, x_n^q - x_n\right)\right)$ для некоторого перестановочного многочлена h от m переменных над полем $\mathbb{F}_q$.

Глава 8

Линейные рекуррентные последовательности

Большую важность ввиду их многочисленных применений имеют последовательности над конечными полями, каждый член которых, будучи элементом основного поля, некоторым простым образом зависит от предшествующих ему членов. Такие последовательности легко получать с помощью рекурсивных процедур, что, безусловно, является преимуществом с точки зрения удобства вычислений. Кроме того, такие последовательности, как правило, обладают полезными структурными свойствами. Практический интерес представляет случай, когда члены последовательности линейным образом зависят от фиксированного числа предыдущих членов. Такие последовательности называются линейными рекуррентными последовательностями. Они применяются в теории кодирования (см. гл. 9), а также в различных областях электроники. Для большинства приложений в качестве основного поля выбирается поле $\mathbb{F}_2$, однако теория рекуррентных последовательностей может быть развита для произвольного конечного поля.

В § 1 мы покажем, как можно технически осуществить получение линейных рекуррентных последовательностей с помощью переключательных схем специального вида, называемых регистрами сдвига с обратной связью. Здесь же мы обсудим основные периодические свойства таких последовательностей. В § 2 вводится понятие импульсной функции, т. е. последовательности, порожденной импульсом. Эти функции представляют как теоретический, так и практический интерес. Так, с их помощью получаются дальнейшие результаты о периодических свойствах рекуррентных последовательностей. Исследование периодичности ведется также с использованием так называемых характеристических многочленов линейных рекуррентных последовательностей. С помощью характеристических многочленов можно также получить явные формулы для членов линейной рекуррентной последовательности. В этом же параграфе определяются последовательности максимального периода.

К теории линейных рекуррентных последовательностей можно подойти как через линейную алгебру, так и через теорию идеалов или теорию формальных степенных рядов. В § 3 представлен подход, основанный на понятии формального степенного ряда.

На этой основе в следующем параграфе вводится минимальный многочлен линейной рекуррентной последовательности. Понятие минимального многочлена очень важно для теории линейных рекуррентных последовательностей, так как порядок минимального многочлена определяет минимальный период соответствующей последовательности.

В § 5 мы будем исследовать множества, состоящие из всех последовательностей, удовлетворяющих данному линейному рекуррентному соотношению. Полученные при этом результаты оказываются полезными для изучения свойств таких операций на множестве линейных рекуррентных последовательностей, как операции почленного сложения или умножения двух последовательностей над произвольным конечным полем или операция бинарного дополнения для последовательностей над полем $\mathbb{F}_2$. Мы рассмотрим также задачу нахождения минимальных периодов последовательностей, порожденных данным линейным рекуррентным соотношением. В § 6 представлены некоторые детерминантные критерии, характеризующие линейные рекуррентные последовательности. Кроме того, в этом параграфе приводится алгоритм Берлекэмпа—Месси для вычисления минимального многочлена рекуррентной последовательности.

§ 7 посвящен вопросам распределения элементов основного поля среди членов линейной рекуррентной последовательности. Здесь основным инструментом исследования является метод тригонометрических сумм.

§ 1. Регистры сдвига с обратной связью. Свойства периодичности

Пусть k — натуральное число, а a, a_0, a_1, ..., a_{k-1} — заданные элементы конечного поля $\mathbb{F}_q$. Последовательность s_0, s_1,... элементов поля $\mathbb{F}_q$, удовлетворяющая соотношению

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n + a, \quad n = 0, 1, \ldots, \tag{8.1}$$

называется *линейной рекуррентной последовательностью* (*k-го порядка*) над полем $\mathbb{F}_q$. Первые члены s_0, s_1, ..., s_{k-1} однозначно определяют всю последовательность и называются ее *начальными значениями*. Соотношение вида (8.1) называется *линейным рекуррентным соотношением* (*k-го порядка*). В старой литературе можно также встретить термин «разностное уравнение». Мы будем называть линейное рекуррентное соотношение *однородным*, если $a = 0$, в противном случае линейное рекуррентное соотношение будет называться *неоднородным*. Соответствующая рекуррентная последовательность s_0, s_1, ... будет называться *однородной* (или

неоднородной) *линейной рекуррентной последовательностью* над полем $\mathbb{F}_q$.

Линейные рекуррентные последовательности можно получать с помощью *регистров сдвига с обратной связью*. Это электронные переключательные схемы специального вида, перерабатывающие информацию, заданную в форме соответствующим образом представленных элементов поля. Регистры сдвига строятся из конструктивных элементов следующих четырех типов. Элементами первого типа являются сумматоры. *Сумматор* имеет два входа и один выход. Если на входе появляются два элемента поля $\mathbb{F}_q$, то выходом является их сумма в поле $\mathbb{F}_q$. Элементами второго типа являются усилители. *Усилитель* имеет один вход и один выход. Если на вход поступает элемент поля $\mathbb{F}_q$, то на выходе усилителя появляется его произведение на некоторый постоянный элемент из поля $\mathbb{F}_q$. Третьим типом конструктивного элемента является *увеличитель*, который работает аналогично усилителю, но в отличие от него прибавляет к поступающему на вход элементу некоторый элемент поля $\mathbb{F}_q$. Элементом четвертого типа является *элемент задержки* (*триггер*). Он имеет один вход и один выход, а его работа регулируется внешними синхронизирующими часами таким образом, что элемент поля $\mathbb{F}_q$, поступивший на вход в данный момент времени, появляется в качестве выхода в следующий момент времени (т. е. на следующем такте работы). Мы не будем здесь касаться технической реализации описанных выше устройств. На рис. 8.1 показано, как эти элементы принято изображать на схемах.

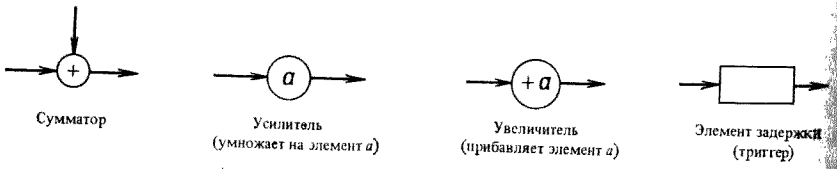


Рис. 8.1

Регистр сдвига с обратной связью строится путем соединения конечного числа указанных выше конструктивных элементов в замкнутую цепь таким образом, что никакие два выхода не присоединяются друг к другу. На самом деле для получения линейных рекуррентных последовательностей следует соединять элементы конструкции довольно специальным образом. Регистр сдвига с обратной связью, вырабатывающий линейную рекуррентную последовательность, удовлетворяющую соотношению (8.1), изображен на рис. 8.2.

В начале работы каждый элемент задержки D_j, $j = 0, 1, \ldots, k-1$, содержит некоторое начальное заполнение s_j. Если считать, что выполнение арифметических операций и передача сигна-

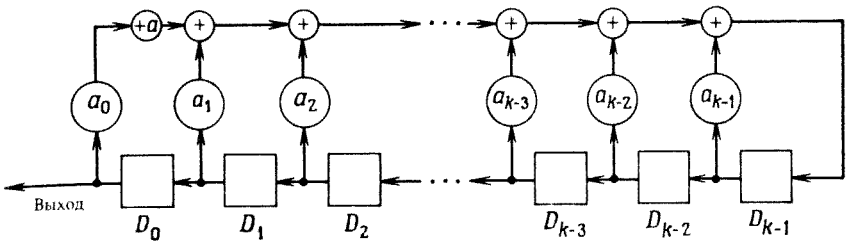


Рис. 8.2

лов по проводам происходят мгновенно, то на следующем такте работы каждый элемент задержки D_j содержит заполнение s_{j+1}. Продолжая этот процесс, мы видим, что выходом регистра сдвига с обратной связью является последовательность элементов s_0, s_1, s_2, ..., получаемых в последовательные моменты времени. Для большинства приложений используются однородные линейные рекуррентные последовательности; в этом случае увеличитель в конструкции соответствующего регистра сдвига не требуется.

8.1. **Пример.** Для того чтобы в поле $\mathbb{F}_5$ получить линейную рекуррентную последовательность, удовлетворяющую однородному линейному рекуррентному соотношению $s_{n+6} = s_{n+5} + 2s_{n+4} + s_{n+1} + 3s_n$, $n = 0, 1, \ldots$, можно использовать регистр сдвига с обратной связью, изображенный на рис. 8.3. Так как $a_2 = a_3 = 0$, соответствующие соединения не нужны. □

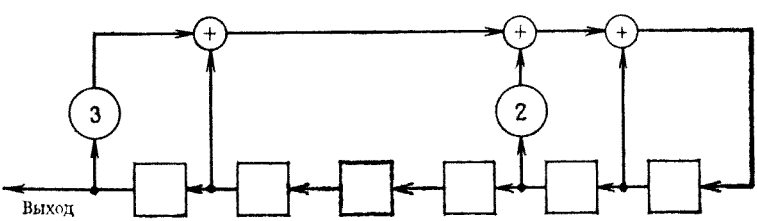


Рис. 8.3

8.2. **Пример.** Рассмотрим однородное линейное рекуррентное соотношение

$$s_{n+7} = s_{n+4} + s_{n+3} + s_{n+2} + s_n, \quad n = 0, 1, \ldots,$$

над полем $\mathbb{F}_2$. Соответствующий этому рекуррентному соотношению регистр сдвига с обратной связью изображен на рис. 8.4.

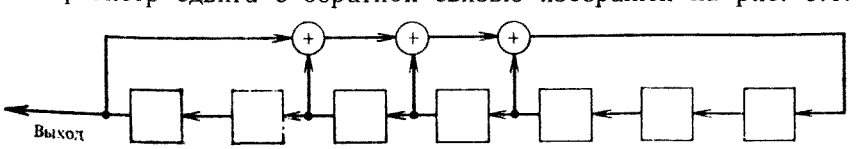


Рис. 8.4

Так как в поле $\mathbb{F}_2$ умножение на константу или сохраняет множимое (при умножении на 1), или обращает его в нуль (при умножении на 0), то в этом случае узел, соответствующий усилителю, не требуется. Его функции исполняет простое наличие соединительного проводника или его отсутствие. Таким образом, регистр сдвига с обратной связью, вырабатывающий бинарную однородную линейную рекуррентную последовательность, может быть сконструирован с использованием лишь элементов задержки, сумматоров и соединяющих проводников. □

Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, удовлетворяющая соотношению (8.1). Как уже было отмечено, эту последовательность можно получить с помощью регистра сдвига с обратной связью, изображенного на рис. 8.2. Если n — целое неотрицательное число, то через n тактов работы элемент задержки D_j, $j = 0, 1, \ldots, k-1$, будет содержать заполнение s_{n+j}. Таким образом, вектор $\mathbf{s}_n = (s_n, s_{n+1}, \ldots, s_{n+k-1})$ естественно назвать *вектором n-го состояния* линейной рекуррентной последовательности (или *внутренним состоянием* регистра сдвига с обратной связью *на n-м такте* работы). Вектор состояния $\mathbf{s}_0 = (s_0, s_1, \ldots, s_{k-1})$ называется *вектором начального состояния*.

Характерной особенностью линейных рекуррентных последовательностей над конечным полем является то, что такие последовательности с некоторого момента (после, возможно, нерегулярного поведения в начале) проявляют свою периодическую природу (т. е. они периодичны в смысле определения 8.3, см. ниже). Прежде чем перейти к детальному изучению этого свойства рекуррентных последовательностей, введем соответствующую терминологию и приведем несколько общих утверждений, касающихся периодических последовательностей.

8.3. Определение. Пусть S — произвольное непустое множество, и пусть $s_0, s_1, \ldots$ — последовательность элементов из множества S. Если существуют целые числа $r > 0$ и $n_0 > 0$, такие, что $s_{n+r} = s_n$ для всех $n \geqslant n_0$, то последовательность $s_0, s_1, \ldots$ называется *периодической последовательностью*, а r — *периодом* указанной последовательности. Наименьший из всех возможных периодов периодической последовательности иазывается *минимальным периодом* последовательности.

8.4 Лемма. *Каждый период периодической последовательности делится на ее минимальный период.*

Доказательство. Пусть r — произвольный период периодической последовательности $s_0, s_1, \ldots$, и пусть r_1 — ее минимальный период. Из этого следует, что $s_{n+r} = s_n$ для всех $n \geqslant n_0$, а $s_{n+r_1} = s_n$ для всех $n \geqslant n_1$ при соответствующем выборе n_0 и n_1. Если r

не делится на r_1, то, применяя алгоритм деления целых чисел, представим r в виде $r = mr_1 + t$, где $m \geqslant 1$, $0 < t < r_1$. Тогда для всех $n \geqslant \max(n_0, n_1)$ получаем

$$s_n = s_{n+r} = s_{n+mr_1+t} = s_{n+(m-1)r_1+t} = \cdots = s_{n+t},$$

откуда следует, что t также является периодом последовательности $s_0, s_1, \ldots$. Это противоречит тому, что r_1 — минимальный период последовательности. □

8.5. **Определение.** Периодическая последовательность $s_0, s_1, \ldots$ с минимальным периодом r называется *чисто периодической*, если равенство $s_{n+r} = s_n$ выполняется для всех $n = 0, 1, \ldots$.

Следующее условие, которое иногда встречается в литературе, эквивалентно определению чисто периодической последовательности.

8.6. **Лемма.** *Последовательность $s_0, s_1, \ldots$ является чисто периодической тогда и только тогда, когда существует целое число $r > 0$, такое, что $s_{n+r} = s_n$ для всех $n = 0, 1, \ldots$.*

Доказательство. Необходимость приведенного условия очевидна. Далее, если условие выполняется, то $s_0, s_1, \ldots$ является периодической последовательностью и, следовательно, имеет минимальный период r_1, причем равенство $s_{n+r_1} = s_n$ справедливо для всех $n \geqslant n_0$ и некоторого $n_0 \in \mathbb{N}$. Пусть теперь n — произвольное целое неотрицательное число, и выберем такое целое $m \geqslant n_0$, для которого $m \equiv n \pmod{r}$. Тогда $s_{n+r_1} = s_{m+r_1} = s_m = s_n$, откуда вытекает, что последовательность $s_0, s_1, \ldots$ является чисто периодической в смысле определения 8.5. □

Пусть $s_0, s_1, \ldots$ — периодическая последовательность, а r — ее минимальный период. Наименьшее неотрицательное целое число n_0, такое, что $s_{n+r} = s_n$ для всех $n \geqslant n_0$, называется *предпериодом* этой последовательности. Периодическая последовательность является чисто периодической, если ее предпериод равен 0.

Вернемся теперь к линейным рекуррентным последовательностям над конечными полями и установим основные результаты о свойствах периодичности у таких последовательностей.

8.7. **Теорема.** *Пусть $\mathbb{F}_q$ — произвольное конечное поле, а k — некоторое натуральное число. Тогда каждая линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$ является периодической. При этом ее минимальный период r удовлетворяет неравенству $r \leqslant q^k$, а в случае однородной последовательности — неравенству $r \leqslant q^k - 1$.*

Доказательство. Заметим прежде всего, что существует ровно q^k различных упорядоченных наборов по k элементов из поля $\mathbb{F}_q$.

Поэтому если рассмотреть совокупность векторов состояний $\mathbf{s}_m$, $0 \leqslant m \leqslant q^k$, данной линейной рекуррентной последовательности k-го порядка над полем $\mathbb{F}_q$, то для некоторых i, j, $0 \leqslant i < j \leqslant q^k$, должно выполняться равенство $\mathbf{s}_j = \mathbf{s}_i$. Из соответствующего линейного рекуррентного соотношения и принципа математической индукции можно получить равенство $\mathbf{s}_{n+j-i} = \mathbf{s}_n$ для всех $n \geqslant i$. Последнее означает, что наша линейная рекуррентная последовательность является периодической последовательностью и, если r — ее минимальный период, то $r \leqslant j - i \leqslant q^k$. Рассмотрим теперь однородную линейную рекуррентную последовательность. Если ни один из ее векторов состояний не является нулевым вектором, то, проведя аналогичные рассуждения с заменой q^k на $q^k - 1$, можно получить неравенство $r \leqslant q^k - 1$. Если же один из ее векторов состояний является нулевым вектором, то все следующие за ним векторы состояний тоже являются нулевыми векторами и, значит, последовательность имеет период $r = 1 \leqslant q^k - 1$. Теорема доказана. □

8.8. Пример. Верхняя оценка для r, полученная в теореме 8.7, достижима. Это можно показать, рассмотрев линейную рекуррентную последовательность первого порядка над полем $\mathbb{F}_p$ (p — простое число), задаваемую соотношением $s_{n+1} = s_n + 1$, $n = 0, 1, \ldots$, и произвольным начальным значением $s_0 \in \mathbb{F}_p$. Если $\mathbb{F}_q$ — произвольное конечное поле, а g — примитивный элемент этого поля (см. определение 2.9), то однородная линейная рекуррентная последовательность первого порядка над этим полем, задаваемая соотношением $s_{n+1} = gs_n$, $n = 0, 1, \ldots$, $s_0 \neq 0$, имеет минимальный период $r = q - 1$. Таким образом, доказана достижимость верхней границы для r и в однородном случае. Позже мы покажем, что в случае произвольного поля $\mathbb{F}_q$ и любого целого $k \geqslant 1$ существует однородная линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, имеющая минимальный период $r = q^k - 1$ (см. теорему 8.33). □

8.9. Пример. Нетрудно заметить, что минимальный период однородной линейной рекуррентной последовательности первого порядка над полем $\mathbb{F}_q$ делит число $q - 1$. Однако для $k \geqslant 2$ минимальный период однородной линейной рекуррентной последовательности k-го порядка не обязан делить число $q^k - 1$. Так, например, можно проверить, что рекуррентная последовательность $s_0, s_1, \ldots$ над полем $\mathbb{F}_5$, задаваемая рекуррентным соотношением $s_{n+2} = s_{n+1} + s_n$. $n = 0, 1, \ldots$, и начальными значениями $s_0 = 0$, $s_1 = 1$, имеет минимальный период, равный 20. □

8.10. Пример. Линейная рекуррентная последовательность над конечным полем является периодической последовательностью, но не обязана быть чисто периодической последовательностью. Для доказательства этого достаточно, например, рассмотреть

линейную рекуррентную последовательность $s_0, s_1, \ldots$ 2-го порядка над полем $\mathbb{F}_q$, задаваемую рекуррентным соотношением $s_{n+2} = s_{n+1}$, $n = 0, 1, \ldots$, и условием $s_0 \neq s_1$. □

Следующий результат дает важное достаточное условие для чистой периодичности линейной рекуррентной последовательности.

8.11. Теорема. *Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность над конечным полем, удовлетворяющая линейному рекуррентному соотношению* (8.1). *Если коэффициент a_0 в* (8.1) *не равен* 0, *то последовательность $s_0, s_1, \ldots$ является чисто периодической.*

Доказательство. По теореме 8.7 линейная рекуррентная последовательность $s_0, s_1, \ldots$ является периодической последовательностью. Если r — ее минимальный период, а n_0 — предпериод, то $s_{n+r} = s_n$ для всех $n \geqslant n_0$. Допустим, что в нашем случае $n_0 \geqslant 1$. Из соотношения (8.1), полагая $n = n_0 + r - 1$ и учитывая, что $a_0 \neq 0$, получаем

$$s_{n_0-1+r} = a_0^{-1}\left(s_{n_0+k-1+r} - a_{k-1}s_{n_0+k-2+r} - \cdots - a_1 s_{n_0+r} - a\right) =$$
$$= a_0^{-1}\left(s_{n_0+k-1} - a_{k-1}s_{n_0+k-2} - \cdots - a_1 s_{n_0} - a\right).$$

Используя соотношение (8.1) для $n = n_0 - 1$, приходим к такому же выражению и для s_{n_0-1}, откуда следует равенство $s_{n_0-1+r} = s_{n_0-1}$. Последнее противоречит тому, что n_0 является предпериодом последовательности $s_0, s_1, \ldots$. □

Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность степени k над полем $\mathbb{F}_q$, удовлетворяющая линейному рекуррентному соотношению

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n, \quad n = 0, 1, \ldots, \tag{8.2}$$

где $a_j \in \mathbb{F}_q$, $0 \leqslant j \leqslant k-1$. С этой линейной рекуррентной последовательностью можно связать матрицу A над полем $\mathbb{F}_q$ размера $k \times k$ следующего вида:

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 & a_{k-1} \end{pmatrix} \tag{8.3}$$

Если $k = 1$, то под матрицей A понимается матрица $A = (a_0)$ размера 1×1. Заметим, что матрица A зависит только от линейного рекуррентного соотношения, определяющего данную рекуррентную последовательность.

8.12. Лемма. *Если $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$, удовлетворяющая соотношению* (8.2), *а A — матрица, связанная с этой последовательностью и задаваемая равенством* (8.3), *то для векторов состояний последовательности $s_0, s_1, \ldots$ справедливо равенство*

$$\mathbf{s}_n = \mathbf{s}_0 A^n, \quad n = 0, 1, \ldots . \tag{8.4}$$

Доказательство. Так как $\mathbf{s}_n = (s_n, s_{n+1}, \ldots, s_{n+k-1})$, то, как нетрудно проверить, для всех $n \geqslant 0$ выполняется равенство $\mathbf{s}_{n+1} = \mathbf{s}_n A$, откуда по индукции получается (8.4). □

Заметим, что множество всех невырожденных $k \times k$-матриц над полем $\mathbb{F}_q$ образует конечную группу относительно операции матричного умножения. (Эта группа называется *общей линейной группой* $GL(k, \mathbb{F}_q)$.)

8.13. Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, такая, что выполняется соотношение* (8.2) *и $a_0 \neq 0$. Тогда минимальный период данной последовательности делит порядок связанной с ней матрицы A, определенной формулой* (8.3) *и рассматриваемой как элемент общей линейной группы $GL(k, \mathbb{F}_q)$.*

Доказательство. Так как $\det A = (-1)^{k-1} a_0 \neq 0$, то матрица A действительно является элементом группы $GL(k, \mathbb{F}_q)$. Если m — порядок A как элемента группы $GL(k, \mathbb{F}_q)$, то из леммы 8.12 получаем, что $\mathbf{s}_{n+m} = \mathbf{s}_0 A^{n+m} = \mathbf{s}_0 A^n = \mathbf{s}_n$ для всех $n \geqslant 0$. Отсюда следует, что m является периодом рассматриваемой рекуррентной последовательности. Утверждение теоремы вытекает теперь из леммы 8.4. □

Отметим, что приведенные выше рассуждения вместе с леммой 8.6 дают другое доказательство теоремы 8.11 для однородного случая. Кроме того, из теоремы 8.13 следует, в частности, что минимальный период последовательности $s_0, s_1, \ldots$ делит порядок группы $GL(k, \mathbb{F}_q)$, который, как известно, равен

$$q^{(k^2-k)/2} (q-1)(q^2-1) \ldots (q^k-1).$$

Пусть теперь $s_0, s_1, \ldots$ — неоднородная линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, удовлетворяющая соотношению (8.1). Заменяя в (8.1) n на $n+1$ и вычитая из полученного равенства исходное равенство (8.1), получаем соотношение

$$s_{n+k+1} = b_k s_{n+k} + b_{k-1} s_{n+k-1} + \cdots + b_0 s_n, \quad n = 0, 1, \ldots, \tag{8.5}$$

где $b_0 = -a_0$, $b_j = a_{j-1} - a_j$ для $j = 1, 2, \ldots, k-1$, $b_k = a_{k-1} + 1$. Таким образом, последовательность $s_0, s_1, \ldots$ можно свести к однородной линейной рекуррентной последовательности

$(k+1)$-го порядка над полем $\mathbb{F}_q$, и, следовательно, результаты, полученные для однородных линейных рекуррентных последовательностей, дают информацию и для неоднородного случая.

Существует и другой подход к рассмотрению *неоднородного случая*. Пусть $s_0, s_1, \ldots$ — неоднородная линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, удовлетворяющая соотношению (8.1). Рассмотрим связанную с ней матрицу C над полем $\mathbb{F}_q$, являющуюся квадратной матрицей размера $(k+1) \times (k+1)$ следующего вида:

$$C = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a \\ 0 & 0 & 0 & \ldots & 0 & a_0 \\ 0 & 1 & 0 & \ldots & 0 & a_1 \\ 0 & 0 & 1 & \ldots & 0 & a_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 & a_{k-1} \end{pmatrix}.$$

Если $k = 1$, то полагаем

$$C = \begin{pmatrix} 1 & a \\ 0 & a_0 \end{pmatrix}.$$

Введем модифицированный вектор состояния рекуррентной последовательности, полагая

$$\mathbf{s}'_n = (1, s_n, s_{n+1}, \ldots, s_{n+k-1}) \quad \text{для } n = 0, 1, \ldots .$$

Тогда, как нетрудно заметить, для всех $n \geqslant 0$ справедливо равенство $\mathbf{s}'_{n+1} = \mathbf{s}'_n C$, откуда по индукции получаем, что $\mathbf{s}'_n = \mathbf{s}'_0 C^n$ для всех $n \geqslant 0$. Если в (8.1) коэффициент a_0 отличен от 0, то $\det C = (-1)^{k-1} a_0 \neq 0$, откуда следует, что матрица C является элементом группы $GL(k+1, \mathbb{F}_q)$. В этом случае, проведя рассуждения, аналогичные доказательству теоремы 8.13, нетрудно показать, что минимальный период последовательности $s_0, s_1, \ldots$ делит порядок матрицы C, рассматриваемой как элемент группы $GL(k+1, \mathbb{F}_q)$.

§ 2. Импульсная функция. Характеристический многочлен

Из всех однородных линейных рекуррентных последовательностей над полем $\mathbb{F}_q$, удовлетворяющих данному линейному рекуррентному соотношению k-го порядка вида (8.2), можно выделить одну последовательность с максимальным значением минимального периода, называемую *импульсной функцией* или *последовательностью, порожденной импульсом*. Эта последовательность

обозначается $d_0, d_1, \ldots$ и однозначно определяется начальными значениями $d_0 = \ldots = d_{k-2} = 0$, $d_{k-1} = 1$ ($d_0 = 1$ для $k = 1$) и линейным рекуррентным соотношением

$$d_{n+k} = a_{k-1} d_{n+k-1} + a_{k-2} d_{n+k-2} + \cdots + a_0 d_n, \quad n = 0, 1, \ldots. \quad (8.6)$$

8.14. Пример. Рассмотрим линейное рекуррентное соотношение

$$s_{n+5} = s_{n+1} + s_n, \quad n = 0, 1, \ldots,$$

над полем $\mathbb{F}_2$. Импульсная функция $d_0, d_1, \ldots$, соответствующая этому рекуррентному соотношению, представляет собой бинарную последовательность

0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, ...

и имеет минимальный период, равный 21. Регистр сдвига с обратной связью, вырабатывающий эту последовательность, показан на рис. 8.5. Эту последовательность можно рассматривать как

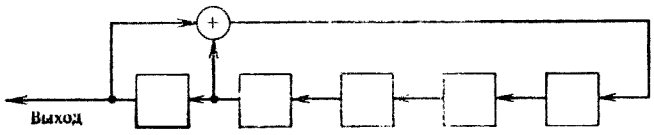


Рис. 8.5

выходную последовательность указанного регистра сдвига, полученную при начальном заполнении следующего вида: все элементы задержки, кроме последнего, в начальный момент времени являются пустыми (т. е. содержат заполнение 0), а в самый правый элемент задержки засылается импульс (т. е. он содержит заполнение 1). Этим, кстати, и объясняются термины «импульсная функция» или «последовательность, порожденная импульсом». □

8.15. Лемма. *Пусть $d_0, d_1, \ldots$ — последовательность над полем $\mathbb{F}_q$, являющаяся импульсной функцией, удовлетворяющей рекуррентному соотношению* (8.6), *и пусть A — связанная с ней матрица вида* (8.3). *Тогда два вектора состояния $\mathbf{d}_m$ и $\mathbf{d}_n$ рекуррентной последовательности $d_0, d_1, \ldots$ совпадают в том и только том случае, когда $A^m = A^n$.*

Доказательство. Достаточность следует из леммы 8.12. Для доказательства необходимости предположим, что $\mathbf{d}_m = \mathbf{d}_n$. Из линейного рекуррентного соотношения (8.6) получаем, что $\mathbf{d}_{m+t} = \mathbf{d}_{n+t}$ для всех $t \geqslant 0$. Из леммы 8.12 следует, что $\mathbf{d}_t A^m = \mathbf{d}_t A^n$ для всех $t \geqslant 0$. Тогда в силу того, что векторы $\mathbf{d}_0, \mathbf{d}_1, \ldots, \mathbf{d}_{k-1}$ образуют базис k-мерного векторного пространства $\mathbb{F}_q^k$ над полем $\mathbb{F}_q$, получаем требуемое равенство $A^m = A^n$. □

8.16. Теорема. *Минимальный период однородной линейной рекуррентной последовательности над полем $\mathbb{F}_q$ делит минимальный период соответствующей импульсной функции.*

Доказательство. Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$, удовлетворяющая соотношению (8.2), а $d_0, d_1, \ldots$ — соответствующая импульсная функция, и пусть A — матрица вида (8.3). Если r — минимальный период последовательности $d_0, d_1, \ldots$, а n_0 — ее предпериод, то $\mathbf{d}_{n+r} = \mathbf{d}_n$ для всех $n \geqslant n_0$. Из леммы 8.15 следует, что $A^{n+r} = A^n$ для всех $n \geqslant n_0$, а тогда по лемме 8.12 $\mathbf{s}_{n+r} = \mathbf{s}_n$ для всех $n \geqslant n_0$. Следовательно, r является периодом последовательности $s_0, s_1, \ldots$. Из леммы 8.4 получаем теперь утверждение теоремы. □

8.17. Теорема. *Если последовательность $d_0, d_1, \ldots$ является импульсной функцией k-го порядка над полем $\mathbb{F}_q$ и удовлетворяет соотношению (8.6) при $a_0 \neq 0$, а A — соответствующая матрица вида (8.3), то тогда минимальный период этой последовательности равен порядку матрицы A как элемента общей линейной группы $GL(k, \mathbb{F}_q)$.*

Доказательство. Если r — минимальный период последовательности $d_0, d_1, \ldots$, то по теореме 8.13 r делит порядок матрицы A. С другой стороны, по теореме 8.11 имеет место равенство $\mathbf{d}_0 = \mathbf{d}_r$. Применяя лемму 8.15, получаем, что $A^r = A^0$, откуда следует искомый результат. □

8.18. Пример. Мы видели, что для линейного рекуррентного соотношения $s_{n+5} = s_{n+1} + s_n$, $n = 0, 1, \ldots$, над полем $\mathbb{F}_2$, рассмотренного в примере 8.14, минимальный период соответствующей импульсной функции равняется 21, что совпадает с порядком матрицы

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

как элемента группы $GL(5, \mathbb{F}_2)$. Если вектор начального состояния некоторой линейной рекуррентной последовательности над полем $\mathbb{F}_2$, удовлетворяющей данному линейному рекуррентному соотношению, совпадает с одним из 21 различных векторов состояний, которые появляются в соответствующей импульсной функции, то минимальный период такой последовательности снова равняется 21 (так как такая последовательность представляет собой сдвиг этой импульсной функции). Если для того же рекуррентного соотношения в качестве вектора начального со-

стояния выбрать вектор (1, 1, 1, 0, 1), то мы получим бинарную последовательность 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, ... Минимальный период этой последовательности равен 7. Такой же минимальный период будет иметь любая рекуррентная последовательность, удовлетворяющая этому соотношению и получающаяся, если в качестве вектора начального состояния взять любой из 7 различных векторов состояний этой последовательности. Если в качестве вектора начального состояния взять вектор (1, 1, 0, 1, 1), то мы получаем бинарную последовательность 1, 1, 0, 1, 1, 0, 1, 1, ..., имеющую минимальный период, равный 3. Такой же минимальный период получается, если в качестве вектора начального состояния рекуррентной последовательности взять любой из трех различных векторов состояния этой последовательности. Вектор начального состояния, равный (0, 0, 0, 0, 0), порождает последовательность с минимальным периодом 1. Таким образом, мы рассмотрели все 32 возможности выбора вектора начального состояния для рекуррентной последовательности, удовлетворяющей нашему рекуррентному соотношению. □

8.19. Теорема. *Пусть* $s_0, s_1, \ldots$ — *однородная линейная рекуррентная последовательность* k-*го порядка над полем* $\mathbb{F}_k$, *а* n_0 — *предпериод этой последовательности. Если существует* k *векторов состояний* $\mathbf{s}_{m_1}, \mathbf{s}_{m_2}, \ldots, \mathbf{s}_{m_k}$, $m_j \geqslant n_0$ $(1 \leqslant j \leqslant k)$, *которые линейно независимы над* $\mathbb{F}_q$, *то как сама последовательность* $s_0, s_1, \ldots$, *так и соответствующая импульсная функция являются чисто периодическими последовательностями, имеющими один и тот же минимальный период.*

Доказательство. Пусть r — минимальный период последовательности $s_0, s_1, \ldots$. По лемме 8.12 для $1 \leqslant j \leqslant k$ справедливо равенство $\mathbf{s}_{m_j} A^r = \mathbf{s}_{m_j+r} = \mathbf{s}_{m_j}$, и, таким образом, A^r равняется единичной $k \times k$-матрице над полем $\mathbb{F}_q$. Отсюда получаем $\mathbf{s}_r = \mathbf{s}_0 A^r = \mathbf{s}_0$, откуда следует, что $s_0, s_1, \ldots$ является чисто периодической последовательностью. Аналогично если через $\mathbf{d}_n$ обозначить n-й вектор состояния соответствующей импульсной функции, то $\mathbf{d}_r = \mathbf{d}_0 A^r = \mathbf{d}_0$. Применив теперь теорему 8.16, получаем утверждение теоремы. □

8.20. Пример. Условие $m_j \geqslant n_0$ в формулировке теоремы 8.19 необходимо ввиду того, что существуют однородные линейные рекуррентные последовательности k-го порядка, не являющиеся чисто периодическими, но содержащие k линейно независимых векторов состояний. Пусть $d_0, d_1, \ldots$ — рекуррентная последовательность 2-го порядка над полем $\mathbb{F}_q$, являющаяся импульсной функцией и задаваемая рекуррентным соотношением $d_{n+2} = d_{n+1}$, $n = 0, 1, \ldots$. Эта последовательность имеет вид 0, 1, 1, 1, ... Очевидно, что векторы состояний $\mathbf{d}_0$ и $\mathbf{d}_1$ линейно незави-

симы над $\mathbb{F}_q$, в то время как сама последовательность $d_0, d_1, \ldots$ не является чисто периодической (в данном случае $n_0 = 1$). Утверждение, обратное утверждению теоремы 8.19, неверно. Чтобы показать это, рассмотрим линейную рекуррентную последовательность 3-го порядка $s_0, s_1, \ldots$ над полем $\mathbb{F}_2$, определяемую рекуррентным соотношением $s_{n+3} = s_n$, $n = 0, 1, \ldots$, с вектором начального состояния $\mathbf{s}_0 = (1, 1, 0)$. Тогда как сама последовательность $s_0, s_1, \ldots$, так и соответствующая импульсная функция являются периодическими последовательностями с минимальным периодом, равным 3. В то же время любые три вектора состояния последовательности $s_0, s_1, \ldots$ линейно зависимы над полем $\mathbb{F}_2$. □

Пусть $s_0, s_1, \ldots$ — линейная однородная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, удовлетворяющая линейному рекуррентному соотношению

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n, \quad n = 0, 1, \ldots, \tag{8.7}$$

где $a_j \in \mathbb{F}_q$, $0 \leqslant j \leqslant k-1$. Многочлен

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0 \in \mathbb{F}_q[x]$$

называется *характеристическим многочленом* данной линейной рекуррентной последовательности. Ясно, что он зависит только от линейного рекуррентного соотношения (8.7). Если A — матрица, определенная в (8.3), то легко заметить, что $f(x)$ совпадает с характеристическим многочленом матрицы A, как он определяется в линейной алгебре, т. е. $f(x) = \det(xI - A)$, где I — единичная матрица размера $k \times k$ над полем $\mathbb{F}_q$. С другой стороны, матрицу A можно рассматривать как сопровождающую матрицу нормированного многочлена $f(x)$.

В качестве первого применения понятия характеристического многочлена рекуррентной последовательности покажем, как в одном важном частном случае члены линейной рекуррентной последовательности могут быть явно выражены через коэффициенты многочлена $f(x)$.

8.21. Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$ и $f(x)$ — ее характеристический многочлен. Если корни $\alpha_1, \ldots, \alpha_k$ многочлена $f(x)$ все различны, то*

$$s^n = \sum_{j=1}^{k} \beta_j \alpha_j^n, \quad n = 0, 1, \ldots, \tag{8.8}$$

где $\beta_1, \ldots, \beta_k$ — различные элементы поля разложения многочлена $f(x)$ над полем $\mathbb{F}_q$, которые однозначно определяются начальными членами рекуррентной последовательности $s_0, s_1, \ldots$.

Доказательство. Константы $\beta_1, \ldots, \beta_k$ можно определить из системы линейных уравнений

$$\sum_{j=1}^{k} \alpha_j^n \beta_j = s_n, \quad n = 0, 1, \ldots, k-1.$$

Так как определитель этой системы является определителем Вандермонда, который отличен от нуля ввиду условий, наложенных на $\alpha_1, \ldots, \alpha_k$, то элементы $\beta_1, \ldots, \beta_k$ определяются однозначно и, как вытекает из правила Крамера, лежат в поле разложения $\mathbb{F}_q(\alpha_1, \ldots, \alpha_k)$ многочлена $f(x)$ над полем $\mathbb{F}_q$. Теперь для того, чтобы доказать равенство (8.8) для всех $n \geqslant 0$, достаточно проверить, удовлетворяют ли рекуррентному соотношению (8.7) элементы из правых частей формулы (8.8) при $\beta_1, \ldots, \beta_k$, определенных, как было указано выше. Но

$$\sum_{j=1}^{k} \beta_j \alpha_j^{n+k} - a_{k-1} \sum_{j=1}^{k} \beta_j \alpha_j^{n+k-1} - a_{k-2} \sum_{j=1}^{k} \beta_j \alpha_j^{n+k-2} - \ldots$$

$$\ldots - a_0 \sum_{j=1}^{k} \beta_j \alpha_j^n = \sum_{j=1}^{k} \beta_j f(\alpha_j) \alpha_j^n = 0$$

для всех $n \geqslant 0$. Тем самым теорема доказана. □

8.22. Пример. Рассмотрим линейную рекуррентную последовательность $s_0, s_1, \ldots$ над полем $\mathbb{F}_2$, задаваемую рекуррентным соотношением $s_{n+2} = s_{n+1} + s_n$, $n = 0, 1, \ldots$, и начальными значениями $s_0 = s_1 = 1$. Соответствующий характеристический многочлен равняется $f(x) = x^2 - x - 1 \in \mathbb{F}_2[x]$. Если $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, то корнями многочлена $f(x)$ являются $\alpha_1 = \alpha$ и $\alpha_2 = 1 + \alpha$. Учитывая начальные значения, получаем соотношения $\beta_1 + \beta_2 = 1$, $\beta_1 \alpha + \beta_2 (1 + \alpha) = 1$ и, следовательно, $\beta_1 = \alpha$, $\beta_2 = 1 + \alpha$. Из теоремы 8.21 следует, что $s_n = \alpha^{n+1} + (1 + \alpha)^{n+1}$ для всех $n \geqslant 0$. Так как $\beta^3 = 1$ для всех ненулевых $\beta \in \mathbb{F}_4$, получаем, что $s_{n+3} = s_n$ для всех $n \geqslant 0$, что согласуется с тем, что минимальный период этой последовательности равен 3. □

8.23. Замечание. Формула, аналогичная формуле (8.8), справедлива и в случае, когда кратность каждого корня многочлена $f(x)$ не превосходит характеристики p поля $\mathbb{F}_q$. Рассмотрим этот случай более подробно. Пусть $\alpha_1, \ldots, \alpha_m$ — различные корни многочлена $f(x)$, и пусть каждый корень α_i, $i = 1, 2, \ldots, m$, имеет кратность $e_i \leqslant p$. Пусть $e_i = 1$, если $\alpha_i = 0$. Тогда

$$s_n = \sum_{i=1}^{m} P_i(n) \alpha_i^n, \quad n = 0, 1, \ldots,$$

где P_i, $i = 1, 2, \ldots, m$, — многочлен степени не более чем e_i, коэффициенты которого однозначно определяются начальными

значениями последовательности и лежат в поле разложения многочлена $f(x)$ над полем $\mathbb{F}_q$. При этом целое число n естественным образом отождествляется с соответствующим элементом поля $\mathbb{F}_q$. Читатель, знакомый с дифференциальными уравнениями, заметит определенную аналогию с общим решением однородного линейного дифференциального уравнения с постоянными коэффициентами. □

В случае когда характеристический многочлен является неприводимым, элементы линейной рекуррентной последовательности могут быть представлены с помощью соответствующей функции следа (определение функции следа и ее основные свойства приведены во второй главе, см. определение 2.22 и теорему 2.23).

8.24. Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность k-го порядка над полем $K = \mathbb{F}_q$, удовлетворяющая уравнению (8.7), а соответствующий характеристический многочлен $f(x)$ является неприводимым многочленом над полем K. Пусть α — корень многочлена $f(x)$ в расширении $F = \mathbb{F}_{q^k}$ поля K. Тогда существует однозначно определенный элемент $\theta \in F$, такой, что*

$$s_n = \mathrm{Tr}_{F/K}(\theta\alpha^n), \quad n = 0, 1, \ldots .$$

Доказательство. Так как элементы $\{1, \alpha, \ldots, \alpha^{k-1}\}$ образуют базис поля F над K, то можно задать однозначно определенное линейное отображение $L\colon F \to K$, полагая $L(\alpha^n) = s_n$ для $n = 0, 1, \ldots, k-1$. По теореме 2.24 существует однозначно определенный элемент $\theta \in F$, такой, что $L(\gamma) = \mathrm{Tr}_{F/K}(\theta\gamma)$ для всех $\gamma \in F$. В частности,

$$s_n = \mathrm{Tr}_{F/K}(\theta\alpha^n), \quad n = 0, 1, \ldots, k-1.$$

Остается показать, что элементы $\mathrm{Tr}_{F/K}(\theta\alpha^n)$, $n = 0, 1, \ldots$, образуют однородную линейную рекуррентную последовательность с характеристическим многочленом $f(x)$. Но если

$$f(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0 \in K[x],$$

то, используя свойства функции следа, получаем

$$\begin{aligned}\mathrm{Tr}_{F/K}(\theta\alpha^{n+k}) - a_{k-1}\mathrm{Tr}_{F/K}(\theta\alpha^{n+k-1}) - \cdots - a_0\mathrm{Tr}_{F/K}(\theta\alpha^n) &= \\ = \mathrm{Tr}_{F/K}(\theta\alpha^{n+k} - a_{k-1}\theta\alpha^{n+k-1} - \cdots - a_0\theta\alpha^n) &= \\ = \mathrm{Tr}_{F/K}(\theta\alpha^n f(\alpha)) = 0 &\end{aligned}$$

для всех $n \geqslant 0$. □

Другие соотношения между линейными рекуррентными последовательностями и их характеристическими многочленами могут быть получены из следующего полиномиального тождества.

8.25. Теорема. *Пусть* $s_0, s_1, \ldots$ — *однородная линейная рекуррентная последовательность* k-*го порядка над полем* $\mathbb{F}_q$, *удовлетворяющая рекуррентному соотношению* (8.7) *и являющаяся чисто периодической последовательностью с периодом* r. *Пусть* $f(x)$ — *характеристической многочлен этой последовательности. Тогда имеет место равенство*

$$f(x)\, s(x) = (1 - x^r)\, h(x), \tag{8.9}$$

где

$$s(x) = s_0 x^{r-1} + s_1 x^{r-2} + \cdots + s_{r-2}x + s_{r-1} \in \mathbb{F}_q[x],$$
$$h(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} a_{i+j+1} s_i x^j \in \mathbb{F}_q[x], \quad a_k = -1. \tag{8.10}$$

Доказательство. Сравним коэффициенты при одинаковых степенях x в обеих частях равенства (8.9). Пусть c_t (соответственно d_t) — коэффициент при x^t, $0 \leqslant t \leqslant k + r - 1$, в левой (соответственно правой) части равенства (8.9). Так как $f(x) = -\sum_{i=0}^{k} a_i x^i$, получаем

$$c_t = -\sum_{\substack{0 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant r-1 \\ i+j=t}} a_i s_{r-1-j}, \quad 0 \leqslant t \leqslant k + r - 1. \tag{8.11}$$

Заметим, что линейное рекуррентиое соотношение (8.7) может быть также записано в виде

$$\sum_{i=0}^{k} a_i s_{n+i} = 0 \quad \text{для всех } n \geqslant 0. \tag{8.12}$$

Выделим теперь для отдельного рассмотрения следующие четыре случая. Если $k \leqslant t \leqslant r - 1$, то из (8.11) и (8.12) следует

$$c_t = -\sum_{i=0}^{k} a_i s_{r-1-t+i} = 0 = d_t.$$

Если $t \leqslant r - 1$ и $t < k$, то из (8.11), (8.12) и периодичности нашей последовательности получаем

$$c_t = -\sum_{i=0}^{t} a_i s_{r-1-t+i} = \sum_{i=t+1}^{k} a_i s_{r-1-t+i} =$$
$$= \sum_{i=t+1}^{k} a_i s_{i-t-1} = \sum_{i=0}^{k-1-t} a_{i+t+1} s_i = d_t.$$

Если $t \geqslant r$ и $t \geqslant k$, из (8.11) следует, что

$$c_t = -\sum_{i=t-r+1}^{k} a_i s_{r-1-t+i} = -\sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i = d_t.$$

Если $r \leqslant t < k$, то из (8.11) и периодичности нашей последовательности вытекает, что

$$c_t = -\sum_{i=t-r+1}^{t} a_i s_{r-1-t+i} = -\sum_{i=0}^{r-1} a_{i+t-r+1} s_i =$$
$$= \sum_{i=r}^{k-1-t+r} a_{i+t-r+1} s_i - \sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i =$$
$$= \sum_{i=0}^{k-1-t} a_{i+t+1} s_{i+r} - \sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i =$$
$$= \sum_{i=0}^{k-1-t} a_{i+t+1} s_i - \sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i = d_t.$$

Таким образом, теорема доказана. □

Лемма 3.1 утверждает, что для любого многочлена $f(x) \in \mathbb{F}_q[x]$, $f(0) \neq 0$, найдется натуральное число e, такое, что $f(x)$ делит $x^e - 1$. Это приводит к понятию порядка многочлена $f(x)$ (см. определение 3.2), который обозначается через ord $(f(x))$.

8.26. Лемма. *Пусть*

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0 \in \mathbb{F}_q[x],$$

$k \geqslant 1$, $a_0 \neq 0$. *Тогда* ord $(f(x))$ *равняется порядку матрицы* A, *определяемой формулой* (8.3) *и рассматриваемой как элемент группы* $GL(k, \mathbb{F}_q)$.

Доказательство. Ввиду того что A — сопровождающая матрица многочлена $f(x)$, то $f(x)$ в свою очередь является минимальным многочленом матрицы A. Следовательно, если I — единичная $k \times k$-матрица над полем $\mathbb{F}_q$, то равенство $A^e = I$ для иекоторого натурального числа e выполняется тогда и только тогда, когда многочлен $f(x)$ делит $x^e - 1$. Искомый результат следует теперь из определений порядка многочлена $f(x)$ и порядка матрицы A как элемента группы $GL(k, \mathbb{F}_q)$. □

8.27. Теорема. *Пусть* $s_0, s_1, \ldots$ — *однородная линейная рекуррентная последовательность над полем* $\mathbb{F}_q$ *и* $f(x) \in \mathbb{F}_q[x]$ — *характеристический многочлен этой последовательности. Тогда минимальный период этой последовательности делит* ord $(f(x))$, *а минимальный период соответствующей импульсной функции равняется* ord $(f(x))$. *При этом если* $f(0) \neq 0$, *то обе последовательности являются чисто периодическими.*

Доказательство. Если $f(0) \neq 0$, то в силу леммы 8.26 результат является простой переформулировкой утверждений теорем 8.13 и 8.17. В этом случае чистая периодичность будет следовать из теоремы 8.11. Если же $f(0) = 0$, то представим $f(x)$ в виде $f(x) = x^h g(x)$, где $g(0) \neq 0$ (как в определении 3.2), и положим

$t_n = s_{n+h}$, $n = 0, 1, \ldots$. Если $\deg(g(x)) > 0$, то $t_0, t_1, \ldots$ — однородная линейная рекуррентная последовательность с характеристическим многочленом $g(x)$. Ее минимальный период совпадает с минимальным периодом последовательности $s_0, s_1, \ldots$. Значит, как было показано выше, минимальный период последовательности $s_0, s_1, \ldots$ делит число $\operatorname{ord}(g(x)) = \operatorname{ord}(f(x))$. Соответствующее утверждение для импульсной функции доказывается аналогичным образом. Если же $g(x)$ — постоянный многочлен, то теорема становится тривиальной. □

Заметим, что при $f(0) \neq 0$ минимальный период импульсной функции можно также получить из равенства (8.9) следующим способом. Для импульсной функции, характеристический многочлен которой равен $f(x)$, многочлен $h(x)$, появляющийся в формуле (8.10), равен просто -1. Значит, если r — минимальный период импульсной функции, то на основании (8.9) $f(x)$ делит $x^r - 1$, и, следовательно, $r \geqslant \operatorname{ord}(f(x))$. С другой стороны, на основании первой части утверждения теоремы 8.27 r должен делить $\operatorname{ord}(f(x))$. Таким образом, получаем искомое равенство $r = \operatorname{ord}(f(x))$.

8.28 Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$ с ненулевым вектором начального состояния. Пусть ее характеристический многочлен $f(x) \in \mathbb{F}_q[x]$ является неприводимым многочленом над полем $\mathbb{F}_q$ и удовлетворяет условию $f(0) \neq 0$. Тогда последовательность $s_0, s_1, \ldots$ является чисто периодической последовательностью и ее минимальный период r равен* $\operatorname{ord}(f(x))$.

Доказательство. Из теоремы 8.27 вытекает, что рассматриваемая последовательность является чисто периодической и ее минимальный период r делит $\operatorname{ord}(f(x))$. С другой стороны, из (8.9) следует, что $f(x)$ делит $(x^r - 1)h(x)$. Так как $s(x)$, а следовательно, и $h(x)$ являются ненулевыми многочленами и так как $\deg(h(x)) < \deg(f(x))$, то из неприводимости $f(x)$ вытекает, что многочлен $f(x)$ делит $x^r - 1$, и, значит, $r \geqslant \operatorname{ord}(f(x))$. □

Дадим теперь другое доказательство следствия 3.4. Для удобства приведем еще раз его формулировку.

8.29. Теорема. *Пусть $f(x) \in \mathbb{F}_q[x]$ — неприводимый многочлен над полем $\mathbb{F}_q$ и $\deg(f(x)) = k$. Тогда* $\operatorname{ord}(f(x))$ *делит* $q^k - 1$.

Доказательство. Не теряя общности, можно считать, что $f(x)$ является нормированным многочленом и $f(0) \neq 0$. Рассмо-

трим однородную лиiейную рекуррентную последовательность над полем $\mathbb{F}_q$ с характеристическим многочленом $f(x)$ и ненулевым вектором начального состояния. По теореме 8.28 эта последовательность является чисто периодической, и минимальный период этой последовательности равняется ord $(f(x))$. Тогда в ней встречаются ord $(f(x))$ различных векторов состояний. Если ord $(f(x))$ меньше $q^k - 1$, общего числа ненулевых k-мерных векторов над полем $\mathbb{F}_q$, то можно выбрать k-мерный вектор, который не встречается в качестве одного из векторов состояния указанной выше последовательности. Возьмем этот вектор в качестве вектора начального состояния другой однородной линейной рекуррентной последовательности над полем $\mathbb{F}_q$ с тем же характеристическим многочленом $f(x)$. Ни один из $e = \text{ord}\,(f(x))$ различиых векторов состояния этой последовательности не равняется ни одному вектору состояния предыдущей последовательности. В противном случае эти две последовательности, начиная с какого-то места, должны были бы совпадать, и тогда вектор начального состояния второй последовательности должен был бы встретиться в первой последовательности в качестве одного из ее векторов состояния, что противоречит его выбору. Продолжая указанным выше образом строить новые рекуррентные последовательности, получаем разбиение множества, состоящего из $q^k - 1$ ненулевых k-мерных векторов над полем $\mathbb{F}_q$, на подмножества мощности $e = \text{ord}\,(f(x))$ каждое, что и доказывает утверждение теоремы. □

8.30. Пример. Рассмотрим линейное рекуррентное соотношение $s_{n+6} = s_{n+4} + s_{n+2} + s_{n+1} + s_n$, $n = 0, 1, \ldots$, над полем $\mathbb{F}_2$. Соответствующий характеристический многочлен $f(x) = x^6 - x^4 - x^2 - x - 1 \in \mathbb{F}_2[x]$ является неприводимым многочленом над полем $\mathbb{F}_2$. Кроме того, $f(x)$ делит $x^{21} - 1$ и не является делителем многочлена вида $x^e - 1$ ни для какого $0 < e < 21$. Таким образом, ord $(f(x)) = 21$. Импульсная функция, соответствующая данному рекуррентному соотношению, имеет вид

0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, ...

Как и должно быть, эта последовательность периодична с минимальным периодом $r = 21$. Если в качестве вектора начального состояния взять вектор (0, 0, 0, 0, 1, 1), то мы получим бинарную последовательность

0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, ...

с минимальным периодом $r = 21$. Если же в качестве вектора начального состояния взять вектор (0, 0, 0, 1, 0, 0), то мы получим бинарную последовательность

0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, ... ,

также имеющую минимальный период 21. При этом каждый из ненулевых 6-мерных векторов над полем $\mathbb{F}_2$ появляется в качестве вектора состояния в точности в одной из этих трех последовательностей. Если в качестве вектора начального состояния взять любой ненулевой вектор, то мы получим рекуррентную последовательность, имеющую минимальный период, равный 21, и совпадающую с точностью до сдвига с одной из трех полученных выше последовательностей.

8.31. Пример. Если многочлен $f(x) \in \mathbb{F}_q[x]$ степени k приводим, то его порядок $\operatorname{ord}(f(x))$ не обязательно делит число $q^k - 1$. Чтобы показать это, рассмотрим, например, многочлен $f(x) = x^5 + x + 1 \in \mathbb{F}_2[x]$. Этот многочлен приводим, так как

$$f(x) = x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1).$$

Из теоремы 8.27 и примера 8.14 следует, что $\operatorname{ord}(f(x))$ равен 21 и не является делителем числа $2^5 - 1 = 31$. □

Для приложений особый интерес представляют линейные рекуррентные последовательности, имеющие очень большой минимальный период. Из теоремы 8.7 известно, что для однородной линейной рекуррентной последовательности k-го порядка над полем $\mathbb{F}_q$ минимальный период не может превышать $q^k - 1$. Для того чтобы построить рекуррентную последовательность, минимальный период которой в точности равен $q^k - 1$, воспользуемся понятием примитивного многочлена (см. определение 3.15).

8.32. Определение. Однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$, характеристический многочлен которой является примитивным многочленом над полем $\mathbb{F}_q$, а вектор начального состояния — ненулевым вектором, называется *последовательностью максимального периода* над полем $\mathbb{F}_q$.

8.33. Теорема. *Каждая последовательность k-го порядка и максимального периода над полем $\mathbb{F}_q$ является чисто периодической последовательностью, а ее минимальный период равняется $q^k - 1$, наибольшему из возможных значений, которое может принимать минимальный период однородной линейной рекуррентной последовательности k-го порядка над полем $\mathbb{F}_q$.*

Доказательство. Тот факт, что рассматриваемая последовательность является чисто пернодической последовательностью, минимальный период которой равен $q^k - 1$, есть следствие теорем 8.28 и 3.16. Остальное легко вытекает из теоремы 8.7. □

8.34. Пример. Характеристическим многочленом рассмотренного в примере 8.2 линейиого рекуррентного соотношения над полем $\mathbb{F}_2$

$$s_{n+7} = s_{n+4} + s_{n+3} + s_{n+2} + s_n, \quad n = 0, 1, \ldots,$$

является многочлен $f(x) = x^7 - x^4 - x^3 - x^2 - 1 \in \mathbb{F}_2[x]$. Так как $f(x)$ — примитивный многочлен над полем $\mathbb{F}_2$, то каждая рекуррентная последовательность с ненулевым начальным вектором, задаваемая указанным линейным рекуррентным соотношением, является последовательностью максимального периода над полем $\mathbb{F}_2$. Если в качестве вектора начального состояния выбрать произвольный ненулевой вектор, то мы получим последовательность $s_0, s_1, \ldots$, имеющую в соответствии с теоремой 8.33 минимальный период $2^7 - 1 = 127$. Таким образом, все возможные иенулевые векторы из $\mathbb{F}_2^7$ встречаются в качестве векторов состояний этой последовательности. Любая другая последовательность максимального периода, получаемая из этого же линейного рекуррентного соотношения, представляет собой некоторый сдвиг последовательности $s_0, s_1, \ldots$. □

§ 3. Производящие функции

До сих пор при изучении линейных рекуррентных последовательностей мы пользовались понятиямн линейной алгебры, алгебры многочленов и теории конечных полей. Использование алгебраического аппарата формальных степенных рядов позволит нам получить другие замечательные результаты, связанные с линейными рекуррентными последовательностями.

Пусть дана произвольная последовательность $s_0, s_1, \ldots$ элементов поля $\mathbb{F}_q$. С этой последовательностью можно связать ее *производящую функцию* от переменной x, которая является просто формальным выражением вида

$$G(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n + \cdots = \sum_{n=0}^{\infty} s_n x^n, \quad (8.13)$$

где x — формальная переменная. В основе этого подхода лежит мысль, что в функции $G(x)$ «собраны» в определенном порядке все члены последовательности $s_0, s_1, \ldots$, так что функция $G(x)$ может некоторым образом отражать свойства этой последовательностн. Название «производящая функция», строго говоря, является неправильным, так как мы рассматриваем $G(x)$ не как функцию аргумента x, а просто как некоторый формальный объект (аналогично многочлены в сущности тоже можно рассматривать как формальные объекты, которые не следует путать с функциями). Термнн «производящая функция» был перенесен сюда со случая последовательностей действительных или комплексных чисел, где может оказаться, что ряд, аналогичный (8.13), сходится при подстановке некоторого действительного или комплексного числа x_0 вместо переменной x, что позволяет приписать какое-то конкретное значенне функции $G(x_0)$. В рассматриваемой же ситуации вопрос о сходимости или расходимости

ряда (8.13) не возникает, так как мы рассматриваем $G(x)$ как «иероглиф» последовательности $s_0, s_1, \ldots$.

В общем случае выражение вида

$$B(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n + \cdots = \sum_{n=0}^{\infty} b_n x^n,$$

где $b_0, b_1, \ldots$ — последовательность элементов из $\mathbb{F}_q$, называется *формальным степенным рядом* (над полем $\mathbb{F}_q$). В таком контексте члены $b_0, b_1, \ldots$ нашей последовательности называются также *коэффициентами* формального степенного ряда. Прилагательное «формальный» вновь отражает ту мысль, что сходимость или расходимость этих выражений (какой бы смысл мы в это ни вкладывали) не имеет никакого отношения к их изучению. Два формальных степенных ряда над $\mathbb{F}_q$

$$B(x) = \sum_{n=0}^{\infty} b_n x^n \quad \text{и} \quad C(x) = \sum_{n=0}^{\infty} c_n x^n$$

считаются равными, если $b_n = c_n$ для всех $n = 0, 1, \ldots$. Таким образом, множество всех формальных степенных рядов над $\mathbb{F}_q$ находится во взаимно однозначном соответствии с множеством всех последовательностей, состоящих из элементов поля $\mathbb{F}_q$. Может показаться, что мы ничего не выиграем от перехода к формальным степенным рядам. На самом деле «смысл существования» этих объектов состоит в том, что мы можем наделить множество формальных степенных рядов над $\mathbb{F}_q$ богатой и интересной алгебраической структурой, причем совершенно естественным образом. Это будет обсуждаться впоследствии.

Заметим, во-первых, что многочлен

$$p(x) = p_0 + p_1 x + \cdots + p_k x^k \in \mathbb{F}_q[x]$$

тоже можно рассматривать как формальный степенной ряд над $\mathbb{F}_q$, отождествляя его с рядом

$$P(x) = p_0 + p_1 x + \cdots + p_k x^k + 0 \cdot x^{k+1} + 0 \cdot x^{k+2} + \cdots .$$

Введем теперь алгебраические операции сложения и умножения формальных степенных рядов таким образом, чтобы они являлись перенесением на множество формальных степенных рядов соответствующих операций, определенных на многочленах. Подробнее, если

$$B(x) = \sum_{n=0}^{\infty} b_n x^n \quad \text{и} \quad C(x) = \sum_{n=0}^{\infty} c_n x^n$$

— два формальных степенных ряда над $\mathbb{F}_q$, то определим их *сумму* как формальный степенной ряд

$$B(x)+C(x)=\sum_{n=0}^{\infty}(b_n+c_n)\,x^n,$$

а их *произведение* — как формальный степенной ряд

$$B(x)\,C(x)=\sum_{n=0}^{\infty}d_nx^n,\ \text{где}\ d_n=\sum_{k=0}^{n}b_kc_{n-k},\quad n=0,\ 1,\ \ldots.$$

Если $B(x)$ и $C(x)$ оба являются многочленами над $\mathbb{F}_q$, то определенные выше операции совпадают со сложением и умножением обычных многочленов. Здесь же надо отметить, что принцип подстановки, который так полезен в алгебре многочленов, не действителен для формальных степенных рядов по той простой причине, что выражение $B(a)$, где a — элемент поля $\mathbb{F}_q$, а $B(x)$ — формальный степенной ряд над $\mathbb{F}_q$, может быть бессмысленным. Это плата за то, что мы игнорируем вопросы сходимости рядов.

8.35. **Пример.** Пусть

$$B(x)=2+x^2\ \text{и}\ C(x)=1+x+x^2+\cdots+x^n+\cdots=\sum_{n=0}^{\infty}1\cdot x^n$$

— формальные степенные ряды над полем $\mathbb{F}_3$. Тогда

$$B(x)+C(x)=x+2x^2+x^3+\cdots+x^n+\cdots=\sum_{n=0}^{\infty}d_nx^n,$$

где $d_0=0$, $d_1=1$, $d_2=2$ и $d_n=1$ для всех $n\geqslant 3$, а

$$B(x)\,C(x)=2+2x+0\cdot x^2+0\cdot x^3+\ldots=2+2x.\qquad\square$$

Очевидно, что сложение формальных степенных рядов над $\mathbb{F}_q$ является ассоциативной и коммутативной операцией. Формальный степенной ряд $0=\sum_{n=0}^{\infty}0\cdot x^n$ является нулем относительно операции сложения. Если $B(x)=\sum_{n=0}^{\infty}b_nx^n$ — произвольный формальный степенной ряд над $\mathbb{F}_q$, то обратным к нему относительно операции сложения является степенной ряд $\sum_{n=0}^{\infty}(-b_n)\,x^n$, который обозначается через $-B(x)$. Обычно мы будем писать $B(x)-C(x)$ вместо $B(x)+(-C(x))$.

Очевидно, что и операция умножения формальных степенных рядов над $\mathbb{F}_q$ является коммутативной операцией, а формальный

степенной ряд $1 = 1 + 0 \cdot x + 0 \cdot x^2 + \ldots + 0 \cdot x^n + \ldots$ — единичный элемент относительно операции умножения. Умножение является ассоциативной операцией, так как если

$$B(x) = \sum_{n=0}^{\infty} b_n x^n, \quad C(x) = \sum_{n=0}^{\infty} c_n x^n, \quad D(x) = \sum_{n=0}^{\infty} d_n x^n,$$

то оба формальных степенных ряда

$$(B(x)\, C(x))\, D(x) \text{ и } B(x)\, (C(x)\, D(x))$$

равняются

$$\sum_{n=0}^{\infty} \Bigg(\sum_{(i,\, j,\, k) \in L(n)} b_i c_j d_k \Bigg) x^n,$$

где $L(n)$ — множество всех упорядоченных троек (i, j, k), $i \geqslant 0$, $j \geqslant 0$, $k \geqslant 0$, $i + j + k = n$. Кроме того, справедлив закон дистрибутивности

$$\begin{aligned} B(x)(C(x) + D(x)) &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} b_k (c_{n-k} + d_{n-k}) \right) x^n = \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} b_k c_{n-k} + \sum_{k=0}^{n} b_k d_{n-k} \right) x^n = \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} b_k c_{n-k} \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} b_k d_{n-k} \right) x^n = \\ &= B(x) C(x) + B(x) D(x). \end{aligned}$$

Тем самым мы показали, что множество всех формальных степенных рядов над $\mathbb{F}_q$ с введенными там операциями сложения и умножения становится коммутативным кольцом с единицей. Это кольцо называется *кольцом формальных степенных рядов* над полем $\mathbb{F}_q$ и обозначается через $\mathbb{F}_q[[x]]$. Кольцо многочленов $\mathbb{F}_q[x]$ является подкольцом кольца $\mathbb{F}_q[[x]]$. Более сильное утверждение содержится в следующей теореме.

8.36. Теорема. *Кольцо $\mathbb{F}_q[[x]]$ формальных степенных рядов над полем $\mathbb{F}_q$ является областью целостности, которая содержит кольцо многочленов $\mathbb{F}_q[x]$ в качестве подкольца.*

Доказательство. Остается проверить, что $\mathbb{F}_q[[x]]$ не содержит делителей нуля, т. е. что произведение двух элементов кольца $\mathbb{F}_q[[x]]$ равняется нулю тогда и только тогда, когда один из

сомножителей равен нулю. Предположим противное. Пусть $B(x)\,C(x) = 0$, и при этом

$$B(x) = \sum_{n=0}^{\infty} b_n x^n \neq 0, \quad C(x) = \sum_{n=0}^{\infty} c_n x^n \neq 0$$

лежат в $\mathbb{F}_q[[x]]$. Пусть k — наименьшее натуральное число, для которого $b_k \neq 0$, а m — наименьшее натуральное число, для которого $c_m \neq 0$. Тогда коэффициент при x^{k+m} в произведении $B(x)\,C(x)$ равняется $b_k c_m \neq 0$, а это противоречит тому, что $B(x)\,C(x) = 0$. □

Для приложений нам понадобится выяснить, какие из элементов кольца $\mathbb{F}_q[[x]]$ обратимы относительно операции умножения, т. е. для каких элементов $B(x) \in \mathbb{F}_q[[x]]$ найдутся соответствующие элементы $C(x) \in \mathbb{F}_q[[x]]$, такие, что $B(x)\,C(x) = 1$. Обратимые степенные ряды можно легко охарактеризовать.

8.37. Теорема. *Формальный степенной ряд*

$$B(x) = \sum_{n=0}^{\infty} b_n x^n \in \mathbb{F}_q[[x]]$$

имеет обратный относительно операции умножения элемент тогда и только тогда, когда $b_0 \neq 0$.

Доказательство. Если

$$C(x) = \sum_{n=0}^{\infty} c_n x^n$$

— такой элемент из $\mathbb{F}_q[[x]]$, что $B(x)\,C(x) = 1$, то коэффициенты $b_0, b_1, \ldots$ и $c_0, c_1, \ldots$ должны удовлетворять следующей бесконечной системе уравнений:

$$\begin{aligned}
b_0 c_0 &= 1,\\
b_0 c_1 + b_1 c_0 &= 0,\\
b_0 c_2 + b_1 c_1 + b_2 c_0 &= 0,\\
&\cdots\cdots\cdots\\
b_0 c_n + b_1 c_{n-1} + \cdots + b_n c_0 &= 0,\\
&\cdots\cdots\cdots
\end{aligned}$$

Из первого уравнения мы получаем, что обязательно $b_0 \neq 0$. При этом если это условие удовлетворяется, то c_0 однозначно определяется из первого уравнения. Переходя ко второму уравнению, видим, что теперь можно однозначно определить c_1. В общем все коэффициенты $c_0, c_1, \ldots$ можно рекурсивно определить из первого уравнения и рекуррентного соотношения

$$c_n = -b_0^{-1} \sum_{k=1}^{n} b_k c_{n-k}, \quad n = 1, 2, \ldots .$$

Получившийся формальный степенной ряд $C(x)$ является обратным к $B(x)$ относительно операции умножения формальных степенных рядов. □

Таким образом, если для $B(x) \in \mathbb{F}_q[[x]]$ существует обратный элемент относительно операции умножения формальных степенных рядов, то этот элемент определен однозначно. Обозначим его через $1/B(x)$. Произведение $A(x)(1/B(x))$, где $A(x) \in \mathbb{F}_q[[x]]$, будет обычно записываться в виде $A(x)/B(x)$. Так как $\mathbb{F}_q[[x]]$ — область целостности, то для указанных выше выражений справедливы обычные правила оперирования с дробями. Элемент, обратный к элементу $B(x)$ относительно умножения, или выражение $A(x)/B(x)$ можно вычислить с помощью алгоритма, приведенного при доказательстве теоремы 8.37. Для подобных вычислений применимо также и обычное деление углом.

8.38. Пример. Пусть многочлен $B(x) = 3 + x + x^2$ рассматривается как формальный степенной ряд над полем $\mathbb{F}_5$. По теореме 8.37 $B(x)$ обратим относительно операции умножения формальных степенных рядов. Вычислим $1/B(x)$ с помощью алгоритма деления углом:

$$\begin{array}{l|l}
1+0\cdot x+0\cdot x^2+0\cdot x^3+0\cdot x^4+0\cdot x^5+0\cdot x^6+\ldots & 3+x+x^2 \\
\cline{2-2}
-1-2x-2x^2 & 2+x+4x^2+2x^4+\ldots \\
\cline{1-1}
3x+3x^2+0\cdot x^3 & \\
-3x-x^2-x^3 & \\
\cline{1-1}
2x^2+4x^3+0\cdot x^4 & \\
-2x^2-4x^3-4x^4 & \\
\cline{1-1}
x^4+0\cdot x^5+0\cdot x^6 & \\
\ldots\ldots\ldots &
\end{array}$$

Таким образом, мы получили, что

$$\frac{1}{3+x+x^2} = 2 + x + 4x^2 + 2x^4 + \ldots\ .$$ □

8.39. Пример. Вычислим $A(x)/B(x) \in \mathbb{F}_2[[x]]$, где

$$A(x) = 1 + x + x^2 + x^3 + \ldots = \sum_{n=0}^{\infty} 1 \cdot x^n,$$

а $B(x) = 1 + x + x^3$. Используя алгоритм деления углом, опуская члены с нулевыми коэффициентами и учитывая то, что в поле $\mathbb{F}_2$ выполняется равенство $-1 = +1$, получаем

$$\begin{array}{l|l}
1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+\ldots & 1+x+x^3 \\
\cline{2-2}
1+x+x^3 & 1+x^2+x^3+x^7+\ldots \\
\cline{1-1}
x^2+x^4+x^5 & \\
x^2+x^3+x^5 & \\
\cline{1-1}
x^3+x^4+x^6 & \\
x^3+x^4+x^6 & \\
\cline{1-1}
x^7+x^8+x^9+x^{10} & \\
\ldots\ldots\ldots &
\end{array}$$

Таким образом,

$$\frac{1+x+x^2+x^3+\cdots}{1+x+x^3}=1+x^2+x^3+x^7+\ldots\ . \qquad \square$$

Для применения теории формальных степенных рядов рассмотрим теперь однородную линейную последовательность k-го порядка $s_0, s_1, \ldots$ над полем $\mathbb{F}_q$, удовлетворяющую линейному рекуррентному соотношению (8.7). Назовем многочлен

$$f^*(x)=1-a_{k-1}x-a_{k-2}x^2-\cdots-a_0x^k\in\mathbb{F}_q[x] \qquad (8.14)$$

возвратным характеристическим многочленом [1]) этой последовательности. Характеристический многочлен $f(x)$ и возвратный характеристический многочлен $f^*(x)$ связаны между собой соотношением $f^*(x)=x^kf(1/x)$. Можно показать, что для производящих функций справедливо следующее фундаментальное равенство.

8.40. Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, удовлетворяющая линейному рекуррентному соотношению* (8.7). *Пусть $f^*(x)\in\mathbb{F}_q[x]$ — возвратный характеристический многочлен этой последовательности, а $G(x)\in\mathbb{F}_q[[x]]$ — производящая функция этой последовательности, определенная в* (8.13). *Тогда имеет место равенство*

$$G(x)=\frac{g(x)}{f^*(x)}, \qquad (8.15)$$

где

$$g(x)=-\sum_{j=0}^{k-1}\sum_{i=0}^{j}a_{i+k-j}s_ix^j\in\mathbb{F}_q[x] \qquad (8.16)$$

и $a_k=-1$. Обратно, если $g(x)$ — производящий многочлен над полем $\mathbb{F}_q$, $\deg(g(x))<k$, а $f^*(x)\in\mathbb{F}_q[x]$ задается равенством (8.14), *то формальный степенной ряд $G(x)\in\mathbb{F}_q[[x]]$, задаваемый равенством* (8.15), *является производящей функцией однородной линейной рекуррентной последовательности k-го порядка над полем $\mathbb{F}_q$, удовлетворяющей линейному рекуррентному соотношению* (8.7).

---

[1]) В литературе этот многочлен называется также *двойственным характеристическим многочленом*. — *Прим. перев.*

Доказательство. Имеем

$$f^*(x)\,G(x) = -\left(\sum_{n=0}^{k} a_{k-n}x^n\right)\left(\sum_{n=0}^{\infty} s_n x^n\right) =$$
$$= -\sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_{i+k-j}s_i\right)x^j - \sum_{j=k}^{\infty}\left(\sum_{i=j-k}^{j} a_{i+k-j}s_i\right)x^j =$$
$$= g(x) - \sum_{j=k}^{\infty}\left(\sum_{i=0}^{k} a_i s_{j-k+i}\right)x^j. \tag{8.17}$$

Теперь, если последовательность $s_0, s_1, \ldots$ удовлетворяет (8.7), то из (8.12) следует, что $f^*(x)\,G(x) = g(x)$. Тогда в силу того, что по теореме 8.37 $f^*(x)$ имеет обратный относительно операции умножения элемент в $\mathbb{F}_q[[x]]$, получаем справедливость равенства (8.15). Обратно, из (8.17) следует, что произведение $f^*(x)\,G(x)$ равняется многочлену степени, меньшей чем k, только тогда, когда

$$\sum_{i=0}^{k} a_i s_{j-k+i} = 0 \quad \text{для всех} \quad j \geqslant k.$$

Последнее как раз означает, что последовательность $s_0, s_1, \ldots$, составленная из коэффициентов формального степенного ряда $G(x)$, удовлетворяет линейному рекуррентному соотношению (8.7). □

Приведенную выше теорему можно коротко сформулировать следующим образом: существует взаимно однозначное соответствие между однородными линейными рекуррентными последовательностями k-го порядка с возвратным характеристическим многочленом $f^*(x)$ и дробями вида $g(x)/f^*(x)$, такими, что $\deg(g(x)) < k$. Равенство (8.15) в этом случае может быть использовано для вычисления членов линейной рекуррентной последовательности с помощью алгоритма деления углом.

8.41. Пример. Рассмотрим линейное рекуррентное соотношение

$$s_{n+4} = s_{n+3} + s_{n+1} + s_n, \quad n = 0, 1, \ldots,$$

над полем $\mathbb{F}_2$. Соответствующий возвратный характеристический многочлен имеет вид

$$f^*(x) = 1 - x - x^3 - x^4 = 1 + x + x^3 + x^4 \in \mathbb{F}_2[x].$$

Если вектор начального состояния равен (1, 1, 0, 1), то многочлен $g(x)$, определенный в (8.16), равен $g(x) = 1 + x^2$. Тогда

производящая функция $G(x)$ рассматриваемой рекуррентной последовательности может быть получена с помощью деления углом:

$$
\begin{array}{l|l}
1 + x^2 & 1 + x + x^3 + x^4 \\
\hline
1 + x + x^3 + x^4 & 1 + x + x^3 + x^4 + x^6 + \ldots \\
\hline
x + x^2 + x^3 + x^4 & \\
x + x^2 + x^4 + x^5 & \\
\hline
x^3 + x^5 & \\
x^3 + x^4 + x^6 + x^7 & \\
\hline
x^4 + x^5 + x^6 + x^7 & \\
x^4 + x^5 + x^7 + x^8 & \\
\hline
x^6 + x^3 & \\
\ldots\ldots\ldots\ldots &
\end{array}
$$

Таким образом,

$$G(x) = \frac{1 + x^2}{1 + x + x^3 + x^4} = 1 + x + x^3 + x^4 + x^6 + \ldots,$$

что соответствует бинарной последовательности 1, 1, 0, 1, 1, 0, 1, ..., имеющей минимальный период 3. Импульсную функцию, связанную с данным линейным рекуррентным соотношением, можно получить, если положить $g(x) = x^3$. Алгоритм деления углом дает в этом случае производящую функцию

$$G(x) = \frac{x^3}{1 + x + x^3 + x^4} = x^3 + x^4 + x^5 + x^9 + x^{10} + x^{11} + \ldots,$$

что соответствует периодической бинарной последовательности 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, ... с минимальным периодом, равным 6. □

Из равенства (8.15) можно получить другое доказательство теоремы 8.25. Действительно, ввиду того что последовательность $s_0, s_1, \ldots$ является чисто периодической последовательностью с минимальным периодом равным r, ее производящая функция $G(x)$ может быть записана в внде

$$G(x) = (s_0 + s_1 x + \cdots + s_{r-1} x^{r-1})(1 + x^r + x^{2r} + \ldots) = \frac{s^*(x)}{1 - x^r},$$

где $s^*(x) = s_0 + s_1 x + \ldots + s_{r-1} x^{r-1}$. С другой стороны, используя обозначения теоремы 8.40, из (8.15) получаем, что $G(x) = g(x)/f^*(x)$. Приравнивая полученные выражения для $G(x)$, приходим к полиномиальному равенству $f^*(x)\, s^*(x) = (1 - x^r)\, g(x)$. Если $f(x)$ и $s(x)$ такие же, как в (8.9), то

$$f(x)\, s(x) = x^k f^*(1/x)\, x^{r-1} s^*(1/x) = (x^r - 1)\, x^{k-1}\, g(1/x).$$

Сравнивая (8.10) и (8.16), получаем

$$x^{k-1}g\,(1/x) = -h\,(x), \tag{8.18}$$

откуда и следует равенство (8.9).

§ 4. Минимальный многочлен

Хотя до сих пор мы этого не отмечали, очевидно, что линейная рекуррентная последовательность удовлетворяет множеству других линейных рекуррентных соотношений помимо того, которое определяет эту последовательность. Так, если последовательность $s_0, s_1, \ldots$ является чисто периодической последовательностью с периодом r, то она удовлетворяет линейным рекуррентным соотношениям $s_{n+r} = s_n$ $(n = 0, 1, \ldots)$, $s_{n+2r} = s_n$ $(n = 0, 1, \ldots)$ и т. д. Экстремальный случай представляет собой последовательность $0, 0, 0, \ldots$, которая удовлетворяет любому однородному линейному рекуррентному соотношению. Следующая теорема описывает, как связаны между собой различные линейные рекуррентные соотношения, которым удовлетворяет данная однородная линейная рекуррентная последовательность.

8.42. Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$. Тогда существует однозначно определенный нормированный многочлен $m(x) \in \mathbb{F}_q[x]$, обладающий следующим свойством: нормированный многочлен положительной степени $f(x) \in \mathbb{F}_p[x]$ является характеристическим многочленом данной последовательности $s_0, s_1, \ldots$ тогда и только тогда, когда $f(x)$ делится на $m(x)$.*

Доказательство. Пусть $f_0(x) \in \mathbb{F}_q[x]$ — характеристический многочлен однородного линейного рекуррентного соотношения, которому удовлетворяет наша последовательность, и пусть $h_0(x) \in \mathbb{F}_q[x]$ — многочлен вида (8.10), определяемый многочленом $f_0(x)$ и исходной последовательностью $s_0, s_1, \ldots$. Если $d(x)$ — нормированный многочлен, являющийся наибольшим общим делителем многочленов $f_0(x)$ и $h_0(x)$, то мы можем записать $f_0(x) = m(x)\,d(x)$, $h_0(x) = b(x)\,d(x)$, где $m(x), b(x) \in \mathbb{F}_q[x]$. Докажем, что $m(x)$ и есть искомый многочлен. Очевидно, что $m(x)$ — нормированный многочлен. Пусть теперь $f(x) \in \mathbb{F}_q[x]$ — произвольный характеристический многочлен данной последовательности, и пусть $h(x) \in \mathbb{F}_q[x]$ — многочлен вида (8.10), определяемый многочленом $f(x)$ и данной последовательностью. Применяя теорему 8.40, получаем, что для производящей функции $G(x)$ нашей последовательности имеет место равенство

$$G(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{g(x)}{f^*(x)},$$

где $g_0(x)$ и $g(x)$ — многочлены, задаваемые формулой (8.16). Следовательно, $g(x) f_0^*(x) = g_0(x) f^*(x)$ и, используя (8.18), приходим к равенству

$$h(x) f_0(x) = -x^{\deg(f(x))-1} g(1/x)\, x^{\deg(f_0(x))} f_0^*(1/x) = \\ = -x^{\deg(f_0(x))-1} g_0(1/x)\, x^{\deg(f(x))} f^*(1/x) = h_0(x) f(x).$$

После деления обеих частей равенства на $d(x)$ получаем $h(x) m(x) = b(x) f(x)$. Тогда в силу того, что $m(x)$ и $b(x)$ взаимно просты, $m(x)$ делит $f(x)$.

Предположим теперь, что $f(x) \in \mathbb{F}_q[x]$ — нормированный многочлен положительной степени, который делится на $m(x)$, т. е. $f(x) = m(x) c(x)$, $c(x) \in \mathbb{F}_q[x]$. Переходя к возвратным многочленам, получаем $f^*(x) = m^*(x) c^*(x)$. Кроме того, имеет место равенство $h_0(x) m(x) = b(x) f_0(x)$. Отсюда, используя соотношение (8.18), получаем

$$g_0(x) m^*(x) = -x^{\deg(f_0(x))-1} h_0(1/x)\, x^{\deg(m(x))} m(1/x) = \\ = -x^{\deg(m(x))-1} b(1/x)\, x^{\deg(f_0(x))} f_0(1/x).$$

Так как $\deg(b(x)) < \deg(m(x))$, произведение первых двух сомножителей (включая знак минус) в правой части приведенного выше равенства является многочленом $a(x) \in \mathbb{F}_q[x]$. Следовательно, справедливо равенство $g_0(x) m^*(x) = a(x) f_0^*(x)$. Тогда из теоремы 8.40 следует, что производящую функцию $G(x)$ нашей последовательности можно представить в виде

$$G(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{a(x)}{m^*(x)} = \frac{a(x) c^*(x)}{m^*(x) c^*(x)} = \frac{a(x) c^*(x)}{f^*(x)}.$$

Так как

$$\deg(a(x) c^*(x)) = \deg(a(x)) + \deg(c^*(x)) < \\ < \deg(m(x)) + \deg(c(x)) = \deg(f(x)),$$

то из второй части теоремы 8.40 следует, что $f(x)$ является характеристическим многочленом нашей последовательности. Очевидно, что существует только один многочлен $m(x)$ с указанными свойствами. □

Однозначно определенный в теореме 8.42 многочлен $m(x) \in \mathbb{F}_q[x]$, соответствующий последовательности $s_0, s_1, \ldots$, называется *минимальным многочленом* этой последовательности. Если $s_n = 0$ для всех $n \geqslant 0$, то минимальный многочлен этой последовательности равен 1. Для всех других однородных линейных рекуррентных последовательностей $m(x)$ является нормированным многочленом степени $\deg(m(x)) > 0$ и представляет собой характеристический многочлен линейного рекуррентного соотношения минимально возможного порядка, которому удовлетво-

ряет наша последовательность. Другой метод вычисления минимального многочлена будет приведен в § 6 настоящей главы.

8.43. Пример. Пусть последовательность $s_0, s_1, \ldots$ является линейной рекуррентной последовательностью над полем $\mathbb{F}_2$, определяемой рекуррентным соотношением

$$s_{n+4} = s_{n+3} + s_{n+1} + s_n, \quad n = 0, 1, \ldots,$$

и вектором начального состояния (1, 1, 0, 1). Для того чтобы найти минимальный многочлен этой последовательности, будем действовать так же, как при доказательстве теоремы 8.42. Можно взять

$$f_0(x) = x^4 - x^3 - x - 1 = x^4 + x^3 + x + 1 \in \mathbb{F}_2[x].$$

Тогда из (8.10) следует, что $h_0(x) = x^3 + x$. Наибольший общий делитель многочленов $f_0(x)$ и $h_0(x)$ равен $d(x) = x^2 + 1$, и, таким образом, минимальный многочлен последовательности $s_0, s_1, \ldots$ равняется $m(x) = f_0(x)/d(x) = x^2 + x + 1$. Легко проверить, что наша последовательность удовлетворяет линейному рекуррентному соотношению

$$s_{n+2} = s_{n+1} + s_n, \quad n = 0, 1, \ldots,$$

что находится в соответствии с общей теорией. Заметим, что $\operatorname{ord}(m(x))$ равен 3 и совпадает с минимальным периодом нашей последовательности (ср. с примером 8.41). В теореме 8.44 мы покажем, что это справедливо и в общем случае. □

Минимальный многочлеи играет ведущую роль при определении минимального периода линейной рекуррентной последовательности. Это видно, например, из следующего результата.

8.44. Теорема. *Пусть* $s_0, s_1, \ldots$ — *однородная линейная рекуррентная последовательность над полем* $\mathbb{F}_q$ *с минимальным многочленом* $m(x) \in \mathbb{F}_q[x]$. *Тогда минимальный период этой последовательности равняется* $\operatorname{ord}(m(x))$.

Доказательство. Если r — минимальный период последовательности $s_0, s_1, \ldots$, а n_0 — ее предпериод, то $s_{n+r} = s_n$ для всех $n \geqslant n_0$. Значит, наша последовательность удовлетворяет однородному рекуррентному соотношению

$$s_{n+n_0+r} = s_{n+n_0}, \quad n = 0, 1, \ldots .$$

Тогда по теореме 8.42 многочлен $m(x)$ делит многочлен $x^{n_0+r} - x^{n_0} = x^{n_0}(x^r - 1)$. Отсюда получаем, что $m(x)$ имеет вид $m(x) = x^h g(x)$, где $h \leqslant n_0$, а $g(x) \in \mathbb{F}_q[x]$, $g(0) \neq 0$ и $g(x)$ делит $x^r - 1$. Из определения порядка многочлена следует, что $\operatorname{ord}(m(x)) = \operatorname{ord}(g(x)) \leqslant r$. С другой стороны, по теореме 8.27 r делит $\operatorname{ord}(m(x))$, откуда и следует, что $r = \operatorname{ord}(m(x))$. □

8.45. Пример. Пусть $s_0, s_1, \ldots$ — линейная однородная последовательность над полем $\mathbb{F}_2$, удовлетворяющая рекуррентному соотношению $s_{n+5} = s_{n+1} + s_n$, $n = 0, 1, \ldots$, с вектором начального состояния (1, 1, 1, 0, 1). Следуя методу доказательства теоремы 8.42, возьмем $f_0(x) = x^5 - x - 1 = x^5 + x + 1 \in \mathbb{F}_2[x]$. Из (8.10) получаем, что $h_0(x) = x^4 + x^3 + x^2$. Тогда $d(x) = x^2 + x + 1$, и, таким образом, минимальный многочлен $m(x)$ нашей последовательности равен $f_0(x)/d(x) = x^3 + x^2 + 1$. Так как $\operatorname{ord}(m(x)) = 7$, то отсюда по теореме 8.44 получаем, что минимальный период нашей последовательности равен 7 (ср. с примером 8.18). □

Из приведенного только что примера видно, как можно находить минимальный период линейной рекуррентной последовательности, не вычисляя ее членов. Этот метод особенно эффективен, если в нашем распоряжении имеется таблица порядков многочленов. Так как такие таблицы обычно включают в себя лишь сведения о порядках неприводимых многочленов (см. § 2, гл. 10), для нахождения порядка данного многочлена необходимо воспользоваться теоремами 3.8 и 3.9 (ср. с примером 3.10).

8.46. Пример. Метод, использованный в примере 8.45, можно также применять и в случае неоднородной линейной рекуррентной последовательности. Пусть $s_0, s_1, \ldots$ — последовательность над полем $\mathbb{F}_2$, удовлетворяющая рекуррентному соотношению

$$s_{n+4} = s_{n+3} + s_{n+1} + s_n + 1, \quad n = 0, 1, \ldots,$$

с вектором начального состояния (1, 1, 0, 1). В соответствии с (8.5) эту же последовательность можно получить с помощью однородного линейного рекуррентного соотношения

$$s_{n+5} = s_{n+3} + s_{n+2} + s_n, \quad n = 0, 1, \ldots,$$

выбирая вектор начального состояния равным (1, 1, 0, 1, 0). Действуя так же, как в примере 8.45, находим соответствующий характеристический многочлен

$$f(x) = x^5 + x^3 + x^2 + 1 = (x + 1)^3 (x^2 + x + 1) \in \mathbb{F}_2[x],$$

который в данном случае совпадает с минимальным многочленом $m(x)$ нашей последовательности. Так как по теореме 3.8 $\operatorname{ord}((x + 1)^3) = 4$, а $\operatorname{ord}(x^2 + x + 1) = 3$, из теоремы 3.9 следует, что $\operatorname{ord}(m(x)) = 12$. Поэтому последовательность $s_0, s_1, \ldots$ является чисто периодической последовательностью с минимальным периодом, равным 12. □

8.47. Пример. Рассмотрим линейную рекуррентную последовательность $s_0, s_1, \ldots$ над полем $\mathbb{F}_2$, задаваемую рекуррентным соотношением

$$s_{n+4} = s_{n+2} + s_{n+1}, \quad n = 0, 1, \ldots,$$

с вектором начального состояния (1, 0, 1, 0). Тогда

$$f(x) = x^4 + x^2 + x = x(x^3 + x + 1) \in \mathbb{F}_2[x]$$

— характеристический многочлен нашей последовательности и в силу того, что ни x, ни $x^3 + x + 1$ не является характеристическим многочленом этой последовательности, получаем $m(x) = x^4 + x^2 + x$. Таким образом, последовательность $s_0, s_1, \ldots$ является периодической, но не чисто периодической, а ее минимальный период равняется $\operatorname{ord}(m(x)) = 7$.

8.48. Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$, а b—некоторое натуральное число. Тогда минимальный многочлен $m_1(x)$ сдвинутой последовательности $s_b, s_{b+1}, \ldots$ делит минимальный многочлен $m(x)$ исходной последовательности $s_0, s_1, \ldots$. Если $s_0, s_1, \ldots$ — чисто периодическая последовательность, то $m_1(x) = m(x)$.*

Доказательство. Для того чтобы доказать первое утверждение, в силу теоремы 8.42 достаточно показать, что любое однородное линейное рекуррентное соотношение, которому удовлетворяет исходная последовательность $s_0, s_1, \ldots$, также справедливо и для сдвинутой последовательности. Последнее очевидно. Для доказательства второго утверждения рассмотрим однородное линейное рекуррентное соотношение

$$s_{n+b+k} = a_{k-1}s_{n+b+k-1} + \cdots + a_0 s_{n+b}, \quad n = 0, 1, \ldots,$$

которому удовлетворяет сдвинутая последовательность. Пусть r — период последовательности $s_0, s_1, \ldots$, так что $s_{n+r} = s_n$ для всех $n \geqslant 0$. Выберем целое число c, для которого $cr \geqslant b$. Тогда, используя линейное рекуррентное соотношение, в котором n заменено на $n + cr - b$, и учитывая свойство периодичности, получаем, что

$$s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n, \quad n \geqslant 0.$$

Последнее означает, что последовательность $s_0, s_1, \ldots$ удовлетворяет тому же линейному рекуррентному соотношению, что и сдвинутая последовательность. Применяя вновь теорему 8.42, получаем, что $m_1(x) = m(x)$. □

8.49. Пример. Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность над полем $\mathbb{F}_2$, рассмотренная в примере 8.47. Ее минимальный многочлен равен $x^4 + x^2 + x$, в то время как минимальный многочлен сдвинутой последовательности $s_1, s_2, \ldots$ равняется $x^3 + x + 1$ и является делителем многочлена $x^4 + x^2 + x$. Этот пример показывает, что второе утверждение теоремы 8.48 может не выполняться в случае, если $s_0, s_1, \ldots$ не является чисто периодической последовательностью. □

8.50. Теорема. *Пусть $f(x) \in \mathbb{F}_q[x]$ — нормированный неприводимый многочлен над полем $\mathbb{F}_q$, и пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$, не являющаяся нулевой последовательностью. Если $f(x)$ — характеристический многочлен последовательности $s_0, s_1, \ldots$, то он равняется ее минимальному многочлену $m(x)$.*

Доказательство. Так как по теореме 8.42 минимальный многочлен $m(x)$ нашей последовательности должен делить многочлен $f(x)$, то в силу неприводимости $f(x)$ получаем, что либо $m(x) = 1$, либо $m(x) = f(x)$. Однако $m(x) = 1$ только для нулевой последовательности. Отсюда вытекает утверждение теоремы. □

Существует общий критерий для определения того, является ли характеристический многочлен линейного рекуррентного соотношения, определяющего данную линейную рекуррентную последовательность, одновременно и минимальным многочленом этой последовательности.

8.51. Теорема. *Пусть $s_0, s_1, \ldots$ — последовательность элементов поля $\mathbb{F}_q$, удовлетворяющая линейному рекуррентному соотношению k-го порядка с характеристическим многочленом $f(x) \in \mathbb{F}_q[x]$. Тогда $f(x)$ совпадает с минимальным многочленом этой последовательности в том и только том случае, когда векторы состояний $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}$ линейно независимы над полем $\mathbb{F}_q$.*

Доказательство. Предположим, что $f(x)$ является минимальным многочленом нашей последовательности. Если векторы $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}$ линейно зависимы над полем $\mathbb{F}_q$, то найдутся элементы $b_0, b_1, \ldots, b_{k-1} \in \mathbb{F}_q$, не все равные 0, такие, что $b_0\mathbf{s}_0 + b_1\mathbf{s}_1 + \ldots + b_{k-1}\mathbf{s}_{k-1} = \mathbf{0}$. Рассмотрим матрицу A из (8.3), соответствующую данному линейному рекуррентному соотношению. Умножая все члены приведенного выше равенства на степени матрицы A, из равенства (8.4) получаем

$$b_0\mathbf{s}_n + b_1\mathbf{s}_{n+1} + \cdots + b_{k-1}\mathbf{s}_{n+k-1} = \mathbf{0}, \quad n = 0, 1, \ldots .$$

В частности,

$$b_0 s_n + b_1 s_{n+1} + \cdots + b_{k-1} s_{n+k-1} = 0 \quad \text{для всех} \quad n = 0, 1, \ldots .$$

Если $b_j = 0$ для всех $1 \leqslant j \leqslant k-1$, то $s_n = 0$ для всех $n \geqslant 0$, что противоречит тому, что минимальный многочлен $f(x)$ рассматриваемой последовательности не является постоянным (т. е. имеет положительную степень). Тогда пусть $j \geqslant 1$ — наибольший индекс, для которого $b_j \neq 0$. Отсюда вытекает, что последовательность $s_0, s_1, \ldots$ удовлетворяет однородному линейному рекуррентному соотношению j-го порядка, где $j < k$. Это противоречит предположению, что $f(x)$ является минимальным многочленом. Таким образом, мы показали, что векторы $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}$ линейно независимы над полем $\mathbb{F}_q$.

Обратно, предположим, что $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}$ линейно независимы над $\mathbb{F}_q$. Так как $\mathbf{s}_0 \neq \mathbf{0}$, минимальный многочлен нашей последовательности имеет положительную степень. Если $f(x)$ не является минимальным многочленом, последовательность $s_0, s_1, \ldots$ должна удовлетворять однородному линейному рекуррентному соотношению m-го порядка с коэффициентами из $\mathbb{F}_q$ для некоторого $1 \leqslant m < k$. Пусть это соотношение имеет вид

$$s_{n+m} = a_{m-1}s_{n+m-1} + \cdots + a_0 s_n, \quad n = 0, 1, \ldots .$$

Однако отсюда следует равенство $\mathbf{s}_m = a_{m-1}\mathbf{s}_{m-1} + \ldots + a_0\mathbf{s}_0$, что противоречит предположению о линейной независимости векторов $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}$. □

8.52. Следствие. *Если последовательность $s_0, s_1, \ldots$ — импульсная функция, соответствующая некоторому однородному линейному рекуррентному соотношению над полем $\mathbb{F}_q$, то минимальный многочлен этой последовательности равен характеристическому многочлену этого линейного рекуррентного соотношения.*

Доказательство. Поскольку импульсная функция обладает тем свойством, что первые k ее векторов состояний линейно независимы, то сформулированное утверждение следует из теоремы 8.51. □

§ 5. Семейства линейных рекуррентных последовательностей

Пусть $f(x) \in \mathbb{F}_q[x]$ — нормированный многочлен положительной степени. Через $S(f(x))$ обозначим множество всех однородных линейных рекуррентных последовательностей над полем $\mathbb{F}_q$ с характеристическим многочленом $f(x)$. Другими словами, $S(f(x))$ состоит из всех последовательностей над полем $\mathbb{F}_q$, которые удовлетворяют однородному линейному рекуррентному соотношению, определяемому многочленом $f(x)$. Если $\deg(f(x)) = k$, то $S(f(x))$ содержит ровно q^k последовательностей, соответствующих выбору q^k различных значений вектора начального состояния.

Множество $S(f(x))$ можно рассматривать как векторное пространство над $\mathbb{F}_q$, если определить соответствующим образом операции над последовательностями элементов из поля $\mathbb{F}_q$. Так, если через σ обозначена последовательность $s_0, s_1, \ldots$, а через τ — последовательность $t_0, t_1, \ldots$, состоящие из элементов поля $\mathbb{F}_q$, то определим их сумму $\sigma + \tau$ как последовательность $s_0 + t_0, s_1 + t_1, \ldots$. Далее, если $c \in \mathbb{F}_q$, то произведение $c\sigma$ определяется как последовательность вида $cs_0, cs_1, \ldots$. Из рекуррентного соотношения непосредственно следует, что множество $S(f(x))$ замкнуто относительно операций сложения и умножения на константу. Нетрудно проверить выполнение аксиом векторного про-

странства. Таким образом, $S(f(x))$ действительно представляет собой векторное пространство над полем $\mathbb{F}_q$. Роль нулевого вектора играет *нулевая последовательность* — последовательность, все члены которой равняются нулевому элементу поля $\mathbb{F}_q$. Так как $S(f(x))$ содержит q^k элементов, размерность полученного векторного пространства равняется k. Выберем k линейно независимых наборов длины k из элементов поля $\mathbb{F}_q$. Если обозначить эти k-наборы через $\mathbf{y}_1, \ldots, \mathbf{y}_k$, то k линейно независимых элементов пространства $S(f(x))$ можно получить, рассматривая последовательности $\sigma_1, \ldots, \sigma_k$ из $S(f(x))$, такие, что вектор $\mathbf{y}_j$, $1 \leqslant j \leqslant k$, является вектором начального состояния последовательности σ_j. Наиболее естественным является выбор в качестве $\mathbf{y}_1, \ldots, \mathbf{y}_k$ стандартного базиса векторов

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \quad \mathbf{e}_2 = (0, 1, \ldots, 0), \ldots, \mathbf{e}_k = (0, \ldots, 0, 1).$$

Другой базис пространства $S(f(x))$, который часто бывает полезным, получается при рассмотрении импульсной функции d_0, d_1, ... из $S(f(x))$, если в качестве $\mathbf{y}_1, \ldots, \mathbf{y}_k$ выбрать первые k ее векторов состояний $\mathbf{d}_0, \mathbf{d}_1, \ldots, \mathbf{d}_{k-1}$.

Теперь рассмотрим соотношения между различными множествами $S(f(x))$.

8.53. Теорема. *Пусть $f(x)$ и $g(x)$ — два нормированных многочлена над полем $\mathbb{F}_q$, не являющиеся постоянными многочленами. Тогда $S(f(x))$ является подмножеством множества $S(g(x))$ в том и только том случае, если $f(x)$ делит $g(x)$.*

Доказательство. Предположим, что $S(f(x)) \subseteq S(g(x))$. Рассмотрим импульсную функцию, принадлежащую $S(f(x))$. В силу следствия 8.52 ее минимальный многочлен равен $f(x)$. По предположению она лежит также и в множестве $S(g(x))$. Следовательно, по теореме 8.42 ее минимальный многочлен $f(x)$ делит $g(x)$. Обратно, если $f(x)$ делит $g(x)$, а $s_0, s_1, \ldots$ — произвольная последовательность из $S(f(x))$, то по теореме 8.42 минимальный многочлен этой последовательности $m(x)$ делит $f(x)$. Следовательно, $m(x)$ делит и $g(x)$, и, применяя вновь теорему 8.42, получаем, что последовательность $s_0, s_1, \ldots$ принадлежит $S(g(x))$. Таким образом, $S(f(x))$ является подмножеством множества $S(g(x))$. □

8.54. Теорема. *Пусть $f_1(x), \ldots, f_h(x)$ — нормированные многочлены над полем $\mathbb{F}_q$, ни один из которых не является постоянным многочленом. Если $f_1(x), \ldots, f_h(x)$ взаимно просты, то пересечение*

$$S(f_1(x)) \cap \ldots \cap S(f_h(x))$$

содержит лишь нулевую последовательность. Если $d(x)$ — нормированный многочлен, $\deg(d(x)) > 0$, являющийся наибольшим общим делителем многочленов $f_1(x), \ldots, f_h(x)$, то

$$S(f_1(x)) \cap \ldots \cap S(f_h(x)) = S(d(x)).$$

Доказательство. Минимальный многочлен $m(x)$ любой последовательности, лежащей в рассматриваемом пересечении, должен делить $f_1(x), \ldots, f_h(x)$. Если эти многочлены взаимно просты, то $m(x) = 1$, а только нулевая последовательность имеет минимальный многочлен, равный 1. Во втором случае мы заключаем, что $m(x)$ делит $d(x)$, а тогда по теореме 8.42 $S(f_1(x)) \cap \ldots \ldots \cap S(f_h(x)) \subseteq S(d(x))$. В свою очередь, обратное включение $S(d(x)) \subseteq S(f_1(x)) \cap \ldots \cap S(f_h(x))$ следует из теоремы 8.53. □

Обозначим через $S(f(x)) + S(g(x))$ множество всех последовательностей вида $\sigma + \tau$, где $\sigma \in S(f(x))$, $\tau \in S(g(x))$. Это определение, разумеется, можно распространить на любое конечное число слагаемых.

8.55. Теорема. *Пусть $f_1(x), \ldots, f_h(x)$ — нормированные многочлены над полем $\mathbb{F}_q$, не являющиеся постоянными. Тогда*

$$S(f_1(x)) + \ldots + S(f_h(x)) = S(c(x)),$$

где $c(x)$ — нормированный многочлен, являющийся наименьшим общим кратным многочленов $f_1(x), \ldots, f_h(x)$.

Доказательство. Достаточно рассмотреть случай $h = 2$, так как общий случай легко получить по индукции. Прежде всего, заметим, что по теореме 8.53 последовательность из $S(f_1(x))$ или из $S(f_2(x))$ обязательно принадлежит и $S(c(x))$. Отсюда следует, что $S(f_1(x)) + S(f_2(x)) \subseteq S(c(x))$. Сравним теперь размерности этих множеств как векторных пространств над полем $\mathbb{F}_q$. Полагая $V_1 = S(f_1(x))$, $V_2 = S(f_2(x))$, обозначая через $d(x)$ нормированный многочлен, являющийся наибольшим общим делителем $f_1(x)$, $f_2(x)$, и применяя теорему 8.54, получаем

$$\dim(V_1 + V_2) = \dim(V_1) + \dim(V_2) - \dim(V_1 \cap V_2) = \\ = \deg(f_1(x)) + \deg(f_2(x)) - \deg(d(x)).$$

Но $c(x) = f_1(x) f_2(x)/d(x)$, откуда

$$\dim(V_1 + V_2) = \deg(c(x)) = \dim(S(c(x))).$$

Таким образом, линейное подпространство $S(f_1(x)) + S(f_2(x)) \subseteq S(c(x))$ имеет ту же размерность, что и линейное пространство $S(c(x))$, откуда следует равенство $S(f_1(x)) + S(f_2(x)) = S(c(x))$. □

В частном случае, когда многочлены $f(x)$ и $g(x)$ являются взаимно простыми нормированными многочленами над полем $\mathbb{F}_q$, не являющимися константами, имеет место соотношение

$$S(f(x)\, g(x)) = S(f(x)) + S(g(x)).$$

Так как в этом случае из теоремы 8.54 следует, что $S(f(x)) \cap S(g(x))$ содержит только нулевую последовательность, то,

говоря языком линейной алгебры, пространство $S(f(x)\,g(x))$ является прямой суммой своих подпространств $S(f(x))$ и $S(g(x))$. Другими словами, любую последовательность $\sigma \in S(f(x)\,g(x))$ можно единственным образом представить в виде $\sigma = \sigma_1 + \sigma_2$, где $\sigma_1 \in S(f(x))$, а $\sigma_2 \in S(g(x))$.

Вспомним теперь, что $S(f(x))$ является векторным пространством над полем $\mathbb{F}_q$ и что размерность этого векторного пространства равняется степени многочлена $f(x)$. Это векторное пространство обладает еще одним интересным свойством: если последовательность $s_0, s_1, \ldots$ лежит в множестве $S(f(x))$, то для любого целого числа $b \geqslant 0$ сдвинутая последовательность $s_b, s_{b+1}, \ldots$ также лежит в $S(f(x))$. Это свойство немедленно вытекает из соответствующего линейного рекуррентного соотношения. Мы сформулируем это свойство в виде утверждения о том, что множество $S(f(x))$ *замкнуто относительно сдвига входящих в него последовательностей*. В совокупности перечисленные свойства полностью характеризуют множества $S(f(x))$.

8.56. Теорема. *Пусть E — некоторое множество последовательностей над полем $\mathbb{F}_q$. Тогда $E = S(f(x))$ для некоторого нормированного многочлена $f(x) \in \mathbb{F}_q[x]$, $\deg(f(x)) > 0$, в том и только том случае, если множество E является конечномерным векторным пространством над полем $\mathbb{F}_q$ (относительно стандартных операций сложения последовательностей и умножения их на константу), которое замкнуто относительно операции сдвига последовательностей.*

Доказательство. Как мы уже отмечали, условия этой теоремы являются необходимыми. Чтобы доказать их достаточность, рассмотрим произвольную ненулевую последовательность $\sigma \in E$. Если σ обозначает последовательность $s_0, s_1, \ldots$, а $b \geqslant 0$ — произвольное целое число, то через $\sigma^{(b)}$ обозначим сдвинутую последовательность $s_b, s_{b+1}, \ldots$. По предположению все последовательности $\sigma^{(0)}, \sigma^{(1)}, \sigma^{(2)}, \ldots$ лежат в E. Но E — конечное множество, откуда следует, что существуют неотрицательные целые числа $i < j$, такие, что $\sigma^{(i)} = \sigma^{(j)}$. Отсюда вытекает, что исходная последовательность σ удовлетворяет однородному линейному рекуррентному соотношению $s_{n+j} = s_{n+i}$, $n = 0, 1, \ldots$. По теореме 8.42 последовательность σ имеет минимальный многочлен $m_\sigma(x) \in \mathbb{F}_q[x]$, и пусть $k = \deg(m_\sigma(x))$. Тогда в силу теоремы 8.51 векторы состояний $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}$ последовательности σ являются линейно независимыми над полем $\mathbb{F}_q$. Значит, последовательности $\sigma^{(0)}, \sigma^{(1)}, \ldots, \sigma^{(k-1)}$ являются линейно независимыми элементами пространства $S(m_\sigma(x))$ и, следовательно, образуют базис пространства $S(m_\sigma(x))$. Так как $\sigma^{(0)}, \sigma^{(1)}, \ldots, \sigma^{(k-1)}$ принадлежат также и векторному пространству E, то $S(m_\sigma(x))$ является линейным подпространством пространства E.

Обозначим через E^* множество последовательностей, полученное из E путем отбрасывания нулевой последовательности. Проводя приведенные выше рассуждения для всех $\sigma \in E^*$, приходим к тому, что конечная сумма векторных пространств $\sum_{\sigma \in E^*} S(m_\sigma(x))$ является линейным подпространством пространства E. С другой стороны, очевидно, что $E \subseteq \sum_{\sigma \in E^*} S(m_\sigma(x))$ и, значит, $E = \sum_{\sigma \in E^*} S(m_\sigma(x))$. Применяя теорему 8.55, получаем

$$E = \sum_{\sigma \in E^*} S(m_\sigma(x)) = S(f(x)),$$

где $f(x)$ — наименьшее общее кратное многочленов $m_\sigma(x)$, а σ пробегает конечное множество E^*. □

Из теоремы 8.55 следует, что сумма двух и более однородных линейных рекуррентных последовательностей над полем $\mathbb{F}_q$ является однородной линейной рекуррентной последовательностью. Характеристический многочлен суммарной последовательности тоже легко получается из этой теоремы. В важных частных случаях минимальный многочлен и минимальный период суммарной последовательности можно непосредственно получить из соответствующих характеристик суммируемых последовательностей.

8.57. Теорема. *Пусть* σ_i, $i = 1, 2, \ldots, h$, *— однородные линейные рекуррентные последовательности над полем* $\mathbb{F}_q$, *а* $m_i(x) \in \mathbb{F}_q[x]$ *— соответствующие минимальные многочлены. Если многочлены* $m_1(x), \ldots, m_h(x)$ *попарно взаимно просты, то минимальный многочлен суммы* $\sigma_1 + \ldots + \sigma_h$ *равен произведению* $m_1(x) \ldots m_h(x)$.

Доказательство. Для доказательства достаточно рассмотреть случай $h = 2$, так как доказательство в общем случае легко получить по индукции. Если один из многочленов $m_1(x)$ или $m_2(x)$ является постоянным многочленом, равным 1, то результат тривиален. Аналогично, если минимальный многочлен $m(x) \in \mathbb{F}_q[x]$, соответствующий сумме $\sigma_1 + \sigma_2$, является постоянным многочленом, равным 1, то результат получается непосредственно. Предположим, что все многочлены $m_1(x)$, $m_2(x)$, $m(x)$ являются многочленами положительной степени. Так как в силу теоремы 8.55

$$\sigma_1 + \sigma_2 \in S(m_1(x)) + S(m_2(x)) = S(m_1(x)\, m_2(x)),$$

то $m(x)$ делит $m_1(x)\, m_2(x)$. Пусть σ_1 — последовательность $s_0, s_1, \ldots$, а σ_2 — последовательность $t_0, t_1, \ldots$, и пусть

$$m(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0.$$

Тогда

$$s_{n+k} + t_{n+k} = a_{k-1}(s_{n+k-1} + t_{n+k-1}) + \cdots + a_0(s_n + t_n),$$
$$n = 0, 1, \ldots$$

Если мы положим

$$u_n = s_{n+k} - a_{k-1}s_{n+k-1} - \cdots - a_0 s_n =$$
$$= -t_{n+k} + a_{k-1}t_{n+k-1} + \cdots + a_0 t_n, \quad n = 0, 1, \ldots,$$

и вспомним, что $S(m_1(x))$ и $S(m_2(x))$ являются векторными пространствами над полем $\mathbb{F}_q$, замкнутыми относительно операции сдвига входящих в них последовательностей (см. теорему 8.56), то мы убедимся, что последовательность $u_0, u_1, \ldots$ лежит как в $S(m_1(x))$, так и в $S(m_2(x))$. По теореме 8.54 она является нулевой последовательностью. Отсюда следует, что $m_1(x)$ делит $m(x)$ и $m_2(x)$ делит $m(x)$, а значит, и $m_1(x)\,m_2(x)$ делит $m(x)$. Таким образом, $m(x) = m_1(x)\,m_2(x)$. □

Если минимальные многочлены $m_1(x), \ldots, m_h(x)$ последовательностей $\sigma_1, \ldots, \sigma_h$ соответственно не являются попарно взаимно простыми, то для определения минимального многочлена суммарной последовательности $\sigma = \sigma_1 + \ldots + \sigma_h$ необходимо учитывать свойства исходных последовательностей $\sigma_1, \ldots, \sigma_h$. Наиболее удобен подход, основанный на использовании производящих функций. Предположим, что $G_i(x) \in \mathbb{F}_q[[x]]$, $i = 1, \ldots, h$, — производящие функции последовательностей σ_i. Тогда для производящей функции $G(x)$ суммарной последовательности σ справедливо равенство $G(x) = G_1(x) + \ldots + G_h(x)$. По теореме 8.40 каждая производящая функция $G_i(x)$ может быть представлена в виде дроби, знаменатель которой является многочленом, возвратным к многочлену $m_i(x)$. Сложим эти дроби, приведя их предварительно к общему знаменателю, а затем, используя вторую часть теоремы 8.40 и метод доказательства теоремы 8.42, найдем минимальный многочлен последовательности σ. Применяя указанный подход, можно также получить другое доказательство теоремы 8.57.

8.58. Пример. Пусть σ_1 — последовательность над полем $\mathbb{F}_2$, являющаяся импульсной функцией и принадлежащая множеству $S(x^4 + x^3 + x + 1)$, а σ_2 — последовательность над $\mathbb{F}_2$, являющаяся импульсной функцией и принадлежащая $S(x^5 + x^4 + 1)$. Тогда по следствию 8.52 соответствующие минимальные многочлены равны

$$m_1(x) = x^4 + x^3 + x + 1 = (x^2 + x + 1)(x + 1)^2 \in \mathbb{F}_2[x],$$

$$m_2(x) = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1) \in \mathbb{F}_2[x].$$

По теореме 8.40 производящая функция $G(x)$ суммарной последовательности $\sigma = \sigma_1 + \sigma_2$ равняется

$$G(x) = \frac{x^3}{(x^2+x+1)(x+1)^2} + \frac{x^4}{(x^2+x+1)(x^3+x^2+1)} = \frac{x^3}{(x^3+x^2+1)(x+1)^2}.$$

В силу второй части теоремы 8.40 возвратный к знаменателю многочлен $f_0(x) = (x^3+x+1)(x+1)^2$, является характеристическим многочленом для σ. Из (8.18) следует, что соответствующий многочлен $h_0(x)$ задается формулой $h_0(x) = -x^4(1/x)^3 = -x$. Так как $f_0(x)$ и $h_0(x)$ взаимно просты, то, используя метод доказательства теоремы 8.42, можно получить минимальный многочлен $m(x)$ последовательности σ:

$$m(x) = (x^3+x+1)(x+1)^2.$$

Заметим, что $m(x)$ является собственным делителем наибольшего общего кратного многочленов $m_1(x)$ и $m_2(x)$, которое равняется

$$(x^2+x+1)(x+1)^2(x^3+x+1). \quad \square$$

Из информации о минимальных многочленах, которую дает теорема 8.57, можно непосредственно получить полезный результат о минимальном периоде суммарной последовательности.

8.59. Теорема. *Пусть каждая из последовательностей* σ_i, $i = 1, \ldots, h$, *является однородной линейной рекуррентной последовательностью над полем* $\mathbb{F}_q$ *с минимальным периодом* r_i *и минимальным многочленом* $m_i(x) \in \mathbb{F}_q[x]$. *Если многочлены* $m_1(x), \ldots, m_h(x)$ *попарно взаимно просты, то минимальный период суммарной последовательности* $\sigma = \sigma_1 + \ldots + \sigma_h$ *равняется* НОК $(r_1, \ldots, r_h)$.

Доказательство. Рассмотрим случай $h = 2$, так как общий случай легко получить по индукции. Тогда если r — минимальный период последовательности $\sigma = \sigma_1 + \sigma_2$, то по теоремам 8.44 и 8.57 $r = \operatorname{ord}(m_1(x)\, m_2(x))$. Применяя теорему 3.9, получаем, что r является наименьшим общим кратным $\operatorname{ord}(m_1(x))$ и $\operatorname{ord}(m_2(x))$, т. е. чисел r_1 и r_2. $\square$

8.60. Пример. Рассмотрим последовательности σ_1 и σ_2 из примера 8.58. Минимальные периоды последовательностей σ_1 и σ_2 равняются соответственно $r_1 = \operatorname{ord}(m_1(x)) = 6$ и $r_2 = \operatorname{ord}(m_2(x)) = 21$. Минимальный период последовательности $\sigma = \sigma_1 + \sigma_2$ равняется $r = \operatorname{ord}(m(x)) = 14$. При вычислении порядков многочленов мы, разумеется, должны воспользоваться теоремой 3.9. Таким образом, периоды последовательностей получены без вычисления их членов. В нашем случае можно, конечно, проверить полученные результаты с помощью непосредственного

вычисления периода. Для этого вычислим члены соответствующих последовательностей:

σ_1: 0,0,0,1,1,1,0,0,0,0,1,1,1,0,0,0,1,1,1,0,0,0,1,1, ... $r_1 = 6$
σ_2: 0,0,0,0,1,1,1,1,1,0,1,0,1,0,0,1,1,0,0,0,1,0,0, ... $r_2 = 21$
$\sigma_1 + \sigma_2$: 0,0,0,1,0,0,1,1,1,1,0,1,1,0,0,0,0,1,0,0,1,1,1, ... $r = 14$

Заметим, что r является собственным делителем НОК (r_1, r_2). □

8.61. Теорема. *Пусть* σ_i, $i = 1, 2, \ldots, h$, — *периодические последовательности над полем* $\mathbb{F}_q$, *а* r_i — *минимальные периоды этих последовательностей. Если числа* $r_1, \ldots, r_h$ *попарно взаимно просты, то минимальный период суммарной последовательности* $\sigma_1 + \ldots + \sigma_h$ *равен произведению* $r_1 \ldots r_h$.

Доказательство. Как и раньше, ограничимся рассмотрением случая $h = 2$. Очевидно, что $r_1 r_2$ является периодом суммарной последовательности $\sigma = \sigma_1 + \sigma_2$. Таким образом, минимальный период последовательности σ, равный r, должен делить произведение $r_1 r_2$. Следовательно, r можно представить в виде $r = d_1 d_2$, где d_1 и d_2 — положительные делители чисел r_1 и r_2 соответственно. В частности, $d_1 r_2$ является периодом последовательности σ. Если σ_1 обозначает последовательность $s_0, s_1, \ldots$, а σ_2 — последовательность $t_0, t_1, \ldots$, то

$$s_{n+d_1 r_2} + t_{n+d_1 r_2} = s_n + t_n$$

для всех достаточно больших n. Но $t_{n+d_1 r_2} = t_n$ для всех достаточно больших n, отсюда получаем, что $s_{n+d_1 r_2} = s_n$ для всех достаточно больших n. Следовательно, r_1 делит $d_1 r_2$, а так как r_1 и r_2 взаимно просты, то r_1 делит d_1, и, значит, $d_1 = r_1$. Аналогично доказывается и равенство $d_2 = r_2$. □

В случае конечного поля $\mathbb{F}_2$ можно ввести интересную операцию над последовательностями элементов этого поля, называемую операцией *бинарного дополнения*. Так, если σ — последовательность над полем $\mathbb{F}_2$, то ее бинарное дополнение, обозначаемое через $\bar{\sigma}$, получается из σ заменой каждого элемента, равного 0, на 1, а каждого элемента, равного 1, — на 0. Бинарное дополнение можно рассматривать как частный случай операции сложения последовательностей, так как последовательность $\bar{\sigma}$ можно получить, прибавляя к σ последовательность 1, 1, 1, ... Следовательно, если σ является однородной линейной рекуррентной последовательностью, то и $\bar{\sigma}$ является однородной линейной рекуррентной последовательностью. Очевидно, что минимальный период $\bar{\sigma}$ совпадает с минимальным периодом σ. Минимальный многочлен последовательности $\bar{\sigma}$ легко можно получить из минимального многочлена исходной последовательности σ.

8.62. Теорема. *Пусть* σ — *однородная линейная рекуррентная последовательность над полем* $\mathbb{F}_2$, *а* $\bar{\sigma}$ — *ее бинарное дополнение.*

Представим минимальный многочлен $m(x) \in \mathbb{F}_2[x]$ *последовательности* σ *в виде* $m(x) = (x+1)^h m_1(x)$, *где* $h \geqslant 0$, $m_1(x) \in \mathbb{F}_2[x]$, $m_1(1) = 1$. *Тогда минимальный многочлен* $\bar{m}(x)$ *последовательности* $\bar{\sigma}$ *задается формулой*

$$\bar{m}(x) = \begin{cases} (x+1)\,m(x), & \text{если } h = 0; \\ m_1(x), & \text{если } h = 1; \\ m(x), & \text{если } h > 1. \end{cases}$$

Доказательство. Пусть ε — последовательность над полем $\mathbb{F}_2$, все члены которой равны 1. Так как $\bar{\sigma} = \sigma + \varepsilon$, а минимальный многочлен последовательности ε равен $x+1$, случай $h = 0$ следует из теоремы 8.57. Если $h \geqslant 1$, то из теоремы 8.55 вытекает, что $\bar{\sigma} = \sigma + \varepsilon \in S(m(x))$. Тогда $\bar{m}(x)$ делит $m(x)$. Если $\bar{m}(x)$ является постоянным многочленом, равным 1, то $\bar{\sigma}$ является нулевой последовательностью и $\sigma = \varepsilon$, а следовательно, теорема в этом случае справедлива. Предположим теперь, что $\deg(\bar{m}(x)) > 0$. Из теорем 8.53 и 8.55 следует, что $\sigma = \bar{\sigma} + \varepsilon \in S(\bar{m}(x) \cdot (x+1))$, и тогда $m(x)$ делит $\bar{m}(x)(x+1)$. Отсюда для $h \geqslant 1$ получаем, что либо $\bar{m}(x) = m(x)$, либо $\bar{m}(x) = (x+1)^{h-1} m_1(x)$. Если $h > 1$, то $\sigma = \bar{\sigma} + \varepsilon \in S(\bar{m}(x))$, откуда следует, что $\bar{m}(x) = m(x)$. Если же $h = 1$, то пусть σ — последовательность $s_0, s_1, \ldots$, а

$$m_1(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$$

является многочленом положительной степенн (случай многочлена нулевой степени тривиален). Положим

$$u_n = s_{n+k} + a_{k-1}s_{n+k-1} + \cdots + a_0 s_n, \quad n = 0, 1, \ldots .$$

Так как $m(x) = (x+1)\,m_1(x)$ — характеристический многочлен последовательности $s_0, s_1, \ldots$, то легко получить, что $u_{n+1} = u_n$ для всех $n \geqslant 0$. Следовательно, $u_n = u_0$ для всех $n \geqslant 0$, и тогда обязательно выполняется равенство $u_0 = 1$, так как иначе $m_1(x)$ был бы характеристическим многочленом последовательности σ. Таким образом,

$$s_{n+k} + 1 = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n \quad \text{для всех } n \geqslant 0.$$

Поскольку $m_1(1) = 1 + a_{k-1} + \ldots + a_0 = 1$, получаем

$$s_{n+k} + 1 = a_{k-1}(s_{n+k-1} + 1) + \cdots + a_0(s_n + 1) \quad \text{для всех } n \geqslant 0,$$

а это означает, что $m_1(x)$ является характеристическим многочленом последовательности $\bar{\sigma}$. Таким образом, в случае $h = 1$ имеет место равенство $\bar{m}(x) = m_1(x)$, что и завершает доказательство теоремы. □

Напомним, что $S(f(x))$ обозначает множество всех однородных линейных рекурреитных последовательностей над полем $\mathbb{F}_q$ с характеристическим многочленом $f(x)$, где $f(x) \in \mathbb{F}_q[x]$ —

нормированный многочлен положительной степени. Мы хотим, во-первых, найти те *целые положительные числа, которые могут встречаться в качестве минимальных периодов* у последовательностей из множества $S(f(x))$, а во-вторых, определить, *для скольких последовательностей* из $S(f(x))$ данное число может быть минимальным периодом.

Запишем многочлен $f(x)$ в виде $f(x) = x^h g(x)$, где $h \geqslant 0$ — целое число, $g(x) \in \mathbb{F}_q[x]$, $g(0) \neq 0$. Случай, когда $g(x)$ является константой, тривиален, так как тогда каждая последовательность из $S(f(x))$ имеет минимальный период 1. Если $h \geqslant 1$, а $g(x)$ является многочленом положительной степени, то, как это было показано в замечаниях, следующих за теоремой 8.55, каждая последовательность $\sigma \in S(f(x))$ может быть единственным образом представлена в виде $\sigma = \sigma_1 + \sigma_2$, где $\sigma_1 \in S(x^h)$, $\sigma_2 \in S(g(x))$. Все члены последовательности σ_1, кроме, может быть, конечного числа первых членов, равняются 0. Таким образом, минимальный период последовательности σ равняется минимальному периоду последовательности σ_2. Далее, из данной последовательности $\sigma_2 \in S(g(x))$ можно получить q^h различных последовательностей из $S(f(x))$, прибавляя к σ_2 любую из q^h последовательностей из $S(x^h)$. Следовательно, если $r_1, \ldots, r_t$ — минимальные периоды последовательностей из $S(g(x))$, а $N_1, \ldots, N_t$ — число последовательностей из $S(g(x))$, имеющих минимальные периоды, равные соответственно $r_1, \ldots, r_t$, то для каждого i, $1 \leqslant i \leqslant t$, существует ровно $q^h N_i$ последовательностей из множества $S(f(x))$, имеющих минимальный период r_i, и никаких других минимальных периодов у последовательностей из $S(f(x))$ быть не может.

Пусть теперь $h = 0$; тогда $f(0) \neq 0$. Предположим, сначала, что $f(x)$ — неприводимый многочлен над полем $\mathbb{F}_q$. В этом случае из теоремы 8.44 и 8.50 мы получаем, что каждая последовательность из $S(f(x))$ с ненулевым вектором начального состояния имеет минимальный период, равный $\operatorname{ord}(f(x))$. Значит, одна последовательность из $S(f(x))$ имеет минимальный период 1, а остальные $q^{\deg(f(x))} - 1$ последовательностей имеют минимальный период $\operatorname{ord}(f(x))$.

Далее, рассмотрим случай, когда $f(x)$ является степенью неприводимого многочлена. Тогда представим $f(x)$ в виде $f(x) = (g(x))^b$, где $g(x) \in \mathbb{F}_q[x]$ — нормированный неприводимый многочлен над полем $\mathbb{F}_q$, а $b \geqslant 2$ — целое число. Тогда минимальный многочлен любой последовательности из множества $S(f(x))$ с нулевым начальным вектором имеет вид $(g(x))^c$, где $1 \leqslant c \leqslant b$. По теореме 8.53

$$S(g(x)) \subseteq S((g(x))^2) \subseteq \ldots \subseteq S(f(x)).$$

Таким образом, если $\deg(g(x)) = k$, то имеется $q^k - 1$ последо-

вательностей из $S(f(x))$ с минимальным многочленом $g(x)$, $q^{2k} - q^k$ последовательностей из $S(f(x))$ с минимальным многочленом $(g(x))^2$ и т. д. В общем случае для любого $c = 1, 2, \ldots, b$ существует ровно $q^{ck} - q^{(c-1)k}$ последовательностей из множества $S(f(x))$, для которых минимальный многочлен равняется $(g(x))^c$. Объединяя полученные результаты с результатами теорем 3.8 и 8.44, получаем следующую теорему.

8.63. Теорема. *Пусть* $f(x) = (g(x))^b$, *где* $g(x) \in \mathbb{F}_q[x]$ — *нормированный неприводимый многочлен над полем* $\mathbb{F}_q$, $g(0) \neq 0$, $\deg(g(x)) = k$, $\operatorname{ord}(g(x)) = e$, b — *натуральное число. Пусть* t — *минимальное целое число, такое, что* $p^t \geqslant b$, *где* p — *характеристика поля* $\mathbb{F}_q$. *Тогда* $S(f(x))$ *содержит следующее число последовательностей со следующими минимальными периодами:* 1 *последовательность с минимальным периодом* 1, $q^k - 1$ *последовательностей с минимальным периодом* e, *а если* $b \geqslant 2$, *то* $q^{kp^j} - q^{kp^{j-1}}$ *последовательностей с минимальным периодом* ep^j, $j = 1, 2, \ldots, t-1$, *и* $q^{kb} - q^{kp^{t-1}}$ *последовательностей с минимальным периодом* ep^t.

В случае когда $f(x) \in \mathbb{F}_q[x]$ — произвольный нормированный многочлен положительной степени, $f(0) \neq 0$, то начнем с его канонического разложения

$$f(x) = \prod_{i=1}^{k} (g_i(x))^{b_i},$$

где $g_i(x)$ — различные нормированные неприводимые многочлены над полем $\mathbb{F}_q$, а b_i — целые положительные числа. Тогда из теоремы 8.55 следует, что

$$S(f(x)) = S\left((g_1(x))^{b_1}\right) + \cdots + S\left((g_h(x))^{b_h}\right).$$

В самом деле, для каждой последовательности σ из $S(f(x))$ существует единственное представление вида $\sigma = \sigma_1 + \ldots + \sigma_h$, где $\sigma_i \in S\left((g_i(x))^{b_i}\right)$, $1 \leqslant i \leqslant h$. Из теоремы 8.63 известно, какие минимальные периоды могут иметь последовательности из $S\left((g_i(x))^{b_i}\right)$. Аналогичные результаты для минимальных периодов последовательностей, лежащих в $S(f(x))$, можно получить, воспользовавшись теоремой 8.59.

8.64. Пример. Пусть

$$f(x) = (x^2 + x + 1)^2 (x^4 + x^3 + 1) \in \mathbb{F}_2[x].$$

По теореме 8.63 $S((x^2 + x + 1)^2)$ содержит последовательность с минимальным периодом 1, 3 последовательности с минимальным периодом 3 и 12 последовательностей с минимальным периодом 6. В то же время $S(x^4 + x^3 + 1)$ содержит последовательность с минимальным периодом 1 и 15 последовательностей с минимальным

периодом 15. Значит, образуя все возможные суммы из последовательностей, входящих в $S((x^2+x+1)^2)$ и $S(x^4+x^3+1)$, и пользуясь теоремой 8.59, получаем, что $S(f(x))$ содержит 1 последовательность с минимальным периодом 1, 3 последовательности с минимальным периодом 3, 12 последовательностей с минимальным периодом 6, 60 последовательностей с минимальным периодом 15 и 180 последовательностей с минимальным периодом 30. □

Мы только что исследовали поведение линейных рекуррентных последовательностей относительно операции почленного сложения. Аналогичную теорию можно развить и для операции почленного умножения, хотя сделать это гораздо труднее. Если σ — последовательность $s_0, s_1, \ldots$, а τ — последовательность $t_0, t_1, \ldots$ над полем $\mathbb{F}_q$, то определим их *произведение* $\sigma\tau$ как последовательность $s_0t_0, s_1t_1, \ldots$. Аналогичню определяется произведение любого конечного числа последовательностей. Пусть S — векторное пространство над полем $\mathbb{F}_q$, состоящее из всех последовательностей над полем $\mathbb{F}_q$ относительно обычных операций почленного сложения последовательностей и умножения последовательностей на константу. Пусть $f_1(x), \ldots, f_h(x)$ — нормированные многочлены над полем $\mathbb{F}_q$, не являющиеся постоянными, и пусть $S(f_1(x)) \ldots S(f_h(x))$ — подпространство пространства S, порожденное всеми произведениями вида $\sigma_1 \ldots \sigma_h$, $\sigma_i \in S(f_i(x))$, $i = 1, 2, \ldots, h$. Тогда имеется следующий фундаментальный результат.

8.65. Теорема. *Если $f_1(x), \ldots, f_h(x)$ — нормированные многочлены над полем $\mathbb{F}_q$, не являющиеся постоянными, то существует не являющийся постоянным нормированный многочлен $g(x) \in \mathbb{F}_q[x]$, такой, что*

$$S(f_1(x)) \ldots S(f_h(x)) = S(g(x)).$$

Доказательство. Положим $E = S(f_1(x)) \ldots S(f_h(x))$. Так как в каждом $S(f_i(x))$, $1 \leqslant i \leqslant h$, содержится последовательность с начальным членом 1, векторное пространство E содержит ненулевую последовательность. Далее, E порождено конечным числом последовательностей и, значит, является конечномерным пространством. Из того, что каждое множество $S(f_i(x))$, $i = 1, \ldots, h$, замкнуто относительно операции сдвига входящих в него последовательностей, получаем, что E обладает таким же свойством, и тогда утверждение доказываемой теоремы следует из теоремы 8.56. □

8.66. Следствие. *Произведение любого конечного числа линейных рекуррентных последовательностей над полем $\mathbb{F}_q$ само является линейной рекуррентной последовательностью над $\mathbb{F}_q$.*

Доказательство. Из замечания, приведенного после (8.5), следует, что данную рекуррентную последовательность всегда

можно рассматривать как однородную рекуррентную последовательность. Тогда искомый результат содержится в теореме 8.65. □

Явно определить многочлен $g(x)$, существование которого утверждается в теореме 8.65, в общем случае совсем не просто. Однако в ряде частных случаев это сделать легче.

Пусть $f_1(x), \ldots, f_h(x)$ — многочлены над полем $\mathbb{F}_q$, не являющиеся константами. Определим $f_1(x) \vee \ldots \vee f_h(x)$ как нормированный многочлен, корни которого являются различными элементами вида $\alpha_1 \ldots \alpha_h$, где α_i — корень многочлена $f_i(x)$ из поля разложения многочлена $f_1(x) \ldots f_h(x)$ над полем $\mathbb{F}_q$. Элемент, являющийся сопряженным (над $\mathbb{F}_q$) к произведению $\alpha_1 \ldots \alpha_h$, сам является элементом такого же вида; отсюда следует, что $f_1(x) \vee \ldots \vee f_h(x)$ является многочленом над полем $\mathbb{F}_h$.

8.67. Теорема. *Пусть* $f_i(x)$, $i = 1, 2, \ldots, h$, — *нормированные многочлены над полем* $\mathbb{F}_q$, *не являющиеся константами и не имеющие кратных корней. Тогда*

$$S(f_1(x)) \ldots S(f_h(x)) = S(f_1(x) \vee \ldots \vee f_h(x)).$$

Для доказательства этой теоремы нам потребуется одна вспомогательная лемма. Предварительно введем несколько новых понятий. Пусть F — конечное расширение поля $\mathbb{F}_q$, и пусть S_F — множество всех последовательностей над полем F. Тогда S_F является векторным пространством относительно операций почленного сложения последовательностей и их умножения на константу (из поля F). В частности, $S_{\mathbb{F}_q} = S$. Если дано h подпространств $V_1, \ldots, V_h$ векториого пространства S_F, то определим произведение $V_1 \ldots V_h$ как подпространство пространства S_F, порожденное всеми пронзведениями вида $\sigma_1 \ldots \sigma_h$, где $\sigma_i \in V_i$, $i = 1, \ldots, h$. Если $f(x) \in F[x]$ — нормированный многочлен, не являющийся константой, то через $S_F(f(x))$ будем обозначать векторное пространство над полем F, состоящее из всех однородных линейных рекуррентных последовательностей над полем F с характеристическим многочленом $f(x)$.

8.68. Лемма. *Пусть* F — *конечное расширение поля* $\mathbb{F}_q$, *и пусть* $f_1(x), \ldots, f_h(x)$ — *нормированные многочлены над полем* $\mathbb{F}_q$, *не являющиеся постоянными. Тогда*

$$S(f_1(x)) \ldots S(f_h(x)) = S \cap (S_F(f_1(x)) \ldots S_F(f_h(x))).$$

Доказательство. Очевидно, что

$$S(f_1(x)) \ldots S(f_h(x)) \subseteq S \cap (S_F(f_1(x)) \ldots S_F(f_h(x))).$$

Чтобы доказать обратное включение, заметим прежде всего, что для каждого $i = 1, \ldots, h$ пространство $S(f_i(x))$ порождает $S_F(f_i(x))$ над полем F, т. е. любая рекуррентная последователь-

ность из $S_F(f_i(x))$ может быть представлена в виде линейной комбинации рекуррентных последовательностей из множества $S(f_i(x))$ с коэффициентами из F. Тогда $S(f_1(x)) \dots S(f_h(x))$ порождает $S_F(f_1(x)) \dots S_F(f_h(x))$ над полем F. Пусть $\rho_1, \dots, \rho_m$ — базис пространства $S(f_1(x)) \dots S(f_h(x))$ над $\mathbb{F}_q$, и пусть $\omega_1, \dots, \omega_k$ — базис F над $\mathbb{F}_q$, причем $\omega_1 \in \mathbb{F}_q$. Тогда любой элемент $\sigma \in S_F(f_1(x)) \dots S_F(f_h(x))$ может быть записан в виде

$$\sigma = \sum_{i=1}^{k} \sum_{j=1}^{m} c_{ij}\omega_i\rho_j,$$

где $c_{ij} \in \mathbb{F}_q$. Пусть для каждого $j = 1, \dots, m$ последовательность ρ_j состоит из элементов $r_{j0}, r_{j1}, \dots, r_{jt} \in \mathbb{F}_q$, и пусть последовательность $\sigma \in S$ — это $s_0, s_1, \dots$. Тогда для членов s_n последовательности σ справедливо равенство

$$s_n = \sum_{i=1}^{k} \left(\sum_{j=1}^{m} c_{ij}r_{jn} \right) \omega_i \in \mathbb{F}_q, \quad n = 0, 1, \dots .$$

Так как коэффициенты при каждом ω_i лежат в $\mathbb{F}_q$, из определения $\omega_1, \dots, \omega_k$ следует, что $\sum_{j=1}^{m} c_{ij}r_{jn} = 0$ для всех n и $2 \leqslant i \leqslant k$. Значит,

$$\sigma = \sum_{j=1}^{m} c_{1j}\omega_1\rho_j \in S(f_1(x)) \dots S(f_h(x)),$$

что и завершает доказательство леммы. □

Доказательство теоремы 8.67. Пусть F — расширение поля $\mathbb{F}_q$, являющееся полем разложения многочлена $f_1(x) \dots f_h(x)$ над полем $\mathbb{F}_q$. Пусть для каждого $i = 1, 2, \dots, h$ элемент α_i пробегает корни многочлена $f_i(x)$. Тогда по теореме 8.55

$$S_F(f_i(x)) = \sum_{\alpha_i} S_F(x - \alpha_i), \quad 1 \leqslant i \leqslant h.$$

Заметим, что для подпространств V_1, V_2, V_3 векторного пространства S_F справедлив закон дистрибутивности:

$$V_1(V_2 + V_3) = V_1V_2 + V_1V_3.$$

В самом деле, по закону дистрибутивности для последовательностей $V_1(V_2 + V_3) \subseteq V_1V_2 + V_1V_3$. С другой стороны, очевидно, что $V_1V_2 \subseteq V_1(V_2 + V_3)$, $V_1V_3 \subseteq V_1(V_2 + V_3)$ и, следовательно, $V_1V_2 + V_1V_3 \subseteq V_1(V_2 + V_3)$. На основании закона дистрибутивности справедливо равенство

$$S_F(f_1(x)) \dots S_F(f_h(x)) = \sum_{\alpha_1, \dots, \alpha_h} S_F(x - \alpha_1) \dots S_F(x - \alpha_h).$$

Нетрудно проверить, что

$$S_F(x-\alpha_1)\ \dots\ S_F(x-\alpha_h)=S_F(x-\alpha_1\dots\alpha_h),$$

откуда по теореме 8.55

$$S_F(f_1(x))\dots S_F(f_h(x))=\sum_{\alpha_1,\dots,\alpha_h} S_F(x-\alpha_1\dots\alpha_h)=$$
$$=S_F(f_1(x)\vee\dots\vee f_h(x)).$$

Утверждение теоремы 8.67 следует теперь из леммы 8.68. □

Теорема 8.67 показывает, в частности, как находить характеристический многочлен для произведения однородных линейных рекуррентных последовательностей в случае, рассматриваемом в этой теореме. *Другой подход* может основываться на теореме 8.21. Для этого достаточно детально разобрать случай произведения двух однородных линейных рекуррентных последовательностей. Пусть последовательность $s_0, s_1, \dots$ лежит в $S(f(x))$, а последовательность $t_0, t_1, \dots$ лежит в $S(g(x))$. Если многочлен $f(x)$ имеет лишь простые корни $\alpha_1, \dots, \alpha_k$, а многочлен $g(x)$ имеет лишь простые корни $\beta_1, \dots, \beta_m$, то по формуле (8.8)

$$s_n=\sum_{i=1}^{k} b_i\alpha_i^n,\quad t_n=\sum_{j=1}^{m} c_j\beta_j^n,\quad n=0,\ 1,\ \dots,$$

где коэффициенты b_i и c_j лежат в конечном расширении поля $\mathbb{F}_q$. Если $\gamma_1, \dots, \gamma_r$ — различные значения, которые могут принимать произведения вида $\alpha_i\beta_j$, $1\leqslant i\leqslant k$, $1\leqslant j\leqslant m$, то

$$u_n=s_nt_n=\sum_{i=1}^{k}\sum_{j=1}^{m} b_ic_j(\alpha_i\beta_j)^n=\sum_{i=1}^{r} d_i\gamma_i^n,\quad n=0,\ 1,\ \dots,$$

где $d_1, \dots, d_r$ — некоторые коэффициенты из конечного расширения поля $\mathbb{F}_q$. Пусть теперь

$$h(x)=f(x)\vee g(x)=x^r-a_{r-1}x^{r-1}-\dots-a_0\in\mathbb{F}_q[x].$$

Тогда для $n=0,\ 1,\ \dots$ получаем

$$u_{n+r}-a_{r-1}u_{n+r-1}-\dots-a_0u_n=\sum_{i=1}^{r} d_i\gamma_i^n h(\gamma_i)=0,$$

и, таким образом, многочлен $h(x)$ будет характеристическим многочленом последовательности $u_0, u_1, \dots$, являющейся произведением последовательностей $s_0, s_1, \dots$ и $t_0, t_1, \dots$.

8.69. Пример. Рассмотрим последовательность 0, 1, 0, 1 ... над полем $\mathbb{F}_2$ с минимальным периодом 2 и минимальным многочленом $(x-1)^2$. Если мы умножим эту последовательность на саму себя, то получим ту же самую последовательность. С другой стороны, $(x-1)^2\vee(x-1)^2=x-1$, что не является характе-

ристическим многочленом последовательности, полученной в результате перемножения. Таким образом, равенство, доказанное в теореме 8.67, может не выполняться, если некоторые из многочленов $f_i(x)$ имеют кратные корни. □

Для операции умножения последовательностей можно получить аналог теоремы 8.61. По понятным причинам мы не будем рассматривать последовательностей, в которых все члены, кроме конечного числа, равны 0.

8.70. Теорема. *Пусть* σ_i, $i = 1, 2, \ldots, h$, — *периодические последовательности над полем* $\mathbb{F}_q$ *с бесконечным числом ненулевых членов. Пусть минимальный период последовательности* σ_i *равен* r_i. *Если числа* $r_1, \ldots, r_h$ *попарно взаимно просты, то минимальный период произведения* $\sigma_1 \ldots \sigma_h$ *равняется* $r_1 \ldots r_h$.

Доказательство. Ограничимся рассмотрением случая $h = 2$, так как общий случай легко получается индукцией по h. Как и в доказательстве теоремы 8.61, нетрудно показать, что минимальный период r последовательности $\sigma_1\sigma_2$ должен иметь вид $r = d_1d_2$, где d_1 — делитель числа r_1, а d_2 — делитель числа r_2. В частности, d_1r_2 является периодом последовательности $\sigma_1\sigma_2$. Таким образом, если σ_1 — это последовательность $s_0, s_1, \ldots$, а σ_2 — последовательность $t_0, t_1, \ldots$, то равенство

$$s_{n+d_1r_2}t_n = s_{n+d_1r_2}t_{n+d_1r_2} = s_nt_n$$

выполняется для всех достаточно больших n. Так как существует целое число b, такое, что $t_n \neq 0$ для всех достаточно больших $n \equiv b \pmod{r_2}$, то для таких n получаем $s_{n+d_1r_2} = s_n$. Зафиксируем теперь достаточно большое n. По китайской теореме об остатках можно выбрать такое целое число $m \geqslant n$, для которого $m \equiv n \pmod{r_1}$ и $m \equiv b \pmod{r_2}$. Тогда

$$s_n = s_m = s_{m+d_1r_2} = s_{n+d_1r_2},$$

и, таким образом, d_1r_2 является периодом последовательности σ_1. Следовательно, r_1 делит d_1r_2, а в силу того, что r_1 и r_2 взаимно просты, r_1 делит d_1, откуда следует, что $d_1 = r_1$. Аналогично доказывается равенство $d_2 = r_2$. □

Операцию умножения последовательностей можно использовать для описания соотношений между однородными линейными рекуррентными последовательностями, характеристические многочлены которых являются степенями друг друга. Рассмотрим случай линейных характеристических многочленов.

8.71. Лемма. *Если* $c \in \mathbb{F}_q$, $c \neq 0$, *а* k — *целое положительное число, то*

$$S((x-c)^k) = S(x-c)\,S((x-1)^k).$$

Доказательство. Пусть последовательность $s_0, s_1, \ldots$ лежит в $S(x-c)$, а последовательность $t_0, t_1, \ldots$ лежит в $S((x-1)^k)$. Тогда $s_n = c^n s_0$ для всех $n = 0, 1, \ldots$, и

$$\sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} t_{n+i} = 0, \quad n = 0, 1, \ldots .$$

Отсюда

$$\sum_{i=0}^{k} \binom{k}{i} (-c)^{k-i} s_{n+i} t_{n+i} = c^{n+k} s_0 \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} t_{n+i} = 0$$

для всех $n = 0, 1, \ldots$, и тогда

$$\sum_{i=0}^{k} \binom{k}{i} (-c)^{k-i} x^i = (x-c)^k$$

— характеристический многочлен последовательности $s_0 t_0, s_1 t_1, \ldots$. Значит, векторное пространство $S(x-c)\,S((x-1)^k)$ является подпространством пространства $S((x-c)^k)$. Так как $c \neq 0$, первое векторное пространство имеет над полем $\mathbb{F}_q$ размерность k и, таким образом, совпадает с пространством $S((x-c)^k)$, которое имеет ту же размерность над $\mathbb{F}_q$. □

8.72. Теорема. *Пусть $f(x) \in \mathbb{F}_q[x]$ — нормированный многочлен, не являющийся константой и не имеющий кратных корней и $f(0) \neq 0$. Пусть k — целое положительное число. Тогда*

$$S((f(x))^k) = S(f(x))\,S((x-1)^k).$$

Доказательство. Пусть F — поле разложения многочлена $f(x)$ над полем $\mathbb{F}_q$. Тогда если α пробегает все корни многочлена $f(x)$, то по теореме 8.55

$$S_F((f(x))^k) = \sum_{\alpha} S_F((x-\alpha)^k).$$

Используя лемму 8.71 и закон дистрибутивности, установленный при доказательстве теоремы 8.67, получаем

$$S_F((f(x))^k) = \sum_{\alpha} S_F((x-1)^k)\,S_F(x-\alpha) =$$

$$= S_F((x-1)^k) \sum_{\alpha} S_F(x-\alpha) = S_F((x-1)^k)\,S_F(f(x)),$$

где последнее равенство следует из теоремы 8.55. Искомый результат вытекает теперь из леммы 8.68. □

§ 6. Характеризация линейных рекуррентных последовательностей

Важной задачей является выяснение того, будет данная последовательность элементов поля $\mathbb{F}_q$ линейной рекуррентной последовательностью нлн нет. С теоретической точкн зрення этот вопрос можно разрешить немедленно, так как *линейные рекуррентные последовательности над полем* $\mathbb{F}_q$ *и только они являются периодическими последовательностями*. Однако периоды некоторых линейных рекуррентных последовательностей (даже сравнительно небольшого порядка) могут быть очень длиннымн, и на практике часто бывает иевозможным определнть природу данной последовательности на основании лишь этого критерия. Другие способы характеризации линейных рекуррентных последовательностей используют понятня линейной алгебры.

Пусть $s_0, s_1, \ldots$ — пронзвольная последовательность элементов поля $\mathbb{F}_q$. Для целых чисел $n \geqslant 0$, $r \geqslant 1$ введем понятие *ганкелева определителя*

$$D_n^{(r)} = \begin{vmatrix} s_n & s_{n+1} & \ldots & s_{n+r-1} \\ s_{n+1} & s_{n+2} & \ldots & s_{n+r} \\ \ldots & \ldots & \ldots & \ldots \\ s_{n+r-1} & s_{n+r} & \ldots & s_{n+2r-2} \end{vmatrix},$$

связанного с этой последовательностью. Как мы увиднм дальше, линейные рекуррентные последовательиости можно охарактеризовать в терминах обращення в нуль достаточного числа ганкелевых определителей, связанных с этой последовательностью.

8.73. **Лемма.** *Пусть* $s_0, s_1, \ldots$ — *произвольная последовательность над полем* $\mathbb{F}_q$, *и пусть* $n \geqslant 0$, $r \geqslant 1$ — *целые числа. Тогда из равенств* $D_n^{(r)} = D_n^{(r+1)} = 0$ *следует равенство* $D_{n+1}^{(r)} = 0$.

Доказательство. Для $m \geqslant 0$ введем вектор $\mathbf{s}_m = (s_m, s_{m+1}, \ldots, s_{m+r-1})$. Из равенства $D_n^{(r)} = 0$ следует, что векторы $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$ линейно зависимы иад полем $\mathbb{F}_q$. Если $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$ тоже линейно зависнмы над $\mathbb{F}_q$, то мы тут же получаем равенство $D_{n+1}^{(r)} = 0$. В протнвном случае вектор $\mathbf{s}_n$ является линейной комбинацией векторов $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$. Пусть $\mathbf{s}'_m = (s_m, s_{m+1}, \ldots, s_{m+r})$ для $m \geqslant 0$. Тогда векторы $\mathbf{s}'_n, \mathbf{s}'_{n+1}, \ldots, \mathbf{s}'_{n+r}$, будучи строками равного нулю определителя $D_n^{(r+1)}$, линейно зависимы над полем $\mathbb{F}_q$. Если $\mathbf{s}'_n, \mathbf{s}'_{n+1}, \ldots, \mathbf{s}'_{n+r-1}$ линейно зависимы над $\mathbb{F}_q$, то, применяя лннейное отображение

$$L_1\colon (a_0, a_1, \ldots, a_r) \in \mathbb{F}_q^{r+1} \longmapsto (a_1, \ldots, a_r) \in \mathbb{F}_q^r,$$

получаем, что $\mathbf{s}_{n+1}, \mathbf{s}_{n+2}, \ldots, \mathbf{s}_{n+r}$ тоже линейно зависимы над $\mathbb{F}_q$ и, следовательно, $D_{n+1}^{(r)} = 0$. В противном случае (если $\mathbf{s}'_n$,

$\mathbf{s}'_{n+1}, \ldots, \mathbf{s}'_{n+r-1}$ линейно независимы) получаем, что вектор $\mathbf{s}'_{n+r}$ является линейной комбинацией $\mathbf{s}'_n, \mathbf{s}'_{n+1}, \ldots, \mathbf{s}'_{n+r-1}$, и тогда, применяя линейное отображение

$$L_2\colon (a_0, a_1, \ldots, a_{r-1}, a_r) \in \mathbb{F}_q^{r+1} \longmapsto (a_0, a_1, \ldots, a_{r-1}) \in \mathbb{F}_q^r,$$

получаем, что $\mathbf{s}_{n+r}$ является линейной комбинацией векторов $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$. Но в рассматриваемом случае $\mathbf{s}_n$ есть линейная комбинация векторов $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$. Таким образом, векторы $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}, \mathbf{s}_{n+r}$, являющиеся строками определителя $D_{n+1}^{(r)}$, линейно зависимы над $\mathbb{F}_q$, откуда следует, что $D_{n+1}^{(r)} = 0$. □

8.74. Теорема. *Последовательность $s_0, s_1, \ldots$ элементов поля $\mathbb{F}_q$ является линейной рекуррентной последовательностью тогда и только тогда, когда существует положительное целое число r, такое, что $D_n^{(r)} = 0$ для всех (кроме, может быть, конечного числа) $n \geqslant 0$.*

Доказательство. Предположим, что последовательность $s_0, s_1, \ldots$ удовлетворяет однородному линейному рекуррентному соотношению k-го порядка. Для любого фиксированного $n \geqslant 0$ рассмотрим определитель $D_n^{(k+1)}$. В силу линейного рекуррентного соотношения, которому подчиняются элементы последовательности $s_0, s_1, \ldots$, $(k+1)$-я строка определителя $D_n^{(k+1)}$ является линейной комбинацией первых k строк, и, следовательно, $D_n^{(k+1)} = 0$. Неоднородный случай сводится к однородному по формуле (8.5). Необходимость доказана.

Докажем достаточность. Пусть $k+1$ — наименьшее натуральное число, такое, что $D_n^{(k+1)} = 0$ для всех, кроме, может быть, конечного числа $n \geqslant 0$. Если $k+1 = 1$, то теорема доказана. Рассмотрим случай $k \geqslant 1$. Тогда найдется целое $m \geqslant 0$, такое, что $D_n^{(k+1)} = 0$ для всех $n \geqslant m$. Если $D_{n_0}^{(k)} = 0$ для некоторого $n_0 \geqslant m$, то по лемме 8.73 $D_n^{(k)} = 0$ для всех $n \geqslant n_0$, что противоречит выбору $k+1$. Следовательно, $D_n^{(k)} \neq 0$ для всех $n \geqslant m$. Положим $\mathbf{s}_n = (s_n, s_{n+1}, \ldots, s_{n+k})$. Заметим, что для всех $n \geqslant m$ векторы $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+k}$, будучи строками определителя $D_n^{(k+1)} = 0$, линейно зависимы над полем $\mathbb{F}_q$. В силу того что $D_n^{(k)} \neq 0$, векторы $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+k-1}$ линейно независимы над $\mathbb{F}_q$, и, значит, $\mathbf{s}_{n+k}$ является линейной комбинацией векторов $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+k-1}$. По индукции легко получить, что для всех $n \geqslant m$ вектор $\mathbf{s}_n$ является линейной комбинацией векторов $\mathbf{s}_m, \mathbf{s}_{m+1}, \ldots, \mathbf{s}_{m+k-1}$. Последние представляют собой k векторов пространства $\mathbb{F}_q^{k+1}$, а следовательно, существует ненулевой вектор $(a_0, a_1, \ldots, a_k) \in \mathbb{F}_q^{k+1}$, для которого выполняются равенства

$$a_0 s_n + a_1 s_{n+1} + \ldots + a_k s_{n+k} = 0 \quad \text{при} \quad m \leqslant n \leqslant m+k-1.$$

Отсюда вытекает, что

$$a_0 s_n + a_1 s_{n+1} + \cdots + a_k s_{n+k} = 0 \quad \text{для всех } n \geqslant m$$

или

$$a_0 s_{n+m} + a_1 s_{n+m+1} + \cdots + a_k s_{n+m+k} = 0 \quad \text{для всех } n \geqslant 0.$$

Таким образом, показано, что последовательность $s_0, s_1, \ldots$ удовлетворяет однородному линейному рекуррентному соотношению, имеющему порядок не более чем $m + k$, □

8.75. Теорема. *Последовательность $s_0, s_1, \ldots$ элементов из поля $\mathbb{F}_q$ является однородной линейной рекуррентной последовательностью с минимальным многочленом степени k тогда и только тогда, когда $D_0^{(r)} = 0$ для всех $r \geqslant k + 1$ и $k + 1$ — наименьшее натуральное число, для которого выполняется это равенство.*

Доказательство. Докажем необходимость. Если данная рекуррентная последовательность является нулевой последовательностью, то необходимость условий очевидна. В случае когда последовательность отлична от нулевой, мы имеем $k \geqslant 1$, и тогда $D_0^{(r)} = 0$ для всех $r \geqslant k + 1$, так как $(k + 1)$-я строка определителя $D_0^{(r)}$ является линейной комбинацией первых k строк. В свою очередь из теоремы 8.51 следует, что $D_0^{(k)} \neq 0$. Таким образом, необходимость условий доказана для всех случаев.

Для доказательства достаточности допустим, что выполняются приведенные условия для ганкелевых определителей. Пользуясь леммой 8.73, индукцией по n можно показать, что $D_n^{(r)} = 0$ для всех $r \geqslant k + 1$ и всех $n \geqslant 0$. В частности, $D_n^{(k+1)} = 0$ для всех $n \geqslant 0$, и тогда по теореме 8.74 последовательность $s_0, s_1, \ldots$ является линейной рекуррентной последовательностью. Если ее минимальный многочлен имеет степень d, то, как мы уже показали выше, $D_0^{(r)} = 0$ для всех $r \geqslant d + 1$ и $d + 1$ является наименьшим натуральным числом, для которого выполняется это равенство. Отсюда получаем, что $d = k$. □

Если известно, что однородная линейная рекуррентная последовательность имеет минимальный многочлен степени $k \geqslant 1$, то сам минимальный многочлен полностью определяется первыми $2k$ членами этой последовательности. Чтобы убедиться в этом, запишем уравнения (8.2) для $n = 0, 1, \ldots, k - 1$ и получим систему из k линейных уравнений относительно неизвестных $a_0, a_1, \ldots, a_{k-1}$, являющихся коэффициентами искомого минимального многочлена. Определитель этой системы равняется $D_0^{(k)}$, и по теореме 8.51 $D_0^{(k)} \neq 0$. Таким образом, рассматриваемая система уравнений имеет единственное решение.

Важным вопросом является нахождение практического метода для *вычисления минимального многочлена* данной однородной линейной рекуррентной последовательности. Один такой метод уже был предложен в процессе доказательства теоремы 8.42. Этот метод предполагает предварительное знание характеристического многочлена данной последовательности и основывается на нахождении наибольшего общего делителя многочленов над полем $\mathbb{F}_q$. Ниже мы приведем и обсудим другой метод нахождения минимальных многочленов. Этот метод представляет собой рекурсивный алгоритм (так называемый *алгоритм Берлекэмпа — Месси*), который после конечного числа шагов дает искомый минимальный многочлен при условии, что нам заранее известна верхняя граница для степени искомого минимального многочлена.

Пусть $s_0, s_1, \ldots$ — последовательность над полем $\mathbb{F}_q$ и $G(x) = \sum_{n=0}^{\infty} s_n x^n$ — соответствующая производящая функция. Для $j = 0, 1, \ldots$ определим многочлены $g_j(x), h_j(x) \in \mathbb{F}_q[x]$, целые числа m_j и элементы $b_j \in \mathbb{F}_q$ следующим образом. Для $j = 0$ полагаем

$$g_0(x) = 1, \quad h_0(x) = x, \quad m_0 = 0. \tag{8.19}$$

Затем последовательно полагаем b_j равным коэффициенту при x^j в $g_j(x)\,G(x)$ и

$$\begin{aligned} g_{j+1}(x) &= g_j(x) - b_j h_j(x), \\ h_{j+1}(x) &= \begin{cases} b_j^{-1} x g_j(x), & \text{если } b_j \neq 0,\ m_j \geqslant 0, \\ x h_j(x) & \text{в противном случае,} \end{cases} \\ m_{j+1} &= \begin{cases} -m_j, & \text{если } b_j \neq 0,\ m_j \geqslant 0, \\ m_j + 1 & \text{в противном случае.} \end{cases} \end{aligned} \tag{8.20}$$

Если $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность с минимальным многочленом степени k, то в результате мы получим, что $g_{2k}(x)$ равняется возвратному минимальному многочлену. Таким образом, искомый минимальный многочлен $m(x)$ определяется равенством $m(x) = x^k g_{2k}(1/x)$. Если заранее известно лишь, что $\deg(m(x)) \leqslant k$, то положим $r = \lfloor k + 1/2 - m_{2k}/2 \rfloor$, где $\lfloor y \rfloor$ означает наибольшее целое число, не превосходящее y. Тогда *минимальный многочлен $m(x)$ определяется равенством* $m(x) = x^r g_{2k}(1/x)$. В обоих случаях из алгоритма сразу же видно, что $m(x)$ зависит только от первых $2k$ членов последовательности $s_0, s_1, \ldots, s_{2k-1}$. Следовательно, производящую функцию $G(x)$ в алгоритме можно заменить многочленом

$$G_{2k-1}(x) = \sum_{n=0}^{2k-1} s_n x^n.$$

8.76. Пример. Первые 8 членов однородной линейной рекуррентной последовательности над полем $\mathbb{F}_3$ порядка $k \leqslant 4$ имеют вид 1, 2, 1, 0, 1, 2, 1, 0. Для того чтобы найти ее минимальный многочлен, применим алгоритм Берлекэмпа — Месси с многочленом

$$G_7(x) = 2x + x^2 + x^4 + 2x^5 + x^6 \in \mathbb{F}_3[x]$$

вместо производящей функции $G(x)$. В следующей таблице приводятся промежуточные результаты, полученные в процессе работы алгоритма.

j	$g_j(x)$	$h_j(x)$	m_j	b_j
0	1	x	0	0
1	1	x^2	1	2
2	$1 + x^2$	$2x$	-1	1
3	$1 + x + x^2$	$2x^2$	0	0
4	$1 + x + x^2$	$2x^3$	1	2
5	$1 + x + x^2 + 2x^3$	$2x + 2x^2 + 2x^3$	-1	2
6	$1 + x^3$	$2x^2 + 2x^3 + 2x^4$	0	1
7	$1 + x^2 + 2x^3 + x^4$	$x + x^4$	0	1
8	$1 + 2x + x^2 + 2x^3$		0	

В этом случае $r = \lfloor 4 + 1/2 - m_8/2 \rfloor = 4$ и, следовательно, $m(x) = x^4 + 2x^3 + x^2 + 2x$. Таким образом, линейное рекуррентное соотношение наименьшего порядка, которому удовлетворяет данная последовательность, имеет вид

$$s_{n+4} = s_{n+3} + 2s_{n+2} + s_{n+1}, \quad n = 0, 1, \ldots . \qquad \square$$

8.77. Пример. Найдем однородную линейную рекуррентную последовательность наименьшего порядка над полем $\mathbb{F}_2$, первые 8 членов которой — это 1, 1, 0, 0, 1, 0, 1, 1. Применим алгоритм Берлекэмпа — Месси, используя многочлен $G_7(x) = 1 + x + x^4 + x^6 + x^7 \in \mathbb{F}_2[x]$ вместо производящей функции $G(x)$. Этапы вычисления приводятся в следующей таблице.

j	$g_j(x)$	$h_j(x)$	m_j	b_j
0	1	x	0	1
1	$1 + x$	x	0	0
2	$1 + x$	x^2	1	1
3	$1 + x + x^2$	$x + x^2$	-1	1
4	1	$x^2 + x^3$	0	1
5	$1 + x^2 + x^3$	x	0	0
6	$1 + x^2 + x^3$	x^2	1	0
7	$1 + x^2 + x^3$	x^3	2	0
8	$1 + x^2 + x^3$		3	

В этом случае $r = \lfloor 4 + 1/2 - m_8/2 \rfloor = 3$ и, следовательно, $m(x) = x^3 + x + 1$. Таким образом, заданные элементы образуют начальный отрезок однородной линейной рекуррентной последовательности $s_0, s_1, \ldots$, удовлетворяющей рекуррентному соотношению $s_{n+3} = s_{n+1} + s_n$, $n = 0, 1, \ldots$, и не существует рекуррентной последовательности меньшего порядка, имеющей тот же начальный отрезок. □

Докажем теперь в общем случае, что после конечного числа шагов *алгоритм Берлекэмпа — Месси приводит к искомому минимальному многочлену*. Для этого введем вспомогательные многочлены $u_j(x), v_j(x) \in \mathbb{F}_q[x]$. Определим их следующими рекуррентными формулами:

$$u_0(x) = 0, \quad v_0(x) = -1, \tag{8.21}$$

$$u_{j+1}(x) = u_j(x) - b_j v_j(x),$$

$$v_{j+1}(x) = \begin{cases} b_j^{-1} x u_j(x), & \text{если } b_j \neq 0, \quad m_j \geqslant 0, \\ x v_j(x) & \text{в противном случае} \end{cases} \tag{8.22}$$

для всех $j = 0, 1, \ldots$, Мы утверждаем, что для всех $j \geqslant 0$

$$\deg(g_j(x)) \leqslant \tfrac{1}{2}(j + 1 - m_j), \quad \deg(h_j(x)) \leqslant \tfrac{1}{2}(j + 2 + m_j). \tag{8.23}$$

Для $j = 0$ это очевидно ввиду (8.19). Если неравенства (8.23) доказаны для некоторого $j \geqslant 0$, то из (8.20) следует, что в случае, когда $b_j \neq 0$, $m_j \geqslant 0$,

$$\deg(g_{j+1}(x)) \leqslant \max(\deg(g_j(x)), \quad \deg(h_j(x))) \leqslant$$
$$\leqslant \tfrac{1}{2}(j + 2 + m_j) = \tfrac{1}{2}(j + 2 - m_{j+1}).$$

В противном случае

$$\deg(g_{j+1}(x)) \leqslant \tfrac{1}{2}(j + 1 - m_j) = \tfrac{1}{2}(j + 2 - m_{j+1}).$$

Второе неравенство в (8.23) доказывается аналогичным образом. Индукцией по j можно также доказать, что для любого $j \geqslant 0$ выполняются неравенства

$$\deg(u_j(x)) \leqslant \tfrac{1}{2}(j - 1 - m_j), \quad \deg(v_j(x)) \leqslant \tfrac{1}{2}(j + m_j). \tag{8.24}$$

Для всех $j \geqslant 0$ вспомогательные многочлены $u_j(x)$ и $v_j(x)$ связаны с многочленами $g_j(x)$ и $h_j(x)$ следующими соотношениями:

$$g_j(x) G(x) \equiv u_j(x) + b_j x^j \pmod{x^{j+1}}. \tag{8.25}$$

$$h_j(x) G(x) \equiv v_j(x) + x^j \pmod{x^{j+1}}. \tag{8.26}$$

В самом деле, для $j = 0$ (8.25) и (8.26) следуют из (8.19), (8.21) и определения константы b_0. Предполагая, что соотношения (8.25) и (8.26) доказаны для некоторого $j \geqslant 0$, получаем

$$g_{j+1}(x)\,G(x) = g_j(x)\,G(x) - b_j h_j(x)\,G(x) \equiv$$
$$\equiv u_j(x) + b_j x^j + c_{j+1}x^{j+1} - b_j(v_j(x) + x^j + d_{j+1}x^{j+1}) \equiv$$
$$\equiv u_{j+1}(x) + e_{j+1}x^{j+1} \pmod{x^{j+2}},$$

где c_{j+1}, d_{j+1}, $e_{j+1} \in \mathbb{F}_q$ — некоторые подходящие коэффициенты. Поскольку $|m_j| \leqslant j$, как это можно показать по индукции, то из (8.24) получаем $\deg(u_{j+1}(x)) \leqslant j$. Таким образом, e_{j+1} является коэффициентом при x^{j+1} в $g_{j+1}(x)\,G(x)$ и, следовательно, $e_{j+1} = b_{j+1}$. Соотношение (8.26) для $j \geqslant 0$ доказывается аналогичным образом.

Далее, по индукции легко доказать, что для всех $j \geqslant 0$

$$h_j(x)\,u_j(x) - g_j(x)\,v_j(x) = x^j. \tag{8.27}$$

Пусть теперь $s(x)$, $u(x)$ — многочлены над полем $\mathbb{F}_q$, связанные соотношением $s(x)\,G(x) = u(x)$ и условием $s(0) = 1$. Тогда из (8.26) следует, что

$$h_j(x)\,u(x) - s(x)\,v_j(x) = s(x)\,(h_j(x)\,G(x) - v_j(x)) \equiv$$
$$\equiv s(x)\,x^j \equiv x^j \pmod{x^{j+1}},$$

и тогда для некоторого $U_j(x) \in \mathbb{F}_q[x]$ получаем

$$h_j(x)\,u(x) - s(x)\,v_j(x) = x^j U_j(x), \quad \text{где} \quad U_j(0) = 1. \tag{8.28}$$

Аналогично, пользуясь (8.25), можно показать, что существует $V_j(x) \in \mathbb{F}_q[x]$, для которого справедливо равенство

$$g_j(x)\,u(x) - s(x)\,u_j(x) = x^j V_j(x). \tag{8.29}$$

Предположим теперь, что минимальный многочлен $m(x)$ данной однородной линейной рекуррентной последовательности удовлетворяет условию $\deg(m(x)) \leqslant k$. Пусть $s(x)$ будет соответствующим возвратным минимальным многочленом. Тогда $s(0) = 1$, $\deg(s(x)) \leqslant k$ и из (8.15) мы получаем, что существует многочлен $u(x) \in \mathbb{F}_q[x]$, для которого выполняются соотношения $s(x)\,G(x) = u(x)$ и $\deg(u(x)) \leqslant \deg(m(x)) - 1 \leqslant k - 1$. Положим в (8.28) $j = 2k$. Воспользовавшись (8.23) и (8.24), получаем

$$\deg(h_{2k}(x)\,u(x)) \leqslant \frac{1}{2}(2k + 2 + m_{2k}) + k - 1 = 2k + \frac{1}{2}m_{2k},$$

$$\deg(s(x)\,v_{2k}(x)) \leqslant k + \frac{1}{2}(2k + m_{2k}) = 2k + \frac{1}{2}m_{2k},$$

откуда

$$\deg(h_{2k}(x)\,u(x) - s(x)\,v_{2k}(x)) \leqslant 2k + \frac{1}{2}m_{2k}.$$

С другой стороны,

$$\deg(h_{2k}(x)u(x) - s(x)v_{2k}(x)) = \deg(x^{2k}U_{2k}(x)) \geqslant 2k,$$

и все эти неравенства совместимы лишь при $m_{2k} \geqslant 0$. Вновь воспользовавшись соотношениями (8.23) и (8.24), нетрудно проверить, что $\deg(g_{2k}(x)\,u(x)) \leqslant 2k - 1/2 - (1/2)\,m_{2k}$ и $\deg(s(x)\cdot u_{2k}(x)) \leqslant 2k - 1/2 - (1/2)\,m_{2k}$. Тогда из (8.29) вытекает, что

$$\deg(x^{2k}V_{2k}(x)) = \deg(g_{2k}(x)u(x) - s(x)u_{2k}(x)) < 2k.$$

Но это возможно лишь при условии, что $V_{2k}(x)$ является нулевым многочленом. Следовательно, из (8.29) вытекает, что $g_{2k}(x)\,u(x) = s(x)\,u_{2k}(x)$. Полагая $j = 2k$ и умножая обе части равенства (8.28) на $g_{2k}(x)$, приходим к равенству

$$h_{2k}(x)\,g_{2k}(x)\,u(x) - s(x)\,g_{2k}(x)\,v_{2k}(x) =$$

$$= s(x)\,(h_{2k}(x)\,u_{2k}(x) - g_{2k}(x)\,v_{2k}(x)) = x^{2k}U_{2k}(x)\,g_{2k}(x).$$

Учитывая (8.27), получаем $s(x) = U_{2k}(x)\,g_{2k}(x)$, откуда вытекает, что $u(x) = U_{2k}(x)\,u_{2k}(x)$. Так как $s(x)$ является возвратным минимальным многочленом, из второй части теоремы 8.40 следует, что многочлены $s(x)$ и $u(x)$ взаимно просты. В силу этого многочлен $U_{2k}(x)$ обязан быть константой, а так как по (8.28) $U_{2k}(0) = 1$, то $U_{2k}(x) = 1$. Значит, $s(x) = g_{2k}(x)$ и соответственно $u(x) = u_{2k}(x)$. Если $\deg(m(x)) = k$, то

$$m(x) = x^k s\left(\frac{1}{x}\right) = x^k g_{2k}\left(\frac{1}{x}\right),$$

как и утверждалось ранее. Если же $\deg(m(x)) = t \leqslant k$, то $s(x) = g_{2t}(x)$, $u(x) = u_{2t}(x)$, $m_{2t} \geqslant 0$. Очевидно, что $\max(\deg(s(x)), 1 + \deg(u(x))) \leqslant t$, и из второй части теоремы 8.40 вытекает

$$t = \max(\deg(s(x)),\ 1 + \deg(u(x))).$$

Тогда из (8.23) и (8.24) следует, что

$$t = \max(\deg(g_{2t}(x)),\ 1 + \deg(u_{2t}(x))) \leqslant t + \frac{1}{2} - \frac{1}{2}\,m_{2t}.$$

Таким образом, m_{2t} равно 0 или 1. Кроме того, заметим, что $g_j(x) = s(x)$ и $b_j = 0$ для всех $j \geqslant 2t$. Тогда $m_j = m_{2t} + j - 2t$ для всех $j \geqslant 2t$ по определению m_j. Полагая $j = 2k$, получаем $t = k + (1/2)\,m_{2t} - (1/2)\,m_{2k}$, и так как m_{2t} равняется 0 или 1, то

$$t = \left\lfloor k + \frac{1}{2} - \frac{1}{2}\,m_{2k} \right\rfloor = r.$$

Таким образом,

$$m(x) = x^r s\left(\frac{1}{x}\right) = x^r g_{2k}\left(\frac{1}{x}\right),$$

что соответствует нашему утверждению.

§ 7. Распределение элементов в линейных рекуррентных последовательностях

В этом параграфе нас будет интересовать следующий вопрос: сколько раз встречается тот или иной элемент поля $\mathbb{F}_q$ на том или ином отрезке линейной рекуррентной последовательности над полем $\mathbb{F}_q$. Для получения общих результатов в этом направлении займемся сначала детальным изучением свойств тригонометрических сумм, связанных с линейными рекуррентными последовательностями. Тогда станет очевидным, что в случае линейных рекуррентных последовательностей с большим минимальным периодом на любом отрезке последовательности, составляющем ее полный период, а также на отрезках, являющихся существенной частью полного периода, элементы основного поля встречаются приблизительно с одинаковой частотой.

Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, удовлетворяющая соотношению (8.1). Пусть r — минимальный период этой последовательности, а n_0 — ее предпериод, т. е. $s_{n+r} = s_n$ для всех $n \geqslant n_0$. Свяжем с этой последовательностью целое положительное число R, определенное следующим образом. Рассмотрим рекуррентную последовательность, являющуюся импульсной функцией и удовлетворяющую соотношению (8.6). Пусть r_1 — минимальный период этой последовательности, а n_1 — ее предпериод. Положим тогда $R = r_1 + n_1$. Разумеется, R зависит только от линейного рекуррентного соотношения (8.1), а не от конкретного вида последовательности $s_0, s_1, \ldots$ Если $s_0, s_1, \ldots$ является однородной линейной рекуррентной последовательностью с характеристическим многочленом $f(x) \in \mathbb{F}_q[x]$, то $r_1 = \operatorname{ord}(f(x))$, а если, кроме того, $f(0) \neq 0$, то по теореме 8.27 $R = \operatorname{ord}(f(x))$. По той же теореме в однородном случае r делит r_1 и $r \leqslant R$.

В тригонометрических суммах, которые мы собираемся рассматривать, будут использоваться аддитивные характеры поля $\mathbb{F}_q$, изучавшиеся в гл. 5, которым будут приписаны веса, определенные с помощью функции $e(t) = e^{2\pi i t}$, где t — действительный аргумент.

8.78. Теорема. *Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, r — ее минимальный период, а n_0 — предпериод. Пусть, далее, R — целое положительное число, определенное выше. Если χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, то для любого целого числа h справедливо неравенство.*

$$\left| \sum_{n=u}^{u+r-1} \chi(s_n) e\left(\frac{hn}{r}\right) \right| \leqslant \left(\frac{r}{R}\right)^{1/2} q^{k/2} \quad \text{для всех} \quad u \geqslant n_0. \tag{8.30}$$

В частности,

$$\left|\sum_{n=u}^{u+r-1}\chi(s_n)\right| \leqslant \left(\frac{r}{R}\right)^{1/2} q^{k/2} \quad \text{для всех} \quad u \geqslant n_0. \tag{8.31}$$

Доказательство. Заменив вектор начального состояния $\mathbf{s}_0$ на вектор $\mathbf{s}_u$ (что не влияет на верхнюю границу в (8.30)), мы можем, не теряя общности, предположить, что последовательность $s_0, s_1, \ldots$ является чисто периодической последовательностью и что $u = 0$. Для произвольного вектора-столбца $\mathbf{b} = (b_0, b_1, \ldots, b_{k-1})^{\mathrm{T}}$ из пространства $\mathbb{F}_b^k$ и произвольного целого числа h положим

$$\sigma(\mathbf{b};\ h) = \sigma(b_0,\ b_1,\ \ldots,\ b_{k-1};\ h) = \sum_{n=0}^{r-1}\chi(b_0 s_n + b_1 s_{n+1} + \cdots + b_{k-1}s_{n+k-1})\, e\left(\frac{hn}{r}\right).$$

Общий член под знаком суммы, рассматриваемый как функция от n, имеет период r. Поэтому мы можем записать

$$\sigma(\mathbf{b};\ h) = \sum_{n=0}^{r-1}\chi(b_0 s_{n+1} + b_1 s_{n+2} + \cdots + b_{k-1}s_{n+k})\, e\left(\frac{h(n+1)}{r}\right).$$

Используя линейное рекуррентное соотношение (8.1), получаем

$$\begin{aligned}|\sigma(\mathbf{b};\ h)| &= \left|\sum_{n=0}^{r-1}\chi(b_0 s_{n+1} + b_1 s_{n+2} + \cdots + b_{k-2}s_{n+k-1} + b_{k-1}a_0 s_n + \right.\\ &\left. + b_{k-1}a_1 s_{n+1} + \cdots + b_{k-1}a_{k-1}s_{n+k-1} + b_{k-1}a)\, e\left(\frac{hn}{r}\right)\right| =\\ &= \left|\sum_{n=0}^{r-1}\chi(b_{k-1}a_0 s_n + (b_0 + b_{k-1}a_1)\, s_{n+1} + \ldots\right.\\ &\left. \cdots + (b_{k-2} + b_{k-1}a_{k-1})\, s_{n+k-1})\, e\left(\frac{hn}{r}\right)\right| =\\ &= |\sigma(b_{k-1}a_0,\ b_0 + b_{k-1}a_1,\ \ldots,\ b_{k-2} + b_{k-1}a_{k-1};\ h)|.\end{aligned}$$

Это равенство может быть записано в виде

$$|\sigma(\mathbf{b};\ h)| = |\sigma(A\mathbf{b};\ h)|,$$

где A — матрица, определяемая формулой (8.3). По индукции получаем, что

$$|\sigma(\mathbf{b};\ h)| = |\sigma(A^j\mathbf{b};\ h)| \quad \text{для всех} \quad j \geqslant 0. \tag{8.32}$$

Пусть $\mathbf{d} = (1,\ 0,\ \ldots,\ 0)^{\mathrm{T}} \in \mathbb{F}_q^k$ — вектор-столбец, и пусть $\mathbf{d}_0$, $\mathbf{d}_1$, ... — векторы состояний импульсной функции $d_0, d_1, \ldots$,

удовлетворяющей (8.6). Тогда мы утверждаем, что два вектора состояний $\mathbf{d}_m$ и $\mathbf{d}_n$ совпадают в том и только том случае, когда $A^m\mathbf{d} = A^n\mathbf{d}$. Действительно, если $\mathbf{d}_m = \mathbf{d}_n$, то из леммы 8.15 следует равенство $A^m\mathbf{d} = A^n\mathbf{d}$. С другой стороны, если $A^m\mathbf{d} = A^n\mathbf{d}$, то $A^{m+i}\mathbf{d} = A^{n+i}\mathbf{d}$ и, значит, $A^m(A^i\mathbf{d}) = A^n(A^i\mathbf{d})$ для всех $j \geqslant 0$. Но в силу того, что векторы $\mathbf{d}, A\mathbf{d}, A^2\mathbf{d}, \ldots, A^{k-1}\mathbf{d}$ образуют базис векторного пространства $\mathbb{F}_q^k$ над полем $\mathbb{F}_q$, мы получаем, что $A^m = A^n$, откуда по лемме 8.15 следует, что $\mathbf{d}_m = \mathbf{d}_n$.

Все различные векторы последовательности $\mathbf{d}_0, \mathbf{d}_1, \ldots$ исчерпываются векторами $\mathbf{d}_0, \mathbf{d}_1, \ldots, \mathbf{d}_{R-1}$. Следовательно, как мы только что показали, различными векторами среди последовательности векторов $\mathbf{d}, A\mathbf{d}, A^2\mathbf{d}, \ldots$ являются в точности векторы $\mathbf{d}, A\mathbf{d}, \ldots, A^{R-1}\mathbf{d}$. Воспользовавшись равенством (8.32), получаем

$$R\,|\sigma(\mathbf{d};\ h)|^2 = \sum_{j=0}^{R-1} |\sigma(A^j\mathbf{d};\ h)|^2 \leqslant \sum_{\mathbf{b}} |\sigma(\mathbf{b};\ h)|^2, \qquad (8.33)$$

где последняя сумма берется по всем векторам $\mathbf{b}$ из пространства $\mathbb{F}_q^k$. В то же время

$$\begin{aligned}
\sum_{\mathbf{b}} |\sigma(\mathbf{b};\ h)|^2 &= \sum_{\mathbf{b}} \sigma(\mathbf{b};\ h)\,\overline{\sigma(\mathbf{b};\ h)} = \\
&= \sum_{b_0, b_1, \ldots, b_{k-1} \in \mathbb{F}_q} \sum_{m,\, n=0}^{r-1} \chi(b_0(s_m - s_n) + b_1(s_{m+1} - \\
&\quad - s_{n+1}) + \cdots + b_{k-1}(s_{m+k-1} - s_{n+k-1}))\, e\left(\frac{h(m-n)}{r}\right) = \\
&= \sum_{m,\, n=0}^{r-1} e\left(\frac{h(m-n)}{r}\right) \cdot \\
&\quad \sum_{b_0, b_1, \ldots, b_{k-1} \in \mathbb{F}_q} \chi(b_0(s_m - s_n))\,\chi(b_1(s_{m+1} - s_{n+1})) \ldots \\
&\quad \ldots \chi(b_{k-1}(s_{m+k-1} - s_{n+k-1})) = \\
&= \sum_{m,\, n=0}^{r-1} e\left(\frac{h(m-n)}{r}\right) \left(\sum_{b_0 \in \mathbb{F}_q} \chi(b_0(s_m - s_n))\right) \ldots \\
&\quad \ldots \left(\sum_{b_{k-1} \in \mathbb{F}_q} \chi(b_{k-1}(s_{m+k-1} - s_{n+k-1}))\right). \qquad (8.34)
\end{aligned}$$

Заметим, что для $c \in \mathbb{F}_q$ из (5.9) следует

$$\sum_{b \in \mathbb{F}_q} \chi(bc) = \begin{cases} 0, & \text{если } c \neq 0, \\ q, & \text{если } c = 0. \end{cases}$$

Таким образом, вклад в последнее выражение в формуле (8.34) дают только те упорядоченные пары (m, n), для которых одновременно выполняются равенства $s_m = s_n, \ldots, s_{m+k-1} = s_{n+k-1}$. Однако в силу того, что $0 \leqslant m, n \leqslant r-1$, это возможно лишь при $m = n$. Отсюда следует, что

$$\sum_{\mathbf{b}} |\sigma(\mathbf{b}; h)|^2 = rq^k.$$

Объединяя это равенство с неравенством (8.33), получаем

$$|\sigma(\mathbf{d}; h)| \leqslant \left(\frac{r}{R}\right)^{1/2} q^{k/2},$$

что и доказывает (8.30). Неравенство (8.31) следует из (8.30), если положить $h = 0$. □

8.79. Замечание. Пусть χ является нетривиальным аддитивным характером поля $\mathbb{F}_q$, и пусть ψ — произвольный мультипликативный характер того же поля. Тогда сумму Гаусса

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c)$$

можно рассматривать как частный случай суммы из (8.30). Чтобы показать это, выберем примитивный элемент g поля $\mathbb{F}_q$ и рассмотрим линейную рекуррентную последовательность $s_0, s_1, \ldots$ 1-го порядка над полем $\mathbb{F}_q$, определяемую равенством $s_0 = 1$ и рекуррентным соотношением $s_{n+1} = gs_n$, $n = 0, 1, \ldots$, Тогда $r = R = q - 1$, а $n_0 = 0$. Заметим, что $\psi(g) = e(h/r)$ для некоторого целого h. На основании этого мы можем записать

$$G(\psi, \chi) = \sum_{n=0}^{r-1} \chi(g^n)\psi(g^n) = \sum_{n=0}^{r-1} \chi(s_n)\, e\left(\frac{hn}{r}\right).$$

Если ψ является нетривиальным характером, то в этом случае из равенства (5.15) следует, что обе части соотношения (8.30) совпадают. □

Суммы, фигурирующие в теореме 8.78, брались по полному периоду данной линейной рекуррентной последовательности. Следующий результат позволяет оценивать суммы, берущиеся по отрезку полного периода. Для этого нам потребуется такая вспомогательная лемма:

8.80. Лемма. *Для любых положительных целых чисел r и N справедливо неравенство*

$$\sum_{h=0}^{r-1} \left| \sum_{j=0}^{N-1} e\left(\frac{hj}{r}\right) \right| < \frac{2}{\pi} r \log r + \frac{2}{5} r + N. \qquad (8.35)$$

Доказательство. Для $r = 1$ неравенство (8.35) тривиально. Для $r \geqslant 2$

$$\left| \sum_{j=0}^{N-1} e\left(\frac{hj}{r}\right) \right| = \frac{|e(hN/r) - 1|}{|e(h/r) - 1|} \leqslant \frac{1}{\sin \pi \|h/r\|} = \operatorname{cosec} \pi \left\| \frac{h}{r} \right\|,$$

$$1 \leqslant h \leqslant r - 1,$$

где $\| t \|$ означает расстояние от действительного числа t до ближайшего целого числа. Отсюда следует, что

$$\sum_{h=0}^{r-1} \left| \sum_{j=0}^{N-1} e\left(\frac{hj}{r}\right) \right| \leqslant \sum_{h=1}^{r-1} \operatorname{cosec} \pi \left\| \frac{h}{r} \right\| + N \leqslant 2 \sum_{h=1}^{\lfloor r/2 \rfloor} \operatorname{cosec} \frac{\pi h}{r} + N. \tag{8.36}$$

Сравнивая суммы с соответствующими интегралами, получаем

$$\begin{aligned} \sum_{h=1}^{\lfloor r/2 \rfloor} \operatorname{cosec} \frac{\pi h}{r} &= \operatorname{cosec} \frac{\pi}{r} + \sum_{h=2}^{\lfloor r/2 \rfloor} \operatorname{cosec} \frac{\pi h}{r} \leqslant \\ &\leqslant \operatorname{cosec} \frac{\pi}{r} + \int_{1}^{\lfloor r/2 \rfloor} \operatorname{cosec} \frac{\pi x}{r}\, dx \leqslant \\ &\leqslant \operatorname{cosec} \frac{\pi}{r} + \frac{r}{\pi} \int_{\pi/r}^{\pi/2} \operatorname{cosec} t\, dt = \\ &= \operatorname{cosec} \frac{\pi}{r} + \frac{r}{\pi} \log \operatorname{ctg} \frac{\pi}{2r} \leqslant \operatorname{cosec} \frac{\pi}{r} + \frac{r}{\pi} \log \frac{2r}{\pi}. \end{aligned}$$

Для $r \geqslant 6$ справедливо неравенство $(\pi/r)^{-1} \sin(\pi/r) \geqslant (\pi/6)^{-1} \cdot \sin(\pi/6)$; следовательно, $\sin(\pi/r) \geqslant 3/r$. Отсюда вытекает, что

$$\sum_{h=1}^{\lfloor r/2 \rfloor} \operatorname{cosec} \frac{\pi h}{r} \leqslant \frac{1}{\pi} r \log r + \left(\frac{1}{3} - \frac{1}{\pi} \log \frac{\pi}{2}\right) r \quad \text{для} \quad r \geqslant 6,$$

и, значит,

$$\sum_{h=1}^{\lfloor r/2 \rfloor} \operatorname{cosec} \frac{\pi h}{r} < \frac{1}{\pi} r \log r + \frac{1}{5} r \quad \text{для} \quad r \geqslant 6.$$

Для $r = 3, 4, 5$ неравенство (8.35) легко получить из (8.36). Для $r = 2$ справедливость неравенства (8.35) проверяется непосредственно. □

8.81. Теорема. *Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, а числа r, n_0 и R*

такие же, как и в теореме 8.78. *Тогда для любого нетривиального аддитивного характера* χ *поля* $\mathbb{F}_q$ *справедливо неравенство*

$$\left|\sum_{n=u}^{u+N-1}\chi(s_n)\right| < \left(\frac{r}{R}\right)^{1/2} q^{k/2}\left(\frac{2}{\pi}\log r + \frac{2}{5} + \frac{N}{r}\right),$$

где $u \geqslant n_0$ *и* $1 \leqslant N \leqslant r$.

Доказательство. Начнем с равенства

$$\sum_{n=u}^{u+N-1}\chi(s_n) = \sum_{n=u}^{u+r-1}\chi(s_n)\sum_{j=0}^{N-1}\frac{1}{r}\sum_{h=0}^{r-1}e\left(\frac{h(n-u-j)}{r}\right),$$

где $1 \leqslant N \leqslant r$.

Оно справедливо, так как сумма по j равняется 1 при $u \leqslant n \leqslant u+N-1$ и 0 при $u+N \leqslant n \leqslant u+r-1$. Переставляя соответствующим образом члены, получаем

$$\sum_{n=u}^{u+N-1}\chi(s_n) = \frac{1}{r}\sum_{h=0}^{r-1}\left(\sum_{j=0}^{N-1}e\left(\frac{-h(u+j)}{r}\right)\right)\left(\sum_{n=u}^{u+r-1}\chi(s_n)\,e\left(\frac{hn}{r}\right)\right),$$

откуда в силу (8.30) следует

$$\left|\sum_{n=u}^{u+N-1}\chi(s_n)\right| \leqslant \frac{1}{r}\sum_{h=0}^{r-1}\left|\sum_{j=0}^{N-1}e\left(\frac{-h(u+j)}{r}\right)\right|\left|\sum_{n=u}^{u+r-1}\chi(s_n)\,e\left(\frac{hn}{r}\right)\right| \leqslant$$

$$\leqslant \frac{1}{r}\left(\frac{r}{R}\right)^{1/2} q^{k/2}\sum_{h=0}^{r-1}\left|\sum_{j=0}^{N-1}e\left(\frac{hj}{r}\right)\right|.$$

Применяя теперь лемму 8.80, получаем искомое неравенство. □

Следует отметить, что неравенства, полученные в теоремах 8.78 и 8.81, представляют интерес лишь в случае, когда минимальный период r последовательности $s_0, s_1, \ldots$ достаточно велик. Для малых r эти результаты становятся слабее тривиальной оценки

$$\left|\sum_{n=u}^{u+N-1}\chi(s_n)\right| \leqslant N \quad \text{для} \quad 1 \leqslant N \leqslant r.$$

Для получения нетривиальных утверждений r должно быть больше, чем $q^{k/2}$.

Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность над полем $\mathbb{F}_q$, r — ее минимальный период, а n_0 — ее предпериод. Если $b \in \mathbb{F}_q$, то через $Z(b)$ обозначим число таких n, $n_0 \leqslant n \leqslant n_0 + r - 1$, для которых $s_n = b$. Иными словами, $Z(b)$ равняется числу появлений элемента $b \in \mathbb{F}_q$ на полном периоде линейной рекуррентной последовательности.

Если $s_0, s_1, \ldots$ является рекуррентной последовательностью k-го порядка и максимального периода, то $Z(b)$ можно определить явно. В соответствии с теоремой 8.33 в этом случае $r = q^k - 1$, а $n_0 = 0$. Тогда векторы состояний нашей последовательности $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{r-1}$ пробегают все ненулевые векторы пространства $\mathbb{F}_q^k$. Следовательно, $Z(b)$ равняется числу ненулевых векторов пространства $\mathbb{F}_q^k$ с b в качестве своей первой координаты. Элементарный подсчет показывает, что $Z(b) = q^{k-1}$ для всех $b \neq 0$ и $Z(0) = q^{k-1} - 1$. Таким образом, в последовательности максимального периода над полем $\mathbb{F}_q$ все элементы поля $\mathbb{F}_q$ встречаются на полном периоде одинаково часто (с точностью до малого отклонения для нулевого элемента).

В общем случае столь равномерного распределения элементов ожидать не приходится. Однако можно оценить разницу между действительным числом появлений данного элемента и идеальным числом r/q. Если r достаточно велико, это отклонение сравнительно мало.

8.82. Теорема. *Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, r — ее минимальный период, а R такое же, как и в теореме 8.78. Тогда для любого элемента $b \in \mathbb{F}_q$*

$$\left| Z(b) - \frac{r}{q} \right| \leqslant \left(1 - \frac{1}{q}\right) \left(\frac{r}{R}\right)^{1/2} q^{k/2}.$$

Доказательство. Зафиксируем $b \in \mathbb{F}_q$ и определим на $\mathbb{F}_q$ действительнозначную функцию δ_b следующим образом: $\delta_b(b) = 1$ и $\delta_b(c) = 0$ для всех $c \neq b$. В силу (5.10) функцию δ_b можно представить в виде

$$\delta_b(c) = \frac{1}{q} \sum_{\chi} \chi(c - b),$$

где $c \in \mathbb{F}_q$, а сумма берется по всем аддитивным характерам χ поля $\mathbb{F}_q$. Тогда

$$Z(b) = \sum_{n=n_0}^{n_0+r-1} \delta_b(s_n) = \sum_{n=n_0}^{n_0+r-1} \frac{1}{q} \sum_{\chi} \chi(s_n - b) =$$

$$= \frac{1}{q} \sum_{\chi} \bar{\chi}(b) \sum_{n=n_0}^{n_0+r-1} \chi(s_n).$$

Выделяя слагаемое, соответствующее тривиальному аддитивному характеру поля $\mathbb{F}_q$, и помечая звездочкой сумму, в которой сум-

мирование производится по всем характерам, кроме тривиального, получаем

$$Z(b) - \frac{r}{q} = \frac{1}{q} \sum_{\chi}^{*} \bar{\chi}(b) \sum_{n=n_0}^{n_0+r-1} \chi(s_n).$$

Используя (8.31) и учитывая то, что существует $q-1$ нетривиальных аддитивных характеров поля $\mathbb{F}_q$, получаем

$$\left| Z(b) - \frac{r}{q} \right| \leqslant \frac{1}{q} \sum_{\chi}^{*} \left| \sum_{n=n_0}^{n_0+r-1} \chi(s_n) \right| \leqslant \left(1 - \frac{1}{q}\right) \left(\frac{r}{R}\right)^{1/2} q^{k/2}. \quad \square$$

8.83. Следствие. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$ и r — ее минимальный период. Пусть минимальный многочлен этой последовательности $m(x) \in \mathbb{F}_q[x]$ имеет степень $k \geqslant 1$ и удовлетворяет условию $m(0) \neq 0$. Тогда для любого элемента $b \in \mathbb{F}_q$ справедливо неравенство*

$$\left| Z(b) - \frac{r}{q} \right| \leqslant \left(1 - \frac{1}{q}\right) q^{k/2}.$$

Доказательство. По теореме 8.44 $r = \operatorname{ord}(m(x))$. Кроме того, в силу замечания, предшествующего теореме 8.78, $R = \operatorname{ord}(m(x))$. Тогда искомый результат следует из теоремы 8.82. $\square$

Если линейная рекуррентная последовательность имеет неприводимый минимальный многочлен, то другой метод, основанный на суммах Гаусса, приводит к несколько лучшим оценкам. В приводимом ниже доказательстве мы воспользуемся формулами для сумм Гаусса из теоремы 5.11.

8.84. Теорема. *Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$ и r — ее минимальный период. Предположим, что минимальный многочлен этой последовательности $m(x)$ является неприводимым многочленом степени k над полем $\mathbb{F}_q$ и при этом удовлетворяет условию $m(0) \neq 0$. Пусть h — наименьшее общее кратное чисел r и $q-1$. Тогда*

$$\left| Z(0) - \frac{(q^k-1)r}{q^k-1} \right| \leqslant \left(1 - \frac{1}{q}\right) \left(\frac{r}{h} - \frac{r}{q^k-1}\right) q^{k/2}, \quad (8.37)$$

а при $b \neq 0$

$$\left| Z(b) - \frac{q^{k-1}r}{q^k-1} \right| \leqslant \left(\frac{r}{h} - \frac{r}{q^k-1} + \frac{h-r}{h} q^{1/2}\right) q^{(k/2)-1}. \quad (8.38)$$

Доказательство. Положим $K = \mathbb{F}_q$, и пусть F — поле разложения многочлена $m(x)$ над полем K. Пусть $\alpha \in F$ — корень

многочлена $m(x)$; тогда $\alpha \neq 0$, так как $m(0) \neq 0$. По теореме 8.24 найдется $\theta \in F$, такой, что

$$s_n = \mathrm{Tr}_{F/K}(\theta\alpha^n), \quad n = 0, 1, \ldots . \tag{8.39}$$

Очевидно, что $\theta \neq 0$. Пусть λ' — канонический аддитивный характер поля K (см. (5.6)). Тогда из соотношения (5.9) вытекает, что для любого фиксированного элемента $b \in K$

$$\frac{1}{q}\sum_{c \in K} \lambda'(c(b - s_n)) = \begin{cases} 1, & \text{если } s_n = b, \\ 0, & \text{если } s_n \neq b, \end{cases}$$

что вместе с (8.39) дает

$$Z(b) = \frac{1}{q}\sum_{n=0}^{r-1}\sum_{c \in K} \lambda'(bc)\,\lambda'(\mathrm{Tr}_{F/K}(-c\theta\alpha^n)).$$

Если λ обозначает канонический аддитивный характер поля F, то λ' и λ связаны между собой равенством $\lambda'(\mathrm{Tr}_{F/K}(\beta)) = \lambda(\beta)$ для всех $\beta \in F$ (см. (5.7)). Таким образом,

$$Z(b) = \frac{1}{q}\sum_{c \in K} \lambda'(bc)\sum_{n=0}^{r-1} \bar{\lambda}(c\theta\alpha^n) =$$

$$= \frac{r}{q} + \frac{1}{q}\sum_{c \in K^*} \lambda'(bc)\sum_{n=0}^{r-1} \bar{\lambda}(c\theta\alpha^n). \tag{8.40}$$

В силу (5.17)

$$\bar{\lambda}(\beta) = \frac{1}{q^k - 1}\sum_{\psi} G(\bar{\psi}, \bar{\lambda})\,\psi(\beta),$$

где $\beta \in F^*$, а суммирование производится по всем мультипликативным характерам ψ поля F. Для элемента $c \in K^*$ получаем

$$\sum_{n=0}^{r-1} \bar{\lambda}(c\theta\alpha^n) = \frac{1}{q^k - 1}\sum_{n=0}^{r-1}\sum_{\psi} G(\bar{\psi}, \bar{\lambda})\,\psi(c\theta\alpha^n) =$$

$$= \frac{1}{q^k - 1}\sum_{\psi} \psi(c\theta)\,G(\bar{\psi}, \bar{\lambda})\sum_{n=0}^{r-1} \psi(\alpha)^n.$$

Внутренняя сумма в последнем выражении является суммой членов геометрической прогрессии. Она равняется нулю, если $\psi(\alpha) \neq 1$ в силу того, что $\psi(\alpha)^r = \psi(\alpha^r) = \psi(1) = 1$. Таким образом,

нам необходимо суммировать лишь по множеству J, состоящему из всех таких характеров ψ, для которых $\psi(\alpha) = 1$. Поэтому

$$\sum_{n=0}^{r-1} \bar{\lambda}(c\theta\alpha^n) = \frac{r}{q^k - 1} \sum_{\psi \in J} \psi(c\theta)\, G(\bar{\psi}, \bar{\lambda}).$$

Подставляя это выражение в (8.40), получаем

$$Z(b) = \frac{r}{q} + \frac{r}{q(q^k-1)} \sum_{c \in K^*} \lambda'(bc) \sum_{\psi \in J} \psi(c\theta)\, G(\bar{\psi}, \bar{\lambda}) =$$

$$= \frac{r}{q} + \frac{r}{q(q^k-1)} \sum_{\psi \in J} \psi(\theta)\, G(\bar{\psi}, \bar{\lambda}) \sum_{c \in K^*} \psi(c)\, \lambda'(bc).$$

Если через ψ' обозначить ограничение характера ψ на K^*, то внутреннюю сумму можно рассматривать как сумму Гаусса над полем K с аддитивным характером $\lambda'_b(c) = \lambda'(bc)$ для $c \in K$. Тогда

$$Z(b) = \frac{r}{q} + \frac{r}{q(q^k-1)} \sum_{\psi \in J} \psi(\theta)\, G(\bar{\psi}, \bar{\lambda})\, G(\psi', \lambda'_b). \qquad (8.41)$$

Пусть теперь $b = 0$. Если λ'_b является тривиальным аддитивным характером поля K, то сумма Гаусса $G(\psi', \lambda'_b)$ обращается в 0 во всех случаях, кроме случая, когда ψ' является тривиальным характером. В последнем случае $G(\psi', \lambda'_b) = q - 1$. Следовательно, имеет смысл брать сумму в (8.41) по множеству A, состоящему из всех таких характеров ψ, для которых $\psi(\alpha) = 1$ и ψ' является тривиальным характером. Тогда

$$Z(0) = \frac{r}{q} + \frac{(q-1)r}{q(q^k-1)} \sum_{\psi \in A} \psi(\theta)\, G(\bar{\psi}, \bar{\lambda}).$$

Тривиальный мультипликативный характер дает в сумму вклад, равный -1 и, следовательно,

$$Z(0) - \frac{(q^{k-1}-1)r}{q^k - 1} = \frac{(q-1)r}{q(q^k-1)} \sum_{\psi \in A}^{*} \psi(\theta)\, G(\bar{\psi}, \bar{\lambda}),$$

где звездочка означает, что тривиальный мультипликативный характер исключен из области суммирования. В силу того, что λ является нетривиальным характером, получаем, что $|G(\bar{\psi}, \bar{\lambda})| = q^{k/2}$ для любого нетривиального ψ. Отсюда

$$\left| Z(0) - \frac{(q^{k-1}-1)r}{q^k - 1} \right| \leqslant \frac{(q-1)r}{q(q^k-1)} (|A| - 1)\, q^{k/2}. \qquad (8.42)$$

Обозначим через H наименьшую подгруппу группы F^*, содержащую α и K^*. Элемент α в циклической группе F^* имеет порядок

r; следовательно, $|H| = h$, где $h = \text{НОК}\ (r, q-1)$. Далее, $\psi \in A$ тогда и только тогда, когда $\psi(\beta) = 1$ для всех $\beta \in H$. Иными словами, A является аннулятором H в группе $(F^*)\hat{}$ (см. стр. 239). Тогда по теореме 5.6

$$|A| = \frac{|F^*|}{H} = \frac{q^k - 1}{h}. \tag{8.43}$$

Теперь неравенство (8.37) непосредственно следует из (8.42) и (8.43).

Рассмотрим случай $b \neq 0$. Вернемся к формуле (8.41) и заметим прежде всего, что аддитивный характер λ_b' является нетривиальным. Следовательно, тривиальный мультипликативный характер дает в сумму из (8.41) вклад, равный 1. Таким образом, мы можем записать

$$Z(b) - \frac{q^{k-1}r}{q^k - 1} = \frac{r}{q(q^k - 1)} \sideset{}{^*}\sum_{\psi \in J} \psi(\theta)\, G(\bar{\psi}, \bar{\lambda})\, G(\psi', \lambda_b').$$

Теперь $G(\psi', \lambda_b') = -1$, если характер ψ' является тривиальным, и $|G(\psi', \lambda_b')| = q^{1/2}$, если характер ψ' нетривиален. Отсюда следует, что

$$\left| Z(b) - \frac{q^{k-1}r}{q^k - 1} \right| \leqslant \frac{r}{q^k - 1}(|A| - 1 + (|J| - |A|)\, q^{1/2})\, q^{(k/2)-1}.$$

Так как J является аннулятором в $(F^*)\hat{}$ подгруппы группы F^*, порожденной элементом α, то по теореме 5.6 $|J| = (q^k - 1)/r$ Вместе с (8.43) это дает (8.38), что и завершает доказательство теоремы. □

Можно также получить результаты, касающиеся распределения элементов основного поля на отрезках последовательности, меньших полного периода. Пусть $s_0, s_1, \ldots$ — произвольная линейная рекуррентная последовательность над полем $\mathbb{F}_q$, r — ее минимальный период, а n_0 — предпериод. Пусть $b \in \mathbb{F}_q$ — произвольный элемент поля, $N_0 \geqslant n_0$ и $1 \leqslant N \leqslant r$. Тогда через $Z(b; N_0, N)$ обозначим число таких n, $N_0 \leqslant n \leqslant N_0 + N - 1$, для которых $s_n = b$.

8.85. Теорема. *Пусть $s_0, s_1, \ldots$ — линейная рекуррентная последовательность k-го порядка над полем $\mathbb{F}_q$, r — ее минимальный период, а n_0 — предпериод, и пусть число R выбрано так же, как и в теореме* 8.78. *Тогда для любого элемента $b \in \mathbb{F}_q$ справедливо неравенство*

$$\left| Z(b; N_0, N) - \frac{N}{q} \right| \leqslant \left(1 - \frac{1}{q}\right)\left(\frac{r}{R}\right)^{1/2} q^{k/2}\left(\frac{2}{\pi}\log r + \frac{2}{5} + \frac{N}{r}\right),$$

где $N_0 \geqslant n_0$ и $1 \leqslant N \leqslant r$.

Доказательство. Используя обозначения и метод доказательства теоремы 8.82, нетрудно получить равенство

$$Z(b;\ N_0,\ N) - \frac{N}{q} = \frac{1}{q} \sum_{\chi}^{*} \bar{\chi}(b) \sum_{n=N_0}^{N_0+N-1} \chi(s_n).$$

В силу того, что имеется ровно $q - 1$ нетривиальных аддитивных характеров поля $\mathbb{F}_q$, из теоремы 8.81 получаем

$$\left| Z(b;\ N_0,\ N) - \frac{N}{q} \right| \leqslant \frac{1}{q} \sum_{\chi}^{*} \left| \sum_{n=N_0}^{N_0+N-1} \chi(s_n) \right| \leqslant$$

$$\leqslant \left(1 - \frac{1}{q}\right) \left(\frac{r}{R}\right)^{1/2} q^{k/2} \left(\frac{2}{\pi} \log r + \frac{2}{5} + \frac{N}{r}\right). \quad \square$$

Метод доказательства теоремы 8.84 также может быть использован для исследования распределения элементов поля $\mathbb{F}_q$ на отрезках последовательности, меньших полного периода (см. упр. 8.69, 8.70 и 8.71).

Комментарии

§ 1. Теория линейных рекуррентных последовательностей имеет очень давнюю историю. В гл. 17 книги Диксона Dickson [40] она прослеживается с 1202 по 1918 г. Первоначально внимание уделялось линейным рекуррентным последовательностям целых чисел, особенно знаменитой *последовательности Фибоначчи* F_0, F_1, F_2, ... , определяемой условиями $F_0 = 0$, $F_1 = 1$ и соотношением $F_{n+2} = F_{n+1} + F_n$, $n = 0, 1, \ldots$. Позднее линейные рекуррентные последовательности над полем действительных или комплексных чисел рассматривались в основном в связи с исчислением конечных разностей. Интерес к линейным рекуррентным последовательностям над конечными полями возник после того, как линейные рекуррентные последовательности над $\mathbb{Z}$ стали рассматривать по модулю простого числа p, получая таким образом линейные рекуррентные последовательности над полем $\mathbb{F}_p$. Начиная с 50-х г. XX в., линейные рекуррентные последовательности над конечными полями нашли важное приложение в теории кодирования и в электронике ввиду их связи с переключательными схемами. Краткий обзор истории развития этого направления за период с 1918 г. можно найти в книге Selmer [3, ch. 2].

Важными классическими работами по теории линейных рекуррентных последовательностей являются работы Lucas [1] и d'Ocagne [1]. Обзор этой тематики можно также найти в книгах Lucas [2, ch. 17, 18] и Bachman [5, ch. 2]. Первый заметный вклад в теорию линейных рекуррентных последовательностей над конечными полями был сделан в статьях Mantel [1] для слу-

чая простого поля $\mathbb{F}_p$ и Scarpis [2] для общего случая $\mathbb{F}_q$. Все последующие работы вплоть до середины XX в. сконцентрированы вокруг линейных рекуррентных последовательностей над кольцами $\mathbb{Z}$ и $\mathbb{Z}/(m)$ (см. Bell [1], Carmichael [1], [2], [3], Engstrom [1], [2], Hall [1], [2], [3], [4], Ward [2], [3], [4], [7], [8], [9], [11], [12], [14], [16] и особенно фундаментальную работу Ward [5]). Кроме того, линейные рекуррентные последовательности над произвольными полями рассматривались в работе Ward [1], а линейные рекуррентные последовательности над произвольными коммутативными кольцами — в статьях Ward [13], [15]. Основополагающей работой по современной теории линейных рекуррентных последовательностей над конечными полями является работа Zierler [4]. Обсуждение этой теории можно найти в книгах Birkhoff, Bartee [1, ch. 13], Dornhoff, Hohn [1, ch. 8], Gill [2], Golomb, [4], Lüneburg, [2], Peterson, Weldon [1], а также в лекциях Selmer [3] и в обзорной статье Fillmore, Marx [1]. По поводу более подробной информации о последовательностях Фибоначчи см. Bachmann [5, ch. 2], Jarden [1], Knuth [2, ch. 1] и Воробьев [1], а также журнал «Fibonacci Quarterly». Линейные рекуррентные последовательности действительных или комплексных чисел исследовались, в частности, в книгах Jordan Ch. [1, ch. 11], Milne-Thomson [1, ch. 13], Montel [1], Nörlund [1, ch. 10], Гельфонд [1, гл. 5] и Маркушевич [1].

Описание технической реализации регистров сдвига с обратной связью и составляющих их элементов приводится в работе McCluskey [1]. В статье Roth [1] обсуждается эффективное построение регистров сдвига с обратной связью с полем $\mathbb{F}_2$ в качестве основного поля. Связь между регистрами сдвига с обратной связью и линейными рекуррентными последовательностями подчеркивается в работах Golomb [4], Peterson, Weldon [1] и Selmer [3]. Обсуждение работы регистра сдвига с обратной связью с точки зрения теории переключательных схем и теории конечных автоматов можно найти в книгах Booth [1, ch. 8], Gill [2], Golomb [4, ch. 2], Zadeh, Polak [1, ch. 2], а с еще более общей точки зрения — в § 5 гл. 9 настоящей монографии.

Теорема 8.7 в сущности была получена в работе Mantel [1]. Теорема 8.11 является частным случаем результата, доказанного в статье Ward [15]. Матрица A из (8.3), являющаяся сопровождающей матрицей характеристического многочлена рекуррентной последовательности, была введена в работе Brenner [1]; там же можно найти доказательство теоремы 8.13. Позднее матричные методы начали интенсивно использоваться при проведении исследований в этой области (см. Golomb [1], Birdsall, Ristenblatt [1], Elspas [1], Friedland [1], Stern, Friedland [1] и Mendelsohn [1]). Эти методы имеют то преимущество, что они могут быть также применены к линейным рекуррентным последовательно-

стям над более общими алгебраическими структурами (см., например, Niederreiter [6]). Вычислительные аспекты матричных методов обсуждались в работах Kamal, Singh, Puri, Nanda [1] и Latawiec [1].

Доказательства формулы для порядка группы $GL(k, \mathbb{F}_q)$ можно найти, например, в книгах Artin [7, ch. 4], Carmichael [4, ch. 10], Dickson [7, part II, ch. 1] или Newman [1, ch. 7]. В них можно также обнаружить формулы для порядков других матричных групп над полем $\mathbb{F}_q$, таких, как специальные линейные группы, ортогональные группы или симплектические группы. Теоретико-групповой аспект этих матричных групп обсуждается, например, в работах Artin [5], [6], Carmichael [4, ch. 10], Chevalley [2], Dickson [7, part II], Dieudonné [2] и Dixon [1]. Последние исследования по теории представлений таких групп можно найти в статье Srinivasan [1]. Формула для порядка группы $GL(k, \mathbb{F}_q)$ является частным случаем формулы для числа $m \times n$-матриц ранга r над полем $\mathbb{F}_q$, которая имеет вид

$$q^{(r^2-r)/2} \prod_{i=0}^{r-1} (q^{m-i} - 1)(q^{n-i} - 1)(q^{i+1} - 1)^{-1},$$

где $1 \leqslant r \leqslant \min(m, n)$. Этот результат для случая простого q был получен в работе Landsberg [1]. Доказательства этой формулы можно найти также в работах Arghiriade, Peterfi [1], Boroş [1], Fisher, Alexander [1]. В статье Porter, Riveland [1] аналогичная формула доказана для случая, когда задано фиксированное число $s \leqslant r$ линейно независимых строк в матрице. В работе Klein [3] рассматривается число $m \times n$-матриц над полем $\mathbb{F}_p$, для которых все миноры порядка $\min(m, n)$ или все миноры порядка не более $\min(m, n)$ являются ненулевыми. Ли в работе Lee A. [1] показал, что не существует матрицы размера $(q-1) \times q$ над полем $\mathbb{F}_q$, в которой все миноры порядков $q-1$ и $q-2$ являются ненулевыми. В работе Carlitz, Hodges [4] получено число прямоугольных матриц заданного ранга, у которых ранги подматриц имеют предписанные заранее значения, а в работах Brawley, Carlitz [1] и Fisher, Alexander [1] получено число таких матриц с предписанными значениями сумм по строкам и столбцам. Другие перечислительные задачи для прямоугольных матриц над полем $\mathbb{F}_q$ изучались в работах Carlitz, Hodges [2], Daykin [2], Fulton J. D. [8], [10], Hodges [7] и Kim [1]. Для квадратных матриц заданного порядка над полем $\mathbb{F}_q$ рассматривались более специальные перечислительные задачи. Так, в работе Buckhiester [1] определено число таких матриц с заданными значениями ранга и следа (см. также статью Johnson, Porter, Varineau [1], где рассматривается случай полного ранга). Райнер (Reiner [1]) и Герстенхабер (Gerstenhaber [1]) нашли число матриц, имеющих заданный характе-

ристический многочлен, а Карлиц и Ходжес (Carlitz, Hodges [3]) получили формулу для числа простых матриц. В статьях Fine, Herstein [1] и Gerstenhaber [1] доказано, что имеется в точности q^{n^2-n} нильпотентных $n \times n$-матриц над полем $\mathbb{F}_q$, а в статье Bollman, Ramirez [1] получено число нильпотентных матриц над $\mathbb{Z}/(m)$ заданного порядка и ранга. Число циркулянтных матриц с заданным рангом подсчитано в работе Berlekamp [2], а в статьях Carlitz [51], [54], Carlitz, Hodges [1] получены соответственно число кососимметрических, симметрических и эрмитовых матриц заданного ранга. Дальнейшее развитие этого направления проведено в работе MacWilliams [3]. В работе Brawley, Carlitz [1] изучались те же вопросы с дополнительными ограничениями на суммы по строкам и столбцам. Приложения полученных результатов можно найти в статье MacDougall [1]. В статье Feit, Fine [1] определено число упорядоченных пар коммутирующих $n \times n$-матриц над полем $\mathbb{F}_q$, аналогичные вопросы рассматривались Карлицом (Carlitz [92]). В работе Kung [1] получено число невырожденных матриц, коммутирующих с данной блочно-диагональной матрицей. Эквивалентность и классы подобия для матриц изучались в работах Brawley [1], Carlitz [104], Carlitz, Hodges [3] и Gow [1]. В статье Brawley, Mullen [1] найдено число диагонализируемых матриц, имеющих заданное число различных собственных значений. Для фиксированной квадратной матрицы A над полем $\mathbb{F}_q$ Дайкин (Daykin [1]) определил число различных матриц вида $f(A)$, имеющих заданный ранг, когда f пробегает $\mathbb{F}_q[x]$. По поводу результатов о числе решений матричных уравнений мы отсылаем читателя к комментариям к § 2 гл. 6 настоящей монографии. С этими перечислительными задачами о матрицах непосредственно связана задача перечисления подпространств векторных пространств над полем $\mathbb{F}_q$. В этой связи Диксон (Dickson [7, part I, ch. 4]) и Мур (Moore [4]) показали, что число r-мерных подпространств n-мерного векторного пространства над полем $\mathbb{F}_q$ задается формулой

$$\prod_{i=0}^{r-1} (q^{n-i} - 1)(q^{r-i} - 1)^{-1}, \quad \text{где} \quad 1 \leqslant r \leqslant n.$$

Как определил Нивен (Niven [1]), наименьшее общее кратное порядков всех элементов группы $GL(k, \mathbb{F}_q)$ равно $p^e M$, где p — характеристика поля $\mathbb{F}_q$, e — наименьшее целое число, для которого $p^e \geqslant k$, а M — наименьшее общее кратное чисел $q - 1$, $q^2 - 1$, ..., $q^k - 1$. Эти результаты были дополнены и обобщены в работе Marshall [1]. Так, утверждение о том, что порядок матрицы A в $GL(k, \mathbb{F}_q)$ делит

$$q^{(k^2-k)/2}(q - 1)(q^2 - 1) \ \ldots \ (q^k - 1),$$

можно усилить до утверждения, что этот порядок делит p^eM. Аналог результата Нивена для $GL(k, Z/(m))$ был получен в работах Davis [1] и Maxfield [1]. Кроме того, Нивен в той же работе Niven [1] получил алгоритм для определения порядка элемента из $GL(k, \mathbb{F}_q)$. Исследованию порядков матриц посвящены также работы Bollman [1], Dai [1], Fillmore, Marx [1], Gaiu [1] и Lüneburg [2, ch. 32, 33].

Теория линейных рекуррентных последовательностей над конечными полями помимо применения к анализу и синтезу регистров сдвига с обратной связью имеет еще одно важное применение, а именно в теории кодирования, особенно в теории циклических кодов (см. § 2 гл. 9 настоящей монографии). Первыми работами по связи линейных рекуррентных последовательностей и регистров сдвига с обратной связью с теорией кодирования были работы Abramson [1], Green, San Soucie [1], Huffman [1], [2], Kasami [1], Mattson, Solomon [1], Peterson [1], Prange [1], Stern, Friedland [1], Yale [1], Zetterberg [1] и Zierler [1], [3]. См. также Massey [3], Mykkeltveit [1], Zierler [5] и Габидулин [1], а кроме того, монографии Ash [1, ch. 5], Lin [2, ch. 4] и Peterson, Weldon [1]. Приложения к вычислениям в $\mathbb{F}_q$ и $\mathbb{F}_q[x]$ рассматривались в работах Bartee, Schneider [1], Berlekamp [4, ch. 2], Bhanu Murthy, Sampath [1], Gill [2, ch. 6], Tanaka, Kasahara, Tezuka, Kasahara [1] и Willett [6]. Алгоритм Миньотта (Mignotte [1]) для определения степени поля разложения многочлена над полем $\mathbb{F}_q$ также основывается на свойствах линейных рекуррентных последовательностей. Другие связи линейных рекуррентных последовательностей с разложением многочленов на множители можно найти в статье Willett [5]. Свойства линейных рекуррентных последовательностей 2-го порядка над конечными простыми полями применялись в работе Niederreiter, Robinson [1] для анализа конечных луп Бола. Применения линейных рекуррентных последовательностей над полем $\mathbb{F}_2$ в криптографии обсуждаются в работе Beker, Piper [1]. Слоэн (Sloane [2]) упоминает о связях между криптографией и регистрами сдвига с обратной связью. Обзор практических приложений линейных рекуррентных последовательностей дается в работах Golomb [3, ch. 1], [4, ch. 1]. О некоторых специальных приложениях последовательностей максимального периода будет упоминаться ниже, в комментариях к § 2 настоящей главы.

Линейные рекуррентные последовательности можно рассматривать и над более общими алгебраическими структурами. Уорд (Ward [1]) изучал рекуррентные последовательности над произвольными полями, а позднее в работах Ward [13], [15] он начал изучать линейные рекуррентные последовательности над коммутативными кольцами. Дальнейшие исследования по этим направлениям можно найти в работах Dade, Robinson, Taussky, Ward

[1], de Carli [1], Duparc [1], Robinson D. W. [4] и Shiue, Sheu [1]. Линейные рекуррентные последовательности над модулями изучались в статьях Nathanson [5] и Niederreiter [5], [6]. Линейные рекуррентные последовательности векторов рассматривались в работах Bollman [1], Daykin [4], Selmer [3, ch. 7], Vince [2]. Свойства периодичности последовательностей над $\mathbb{F}_q$ и $Z/(m)$, удовлетворяющих рекуррентным соотношениям вида

$$s_{n+k} = a_{k-1}(n)\, s_{n+k-1} + a_{k-2}(n)\, s_{n+k-2} + \cdots + a_0(n)\, s_n,$$

где коэффициенты $a_i(n)$ периодичны по n, изучали Нечаев [1], [3] и Полосуев [1]. Свойства периодичности, получаемые из рекуррентных соотношений других типов, были получены Дюпарком (Duparc [2]). Линейные рекуррентные последовательности над полем $\mathbb{F}_q$ представляют собой одномерный случай в теории линейных рекуррентных массивов над $\mathbb{F}_q$. Эта теория была развита в работах MacWilliams, Sloane [1], Nomura, Fukuda [1], Nomura, Miyakawa, Imai, Fukuda [1], [2], [3], Sakata [1], [2].

§ 2. Особая роль, которую играет импульсная функция, была отмечена еще в классической литературе по линейным рекуррентным последовательностям (см., например, Lucas [2, ch. 17] и d'Ocagne [1]). Теоремы 8.16 и 8.19 были получены Уордом (Ward [5]), а теорема 8.17 была доказана для простого q Спейсером (Speiser [1]). Другие результаты, имеющие отношение к импульсным функциям, можно найти в работах Ajtai [1], Kiss, Bui Minh Phong [1], Robinson D. W. [2] и Selmer [3, ch. 3, 4]. Отметим в связи с теоремой 8.19, что Грот (Groth [1]) использовал число линейно независимых векторов состояний для введения меры сложности на последовательностях над полем $\mathbb{F}_2$.

Понятие характеристического многочлена и основная идея теоремы 8.21 восходят еще к Лагранжу (Lagrange [1], [5]), который получил аналогичную теорему для линейных рекуррентных последовательностей над полем действительных чисел. Результат, приведенный в замечании 8.23, хорошо известен для линейных рекуррентных последовательностей над полем действительных или комплексных чисел (см. Jordan Ch. [1, ch. 11], Milne-Thomson [1, ch. 13] и Маркушевич [1]). Нетрудно заметить, что этот результат может быть перенесен на случай конечных полей при наличии ограничений на кратность корней характеристического многочлена. Но и без этих ограничений все же имеются способы получения представления в явном виде для членов последовательности (см. Fillmore, Marx [1]). Положим в теореме 8.21 все β_j равными 1. Получаемая при этом последовательность привлекала внимание исследователей (см. Selmer [2], [3, ch. 5], Ward [3], [4], Wegner [2], [4]). Теорему 8.24 можно найти у ван Линта (van Lint [1, ch. 3]). Более сложная формула справедлива для случая, когда характеристический многочлен не имеет крат-

ных корней (см. Niederreiter [8] и упр. 8.41). Аракелов и Варшамов [1] показали, что n-й член однородной рекуррентной последовательности k-го порядка над полем $\mathbb{F}_q$ может быть представлен в виде

$$s_n = g_0(n)\, s_0 + \cdots + g_{k-1}(n)\, s_{k-1},$$

где $g_i(n) \in \mathbb{F}_q$. Здесь же изучались выражения для $g_i(n)$. Алгоритмы для вычисления s_n при больших n обсуждаются в работах Gries, Levin [1], Miller, Brown [1], Pettorossi [1], Pettorossi, Burstall [1], Selmer [3, ch. 5], Urbanek [1], Wilson, Shortt [1]. Теорема 8.25 по существу получена Уордом (Ward [5]). Результаты из линейной алгебры, использованные при доказательстве леммы 8.26, а именно то, что f является минимальным многочленом соответствующей сопровождающей матрицы, можно найти, например, в книге Hoffman, Kunze [1, ch. 7]. Лемма 8.26 и теорема 8.27 непосредственно приводят к результатам о порядке сопровождающих матриц как элементов группы $GL(k, \mathbb{F}_q)$, таким, например, как верхняя граница $q^k - 1$ для порядка таких матриц, полученная Гуптой (Gupta [1]). Линейные рекуррентные последовательности, характеристические многочлены которых являются трехчленами, изучались в работах Goldstein, Zierler [1], Lunnon, Pleasants, Stephens [1], Young [1] и Аракелов, Тененгольц [1]. Кумари (Kumari [1]) рассматривал другой специальный класс линейных рекуррентных последовательностей.

Первое детальное изучение последовательностей максимального периода (называемых также *m-последовательностями* или (в электронике) *псевдослучайными последовательностями* (pseudo-noise sequences)) было предпринято Голомбом (Golomb [1]), но там эти исследования ограничивались случаем последовательностей над полем $\mathbb{F}_2$ (см. также Golomb [2], [4, ch. 3, 4, 6], Golomb, Welsh [1]). Более глубокое исследование таких последовательностей над произвольным полем $\mathbb{F}_q$ можно найти в работах Zierler [4], Selmer [3]. В статье Daykin, Dresel, Hilton [1] рассматривались последовательности 2-го порядка, имеющие максимальный период. Ряд работ был посвящен эффективным методам построения последовательностей максимального периода (см. Ball, Spittle, Liu [1], Eier, Malleck [1], Harvey [1], Lempel [1], Lempel, Eastman [1], Möhrmann [1], [2], Scholefield [1], Surböck, Weinrichter [1]). Различные обобщения последовательностей максимального периода встречаются в работах MacWilliams, Sloane [1], Nomura, Miyakawa, Imai, Fukuda [1], [3], Sakata [1] и Нечаев [1].

Построение последовательностей де Брейна с использованием последовательностей максимального периода (см. упр. 8.19) было предложено Мантелем (Mantel [1]), см. также работу Rees [1]. Существование (m, k)-последовательностей де Брейна для произвольных параметров m и k было впервые доказано Мартином

(Martin [1]), а частный случай $m = 2$ был изучен ранее в работе Flye Sainte-Marie [1]. Последовательности де Брейна получили свое название после появления работы de Bruijn [1]. Другие результаты о последовательностях де Брейна можно найти, например, в работах Arazi [2], Fredricksen [1], Fredricksen, Kessler [1], Golomb [4, ch. 6], Golomb, Welch [1], Good [1], а также в обзорной статье Fredricksen [2]. Связанное с этим понятие кодового кольца изучали Радченко и Филиппов [1], [2]. Другое приложение к комбинаторике последовательности максимального периода находят в теории разностных множеств (см. определение 9.75). Эти вопросы освещаются в работах Butson [1], Golomb [3, ch. 4]. Laxton, Anderson [1], Selmer [3, ch. 6]. Работа Butson [1] содержит также приложение к построению матриц Адамара (см. определение 9.86). Этой же тематике посвящена и работа MacWilliams, Sloane [1]. В статье Bartee, Schneider [1] векторы состояний последовательности k-го порядка над полем $\mathbb{F}_q$, имеющей максимальный период, вместе с нулевым вектором использованы для описания элементов поля $\mathbb{F}_{q^k}$ (см. также MacWilliams, Sloane [1], Mönnig [1]). Голомб (Golomb [1]) впервые начал использовать последовательности максимального периода в качестве генераторов псевдо-случайных чисел (см. также Golomb [3, ch. 1], [4, ch. 3], Knuth [3, ch. 3], Niederreiter [7], [10], [12], [13], Tausworthe [1] и Павлов, Походзей [1]. Некоторые приложения последовательностей максимального периода к теории кодирования встречаются в работах Green, San Soucie [1], MacWilliams, Sloane [1], Weng [1], Yale [1], Zierler [3] и Грушко [1]. По поводу других приложений последовательностей максимального периода отсылаем к работам Bartee, Schneider [1], Golomb [3, ch. 2], Laxton, Anderson [1], Mohanty [1], Nadler, Sengupta [1] и Сагалович [1].

§ 3. Использование производящих функций в теории линейных рекуррентных последовательностей над конечными полями началось с работ Голомба (Golomb [1]) и Хаффмэна (Huffman [1], [2]). Затем этот подход более полно использовался в работах Friedland [1], Richalet [1], Stern, Friedland [1], Zierler [4] и Назаров [1]; см. также книги Lüneburg [3, ch. 24, 25] и Selmer [3, ch. 3]. Формальные степенные ряды над полем $\mathbb{F}_2$, представляющие «почти периодические» последовательности, изучались в работе Baum, Herzberg, Lomonaco, Sweet [1]. Более общие последовательности, имеющие в качестве производящих функций алгебраические функции над $\mathbb{F}_q$, появились в работе Furstenberg [1].

Другой подход к линейным рекуррентным последовательностям над полем $\mathbb{F}_q$ основывается на теории идеалов — см. работы Hall [3], Peterson [1], Laksov [1] и Ward [5]. Обзоры по этой

тематике можно найти в книгах Peterson, Weldon [1, ch. 7] и Selmer [3, ch. 3]. В работах Hemmati, Costello [1] и Ikai, Kosako, Kojima [1], [2] применяется комбинированный подход с использованием теории производящих функций и теории идеалов в кольце $\mathbb{F}_q[x]$.

§ 4. Все основные результаты о минимальных многочленах можно найти в работе Zierler [4]. Теорему 8.44 можно найти также в статье Friedland, Stern [1]. Наше доказательство теоремы 8.42 имеет то преимущество, что оно является конструктивным (см. также Willett [1]). Набросок более короткого, но неконструктивного доказательства приводится в упр. 8.25 (см. также Zierler [4]). Другие подходы к понятию минимального многочлена можно найти в работах Laksov [1] и Selmer [3, ch. 4]. Теорема 8.44 представляет собой важное связующее звено с теорией порядков многочленов (см. § 1 гл. 3 настоящей монографии). Теорема 8.51 очевидным образом связана с детерминантным критерием из § 6 настоящей главы, где также содержится и другой метод нахождения минимальных многочленов.

Фитцпатрик (Fitzpatrick [1]) исследовал проблему получения линейной рекуррентной последовательности над полем $\mathbb{F}_2$ заданного заранее периода с помощью рекуррентного соотношения минимально возможного порядка. Много работ было посвящено определению минимального периода последовательности Фибоначчи над $\mathbb{F}_p$ или $Z/(m)$ (см. Barner [1], Catlin [1], Fulton, Morris [1], Halton [1], Kluyver [1], Mamangakis [1], Robinson D. W. [1], Stanley [1], [2], Täcklind [1], Vince [1], Vinson [1], Wall [1]), а также более общих последовательностей 2-го порядка над $\mathbb{F}_p$ или $Z/(m)$ (см. Bundschuh, Shiue [2], Kiss, Bui Minh Phong [1], Robinson D. W. [3], Smith, Hoggatt [1], Sommer [2], [3], [4], Wyler [1], Yalavigi [1], [2], Yalavigi, Krishna [1]). Исследования, касающиеся минимальных периодов линейных рекуррентных последовательностей высших порядков над кольцами вычетов, проводились в работах Carmichael [2], [3], Engstrom [1], [2], Hall [3], Ward [2], [5].

§ 5. Основополагающей работой по структуре векторных пространств $S(f(x))$ является работа Zierler [4], где получены теоремы 8.53, 8.54, 8.55 и 8.56, а также результаты о минимальном периоде суммарных последовательностей. Пространства $S(f(x))$ изучались также в работах Fillmore, Marx [1] и Selmer [3, ch. 3, 4]. Операция бинарного дополнения изучалась в книге Selmer [3, ch. 6]. В статье Kumar, Kumari [1] рассматривался эффект перехода к бинарному дополнению только в одном или в двух местах на длине одного периода. Теорема 8.63 была получена в работе Ward [5] для случая конечных простых полей. Переход к произвольному $f(x)$, описанный вслед за теоремой 8.63 (ср. с примером 8.64), можно также получить с помощью символического метода

из § 5 следующей главы, который пригоден и для более общего случая. Распределение минимальных периодов в $S(f(x))$, называемое также *цикловой структурой* пространства $S(f(x))$, обсуждается в работах Fillmore, Marx [1], Selmer [3, ch. 4] и Zierler [4]. Вопрос совпадения, возникающий в этом контексте, был решен в работе Duvall, Kibler [1]. В статье Ward [9] изучалось распределение минимальных периодов для случая линейных рекуррентных соотношений над $Z/(m)$. Вопрос, какие значения может принимать минимальный период линнейной рекуррентной последовательности k-го порядка над полем $\mathbb{F}_q$ при фиксированных k и q, изучался в книге Lüneburg [2, ch. 32, 33].

Тот факт, что в результате почленного умножения линейных рекуррентных последовательностей получается снова линейная рекуррентная последовательность, был отмечен еще в статье l'Ocagne [1], где исследовались последовательности действительных чисел и был доказан более слабый вариант теоремы 8.67, а именно, что для этого случая

$$S(f_1(x)) \ \ldots \ S(f_h(x)) \subseteq S(f_1(x) \vee \ \ldots \ \vee f_h(x)).$$

Для конечных полей операция почленного умножения последовательностей впервые изучалась в книге Selmer [3, ch. 4]. Более тщательное исследование этого вопроса было проделано в работе Zierler, Mills [1], где были получены теоремы 8.67 и 8.72. В этой же работе было показано, как использовать полученные результаты для нахождения многочлена $g(x)$ из теоремы 8.65 в общем случае. Взаимосвязь между множествами $S(f(x))$ и $S((f(x))^k)$ изучалась в статье Fillmore, Marx [1]. Некоторые элементарные замечания относительно операции почленного умножения последовательностей содержатся в работе Brousseau [1]. В статье Furstenberg [1] получен аналог следствия 8.66 для более общих типов последовательностей над полем $\mathbb{F}_q$.

Операция над последовательностями, называемая *децимацией* (decimation) или *разрядкой*, была предложена Голомбом (Golomb [1]) и определяется следующим образом: если σ — последовательность элементов $s_0, s_1, s_2, \ldots$ из поля $\mathbb{F}_q$, а $d \in \mathbb{N}$ — натуральное число, то разреженная последовательность $\sigma^{(d)}$ состоит из членов $s_0, s_d, s_{2d}, \ldots$, т. е. $\sigma^{(d)}$ получается путем выбора каждого d-го члена исходной последовательности σ, начиная с s_0. Частные случаи этой операции появлялись в работах Hall [3] и Ward [3]. Подробное исследование этой операции было проделано в работах Golomb [2] и Zierler [4]. Основное внимание уделялось разрядке последовательностей максимального периода ввиду того, что все последовательности k-го порядка над полем $\mathbb{F}_q$, имеющие максимальный период, могут быть получеиы (с точностью до сдвига) из одной последовательности такого типа с помощью соответствующей разрядки (см. Golomb [2], Selmer [3, ch. 5]). Дальней-

шее исследование свойств этой операции проводилось в работах Arazi [1], Duvall, Mortick [1], Golomb [4, ch. 3, 4], Selmer [3, ch. 5], Surböck, Weinrichter [1], Willett [2] и Павлов, Походзей [1]. Если $f(x)$ — нормированный многочлен, не являющийся константой, над полем $\mathbb{F}_q$ и $f(0) \neq 0$, то последовательность $\sigma \in S(f(x))$ называется *характеристической последовательностью* для $f(x)$, если $\sigma^{(q)} = \sigma$. Это понятие было впервые введено и исследовано в работе Gold [1]. В работе Willett [4] приведены таблицы характеристических последовательностей для примитивных многочленов над полем $\mathbb{F}_2$. В статье Willett [5] доказано, что множество характеристических последовательностей для $f(x)$ образует подпространство пространства $S(f(x))$ и размерность этого подпространства равняется числу различных нормированных неприводимых делителей многочлена $f(x)$.

В работе Goka [1] рассматривалась операция перехода от последовательности $s_0, s_1, s_2, \ldots$ над полем $\mathbb{F}_2$ к последовательности $s_0 + s_1, s_1 + s_2, s_2 + s_3, \ldots$ сумм соседних членов. Эта операция под названием «взятие производной» изучалась и в статье Nathanson [1]. Обратная к ней операция изучалась в работах Nathanson [1], [2], а различные ее обобщения — в работах Nathanson [3], [5]. Способы разложения периодических последовательностей над полем $\mathbb{F}_2$ рассматривались в статьях Hwang, Sheng, Hsieh [1] и Weng [1].

§ 6. Подробную сводку соотношений между линейными рекуррентными последовательностями и ганкелевыми определителями можно найти в книге Pólya, Szegö [1, sec. VII, prob. 17—29]. Теорема 8.75 была впервые получена Кронекером (Kronecker [4]) для последовательностей над полем действительных чисел, но его доказательство справедливо для любого поля. Другие варианты теоремы Кронекера можно найти в работах d'Ocagne [1], Maillet [1] и Perrin [1]. Обсуждение этих детерминантных критериев можно также найти в работах Lüneburg [2, ch. 26], Selmer [3, ch. 4] и Willett [3].

Алгоритм Берлекэмпа—Месси был получен в работах Берлекэмпа (Berlekamp [4]) и Месси (Massey [4]) в связи с одной задачей из теории кодирования (см. § 2 следующей главы и комментарии к нему в конце главы). Бартон (Burton [1]) упростил этот алгоритм для случая поля $\mathbb{F}_q$ при четном q. В статье Berlekamp, Fredricksen, Proto [1] отмечено, что в то время как любых $2k$ последовательных членов однородной линейной рекуррентной последовательности над полем $\mathbb{F}_q$, имеющей минимальный многочлен степени $k \geqslant 1$, будет достаточно для определения минимального многочлена, никакого числа членов, меньшего $2k$, не будет достаточно для его определения при условии, что $q \neq 2$. Если же $q = 2$, то $2k - 1$ членов иногда может быть достаточно для определения минимального многочлена, но $2k - 2$ никогда не

будет достаточно. Дальнейшие замечания по этому вопросу, относящиеся к случаю $q = 2$, можно найти в работе Dillon, Morris [1]. Густавсон (Gustavson [1]) оценил среднее число сложений и умножений, требуемое алгоритмом Берлекэмпа—Месси. Обсуждение этого алгоритма можно также найти в книге Dornhoff, Hohn [1, ch. 9]. Еще ряд замечаний и ссылок по поводу этого же алгоритма можно найти в комментариях к § 2 следующей главы.

§ 7. Первой работой, посвященной распределению элементов основного поля в рекуррентной последовательности, является работа Scarpis [2], в которой изучается $Z(0)$ для линейных рекуррентных последовательностей 2-го порядка над полем $\mathbb{F}_p$ с нечетным q. Позднее в статье Ward [3] изучалось распределение элементов в линейных рекуррентных последовательностях 3-го порядка над полем $\mathbb{F}_p$. Случаи последовательностей более высокого порядка рассматривались в работах Hall [3], [4]. Мощный метод тригонометрических сумм был впервые применен для исследования этих вопросов Коробовым [1]. Теоремы 8.78 и 8.81 являются частными случаями результатов Нидеррайтера (Niederreiter [5], [6]). Оценку (8.31) в большинстве случаев можно улучшить (см. упр. 8.66). Оценка, полученная в теореме 8.81, оказывается неулучшаемой (см. Niederreiter [5]). Другими работами по тригонометрическим суммам такого вида являются статьи Niederreiter [7], [8] и Нечаев [5], [6]. Случай более общих рекуррентных соотношений рассматривался в работах Niederreiter [11] и Нечаев [2].

Простая формула для $Z(b)$ в случае последовательности максимального периода была впервые получена в работе Golomb [1] для последовательностей над полем $\mathbb{F}_2$. Теорема 8.82 доказана в статье Niederreiter [6]. Оценка такого типа была получена раньше комбинаторными методами в работе Hall [4] для случая однородной линейной рекуррентной последовательности k-го порядка над полем $\mathbb{F}_p$ с неприводимым характеристическим многочленом. Еще раньше Холл (Hall [3]) показал, что если в этом случае минимальный период превосходит величину $p^{k/2}$, то в последовательности обязан встретиться элемент 0. Селмер (Selmer [3, ch. 5]) получил аналог результатов Холла для случая, когда $q = 2$ и характеристический многочлен является произведением двух различных неприводимых многочленов над полем $\mathbb{F}_2$. Теорема 8.84 доказана в работе McEliece [5]. Распространение этого метода на случай, когда минимальный многочлен не имеет кратных сомножителей, можно найти в работе Niederreiter [8]. Результат теоремы 8.85 о распределенни элементов поля на отрезках рекуррентных последовательностей длины, меньшей периода, был получен в работе Niederreiter [6]. Там же было показано, что эта оценка неулучшаема. Распределение элементов, принадлежащих данному подмножеству поля $\mathbb{F}_q$ (например, принадлежащих множеству

примитивных элементов поля $\mathbb{F}_q$), в линейных рекуррентных последовательностях над полем $\mathbb{F}_q$ рассматривалось в следующих работах: Niederreiter [6], Коробов [1], Нечаев [4], Нечаев, Степанова [1] и Шпарлинский [1]. Аналогичные вопросы для последовательностей, удовлетворяющих более общим рекуррентным соотношениям, изучались Нечаевым и Полосуевым [1]. Многие результаты из этой работы могут быть перенесены на случай линейных рекуррентных последовательностей над кольцом $Z/(m)$ (см. Niederreiter [6], Нечаев [4]).

Голомб (Golomb [9]) рассматривал последовательности над полем $\mathbb{F}_2$ с периодом (не обязательно минимальным), равным $2^k - 1$, в которых число появлений 0 и 1 такое же, как в минимальном периоде последовательностей k-го порядка, имеющих максимальный период. В статье Hemmati, Costello [1] построены линейные рекуррентные последовательности над полем $\mathbb{F}_q$, для которых $Z(0) = 0$. Макэлайс (McEliece [4]) получил значения для $Z(b)$ по различным модулям, равным степеням характеристики поля $\mathbb{F}_q$. Исследование распределения элементов в линейных рекуррентных последовательностях небольших порядков было проделано в работах Scarpis [2], Ward [3], Hall [2], а также в появившихся позднее работах Bloom [1], Bruckner [1], Burr [1], Shah [1], Zeckendorf [1]. Некоторые из этих работ охватывают случай последовательностей над кольцом $Z/(m)$. Результаты о свойствах распределения элементов поля в линейных рекуррентных последовательностях находят применение в теории кодирования (см. McEliece [5], Niederreiter [8]), а также при получении псевдослучайных чисел (см., например, Golomb [1], [4, ch. 3], Niederreiter [7], [10]).

Линейные рекуррентные последовательности над полем $\mathbb{F}_q$, для которых $Z(b)$ имеет одно и то же значение для всех $b \in \mathbb{F}_q$, привлекают особое внимание. Последовательность с таким свойством называется *равномерно распределенной* (uniformly distributed, equidistributed) над $\mathbb{F}_q$ согласно определению, приведенному впервые в работе Gotusso [1] (см. также Kuipers, Niederreiter [1, ch. 5]. Изучение равномерно распределенных линейных рекуррентных последовательностей было начато в работах Kuipers, Shiue [1], [2], [3], [4]. В них рассматривался случай последовательностей 2-го порядка над конечными простыми полями или над кольцами вычетов $Z/(m)$. В частности, последовательность Фибоначчи является равномерно распределенной над $Z/(m)$ тогда и только тогда, когда m — степень числа 5 (по поводу доказательства необходимости см. Kuipers, Shiue [4], а достаточности — Niederreiter [4]). Равномерно распределенные линейные рекуррентные последовательности 2-го порядка над кольцом $Z/(m)$ изучались в работе Nathanson [4] для случая простого числа m, в работе Bundschuh, Shiue [1] для случая m, равного степени

простого числа (см. также Webb, Long [1]), а также в работе Bumby [1] для случая произвольного m. С этими исследованиями также связаны статьи Bundschuh [1], Cavior [7], Shiue [1], Shiue, Hu [1]. Равномерно распределенные линейные рекуррентные последовательности 2-го и 3-го порядков над полем $\mathbb{F}_q$ исследовались в работе Niederreiter, Shiue [1], а последовательности 4-го порядка — в работах Niederreiter, Shiue [1], [2]. Найт и Уэбб (Knight, Webb [1]) изучали равномерно распределенные линейные рекуррентные последовательности 3-го порядка над кольцом $Z/(m)$. В статье Niederreiter, Shiue [1] показано, что если линейная рекуррентная последовательность произвольного порядка является равномерно распределенной последовательностью над полем $\mathbb{F}_q$, то ее минимальный многочлен обязан иметь по меньшей мере один кратный корень, отличный от 0. В этой же работе изучались последовательности, минимальные многочлены которых разлагаются на множители некоторым специальным образом. Результаты, касающиеся равномерно распределенных линейных рекуррентных последовательностей произвольного порядка над кольцом $Z/(m)$, можно найти в работах Kuipers [3], Niederreiter [11], Rieger [1], [2], [3].

Вопрос о частоте появления того или иного элемента поля в линейной рекуррентной последовательности можно обобщить следующим образом: какова частота появления того или иного блока элементов среди блоков, составленных из стоящих подряд членов данной последовательности. Для последовательностей k-го порядка над полем $\mathbb{F}_q$, имеющих максимальный период, число появлений данного блока длины $l \leqslant k$ на отрезке последовательности длины, равной полному периоду, может быть определено непосредственно с помощью прямых комбинаторных подсчетов (см. Golomb [1] для случая $q = 2$ и Zierler [4] для общего случая). Дальнейшие результаты, касающиеся распределения блоков, составленных из элементов основного поля, в линейных рекуррентных последовательностях, можно найти в работах Feng [1], Fredricsson [1], Jordan, Wood [1], Laksov [1], Lindholm [1], Selmer [3, ch. 5], Zierler [4]. Связь с псевдослучайными числами, полученными с помощью линнейных рекуррентных соотношений, изучается в работах Niederreiter [9], [12], [13]. С этой же тематикой связан и вопрос о корреляционных функциях последовательностей, нашедших важное применение в исследованиях по электронике. Если $s_0, s_1, \ldots$ и $t_0, t_1, \ldots$ — две последовательности над полем $\mathbb{F}_q$, имеющие период r, а χ — нетривиальный аддитивный характер $\mathbb{F}_q$, то тогда соответствующая *кросс-корреляционная функция* $C(h)$ определяется формулой

$$C(h) = \sum_{n=0}^{r-1} \chi(s_n)\,\bar{\chi}(t_{n+h}),$$

где $h = 0, 1, \ldots, r-1$, а $\bar{\chi}$ означает сопряженный характер (см. § 1 гл. 5 настоящей монографии). Если последовательности $s_0, s_1, \ldots$ и $t_0, t_1, \ldots$ совпадают, то мы говорим об *автокорреляционной функции*. Для последовательностей максимального периода над полем $\mathbb{F}_2$ автокорреляционная функция изучалась в работе Golomb [1]. На случай произвольного поля этот результат распространил Цирлер (Zierler [4]). Кросс-корреляционная функция для двух последовательностей максимального периода над полем $\mathbb{F}_2$ рассматривалась в статье Golomb [2]. Другие результаты о корреляционных функциях можно найти в работах Feng [1], Gold [2], [3], Golomb [4, ch. 3, 4, 6], [5], Golomb, Welch [1], Helleseth [2], Lee, Smith [1], Lempel, Cohn, Eastman [1], Maritsas [1], McEliece [7], Mohanty [1], Selmer [3, ch. 6], Ипатов [1], а также обзор в статье Helleseth [1]. Некоторые корреляционные свойства последовательностей над полем $\mathbb{F}_2$ изучались также в работе MacWilliams, Odlyzko [1].

[Соболь [1*], [2*] использовал теорию линейных рекуррентных последовательностей над конечным полем для построения последовательностей точек, равномерно распределенных в единичном s-мерном кубе с наименьшим возможным отклонением. Шпарлинским [1*] показано, что для «почти всех» начальных условий вычеты членов линейной рекуррентной последовательности по простому модулю равномерно распределены. Подобные же результаты были получены Эгами (Egami [1*]) в связи с одной задачей теории алгебраических чисел.

По тематике восьмой главы кроме указанных имеются еще работы: Кисловская [1*] и Нечаев [1*]. — *Перев.*]

Упражнения

8.1. Построить регистр сдвига с обратной связью, реализующий линейное рекурреитное соотношение

$$s_{n+5} = s_{n+4} - s_{n+3} - s_{n+1} + s_n, \quad n = 0, 1, \ldots,$$

над полем $\mathbb{F}_3$.

8.2. Построить регистр сдвига с обратной связью, реализующий линейное рекурреитное соотношение

$$s_{n+7} = 3s_{n+5} - 2s_{n+4} + s_{n+3} + 2s_n + 1, \quad n = 0, 1, \ldots,$$

над полем $\mathbb{F}_7$.

8.3. Пусть r — период периодической последовательности $s_0, s_1, \ldots$, и пусть n_0 — наименьшее неотрицательное целое число, для которого выполняется равенство $s_{n+r} = s_n$ при всех $n \geqslant n_0$. Доказать, что n_0 совпадает с предпернодом последовательности $s_0, s_1, \ldots$.

8.4. Определить порядок матрицы

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

как элемента общей линейной группы $GL(4, \mathbb{F}_3)$.

8.5. Доказать результаты из примера 8.18 с помощью методов § 5.

8.6. Пользуясь равенством (8.8), получить явную формулу для членов линейной рекуррентной последовательности над полем $\mathbb{F}_3$, определяемой рекуррентным соотношением $s_{n+3} = -s_{n+1} + s_n$, $n = 0, 1, \ldots$, и начальными условиями $s_0 = s_1 = 1$, $s_2 = 0$.

8.7. Пользуясь результатом, приведенным в замечании 8.23, получить явную формулу для членов рекуррентной последовательности над полем $\mathbb{F}_4$, определяемой рекуррентным соотношением $s_{n+4} = \alpha s_{n+3} + s_{n+1} + \alpha s_n$, $n = 0, 1, \ldots$, где α — примитивный элемент поля $\mathbb{F}_4$, и начальными условиями $s_0 = s_1 = s_2 = 0$, $s_3 = 1$.

8.8. Доказать, что члены s_n, задаваемые формулой, приведенной в замечании 8.23, удовлетворяют однородному линейному рекуррентному соотношению с характеристическим многочленом $f(x)$.

8.9. Доказать результат, приведенный в замечании 8.23, для случая $e_i \leqslant 2$, $i = 1, 2, \ldots, m$, и $e_i = 1$, если $\alpha_i = 0$.

8.10. Представить элементы линейной рекуррентной последовательности над полем $\mathbb{F}_2$, определяемой рекуррентным соотношением $s_{n+3} = s_{n+2} + s_n$, $n = 0, 1, \ldots$, и начальными условиями $s_0 = 0$, $s_1 = s_2 = 1$, с помощью подходящей функции следа.

8.11. Доказать лемму 8.26, используя линейные рекуррентные последовательности.

8.12. Найти минимальный период последовательности, порожденной импульсом и удовлетворяющей линейному рекуррентному соотношению $s_{n+7} = s_{n+6} + s_{n+5} + s_{n+1} + s_n$, $n = 0, 1, \ldots$, над полем $\mathbb{F}_2$.

8.13. Найти минимальный период последовательности, порожденной импульсом, соответствующей линейному рекуррентному соотношению $s_{n+10} = s_{n+7} + s_{n+2} + s_{n+1} + s_n$, $n = 0, 1, \ldots$, над полем $\mathbb{F}_2$.

8.14. Доказать теорему 8.27, пользуясь производящими функциями.

8.15. Найти линейную рекуррентную последовательность наименьшего порядка над полем $\mathbb{F}_2$, минимальный период которой равен 21.

8.16. Найти линейную рекуррентную последовательность наименьшего порядка над полем $\mathbb{F}_2$, минимальный период которой равен 24.

8.17. Пусть r — минимальный период *последовательности Фибоначчи* над полем $\mathbb{F}_q$, т. е. последовательности, определяемой рекуррентным соотношением $s_{n+2} = s_{n+1} + s_n$, $n = 0, 1, \ldots$, и начальными условиями $s_0 = 0$, $s_1 = 1$. Пусть p — характеристика поля $\mathbb{F}_q$. Доказать, что $r = 20$, если $p = 5$, r делит $p - 1$, если $p \equiv \pm 1 \pmod 5$, r делит $p^2 - 1$ во всех остальных случаях.

8.18. Построить последовательность максимального периода над полем $\mathbb{F}_3$, имеющую минимальный период, равный 80.

8.19. *(m, k)-последовательностью де Брейна* называется конечная последовательность $s_0, s_1, \ldots, s_{N-1}$, содержащая $N = m^k$ членов, взятых из множества, содержащего m различных элементов, такая, что все наборы длины k вида $(s_n, s_{n+1}, \ldots, s_{n+k-1})$, $n = 0, 1, \ldots, N-1$, где нижние индексы берутся по модулю N, являются различными. Доказать, что если $d_0, d_1, \ldots$ — последовательность k-го порядка, порожденная импульсом и являющаяся последовательностью максимального периода над полем $\mathbb{F}_q$, то последовательность $s_0 = 0$, $s_n = d_{n-1}$, $1 \leqslant n \leqslant q^k - 1$, является (q, k)-последовательностью де Брейна.

8.20. Построить $(2, 5)$-последовательность де Брейна.

8.21. Пусть $B(x) = 2 - x + x^3 \in \mathbb{F}_7[x]$. Найти первые шесть ненулевых членов формального степенного ряда $1/B(x)$.

8.22. Пусть

$$A(x) = -1 - x + x^2, \qquad B(x) = \sum_{n=0}^{\infty} (-1)^n x^n \in \mathbb{F}_3[[x]].$$

Найти первые пять ненулевых членов формального степенного ряда $A(x)/B(x)$.

8.23. Рассмотрим линейную рекуррентную последовательность над полем $\mathbb{F}_3$, задаваемую рекуррентным соотношением $s_{n+5} = s_{n+4} + s_{n+2} - s_{n+1} + s_n$, $n = 0, 1, \ldots$, и начальными значениями $s_0 = s_1 = s_2 = 1$, $s_3 = s_4 = -1$. Представить производящую функцию этой последовательности в виде (8.15).

8.24. Найти первые восемь членов последовательности, порожденной импульсом и соответствующей линейному рекуррентному соотношению $s_{n+5} = s_{n+3} + s_{n+2} + s_n$, $n = 0, 1, \ldots$, над полем $\mathbb{F}_2$. Воспользоваться операцией деления углом.

8.25. Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$. Доказать, что множество всех многочленов $f(x) = a_k x^k + \ldots + a_1 x + a_0 \in \mathbb{F}_q[x]$, таких, что $a_k s_{n+k} + \ldots + a_1 s_{n+1} + a_0 s_n = 0$ для всех $n = 0, 1, \ldots$, образует идеал в кольце $\mathbb{F}_q[x]$. Вывести отсюда, что существует однозначно определенный минимальный многочлен рекуррентной последовательности.

8.26. Рассмотрим линейную рекуррентную последовательность над полем $\mathbb{F}_2$, определяемую рекуррентным соотношением $s_{n+8} = s_{n+7} + s_{n+6} + s_{n+5} + s_n$, $n = 0, 1, \ldots$, и начальными значениями $s_0 = s_3 = s_4 = s_5 = s_6 = 0$, $s_1 = s_2 = s_7 = 1$. Используя метод доказательства теоремы 8.42, найти минимальный многочлен данной рекуррентной последовательности.

8.27. Рассмотрим линейную рекуррентную последовательность над полем $\mathbb{F}_5$, определяемую рекуррентным соотношением $s_{n+4} = 3s_{n+2} - s_{n+1} + s_n$, $n = 0, 1, \ldots$, и начальными значениями $s_0 = s_1 = s_2 = 1$, $s_3 = -1$. Используя метод доказательства теоремы 8.42, найти минимальный многочлен данной рекуррентной последовательности.

8.28. Показать, что однородная линейная рекуррентная последовательность над конечным полем является чисто периодической последовательностью тогда и только тогда, когда ее минимальный многочлен $m(x)$ удовлетворяет условию $m(0) \neq 0$.

8.29. Пусть дана однородная линейная рекуррентная последовательность над конечным полем и $m(x)$ — ее минимальный многочлен. Доказать, что длина предпериода данной последовательности равняется кратности элемента 0 как корня многочлена $m(x)$.

8.30. Доказать следствие 8.52, используя способ построения минимального многочлена, приведенный в доказательстве теоремы 8.42.

8.31. Пользуясь критерием, полученным в теореме 8.51, найти минимальный многочлен линейной рекуррентной последовательности над полем $\mathbb{F}_2$, задаваемой рекуррентным соотношением $s_{n+6} = s_{n+3} + s_{n+2} + s_{n+1} + s_n$, $n = 0, 1, \ldots$, и вектором начального состояния $(1, 1, 1, 0, 0, 1)$.

8.32. Найти минимальный период линейной рекуррентной последовательности из упр. 8.26.

8.33. Найти минимальный период линейной рекуррентной последовательности из упр. 8.27.

8.34. Найти минимальный период линейной рекуррентной последовательности над полем $\mathbb{F}_2$, задаваемой рекуррентным соотношением $s_{n+9} = s_{n+7} + s_{n+4} + s_{n+1} + s_n$, $n = 0, 1, \ldots$, и начальными значениями $s_0 = s_1 = s_2 = s_6 = s_7 = 0$, $s_3 = s_4 = s_5 = s_8 = 1$.

8.35. Найти минимальный период линейной рекуррентной последовательности над полем $\mathbb{F}_3$, заданной рекуррентным соотношением $s_{n+5} = s_{n+4} - s_{n+3} + s_{n+2} + s_n$, $n = 0, 1, \ldots$, и начальными значениями $s_0 = s_1 = 1$, $s_2 = s_3 = 0$, $s_4 = -1$.

8.36. Найти минимальный период линейной рекуррентной последовательности над полем $\mathbb{F}_3$, определяемой рекуррентным соотношением $s_{n+4} = s_{n+3} + s_{n+2} - s_n - 1$, $n = 0, 1, \ldots$, и вектором начального состояния $(0, -1, 1, 0)$.

8.37. Доказать, что линейная рекуррентная последовательность k-го порядка $s_0, s_1, \ldots$ над полем $\mathbb{F}_q$ имеет минимальный период, равный q^k, только в следующих случаях:

(a) $k = 1$, q — простое число, $s_{n+1} = s_n + a$, $n = 0, 1, \ldots, a \in \mathbb{F}_q^*$;
(b) $k = 2$, $q = 2$, $s_{n+2} = s_n + 1$, $n = 0, 1, \ldots$.

8.38. Пусть дана однородная линейная рекуррентная последовательность над полем $\mathbb{F}_q$ и $m(x) \in \mathbb{F}_q[x]$ — ее минимальный многочлен, отличный от константы. Пусть корни этого многочлена отличны от нуля и не являются кратными. Доказать, что минимальный период данной последовательности равен такому наименьшему натуральному числу r, при котором выполняется равенство $\alpha^r = 1$ для всех корней α многочлена $m(x)$.

8.39. Доказать, что если однородной линейной рекуррентной последовательности σ над полем $\mathbb{F}_q$ соответствует минимальный многочлен $f(x) \in \mathbb{F}_q[x]$ и $\deg(f(x)) = n \geqslant 1$, то любую последовательность из множества $S(f(x))$ можно единственным образом представить в виде линейной комбинации исходной последовательности $\sigma = \sigma^{(0)}$ и последовательностей $\sigma^{(1)}, \sigma^{(2)}, \ldots, \sigma^{(n-1)}$, полученных с помощью сдвигов исходной последовательности σ, с коэффициентами из поля $\mathbb{F}_q$.

8.40. Пусть $f_1(x), \ldots, f_k(x)$ — попарно взаимно простые нормированные многочлены над полем $\mathbb{F}_q$, не являющиеся константами. Показать, что пространство $S(f_1(x) \ldots f_k(x))$ является прямой суммой линейных подпространств $S(f_1(x)), \ldots, S(f_k(x))$.

8.41. Пусть $s_0, s_1, \ldots$ — однородная линейная рекуррентная последовательность над полем $K = \mathbb{F}_q$, а $f(x)$ — ее характеристический многочлен. Пусть $f(x) = f_1(x) \ldots f_r(x)$, где $f_i(x)$ — различные нормированные неприводимые многочлены над полем K. Пусть, далее, α_i $(i = 1, \ldots, r)$ является фиксированным корнем многочлена $f_i(x)$ в его поле разложения F_i над K. Доказать, что существуют однозначно определенные элементы $\theta_1 \in F_1, \ldots, \theta_r \in F_r$, для которых выполняется равенство

$$s_n = \mathrm{Tr}_{F_1/K}(\theta_1 \alpha_1^n) + \cdots + \mathrm{Tr}_{F_r/K}(\theta_r \alpha_r^n), \quad n = 0, 1, \ldots .$$

8.42. Пользуясь обозначениями, введенными в упр. 8.41, показать, что $f(x)$ является минимальным многочленом последовательности $s_0, s_1, \ldots$ тогда и только тогда, когда $\theta_i \neq 0$ для всех $i = 1, \ldots, r$. Получить отсюда, что число последовательностей в $S(f(x))$, минимальным многочленом которых является $f(x)$, задается формулой $(q^{k_1} - 1) \ldots (q^{k_r} - 1)$, где $k_i = \deg(f_i(x))$, $i = 1, \ldots, r$.

8.43. Пусть σ_1 и σ_2 — последовательности, порожденные импульсом, над полем $\mathbb{F}_2$, связанные с линейными рекуррентными соотношениями $s_{n+6} = s_{n+3} + s_n$ $(n = 0, 1, \ldots)$ и $s_{n+3} = s_{n+1} + s_n$ $(n = 0, 1, \ldots)$ соответственно. Найти минимальный период последовательности $\sigma_1 + \sigma_2$.

8.44. Пусть σ_1 — линейная рекуррентная последовательность над полем $\mathbb{F}_3$, заданная рекуррентным соотношением $s_{n+3} = s_{n+2} - s_{n+1} - s_n$, $n = 0, 1, \ldots$, и вектором начального состояния $(0, 1, 0)$. Пусть σ_2 — линейная рекуррентная последовательность над тем же полем, заданная рекуррентным соотношением $s_{n+5} = -s_{n+3} - s_{n+2} + s_n$, $n = 0, 1, \ldots$, и вектором начального состояния $(1, 1, 1, 0, 1)$. Пользуясь методом, приведенным в примере 8.58, найти минимальный многочлен последовательности $\sigma = \sigma_1 + \sigma_2$.

8.45. Найти минимальный период последовательности σ из упр. 8.44.

8.46. Пусть дана однородная линейная рекуррентная последовательность над полем $\mathbb{F}_2$ и $x^6 + x^5 + x^4 + 1 \in \mathbb{F}_2[x]$ — ее минимальный многочлен. Найти минимальный многочлен последовательности, являющийся биарным дополнением к исходной.

8.47. Пусть $f(x) = x^9 + x^7 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. Найти минимальные периоды последовательностей из $S(f(x))$, а также число последовательностей, соответствующих каждому значению минимального периода.

8.48. Пусть $f(x) = (x + 1)^3 (x^3 - x + 1) \in \mathbb{F}_3[x]$. Найти значения, которые могут принимать минимальные периоды последовательностей из множества $S(f(x))$, а также число последовательностей, соответствующих каждому из этих значений.

8.49. Пусть $f(x) = x^5 - 2x^4 - x^2 - 1 \in \mathbb{F}_5[x]$. Найти значения минимальных периодов, которые могут встречаться у последовательностей из множества $S(f(x))$, а также число последовательностей, соответствующих каждому из этих значений.

8.50. Найти нормированный многочлен $g(x) \in \mathbb{F}_3[x]$, для которого

$$S(x+1)\,S(x^2+x-1)\,S(x^2-x-1) = S(g(x)).$$

8.51. Найти нормированный многочлен $g(x) \in \mathbb{F}_2[x]$, для которого

$$S(x^2+x+1)\,S(x^5+x^4+1) = S(g(x)).$$

8.52. Для нечетных q найти нормированный многочлен $g(x) \in \mathbb{F}_q[x]$, такой, что

$$S((x-1)^2)\,S((x-1)^2) = S(g(x)).$$

Что будет, если q четно?

8.53. Доказать, что $f \vee (gh) = (f \vee g)(f \vee h)$, где $f, g, h \in \mathbb{F}_q[x]$ — многочлены, не являющиеся константами, при условии, что сомножители в правой части приведенного выше равенства взаимно просты.

8.54. Рассмотрим последовательность над полем $\mathbb{F}_2$, порожденную импульсом и соответствующую линейному рекуррентному соотношению $s_{n+4} = s_{n+2} + s_n$, $n = 0, 1, \ldots$, и линейную рекуррентную последовательность над тем же полем, задаваемую рекуррентным соотношением $s_{n+1} = s_n$, $n = 0, 1, \ldots$, и вектором начального состояния $(0, 1, 1, 1)$. На примере этих последовательностей показать, что аналог теоремы 8.59 для операции умножения последовательностей не справедлив.

8.55. Пусть $r \in \mathbb{N}$, $f \in \mathbb{F}_q[x]$, $\deg(f) > 0$, и пусть $\sigma_r(f)$ обозначает сумму r-х степеней различных корней многочлена $f(x)$. Доказать, что для многочленов $f, g \in \mathbb{F}_q[x]$, не являющихся константами, справедливо равенство $\sigma_r(f \vee g) = \sigma_r(f)\,\sigma_r(g)$ при условии, что число различных корней многочлена $f \vee g$ равняется произведению числа различных корней многочлена f и числа различных корней многочлена g.

8.56. Пусть $s_0, s_1, \ldots$ — произвольная последовательность элементов поля $\mathbb{F}_q$, и пусть $n \geqslant 0$, $r \geqslant 1$ — целые числа. Доказать, что если ганкелевы определители $D_{n+2}^{(r)}$ и $D_n^{(r+1)}$ равны 0, то и $D_{n+1}^{(r)} = 0$.

8.57. Доказать, что последовательность $s_0, s_1, \ldots$ над полем $\mathbb{F}_q$ является однородной линейной рекуррентной последовательностью с минимальным многочленом степени k тогда и только тогда, когда $D_n^{(k+1)} = 0$ для всех $n \geqslant 0$ и $k+1$ является наименьшим натуральным числом, для которого это выполняется.

8.58. Получить полное доказательство второго неравенства в формуле (8.23).

8.59. Доказать неравенства из формулы (8.24).

8.60. Дать полное доказательство формулы (8.26).

8.61. Доказать формулу (8.27).

8.62. Пусть первые 10 членов однородной линейной рекуррентной последовательности над полем $\mathbb{F}_2$ порядка $k \leqslant 5$ равны соответственно 0, 1, 1, 0, 0, 0, 0, 1, 1, 1. С помощью алгоритма Берлекэмпа — Месси найти минимальный многочлен этой последовательности.

8.63. Пусть первые 8 членов однородной линейной рекуррентной последовательности над полем $\mathbb{F}_5$ порядка $k \leqslant 4$ равны соответственно 2, 1, 0, 1, -2, 0, -2, -1. С помощью алгоритма Берлекэмпа — Месси найти минимальный многочлен этой последовательности.

8.64. Пусть первые 10 членов однородной линейной рекуррентной последовательности над полем $\mathbb{F}_3$ порядка $k \leqslant 5$ равны соответственно 1, -1, 0, -1, 0, 0, 0, 0, 1, 0. С помощью алгоритма Берлекэмпа — Месси найти минимальный многочлен этой последовательности.

8.65. Найти однородную линейную рекуррентную последовательность наименьшего порядка над полем $\mathbb{F}_5$, первые 10 членов которой равны соответственно 2, 0, -1, -2, 0, 0, -2, 2, -1, -2.

8.66. Пусть выполняются условия теоремы 8.78, и пусть, кроме того, характеристический многочлен $f(x)$ последовательности $s_0, s_1, \ldots$ удовлетворяет условию $f(0) \neq 0$. Доказать следующую формулу, являющуюся усилением (8.31):

$$\left| \sum_{n=u}^{u+r-1} \chi(s_n) \right| \leqslant \left(\frac{r}{R}\right)^{1/2} (q^k - r)^{1/2} \quad \text{для всех} \quad u \geqslant 0.$$

(*Указание.* Воспользоваться тем, что в (8.33) случай $\mathbf{b} = \mathbf{0}$ можно исключить.)

8.67. Пусть выполнены условия теоремы 8.84, и пусть число r является делителем числа $(q^k - 1)/(q - 1)$. Пусть также $(q^k - 1)/r$ и k будут взаимно просты. Доказать, что $Z(0) = (q^{k-1} - 1)\, r/(q^k - 1)$.

8.68. Пусть выполнены условия теоремы 8.84, и пусть q будет нечетным числом, а $h = (q^k - 1)/2$. Доказать, что в этом случае в формуле (8.37) имеет место равенство.

8.69. Пусть выполнены условия теоремы 8.84, а $Z(b;\ N_0,\ N)$ такое же, как в теореме 8.85. Доказать справедливость следующего равенства:

$$Z(b;\ N_0,\ N) = \frac{N}{r} Z(b) + \frac{1}{q(q^k - 1)} \sum_{\substack{\psi \\ \psi(\alpha) \neq 1}} \psi(\theta)\, G(\bar{\psi},\ \bar{\lambda})\, G(\psi',\ \lambda'_b)\, \frac{\psi(\alpha)^{N_0+N} - \psi(\alpha)^{N_0}}{\psi(\alpha) - 1}.$$

8.70. Из результата, полученного в упр. 8.69, вывести неравенство

$$\left| Z(0;\ N_0,\ N) - \frac{(q^{k-1} - 1)\, N}{q^k - 1} \right| \leqslant \left(1 - \frac{1}{q}\right) \left(\frac{N}{h} - \frac{N}{q^k - 1}\right) q^{k/2} + q^{(k/2)-1} \left(\frac{2}{\pi} \log \frac{h}{q-1} + \varepsilon_h\right),$$

где $\varepsilon_h = 0$ при $h = q - 1$ и $\varepsilon_h = 2/5$ при $h > q - 1$.

8.71. Из результата, полученного в упр. 8.69, вывести для $b \neq 0$ неравенство

$$\left| Z(b;\ N_0,\ N) - \frac{q^{k-1} N}{q^k - 1} \right| \leqslant \left(\frac{2}{\pi} \log r + \frac{2}{5} + \frac{N(h-r)}{hr}\right) q^{(k-1)/2} + \left(\frac{N}{h} - \frac{N}{q^k - 1}\right) q^{(k/2)-1}.$$

Глава 9

Приложения конечных полей

Одной из основных областей приложения конечных полей является теория кодирования. Эта теория берет свое начало в знаменитой теореме Шеннона о кодировании. В ней утверждается, что существуют коды, применение которых позволяет передавать информацию с произвольно малой вероятностью ошибки на скоростях, близких к пропускной способности канала. Одной из целей алгебраической теории кодирования — теории кодов, исправляющих ошибки, и кодов, обнаруживающих ошибки, — является поиск методов построения таких кодов.

В течение двух последних десятилетий на развитие теории кодирования все больше и больше оказывают влияние такие разделы абстрактной алгебры, как теория конечных полей и теория многочленов над конечными полями. В частности, важной вехой в этом направлении явилось описание избыточных кодов с помощью многочленов над полем $\mathbb{F}_q$. Тот факт, что регистры сдвига можно использовать для кодирования и декодирования информации, позволяет установить связь теории кодирования с теорией линейных рекуррентных последовательностей. В §§ 1 и 2, посвященных алгебраической теории кодирования, мы ограничимся обсуждением основных свойств блочных кодов, непосредственно связанных с конечными полями, и не будем касаться задач технической реализации того или иного кода.

§ 3 содержит некоторые результаты, касающиеся применения теории конечных полей в геометрии, а именно для исследования аффинных и проективных плоскостей, содержащих конечное число точек и прямых.

§ 4 посвящен комбинаторике и содержит разнообразные приложения конечных полей в этой области, особенно в задачах планирования экспериментов.

В последнем, пятом параграфе мы приведем определение линейной модулярной системы и покажем, как теория конечных полей используется в теории линейных модулярных систем. Под системой можно понимать некоторое устройство, в которое в определенные моменты времени что-то поступает (например материя, энергия, информация) и которое само в определенные моменты времени что-то выдает. Например, мы можем наглядно

представлять себе некоторую систему как электрическую сеть в которую поступает электрический сигнал, а выходом являются текущие показания приборов. Систему можно также представлять в виде сети переключательных элементов, входом которой является установка входных переключателей, а выходом — конфигурация горящих сигнальных лампочек.

Мы особо подчеркиваем, что приводимые ниже приложения даются лишь для того, чтобы привести примеры использования разнообразных свойств конечных полей. Поэтому эти примеры касаются скорее алгебраических и комбинаторных аспектов приложений конечных полей и оставляют в стороне вопросы практического использования. Так, например, мы не будем обсуждать задачи анализа экспериментальных данных или вопросы анализа и синтеза линейных модулярных систем, не будем мы также касаться тех свойств геометрических конструкций, которые непосредственно не связаны с конечными полями.

§ 1. Линейные коды

Большое значение в настоящее время приобрели проблемы передачи информации и, в частности, вопросы кодирования и декодирования информации в целях ее надежной передачи по «зашумленным» каналам. Обычно бывает необходимо передать сообщение, состоящее из конечной последовательности символов, являющихся элементами некоторого конечного алфавита. Если, например, этот алфавит состоит из символов 0 и 1, то передаваемое сообщение можно рассматривать как некоторое двоичное число. В общем случае предполагается, что алфавит является некоторым конечным полем. Передача конечной последовательности элементов алфавита по каналу связи не обязательно осуществляется в «точном» виде в том смысле, что каждый бит информации передается по каналу не изменяясь. Ввиду того что не существует идеального канала без «шумов», получатель передаваемого сообщения может получить искаженную информацию и ошибочно истолковать переданные сигналы.

Одной из основных задач теории кодирования является стремление к тому, чтобы вероятность ошибок, появляющихся в результате шума в канале связи, была сведена к минимуму. Методы повышения надежности передачи сообщений в основном базируются на свойствах конечных полей.

Основной идеей алгебраической теории кодирования является передача *избыточной информации* вместе с тем сообщением, которое необходимо передать. Это означает, что последовательность символов, составляющая передаваемое сообщение, некоторым специальным образом преобразуется в более длинную последовательность.

Простая модель системы связи изображена на рис. 9.1. Мы

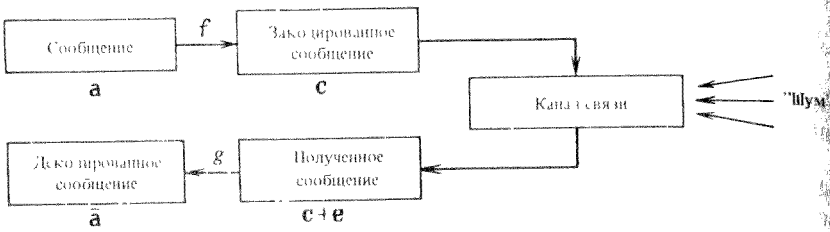


Рис. 9.1

предполагаем, что символы, составляющие исходное сообщение, и символы, составляющие закодированное сообщение, являются элементами одного и того же конечного поля $\mathbb{F}_q$. Кодирование означает, что блок из k символов передаваемого сообщения $a_1a_2 \ldots a_k$, $a_i \in \mathbb{F}_q$, заменяется *кодовым словом* $c_1c_2 \ldots c_n$ длины $n > k$, которое образовано символами $c_i \in \mathbb{F}_q$. Мы будем рассматривать кодовое слово как n-мерную вектор-строку $\mathbf{c} \in \mathbb{F}_q^n$. Таким образом, отображение f на рис. 9.1 является функцией из $\mathbb{F}_q^k$ в $\mathbb{F}_q^n$, называемой *схемой кодирования*, а g — функцией из $\mathbb{F}_q^n$ в $\mathbb{F}_q^k$, называемой *схемой декодирования*.

Простая разновидность схемы кодирования возникает в случае, когда в сообщении каждый блок из k символов $a_1a_2 \ldots a_k$ кодируется кодовым словом вида

$$a_1a_2 \ldots a_kc_{k+1} \ldots c_n,$$

где первые k символов совпадают с k символами исходного сообщения и называются *информационными символами*, а дополнительные $n - k$ символов $c_i \in \mathbb{F}_q$ называются *проверочными* (или *контрольными*) *символами*. Такую схему кодирования часто представляют в следующем виде. Пусть H — заданная $(n - k) \times n$-матрица, образованная элементами поля $\mathbb{F}_q$ и имеющая вид

$$H = (A \;\; I_{n-k}),$$

где A — матрица размера $(n - k) \times k$, а I_{n-k} — единичная матрица порядка $n - k$. Тогда проверочные символы $c_{k+1}, \ldots, c_n$ могут быть определены из системы уравнений

$$H\mathbf{c}^{\mathrm{T}} = \mathbf{0},$$

где $\mathbf{c}$ — кодовое слово, а $^{\mathrm{T}}$ обозначает транспонирование. Уравнения, образующие эту систему, называются *проверочными уравнениями* или *уравнениями проверки на четность* [1]).

[1]) Название берет свое начало в исследованиях по бинарным кодам, т. е. кодам над полем $\mathbb{F}_2$. — *Прим. перев.*

9.1. Пример. Пусть H есть 3×7-матрица над полем $\mathbb{F}_2$ следующего вида:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Проверочные символы можно найти из системы уравнений $H\mathbf{c}^{\mathrm{T}} = \mathbf{0}$, считая c_1, c_2, c_3, c_4 заданными:

$$\begin{aligned} c_1 \quad &+ c_3 + c_4 + c_5 &&= 0, \\ c_1 + c_2 \quad &+ c_4 \quad + c_6 &&= 0, \\ c_1 + c_2 + c_3 \quad &+ c_7 &&= 0. \end{aligned}$$

Тогда проверочные символы c_5, c_6, c_7 можно выразить следующим образом:

$$\begin{aligned} c_5 &= c_1 \quad + c_3 + c_4, \\ c_6 &= c_1 + c_2 \quad + c_4, \\ c_7 &= c_1 + c_2 + c_3. \end{aligned}$$

Значит, схема кодирования в этом случае является линейным отображением из $\mathbb{F}_2^4$ в $\mathbb{F}_2^7$, которое имеет вид

$$(a_1, a_2, a_3, a_4) \to$$
$$\to (a_1, a_2, a_3, a_4, a_1 + a_3 + a_4, \quad a_1 + a_2 + a_4, a_1 + a_2 + a_3). \square$$

В общем случае в связи со схемами кодирования, задаваемыми линейными отображениями, мы будем пользоваться следующей терминологией.

9.2. Определение. Пусть H — матрица над полем $\mathbb{F}_q$ размера $(n - k) \times n$ и ранга $n - k$. Множество C всех n-мерных векторов $\mathbf{c} \in \mathbb{F}_q^n$, таких, что $H\mathbf{c}^{\mathrm{T}} = \mathbf{0}$, называется *линейным* (n, k)-*кодом* над полем $\mathbb{F}_q$. Число n называется *длиной* кода, а k — *размерностью* кода. Элементы множества C называются *кодовыми словами* (или *кодовыми векторами*), матрица H называется *проверочной матрицей* кода C. Если $q = 2$, C называется *бинарным кодом*. Если матрица H имеет вид $H = (A \; I_{n-k})$, то код C называется *систематическим кодом*.

Заметим, что множество C решений системы линейных уравнений $H\mathbf{c}^{\mathrm{T}} = \mathbf{0}$ является k-мерным подпространством векторного пространства $\mathbb{F}_q^n$. Так как кодовые слова образуют группу по сложению, то C также называется *групповым кодом*. Кроме того, C можно рассматривать как нуль-пространство матрицы H [1]).

[1]) То есть как ядро линейного отображения, задаваемого матрицей H, или пространство решений однородной системы линейных уравнений с матрицей H — *Прим. перев.*

9.3. Пример (*код с общей проверкой на четность*). Пусть $r = 2$, и пусть передаваемое сообщение имеет вид $a_1 \ldots a_k$. Тогда определим схему кодирования f следующим образом:

$$f\colon a_1 \ldots a_k \longmapsto b_1 \ldots b_{k+1},$$

где $b_i = a_i$ для $i = 1, \ldots, k$, а

$$b_{k+1} = \begin{cases} 0, & \text{если } \sum_{i=1}^{k} a_i = 0, \\ 1, & \text{если } \sum_{i=1}^{k} a_i = 1. \end{cases}$$

Следовательно, сумма всех элементов любого кодового слова $b_1 \ldots b_{k+1}$ равна 0. Если сумма элементов полученного слова равняется 1, то получатель узнает, что в процессе передачи в сообщении появилась ошибка. Если положить $n = k + 1$, то полученный код является линейным $(n, n-1)$-кодом с проверочной матрицей $H = (11 \ldots 1)$.

9.4. Пример (*код с повторением*). В коде с повторением каждое кодовое слово содержит только один информационный символ a_1 и $n - 1$ проверочных символов $c_2 = \ldots = c_n = a_1$, т. е. символ a_1 повторяется еще $n - 1$ раз. Этот код является линейным $(n, 1)$-кодом с проверочной матрицей $H = (-\mathbf{1}\ I_{n-1})$.

Из проверочного уравнения $H\mathbf{c}^{\mathrm{T}} = \mathbf{0}$, где $H = (A\ \ I_{n-k})$, следует, что

$$\mathbf{c}^{\mathrm{T}} = \begin{pmatrix} I_k \\ -A \end{pmatrix} \mathbf{a}^{\mathrm{T}} = [\mathbf{a}\,(I_k\ \ -A^{\mathrm{T}})]^{\mathrm{T}},$$

где $\mathbf{a} = a_1 \ldots a_k$ — передаваемое сообщение, а $\mathbf{c} = c_1 \ldots c_n$ — соответствующее кодовое слово. Это приводит к следующему определению.

9.5. Определение. Матрица $G = (I_k\ \ -A^{\mathrm{T}})$ размера $k \times n$ называется *канонической* (или *стандартной*) *порождающей* (или *кодирующей*) *матрицей* линейного (n, k)-кода с проверочной матрицей $H = (A\ \ I_{n-k})$.

Из уравнений $H\mathbf{c}^{\mathrm{T}} = \mathbf{0}$ и $\mathbf{c} = \mathbf{a}G$ следует, что матрицы H и G связаны равенством

$$GH^{\mathrm{T}} = 0. \tag{9.1}$$

Код C совпадает с пространством строк канонической порождающей матрицы G [1]). В более общем случае любая $k \times n$-матрица G,

[1]) То есть с образом линейного отображения, задаваемого матрицей G. — *Прим. перев.*

пространство строк которой равняется C, называется *порождающей матрицей* кода C.

9.6. **Пример.** Каноническая порождающая матрица для кода с проверочной матрицей H из примера 9.1 имеет вид

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \qquad \square$$

9.7. **Определение.** Если $\mathbf{c}$ — кодовое слово, а $\mathbf{y}$ — слово, полученное после передачи сообщения по зашумленному каналу, то разность $\mathbf{e} = \mathbf{y} - \mathbf{c} = e_1 \ldots e_n$ называется *вектором ошибок* или *шумовым словом*.

9.8. **Определение.** Пусть $\mathbf{x}$ и $\mathbf{y}$ — два вектора пространства $\mathbb{F}_q^n$. Тогда

(i) *расстоянием Хэмминга* $d(\mathbf{x}, \mathbf{y})$ между векторами $\mathbf{x}$ и $\mathbf{y}$ называется число координат, которыми векторы $\mathbf{x}$ и $\mathbf{y}$ отличаются друг от друга;

(ii) *весом* (*Хэмминга*) $w(\mathbf{x})$ вектора $\mathbf{x}$ называется число ненулевых координат этого вектора.

Таким образом, если $\mathbf{x}$ — передаваемое кодовое слово, а $\mathbf{y}$ — полученное после передачи слово, то величина $d(\mathbf{x}, \mathbf{y})$ дает число ошибок, появившихся при передаче слова $\mathbf{x}$. Ясно, что $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$ и $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$. Доказательство следующей леммы оставляется читателю в качестве упражнения.

9.9. **Лемма.** *Расстояние Хэмминга является метрикой в пространстве* $\mathbb{F}_q^n$, *т. е. для любых* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$ *выполняются следующие соотношения*:

(i) $d(\mathbf{x}, \mathbf{y}) = 0$ *тогда и только тогда, когда* $\mathbf{x} = \mathbf{y}$;
(ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;
(iii) $d(\mathbf{x}, \mathbf{z}) \leqslant d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

При декодировании полученного слова $\mathbf{y}$ обычно стараются найти кодовое слово $\mathbf{c}$, для которого $w(\mathbf{y} - \mathbf{c})$ принимает наименьшее возможное значение, исходя при этом из естественного предположения, что малое число ошибок встречается чаще, чем большое. Таким образом, при декодировании мы ищем кодовое слово $\mathbf{c}$, ближайшее в смысле расстояния Хэмминга к полученному слову $\mathbf{y}$. Это правило называется *декодированием в ближайшее кодовое слово*.

9.10. **Определение.** Если t — некоторое натуральное число, то код $C \subseteq \mathbb{F}_q^n$ называется *кодом, исправляющим* t *ошибок*, если для любого $\mathbf{y} \in \mathbb{F}_q^n$ найдется не более одного слова $\mathbf{c} \in C$, такого, что $d(\mathbf{y}, \mathbf{c}) \leqslant t$.

Если $\mathbf{c} \in C$ — передаваемое кодовое слово и при передаче появилось не более t ошибок, то $d(\mathbf{y}, \mathbf{c}) \leqslant t$ для полученного слова $\mathbf{y}$. Если C — код, исправляющий t ошибок, то для всех кодовых слов $\mathbf{z} \neq \mathbf{c}$ должно выполняться соотношение $d(\mathbf{y}, \mathbf{z}) > t$; это означает, что $\mathbf{c}$ является ближайшим к $\mathbf{y}$ кодовым словом и что декодирование в ближайшее кодовое слово дает правильный результат. Таким образом, одна из задач теории кодирования состоит в построении таких кодов, для которых кодовые слова находятся на значительном расстоянии друг от друга. С другой стороны, естественно стремиться передать по возможности больше информации в единицу времени. Согласование этих двух тенденций составляет одну из проблем теории кодирования.

9.11. Определение. Число

$$d_C = \min_{\substack{\mathbf{u}, \mathbf{v} \in C \\ \mathbf{u} \neq \mathbf{v}}} d(\mathbf{u}, \mathbf{v}) = \min_{\mathbf{0} \neq \mathbf{c} \in C} w(\mathbf{c})$$

называется *минимальным расстоянием* (или просто *расстоянием*) линейного кода C.

9.12. Теорема. *Код C с минимальным расстоянием d_C может исправлять t ошибок, если $d_C \geqslant 2t + 1$.*

Доказательство. Шар $B_t(\mathbf{x})$ радиуса t с центром в точке $\mathbf{x} \in \mathbb{F}_q^n$ состоит из всех векторов $\mathbf{y} \in \mathbb{F}_q^n$, таких, что $d(\mathbf{x}, \mathbf{y}) \leqslant t$. Правило декодирования в ближайшее кодовое слово гарантирует, что каждое полученное в результате передачи слово, содержащее не более t ошибок, должно лежать в шаре радиуса t с центром в переданном кодовом слове. Для того чтобы можно было исправить t ошибок, шары радиуса t с центрами в кодовых словах $\mathbf{x}$ должны не пересекаться. Если $\mathbf{u} \in B_t(\mathbf{x})$ и $\mathbf{u} \in B_t(\mathbf{y})$, $\mathbf{x}, \mathbf{y} \in C$, $\mathbf{x} \neq \mathbf{y}$, то

$$d(\mathbf{x}, \mathbf{y}) \leqslant d(\mathbf{x}, \mathbf{u}) + d(\mathbf{u}, \mathbf{y}) \leqslant 2t,$$

что противоречит тому, что $d_C \geqslant 2t + 1$. □

9.13. Пример. Код из примера 9.1 имеет минимальное расстояние $d_C = 3$ и, следовательно, может исправлять одну ошибку.

Следующая лемма часто бывает полезна при определении минимального расстояния кода.

9.14. Лемма. *Для того чтобы линейный код C с проверочной матрицей H имел минимальное расстояние $d_C \geqslant s + 1$, необходимо и достаточно, чтобы любые s столбцов матрицы H были линейно независимы.*

Доказательство. Предположим, что найдутся s линейно зависимых столбцов матрицы H; тогда $H\mathbf{c}^{\mathrm{T}} = \mathbf{0}$ и $w(\mathbf{c}) \leqslant s$ для некоторого $\mathbf{c} \in C$, $\mathbf{c} \neq \mathbf{0}$. Отсюда следует, что $d_C \leqslant s$. Аналогично

если любые s столбцов матрицы H линейно независимы, то не существует $\mathbf{c} \in C$, $\mathbf{c} \neq \mathbf{0}$, с весом $w(\mathbf{c}) \leqslant s$; следовательно, $d_C \geqslant s + 1$. □

Опишем теперь простой алгоритм декодирования линейных кодов. Пусть C является линейным (n, k)-кодом над полем $\mathbb{F}_q$. Векторное пространство $\mathbb{F}_q^n/C$ состоит из всех смежных классов $\mathbf{a} + C = \{\mathbf{a} + \mathbf{c} \mid \mathbf{c} \in C\}$, где $\mathbf{a} \in \mathbb{F}_q^n$. Каждый смежный класс содержит q^k векторов. Можно считать, что пространство $\mathbb{F}_q^n$ разбивается на смежные классы по подпространству C, а именно

$$\mathbb{F}_q^n = (\mathbf{a}^{(0)} + C) \cup (\mathbf{a}^{(1)} + C) \cup \ldots \cup (\mathbf{a}^{(s)} + C),$$

где $\mathbf{a}^{(0)} = \mathbf{0}$ и $s = q^{n-k} - 1$. Вектор $\mathbf{y}$ принятого сообщения должен лежать в одном из этих смежных классов, например в $\mathbf{a}^{(i)} + C$. Если передаваемым кодовым словом было $\mathbf{c}$, то для вектора ошибок $\mathbf{e}$ получаем равенство

$$\mathbf{e} = \mathbf{y} - \mathbf{c} = \mathbf{a}^{(i)} + \mathbf{z} \in \mathbf{a}^{(i)} + C$$

для некоторого $\mathbf{z} \in C$. Отсюда приходим к следующей схеме декодирования.

9.15. Декодирование линейных кодов. Если после передачи получен вектор $\mathbf{y}$, то все возможные значения вектора ошибок $\mathbf{e}$ лежат в одном смежном классе с вектором $\mathbf{y}$. Наиболее вероятным вектором ошибок является вектор $\mathbf{e}$, имеющий минимальный вес среди всех векторов смежного класса, содержащего вектор $\mathbf{y}$. Тогда мы декодируем $\mathbf{y}$ как $\mathbf{x} = \mathbf{y} - \mathbf{e}$.

Описанную выше процедуру можно реализовать с помощью *алгоритма декодирования по лидеру смежного класса*.

9.16. Определение. Пусть $C \subseteq \mathbb{F}_q^n$ — линейный (n, k)-код, и пусть $\mathbb{F}_q^n/C$ — факторпространство пространства $\mathbb{F}_q^n$. Элемент минимального веса в смежном классе $\mathbf{a} + C$ называется *лидером смежного класса* $\mathbf{a} + C$. Если в смежном классе $\mathbf{a} + C$ несколько векторов имеют минимальный вес, то в качестве лидера смежного класса выбирается любой из них.

Пусть $\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}$ — лидеры смежных классов, отличных от C, и пусть $\mathbf{c}^{(1)} = \mathbf{0}, \mathbf{c}^{(2)}, \ldots, \mathbf{c}^{(q^k)}$ — все кодовые слова из C. Рассмотрим следующую таблицу:

$$\begin{array}{cccc}
\mathbf{c}^{(1)} & \mathbf{c}^{(2)} & \ldots & \mathbf{c}^{(q^k)} \\
\mathbf{a}^{(1)} + \mathbf{c}^{(1)} & \mathbf{a}^{(1)} + \mathbf{c}^{(2)} & \ldots & \mathbf{a}^{(1)} + \mathbf{c}^{(q^k)} \\
\ldots & \ldots & \ldots & \ldots \\
\mathbf{a}^{(s)} + \mathbf{c}^{(1)} & \mathbf{a}^{(s)} + \mathbf{c}^{(2)} & \ldots & \mathbf{a}^{(s)} + \mathbf{c}^{(q^k)}
\end{array}$$

строка кодовых слов; остальные смежные классы; столбец лидеров смежных классов

Если принято слово $\mathbf{y} = \mathbf{a}^{(i)} + \mathbf{c}^{(j)}$, то получатель считает, что вектор ошибок $\mathbf{e}$ совпадает с $\mathbf{a}^{(i)}$ — лидером соответствующего смежного класса — и декодирует слово $\mathbf{y}$ как кодовое слово $\mathbf{x} = \mathbf{y} - \mathbf{e} = \mathbf{c}^{(j)}$. Таким образом, $\mathbf{y}$ декодируется как кодовое слово, стоящее в приведенной выше таблице в столбце, содержащем слово $\mathbf{y}$. Смежный класс, содержащий вектор $\mathbf{y}$, можно определить с помощью так называемого синдрома вектора $\mathbf{y}$.

9.17. Определение. Пусть H — проверочная матрица линейного (n, k)-кода C. Тогда вектор $S(\mathbf{y}) = H\mathbf{y}^{\mathrm{T}}$ длины $n - k$ называется *синдромом* вектора $\mathbf{y}$.

9.18. Теорема. *Если* $\mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$, *то*

(i) $S(\mathbf{y}) = \mathbf{0}$ *тогда и только тогда, когда* $\mathbf{y} \in C$;

(ii) $S(\mathbf{y}) = S(\mathbf{z})$ *тогда и только тогда, когда* $\mathbf{y} + C = \mathbf{z} + C$.

Доказательство. Пункт (i) немедленно следует из определения кода C через матрицу H. Для доказательства п. (ii) заметим, что равенство $S(\mathbf{y}) = S(\mathbf{z})$ имеет место тогда и только тогда, когда $H\mathbf{y}^{\mathrm{T}} = H\mathbf{z}^{\mathrm{T}}$ или, что то же самое, когда $H(\mathbf{y} - \mathbf{z})^{\mathrm{T}} = \mathbf{0}$, т. е. $\mathbf{y} - \mathbf{z} \in C$. Последнее равносильно тому, что $\mathbf{y} + C = \mathbf{z} + C$. □

Если $\mathbf{e} = \mathbf{y} - \mathbf{c}$, $\mathbf{c} \in C$, $\mathbf{y} \in \mathbb{F}_q^n$, то

$$S(\mathbf{y}) = S(\mathbf{c} + \mathbf{e}) = S(\mathbf{c}) + S(\mathbf{e}) = S(\mathbf{e}), \tag{9.2}$$

т. е. векторы $\mathbf{y}$ и $\mathbf{e}$ лежат в одном смежном классе. Лидер этого смежного класса имеет тот же синдром. Таким образом, получаем следующий алгоритм декодирования.

9.19. Алгоритм декодирования по лидеру смежного класса. Пусть $C \subseteq \mathbb{F}_q^n$ — линейный (n, k)-код, и пусть $\mathbf{y}$ — принятый вектор. Для того чтобы исправить ошибки, имеющиеся в $\mathbf{y}$, вычислим $S(\mathbf{y})$ и найдем такой лидер смежного класса $\mathbf{e}$, синдром которого равен $S(\mathbf{y})$. Тогда декодируем $\mathbf{y}$ как $\mathbf{x} = \mathbf{y} - \mathbf{e}$. Здесь $\mathbf{x}$ — кодовое слово, находящееся на минимальном расстоянии от $\mathbf{y}$.

9.20. Пример. Пусть C — бинарный линейный (4, 2)-код с порождающей матрицей G и проверочной матрицей H:

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Если получено слово $\mathbf{y} = 1110$, то можно просто посмотреть, где оно встречается в приводимой на следующей странице таблице смежных классов.

Однако для больших таблиц этот процесс требует большой затраты времени. Следуя алгоритму, найдем сначала $S(\mathbf{y})$:

передаваемая информация	00	10	01	11	
кодовые слова	0000	1010	0111	1101	$\binom{0}{0}$
другие смежные классы	1000	0010	1111	0101	$\binom{1}{0}$
	0100	1110	0011	1001	$\binom{1}{1}$
	0001	1011	0110	1100	$\binom{0}{1}$
	лидеры смежных классов				синдромы

в нашем случае $S(\mathbf{y}) = H\mathbf{y}^{\mathrm{T}} = \binom{1}{1}$. Полагаем теперь, что ошибка, наложившаяся на передававшееся кодовое слово, равняется лидеру смежного класса 0100, имеющему тот же синдром $\binom{1}{1}$. Тогда передававшееся кодовое слово скорее всего было словом 1010, а сообщение, которое передавали, имело вид 10. □

В случае линейных кодов с большими параметрами становится практически невозможным найти лидеров смежных классов. Так, например, линейный (50, 20)-код над полем $\mathbb{F}_2$ имеет около 10^9 смежных классов. Таким образом, чтобы преодолеть подобные затруднения, необходимо строить специальные коды. Вначале отметим следующее обстоятельство.

9.21. Теорема. *В случае бинарного линейного (n, k)-кода с проверочной матрицей H синдром получаемого вектора $\mathbf{y}$ равняется сумме столбцов матрицы H, которые соответствуют тем координатам передававшегося кодового слова $\mathbf{x}$, в которых появились ошибки.*

Доказательство. Пусть $\mathbf{y} \in \mathbb{F}_2^n$ — полученный вектор, $\mathbf{y} = \mathbf{x} + \mathbf{e}$, $\mathbf{x} \in C$; тогда из (9.2) получаем, что $S(\mathbf{y}) = H\mathbf{e}^{\mathrm{T}}$. Пусть $i_1, i_2, \ldots$ — координаты с ошибками, т. е. $\mathbf{e} = 0 \ldots 01_{i_1}0 \ldots 01_{i_2}0 \ldots$. Тогда $S(\mathbf{y}) = \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \ldots$, где $\mathbf{h}_i$ означает i-й столбец матрицы H. □

Если все столбцы матрицы H различны, то наличие единственной ошибки в i-й координате полученного слова приводит к тому, что $S(\mathbf{y}) = \mathbf{h}_i$, и, таким образом, одна ошибка может быть исправлена. Локализация ошибок упрощается при использовании следующего класса кодов.

9.22. Определение. Бинарный код C_m длины $n = 2^m - 1$, $m \geqslant 2$, с проверочной матрицей H размера $m \times (2^m - 1)$ назы-

вается *бинарным кодом Хэмминга*, если столбцы матрицы H представляют собой двоичную запись чисел $1, 2, \ldots, 2^m - 1$.

9.23. Лемма. *Бинарный код C_m является кодом размерности $2^m - m - 1$, исправляющим одну ошибку.*

Доказательство. По определению проверочной матрицы H кода C_m ее ранг равняется m. Кроме того, любые два столбца этой матрицы линейно независимы. Так как матрица H вместе с любыми двумя столбцами содержит также столбец, равный их сумме, то по лемме 9.14 минимальное расстояние кода C_m равняется 3. Таким образом, в силу теоремы 9.12 код C_m является кодом, исправляющим одну ошибку. □

9.24. Пример. Пусть C_3 является (7,4)-кодом Хэмминга с проверочной матрицей

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Если синдром полученного слова $\mathbf{y}$ равняется, например, $S(\mathbf{y}) = (1\ 0\ 1)^{\mathrm{T}}$, то отсюда мы заключаем, что имеется ошибка в пятой координате, так как 101 является бинарной записью числа 5. □

Коды Хэмминга можно также определить и для небинарного случая, т. е. над произвольным конечным полем $\mathbb{F}_q$. Здесь проверочная матрица H имеет размер $m \times [(q^m - 1)/(q - 1)]$ и столбцы этой матрицы попарно линейно независимы. Такая матрица определяет линейный $((q^m - 1)/(q - 1),\ (q^m - 1)/(q - 1) - m)$-код с минимальным расстоянием, равным 3.

Опишем теперь некоторые соотношения между длиной n кодовых слов, числом k информационных символов и минимальным расстоянием d_C линейного кода C над полем $\mathbb{F}_q$.

9.25. Теорема (граница Хэмминга). *Пусть C — код над полем $\mathbb{F}_q$, исправляющий t ошибок и содержащий M кодовых слов, а n — длина этого кода. Тогда*

$$M\left(1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t\right) \leqslant q^n.$$

Доказательство. Имеется ровно $\binom{n}{m}(q-1)^m$ векторов над полем $\mathbb{F}_q$ длины n и веса m. Все шары радиуса t с центрами в кодовых словах попарно не пересекаются, и каждый из M шаров содержит

$$1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t$$

векторов пространства $\mathbb{F}_q^n$, которое само содержит q^n векторов. □

9.26. Теорема (граница Плоткина). *Для линейного (n, k)-кода C над полем $\mathbb{F}_q$ с минимальным расстоянием d_C выполняется неравенство*

$$d_C \leqslant \frac{nq^{k-1}(q-1)}{q^k-1}.$$

Доказательство. Пусть $1 \leqslant i \leqslant n$ таково, что C содержит кодовое слово с ненулевой i-й координатой. Пусть D — подпространство в C, состоящее из всех кодовых слов с i-й координатой, равной 0. Тогда факторпространство C/D содержит q элементов, которые соответствуют q возможностям выбора i-й компоненты в кодом слове. Таким образом, из равенства $|C|/|D| = |C/D|$ вытекает, что $|D| = q^{k-1}$. Подсчитывая сумму весов кодовых слов из C, получаем, что она не превышает величины $nq^{k-1}(q-1)$. Минимальное расстояние d_C кода C равняется минимальному весу ненулевого слова и, следовательно, должно удовлетворять доказываемому неравенству, так как общее число кодовых слов ненулевого веса равно $q^k - 1$. □

9.27. Теорема (граница Варшамова—Гилберта). *Если выполняется неравенство*

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i,$$

то существует линейный (n, k)-код над полем $\mathbb{F}_q$ с минимальным расстоянием, не меньшим чем d.

Доказательство. Докажем эту теорему путем построения проверочной $(n-k) \times n$-матрицы H искомого кода. В качестве первого столбца матрицы H выберем произвольный набор длины $n-k$ элементов поля $\mathbb{F}_q$. В качестве второго столбца возьмем любой набор той же длины элементов $\mathbb{F}_q$, подчиненный единственному условию, чтобы он не равнялся произведению первого столбца на элемент поля $\mathbb{F}_q$. Вообще предположим, что выбрано $j-1$ столбцов, причем любые $d-1$ из них являются линейно независимыми. Тогда имеется не более

$$\sum_{i=0}^{d-2} \binom{j-1}{i} (q-1)^i$$

векторов, которые являются линейными комбинациями не более чем $d-2$ векторов из числа выбранных $j-1$ вектор-столбцов. Если выполняется неравенство, приведенное в условии теоремы, то можно выбрать j-й столбец таким образом, чтобы он был линейно независимым от любых $d-2$ столбцов из числа первых $j-1$ столбцов. Указанное построение можно проделать таким

образом, что ранг матрицы H будет равен $n - k$. По лемме 9.14 полученный в результате код будет иметь минимальное расстояние, не меньше чем d. □

Для данного линейного кода C можно ввести понятие дуального кода. Пусть даны кодовые слова $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$. Тогда их *скалярное произведение* $\mathbf{u} \cdot \mathbf{v}$ определим равенством $\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \ldots + u_n v_n$. Если $\mathbf{u} \cdot \mathbf{v} = 0$, то слова $\mathbf{u}$ и $\mathbf{v}$ называются *ортогональными*.

9.28. Определение. Пусть C — линейный (n, k)-код над полем $\mathbb{F}_q$. Тогда соответствующий *дуальный* (или *ортогональный*) *код* $C^\perp$ определяется как

$$C^\perp = \{\mathbf{u} \in \mathbb{F}_q^n \mid \mathbf{u} \cdot \mathbf{v} = 0 \quad \text{для всех } \mathbf{v} \in C\}.$$

Мы знаем, что код C является k-мерным подпространством n-мерного пространства $\mathbb{F}_q^n$; размерность же подпространства $C^\perp$ равна $n - k$. Код $C^\perp$ является линейным $(n, n - k)$-кодом. Нетрудно показать, что его порождающей матрицей будет матрица H — проверочная матрица кода C. Соответственно проверочной матрицей кода $C^\perp$ является матрица G — порождающая матрица кода C.

Важную информацию о коде можно получить, изучая вес кодовых слов. Так, например, при определении вероятности ошибки декодирования или при исследовании некоторых алгоритмов декодирования важно знать распределение весов кодовых слов. Существует фундаментальная связь между распределением весов в линейном коде и в его дуальном коде, которая устанавливается в теореме 9.32.

9.29. Определение. Пусть A_i обозначает число кодовых слов $\mathbf{c} \in C$ веса i, где $0 \leqslant i \leqslant n$. Тогда многочлен

$$A(x, y) = \sum_{i=0}^{n} A_i x^i y^{n-i}$$

от двух переменных x и y над полем комплексных чисел называется *нумератором весов* или *весовой функцией кода* C.

Далее нам понадобится понятие характера конечного поля (см. гл. 5).

9.30. Определение. Пусть χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$, и пусть $\mathbf{u} \cdot \mathbf{v}$ обозначает скалярное произведение векторов $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$. Для фиксированного $\mathbf{v} \in \mathbb{F}_q^n$ определим отображение $\chi_{\mathbf{v}}: \mathbb{F}_q^n \to \mathbb{C}$ равенством

$$\chi_{\mathbf{v}}(\mathbf{u}) = \chi(\mathbf{v} \cdot \mathbf{u}), \quad \mathbf{u} \in \mathbb{F}_q^n.$$

Если V — векторное пространство над полем $\mathbb{C}$ комплексных чисел, а f – отображение из $\mathbb{F}_q^n$ в V, то определим отображение g_f $\mathbb{F}_q^n \to V$ равенством

$$g_f(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{F}_q^n} \chi_{\mathbf{v}}(\mathbf{u}) f(\mathbf{v}), \quad \mathbf{u} \in \mathbb{F}_q^n.$$

9.31. Лемма. *Пусть E — подпространство пространства $\mathbb{F}_q^n$ $E^\perp$ – его ортогональное дополнение, f: $\mathbb{F}_q^n \to V$ — отображение из векторного пространства $\mathbb{F}_q^n$ в векторное пространство V над полем $\mathbb{C}$, а χ — нетривиальный аддитивный характер поля $\mathbb{F}_q$ Тогда*

$$\sum_{\mathbf{u} \in E} g_f(\mathbf{u}) = |E| \sum_{\mathbf{v} \in E^\perp} f(\mathbf{v}).$$

Доказательство.

$$\sum_{\mathbf{u} \in E} g_f(\mathbf{u}) = \sum_{\mathbf{u} \in E} \sum_{\mathbf{v} \in \mathbb{F}_q^n} \chi_{\mathbf{v}}(\mathbf{u}) f(\mathbf{v}) = \sum_{\mathbf{v} \in \mathbb{F}_q^n} \sum_{\mathbf{u} \in E} \chi(\mathbf{v} \cdot \mathbf{u}) f(\mathbf{v}) =$$

$$= |E| \sum_{\mathbf{v} \in E^\perp} f(\mathbf{v}) + \sum_{\mathbf{v} \notin E^\perp} \sum_{c \in \mathbb{F}_q} \sum_{\substack{\mathbf{u} \in E \\ \mathbf{v} \cdot \mathbf{u} = c}} \chi(c) f(\mathbf{v}).$$

Для фиксированного $\mathbf{v} \notin E^\perp$ отображение $\mathbf{u} \in E \longmapsto \mathbf{v} \cdot \mathbf{u}$ является нетривиальным линейным функционалом на E. Тогда, используя формулу (5.9), получаем

$$\sum_{\mathbf{u} \in E} g_f(\mathbf{u}) = |E| \sum_{\mathbf{v} \in E^\perp} f(\mathbf{v}) + \frac{|E|}{q} \sum_{\mathbf{v} \notin E^\perp} f(\mathbf{v}) \sum_{c \in \mathbb{F}_q} \chi(c) =$$

$$= |E| \sum_{\mathbf{v} \in E^\perp} f(\mathbf{v}). \qquad \square$$

Применим теперь эту лемму в случае, когда V — пространство комплексных многочленов от двух переменных x, y, а отображение f определяется по формуле $f(\mathbf{v}) = x^{w(\mathbf{v})} y^{n - w(\mathbf{v})}$, где $w(\mathbf{v})$ обозначает вес вектора $\mathbf{v} \in \mathbb{F}_q^n$.

9.32. Теорема (тождество Мак-Вильямс). *Пусть C — линейный (n, k)-код над полем $\mathbb{F}_q$, а $C^\perp$ — его дуальный код. Если $A(x, y)$ — весовая функция кода C, а $A^\perp(x, y)$ — весовая функция кода $C^\perp$, то*

$$A^\perp(x, y) = q^{-k} A(y - x, y + (q - 1)x).$$

Доказательство. Пусть f: $\mathbb{F}_q^n \to \mathbb{C}[x, y]$ — определенное выше отображение; тогда весовую функцию кода $C^\perp$ можно представить в виде

$$A^\perp(x, y) = \sum_{\mathbf{v} \in C^\perp} f(\mathbf{v}).$$

Пусть g_f — отображение, заданное выше (см. определение 9.30). Для $v \in \mathbb{F}_q$ положим

$$|v| = \begin{cases} 1, & \text{если } v \neq 0, \\ 0, & \text{если } v = 0. \end{cases}$$

Тогда для $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ получаем

$$g_f(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{F}_q^n} \chi(\mathbf{v} \cdot \mathbf{u})\, x^{w(\mathbf{v})} y^{n-w(\mathbf{v})} =$$

$$= \sum_{v_1, \ldots, v_n \in \mathbb{F}_q} \chi(u_1 v_1 + \cdots + u_n v_n) \cdot$$

$$\cdot x^{|v_1| + \cdots + |v_n|} y^{(1-|v_1|) + \cdots + (1-|v_n|)} =$$

$$= \sum_{v_1, \ldots, v_n \in \mathbb{F}_q} \prod_{i=1}^{n} [\chi(u_i v_i)\, x^{|v_i|} y^{1-|v_i|}] =$$

$$= \prod_{i=1}^{n} \sum_{v \in \mathbb{F}_q} [\chi(u_i v)\, x^{|v|} y^{1-|v|}].$$

В случае когда $u_i = 0$, справедливо равенство $\chi(u_i v) = \chi(0) = 1$, а следовательно, соответствующий сомножитель в последнем произведении равен $(q-1)x + y$. При $u_i \neq 0$ соответствующий сомножитель равняется

$$y + x \sum_{v \in \mathbb{F}_q^*} \chi(v) = y - x.$$

Таким образом,

$$g_f(\mathbf{u}) = (y-x)^{w(\mathbf{u})} (y + (q-1)x)^{n-w(\mathbf{u})}.$$

Из леммы 9.31 следует, что

$$|C|\, A^{\perp}(x, y) = |C| \sum_{\mathbf{v} \in C^{\perp}} f(\mathbf{v}) = \sum_{\mathbf{u} \in C} g_f(\mathbf{u}) = A(y-x, y + (q-1)x).$$

И наконец, $|C| = q^k$ по условию теоремы. Тем самым теорема доказана. □

9.33. Следствие. *В весовых функциях $A(x, y)$ и $A^{\perp}(x, y)$ положим $x = z$, $y = 1$. Полученные при этом многочлены обозначим через $A(z)$ и $A^{\perp}(z)$ соответственно. Тогда тождество Мак-Вильямс можно записать в виде*

$$A^{\perp}(z) = q^{-k} (1 + (q-1)z)^n A\left(\frac{1-z}{1 + (q-1)z}\right).$$

9.34. Пример. Пусть C_m — бинарный код Хэмминга длины $n = 2^m - 1$ и размерности $n - m$ над $\mathbb{F}_2$. Порождающей матрицей его дуального кода $C_m^{\perp}$ является проверочная матрица H

кода C_m. Эта матрица состоит из всех возможных ненулевых столбцов длины m над полем $\mathbb{F}_2$. Код $C_m^\perp$ состоит из нулевого вектора и $2^m - 1$ векторов веса 2^{m-1}. Таким образом, весовая функция кода $C_m^\perp$ равняется

$$y^n + (2^m - 1)\, x^{2^{m-1}} y^{2^{m-1}-1}.$$

По теореме 9.32 весовая функция кода C_m определяется формулой

$$A(x, y) = \frac{1}{n+1}\,[(y+x)^n + n(y-x)^{(n+1)/2}(y+x)^{(n-1)/2}].$$

Пусть $A(z) = A(z, 1)$, т. е. $A(z) = \sum_{i=0}^{n} A_i z^i$. Тогда нетрудно проверить, что $A(z)$ удовлетворяет дифференциальному уравнению

$$(1 - z^2)\frac{dA(z)}{dz} + (1 + nz)A(z) = (1+z)^n$$

с начальным условием $A(0) = A_0 = 1$. Это эквивалентно соотношению

$$iA_i = \binom{n}{i-1} - A_{i-1} - (n - i + 2)A_{i-2}, \quad i = 2, 3, \ldots, n,$$

с начальными условиями $A_0 = 1$, $A_1 = 0$. □

§ 2. Циклические коды

Циклические коды — это особая разновидность линейных кодов, они отличаются достаточно хорошо изученной математической структурой и удивительно просты в реализации.

9.35. Определение. Линейный (n, k)-код C над полем $\mathbb{F}_q$ называется *циклическим*, если из того, что вектор $(a_0, a_1, \ldots, a_{n-1})$ принадлежит C, следует, что его циклический сдвиг $(a_{n-1}, a_0, \ldots, a_{n-2})$ принадлежит C.

С настоящего момента мы будем предполагать, что НОД $(n, q) = 1$. Обозначим через $(x^n - 1)$ идеал кольца $\mathbb{F}_q[x]$, порожденный многочленом $x^n - 1 \in \mathbb{F}_q[x]$. Тогда все элементы факторкольца $\mathbb{F}_q[x]/(x^n - 1)$ можно представлять многочленами степени, меньшей чем n. Очевидно, что это факторкольцо изоморфно $\mathbb{F}_q^n$ как векторное пространство над полем $\mathbb{F}_q$, а изоморфизм имеет вид

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

В силу существования указанного изоморфизма мы будем представлять элементы $\mathbb{F}_q[x]/(x^n - 1)$ или в виде многочленов степени, меньшей чем n, которые рассматриваются по модулю $x^n - 1$, или в виде векторов или слов над полем $\mathbb{F}_q$. Умножение

многочленов по модулю $x^n - 1$ мы определяем обычным образом: если $f \in \mathbb{F}_q[x]/(x^n - 1)$, $g_1, g_2 \in \mathbb{F}_q[x]$, то $g_1 g_2 = f$ означает, что $g_1 g_2 \equiv f \pmod{(x^n - 1)}$.

Циклический (n, k)-код C можно получить путем умножения каждого сообщения, содержащего k информационных символов (и которое мы отождествляем с многочленом степени, меньшей чем k), на фиксированный многочлен $g(x)$ степени $n - k$, где $g(x)$ является делителем $x^n - 1$. Многочлены $g(x)$, $xg(x)$, ..., $x^{k-1}g(x)$ соответствуют кодовым словам кода C. Порождающая матрица кода C имеет вид

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix},$$

где $g(x) = g_0 + g_1 x + \dots + g_{n-k}x^{n-k}$. Очевидно, что строки матрицы G линейно независимы, и, таким образом, ранг матрицы G равен k — размерности кода C. Если

$$h(x) = (x^n - 1)/g(x) = h_0 + h_1(x) + \dots + h_k x^k,$$

то матрица

$$H = \begin{pmatrix} 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \\ 0 & 0 & \dots & h_k & h_{k-1} & \dots & h_0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

является проверочной матрицей кода C. Код с порождающей матрицей H, т. е. код, дуальный к коду C, также является циклическим кодом.

Так как мы отождествляем векторы $(a_0, a_1, \dots, a_{n-1})$ над полем $\mathbb{F}_q$ и многочлены $a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$ над тем же полем, то код C можно рассматривать как подмножество фактор-кольца $\mathbb{F}_q[x]/(x^n - 1)$.

9.36. Теорема. *Линейный код C является циклическим тогда и только тогда, когда он будет идеалом кольца $\mathbb{F}_q[x]/(x^n - 1)$.*

Доказательство. Если C является идеалом и $(a_0, a_1, \dots, a_{n-1}) \in C$, то и

$$x \cdot (a_0 + a_1 x + \dots + a_{n-1}x^{n-1}) = (a_{n-1}, a_0, \dots, a_{n-2}) \in C.$$

Обратно, если из того, что $(a_0, a_1, \dots, a_{n-1}) \in C$, следует, что и $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$, то для любого многочлена $a(x) \in C$ многочлен $x \cdot a(x)$ также принадлежит C, а следовательно, и $x^2 a(x) \in C$, $x^3 a(x) \in C$ и т. д. Тогда для любого многочлена $b(x)$ произведение $b(x) \cdot a(x)$ принадлежит C. Последнее означает, что C является идеалом. □

Каждый идеал кольца $\mathbb{F}_q[x]/(x^n - 1)$ является главным; в частности, любой ненулевой идеал C порождается нормированным многочленом степени, меньшей чем n, и если обозначить этот многочлен через $g(x)$, то $g(x)$ делит $x^n - 1$.

9.37. **Определение.** Пусть $C = (g(x))$ — циклический код. Тогда многочлен $g(x)$ называется *порождающим многочленом* кода C, а многочлен $h(x) = (x^n - 1)/g(x)$ называется *проверочным многочленом* кода C.

Пусть $x^n - 1 = f_1(x) f_2(x) \dots f_m(x)$ — разложение многочлена $x^n - 1$ на нормированные неприводимые многочлены над полем $\mathbb{F}_q$. В силу предположения о том, что НОД $(n, q) = 1$, получаем, что кратные сомножители в этом разложении отсутствуют. Если многочлен $f_i(x)$ неприводим над полем $\mathbb{F}_q$, то идеал $(f_i(x))$ является максимальным идеалом, а циклический код порожденный многочленом $f_i(x)$, называется *максимальным циклическим кодом*. Код, порожденный многочленом $(x^n - 1)/f_i(x)$, называется *неприводимым циклическим кодом*. Можно найти все циклические коды длины n над $\mathbb{F}_q$, разлагая многочлен $x^n - 1$ на множители указанным выше образом и выбирая в качестве порождающего многочлена любой из $2^m - 2$ нетривиальных нормированных делителей многочлена $x^n - 1$.

Если $h(x)$ — проверочный многочлен циклического кода $C \subseteq \mathbb{F}_q[x]/(x^n - 1)$, а $v(x) \in \mathbb{F}_q[x]/(x^n - 1)$, то $v(x) \in C$ тогда и только тогда, когда $v(x) h(x) \equiv 0 \pmod{(x^n - 1)}$. Многочлен $a(x) = a_0 + a_1 x + \dots + a_{k-1} x^{k-1}$, соответствующий передаваемой информации, кодируется кодом C в многочлен $w(x) = a(x) \cdot g(x)$, где $g(x)$ — порождающий многочлен этого кода. Если многочлен $v(x)$, соответствующий принимаемой информации, разделить на $g(x)$, то получение ненулевого остатка означает наличие ошибки в принятом сообщении. Каноническую порождающую матрицу кода C можно получить следующим образом. Пусть $\deg(g(x)) = n - k$. Тогда существуют единственным образом определяемые многочлены $a_j(x)$ и $r_j(x)$, такие, что $\deg(r_j(x)) < n - k$ и

$$x^j = a_j(x) g(x) + r_j(x).$$

Следовательно, $x^j - r_j(x)$ является кодовым многочленом; кодовым является и многочлен $g_j(x) = x^k (x^j - r_j(x))$, взятый по модулю $x^n - 1$. Многочлены $g_j(x)$, $j = n - k, \dots, n - 1$, линейно независимы и образуют каноническую порождающую матрицу $(I_k \; R)$, где I_k — единичная матрица размера $k \times k$, а R — матрица размера $k \times (n - k)$, i-я строка которой образована коэффициентами многочлена $r_{n-k-1+i}(x)$.

9.38. **Пример.** Пусть $n = 7$, $q = 2$. Тогда

$$x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Многочлен $g(x) = x^3 + x^2 + 1$ порождает циклический (7,4)-код с проверочным многочленом $h(x) = x^4 + x^3 + x^2 + 1$. Соответствующая каноническая порождающая матрица G и проверочная матрица H имеют вид .

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \quad \square$$

Напомним полученный в гл. 8 результат о том, что если $f \in \mathbb{F}_q[x]$ — многочлен вида

$$f(x) = f_0 + f_1 x + \cdots + f_k x^k, \quad f_0 \neq 0, \ f_k = 1,$$

то решениями линейного рекуррентного соотношения

$$\sum_{j=0}^{k} f_j a_{i+j} = 0, \quad i = 0, 1, \ldots,$$

являются чисто периодические последовательности с периодом, равным n. Множество n-наборов, состоящих из первых n членов каждого такого решения и рассматриваемых как многочлены по модулю $x^n - 1$, образует идеал, порожденный в кольце $\mathbb{F}_q[x]/(x^n - 1)$ многочленом $g(x)$. Здесь $g(x)$ — многочлен степени $n - k$, возвратный к многочлену $(x^n - 1)/f(x)$ [1]). Таким образом, *можно использовать для получения кодовых слов в циклических кодах линейные рекуррентные соотношения*, причем этот процесс можно легко реализовать технически с помощью регистров сдвига.

9.39. Пример. Пусть $f(x) = x^3 + x + 1$ — делитель многочлена $x^7 - 1$ над полем $\mathbb{F}_2$. Соответствующее линейное рекуррентное соотношение имеет вид $a_{i+3} + a_{i+1} + a_i = 0$. Оно порождает циклический (7,3)-код, который, например, кодирует слово 111 в слово 1110010. Порождающим многочленом в этом случае является многочлен, возвратный к многочлену $(x^7 - 1)/f(x)$, т. е. $g(x) = x^4 + x^3 + x^2 + 1$. $\square$

Циклические коды можно также описать путем задания корней всех кодовых многочленов, перейдя в соответствующее расширение поля $\mathbb{F}_q$. Условие, что все кодовые многочлены делятся на порождающий многочлен $g(x)$ циклического кода, означает просто, что все кодовые многочлены должны принимать значение 0 на корнях многочлена $g(x)$. Пусть $\alpha_1, \ldots, \alpha_s$ — элементы фиксированного расширения поля $\mathbb{F}_q$, а $p_i(x)$, $i = 1, \ldots, s$, — минимальный многочлен элемента α_i над полем $\mathbb{F}_q$. Пусть $n \in \mathbb{N}$ таково, что $\alpha_i^n = 1$ для всех $i = 1, \ldots, s$. Положим $g(x) = \text{НОК}(p_1(x), \ldots$

[1]) См. гл. 8, § 3. — *Прим. перев.*

..., $p_s(x)$). Тогда многочлен $g(x)$ делит $x^n - 1$. Если $C \subseteq \mathbb{F}_q^n$ — циклический код с порождающим многочленом $g(x)$, то $v(x) \in C$ тогда и только тогда, когда $v(\alpha_i) = 0$, $i = 1, \ldots, s$. В качестве примера того, как связаны описания циклического кода с помощью порождающего многочлена и с помощью кодовых многочленов, докажем следующий результат. При этом используется понятие эквивалентности кодов, определяемое в упр. 9.10.

9.40. Теорема. *Бинарный циклический код длины $n = 2^m - 1$, порождающий многочлен которого является минимальным многочленом над полем $\mathbb{F}_2$ для некоторого примитивного элемента поля $\mathbb{F}_{2^m}$, эквивалентен бинарному $(n, n - m)$-коду Хэмминга.*

Доказательство. Обозначим через α примитивный элемент поля $\mathbb{F}_{2^m}$, и пусть

$$p(x) = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{2^{m-1}})$$

— минимальный многочлен элемента α над полем $\mathbb{F}_2$. Рассмотрим теперь циклический код C, порожденный многочленом $p(x)$. Построим матрицу H размера $m \times (2^m - 1)$, j-й столбец которой имеет вид $(c_0, c_1, \ldots, c_{m-1})^{\mathrm{T}}$, где $c_i \in \mathbb{F}_2$ и

$$\alpha^{j-1} = \sum_{i=0}^{m-1} c_i \alpha^i, \quad j = 1, 2, \ldots, 2^m - 1.$$

Если $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ и $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_2[x]$, то вектор $H\mathbf{a}^{\mathrm{T}}$ соответствует элементу $a(\alpha)$, выраженному в базисе $\{1, \alpha, \ldots, \alpha^{m-1}\}$. Следовательно, равенство $H\mathbf{a}^{\mathrm{T}} = \mathbf{0}$ выполняется только тогда, когда минимальный многочлен $p(x)$ делит $a(x)$. Таким образом, матрица H является проверочной матрицей кода C. В силу того что столбцы матрицы H представляют собой перестановку двоичной записи чисел 1, 2, ..., $2^m - 1$, все они различны. Теорема доказана. □

9.41. Пример. Многочлен $x^4 + x + 1$ является примитивным многочленом над полем $\mathbb{F}_2$, и, следовательно, его корнем будет примитивный элемент $\alpha \in \mathbb{F}_{16}$. Если для всех 15 элементов $\alpha^j \in \mathbb{F}_{16}^*$, $j = 0, 1, \ldots, 14$, воспользоваться векторной записью, выражая их в базисе $\{1, \alpha, \alpha^2, \alpha^3\}$, и из полученных векторов, используя их как столбцы, образовать матрицу размера 4×15, то мы получим проверочную матрицу кода, эквивалентного (15, 11)-коду Хэмминга. При этом сообщение вида $(a_0, a_1, \ldots, a_{10})$ кодируется в кодовый многочлен

$$w(x) = a(x)(x^4 + x + 1),$$

где $a(x) = a_0 + a_1 x + \cdots + a_{10}x^{10}$. Предположим теперь, что многочлен $v(x)$, соответствующий полученному сообщению, содержит одну ошибку, т. е. что $v(x) = w(x) + x^{e-1}$, в то время

как передавалось сообщение, соответствующее многочлену $w(x)$. Тогда синдром равняется $w(\alpha) + \alpha^{e-1} = \alpha^{e-1}$. Отсюда получатель заключает, что в принятом сообщении на месте с номером e имеется ошибка. □

9.42. Теорема. *Пусть $C \subseteq \mathbb{F}_q[x]/(x^n - 1)$ циклический код с порождающим многочленом $g(x)$, и пусть $\alpha_1, \ldots, \alpha_{n-k}$ — корни многочлена $g(x)$. В этом случае многочлен $f \in \mathbb{F}_q[x]/(x^n - 1)$ является кодовым многочленом тогда и только тогда, когда вектор $(f_0, f_1, \ldots, f_{n-1})$, образованный коэффициентами многочлена f, лежит в нуль-пространстве матрицы*

$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \ldots & \alpha_{n-k}^{n-1} \end{pmatrix}. \tag{9.3}$$

Доказательство. Пусть $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$; тогда $f(\alpha_i) = f_0 + f_1\alpha_i + \cdots + f_{n-1}\alpha_i^{n-1} = 0$ для всех $1 \leqslant i \leqslant n - k$, а это значит, что

$$(1, \alpha_i, \ldots, \alpha_i^{n-1})(f_0, f_1, \ldots, f_{n-1})^{\mathrm{T}} = 0, \quad 1 \leqslant i \leqslant n - k,$$

тогда и только тогда, когда $H(f_0, f_1, \ldots, f_{n-1})^{\mathrm{T}} = 0$. □

Напомним (см. § 1), что для исправления ошибки в полученном слове $\mathbf{y}$ необходимо определить синдром этого слова. В случае циклического кода синдром, который является вектором длины $n - k$, часто бывает возможно заменить другим более простым объектом. Например, пусть α — примитивный корень n-й степени из 1 в поле $\mathbb{F}_{q^m}$, и пусть $g(x)$ — порождающий многочлен кода — является минимальным многочленом элемента α над полем $\mathbb{F}_q$. В силу того что g делит многочлен $f \in \mathbb{F}_q[x]/(x^n - 1)$ тогда и только тогда, когда $f(\alpha) = 0$, матрицу H из (9.3) можно заменить матрицей H вида

$$H = (1\ \alpha\ \alpha^2\ \ldots\ \alpha^{n-1}).$$

Тогда в роли синдрома выступает вектор $S(\mathbf{y}) = H\mathbf{y}^{\mathrm{T}}$, причем $S(\mathbf{y}) = y(\alpha)$, так как $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$ можно рассматривать как многочлен $y(x)$ с коэффициентами y_i. Далее, будем обозначать через $\mathbf{w}$ передаваемое слово, через $\mathbf{v}$ — принимаемое слово, а через $w(x)$ и $v(x)$ — соответствующие многочлены. Предположим, что $e^{(j)}(x) = x^{j-1}$, $1 \leqslant j \leqslant n$, — многочлен ошибок, соответствующий единственной ошибке, и пусть $\mathbf{v} = \mathbf{w} + \mathbf{e}^{(j)}$. Тогда

$$v(\alpha) = w(\alpha) + e^{(j)}(\alpha) = e^{(j)}(\alpha) = \alpha^{j-1}.$$

Величина $e^{(j)}(\alpha)$ называется *локатором ошибки*. В этом случае синдром $S(\mathbf{v}) = \alpha^{j-1}$ однозначно определяет ошибку, так как $e^{(i)}(\alpha) \neq e^{(j)}(\alpha)$ при $1 \leqslant i, j \leqslant n$ и $i \neq j$.

Прежде чем переходить к циклическим кодам общего вида, рассмотрим следующий пример.

9.43. **Пример.** Пусть элемент $\alpha \in \mathbb{F}_{16}$ — корень многочлена $x^4 + x + 1 \in \mathbb{F}_2[x]$. Тогда минимальными многочленами элементов α и α^3 над полем $\mathbb{F}_2$ являются соответственно $m^{(1)}(x) = x^4 + x + 1$ и $m^{(3)}(x) = x^4 + x^3 + x^2 + x + 1$. Оба многочлена $m^{(1)}(x)$ и $m^{(3)}(x)$ суть делители многочлена $x^{15} - 1$. Теперь мы можем определить бинарный циклический код C с порождающим многочленом $g = m^{(1)}m^{(3)}$. Так как g делит многочлен $f \in \mathbb{F}_2[x]/(x^{15} - 1)$ тогда и только тогда, когда $f(\alpha) = f(\alpha^3) = 0$, то матрицу H в (9.3) можно заменить матрицей H вида

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{42} \end{pmatrix}.$$

Ниже мы покажем (см. теорему 9.45 и пример 9.47), что минимальное расстояние кода C не меньше 5; следовательно, код C может исправлять 2 ошибки. Код C является циклическим (15,7)-кодом. Пусть

$$S_1 = \sum_{i=0}^{14} v_i \alpha^i, \quad S_3 = \sum_{i=0}^{14} v_i \alpha^{3i}$$

— компоненты синдрома $S(\mathbf{v}) = H\mathbf{v}^{\mathrm{T}}$. Тогда $\mathbf{v} \in C$ в том и только том случае, когда $S(\mathbf{v}) = H\mathbf{v}^{\mathrm{T}} = \mathbf{0}$. В свою очередь это соотношение равносильно тому, что $S_1 = S_3 = 0$. Если элементы поля $\mathbb{F}_{16}$ представить в двоичной векторной записи, т. е. вместо элемента α^k поместить соответствующий вектор-столбец, то указанная выше матрица H принимает вид

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

При этом столбцы матрицы H определялись следующим образом: первые 4 координаты 1-го столбца являются коэффициентами в записи элемента 1 в виде $1 = 1 \cdot \alpha^0 + 0 \cdot \alpha^1 + 0 \cdot \alpha^2 + 0 \cdot \alpha^3$, первые 4 координаты 2-го столбца являются коэффициентами в записи элемента α в виде $\alpha = 0 \cdot \alpha^0 + 1 \cdot \alpha^1 + 0 \cdot \alpha^2 + 0 \cdot \alpha^3$ и т. д. Последние 4 координаты 1-го столбца являются коэффи-

циентами в записи элемента 1 в виде $1 = 1\cdot\alpha^0 + 0\cdot\alpha^1 + 0\cdot\alpha^2 + 0\cdot\alpha^3$, последние 4 координаты 2-го столбца являются коэффициентами в записи элемента α^3 в виде $\alpha^3 = 0\cdot\alpha^0 + 0\cdot\alpha^1 + 0\cdot\alpha^2 + 1\cdot\alpha^3$ и т. д. Для вычисления используется соотношение $\alpha^4 + \alpha + 1 = 0$.

Допустим, что полученный вектор $\mathbf{v} = (v_0, \ldots, v_{14})$ содержит не более двух ошибок. Например, $e(x) = x^{a_1} + x^{a_2}$, где $0 \leqslant a_1, a_2 \leqslant 14$, $a_1 \neq a_2$. Тогда

$$S_1 = \alpha^{a_1} + \alpha^{a_2}, \quad S_3 = \alpha^{3a_1} + \alpha^{3a_2}.$$

Пусть $\eta_1 = \alpha^{a_1}$, $\eta_2 = \alpha^{a_2}$ — локаторы ошибок; значит,

$$S_1 = \eta_1 + \eta_2, \quad S_3 = \eta_1^3 + \eta_2^3,$$

поэтому

$$S_3 = S_1^3 + S_1^2\eta_1 + S_1\eta_1^2,$$

а следовательно,

$$1 + S_1\eta_1^{-1} + \left(S_1^2 + S_3S_1^{-1}\right)\eta_1^{-2} = 0.$$

Если имеется 2 ошибки, то η_1^{-1} и η_2^{-1} являются корнями многочлена

$$s(x) = 1 + S_1x + \left(S_1^2 + S_3S_1^{-1}\right)x^2. \tag{9.4}$$

Если имеется только одна ошибка, то $S_1 = \eta_1$, $S_3 = \eta_1^3$, а следовательно, $S_1^3 + S_3 = 0$, и тогда

$$s(x) = 1 + S_1x. \tag{9.5}$$

Если ошибок нет, то $S_1 = S_3 = 0$, и получено правильное кодовое слово $\mathbf{w}$.

Итак, в начале мы вычисляем синдром $S(\mathbf{v}) = H\mathbf{v}^{\mathrm{T}}$ для полученного вектора $\mathbf{v}$, затем найдем $s(x)$ и, наконец, с помощью корней многочлена $s(x)$ найдем ошибки. Если $S_1 \neq 0$, то многочлен, определенный формулой (9.5), имеет корень в поле $\mathbb{F}_{16}$. Если многочлен, заданный формулой (9.4), не имеет корней в поле $\mathbb{F}_{16}$, то мы получаем, что вектор ошибок $e(x)$ имеет более двух ненулевых компонент и, следовательно, эти ошибки нельзя исправить с помощью данного (15,7)-кода.

Пусть, например, полученное слово имеет вид

$$\mathbf{v} = 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0.$$

Тогда $S(\mathbf{v}) = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$ задается формулами

$$S_1 = 1 + \alpha^3 + \alpha^4 + \alpha^5 = \alpha^2 + \alpha^3.$$
$$S_3 = 1 + \alpha^9 + \alpha^{12} + \alpha^{15} = 1 + \alpha^2.$$

Многочлен $s(x)$ из (9.4) имеет вид

$$s(x) = 1 + (\alpha^2 + \alpha^3)\, x + [1 + \alpha + \alpha^2 + \alpha^3 + (1 + \alpha^2)(\alpha^2 + \alpha^3)^{-1}]\, x^2 = 1 + (\alpha^2 + \alpha^3)\, x + (1 + \alpha + \alpha^3)\, x^2.$$

Методом проб и ошибок найдем, что корни многочлена $s(x)$ равняются α и α^7. Следовательно, $\eta_1^{-1} = \alpha$, $\eta_2^{-1} = \alpha^7$, т. е. $\eta_1 = \alpha^{14}$, $\eta_2 = \alpha^8$. Таким образом, мы знаем, что ошибки должны находиться на местах, соответствующих x^8 и x^{14}, т. е. в 9-й и 15-й компонентах вектора $\mathbf{v}$. Переданное кодовое слово должно, следовательно, иметь вид

$$\mathbf{w} = 100111001000001.$$

Кодовое слово $\mathbf{w}$ декодируется путем деления соответствующего ему многочлена на порождающий многочлен $g(x)$. В результате мы получаем многочлен $1 + x^3 + x^5 + x^6$ и остаток, равный 0. Таким образом, заключаем, что переданное сообщение имело вид 1001011. □

9.44. Определение. Пусть b — целое неотрицательное число, и пусть $\alpha \in \mathbb{F}_{q^m}$ — примитивный корень n-й степени из 1, где m является мультипликативным порядком числа q по модулю n. Тогда *кодом Боуза — Чоудхури—Хоквингема* (или БЧХ-*кодом*) длины n с *конструктивным расстоянием* d, $2 \leqslant d \leqslant n$, над полем $\mathbb{F}_q$ называется циклический код, определяемый корнями порождающего многочлена

$$\alpha^b,\ \alpha^{b+1},\ \ldots,\ \alpha^{b+d-2}.$$

Если через $m^{(i)}(x)$ обозначить минимальный многочлен элемента α^i над полем $\mathbb{F}_q$, то порождающий многочлен $g(x)$ соответствующего БЧХ-кода имеет вид

$$g(x) = \text{НОК}\,(m^{(b)}(x),\ m^{(b+1)}(x),\ \ldots,\ m^{(b+d-2)}(x)).$$

Важны также и некоторые частные случаи общего определения 9.44. Так, если $b = 1$, то соответствующий БЧХ-код называется БЧХ-*кодом в узком смысле*. Если $n = q^m - 1$, то соответствующий БЧХ-код называется *примитивным*. Если $n = q - 1$, то БЧХ-код длины n над полем $\mathbb{F}_q$ называется *кодом Рида — Соломона*.

9.45. Теорема. *Минимальное расстояние* БЧХ-*кода с конструктивным расстоянием* d *не меньше, чем* d.

Доказательство. БЧХ-код совпадает с нуль-пространством проверочной матрицы

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \ldots & \alpha^{(n-1)(b+d-2)} \end{pmatrix}.$$

Покажем, что любые $d-1$ столбцов этой матрицы линейно независимы. Если мы рассмотрим определитель для любых $d-1$ различных столбцов матрицы H, то получим

$$\begin{vmatrix} \alpha^{bi_1} & \alpha^{bi_2} & \dots & \alpha^{bi_{d-1}} \\ \alpha^{(b+1)i_1} & \alpha^{(b+1)i_2} & \dots & \alpha^{(b+1)i_{d-1}} \\ \dots & \dots & \dots & \dots \\ \alpha^{(b+d-2)i_1} & \alpha^{(b+d-2)i_2} & \dots & \alpha^{(b+d-2)i_{d-1}} \end{vmatrix} =$$

$$= \alpha^{b(i_1+i_2+\dots+i_{d-1})} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{d-1}} \\ \dots & \dots & \dots & \dots \\ \alpha^{i_1(d-2)} & \alpha^{i_2(d-2)} & \dots & \alpha^{i_{d-1}(d-2)} \end{vmatrix} =$$

$$= \alpha^{b(i_1+i_2+\dots+i_{d-1})} \prod_{1 \leqslant k < j \leqslant d-1} (\alpha^{i_j} - \alpha^{i_k}) \neq 0.$$

Следовательно, минимальное расстояние этого кода не меньше, чем d.

9.46. Пример. Пусть $m^{(1)}(x) = x^4 + x + 1$ — минимальный многочлен над полем $\mathbb{F}_2$ для примитивного элемента $\alpha \in \mathbb{F}_{16}$. Представим степени α^i, $0 \leqslant i \leqslant 14$, в виде линейных комбинаций элементов 1, α, α^2, α^3 и получим, таким образом, проверочную матрицу H для кода, эквивалентного (15,11)-коду Хэмминга:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} =$$

$$= (1 \ \alpha \ \alpha^2 \ \alpha^3 \ \alpha^4 \ \alpha^5 \ \alpha^6 \ \alpha^7 \ \alpha^8 \ \alpha^9 \ \alpha^{10} \ \alpha^{11} \ \alpha^{12} \ \alpha^{13} \ \alpha^{14}).$$

Этот код можно также рассматривать как БЧХ-код в узком смысле над полем $\mathbb{F}_2$ с конструктивным расстоянием $d = 3$ (заметим, что элемент α^2 также является корнем многочлена $m^{(1)}(x)$). Минимальное расстояние этого кода также равно 3, поэтому он может исправлять одну ошибку. Для того чтобы декодировать полученный вектор $\mathbf{v} \in \mathbb{F}_2^{15}$, нам надо найти синдром $S(v) = H\mathbf{v}^{\mathrm{T}}$. В данном случае для циклического (15,11)-кода этот синдром определяется разложением элемента $v(\alpha)$ в базисе $\{1, \alpha, \alpha^2, \alpha^3\}$. Чтобы получить его, разделим $v(x)$ на $m^{(1)}(x)$. Пусть, скажем, $v(x) = a(x)\, m^{(1)}(x) + r(x)$, где $\deg(r(x)) < 4$; тогда $v(\alpha) = r(\alpha)$, так что компоненты синдрома равняются коэффициентам многочлена $r(x)$.

Например, пусть

$$\mathbf{v} = 0\,1\,0\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,1,$$

тогда $r(x) = 1 + x$ и, следовательно,

$$S(v) = H\mathbf{v}^{\mathrm{T}} = (1\ 1\ 0\ 0)^{\mathrm{T}} = 1 + \alpha.$$

Далее, нам надо найти вектор ошибки $\mathbf{e}$ веса $w(\mathbf{e}) \leqslant 1$, имеющий тот же самый синдром. Для этого мы должны определить j, $0 \leqslant j \leqslant 14$, такое, что $\alpha^j = H\mathbf{v}^{\mathrm{T}}$. В нашем случае $j = 4$, т. е. в полученном векторе $\mathbf{v}$ ошибочной является пятая координата, и, таким образом, переданное слово имело вид

$$\mathbf{w} = 010100001011101. \qquad \square$$

9.47. **Пример.** Пусть $q = 2$, $n = 15$, $d = 4$. Тогда многочлен $x^4 + x + 1$ является неприводимым над полем $\mathbb{F}_2$, а его корни — примитивные элементы поля $\mathbb{F}_{16}$. Если α — один из этих корней, то α^2 также является корнем этого многочлена, а α^3 — корень многочлена $x^4 + x^3 + x^2 + x + 1$. Тогда БЧХ-код в узком смысле с конструктивным расстоянием $d = 4$ может порождаться многочленом

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Этот многочлен будет также порождающим для БЧХ-кода с конструктивным расстоянием $d = 5$, так как α^4 также является корнем многочлена $x^4 + x + 1$. Размерность этого кода равна $15 - \deg(g(x)) = 7$. Этот код уже был детально изучен в примере 9.43. $\square$

БЧХ-коды важны ввиду того, что для любого положительного целого числа d можно построить БЧХ-код с минимальным расстоянием, не меньшим чем d. Для того чтобы получить БЧХ-код с бóльшим минимальным расстоянием, мы должны увеличить его длину n и, следовательно, степень m расширения поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$. БЧХ-код с конструктивным расстоянием $d \geqslant 2t + 1$ будет исправлять t ошибок (и, разумеется, любое меньшее число ошибок), но в то же время для того, чтобы получить код с таким кодовым расстоянием, мы должны использовать кодовые слова большей длины.

Опишем теперь *алгоритм декодирования* БЧХ-*кодов*. Обозначим через $w(x)$, $v(x)$ и $e(x)$ соответственно передаваемый кодовый многочлен, принимаемый многочлен и многочлен ошибок; тогда $v(x) = w(x) + e(x)$. Прежде всего нам надо найти синдром вектора $\mathbf{v}$

$$S(\mathbf{v}) = H\mathbf{v}^{\mathrm{T}} = (S_b, S_{b+1}, \ldots, S_{b+d-2})^{\mathrm{T}},$$

где

$$S_j = v(\alpha^j) = w(\alpha^j) + e(\alpha^j) = e(\alpha^j), \quad b \leqslant j \leqslant b + d - 2.$$

Если имеется $r \leqslant t$ ошибок, то

$$e(x) = \sum_{i=1}^{r} c_i x^{a_i},$$

где $a_1, \ldots, a_r$ — различные элементы из $\{0, 1, \ldots, n-1\}$. Элементы $\eta_i = \alpha^{a_i} \in \mathbb{F}_{q^m}$ называются *локаторами ошибки*, а элементы $c_i \in \mathbb{F}_q^*$ — *значениями ошибки*. Таким образом, для синдрома вектора $\mathbf{v}$ получаем формулу

$$S_j = e(\alpha^j) = \sum_{i=1}^{r} c_i \eta_i^j, \quad b \leqslant j \leqslant b + d - 2.$$

Учитывая правила вычисления в поле $\mathbb{F}_{q^m}$, приходим к равенствам

$$S_j^q = \left(\sum_{i=1}^{r} c_i \eta_i^j\right)^q = \sum_{i=1}^{r} c_i^q \eta_i^{jq} = \sum_{i=1}^{r} c_i \eta_i^{jq} = S_{jq}. \tag{9.6}$$

Нам надо найти неизвестные пары (η_i, c_i), $i = 1, \ldots, r$. Координаты S_i синдрома $S(\mathbf{v})$ можно считать известными, так как их можно определить по полученному вектору $\mathbf{v}$. В бинарном случае каждая ошибка полностью характеризуется величиной η_i, так как в этом случае все c_i могут принимать лишь значение, равное 1.

Следующим шагом декодирующего алгоритма является определение коэффициентов σ_i, задаваемых полиномиальным тождеством

$$\prod_{i=1}^{r} (\eta_i - x) = \sum_{i=0}^{r} (-1)^i \sigma_{r-i} x^i = \sigma_r - \sigma_{r-1} x + \cdots + (-1)^r \sigma_0 x^r.$$

Таким образом, $\sigma_0 = 1$, а $\sigma_1, \ldots, \sigma_r$ — элементарные симметрические многочлены от $\eta_1, \ldots, \eta_r$. Подставляя η_i вместо x, получаем

$$(-1)^r \sigma_r + (-1)^{r-1} \sigma_{r-1} \eta_i + \cdots + (-1)\, \sigma_1 \eta_i^{r-1} + \eta_i^r = 0, \quad i = 1, \ldots, r.$$

Умножая на $c_i \eta_i^j$ и суммируя эти равенства по всем $i = 1, \ldots, r$, получаем

$$(-1)^r \sigma_r S_j + (-1)^{r-1} \sigma_{r-1} S_{j+1} + \cdots + (-1)\, \sigma_1 S_{j+r-1} + S_{j+r} = 0,$$

где $j = b, b+1, \ldots, b+r-1$.

9.48. Лемма. *Система уравнений*

$$\sum_{i=1}^{r} c_i \eta_i^j = S_j, \quad j = b, b+1, \ldots, b+r-1,$$

относительно неизвестных c_i разрешима, если η_i являются различными элементами из $\mathbb{F}_{q^m}^*$.

Доказательство. Определитель этой системы уравнений равняется

$$\begin{vmatrix} \eta_1^b & \eta_2^b & \dots & \eta_r^b \\ \eta_1^{b+1} & \eta_2^{b+1} & \dots & \eta_r^{b+1} \\ \dots & \dots & \dots & \dots \\ \eta_1^{b+r-1} & \eta_2^{b+r-1} & \dots & \eta_r^{b+r-1} \end{vmatrix} = \eta_1^b \eta_2^b \dots \eta_r^b \prod_{1 \leqslant i < j \leqslant r} (\eta_j - \eta_i) \neq 0. \square$$

9.49. Лемма. *Система уравнений*

$$(-1)^r \sigma_r S_j + (-1)^{r-1} \sigma_{r-1} S_{j+1} + \dots + (-1)\sigma_1 S_{j+r-1} + S_{j+r} = 0,$$
$$j = b,\ b+1,\ \dots,\ b+r-1,$$

относительно неизвестных $(-1)^i \sigma_i$, $i = 1, 2, \dots, r$, *однозначно разрешима тогда и только тогда, когда в полученном слове имеется* r *ошибок.*

Доказательство. Матрицу, соответствующую этой системе уравнений, можно представить в виде

$$\begin{pmatrix} S_b & S_{b+1} & \dots & S_{b+r-1} \\ S_{b+1} & S_{b+2} & \dots & S_{b+r} \\ \dots & \dots & \dots & \dots \\ S_{b+r-1} & S_{b+r} & \dots & S_{b+2r-2} \end{pmatrix} = VDV^{\mathrm{T}},$$

где

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \eta_1 & \eta_2 & \dots & \eta_r \\ \dots & \dots & \dots & \dots \\ \eta_1^{r-1} & \eta_2^{r-1} & \dots & \eta_r^{r-1} \end{pmatrix}$$

и

$$D = \begin{pmatrix} c_1 \eta_1^b & 0 & \dots & 0 \\ 0 & c_2 \eta_2^b & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_r \eta_r^b \end{pmatrix}.$$

Матрица данной системы невырожденна тогда и только тогда, когда матрицы V и D являются невырожденными. Матрица V является матрицей Вандермонда; она невырожденна тогда и только тогда, когда все η_i, $i = 1, \dots, r$, различны. Матрица D невырожденна тогда и только тогда, когда все η_i и c_i отличны от 0. Оба условия выполняются в том и только том случае, когда в полученном векторе имеется r ошибок. $\square$

Введем так называемый *многочлен локаторов ошибки*:

$$s(x) = \prod_{i=1}^{r} (1 - \eta_i x) = \sum_{i=0}^{r} (-1)^i \sigma_i x^i,$$

где σ_i определены выше. Корни многочлена $s(x)$ равны $\eta_1^{-1}, \ldots, \eta_r^{-1}$. Для того чтобы найти эти корни, можно воспользоваться *процедурой Ченя*. Для этого нам надо, во-первых, узнать, является ли число α^{n-1} локатором ошибки, т. е. является ли элемент $\alpha = \alpha^{-(n-1)}$ корнем многочлена $s(x)$. Чтобы проверить это, рассмотрим сумму

$$1 - \sigma_1\alpha + \sigma_2\alpha^2 + \cdots + (-1)^r \sigma_r\alpha^r.$$

Если она равна -1, то α^{n-1} является локатором ошибки, так как в этом случае $s(\alpha) = 0$. В общем случае точно таким же образом проверяем элементы α^{n-m} для $m = 1, 2, \ldots, n$. В бинарном случае обнаружение местонахождения ошибки равносильно ее исправлению. Приведем теперь полностью алгоритм декодирования БЧХ-кодов, обозначая при этом $(-1)^i\sigma_i$ через τ_i.

9.50. Декодирование БЧХ-кодов. Предположим, что в переданном кодовом слове $\mathbf{w}$, закодированном с помощью БЧХ-кода с конструктивным расстоянием $d \geqslant 2t + 1$, появилось не более t ошибок.

Шаг 1. Находим синдром полученного слова $\mathbf{v}$

$$S(\mathbf{v}) = (S_b, S_{b+1}, \ldots, S_{b+d-2})^{\mathrm{T}}.$$

Пусть

$$S_j = \sum_{i=1}^{r} c_i\eta_i^j, \quad b \leqslant j \leqslant b + d - 2.$$

Шаг 2. Находим максимальное число $r \leqslant t$, такое, что система уравнений

$$S_{j+r} + S_{j+r-1}\tau_1 + \cdots + S_j\tau_r = 0, \quad b \leqslant j \leqslant b + r - 1,$$

относительно неизвестных τ_i имеет невырожденную матрицу коэффициентов. Тем самым получаем число появившихся ошибок. Построим многочлен локаторов ошибки

$$s(x) = \prod_{i=1}^{r} (1 - \eta_i x) = \sum_{i=0}^{r} \tau_i x^i.$$

Коэффициенты τ_i выражаем через S_j.

Шаг 3. Решаем уравнение $s(x) = 0$, подставляя в $s(x)$ вместо x степени элемента α. Тем самым находим локаторы ошибки η_i (процедура Ченя).

Шаг 4. Подставляем η_i в первые r уравнений, образованных на шаге 1, и определяем значения ошибки c_i. После чего из уравнения $w(x) = v(x) - e(x)$ находим переданное слово $\mathbf{w}$.

9.51. Замечание. Заметим, что самым трудным шагом этого алгоритма является шаг 2. Имеются различные методы для его реализации. Одним из них является использование алгоритма

Берлекэмпа—Месси из гл. 8 для определения неизвестных коэффициентов τ_i в линейном рекуррентном соотношении для S_j. □

9.52. Пример. Рассмотрим БЧХ-код с конструктивным расстоянием $d = 5$, который может исправлять любую одиночную или двойную ошибку. В этом случае положим $b = 1$, $n = 15$, $q = 2$. Если через $m^{(i)}(x)$ обозначить минимальный многочлен над полем $\mathbb{F}_2$ элемента α^i, где примитивный элемент $\alpha \in \mathbb{F}_{16}$ является корнем многочлена $x^4 + x + 1$, то

$$m^{(1)}(x) = m^{(2)}(x) = m^{(4)}(x) = m^{(8)}(x) = 1 + x + x^4,$$

$$m^{(3)}(x) = m^{(6)}(x) = m^{(12)}(x) = m^{(9)}(x) = 1 + x + x^2 + x^3 + x^4.$$

Таким образом, порождающий многочлен рассматриваемого БЧХ-кода имеет вид

$$g(x) = m^{(1)}(x)\, m^{(3)}(x) = 1 + x^4 + x^6 + x^7 + x^8.$$

Этот код является линейным (15,7)-кодом с проверочным многочленом

$$h(x) = (x^{15} - 1)/g(x) = 1 + x^4 + x^6 + x^7.$$

В качестве базиса этого (15,7)-БЧХ-кода возьмем векторы, соответствующие многочленам

$$g(x),\ xg(x),\ x^2g(x),\ x^3g(x),\ x^4g(x),\ x^5g(x),\ x^6\,g(x).$$

Таким образом, получаем порождающую матрицу

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Предположим теперь, что полученное слово $\mathbf{v}$ имеет вид

$$1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,0;$$

тогда соответствующий многочлен $v(x)$ имеет вид

$$v(x) = 1 + x^3 + x^6 + x^7 + x^{12}.$$

В соответствии с шагом 1 декодирующего алгоритма найдем его синдром, воспользовавшись при этом для упрощения вычислений соотношениями (9.6):

$$S_1 = e(\alpha) = v(\alpha) = 1,$$

$$S_2 = e(\alpha^2) = v(\alpha^2) = 1,$$

$$S_3 = e(\alpha^3) = v(\alpha^3) = \alpha^4,$$
$$S_4 = e(\alpha^4) = v(\alpha^4) = 1.$$

Максимальная невырожденная система линейных уравнений относительно неизвестных τ_i (шаг 2) имеет в этом случае вид

$$S_2\tau_1 + S_1\tau_2 = S_3,$$
$$S_3\tau_1 + S_2\tau_2 = S_4,$$

или

$$\tau_1 + \tau_2 = \alpha^4,$$
$$\alpha^4\tau_1 + \tau_2 = 1.$$

Очевидно, что матрица этой системы невырожденна. Следовательно, число встретившихся ошибок должно равняться 2, т. е. $r = 2$. Решая эту систему уравнений, получаем $\tau_1 = 1$, $\tau_2 = \alpha$. Подставляя эти значения в $s(x)$ и считая, что $\tau_0 = 1$, получаем, что

$$s(x) = 1 + x + \alpha x^2.$$

Так как корни этого многочлена лежат в $\mathbb{F}_{16}$, то $\eta_1^{-1} = \alpha^8$, $\eta_2^{-1} = \alpha^6$ и, следовательно, $\eta_1 = \alpha^7$, $\eta_2 = \alpha^9$. Отсюда мы делаем вывод, что ошибки появились в 8-й и 10-й компонентах переданного слова. Исправив эти ошибки в полученном многочлене, получаем

$$w(x) = v(x) - e(x) = (1 + x^3 + x^6 + x^7 + x^{12}) - (x^7 + x^9) =$$
$$= 1 + x^3 + x^6 + x^9 + x^{12}.$$

Соответствующее кодовое слово —

$$1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0.$$

Исходную информацию (до кодирования) можно получить с помощью деления исправленного многочлена (т. е. переданного кодового многочлена $w(x)$) на многочлен $g(x)$. В результате получаем

$$w(x)/g(x) \qquad 1 + x^3 + x^4,$$

что соответствует передаваемому сообщению $1\,0\,0\,1\,1\,0\,0$. □

§ 3. Конечные геометрии

Этот параграф посвящен применению теории конечных полей в геометрии. В известном смысле теорию кодирования можно также рассматривать и как раздел геометрии, и как раздел комбинаторики, так как в ней изучаются вопросы упаковки шаров в метрическом пространстве конечной мощности, как правило, в конечномерном векторном пространстве над полем $\mathbb{F}_q$.

Проективная плоскость состоит из множества точек и множества

прямых, которые связаны между собой отношением инцидентности. Это отношение позволяет для каждой точки и каждой прямой установить, лежит данная точка на данной прямой или нет. Для того чтобы дать строгое определение, необходимо сформулировать несколько аксиом.

9.53. **Определение.** *Проективная плоскость* определяется как множество элементов, называемых *точками*, вместе с выделенными подмножествами этого множества, называемыми *прямыми*, и отношением I, называемым *отношением инцидентности* между точками и прямыми и удовлетворяющим следующим условиям:

(i) каждая пара различных прямых инцидентна единственной точке (т. е. для каждой пары различных прямых существует единственная точка, лежащая на обеих прямых и называемая их *пересечением*);

(ii) каждая пара различных точек инцидентна единственной прямой (т. е. для каждой пары различных точек существует единственная прямая, содержащая обе эти точки, иначе — прямая, проходящая через эти точки);

(iii) существуют четыре точки, такие, что никакие три из них не инцидентны одной и той же прямой (т. е. существуют четыре точки, такие, что никакие три из них не лежат на одной прямой).

Отсюда следует, что каждая прямая содержит по меньшей мере 3 точки и что через каждую точку проходят по меньшей мере 3 прямые. Если множество точек проективной плоскости конечно, то мы будем говорить о *конечной проективной плоскости*. Из трех приведенных выше аксиом нетрудно вывести, что условие (iii) выполняется и в случае, если в нем поменять местами понятия «точка» и «прямая». Тем самым устанавливается *принцип двойственности* между точками и прямыми, из которого в свою очередь можно получить следующий результат:

9.54. **Теорема.** *Пусть* Π *— конечная проективная плоскость. Тогда*

(i) *существует целое число* $m \geqslant 2$, *такое, что каждая точка* (*прямая*) *плоскости* Π *инцидентна в точности* $m + 1$ *прямым* (*точкам*) *плоскости* Π;

(ii) Π *содержит ровно* $m^2 + m + 1$ *точек* (*прямых*).

9.55. **Пример.** Простейшая конечная проективная плоскость получается при $m = 2$, в ней через каждую точку проходят ровно 3 прямые и каждая прямая содержит ровно 3 точки. Всего же плоскость содержит 7 точек и 7 прямых. Такая проективная плоскость называется *плоскостью Фано*; на рис. 9.2 приводится ее схематическое изображение. Плоскость содержит точки A, B, C, D, E, F и G и прямые ADC, AGE, AFB, CGF, CEB, DGB и DEF. Так как для конечных плоскостей обычное геометрическое

понятие «прямой» теряет смысл, подмножество DEF в конечной проективной плоскости считается прямой. □

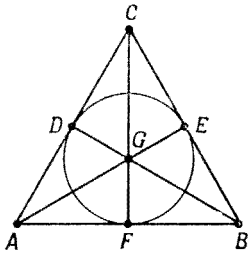


Рис 9.2.

Число m, появляющееся в теореме 9.54, называется *порядком* конечной проективной плоскости. Как мы увидим далее, конечные проективные плоскости порядка m существуют для всех целых m, имеющих вид $m = p^n$, где p — простое число. Известно, что не существует проективной плоскости порядка $m = 6$, однако неизвестно, существует ли такая плоскость для $m = 10$. Для $m = 9$ найден целый набор плоскостей с этим параметром, однако не найдено еще ни одной плоскости, порядок которой не был бы степенью простого числа.

В обычной аналитической геометрии мы представляем точки плоскости в виде упорядоченной пары действительных чисел (x, y), а прямые — как множества точек, удовлетворяющих уравнению вида $ax + by + c = 0$ при условии, что числа a и b не равны одновременно 0. Заменим теперь поле действительных чисел любым другим полем, в частности некоторым конечным полем. Такой тип геометрии известен как аффинная геометрия (или евклидова геометрия). Тем самым мы приходим к понятию аффинной плоскости.

9.56. Определение. *Аффинной плоскостью* называется тройка $(\mathscr{P}, \mathscr{L}, I)$, состоящая из множеств точек $\mathscr{P}$, множества прямых $\mathscr{L}$ и отношения инцидентности I. При этом должны выполняться следующие условия:

(i) каждая пара различных точек инцидентна единственной прямой;

(ii) каждая точка $P \in \mathscr{P}$, не лежащая на прямой $L \in \mathscr{L}$, лежит на единственной прямой $M \in \mathscr{L}$, которая не пересекается с L;

(iii) существуют четыре точки, такие, что никакие три из них не лежат на одной прямой.

Доказательство следующей теоремы вытекает непосредственно из определений.

9.57. Теорема. *Пусть K — произвольное поле, и пусть $\mathscr{P}$ обозначает множество упорядоченных пар (x, y), $x, y \in K$, а $\mathscr{L}$*

состоит из таких подмножеств L множества $\mathscr{P}$, элементы которых удовлетворяют линейным уравнениям, т. е. $L \in \mathscr{L}$ тогда и только тогда, когда найдутся такие элементы $a, b, c \in K$, $(a, b) \neq (0, 0)$, для которых $L = \{(x, y) \mid ax + by + c = 0\}$. Точка $P \in \mathscr{P}$ инцидентна прямой $L \in \mathscr{L}$ тогда и только тогда, когда $P \in L$. Тогда тройка $(\mathscr{P}, \mathscr{L}, I)$ с определенным выше отношением инцидентности является аффинной плоскостью и обозначается через $AG(2, K)$.

Нетрудно показать, что если $|K| = m$, то каждая прямая в $AG(2, K)$ содержит ровно m точек. Из $AG(2, K)$ можно построить проективную плоскость. Для этого надо добавить еще одну прямую. Верно и обратное: из любой проективной плоскости можно получить аффинную плоскость, если удалить из проективной плоскости одну прямую и все точки, принадлежащие ей. Покажем это.

С этой целью несколько изменим обозначения для точек плоскости $AG(2, K)$: будем обозначать их через $(x, y, 1)$, т. е. (x, y, z), где $z = 1$. Тогда уравнение прямой принимает вид $ax + by + cz = 0$, где $(a, b) \neq (0, 0)$. Добавим к $\mathscr{P}$ множество точек

$$L_\infty = \{(1, 0, 0)\} \cup \{(x, 1, 0) \mid x \in K\}$$

и образуем новое множество точек $\mathscr{P}' = \mathscr{P} \cup L_\infty$. Точки из L_∞ можно представить с помощью уравнения $z = 0$, поэтому множество L_∞ можно рассматривать как прямую. Добавим эту новую прямую к множеству прямых $\mathscr{L}$ и образуем новое множество $\mathscr{L}' = \mathscr{L} \cup \{L_\infty\}$. Естественным образом перенося на множества $\mathscr{P}'$ и $\mathscr{L}'$ отношение инцидентности I, можно проверить, что тройка $(\mathscr{P}', \mathscr{L}', I')$ удовлетворяет всем аксиомам проективной плоскости.

9.58. Теорема. *Пусть $AG(2, K) = (\mathscr{P}, \mathscr{L}, I)$, и пусть*

$$\mathscr{P}' = \mathscr{P} \cup \{(1, 0, 0)\} \cup \{(x, 1, 0) \mid x \in K\} = \mathscr{P} \cup L_\infty,$$
$$\mathscr{L}' = \mathscr{L} \cup \{L_\infty\},$$

а отношение инцидентности I, перенесенное на множества $\mathscr{P}'$ и $\mathscr{L}'$, обозначено через I'. Тогда $(\mathscr{P}', \mathscr{L}', I')$ является проективной плоскостью и обозначается через $PG(2, K)$.

9.59. Пример. Плоскость $PG(2, \mathbb{F}_2)$ — проективная плоскость над полем $\mathbb{F}_2$ — содержит 7 точек: точки $(0, 0, 1)$, $(1, 0, 1)$, $(0, 1, 1)$, $(1, 1, 1)$ с координатой $z \neq 0$ и три различные точки прямой $z = 0$, а именно $(1, 0, 0)$, $(0, 1, 0)$, $(1, 1, 0)$. Нетрудно проверить, что плоскость $PG(2, \mathbb{F}_2)$ содержит также 7 прямых и что эта проективная плоскость является на самом деле плоскостью Фано из примера 9.55. □

При построении $PG(2, K)$ из $AG(2, K)$ мы видели, что каждая прямая из $AG(2, K)$ должна пересечься с добавленной прямой L_∞,

т. е. что к каждой прямой из $AG(2, K)$ надо добавить по одной точке. Прямая L_∞ также содержит $m+1$ точек в случае, если поле K содержит m элементов. Так как для любой степени простого числа $m = p^n = q$ существует конечное поле $\mathbb{F}_q$, то справедлива следующая теорема.

9.60. Теорема. *Для любой степени простого числа $q = p^n$, p — простое число, $n \in \mathbb{N}$, существует конечная проективная плоскость порядка q, а именно $PG(2, \mathbb{F}_q)$.*

Дополнительная прямая L_∞, добавленная к аффинной плоскости для того, чтобы получить проективную плоскость, иногда называется *бесконечно удаленной прямой*. Если две прямые пересекаются по точке, лежащей на L_∞, то они называются *параллельными*.

Приведем теперь без доказательства две интересные теоремы, которые справедливы для всех проективных плоскостей, имеющих аналитическое представление в терминах теории полей. Два треугольника $\triangle A_1B_1C_1$ и $\triangle A_2B_2C_2$ называются *находящимися в перспективе относительно точки O*, если прямые A_1A_2, B_1B_2 и C_1C_2 проходят через точку O. Точки, лежащие на одной прямой, называются *коллинеарными*.

9.61. Теорема (Дезарг). *Если $\triangle A_1B_1C_1$ и $\triangle A_2B_2C_2$ находятся в перспективе относительно точки O, то точки пересечения прямых A_1B_1 и A_2B_2, A_1C_1 и A_2C_2, B_1C_1 и B_2C_2 являются коллинеарными.*

Эта теорема иллюстрируется рис. 9.3: точки пересечения соответствующих прямых обозначаются через P, Q и R и лежат на одной прямой.

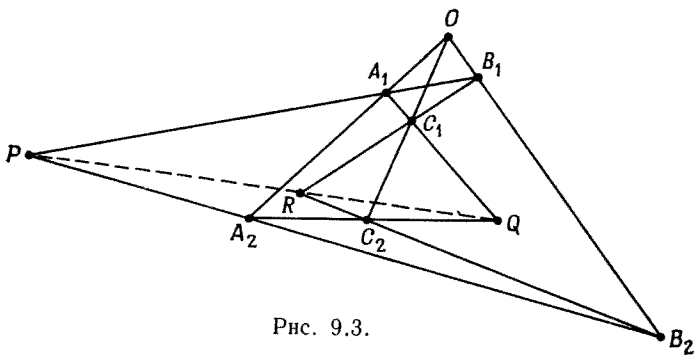


Рис. 9.3.

9.62. Теорема (Папп). *Если A_1, B_1, C_1 — точки некоторой прямой, а A_2, B_2, C_2 — точки другой прямой, лежащей в той же плоскости, и если прямые A_1B_2 и A_2B_1 пересекаются в точке P, A_1C_2 и A_2C_1 пересекаются в точке Q, а B_1C_2 и B_2C_1 пересекаются в точке R, то точки P, Q и R коллинеарны.*

Рисунок 9.4 является иллюстрацией к теореме Паппа. Обе

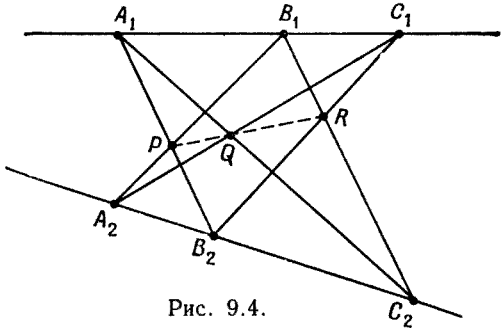


Рис. 9.4.

приведенные выше теоремы играют важную роль в проективной геометрии. Если теорема Дезарга справедлива в некоторой проективной плоскости, то координаты точек этой плоскости можно задать через элементы некоторого тела R. В этом случае каждая точка задается упорядоченной тройкой (x_0, x_1, x_2) *трех однородных координат*, где x_i — элементы тела R, не равные одновременно 0. При этом тройка (ax_0, ax_1, ax_2), $0 \neq a \in R$, представляет ту же самую точку. Таким образом, если тело R конечно и $|R| = m$, то для каждой точки имеется $m - 1$ представлений. Поэтому, поскольку всего имеется $m^3 - 1$ возможных троек координат, общее число различных точек проективной плоскости равно

$$(m^3 - 1)/(m - 1) = m^2 + m + 1.$$

Прямая определяется как множество таких точек, координаты которых удовлетворяют одному из следующих уравнений: $x_0 + a_1x_1 + a_2x_2 = 0$, $x_1 + a_2x_2 = 0$ или $x_2 = 0$ $(a_i \in R)$. Таким образом, плоскость содержит $m^2 + m + 1$ прямых, и можно непосредственно проверить, что определенные таким образом точки и прямые удовлетворяют аксиомам проективной плоскости.

Из теоремы Веддербёрна (теорема 2.55) нам известно, что любое конечное тело является полем, а именно конечным полем $\mathbb{F}_q$. В этом случае уравнение прямой можно записать в виде $a_0x_0 + a_1x_1 + a_2x_2 = 0$, где числа a_i не равны одновременно нулю, при этом уравнение $(aa_0)\, x_0 + (aa_1)\, x_1 + (aa_2)\, x_2 = 0$, где $a \in \mathbb{F}_q^*$, задает ту же самую прямую. Прямая, проходящая через точки (y_0, y_1, y_2) и (z_0, z_1, z_2), может быть также определена как множество точек с координатами $(ay_0 + bz_0,\ ay_1 + bz_1,\ ay_2 + bz_2)$, где числа $a, b \in \mathbb{F}_q$ не равняются одновременно 0. Всего существует $q^2 - 1$ таких троек, а в силу того, что одновременное умножение элементов a и b на один и тот же ненулевой элемент задает ту же самую точку, мы получаем, что наша прямая содержит $q + 1$ различных точек.

В проективной плоскости $PG(2, \mathbb{F}_q)$ справедлива как теорема Дезарга, так и обратное к ней утверждение; доказательство этого

опирается на коммутативность операции умножения в поле $\mathbb{F}_q$. В общем случае, когда координаты точек проективной плоскости являются элементами некоммутативного кольца, теорема Дезарга и ее обращение могут не выполняться. Отсюда становится ясной та важная роль, которую играет в этом контексте теорема Веддербёрна.

Проективная плоскость, в которой справедлива теорема Дезарга, называется *дезарговой плоскостью*, в противном случае плоскость называется *недезарговой*. Дезарговы плоскости порядка m существуют только для чисел m, равных степеням простых чисел, причем для каждого заданного числа $m = p^n$, где p — простое число, существует с точностью до изоморфизма только одна дезаргова плоскость порядка m. В конечной дезарговой плоскости всегда можно ввести координаты, являющиеся элементами некоторого конечного поля. Так как такое поле существует только в случае, когда порядок m этой плоскости является степенью простого числа, то проективная плоскость, в которой каждая прямая содержит $m + 1$ точек, где число m не является степенью простого числа, обязана быть недезарговой плоскостью. Неизвестно, существуют ли такие плоскости для m, не равного степени простого числа. Если удастся доказать, что с точностью до изоморфизма существует только одна конечная проективная плоскость данного порядка m, то отсюда получится, что для m, равного степени простого числа, проективная плоскость порядка m обязана быть дезарговой. Это справедливо для $m = 2, 3, 4, 5, 7, 8$. Для простого m известны только дезарговы плоскости. Однако было показано, что для всех $m = p^n$, $n \geqslant 2$, кроме случаев $m = 4$ и $m = 8$, существуют и недезарговы плоскости порядка m.

Из теоремы Паппа следует теорема Дезарга. Кроме того, если в некоторой проективной плоскости справедлива теорема Паппа, то кольцо, элементами которого являются координаты точек этой плоскости, должно быть коммутативно относительно операции умножения. Теорема Паппа справедлива в $PG(2, \mathbb{F}_q)$ при любом q, равном степени простого числа. Теорема Паппа также справедлива и в любой конечной дезарговой плоскости.

Имеется существенное различие между свойствами плоскости $PG(2, \mathbb{F}_q)$ для четного q и плоскости $PG(2, \mathbb{F}_q)$ для нечетного q. Это различие выражено в следующей теореме.

9.63. Теорема. *Точки, образующие диагональ полного четырехвершинника*[1] *в* $PG(2, \mathbb{F}_q)$, *являются коллинеарными тогда и только тогда, когда* q *четно.*

---

[1]) *Полным четырехвершинником* называется совокупность, состоящая из четырех точек (вершин), лежащих в одной плоскостн, нз которых никакие три не лежат на одной прямой, н шести соединяющих нх прямых (сторон); его *диагональ* состоит из точек пересечения несмежных, т. е. не имеющих общей вершины, сторон. — *Прим. перев.*

Доказательство. Предположим, не теряя общности, что вершинами нашего четырехвершинника являются точки (1, 0, 0), (0, 1, 0), (0, 0, 1) и (1, 1, 1). Шесть его сторон задаются соотношениями $x_2 = 0$, $x_1 = 0$, $x_1 - x_2 = 0$, $x_0 = 0$, $x_0 - x_2 = 0$, $x_0 - x_1 = 0$. В то же время диагональными точками являются точки (1, 1, 0), (1, 0, 1) и (0, 1, 1). Прямая, проходящая через первые две точки, содержит все точки с координатами $(a + b, a, b)$, где $(a, b) \neq (0, 0)$. Нетрудно видеть, что третья точка лежит на этой прямой тогда и только тогда, когда $a = b$ и $a + b = 0$. В конечном поле $\mathbb{F}_q$ это выполняется лишь в том случае, когда характеристика поля равна 2. □

Иллюстрацией последнего случая может служить пример 9.55. Пусть вершинами полного четырехвершинника являются точки C, D, E, G. В этом случае диагональными точками являются точки A, F и B, которые лежат на одной прямой.

Введем теперь некоторые понятия, аналогичные известным понятиям из аналитической геометрии. Ограничимся при этом рассмотрением дезарговых плоскостей, координаты в которых являются элементами конечного поля $\mathbb{F}_q$.

Пусть две различные прямые заданы уравнениями

$$\begin{aligned} a_{01}x_0 + a_{11}x_1 + a_{21}x_2 &= 0, \\ a_{02}x_0 + a_{12}x_1 + a_{22}x_2 &= 0. \end{aligned} \tag{9.7}$$

Пусть P — точка пересечения этих прямых. Все прямые, проходящие через точку P, образуют пучок, и каждая прямая из этого пучка задается уравнением вида

$$(ra_{01} + sa_{02})\,x_0 + (ra_{11} + sa_{12})\,x_1 + (ra_{21} + sa_{22})\,x_2 = 0,$$

где элементы $r, s \in \mathbb{F}_q$ не равны одновременно 0. Пучок содержит $q + 1$ прямых: две прямые, заданные уравнениями (9.7), которые соответствуют случаям $s = 0$ и $r = 0$, и $q - 1$ прямых, соответствующих $q - 1$ различным значениям произведения rs^{-1}, где $r \neq 0$, $s \neq 0$. Пусть имеется другой пучок прямых, проходящий через точку $Q \neq P$ и задаваемый уравнением

$$(rb_{01} + sb_{02})\,x_0 + (rb_{11} + sb_{12})\,x_1 + (rb_{21} + sb_{22})\,x_2 = 0.$$

Проективное соответствие между прямыми этих пучков можно задать следующим образом: прямая одного пучка, задаваемая парой (r, s), соответствует той прямой другого пучка, которая задается той же парой параметров (r, s). Каждая пара соответствующих друг другу прямых пересекается в единственной точке. Исключение представляет случай, когда прямая PQ соответствует

самой себе. Координаты точек пересечения удовлетворяют уравнению

$$(a_{01}x_0 + a_{11}x_1 + a_{21}x_2)(b_{02}x_0 + b_{12}x_1 + b_{22}x_2) - \\ - (a_{02}x_0 + a_{12}x_1 + a_{22}x_2)(b_{01}x_0 + b_{11}x_1 + b_{21}x_2) = 0, \qquad (9.8)$$

которое получается исключением параметров r и s из уравнений соответствующих пучков.

9.64. Определение. Множество точек, координаты которых удовлетворяют уравнению (9.8), называется *коникой*. Если в результате установленного выше соответствия прямая PQ соответствует сама себе, то коника называется *вырожденной*. В этом случае она состоит из $2q + 1$ точек, которые образуют две пересекающиеся прямые. *Невырожденная* коника состоит из $q + 1$ точек, являющихся точками пересечения соответствующих прямых. Прямая, имеющая с коникой ровно одну общую точку, называется *касательной*; прямая, имеющая с коникой две общие точки, называется *секущей*.

Уравнение, задающее невырожденную конику, является квадратным, поэтому прямая не может иметь с невырожденной коникой более двух общих точек. Возьмем одну точку невырожденной коники и соединим ее прямыми с остальными q точками коники. Получившиеся прямые являются секущими. Так как через каждую точку проходит $q + 1$ прямых, то оставшаяся прямая является касательной.

Таким образом, $q + 1$ точек невырожденной коники обладают тем свойством, что никакие три из них не лежат на одной прямой. Можно доказать, что невырожденной коникой является любое множество, состоящее из $q + 1$ точек проективной плоскости $PG(2, \mathbb{F}_q)$, где q нечетно, обладающих тем свойством, что никакие три из них не коллинеарны.

Следующая теорема, которую мы докажем только частично, иллюстрирует разницу между свойствами коник в дезарговых плоскостях четного и нечетного порядков.

9.65. Теорема. (i) *В дезарговой плоскости нечетного порядка через каждую точку, не лежащую на невырожденной конике, либо проходят две касательные к этой конике, либо не проходит ни одной.*

(ii) *В дезарговой плоскости четного порядка все касательные к невырожденной конике пересекаются в одной точке.*

Доказательство. Доказательство п. (ii) служит примером того, как свойства конечных полей используются в теории конечных проективных плоскостей. Предположим, не теряя общности, что три точки $A = (1, 0, 0)$, $B = (0, 1, 0)$ и $C = (0, 0, 1)$ являются точками невырожденной коники, лежащей в дезарговой плоскости

четного порядка. Пусть касательные, проходящие через эти точки, заданы соответственно уравнениями $x_1 - k_0x_2 = 0$, $x_2 - k_1x_0 = 0$, $x_0 - k_2x_1 = 0$. Пусть $P = (t_0, t_1, t_2)$ — какая-либо другая точка нашей коники. Ни одна из координат t_i не может равняться 0, так как иначе точка P лежала бы на одной из прямых, проходящих через какие-нибудь две точки из множества $\{A, B, C\}$. Последнее противоречило бы тому, что никакие три точки невырожденной коники не лежат на одной прямой. Таким образом, прямую PA можно задать уравнением $x_1 - t_1t_2^{-1}x_2 = 0$, прямую PB — уравнением $x_2 - t_2t_0^{-1}x_0 = 0$, прямую PC — уравнением $x_0 - t_0t_1^{-1}x_1 = 0$.

Рассмотрим уравнение прямой PA. Поскольку в качестве P мы взяли произвольную точку коники, отличную от точек A, B, C, отношение $t_1t_2^{-1}$ пробегает все множество элементов поля $\mathbb{F}_q$, отличных от 0 и k_0. Так как

$$\prod_{c \in \mathbb{F}_q^*} (x - c) = x^{q-1} - 1,$$

то произведение всех ненулевых элементов поля $\mathbb{F}_q$ равняется $(-1)^q$. Тогда, если умножить произведение всех $q-2$ возможных значений отношения $t_1t_2^{-1}$ на k_0, то мы получим $(-1)^q = 1$, так как q четно. Таким образом,

$$k_0 \prod t_1t_2^{-1} = 1, \quad k_1 \prod t_2t_0^{-1} = 1, \quad k_2 \prod t_0t_1^{-1} = 1,$$

где произведение берется по всем точкам коники, отличным от A, B и C. Перемножая эти три равенства, получаем $k_0k_1k_2 = 1$. Следовательно, точки $(1, k_0k_1, k_1)$, $(k_2, 1, k_1k_2)$ и $(k_0k_2, k_0, 1)$ совпадают. Значит, все три касательные, проходящие через точки A, B и C, пересекаются в одной точке. А так как точки A, B и C выбирались произвольно, то мы получаем, что любые три касательные нашей коники пересекаются в одной и той же точке. □

Существуют интересные связи между перестановочными многочленами конечных полей (см. гл. 7) и конечными проективными плоскостями. Продемонстрируем одну из них.

9.66. **Определение.** *Овалом* в проективной плоскости $PG(2, \mathbb{F}_q)$, где q четно, называется множество из $q + 2$ точек этой плоскости, никакие три из которых не лежат на одной прямой.

В качестве примера овала можно взять $q + 1$ точек, образующих невырожденную конику в $PG(2, \mathbb{F}_q)$, где q четно, и добавить к ним точку пересечения всех касательных этой коники (см. теорему 9.65 (ii)). В следующей теореме указывается канонический вид овала.

9.67. Теорема. *Любой овал в проективной плоскости* $PG(2, \mathbb{F}_q)$, *где* q *четно и* $q > 2$, *может быть записан в виде*

$$A(f) = \{(f(c),\ c,\ 1) \mid c \in \mathbb{F}_q\} \cup \{(1,\ 0,\ 0),\ (0,\ 1,\ 0)\},$$

где f *принадлежит* $\mathbb{F}_q[x]$ *и удовлетворяет следующим условиям*

(i) f — *перестановочный многочлен поля* $\mathbb{F}_q$, *такой, что* $\deg(f) < q$ *и* $f(0) = 0$, $f(1) = 1$;

(ii) *для любого* $a \in \mathbb{F}_q$ *многочлен* $g_a(x) = [f(x + a) + f(a)]/x$ *является перестановочным многочленом поля* $\mathbb{F}_q$, *причем* $g_a(0) = 0$.

Верно и обратное: каждое такое множество $A(f)$ *является овалом.*

Доказательство. Пусть D — овал в плоскости $PG(2, \mathbb{F}_q)$. Мы можем преобразовать координаты на плоскости таким образом, чтобы точки $P_0 = (1, 0, 0)$, $P_1 = (0, 1, 0)$, $P_2 = (0, 0, 1)$ и $P_3 = (1, 1, 1)$ были точками овала D. Тогда никакая другая точка из D не лежит на прямой P_0P_1. Следовательно, q точек овала D, отличных от P_0 и P_1, можно представить в виде $(d_i, c_i, 1)$, $1 \leqslant i \leqslant q$, где $d_i, c_i \in \mathbb{F}_q$. Так как каждая прямая, проходящая через точку P_0, содержит еще только одну точку овала D, то $c_i \neq c_j$ при $i \neq j$. Аналогично так как каждая прямая, проходящая через точку P_1, также содержит еще только одну точку овала D, то $d_i \neq d_j$ при $i \neq j$. Таким образом,

$$\{c_1,\ \ldots,\ c_q\} = \{d_1,\ \ldots,\ d_q\} = \mathbb{F}_q.$$

И, следовательно, в силу (7.1) существует перестановочный многочлен $f(x)$ поля $\mathbb{F}_q$, для которого $f(c_i) = d_i$, $1 \leqslant i \leqslant q$ и $\deg(f) < q$. Так как $P_2,\ P_3 \in D$, получаем, что $f(0) = 0$, $f(1) = 1$. Значит, $D = A(f)$, где f удовлетворяет условию (i).

Остается показать, что условие (ii) эквивалентно тому, что никакие три точки из множества $A(f) \setminus \{P_0, P_1\}$ не лежат на одной прямой. Последнее условие выполняется тогда и только тогда, когда

$$\begin{vmatrix} f(b) & b & 1 \\ f(c) & c & 1 \\ f(d) & d & 1 \end{vmatrix} \neq 0$$

для всех различных $b, c, d \in \mathbb{F}_q$. Это означает, что

$$[f(b) + f(c)](b + c)^{-1} \neq [f(b) + f(d)](b + d)^{-1},$$

т. е. для любого $a \in \mathbb{F}_q$ выражение $[f(t) + f(a)](t + a)^{-1}$ принимает различные значения из $\mathbb{F}_q^*$ при различных t из поля $\mathbb{F}_q$, отличных от элемента a. Подставляя вместо t выражение $x + a$, получаем, что многочлен

$$g_a(x) = [f(x + a) + f(a)]/x$$

задает перестановку элементов из $\mathbb{F}_q^*$. Так как $\deg(g_a) \leqslant q-2$, то из формулы (7.1) получаем

$$g_a(x) = \sum_{c \in \mathbb{F}_q} g_a(c)\,(1-(x-c)^{q-1}).$$

Тогда, сравнивая коэффициенты при x^{q-1} и применяя на последнем этапе лемму 7.3, получаем

$$0 = -\sum_{c \in \mathbb{F}_q} g_a(c) = g_a(0) + \sum_{c \in \mathbb{F}_q^*} g_a(c) = g_a(0) + \sum_{b \in \mathbb{F}_q^*} c =$$
$$= g_a(0) + \sum_{c \in \mathbb{F}_q} c = g_a(0).$$

Отсюда следует, что $g_a(x)$ является перестановочным многочленом поля $\mathbb{F}_q$. □

9.68. Следствие. *Если* $f(x) = \sum_{i=1}^{q-1} b_i x^i$, *а* $A(f)$ — *соответствующий овал в проективной плоскости* $PG(2, \mathbb{F}_q)$, q *четно и* $q > 2$, *то* f *обязательно имеет вид*

$$f(x) = \sum_{j=1}^{(q-2)/2} b_{2j} x^{2j}.$$

Доказательство. Из условия (ii) теоремы 9.67 следует, что для всех $a \in \mathbb{F}_q$ справедливо равенство

$$0 = g_a(0) = b_1 + b_3 a^2 + b_5 a^4 + \cdots + b_{q-1} a^{q-2}.$$

Отсюда следует, что $b_1 = b_3 = b_5 = \ldots = b_{q-1} = 0$. □

9.69. Следствие. *Множество* $A(x^k)$, $1 \leqslant k < q$, *является овалом в проективной плоскости* $PG(2, \mathbb{F}_q)$, *где* $q > 2$ *четно, тогда и только тогда, когда выполнены следующие условия*: (i) НОД $(k, q-1) = 1$; (ii) НОД $(k-1, q-1) = 1$; (iii) *многочлен* $[(x+1)^k + 1]/x$ *является перестановочным многочленом поля* $\mathbb{F}_q$.

Доказательство. В силу теоремы 7.8 (ii) условие (i) эквивалентно условию (i) теоремы 9.67. Аналогично условие (ii) эквивалентно условию теоремы 9.67 для $a = 0$. Если $a \in \mathbb{F}_q^*$, то

$$g_a(x) = [(x+a)^k + a^k]/x = a^{k-1}[(a^{-1}x+1)^k + 1]/(a^{-1}x) =$$
$$= a^{k-1} g_1(a^{-1}x).$$

Таким образом, g_a является перестановочным многочленом поля $\mathbb{F}_q$ тогда и только тогда, когда таковым является многочлен g_1. Кроме того, если g_1 является перестановочным многочле-

ном поля $\mathbb{F}_q$, то из соотношений $g_1(0) \in \mathbb{F}_q$, $g_1(1) = 1$ вытекает, что $g_1(0) = 0$ и, следовательно, $g_a(0) = 0$. □

Конструкцию, аналогичную проективной плоскости, можно дать и в случае, когда размерность пространства больше, чем 2.

9.70. Определение. *Проективным пространством* или *m-пространством*, или *проективной геометрией* называется множество точек, в котором выделены некоторые подмножества точек, называемые прямыми, удовлетворяющие следующим условиям:

(i) Существует единственная прямая, проходящая через любую пару несовпадающих точек.

(ii) Прямая, пересекающая две прямые, являющиеся сторонами некоторого треугольника, пересекает также и третью его сторону.

(iii) Каждая прямая содержит по крайней мере 3 точки.

(iv) k-пространство определим следующим образом. 0-пространство является точкой. Если $A_0, \ldots, A_k$ — точки, не лежащие в одном $(k-1)$-пространстве, то все точки, лежащие на прямых, проходящих через A_0 и какую-нибудь точку $(k-1)$-пространства, заданного точками $A_1, \ldots, A_k$, образуют k-пространство. Таким образом, прямая является 1-пространством, а все остальные пространства определяются рекурсивно. Аксиома (iv) требует: если $k < m$, то не все точки рассматриваемого множества лежат в одном k-пространстве.

(v) Рассматриваемое множество точек не порождает $(m+1)$-пространство.

Мы будем говорить, что m-пространство имеет *размерность* m. Если имеется k-пространство, являющееся подпространством проективного пространства более высокой размерности, то мы будем называть его *k-плоскостью*. $(m-1)$-плоскость проективного пространства размерности m называется *гиперплоскостью*. 2-пространство является проективной плоскостью в смысле определения 9.53. Можно доказать, что в любой 2-плоскости любого проективного пространства размерности не меньше 3 всегда справедлива теорема Дезарга (теорема 9.61). Теорема Дезарга может не выполняться только в таких проективных плоскостях, которые нельзя вложить в проективное пространство большей размерности.

Проективное пространство, состоящее из конечного числа точек, называется *конечным проективным пространством* (*конечной проективной геометрией*, *конечным m-пространством*). По аналогии с $PG(2, \mathbb{F}_q)$ можно построить конечное m-пространство $PG(m, \mathbb{F}_q)$. Определим точку как упорядоченный набор $(x_0, x_1, \ldots, x_m)$, где координаты x_i лежат в $\mathbb{F}_q$ и не все одновременно равняются 0. Набор вида $(ax_0, ax_1, \ldots, ax_m)$, где $a \in \mathbb{F}_q^*$, определяет ту же самую точку, что и набор $(x_0, x_1, \ldots, x_m)$. Таким образом, $PG(m, \mathbb{F}_q)$ содержит $(q^{m+1}-1)/(q-1)$ различных точек.

k-плоскостью в пространстве $PG(m, \mathbb{F}_q)$ является множество всех таких точек, координаты которых удовлетворяют системе из $m - k$ линейно независимых однородных линейных уравнений

$$a_{10}x_0 + \cdots + a_{1m}x_m = 0,$$

$$\cdots\cdots\cdots\cdots$$

$$a_{m-k,0}x_0 + \cdots + a_{m-k,m}x_m = 0$$

с коэффициентами $a_{ij} \in \mathbb{F}_q$. С другой стороны, k-плоскость — это множество всех точек с координатами

$$(a_0x_{00} + \cdots + a_kx_{k0}, \ \ldots, \ a_0x_{0m} + \cdots + a_kx_{km}),$$

где элементы $a_i \in \mathbb{F}_q$ не все одновременно равны 0, а $k + 1$ заданных точек

$$(x_{00}, \ \ldots, \ x_{0m}), \ \ldots, \ (x_{k0}, \ \ldots, \ x_{km})$$

линейно независимы. Последнее означает, что матрица

$$\begin{pmatrix} x_{00} & \cdots & x_{0m} \\ x_{10} & \cdots & x_{1m} \\ \cdots & \cdots & \cdots \\ x_{k0} & \cdots & x_{km} \end{pmatrix}$$

имеет ранг $k + 1$. Число точек в k-плоскости равняется $(q^{k+1} - 1)/(q - 1)$; прямая содержит $q + 1$ точек, а плоскость содержит $q^2 + q + 1$ точек. Нетрудно проверить, что $PG(m, \mathbb{F}_q)$ удовлетворяет всем пяти аксиомам m-пространства.

Мы знаем, что в поле $\mathbb{F}_{q^{m+1}}$ любую степень первообразного элемента α можно представить в виде многочлена от α степени не выше m с коэффициентами из поля $\mathbb{F}_q$. Если

$$\alpha^i = a_m\alpha^m + \cdots + a_0,$$

мы можем рассматривать α^i как точку пространства $PG(m, \mathbb{F}_q)$ с координатами $(a_0, \ldots, a_m)$. Две степени α^i и α^j задают одну и ту же точку тогда и только тогда, когда для некоторого $a \in \mathbb{F}_q^*$ выполняется равенство $\alpha^i = a\alpha^j$, т. е. тогда и только тогда, когда

$$i \equiv j \pmod{(q^{m+1} - 1)/(q - 1)}.$$

k-плоскость S, содержащая $k + 1$ линейно независимых точек, которые соответствуют степеням $\alpha^{i_0}, \ldots, \alpha^{i_k}$, содержит все точки, которые можно представить в виде $\sum_{r=0}^{k} a_r\alpha^{i_r}$, где элементы a_r принадлежат $\mathbb{F}_q$ и не все одновременно равны 0. Если положить $v = (q^{m+1} - 1)/(q - 1)$, то для каждого значения $h = 0, 1, \ldots, v - 1$ точки вида $\sum_{r=0}^{k} a_r\alpha^{i_r+h}$ (где $a_r \in \mathbb{F}_q$ и не все a_r одновре-

менно равны 0) тоже образуют k-плоскость. Обозначим k-плоскость, соответствующую заданному значению h, через S_h. Тогда $S_v = S_0 = S$, так как $\alpha^v \in \mathbb{F}_q$. Пусть j — наименьшее натуральное число, для которого $S_j = S$. Тогда из равенства $S_{nj} = S$ для всех $n \in \mathbb{N}$ следует, что j делит v, т. е. что $v = tj$. Назовем число j *циклом* k-плоскости S.

Если α^{d_0} определяет точку, принадлежащую k-плоскости S, то этим же свойством обладают и точки, соответствующие показателям степени

$$d_0,\ d_0 + j,\ \ldots,\ d_0 + (t-1)\,j$$

в силу того, что $S_{nj} = S$ для всех $n = 0, 1, \ldots, t-1$. Другие точки поверхности S можно задать с помощью степеней элемента α со следующими показателями:

$$\begin{aligned} &d_1, \quad d_1 + j, \quad \ldots, \quad d_1 + (t-1)\,j, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &d_{u-1}, \quad d_{u-1} + j, \quad \ldots, \quad d_{u-1} + (t-1)\,j, \end{aligned}$$

где $d_{r_1} - d_{r_2}$ не делится на j, если $r_1 \neq r_2$. Число всех таких различных точек равно $tu = (q^{k+1} - 1)/(q-1)$.

Если $tj = (q^{m+1} - 1)/(q-1)$ и $tu = (q^{k+1} - 1)/(q-1)$ взаимно просты, то $t = 1$, $j = v$ и все k-плоскости имеют цикл v. Последнее выполняется в случае $k = m - 1$ и в случае $k = 1$ при условии, что m четно.

9.71. Пример. Рассмотрим проективную геометрию $PG(3, \mathbb{F}_2)$, которая содержит 15 точек, 35 прямых и 15 плоскостей; при этом $q^{m+1} = 16$. Используя в качестве элемента $\alpha \in \mathbb{F}_{16}$ корень примитивного многочлена $x^4 + x + 1 \in \mathbb{F}_2[x]$, установим соответствие между степенями элемента α и точками из $PG(3, \mathbb{F}_2)$:

$A = (0, 0, 0, 1) \sim \alpha^3$, $F = (0, 1, 1, 0) \sim \alpha^5$, $K = (1, 0, 1, 1) \sim \alpha^{13}$,

$B = (0, 0, 1, 0) \sim \alpha^2$, $G = (0, 1, 1, 1) \sim \alpha^{11}$, $L = (1, 1, 0, 0) \sim \alpha^4$,

$C = (0, 0, 1, 1) \sim \alpha^6$, $H = (1, 0, 0, 0) \sim \alpha^0$, $M = (1, 1, 0, 1) \sim \alpha^7$,

$D = (0, 1, 0, 0) \sim \alpha^1$, $I = (1, 0, 0, 1) \sim \alpha^{14}$, $N = (1, 1, 1, 0) \sim \alpha^{10}$,

$E = (0, 1, 0, 1) \sim \alpha^9$, $J = (1, 0, 1, 0) \sim \alpha^8$, $O = (1, 1, 1, 1) \sim \alpha^{12}$.

Плоскость

$$S = S_0 = \{a_0\alpha^0 + a_1\alpha^1 + a_2\alpha^2 \mid a_0,\ a_1,\ a_2 \in \mathbb{F}_2,\ (a_0,\ a_1,\ a_2) \neq (0,\ 0,\ 0)\}$$

совпадает с плоскостью, определяемой уравнением $x_3 = 0$. Она содержит точки B, D, F, H, J, L, N, и ее цикл равен 15, так же как и цикл любой другой гиперплоскости. Плоскость

$$S_1 = \{a_0\alpha^1 + a_1\alpha^2 + a_2\alpha^3 \mid a_0,\ a_1,\ a_2 \in \mathbb{F}_2,\ (a_0,\ a_1,\ a_2) \neq (0,\ 0,\ 0)\}$$

совпадает с плоскостью, определяемой уравнением $x_0 = 0$, и содержит точки A, B, C, D, E, F, G и т. д. Цикл прямой

$$\{a_0\alpha^3 + a_1\alpha^8 \mid a_0,\ a_1 \in \mathbb{F}_2,\ (a_0,\ a_1) \neq (0,\ 0)\},$$

совпадающей с прямой AJK, равен 5. Обе прямые ABC и ADE имеют цикл 15. Таким образом, указаны все $5 + 15 + 15 = 35$ прямых. □

Конечной аффинной (или *евклидовой*) *геометрией*, обозначаемой через $AG(m, \mathbb{F}_q)$, называется множество k-плоскостей (для всех возможных k), которое остается, если из $PG(m, \mathbb{F}_q)$ выбросить некоторую гиперплоскость вместе со всеми k-плоскостями, содержащимися в этой гиперплоскости. Все выброшенные k-плоскости называются *бесконечно удаленными k-плоскостями*. Те из оставшихся k-плоскостей, которые пересекаются по бесконечно удаленной k-плоскости, называются *параллельными*. Принято выбрасывать гиперплоскость, определяемую уравнением $x_m = 0$. Тогда мы можем считать, что координата x_m у всех точек из $AG(m, \mathbb{F}_q)$ равняется 1, и рассматривать для этих точек только остальные координаты. Так как $PG(m, \mathbb{F}_q)$ содержит $q^m + \ldots + q + 1$ точек, а удаленная гиперплоскость содержит $q^{m-1} + \ldots + q + 1$ точек, то $AG(m, \mathbb{F}_q)$ содержит q^m точек.

k-плоскость в $AG(m, \mathbb{F}_q)$ состоит из всех q^k точек, координаты которых удовлетворяют системе уравнений

$$a_{i0}x_0 + \cdots + a_{i,\,m-1}x_{m-1} + a_{im} = 0, \quad i = 1,\ \ldots,\ m - k,$$

матрица коэффициентов которой имеет ранг $m - k$. В частности, гиперплоскость задается уравнением

$$a_0x_0 + \cdots + a_{m-1}x_{m-1} + a_m = 0,$$

в котором не все коэффициенты $a_0, \ldots, a_{m-1}$ равны 0. Если зафиксировать коэффициенты $a_0, \ldots, a_{m-1}$, а a_m заставить пробегать все множество элементов поля $\mathbb{F}_q$, то мы получаем пучок параллельных гиперплоскостей.

§ 4. Приложения к комбинаторике

В этом параграфе мы опишем некоторые примеры использования конечных полей в комбинаторике.

Имеется тесная связь между конечными геометриями и так называемыми *схемами* [1]). Схемы, которые мы собираемся рас-

[1]) В комбинаторной литературе термин design обычно переводят как «блок-схема», но мы будем употреблять последний термин в качестве краткого синонима уравновешенной неполной блок-схемы, тем более что это не приводит к недоразумениям. — *Прим. перев.*

сматривать, состоят из двух непустых множеств объектов и отношения инцидентности между объектами, принадлежащими разным множествам. Так, например, объектами могут быть точки и прямые, а отношение инцидентности определяет, лежит данная точка на данной прямой или нет. Терминология, которая обычно используется в этой области комбинаторнки, берет свое начало в статистических приложениях, точнее в теорнн планирования экспериментов. Два типа объектов обычно называются *элементами* и *блоками*. В приложениях, заложивших основы этой теории, элементами обычно были сорта растений или удобрения. Число элементов обычно обозначается через v, а число блоков — через b.

Схема, в которой каждый блок содержит одно и то же число элементов, равное k, а каждый элемент инцидентен одному и тому же числу блоков r, называется *схемой инцидентности* или *тактической конфигурацией*. Очевидно, что

$$vr = bk. \tag{9.9}$$

Если $v = b$ и, следовательно, $r = k$, то соответствующая схема инцидентности называется *симметричной*. Например, точки и прямые проективной плоскости $PG(2, \mathbb{F}_q)$ образуют симметричную схему инцидентности с $v = b = q^2 + q + 1$ и $r = k = q + 1$. Свойство проективной плоскости, состоящее в том, что каждая пара различных точек инцидентна единственной прямой, приводит к следующему определению, обобщающему это свойство.

9.72. Определение. Схема инцидентности называется *уравновешенной неполной блок-схемой* или (v, k, λ)-*блок-схемой*, если $v \geqslant k \geqslant 2$ и каждая пара различных элементов инцидентна одному и тому же числу блоков λ. Далее для краткости будем называть ее просто *блок-схемой*.

Если для любого фиксированного элемента a_1 подсчитать двумя способами число всех различных пар (a_2, B), где $a_2 \neq a_1$, а B — блок, инцидентный паре (a_1, a_2), то мы приходим к тождеству

$$r(k - 1) = \lambda(v - 1), \tag{9.10}$$

которое должно выполняться для любой (v, k, λ)-блок-схемы. Таким образом, из (9.9) и (9.10) следует, что параметры b и r блок-схемы определяются значениями параметров v, k и λ.

9.73. Пример. Пусть $\{0, 1, 2, 3, 4, 5, 6\}$ — множество элементов, а подмножества $\{0, 1, 3\}$, $\{1, 2, 4\}$, $\{2, 3, 5\}$, $\{3, 4, 6\}$, $\{4, 5, 0\}$, $\{5, 6, 1\}$, $\{6, 0, 2\}$ образуют множество блоков. Отношение инцидентности между элементами и блоками определяется очевидным образом. Тогда это симметричная блок-схема с $v = b = 7$, $r = k = 3$ и $\lambda = 1$. Эта схема эквивалентна плоскости Фано из примера 9.55. В общем случае если $k = 3$, а $\lambda = 1$, то

соответствующая блок-схема называется *системой троек Штейнера*.

9.74. Пример. Блок-схему можно получить, выбирая в качестве элементов точки некоторой проективной или аффинной геометрии, а в качестве блоков t-плоскости для некоторого фиксированного t, $1 \leqslant t < m$, где m — порядок соответствующей геометрии. В случае проективной геометрии $PG(m, \mathbb{F}_q)$ параметры соответствующей блок-схемы имеют вид

$$v = \frac{q^{m+1}-1}{q-1}, \quad b = \prod_{i=1}^{t+1} \frac{q^{m-t+i}-1}{q^i-1}, \quad r = \prod_{i=1}^{t} \frac{q^{m-t+i}-1}{q^i-1},$$

$$k = \frac{q^{t+1}-1}{q-1}, \quad \lambda = \prod_{i=1}^{t-1} \frac{q^{m-t+i}-1}{q^i-1},$$

где при $t = 1$ последнее произведение полагается равным 1. Полученная блок-схема является симметричной, если $t = m - 1$, т. е. если блоки являются гиперплоскостями проективной геометрии $PG(m, \mathbb{F}_q)$. В случае аффинной геометрии $AG(m, \mathbb{F}_q)$ параметры соответствующей блок-схемы задаются формулами

$$v = q^m, \quad b = q^{m-t} \prod_{i=1}^{t} \frac{q^{m-t+i}-1}{q^i-1}, \quad r = \prod_{i=1}^{t} \frac{q^{m-t+i}-1}{q^i-1},$$

$$k = q^t, \quad \lambda = \prod_{i=1}^{t-1} \frac{q^{m-t+i}-1}{q^i-1},$$

где, как и выше, $\lambda = 1$ при $t = 1$. В аффинном случае такая блок-схема не может быть симметричной. □

Схему инцидентности можно описать с помощью ее *матрицы инцидентности*. Эта матрица, обозначаемая в дальнейшем через A, имеет v строк и b столбцов, строки соответствуют элементам схемы, а столбцы — блокам. Занумеруем элементы и блоки. Тогда если i-й элемент инцидентен j-му блоку, то положим (i, j)-й элемент матрицы A равным 1, в противном случае положим его равным 0. Сумма элементов по каждой строке равняется r, сумма по каждому столбцу равняется k.

Если A — матрица инцидентности (v, k, λ)-блок-схемы, то скалярное произведение любых двух не равных между собой строк матрицы A равняется λ. Отсюда следует, что если через A^{T} обозначить транспонированную матрицу A, то

$$AA^{\mathrm{T}} = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \dots & \dots & \dots & \dots \\ \lambda & \lambda & \dots & r \end{pmatrix} = (r-\lambda)I + \lambda J,$$

где I обозначает единичную матрицу размера $v \times v$, а J — матрицу того же размера, все элементы которой равняются 1. Для того чтобы найти определитель матрицы AA^{T}, вычтем сначала первый столбец из всех остальных, а затем прибавим к первой строке сумму всех остальных строк. В результате, используя (9.10), получаем

$$\det(AA^{\mathrm{T}}) = \begin{vmatrix} rk & 0 & 0 & \dots & 0 \\ \lambda & r-\lambda & 0 & \dots & 0 \\ \lambda & 0 & r-\lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \lambda & 0 & 0 & \dots & r-\lambda \end{vmatrix} = rk(r-\lambda)^{v-1}.$$

Если $v = k$, блок-схема становится тривиальной, так как в этом случае каждый блок инцидентен всем v элементам. Если $v > k$, то по (9.10) $r > \lambda$, и тогда ранг матрицы AA^{T} равняется v. Матрица A не может иметь меньший ранг. Таким образом, мы получаем соотношение

$$b \geqslant v. \tag{9.11}$$

Из (9.9) и (9.11) получаем также, что $r \geqslant k$.

Для *симметричной* (v, k, λ)-блок-схемы справедливо равенство $r = k$. Отсюда следует, что $AJ = JA$ и что матрица A коммутирует с матрицей $(r-\lambda)I + \lambda J = AA^{\mathrm{T}}$. Если $v > k$, то A — невырожденная матрица, и потому $A^{\mathrm{T}}A = AA^{\mathrm{T}} = (r-\lambda)I + \lambda J$. Отсюда следует, что *любые два различных блока имеют ровно λ общих элементов*. Последнее свойство очевидным образом справедливо, если $v = k$.

Мы видели, что условия (9.9), (9.10), а также (9.11) являются необходимыми для существования блок-схемы с параметрами v, b, r, k, λ. Однако эти условия не являются достаточными для существования соответствующей блок-схемы. Так, например, известно, что блок-схем с параметрами $v = b = 43$, $r = k = 7$ и $\lambda = 1$ не существует.

Элементы и блоки симметричной (v, k, λ)-блок-схемы с $k \geqslant 3$ и $\lambda = 1$ удовлетворяют условиям, которым должны удовлетворять точкн и прямые конечной проективной плоскости. Верно и обратное. Таким образом, *понятия симметричной $(v, k, 1)$-блок-схемы с $k \geqslant 3$ и конечной проективной плоскости эквивалентны*.

Рассмотрим блок-схему из примера 9.73. Будем рассматривать элементы этой блок-схемы 0, 1, 2, 3, 4, 5, 6 как целые числа по модулю 7. Каждый блок этой схемы обладает тем свойством, что разности между различными входящими в него элементами пробегают все ненулевые вычеты по модулю 7. Это приводит к следующему определению.

9.75. Определение. Множество $D = \{d_1, \ldots, d_k\}$, состоящее из $k \geqslant 2$ различных вычетов по модулю v, называется (v, k, λ)-*разностным множеством*, если для любого $d \not\equiv 0 \pmod{v}$ существует ровно λ упорядоченных пар (d_i, d_j), $d_i, d_j \in D$, таких, что $d_i - d_j \equiv d \pmod{v}$.

Следующий результат устанавливает связь между разностными множествами, блок-схемами и конечными проективными плоскостями.

9.76. Теорема. *Пусть* $\{d_1, \ldots, d_k\}$ *является* (v, k, λ)-*разностным множеством. Тогда если в качестве элементов взять все вычеты по модулю* v, *а в качестве блоков—множества вида*

$$B_t = \{d_1 + t, \ \ldots, \ d_k + t\}, \quad t = 0, \ 1, \ \ldots, \ v - 1,$$

то мы получим симметричную (v, k, λ)-*блок-схему с очевидным отношением инцидентности.*

Доказательство. Каждый вычет по модулю v, скажем a, встречается только в тех блоках, нижний индекс которых равен одной из величин $a - d_1, \ldots, a - d_k$ по модулю v. Отсюда получаем, что каждый элемент инцидентен одному и тому же числу блоков, равному k. Каждая пара различных вычетов по модулю v, скажем a и c, принадлежит одному блоку B_t тогда и только тогда, когда $a \equiv d_i + t \pmod{v}$ и $c \equiv d_j + t \pmod{v}$ для некоторых d_i и d_j. Следовательно, $a - c \equiv d_i - d_j \pmod{v}$. Верно и обратное: если пара (d_i, d_j) является решением последнего сравнения, то оба элемента a и c встречаются в блоке B_t, где $t \equiv a - d_i \pmod{v}$. По условию теоремы имеется ровно λ различных решений вида (d_i, d_j), поэтому выполнены все условия для существования симметричной (v, k, λ)-блок-схемы. □

9.77. Следствие. *Пусть* $\{d_1, \ldots, d_k\}$ *является* $(v, k, 1)$-*разностным множеством с* $k \geqslant 3$. *Тогда вычеты по модулю* v *и блоки* B_t, $t = 0, \ 1, \ \ldots, \ v - 1$, *определенные в теореме* 9.76, *удовлетворяют всем условиям, налагаемым на точки и прямые конечной проективной плоскости порядка* $k - 1$.

Доказательство. Сформулированное утверждение следует из теоремы 9.76 и того, что симметричная $(v, k, 1)$-блок-схема с $k \geqslant 3$ является конечной проективной плоскостью. □

Из теоремы 9.76 и соотношения (9.10) следует, что параметры разностного множества v, k и λ связаны тождеством $k(k - 1) = \lambda(v - 1)$. Это тождество можно также получить непосредственно из определения разностного множества.

9.78. Пример. Множество $\{0, 1, 2, 4, 5, 8, 10\}$, составленное из вычетов по модулю 15, является (15, 7, 3)-разностным множеством. По теореме 9.76 блоки вида

$$B_t = \{t, t+1, t+2, t+4, t+5, t+8, t+10\},$$
$$t = 0, 1, \ldots, 14,$$

образуют симметричную (15, 7, 3)-блок-схему. Ее блоки можно отождествить с 15 плоскостями проективной геометрии $PG(3, \mathbb{F}_2)$, в то время как все 15 вычетов по модулю 15 отождествляются с точками той же геометрии. Каждая из этих плоскостей является плоскостью Фано $PG(2, \mathbb{F}_2)$. Для каждого блока B_t все его прямые можно получить из прямой

$$L_t = B_t \cap B_{t-4} = \{t, t+1, t+4\},$$

принадлежащей плоскости B_t, с помощью циклической перестановки

$$t \to t+1 \to t+2 \to t+4 \to t+5 \to t+10 \to t+8 \to t.$$

Например, прямые, лежащие в плоскости $B_0 = \{0, 1, 2, 4, 5, 10, 8\}$, имеют вид

$$\{0, 1, 4\}, \{1, 2, 5\}, \{2, 4, 10\}, \{4, 5, 8\}, \{5, 10, 0\}, \{10, 8, 1\},$$
$$\{8, 0, 2\}.$$ □

Примеры разностных множеств можно строить на основе конечных проективных геометрий. Отождествим, как и в рассуждении, предшествующем примеру 9.71, точки проективной геометрии $PG(m, \mathbb{F}_q)$ со степенями элемента α, где α является примитивным элементом поля $\mathbb{F}_{q^{m+1}}$, причем показатели степени элемента α берутся по модулю $v = (q^{m+1} - 1)/(q - 1)$. Пусть S — произвольная гиперплоскость в $PG(m, \mathbb{F}_q)$. Тогда S имеет цикл v, и, таким образом, все гиперплоскости $S_h = \alpha^h S$, $h = 0, 1, \ldots, v-1$, являются различными. А так как число всех гиперплоскостей этого пространства равно v, то ими исчерпываются все гиперплоскости пространства $PG(m, \mathbb{F}_q)$. Таким образом, приводимый ниже список является полным списком всех гиперплоскостей проективного пространства $PG(m, \mathbb{F}_q)$ (в нем точки, лежащие на соответствующей гиперплоскости, задаются соответствующим показателем степени элемента α):

$$\begin{array}{lllll} S_0: & d_1 & d_2 & \ldots & d_k \\ S_1: & d_1+1 & d_2+1 & \ldots & d_k+1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ S_{v-1}: & d_1+v-1 & d_2+v-1 & \ldots & d_k+v-1 \end{array}$$

Здесь $k = (q^m - 1)/(q - 1)$ — число точек одной гиперплоскости. Если мы выделим те строки, которые содержат какое-то конкретное значение, скажем 0, то получим k гиперплоскостей, проходящих через точку α^0. Эти k строк имеют вид

$$\begin{matrix} d_1 - d_1 & d_2 - d_1 & \dots & d_k - d_1 \\ d_1 - d_2 & d_2 - d_2 & \dots & d_k - d_2 \\ \dots & \dots & \dots & \dots \\ d_1 - d_k & d_2 - d_k & \dots & d_k - d_k \end{matrix}$$

Каждая точка, отличная от α^0, встречается в этих k гиперплоскостях столько раз, сколько имеется различных гиперплоскостей, проходящих через две различные точки, а именно в $\lambda = (q^{m-1} - 1)/(q - 1)$ из них. Таким образом, среди элементов, не стоящих на диагонали, каждый ненулевой вычет по модулю v встречается ровно λ раз. Следовательно, $\{d_1, \dots, d_k\}$ является (v, k, λ)-разностным множеством. Следующая теорема объединяет полученные результаты.

9.79. Теорема. *Точки любой гиперплоскости пространства $PG(m, \mathbb{F}_q)$ образуют (v, k, λ)-разностное множество с параметрами*

$$v = \frac{q^{m+1} - 1}{q - 1}, \quad k = \frac{q^m - 1}{q - 1}, \quad \lambda = \frac{q^{m-1} - 1}{q - 1}.$$

9.80. Пример. Рассмотрим гиперплоскость проективного пространства $PG(3, \mathbb{F}_2)$ (см. пример 9.71), определяемую уравнением $x_1 = 0$. Она содержит точки A, B, C, H, I, J, K. Эти точки можно отождествить со степенями элемента α, причем соответствующие показатели степени образуют (15, 7, 3)-разностное множество $\{0, 2, 3, 6, 8, 13, 14\}$. □

Другим разделом комбинаторики, в котором применяется теория конечных полей, является теория ортогональных латинских квадратов.

9.81. Определение. Таблица

$$L = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

называется *латинским квадратом* порядка n, если любая строка и любой столбец этой таблицы содержат ровно по одному разу каждый элемент из данного множества, содержащего n элементов. Два латинских квадрата (a_{ij}) и (b_{ij}) порядка n называются *ортогональными*, если все n^2 упорядоченных пар (a_{ij}, b_{ij}) различны.

9.82. Теорема. *Для любого натурального числа n существует латинский квадрат порядка n.*

Доказательство. Рассмотрим таблицу (a_{ij}), где $a_{ij} \equiv i + j \pmod n$, $1 \leqslant a_{ij} \leqslant n$. Тогда из равенства $a_{ij} = a_{ik}$ следует, что $i + j \equiv i + k \pmod n$, т. е. $j \equiv k \pmod n$, откуда $j = k$, так как $1 \leqslant i, j, k \leqslant n$. Аналогично из равенства $a_{ij} = a_{kj}$ следует, что $i = k$. Таким образом, элементы каждой строки и каждого столбца все различны. □

Ортогональные латинские квадраты впервые изучались Эйлером. Он выдвинул гипотезу, что не существует пары ортогональных латинских квадратов порядка n, если n равно произведению 2 и нечетного числа. Эта гипотеза была опровергнута в 1959 г. после того, как была построена пара ортогональных латинских квадратов порядка 22.

Для некоторых значений n существует более двух взаимно ортогональных латинских квадратов порядка n (т. е. таких латинских квадратов, каждая пара которых ортогональна). Ниже, используя существование конечных полей порядка q, мы покажем, что если число $n = q$ является степенью простого числа, то существует $q - 1$ попарно ортогональных латинских квадратов порядка q.

9.83. Теорема. *Пусть $a_0 = 0$, a_1, a_2, ..., a_{q-1} — элементы поля $\mathbb{F}_q$. Тогда таблицы вида*

$$L_k = \begin{pmatrix} a_0 & a_1 & \dots & a_{q-1} \\ a_k a_1 & a_k a_1 + a_1 & \dots & a_k a_1 + a_{q-1} \\ a_k a_2 & a_k a_2 + a_1 & \dots & a_k a_2 + a_{q-1} \\ \dots & \dots & \dots & \dots \\ a_k a_{q-1} & a_k a_{q-1} + a_1 & \dots & a_k a_{q-1} + a_{q-1} \end{pmatrix}, \quad k = 1, \dots, q-1,$$

образуют множество из $q - 1$ попарно ортогональных латинских квадратов порядка q.

Доказательство. Каждая таблица L_k, очевидно, является латинским квадратом. Пусть $a_{ij}^{(k)} = a_k a_{i-1} + a_{j-1}$ есть (i, j)-й элемент латинского квадрата L_k. Если $k \neq m$, то предположим, что для некоторых $1 \leqslant i, j, g, h \leqslant q$

$$(a_{ij}^{(k)}, a_{ij}^{(m)}) = (a_{gh}^{(k)}, a_{gh}^{(m)}).$$

Тогда

$$(a_k a_{i-1} + a_{j-1}, a_m a_{i-1} + a_{j-1}) = (a_k a_{g-1} + a_{h-1}, a_m a_{g-1} + a_{h-1}),$$

откуда

$$a_k (a_{i-1} - a_{g-1}) = a_{h-1} - a_{j-1}, \quad a_m (a_{i-1} - a_{g-1}) = a_{h-1} - a_{j-1}.$$

Так как $a_k \neq a_m$, получаем, что $a_{i-1} = a_{g-1}$, $a_{h-1} = a_{j-1}$ и, следовательно, $i = g$, $j = h$. Таким образом, все упорядоченные пары одинаково расположенных элементов в L_k и L_m являются различными, т. е. L_k и L_m ортогональны. □

9.84. Пример. Ниже приводится множество из 4 попарно ортогональных латинских квадратов порядка 5, построенных методом, указанным в теореме 9.83:

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix}, \quad L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix},$$

$$L_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}, \quad L_4 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}. \quad \square$$

Следующий результат, рассматривающий случай латинских квадратов порядка n, когда n не является степенью простого числа, доказывается методом, аналогичным доказательству теоремы 9.83.

9.85. Теорема. *Пусть* $q_1, \ldots, q_s$ *— степени простых чисел, и пусть*

$$a_0^{(i)} = 0,\ a_1^{(i)},\ a_2^{(i)},\ \ldots,\ a_{q_i-1}^{(i)}$$

— элементы поля $\mathbb{F}_{q_i}$. *Определим* s*-наборы*

$$b_k = (a_k^{(1)},\ \ldots.\ a_k^{(s)}), \quad \text{где } 0 \leqslant k \leqslant r = \min_{1 \leqslant i \leqslant s} (q_i - 1),$$

и пусть $b_{r+1}, \ldots, b_{n-1}$, $n = q_1 \ldots q_s$, *— все остальные* s*-наборы, которые можно получить, беря в качестве* i*-й координаты элемент поля* $\mathbb{F}_{q_i}$. *На множестве этих* s*-наборов можно определить операции покоординатного сложения и умножения. Тогда таблицы вида*

$$L_k = \begin{pmatrix} b_0 & b_1 & \ldots & b_{n-1} \\ b_k b_1 & b_k b_1 + b_1 & \ldots & b_k b_1 + b_{n-1} \\ b_k b_2 & b_k b_2 + b_1 & \ldots & b_k b_2 + b_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ b_k b_{n-1} & b_k b_{n-1} + b_1 & \ldots & b_k b_{n-1} + b_{n-1} \end{pmatrix}, \quad k = 1, \ldots, r,$$

образуют множество из r попарно ортогональных латинских квадратов порядка n.

Схемы инцидентности и латинские квадраты используются при *планировании статистических экспериментов*. Например, пусть нам требуется сравнить урожайность n сортов пшеницы на данном типе почвы. Пусть опытный участок представляет собой прямоугольное поле, разбитое на n^2 участков. Даже если мы будем очень тщательно выбирать опытное поле, все равно различные его участки будут отличаться по плодородию почвы. Поэтому если засеять участки первого ряда одним сортом пшеницы, то может оказаться, что именно первый ряд участков отличается наиболее высоким плодородием почвы, и мы сделаем неправильный вывод о высокой урожайности этого сорта пшеницы. Наши оценки будут более правильными, если засеять участки таким образом, что один сорт пшеницы будет встречаться по одному разу в каждом вертикальном и каждом горизонтальном рядах. Другими словами, посев n сортов пшеницы надо провести таким образом, чтобы получился латинский квадрат порядка n.

Часто бывает необходимо одновременно учесть и другие факторы, влияющие на урожайность. Пусть, например, мы хотим использовать n различных видов удобрений и оценить эффективность их использования. Тогда мы распределим удобрения и сорта пшеницы по n^2 участкам таким образом, чтобы как размещение удобрений, так и размещение сортов пшеницы определяли латинский квадрат порядка n и чтобы при этом каждый сорт пшеницы и каждое удобрение «сходились» ровно на одном участке. Таким образом, на языке комбинаторики латинские квадраты, соответствующие размещению сортов пшеницы и размещению видов удобрений, должны быть ортогональны. Аналогичные применения существуют и для уравновешенных неполных блок-схем.

В качестве еще одного примера применения теории конечных полей к комбинаторике рассмотрим так называемые матрицы Адамара. Эти матрицы используются в теории кодирования, в теории связи, а также в физнке (в виде преобразований Адамара) в задачах, связанных с определением веса, сопротивлеиия, напряжения и т. п.

9.86. Определение. *Матрицей Адамара* H_n называется $(n \times n)$-матрица, элементами которой являются $+1$ и -1, удовлетворяющая соотношению

$$H_n H_n^{\mathrm{T}} = nI.$$

Так как $H_n^{-1} = (1/n)\, H_n^{\mathrm{T}}$, то справедливо также соотношение $H_n^{\mathrm{T}} H_n = nI$. Таким образом, любые две различные строки, так же как и любые два различных столбца матрицы H_n, являются ортогональными.

Адамар показал, что определитель любой действительной $(n \times n)$-матрицы M с элементами, по абсолютной величине не превосходящими 1, удовлетворяет неравенству $|\det M| \leqslant n^{n/2}$. В случае матрицы Адамара H_n мы имеем $\det(H_n H_n^{\mathrm{T}}) = n^n$, так что $|\det H_n| = n^{n/2}$, т. е. указанная верхняя граница достижима.

Одновременная смена знаков у всех элементов любой строки или любого столбца не меняет свойств, определяющих матрицу Адамара. Назовем матрицу Адамара H_n *нормализованной*, если все элементы ее первой строки и первого столбца равны $+1$. Нетрудно показать, что порядок n матрицы Адамара (a_{ij}) может лишь равняться 1, 2 или быть кратным 4. В самом деле, для всех $n \geqslant 3$

$$\sum_{j=1}^{n} (a_{1j} + a_{2j})(a_{1j} + a_{3j}) = \sum_{j=1}^{n} a_{1j}^2 = n;$$

и при этом каждый член в первой сумме равен или 0, или 4. Существует гипотеза, что для любого допустимого значения n существует соответствующая матрица Адамара H_n.

9.87. Пример. Нормализованные матрицы Адамара низших порядков имеют вид

$$H_1 = (1), \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \quad \square$$

Приведем теперь конструктивный метод получения матриц Адамара, использующий свойства конечных полей.

9.88. Теорема. *Пусть* $a_1, \ldots, a_q$ *— элементы поля* $\mathbb{F}_q$, $q \equiv 3 \pmod 4$, *и пусть* η *— квадратичный характер поля* $\mathbb{F}_q$. *Тогда матрица*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & -1 & b_{12} & b_{13} & \ldots & b_{1q} \\ 1 & b_{21} & -1 & b_{23} & \ldots & b_{2q} \\ 1 & b_{31} & b_{32} & -1 & \ldots & b_{3q} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & b_{q1} & b_{q2} & b_{q3} & \ldots & -1 \end{pmatrix},$$

где $b_{ij} = \eta(a_j - a_i)$, $1 \leqslant i, j \leqslant q$, $i \neq j$, *является матрицей Адамара порядка* $q + 1$.

Доказательство. Так как все элементы матрицы H равны ± 1, то достаточно показать, что скалярное произведение любых

двух различных строк матрицы H равняется 0. Скалярное произведение 1-й и $(i+1)$-й строк $(1 \leqslant i \leqslant q)$ равно в силу (5.12)

$$1 + (-1) + \sum_{j \neq i} b_{ij} = \sum_{j \neq i} \eta(a_j - a_i) = \sum_{c \in \mathbb{F}_q^*} \eta(c) = 0.$$

Скалярное произведение $(i+1)$-й и $(k+1)$-й строк $(1 \leqslant i < k \leqslant q)$ в свою очередь равно

$$\begin{aligned} 1 - b_{ki} - b_{ik} + \sum_{j \neq i,\, k} b_{ij} b_{kj} = \\ = 1 - \eta(a_i - a_k) - \eta(a_k - a_i) + \sum_{j \neq i,\, k} \eta(a_j - a_i)\,\eta(a_j - a_k) = \\ = 1 - [1 + \eta(-1)]\,\eta(a_i - a_k) + \sum_{c \in \mathbb{F}_q} \eta((c - a_i)(c - a_k)) = 0 \end{aligned}$$

в силу того, что $\eta(-1) = -1$ для $q \equiv 3 \pmod 4$ (см. замечание 5.13), и того, что последняя сумма равна -1 (см. теорему 5.48). □

Если H_n — матрица Адамара порядка n, то матрица

$$\begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

является матрицей Адамара порядка $2n$. Следовательно, этим методом можно получить матрицы Адамара порядка $2^h(q+1)$, где $h \geqslant 0$ и число $q \equiv 3 \pmod 4$ является степенью простого числа. Беря же в качестве исходной матрицу H_1 из примера 9.87, можно получить матрицы Адамара порядка 2^h, $h \geqslant 0$.

§ 5. Линейные модулярные системы

Теория систем — это дисциплина, которая ставит своей целью выработку единого абстрактного подхода и единого аппарата для изучения поведения систем различных типов. Она представляет собой совокупность методов, технических приемов и алгоритмов для решения задач, возникающих при анализе или синтезе систем, при их распознавании, оптимизации и т. п. Основной интерес для специалистов по теории систем представляет математическая структура данной системы, а не ее физическая реализация, область применения или то, какой является система — электрической, механической, экономической, биологической, химической и т. д. Для специалиста по теории систем существенным является, линейна система или нет, является она системой с дискретным временем или с непрерывным временем, детерминированной или стохастической, с дискретным или непрерывным пространством состояний и т. д.

Во введении к настоящей главе мы привели неформальное описание систем. Приведем теперь строгое определение системы

с конечным числом состояний, которая представляет собой идеализированную модель для большого числа физических приборов и явлений. Идеи и методы, развиваемые для систем с конечным числом состояний, оказываются полезными при решении разнообразных задач, появляющихся при исследовании нервной деятельности человека, анализе синтаксиса естественного языка, конструировании вычислительных машин и т. п.

9.89. Определение. *Полная детерминированная система* $\mathscr{M}$ *с конечным числом состояний* определяется следующими элементами:

(1) Конечным непустым множеством $U = \{\alpha_1, \alpha_2, \ldots, \alpha_h\}$, называемым *входным алфавитом* системы $\mathscr{M}$. Элемент множества U называется *входным символом*.

(2) Конечным непустым множеством $Y = \{\beta_1, \beta_2, \ldots, \beta_s\}$, называемым *выходным алфавитом* системы $\mathscr{M}$. Элемент множества Y называется *выходным символом*.

(3) Конечным непустым множеством $S = \{\sigma_1, \sigma_2, \ldots, \sigma_r\}$, называемым *множеством (внутренних) состояний* системы $\mathscr{M}$. Элемент множества S называется (*внутренним*) *состоянием* системы.

(4) *Функцией перехода* f (или *функцией следующего состояния*), которая отображает множество всех упорядоченных пар (σ_i, α_j) в множество S.

(5) *Функцией выхода* g, которая отображает множество всех упорядоченных пар (σ_i, α_j) в множество Y.

Систему $\mathscr{M}$ с конечным числом состояний можно рассматривать как некоторое устройство, вход, выход и внутреннее состояние которого в момент времени t обозначаются соответственно через $u(t)$, $y(t)$, $s(t)$, причем эти величины определены лишь для целых значений параметра t и принимают значения в множествах U, Y и S соответственно. Если заданы внутреннее состояние и вход системы $\mathscr{M}$ в момент времени t, то внутреннее состояние системы в момент $t+1$ и ее выход в момент t определяются по следующим формулам:

$$s(t+1) = f(s(t), u(t)),$$
$$y(t) = g(s(t), u(t)).$$

Линейные модулярные системы образуют специальный класс систем с конечным числом состояний. Для них входной и выходной алфавиты, а также множество внутренних состояний системы наделяются структурой векторного пространства над конечным полем $\mathbb{F}_q$, а функции перехода и выхода являются линейными функциями. Линейные модулярные системы находят широкое применение при управлении сетями компьютеров, для получения кодов, исправляющих ошибки, в генераторах случайных чисел и т. д.

9.90. Определение. *Линейная модулярная система* (*ЛМС*) $\mathscr{M}$ порядка n над полем $\mathbb{F}_q$ задается следующими элементами:

(1) k-мерным векторным пространством над полем $\mathbb{F}_q$, обозначаемым через U и называемым *пространством входов* линейной системы $\mathscr{M}$. Элементы этого пространства называются *входами* и записываются в виде векторов-столбцов.

(2) m-мерным векторным пространством над полем $\mathbb{F}_q$, обозначаемым через Y и называемым *пространством выходов* линейной системы $\mathscr{M}$. Элементы этого пространства называются *выходами* и записываются в виде векторов-столбцов.

(3) n-мерным векторным пространством над полем $\mathbb{F}_q$, обозначаемым через S и называемым *пространством* (*внутренних*) *состояний* линейной системы $\mathscr{M}$. Элементы этого пространства называются (*внутренними*) *состояниями* системы и записываются в виде векторов-столбцов.

(4) Четырьмя *характеристическими матрицами* над полем $\mathbb{F}_q$:

$$A = (a_{ij})_{n\times n}, \quad B = (b_{ij})_{n\times k},$$

$$C = (c_{ij})_{m\times n}, \quad D = (d_{ij})_{m\times k}.$$

Матрица A называется *основной характеристической матрицей ЛМС* $\mathscr{M}$.

(5) Правилом, связывающим внутреннее состояние ЛМС в момент времени $t+1$ и ее выход в момент времени t с внутренним состоянием и входом ЛМС в момент времени t:

$$\mathbf{s}(t+1) = A\mathbf{s}(t) + B\mathbf{u}(t),$$

$$\mathbf{y}(t) = C\mathbf{s}(t) + D\mathbf{u}(t).$$

ЛМС над полем $\mathbb{F}_q$ может быть реализована с помощью переключательной схемы, построенной из сумматоров, усилителей и элементов задержки (ср. с § 1 гл. 8). Нам будет удобно пользоваться сумматорами, которые складывают более чем по два элемента поля. То есть *сумматор* имеет два или более входов

$$u_1(t),\ u_2(t),\ \ldots,\ u_r(t) \in \mathbb{F}_q$$

и единственный выход

$$y_1(t) = u_1(t) + u_2(t) + \ldots + u_r(t).$$

Усилитель, соответствующий константе $a \in \mathbb{F}_q$, имеет единственный вход $u_1(t) \in \mathbb{F}_t$ и единственный выход $y_1(t) = a \cdot u_1(t)$. *Элемент задержки* имеет единственный вход $u_1(t) \in \mathbb{F}_q$ и единственный выход $y_1(t) = u_1(t-1)$. Схематически эти компоненты изображены на рис. 9.5.

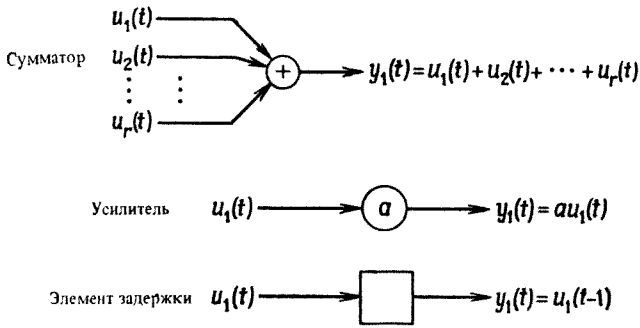


Рис. 9.5.

Опишем теперь, как можно получить схему переключательной сети, моделирующей работу данной ЛМС (см. рис. 9.6).

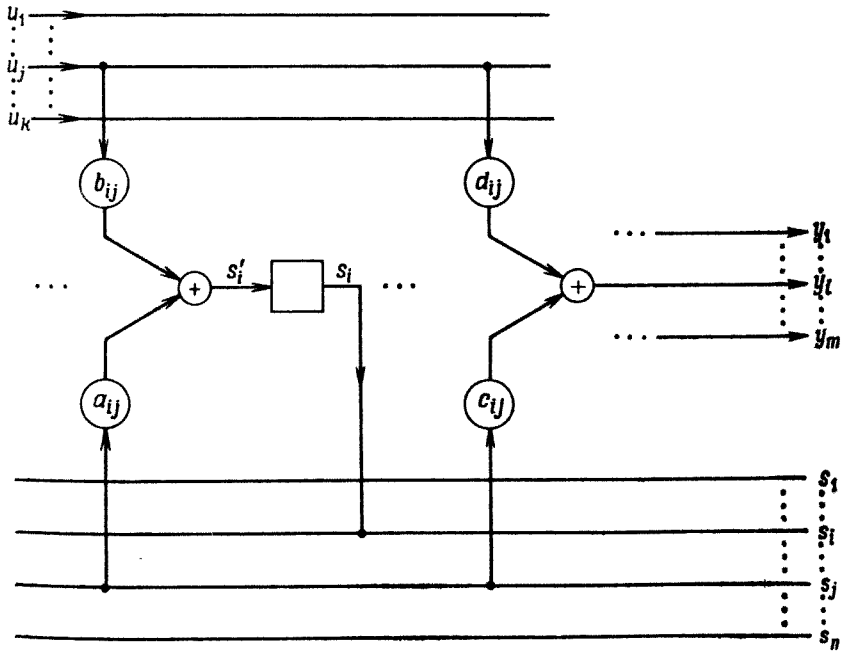


Рис. 9.6.

1. Изобразить в виде прямых k входов системы, пометив их символами $u_1, \ldots, u_k$, m выходов системы, пометив их символами $y_1, \ldots, y_m$, и n элементов задержки. Выходом i-го элемента задержки является $s_i = s_i(t)$, а его входом является $s_i' = s_i(t+1)$.

2. Поместить сумматоры перед каждым выходом системы y_l и перед каждым элементом задержки.

3. Входами сумматора, помещенного перед i-м элементом задержки, являются сигналы s_j, проходящие через усилители с константами a_{ij}, $1 \leqslant i, j \leqslant n$, и сигналы u_j, проходящие через усилители с константами b_{ij}, $1 \leqslant j \leqslant k$.

4. Входами сумматора, соответствующего выходу системы y_i, $1 \leqslant i \leqslant m$, являются сигналы s_j, проходящие через усилители с константами c_{ij}, $1 \leqslant j \leqslant n$, и сигналы u_j, проходящие через усилители с константами d_{ij}, $1 \leqslant j \leqslant k$.

Если положить

$$\mathbf{u}(t) = \begin{pmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ u_k \end{pmatrix}, \quad \mathbf{y}(t) = \begin{pmatrix} y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_m \end{pmatrix}, \quad \mathbf{s}(t) = \begin{pmatrix} s_1 \\ \cdot \\ \cdot \\ \cdot \\ s_n \end{pmatrix}, \quad \mathbf{s}(t+1) = \begin{pmatrix} s_1' \\ \cdot \\ \cdot \\ \cdot \\ s_n' \end{pmatrix},$$

то переключательная схема, изображенная на рис. 9.6, функционирует по законам, приведенным в определении 9.90 (5).

9.91. Пример. Пусть характеристические матрицы ЛМС четвертого порядка над полем $\mathbb{F}_3$ имеют вид

$$A = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$C = \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Тогда схема, реализующая данную ЛМС, изображена на рис. 9.7. □

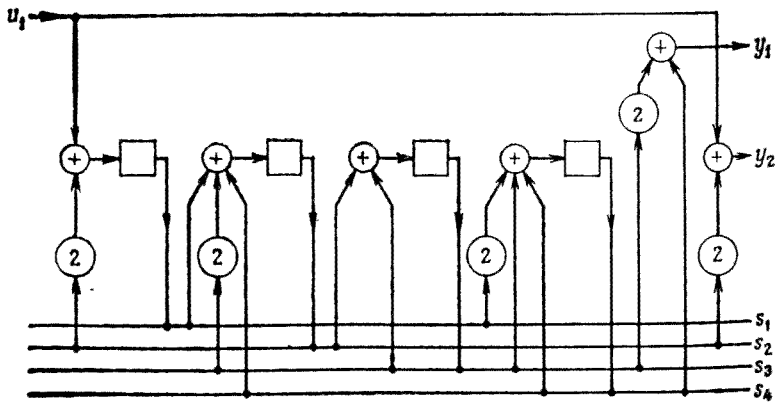


Рис. 9.7.

Верно и обратное: любую переключательную схему, построенную из конечного числа сумматоров, усилителей и элементов задержки над полем $\mathbb{F}_q$, можно следующим образом представить как ЛМС над полем $\mathbb{F}_q$ (при условии, что каждый замкнутый контур содержит по крайней мере один элемент задержки):

1. Выделить в данной переключательной схеме все элементы задержки, все входы и выходы системы и пометить их так, как это было сделано на рис. 9.6.

2. Проследить все пути от s_j к s_i'; найти произведение констант соответствующих всем усилителям, расположенным вдоль каждого такого пути, и сложить все полученные произведения. Полученную сумму обозначить через a_{ij}.

3. Пусть через b_{ij} обозначены аналогичные суммы, соответствующие путям от u_j к s_i', через c_{ij} — суммы, соответствующие путям от s_j к y_i, а через d_{ij} — суммы, соответствующие путям от u_j к y_i.

Тогда данная переключательная схема является реализацией ЛМС над полем $\mathbb{F}_q$ с матрицами $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ и $D = (d_{ij})$, элементы которых определены выше.

Состояния и выходы ЛМС зависят от начального состояния $\mathbf{s}(0)$ и последовательности входов $\mathbf{u}(t)$, $t = 0, 1, \ldots$. Эту зависимость можно выразить явным образом.

9.92. Теорема (формула полной реакции). *Если дана ЛМС с характеристическими матрицами A, B, C, D, то*

$$\text{(i)}\quad \mathbf{s}(t) = A^t\mathbf{s}(0) + \sum_{i=0}^{t-1} A^{t-i-1}B\mathbf{u}(i), \quad t = 1, 2, \ldots,$$

$$\text{(ii)}\quad \mathbf{y}(t) = CA^t\mathbf{s}(0) + \sum_{i=0}^{t} H(t-i)\,\mathbf{u}(i), \quad t = 0, 1, \ldots,$$

где

$$H(t) = \begin{cases} D, & \text{если} \quad t = 0, \\ CA^{t-1}B, & \text{если} \quad t \geqslant 1. \end{cases}$$

Доказательство. (i) Пусть в определении 9.90 (5) $t = 0$, тогда

$$\mathbf{s}(1) = A\mathbf{s}(0) + B\mathbf{u}(0),$$

что доказывает (i) для $t = 1$. Предположим, что (i) выполняется для некоторого $t \geqslant 1$; тогда

$$\mathbf{s}(t+1) = A\left(A^t\mathbf{s}(0) + \sum_{i=0}^{t-1} A^{t-i-1}B\mathbf{u}(i)\right) + B\mathbf{u}(t) =$$

$$= A^{t+1}\mathbf{s}(0) + \sum_{i=0}^{t} A^{t-i}B\mathbf{u}(i),$$

т. е. (i) справедливо и для $t + 1$.

(ii) В силу п. (i) и определения 9.90 (5) получаем, что

$$\mathbf{y}(t) = C\left(A^t\mathbf{s}(0) + \sum_{i=0}^{t-1} A^{t-i-1}B\mathbf{u}(i)\right) + D\mathbf{u}(t) =$$

$$= CA^t\mathbf{s}(0) + \sum_{i=0}^{t} H(t-i)\,\mathbf{u}(i),$$

где $H(t-i) = CA^{t-i-1}B$ для $t - i \geqslant 1$ и $H(t-i) = D$ для $t - i = 0$. □

В силу теоремы 9.92 (ii) мы можем разложить выход произвольной ЛМС на две компоненты: *свободную компоненту*

$$\mathbf{y}(t)_{\text{св}} = CA^t\mathbf{s}(0),$$

получаемую, когда $\mathbf{u}(t) = \mathbf{0}$ для всех $t \geqslant 0$, и *вынужденную компоненту*

$$\mathbf{y}(t)_{\text{вын}} = \sum_{i=0}^{t} H(t-i)\,\mathbf{u}(i),$$

получаемую для случая $\mathbf{s}(0) = \mathbf{0}$. Если дана произвольная входная последовательность $\mathbf{u}(t)$, $t = 0, 1, \ldots$, и произвольное начальное состояние $\mathbf{s}(0)$, то эти две компоненты можно определить по отдельности, а затем сложить.

Оставшаяся часть этого параграфа будет посвящена изучению поведения ЛМС в *автономном случае*, т. е. когда $\mathbf{u}(t) = \mathbf{0}$ для всех $t \geqslant 0$. Для этого нам окажутся полезными некоторые понятия из теории графов. Если дана ЛМС $\mathscr{M}$ порядка n над полем $\mathbb{F}_q$ с основной характеристической матрицей A, то *графом состояний системы* $\mathscr{M}$ (или *графом матрицы* A) называется ориентированный граф, имеющий q^n вершин, которые поставлены во взаимно однозначное соответствие со всеми возможными внутренними состояниями ЛМС $\mathscr{M}$. При этом вершины $\mathbf{s}_1$ и $\mathbf{s}_2$ соединены дугой, идущей из $\mathbf{s}_1$ в $\mathbf{s}_2$, тогда и только тогда, когда $\mathbf{s}_2 = A\mathbf{s}_1$. В этом случае мы говорим, что $\mathbf{s}_1$ *переходит в* $\mathbf{s}_2$. *Путем длины* r в графе состояний называется последовательность из r дуг $b_1, b_2, \ldots, b_r$ и $r + 1$ вершин $v_1, v_2, \ldots, v_{r+1}$, такая, что для всех $i = 1, 2, \ldots, r$ дуга b_i направлена из вершины v_i в вершину v_{i+1}. Если все v_i различны, за исключением того, что $v_{r+1} = v_1$, то такой путь называется *циклом длины* r. Если v_i для любого $i = 1, 2, \ldots, r - 1$ является единственной вершиной, переходящей в v_{i+1}, а единственной вершиной, переходящей в v_1, является v_r, то такой цикл называется *циклом без подходов*. Так, на рис. 9.8 изображен цикл без подходов длины 8.

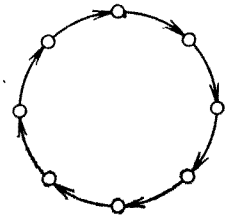


Рис. 9.8.

Порядок данного состояния $\mathbf{s}$ равняется наименьшему положительному числу t, такому, что $A^t\mathbf{s} = \mathbf{s}$. Таким образом, порядок $\mathbf{s}$ совпадает с длиной цикла, содержащего $\mathbf{s}$. Далее, пусть матрица A невырожденна, т. е. $\det A \neq 0$. Очевидно, что в этом случае соответствующий граф состояний состоит из циклов без подходов. Порядок характеристической матрицы A равняется наименьшему положительному числу t, такому, что $A^t = I$, где I — единичная матрица размера $n \times n$.

9.93. Лемма. *Если $t_1, \ldots, t_k$ — все значения, принимаемые порядками состояний некоторой* ЛМС *с невырожденной характеристической матрицей A, то порядок матрицы A равняется* НОК $(t_1, \ldots, t_k)$.

Доказательство. Пусть t — порядок матрицы A, а $t' =$ $=$ НОК $(t_1, \ldots, t_k)$. Так как $A^t\mathbf{s} = \mathbf{s}$ для всех $\mathbf{s}$, то величина t должна делиться на t'. Кроме того, $(A^{t'} - I)\,\mathbf{s} = \mathbf{0}$ для всех $\mathbf{s}$, отсюда $A^{t'} = I$. Таким образом, $t' \geqslant t$ и, следовательно, $t = t'$. □

9.94. Лемма. *Пусть матрица A имеет вид*

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

где A_1 и A_2 — квадратные матрицы, а $\begin{pmatrix} \mathbf{s}_1 \\ \mathbf{0} \end{pmatrix}$ и $\begin{pmatrix} \mathbf{0} \\ \mathbf{s}_2 \end{pmatrix}$ — два состояния, представленных в соответствии с разбиением матрицы A и имеющих порядки соответственно t_1 и t_2. Тогда порядок состояния $\mathbf{s} = \begin{pmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{pmatrix}$ равняется $t =$ НОК (t_1, t_2).

Доказательство. Утверждение леммы непосредственно вытекает из того, что $A^t \begin{pmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{pmatrix}$ тогда и только тогда, когда $A_1^t\mathbf{s}_1 = \mathbf{s}_1$ и $A_2^t\mathbf{s}_2 = \mathbf{s}_2$. □

Пусть $\mathscr{M}$ будет ЛМС с невырожденной основной характеристической матрицей A. Тогда граф состояний системы $\mathscr{M}$ с точностью до изоморфизма определяется формальной суммой вида

$$\Sigma = (n_1, t_1) \dotplus (n_2, t_2) \dotplus \cdots \dotplus (n_R, t_R),$$

где пара (n_i, t_i) означает, что число циклов длины t_i равно n_i. Σ называется *цикловой суммой* системы $\mathscr{M}$ (или матрицы A), а пара (n_i, t_i) называется ее *цикловым членом*. Предполагается, что цикловые члены перестановочны относительно операции $\dotplus$ и при этом $(n', t) \dotplus (n'', t) = (n' + n'', t)$.

Пусть матрица A имеет вид

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

где A_1 и A_2 — квадратные матрицы, и пусть граф состояний, соответствующий матрице A_i, $i = 1, 2$, имеет n_i циклов длины t_i. Таким образом, имеется $n_1 t_1$ состояний вида $\begin{pmatrix} s_1 \\ 0 \end{pmatrix}$ порядка t_1 и $n_2 t_2$ состояний вида $\begin{pmatrix} 0 \\ s_2 \end{pmatrix}$ порядка t_2. По лемме 9.94 граф состояний матрицы A должен содержать $n_1 n_2 t_1 t_2$ состояний порядка НОК (t_1, t_2) и соответственно

$$n_1 n_2 t_1 t_2 / \text{НОК}\ (t_1, t_2) = n_1 n_2 \text{НОД}\ (t_1, t_2)$$

циклов длины НОК (t_1, t_2).

Произведение двух цикловых членов является цикловым членом, определяемым формулой

$$(n_1, t_1) \cdot (n_2, t_2) = (n_1 n_2 \text{НОД}\ (t_1, t_2),\ \text{НОК}\ (t_1, t_2)).$$

Произведение двух цикловых сумм определяется как формальная сумма всех возможных попарных произведений цикловых членов из соответствующих цикловых сумм. Другими словами, это произведение вычисляется в соответствии с законами дистрибутивности.

9.95. Теорема. *Если*

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

а цикловые суммы, соответствующие A_1 и A_2, обозначены через Σ_1 и Σ_2, то цикловая сумма, соответствующая матрице A, равняется $\Sigma_1 \Sigma_2$.

Наша задача — найти алгоритм для вычисления цикловой суммы, соответствующей ЛМС над полем $\mathbb{F}_q$ с невырожденной характеристической матрицей A. Для этого нам потребуются некоторые понятия из теории матриц. *Характеристический многочлен* квадратной матрицы M над полем $\mathbb{F}_q$ определяется как $\det(xI - M)$. *Минимальным многочленом* $m(x)$ той же матрицы M называется нормированный многочлен минимальной степени над

полем $\mathbb{F}_q$, такой, что $m(M) = 0$, где 0 — нулевая матрица. Если дан нормированный многочлен над полем $\mathbb{F}_q$

$$g(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0,$$

то его *сопровождающая матрица* определяется как матрица вида

$$M(g(x)) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -a_{k-1} \end{pmatrix}.$$

В этом случае многочлен $g(x)$ является и характеристическим и минимальным многочленом матрицы $M(g(x))$.

Пусть M — квадратная матрица над полем $\mathbb{F}_q$, а $g_1(x), \ldots, g_w(x)$ — ее нормированные элементарные делители. Тогда произведение $g_1(x) \ldots g_w(x)$ равняется характеристическому многочлену матрицы M, и матрица M подобна матрице

$$M^* = \begin{pmatrix} M(g_1(x)) & 0 & \ldots & 0 \\ 0 & M(g_2(x)) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & M(g_w(x)) \end{pmatrix},$$

т. е. $M = P^{-1}M^*P$, где P — некоторая невырожденная матрица над полем $\mathbb{F}_q$. Матрица M^* называется *рациональной канонической формой* матрицы M, а подматрицы $M(g_i(x))$ называются *элементарными блоками* матрицы M^*.

Пусть невырожденная матрица A является основной характеристической матрицей ЛМС над полем $\mathbb{F}_q$. Для того чтобы найти ее цикловую сумму, матрицу A можно заменить подобной матрицей. Таким образом, вместо A можно рассматривать рациональную каноническую форму A^* матрицы A. Применяя теорему 9.95, по индукции получаем следующее. Пусть $g_1(x), \ldots, g_w(x)$ — нормированные элементарные делители матрицы A, и пусть Σ_i — цикловая сумма сопровождающей матрицы $M(g_i(x))$. Тогда цикловая сумма Σ матрицы A^*, а следовательно, и матрицы A определяется формулой

$$\Sigma = \Sigma_1 \Sigma_2 \ldots \Sigma_w$$

Пусть характеристический многочлен $f(x)$ матрицы A представлен в виде

$$f(x) = \prod_{j=1}^{r} p_j(x)^{e_j},$$

где $p_j(x)$ — различные нормированные неприводимые многочлены над полем $\mathbb{F}_q$. Тогда элементарные делители матрицы A имеют вид

$$p_j(x)^{e_{j1}},\ p_j(x)^{e_{j2}},\ \ldots,\ p_j(x)^{e_{jk_j}},\quad j=1,\ 2,\ ,\ \ldots,\ r,$$

где

$$e_{j1}\geqslant e_{j2}\geqslant\cdots\geqslant e_{jk_j}>0,\quad e_{j1}+e_{j2}+\cdots+e_{jk_j}=e_j.$$

Минимальный многочлен матрицы A равняется

$$m(x)=\prod_{j=1}^{r}p_j(x)^{e_{j1}}.$$

Остается определить цикловые суммы элементарных блоков $M(g_i(x))$ матрицы A^*, где $g_i(x)=p(x)^e$, а $p(x)$ — некоторый нормированный неприводимый делитель многочлена $f(x)$. Следующий результат позволяет решить поставленную задачу.

9.96. Теорема. *Пусть $p(x)$ — нормированный неприводимый многочлен над полем $\mathbb{F}_q$, $\deg(p(x))=d$, и пусть $t_h=\operatorname{ord}(p(x)^h)$. Тогда цикловая сумма матрицы $M(p(x)^e)$ определяется формулой*

$$(1,\ 1)\dotplus\left(\frac{q^d-1}{t_1},\ t_1\right)\dotplus\left(\frac{q^{2d}-q^d}{t_2},\ t_2\right)\dotplus\cdots\dotplus\left(\frac{q^{ed}-q^{(e-1)d}}{t_e},\ t_e\right).$$

В итоге мы получили следующий *алгоритм для определения цикловой суммы* ЛМС $\mathscr{M}$ над полем $\mathbb{F}_q$ с невырожденной основной характеристической матрицей A:

С1. Найти элементарные делители матрицы A; пусть это будут многочлены $g_1(x),\ \ldots,\ g_w(x)$.

С2. Пусть $g_i(x)=f_i(x)^{m_i}$, где $f_i(x)$ — нормированный неприводимый многочлен над полем $\mathbb{F}_q$. Найти порядки $t_1^{(i)}=\operatorname{ord}(f_i(x))$.

С3. Для $i=1,\ 2,\ \ldots,\ w$ и $h=1,\ 2,\ \ldots,\ m_i$ найти порядки $t_h^{(i)}=\operatorname{ord}(f_i(x)^h)$, воспользовавшись формулой $t_h^{(i)}=t_1^{(i)}p^{c_h}$, где p — характеристика поля $\mathbb{F}_q$, а c_h — наименьшее целое число, такое, что $p^{c_h}\geqslant h$ (см. теорему 3.8).

С4. Пользуясь теоремой 9.96, найти цикловые суммы Σ_i для матриц $M(g_i(x))$, $i=1,\ 2,\ \ldots,\ w$.

С5. Тогда цикловая сумма Σ системы $\mathscr{M}$ задается формулой $\Sigma=\Sigma_1\Sigma_2\ldots\Sigma_w$.

9.97. Пример. Пусть основная характеристическая матрица ЛМС $\mathscr{M}$ над полем $\mathbb{F}_2$ имеет вид

$$A=\begin{pmatrix}0&0&1&0&0\\1&0&1&0&0\\0&1&1&0&0\\0&0&0&0&1\\0&0&0&1&1\end{pmatrix}.$$

В этом случае

$$g_1(x) = x^3 + x^2 + x + 1 = (x+1)^3, \quad f_1(x) = x + 1, \quad m_1 = 3,$$
$$g_2(x) = x^2 + x + 1, \quad f_2(x) = x^2 + x + 1, \quad m_2 = 1.$$

Выполнив шаги С2 и С3, получаем $t_1^{(1)} = 1$, $t_2^{(1)} = 2$, $t_3^{(1)} = 4$, $t_1^{(2)} = 3$. Тогда по теореме 9.96

$$\Sigma_1 = (1, 1) \dot{+} (1, 1) \dot{+} (1, 2) \dot{+} (1, 4) = (2, 1) \dot{+} (1, 2) \dot{+} (1, 4),$$
$$\Sigma_2 = (1, 1) \dot{+} (1, 3)$$

и, следовательно,

$$\Sigma = \Sigma_1\Sigma_2 = [(2, 1) \dot{+} (1, 2) \dot{+} (1, 4)]\,[(1, 1) \dot{+} (1, 3)] = (2, 1) \dot{+} (1, 2) \dot{+} (2, 3) \dot{+} (1, 4) \dot{+} (1, 6) \dot{+} (1, 12).$$

Таким образом, граф состояний ЛМС $\mathscr{M}$ содержит два цикла длины 1, один цикл длины 2, два цикла длины 3 и по одному циклу длин 4, 6 и 12. □

Из шага С5 можно получить, что порядки состояний ЛМС $\mathscr{M}$ задаются формулой

$$\text{НОК}\left(t_{h_1}^{(1)}, t_{h_2}^{(2)}, \ldots, t_{h_w}^{(w)}\right)$$

для всех возможных комбинаций целочисленных значений параметров $h_1, \ldots, h_w$, $0 \leqslant h_i \leqslant m_i$. Если мы хотим найти все возможные значения порядков состояний системы $\mathscr{M}$, не вычисляя предварительно ее цикловую сумму, то можно воспользоваться следующей теоремой.

9.98. Теорема. *Пусть $\mathscr{M}$ — ЛМС с невырожденной основной характеристической матрицей A. Пусть минимальный многочлен матрицы A имеет каноническое разложение*

$$m(x) = p_1(x)^{b_1} \ldots p_r(x)^{b_r},$$

и пусть $t_h^{(j)} = \operatorname{ord}(p_j(x)^h)$. Тогда значения порядков состояний системы $\mathscr{M}$ — это все целые числа вида

$$\text{НОК}\left(t_{h_1}^{(1)}, t_{h_2}^{(2)}, \ldots, t_{h_r}^{(r)}\right),$$

где $0 \leqslant h_j \leqslant b_j$, $1 \leqslant j \leqslant r$.

Комментарии

§ 1. Теорема Шеннона, о которой говорится во введении к настоящей главе, была получена в работе Shannon [1] (см. также Shannon, Weaver [1]). Эта работа знаменует начало теории информации как математической дисциплины. Доказательства этой теоремы Шеннона, а также обоснования теории информации

можно найти в книгах Abramson [2], Ash [1], Guiaşu [1] (в последней приводится подробная библиография по теории информации), а также в монографиях McEliece [6] и Wolfowitz [1]. Теория кодирования с точки зрения информации изучается в работах Balakrishnan [1], Gallager [1], Ingels [1], Lucky, Salz, Weldon [1], McEliece [6], Slepian [4].

Первый нетривиальный пример кода, исправляющего ошибки, над конечным полем появляется в фундаментальной работе Шеннона (Shannon [1]). Этот код называется теперь (7, 4)-кодом Хэмминга, и его построение приписывается Хэммингу (см. Hamming [1]). Ранее в работе Friedman, Mendelsohn [1] изучались коды длины 5 с минимальным расстоянием не меньше чем 2 над алфавитом из 26 букв. Важный вклад в основание общей теории линейных кодов был сделан в работах Golay [1], Hamming [1], Muller [1], Reed [1], Slepian [1], [2], [3]. По поводу краткой истории алгебраической теории кодирования мы отсылаем читателя к превосходному сборнику статей под редакцией Блейка Blake [1].

Детальное изучение алгебраической теории кодирования можно найти в книгах Berlekamp [4], Blake, Mullin [1], Duske, Jürgensen [1], Lin [2], MacWilliams, Sloane [2] (последняя книга снабжена обширной библиографией), а также в книгах McEliece [6], Peterson, Weldon [1], van Lint [1], von Ammon, Tröndle [1] и Удалов, Супруи [1]. Некоторые книги по прикладной алгебре также содержат материал по алгебраической теории кодирования, см., например, книги Birkhoff, Bartee [1], Dornhoff, Hohn [1], Lidl, Pilz [1], Lidl, Wiesenbauer [1]. Обзорами по теории кодирования являются работы Berlekamp [8], Kautz, Levitt [1], Sloane [1] и Добрушин [1]. Книги, вышедшие под редакцией Берлекэмпа (Berlekamp [9]) и Манна (Mann [5]), представляют собой интересные сборники работ по теории кодирования.

Коды Хемминга были введены в работах Golay [1] и Hamming [1]. По поводу различных границ для кодов см. работы Hamming [1] (граница Хэмминга), Plotkin [1] (граница Плоткина), Singleton [1] (граница Синглетона) (см. упр. 9.5), Gilbert [1], Варшамов [1] (граница Гилберта—Варшамова). Теорема 9.32 была получена в работе MacWilliams [1]. Приведенное нами доказательство этой теоремы заимствовано у ван Лиита (van Lint [1]). Другие доказательства этой теоремы можно найти в книгах Berlekamp [4, ch. 16], McEliece [6, ch. 7], а также Chang, Wolf [1]. Аналог этого результата для нелинейных кодов приводится в работе MacWilliams, Sloane, Goethals [1]. Равенство из упр. 9.19 получено в работе Pless [1].

Широко изучались *совершенные коды* (см. упр. 9.8 и 9.9). Помимо двух совершенных линейных кодов, приводимых в этих

пражнениях, существуют два совершенных линейных кода, полученных Голеем в работе Golay [1], а именно (23, 12)-код над полем $\mathbb{F}_2$ и (11, 6)-код над полем $\mathbb{F}_3$. В работе Tietäväinen [14] показано, что произвольный (линейный или нелинейный) совершенный код $C \subseteq \mathbb{F}_q^n$ или содержит только одно кодовое слово, или совпадает с $\mathbb{F}_q^n$, или является бинарным кодом с повторением нечетной длины, или имеет те же параметры (т. е. длину, число кодовых слов и минимальное расстояние), что и один из кодов Хэмминга или Голея (см. также Зиновьев, Леонтьев [1] и Tietäväinen [15]). Известно, что любой код, параметры которого совпадают с параметрами одного из кодов Голея, сам эквивалентен соответствующему коду Голея (см. Delsart, Goethals [3], MacWilliams, Sloane [2, ch. 20]). В работах Lindström [1], Schönheim [2] и Васильев Ю. Л. [1] построены нелинейные совершенные коды с теми же параметрами, что и у кодов Хэмминга. Прекрасные обзоры результатов, касающихся совершенных кодов, содержатся в книгах MacWilliams, Sloane [2, ch. 6] и в статьях van Lint [3], [4].

Взаимосвязь между теорией кодирования и комбинаторикой способствует развитию обеих дисциплин. Имеются многочисленные примеры того, как техника, разработанная для одной из этих областей, позволяет получать результаты, применимые в другой области. Так, например, результат, эквивалентный границе Хэмминга для кодов, был получен Рао (Rao C. R. [1]) еще задолго до зарождения кодирования в связи с исследованием комбинаторных схем. Много интересных результатов, связывающих теорию кодирования и комбинаторику, можно найти в работах Assmus, Mattson [1], [2], Blake [2], Cameron, van Lint [1], [2], MacWilliams, Sloane [2]. Конечные геометрии использовались в работах Rudolph [1], Lin [1], Delsarte P. [1], Sachar [1] и ряде других для построения и анализа различных кодов. Геометрия кодов подробным образом разбирается в монографии Берлекэмпа (Berlekamp [4, ch. 15]) и в книге Peterson, Weldon [1, ch. 10].

§ 2. Циклические коды были введены в работе Prange [1]. Другими ранними работами по циклическим кодам являются статьи Abramson [1], Green, San Soucie [1], Peterson, Brown [1], Prange [2], Yale [1]. В работе Elspas, Short [1] изучалась связь между циклическими кодами и каноническим разложением порождающего многочлена, а в работе Zetterberg [1] рассматривались неприводимые циклические коды.

Связь между многочленами по модулю $x^n - 1$ и циклическими кодами длины n исследовалась Мак-Вильямс (MacWilliams [2]), Питерсоном и Брауном (Peterson, Brown [1]). Многочлены по модулю $x^n - 1$ также связаны с алгеброй циркулянтных матриц

размера $n \times n$ (см. Karlin [1]). Связь между линейными рекуррентными последовательностями, регистрами сдвига и циклическими кодами исследовалась в работах Abramson [1], Berlekamp [4, ch. 5], Green, San Soucie [1], Peterson, Weldon [1, ch. 8], Prange [2], Yale [1], Zetterberg [1], Zierler [5].

Коды Боуза—Чоудхури—Хоквингема (БЧХ-коды) были введены в работах Hocquenghem [1], Bose, Ray-Chaudhuri [1] для бинарного случая и в работе Gorenstein, Zierler [1] для случая произвольного конечного поля. Питерсон показал (см. Peterson [1]), что БЧХ-коды являются циклическими кодами. Другими основополагающими работами по БЧХ-кодам являются статьи Bose, Ray-Chaudhuri [2] и Mattson, Solomon [1]. Обобщения теоремы 9.45 можно найти в работе Hartmann, Tzeng [1]. Результаты о минимальном расстоянии и распределении весов в БЧХ-кодах можно найти в работах Berlekamp [5], Goldman, Kliman, Smola [1], MacWilliams, Sloane [2, ch. 9], Peterson [2] и Peterson, Weldon [1, ch. 9].

Первый алгоритм для декодирования БЧХ-кодов был описан Питерсоном в работе Peterson [1]. Другие декодирующие алгоритмы были предложены в работах Berlekamp [1], Forney [1], Gorenstein, Zierler [1], Massey [2] до того, как Берлекэмп (Berlekamp [4]) и Месси (Massey [4]) получили свой эффективный алгоритм (см. также § 6 гл. 8 настоящей монографии). Для случая малого числа ошибок этот результат был улучшен в работе Chen C. L. [2]. Связь между непрерывными дробями, алгоритмом Евклида и алгоритмом Берлекэмпа—Месси изучалась в работах Mills [4], Reed, Scholtz, Truong, Welch [1], Reed, Truong [4], Reed, Truong, Miller [3], Welch, Scholtz [1]. Алгоритм Евклида и алгоритм Берлекэмпа—Месси могут быть также использованы при декодировании кодов других типов (см. Goppa [1], Helgert [1], Mandelbaum [2], [3], Patterson N. J. [1], Retter [1], Sarwate [1], Sugiyama, Kasahara, Hirasawa, Namekawa [1], [2]). В работе Michelson [1] рассматривались вопросы декодирования БЧХ-кодов с помощью ЭВМ. Процедура Ченя (шаг 3 в 9.50) была описана в работе Chien [1].

Коды Рида—Соломона начали изучаться в работе Reed, Solomon [1]. Дальнейшие результаты о кодах Рида—Соломона и их декодировании можно найти в работах Liu, Reed, Truong [2], MacWilliams, Sloane [2, ch. 10], Mandelbaum [1], Reed, Scholtz, Truong, Welch [1], Reed, Truong, Miller [3], Reed, Truong, Welch [1]. В работе Blahut [1] приводится обзор применений дискретных преобразований Фурье при декодировании кодов Рида—Соломона и ряда других кодов. Информацию о *реверсивных кодах* (см. упр. 9.33) можно найти в книге MacWilliams, Sloane [2, ch. 7] и в работе Massey [1]. Класс полиноминальных кодов, включающий в себя БЧХ-коды и конечно-геометрические коды,

был введен в работе Kasami, Lin, Peterson [1] (см. также Delsarte P. [2], Gore, Cooper [1], Peterson, Weldon [1, ch. 10]).

Информацию о распределении весов в циклических кодах можно найти в работах Baumert, McEliece [1], Berlekamp [4, ch. 16], Chen C. L. [1], Delsarte, Goethals [1], Hartmann, Riek, Longobardi [1], Hartmann, Tzeng, Chien [1], Helleseth, Kløve, Mykkeltveit [1], MacWilliams, Seery [1], MacWilliams, Sloane [2, ch. 8], Peterson, Weldon [1, appendix D]. Подход к задаче распределения весов, основанный на использовании гауссовых сумм (см. Baumert, McEliece [1], McEliece [5], McEliece, Rumsey [1]) приводит к получению общего неравенства для весов кодовых слов в циклических кодах (Niederreiter [8]).

§ 3. Наиболее исчерпывающий обзор по проективным геометриям над конечными полями приводится в работе Hirschfeld [5]. Конечные проективные плоскости рассматриваются также во многих книгах по проективной геометрии, таких, как например, Baer [1], Blumenthal [1], Horadam [1], Hughes, Piper [1], Pickert [1], Segre [6], Veblen, Young [1]. По вопросам конечных геометрий особенно рекомендуем Albert, Sandler [1], Berman, Fryer [1], Carmichael [4, ch. 11], Dembowski [2], Hall [6], [8], Kárteszi [1], Segre [2], Vajda [1], van Lint [2].

Плоскость Фано из примера 9.55 впервые появляется в работе Fano [1]. Отсутствие проективных плоскостей 6-го порядка вытекает из работы Tarry [1]. В работе Bruck, Ryser [1] доказан более общий результат, а именно если $m \equiv 1, 2 \pmod 4$, то конечная проективная плоскость порядка m может существовать только в том случае, если m можно представить в виде суммы квадратов двух целых чисел (см. также книгу Hall [8, ch. 12]). Теорема 9.60 была получена в работе Veblen, Bussey [1]. Свойства коник и овалов более детально изучаются в книге Hirschfeld [5, ch. 7, 8]; тем же можно найти доказательство теоремы 9.65 (i). Теорема 9.67 и следствия из нее были получены в работах Segre [1], [8] (см. также Hirschfeld [3]). Связь с перестановочными многочленами исследуется в работе Hirschfeld [2].

Для введения координат в конечной дезарговой плоскости был использован один метод из работы Гильберта Hilbert [3]. Тех, кто интересуется задачей введения системы координат в проективной плоскости, отсылаем к работам Albert, Sandler [1], Hall [6], [8], где вводится понятие *тернарного кольца*. Специальный класс тернарных колец представляют *системы Веблена—Веддербёрна*. Если умножение в системе Веблена—Веддербёрна ассоциативно, то такая система называется *почти-полем* (nearfield). Каждое конечное поле является почти-полем; все конечные почти-поля описаны в работе Zassenhaus [1]. Более подробную информацию о почти-полях можно найти в работе Pilz [1]. Система Веблена—Веддербёрна, в которой выполняются оба за-

кона дистрибутивности, называется *полуполем* или *неассоциативным кольцом с делением* (см. Albert [2]). Построение конечных недезарговых плоскостей проводилось в работах Albert, Sandler [1], Hall [8], Hughes [1], Knuth [1], Neumann H [1], Veblen, Wedderburn [1].

Конечные поля использовались в статье Crowe [1] для построения конечных гиперболических плоскостей. Приложения конечных геометрий к теории кодирования можно найти в работах Assmus, Mattson [2], Berlekamp [4, ch. 15], Cameron, van Lint [1], [2], Delsarte P. [1], Lin [1], Peterson, Weldon [1, ch. 10], Rudolph [1], Sachar [1].

§ 4. Большинство понятий, описанных в этом разделе, можно найти в книгах по комбинаторике, см., например, Hall [8], Ryser [1], Street, Wallis [1].

Определение уравновешенной неполной блок-схемы может быть обобщено следующим образом. Схема инцидентности называется *t-схемой* с параметрами (v, k, λ), если $v \geqslant k \geqslant t \geqslant 1$ и каждое множество из t различных элементов инцидентно одному и тому же числу блоков, равному λ. Тогда (v, k, λ)-блок-схема совпадает с 2-схемой с параметрами (v, k, λ). Наиболее значительной задачей в этой области является вопрос существования нетривиальных t-схем с $t > 5$ (тривиальной t-схемой является такая схема, в которой каждое множество из k различных элементов является блоком).

Важное необходимое условие для существования симметричных уравновешенных неполных блок-схем было получено Бруком, Райзером и Човлой, а именно: если симметричная (v, k, λ)-блок-схема существует, то

(i) если v четно, то $k - \lambda$ является квадратом;

(ii) если v нечетно, то уравнение $z^2 = (k - \lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$ имеет решение (x, y, z) в целых числах, не все из которых равны 0.

Этот результат был доказан в работе Bruck, Ryser [1] для случая $\lambda = 1$ и в работе Chowla, Ryser [1] в общем случае (см. также Hall [8, ch. 10], Ryser [1, ch. 8], [3], Shrikhande [1]). Другие результаты по схемам можно найти в работах Bose R. C. [2], Bridges, Ryser [1], Cameron [1], Cameron, van Lint [1], [2], Dembowski [1], [2], Hanani [1], Hughes [2], Lüneburg [1], Ryser [2], van Lint, Ryser [1], Wilson [1], [2]. Связь между схемами и теорией кодирования обсуждается в работах Assmus, Mattson [1], [2], Blake [2], Cameron, van Lint [1], [2], MacWilliams, Sloane [2].

Разностные множества из теоремы 9.79 были открыты в работе Singer [1]. Поэтому они часто называются *разностными множествами Зингера*. Прекрасные обзоры по разностным множествам содержатся в работах Baumert [1], Hall [5], [8], Mann

[3], [4], Storer [1]. Дальнейшие результаты можно найти в работах Bruck [1], Evans, Mann [1], Gordon, Mills, Welch [1], Hall [7], Lehmer E. [3], MacWilliams, Mann [1], McEliece [1], Menon [2], Turyn [1], Whiteman [12]. Приложение некоторых разностиых множеств Зингера к теории кодирования можно найти в статье Graham, MacWilliams [1]. Существуют интересные связи между разностными множествами, с одной стороны, и суммами Гаусса, суммами Якоби и циклотомией, с другой стороны. Эти связи отражены в работах Baumert [1, ch. 5], Baumert, Fredricksen [1], Baumert, Mills, Ward [1], Berndt, Chowla [1], Berndt, Evans [1], Chowla S. [4], Evans [4], [10], Hall [5], [7], Lehmer E. [3], Mann [3], Menon [2], Muskat, Whiteman [1], Storer [1], Whiteman [10], [11], Yamamoto [3].

По поводу латинских квадратов обычно ссылаются на книгу Dénes, Keedwell [1]; см. также Childs [1], Hall [8], Mann [2], Ryser [1], Street, Wallis [1], Vajda [2]. Теорема 9.83 получена в работе MacNeish [1] (см. также Mann [1], [2], Ryser [1]). Ортогональные латинские квадраты впервые изучались Эйлером (Euler [1]), который выдвинул гипотезу о том, что для $n \equiv 2 \pmod 4$ не существует пары ортогональных латинских квадратов порядка n. В работе Tarry [1] этот результат был подтвержден для случая $n = 6$, однако Боуз и Шрикханд (Bose, Shrikhande [2]) опровергли гипотезу Эйлера, построив пару ортогональных латинских квадратов порядка 22. Вскоре после этого Паркер (Parker [1]) нашел пару ортогональных латинских квадратов порядка 10. И наконец, в работе Bose, Shrikhande, Parker [1] показано, что для любого $n > 6$ существует пара ортогональных латинских квадратов порядка n. С этой тематикой связаны также работы Bose, Shrikhande [3] и Parker [2]. В статьях Bose R. C. [1], Stevens W. L. [1] показано, что конечная проективная плоскость порядка n существует тогда и только тогда, когда существует множество из $n - 1$ попарно ортогональных латинских квадратов порядка n. Необходимо отметить, что множество, состоящее из взаимно ортогональных латинских квадратов порядка n, не может содержать более $n - 1$ квадратов.

Вопросы применения схем инцидентности и ортогональных латинских квадратов при планировании статистических экспериментов обсуждаются в работах Mann [2], Raghavarao [1], Vajda [2]. Оригинальный подход к вопросам планирования экспериментов можно найти в книге Fisher [1].

Матрицы Адамара исследуются во многих книгах по комбинаторике (см., например, Hall [8], van Lint [2]). При этом используются разные методы их построения (см. Baumert, Hall [1], Ehlich [1], Paley [3], Wallis, Street, Wallis [1]). Вопросы использования матриц Адамара в теории кодирования изучались в работах Bose, Shrikhande [1], Golomb, Baumert [1], MacWilliams,

Sloane [1, ch 2]. В последней книге также содержится обзор их применения в других областях математики. Матрицы сходных типов изучались в работах Belevitch [1], Butson [1], Delsarte, Goethals, Seidel [1], Goethals, Seidel [1], MacWilliams [4], Wallis, Street, Wallis [1].

§ 5. Прекрасными источниками сведений по системам с конечным числом состояний (или просто конечным автоматам) и линейиым модулярным системам являются книги Arbib, Falb, Kalman [1], Booth [1], Dornhoff, Hohn [1, ch. 1, 8], Gill [1], [2], Harrison [1], Zadeh, Desoer [1], Zadeh, Polak [1, ch. 2]. В последней книге содержится много ссылок на работы по линейным модулярным системам. Некоторые классические работы по данной тематике собраны в сборнике под редакцией Каутца (Kautz [1]) (см. также Crowell [1], Elspas [1], Friedland [1], Huffman [1]). Условия, при которых конечный автомат можно реализовать в виде линейной модулярной системы, изучались в работах Eichner [1] и Hartfiel, Maxson [1], а также в ряде других работ. В статье Matluk, Gill [1] показано, как линейную модулярную систему над кольцом $\mathbb{Z}/(m)$ можно разложить на линейные модулярные системы над конечными полями. Линейные модулярные системы над кольцами $\mathbb{Z}/(m)$ изучались также в работе Bollman [2]. Калман (Kalman [1], [2]) изучал линейные модулярные системы с точки зрения динамических систем. За детальным обсуждением свойств рациональных канонических форм матриц отсылаем к работам Dornhoff, Hohn [1, ch. 7] и Herstein [4, ch. 6].

Кратко упомянем некоторые другие приложения конечных полей. На арифметике конечных полей может быть основан теоретический анализ переключательных цепей (см. Green, Taylor [1], [3], Moisil [1]—[4], Moisil, Popovici [1], Murakami, Reed [1], Rudeanu [1], Vaida [1]). Конечные поля используются при вычислении переключательных фуикций (см. Benjauthrit, Reed) [1], [2], Davio, Deschamps, Thayse [1], Labunec, Sitnikov [1], Pradhan [1], Takahashi [1], Thayse [1], Yin [1]) и общих логических функций (см. Karpovsky [1]). Мендельсон (Mendelsohn [2]) использовал конечные поля для моделирования квазигрупповых тождеств. Свойства конечных полей находят разнообразные применения в криптографии (см. Beker, Piper [1], [2], Brawley, Levine [1], Cooper [1], Diffie, Hellman [1], Hartwig, Levine [1], Herlestam, Johannesson [1], Hershey [1], Konheim [1], Krishnamurthy, Ramachandran [1], Levine, Brawley [1], [2], Levine, Hartwig [1], Pohlig, Hellman [1], Sloane [2]). В статье Redinbo [1] изучались приложения конечных полей к исследованию матричных процессоров, в работе Nicholson [1] они применялись при вычислении конечных преобразований Фурье, а в работе English [1] свойства конечных полей применялись к анализу алгоритмов.

[В работах Tsfasman, Vladuts, Zink [1*], Цфасман [1*] и Влэдуц, Кацман, Цфасман [1*], основанных на идее работы Гоппы [2] и оценках рациональных точек на кривых большого рода над конечным полем (см. Манин [5], Ihara [1]), были получены новые результаты, относящиеся к теории кодирования. В работах Шпарлинского [2*], [5*] предложен один комбинаторный метод, который применяется к некоторым задачам теории кодирования.

По тематике девятой главы имеются также работы: de Vroedt [1*], Helleseth [1*], Lidl, Niederreiter [1*], Oberst, Dur [1*], Tappe [1*], Варшамов, Тененгольц [1*], Вишневский [1*], [2*], Гоппа [1*], [2*], Думер, Зиновьев [1*] и Сидельников [1*], [2*]. — *Перев.*]

Упражнения

9.1. Найти все кодовые слова, определить минимальное расстояние и найти проверочную матрицу бинарного линейного (5,3)-кода, задаваемого порождающей матрицей

$$G = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

9.2. Доказать, что линейный код может обнаруживать s или меньшее число ошибок тогда и только тогда, когда его минимальное расстояние $d \geqslant s + 1$.

9.3. Доказать, что расстояние Хэмминга является метрикой в пространстве $\mathbb{F}_q^n$.

9.4. Пусть H — проверочная матрица некоторого линейного кода. Доказать, что код имеет минимальное расстояние d тогда и только тогда, когда любые $d - 1$ столбцов матрицы H линейно независимы и при этом имеется d линейно зависимых столбцов.

9.5. Доказать, что если линейный (n, k)-код имеет минимальное расстояние d, то $n - k + 1 \geqslant d$ (граница Синглетона).

9.6. Пусть G_1 — порождающая матрица линейного (n_1, k)-кода с минимальным расстоянием d_1, а G_2 — порождающая матрица линейного (n_2, k)-кода с минимальным расстоянием d_2. Показать, что линейные коды с порождающими матрицами

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix} \quad \text{и} \quad (G_1 \quad G_2)$$

являются $(n_1 + n_2, 2k)$-кодом и $(n_1 + n_2, k)$-кодом с минимальными расстояниями $\min(d_1, d_2)$ и $d \geqslant d_1 + d_2$ соответственно.

9.7. Пусть даны натуральные числа k и d. Доказать, что если бинарный линейный (n, k)-код имеет минимальное расстояние $d = d_0$, то

$$n \geqslant d_0 + d_1 + \ldots + d_{k-1},$$

где $d_{i+1} = \lfloor (d_i + 1)/2 \rfloor$, $i = 0, 1, \ldots, k - 2$. Здесь $\lfloor x \rfloor$ обозначает наибольшее целое число, не превосходящее x.

9.8. Код $C \subseteq \mathbb{F}_q^n$ называется *совершенным*, если для некоторого целого числа t шары $B_t(\mathbf{c})$ радиуса t с центром в кодовых словах $\mathbf{c}$ попарно не пересекаются и «заполняют» все пространство $\mathbb{F}_q^n$, т. е.

$$\bigcup_{\mathbf{c} \in C} B_t(\mathbf{C}) = \mathbb{F}_q^n.$$

Доказать, что в бинарном случае коды Хэмминга и коды с повторением нечетной длины являются совершенными кодами.

9.9. Пользуясь определением из упр. 9.8, показать, что все коды Хэмминга над полем $\mathbb{F}_q$ являются совершенными.

9.10. Два линейных (n, k)-кода C_1 и C_2 над полем $\mathbb{F}_q$ называются *эквивалентными*, если кодовые слова кода C_1 можно получить из кодовых слов кода C_2 с помощью некоторой фиксированной перестановки координат в словах из кода C_2. Пусть G — порождающая матрица линейного кода C. Показать, что любая перестановка строк матрицы G или любая перестановка столбцов этой матрицы приводит к порождающей матрице некоторого линейного кода, эквивалентного коду C.

9.11. Используя определение эквивалентности кодов из упр. 9.10, показать, что бинарные линейные коды с порождающими матрицами

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{и} \quad G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

являются эквивалентными.

9.12. Пусть C — линейный (n, k)-код. Доказать, что размерность $C^{\perp}$ равна $n - k$.

9.13. Доказать, что для любого линейного кода C выполняется соотношение $(C^{\perp})^{\perp} = C$.

9.14. Доказать, что для любых линейных кодов C_1 и C_2 над полем $\mathbb{F}_q$, имеющих одинаковую длину, справедливо соотношение $(C_1 + C_2)^{\perp} = C_1^{\perp} \cap C_2^{\perp}$.

9.15. Пусть C — бинарный $(n, 1)$-код с повторением. Доказать, что код $C^{\perp}$ является $(n, n-1)$-кодом с проверкой на четность.

9.16. Найти порождающую матрицу и все кодовые слова (7,3)-кода, дуального к бинарному коду Хэмминга C_3.

9.17. Определить дуальный код $C^{\perp}$ для кода, определенного в упр. 9.1. Получить таблицу смежных классов пространства $\mathbb{F}_5^2$ по модулю $C^{\perp}$, найти лидеров смежных классов и соответствующие синдромы. Если полученное слово имеет вид $\mathbf{y} = 01001$, то какой вид должно, по всей вероятности, было иметь переданное сообщение?

9.18. Применяя теорему 9.32 к бинарному линейному коду $C = \{000, 011, 101, 110\}$, найти его дуальный код и перечислители весов, а также проверить тождество Мак-Вильямс.

9.19. Пусть C — бинарный линейный (n, k)-код с перечислителем весов

$$A(x, y) = \sum_{i=0}^{n} A_i x^i y^{n-i},$$

и пусть

$$A^{\perp}(x, y) = \sum_{i=0}^{n} A_i^{\perp} x^i y^{n-i}$$

— перечислитель дуального кода $C^{\perp}$. Показать, что для $r = 0, 1, \ldots$ справедливо следующее равенство:

$$\sum_{i=0}^{n} i^r A_i = \sum_{i=0}^{n} (-1)^i A_i^{\perp} \sum_{t=0}^{r} t!\, S(r, t)\, 2^{k-t} \binom{n-i}{n-t},$$

где

$$S(r, t) = \frac{1}{t!} \sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} j^r$$

— числа Стирлинга второго рода, а биномиальный коэффициент $\binom{m}{h}$ полагается равным 0 для $h > m$ и $h < 0$. Выписать в явном виде полученные тождества для $r = 0, 1, 2$.

9.20. Пусть $n = (q^m - 1)/(q - 1)$, а β — примитивный корень n-й степени из единицы в поле $\mathbb{F}_{q^m}$, $m \geqslant 2$. Доказать, что нуль-пространство матрицы

$$H = (1 \ \beta \ \beta^2 \ \ldots \ \beta^{n-1})$$

является кодом над полем $\mathbb{F}_q$ с минимальным расстоянием $d \geqslant 3$ тогда и только тогда, когда НОД $(m, q - 1) = 1$.

9.21. Пусть α — примитивный элемент поля $\mathbb{F}_9$ с минимальным многочленом $x^2 - x - 1$ над полем $\mathbb{F}_3$. Найти порождающий многочлен БЧХ-кода над полем $\mathbb{F}_3$ длины 8 и размерности 4. Определить минимальное расстояние этого кода.

9.22. Найти порождающий многочлен БЧХ-кода над полем $\mathbb{F}_2$ размерности 12 с конструктивным расстоянием 5.

9.23. Определить размерность БЧХ-кода над полем $\mathbb{F}_3$, исправляющего 5 ошибок и имеющего длину 80.

9.24. Используя примитивный элемент $\alpha \in \mathbb{F}_{16}$ с минимальным многочленом $\alpha^4 = \alpha^3 + 1$, найти порождающий многочлен бинарного БЧХ-кода длины 15, исправляющего 3 ошибки.

9.25. Найти порождающий многочлен $g(x)$ для бинарного $(31, 31 - \deg g(x))$-БЧХ-кода с конструктивным расстоянием $d = 9$.

9.26. Пусть m и t — натуральные числа. Показать, что существует бинарный БЧХ-код длины $2^m - 1$, который исправляет все комбинации по t или менее ошибок, используя при этом не более чем mt контрольных символов.

9.27. Описать (15, 13)-код Рида — Соломона над полем $\mathbb{F}_{16}$, определив его порождающий многочлен и число ошибок, которое этот код может исправлять.

9.28. Доказать, что минимальное расстояние кода Рида — Соломона с порождающим многочленом

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i)$$

равно d.

9.29. Определить, является ли БЧХ-кодом код, дуальный произвольному БЧХ-коду. Аналогично является ли кодом Рида — Соломона код, дуальный произвольному коду Рида — Соломона?

9.30. В примере 9.43 найти локаторы ошибок, зная, что синдром полученного вектора равен $(10010110)^{\mathrm{T}}$. Найти порождающую матрицу этого кода.

9.31. Пусть бинарный БЧХ-код, исправляющий 2 ошибки, имеет длину 31 и задается корнем α многочлена $x^5 + x^2 + 1$ над полем $\mathbb{F}_{32}$. Пусть синдром полученного слова имеет вид $(1110011101)^{\mathrm{T}}$. Найти многочлен ошибок.

9.32. Пусть α — примитивный элемент поля $\mathbb{F}_{16}$, $\alpha^4 = \alpha + 1$, и пусть $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ — порождающий многочлен бинарного (15,5)-БЧХ-кода. Пусть получено слово $\mathbf{v} = 000101100100011$. Определить переданное кодовое слово и сообщение, которое было закодировано.

9.33. Код C называется *реверсивным*, если из того, что $(a_0, a_1, \ldots, a_{n-1}) \in C$, следует, что и $(a_{n-1}, \ldots, a_1, a_0) \in C$.

(a) Доказать, что циклический код $C = (g(x))$ является реверсивным тогда и только тогда, когда обратная величина к любому корню многочлена $g(x)$ также является корнем многочлена $g(x)$.

(b) Доказать, что произвольный циклический код над полем $\mathbb{F}_q$ является реверсивным, если -1 совпадает с некоторой степенью числа q по модулю n.

9.34. Пусть дан циклический (n, k)-код, и пусть линейный $(n - m, k - m)$-код получен из него в результате вычеркивания m последних строк и m последних столбцов в порождающей матрице этого кода, приведенной перед теоремой 9.36. Показать, что получающийся при этом код, вообще говоря, не является циклическим, но имеет минимальное расстояние, не меньшее, чем минимальное расстояние исходного кода. (*Замечание.* Такой $(n - m, k - m)$-код называется *укороченным циклическим кодом*.)

9.35. Перечислить все точки и прямые в $PG(2, \mathbb{F}_3)$. Нарисовать диаграмму всех пересечений. Перечислить все точки прямой L_∞ и указать семейства параллельных прямых в $AG(2, \mathbb{F}_3)$.

9.36. В $PG(2, \mathbb{F}_4)$ рассмотрим четырехвершинник $A = (1, 1, 1 + \beta)$, $B = (0, 1, \beta)$, $C = (1, 1, \beta)$, $D = (1, 1 + \beta, \beta)$, где β — примитивный элемент поля $\mathbb{F}_4$. Найти диагональные точки этого четырехвершинника и проверить, что они коллинеарны.

9.37. Доказать, что в $PG(2, \mathbb{F}_4)$ найдутся шесть точек, никакие три из которых не лежат на одной прямой. Четыре из них совпадают с точками A, B, C и D из упр. 9.36. Найти оставшиеся две точки.

9.38. Найти уравнение коники, которая образована точками A, B, C, D из упр. 9.36 и точкой $E = (1, 1 + \beta, 1 + \beta)$. Определить касательные к этой конике и найти точку их пересечения.

9.39. Показать, что не все касательные к невырожденной конике в проективном пространстве $PG(2, \mathbb{F}_5)$ пересекаются в одной точке.

9.40. Доказать, что если L — множество таких точек пространства $PG(2, \mathbb{F}_q)$, что каждая прямая из $PG(2, \mathbb{F}_q)$ содержит точку множества L, то $|L| \geqslant q + 1$, причем равенство достигается тогда и только тогда, когда L является прямой нашего пространства.

9.41. Доказать, что среди любых $m + 3$ точек конечной проективной плоскости порядка m найдутся три коллинеарные точки. (*Замечание.* Тем самым будет показано, что овал в пространстве $PG(2, \mathbb{F}_q)$ при нечетном q содержит максимальное число точек, обладающих тем свойством, что никакие три из них не лежат на одной прямой.)

9.42. Показать, что если в проективном пространстве $PG(2, \mathbb{F}_q)$, где q четно, у двух овалов более половины точек общие, то эти овалы совпадают.

9.43. Пусть q четно. Невырожденная коника в $PG(2, \mathbb{F}_q)$ вместе с точкой пересечения всех касательных к этой конике называется *регулярным овалом*. Показать, что если $q = 2$ или $q = 4$, то любой овал в $PG(2, \mathbb{F}_q)$ является регулярным.

9.44. Пусть $q = 2^h$ и $1 \leqslant n < h$. Доказать, что множество $A(x^{2^n})$ (см. теорему 9.67) является овалом в $PG(2, \mathbb{F}_q)$ тогда и только тогда, когда НОД $(n, h) = 1$.

9.45. Пусть $q = 2^h$, $h > 1$, рассмотрим $PG(2, \mathbb{F}_q)$. Показать, что

(a) если $\deg(f) = 2$, то $A(f)$ является овалом тогда и только тогда, когда $A(f) = A(x^2)$;

(b) если $\deg(f) = 4$, то $A(f)$ является овалом тогда и только тогда, когда h нечетно и $A(f) = A(x^4)$.

9.46. Пусть $A(f)$ такое же, как и в теореме 9.67. Тогда $A(f)$ называется *трансляционным овалом*, если оно является овалом, а многочлен f индуцирует эндоморфизм аддитивной группы поля $\mathbb{F}_q$. Доказать, что $A(f)$ является трансляционным овалом тогда и только тогда, когда выполняются следующие условия:

(a) $f(a + b) = f(a) + f(b)$ для всех $a, b \in \mathbb{F}_q$;

(b) f является перестановочным многочленом поля $\mathbb{F}_q$, $\deg(f) < q$ и $f(1) = 1$;

(c) $f(x)\,x$ является перестановочным многочлеиом поля $\mathbb{F}_q$ со свободным членом, равным 0. Доказать также, что если $\deg(f) < q$, то f удовлетворяет условию (a) тогда и только тогда, когда он является p-многочленом, где p — характеристика поля $\mathbb{F}_q$.

9.47. Пусть $q = 2^h$ и $1 \leqslant n < h$. Доказать, что $A(x^{2^n})$ является трансляционным овалом в $PG(2, \mathbb{F}_q)$, если НОД $(n, h) = 1$.

9.48. Определить число точек, прямых, плоскостей и гиперплоскостей в пространстве $PG(4, \mathbb{F}_3)$. Сколько плоскостей проходит через данную прямую?

9.49. В $PG(4, \mathbb{F}_3)$ найти все 3-пространства, проходящие через плоскость, определяемую точками (1, 0, 0, 0, 0), (0, 0, 1, 0, 0) и (0, 0, 0, 0, 1).

9.50. Показать, что число k-плоскостей проективного пространства $PG(m, \mathbb{F}_q)$, $1 \leqslant k < m$, или, что то же самое, содержащихся в m-плоскостях некоторой проективной геометрии более высокой размерности над полем $\mathbb{F}_q$, равно

$$\frac{(q^{m+1}-1)(q^m-1)\ldots(q^{m-k+1}-1)}{(q^{k+1}-1)(q^k-1)\ldots(q-1)}.$$

9.51. Показать, что система блоков

$$\{1, 2, 3\},\ \{1, 4, 7\},\ \{1, 5, 9\},\ \{1, 6, 8\},\ \{4, 5, 6\},\ \{2, 5, 8\},$$
$$\{2, 6, 7\},\ \{2, 4, 9\},\ \{7, 8, 9\},\ \{3, 6, 9\},\ \{3, 4, 8\},\ \{3, 5, 7\},$$

образует блок-схему и определить параметры v, b, r, k и λ этой блок-схемы.

9.52. Решить следующий частный случай задачи Киркмана о школьницах. Учительница каждый день выводит на прогулку 9 девочек, построив их в три ряда по три человека в каждом. Найти способ организовать прогулки таким образом, чтобы в течение четырех дней подряд ни одна из девочек не встречалась в одной тройке ни с одной своей одноклассницей более чем 1 раз.

9.53. Пусть в школе, где учится b мальчиков, имеется t спортивных команд по k человек в каждой команде. Пусть комаиды организованы таким образом, что каждый мальчик входит в одинаковое число команд и каждая пара мальчиков тоже входит в одинаковое число команд. В какое число команд может при этом входить один мальчик и сколько раз два мальчика могут входить в одну команду?

9.54. Доказать, что если v четно, то для симметричной (v, k, λ)-блок-схемы величина $k - \lambda$ является квадратом.

9.55. Проверить, что $\{0, 1, 2, 3, 5, 7, 12, 13, 16\}$ является разностным множеством по модулю 19. Определить соответствующие параметры v, k и λ.

9.56. Показать, что $\{0, 4, 5, 7\}$ является разностным множеством по модулю 13, а связанная с этим разностным множеством проективная геометрия совпадает с $PG(2, \mathbb{F}_3)$.

9.57. Доказать следующее обобщение теоремы 9.76. Пусть

$$\{d_{i1}, \ldots, d_{ik}\}, \quad i = 1, \ldots, s,$$

— система (v, k, λ)-разностных множеств.Тогда если все вычеты по модулю v принять за элементы блок-схемы, то vs блоков вида

$$\{d_{i1} + t, \ldots, d_{ik} + t\}, \quad t = 0, 1, \ldots, v-1, \quad i = 1, \ldots, s,$$

образуют $(v, k, \lambda s)$-блок-схему.

9.58. Пусть $L^{(k)} = \left(a_{ij}^{(k)}\right)$, где $a_{ij}^{(k)} \equiv i + jk \pmod 9$, $0 \leqslant a_{ij}^{(k)} < 9$, $1 \leqslant i, j \leqslant 9$. Какие из матриц $L^{(k)}$, $k = 1, 2, \ldots, 8$, являются латинскими квадратами? Являются ли $L^{(2)}$ и $L^{(5)}$ ортогональными?

9.59. Латинский квадрат порядка n называется *нормализованным*, если его первый столбец и его первая строка представляют собой упорядоченное мно-

жество $\{1, 2, \ldots, n\}$. Сколько существует различных нормализованных латинских квадратов порядка n для каждого $n \leqslant 4$?

9.60. Пусть L — латинский квадрат порядка m, образованный элементами $\{1, 2, \ldots, m\}$, а M — латинский квадрат порядка n, образованный элементами $\{1, 2, \ldots, n\}$. С помощью L и M построить латинский квадрат порядка mn с элементами из множества $\{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}$.

9.61. Построить три попарно ортогональных латинских квадрата порядка 4.

9.62. Доказать, что если $n \geqslant 2$, то существует не более чем $n - 1$ попарно ортогональных латинских квадратов порядка n.

9.63. *Магический квадрат* порядка n образуется целыми числами от 1 до n^2, записанными в виде матрицы размера $n \times n$ таким образом, что сумма элементов по любой строке, любому столбцу и по обеим диагоналям равняется одному и тому же числу. Пусть $A = (a_{ij})$ и $B = (b_{ij})$ — два ортогональных латинских квадрата порядка n, образованные числами $\{0, 1, \ldots, n-1\}$. Пусть при этом сумма элементов, стоящих по каждой из диагоналей матриц A или B, равняется $n(n-1)/2$. Показать, что $M = (na_{ij} + b_{ij} + 1)$ является магическим квадратом порядка n. Построить магический квадрат порядка 4, используя два ортогональных латинских квадрата, полученных в упр. 9.61.

9.64. Найти матрицы Адамара порядков 8 и 12.

9.65. Показать, что если H_m и H_n — матрицы Адамара, то существует матрица Адамара H_{mn}.

9.66. Показать, что из нормализованной матрицы Адамара порядка $4t$, $t \geqslant 2$, можно построить симметричную $(4t-1, 2t-1, t-1)$-блок-схему.

9.67. Доказать, что граф состояний ЛМС над полем $\mathbb{F}_q$ с невырожденной основной характеристической матрицей представляет собой цикл без подходов.

9.68. Показать, что графы состояний, соответствующие подобным основным характеристическим матрицам над полем $\mathbb{F}_q$, являются изоморфными. (*Замечание.* Две матрицы A и B над полем $\mathbb{F}_q$ называются *подобными*, если существует невырожденная матрица P над полем $\mathbb{F}_q$, такая, что $B = PAP^{-1}$.)

9.69. Пусть основная характеристическая матрица A ЛМС $\mathscr{M}$ над полем $\mathbb{F}_2$ имеет минимальный многочлен вида $(x+1)^5 (x^3 + x + 1)^3$. Какие порядки могут иметь внутренние состояния ЛМС $\mathscr{M}$?

9.70. Найти порядки всех внутренних состояний ЛМС $\mathscr{M}$ из примера 9.97.

9.71. Пусть основная характеристическая матрица A ЛМС $\mathscr{M}$ над полем $\mathbb{F}_q$ обладает тем свойством, что ее минимальный многочлен совпадает с ее характеристическим многочленом. Пусть минимальный многочлен матрицы A имеет вид $p(x)^e$, где $p(x)$ — нормированный неприводимый многочлен над полем $\mathbb{F}_q$, $\deg(p(x)) = d$. Не пользуясь теоремой 9.96, доказать, что цикловая сумма ЛМС $\mathscr{M}$ задается формулой, приведенной в этой теореме.

9.72. Найти цикловую сумму ЛМС $\mathscr{M}$ над полем $\mathbb{F}_3$, определенной в примере 9.91.

9.73. Доказать теорему 9.98.

Глава 10

Таблицы

В этой главе собраны некоторые таблицы, облегчающие вычисления в конечных полях, а также таблицы неприводимых и примитивных многочленов над конечными полями. Описание этих таблиц приводится соответственно в § 1 и 2.

§ 1. Вычисления в конечных полях

Операции умножения и деления ненулевых элементов поля $\mathbb{F}_q$ можно выполнять, пользуясь аналогом понятия логарифма. При этом вместо термина «логарифм» нам будет предпочтительнее пользоваться термином «индекс». Если b — примитивный элемент поля $\mathbb{F}_q$, то для любого элемента $a \in \mathbb{F}_q^*$ существует единственное целое число r, $0 \leqslant r < q - 1$, такое, что $a = b^r$. Это число r называется *индексом* элемента a (по основанию b) и обозначается через $\operatorname{ind}_b(a)$ (или просто $\operatorname{ind}(a)$, если элемент b фиксирован). Индекс как функция (будем называть ее *индексной функцией*) удовлетворяет следующим основным условиям:

$$\operatorname{ind}(ac) \equiv \operatorname{ind}(a) + \operatorname{ind}(c) \pmod{(q-1)},$$

$$\operatorname{ind}(ac^{-1}) \equiv \operatorname{ind}(a) - \operatorname{ind}(c) \pmod{(q-1)}.$$

Функция, обратная к индексной функции и соответствующая взятию антилогарифма, называется *экспоненциальной функцией* и обозначается через $\exp_b$ или просто exp. При этом выполняются соотношения

$$\exp(r) = b^r, \quad \exp(\operatorname{ind}(a)) = a, \quad \operatorname{ind}(\exp(r)) = r.$$

Имея таблицу функций ind и exp для поля $\mathbb{F}_q$, можно легко выполнять все четыре действия в поле $\mathbb{F}_q$ — сложение, вычитание, умножение и деление. Для выполнения сложения и вычитания в поле $\mathbb{F}_q$ это поле удобно рассматривать как векторное пространство над его простым подполем $\mathbb{F}_p$; для выполнения умножения и деления в поле $\mathbb{F}_q$ используются свойства функции ind, а таблица функций exp и ind позволяет переходить от одних обозначений к другим. В табл. А приводится полный список ненулевых элементов и соответствующих им индексов для всех конечных полей $\mathbb{F}_q$, где q — составное число, не превосходящее 128. В ко-

лонке, соответствующей значениям функции exp, скобки и запятые, обычно используемые для записи вектора, соответствующего заданному элементу

$$a = (a_1, \ldots, a_n) = a_1 b^{n-1} + a_2 b^{n-2} + \ldots + a_n, \quad 0 \leqslant a_i < p,$$

поля $\mathbb{F}_q$, где $q = p^n$, будут опускаться.

10.1. Пример. В качестве примера использования таблицы A вычислим в поле $\mathbb{F}_9$ выражение

$$[(b + 1) + (2b + 2)\, b]\, (b + 2)^{-1} + b.$$

Используя ту часть табл. A, которая соответствует полю $\mathbb{F}_9$, получаем

$$\text{ind}\ ((2b + 2)\, b) \equiv \text{ind}\ (2b + 2) + \text{ind}\ (b) \equiv 3 + 1 \equiv$$
$$\equiv 4 \pmod 8,$$
$$(2b + 2)\, b = \exp(4) = 2.$$

Тогда $(b + 1) + (2b + 2)\, b = b$ и

$$\text{ind}\ ([(b + 1) + (2b + 2)\, b]\, (b + 2)^{-1}) \equiv \text{ind}\ (b) - \text{ind}\ (b + 2) \equiv$$
$$\equiv 1 - 6 \equiv 3 \pmod 8,$$

$$[(b + 1) + (2b + 2)\, b]\, (b + 2)^{-1} = \exp(3) = 2b + 2.$$

Таким образом, исходное выражение равно $(2b + 2) + b = 2$. □

Таблица B предоставляет другую возможность для выполнения арифметических операций в конечных полях. Первые две ее колонки представляют собой таблицы *логарифмов Якоби* $L(n)$ для полей $\mathbb{F}_{2^k}$, где $2 \leqslant k \leqslant 6$ (определение логарифма Якоби см. в упр. 2.8). Символ $n \to s$ здесь означает, что $L(n) = s$ (относительно некоторого фиксированного примитивного элемента b). В случае когда характеристика поля равна 2, величина $L(0)$ является неопределенной. Перемножение элементов b^n производится обычным образом, т. е. $b^m \cdot b^n = b^{m+n}$ сложение же их производится по правилу

$$b^m + b^n = b^{m + L(n-m)}$$

(указанному в упр. 2.8). Символ $+$, расположенный перед величиной n, здесь указывает на то, что элемент b^n является примитивным.

10.2. Пример. Используя табл. B, вычислим выражение

$$(b^6 + b^{25} + b^{44})\, (1 + b^{35})^{-1} + b^{28}$$

в поле $\mathbb{F}_{64}$. Получаем: $b^6 + b^{25} = b^{6 + L(19)} = b^{40}$ и $b^{40} + b^{44} = b^{40 + L(4)} = b^{72}$. Так как $1 + b^{35} = b^{L(35)} = b^{31}$, то

$$(b^6 + b^{25} + b^{44})\, (1 + b^{35})^{-1} = b^{72} b^{-31} = b^{41}.$$

Далее, поскольку и аргумент функции L, и показатель степени элемента b рассматриваются по модулю 63, то

$$b^{41} + b^{28} = b^{41+L(-13)} = b^{41+L(50)} = b^{101} = b^{38},$$

что и является искомым результатом. Заметим, что полученный элемент b^{38} является примитивным элементом поля $\mathbb{F}_{64}$. □

В остальной части табл. В приводятся сведения о *минимальных* и *характеристических многочленах*, а также о *дуальных базисах*. Рассмотрим в качестве примера две следующие строки из таблицы для поля $\mathbb{F}_{64}$ над полем $\mathbb{F}_2$:

$$+20 \to 26\ [100001]\ 26\ 6\ 49\ 29\ 9\ 46 : 19$$
$$21 \to 42\ [101011] \qquad [11]$$

Символ $[a_1 a_2 \ldots a_m]$ означает, что многочлен вида $x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_m$ является характеристическим многочленом данного элемента относительно данного расширения поля. Так, $x^6 + x^5 + 1$ является характеристическим многочленом элемента $b^{20} \in \mathbb{F}_{64}$ над полем $\mathbb{F}_2$, а $x^6 + x^5 + x^3 + x + 1$ — характеристическим многочленом элемента $b^{21} \in \mathbb{F}_{64}$ над $\mathbb{F}_2$. Если b^n является образующим элементом данного расширения поля, то множество чисел, расположенных между характеристическим многочленом и двоеточием, описывает дуальный базис к полиномиальному базису, определяемому элементом b^n. Если же элемент b^n не является образующим элементом расширения, то в квадратных скобках приводится минимальный многочлен элемента b^n относительно данного расширения (многочлен задается описанным выше символическим способом). Например, b^{20} является образующим элементом поля $\mathbb{F}_{64}$ над $\mathbb{F}_2$. Тогда дуальным базисом к полиномиальному базису $\{1, b^{20}, b^{40}, b^{60}, b^{80}, b^{100}\}$ поля $\mathbb{F}_{64}$ над $\mathbb{F}_2$ служит базис $\{b^{26}, b^6, b^{49}, b^{29}, b^9, b^{46}\}$. С другой стороны, b^{21} не является образующим элементом поля $\mathbb{F}_{64}$ над $\mathbb{F}_2$. Минимальным многочленом элемента b^{21} над полем $\mathbb{F}_2$ будет $x^2 + x + 1$; таким образом, $b^{21} \in \mathbb{F}_4$. Если b^n — не только образующий элемент данного расширения, но, кроме того, определяет и некоторый *нормальный базис* этого расширения, то число, стоящее после двоеточия, указывает элемент, определяющий *дуальный нормальный базис*. Например, элемент b^{20} определяет нормальный базис

$$\{b^{20}, (b^{20})^2, (b^{20})^4, (b^{20})^8, (b^{20})^{16}, (b^{20})^{32}\}$$

поля $\mathbb{F}_{64}$ над полем $\mathbb{F}_2$, а его дуальный базис имеет вид

$$\{b^{19}, (b^{19})^2, (b^{19})^4, (b^{19})^8, (b^{19})^{16}, (b^{19})^{32}\}.$$

Элементы подполей данного расширения (кроме подполя $\mathbb{F}_2$) обозначаются в табл. В заглавными буквами, значения которых

выясняются при рассмотрении соответствующих минимальных многочленов. Так, например, в таблице для поля $\mathbb{F}_{64}$ буквой X обозначен элемент $b^{21} \in \mathbb{F}_4$, а буквой D — элемент $b^{27} \in \mathbb{F}_8$.

§ 2. Таблицы непроводимых многочленов

В табл. C приводятся все нормированные неприводимые многочлены степени n над простыми полями $\mathbb{F}_p$ для малых значений параметров n и p, а именно при $p = 2$ для всех $n \leqslant 11$, при $p = 3$ для $n \leqslant 7$, при $p = 5$ для $n \leqslant 5$ и при $p = 7$ для $n \leqslant 4$. Многочлен $a_0x^n + a_1x^{n-1} + \ldots + a_n$ сокращенно записывается в виде $a_0a_1 \ldots a_n$, где $a_0 = 1$. Левая колонка, помеченная значением параметра n, содержит все нормированные неприводимые многочлены f степени n над полем $\mathbb{F}_p$. Правая колонка, помеченная символом e, содержит соответствующее зиачение ord (f).

Таблица D содержит по одному примитивному многочлену степени n над полем $\mathbb{F}_2$ для каждого значения $n \leqslant 100$. В этой таблице многочлен обозначается набором степеней его ненулевых членов. Так, набор 610 обозначает многочлен $x^6 + x + 1$.

В табл. E приводятся все примитивные многочлены вида $x^2 + a_1x + a_2$ над полями $\mathbb{F}_p$, где $11 \leqslant p \leqslant 31$. Для простых $p < 11$ все квадратичные примитивные многочлены можно получить из табл. C, выделяя те многочлены f над $\mathbb{F}_p$, для которых ord $(f) = p^2 - 1$.

В табл. F приводится по одному примитивному многочлену степени n над полем $\mathbb{F}_p$ для всех $n \geqslant 2$ и p, таких, что $p < 50$ и $p^n < 10^9$. Здесь многочлен $x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$ обозначается набором $a_1a_2 \ldots a_n$.

Комментарии

§ 1. Таблица A взята из работы Alanen, Knuth [2]. Первую большую таблицу такого типа можно найти в работе Jacobi [3], где приводятся примитивные корни по модулю p и соответствующие им индексы для всех простых чисел $p < 1000$. Аналогичная, но не столь полная таблица была построеиа ранее в работе Crelle [1]. В работе Desmarest [1] приводится список примитивных корней по модулю p для всех простых чисел $p < 10\,000$. В работе Wertheim [1] построена таблица наименьших положительных примитивных корней по модулю p для всех простых чисел $p < 6200$. В работе Cunningham, Woodall, Creak [1] эта таблица продолжена до значений $p \leqslant 25\,409$ (фрагменты этой таблицы можно найти также в работе Albert [3, appendix I]), а в работе Western, Miller [1] она продолжена уже до значений $p \leqslant 50\,021$. Литвер

и Юдина [1] вычислили по одному примитивному корню по модулю p для каждого простого числа $p \leqslant 1\,001\,321$. В работе Osborn [1] построена полная таблица всех примитивных корней по модулю p для всех простых чисел $p < 1\,000$, а в работе Hauptman, Vegh, Fisher [1] эта таблица продолжена для всех $p < 5000$. Вестерн и Миллер (Western, Miller [1]) построили таблицы индексов относительно наименьшего положительного примитивного корня по модулю p для всех $p \leqslant 50\,021$ (см. также работу Andree [1], где приводится еще одна таблица индексов для конечных простых полей). Таблицы индексов для непростых конечных полей приводятся в работах Bussey [1], [2] (см. также Albert [3 appendix III], где помещены фрагменты из этих таблиц), и несколько позже в работе Alanen, Knuth [2]. Алгоритмы для вычисления значений индексов рассматриваются в работах Herlestam, Johannesson [1], Pohlig, Hellman [1], Pollard [3], Zierler [9].

В табл. В приводится лишь часть вычислительных результатов, полученных в работе Conway [1]. Логарифм Якоби был введен в работе Jacobi [2], где также была приведена таблица его значений для всех конечных простых полей $\mathbb{F}_p$ с $p \leqslant 103$. Другие ссылки, связанные с вычислениями в конечных полях, можно найти в комментариях к § 1 гл. 4.

§ 2. Таблица С взята из работы Church [1]. Список неприводимых многочленов небольшой степени над полями $\mathbb{F}_p$, $p \leqslant 19$, был приведен еще Жорданом (Jordan C. [3]). Таблица С была несколько расширена Гараковым [3], поднявшим на единицу границу для n и добавившим случаи $p = 11$ и $n \leqslant 4$. Другое расширение этой таблицы было получено в работе Chang, Godwin [1], где были рассмотрены случаи $11 \leqslant p \leqslant 37$ для $n = 2$ и $11 \leqslant p \leqslant 19$ для $n = 3$. Некоторые неприводимые трехчлены над $\mathbb{F}_p$ приводятся в работе Mortimer, Williams [1]. Таблицы неприводимых многочленов над некоторыми непростыми конечными полями были построены в работе Green, Taylor [2], где были рассмотрены случаи $n \leqslant 5$ для $\mathbb{F}_4$, $n \leqslant 3$ для $\mathbb{F}_8$ и $\mathbb{F}_9$ и $n = 2$ для $\mathbb{F}_{16}$. Более широко (ввиду важности приложений) представлен в таблицах неприводимых многочленов случай поля $\mathbb{F}_2$. Такие таблицы приводились в работах Golomb [1], [4, ch. 3] и Гараков [1], однако они не покрывают табл. С. Марш (Marsh [1]) составил список всех неприводимых многочленов степени $n \leqslant 19$ над полем $\mathbb{F}_2$ (см. также Albert [3, appendix IV] и Peterson, Weldon [1, appendix C], где приводится часть этого списка; в статье Mossige [1] рассмотрен случай $10 \leqslant n \leqslant 20$. В книге Peterson, Weldon [1, appendix C] приводится по одному неприводимому многочлену над полем $\mathbb{F}_2$ для каждого значения n, $17 \leqslant n \leqslant 34$ и каждого возможного порядка. Списки неприводимых трехчленов над полем $\mathbb{F}_2$ можно найти в работах Fredricksen,

Wisniewski [1], Golomb [4, ch. 5], Golomb, Welch, Hales [1], Zierler [7] и Zierler, Brillhart [1], [2].

Таблица D взята из работы Watson E. J. [1], а табл. E и F — из работы Alanen, Knuth [2]. Небольшую таблицу примитивных многочленов над конечными простыми полями $\mathbb{F}_p$, где $p \leqslant 11$, можно также найти в монографии Dickson [7, part I, ch. 3]. В статьях Bussey [1], [2] приводится по одному примитивному многочлену степени n над $\mathbb{F}_p$ для каждого $n \geqslant 2$ и p, таких, что $p^n < 1000$ (см. также Albert [3, appendix III]) и Heuzé [1]. В работе Alanen, Knuth [1] приводится по одному примитивному многочлену степени n над полем $\mathbb{F}_p$ для следующих значений p и n: $11 \leqslant p \leqslant 17$, $3 \leqslant n \leqslant 5$. В работе Sugimoto [1] приводится таблица примитивных многочленов над полем $\mathbb{F}_p$ для $3 \leqslant p \leqslant 47$. Грин и Тэйлор (Green, Taylor [2]) рассматривали непростые конечные поля и привели по одному примитивному многочлену для каждого из следующих случаев: $n \leqslant 11$ для $\mathbb{F}_4$, $n \leqslant 7$ для $\mathbb{F}_8$ и $\mathbb{F}_9$ и $n \leqslant 5$ для $\mathbb{F}_{16}$. В статье Beard, West [1] приводится таблица примитивных многочленов специального вида. Таблица D была расширена в статье Stahnke [1], где приведено по одному примитивному многочлену над полем $\mathbb{F}_2$ для каждого значения $n \leqslant 168$. Примитивные трехчлены над полем $\mathbb{F}_2$ можно найти в работах Rodemich, Rumsey [1], Zierler [6] и Zierler, Brillhart [1], [2].

Ллойд в работе Lloyd [1] привел таблицу канонического разложения на множители для всех многочленов над полем $\mathbb{F}_2$ степени $n \leqslant 4$ и над полем $\mathbb{F}_3$ степени $n \leqslant 3$. Эта таблица была расширена в работе Lloyd [2], где были представлены все многочлены над полем $\mathbb{F}_p$, $p = 2, 3, 5, 7$, степеней не больше, чем 11, 11, 8, 6 соответственно, а также в работе Lloyd, Remmers [1]. Таблицы разложения на множители двучленов вида $x^n - 1$ можно найти в работах Beard, West [2] и McEliece [3]. Таблицы разложения на множители трехчленов можно найти в работах Beard, West [3], Golomb [4, ch. 5] Golomb, Welch, Hales [1], Mortimer, Williams [1] и Zierler [7].

ТАБЛИЦА А

exp	ind
$GF(2^2)$	
01	0
10	1
11	2
$GF(2^3)$	
001	0
010	1
100	2
101	3
111	4
011	5
110	6
$GF(2^4)$	
0001	0
0010	1
0100	2
1000	3
1001	4
1011	5
1111	6
0111	7
1110	8
0101	9
1010	10
1101	11
0011	12
0110	13
1100	14
$GF(2^5)$	
00001	0
00010	1
00100	2
01000	3
10000	4
01001	5
10010	6
01101	7
11010	8
11101	9
10011	10
01111	11
11110	12
10101	13
01010	14
10100	15
01001	16
10010	17
00101	18
01010	19
10100	20
01001	21
10010	22
00101	23
01010	24
10100	25
01001	26
10010	27
00101	28
01010	29
10100	30
$GF(2^6)$	
000001	0
000010	1
000100	2
001000	3
010000	4
100000	5
100001	6
100011	7
100111	8
101111	9
111111	10
011111	11
111110	12
011101	13
111010	14
010101	15
101010	16
110101	17
001011	18
010110	19
101100	20
111001	21
010011	22
100110	23
101101	24
111011	25
010111	26
101110	27
111101	28
011011	29
110110	30
001101	31
011010	32
110100	33
001001	34
010010	35
100100	36
101001	37
110011	38
000111	39
001110	40
011100	41
111000	42
010001	43
100010	44
100101	45
101011	46
110111	47
001111	48
011110	49
111100	50
011001	51
110010	52
000101	53
001010	54
010100	55
101000	56
110001	57
000011	58
000110	59
001100	60
011000	61
110000	62
$GF(2^7)$	
0000001	0
0000010	1
0000100	2
0001000	3
0010000	4
0100000	5
1000000	6
0000011	7
0000110	8
0001100	9
0011000	10
0110000	11
1100000	12
1000011	13
0000101	14
0001010	15
0010100	16
0101000	17
1010000	18
0100011	19
1000110	20
0001111	21
0011110	22
0111100	23
1111000	24
1110011	25
1100101	26
1001001	27
0010001	28
0100010	29
1000100	30
0001011	31
0010110	32
0101100	33
1011000	34
0110011	35
1100110	36
1001111	37
0011101	38
0111010	39
1110100	40
1101011	41
1010101	42
0101001	43
1010010	44
0100111	45
1001110	46
0011111	47
0111110	48
1111100	49
1111011	50
1110101	51
1101001	52
1010001	53

exp	ind
$GF(2^7)$	
0100001	54
1000010	55
0000111	56
0001110	57
0011100	58
0111000	59
1110000	60
1100011	61
1000101	62
0001001	63
0010010	64
0100100	65
1001000	66
0010011	67
0100110	68
1001100	69
0011011	70
0110110	71
1101100	72
1011011	73
0110101	74
1101010	75
1010111	76
0101101	77
1011010	78
0110111	79
1101110	80
1011111	81
0111101	82
1111010	83
1110111	84
1101101	85
1011001	86
0110001	87
1100010	88
1000111	89
0001101	90
0011010	91
0110100	92
1101000	93
1010011	94
0100101	95
1001010	96
0010111	97
0101110	98
1011100	99
0111011	100

exp	ind
$GF(2^7)$	
1110110	101
1101111	102
1011101	103
0111001	104
1110010	105
1100111	106
1001101	107
0011001	108
0110010	109
1100100	110
1001011	111
0010101	112
0101010	113
1010100	114
0101011	115
1010110	116
0101111	117
1011110	118
0111111	119
1111110	120
1111111	121
1111101	122
1111001	123
1110001	124
1100001	125
1000001	126
$GF(3^2)$	
01	0
10	1
21	2
22	3
02	4
20	5
12	6
11	7
$GF(3^3)$	
001	0
010	1
100	2
102	3
122	4
022	5
220	6
101	7

exp	ind
$GF(3^3)$	
112	8
222	9
121	10
012	11
120	12
002	13
020	14
200	15
201	16
211	17
011	18
110	19
202	20
221	21
111	22
212	23
021	24
210	25
$GF(3^4)$	
0001	0
0010	1
0100	2
1000	3
2001	4
1012	5
2121	6
2212	7
0122	8
1220	9
1201	10
1011	11
2111	12
2112	13
2122	14
2222	15
0222	16
2220	17
0202	18
2020	19
1202	20
1021	21
2211	22
0112	23
1120	24
0201	25
2010	26

exp	ind
$GF(3^4)$	
1102	27
0021	28
0210	29
2100	30
2002	31
1022	32
2221	33
0212	34
2120	35
2202	36
0022	37
0220	38
2200	39
0002	40
0020	41
0200	42
2000	43
1002	44
2021	45
1212	46
1121	47
0211	48
2110	49
2102	50
2022	51
1222	52
1221	53
1211	54
1111	55
0111	56
1110	57
0101	58
1010	59
2101	60
2012	61
1122	62
0221	63
2210	64
0102	65
1020	66
2201	67
0012	68
0120	69
1200	70
1001	71
2011	72
1112	73
0121	74

exp	ind
$GF(3^4)$	
1210	75
1101	76
0011	77
0110	78
1100	79
$GF(5^2)$	
01	0
10	1
43	2
42	3
32	4
44	5
02	6
20	7
31	8
34	9
14	10
33	11
04	12
40	13
12	14
13	15
23	16
11	17
03	18
30	19
24	20
21	21
41	22
22	23
$GF(5^3)$	
001	0
010	1
100	2
403	3
132	4
223	5
031	6
310	7
304	8
244	9
241	10
211	11
411	12

exp	ind
$GF(5^3)$	
212	13
421	14
312	15
324	16
444	17
042	18
420	19
302	20
224	21
041	22
410	23
202	24
321	25
414	26
242	27
221	28
011	29
110	30
003	31
030	32
300	33
204	34
341	35
114	36
043	37
430	38
402	39
122	40
123	41
133	42
233	43
131	44
213	45
431	46
412	47
222	48
021	49
210	50
401	51
112	52
023	53
230	54
101	55
413	56
232	57
121	58
113	59
033	60

exp	ind
$GF(5^3)$	
330	61
004	62
040	63
400	64
102	65
423	66
332	67
024	68
240	69
201	70
311	71
314	72
344	73
144	74
343	75
134	76
243	77
231	78
111	79
013	80
130	81
203	82
331	83
014	84
140	85
303	86
234	87
141	88
313	89
334	90
044	91
440	92
002	93
020	94
200	95
301	96
214	97
441	98
012	99
120	100
103	101
433	102
432	103
422	104
322	105
424	106
342	107
124	108

exp	ind
$GF(5^3)$	
143	109
333	110
034	111
340	112
104	113
443	114
032	115
320	116
404	117
142	118
323	119
434	120
442	121
022	122
220	123
$GF(7^2)$	
01	0
10	1
64	2
53	3
56	4
16	5
54	6
66	7
03	8
30	9
45	10
12	11
14	12
34	13
15	14
44	15
02	16
20	17
51	18
36	19
35	20
25	21
31	22
55	23
06	24
60	25
13	26

exp	ind
$GF(7^2)$	
24	27
21	28
61	29
23	30
11	31
04	32
40	33
32	34
65	35
63	36
43	37
62	38
33	39
05	40
50	41
26	42
41	43
42	44
52	45
46	46
22	47
$GF(11^2)$	
01	0
10	1
*4	2
57	3
29	4
78	5
16	6
54	7
*9	8
*7	9
87	10
**	11

exp	ind
$GF(11^2)$	
07	12
70	13
46	14
25	15
38	16
51	17
79	18
26	19
48	20
45	21
15	22
44	23
05	24
50	25
69	26
32	27
*1	28
27	29
58	30
39	31
61	32
62	33
72	34
66	35
02	36
20	37
98	38
*3	39
47	40
35	41
21	42
*8	43
97	44
93	45
53	46
99	47
03	48

exp	ind
$GF(11^2)$	
30	49
81	50
4*	51
65	52
*2	53
37	54
41	55
85	56
8*	57
2*	58
88	59
0*	60
*0	61
17	62
64	63
92	64
43	65
*5	66
67	67
12	68
14	69
34	70
11	71
04	72
40	73
75	74
96	75
83	76
6*	77
42	78
95	79
73	80
76	81
*6	82
77	83

exp	ind
$GF(11^2)$	
06	84
60	85
52	86
89	87
1*	88
94	89
63	90
82	91
5*	92
59	93
49	94
55	95
09	96
90	97
23	98
18	99
74	100
86	101
9*	102
13	103
24	104
28	105
68	106
22	107
08	108
80	109
3*	110
71	111
56	112
19	113
84	114
7*	115
36	116
31	117
91	118
33	119

Символ * означает элемент 10 в поле F_{11}.

$\mathbb{F}_4$ над $\mathbb{F}_2$

0 → * [01] [1]
+1 → 2 [11]2 0:1
+2 → 1 [11]1 0:2

$\mathbb{F}_8$ над $\mathbb{F}_2$

0 → * [111] [1]
+1 → 5 [101]4 3 5:1
+2 → 3 [101]1 6 3:2
+3 → 2 [011]0 6 3:-
+4 → 6 [101]2 5 6:4
+5 → 1 [011]0 3 5:-
+6 → 4 [011]0 5 6:-

$\mathbb{F}_{16}$ над $\mathbb{F}_2$

0 → * [0001] [1]
+1 → 4 [0011]14 2 1 0: -
+2 → 8 [0011]13 4 2 0: -
3 → 14 [1111]14 10 1 2:11
+4 → 1 [0011]11 8 4 0: -
5 → 10 [0101] [11]
6 → 13 [1111]13 5 2 4: 7
+7 → 9 [1001] 9 2 10 1: 6
+8 → 2 [0011] 7 1 8 0: -
9 → 7 [1111] 7 5 8 1:13
10 → 5 [0101] [11]
+11 → 12 [1001]12 1 5 8: 3
12 → 11 [1111]11 10 4 8:14
+13 → 6 [1001] 6 8 10 4: 9
+14 → 3 [1001] 3 4 5 2:12

над $\mathbb{F}_4$

[01] [1]
[1X] 4 0: 1
[1Y] 8 0: 2
[Y1] 2 5:13
[1X] 1 0: 4
[0Y] [X]
[X1] 4 10:11
[XX] 8 10:12
[1Y] 2 0: 8
[X1] 1 10:14
[0X] [Y]
[YY] 4 5: 6
[Y1] 8 5: 7
[XX] 2 10: 3
[YY] 1 5: 9

$\mathbb{F}_{32}$ над $\mathbb{F}_2$

0 * [10011] [1]
+1 → 19 [10111]16 3 6 5 17: 1
+2 → 7 [10111] 1 6 12 10 3: 2
+3 → 11 [01001] 0 28 25 6 3: -
+4 → 14 [10111] 2 12 24 20 6: 4
+5 → 29 [01111] 4 28 5 14 9: -
+6 → 22 [01001] 0 25 19 12 6: -
+7 → 2 [00101]27 20 17 10 3: -
+8 → 28 [10111] 4 24 17 9 12: 8
+9 → 15 [01111] 1 7 9 19 10: -
+10 → 27 [01111] 8 25 10 28 18: -
+11 → 3 [11101]23 12 7 6 3:15
+12 → 13 [01001] 0 19 7 24 12: -
+13 → 12 [11101]30 17 28 24 12:29
+14 → 4 [00101]23 9 3 20 6: -
+15 → 9 [11011]26 20 5 19 10:11

$\mathbb{F}_{32}$ над $\mathbb{F}_2$

+16 → 25 [10111] 8 17 3 18 24:16
+17 → 21 [01001] 0 14 28 3 17: -
+18 → 30 [01111] 2 14 18 7 20: -
+19 → 1 [00101]29 10 24 5 17: -

+20 → 23 [01111]16 19 20 25 5: -
+21 → 17 [11101]27 6 19 3 17:23
+22 → 6 [11101]15 24 14 12 6:30
+23 → 20 [11011]13 10 18 25 5:21
+24 → 26 [01001] 0 7 14 17 24: -
+25 → 16 [00101]30 5 12 18 24: -
+26 → 24 [11101]29 3 25 17 24:27
+27 → 10 [11011]22 5 9 28 18:26
+28 → 8 [00101]15 18 6 9 12: -
+29 → 5 [11011]11 18 20 14 9:13

+30 → 18 [11011]21 9 10 7 20:22

$\mathbb{F}_{64}$ над $\mathbb{F}_2$	над $\mathbb{F}_4$	над $\mathbb{F}_8$
0 → * [010101] [1]	[111] [1]	[01] [1]
+ 1 → 8 [101101]44 43 58 54 53 45: -	[*XXX*]47 54 27: 8	[1*A*] 8 0: 1
+ 2 → 16 [101101]25 23 53 45 43 27: -	[*YYY*]31 45 54:16	[1*B*] 16 0: 2
3 → 53 [010111]60 47 46 43 3 0: -	[0*Y*1] 0 6 3: -	[*FD*]42 18:39
+ 4 → 32 [101101]50 46 43 27 23 54: -	[*XXX*]62 27 45:32	[1*C*] 32 0: 4
+ 5 → 38 [100001]38 33 28 23 18 43:52	[*XYY*]23 56 49: -	[*CF*] 4 27:59
6 → 43 [010111]57 31 29 23 6 0: -	[0*X*1] 0 12 6: -	[*DE*]21 36:15
7 → 62 [001001]42 35 28 0 56 49: -	[00*X*] 0 56 49: -	[*E*1] 2 9:25
+ 8 → 1 [101101]37 29 23 54 46 45: -	[*YYY*]61 54 27: 1	[1*A*] 1 0: 8
9 → 45 [010001] [101]	[101] 36 27 45: 9	[0*B*] [*A*]
+10 → 13 [100001]13 3 56 46 36 23:41	[*YXX*]46 49 35: -	[*AD*] 8 54:55
+11 → 51 [110011]37 14 3 55 36 48:11	[*X*1*Y*]55 48 24:25	[*AC*]16 54:56
12 → 23 [010111]51 62 58 46 12 0: -	[0*Y*1] 0 24 12: -	[*EF*]42 9:30
+13 → 10 [100111]10 7 59 46 33 23:17	[*XYX*]43 49 35: -	[*AE*]32 54:58
14 → 61 [001001]21 7 56 0 49 35: -	[00*Y*] 0 49 35: -	[*F*1] 4 18:50
15 → 44 [110101]51 36 46 31 47 3:15	[*Y*01] 18 3 33:57	[*CA*]21 27: 6
+16 → 2 [101101]11 58 46 45 29 27: -	[*XXX*]59 45 54: 2	[1*B*] 2 0:16
+17 → 41 [100001]41 24 7 53 36 58:13	[*XYY*]53 14 28: -	[*AD*] 1 54:62
18 → 27 [010001] [101]	[101] 9 54 27:18	[0*C*] [*B*]
+19 → 34 [100111]34 49 62 43 24 53:20	[*XYX*]58 28 56: -	[*BF*] 8 45:46
+20 → 26 [100001]26 6 49 29 9 46:19	[*XYY*]29 35 7: -	[*BE*]16 45:47
21 → 42 [101011] [11]	[*XY*1] [*X*]	[11] 42 0:21
+22 → 39 [110011]11 28 6 47 9 33:22	[*Y*1*X*]47 33 48:50	[*BA*]32 45:49
+23 → 12 [000011]40 29 6 46 23 0: -	[1*XY*]31 24 12:58	[*EB*] 4 9:41
24 → 46 [010111]39 61 53 29 24 0: -	[0*X*1] 0 48 24: -	[*FD*]21 18:60
+25 → 30 [110011]44 49 24 62 36 6:25	[*Y*1*X*]62 6 3:11	[*AC*] 2 54: 7

F_{64}	над F_2	над F_4	над F_8
+26 → 20 [100111]20 14 55 29 3 46:34		[*YXY*]23 35 7: -	[*BF*] 1 45:53
27 → 18 [000101] [011]		[011] 0 54 27: -	[*OE*] [*D*]
28 → 59 [001001]42 14 49 0 35 7: -		[00*X*] 0 35 7: -	[*D*1] 8 36:37
+29 → 48 [000011]34 53 24 58 29 0: -		[1*XY*]61 33 48:43	[*DA*]16 36:38
30 → 25 [110101]39 9 29 62 31 6:30		[*X*01] 36 6 3:51	[*AB*]42 54:12
+31 → 35 [011011]25 29 61 0 24 56: -		[11*X*] 46 28 56: -	[*DD*]32 36:40
+32 → 4 [101101]22 53 29 27 58 54: -		[*YYY*]55 27 45: 4	[1*C*] 4 0:32
33 → 58 [010111]30 55 23 53 33 0: -		[0*X*1] 0 3 33: -	[*EF*]21 9:51
+34 → 19 [100001]19 48 14 43 9 53:26		[*YXX*]43 28 56: -	[*BE*] 2 45:61
35 → 31 [001001]21 49 14 0 28 56: -		[00*Y*] 0 28 56: -	[*D*1] 1 36:44
36 → 54 [010001] [101]		[101] 18 45 54:36	[*OA*] [*C*]
+37 → 57 [110011]50 7 33 59 18 24:37		[*Y*1*X*]59 24 12:44	[*CB*] 8 27:28
+38 → 5 [100111] 5 35 61 23 48 43:40		[*YXY*]53 56 49: -	[*CD*] 16 27:29
39 → 22 [110101]57 18 23 47 55 33:39		[*X*01] 9 33 48:60	[*BC*]42 45: 3
+40 → 52 [100001]52 12 35 58 18 29:38		[*YXX*]58 7 14: -	[*CF*]32 27:31
+41 → 17 [100111]17 56 31 53 12 58:10		[*YXY*]29 14 28: -	[*AE*] 4 54:23
42 → 21 [101011] [11]		[*YX*1] [*Y*]	[11] 21 0:42
+43 → 6 [000011]20 46 3 23 43 0: -		[1*YX*] 47 12 6:29	[*DA*] 2 36:52
+44 → 15 [110011]22 56 12 31 18 3:44		[*X*1*Y*]31 3 33:37	[*CB*] 1 27:35
45 → 9 [000101] [011]		[011] 0 27 45: -	[*OD*] [*F*]
+46 → 24 [000011]17 58 12 29 46 0: -		[1*YX*] 62 48 24:53	[*FC*] 8 18:19
+47 → 49 [011011]44 46 62 0 12 28: -		[11*Y*] 23 14 28: -	[*FF*]16 18:20
48 → 29 [010111]15 59 43 58 48 0: -		[0*Y*1] 0 33 48: -	[*DE*]42 36:57
49 → 47 [001001]42 56 7 0 14 28: -		[00*X*] 0 14 28: -	[*F*1] 32 18:22
+50 → 60 [110011]25 35 48 61 9 12:50		[*X*1*Y*]61 12 6:22	[*BA*] 4 45:14
51 → 11 [110101]60 9 43 55 59 48:51		[*Y*01] 36 48 24:30	[*AB*]21 54:33
+52 → 40 [100111]40 28 27 58 6 29: 5		[*XYX*]46 7 14: -	[*CD*] 2 27:43
+53 → 3 [000011]10 23 33 43 53 0: -		[1*XY*] 55 6 3:46	[*FC*] 1 18:26
54 → 36 [000101] [011]		[011] 0 45 54: -	[*OF*] [*E*]
+55 → 56 [011011]22 23 31 0 6 14: -		[11*X*] 43 7 14: -	[*EE*] 8 9:10
56 → 55 [001001]21 28 35 0 7 14: -		[00*Y*] 0 7 14: -	[*E*1] 16 9:11
57 → 37 [110101]30 36 53 59 61 24:57		[*X*01] 18 24 12:15	[*CA*] 42 27:48
+58 → 33 [000011] 5 43 48 53 58 0: -		[1*YX*] 59 3 33:23	[*EB*]32 9:13
+59 → 28 [011011]11 43 47 0 3 7: -		[11*Y*] 53 35 7: -	[*DD*] 4 36: 5
60 → 50 [110101]15 18 58 61 62 12:60		[*Y*01] 9 12 6:39	[*BC*]21 45:24
+61 → 14 [011011]37 53 55 0 33 35: -		[11*X*]58 49 35: -	[*EF*] 2 18:34
+62 → 7 [011011]50 58 59 0 48 49: -		[11*Y*]29 56 49: -	[*EE*] 1 9:17

ТАБЛИЦА С

Неприводимые многочлены по модулю 2

$n = 1$	e
10	1
11	1

$n = 2$	e
111	3

$n = 3$	e
1011	7
1101	7

$n = 4$	e
10011	15
11001	15
11111	5

$n = 5$	e
100101	31
101001	31
101111	31
110111	31
111011	31
111101	31

$n = 6$	e
1000011	63
1001001	9
1010111	21
1011011	63
1100001	63
1100111	63
1101101	63
1110011	63
1110101	21

$n = 7$	e
10000011	127
10001001	127
10001111	127
10010001	127
10011101	127
10100111	127
10101011	127
10111001	127
10111111	127
11000001	127
11001011	127
11010011	127
11010101	127
11100101	127
11101111	127
11110001	127
11110111	127
11111101	127

$n = 8$	e
100011011	51
100011101	255
100101011	255
100101101	255
100111001	17
100111111	85
101001101	255
101011111	255
101100011	255
101100101	255
101101001	255
101110001	255
101110111	85
101111011	85
110000111	255
110001011	85
110001101	255
110011111	51
110100011	85
110101001	255
110110001	51
110111101	85
111000011	255
111001111	255
111010111	17
111011101	85
111100111	255
111110011	51
111110101	255
111111001	85

$n = 9$	e
1000000011	73
1000010001	511
1000010111	73
1000011011	511
1000100001	511
1000101101	511
1000110011	511
1001001011	73
1001011001	511
1001011111	511
1001100101	73
1001101001	511
1001101111	511
1001110111	511
1001111101	511
1010000111	511
1010010101	511
1010011001	73
1010100011	511
1010100101	511
1010101111	511
1010110111	511
1010111101	511
1011001111	511
1011010001	511
1011011011	511
1011110101	511
1011111001	511
1100000001	73
1100010011	511
1100010101	511
1100011111	511
1100100011	511
1100110001	511
1100111011	511
1101001001	73
1101001111	511
1101011011	511
1101100001	511
1101101011	511
1101101101	511
1101110011	511
1101111111	511
1110000101	511
1110001111	511
1110100001	73
1110110101	511
1110111001	511
1111000111	511
1111001011	511
1111001101	511
1111010101	511
1111011001	511
1111100011	511
1111101001	511
1111111011	511

$n = 10$	e
10000001001	1023
10000001111	341
10000011011	1023
10000011101	341
10000100111	1023
10000101101	1023
10000110101	93
10001000111	341
10001010011	341
10001100011	341
10001100101	1023
10001101111	1023
10010000001	1023
10010001011	1023
10010011001	341
10010101001	33
10010101111	341
10011000101	1023
10011001001	341
10011010111	1023
10011100111	1023
10011101101	341
10011110011	1023
10011111111	1023
10100001011	93
10100001101	1023
10100011001	1023
10100011111	341
10100100011	1023
10100110001	1023
10100111101	1023
10101000011	1023
10101010111	1023
10101100001	93
10101100111	341
10101101011	1023
10110000101	1023
10110001111	1023
10110010111	1023
10110011011	341
10110100001	1023
10110101011	341
10110111001	341
10111000001	341

10111000111	1023
10111100101	1023
10111110111	1023
10111111011	1023
11000010011	1023
11000010101	1023
11000100011	33
11000100101	1023
11000110001	341
11000110111	1023
11001000011	1023
11001001111	1023
11001010001	341
11001011011	1023
11001111001	1023
11001111111	1023
11010000101	93
11010001001	1023
11010100111	93
11010101101	341
11010110101	1023
11010111111	341
11011000001	1023
11011001101	341
11011010011	1023
11011011111	1023
11011110111	341
11011111101	1023
11100001111	341
11100010001	341
11100010111	1023
11100011101	1023
11100100001	1023
11100101011	93
11100110101	341
11100111001	1023
11101000111	1023
11101001101	1023
11101010101	1023
11101011001	1023
11101100011	1023
11101111011	341
11101111101	1023
11110000001	341
11110000111	341
11110001101	1023
11110010011	1023
11110101001	341
11110110001	1023
11111000101	341
11111011011	1023
11111101011	341
11111110011	1023
11111111001	1023
11111111111	11

$n = 11$	e
100000000101	2047
100000010111	2047
100000101011	2047
100000101101	2047
100001000111	2047
100001100011	2047
100001100101	2047
100001110001	2047
100001111011	2047
100010001101	2047
100010010101	2047
100010011111	2047
100010101001	2047
100010110001	2047
100011000011	89
100011001111	2047
100011010001	2047
100011100001	2047
100011100111	2047
100011101011	2047
100011110101	2047
100100001101	2047
100100010011	2047
100100100101	2047
100100101001	2047
100100110111	89
100100111011	2047
100100111101	2047
100101000101	2047
100101001001	2047
100101010001	2047
100101011011	2047
100101110011	2047
100101110101	2047
100101111111	2047
100110000011	2047
100110001111	2047
100110101011	2047
100110101101	2047
100110111001	2047
100111000111	2047
100111011001	2047
100111100101	2047
100111101111	89
100111110111	2047
101000000001	2047
101000000111	2047
101000010011	2047
101000010101	2047
101000101001	2047
101001001001	2047
101001100001	2047
101001101101	2047
101001111001	2047
101001111111	2047
101010000101	2047
101010010001	2047
101010011101	2047
101010100111	2047
101010101011	2047
101010110011	2047
101010110101	2047
101011010011	2047
101011011111	2047
101011100011	23
101011101001	2047
101011101111	2047
101011110001	2047
101011111011	2047
101100000011	2047
101100001001	2047
101100010001	2047
101100110011	2047
101100111111	2047
101101000001	2047
101101001011	2047
101101011001	2047
101101011111	2047
101101100101	2047
101101101111	2047
101101111101	2047
101110000111	2047
101110001011	2047
101110010011	2047
101110010101	2047
101110101111	2047
101110110111	2047
101110111101	2047
101111001001	2047
101111011011	2047
101111011101	2047
101111100111	2047
101111101101	2047
110000001011	2047
110000001101	2047
110000011001	2047
110000011111	2047
110000110001	89
110001010111	2047
110001100001	2047
110001101011	2047
110001110011	2047
110001110101	23
110010000101	2047
110010001001	2047
110010010111	2047
110010011011	2047
110010011101	2047
110010110011	2047
110011000111	2047
110011001101	2047
110011010011	2047
110011010101	2047
110011100011	2047
110011101001	2047
110011110111	2047
110100000011	2047
110100001111	2047
110100011101	2047
110100100111	2047
110100101101	2047
110101000001	2047
110101000111	2047
110101010101	2047
110101011001	2047
110101100011	2047
110101101111	2047
110101110001	2047
110110010011	2047
110110011111	2047
110110101001	2047
110110111011	2047
110110111101	2047
110111001001	2047
110111010111	2047
110111011011	2047
110111100001	2047
110111100111	2047
110111110101	2047
111011111111	89
111000000101	2047

Неприводимые многочлены по модулю 2

1110000011101	2047
1110000100001	2047
1110001000111	2047
1110001010011	2047
1110001100111	2047
1110001111001	2047
1110010000111	2047
1110010010111	2047
1110010100101	2047
1110010111111	2047
1110011001001	2047
1110011010101	2047
1110011011111	2047
1110011110001	2047

1110011111011	2047
1110011111101	2047
1110100000001	2047
1110100100011	2047
1110100111111	2047
1110101000011	2047
1110101011011	2047
1110110010001	89
1110111001111	2047
1110111011101	2047
1110111110011	2047

1110111111001	2047
1111000001011	2047
1111000011001	2047
1111000110001	2047
1111000110111	2047
1111001011101	2047
1111001101011	2047
1111010110101	2047
1111011111001	89
1111100000011	2047

1111110010001	2047
1111110010111	2047
1111110011011	2047
1111110100111	2047
1111110101101	2047
1111110110101	2047
1111111001101	2047
1111111010011	2047
1111111100101	2047
1111111101001	2047
1111111111011	89

Неприводимые многочлены по модулю 3

$n=1$	e
10	1
11	2
12	1

$n=2$	e
101	4
112	8
122	8

$n=3$	e
1021	26
1022	13
1102	13
1112	13
1121	26
1201	26
1211	26
1222	13

$n=4$	e
10012	80
10022	80
10102	16
10111	40
10121	40
10202	16
11002	80
11021	20
11101	40
11111	5
11122	80
11222	80
12002	80
12011	20

12101	40
12112	80
12121	10
12212	80

$n=5$	e
100021	242
100022	121
100112	121
100211	242
101011	242
101012	121
101102	121
101122	121
101201	242
101221	242
102101	242
102112	121
102122	11
102202	121
102211	242
102221	22
110002	121
110012	121
110021	242
110101	242
110111	242
110122	121
111011	242
111121	242
111211	242
111212	121
112001	242
112022	121
112102	11
112111	242
112201	242
112202	121

120001	242
120011	242
120022	121
120202	121
120212	121
120221	242
121012	121
121111	242
121112	121
121222	121
122002	121
122021	242
122101	242
122102	121
122201	22
122212	121

$n=6$	e
1000012	728
1000022	728
1000111	364
1000121	364
1000201	52
1001012	728
1001021	364
1001101	91
1001122	104
1001221	182
1002011	364
1002022	728
1002101	182
1002112	104
1002211	91
1010201	52
1010212	728
1010222	728
1011001	91
1011011	364

1011022	728
1011122	728
1012001	182
1012012	728
1012021	364
1012112	728
1020001	52
1020101	52
1020112	728
1020122	728
1021021	364
1021102	56
1021112	728
1021121	91
1022011	364
1022102	56
1022111	182
1022122	728
1100002	728
1100012	56
1100111	364
1101002	728
1101011	28
1101101	364
1101112	728
1101212	728
1102001	364
1102111	91
1102121	91
1102201	364
1102202	728
1110001	364
1110011	364
1110122	728
1110202	728
1110221	182
1111012	728
1111021	182
1111111	7

1111112	728
1111222	728
1112011	91
1112201	182
1112222	728
1120102	728
1120121	91
1120222	728
1121012	728
1121102	728
1121122	104
1121212	728
1121221	364
1122001	91
1122002	104
1122122	104
1122202	728
1122221	364
1200002	728
1200022	56
1200121	364
1201001	364
1201111	182
1201121	182
1201201	364
1201202	728
1202002	728
1202021	28
1202101	364
1202122	728
1202222	728
1210001	364
1210021	364
1210112	728
1210202	728
1210211	91
1211021	182
1211201	91
1211212	728

1212011	91
1212022	728
1212121	14
1212122	728
1212212	728
1220102	728
1220111	182
1220212	728
1221001	182
1221002	104
1221112	104
1221202	728
1221211	364
1222022	728
1222102	728
1222112	104
1222211	364
1222222	728

$n = 7$	e
10000102	1093
10000121	2186
10000201	2186
10000222	1093
10001011	2186
10001012	1093
10001102	1093
10001111	2186
10001201	2186
10001212	1093
10002112	1093
10002122	1093
10002211	2186
10002221	2186
10010122	1093
10010222	1093
10011002	1093
10011101	2186
10011211	2186
10012001	2186
10012022	1093
10012111	2186
10012202	1093
10020121	2186
10020221	2186
10021001	2186
10021112	1093
10021202	1093
10022002	1093
10022021	2186
10022101	2186
10022212	1093
10100011	2186
10100012	1093
10100102	1093
10100122	1093
10100201	2186
10100221	2186
10101101	2186
10101112	1093
10101202	1093
10101211	2186
10102102	1093
10102201	2186
10110022	1093
10110101	2186
10110211	2186
10111001	2186
10111102	1093
10111121	2186
10111201	2186
10112002	1093
10112012	1093
10112021	2186
10112111	2186
10112122	1093
10120021	2186
10120112	1093
10120202	1093
10121002	1093
10121102	1093
10121201	2186
10121222	1093
10122001	2186
10122011	2186
10122022	1093
10122212	1093
10122221	2186
10200001	2186
10200002	1093
10200101	2186
10200112	1093
10200202	1093
10200211	2186
10201021	2186
10201022	1093
10201121	2186
10201222	1093
10202011	2186
10202012	1093
10210001	2186
10210121	2186
10210202	1093
10211101	2186
10211111	2186
10211122	1093
10211221	2186
10212011	2186
10212022	1093
10212101	2186
10212112	1093
10212212	1093
10220002	1093
10220101	2186
10220222	1093
10221122	1093
10221202	1093
10221212	1093
10221221	2186
10222012	1093
10222021	2186
10222111	2186
10222202	1093
10222211	2186
11000101	2186
11000222	1093
11001022	1093
11001112	1093
11001211	2186
11002012	1093
11002022	1093
11002121	2186
11002202	1093
11010001	2186
11010022	1093
11010121	2186
11010221	2186
11011111	2186
11011202	1093
11012002	1093
11012102	1093
11012212	1093
11020021	2186
11020022	1093
11020102	1093
11020112	1093
11020201	2186
11020222	1093
11021111	2186
11021122	1093
11021201	2186
11021212	1093
11022101	2186
11022122	1093
11022211	2186
11022221	2186
11100002	1093
11100022	1093
11100121	2186
11100212	1093
11101012	1093
11101022	1093
11101102	1093
11101111	2186
11101121	2186
11102002	1093
11102111	2186
11102222	1093
11110001	2186
11110012	1093
11110111	2186
11110112	1093
11110211	2186
11110222	1093
11111011	2186
11111021	2186
11111201	2186
11111222	1093
11112011	2186
11112221	2186
11120102	1093
11120111	2186
11120122	1093
11120212	1093
11120221	2186
11121001	2186
11121101	2186
11121202	1093
11122021	2186
11122112	1093
11122201	2186
11122222	1093
11200201	2186
11200202	1093
11201012	1093
11201021	2186
11201101	2186
11201111	2186
11201221	2186
11201222	1093
11202002	1093
11202121	2186
11202211	2186
11202212	1093
11210002	1093
11210011	2186
11210021	2186
11210101	2186
11211001	2186
11211022	1093
11211122	1093
11211212	1093
11211221	2186
11212012	1093
11212112	1093
11212202	1093
11220001	2186
11220112	1093
11220211	2186
11221022	1093
11221102	1093
11221112	1093
11221121	2186
11222011	2186
11222102	1093
11222122	1093
11222201	2186
11222221	2186
12000121	2186
12000202	1093
12001021	2186
12001112	1093
12001211	2186
12002011	2186
12002021	2186
12002101	2186
12002222	1093
12010021	2186
12010022	1093
12010102	1093
12010121	2186
12010201	2186
12010211	2186
12011102	1093
12011111	2186
12011212	1093
12011221	2186
12012112	1093
12012122	1093

Неприводимые многочлены по модулю 3

12012202	1093	12101201	2186	12112211	2186	12201121	2186	12212122	1093
12012221	2186	12101212	1093	12120002	1093	12201122	1093	12212201	2186
12020002	1093	12101222	1093	12120011	2186	12201202	1093	12212221	2186
12020021	2186	12102001	2186	12120112	1093	12201212	1093	12220001	2186
12020122	1093	12102121	2186	12120121	2186	12202001	2186	12220012	1093
12020222	1093	12102212	1093	12120211	2186	12202111	2186	12220022	1093
12021101	2186	12110111	2186	12120212	1093	12202112	1093	12220202	1093
12021212	1093	12110122	1093	12121012	1093	12202222	1093	12221002	1093
12022001	2186	12110201	2186	12121022	1093	12210002	1093	12221021	2186
12022111	2186	12110212	1093	12121102	1093	12210112	1093	12221111	2186
12022201	2186	12110221	2186	12121121	2186	12210211	2186	12221122	1093
12100001	2186	12111002	1093	12122012	1093	12211021	2186	12221221	2186
12100021	2186	12111101	2186	12122122	1093	12211201	2186	12222011	2186
12100111	2186	12111202	1093	12200101	2186	12211211	2186	12222101	2186
12100222	1093	12112022	1093	12200102	1093	12211222	1093	12222211	2186
12101011	2186	12112102	1093	12201011	2186	12212012	1093		
12101021	2186	12112121	2186	12201022	1093	12212102	1093		

Неприводимые многочлены по модулю 5

$n = 1$	e
10	1
11	2
12	4
13	4
14	1

$n = 2$	e
102	8
103	8
111	3
112	24
123	24
124	12
133	24
134	12
141	6
142	24

$n = 3$	e
1011	62
1014	31
1021	62
1024	31
1032	124
1033	124
1042	124
1043	124
1101	62
1102	124
1113	124
1114	31
1131	62
1134	31
1141	62
1143	124
1201	62
1203	124
1213	124
1214	31
1222	124
1223	124
1242	124
1244	31
1302	124
1304	31
1311	62
1312	124
1322	124
1323	124
1341	62
1343	124
1403	124
1404	31
1411	62
1412	124
1431	62
1434	31
1442	124
1444	31

$n = 4$	e
10002	16
10003	16
10014	312
10024	312
10034	312
10044	312
10102	48
10111	78
10122	624
10123	624
10132	624
10133	624
10141	39
10203	48
10221	39
10223	208
10231	78
10233	208
10303	48
10311	156
10313	208
10341	156
10343	208
10402	48
10412	624
10413	624
10421	156
10431	156
10442	624
10443	624
11004	312
11013	624
11023	624
11024	104
11032	624
11041	52
11042	624
11101	78
11113	624
11114	312
11124	104
11133	208
11142	208
11202	624
11212	624
11213	208
11221	156
11222	208
11234	104
11244	312
11301	156
11303	624
11321	39
11342	624
11344	312
11402	208
11411	13
11414	312
11441	52
11443	624
12004	312
12013	624
12014	104
12021	26
12022	624
12033	624
12042	624
12102	208
12121	13
12123	624
12131	52
12134	312
12201	39
12203	624
12211	156
12222	624
12224	312
12302	624
12311	39
12312	208
12324	312
12332	624
12333	208
12344	104
12401	156
12414	104
12422	208
12433	624
12434	312
12443	208
13004	312
13012	624
13023	624
13031	13
13032	624
13043	624
13044	104
13102	208
13121	52
13124	312
13131	26
13133	624
13201	78
13203	624
13232	624
13234	312
13241	156
13302	624
13314	104
13322	624
13323	208
13334	312
13341	78
13342	208
13401	156
13413	208
13423	624
13424	312
13432	208
13444	104
14004	312
14011	52
14012	624
14022	624
14033	624
14034	104
14043	624
14101	39
14112	208
14123	208

14134	104	101033	284	103014	781	110123	3124	112034	781	114014	781
14143	624	101103	3124	103022	3124	110131	1562	112104	781	114024	781
14144	312	101104	781	103023	3124	110142	3124	112113	3124	114033	3124
14202	624	101141	1562	103101	1562	110144	781	112133	3124	114044	781
14214	312	101142	3124	103104	781	110202	284	112142	3124	114102	3124
14224	104	101203	3124	103111	1562	110213	3124	112143	284	114132	3124
14231	156	101204	781	103112	3124	110232	3124	112201	1562	114141	1562
14232	208	101212	3124	103143	3124	110243	3124	112212	3124	114201	1562
14242	624	101213	284	103144	71	110244	781	112214	781	114204	71
14243	208	101301	1562	103211	1562	110301	1562	112234	781	114233	3124
14301	156	101302	3124	103212	3124	110303	3124	112241	1562	114242	3124
14303	624	101312	284	103221	1562	110322	3124	112243	3124	114314	781
14312	624	101313	3124	103223	3124	110331	1562	112301	1562	114321	1562
14314	312	101401	1562	103232	3124	110333	3124	112311	1562	114322	3124
14331	78	101402	3124	103233	3124	110343	3124	112313	3124	114331	1562
14402	208	101443	3124	103313	3124	110403	3124	112314	781	114343	3124
14411	52	101444	781	103314	781	110411	1562	112323	3124	114401	1562
14413	624	102001	1562	103322	3124	110421	1562	112334	71	114403	3124
14441	26	102004	781	103324	781	110432	3124	112342	3124	114424	781
14444	312	102012	3124	103332	3124	110441	1562	112422	3124	114431	22
		102013	3124	103333	3124	110442	3124	112433	3124	114434	781
$n = 5$	e	102021	1562	103401	1562	110444	781	112441	1562	114442	3124
		102024	781	103404	781	111003	284	113002	3124	120003	3124
100041	1562	102112	3124	103413	3124	111013	3124	113004	781	120013	3124
100042	3124	102114	781	103414	781	111021	1562	113034	781	120042	3124
100043	3124	102121	1562	103441	142	111022	3124	113044	781	120104	71
100044	781	102122	3124	103442	3124	111024	781	113103	3124	120111	1562
100102	3124	102131	1562	104021	1562	111032	3124	113111	1562	120134	781
100114	781	102134	781	104024	781	111044	781	113134	781	120141	1562
100124	71	102202	3124	104031	142	111102	3124	113142	284	120143	3124
100132	3124	102203	3124	104034	71	111114	781	113143	3124	120201	1562
100143	3124	102211	1562	104101	1562	111123	3124	113211	1562	120212	3124
100201	1562	102213	3124	104103	3124	111212	44	113222	3124	120222	3124
100212	3124	102242	284	104111	142	111224	781	113224	71	120234	781
100222	284	102244	781	104114	781	111231	1562	113231	1562	120242	3124
100231	1562	102302	3124	104202	3124	111234	781	113241	1562	120243	3124
100244	781	102303	3124	104204	781	111301	1562	113243	284	120244	781
100304	781	102312	3124	104241	1562	111311	1562	113304	781	120321	1562
100313	3124	102314	781	104243	3124	111312	3124	113312	3124	120332	3124
100323	284	102341	1562	104301	1562	111324	71	113321	1562	120343	3124
100334	781	102343	284	104303	3124	111334	781	113323	3124	120344	781
100341	1562	102411	1562	104342	3124	111401	142	113324	781	120401	1562
100403	3124	102413	3124	104344	781	111404	781	113332	3124	120402	3124
100411	1562	102423	3124	104402	3124	111423	3124	113342	3124	120424	781
100421	142	102424	781	104404	781	111431	1562	113412	3124	120431	1562
100433	3124	102431	1562	104411	1562	111433	3124	113422	3124	120432	3124
100442	3124	102434	781	104414	71	111442	3124	113434	781	120441	1562
101022	3124	103002	3124	110004	781	112012	3124	114001	1562	121002	3124
101023	3124	103003	3124	110014	781	112023	3124	114011	1562	121012	3124
101032	284	103011	1562	110041	1562	112032	3124	114012	3124	121013	3124

121014	781	123034	781	130103	3124	132042	3124	134022	3124	141023	3124
121023	3124	123102	3124	130104	781	132102	3124	134023	3124	141024	781
121031	1562	123113	3124	130121	1562	132111	1562	134031	1562	141033	3124
121043	3124	123114	781	130133	3124	132122	3124	134042	3124	141041	1562
121102	3124	123133	3124	130134	781	132123	3124	134103	3124	141101	1562
121103	284	123141	1562	130144	781	132124	781	134111	1562	141104	71
121131	1562	123142	3124	130224	781	132131	1562	134113	3124	141122	3124
121144	781	123224	781	130233	3124	132141	1562	134122	284	141132	3124
121201	1562	123231	1562	130241	1562	132204	781	134132	3124	141134	781
121202	3124	123242	3124	130242	3124	132213	3124	134201	1562	141143	3124
121223	3124	123303	3124	130304	781	132232	3124	134212	3124	141204	781
121232	44	123311	1562	130313	3124	132241	142	134224	781	141213	3124
121233	3124	123331	1562	130323	3124	132244	781	134302	3124	141214	781
121244	781	123341	142	130331	1562	132311	1562	134303	284	141221	142
121304	781	123344	781	130341	1562	132321	1562	134324	781	141231	1562
121334	781	123402	3124	130342	3124	132332	3124	134333	3124	141313	44
121342	3124	123411	1562	130343	3124	132413	3124	134334	781	141321	1562
121413	3124	123412	3124	130401	142	132421	1562	134341	1562	141331	1562
121422	3124	123413	3124	130414	781	132422	284	134411	22	141334	781
121424	781	123421	1562	130431	1562	132433	3124	134422	3124	141403	3124
121432	3124	123433	284	130442	3124	132443	3124	134432	3124	141411	1562
121441	1562	123444	781	130444	781	132444	71	134433	3124	141422	3124
122003	3124	124001	142	131003	3124	133011	1562	140001	1562	142013	3124
122004	781	124011	1562	131011	1562	133024	781	140011	1562	142022	3124
122033	3124	124022	3124	131012	3124	133031	1562	140044	781	142031	1562
122043	3124	124023	3124	131013	3124	133032	3124	140102	3124	142033	3124
122112	3124	124024	781	131022	3124	133103	3124	140114	781	142123	3124
122123	284	124034	781	131034	781	133112	3124	140124	781	142132	3124
122124	781	124043	3124	131042	3124	133113	3124	140133	3124	142144	781
122132	3124	124114	11	131112	3124	133114	781	140141	1562	142204	781
122141	142	124123	3124	131121	1562	133124	781	140143	3124	142211	1562
122142	3124	124132	3124	131123	3124	133132	284	140144	781	142212	3124
122214	781	124133	3124	131133	3124	133141	1562	140202	3124	142214	781
122224	781	124202	284	131144	781	133202	3124	140204	781	142222	3124
122233	3124	124203	3124	131201	1562	133214	781	140223	3124	142231	142
122301	1562	124221	1562	131231	1562	133234	781	140232	3124	142243	3124
122312	3124	124231	1562	131243	3124	133241	1562	140234	781	142304	781
122333	3124	124232	3124	131303	3124	133244	71	140242	3124	142311	1562
122341	1562	124244	781	131304	781	133321	1562	140303	284	142313	3124
122344	71	124304	781	131322	3124	133334	781	140312	3124	142331	1562
122403	3124	124313	3124	131332	3124	133343	3124	140333	3124	142342	3124
122414	781	124321	1562	131333	44	133403	3124	140341	1562	142344	781
122421	1562	124402	3124	131341	1562	133411	1562	140342	3124	142401	1562
122422	3124	124412	3124	131402	284	133412	3124	140422	3124	142412	3124
122423	3124	124414	781	131403	3124	133432	3124	140434	781	142432	3124
122434	781	124423	284	131434	781	133443	3124	140441	1562	142442	284
122444	781	124433	3124	131441	1562	133444	781	140443	3124	142443	3124
123014	781	130002	3124	132001	1562	134004	71	141002	284	143001	1562
123021	1562	130012	3124	132002	3124	134014	781	141012	3124	143003	3124
123033	3124	130043	3124	132032	3124	134021	1562	141021	1562	143031	1562

Неприводимые многочлены по модулю 5

143041	1562	143224	781	143344	781	144013	3124	144131	1562	144301	142
143113	3124	143233	3124	143402	3124	144014	781	144134	11	144304	781
143123	3124	143243	3124	143414	781	144021	1562	144143	3124	144332	3124
143131	1562	143314	781	143431	1562	144032	3124	144211	1562	144343	3124
143201	1562	143321	142	143442	3124	144041	1562	144223	3124	144403	3124
143213	3124	143323	3124	143443	284	144102	3124	144224	781	144433	3124
143221	1562	143334	781	144004	781	144104	781	144234	781	144444	781
143222	3124	143342	284	144011	1562	144121	1562	144242	3124		

Неприводимые многочлены по модулю 7

$n=1$	e	1021	38	1304	342	1552	342	10135	2400	10524	1200
		1026	19	1306	57	1556	57	10145	2400	10525	2400
10	1	1032	342	1311	38	1563	171	10151	200	10531	80
11	2	1035	171	1314	342	1564	342	10161	400	10533	2400
12	6	1041	114	1322	342	1565	171	10162	600	10536	800
13	3	1046	57	1325	171	1566	57	10203	96	10541	80
14	6	1052	342	1333	171	1604	342	10205	96	10543	2400
15	3	1055	171	1334	342	1606	57	10211	200	10546	800
16	1	1062	342	1335	171	1612	342	10214	1200	10554	1200
		1065	171	1336	19	1615	171	10224	600	10555	2400
$n=2$	e	1101	114	1341	38	1621	114	10236	800	10565	2400
		1103	171	1343	171	1623	171	10246	800	10603	96
101	4	1112	342	1352	342	1632	342	10254	600	10606	32
102	12	1115	171	1354	342	1636	19	10261	200	10613	2400
104	12	1124	342	1362	342	1641	114	10264	1200	10621	400
113	48	1126	57	1366	57	1644	342	10305	96	10623	2400
114	24	1131	38	1401	114	1653	171	10306	32	10632	240
116	16	1135	171	1403	171	1654	342	10316	800	10635	2400
122	24	1143	171	1413	171	1655	171	10322	1200	10636	800
123	48	1146	57	1416	19	1656	57	10326	800	10642	240
125	48	1151	114	1422	342	1662	342	10333	2400	10645	2400
131	8	1152	342	1425	171	1664	342	10334	240	10646	800
135	48	1153	171	1431	38			10335	2400	10651	400
136	16	1154	342	1432	342	$n=4$	e	10343	2400	10653	2400
141	8	1163	171	1433	171			10344	240	10663	2400
145	48	1165	171	1434	342	10011	400	10345	2400	11001	400
146	16	1201	38	1444	342	10012	1200	10352	1200	11003	480
152	24	1203	171	1446	19	10014	1200	10356	800	11013	2400
153	48	1214	342	1453	171	10023	480	10366	800	11026	800
155	48	1216	57	1455	171	10025	480	10405	96	11031	400
163	48	1223	171	1461	114	10026	160	10406	32	11042	75
164	24	1226	57	1465	171	10053	480	10412	1200	11054	300
166	16	1233	171	1504	342	10055	480	10414	600	11056	800
		1235	171	1506	19	10056	160	10422	600	11062	1200
$n=3$	e	1242	342	1511	114	10061	400	10433	2400	11063	2400
		1245	171	1513	171	10062	1200	10443	2400	11101	400
1002	18	1251	114	1521	114	10064	1200	10452	600	11103	2400
1003	9	1255	171	1524	342	10103	96	10462	1200	11105	2400
1004	18	1261	114	1532	342	10106	32	10464	600	11111	5
1005	9	1262	342	1534	342	10111	400	10503	96	11112	1200
1011	114	1263	171	1542	342	10112	600	10505	96	11124	75
1016	57	1264	342	1545	171	10121	200	10515	2400	11134	240

11136	800	11556	800	12266	800	12665	480	13432	1200	14125	2400
11141	400	11562	1200	12303	2400	13004	1200	13434	1200	14132	1200
11152	1200	11566	160	12304	240	13005	480	13436	800	14145	2400
11153	2400	11602	240	12311	200	13011	400	13441	20	14156	800
11161	100	11605	2400	12323	2400	13015	2400	13443	2400	14165	2400
11163	480	11614	600	12325	2400	13022	300	13445	2400	14204	1200
11166	800	11625	2400	12332	120	13023	2400	13455	2400	14205	2400
11201	200	11626	800	12345	480	13031	50	13456	800	14206	800
11204	600	11631	40	12346	800	13044	1200	13465	2400	14211	400
11213	2400	11643	2400	12351	100	13053	2400	13501	80	14214	15
11223	2400	11646	160	12354	600	13065	2400	13506	800	14222	75
11225	2400	11652	600	12356	800	13103	2400	13512	600	14232	240
11232	60	11653	2400	12361	200	13106	800	13513	2400	14233	2400
11233	2400	11654	300	12363	2400	13115	2400	13516	800	14244	1200
11236	800	11664	600	12365	2400	13126	800	13521	200	14251	400
11241	400	11665	2400	12402	1200	13135	2400	13522	300	14255	2400
11244	1200	11666	800	12403	2400	13142	1200	13525	2400	14263	2400
11245	2400	12002	1200	12406	800	13151	400	13533	480	14264	300
11252	240	12006	160	12412	15	13155	2400	13535	2400	14265	480
11254	300	12016	800	12414	1200	13161	400	13544	120	14302	1200
11266	160	12025	2400	12421	25	13166	160	13553	2400	14314	150
11321	200	12032	1200	12431	80	13204	1200	13556	800	14325	2400
11323	2400	12044	75	12435	2400	13205	2400	13562	600	14335	2400
11324	150	12051	100	12442	1200	13206	800	13611	40	14341	25
11331	400	12055	2400	12454	1200	13213	2400	13612	1200	14346	800
11332	300	12064	1200	12456	800	13214	300	13616	800	14353	2400
11334	600	12066	800	12462	300	13215	480	13623	480	14354	1200
11351	200	12101	200	12465	2400	13221	400	13624	600	14361	400
11355	2400	12102	600	12466	160	13225	2400	13626	800	14363	480
11356	160	12116	800	12521	50	13234	1200	13641	100	14402	600
11362	120	12123	2400	12522	600	13242	240	13642	600	14404	600
11364	1200	12126	800	12526	800	13243	2400	13644	1200	14415	2400
11365	2400	12134	60	12531	200	13252	150	13652	75	14425	2400
11405	2400	12135	2400	12532	1200	13261	400	13654	600	14426	800
11406	800	12136	800	12534	300	13264	30	13655	2400	14431	20
11412	1200	12141	400	12552	600	13302	1200	14004	1200	14433	2400
11415	480	12142	1200	12553	2400	13311	400	14005	480	14435	2400
11422	1200	12143	2400	12555	480	13313	480	14015	2400	14442	1200
11423	2400	12151	100	12561	400	13323	2400	14023	2400	14444	1200
11434	1200	12154	240	12563	2400	13324	1200	14034	1200	14446	800
11443	2400	12165	480	12564	120	13331	50	14041	25	14451	80
11455	2400	12203	2400	12601	400	13336	800	14052	300	14452	300
11463	2400	12205	2400	12612	150	13345	2400	14053	2400	14463	480
11504	1200	12213	480	12626	800	13355	2400	14061	400	14501	80
11511	50	12214	1200	12636	800	13364	75	14065	2400	14506	800
11523	2400	12224	1200	12643	2400	13402	600	14103	2400	14512	600
11533	2400	12226	800	12644	75	13404	600	14106	800	14523	2400
11542	75	12231	400	12652	1200	13413	480	14111	400	14526	800
11545	2400	12246	800	12655	2400	13421	80	14116	160	14534	120
11551	400	12253	2400	12664	1200	13422	300	14121	400	14543	480

14545	2400	15121	100	15353	2400	15622	1200	16204	600	**16453**	**2400**
14551	200	15124	240	15355	2400	15625	2400	16216	160	**16462**	**1200**
14552	300	15131	400	15361	200	15633	2400	16222	240	**16465**	**480**
14555	2400	15132	1200	15402	1200	15634	150	16224	300	**16504**	**1200**
14562	600	15133	2400	15403	2400	15646	800	16231	400	**16512**	**1200**
14563	2400	15144	60	15406	800	15656	800	16234	1200	**16516**	**160**
14566	800	15145	2400	15412	300	15662	75	16235	2400	**16521**	**400**
14622	150	15146	800	15415	2400	16001	400	16242	60	**16526**	**800**
14624	600	15153	2400	15416	160	16003	480	16243	2400	**16532**	**150**
14625	2400	15156	800	15424	1200	16012	1200	16246	800	**16535**	**2400**
14631	100	15166	800	15426	800	16013	2400	16253	2400	**16543**	**2400**
14632	600	15203	2400	15432	1200	16024	300	16255	2400	**16553**	**2400**
14634	1200	15205	2400	15441	80	16026	800	16263	2400	**16561**	**25**
14653	480	15216	800	15445	2400	16032	150	16312	120	**16602**	**240**
14654	600	15223	2400	15451	50	16041	400	16314	1200	**16605**	**2400**
14656	800	15236	800	15462	30	16056	800	16315	2400	**16614**	**600**
14661	40	15241	400	15464	1200	16063	2400	16321	200	**16615**	**2400**
14662	1200	15254	1200	15511	400	16101	400	16325	2400	**16616**	**800**
14666	800	15256	800	15513	2400	16103	2400	16326	160	**16622**	**600**
15002	1200	15263	480	15514	120	16105	2400	16341	400	**16623**	**2400**
15006	160	15264	1200	15522	600	16111	100	16342	300	**16624**	**300**
15014	1200	15303	2400	15523	2400	16113	480	16344	600	**16633**	**2400**
15016	800	15304	240	15525	480	16116	800	16351	200	**16636**	**160**
15021	100	15311	200	15541	200	16122	1200	16353	2400	**16641**	**40**
15025	2400	15313	2400	15542	1200	16123	2400	16354	75	**16655**	**2400**
15034	150	15315	2400	15544	300	16131	400	16405	2400	**16656**	**800**
15042	1200	15321	100	15551	25	16144	240	16406	800	**16664**	**600**
15055	2400	15324	600	15552	600	16146	800	16413	2400		
15066	800	15326	800	15556	800	16154	150	16425	2400		
15101	200	15335	480	15601	400	16161	10	16433	2400		
15102	600	15336	800	15614	1200	16162	1200	16444	1200		
15115	480	15342	120	15615	480	16201	200	16452	1200		

ТАБЛИЦА D

1	0					
2	1	0				
3	1	0				
4	1	0				
5	2	0				
6	1	0				
7	1	0				
8	4	3	2	0		
9	4	0				
10	3	0				
11	2	0				
12	6	4	1	0		
13	4	3	1	0		
14	5	3	1	0		
15	1	0				
16	5	3	2	0		
17	3	0				
18	5	2	1	0		
19	5	2	1	0		
20	3	0				
21	2	0				
22	1	0				
23	5	0				
24	4	3	1	0		
25	3	0				
26	6	2	1	0		
27	5	2	1	0		
28	3	0				
29	2	0				
30	6	4	1	0		
31	3	0				
32	7	5	3	2	1	0
33	6	4	1	0		
34	7	6	5	2	1	0
35	2	0				
36	6	5	4	2	1	0
37	5	4	3	2	1	0
38	6	5	1	0		
39	4	0				
40	5	4	3	0		
41	3	0				
42	5	4	3	2	1	0
43	6	4	3	0		
44	6	5	2	0		
45	4	3	1	0		
46	8	5	3	2	1	0
47	5	0				
48	7	5	4	2	1	0
49	6	5	4	0		
50	4	3	2	0		
51	6	3	1	0		
52	3	0				
53	6	2	1	0		
54	6	5	4	3	2	0
55	6	2	1	0		
56	7	4	2	0		
57	5	3	2	0		
58	6	5	1	0		
59	6	5	4	3	1	0
60	1	0				
61	5	2	1	0		
62	6	5	3	0		
63	1	0				
64	4	3	1	0		
65	4	3	1	0		
66	8	6	5	3	2	0
67	5	2	1	0		
68	7	5	1	0		
69	6	5	2	0		
70	5	3	1	0		
71	5	3	1	0		
72	6	4	3	2	1	0
73	4	3	2	0		
74	7	4	3	0		
75	6	3	1	0		
76	5	4	2	0		
77	6	5	2	0		
78	7	2	1	0		
79	4	3	2	0		
80	7	5	3	2	1	0
81	4	0				
82	8	7	6	4	1	0
83	7	4	2	0		
84	8	7	5	3	1	0
85	8	2	1	0		
86	6	5	2	0		
87	7	5	1	0		
88	8	5	4	3	1	0
89	6	5	3	0		
90	5	3	2	0		
91	7	6	5	3	2	0
92	6	5	2	0		
93	2	0				
94	6	5	1	0		
95	6	5	4	2	1	0
96	7	6	4	3	2	0
97	6	0				
98	7	4	3	2	1	0
99	7	5	4	0		
100	8	7	2	0		

ТАБЛИЦА Е

$p = 11$ $n = 2$ $q = 121$ $120 = 2^3 \cdot 3 \cdot 5$ $\varphi(120)/2 = 16$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
4	2	2	6	1	7	1	8
5	2	3	6	4	7	3	8
6	2	8	6	7	7	8	8
7	2	9	6	10	7	10	8

$p = 13$ $n = 2$ $q = 169$ $168 = 2^3 \cdot 3 \cdot 7$ $\varphi(168)/2 = 24$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
1	2	2	6	2	7	4	11
4	2	3	6	3	7	5	11
6	2	4	6	6	7	6	11
7	2	9	6	7	7	7	11
9	2	10	6	10	7	8	11
12	2	11	6	11	7	9	11

$p = 17$ $n = 2$ $q = 289$ $288 = 2^5 \cdot 3^2$ $\varphi(288)/2 = 48$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
1	3	2	6	1	10	2	12
6	3	6	6	3	10	3	12
7	3	8	6	4	10	5	12
10	3	9	6	13	10	12	12
11	3	11	6	14	10	14	12
16	3	15	6	16	10	15	12
3	5	1	7	2	11	4	14
5	5	4	7	7	11	6	14
8	5	5	7	8	11	7	14
9	5	12	7	9	11	10	14
12	5	13	7	10	11	11	14
14	5	16	7	15	11	13	14

$p = 19$ $n = 2$ $q = 361$ $360 = 2^3 \cdot 3^2 \cdot 5$ $\varphi(360)/2 = 48$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
1	2	10	3	3	13	11	14
4	2	11	3	4	13	12	14
7	2	12	3	6	13	13	14
8	2	18	3	9	13	18	14
11	2	2	10	10	13	4	15
12	2	4	10	13	13	5	15
15	2	6	10	15	13	6	15
18	2	9	10	16	13	9	15
1	3	10	10	1	14	10	15
7	3	13	10	6	14	13	15
8	3	15	10	7	14	14	15
9	3	17	10	8	14	15	15

$p = 23$ $n = 2$ $q = 529$ $528 = 2^4 \cdot 3 \cdot 11$ $\varphi(528)/2 = 80$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
2	5	2	10	1	14	3	17	4	20
4	5	3	10	3	14	4	17	7	20
5	5	6	10	5	14	6	17	8	20
8	5	10	10	10	14	11	17	10	20
15	5	13	10	13	14	12	17	13	20
18	5	17	10	18	14	17	17	15	20

$p = 23$ $n = 2$ $q = 529$ $528 = 2^4 \cdot 3 \cdot 11$ $\varphi(528)/2 = 80$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
19	5	20	10	20	14	19	17	16	20
21	5	21	10	22	14	20	17	19	20
1	7	3	11	5	15	1	19	5	21
2	7	7	11	9	15	2	19	6	21
4	7	8	11	10	15	7	19	7	21
9	7	9	11	11	15	11	19	9	21
14	7	14	11	12	15	12	19	14	21
19	7	15	11	13	15	16	19	16	21
21	7	16	11	14	15	21	19	17	21
22	7	20	11	18	15	22	19	18	21

$p = 29$ $n = 2$ $q = 841$ $840 = 2^3 \cdot 3 \cdot 5 \cdot 7$ $\varphi(840)/2 = 96$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
5	2	1	8	6	11	7	15	2	19	5	26
7	2	7	8	9	11	9	15	4	19	6	26
11	2	10	8	10	11	11	15	7	19	8	26
14	2	14	8	11	11	12	15	8	19	12	26
15	2	15	8	18	11	17	15	21	19	17	26
18	2	19	8	19	11	18	15	22	19	21	26
22	2	22	8	20	11	20	15	25	19	23	26
24	2	28	8	23	11	22	15	27	19	24	26
1	3	3	10	1	14	4	18	3	21	2	27
2	3	5	10	3	14	8	18	4	21	3	27
9	3	9	10	8	14	13	18	6	21	6	27
14	3	10	10	13	14	14	18	12	21	13	27
15	3	19	10	16	14	15	18	17	21	16	27
20	3	20	10	21	14	16	18	23	21	23	27
27	3	24	10	26	14	21	18	25	21	26	27
28	3	26	10	28	14	25	18	26	21	27	27

$p = 31$ $n = 2$ $q = 961$ $960 = 2^6 \cdot 3 \cdot 5$ $\varphi(960)/2 = 128$

a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
2	3	2	11	1	12	1	13	1	17	2	21	1	22	1	24
5	3	3	11	3	12	4	13	2	17	5	21	4	22	3	24
6	3	4	11	4	12	6	13	3	17	7	21	5	22	4	24
7	3	5	11	10	12	8	13	6	17	8	21	7	22	5	24
8	3	6	11	11	12	9	13	7	17	11	21	9	22	7	24
10	3	9	11	12	12	10	13	8	17	12	21	10	22	8	24
14	3	11	11	14	12	12	13	9	17	13	21	14	22	12	24
15	3	15	11	15	12	13	13	11	17	15	21	15	22	13	24
16	3	16	11	16	12	18	13	20	17	16	21	16	22	18	24
17	3	20	11	17	12	19	13	22	17	18	21	17	22	19	24
21	3	22	11	19	12	21	13	23	17	19	21	21	22	23	24
23	3	25	11	20	12	22	13	24	17	20	21	22	22	24	24
24	3	26	11	21	12	23	13	25	17	23	21	24	22	26	24
25	3	27	11	27	12	25	13	28	17	24	21	26	22	27	24
26	3	28	11	28	12	27	13	29	17	26	21	27	22	28	24
29	3	29	11	30	12	30	13	30	17	29	21	30	22	30	24

ТАБЛИЦА F

p^n	$a_1a_2a_3\cdots a_n$	p^n	$a_1a_2a_3\cdots a_n$	p^n	$a_1a_2\cdots a_{n-1}a_n$
2^2	11	5^2	12	19^2	1 2
2^3	101	5^3	102	19^3	10 16
2^4	1001	5^4	1013	19^4	100 2
2^5	01001	5^5	00102	19^5	0001 16
2^6	100001	5^6	100002	19^6	00001 3
2^7	0000011	5^7	1000002	19^7	010000 9
2^8	11000011	5^8	00101003		
2^9	000100001	5^9	011000003	23^2	1 7
2^{10}	0010000001	5^{10}	1010000003	23^3	10 16
2^{11}	01000000001	5^{11}	10000000002	23^4	001 11
2^{12}	110000010001	5^{12}	000010010003	23^5	1000 18
2^{13}	1100100000001			23^6	10000 7
2^{14}	11000000000101				
2^{15}	100000000000001	7^2	13	29^2	1 3
2^{16}	1010000000010001	7^3	112	29^3	01 18
2^{17}	00100000000000001	7^4	1103	29^4	100 2
2^{18}	00000010000000001	7^5	10004	29^5	0100 26
2^{19}	1100100000000000001	7^6	110003	29^6	00001 3
2^{20}	0010000000000000001	7^7	0100004		
2^{21}	01000000000000000001	7^8	10000003		
2^{22}	100000000000000000001	7^9	100001002	31^2	1 12
2^{23}	000010000000000000001	7^{10}	1100000003	31^3	01 28
2^{24}	110000100000000000001			31^4	100 13
2^{25}	001000000000000000000001			31^5	0100 20
2^{26}	110001000000000000000001	11^2	17	31^6	10000 12
2^{27}	110010000000000000000001	11^3	105		
2^{28}	001000000000000000000000001	11^4	0012		
2^{29}	010000000000000000000000001	11^5	01109	37^2	1 5
		11^6	100017	37^3	10 24
		11^7	1000005	37^4	001 2
		11^8	00010012	37^5	0001 32
3^2	12				
3^3	201				
3^4	1002	13^2	1 2	41^2	1 12
3^5	10101	13^3	10 7	41^3	01 35
3^6	100002	13^4	101 2	41^4	001 17
3^7	1010001	13^5	0101 11	41^5	1000 35
3^8	00100002	13^6	10100 6		
3^9	010100001	13^7	001000 6	43^2	1 3
3^{10}	1010000002	13^8	0110000 2	43^3	01 40
3^{11}	10000010001			43^4	001 20
3^{12}	100010000002			43^5	1000 40
3^{13}	1000001000001	17^2	1 3		
3^{14}	10000000000002	17^3	01 14		
3^{15}	100000000010001	17^4	100 5	47^2	1 13
3^{16}	00000010000000002	17^5	1000 14	47^3	10 42
3^{17}	10000001000000001	17^6	10000 3	47^4	100 5
3^{18}	100000000000100002	17^7	000100 14	47^5	0001 42

Литература [1]

ABERTH O. [1] The elementary symmetric functions in a finite field of prime order, Illinois J. Math. **8**, 132—138 (1964).

ABRAMSON N. M. [1] Error-correcting codes from linear sequential circuits, Proc. Fourth London Symp. on Information Theory (C. Cherry, ed.), pp. 26—40, Butterworths, London, 1961.

[2] Information Theory and Coding, McGraw-Hill, New York, 1963.

ADLEMAN L. M. [1] On distinguishing prime numbers from composite numbers, Proc. 2lst Annual Symp. on Foundations of Computer Science (Syracuse, N. Y., 1980), pp. 387—406, IEEE Computer Society, Long Beach, Cal., 1980.

ADLEMAN L. M., MANDERS K., MILLER G. [1] On taking roots in finite fields, Proc. 18th Annual Symp. on Foundations of Computer Science (Providence, R. I., 1977), pp. 175—178, IEEE Computer Society, Long Beach, Cal., 1977.

ADLEMAN L. M., POMERANCE C., RUMELY R. S. [1] On distinguishing prime numbers from composite numbers, Ann. of Math. **117**, № 1, 173—206 (1983).

ADOLPHSON A., SPERBER S. [1] Exponential sums on the complement of a hypersurface, Amer. J. Math. **102**, 461—487 (1980).

AGARWAL R. C., BURRUS C. S. [1] Number theoretic transforms to implement fast digital convolution, Proc. IEEE **63**, 550—560 (1975).

AGOU S. [1] Sur la décomposition de certains idéaux premiers, Publ. Dép. Math. Lyon **7**, no. 1, 41—46 (1969).

[2] Formules explicites intervenant dans la division euclidienne des polynômes à coefficients dans un anneau unitaire et applications diverses, Publ. Dép. Math. Lyon **8**, no. 1, 107—121 (1971).

[3] Polynômes sur un corps fini, Bull. Sci. Math. (2) **95**, 327—330 (1971).

[4] Sur l'irréductibilité des polynômes à coefficients dans un corps fini, C. R. Acad. Sci. Paris Sér. A **272**, 576—577 (1971).

[5] Sur des formules explicites intervenant dans la division euclidiene des polynômes et leurs conséquences, C. R. Acad. Sci. Paris Sér. A 273, 209—211 (1971).

[6] Une démonstration de la loi de réciprocité quadratique, Publ. Dép. Math. Lyon **9**, no. 3, 55—57 (1972).

[7] Sur l'irréductibilité de certains polynômes à plusieurs indéterminées et à coefficients dans un corps fini, Publ. Dép. Math. Lyon **12**, no. 1, 5—12 (1975).

[8] Factorisation des polynômes à coefficients dans un corps fini, Publ. Dép. Math. Lyon **13**, no. 1, 63—71 (1976).

[9] Critères d'irréductibilité des polynômes composés à coefficients dans un corps fini, Acta Arith. **30**, 213—223 (1976).

[10] Factorisation sur un corps fini F_{p^n} des polynômes composés $f(X^s)$ lorsque $f(X)$ est un polynôme irréductible de $F_{p^n}[X]$, L'Enseignement Math. (2) **22**, 305—312 (1976).

[11] Factorisation sur un corps fini K des polynômes composés $f(X^s)$ lorsque $f(X)$ est un polynôme irréductible de $K[X]$, C. R. Acad. Sci. Paris Sér.

---

[1]) При переводе работы отечественных авторов вынесены в отдельный список; см. с. 790—798, 802—805. — *Прим. перев.*

A **282**, 1067—1068 (1976).

[12] Polynômes irréductibles primitifs à coefficients dans un corps fini, Publ. Dép. Math. Lyon **14**, no. 4, 17—20 (1977).

[13] Irréductibilité des polynômes $f\left(X^{p^n} - aX\right)$ sur un corps fini F_{p^s}, J. reine angew. Math. **292**, 191—195 (1977).

[14] Factorisation sur un corps fini F_{p^n} des polynômes composés $f\left(X^{p^r} - aX\right)$ lorsque $f(X)$ est un polynome irréductible de $F_{p^n}[X]$, J. Number Theory **9**, 229—239 (1977).

[15] Irréductibilité des polynômes $f\left(X^{p^{2r}} - aX^{p^r} - bX\right)$ sur un corps fini F_{p^s}, J. Number Theory **10**, 64—69 (1978).

[16] Irréductibilité des polynômes $f\left(X^{p^{2r}} - aX^{p^r} - bX\right)$ sur un corps fini F_{p^s}, J. Number Theory **11**, 20 (1979).

[17] Sur le degré minimum de certains polynômes hyponormaux sur un corps fini, Proc. Queen's Number Theory Conf. (Kingston, Ont., 1979), Queen's Papers in Pure and Appl. Math., no. 54, pp. 115—118, Queen's Univ., Kingston, Ont., 1980.

[18] Irréductibilité des polynômes $f\left(\sum_{i=0}^{m} a_i X^{p^{ri}}\right)$ sur un corps fini F_{p^s}, Canad. Math. Bull. **23**, 207—212 (1980).

[19] Sur la factorisation des polynômes $f\left(X^{p^{2r}} - aX^{p^r} - bX\right)$ sur un corps fini F_{p^s}, J. Number Theory **12**, 447—459 (1980).

[20] Sur une classe de polynômes hyponormaux sur un corps fini, Acta Arith. **39**, 105—111 (1981).

AHMAD S. [1] Cycle structure of automorphisms of finite cyclic groups, J. Combinatorial Theory **6**, 370—374 (1969).

[2] Split dilations of finite cyclic groups with applications to finite fields, Duke Math. J. **37**, 547—554 (1970).

AHO A. V., HOPCROFT J. E., ULLMAN J. D. [1] The Design and Analysis of Computer Algorithms, Addison-Wesley, Reading, Mass., 1975. [Имеется перевод: АХО А., ХОПКРОФТ ДЖ., УЛЬМАН ДЖ. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.]

AJTAI M. [1] Divisibility properties of recurring sequences, Compositio Math. **21**, 43—51 (1969).

AKHTAR S. [1] Values of symmetric functions, Panjab Univ. J. Math. (Lahore) **2**, 43—61 (1969).

ALANEN J. D., KNUTH D. E. [1] A table of minimum functions for generating Galois fields of $GF(p^n)$, Sankhya Ser. A **23**, 128 (1961).

[2] Tables of finite fields, Sankhya Ser. A **26**, 305—328 (1964).

ALBERT A. A. [1] Symmetric and alternate matrices in an arbitrary field, I, Trans. Amer. Math. Soc. **43**, 386—436 (1938).

[2] On nonassociative division algebras, Trans. Amer. Math. Soc. **72**, 296—309 (1952).

[3] Fundamental Concepts of Higher Algebra, Univ. of Chicago Press, Chicago, 1956. [Имеется перевод гл. 5 «Конечные поля»: В кн: Кибернетический сборник, нов. сер., вып. 3. — М.: Мир, 1966, с. 7—49.]

[4] On certain trinomial equations in finite fields, Ann. of Math. (2) **66**, 170—178 (1957).

[5] On certain polynomial systems, Scripta Math. **28**, 15—19 (1967).

ALBERT A. A., SANDLER R. [1] An Introduction to Finite Projective Planes, Holt, Rinehart and Winston, New York, 1968.

ALMKVIST G. [1] Invariants, mostly old ones, Pacific J. Math. **86**, 1—13 (1980).

ALTHAUS H. L., LEAKE R. J. [1] Inverse of a finite-field Vandermonde matrix, IEEE Trans. Information Theory **IT-15**, 173 (1969).

ANDERSON D. D. [1] Problem 6201, Amer. Math. Monthly **85**, 203 (1978); Solution, ibid. **86**, 869—870 (1979).
ANDERSON D. R., STIFFLER J. J. [1] Lower bounds for the maximum modulus of certain classes of trigonometric sums, Duke Math. J. **30**, 171—176 (1963).
ANDREE R. V. [1] A Table of Indices and Power Residues for all Primes and Prime Powers below 2000, W. W. Norton, New York, 1962.
ANDREWS G. E. [1] A note on the Bombieri—Selberg formula for algebraic curves, Portugal. Math. **27**, 75—81 (1968).
ANKENY N. C. [1] The least quadratic non-residue, Ann. of Math. (2) **55**, 65—72 (1952).
[2] Equations in finite fields, Proc. Nat. Acad. Sci. U. S. A. **40**, 1072—1073 (1954).
[3] Criterion for rth power residuacity, Pacific J. Math. **10**, 1115—1124 (1960).
ANKENY N. C., ERDÖS P. [1] The insolubility of classes of diophantine equations, Amer. J. Math. **76**, 488—496 (1954).
APOSTOL T. M. [1] Dirichlet L-functions and character power sums, J. Number Theory **2**, 223—234 (1970).
[2] Introduction to Analytic Number Theory, Springer-Verlag, New York—Heidelberg—Berlin, 1976.
ARAZI B. [1] Decimation of m-sequences leading to any desired phase shift, Electron. Lett. **13**, 213—215 (1977).
[2] On the synthesis of de Bruijn sequences, Information and Control **49**, 81—90 (1981).
ARBIB M. A., FALB P. L., KALMAN R. E. [1] Topics in Mathematical System Theory, McGraw-Hill, New York, 1969. [Имеется перевод: КАЛМАН Р., ФАЛБ П., АРБИБ М. Очерки по математической теории систем. — М.: Мир, 1971.]
ARF C. [1] Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (Teil I), J. reine angew. Math. **183**, 148—167 (1941).
ARGHIRIADE E., PETERFI I. [1] On matrices with elements from a finite field (Romanian), Lucrâr. Sti. Inst. Ped. Timisoara Mat.-Fiz. 1960, 19—23.
ARMITAGE J. V. [1] On the genus of curves over finite fields, Mathematika **9**, 115—117 (1962).
[2] The product of N linear forms in a field of series and the Riemann hypothesis for curves, Bull. Soc. Math. France Mém. **25**, pp. 17—27, Soc. Math. France, Paris, 1971.
ARNDT F. [1] Einfacher Beweis für die Irreduzibilität einer Gleichung in der Kreisteilung, J. reine angew. Math. **56**, 178—181 (1858).
ARNOUX G. [1] Arithmétique graphique. Introduction à l'étude des fonctions arithmétiques, Gauthier-Villars, Paris, 1906.
ARTIN E. [1] Quadratische Körper im Gebiet der höheren Kongruenzen, I, II, Math. Z. **19**, 153—206, 207—246 (1924).
[2] Uber einen Satz von Herrn J. H. Maclagan Wedderburn, Abh. Math. Sem. Univ. Hamburg **5**, 245—250 (1927).
[3] Linear mappings and the existence of a normal basis, Studies and Essays Presented to R. Courant on His 60th Birthday, pp. 1—5, Interscience, New York, 1948.
[4] The influence of J. H. M. Wedderburn on the development of modern algebra, Bull. Amer. Math. Soc. **56**, 65—72 (1950).
[5] The orders of the linear groups, Comm. Pure Appl. Math. **8**, 355—365 (1955).
[6] The orders of the classical simple groups, Comm. Pure Appl. Math. **8**, 455—472 (1955).
[7] Geometric Algebra, Interscience, New York, 1957. [Имеется перевод: АРТИН Э. Геометрическая алгебра. — М.: Наука, 1969.]
[8] Galois Theory, 2nd ed., Univ. of Notre Dame Press, South Bend, Ind., 1966. [Имеется перевод: АРТИН Э. Теория Галуа (укр.). — Киев: Радяньска школа, 1963.]

[9] Algebraic Numbers and Algebraic Functions, Gordon and Breach, New York, 1967.

ARWIN A. [1] Über das Auflösen der Kongruenzen von dem dritten und vierten Grade nach einem Primzahlmodulus, Lunds Univ. Årsskrift N. F. (Avd. 2) **12**, no. 3 (1915).

[2] Über Kongruenzen von dem fünften und höheren Graden nach einem Primzahlmodulus, Ark. Mat. Astron. Fys. **14**, no. 7 (1919).

ASH R. [1] Information Theory, Wiley-Interscience, New York, 1965.

ASSMUS E. F., Jr., MATTSON H. F., Jr. [1] On tactical configurations and error-correcting codes, J. Combinatorial Theory **2**, 243—257 (1967).

[2] Coding and combinatorics, SIAM Rev. **16**, 349—388 (1974).

AUSLANDER L., TOLIMIERI R. [1] Is computing with the finite Fourier transform pure or applied mathematics? Bull. Amer. Math. Soc. (N. S.) **1**, 847—897 (1979).

AX J. [1] Zeroes of polynomials over finite fields, Amer. J. Math. **86**, 255—261 (1964).

[2] Solving diophantine problems modulo every prime, Ann. of Math. (2) **85**, 161—183 (1967).

[3] The elementary theory of finite fields, Ann. of Math. (2) 88, 239—271 (1968).

AX J., KOCHEN S. [1] Diophantine problems over local fields. I, Amer. J. Math. 87, 605—630 (1965). [Имеется перевод: АКС ДЖ., КОХЕН С. Диофантовы проблемы над конечными полями. — Математика, т. 9, № 5 (1965), с. 3—26.]

AYOUB R. [1] An Introduction to the Analytic Theory of Numbers, American Math. Society, Providence, R. I., 1963.

BACHMANN P. [1] Die Lehre von der Kreistheilung, Teubner, Leipzig, 1872.

[2] Zahlentheorie, Band 2: Die analytische Zahlentheorie, Teubner, Leipzig, 1894.

[3] Die Arithmetik der quadratischen Formen, Teubner, Leipzig, 1898.

[4] Niedere Zahlentheorie, Erster Teil, Teubner, Leipzig, 1902.

[5] Niedere Zahlentheorie, Zweiter Teil, Teubner, Leipzig, 1910.

[6] Das Fermatproblem in seiner bisherigen Entwicklung, de Gruyter, Berlin, 1919; Springer-Verlag, Berlin—Heidelberg—New York, 1976.

BAER R. [1] Linear Algebra and Projective Geometry, Academic Press, New York, 1952. [Имеется перевод: БЭР Р. Линейная алгебра и проективная геометрия. — М.: ИЛ, 1955.]

BAJOGA B. G. [1] Generation of irreducible polynomials from trinomials over *GF* (2). II, Information and Control **37**, 5—18 (1978).

BAJOGA B. G., WALBESSER W. J. [1] Generation of irreducible polynomials from trinomials over *GF* (2), I, Information and Control **30**, 396—407 (1976).

BALAKRISHNAN A. V. [1] Communication Theory, McGraw-Hill, New York, 1968.

BALDISSERRI N. [1] Sul numero dei punti di cubiche ellittiche, a moltiplicazione complessa, ridotte modulo p, Boll. Un. Mat. Ital. (5) **16A**, 367—373 (1979).

BALL J. R., SPITTLE A. H., LIU H. T. [1] High-speed m-sequence generation: a further note, Electron. Lett. **11**, 107—108 (1975).

BALLIEU R. [1] Factorisation des polynômes cyclotomiques modulo un nombre premier, Ann. Soc. Sci. Bruxelles Sér. I **68**, 140—144 (1954).

BAMBAH R. P., CHOWLA S. [1] On the sign of the Gaussian sum, Proc. Nat. Inst. Sci. India Part A **13**, 175—176 (1947).

BARNER K. [1] Zur Fibonacci-Folge modulo p, Monatsh. Math. **69**, 97—104 (1965).

[2] Zur Reziprozität quadratischer Charaktersummen in algebraischen Zahlkörpern, Monatsh. Math. **71**, 369—384 (1967).

BARNETT S. [1] Greatest common divisor of several polynomials, Proc. Cambridge Philos. Soc. **70**, 263—268 (1971).

BARRUCAND P. [1] Sommes de Gauss et séries singulières de Hardy pour les cubes, C. R. Acad. Sci. Paris **250**, 4249—4251 (1960).

BARTEE T. C., SCHNEIDER D. I. [1] Computation with finite fields, Information and Control **6**, 79—98 (1963).

BATEMAN P. T., CHOWLA S., ERDÖS P. [1] Remarks on the size of $L(1, \chi)$, Publ. Math. Debrecen **1**, 165—182 (1950).

BATEMAN P. T., DUQUETTE A. L. [1] The analogue of the Pisot—Vijayaraghavan numbers in fields of formal power series, Illinois J. Math. **6**, 594—606 (1962).

BAUM L. E., HERZBERG N. P., LOMONACO S. J., Jr., SWEET M. M. [1] Fields of almost periodic sequences, J. Combinatorial Theory Ser. A **22**, 169—180 (1977).

BAUM L. E., NEUWIRTH L. P. [1] Decomposition of vector spaces over *GF* (2) into disjoint equidimensional affine spaces, J. Combinatorial Theory Ser. A **18**, 88—100 (1975).

BAUM L. E., SWEET M. M. [1] Continued fractions of algebraic power series in characteristic 2, Ann. of Math. (2) **103**, 593—610 (1976).

[2] Badly approximable power series in characteristic 2, Ann. of Math. (2) **105**, 573—580 (1977).

BAUMERT L. D. [1] Cyclic Difference Sets. Lecture Notes in Math., vol. **182**, Springer-Verlag, Berlin—Heidelberg—New York, 1971.

BAUMERT L. D., FREDRICKSEN H. [1] The cyclotomic numbers of order eighteen with applications to difference sets, Math. Comp. **21**, 204—219 (1967).

BAUMERT L. D., HALL M., Jr. [1] A new construction for Hadamard matrices, Bull. Amer. Math. Soc. **71**, 169—170 (1965).

BAUMERT L. D., MCELIECE R. J. [1] Weights of irreducible cyclic codes, Information and Control **20**, 158—175 (1972).

BAUMERT L. D., MILLS W. H., WARD R. L. [1] Uniform cyclotomy, J. Number Theory **14**, 67—82 (1982).

BAYER P., NEUKIRCH J. [1] On values of zeta functions and l-adic Euler characteristics, Invent. Math. **50**, 35—64 (1978).

BEARD J. T. B., Jr. [1] Matrix fields over prime fields, Duke Math. J. **39**, 313—321 (1972).

[2] Matrix fields over finite extensions of prime fields, Duke Math. J. **39**, 475—484 (1972).

[3] The number of matrix fields over *GF* (*q*), Acta Arith. **25**, 315—329 (1974).

[4] A rational canonical form for matrix fields, Acta Arith. **25**, 331—335 (1974).

[5] Computing in *GF* (*q*), Math. Comp. **28**, 1159—1166 (1974).

[6] Unitary perfect polynomials over *GF* (*q*), Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **62**, 417—422 (1977).

BEARD J. T. B., Jr., BULLOCK A. T., HARBIN M. S. [1] Infinitely many perfect and unitary perfect polynomials, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **63**, 294—303 (1977).

BEARD J. T. B., Jr., DOYLE J. K., MANDELBERG K. I. [1] Square-separable primes and unitary perfect polynomials, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **68**, 397—401 (1980).

BEARD J. T. B., Jr., HARBIN M. S. [1] Nonsplitting unitary perfect polynomials over *GF* (*q*). Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **66**, 179—185 (1979).

BEARD J. T. B., Jr., MCCONNEL R. [1] Matrix fields over the integers modulo m, Linear Algebra Appl. **14**, 95—105 (1976).

BEARD J. T. B., Jr., O'CONNELL J. R., Jr., WEST K. I. [1] Perfect polynomials over *GF* (*q*), Atti Accad. Nar. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **62**, 283—291 (1977).

BEARD J. T. B., Jr., WEST K. I. [1] Some primitive polynomials of the third kind, Math. Comp. **28**, 1166—1167 (1974).

[2] Factorization tables for $x^n - 1$ over $GF(q)$, Math. Comp **28**, 1167—1168 (1974).
[3] Factorization tables for trinomials over $GF(q)$, Math. Comp. **30**, 179—183 (1976).
BEDOCCHI E. [1] Cubiche ellittiche su F_p, Boll. Un. Mat. Ital. (5) **17B**, 269—277 (1980).
[2] Classi di isomorfismo delle cubiche di F_q, Rend. Circ. Mat. Palermo (2) **30**, 397—415 (1981).
BEEGER N. G. W. H. [1] Sur l'identité de M. G. Rados, Rend. Circ. Mat. Palermo **51**, 312—314 (1927).
BEKER H., PIPER F. C. [1] Shift register sequences, Combinatorics (Swansea, 1981), London Math. Soc. Lecture Note Series, no. 52, pp. 56—79, Cambridge Univ. Press, Cambridge, 1981.
[2] Cipher Systems. The Protection of Communications, Northwood Books, London, 1982.
BELEVITCH V. [1] Conference networks and Hadamard matrices, Ann. Soc. Sci. Bruxelles Sér. I **82**, 13—32 (1968).
BELL E. T. [1] Notes on recurring series of the third order, Tôhoku Math. J. **24**, 168—184 (1925).
BELLMAN R. [1] A note on the solution of polynomial congruences, Boll. Un. Mat. Ital. (3) **19**, 60—63 (1964).
BENJAUTHRIT B., REED I. S. [1] Galois switching functions and their applications, IEEE Trans. Computers **C-25**, 78—86 (1976).
[2] On the fundamental structure of Galois switching functions, IEEE Trans. Computers **C-27**, 757—762 (1978).
BERGER T. R., REUNER I. [1] A proof of the normal basis theorem, Amer. Math. Monthly **82**, 915—918 (1975).
BERGSTRÖM H. [1] Die Klassenzahlformel für reelle quadratische Zahlkörper mit zusammengesetzter Diskriminante als Produkt verallgemeinerter Gaußscher Summen, J. reine angew. Math. **186**, 91—115 (1944/45).
BERGUM G. E., JORDAN J. H. [1] The distribution of quadratic residues in fields of order p^2, Math. Mag. **45**, 194—200 (1972).
BERLEKAMP E. R. [1] On decoding binary Bose-Chaudhuri—Hocquenghem codes, IEEE Trans. Information Theory **IT-11**, 577—579 (1965).
[2] Distribution of cyclic matrices in a finite field, Duke Math. J. **33**, 45—48 (1966).
[3] Factoring polynomials over finite fields, Bell System Tech. J. **46**, 1853—1859 (1967).
[4] Algebraic Coding Theory, McGraw-Hill, New York, 1968. [Имеется перевод: БЕРЛЕКЭМП Э. Алгебраическая теория кодирования. — М.: Мир, 1971.]
[5] Weight enumeration theorems, Proc. Sixth Allerton Conf. on Circuit and Systems Theory, pp. 161—170, Univ. of Illinois Press, Urbana, Ill., 1968.
[6] Factoring polynomials over large finite fields, Math. Comp. **24**, 713—735 (1970).
[7] Factoring polynomials, Proc. Third Southeastern Conf. on Combinatorics, Graph Theory, and Computing (Boca Raton, Fla., 1972), pp. 1—7, Utilitas Math., Winnipeg, Man., 1972.
[8] A survey of coding theory, J. Royal Statist. Soc. Ser. A **135**, 44—73 (1972).
[9] Key Papers in the Development of Coding Theory, IEEE Press, New York, 1974.
[10] An analog to the discriminant over fields of characteristic two, J. Algebra **38**, 315—317 (1976).
BERLEKAMP E. R., FREDRICKSEN H., PROTO R. C. [1] Minimum conditions for uniquely determining the generator of a linear sequence, Utilitas Math. **5**, 305—315 (1974).
BERLEKAMP E. R., RUMSEY H., SOLOMON G. [1] On the solution of algebraic equations over finite fields, Information and Control **10**, 553—564(1967).

BERMAN G., FRYER K. D. [1] Introduction to Combinatorics, Academic Press, New York, 1972.
BERNDT B. C. [1] On Gaussian sums and other exponential sums with periodic coefficients, Duke Math. J. **40**, 145—156 (1973).
BERNDT B. C., CHOWLA S. [1] The reckoning of certain quartic and octic Gauss sums, Glasgow Math. J. **18**, 153—155 (1977).
BERNDT B. C., EVANS R. J. [1] Sums of Gauss, Jacobi, and Jacobsthal, J. Number Theory **11**, 349—398 (1979).
[2] Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer, Illinois J. Math. **23**, 374—437 (1979).
[3] Half Gauss sums, Math. Ann. **249**, 115—125 (1980).
[4] The determination of Gauss sums, Bull. Amer. Math. Soc. (N. S.) **5**, 107—129 (1981); Corrigendum, ibid. **7**, 441 (1982).
BERNSTEIN B. A. [1] A general theory of representation of finite operations and relations, Bull. Amer. Math. Soc. **32**, 533—536 (1926).
[2] Modular representations of finite algebras, Proc. International Math. Congress (Toronto, 1924), vol. 1, pp. 207—216, Univ. of Toronto Press, Toronto, 1928.
BERNSTEIN B. A., DEBELY Y. N. [1] A practical method for the modular representation of finite operations and relations, Bull. Amer. Math. Soc. **38**, 110—114 (1932).
BERTRAM E. A. [1] Polynomials which commute with a Tchebycheff polynomial, Amer. Math. Monthly **78**, 650—653 (1971).
BETTI E. [1] Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo, Ann. Sci. Mat. Fis. **2**, 5—19 (1851).
[2] Sulla risoluzione delle equazioni algebriche, Ann. Sci. Mat. Fis. **3**, 49—115 (1852).
[3] Sopra la teorica delle sostituzioni, Ann. Sci. Mat. Fis. **6**, 5—34 (1855).
BEYER G. [1] Über eine Klasseneinteilung aller kubischen Restcharaktere, Abh. Math. Sem. Univ. Hamburg **19**, 115—116 (1954).
BHANU MURTHY B. S., SAMPATH S. [1] An application of linear feedback shift registers in the computation of polynomial arithmetic, Internat. J. Electron. **45**, 177—185 (1978).
BHASKARAN M. [1] Sums of mth powers in algebraic and abelian number fields, Arch. Math. **17**, 497—504 (1966); Correction, ibid. **22**, 370—371 (1971).
BIERSTEDT R. G., MILLS W. H. [1] On the bound for a pair of consecutive quartic residues of a prime, Proc. Amer. Math. Soc. **14**, 628—632 (1963).
BILHARZ H. [1] Primidvisor mit vorgegebener Primitivwurzel, Math. Ann. **114**, 476—492 (1937).
BINI D., CAPOVANI M. [1] Lower bounds of the complexity of linear algebras, Inform. Process. Lett. **9**, no. 1, 46—47 (1979).
BIRCH B. J. [1] Waring's problem for $\mathfrak{p}$-adic number fields, Acta Arith. **9**, 169—176 (1964).
[2] How the number of points of an elliptic curve over a fixed prime field varies, J. London Math. Soc. **43**, 57—60 (1968).
BIRCH B. J., LEWIS D. J. [1] $\mathfrak{p}$-adic forms, J. Indian Math. Soc. **23**, 11—32 (1959).
[2] Systems of three quadratic forms, Acta Arith. **10**, 423—442 (1965).
BIRCH B. J., LEWIS D. J., MURPHY T. G. [1] Simultaneous quadratic forms, Amer. J. Math. **84**, 110—115 (1962).
BIRCH B. J., SWINNERTON-DYER H. P. F. [1] Note on a problem of Chowla, Acta Arith. **5**, 417—423 (1959).
[2] Notes on elliptic curves. II, J. reine angew. Math. **218**, 79—108 (1965).
BIRDSALL T. G., RISTENBLATT M. P. [1] Introduction to linear shift-register generated sequences, EDG Tech. Report No. 90, Univ. of Michigan Research Institute, Ann Arbor, Mich., 1958.
BIRKHOFF G., BARTEE T. C. [1] Modern Applied Algebra, McGraw-Hill, New York, 1970. [Имеется перевод БИРКГОФФ Г., БАРТИ Т. Современная прикладная алгебра. — М.: Мир, 1976.]

BIRKHOFF G., MACLANE S. [1] A Survey of Modern Algebra, 4th ed., Macmillan, New York, 1977.

BIRKHOFF G. D., VANDIVER H. S. [1] On the integral divisors of $a^n - b^n$, Ann. of Math. (2) **5**, 173—180 (1904).

BLAHUT R. E. [1] Algebraic codes in the frequency domain, Algebraic Coding Theory and Applications (G. Longo, ed.), CISM Courses and Lectures, vol. 258, pp. 447—494, Springer-Verlag, Vienna, 1979.

BLAKE I. F. [1] Algebraic Coding Theory: History and Development, Dowden—Hutchinson—Ross, Stroudsburg, Penn., 1973.

[2] Codes and designs, Math. Mag. **52**, 81—95 (1979).

BLAKE I. F., MULLIN R. C. [1] The Mathematical Theory of Coding, Academic Press, New York, 1975.

BLANCHARD A. [1] Les corps non commutatifs, Presses Univ. de France, Paris, 1972.

BLANKINSHIP W. A. [1] A new version of the Euclidean algorithm, Amer. Math. Monthly **70**, 742—745 (1963).

BLOCK H. D., THIELMAN H. P. [1] Commutative polynomials, Quart. J. Math. (2) **2**, 241—243 (1951).

BLOOM D. M. [1] On periodicity in generalized Fibonacci sequences, Amer. Math Monthly **72**, 856—861 (1965).

BLUMENTHAL L. M. [1] A Modern View of Geometry, W. H. Freeman, San Francisco, 1961.

BOCHNER S. [1] Remarks on Gaussian sums and Tauberian theorems, J. Indian Math. Soc. **15**, 97—104 (1951).

BOLLMAN D. [1] Some periodicity properties of transformations on vector spaces over residue class rings, J. Soc. Indust. Appl. Math. **13**, 902—912 (1965).

[2] Some periodicity properties of modules over the ring of polynomials with coefficients in a residue class ring, SIAM J. Appl. Math. **14**, 237—241 (1966).

BOLLMAN D., RAMIREZ H. [1] On the number of nilpotent matrices over Z_m, J. reine angew. Math. **238**, 85—88 (1969).

BOMBIERI E. [1] Sull'analogo della formula di Selberg nei corpi di funzioni, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **35**, 252—257 (1963).

[2] Nuovi risultati sulla geometria di una ipersuperficie cubica a tre dimensioni, Rend. Mat. e Appl. (5) **25**, 22—28 (1966).

[3] On exponential sums in finite fields, Les Tendances Géométriques en Algèbre et Théorie des Nombres, pp. 37—41, Edition du Centre National de la Recherche Scientifique, Paris, 1966.

[4] On exponential sums in finite fields, Amer. J. Math. **88**, 71—105 (1966). [Имеется перевод: БОМБЬЕРИ Э. Об экспоненциальных суммах в конечных полях. — Математика, т. 12, № 2, 1968, с. 58—87.]

[5] Counting points on curves over finite fields (d'après S. A. Stepanov), Séminaire Bourbaki 1972/73, Exp. 430, Lecture Notes in Math., vol. 383, pp. 234—241, Springer-Verlag, Berling—Heidelberg—New York, 1974.

[6] Hilbert's 8th problem: an analogue, Proc. Symp. Pure Math., vol. 28, pp. 269—274, American Math. Society, Providence, R. I., 1976.

[7] On exponential sums in finite fields, II, Invent. Math. **47**, 29—39 (1978).

BOMBIERI E., DAVENPORT H. [1] On two problems of Mordell, Amer. J. Math. **88**, 61—70 (1966). [Имеется перевод: БОМБЬЕРИ Э., ДЭВЕНПОРТ Г. О двух проблемах Морделла. — Математика, т. 12, № 2, 1968, с. 49—57.]

BOMBIERI E., SWINNERTON-DYER H. P. F. [1] On the local zeta function of a cubic threefold, Ann. Scuola Norm. Sup. Pisa (3) **21**, 1—29 (1967).

BOOTH T. L. [1] Sequential Machines and Automata Theory, Wiley, New York, 1967.

BOREL E., DRACH J. [1] Introduction à l'étude de la théorie des nombres et de l'algèbre supérieure, Nony, Paris, 1895.

BORHO W. [1] Kettenbrüche im Galoisfeld, Abh. Math. Sem. Univ. Hamburg **39**, 76—82 (1973).
BORODIN A., MUNRO I. [1] The computational Complexity of Algebraic and Numeric Problems, American Elsevier, New York, 1975.
BOROS E. [1] On matrices with elements of a finite field (Romanian), Lucrări Şti. Inst. Ped. Timisoara Mat.-Fiz. 1961, 41—47.
BOROSH I., MORENO C. J., PORTA H. [1] Elliptic curves over finite fields. I, Proc. Number Theory Conference (Boulder, Colo., 1972), pp. 147—155, Univ. of Colorado, Boulder, Colo., 1972.
[2] Elliptic curves over finite fields. II, Math. Comp. **29**, 951—964 (1975).
BOSE N. K. [1] A criterion to determine if two multivariable polynomials are relatively prime, Proc. IEEE **60**, 134—135 (1972).
BOSE R. C. [1] On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares, Sankhya **3**, 323—338 (1938).
[2] On the construction of balanced incomplete block designs, Ann. of Eugenics **9**, 353—399 (1939).
BOSE R. C., CHOWLA S., RAO C. R. [1] On the integral order (mod p) of quadratics $x^2 + ax + b$, with applications to the construction of minimum functions for $GF(p^2)$, and to some number theory results, Bull. Calcutta Math. Soc. **36**, 153—174 (1944).
[2] Minimum functions in Galois fields, Proc. Nat. Acad. Sci. India Sect. A **15**, 191—192 (1945).
[3] On the roots of a well-known congruence, Proc. Nat. Acad. Sci. India Sect. A **15**, 193 (1945).
BOSE R. C., RAY-CHAUDHURI D. K. [1] On a class of error correcting binary group codes, Information and Control **3**, 68—79 (1960). [Имеется перевод: БОУЗ Р. К., РОЙ-ЧОУДХУРИ Д. К. Об одном классе двоичных групповых кодов с исправлением ошибок. — В ки.: Кибернетический сборник, вып. 2. — М.: ИЛ, 1961, с. 83—94.]
[2] Further results on error correcting binary group codes, Information and Control **3**, 279—290 (1960). [Имеется перевод: БОУЗ Р. К., РОЙ-ЧОУДХУРИ Д. К. Дальнейшие результаты относительно двоичных групповых кодов с исправлением ошибок. — В кн.: Кибернетический сборник, вып. 6. — М.: ИЛ, 1963, с. 7—19.]
BOSE R. C., SHRIKHANDE S. S. [1] A note on a result in the theory of code construction, Information and Control **2**, 183—194 (1959).
[2] On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4t + 2$, Proc. Nat. Acad. Sci. U. S. A. **45**, 734—737 (1959).
[3] On the construction of sets of mutually orthogonal Latin squares and the falsily of a conjecture of Euler, Trans. Amer. Math. Soc. **95**, 191—209 (1960).
BOSE R. C., SHRIKHANDE S. S., PARKER E. T. [1] Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, Canad. J. Math. **12**, 189—203 (1960).
BOTTEMA O. [1] On the Betti—Mathieu group (Dutch), Nieuw Arch. Wisk. (2) **16**, no. 4, 46—50 (1930).
BOURBAKI N. [1] Algèbre, Ch. V, Actualités Sci. Ind., no. 1102, Hermann, Paris, 1950. [Имеется перевод: БУРБАКИ Н. Алгебра. Многочлены и поля. Упорядоченные группы. — М.: Наука, 1965.]
[2] Algèbre, Ch. VIII, Actualités Sci. Ind., no. 1261, Hermann, Paris, 1958. [Имеется перевод: БУРБАКИ Н. Алгебра. Модули, кольца, формы. — М.: Наука, 1966.]
BOVEY J. D. [1] On the congruence $a_1x_1^k + \ldots + a_sx_s^k \equiv N \pmod{p^n}$, Acta Arith. **23**, 257—269 (1973).
[2] Γ* (8), Acta Arith. **25**, 145—150 (1974).
[3] A note on Waring's problem in p-adic fields, Acta Arith. **29**, 343—351 (1976).

[4] A new upper bound for Waring's problem (mod p), Acta Arith. **32**, 157—162 (1977).
BOYARSKY M. [1] p-adic gamma functions and Dwork cohomology, Trans. Amer. Math. Soc. **257**, 359—369 (1980).
BOYCE W. M. [1] On polynomials which commute with a given polynomial, Proc. Amer. Math. Soc. **33**, 229—234 (1972).
BRAHANA H. R. [1] On cubic congruences, Bull. Amer. Math. Soc. **39**, 962—969 (1933).
[2] Note on irreducible quartic congruences, Trans. Amer. Math. Soc. **38**, 395—400 (1935).
BRANDIS A. [1] Ein gruppentheoretischer Beweis für die Kommutativität endlicher Divisionsringe, Abh. Math. Sem. Univ. Hamburg **26**, 234—236 (1963).
BRAUER A. [1] Über Sequenzen von Potenzresten, Sitzungsber. Preuß. Akad. Wiss. Phys.-Math. Kl. **1928**, 9—16.
[2] Über den kleinsten quadratischen Nichtrest, Math. Z. **33**, 161—176 (1931).
[3] Über Sequenzen von Potenzresten. II, Sitzungsber, Preuß. Akad. Wiss. Phys.-Math. Kl. **1931**, 329—341.
[4] Über die Verteilung der Potenzreste, Math. Z. **35**, 39—50 (1932).
[5] Combinatorial methods in the distribution of kth power residues, Proc. Conf. Combinatorial Math. and Its Appl. (Chapel Hill, N. C., 1967), pp. 14—37, Univ. of North Carolina Press, Chapel Hill, N. C., 1969.
BRAUER R. [1] A note on systems of homogeneous algebraic equations, Bull. Amer. Math. Soc. **51**, 749—755 (1945).
BRAUN H. [1] Geschlechter quadratischer Formen, J. reine angew. Math. **182**, 32—49 (1940).
BRAWLEY J. V. [1] Enumeration of canonical sets by rank, Amer. Math. Monthly **74**, 175—177 (1967).
[2] Certain sets of involutory matrices and their groups, Duke Math. J. **36**, 473—478 (1969).
[3] Polynomials over a ring that permute the matrices over that ring, J. Algebra **38**, 93—99 (1976).
[4] The number of polynomial functions which permute the matrices over a finite field, J. Combinatorial Theory Ser. A **21**, 147—154 (1976).
[5] A note on polynomial matrix functions over a finite field, Linear Algebra Appl. **28**, 35—38 (1979).
BRAWLEY J. V., CARLITZ L. [1] Enumeration of matrices with prescribed row and column sums, Linear Algebra Appl. **6**, 165—174 (1973).
[2] A characterization of the $n \times n$ matrices over a finite field, Amer. Math. Monthly **80**, 670—672 (1973); Addendum, ibid. **80**, 1041—1043 (1973).
BRAWLEY J. V., CARLITZ L., LEVINE J. [1] Power sums of matrices over a finite field, Duke Math. J. **41**, 9—24 (1974).
[2] Scalar polynomial functions on the $n \times n$ matrices over a finite field, Linear Algebra Appl. **10**, 199—217 (1975).
BRAWLEY J. V., CARLITZ L., VAUGHAN T. P. [1] Linear permutation polynomials with coefficients in a subfield, Acta. Arith. **24**, 193—199 (1973).
BRAWLEY J. V., GAMBLE R. O. [1] Involutory matrices over finite commutative rings, Linear Algebra Appl. **21**, 175—188 (1978).
BRAWLEY J. V., HANKINS M. [1] On the distribution by rank of bases for vector spaces of matrices over a finite field, Linear Algebra Appl. **39**, 91—101 (1981).
BRAWLEY J. V., LEVINE J. [1] Equivalence classes of linear mappings with applications to algebraic cryptography. I, II, Duke Math. J. **39**, 121—132, 133—142 (1972).
[2] Equivalence classes of involutory mappings, Duke Math. J. **39**, 211—217 (1972).
BRAWLEY J. V., MULLEN G. L. [1] A note of equivalence classes of matrices over a finite field, Internat. J. Math. and Math. Sci. **4**, 279—287 (1981).

BREMNER A., MORTON P. [1] Polynomial relations in characteristic p, Quart. J. Math. (2) **29**, 335—347 (1978).

BRENNER J. L. [1] Linear recurrence relations, Amer. Math. Monthly **61**, 171—173 (1954).

BRENNER J. L., CARLITZ L. [1] Covering theorems for finite nonabelian simple groups. III. Solutions of the equation $\alpha x^2 + \beta t^2 + \gamma t^{-2} = a$ in a finite field, Rend. Sem. Mat. Univ. Padova **55**, 81—90 (1976).

BRESSOUD D. M. [1] On the value of Gaussian sums, J. Number Theory **13**, 88—94 (1981).

BREWER B. W. [1] On the quadratic reciprocity law, Amer. Math. Monthly **58**, 177—179 (1951).

[2] On certain character sums, Trans. Amer. Math. Soc. **99**, 241—245 (1961).

[3] On primes of the form $u^2 + 5v^2$, Proc. Amer. Math. Soc. **17**, 502—509 (1966).

BRIDGES W. G., RYSER H. J. [1] Combinatorial designs and related systems, J. Algebra **13**, 432—446 (1969).

BRILLHART J. [1] Some modular results on the Euler and Bernoulli polynomials, Acta Arith. **21**, 173—181 (1972).

BRILLHART J., LEHMER D. H., LEHMER E. [1] Bounds for pairs of consecutive seventh and higher power residues, Math. Comp. **18**, 397—407 (1964).

BRILLHART J., LEHMER D. H., SELFRIDGE J. L. [1] New primality criteria and factorizations of $2^m \pm 1$, Math. Comp. **29**, 620—647 (1975).

BRILLHART J., SELFRIDGE J. L. [1] Some factorizations of $2^n \pm 1$ and related results, Math. Comp. **21**, 87—96 (1967); Corrigendum, ibid. **21**, 751 (1967).

BRIOSCHI F. [1] Des substitutions de la forme $\theta(r) \equiv \varepsilon (r^{n-2} + ar^{(n-3)/2})$ pour un nombre n premier de lettres, Math. Ann. **2**, 467—470 (1870).

[2] Un teorema nella teorica delle sostituzioni, Rend. Reale Ist. Lombardo Sci. Lett. (2) **12**, 483—485 (1879).

[3] Sur les fonctions de sept lettres, C. R. Acad. Sci. Paris **95**, 665—669, 814—817, 1254—1257 (1882).

BROUSSEAU A. [1] Recursion relations of products of linear recursion sequences, Fibonacci Quart. **14**, 159—166 (1976).

BROWKIN J. [1] On zeros of forms, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. **17**, 611—616 (1969).

[2] Theory of Fields (Polish), Biblioteka Matematyczna, vol. 49, PWN, Warsaw, 1977.

BROWN E. [1] The first proof of the quadratic reciprocity law, revisited, Amer. Math. Monthly **88**, 257—264 (1981).

BROWN H., ZASSENHAUS H. [1] Some empirical observations on primitive roots, J. Number Theory **3**, 306—309 (1971).

BROWN W. S. [1] On Euclid's algorithm and the computation of polynomial greatest common divisors, J. Assoc. Comput. Mach. **18**, 478—504 (1971).

BRUCK R. H. [1] Difference sets in a finite group, Trans. Amer. Math. Soc. **78**, 464—481 (1955).

[2] Computational aspects of certain combinatorial problems, Proc. Symp. Applied Math., vol. 6, pp. 31—43, McGraw-Hill, New York, 1956.

BRUCK R. H., RYSER H. J. [1] The nonexistence of certain finite projective planes, Canad. J. Math. **1**, 88—93 (1949).

BRUCKNER G. [1] Fibonacci sequence modulo a prime $p \equiv 3 \pmod 4$, Fibonacci Quart. **8**, 217—220 (1970).

BRUEN A. [1] Permutation functions on a finite field, Canad. Math. Bull. **15**, 595—597 (1972).

BRUEN A., LEVINGER B. [1] A theorem on permutations of a finite field, Canad. J. Math. **25**, 1060—1065 (1973).

BRUGGEMAN R. W. [1] Fourier Coefficients of Automorphic Forms, Lecture Notes in Math., vol. 865, Springer-Verlag, Berlin—Heidelberg—New York, 1981.

BRUHAT F. [1] Lectures on Some Aspects of p-adic Analysis, Tata Institute of Fundamental Research, Bombay, 1963.

BU T. [1] Partitions of a vector space, Discrete Math. **31**, 79—83 (1980).

BUCKHIESTER P. G. [1] The number of $n \times n$ matrices of rank r and trace α over a finite field, Duke Math. J. **39**, 695—699 (1972).

[2] Gauss sums and the number of solutions to the matrix equation $XAX^{\tau} = 0$ over $GF(2^y)$, Acta Arith. **23**, 271—278 (1973).

[3] The number of solutions to the matrix equation $XAX^{\tau} = C$, A and C nonalternate and of full rank, over $GF(2^y)$, Math. Nachr. **63**, 37—41 (1974).

[4] Rank r solutions to the matrix equation $XAX^{\tau} = C$, A nonalternate, C alternate, over $GF(2^y)$, Canad. J. Math. **26**, 78—90 (1974).

[5] Rank r solutions to the matrix equation $XAX^{\tau} = C$, A alternate, over $GF(2^y)$, Trans. Amer. Math. Soc. **189**, 201—209 (1974).

[6] Rank r solutions to the matrix equation $XAX^{\tau} = C$, A and C nonalternate, over $GF(2^y)$, Math. Nachr. **63**, 413—422 (1974).

BUMBY R. T. [1] A distribution property for linear recurrence of the second order, Proc. Amer. Math. Soc. **50**, 101—106 (1975).

BUNDSCHUH P. [1] On the distribution of Fibonacci numbers, Tamkang J. Math. **5**, 75—79 (1974).

[2] Transzendenzmasse in Körpern formaler Laurentreihen, J. reine angew. Math. 299/300, 411—432 (1978).

BUNDSCHUH P., SHIUE J.-S.: [1] Solution of a problem on the uniform distribution of integers, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **55**, 172—177 (1973).

[2] A generalization of a paper by D. D. Wall, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **56**, 135—144 (1974).

BURDE K. [1] Verteilungseigenschaften von Potenzresten, J. reine angew. Math. **249**, 133—172 (1971).

[2] p-dimensionale Vektoren modulo, p. I, J. reine angew. Math. **268/269**, 302—314 (1974).

[3] Sequenzen der Länge 2 von Restklassencharakteren, J. reine angew. Math. **272**, 194—202 (1975).

[4] Über allgemeine Sequenzen der Länge 3 von Legendresymbolen, J. reine angew. Math. **272**, 203—216 (1975).

[5] p-dimensionale Vektoren modulo p. II, J. reine angew. Math. **278/279**, 353—364 (1975).

[6] Zur Herleitung von Reziprozitätsgesetzen unter Benutzung von endlichen Körpern, J. reine angew. Math. **293/294**, 418—427 (1977).

[7] Potenzen von Galoisfeldern, J. reine angew. Math. **307/308**, 194—220 (1979).

[8] Pythagoräiche Tripel und Reziprozität in Galoisfeldern, J. Number Theory **12**, 278—282 (1980).

[9] Ein Reziprozitätsgesetz in Galoisfeldern, J. Number Theory **13**, 66—87 (1981).

BURGESS D. A. [1] The distribution of quadratic residues and non-residues, Mathematika **4**, 106—112 (1957). [Имеется перевод: БЕРДЖЕСС Д. А. Распределение квадратичных вычетов и невычетов. — Математика, т. 2, № 6, 1958, с. 3—9.]

[2] On character sums and primitive roots, Proc. London Math. Soc. (3) **12**, 179—192 (1962). [Имеется перевод: БЕРДЖЕСС Д. А. О суммах характеров и первообразных корнях. — Математика, т. 7, № 4, 1963, с. 3—16.]

[3] On character sums and L-series, Proc. London Math. Soc. (3) **12**, 193—206 (1962). [Имеется перевод: БЕРДЖЕСС Д. А. О суммах характеров и L-рядах. — Математика, т. 7, № 4, 1963, с. 17—30.]

[4] A note on the distribution of residues and non-residues, J. London Math. Soc. **38**, 253—256 (1963).
[5] On character sums and L-series. II, Proc. London Math. Soc. (3) **13**, 524—536 (1963).
[6] On Dirichlet characters of polynomials, Proc. London Math. Soc. (3) **13**, 537—548 (1963).
[7] Character sums and primitive roots in finite fields, Proc. London Math. Soc. (3) **17**, 11—25 (1967).
[8] On the quadratic character of a polynomial, J. London Math. Soc. **42**, 73—80 (1967).
[9] A note on character sums of binary quadratic forms, J. London Math. Soc. **43**, 271—274 (1968).
[10] A note on character sums over finite fields, J. reine angew. Math. **255**, 80—82 (1972).
[11] Dirichlet characters and polynomials, Труды международной конференции по теории чисел (Москва, 1971); Труды Матем. инст. им. Стеклова АН СССР, т. **132**, 1973, с. 203—205.
BURR S. A. [1] On moduli for which the Fibonacci sequence contatins a complete system of residues, Fibonacci Quart. **9**, 497—504 (1971).
BURTON H. O. [1] Inversionless decoding of binary BCH codes, IEEE Trans. Information Theory IT-**17**, 464—466 (1971).
BUSSEY W. H. [1] Galois field tables for $p^n \leqslant 169$, Bull. Amer. Math. Soc. **12**, 22—38 (1905.)
[2] Tables of Galois fields of order less than 1000, Bull. Amer. Math. Soc. **16**, 188—206 (1909).
BUTLER M. C. R. [1] On the reducibility of polynomials over finite fields, Quart, J. Math. (2) **5**, 102—107 (1954).
[2] The irreducible factors of $f(x^m)$ over a finite field, J. London Math. Soc. **30**, 480—482 (1955).
BUTSON A. T. [1] Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences, Canad. J. Math. **15**, 42—48 (1963).
BYERS G.C. [1] Class number relations for quadratic forms over $GF[q, x]$, Duke Math. J. **21**, 445—461 (1954).
CAILLER C. [1] Sur les congruences du troisième degré, L'Enseignement Math. **10**, 474—487 (1908).
CALABI E., WILF H. S. [1] On the sequential and random selection of subspaces over a finite field, J. Combinatorial Theory Ser. A **22**, 107—109 (1977).
CALLAHAN R., SMITH R. A. [1] L-function of a quadratic form, Trans. Amer. Math. Soc. **217**, 297—309 (1976).
CALMET J., LOOS R. [1] An improvement of Rabin's probabilistic algorithm for generating irreducible polynomials over $GF(p)$, Inform. Process. Lett. **11**, 94—95 (1980).
[2] A SAC-2 implementation of arithmetic and root finding over lagre finite fields, Tech. Report, Univ. of Karlsruhe, 1983.
CAMERON P. J. [1] Extending symmetric designs, J. Combinatorial Theory Ser. A **14**, 214—220 (1973).
CAMERON P. J., HALL J. I., VAN LINT J. H., SPRINGER T. A., VAN TILBORG H. C. A., [1] Translates of subgroups of the multiplicative group of a finite field, Indag. Math. 37, 285—289 (1975).
CAMERON P.-J., SEIDEL J. J. [1] Quadratic forms over $GF(2)$, Indag. Math. **35**, 1—8 (1973).
CAMERON P. J., VAN LINT J. H. [1] Graph Theory, Coding Theory and Block Designs, London Math. Soc. Lecture Note Series, no. 19, Cambridge Univ. Press, London, 1975. [Имеется перевод: КАМЕРОН П., ВАН ЛИНТ ДЖ. Теория графов, теория кодирования и блок-схемы. — М. Наука, 1980.]

[2] Graphs, Codes, and Designs, London Math. Soc. Lecture Note Series, no. 43, Cambridge Univ. Press, Cambridge, 1980.

CAMION P. [1] A proof of some properties of Reed—Muller codes by means of the normal basis theorem, Proc. Conf. Combinatorial Math. and Its Appl. (Chapel Hill, N. C., 1967), pp. 371—376, Univ. of North Carolina Press, Chapel Hill, N. C., 1969.

[2] Un algorithme de construction des idempotents primitifs d'idéaux d'algèbres sur F_q, C. R. Acad. Sci. Paris Sér. A **291**, 479—482 (1980).

[3] Factorization des polynômes de $\mathbb{F}_q[X]$, Rev. CETHEDEC **1981**, no 2, 5—21.

CAMPBELL A. D. [1] Plane cubic curves in the Galois fields of order 2^n, Ann. of Math. (2) **27**, 395—406 (1926).

[2] Pencils of conics in the Galois fields of order 2^n, Amer. J. Math. **45**, 401—406 (1927).

[3] Plane cubic curves in the Galois fields of order ρ^n, $\rho > 3$, Messenger of Math. **58**, 33—48 (1928).

[4] The discriminant of the m-ary quadratic in the Galois fields of order 2^n, Ann. of Math. (2) **29**, 395—398 (1928).

[5] Nets of conics in the Galois fields of order 2^n, Bull. Amer. Math. Soc. **34**, 481—489 (1928).

[6] Pencils of quadrics in the Galois fields of order 2^n, Tôhoku Math. J. **34**, 236—248 (1931).

[7] Apolarity in the Galois fields of order 2^n, Bull. Amer. Math. Soc. **38**, 52—56 (1932).

[8] Plane quartic curves in the Galois fields of order 2^n, Tôhoku Math. J. **37**, 88—93 (1933).

[9] Pseudo-covariants of an n-ic in m variables in a Galois field that consists of terms of this n-ic, Bull. Amer. Math. Soc. **39**, 252—256 (1933).

[10] Note on cubic surfaces in the Galois fields of order 2^n, Bull. Amer. Math. Soc. **39**, 406—410 (1933).

[11] Pseudo-covariants of n-ics in a Galois field, Tôhoku Math. J **43**, 17—29 (1937).

CANADAY E. F. [1] The sum of the divisors of a polynomial, Duke Math. J. **8**, 721—737 (1941).

CANTOR D. G., ZASSENHAUS H. [1] A new algorithm for factoring polynomials over finite fields, Math. Comp. **36**, 587—592 (1981).

CAPELLI A. [1] Sulla rudittibilità delle equazioni algebriche I, Rend Accad. Sci. Fis. Mat. Napoli (3) **3**, 243—252 (1897).

[2] Sulla riduttibilità delle equazioni algebriche II, Rend. Accad. Sci. Fis. Mat. Napoli (3) **4**, 84—90 (1898).

[3] Sulla riduttibilità della funzione $x^n - A$ in un campo qualunque di razionalità, Math. Ann. **54**, 602—603 (1901).

CAR M. [1] Le problème de Waring pour l'anneau des polynômes sur un corps fini, C. R. Acad. Sci. Paris Sér. A. **273**, 141—144 (1971).

[2] Le problème de Goldbach pour l'anneau des polynômes sur un corps fini, C. R. Acad. Sci. Paris Sér. A **273**, 201—204 (1971).

[3] Le problème de Waring pour l'anneau des polynômes sur un corps fini, Sém. Théorie des Nombres 1972—1973, Exp. 6, Univ. Bordeaux I, Talence, 1973.

[4] La méthode des sommes trigonometriques pour $\mathbb{F}_q[X]$, Jornées de Théorie Additive des Nombres (Bordeaux, 1977), pp. 19—33, Univ. Bordeaux I, Talence, 1978.

[5] Normes dans $\mathbb{F}_q[X]$ de polynômes de $\mathbb{F}_{q^h}[X]$, C. R. Acad. Sci. Paris Sér. A **288**, 669—672 (1979); Correction, ibid. **288**, 1049 (1979).

[6] Sommes de carrés et d'irréductibles dans $\mathbb{F}_q[X]$, Ann. Fac. Sci. Toulouse **3**, 129—166 (1981).
[7] Factorisation dans $\mathbb{F}_q[X]$, C. R. Acad. Sci. Paris Sér. I **294**, 147—150 (1982).
CARCANAGUE J. [1] Propriétés des q-polynômes, C. R. Acad. Sci. Paris Sér. A **265**, 415—418 (1967).
[2] q-polynômes abéliens sur un corps K, C. R. Acad. Sci. Paris Sér. A **265**, 496—499 (1967).
CAREY F. S. [1] Notes on the division of the circle, Quart. J. Pure Appl. Math. **26**, 322—371 (1893).
CARLITZ L. [1] The arithmetic of polynomials in a Galois field, Proc. Nat. Acad. Sci. U. S. A. **17**, 120—122 (1931).
[2] The arithmetic of polynomials in a Galois field, Amer. J. Math. **54**, 39—50 (1932).
[3] On polynomials in a Galois field, Bull. Amer. Math. Soc. **38**, 736—744 (1932).
[4] On a theorem of higher reciprocity, Bull. Amer. Math. Soc. **39**, 155—160 (1933).
[5] On the representation of a polynomial in a Galois field as the sum of an even number of squares, Trans. Amer. Math. Soc. **35**, 397—410 (1933).
[6] On polynomials in a Galois field: Some formulae involving divisor functions, Proc. London Math. Soc. (2) **38**, 116—124 (1935).
[7] On certain functions connected with polynomials in a Galois field, Duke Math. J. **1**, 137—168 (1935).
[8] On the representation of a polynomial in a Galois field as the sum of an odd number of squares, Duke Math. J. **1**, 298—315 (1935).
[9] A theorem on higher congruences, Bull. Amer. Math. Soc. **41**, 844—846 (1935).
[10] On certain higher congruences, Bull. Amer. Math. Soc. **41**, 907—914 (1935).
[11] On certain equations in relative-cyclic fields, Duke Math. J. **2**, 650—659 (1936).
[12] On factorable polynomials in several indeterminates, Duke Math. J. **2**, 660—670 (1936).
[13] Sums of squares of polynomials, Duke Math. **3**, 1—7 (1937).
[14] An arithmetic function, Bull. Amer. Math. Soc. **43**, 271—276 (1937).
[15] Some formulae for factorable polynomials in several indeterminates, Bull. Amer. Math. Soc. **43**, 299—304 (1937).
[16] An analogue of the von Staudt—Clausen theorem, Duke Math. J. **3**, 503—517 (1937).
[17] Criteria for certain higher congruences, Amer. J. Math. **59**, 618—628 (1937).
[18] A class of polynomials, Trans. Amer. Math. Soc. **43**, 167—182 (1938).
[19] Some sums involving polynomials in a Galois field, Duke Math. J. **5**, 941—947 (1939).
[20] A set of polynomials, Duke Math. J. **6**, 486—504 (1940).
[21] Linear forms and polynomials in a Galois field, Duke Math. J. **6**, 735—749 (1940).
[22] An analogue of the Staudt—Clausen theorem, Duke Math. J. **7**, 62—67 (1940).
[23] An analogue of the Bernoulli polynomials, Duke Math. J. **8**, 405—412 (1941).
[24] The reciprocal of certain series, Duke Math. J. **9**, 234—243 (1942).
[25] The reciprocal of certain types of Hurwitz series, Duke Math. J. **9**, 629—642 (1942).
[26] Some topics in the arithmetic of polynomials, Bull. Amer. Math. Soc. **48**, 679—691 (1942).
[27] The singular series for sums of squares of polynomials, Duke Math. J. **14**, 1105—1120 (1947).

[28] Representations of arithmetic functions in $GF[p^n, x]$, Duke Math. J. **14**, 1121—1137 (1947).
[29] A problem of Dickson's, Duke Math. J. **14**, 1139—1140 (1947).
[30] Representations of arithmetic functions in $GF[p^n, x]$. II, Duke Math. J. **15**, 795—801 (1948).
[31] Finite sums and interpolation formulas over $GF[p^n, x]$, Duke Math. J. **15**, 1001—1012 (1948).
[32] Some applications of a theorem of Chevalley, Duke Math. J. **18**, 811—819 (1951).
[35] Diophantine approximation in fields of characteristic p, Trans. Amer. Math. Soc. **72**, 187—208 (1952).
[34] Some problems involving primitive roots in a finite field, Proc. Nat. Acad. Sci. U. S. A. **38**, 314—318 (1952); Errata, ibid. **38**, 618 (1952).
[35] Primitive roots in a finite field, Trans. Amer. Math. Soc. **73**, 373—382 (1952).
[36] Note on an arithmetic function, Amer. Math. Monthly **59**, 386—387 (1952).
[37] Sums of primitive roots in a finite field, Duke Math. J. **19**, 459—469 (1952).
[38] A problem of Dickson, Duke Math. J. **19**, 471—474 (1952).
[39] The number of solutions of certain equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **38**, 515—519 (1952); Errata, ibid. **38**, 618 (1952).
[40] A theorem of Dickson on irreducible polynomials, Proc. Amer. Math Soc. **3**, 693—700 (1952).
[41] Distribution of primitive roots in a finite field, Quart. J. Math. (2) **4**, 4—10 (1953).
[42] Note on a conjecture of André Weil, Proc. Amer. Math. Soc. **4**, 5—9 (1953).
[43] Sone special equations in a finite field, Pacific J. Math. **3**, 13—24 (1953).
[44] A theorem of Stickelberger, Math. Scand. **1**, 82—84 (1953).
[45] A reciprocity formula for weighted quadratic partitions, Math. Scand. **1**, 286—288 (1953).
[46] Weighted quadratic partitions over a finite field, Canad. J. Math. **5**, 317—323 (1953).
[47] Invariantive theory of equations in a finite field, Trans. Amer. Math. Soc. **75**, 405—427 (1953).
[48] A note on partitions in $GF[q, x]$, Proc. Amer. Math. Soc. **4**, 464—469 (1953).
[49] Permutations in a finite field, Proc. Amer. Math. Soc. **4**, 538 (1953).
[50] Certain special equations in a finite field, Monatsh. Math. **58**, 5—12 (1954).
[51] Representations by skew forms in a finite field, Arch. Math. **5**, 19—31 (1954).
[52] The number of solutions of some equations in a finite field, Portug. Math. **13**, 25—31 (1954).
[53] A note on modular invariants, Nieuw Arch. Wisk (3) **2**, 28—31 (1954).
[54] Representations by quadratic forms in a finite field, Duke Math. J. **21**, 123—137 (1954).
[55] A problem involving quadratic forms in a finite field, Math. Nachr. **11**, 135—142 (1954).
[56] Pairs of quadratic equations in a finite field, Amer. J. Math. **76**, 137—154 (1954).
[57] Sums of primitive roots of the first and second kind in a finite field, Math. Nachr. **12**, 155—172 (1954).
[58] The number of solutions of some special equations in a finite field, Pacific J. Math. **4**, 207—217 (1954).
[59] Invariant theory of systems of equations in a finite field, J. Analyse Math. **3**, 382—413 (1954).
[60] The number of solutions of a special quadratic congrunce, Portugal. Math. **14**, 9—14 (1955).
[61] On the number of distinct values of a polynomial with coefficients in a finite field, Proc. Japan Acad. **31**, 119—120 (1955).

[62] The number of solutions of certain types of equations in a finite field, Pacific J. Math. 5, 177—181 (1955).
[63] The number of solutions of some equations in a finite field, J. Math. Soc. Japan 7, 209—223 (1955).
[64] A special symmetric equation in a finite field, Acta Math. Acad. Sci. Hungar. 6, 445—450 (1955).
[65] Solvability of certain equations in a finite field, Quart. J. Math. (2) 7, 3—4 (1956).
[66] A note on nonsigular forms in a finite field, Proc. Amer. Math. Soc. 7, 27—29 (1956).
[67] An application of a theorem of Stickelberger, Simon Stevin 31, 27—30 (1956).
[68] Sets of primitive roots, Compositio Math. 13, 65—70 (1956).
[69] Class number formulas for quadratic forms over $GF[q, x]$, Duke Math. J. 23, 225—235 (1956).
[70] A special quartic congruence, Math. Scand. 4, 243—246 (1956).
[71] The number of solutions of a particular equation in a finite field, Publ. Math. Debrecen 4, 379—383 (1956).
[72] Weighted quadratic partitions over $GF[q, x]$, Duke Math. J. 23, 493—505 (1956).
[73] Note on a quartic congruence, Amer. Math. Monthly 63, 569—571 (1956).
[74] A note on Gauss' sum, Proc. Amer. Math. Soc. 7, 910—911 (1956).
[75] The number of points on certain cubic surfaces over a finite field, Boll. Un. Mat. Ital. (3) 12, 19—21 (1957).
[76] Some cyclotomic determinants, Bull. Calcutta Math. Soc. 49, 49—51 (1957).
[77] Some theorems on polynomials, Ark. Mat. 3, 351—353 (1957).
[78] A theorem of Dickson on nonvanishing cubic forms in a finite field, Proc. Amer. Math. Soc. 8, 975—977 (1957).
[79] Quadratic residues and Tchebycheff polynomials, Portugal. Math. 18, 193—198 (1959).
[80] Some cyclotomic matrices, Acta Arith. 5, 293—308 (1959).
[81] A note on exponential sums, Acta Sci. Math. Szeged 21, 135—143 (1960).
[82] A theorem on permutations in a finite field, Proc. Amer. Math. Soc. 11, 456—459 (1960).
[83] Some theorems on permutation polynomials, Bull. Amer. Math. Soc. 68, 120—122 (1962).
[84] A theorem on «ordered» polynomials in a finite field, Acta Arith. 7, 167—172 (1962).
[85] Some identities over a finite field, Quart. J. Math. (2) 13, 299—303 (1962).
[86] A note on permutation functions over a finite field, Duke Math. J. 29, 325—332 (1962).
[87] Solvability of certain equations in a finite field, Acta Arith. 7, 389—397 (1962).
[88] A note on finite fields, Proc. Amer. Math. Soc. 13, 546—549 (1962).
[89] Note on a problem of Dickson, Proc. Amer. Math. Soc. 14, 98—100 (1963).
[90] A note on permutations in an arbitrary field, Proc. Amer. Math. Soc. 14, 101 (1963).
[91] A note on the Betti—Mathieu group, Portugal. Math. 22, 121—125 (1963).
[92] Classes of pairs of commuting matrices over a finite field, Amer. Math. Monthly 70, 192—195 (1963).
[93] Permutations in finite fields, Acta Sci. Math. Szeged 24, 196—203 (1963).
[94] Simultaneous representations in quadratic and linear forms over $GF[q, x]$, Duke Math. J. 30, 259—270 (1963).
[95] The distribution of irreducible polynomials in several indeterminates, Illinois J. Math. 7, 371—375 (1963).
[96] A property of irreducible polynomials related to Mersenne primes, Univ. Nac. Tucumán Rev. Ser. A 15, 43—46 (1964).

[97] Functions and polynomials (mod p^n), Acta Arith. **9**, 67—78 (1964).
[98] A note on multiple Kloosterman sums, J. Indian Math. Soc. **29**, 197—200 (1965).
[99] The distribution of irreducible polynomials in several indeterminates II, Canad. J. Math. **17**, 261—266 (1965).
[100] A note on multiple exponential sums, Pacific J. Math. **15**, 757—765 (1965).
[101] A conjecture concerning a certain system of equations in a finite field, Rev. Roum. Math. Pures Appl. **11**, 277—282 (1966).
[102] A note on quadrics over a finite field, Duke Math. J. **33**, 453—458 (1966).
[103] A note on irreducible cubics mod p, Norske Vid. Selsk. Forh. (Trondheim) **40**, 25—30 (1967).
[104] Restricted product of the characteristic polynomials of matrices over a finite field, Illinois J. Math. **11**, 128—133 (1967).
[105] Some theorems on irreducible reciprocal polynomials over a finite field, J. reine angew. Math. **227**, 212—220 (1967).
[106] A note on Gauss's sum, Le Matematiche (Catania) **23**, 147—150 (1968).
[107] Some formulas related to Gauss's sum, Rend. Sem. Mat. Univ. Padova **41**, 222—226 (1968).
[108] A note on exponential sums, Pacific J. Math. **30**, 35—37 (1969).
[109] Gauss sums over finite fields of order 2^n, Acta Arith. **15**, 247—265 (1969).
[110] A theorem on sets of polynomials over a finite field, Acta Arith. **15**, 267—268 (1969).
[111] Kloosterman sums and finite field extensions, Acta Arith. **16**, 179—193 (1969).
[112] Factorization of a special polynomial over a finite field, Pacific J. Math. 32, 603—614 (1970).
[113] Reduction formulas for certain multiple exponential sums, Czechoslovak Math. J. **20**, 616—627 (1970).
[114] The number of solutions of certain matrix equations over a finite field, Math. Nachr. **56**, 105—109 (1973).
[115] Correspondences in a finite field. I, Acta Arith. **27**, 101—123 (1975).
[116] A note on sums of three squares in $GF[q, x]$, Math. Mag **48**, 109—110 (1975).
[117] Correspondences in a finite field. II, Indiana Univ. Math. J. **24**, 785—811 (1975).
[118] A theorem on lacunary polynomials in a finite field, Amer. Math. Monthly 83, 37—38 (1976).
[119] Some theorems on polynomials over a finite field, Amer. Math. Monthly **84**, 29—32 (1977).
[120] A theorem on linear exponential sums, Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz. **577-598**, 55—56 (1977).
[121] Functions and correspondences in a finite field, Bull. Amer. Math. Soc. **83**, 139—165 (1977).
[122] A note on exponential sums, Math. Scand. **42**, 39—48 (1978).
[123] Polynomial characteristic functions for $GF(p)$ and irregular primes, Rocky Mountain J. Math. **8**, 583—587 (1978).
[124] Explicit evaluation of certain exponential sums, Math. Scand. **44**, 5—16 (1979).
[125] Evaluation of some exponential sums over a finite field, Math. Nachr. **96**, 319—339 (1980).

CARLITZ L., COHEN E. [1] Divisor functions of polynomials in a Galois field, Duke Math. J. **14**, 13—20 (1947).
[2] Cauchy products of divisor functions in $GF[p^n, x]$, Duke Math. J. **14**, 707—722 (1947).
[3] The number of representations of a polynomial in certain special quadratic forms, Duke Math. J. **15**, 219—228 (1948).

GARLITZ L., CORSON H. H. [1] Some special equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **41**, 752—754 (1955).
[2] Some special equations in a finite field, Monatsh. Math. **60**, 114—122 (1956).
CARLITZ L., HAYES D. R. [1] Permutations with coefficients in a subfield, Acta Arith. **21**, 131—135 (1972).
CARLITZ L., HODGES J. H. [1] Representations by Hermitian forms in a finite field, Duke Math. J. **22**, 393—405 (1955).
[2] Distribution of bordered symmetric, skew and hermitian matrices in a finite field, J. reine angew. Math. **195**, 192—201 (1956).
[3] Distribution of matrices in a finite field, Pacific J. Math. **6**, 225—230 (1956).
[4] Enumeration of matrices of given rank with submatrices of given rank, Linear Algebra Appl. **16**, 285—291 (1977).
CARLITZ L., LEWIS D. J., MILLS W. H., STRAUS E. G. [1] Polynomials over finite fields with minimum value sets, Mathematika **8**, 121—130 (1961).
CARLITZ L., LONG A. F., Jr. [1] The factorization of $Q(L(x_1), \ldots, L(x_k))$ over a finite field where $Q(x_1, \ldots, x_k)$ is of first degree and $L(x)$ is linear, Acta Arith. **32**, 407—420 (1977).
CARLITZ L., LUTZ J. A. [1] A characterization of permutation polynomials over a finite field, Amer. Math. Monthly **85**, 746—748 (1978).
CARLITZ L., UCHIYAMA S. [1] Bounds for exponential sums, Duke Math. J. **24**, 37—41 (1957).
CARLITZ L., WELLS C. [1] The number of solutions of a special system of equations in a finite field, Acta Arith. **12**, 77—84 (1966).
CARMICHAEL R. D. [1] On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15**, 30—70 (1913).
[2] On sequences of integers defined by recurrence relations, Quart. J. Pure Appl. Math. **48**, 343—372 (1920).
[3] A simple principle of unification in the elementary theory of numbers, Amer. Math. Monthly **36**, 132—143 (1929).
[4] Introduction to the Theory of Groups of Finite Order, Ginn & Co., Boston, 1937; Dover, New York, 1956.
CARTIER P. [1] Sur une généralisation des symboles de Legendre—Jacobi, L'Enseignement Math. (2) **16**, 31—48 (1970).
CASSELS J. W. S. [1] Diophantine equations with special reference to elliptic curves, J. London Math. Soc. **41**, 193— 291 (1966). [Имеется перевод: КАССЕЛС ДЖ. Диофантовы уравнения со специальным рассмотрением эллиптических кривых. — Математика, т. 12, № 1, 1968, с. 111—160, № 2, 1968, с. 3—48.]
[2] On the determination of generalized Gauss sums, Arch. Math. (Brno) **5**, 79—84 (1969).
[3] On Kummer sums, Proc. London Math. Soc. (3) **21**, 19—27 (1970). [Имеется перевод: КАССЕЛС ДЖ. О суммах Куммера. — Математика, т. 16, № 1, 1972, с. 157—164.]
[4] On cubic trigonometric sums, Actes du Congrès International des Mathématiciens (Nice, 1970), vol. 1, pp. 377—379, Gauthier-Villars, Paris, 1971.
[5] Trigonometric sums and elliptic functions, Algebraic Number Theory (S. Iyanaga, ed.), pp. 1—7, Japan Soc. for the Promotion of Science, Tokyo, 1977.
CATLIN P. A. [1] A lower bound for the period of the Fibonacci series modulo m, Fibonacci Quart. **12**, 349—350 (1974).
CAUCHY A.-L. [1] Recherches sur les nombres, J. de L'Ecole Polytechnique **9**, 99—116 (1813); Oeuvres (II), vol. 1, pp. 39—63, Gauthier-Villars, Paris, 1905.
[2] Mémoire sur la théorie des nombres, Bull. Sci. Math. de M. Férussac **12**, 205—221 (1829); Oeuvres (II), vol. 2, pp. 88—107, Gauthier-Villars, Paris, 1958.
[3] Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers, Exercises de Math. **4** (1829); Oeuvres (II), vol. 9, pp. 298—341, Gauthier-Villars, Paris, 1891.

[4] Mémoire sur la théorie des nombres, Mém. Acad. Sci. Inst. de France **17** (1840); Ouevres (I), vol. 3, Gauthier-Villars, Paris, 1911.
[5] Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes, C. R. Acad. Sci. Paris **10**, 560—572 (1840); J. Math. Pures Appl. **5**, 154—168 (1840); Oeuvres (1), vol. 5, pp. 152—166, Gauthier-Villars, Paris, 1885.
CAVIOR S. R. [1] A note on octic permutation polynomials, Math. Comp. **17**, 450—452 (1963).
[2] Equivalence classes of functions over a finite field, Acta Arith. **10**, 119—136 (1964).
[3] Exponential sums related to polynomials over the *GF* (*p*), Proc. Amer. Math. Soc. **15**, 175—178 (1964).
[4] On the least non-negative trace of a polynomial over a finite field, Boll. Un. Mat.Ital. (3) **20**, 120—121 (1965).
[5] Uniform distribution of polynomials modulo *m*, Amer. Math. Monthly **73**, 171—172 (1966).
[6] Equivalence classes of sets of polynomials over a finite field, J. reine angew. Math. **225**, 191—202 (1967).
[7] Uniform distribution (mod *m*) of recurrent sequences, Fibonacci Quart. **15**, 265—267 (1977).
CAZACU C. [1] Application of two-valued logic in the theory of numbers (Romanian), An. Sti. Univ. «Al. I. Cuza» Iasi Sect. I (N. S.) **6**, 481—492 (1960).
[2] Предикаты в конечных полях, An. Sti. Univ. «Al. I. Cuza» Iasi Sect. I (N. S.) **11**, 221—238 (1965).
[3] Предикаты с кванторами в конечных полях, An. Sti. Univ. «Al. I. Cuza» Iasi Sect. I (N. S.) **13**, 241—247 (1967).
CAZACU C., SIMOVICI D. [1] A new approach of some problems concerning polynomials over finite fields, Information and Control **22**, 503—511 (1973).
CECCHERINI P. V. [1] Some new results on certain finite structures, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **56**, 840—855 (1974).
CECCHERINI P. V., HIRSCHFELD J. W. P. [1] On the number of zeros over a finite field of certain symmetric polynomials, Canad. Math. Bull. **23**, 327—332 (1980).
CHALK J. H. H. [1] The number of solutions of congruences in incomplete residue systems, Canad. J. Math. **15**, 291—296 (1963).
[2] The Vinogradov—Mordell—Tietäväinen inequalities, Indag. Math. **42**, 367—374 (1980).
CHALK J. H. H., SMITH R. A. [1] On Bombieri's estimate for exponential sums, Acta Arith. **18**, 191—212 (1971).
CHALK J. H. H., WILLIAMS K. S. [1] The distribution of solutions of congruences, Mathematika **12**, 176—192 (1965); Corrigendum and Addendum, ibid. **16**, 98—100 (1969).
CHANG J. A., GODWIN H. J. [1] A table of irreducible polynomials and their exponents, Proc. Cambridge Philos. Soc. **65**, 513—522 (1969).
CHANG S. C., WOLF J. K. [1] A simple derivation of the MacWilliams identity for linear codes, IEEE Trans. Information Theory **IT-26**, 476—477 (1980).
CHANG T-H. [1] Lösung der Kongruenz $x^2 \equiv a \pmod{p}$ nach einem Primzahlmodul $p = 4n + 1$, Math. Nachr. **22**, 136—142 (1960).
CHAO C. Y. [1] On equivalence classes of matrices, Bull. Malaysian Math. Soc (2) **4**, 29—36 (1981).
CHÂTELET F. [1] Classification des courbes de genre un, dans le corps des restes, module *p*, C. R. Acad. Sci. Paris **208**, 487—489 (1939).
[2] Les courbes de genre 1 dans un champ de Galois, C. R. Acad. Sci. Paris **224**, 1616—1618 (1947).
CHEN C. L. [1] Computer results on the minimum distance of some binary cyclic codes, IEEE Trans. Information Theory **IT-16**, 359—360 (1970).

[2] High-speed decoding of BCH codes, IEEE Trans. Information Theory **IT-27**, 254—256 (1981).

CHEN J. M., LI X. M. [1] The structure of the polynomials over the finite field defined by Q $[f]$-matrix (Chinese), Acta Math. Sinica **20**, 294—297 (1977).

CHEN J. R. [1] On the representation of a natural number as a sum of terms of the form $x(x+1)\ldots(x+k-1)/k!$ (Chinese), Acta Math. Sinica **9**, 264—270 (1959).

[2] On Professor Hua's estimate of exponential sums, Sci. Sinica **20**, 711—719 (1977).

CHERLY J. [1] Addition theorems in $F_q[x]$, J. reine angew. Math. **293/294**, 223—227 (1977).

[2] A lower bound theorem in $F_q[x]$, J. reine angew. Math. **303/304**, 253—264 (1978).

[3] On complementary sets of group elements, Arch. Math. **35**, 313—318 (1980).

CHEVALLEY C. [1] Démonstration d'une hypothèse de M. Artin, Abh. Math. Sem. Univ. Hamburg **11**, 73—75 (1936).

[2] Sur certains groupes simples, Tôhoku Math. J. (2) **7**, 14—66 (1955).

CHIEN R. T. [1] Cyclic decoding procedures for Bose—Chaudhuri—Hocquenghem codes, IEEE Trans. Information Theory **IT-10**, 357—363 (1964).

CHIEN R. T., CUNNINGHAM B. D. [1] Hybrid methods for finding roots of a polynomial with application to BCH decoding, IEEE Trans. Information **IT-15**, 329—335 (1969).

CHILDS L. [1] A Concrete Introduction to Higher Algebra, Springer-Verlag, New York—Heidelberg—Berlin, 1979.

CHILDS L., ORZECH M. [1] On modular group rings, normal bases, and fixed points, Amer. Math. Monthly **88**, 142—145 (1981).

CHINBURG T. [1] 'Easier' Waring problem for commutative rings, Acta Arith. **35**, 303—331 (1979).

CHOR B.-Z. [1] Arithmetic of finite fields, Inform. Process. Lett. **14**, 4—6 (1982).

CHOWLA I. [1] The number of solutions of a congruence in two variables, Proc. Nat. Acad. Sci. India Sect. A **4**, 654—655 (1936).

[2] On the number of solutions of some congruences in two variables, Proc. Nat. Acad. Sci. India Sect. A **5**, 40—44 (1937).

[3] Generalization of a theorem of Dickson, Proc. Nat. Acad. Sci. India Sect. A **8**, 223—226 (1938).

[4] On Waring's problem (mod p), Proc. Nat. Acad. Sci. India Sect. A **13**, 195—220 (1943).

CHOWLA P. [1] On some polynomials which represent every natural number exactly once, Norske Vid. Selsk. Forh. (Trondheim) **34**, 8—9 (1961).

[2] A new proof and generalization of some theorems of Brewer, Norske Vid. Selsk. Forh. (Trondheim) **41**, 1—3 (1968).

CHOWLA P., CHOWLA S. [1] On the integer points on some special hyper-elliptic curves over a finite field, J. Number Theory **8**, 280—281 (1976).

[2] On kth power residues, J. Number Theory **10**, 351—353 (1978).

CHOWLA S. [1] Some formulae of the Gauss sum type, Tôhoku Math. J. **30**, 226—234 (1929); Corrigenda, ibid. **32**, 109—110 (1930).

[2] Some formulae of the Gauss sum type (II), Tôhoku Math. J. **32**, 352—353 (1930).

[3] A theorem on characters. II, J. Indian Math. Soc. **19**, 279—284 (1932)

[4] A property of biquadratic residues, Proc. Nat. Acad. Sci. India Sect. A **14**, 45—46 (1944).

[5] A formula similar to Jacobsthal's for the explicit value of x in $p = x^2 + y^2$ where p is a prime of the form $4k+1$, Proc. Lahore Philos. Soc. **7** (1945).

[6] The last entry in Gauss' diary, Proc. Nat. Acad. Sci. U. S. A. **35**, 244—246 (1949).

[7] The Riemann zeta and allied functions, Bull. Amer. Math. Soc. **58**, 287—305 (1952).
[8] Some results in number-theory, Norske Vid. Selsk. Forh. (Trondheim) **33**, 43—44 (1960).
[9] A generalization of Meyer's theorem on indefinite quadratic forms in five or more variables, J. Indian Math. Soc. **25**, 41 (1961).
[10] On the congruence $\sum_{i=1}^{s} a_i x_i^k \equiv 0 \pmod{p}$, J. Indian Math. Soc. **25**, 47—48 (1961).
[11] On a formula of Jacobsthal, Norske Vid. Selsk. Forh. (Trondheim) **34**, 105—106 (1961).
[12] Some conjectures in elementary number theory, Norske Vid. Selsk. Forh. (Trondheim) **35**, 13 (1962).
[13] On Gaussian sums, Norske Vid. Selsk. Forh. (Trondheim) **35**, 66—67 (1962).
[14] On Gaussian sums, Proc. Nat. Acad. Sci. U. S. A. **48**, 1127—1128 (1962).
[15] On a conjecture of Artin. I, II, Norske Vid. Selsk. Forh. (Trondheim) **36**, 135—138, 139—141 (1963).
[16] The Riemann Hypothesis and Hilbert's Tenth Problem, Gordon and Breach, New York, 1965.
[17] A note on the construction of finite Galois fields $GF(p^n)$, J. Math. Anal. Appl. **15**, 53—54 (1966).
[18] An algebraic proof of the law of quadratic reciprocity, Norske Vid. Selsk. Forh. (Trondheim) **39**, 59 (1966).
[19] On the class-number of the function field $y^2 = f(x)$ over $GF(p)$. I, II, Norske Vid. Selsk. Forh. (Trondheim) **39**, 86—88 (1966); ibid. **40**, 7—10 (1967).
[20] Observation on a theorem of Stark, Norske Vid. Selsk. Forh. (Trondheim) **40**, 34—36 (1967).
[21] On some character sums, Norske Vid. Selsk. Forh. (Trondheim) **40**, 62—66 (1967).
[22] On Kloosterman's sum, Norske Vid. Selsk. Forh. (Trondheim) **40**, 70—72 (1967).
[23] On substitution polynomials (mod p), Norske Vid. Selsk. Forh. (Trondheim) **41**, 4—6 (1968).

CHOWLA S., COWLES J., COWLES M. [1] On the number of zeros of diagonal cubic forms, J. Number Theory **9**, 502—506 (1977).
[2] Congruence properties of the number of solutions of some equations, J. reine angew. Math. **298**, 101—103 (1978).
[3] The number of zeroes of $x^3 + y^3 + cz^3$ in certain finite fields, J. reine angew. Math. **299/300**, 406—410 (1978).
[4] On the difference of cubes (mod p), Acta Arith. **37**, 61—65 (1980).

CHOWLA S., HASSE H. [1] On a paper of Bombieri, Norske Vid. Selsk. Forh. (Trondheim) **41**, 30—33 (1968).

CHOWLA S., MANN H. B., STRAUS E. G. [1] Some applications of the Cauchy—Davenport theorem, Norske Vid. Selsk. Forh. (Trondheim) **32**, 74—80 (1959).

CHOWLA S., RYSER H. J. [1] Combinatorial problems, Canad. J. Math. **2**, 93—99 (1950).

CHOWLA S., SHIMURA G. [1] On the representation of zero by a linear combination of kth powers, Norske Vid. Selsk. Forh. (Trondheim) **36**, 169—176 (1963).

CHOWLA S., SMITH R. A. [1] On certain functional equations, Norske Vid. Selsk. Forh. (Trondheim) **40**, 43—47 (1967).

CHOWLA S., VIJAYARAGHAVAN T. [1] The complete factorization (mod p) of the cyclotomic polynomial of order $p^2 - 1$, Proc. Nat. Acad. Sci. India Sect. A **14**, 101—105 (1044).

CHOWLA S., ZASSENHAUS H. [1] Some conjectures concerning finite fields, Norske Vid. Selsk. Forh. (Trondheim) **41**, 34—35 (1968).

CHURCH R. [1] Tables of irreducible polynomials for the first four prime moduli, Ann. of Math. (2) **36**, 198—209 (1935).

CICCHESE M. [1] Sulle cubiche di un piano di Galois, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **32**, 38—42 (1962).
[2] Sulle cubiche di un piano di Galois, Rend. Mat. e Appl. (5) **24**, 291—330 (1965).
[3] Sulle cubiche di un piano lineare $S_{2,q}$, con $q \equiv 1 \pmod 3$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **48**, 584—588 (1970).
[4] Sulle cubiche di un piano lineare $S_{2,q}$, con $q \equiv 1 \pmod 3$, Rend. Mat. (6) **4**, 349—383 (1971).
CIPOLLA M. [1] Un metodo per la risoluzione della congruenza di secondo grado, Rend. Accad. Sci. Fis. Mat. Napoli (3) **9**, 153—163 (1903).
[2] Formule di risoluzione della congruenza binomia quadratica e biquadratica, Rend. Accad. Sci. Fis. Mat. Napoli (3) **11**, 13—17 (1905).
[3] Sulle funzioni simmetriche delle soluzioni comuni a piú congruenze secondo un modulo primo, Periodico di Mat. **22**, 36—41 (1907).
[4] Sulla risoluzione apiristica delle congruenze binomie secondo un modulo primo, Math. Ann. **63**, 54—61 (1907).
[5] Formule di risoluzione apiristica delle equazioni di grado qualunque in un corpo finito, Rend. Circ. Mat. Palermo **54**, 199—206 (1930).
CLAASEN H. L. [1] The group of units in $GF(q)[x]/(a(x))$, Indag. Math. **39**, 245—255 (1977).
[2] The multiplications in $GF(q)[x]/(a(x))$ considered as linear transformations, Linear Algebra Appl. **22**, 105—123 (1978).
CLAY J. R., MALONE J. J., Jr. [1] The near-rings with identities on certain finite groups, Math. Scand. **19**, 146—150 (1966).
COHEN E. [1] Sums of an even number of squares in $GF[p^n, x]$, I, II, Duke Math. J. **14**, 251—267, 543—557 (1947).
[2] Sums of an odd number of squares in $GF[p^n, x]$, Duke Math. J. **15**, 501—511 (1948).
[3] An extension of Ramanujan's sums, Duke Math. J. **16**, 85—90 (1949).
[4] Sums of products of polynomials in a Galois field, Duke Math. J. **18**, 425—430 (1951).
[5] Rings of arithmetic functions, Duke Math. J. **19**, 115—129 (1952).
[6] Arithmetic functions of polynomials, Proc. Amer. Math. Soc. **3**, 352—358 (1952).
[7] Representations by cubic congruences, Proc. Nat. Acad. Sci. U. S. **A. 39**, 119—121 (1953).
[8] Congruence representations in algebraic number fields, Trans. Amer. Math. Soc. **75**, 444—470 (1953).
[9] The number of solutions of certain cubic congruences, Pacific J. Math. **5**, 877—886 (1955).
[10] Simultaneous pairs of linear and quadratic equations in a Galois field, Canad. J. Math. **9**, 74—78 (1957).
[11] The number of simultaneous solutions of a quadratic equation and a pair of linear equations over a Galois field, Rev. Roum. Math. Pures Appl. **8**, 297—303 (1963).
[12] Linear and quadratic equations in a Galois field with applications to geometry, Duke Math. J. **32**, 633—641 (1965).
[13] Quadratic congruences with an odd number of summands, Amer. Math. Monthly **73**, 138—143 (1966).
COHEN H., LENSTRA H. W., Jr. [1] Primality testing and Jacobi sums, Report 82-18, Dept. of Math., Univ. of Amsterdam, 1982.
COHEN S. D. [1] The distribution of irreducible polynomials in several indeterminates over a finite field, Proc. Edinburgh Math. Soc. (2) **16**, 1—17 (1968).
[2] On irreducible polynomials of certain types in finite fields, Proc. Cambridge Philos. Soc. **66**, 335—344 (1969).
[3] Further arithmetical functions in finite fields, Proc. Edinburgh Math. Soc. (2) **16**, 349—363 (1969).

[4] Some arithmetical functions in finite fields, Glasgow Math. J. **11**, 21—36 (1970).
[5] The distribution of polynomials over finite fields, Acta Arith. **17**, 255—271 (1970).
[6] The distribution of polynomials over finite fields, II, Acta Arith. **20**, 53—62 (1972).
[7] Uniform distribution of polynomials over finite fields, J. London Math. Soc. (2) **6**, 93—102 (1972).
[8] The values of a polynomial over a finite field, Glasgow Math. J. **14**, 205—208 (1973).
[9] Value sets of functions over finite fields, Acta Arith. **39**, 339—359 (1981).
[10] The irreducibility of compositions of linear polynomials over a finite field, Compositio Math. **47**, 149—152 (1982).
COLLINS G. E. [1] Computing multiplicative inverses in *GF* (*p*), Math. Comp **23**, 197—200 (1969).
[2] The calculation of multivariate polynomial resultants, J. Assoc. Comput. Mach. **18**, 515—532 (1971).
[3] Computer algebra of polynomials and rational functions, Amer. Math. Monthly **80**, 725—755 (1973).
CONSTANTIN J., COURTEAU B. [1] Partitions linéaires arguésiennes d'un espace vectoriel, Discrete Math. **33**, 139—147 (1981).
CONWAY J. H. [1] A tabulation of some information concerning finite fields, Computers in Mathematical Research (R. F. Churchhouse and J.-C. Herz, eds.), pp. 37—50, North-Holland, Amsterdam, 1968.
COOPER R. H. [1] Linear transformations in Galois fields and their application to cryptography, Cryptologia **4**, 184—188 (1980).
CORDES C. M. [1] A note on Pall partitions over finite fields, Linear Algebra Appl. **12**, 81—85 (1975).
[2] Some results on totally isotropic subspaces and five-dimensional quadratic forms over *GF* (*q*), Canad. J. Math. **27**, 271—275 (1975).
CORDONE G. [1] Sulla congruenza generale di 4° grado secondo un modulo primo, Rend. Circ. Mat. Palermo **9**, 209—243 (1895).
CORNACCHIA G. [1] Sulla congruenza $x^n + y^n \equiv z^n \pmod{p}$, Giorn. Mat. Battaglini **47**, 219—268 (1909).
CORSON H. H. [1] On some special systems of equations, Pacific J. Math. **6**, 449—452 (1956).
CORZATT C. E. [1] Permutation polynomials over the rational numbers, Pacific J. Math. **61**, 361—382 (1975).
CRAMPTON T. H. M., WHAPLES G. [1] Additive polynomials. II, Trans. Amer. Math. Soc. **78**, 239—252 (1955).
CRAVEN T., CSORDAS G. [1] Multiplier sequences for fields, Illinois J. Math. **21**, 801—817 (1977).
CRELLE A. L. [1] Table des racines primitives etc. pour les nombres premiers depuis 3 jusqu'à 101, precédée d'une note sur le calcul de cette table, J. reine angew. Math. **9**, 27—53 (1832).
CROWE D. W. [1] The trigonometry of *GF* (2^{2n}) and finite hyperbolic planes, Mathematika **11**, 83—88 (1964).
CROWELL R. H. [1] Graphs of linear transformations over finite fields, J. Soc. Indust. Appl. Math. **10**, 103—112 (1962).
CUNNINGHAM A. J. C. [1] Factorisation of $(y^n \mp 1)$, $y > 12$, Messenger of Math. **57**, 72—80 (1927).
CUNNINGHAM A. J. C., WOODALL H. J. [1] Factorization of $y^n \pm 1$, $y = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers (*n*), Hodgson, London, 1925.
CUNNINGHAM A. J. C., WOODALL H. J., CREAK T. G. [1] On least primitive roots, Proc. London Math. Soc. **21**, 343—358 (1923).

ČUPONA G. [1] On periodic fields (Macedonian), Bull. Soc. Math. Phys. Macédoine **11**, 5—8 (1960).
CURTIS C. W. [1] Representation of finite groups of Lie type, Bull. Amer. Math. Soc. (N. S.) **1**, 721—757 (1979).
CZARNOTA A. [1] Congruences satisfied by a sum of powers of primitive roots with respect to a prime modulus (Polish), Prace Mat. **8**, 131—142 (1963/64).
DADE E. C., ROBINSON D. W., TAUSSKY O., WARD M. [1] Divisors of recurrent sequences, J. reine angew. Math. **214/215**, 180—183 (1964).
DAI Z. D. [1] The period of a circulant over a finite field (Chinese), Acta Math. Sinica **23**, 70—77 (1980).
DAI Z. D., FENG X. [1] Notes on finite geometries and the construction of PBIB designs. IV. Some «Anzahl» theorems in orthogonal geometry over finite fields of characteristic not 2, Sci. Sinica **13**, 2001—2004 (1964).
[2] Studies in finite geometries and the construction of incomplete block designs. IV. Some «Anzahl» theorems in orthogonal geometry over finite fields of characteristic $\neq 2$ (Chinese), Acta Math. Sinica **15**, 545—558 (1965); Chinese Math. Acta **7**, 265—280 (1965).
DALEN K. [1] On a theorem of Stickelberger, Math. Scand. **3**, 124—126 (1955).
DALLA R. H., PORTER A. D. [1] A consideration by rank of the matrix equation $AX_1 \ldots X_n = B$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **52**, 301—311 (1972).
[2] The matrix equation $U_1 \ldots U_n A V_1 \ldots V_m = B$ over a finite field, Math. Nachr. **57**, 321—335 (1973).
DARBI G. [1] Sulla riducibilità delle equazioni algebriche, Ann. Mat. Pura Appl. (4) **4**, 185—208 (1927).
DAVENPORT H. [1] On the distribution of quadratic residues (mod p), J. London Math. Soc. **6**, 49—54 (1931).
[2] On the distribution of l-th power residues (mod p), J. London Math. Soc. **7**, 117—121 (1932).
[3] On the distribution of quadratic residues (mod p). II, J. London Math. Soc. **8**, 46—52 (1933).
[4] On certain exponential sums, J. reine angew. Math. **169**, 158—176 (1933).
[5] On the addition of residue classes, J. London Math. Soc. **10**, 30—32 (1935).
[6] On primitive roots in finite fields, Quart. J. Math. **8**, 308—312 (1937).
[7] On character sums in finite fields, Acta Math. **71**, 99—121 (1939).
[8] Multiplicative Number Theory, Markham, Chicago, 1967. [Имеется перевод: ДЭВЕНПОРТ Г. Мультипликативная теория чисел. — М.: Наука, 1971.]
[9] Bases for finite fields, J. London Math. Soc. **43**, 21—39 (1968); Addendum, ibid. **44**, 378 (1969).
[10] A property of polynomials over a finite field, Mathematika **22**, 151—153 (1975).
DAVENPORT H., ERDÖS P. [1] The distribution of quadratic and higher residues, Publ. Math. Debrecen **2**, 252—265 (1952).
DAVENPORT H., HASSE H. [1] Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. reine angew. Math. **172**, 151—182 (1935).
DAVENPORT H., HEILBRONN H. [1] On an exponential sum, Proc. London Math. Soc. (2) **41**, 449—453 (1936).
DAVENPORT H., LEWIS D. J. [1] Exponential sums in many variables, Amer. J. Math. **84**, 649—665 (1962).
[2] Notes on congruences (I), Quart. J. Math. (2) **14**, 51—60 (1963).
[3] Character sums and primitive roots in finite fields, Rend. Circ. Mat. Palermo (2) **12**, 129—136 (1963).
[4] Notes on congruences (II), Quart. J. Math. (2) **14**, 153—159 (1963).
[5] Homogeneous additive equations, Proc. Royal Soc. London Ser. A **274**, 443—460 (1963).
[6] Cubic equations of additive type, Phil. Trans. Royal Soc. London Ser. A **261**, 97—136 (1966).

[7] Notes on congruences (III), Quart. J. Math. (2) **17**, 339—344 (1966).
[8] Simultaneous equations of additive type, Phil. Trans. Royal Soc. London Ser. A **264**, 557—595 (1969).
DAVIDA G. I. [1] Inverse of elements of a Galois field, Electron. Lett. **8**, 518—520 (1972).
DAVIO M., DESCHAMPS J.-P., THAYSE A. [1] Discrete and Switching Functions, McGraw-Hill, New York, 1978.
DAVIS A. S. [1] The Euler—Fermat theorem for matrices, Duke Math. J. **18**, 613—617 (1951).
DAYKIN D. E. [1] On the rank of the matrix $f(A)$ and the enumeration of certain matrices over a finite field, J. London Math. Soc. **35**, 36—42 (1960).
[2] Distribution of bordered persymmetric matrices in a finite field, J. reine angew. Math. **203**, 47—54 (1960).
[3] The irreducible factors of $(cx + d)\, x^{q^m} - (ax + b)$ over $GF(q)$, Quart. J. Math. (2) **14**, 61—64 (1963).
[4] On linear sequences over a finite field, Amer. Math. Monthly **70**, 637—642 (1963).
[5] Polynomials over a finite field, J. London Math. Soc. **40**, 326—331 (1965).
[6] Generation of irreducible polynomials over a finite field, Amer. Math. Monthly **72**, 646—648 (1965).
DAYKIN D. E., DRESEL L. A. G., HILTON A. J. W. [1] The structure of second order sequences in a finite field, J. reine angew. Math. **270**, 77—96 (1974).
DE BRUIJN N. G. [1] A combinatorial problem, Indag. Math. **8**, 461—467 (1946)
DE CARLI D. J. [1] A generalized Fibonacci sequence over an arbitrary ring, Fibonacci Quart. **8**, 182—184, 198 (1970).
DEDEKIND R. [1] Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus, J. reine angew. Math. **54**, 1—26 (1857), Gesammelte Math. Werke, vol. 1, pp. 40—66, Vieweg, Braunschweig, 1930.
[2] Beweis für die Irreductibilität der Kreistheilungsgleichungen, J. reine angew. Math. **54**, 27—30 (1857); Gesammelte Math. Werke, vol. 1, pp. 68—71, Vieweg, Braunschweig, 1930.
[3] Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abh. Kgl. Ges. Wiss. Göttingen **23**, 1—23 (1878); Gesammelte Math. Werke, vol. 1, pp. 202—230, Vieweg, Braunschweig, 1930.
DE GROOTE R. [1] Les cubiques dans un plan projectif sur un corps de caractéristique trois, Acad. Roy. Belg. Bull. Cl. Sci. (5) **59**, 1140—1155 (1973).
[2] Les cubiques dans un plan projectif sur un corps fini de caractéristique 3, Acad. Roy. Belg. Bull. Cl. Sci. (5) **60**, 43—57 (1974).
DE GROOTE R., HIRSCHFELD J. W. P. [1] The number of points on an elliptic cubic curve over a finite field, European J. Combin. **1**, 327—333 (1980).
DELIGNE P. [1] La conjecture de Weil pour les surfaces $K3$, Invent. Math. **15**, 206—226 (1972).
[2] Les intersections complètes de niveau de Hodge un, Invent. Math. **15**, 237—250 (1972).
[3] La conjecture de Weil. I, Inst. Hautes Etudes Sci. Publ. Math. **43**, 273—307 (1974).
[4] Applications de la formule des traces aux sommes trigonométriques, Cohomologie Etale (Séminaire de Géométrie Algébrique du Bois—Marie SGA $4^1/_2$), Lecture Notes in Math., vol. 569, pp. 168—232, Springer-Verlag, Berlin—Heidelberg—New York, 1977.
[5] Sommes de Gauss cubiques et revêtements de SL (2) (d'après S. J. Patterson), Séminaire Bourbaki 1978/79, Exp. 539, Lecture Notes in Math., vol. 770, pp. 244—277, Springer-Verlag, Berlin—Heidelberg—New York, 1980.
[6] La conjecture de Weil. II, Inst. Hautes Etudes Sci. Publ. Math. **52**, 137—252 (1980).
DELSARTE J. [1] Nombre de solutions des équations polynômiales sur un corps

fini (d'après A. Weil), Séminaire Bourbaki 1950/1951, Exp. 39, Benjamin, New York, 1966.
DELSARTE P. [1] A geometric approach to a class of cyclic codes, J. Combinatorial Theory **6**, 340—359 (1969).
[2] On cyclic codes that are invariant under the general linear group, IEEE Trans. Information Theory **IT-16**, 760—769 (1970).
[3] Bilinear forms over a finite field, with applications to coding theory, J. Combinatorial Theory Ser. A **25**, 226—241 (1978).
DELSARTE P., GOETHALS J.-M. [1] Irreducible binary cyclic codes of even dimension, Proc. Second Chapel Hill Conf. on Combinatorial Math. and Its Appl. (Chapel Hill, N. C., 1970), pp. 100—113, Univ. of North Carolina Press, Chapel Hill, N. C., 1970.
[2] Alternating bilinear forms over $GF(q)$, J. Combinatorial Theory Ser. A **19**, 26—50 (1975).
[3] Unrestricted codes with the Golay parameters are unique, Discrete Math. **12**, 211—224 (1975).
DELSARTE P., GOETHALS J.-M., SEIDEL J. J. [1] Orthogonal matrices with zero diagonal II, Canad. J. Math. **23**, 816—832 (1971).
DELSARTE P., MCELIECE R. J. [1] Zeros of functions in finite abelian group algebras, Amer. J. Math. **98**, 197—224 (1976).
DE MATHAN B. [1] Sur un théorème métrique d'équirépartition mod 1 dans un corps de séries formelles sur un corps fini, C. R. Acad. Sci. Paris Sér. A **265**, 289—291 (1967).
[2] Théorème de Koksma dans un corps de séries formelles sur un corps fini, Sém. Delange—Pisot—Poitou 1967/68, Théorie des Nombres, Exp. 4, Secrétariat Math., Paris, 1969.
[3] Approximations diophantiennes dans un corps local, Bull. Soc. Math. France Suppl. Mém. **21** (1970).
DEMBOWSKI P. [1] Möbiusebenen gerader Ordnung, Math. Ann. **157**, 179—205 (1964).
[2] Finite Geometries, Springer-Verlag, Berlin—Heidelberg—New York, 1968.
DÉNES J., KEEDWELL A. D. [1] Latin Squares and Their Applications, Academic Press, New York, 1974.
DE POLIGNAC C. [1] Sur la représentation analytique des substitutions, Bull. Soc. Math. France **9**, 59—67 (1881).
DESHOUILLERS J.-M. [1] Sur la répartition modulo 1 des puissances d'un élément de $\mathbb{F}_q((X))$, Proc. Quenn's Number Theory Conf. (Kingston, Ont., 1979), Queen's Papers in Pure and Appl. Math., no. 54, pp. 437—439, Queen's Univ., Kingston, Ont., 1980.
[2] La répartition modulo 1 des puissances de rationnels dans l'anneau des séries formelles sur un corps fini, Sém. Théorie des Nombres 1979—1980, Exp. 5, Univ. Bordeaux I, Talence, 1980.
[3] La répartition modulo 1 des puissances d'un élément dans $F_q((X))$, Recent Progress in Analytic Number Theory (H. Halberstam and C. Hooley, eds.), vol. 2, pp. 69—72, Academic Press, London, 1981.
DESHOUILLERS J.-M., IWANIEC H. [1] Kloosterman sums and Fourier coefficients of cusp forms, Invent. Math. **70**, 219—288 (1982).
DESMAREST E. [1] Théorie des nombres, Paris, 1852.
DEURING M. [1] Galoissche Theorie und Darstellungstheorie, Math. Ann. **107**, 140—144 (1933).
[2] Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg **14**, 197—272 (1941).
[3] The zeta-functions of algebraic curves and varieties, J. Indian Math. Soc. **20**, 89—101 (1956).
[4] Lectures on the Theory of Algebraic Functions of one Variable, Lecture Notes in Math., vol. 314, Springer-Verlag, Berlin—Heidelberg—New York, 1973.

DICKEY L. J., KAIRIES H.-H., SHANK H. S. [1] Analogs of Bernoulli polynomials in fields Z_p, Aequationes Math. **14**, 401—404 (1976).

DICKSON L. E. [1] Analytic functions suitable to represent substitutions, Amer. J. Math. **18**, 210—218 (1896).

[2] The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. of Math. **11**, 65—120, 161—183 (1897).

[3] Higher irreducible congruences, Bull. Amer. Math. Soc. **3**, 381—389 (1897).

[4] Determination of the structure of all linear homogeneous groups in a Galois field which are defined by a quadratic invariant, Amer. J. Math. **21**, 193—256 (1899).

[5] Certain subgroups of the Betti—Mathieu group, Amer. J. Math. **22**, 49—54 (1900).

[6] Proof of the existence of the Galois field of order p^r for every integer r and prime number p, Bull. Amer. Math. Soc. **6**, 203—204 (1900).

[7] Linear Groups with an Exposition of the Galois Field Theory, Teubner, Leipzig, 1901; Dover, New York, 1958.

[8] On finite algebras, Göttinger Nachr. **1905**, 358—393.

[9] Criteria for the irreducibility of functions in a finite field, Bull. Amer. Math. Soc. **13**, 1—8 (1906).

[10] On the theory of equations in a modular field, Bull. Amer. Math. Soc. **13**, 8—10 (1906).

[11] On quadratic, hermitian and bilinear forms, Trans. Amer. Math. Soc. **7**, 275—292 (1906).

[12] Invariants of binary forms under modular transformations, Trans. Amer. Math. Soc. **8**, 205—232 (1907).

[13] Invariants of the general quadratic form modulo 2, Proc. London Math. Soc. (2) **5**, 301—324 (1907).

[14] On the last theorem of Fermat, Messenger of Math. (2) **38**, 14—32 (1908).

[15] On the canonical forms and automorphs of ternary cubic forms, Amer. J. Math. **30**, 117—128 (1908).

[16] On triple algebras and ternary cubic forms, Bull. Amer. Math. Soc. **14**, 160—169 (1908).

[17] On the congruence $x^n + y^n + z^n \equiv 0 \pmod{p}$, Amer. Math. Monthly **15**, 217—222 (1908).

[18] Invariantive reduction of quadratic forms in the $GF[2^n]$, Amer. J. Math. **30**, 263—281 (1908).

[19] On higher congruences and modular invariants, Bull. Amer. Math. Soc. **14**, 313—318 (1908).

[20] On families of quadratic forms in a general field, Quart. J. Pure Appl. Math. **39**, 316—333 (1908).

[21] On the last theorem of Fermat. II, Quart. J. Pure Appl. Math. **40**, 27—45 (1908).

[22] Rational reduction of a pair of binary quadratic forms; their modular invariants, Amer. J. Math. **31**, 103—146 (1909).

[23] Definite forms in a finite field, Trans. Amer. Math. Soc. **10**, 109—122 (1909).

[24] General theory of modular invariants, Trans. Amer. Math. Soc. **10**, 123—158 (1909).

[25] On the congruence $x^n + y^n + z^n \equiv 0 \pmod{p}$, J. reine angew. Math. **135**, 134—141 (1909).

[26] Lower limit for the number of sets of solutions of $x^e + y^e + z^e \equiv 0 \pmod{p}$, J. reine angew. Math. **135**, 181—188 (1909).

[27] A theory of invariants, Amer. J. Math. **31**, 337—354 (1909).

[28] On the representation of numbers by modular forms, Bull. Amer. Math. Soc. **15**, 338—347 (1909).

[29] An invariantive investigation of irreducible binary modular forms, Trans. Amer. Math. Soc. **12**, 1—18 (1911).
[30] A fundamental system of invariants of the general modular linear group with a solution of the form problem, Trans. Amer. Math. Soc. **12**, 75—98 (1911).
[31] Note on cubic equations and congruences, Ann. of Math. (2) **12**, 149—152 (1911).
[32] On non-vanishing forms, Quart. J. Pure Appl. Math. **42**, 162—171 (1911).
[33] Congruencial theory of functions of several variables, Bull. Amer. Math. Soc. **17**, 293—294 (1911).
[34] Proof of the finiteness of modular covariants, Trans. Amer. Math. Soc. **14**, 299—310 (1913).
[35] On Invariants and the Theory of Numbers, American Math. Society, New York, 1914.
[36] The invariants, seminvariants and linear covariants of the binary quartic form modulo 2, Ann. of Math. (2) **15**, 114—117 (1914).
[37] Modular invariants of the system of a binary cubic, quadratic and linear form, Quart. J. Pure Appl. Math. **45**, 373—384 (1914).
[38] Recent progress in the theories of modular and formal invariants and in modular geometry, Proc. Nat. Acad. Sci. U. S. A. **1**, 1—4 (1915).
[39] Projective classification of cubic surfaces modulo 2, Ann. of Math. (2) **16**, 139—157 (1915).
[40] History of the theory of Numbers, vol. 1, Carnegie Institute, Washington, D. C., 1919.
[41] History of the Theory of Numbers, vol. 2, Carnegie Institute, Washington, D. C., 1920.
[42] History of the Theory of Numbers, vol. 3, Carnegie Institute, Washington, D. C., 1923.
[43] Ternary quadratic forms and congruences, Ann. of Math. (2) **28**, 333—341 (1927).
[44] Cyclotomy and trinomial congruences, Trans. Amer. Math. Soc. **37**, 363—380 (1935).
[45] Cyclotomy when e is composite, Trans. Amer. Math. Soc. **38**, 187—200 (1935).
[46] Cyclotomy, higher conrguences, and Waring's problem, Amer. J. Math. **57**, 391—424 (1935).
[47] Cyclotomy, higher congruences, and Waring's problem II, Amer. J. Math. **57**, 463—474 (1935).
[48] Congruences involving only e-th powers, Acta Arith. **1**, 161—167 (1936).
DICKSON L. E., MITCHELL H. H., VANDIVER H. S., WAHLIN G. E. [1] Algebraic Numbers, National Research Council, Washington, D. C., 1923.
DIDERRICH G. T., MANN H. B. [1] Representations by k-th powers in $GF(q)$, J. Number Theory **4**, 269—273 (1972).
DIEUDONNÉ J. [1] Pseudo-discriminant and Dickson invariant, Pacific J. Math. **5**, 907—910 (1955).
[2] La géométrie des groupes classiques, 3rd ed., Springer-Verlag, Berlin—Heidelberg—New York, 1971. [Имеется перевод: ДЬЕДОННЕ Ж. Геометрия классических групп. — М.: Мир. 1974.]
DIFFIE W., HELLMAN M. E. [1] New directions in cryptography, IEEE Trans. Information Theory IT-22, 644—654 (1976).
DIJKSMA A. [1] The measure theoretic approach to uniform distribution of sequences in $GF[q, x]$, Mathematica (Cluj) **11**, 221—240 (1969).
[2] Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$, Part I, Indag. Math. **31**, 376—383 (1969).
[3] Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$, Part II, Indag. Math. **32**, 187—195 (1970).
[4] Metrical theorems concerning uniform distribution in $GF[q, x]$ and $GF\{q, x\}$, Nieuw Arch. Wisk. (3) **18**, 279—293 (1970).
DILLON J. F., MORRIS R. A. [1] On a paper of E. R. Berlekamp, H. M. Fredricksen and R. C. Proto: «Minimum conditions for uniquely determining

the generator of a linear sequence» (Utilitas Math. 5 (1974), 305—315), Utilitas Math. 5, 317—322 (1974).

DIRICHLET G. L. [1] Über eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen, Abh. Königl. Preuss. Akad. Wiss. **1835**, 391—407; Werke, vol. 1, pp. 237—256, Reimer, Berlin, 1889.

DIXON J. D. [1] The Structure of Linear Groups, Van Nostrand Reinhold, London, 1971.

D'OCAGNE M. [1] Mémoire sur les suites récurrentes, J. de l'Ecole Polytechnique **64**, 151—224 (1894).

DOČEV K., DIMITROV D. [1] Certain properties of homogeneous equations in finite fields (Bulgarian), Ann. Univ. Sofia Fac. Math. Méc. **64**, 269—276 (1969/70).

DODSON M. M. [1] Homogeneous additive congruences, Phil. Trans. Royal Soc. London Ser. A **261**, 163—210 (1967).

[2] On Waring's problem in $GF[p]$, Acta Arith. **19**, 147—173 (1971).

[3] On a function due to S. Chowla, J. Number Theory **5**, 287—292 (1973).

[4] On Waring's Problem in p-adic fields, Acta Arith. **22**, 315—327 (1973).

DODSON M. M., TIETÄVÄINEN A. [1] A note on Waring's problem in $GF(p)$, Acta Arith. **30**, 159—167 (1976).

DODUNEKOV S. M. [1] Существенно различные неприводимые полиномы над конечным полем, Ann. Univ. Sofia Fac. Math. Méc. **66**, 169—175 (1971/72).

[2] Коды Гоппы, Ann. Univ. Sofia Fac. Math. Méc. **68**, 317—322 (1973/74).

DOREY F., WHAPLES G. [1] Prime and composite polynomials, J. Algebra **28**, 88—101 (1974).

DÖRGE K. [1] Zur Verteilung der quadratischen Reste, Jber. Deutsch. Math.-Verein, **38**, 41—49 (1929).

DORNHOFF L. L., HOHN F. E. [1] Applied Modern Algebra, Macmillan, New York, 1978.

DRESS F. [1] Fonctions arithmétiques sur l'anneau des polynômes à coefficients dans un corps fini, Sém. Delange—Pisot 1962/63, Exp. 13, Secrétariat Math., Paris, 1967.

DUBOIS E., PAYSAN-LE ROUX R. [1] Approximations simultanées dans un corps de séries formelles, C. R. Acad. Sci. Paris Sér. A **274**, 437—440 (1972).

DUNN K. B., LIDL R. [1] Iterative roots of functions over finite fields, Math. Nachr., **115**, 319—329 (1984).

DUNTON M. [1] Nontrivial solutions of $ax^3 + by^3 \equiv c \pmod{p}$, Norske Vid. Selsk. Forh. (Trondheim) **33**, 45—46 (1960).

[2] Bounds for pairs of cubic residues, Proc. Amer. Math. Soc. **16**, 330—332 (1965).

DUPARC H. J. A. [1] Periodicity properties of recurring sequences. I, II, Indag. Math. **16**, 331—342, 473—485 (1954).

[2] Periodicity properties of certain sets of integers, Indag. Math. **17**, 449—458 (1955).

DUSKE J., JÜRGENSEN H. [1] Codierungstheorie, Reihe Informatik, vol. 13, Bibliographisches Institut, Mannheim, 1977.

DUVALL P. F., KIBLER R. E. [1] On the parity of the frequency of cycle lengths of shift register sequences, J. Combinatorial Theory Ser. A **18**, 357—361 (1975).

DUVALL P. F., MORTICK J. C. [1] Decimation of periodic sequences, SIAM J. Appl. Math. **21**, 367—372 (1971).

DWORK B. [1] On the congruence properties of the zeta function of algebraic varieties, J. reine angew. Math. **203**, 130—142 (1960).

[2] On the rationality of the zeta function of an algebraic variety, Amer. J. Math. 82, 631—648 (1960).

[3] On the zeta function of a hypersurface I, Inst. Hautes Etudes Sci. Publ. Math. **12**, 5—68 (1968).

[4] A deformation theory for the zeta function of a hypersurface, Proc. Interna-

tional Congress of Math. (Stockholm, 1962), pp. 247—259, Institut Mittag-Leffler, Djursholm, 1963.
[5] On the zeta function of a hypersurface. II, Ann. of Math. (2) **80**, 227—299 (1964).
[6] Analytic theory of the zeta function of algebraic varieties, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), pp. 18—32, Harper and Row, New York, 1965.
[7] On zeta functions of hypersurfaces, Les Tendances Géométriques en Algèbre et Théorie des Nombres, pp. 77—82, Edition du Centre National de la Recherche Scientifique, Paris, 1966.
[8] On the zeta function of a hypersurface. III, Ann. of Math. (2) **83**, 457—519 (1966).
[9] On the rationality of zeta functions and L-series, Proc. Conf. Local Fields (Driebergen, 1966), pp. 40—55, Springer-Verlag, Berling—Heidelberg—New York, 1967.
[10] p-adic cycles, Inst. Hautes Etudes Sci. Publ. Math. **37**, 27—115 (1969).
[11] Bessel functions as p-adic functions of the argument, Duke Math. J. **41**, 711—738 (1974).
DYE R. H. [1] On the Arf-invariant, J. Algebra **53**, 36—39 (1978).
EHLICH H. [1] Neue Hadamard-Matrizen, Arch. Math. **16**, 34—36 (1965).
EICHLER M. [1] Einführung in die Theorie der algebraischen Zahlen und Funktionen, Birkhäuser Verlag, Basel, 1963.
EICHNER L. [1] Lineare Realisierbarkeit endlicher Automaten über enldichen Körpern, Acta Inform. **3**, 75—100 (1973).
EIER R., LIDL R. [1] Tschebyscheffpolynome in einer und zwei Variablen, Abh. Math. Sem. Univ. Hamburg **41**, 17—27 (1974).
EIER R., MALLECK H. [1] Anwendung von Multiplextechniken bei der Erzeugung von schnellen Pseudozufallsfolgen, Nachrichtentechn. Z. **28**, 227—231 (1975).
EISENSTEIN G. [1] Beiträge zur Kreistheilung, J. reine angew. Math. **27**, 269—278 (1844); Math. Werke, vol. 1, pp. 45—54, Chelsea, New York, 1975.
[2] Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen, J. reine angew. Math. **27**, 289—310 (1844); Math. Werke, vol. 1, pp. 59—80, Chelsea, New York, 1975.
[3] La loi de réciprocité tirée des formules de Mr. Gauss, sans avoir déterminé préalablement le signe du radical, J. reine angew. Math. **28**, 41—43 (1844); Math. Werke, vol. 1, pp. 114—116, Chelsea, New York, 1975.
[4] Lois de réciprocité, J. reine angew. Math. **28**, 53—67 (1844); Math. Werke, vol. 1, pp. 126—140, Chelsea, New York, 1975.
[5] Zur Theorie der quadratischen Zerfällung der Primzahlen $8n + 3$, $7n + 2$ und $7n + 4$, J. reine angew. Math. **37**, 97—126 (1848); Math. Werke, vol. 2, pp. 506—535, Chelsea, New York, 1975.
[6] Lehrsätze, J. reine angew. Math. **39**, 180—182 (1850); Math. Werke, vol. 2, pp. 620—622, Chelsea, New York, 1975.
ELLIOTT P. D. T. A. [1] Some notes on k-th power residues, Acta Arith. **14**, 153—162 (1968).
[2] A restricted mean value theorem, J. London Math. Soc. (2) **1**, 447—460 (1969).
[3] On the mean value of $f(p)$, Proc. London Math. Soc. (3) **21**, 28—96 (1970).
[4] The distribution of power residues and certain related results, Acta Arith. **17**, 141—159 (1970).
[5] A remark on the Dirichlet values of a completely reducible polynomial (mod p), J. Number Theory **13**, 12—17 (1981).
ELLISON W. J. [1] Waring's problem, Amer. Math. Monthly **78**, 10—36 (1971).
ELSPAS B. [1] The theory of autonomous linear sequential networks, IRE Trans. Circuit Theory **CT-6**, 45—60 (1959). [Имеется перевод: ЭЛСПАС Б. Теория автономных линейных последовательных цепей. — В кн.: Киберн. сборник, вып. 7. — М.: ИЛ, 1963, с. 90—128.]

ELSPAS B., SHORT R. A. [1] A note on optimum burst-error-correcting codes, IRE Trans. Information Theory **IT-8**, 39—42 (1962). [Имеется перевод: ЭЛСПАС Б., ШОРТ Р. Об оптимальных кодах, исправляющих пакеты ошибок. — В кн.: Теория кодирования. — М.: Мир, 1964, с. 83—96.]

EMRE E., HÜSEYIN Ö. [1] Relative primeness of multivariable polynomials, IEEE Trans. Circuits and Systems **CAS-22**, 56—57 (1975).

ENGLISH W. R. [1] Synthesis of finite state algorithms in a Galois field $GF[p^n]$, IEEE Trans. Computers **C-30**, 225—229 (1981).

ENGSTROM H. T. [1] Periodicity in sequences defined by linear recurrence relations, Proc. Nat. Acad. Sci. U. S. A. **16**, 663—665 (1930).

[2] On sequences defined by linear recurrence relations, Trans. Amer. Math. Soc. **33**, 210—218 (1931).

[3] Polynomial substitutions, Amer. J. Math. **63**, 249—255 (1941).

ENNOLA V. [1] Note on an equation in a finite field, Ann. Acad. Sci. Fenn. Ser. AI **314** (1962).

ERDÖS P. [1] Some recent advances and current problems in number theory, Lectures on Modern Mathematics, vol. 3, pp. 196—244, Wiley, New York, 1965.

ESCOTT E. B. [1] Cubic congruences with three real roots, Ann. of Math. (2) **11**, 86—92 (1910).

ESTERMANN T. [1] Vereinfachter Beweis eines Satzes von Kloosterman, Abh. Math. Sem. Univ. Hamburg **7**, 82—98 (1930).

[2] On the sign of the Gaussian sum, J. London Math. Soc. **20**, 66—67 (1945).

[3] On Kloosterman's sum, Mathematika **8**, 83—86 (1961).

[4] A new application of the Hardy—Littlewood—Kloosterman method, Proc. London Math. Soc. (3) **12**, 425—444 (1962).

EULER L. [1] Recherches sur une nouvelle espèce de quarrés magiques, Verh. Zeeuwsch Genootsch. der Wetensch. Vissingen **9**, 85—239 (1782).

EVANS R. J. [1] Generalizations of a theorem of Chowla on Gaussian sums, Houston J. Math. **3**, 343—349 (1977).

[2] Resolution of sign ambiguities in Jacobi and Jacobsthal sums, Pacific J. Math. **81**, 71—80 (1979).

[3] Unambiguous evaluations of bidecic Jacobi and Jacobsthal sums, J. Australian Math. Soc. Ser. A **28**, 235—240 (1979).

[4] Bioctic Gauss sums and sixteenth power residue difference sets, Acta Arith. **38**, 37—46 (1980).

[5] Note on intersections of translates of powers in finite fields, Hokkaido Math. J. **9**, 135—137 (1980).

[6] The $2r$-th power character of 2, J. reine angew. Math. **315**, 174—189 (1980).

[7] Identities for products of Gauss sums over finite fields, L'Enseignement Math. (2) **27**, 197—209 (1981).

[8] Pure Gauss sums over finite fields, Mathematika **28**, 239—248 (1981).

[9] Rational reciprocity laws, Acta Arith. **39**, 281—294 (1981).

[10] Twenty-fourth power residue difference sets, Math. Comp. (to appear).

EVANS R. J., HILL J. R. [1] The cyclotomic numbers of order sixteen, Math. Comp. **33**, 827—835 (1979).

EVANS T. A., MANN H. B. [1] On simple difference sets, Sankhyā **11**, 357—364 (1951).

FADINI A. [1] Un'interpretazione mediante algebre dei campi finiti di Galois di ordine p^n, Rend. Accad. Sci. Fis. Mat. Napoli (4) **19**, 42—44 (1952).

FAIRCLOTH O. B. [1] Summary of new results concerning the solutions of equations in finite fields, Proc. Nat. Acad. Sci. U. S. A. **37**, 619—622 (1951).

[2] On the number of solutions of some general types of equations in a finite field, Canad. J. Math. **4**, 343—351 (1952).

FAIRCLOTH O. B., VANDIVER H. S. [1] On multiplicative properties of a generalized Jacobi—Cauchy cyclotomic sum, Proc. Nat. Acad. Sci. U. S. A. **36**, 260—267 (1950).

[2] On certain diophantine equations in rings and fields, Proc. Nat. Acad. Sci. U. S. A. **38**, 52—57 (1952).

FANO G. [1] Sui postulati fondamentali della geometria proiettiva in uno spazio a un numero qualunque di dimensioni, Giorn. Mat. Battaglini **30**, 106—132 (1892).

FATEMAN R. J. [1] Polynomial multiplication, powers and asymptotic analysis: Some comments, SIAM J. Computing **3**, 196—213 (1974).

FATOU P. [1] Sur les fonctions qui admettent plusieurs théorèmes de multiplication, C. R. Acad. Sci. Paris. **173**, 571—573 (1921).

FEIT W., FINE N. J. [1] Pairs of commuting matrices over a finite field, Duke Math. J. **27**, 91—94 (1960).

FEIT W., REES E. [1] A criterion for a polynomial to factor completely over the integers, Bull. London Math. Soc. **10**, 191—192 (1978).

FENG K. Q. [1] Pseudo-random properties of linear shift register sequences (Chinese), Acta Math. Sinica **19**, 192—202 (1976).

FENG X., DAI Z. D. [1] Notes on finite geometries and the construction of PBIB designs. V. Some «Anzahl» theorems in orthogonal geometry over finite fields of characteristic 2, Sci. Sinica **13**, 2005—2008 (1964).

[2] Studies in finite geometries and the construction of incomplete block designs. V. Some «Anzahl» theorems in orthogonal geometry over finite fields of characteristic 2 (Chinese), Acta Math. Sinica **15**, 664—682 (1965); Chinese Math. Acta **7**, 392—410 (1965).

FIDUCCIA C. M., ZALCSTEIN Y. [1] Algebras having linear multiplicative complexities, J. Assoc. Comput. Mach. **24**, 311—331 (1977).

FILLMORE J. P. [1] A note on split dilations defined by higher residues, Proc. Amer. Math. Soc. **18**, 171—174 (1967).

FILLMORE J. P., MARX M. L. [1] Linear recursive sequences, SIAM Rev. **10**, 342—353 (1968).

FINE N. J. [1] On the asymptotic distribution of the elementary symmetric functions (mod p), Trans. Amer. Math. Soc. **69**, 109—129 (1950).

FINE N. J., HERSTEIN I. N. [1] The probability that a matrix be nilpotent, Illinois J. Math. **2**, 499—504 (1958).

FINE N. J., NIVEN I. [1] The probability that a determinant be congruent to a (mod m), Bull. Amer. Math. Soc. **50**, 89—93 (1944).

FISHER R. A. [1] The Design of Experiments, Oliver and Boyd, Edinburgh, 1942.

FISHER S. D., ALEXANDER M. N. [1] Matrices over a finite field, Amer. Math. Monthly **73**, 639—641 (1966).

FITZPATRICK G. B. [1] Synthesis of binary ring counters of given periods, J. Assoc. Comput. Mach. **7**, 287—297 (1960).

FLYE SAINTE-MARIE C. [1] Réponse à la question 48, L'Interméd. Math. **1**, 107—110 (1894).

FORNEY G. D., Jr. [1] On decoding BCH codes, IEEE Trans. Information Theory **IT-11**, 549—557 (1965).

FORSYTH A. R. [1] Primitive roots of prime numbers and their residues, Messenger of Math. (2) **13**, 169—192 (1884).

FRALEIGH J. B. [1] A First Course in Abstract Algebra, Addison-Wesley, Reading, Mass., 1967.

FRAME J. S. [1] A short proof of quadratic reciprocity, Amer. Math. Monthly **85**, 818—819 (1978).

FRATTINI G. [1] Intorno ad un teorema di Lagrange, Atti Reale Accad. Lincei Rend. (4) **1**, 136—142 (1885).

[2] Sulle congruenze omogenee e simmetriche con un numero primo di variabili, Periodico di Mat. **29**, 49—53 (1913).

FRAY R., GILMER R. [1] On solvability by radicals of finite fields, Math. Ann. **199**, 279—291 (1972).

FREDMAN M. L. [1] Congruence formulas obtained by counting irreducibles, Pacific J. Math. **35**, 613—624 (1970).

[2] The distribution of absolutely irreducible polynomials in several indeterminates, Proc. Amer. Math. Soc. **31**, 387—390 (1972).

FREDRICKSEN H. [1] A class of nonlinear de Bruijn cycles, J. Combinatorial Theory Ser. A **19**, 192—199 (1975).

[2] A survey of full length nonlinear shift register cycle algorithms, SIAM Rev. **24**, 195—221 (1982).

FREDRICKSEN H., KESSLER I. [1] Lexicographic compositions and de Bruijn sequences, J. Combinatorial Theory Ser. A **22**, 17—30 (1977).

FREDRICKSEN H., WISNIEWSKI R. [1] On trinomials $x^n + x^2 + 1$ and $x^{8l\pm3} + x^k + 1$ irreducible over *GF* (2), Information and Control **50**, 58—63 (1981).

FREDRICSSON S. A. [1] Pseudo-randomness properties of binary shift register sequences, IEEE Trans. Information Theory **IT-21**, 115—120 (1975).

FRIED M. [1] Arithmetical properties of value sets of polynomials, Acta Arith. **15**, 91—115 (1969).

[2] On a conjecture of Schur, Michigan Math. J. **17**, 41—55 (1970).

[3] On a theorem of Ritt and related Diophantine problems, J. reine angew. Math. **264**, 40—55 (1973).

[4] On a theorem of MacCluer, Acta Arith. **25**, 121—126 (1974).

[5] Arithmetical properties of function fields (II). The generalized Schur problem, Acta Arith. **25**, 225—258 (1974).

FRIED M., MACRAE R. E. [1] On the invariance of chains of fields, Illinois J. Math. **13**, 165—171 (1969).

FRIED M., SACERDOTE G. [1] Solving diophantine problems over all residue class fields of a number field and all finite fields, Ann. of Math. (2) **104**, 203—233 (1976).

FRIEDLAND B. [1] Linear modular sequential circuits, IRE Trans. Circuit Theory **CT-6**, 61—68 (1959).

FRIEDLAND B., STERN T. E. [1] On periodicity of state in linear modular sequential circuits, IRE Trans. Information Theory **IT-5**, 136—137 (1959).

FRIEDLANDER J. B. [1] A note on primitive roots in finite fields, Mathematika **19**, 112—114 (1972).

[2] On the least kth power non-residue in an algebraic number field, Proc. London Math. Soc. (3) **26**, 19—34 (1973).

[3] Character sums in quadratic fields, Proc. London Math. Soc. (3) **28**, 99—111 (1974).

FRIEDMAN W. F., MENDELSOHN C. J. [1] Notes on code words, Amer. Math Monthly **39**, 394—409 (1932).

FRÖBERG C.-E. [1] New results on the Kummer conjecture, BIT **14**, 117—119 (1974).

FRÖHLICH A. [1] Non-abelian Jacobi sums, Number Theory and Algebra (H. Zassenhaus, ed.), pp. 71—75, Academic Press, New York, 1977.

[2] Stickelberger without Gauss sums, Algebraic Number Fields (A. Fröhlich, ed.) pp. 589—607, Academic Press, London, 1977.

FRÖHLICH A., TAYLOR M. J. [1] The arithmetic theory of local Galois Gauss sums for tame characters, Phyl. Trans. Royal Soc. London Ser. A **298**, 141—181 (1980).

FROLOV M. [1] Sur les racines primitives, Bull. Soc. Math. France **21**, 113—128 (1893), ibid. **22**, 241—245 (1894).

FRYER K. D. [1] Note on permutations in a finite field, Proc. Amer. Math. Soc. **6**, 1—2 (1955).

[2] A class of permutation groups of prime degree. Canad J. Math. **7**, 24—34 (1955)

FULTON J. D. [1] Symmetric involutory matrices over finite fields and modular rings of integers, Duke Math. J. **36**, 401—407 (1969).

[2] Stochastic involutions over a finite field, Duke Math. J. **39**, 391—399 (1972).

[3] Characterization and enumeration of linear classes of involutions over a finite field, Linear Algebra Appl. **6**, 119—127 (1973).
[4] Linear classes of involutions over fields of characteristic two, Linear Algebra Appl. **6**, 129—142 (1973).
[5] Representations by quadratic forms of arbitrary rank in a finite field of characteristic two, Linear and Multilinear Algebra **4**, 89—101 (1976).
[6] Representations by Hermitian forms in a finite field of characteristic two, Canad J. Math. **29**, 169—179 (1977).
[7] Representations by quadratic forms in a finite field of characteristic two, Math. Nachr. **77**, 237—243 (1977).
[8] Generalized inverses of matrices over a finite field, Discrete Math. **21**, 23—29 (1978).
[9] Gauss sums and solutions to simultaneous equations over $GF(2^y)$, Acta Arith. **35**, 17—24 (1979).
[10] Generalized inverses of matrices over fields of characteristic two, Linear Algebra Appl. **28**, 69—76 (1979).
FULTON J. D., MORRIS W. L. [1] On arithmetical functions related to the Fibonacci numbers, Acta Arith. **16**, 105—110 (1969).
FULTON W. [1] A fixed point formula for varieties over finite fields, Math. Scand. **42**, 189—196 (1978).
FURQUIM DE ALMEIDA F. [1] On a formula of Cipolla (Portuguese), Summa Brasil. Math. **1**, no. 10, 207—219 (1946).
[2] The law of quadratic reciprocity (Portuguese), Bol. Soc. Mat. São Paulo **3**, no. 1—2, 3—8 (1948).
FURSTENBERG H. [1] Algebraic functions over finite fields, J. Algebra **7**, 271—277 (1967).
FURTADO GOMIDE E. [1] On the theorem of Artin—Weil (Portuguese), Bol. Soc. Mat. São Paulo **4**, 1—18 (1949).
GAAL L. [1] Classisal Galois Theory with Examples, Markham, Chicago, 1971.
GAIU E. [1] Congruences of matrices having integer elements (Romanian), Gaz. Mat. Fiz. Ser. A **11**, 334—337 (1959).
GALLAGER R. G. [1] Information Theory and Reliable Communication, Wiley, New York, 1968. [Имеется перевод: ГАЛЛАГЕР Р. Теория информации и надежная связь. — М.: Советское радио, 1974.]
GALOIS E. [1] Sur la théorie des nombres, Bull. Sci. Math. de M. Férussac **13**, 428—435 (1830); J. Math. Pures Appl. **11**, 398—407 (1846); Oeuvres math., pp. 15—23, Gauthier-Villars, Paris, 1897. [Имеется перевод: ГАЛУА Э. Из теории чисел. — В кн.: Галуа Э. Сочинения. М.—Л.: ОНТИ, 1936, с. 35—47.]
GAUSS C. F. [1] Disquisitiones Arithmeticae, Fleischer, Leipzig, 1801; Werke, vol. 1, Königl. Gesellschaft der Wissenschaften, Göttingen, 1863; Untersuchungen über Höhere Arithmetik (H. Maser, ed.), pp. 1—453, Springer, Berlin, 1889; Yale Univ. Press, New Haven, Conn., 1966. [Имеется перевод: ГАУСС К. Ф. Арифметические исследования. — В кн.: Гаусс К. Ф. Труды по теории чисел. — М.: Изд. АН СССР, 1959, с. 7—583.]
[2] Summatio quarumdam serierum singularium, Comment. Soc. Reg. Sci. Gottingensis 1 (1811); Werke, vol. 2, pp. 11—45, Königl. Gesellschaft der Wissenschaften, Göttingen, 1876; Untersuchungen über Höhere Arithmetik (H. Maser, ed), pp. 463—495, Springer, Berlin, 1889. [Имеется перевод: ГАУСС К. Ф. Суммнрованне некоторых рядов особого вида. — В кн.: Гаусс К. Ф. Труды по теорни чисел. — М.: Изд. АН СССР, 1959, с. 594—635.]
[3] Theoria residuorum biquadraticorum. Commentatio prima, Comment. Soc. Reg. Sci. Gottingensis **6** (1828); Werke, vol. 2, pp. 65—92, Königl. Gesellschaft der Wissenschaften, Göttingen, 1876; Untersuchungen über Höhere Arithmetik (H. Maser, ed.), pp. 511—533, Springer, Berlin, 1889. [Имеется перевод: ГАУСС К. Ф. Теория биквадратичных вычетов. Сочинение первое.—

В ки.: Гаусс К. Ф. Труды по теории чисел. — М.: Изд. АН СССР, 1959, с. 655—685.]

[4] Analysis residuorum: Caput octavum. Disquisitiones generales de congruentiis, Werke, vol. 2, pp. 212—240, Königl. Gesellschaft der Wissenschaften, Göttingen, 1876; Untersuchungen über Höhere Arithmetik (H. Maser, ed.), pp. 602—629, Springer, Berlin, 1889. [Имеется перевод: ГАУСС К. Ф. Учение о вычетах. Общие исследования о сравнениях. — В кн.: Гаусс К. Ф. Труды по теории чисел. — М.: Изд. АН СССР, 1959, с. 773—806.]

[5] Disquisitionum circa aequationes puras ulterior evolutio, Werke, vol. 2, pp. 243—265, Königl. Gesellschaft der Wissenschaften, Göttingen, 1876; Untersuchungen über Höhere Arithmetik (H. Maser, ed.), pp. 630—652, Springer, Berlin, 1889. [Имеется перевод: ГАУСС К. Ф. Дальнейшее развитие исследований о чистых уравнениях. — В ки.: Гаусс К. Ф. Труды по теории чисел. — М.: Изд. АН СССР, 1959, с. 807—835.]

GAY D., VÉLEZ W. Y. [1] On the degree of the splitting field of an irreducible binomial, Pacific J. Math. **78**, 117—120 (1978).

GEGENBAUER L. [1] Die Bedingungen für die Existenz einer bestimmten Anzahl von Wurzeln einer Congruenz, Sitzungsber. Wien Abt. II **95**, 165—169 (1887).

[2] Über Congruenzen, Sitzungsber. Wien Abt. II **95**, 610—617 (1887).

[3] Über ein Theorem des Herrn Pepin, Sitzungsber. Wien Abt. II **95**, 838—842 (1887).

[4] Zur Theorie der Congruenzen, Sitzungsber. Wien Abt. II **98**, 652—672 (1889).

[5] Zur Theorie der Congruenzen mit mehreren Unbekannten, Sitzungsber Wien Abt. II **99**, 790—813 (1890).

[6] Einige mathematische Theoreme, Sitzungsber. Wien Abt. II **102**, 549—564 (1893).

[7] Ueber Congruenzen in Bezug auf einen Primzahlmodul, Monatsh. Math. Phys. **5**, 230—232 (1894).

GEIJSEL J. M. [1] Transcendence in Fields of Positive Characteristic, Mathematical Centre Tracts, vol. 91, Mathematisch Centrum, Amsterdam, 1979.

GERJETS M. S., BERGUM G. E. [1] The distribution of primitive roots in fields of order p^2, Bull. Calcutta Math. Soc. **68**, 53—62 (1976).

GERST I., BRILLHART J. [1] On the prime divisors of polynomials, Amer. Math. Monthly **78**, 250—266 (1971).

GERSTENHABER M. [1] On the number of nilpotent matrices with coefficients in a finite field, Illinois J. Math. **5**, 330—333 (1961).

GHENT K. S. [1] Sums of values of a polynomial multiplied by constants, Duke Math. J. **3**, 518—528 (1937).

GILBERT E. N. [1] A comparison of signalling alphabets, Bell System Tech. J. **31**, 504—522 (1952).

GILL A. [1] Introduction to the Theory of Finite-State Machines, McGraw-Hill, New York, 1962. [Имеется перевод: ГИЛЛ А. Введение в теорию конечных автоматов. — М.: Наука, 1966.]

[2] Linear Sequential Circuits: Analysis, Synthesis, and Applications, McGraw-Hill, New York, 1966. [Имеется перевод: ГИЛЛ А. Линейные последовательные машины. Анализ, синтез и применение. — М.: Наука, 1974.]

GILL A., JACOB J. P. [1] On a mapping polynomial for Galois fields, Quart. Appl. Math. **24**, 57—62 (1966).

GILLETT J. R. [1] Character sums of polynomials to a prime modulus, Proc. London Math. Soc. (3) **27**, 205—221 (1973).

GILMER R. [1] Finite rings having a cyclic multiplicative group of units, Amer. J. Math. **85**, 447—452 (1963).

GILMER R., MOTT J. L. [1] An algebraic proof of a theorem of A. Robinson, Proc. Amer. Math. Soc. **29**, 461—466 (1971).

GIUDICI R. E. [1] Quadratic residues in $GF(p^2)$, Math. Mag. **44**, 153—157 (1971).

[2] Residui quadratici in un campo di Galois, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **52**, 461—466 (1972).
GIUDICI R. E., MARGAGLIO C. [1] On the factorization of polynomials of the fourth degree (Spanish), Sci. Valparaiso **147**, 70—76 (1976).
[2] A geometric characterization of the generators in a quadratic extension of a finite field, Rend. Sem. Mat. Univ. Padova **62**, 103—114 (1980).
GIUDICI R. E., MUSKAT J. B., ROBINSON S. F. [1] On the evaluation of Brewer's character sums, Trans. Amer. Math. Soc. **171**, 317—347 (1972).
GŁAZEK K. [1] On weak automorphisms of finite fiels, Finite Algebra and Multiple-Valued Logic (Szeged, 1979), Colloq. Math. Soc. János Bolyai, vol. 28, pp. 275—300, North-Holland, Amsterdam, 1981.
GLENN O. E. [1] Theorems of finiteness in formal concomitant theory, modulo p, Proc. International Math. Congress (Toronto, 1924), vol. 1, pp. 331—345, Univ. of Toronto Press, Toronto, 1928.
GOETHALS J.-M. [1] Nonlinear codes defined by quadratic forms over $GF(2)$, Information and Control **31**, 43—74 (1976).
GOETHALS J.-M., SEIDEL J. J. [1] Orthogonal matrices with zero diagonal, Canad. J. Math. **19**, 1001—1010 (1967).
GOGIA S. K., LUTHAR I. S. [1] Norms from certain extensions of $F_q(T)$, Acta Arith. **38**, 325—340 (1981).
GOKA T. [1] An operator on binary sequences, SIAM Rev. **12**, 264—266 (1970).
GOLAY M. J. E. [1] Notes on digital coding, Proc. IRE **37**, 657 (1949).
GOLD R. [1] Characteristic linear sequences and their coset functions, SIAM J. Appl. Math. **14**, 980—985 (1966).
[2] Optimal binary sequences for spread spectrum multiplexing, IEEE Trans. Information Theory **IT-13**, 619—621 (1967).
[3] Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Information Theory **IT-14**, 154—156 (1968).
GOLDBERG M. [1] The group of the quadratic residue tournament, Canad. Math. Bull. **13**, 51—54 (1970).
GOLDMAN H. D., KLIMAN M., SMOLA H. [1] The weight structure of some Bose—Chaudhuri codes, IEEE Trans. Information Theory **IT-14**, 167—168 (1968).
GOLDSTEIN R. M., ZIERLER N. [1] On trinomial recurrences, IEEE Trans. Information Theory **IT-14**, 150—151 (1968).
GOLOMB S. W. [1] Sequences with randomness properties, Glenn L. Martin Co. Final Report, Baltimore, Md., 1955; reprinted in Golomb [4].
[2] Structural properties of PN sequences, Technical Report, Jet Propulsion Lab., California Institute of Technology, Pasadena, Cal., 1958; reprinted in Golomb [4].
[3] Digital Communications with Space Applications, Prentice-Hall, Englewood Cliffs, N. J., 1964.
[4] Shift Register Sequences, Holden-Day, San Francisco, 1967.
[5] Theory of transformation groups of polynomials over GF (2) with application to linear shift register sequences, Information Sciences **1**, 87—109 (1968).
[6] Irreducible polynomials, synchronization codes, primitive necklaces, and the cyclotomic algebra, Proc. Conf. Combinatorial Math. and Its Appl. (Chapel Hill, N. C., 1967), pp. 358—370, Univ. of North Carolina Press, Chapel Hill, N. C., 1969.
[7] Cyclotomic polynomials and factorization theorems, Amer. Math. Monthly **85**, 734—737 (1978); Corrections, ibid. **88**, 338—339 (1981).
[8] Obtaining specified irreducible polynomials over finite fields, SIAM J. Algebraic Discrete Methods **1**, 411—418 (1980).
[9] On the classification of balanced binary sequences of period $2^n - 1$, IEEE Trans. Information Theory **IT-26**, 730—732 (1980).
GOLOMB S. W., BAUMERT L. D. [1] The search for Hadamard matrices, Amer. Math. Monthly **70**, 12—17 (1963).

GOLOMB S. W., LEMPEL A. [1] Second order polynomial recursions, SIAM J. Appl. Math. **33**, 587—592 (1977).
GOLOMB S. W., REED I. S., TRUONG T. K. [1] Integer convolutions over the finite field $GF(3 \cdot 2^n + 1)$; SIAM J. Appl. Math. **32**, 356—365 (1977).
GOLOMB S. W., WELCH L. R. [1] Nonlinear shift register sequences, Memo 20-149, Jet Propulsion Lab., California Institute of Technology, Pasadena, Cal., 1957; reprinted in Golomb [4].
GOLOMB S. W., WELCH L. R., HALES A. [1] On the factorization of trinomials over *GF* (2), Memo 20-189, Jet Propulsion Lab., California Institute of Technology, Pasadena, Cal., 1959; reprinted in Golomb [4].
GOOD I. J. [1] Normal recurring decimals, J. London Math. Soc. **21**, 167—169 (1946).
GOODSTEIN R. L. [1] Polynomial generators over Galois fields, J. London Math Soc **36**, 29—32 (1961).
GORDON B., MILLS W. H., WELCH L. R. [1] Some new difference sets, Canad J. Math. **14**, 614—625 (1962).
GORDON J. A. [1] Very simple method to find the minimum polynomial of an arbitrary nonzero element of a finite field, Electron. Lett. **12**, 663—664 (1976).
GORE W. C., COOPER A. B. [1] Comments on polynomial codes, IEEE Trans Information Theory **IT-16**, 635—638 (1970).
GORENSTEIN D. C., ZIERLER N. [1] A class of error-correcting codes in p^m symbols, J. Soc. Indust. Appl. Math. **9**, 207—214 (1961). [Имеется перевод ГОРЕНСТЕЙН Д., ЦИРЛЕР Н. Класс кодов из p^m символов с исправлением ошибок. — В кн.: Кибернетический сборник, вып. 7. — М.: ИЛ, 1963, с. 80—89.]
GOSS D. [1] Von Staudt for $F_{q'}$ [*T*], Duke Math. J. **45**, 885—910 (1978).
[2] Modular forms for F_r [*T*], J. reine angew Math. **317**, 16—39 (1980).
[3] The algebraist's upper half-plane, Bull. Amer. Math. Soc. (N. S.) **2**, 391—415 (1980).
GOTUSSO L. [1] Successioni uniformemente distribuite in corpi finiti, Atti Sem. Mat. Fis. Univ. Modena **12**, 215—232 (1962/63).
GOW R. [1] The number of equivalence classes of nondegenerate bilinear and sesquilinear forms over a finite field, Linear Algebra Appl. **41**, 175—181 (1981).
GRAHAM R. L. [1] On quadruples of consecutive *k*th power residues, Proc. Amer. Math. Soc. **15**, 196—197 (1964).
GRAHAM R. L., MACWILLIAMS F. J. [1] On the number of information symbols in difference-set cyclic codes, Bell System Tech. J. **45**, 1057—1070 (1966). [Имеется перевод: ГРЭХЕМ Р. Л., МАК-ВИЛЬЯМС ДЖ. О числе информационных символов циклических кодов, задаваемых разностными множествами. — В кн.: Некоторые вопросы теории кодирования. — М., 1970, с. 22—35.]
GRANDET-HUGOT M. [1] Une propriété des «nombres de Pisot» dans un corps de séries formelles, C. R. Acad. Sci. Paris. Sér. A **265**, 39—41 (1967); Errata, ibid. **265**, 551 (1967).
[2] Éléments algébriques remarquables dans un corps de séries formelles, Acta Arith. **14**, 177—184 (1968).
GRANDI A. [1] Un teorema sulla rappresentazione analitica delle sostituzioni sopra un numero primo di elementi, Giorn. Mat. Battaglini **19**, 238—244 (1881).
[2] Generalizzazione di un teorema sulla rappresentazione analitica delle sostituzioni, Rend. Reale Ist. Lombardo Sci. Lett. (2) **16**, 101—111 (1883).
GRANT H. S. [1] A generalization of a cyclotomic formula, Bull. Amer. Math. Soc. **42**, 550—556 (1936).
GRAS G. [1] Sommes de Gauss sur les corps finis, Publ. Math. Fac. Sci. Besancon **1977—1978**, no. 1.
GRAY J. F. [1] Diagonal forms of odd degree over a finite field, Michigan Math. J. **7**, 297—301 (1960).
GREEN D. H., TAYLOR I. S. [1] Modular representation of multiple-value logic systems, Proc. IEE **121**, 409—418 (1974).

[2] Irreducible polynomials over composite Galois fields and their applications in coding techniques, Proc. IEE **121**, 935—939 (1974).
[3] Multiple-valued switching circuit design by means of generalised Reed—Muller expansions, Digital Process **2**, 63—81 (1976).
GREEN J. H., Jr., SAN SOUCIE R. L. [1] An error-correcting endcoder and decoder of high efficiency, Proc. IRE **46**, 1741—1744 (1958).
GREENBERG M. J. [1] Lectures on Forms in Many Variables, Benjamin, New York, 1969.
GREENWOOD R. E., GLEASON A. M. [1] Combinatorial relations and chromatic graphs, Canad. J. Math. **7**, 1—7 (1955).
GRIES D., LEVIN G. [1] Computing Fibonacci numbers (and similarly defined functions) in log time, Inform. Process. Lett. **11**, no. 2, 68—69 (1980).
GROSS B. H., KOBLITZ N. [1] Gauss sums and the p-adic Γ-function, Ann. of Math. (2) **109**, 569—581 (1979).
GROTH E. J. [1] Generation of binary sequences with controllable complexity, IEEE Trans. Information Theory **IT-17**, 288—296 (1971).
GROTHENDIECK A. [1] Sur une note de Mattuck—Tate, J. reine angew. Math. **200**, 208—215 (1958).
[2] Formule de Lefschetz et rationalité des fonctions L, Séminaire Bourbaki 1964/65, Exp. 279, Benjamin, New York, 1966; Dix exposés sur la cohomologie des schémas, Advanced Studies in Pure Math., vol. 3, pp. 31—45, North-Holland, Amsterdam, 1968.
[3] Cohomologie l-adique et fonctions L, Séminaire de Géométrie Algébrique du Bois—Marie 1965—66 (SGA 5), Lecture Notes in Math., vol. 589, Springer-Verlag, Berlin—Heidelberg—New York, 1977.
GRUNDHÖFER T. [1] Über Abbildungen mit eingeschränktem Differenzenprodukt auf einem endlichen Körper, Arch. Math. **37**, 59—62 (1981).
GUERRIER W. J. [1] The factorization of the cyclotomic polynomials mod p, Amer. Math. Monthly **75**, 46 (1968).
GUIAŞU S. [1] Information Theory with Applications, McGraw-Hill, New York, 1977.
GUINAND A. P. [1] Gauss sums and primitive characters, Quart. J. Math. **16**, 59—63 (1945).
GUNJI H., ARNON D. [1] On polynomial factorization over finite fields, Math. Comp. **36**, 281—287 (1981).
GUPTA H. [1] On a problem in matrices, Proc. Nat. Inst. Sci. India A **30**, 556—560 (1964).
GUSTAVSON F. G. [1] Analysis of the Berlekamp—Massey linear feedback shift-register synthesis algorithm, IBM J. Res. Develop. **20**, 204—212 (1976).
GWEHENBERGER G. [1] Über den Grad von rationalen Funktionen, die Permutationen darstellen, Monatsh. Math. **75**, 215—222 (1971).
HALL M., Jr. [1] Divisibility sequences of third order, Amer. J. Math. **58**, 577—584 (1936).
[2] Divisors of second-order sequences, Bull. Amer. Math. Soc. **43**, 78—80 (1937).
[3] An isomorphism between linear recurring sequences and algebraic rings, Trans. Amer. Math. Soc. **44**, 196—218 (1938).
[4] Equidistribution of residues in sequences, Duke Math. J. **4**, 691—695 (1938).
[5] A survey of difference sets, Proc. Amer. Math. Soc. **7**, 975—986 (1956).
[6] The Theory of Groups, Macmillan, New York, 1959. [Имеется перевод: ХОЛЛ М. Теория групп. — М.: ИЛ, 1962.]
[7] Characters and cyclotomy, Proc. Symp. Pure Math., vol. 8, pp. 31—43, American Math. Society, Providence, R. I., 1965.
[8] Combinatorial Theory, Blaisdell, Waltham, Mass., 1967. [Имеется перевод: ХОЛЛ М. Комбинаторика. — М.: Мир, 1970.]
HALTON J. H. [1] On the divisibility properties of Fibonacci numbers, Fibonacci Quart. **4**, 217—240 (1966).

HAMMING R. W. [1] Error detecting and error correcting codes, Bell System Tech. J. **29**, 147—160 (1950). [Имеется перевод: ХЭММИНГ Р. В. Коды с обнаружением и исправлением ошибок. — В кн.: Коды с обнаружением и исправлением ошибок. — М.: ИЛ, 1956, с. 7—23.]
HANANI H. [1] Balanced incomplete block designs and related designs, Discrete Math. **11**, 255—369 (1975).
HANNEKEN C. B. [1] Irreducible quintic congruences, Duke Math. J. **22**, 107—118 (1955).
[2] Irreducible congruences over *GF* (*p*), Proc. Amer. Math. Soc. **10**, 18—26 (1959).
[3] Irreducible sextic congruences, Duke Math. J. **26**, 81—93 (1959).
[4] Irreducible congruences of prime power degree, Trans. Amer. Math. Soc. **153**, 167—179 (1971)
[5] Irreducible congruences over *GF* (2), Trans. Amer. Math. Soc. **193**, 291—301 (1974).
HARDER G. [1] Eine Bemerkung zu einer Arbeit von P. E. Newstead, J. reine angew. Math. **242**, 16—25 (1970).
HARDMAN N. R., JORDAN J. H. [1] The distribution of quadratic residues in fields of order p^2, Math. Mag. **42**, 12—17 (1969).
HARDY G. H., LITTLEWOOD J. E. [1] Some problems of «Partitio Numerorum»; I: A new solution of Waring's problem, Göttinger Nachr. **1920**, 33—54.
[2] A new solution of Waring's problem, Quart. J. Math. **48**, 272—293 (1920).
[3] Some problems of «Partitio Numerorum»: IV. The singular series in Waring's problem and the value of the number $G(k)$, Math. Z. **12**, 161—188 (1922).
[4] Some problems of «partitio numerorum» (VIII): The number $\Gamma(k)$ in Waring's problem, Proc. London Math. Soc. (2) **28**, 518—542 (1927).
HARIS S. J. [1] Number theoretical developments arising from the Siegel formula, Bull. Amer. Math. Soc. (N. S.) **2**, 417—433 (1980).
HARRISON M. A. [1] Lectures on Linear Sequential Machines, Academic Press, New York, 1969.
HARTFIEL D. J., MAXSON C. J. [1] A semigroup characterization of a linearly realizable automaton over *GF* (*p*), J. Comput. System Sci. **14**, 150—155 (1977).
HARTMANN C. R. P., RIEK J. R., Jr., LONGOBARDI R. J. [1] Weight distributions of some classes of binary cyclic codes, IEEE Trans. Information Theory **IT-21**, 345—350 (1975).
HARTMANN C. R. P., TZENG K. K. [1] Generalizations of the BCH bound, Information and Control **20**, 489—498 (1972).
HARTMANN C. R. P., TZENG K. K., CHIEN R. T. [1] Some results on the minimum distance structure of cyclic codes, IEEE Trans. Information Theory **IT-18**, 402—409 (1972).
HARTWIG R. E., LEVINE J. [1] Applications of the Drazin inve se to the Hill cryptographic system. III, IV, Cryptologia **5**, 67—77, 213— 8 (1981).
HARVEY J. T. [1] High-speed *m*-sequence generation, Electro Lett. **10**, 480—481 (1974).
HASSE H. [1] Swei Bemerkungen zu der Arbeit «Zur Arithmetik der Polynome» von U. Wegner in den Mathematischen Annalen, Bd. **105**, S. 628—631, Math. Ann. **106**, 455—456 (1932).
[2] Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen, Göttinger Nachr. **1933**, 253—262.
[3] Über die Kongruenzzetafunktionen, Sitzungsber. Preuss. Akad. Wiss. Berlin Math.-Phys. Kl. **17**, 250—263 (1934).
[4] Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Sem. Univ. Hamburg **10**, 325—348 (1934).
[5] Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, J. reine angew. Math. **172**, 37—54 (1935).

[6] Zur Theorie der abstrakten elliptischen Funktionenkörper, Göttinger Nachr. **1935**, 119—129.
[7] Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik, J. reine angew. Math. **175**, 50—54 (1936).
[8] Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II, III, J. reine angew. Math. **175**, 55—62, 69—88, 193—208 (1936).
[9] Produktformeln für verallgemeinerte Gaußsche Summen und ihre Anwendung auf die Klassenzahlformel für reelle quadratische Zahlkörper, Math. Z. **46**, 303—314 (1940).
[10] Allgemeine Theorie der Gaußschen Summen in algebraischen Zahlkörper, Abh. Deutsch. Akad. Wiss. Berlin Math.-Naturw. Kl. **1951**, no. 1, 4—23.
[11] Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.
[12] Gaußsche Summen zu Normalkörpern über endlich-algebraischen Zahlkörpern, Abh. Deutsch. Akad. Wiss. Berlin Math.-Naturw. Kl. **1952**, no. 1, 1—19.
[13] Artinsche Führer, Artinsche L-Funktion und Gaußsche Summen über endlich-algebraischen Zahlkörpern, Acta Salmanticensia Ciencias Sec. Mat. **4**, 1—113 (1954).
[14] Der 2^n-te Potenzcharakter von 2 im Körper der 2^n-ten Einheitswurzeln, Rend. Circ. Mat. Palermo (2) **7**, 185—243 (1958).
[15] Vorlesungen über Zahlentheorie, 2nd ed., Springer-Verlag, Berlin—Göttingen—Heidelberg—New York, 1964. [Имеется перевод: ХАССЕ Г. Лекции по теории чисел. — М. : ИЛ, 1953.]
[16] Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II: Reziprozitätsgesetz, 2nd ed., Physica-Verlag, Würzburg, 1965.
[17] Modular functions and elliptic curves over finite fields, Rend. Mat. e Appl. (5) **25**, 248—266 (1966).
[18] The Riemann Hypothesis in Function Fields, Univ. of Pennsylvania Press, Philadelphia, 1969.
HAUPTMAN H., VEGH E., FISHER J. [1] Table of all Primitive Roots for Primes Less than 5000, Naval Research Laboratory, Washington, D. C., 1970.
HAUSNER A. [1] On the quadratic reciprocity theorem, Arch. Math. **12**, 182—183 (1961).
HAYASHI H. S. [1] The number of solutions of certain quintic congruences, Duke Math. J. 33, 747—756 (1966).
[2] On a criterion for power residuacity, Mem. Fac. Sci. Kyushu Univ. Ser. A **27**, 211—220 (1973).
HAYES D. R. [1] A polynomial analog of the Goldbach conjecture, Bull. Amer. Math. Soc. **69**, 115—116 (1963); Correction, ibid. **69**, 493 (1963).
[2] The distribution of irreducibles in $GF[q, x]$, Trans. Amer. Math. Soc. **117**, 101—127 (1965).
[3] A polynomial generalized Gauss sum, J. reine angew. Math. **222**, 113—119 (1966).
[4] The expression of a polynomial as a sum of three irreducibles, Acta Arith. **11**, 461—488 (1966).
[5] A geometric approach to permutation polynomials over a finite field, Duke Math. J. **34**, 293—305 (1967).
[6] The Galois group of $x^n + x - t$, Duke Math. J. **40**, 459—461 (1973).
HAZLETT O. C. [1] A symbolic theory of formal modular covariants, Trans. Amer. Math. Soc. **24**, 286—311 (1922).
[2] Annihilators of modular invariants and covariants, Ann. of Math. (2) **23**, 198—211 (1923),
[3] Notes on formal modular protomorphs, Amer. J. Math. **49**, 181—188 (1927).
[4] On formal modular invariants, J. Math. Pures Appl. (9) **9**, 327—332 (1930).

HEATH-BROWN D. R., PATTERSON S. J. [1] The distribution of Kummer sums at prime arguments, J. reine angew. Math. **310**, 111—130 (1979).
HECKE E. [1] Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper, Göttinger Nachr. **1917**, 299—318.
[2] Reziprozitätsgesetz und Gaußsche Summen in quadratischen Zahlkörpern, Göttinger Nachr. **1919**, 265—278.
[3] Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. II, Math. Z. **6**, 11—51 (1920).
[4] Vorlesungen über die Theorie der algebraischen Zahlen, Akademische Verlagsgesellschaft, Leipzig, 1923. [Имеется перевод: ГЕККЕ Э. Лекции по теории алгебраических чисел. — М.-Л.: Гостехиздат, 1940.]
HEISLER J. [1] A characterization of finite fields, Amer. Math. Monthly **74**, 537—538 (1967); Correction, ibid. **74**, 1211 (1967).
[2] Diagonal forms over finite fields, J. Number Theory **6**, 50—51 (1974).
HELGERT H. J. [1] Decoding of alternant codes, IEEE Trans. Information Theory **IT-23**, 513—514 (1977).
HELLESETH T. [1] Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. **16**, 209—232 (1976).
[2] A note on the cross-correlation function between two binary maximal length linear sequences, Discrete Math. **23**, 301—307 (1978).
HELLESETH T., KLØVE T., MYKKELTVEIT J. [1] The weight distribution of irreducible cyclic codes with block length $n_1 ((q^l - 1)/N)$, Discrete Math. **18**, 179—211 (1977).
HELVERSEN-PASOTTO A. [1] Série discrète de GL (3, F_q) et sommes de Gauss, C. R. Acad. Sci. Paris Sér. A **275**, 263—266 (1972).
[2] L'identité de Barnes pour les corps finis, Sém. Delange—Pisot—Poitou 1977/78, Théorie des Nombres, Exp. 22, Secrétariat Math., Paris, 1978.
[3] L'identité de Barnes pour les corps finis, C. R. Acad. Sci. Paris Sér. A **286**, 297—300 (1978).
[4] Darstellungen von GL (3, F_q) und Gaußsche Summen, Math. Ann. **260**, 1—21 (1982).
HEMMATI F., COSTELLO D. J., Jr. [1] An algebraic construction for q-ary shift register sequences, IEEE Trans. Computers C-**27**, 1192—1195 (1978).
HENSEL K. [1] Über die Darstellung der Zahlen eines Gattingsbereiches für einen beliebigen Primdivisor, J. reine angew. Math. **103**, 230—237 (1888).
[2] Über die zu einem algebraischen Körper gehörigen Invarianten, J. reine angew. Math. **129**, 68—85 (1905).
HERGET W. [1] Über die Funktionalgleichung $f(x) = d^{m-1} \sum_{i=0}^{d-1} f(x + i/d)$ in den Körpern Z_p, Manuscripta Math. **23**, 131—141 (1978).
[2] Bernoulli-Polynome in den Restklassenringen Z_n, Glasnik Mat. (3) **14**, 27—33 (1979).
HERGLOTZ G. [1] Zur letzten Eintragung im Gaußschen Tagebuch, Ber. Math.-Phys. Kl. Sächs. Akad. Wiss. Leipzig **73**, 271—276 (1921).
HERLESTAM T., JOHANNESSON R. [1] On computing logarithms over $GF(2^p)$, BIT **21**, 326—334 (1981).
HERMITE C. [1] Sur la théorie des formes quadratiques. II, J. reine angew. Math. **47**, 343—368 (1854); Oeuvres, vol. 1, pp. 234—263, Gauthier-Villars, Paris, 1905.
[2] Sur les fonctions de sept lettres, C. R. Acad. Sci. Paris **57**, 750—757 (1863); Oeuvres, vol. 2, pp. 280—288, Gauthier-Villars, Paris, 1908.
HERSHEY J. E. [1] Implementation of Mitre public key cryptographic system, Electron. Lett. **16**, 930—931 (1980).
HERSTEIN I. N. [1] An elementary proof of a theorem of Jacobson, Duke Math. J. **21**, 45—48 (1954).
[2] Wedderburn's theorem and a theorem of Jacobson, Amer. Math. Monthly **68**, 249—251 (1961).

[3] Noncommutative Rings, Carus Math. Monographs, no. 15, Math. Assoc. of America, Washington, D. C., 1968. [Имеется перевод: ХЕРСТЕЙН И. Некоммутативные кольца. — М.: Мир, 1972.]
[4] Topics in Algebra, 2nd ed., Xerox College Publ., Lexington, Mass., 1975.
HEUZÉ G. [1] Sur les corps finis, Math. Sci. Humaines **47**, 57—59 (1974).
HILBERT D. [1] Über diophantische Gleichungen, Göttinger Nachr. **1897**, 48—54.
[2] Die Theorie der algebraischen Zahlkörper, Jber. Deutsch. Math.-Verein. **4**, 175—546 (1897).
[3] Grundlagen der Geometrie, Teubner, Leipzig, 1899; Open Court, Chicago, 1971. [Имеется перевод: ГИЛЬБЕРТ Д. Основания геометрии. — М.-Л.: Гостехиздат, 1948.]
HINZ J. G. [1] Einige Bemerkungen zum Beweis eines Satzes von J. H. Maclagan—Wedderburn, J. reine angew. Math. **290**, 109—112 (1977).
HIRSCHFELD J. W. P. [1] A curve over a finite field, the number of whose points is not increased by a quadratic extension of the field, and sub-Hermitian forms, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **42**, 365—367 (1967).
[2] Rational curves on quadrics over finite fields of characteristic two, Rend. Mat. (6) **4**, 773—795 (1971).
[3] Ovals in Desarguesian planes of even order, Ann. Mat. Pura Appl. (4) **102**, 79—89 (1975).
[4] Cyclic projectivities in $PG(n, q)$, Teorie Combinatorie (Rome, 1973), vol. 1, pp. 201—211, Accad. Naz. dei Lincei, Rome, 1976.
[5] Projective Geometries over Finite Fields, Clarendon Press, Oxford, 1979.
HOCQUENGHEM A. [1] Codes correcteurs d'erreurs, Chiffres **2**, 147—156 (1959).
HODGES J. H. [1] Exponential sums for symmetric matrices in a finite field, Math. Nachr. **14**, 331—339 (1955).
[2] Representations by bilinear forms in a finite field, Duke Math. J. **22**, 497—509 (1955).
[3] Weighted partitions for symmetric matrices in a finite field, Math. Z. **66**, 13—24 (1956).
[4] Exponential sums for skew matrices in a finite field, Arch. Math. **7**, 116—121 (1956).
[5] The matric equation $AX = B$ in a finite field, Amer. Math. Monthly **63**, 243—244 (1956).
[6] Weighted partitions for general matrices over a finite field, Duke Math. J. **23**, 545—552 (1956).
[7] Distribution of bordered matrices in a finite field, J. reine angew. Math. **198**, 10—13 (1957).
[8] Weighted partitions for skew matrices over a finite field, Arch. Math. **8**, 16—22 (1957).
[9] Some matrix equations over a finite field, Ann. Mat. Pura Appl. (4) **44**, 245—250 (1957).
[10] Weighted partitions for Hermitian matrices over a finite field, Math. Nachr. **17**, 93—100 (1958).
[11] Scalar polynomial equations for matrices over a finite field, Duke Math. J. **25**, 291—296 (1958).
[12] The matrix equations $X^2 - I = 0$ over a finite field, Amer. Math. Monthly **65**, 518—520 (1958).
[13] Some determinantal equations over a finite field, Math. Z. **72**, 355—361 (1960).
[14] A note on systems of matrix equations over a finite field, Portugal. Math. **21**, 99—106 (1962).
[15] Some polynomial equations for determinants over a finite field, Monatsh. Math. **66**, 322—330 (1962).
[16] Generalized weighted m-th power partitions over a finite field, Duke Math. J. **29**, 405—412 (1962).

[17] Simultaneous pairs of linear and quadratic matrix equations over a finite field, Math. Z. **84**, 38—44 (1964).
[18] A bilinear matrix equation over a finite field, Duke Math. J. **31**, 661—666 (1964).
[19] The matrix equation $AXC = B$ over a finite field, Riv. Mat. Univ. Parma (2) **6**, 79—81 (1965).
[20] Determinantal equations related to Hermitian forms over a finite field, Monatsh. Math. **69**, 215—224 (1965).
[21] A symmetric matrix equation over a finite field, Math. Nachr. **30**, 221—228 (1965).
[22] A skew matrix equation over a finite field, Arch. Math. **17**, 49—55 (1966).
[23] Uniform distribution of sequences in $GF[q, x]$, Acta Arith. **12**, 55—75 (1966).
[24] An Hermitian matrix equation over a finite field, Duke Math. J. **33**, 123—129 (1966).
[25] Some pairs of matrix equations over a finite field, Scripta Math. **27**, 289—301 (1966).
[26] Uniform distribution of polynomial-generated sequences in $GF[q, x]$, Ann. Mat. Pura Appl. (4) **82**, 135—142 (1969).
[27] On uniform distribution of sequences in $GF\{q, x\}$ and $GF[q, x]$, Ann. Mat. Pura Appl. (4) **85**, 287—294 (1970).
[28] Note on some partitions of a rectangular matrix, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **59**, 662—666 (1975).
[29] Ranked partitions of rectangular matrices over finite fields, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **60**, 6—12 (1976).
[30] Note on a linear matrix equation over a finite field, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **63**, 304—309 (1977).
HOFFMAN K., KUNZE R. [1] Linear Algebra, 2nd ed., Prentice-Hall, Englewood Cliffs, N. J., 1971.
HOHLER P. [1] Eine zahlentheoretische Konstruktion der Galois-Felder $GF(p^2)$, Elemente der Math. **31**, 64—66 (1976).
HOLZER L. [1] Zahlentheorie, vol. 1, Teubner, Leipzig, 1958.
HONG S. J., BOSSEN D. C. [1] On some properties of self-reciprocal polynomials, IEEE Trans. Information Theory **IT-21**, 462—464 (1975).
HOOLEY C. [1] An asymptotic formula in the theory of numbers, Proc. London Math. Soc. (3) **7**, 396—413 (1957).
[2] On the distribution of the roots of polynomial congruences, Mathematika **11**, 39—49 (1964).
[3] Applications of Sieve Methods to the Theory of Numbers, Cambridge Univ. Press, Cambridge, 1976.
[4] On another sieve method and the numbers that are a sum of two h-th powers, Proc. London Math. Soc. (3) **43**, 73—109 (1981).
[5] On Waring's problem for two squares and three cubes, J. reine angew. Math. **328**, 161—207 (1981).
[6] On exponential sums and certain of their applications, Journées Arithmétiques 1980 (J. V. Armitage, ed.), London Math. Soc. Lecture Note Series, no. 56, pp. 92—122, Cambridge Univ. Press, Cambridge, 1982.
HOPF H. [1] Über die Verteilung quadratischer Reste, Math. Z. **32**, 222—231 (1930).
HORADAM A. F. [1] A Guide to Undergraduate Projective Geometry, Pergamon Press Australia, Rushcutters Bay, N. S. W., 1970.
HORAKOVA K., SCHWARZ Š. [1] Циклические матрицы и алгебраические уравнения над конечным полем, Mat.-Fyz. Časopis Sloven. Akad. Vied, **12**, 36—46 (1962).
HOUNDONOUGBO V. [1] Développement en fraction continue sur $K(X)$. Fonction profondeur, C. R. Acad. Sci. Paris Sér. A **286**, 1037—1039 (1978).

[2] Mesure de répartition d'une suite $(\theta^n)_{n \in \mathbb{N}^*}$ dans un corps de séries formelles sur un corps fini, C. R. Acad. Sci. Paris Sér. A **288**, 997—999 (1979).
HUA L.-K. [1] On Waring's problem with polynomial summands, Amer. J. Math. **58**, 553—562 (1936).
[2] On a generalized Waring's problem, Proc. London Math. Soc. (2) **43**, 161—182 (1937).
[3] On an exponential sum, J. London Math. Soc. **13**, 54—61 (1938).
[4] On Waring's problem with cubic polynomial summands, Science Reports National Tsing Hua Univ. **4**, 55—83 (1940).
[5] On Waring's problem with cubic polynomial summands, J. Indian Math. Soc. **4**, 127—135 (1940).
[6] On an exponential sum, J. Chinese Math. Soc. **2**, 301—312 (1940).
[7] Sur une somme exponentielle, C. R. Acad. Sci. Paris **210**, 520—523 (1940).
[8] Sur le problème de Waring relatif à un polynome du troisième degré, C. R. Acad. Sci. Paris **210**, 650—652 (1940).
[9] Аддитивная теория простых чисел. — Труды Матем. инст. им. Стеклова АН СССР, т. **22**, 1947.
[10] On the number of solutions of Tarry's problem, Acta Sci. Sinica **1**, 1—76 (1952).
[11] On exponential sums, Sci. Record (N. S.) **1**, 1—4 (1957).
[12] Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie, Enzyklopädie der Math. Wissenschaften, Band I2, Heft 13, Teil I, Teubner, Leipzig, 1959. [Имеется перевод: ХУА ЛО-ГЕН. Метод тригонометрических сумм и его применения в теории чисел. — М.: Мир, 1964.]
HUA L.-K., MIN S. H. [1] On the number of solutions of certain congruences, Science Reports National Tsing Hua Univ. **4**, 113—133 (1940).
[2] On a double exponential sum, Acad. Sinica Science Record **1**, 23—25 (1942).
[3] On a double exponential sum, Science Reports National Tsing Hua Univ. **4**, 484—518 (1947).
HUA L.-K., VANDIVER H. S. [1] On the existence of solutions of certain equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **34**, 258—263 (1948).
[2] Characters over certain types of rings with application to the theory of equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **35**, 94—99 (1949).
[3] On the number of solutions of some trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **35**, 477—481 (1949).
[4] On the nature of the soiutions of certain equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **35**, 481—487 (1949).
HUDSON M. [1] On the least non-residue of a polynomial, J. London Math. Soc. **41**, 745—749 (1966).
HUDSON R. H. [1] On the distribution of k-th power nonresidues, Duke Math. J. **39**, 85—88 (1972).
[2] A bound for the first occurrence of three consecutive integers with equal quadratic character, Duke Math. J. **40**, 33—39 (1973).
[3] A note on Dirichlet characters, Math. Comp. **27**, 973—975 (1973).
[4] On the least k-th power non-residue, Ark. Mat. **12**, 217—220 (1974).
[5] Power residues and nonresidues in arithmetic progressions, Trans. Amer. Math. Soc. **194**, 277—289 (1974).
[6] A sharper bound for the least pair of consecutive k-th power non-residues of non-pripcipal characters (mod p) of order $k > 3$, Acta Arith. **30**, 133—135 (1976).
HUDSON R. H., WILLIAMS K. S. [1] Resolution of ambiguities in the evaluation of cubic and quartic Jacobsthal sums, Pacific J. Math. **99**, 379—386 (1982).
HUFFMAN D. A. [1] The synthesis of linear sequential coding networks, Proc. Third London Symp. on Information Theory (C. Cherry, ed.), pp. 77—95, Butterworths, London, 1956.

[2] A linear circuit viewpoint on error-correcting codes, IRE Trans. Information Theory **IT-2**, no. 3, 20—28 (1956).
HUGHES D. R. [1] A class of non-Desarguesian projective planes, Canad. J Math. **9**, 378—388 (1957).
[2] On t-designs and groups, Amer. J. Math. **87**, 761—778 (1965).
HUGHES D. R., PIPER F. C. [1] Projective Planes, Springer-Verlag, New York—Heidelberg—Berlin, 1973.
HULE H., MÜLLER W. B. [1] Cyclic groups of permutations induced by polynomials over Galois fields (Spanish), An. Acad. Brasil. Ci.**45**, 63—67 (1973).
HULL R. [1] The numbers of solutions of congruences involving only k-th powers, Trans. Amer. Math. Soc. **34**, 908—937 (1932).
HURWITZ A. [1] Über höhere Kongruenzen, Archiv Math. Phys. (3) **5**, 17—27 (1903).
[2] Über die Kongruenz $ax^e + by^e + cz^e \equiv 0 \pmod p$, J. reine angew. Math. **136**, 272—292 (1909).
HUSTON R. E. [1] Asymptotic generalizations of Waring's theorem, Proc. London Math. Soc. (2) **39**, 82—115 (1935).
HWANG J. C., SHENG C. L., HSIEH C. C. [1] On the modulo-two-sum decomposition of binary sequences of finite periods, Internat. J. Electron. **39**, 97—104 (1975).
IGUSA J. [1] On the theory of algebraic correspondences and its application to the Riemann hypothesis in function fields, J. Math. Soc. Japan **1**, 147—197 (1949).
IHARA Y. [1] Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA **28**, 721—724 (1981).
IKAI T., KOSAKO H., KOJIMA Y. [1] Subsequences in linear recurring sequences, Electron. Commun. Japan **53**, no. 12, 159—166 (1970).
[2] Nonperiod-length subsequences including a cyclic subspace. Subsequences in linear recurring sequences, Systems—Computers—Controls **2**, no. 4, 34—41 (1971).
INGELS F. M. [1] Information and Coding Theory, Intext Educ. Publ., San Francisco—Toronto—London, 1971.
IRELAND K. [1] On the zeta function of an algebraic variety, Amer. J. Math. **89**, 643—660 (1967).
IRELAND K., ROSEN M. I. [1] Elements of Number Theory, Bogden & Quigley, Tarrytown-on-Hudson, N. Y., 1972. [Имеется перевод расширенного издания 1982 г.: АЙЕРЛЭНД К., РОУЗЕН М. Классическое введение в современную теорию чисел. — М.: Мир, 1987.]
ISHIMURA S. [1] On Gaussian sums associated with a character of order 5 and a rational prime number $p \equiv 1 \pmod 5$, J. Tsuda College **8**, 27—35 (1976).
IWANIEC H. [1] Mean values for Fourier coefficients of cusp forms and sums of Kloosterman sums, Journées Arithmétiques 1980 (J. V. Armitage, ed.), London Math. Soc. Lecture Note Series, no. 56, pp. 306—321, Cambridge Univ. Press, Cambridge, 1982.
IWASAWA K. [1] A note on Jacobi sums, Symposia Math., vol. 15, pp. 447—459, Academic Press, London, 1975.
JACOBI C. G. J. [1] Brief an Gauss vom 8. Februar 1827, Gesammelte Werke, vol. 7, pp. 393—440, Reimer, Berlin, 1891.
[2] Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie, Monatsber. Königl. Akad. Wiss. Berlin **1837**, 127—136; J. reine angew. Math. **30**, 166—182 (1846); Gesammelte Werke, vol. 6, pp. 254—274, Reimer, Berlin, 1891.
[3] Canon Arithmeticus, Typis Academicis, Berlin, 1839; expanded edition, Akademie-Verlag, Berlin, 1956.
JACOBSON N. [1] Structure theory for algebraic algebras of bounded degree, Ann. of Math. (2) **46**, 695—707 (1945).

[2] Lectures in Abstract algebra, vol. 3: Theory of Fields and Galois Theory, Van Nostrand, New York, 1964.

JACOBSTHAL E. [1] Anwendungen einer Formel aus der Theorie der quadratischen Reste, Dissertation, Berlin, 1906.

[2] Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate, J. reine angew. Math. **132**, 238—245 (1907).

[3] Über vertauschbare Polynome, Math. Z. **63**, 243—276 (1955).

JAMISON R. E. [1] Covering finite fields with cosets of subspaces, J. Combinatorial Theory Ser. A **22**, 253—266 (1977).

JÄNICHEN W. [1] Über einen zahlentheoretischen Satz von Hurwitz, Math. Z. **17**, 277—292 (1923).

JARDEN D. [1] Recurring Sequences, 2nd ed., Riveon Lematematika, Jerusalem, 1966.

JEGER M. [1] Irreduzible Polynome als kombinatorische Figuren, Elemente der Math. **28**, 86—92 (1973).

JOHNSEN J. [1] On the distribution of powers in finite fields, J. reine angew. Math. **251**, 10—19 (1971).

[2] On the large sieve method in $GF[q, x]$, Mathematika **18**, 172—184 (1971).

JOHNSON L. S., PORTER A. D., VARINEAU V. J. [1] Communtators over finite fields, Publ. Math. Debrecen **25**, 259—264 (1978).

JOLY J.-R. [1] Sommes de puissances d-ièmes dans un anneau commutatif, Acta Arith. **17**, 37—114 (1970).

[2] Sommes de carrés dans certains anneaux principaux, Bull. Sci. Math. (2) **94**, 85—95 (1970).

[3] Nombre de solutions de certaines équations diagonales sur un corps fini, C. R. Acad. Sci. Paris Sér. A **272**, 1549—1552 (1971).

[4] Démonstration cyclotomique de la loi de réciprocité cubique, Bull. Sci. Math. (2) **96**, 273—278 (1972).

[5] Equations et variétés algébriques sur un corps fini, L'Enseignement Math. (2) **19**, 1—117 (1973).

JORDAN C. [1] Sur les congruences du second degré, C. R. Acad. Sci. Paris **62**, 687—690 (1866); Oeuvres, vol. 3, pp. 363—365, Gauthier-Villars, Paris, 1962.

[2] Traité des substitutions et des équations algébriques, Gauthier-Villars, Paris, 1870.

[3] Sur la résolution des équations les unes par les autres, C. R. Acad. Sci. Paris **72**, 283—290 (1871); Oeuvres, vol. 1, pp. 277—284, Gauthier-Villars, Paris, 1961.

[4] Sur les sommes de Gauss à plusieurs variables, C. R. Acad. Sci. Paris **73**, 1316—1319 (1871); Oeuvres, vol. 3, pp. 367—369, Gauthier-Villars, Paris, 1962.

[5] Sur les formes réduites des congruences du second degré, C. R. Acad. Sci. Paris **74**, 1093—1095 (1872); Oeuvres, vol. 3, pp. 371—373, Gauthier-Villars, Paris, 1962.

[6] Sur la forme canonique des congruences du second degré et le nombre de leurs solutions, J. Math. Pures Appl. (2) **17**, 368—402 (1872); Oeuvres, vol. 3, pp. 375—409, Gauthier-Villars, Paris, 1962.

[7] Sur le nombre des solutions de la congruence $|a_{ik}| \equiv A \bmod M$, J. Math. Pures Appl. (6) **7**, 409—416 (1911); Oeuvres, vol. 3, pp. 543—550, Gauthier-Villars, Paris, 1962.

JORDAN CH. [1] Calculus of Finite Differences, Chelsea, New York, 1950.

JORDAN H. F., WOOD D. C. M. [1] On the distribution of sums of successive bits of shift-register sequences, IEEE Trans. Computers **C-22**, 400—408 (1973).

JORDAN J. H. [1] Pairs of consecutive power residues or non-residues, Canad. J. Math. **16**, 310—314 (1964).

[2] The distribution of cubic and quintic non-residues, Pacific J. Math, **16**, 77—85 (1966).
[3] Character sums in $Z(i)/(p)$, Proc. London Math. Soc. (3) **17**, 1—10 (1967).
[4] The distribution of kth power residues and nonresidues, Proc. Amer. Math. Soc. **19**, 678—680 (1968).
[5] The distribution of k-th power non-residues, Duke Math. J. **37**, 333—340 (1970).
JULIA G. [1] Mémoire sur la permutabilité des fractions rationnelles, Ann. Sci. Ecole Norm. Sup. (3) **39**, 131—215 (1922).
JUNG F. R. [1] Solutions of some systems of equations over a finite field with applications to geometry, Duke Math. J. **39**, 189—202 (1972).
[2] On conics over a finite field, Canad. J. Math. **26**, 1281—1288 (1974).
KACZYNSKI T. J. [1] Another proof of Wedderburn's theorem, Amer. Math. Monthly **71**, 652—653 (1964).
KALMAN R. E. [1] Mathematical description of linear dynamical systems, SIAM J. Control **1**, 152—192 (1963).
[2] Algebraic aspects of the theory of dynamical systems, Differential Equations and Dynamical Systems (J. K. Hale and J. P. LaSalle, eds.), pp. 133—146, Academic Press, New York, 1967.
KAMAL A. K., SINGH H., PURI S., NANDA N. K. [1] On the evaluation of transition matrices in finite fields, Internat. J. Systems Sci. **6**, 561—564 (1975).
KAMKE E. [1] Zur Arithmetik der Polynome, Math. Z. **19**, 247—264 (1924).
KANTOR R. [1] Über die Anzahl inkongruenter Werte ganzer, rationaler Funktionen, Monatsh. Math. Phys. **26**, 24—39 (1915).
KAPLAN P. [1] Démonstration des lois de réciprocité quadratique et biquadratique, J. Fac. Sci. Univ. Tokyo Sect. I **16**, 115—145 (1969).
KARAMATA J., TOMIĆ M., [1] Sur une inégalité de Kusmin—Landau relative aux sommes trigonométriques et son application à la somme de Gauss, Acad. Serbe Sci. Publ. Inst. Math. **3**, 207—218 (1950).
KARLIN M. [1] New binary coding results by circulants, IEEE Trans. Information Theory **IT-15**, 81—92 (1969).
KARPOVSKY M. G. [1] Finite Orthogonal Series in the Design of Digital Devices, Wiley, New York, 1976.
KARTESZI F. [1] Introduction to Finite Geometries, North-Holland, Amsterdam, 1976.
KASAMI T. [1] Systematic codes using binary shift register sequences, J. Info. Processing Soc. Japan **1**, 198—200 (1960).
KASAMI T., LIN S., PETERSON W. W. [1] Polynomial codes, IEEE Trans. Information Theory **IT-14**, 807—814 (1968).
KATZ N. M. [1] On a theorem of Ax, Amer. J. Math. **93**, 485—499 (1971).
[2] Travaux de Dwork, Séminaire Bourbaki 1971/72, Exp. 409, Lecture Notes in Math., vol. 317, pp. 167—200, Springer-Verlag, Berlin—Heidelberg—New York, 1973.
[3] An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields, Proc. Symp. Pure Math., vol. 28, pp. 275—305, American Math. Society, Providence, R. I., 1976.
[4] Sommes exponentielles, Astérisque, no. 79, Soc. Math. France, Paris, 1980.
[5] Crystalline cohomology, Dieudonné modules, and Jacobi sums, Automorphic Forms, Representation Theory and Arithmetic (Bombay, 1979), Tata Inst. Fund. Res. Studies in Math., vol. 10, pp. 165—246, Tata Institute of Fundamental Research, Bombay, 1981.
KAUTSCHITSCH H. [1] Kommutative Teilhalbgruppen der Kompositionshalbgruppe von Polynomen und formalen Potenzreihen, Monatsh. Math. **74**, 421—436 (1970).
[2] Über vertauschbare Polynome mit vorgegebenen Gradzahlen, Arch. Math. **27**, 611—619 (1976).

KAUTZ W. H. [1] Linear Sequential Switching Circuits—Selected Technical Papers, Holden-Day, San Francisco, 1965.
KAUTZ W. H., LEVITT K. N. [1] A survey of progress in coding theory in the Soviet Union, IEEE Trans. Information Theory **IT-15**, 197—245 (1969).
KELLER G., OLSON F. R. [1] Counting polynomial functions (mod p^n), Duke Math. J. **35**, 835—838 (1968).
KEMPFERT H. [1] On the factorization of polynomials, J. Number Theory **1**, 116—120 (1969).
KEMPNER A. J. [1] Polynomials and their residue systems, Trans. Amer. Math. Soc. **22**, 240—266, 267—288 (1921).
[2] Polynomials of several variables and their residue systems, Trans. Amer. Math. Soc. **27**, 287—298 (1925).
KHADZHIIVANOV N. G., NENOV N. D. [1] Число нетривиальных решений уравнения Ферма $x^n + y^n = z^n$ в поле Галуа. C. R. Acad. Bulgare Sci. **32**, 557—560 (1979).
KIEFE C. [1] Sets definable over finite fields: their zeta-functions, Trans. Amer. Math. Soc. **223**, 45—59 (1976).
KIM J. B. [1] The number of generalized inverses of a matrix, Algebraic Theory of Semigroups (Szeged, 1976), Colloq. Math. Soc. János Bolyai, vol. 20, pp. 277—280, North-Holland, Amsterdam, 1979.
KISS P., BUI MINH PHONG [1] On a function concerning second-order recurrences, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **21**, 119—122 (1978).
KLEIMAN S. L. [1] Algebraic cycles and the Weil conjectures, Dix exposés sur la cohomologie des schémas, Advanced Studies in Pure Math., vol. 3, pp. 359—386, North-Holland, Amsterdam, 1968.
KLEIN F. [1] Zur Theorie der linearen Kongruenzensysteme, J. reine angew. Math. **159**, 238—245 (1928).
[2] Zur Theorie der Systeme von Potenzproduktkongruenzen, J. reine angew. Math. **164**, 141—150 (1931).
[3] Über rechteckige Matrizen, bei denen die Determinanten maximaler Reihenanzahl teilerfremd zu einem Modul sind, Jber. Deutsch. Math.-Verein. **40**, 233—238 (1931).
KLINGENBERG W., WITT E. [1] Über die Arfsche Invariante quadratischer Formen mod 2, J. reine angew. Math. **193**, 121—122 (1954).
KLOBE W. [1] Über eine untere Abschätzung der n-ten Kreisteilungspolynome $g_n(z) = \prod_{d/n}(z^d - 1)^{\mu(n/d)}$, J. reine angew. Math. **187**, 68—69 (1949).
KLOOSTERMAN H. D. [1] On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. **49**, 407—464 (1926).
[2] Asymptotische Formeln für die Fourierkoeffizienten ganzer Modulformen, Abh. Math. Sem. Univ. Hamburg **5**, 337—352 (1927).
[3] Thetareihen in total-reellen algebraischen Zahlkörpern, Math. Ann. **103**, 279—299 (1930).
[4] On the singular series in Waring's problem and in the problem of the representation of integers as a sum of powers of primes, Indag. Math. **1**, 51—56 (1939).
[5] The behaviour of general theta functions under the modular group and the characters of binary modular congruence groups. II, Ann. of Math. (2) **47**, 376—447 (1946).
[6] The law of quadratic reciprocity, Indag. Math. **27**, 163—164 (1965).
KLÖSGEN W. [1] Untersuchungen über Fermatsche Kongruenzen, Gesellschaft für Mathematik und Datenverarbeitung, no. 36, Bonn, 1970.
KLUYVER J. C. [1] Problem 139 (Dutch), Wiskundige Opgaven **14**, 278—280 (1928).
KNEE D., GOLDMAN H. D. [1] Quasi-self-reciprocal polynomials and potentially large minimum distance BCH codes, IEEE Trans. Information Theory **IT-15**, 118—121 (1969).

KNESER A. [1] Arithmetische Begründung einiger algebraischer Fundamentalsätze, J. reine angew. Math. **102**, 20—55 (1888).

KNIGHT M. J., WEBB W. A. [1] Uniform distribution of third order linear recurrence sequences, Acta Arith. **36**, 7—20 (1980).

KNOPFMACHER J. [1] Abstract Analytic Number Theory, North-Hollang, Amsterdam, 1975.

[2] Analytic Arithmetic of Algebraic Function Fields, Lecture Notes in Pure and Appl. Math., vol. 50, Dekker, New York, 1979.

KNOPP M. I. [1] Automorphic forms of nonnegative dimension and exponential sums, Michigan Math. J. **7**, 257—287 (1960).

KNUTH D. E. [1] Finite semi-fields and projective planes, J. Algebra **2**, 182—217 (1965).

[2] The Art of Computer Programming, vol. 1: Fundamental Algorithms, Addison-Wesley, Reading, Mass., 1968. [Имеется перевод: КНУТ Д. Е. Искусство программирования для ЭВМ. т. 1. Основные алгоритмы. — М.: Мир, 1976.]

[3] The Art of Computer Programming, vol. 2: Seminumerical Algorithms, Addison-Wesley, Reading, Mass., 1969; 2nd ed., Addison-Wesley, Reading, Mass., 1981. [Имеется перевод: КНУТ Д. Е. Искусство программирования для ЭВМ. т. 2. Получисленные алгоритмы. — М.: Мир, 1977.]

KOBLITZ N. [1] p-adic variation of the zeta-function over families of varieties defined over finite fields, Compositio Math. **31**, 119—218 (1975).

[2] p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer-Verlag, New York—Heidelberg—Berlin, 1977. [Имеется перевод: КОБЛИЦ Н. p-адические числа, p-адический анализ и дзета-функции. — М.: Мир, 1982.]

[3] p-adic Analysis: A Short Course on Recent Work, London Math. Soc. Lecture Note Series, no. 46, Cambridge Univ. Press, Cambridge, 1980.

[4] The p-adic approach to solutions of equations over finite fields, Amer. Math. Monthly **87**, 115—118 (1980).

KOCHENDÖRFFER R. [1] Introduction to Algebra, Wolters-Noordhoff, Groningen, 1972.

KONDO T. [1] On Gaussian sums attached to the general linear groups over finite fields, J. Math. Soc. Japan **15**, 244—255 (1963).

KONHEIM A. G. [1] Cryptography. A Primer, Wiley, New York, 1981.

KORNBLUM H. [1] Über die Primfunktionen in einer arithmetischen Progression, Math. Z. **5**, 100—111 (1919).

KÖRNER O., STÄHLE H. [1] Remarks on Hua's estimate of complete trigonometrical sums, Acta Arith. **35**, 353—359 (1979).

KOUTSKÝ K. [1] On the quadratic character of numbers and on the generalization of a theorem of Lagrange on the distribution of quadratic residues (Czech), Rozpravy Ceské Akad. Ved. **39** (1930), no. 43.

[2] On the distribution of power residues for a prime modulus (Czech), Čas. Pěst. Mat. Fys. **59**, 65—82 (1930).

KRAÏTCHIK M. [1] Recherches sur la théorie des nombres. II: Factorisation, Gauthier-Villars, Paris, 1929.

[2] On the factorization of $2^n \pm 1$, Scripta Math. **18**, 39—52 (1952).

KRASNER M. [1] Sur la primitivité des corps $\mathfrak{p}$-adiques, Mathematica (Cluj) **13**, 72—191 (1937).

[2] Sur la représentation exponentielle dans les corps relativement galoisiens de nombres $\mathfrak{p}$-adiques, Acta Arith. **3**, 133—173 (1939).

KRÄTZEL E. [1] Kubische und biquadratische Gaußsche Summen, J. reine angew Math. **228**, 159—165 (1967).

KRISHNAMURTHY E. V. [1] Exact inversion of a rational polynomial matrix using finite field transforms, SIAM J. Appl. Math. **35**, 453—464 (1978).

KRISHNAMURTHY E. V., RAMACHANDRAN V. [1] A cryptographic system based on finite field transforms, Proc. Indian Acad. Sci. Sect. A **89**, no. 2, 75—93 (1980).

KRONECKER L. [1] Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$, J. Math. Pures Appl. **19**, 177—192 (1854); Werke, vol. 1, pp. 75—92, Teubner, Leipzig, 1895.

[2] Sur une formule de Gauss, J. Math. Pures Appl. (2) **1**, 392—395 (1856); Werke, vol. 4, pp. 171—175, Teubner, Leipzig, 1929.

[3] Über den vierten Gauss'schen Beweis des Reciprocitätsgesetzes für die quadratischen Reste, Monatsber. Preuss. Akad. Wiss. Berlin **1880**, 686—698, 854—860; Werke, vol. 4, pp. 275—294, Teubner, Leipzig, 1929.

[4] Zur Theorie der Elimination einer Variabeln aus zwei algebraischen Gleichungen, Monatsber. Preuss. Akad. Wiss. Berlin **1881**, 535—600; Werke, vol. 2, pp. 113—192, Teubner, Leipzig, 1897.

[5] Grundzüge einer arithmetischen Theorie der algebraischen Grössen, J. reine angew. Math. **92**, 1—122 (1882); Werke, vol. 2, pp. 237—387, Teubner, Leipzig, 1897.

[6] Zur Theorie der Abelschen Gleichungen, J. reine angew. Math. **93**, 338—364 (1882); Werke, vol. 4, pp. 131—162, Teubner, Leipzig, 1929.

[7] Über einige Anwendungen der Modulsysteme auf elementare algebraische Fragen, J. reine angew. Math. **99**, 329—371 (1886); Werke, vol. 3, part 1, pp. 145—208, Teubner, Leipzig, 1899.

[8] Ein Fundamentalsatz der allgemeinen Arithmetik, J. reine angew. Math. **100**, 490—510 (1887); Werke, vol. 3, part 1, pp. 209—240, Teubner, Leipzig, 1899.

[9] Summirung der Gauss'schen Reihen $\sum_{h=0}^{h=n-1} e^{2h^2\pi i/n}$, J. reine angew. Math. **105**, 267—268 (1889); Werke, vol. 4, pp. 295—300, Teubner, Leipzig, 1929.

KUBOTA R. M. [1] Waring's problem for $F_q[x]$, Dissertationes Math. **117**, 1—60 (1974).

KUBOTA T. [1] Über quadratische Charaktersummen, Nagoya Math. J. **19**, 15—25 (1961).

[2] Local relation of Gauss sums, Acta Arith. **6**, 285—294 (1961).

[3] Über eine Verallgemeinerung der Reziprozität der Gaußschen Summen, Math. Z. **82**, 91—100 (1963).

[4] Some arithmetical applications of an elliptic function, J. reine angew. Math. **214/215**, 141—145 (1964).

[5] On a special kind of Dirichlet series, J. Math. Soc. Japan **20**, 193—207 (1968).

[6] Some results concerning reciprocity law and real analytic automorphic functions, Proc. Symp. Pure Math., vol. 20, pp. 382—395, American Math. Society, Providence, R. I., 1971.

KÜHNE H. [1] Eine Wechselbeziehung zwischen Functionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt, J. reine angew. Math. **124**, 121—133 (1902).

[2] Angenäherte Auflösung von Congruenzen nach Primmodulsystemen in Zusammenhang mit den Einheiten gewisser Körper, J. reine angew. Math. **126**, 102—115 (1903).

[3] Bemerkungen zu der Abhandlung des Herrn Hurwitz: Über höhere Kongruenzen, Archiv Math. Phys. (3) **6**, 174—176 (1904).

KUIPERS L. [1] A remark on a theorem of L. Carlitz, Mat. Vesnik **9**, 113—116 (1972).

[2] A remark on asymptotic distribution in $GF[p^r, x]$, Rev. Roum. Math. Pures Appl. **18**, 1217—1221 (1973).

[3] Einige Bemerkungen zu einer Arbeit von G. J. Rieger, Elemente der Math. **34**, 32—34 (1979).

KUIPERS L., NIEDERREITER H. [1] Uniform Distribution of Sequences, Wiley-Interscience, New York, 1974.

KUIPERS L., SCHEELBEEK P. A. J. [1] Uniform distribution of sequences from direct products of groups, Ann. Sc. Norn.. Sup. Pisa **22**, 599—606 (1968).
KUIPERS L., SHIUE J.-S. [1] On the distribution modulo m of sequences of generalized Fibonacci numbers, Tamkang J. Math. **2**, 181—186 (1971).
[2] A distribution property of a linear recurrence of the second order, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **52**, 6—10 (1972).
[3] A distribution property of the sequence of Lucas numbers, Elemente der Math. **27**, 10—11 (1972).
[4] A distribution property of the sequence of Fibonacci numbers, Fibonacci Quart. **10**, 375—376 (1972).
KUMAR I. J., KUMARI M. [1] Local complementation of periodic sequences over *GF* (2), J. Combin. Inform. System. Sci. **6**, 178—186 (1981).
KUMARI M. [1] Concatenation properties of δ-sequences over *GF* (2), J. Inform. Optim. Sci. **2**, 147—160 (1981).
KUMMER E. E. [1] Eine Aufgabe, betreffend die Theorie der cubischen Reste, J. reine angew. Math. **23**, 285—286 (1842); Collected Papers, vol. 1, pp. 143—144, Springer-Verlag, Berlin—Heidelberg—New York, 1975.
[2] De residuis cubicis disquisitiones nonnullae analyticae, J. reine angew. Math. **32**, 341—359 (1846); Collected Papers, vol. 1, pp. 145—163, Springer-Verlag, Berlin—Heidelberg—New York, 1975.
[3] Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren, J. reine angew. Math. **35**, 327—367 (1847); Collected Papers, vol. 1, pp. 211—251, Springer-Verlag, Berlin—Heidelberg—New York, 1975.
[4] Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste, Monatsber. Königl. Akad. Wiss. Berlin **1850**, 154—165; Collected Papers, vol. 1, pp. 345—357, Springer-Verlag, Berlin—Heidelberg—New York, 1975.
[5] Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers, J. Math. Pures Appl. **16**, 377—498 (1851); Collected Papers, vol. 1, pp. 363—484, Springer-Verlag, Berlin—Heidelberg—New York, 1975.
[6] Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, J. reina angew. Math. **44**, 93—146 (1852); Collected Papers, vol. 1, pp. 485—538, Springer-Verlag, Berlin—Heidelberg—New York, 1975.
[7] Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, Math. Abh. Königl. Akad. Wiss. Berlin **1856**, 1—47; Collected Papers, vol. 1, pp. 583—629, Springer-Verlag, Berlin—Heidelberg—New York, 1975.
KUNERT D. [1] Ein neuer Beweis für die Reziprozitätsformel der Gaußschen Summen in beliebigen algebraischen Zahlkörpern, Math. Z. **40**, 326—347 (1936).
KUNG J. P. S. [1] The cycle structure of a linear transformation over a finite field, Linear Algebra Appl. **36**, 141—155 (1981).
KUSTAANHEIMO P., QVIST B. [1] On differentiation in Galois fields, Suom. Tiedeak. Toimituk. Helsinki Ser. A I 137 (1952).
KUTZKO P. C. [1] The cyclotomy of finite commutative P.I. R.'s, Illinois J. Math. **19**, 1—17 (1975).
LAFFEY T. J. [1] Infinite rings with all proper subrings finite, Amer. Math. Monthly **81**, 270—272 (1974).
LAGRANGE J.-L. [1] Sur l'intégration d'une équation différentielle a différences finies, qui contient la théorie des suites récurrentes, Misc. Taurinensia **1** (1759); Oeuvres, vol. 1, pp. 23—36, Gauthier-Villars, Paris, 1867.
[2] Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers, Mémoires Acad. Roy. Berlin **24** (1770); Oeuvres, vol. 2, pp. 655—726, Gauthier-Villars, Paris, 1868.

[3] Démonstration d'un théorème d'arithmétique, Nouv. Mémoires Acad. Roy. Berlin **1770**, 123—133; Oeuvres, vol. 3, pp. 189—201, Gauthier-Villars, Paris, 1869.
[4] Réflexions sur la résolution algébrique des équations, Nouv. Mémoires Acad. Roy. Berlin **1770**, 134—215; ibid. **1771**, 138—254; Oeuvres, vol. 3, pp. 205—421, Gauthier-Villars, Paris, 1869.
[5] Recherches sur les suites récurrentes dont les termes varient de plusieurs manières différentes, ou sur l'intégration des équations linéaires aux différences finies et partielles; et sur l'usage de ces équations dans la théorie des hasards, Nouv. Mémoires Acad. Roy. Berlin **1775**, 183—272; Oeuvres, vol. 4, pp. 151—251, Gauthier-Villars, Paris, 1869.

LAKKIS K. [1] Die galoisschen Gauss'schen Summen von Hasse, Bull. Soc. Math. Grèce **7**, 183—371 (1966).
[2] Die verallgemeinerten Gaußschen Summen, Arch. Math. **17**, 505—509 (1966).
[3] Die lokalen verallgemeinerten Gauss'schen Summen, Bull. Soc. Math. Grèce **8**, 143—150 (1967).

LAKSOV D. [1] Linear recurring sequences over finite fields, Math. Scand. **16**, 181—196 (1965).

LAL M. [1] On the separability of multivariable polynomials, Proc. IEEE **63**, 718—719 (1975).

LAMPRECHT E. [1] Allgemeine Theorie der Gaußschen Summen in endlichen kommutativen Ringen, Math. Nachr. **9**, 149—196 (1953).
[2] Gaußsche Summen in endlichen Ringen und ihre Anwendungen, Bericht Math.-Tagung (Berlin, 1953), pp. 179—185, Deutscher Verlag der Wissenschaften, Berlin, 1953.
[3] Struktur und Relationen allgemeiner Gaußscher Summen in endlichen Ringen, J. reine angew. Math. **197**, 1—26, 27—48 (1957).

LANDAU E. [1] Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen, Göttinger Hachr. **1918**, 79—97.
[2] Vorlesungen über Zahlentheorie, vol. 1, part 2, Hirzel, Leipzig, 1927.
[3] Über das Vorzeichen der Gaußschen Summe, Göttinger Nachr. **1928**, 19—20.
[4] Zum Waringschen Problem. III, Math. Z. **32**, 699—702 (1930).
[5] Elementary Number Theory, 2nd ed., Chelsea, New York, 1958.

LANDSBERG G. [1] Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe, J. reine angew. Math. **111**, 87—88 (1893).
[2] Zur Theorie der Gaussschen Summen und der linearen Transformation der Thetafunctionen, J. reine angew. Math. **111**, 234—253 (1893).

LANG S. [1] Abelian Varieties, Interscience, New York, 1959.
[2] Some theorems and conjectures in diophantine equations, Bull. Amer. Math. Soc. **66**, 240—249 (1960).
[3] Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.
[4] Algebra, Addison-Wesley, Reading, Mass., 1971. [Имеется перевод предыдущего издания: ЛЕНГ С. Алгебра. — М.: Мир, 1968.]
[5] Cyclotomic Fields, Springer-Verlag, New York—Heidelberg—Berlin, 1978.
[6] Cyclotomic Fields, vol. 2, Springen-Verlag, New York—Heidelberg—Berlin, 1980.

LANG S., WEIL A. [1] Number of points of varieties in finite fields, Amer. J. Math. **76**, 819—827 (1954).

LATAWIEC K. J. [1] On different time-domain solutions of the problem of generating shifted linear binary sequences, Problemy Uprav. i Teor. Informacii **6**, 223—230 (1977).

LAUMON G. [1] Majorations de sommes trigonométriques (d'après P. Deligne et N. Katz), Astérisque, no. 82—83, pp. 221—258, Soc. Math. France, Paris, 1981.

LAUSCH H., MÜLLER W. B., NÖBAUER W. [1] Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenringes modulo n, J. reine angew. Math. **261**, 88—99 (1973).

LAUSCH H., NÖBAUER W. [1] Algebra of Polynomials, North-Holland, Amsterdam, 1973.
LAXTON R. R., ANDERSON J. A. [1] Linear recurrences and maximal length sequences, Math. Gaz. **56**, 299—309 (1972).
LEAHEY W. [1] Sums of squares of polynomials with coefficients in a finite field, Amer. Math. Monthly **74**, 816—819 (1967).
LEBESGUE V. A. [1] Recherches sur les nombres. I, II, III, J. Math. Pures Appl. **2**, 253—292 (1837); ibid. **3**, 113—131, 132—144 (1838).
[2] Démonstration de quelques formules d'un mémoire de M. Jacobi, J. Math. Pures Appl. **19**, 289—300 (1854).
[3] Démonstration de l'irréductibilité de l'équation aux racines primitives de l'unité, J. Math. Pures Appl. (2) **4**, 105—110 (1859).
[4] Note sur les congruences, C. R. Acad. Sci. Paris **51**, 9—13 (1860).
[5] Sur une congruence du deuxième degré à plusieurs inconnues, C. R. Acad. Sci. Paris **62**, 868—872 (1866).
LEE A. [1] Über einige Extremalaufgaben bezüglich endlicher Körper, Acta Math. Acad. Sci. Hungar. **13**, 235—243 (1962).
LEE J. J., SMITH D. R. [1] Families of shift-register sequences with impulsive correlation properties, IEEE Trans. Information Theory **IT-20**, 255—261 (1974).
LEE M. A. [1] Some irreducible polynomials which are reducible mod p for all p, Amer. Math. Monthly **76**, 1125 (1969).
LEHMER D. H. [1] Tests for primality by the converse of Fermat's theorem, Bull. Amer. Math. Soc. **33**, 327—340 (1927).
[2] An extended theory of Lucas' functions, Ann. of Math. (2) **31**, 419—448 (1930).
[3] Some new factorizations of $2^n \pm 1$, Bull. Amer. Math. Soc. **39**, 105—108 (1933).
[4] A photo-electric number sieve, Amer. Math Monthly **40**, 401—406 (1933).
[5] A machine for combining sets of linear congruences, Math. Ann. **109**, 661—667 (1934).
[6] On the series for the partition function, Trans. Amer. Math. Soc. **43**, 271—295 (1938).
[7] A factorization theorem applied to a test for primality, Bull. Amer. Math. Soc. **45**, 132—137 (1939).
[8] On certain character matrices, Pacific J. Math. **6**, 491—499 (1956).
[9] Power character matrices, Pacific J. Math. **10**, 895—907 (1960).
[10] Computer technology applied to the theory of numbers, Studies in Number Theory (W. J. LeVeque, ed.), pp. 117—151, Prentice-Hall, Englewood Cliffs, N. J., 1969.
[11] Incomplete Gauss sums, Mathematika **23**, 125—135 (1976).
LEHMER D. H., LEHMER E. [1] On the cubes of Kloosterman sums, Acta Arith. **6**, 15—22 (1960).
[2] On runs of residues, Proc. Amer. Math. Soc. **13**, 102—106 (1962).
[3] The cyclotomy of Kloosterman sums, Acta Arith. **12**, 385—407 (1967).
[4] The cyclotomy of hyper-Kloostermán sums, Acta Arith. **14**, 89—111 (1968).
LEHMER D. H., LEHMER E., MILLS W. H. [1] Pairs of consecutive power resudues, Canad. J. Math. **15**, 172—177 (1963).
LEHMER D. H., LEHMER E., MILLS W. H., SELFRIDGE J. L. [1] Machine proof of a theorem on cubic residues, Math. Comp. **16**, 407—415 (1962).
LEHMER E. [1] On the quintic character of 2, Bull. Amer. Math. Soc. **55**, 62—63 (1949).
[2] The quintic character of 2 and 3, Duke Math. J. **18**, 11—18 (1951).
[3] On residue difference sets, Canad. J. Math. **5**, 425—432 (1953).
[4] On the number of solutions of $u^k + D \equiv w^2 \pmod{p}$, Pacific J. Math. **5**, 103—118 (1955).

[5] On the location of Gauss sums, Math. Tables Aids Comput. **10**, 194—202 (1956).

[6] On Euler's criterion, J. Austral. Math. Soc. **1**, 64—70 (1959).

[7] On Jacobi functions, Pacific J. Math. **10**, 887—893 (1960).

[8] Artiads characterized, J. Math. Anal. Appl. **15**, 118—131 (1966).

LEHMER E., VANDIVER H. S. [1] On the computation of the number of solutions of certain trinomial congruences, J. Assoc. Comput. Mach. **4**, 505—510 (1957).

LEHTI R. [1] Evaluation matrices for polynomials in Galois fields, Soc. Sci. Fenn. Comment. Phys.-Math. **22**, no. 3, 1959.

LEMPEL A. [1] Analysis and synthesis of polynomials and sequences over *GF* (2), IEEE Trans. Information Theory **IT-17**, 297—303 (1971).

[2] Matrix factorization over *GF* (2) and trace-orthogonal bases of *GF* (2^n), SIAM J. Computing **4**, 175—186 (1975).

LEMPEL A., COHN M., EASTMAN W. L. [1] A class of balanced binary sequences with optimal autocorrelation properties, IEEE Trans. Information Theory **IT-23**, 38—42 (1977).

LEMPEL A., EASTMAN W. L. [1] High speed generation of maximal length sequences, IEEE Trans. Computers **C-20**, 227—229 (1971).

LEMPEL A., WINOGRAD S. [1] A new approach to error-correcting codes, IEEE Trans. Information Theory **IT-23**, 503—508 (1977).

LENSTRA A. K. [1] Lattices and factorization of polynomials, SIGSAM Bull. **15**, no. 3, 15—16 (1981).

LENSTRA A. K., LENSTRA H. W., Jr., LOVÁSZ L. [1] Factoring polynomials with rational coefficients, Math. Ann. **261**, 515—534 (1982).

LENSTRA H. W., Jr. [1] Primitive normal bases for finite fields, unpublished manuscript, 1977.

[2] Primality testing algorithms (after Adleman, Rumely and Williams), Séminaire Bourbaki 1980/81, Exp. 576, Lecture Notes in Math., vol. 901, pp. 243—257, Springer-Verlag, Berlin—Heidelberg—New York, 1981.

LEONARD P. A. [1] On constructing quartic extensions of *GF* (*p*), Norske Vid. Selsk. Forh. (Trondheim) **40**, 96—97 (1967).

[2] On factorizations of certain trinomials, Norske Vid. Selsk. Forh. (Trondheim) **42**, 56—62 (1969).

[3] On factoring quartics (mod *p*), J. Number Theory **1**, 113—115 (1969).

[4] A note on cubics over *GF* (2^n), Norske Vid. Selsk. Skr. (Trondheim) **1974**, no. 1.

[5] Factorization of general polynomials, J. Number Theory **6**, 335—338 (1974).

LEONARD P. A., MORTIMER B. C., WILLIAMS K. S. [1] The eleventh power character of 2, J. reine angew. Math. **286**, 213—222 (1976).

LEONARD P. A., WILLIAMS K. S. [1] Quartics over *GF* (2^n), Proc. Amer. Math. Soc. **36**, 347—350 (1972).

[2] A diophantine system of Dickson, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **56**, 145—150 (1974).

[3] The cyclotomic numbers of order seven, Proc. Amer. Math. Soc. **51**, 295—300 (1975).

[4] Jacobi sums and a theorem of Brewer, Rocky Mountain J. Math. **5**, 301—308 (1975); Erratum, ibid. **6**, 509 (1976).

[5] The cyclotomic numbers of order eleven, Acta Arith. **26**, 365—383 (1975).

[6] A rational sixteenth power reciprocity law, Acta Arith. **33**, 365—377 (1977).

[7] Evaluation of certain Jacobsthal sums, Boll. Un. Mat. Ital. (5) **15**, 717—723 (1978).

LEOPOLDT H.-W. [1] Zur Arithmetik in abelschen Zahlkörpern, J. reine angew. Math. **209**, 54—71 (1962).

LERCH M. [1] Zur Theorie der Gaußschen Summen, Math. Ann. **57**, 554—567 (1903).

LEVI H. [1] Composite polynomials with coefficients in an arbitrary field of characteristic zero, Amer. J. Math. **64**, 389—400 (1942).
LEVINE J., BRAWLEY J. V. [1] Involutory commutants with some applications to algebraic cryptography. I, II, J. reine angew. Math. **224**, 20—43 (1966); ibid. **227**, 1—24 (1967).
[2] Some cryptographic applications of permutation polynomials, Cryptologia **1**, 76—92 (1977).
LEVINE J., HARTWIG R. E. [1] Applications of the Drazin inverse to the Hill cryptographic system. I, II, Cryptologia **4**, 71—85, 150—168 (1980).
LEWIS D. J. [1] Singular quartic forms, Duke Math. J. **21**, 39—44 (1954).
[2] Cubic congruences, Michigan Math. J. **4**, 85—95 (1957).
[3] Diagonal forms over finite fields, Norske Vid. Selsk. Forh. (Trondheim) **33**, 61—65 (1960).
LEWIS D. J., SCHUUR S. E. [1] Varieties of small degree over finite fields, J. reine angew. Math. **262/263**, 293—306 (1973).
LIANG J. J. [1] On the solutions of trinomial equations over finite fields, Bull. Calcutta Math. Soc. **70**, 379—382 (1978).
LIBRI G. [1] Mémoire sur la théorie des nombres, J. reine angew. Math. **9**, 169—188 (1832).
[2] Mémoire sur la théorie des nombres, J. reine angew. Math. **9**, 261—276 (1832).
LIDL R. [1] Über Permutationspolynome in mehreren Unbestimmten, Monatsh. Math. **75**, 432—440 (1971).
[2] Über die Darstellung von Permutationen durch Polynome, Abh. Math. Sem. Univ. Hamburg **37**, 108—111 (1972).
[3] Über Permutationsfunktionen in mehreren Unbestimmten, Acta Arith. **20**, 291—296 (1972).
[4] Tschebyscheffpolynome und die dadurch dargestellten Gruppen, Monatsh. Math. **77**, 132—147 (1973).
[5] Reguläre Polynome über endlichen Körpern, Beiträge zur Algebra und Geometrie **2**, 55—59 (1974).
[6] Über die Struktur einer durch Tschebyscheffpolynome in zwei Variablen dargestellten Permutationsgruppe, Beiträge zur Algebra und Geometrie **3**, 41—48 (1974).
[7] Einige ungelöste Probleme bei endlichen Körpern, Math. Balkanica **4**, 409—414 (1974).
[8] Tschebyscheffpolynome in mehreren Variablen, J. reine angew. Math. **273**, 178—198 (1975).
LIDL R., MÜLLER W. B. [1] Über Permutationsgruppen, die durch Tschebyscheff-Polynome erzeugt werden, Acta Arith. **30**, 19—25 (1976).
LIDL R., NIEDERREITER H. [1] On orthogonal systems and permutation polynomials in several variables, Acta Arith. **22**, 257—265 (1973).
LIDL R., PILZ G. [1] Angewandte abstrakte Algebra. I, II, Bibliographisches Institut, Mannheim, 1982.
LIDL R., WELLS C. [1] Chebyshev polynomials in several variables, J. reine angew. Math. **255**, 104—111 (1972).
LIDL R., WIESENBAUER J. [1] Ringtheorie und Anwendungen, Akademische Verlagsgesellschaft, Wiesbaden, 1980.
LIN S. [1] On a class of cyclic codes, Error Correcting Codes (H. B. Mann, ed.), pp. 131—148, Wiley, New York, 1968.
[2] An Introduction to Error-Correcting Codes, Prentice-Hall, Englewood Cliffs, N. J., 1970.
LINDGREN H. [1] Polynomial solutions of binomial congruences, J. Austral. Math. Soc. **1**, 257—280 (1960).
LINDHOLM J. H. [1] An analysis of the pseudo-randomness properties of subsequences of long *m*-sequences, IEEE Trans. Information Theory **IT-14**, 569—576 (1968).

LINDSTRÖM B. [1] On group and nongroup perfect codes in q symbols, Math Scand. **25**, 149—158 (1969).

LITZINGER M. [1] A basis for residual polynomials in n variables, Trans. Amer. Math. Soc. **37**, 216—225 (1935).

LIU K. Y., REED I. S., TRUONG T. K. [1] Fast number-theoretic transforms for digital filtering, Electron. Lett. **12**, 644—646 (1976).

[2] High-radix transforms for Reed—Solomon codes over Fermat primes, IEEE Trans. Information Theory **IT-23**, 776—778 (1977).

LLOYD D. B. [1] Factorization of the general polynomial by means of its homomorphic congruential functions, Amer. Math. Monthly **71**, 863—870 (1964).

[2] The use of finite polynomial rings in the factorization of the general polynomial, J. Res. Nat. Bur. Standards Sect. B **69**, 189—212 (1965).

LLOYD D. B., REMMERS H. [1] Polynomial factor tables over finite fields, Math. Algorithms **2**, 85—99 (1967).

LONDON D., ZIEGLER Z. [1] Functions over the residue field modulo a prime, J. Austral. Math. Soc. **7**, 410—416 (1967).

LONG A. F., Jr. [1] Some theorems on factorable irreducible polynomials, Duke Math. J. **34**, 281—291 (1967).

[2] Classification of irreducible factorable polynomials over a finite field, Acta Arith. **12**, 301—313 (1967).

[3] Factorization of irreducible polynomials over a finite field with the substitution $x^{p^r} - x$ for x, Duke Math. J. **40**, 63—76 (1973).

[4] Factorization of irreducible polynomials over a finite field with the substitution $x^{q^r} - x$ for x, Acta Arith. **25**, 65—80 (1973).

[5] A theorem on factorable irreducible polynomials in several variables over a finite field with the substitution $x_i^{q^r} - x_i$ for x_i, Math. Nachr. **63**, 123—130 (1974).

LONG A. F., Jr., VAUGHAN T. P. [1] Factorization of $Q(h(T)(x))$ over a finite field, where $Q(x)$ is irreducible and $h(T)(x)$ is linear. II, Linear Algebra Appl. **11**, 53—72 (1975).

[2] Factorization of $Q(h(T)(x))$ over a finite field, where $Q(x)$ is irreducible and $h(T)(x)$ is linear. I, Linear Algebra Appl. **13**, 207—221 (1976).

LONG C. T., WEBB W. A. [1] Normality in $GF\{q, x\}$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **54**, 848—853 (1973).

LOWE R. D., ZELINSKY D. [1] Which Galois fields are pure extensions? Math. Student **21**, 37—41 (1953).

LOXTON J. H. [1] Products related to Gauss sums, J. reine angew. Math. **268/269**, 53—67 (1974).

[2] On the determination of Gauss sums, Sém. Delange—Pisot—Poitou 1976/77, Théorie des Nombres, Exp. 27, Secrétariat Math., Paris, 1977.

[3] Some conjectures concerning Gauss sums, J. reine angew. Math. **297**, 153—158 (1978).

LOXTON J. H., SMITH R. A. [1] On Hua's estimate for exponential sums, J. London Math. Soc. (2) **26**, 15—20 (1982).

[2] Estimates for multiple exponential sums, J. Austral. Math. Soc. Ser. **A 33**, 125—134 (1982).

LUBELSKI S. [1] Zur Theorie der höheren Kongruenzen, J. reine angew. Math. **162**, 63—68 (1930).

[2] Zur Reduzibilität von Polynomen in der Kongruenztheorie, Acta Arith. **1**, 169—183 (1936).

[3] Über zwei Wegnersche Sätze, Izv. Akad. Nauk SSSR Ser. Mat. **5**, 395—398 (1941).

LUBKIN S. [1] On a conjecture of André Weil, Amer. J. Math. **89**, 443—548 (1967).

[2] A p-adic proof of Weil's conjectures, Ann of Math. (2) **87**, 105—194, 195—255 (1968).
[3] A result on the Weil zeta function, Trans. Amer. Math. Soc. **139**, 297—300 (1969).
[4] Finite generations of lifted p-adic homology with compact supports. Generalization of the Weil conjectures to singular, noncomplete algebraic varieties, Algebraic Geometry (Copenhagen, 1978), pp. 317—373, Lecture Notes in Math., vol. 732, Springer-Verlag, Berlin—Heidelberg—New York, 1979.
[5] Finite generation of lifted p-adic homology with compact supports. Generalization of the Weil conjectures to singular, noncomplete algebraic varieties, J. Number Theory **11**, 412—464 (1979).
LUCAS E. [1] Théorie des fonctions numériques simplement périodiques, Amer. J. Math. **1**, 184—240, 289—321 (1878).
[2] Théorie des nombres, Gauthier-Villars, Paris, 1891.
LUCKY R. W., SALZ J., WELDON E. J., Jr. [1] Principles of Data Communication, McGraw-Hill, New York, 1968.
LUH J. [1] On the representation of vector spaces as a finite union of subspaces, Acta Math. Acad. Sci. Hungar. **23**, 341—342 (1972).
LÜNEBURG H. [1] Transitive Erweiterungen endlicher Permutationsgruppen, Lecture Notes in Math., vol. 84, Springer-Verlag, Berlin—Heidelberg—New York, 1969.
[2] Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen, Bibliographisches Institut, Mannheim, 1979.
LÜNEBURG H., PLAUMANN P. [1] Die Funktionalgleichung von Golab und Schinzel in Galoisfeldern, Arch. Math. **28**, 55—59 (1977).
LUNNON W. F., PLEASANTS P. A. B., STEPHENS N. M. [1] Arithmetic properties of Bell numbers to a composite modulus, Acta Arith. **35**, 1—16 (1979).
MACCLUER C. R. [1] On a conjecture of Davenport and Lewis concerning exceptional polynomials, Acta Arith. **12**, 289—299 (1967).
MACDOUGALL J. A. [1] Bivectors over a finite field, Canad. Math. Bull. **24**, 489—490 (1981).
MACNEISH H. F. [1] Euler squares, Ann. of Math. (2) **23**, 221—227 (1922).
MACWILLIAMS F. J. [1] A theorem on the distribution of weights in a systematic code, Bell System Tech. J. **42**, 79—94 (1963).
[2] The structure and properties of binary cyclic alphabets, Bell System Tech. J. **44**, 303—332 (1965). [Имеется перевод: МАК-ВИЛЬЯМС ДЖ. Структура и свойства бинарных циклических алфавитов. — В кн.: Киберн. сборник, нов. сер., вып. 4. — М.: Мир, 1967, с. 7—42.]
[3] Orthogonal matrices over finite fields, Amer. Math. Monthly **76**, 152—164 (1969).
[4] Orthogonal circulant matrices over finite fields, and how to find them, J. Combinatorial Theory **10**, 1—17 (1971).
MACWILLIAMS F. J., MANN H. B. [1] On the p-rank of the design matrix of a difference set, Information and Control **12**, 474—488 (1968).
MACWILLIAMS F. J., ODLYZKO A. M. [1] Pelikán's conjecture and cyclotomic cosets, J. Combinatorial Theory Ser. A **22**, 110—114 (1977).
MACWILLIAMS F. J., SEERY J. [1] The wight distributions of some minimal cyclic codes, IEEE Trans. Information Theory **IT-27**, 796—806 (1981).
MACWILLIAMS F. J., SLOANE N. J. A. [1] Pseudo-random sequences and arrays, Proc. IEEE **64**, 1715—1729 (1976).
[2] The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977. [Имеется перевод: МАК-ВИЛЬЯМС Ф. ДЖ., СЛОЭН Н. ДЖ. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.]
MACWILLIAMS F. J., SLOANE N. J. A., GOETHALS J.-M. [1] The MacWilliams identities for nonlinear codes, Bell System Tech. J. **51**, 803—819 (1972).

MADDEN D. J. [1] Polynomials and primitive roots in finite fields, J. Number Theory **13**, 499—514 (1981).

MAILLET E. [1] Des conditions pour que l'échelle d'une suite récurrente soit irréductible, Nouv. Ann. Math. (3) **14**, 152—157, 197—206 (1895).

MAMANGAKIS S. E. [1] Remarks on the Fibonacci series modulo *m*, Amer. Math. Monthly **68**, 648—649 (1961).

MANDELBAUM D. [1] On decoding of Reed—Solomon codes, IEEE Trans. Information Theory **IT-17**, 707—712 (1971).

[2] Some results in decoding of certain maximal-distance and BCH codes, Information and Control **20**, 232—243 (1972).

[3] A method for decoding of generalized Goppa codes, IEEE Trans. Information Theory **IT-23**, 137—140 (1977); Addition, ibid, **IT-24**, 268 (1978).

MANN H. B. [1] The construction of orthogonal Latin squares, Ann. Math. Statist. **13**, 418—423 (1942).

[2] Analysis and Design of Experiments, Dover, New York, 1949.

[3] Addition Theorems, Wiley-Interscience, New York, 1965.

[4] Recent advances in difference sets, Amer. Math. Monthly **74**, 229—235 (1967).

[5] Error Correcting Codes, Proc. Symp. Math. Research Center (Univ. of Wisconsin, Madison, Wis., 1968), Wiley, New York, 1968.

[6] The solution of equations by radicals, J. Algebra **29**, 551—554 (1974).

MANTEL W. [1] Residues of recurring series (Dutch), Nieuw Arch. Wisk. (2) **1**, 172—184 (1894).

[2] Problem 91 (Dutch), Wiskundige Opgaven **12**, 213—214 (1918).

MARITSAS D. G. [1] On the statistical properties of a class of linear product feedback shift-register sequences, IEEE Trans. Computers **C-22**, 961—962 (1973).

MAROULAS J., BARNETT S. [1] Greatest common divisor of generalized polynomials and polynomial matrices, Linear Algebra Appl. **22**, 195—210 (1978).

MARSH R. W. [1] Table of Irreducible Polynomials over *GF* (2) through Degree 19, Office of Techn. Serv., U. S. Dept. of Commerce, Washington, D. C., 1957.

MARSH R. W., GLEASON A. M. [1] Problem 4709, Amer. Math. Monthly **63**, 669 (1956); Solution, ibid. **64**, 747—748 (1957).

MARSH R. W., MILLS W. H., WARD R. L., RUMSEY H., WELCH L. R. [1] Round trinomials, Pacific J. Math. **96**, 175—192 (1981).

MARSHALL J. B. [1] On the extension of Fermat's theorem to matrices of order *n*, Proc. Edinburgh Math. Soc. (2) **6**, 85—91 (1939).

MARTIN M. H. [1] A problem in arrangements, Bull. Amer. Math. Soc. **40**, 859—864 (1934).

MARTINET J. [1] Character theory and Artin *L*-functions, Algebraic Number Fields (A. Fröhlich, ed.), pp. 1—87, Academic Press, London, 1977.

MASSEY J. L. [1] Reversible codes, Information and Control **7**, 369—380 (1964).

[2] Step-by-step decoding of the Bose—Chaudhuri—Hocquenghem codes, IEEE Trans. Information Theory **IT-11**, 580—585 (1965).

[3] Some algebraic and distance properties of convolutional codes, Error Correcting Codes (H. B. Mann, ed.), pp. 89—109, Wiley, New York, 1968.

[4] Shift-register synthesis and BCH decoding, IEEE Trans. Information Theory **IT-15**, 122—127 (1969).

MATEOS MATEOS F. [1] Classification of congruent symmetric matrices defined over a finite field (Spanish), Gac. Mat. Madrid **30**, 74—85 (1978).

MATHER M. [1] The number of non-homogeneous lattice points in plane subsets, Math. Proc. Cambridge Philos. Soc. **83**, 25—29 (1978).

MATHIEU E. [1] Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables, J. Math. Pures Appl. (2) **6**, 241—323 (1861).

MATLUK M. M., GILL A. [1] Decomposition of linear sequential circuits over residue class rings, J. Franklin Inst. **294**, 167—180 (1972).

MATTHEWS C. R. [1] Gauss sums and elliptic functions. I. The Kummer sum, Invent. Math. **52**, 163—185 (1979).

[2] Gauss sums and elliptic functions. II. The quartic sum, Invent. Math. **54**, 23—52 (1979).

MATTHEWS K. R. [1] Waring's theorem for polynomials over a finite field, Dissertation, Univ. of Queensland, 1966.

MATTHEWS R. [1] Some generalisations of Chebyshev polynomials and their induced group structure over a finite field, Acta Arith. **41**, 323—335 (1982).

[2] The structure of the group of permutations induced by Chebyshev polynomial vectors over the ring of integers mod m, J. Austral. Math. Soc. Ser. A **32**, 88—103 (1982).

[3] Orthogonal systems of polynomials over a finite field with coefficients in a subfield, Papers in Algebra, Analysis and Statistics (R. Lidl, ed.), Contemporary Math., vol. 9, pp. 295—302, American Math. Society, Providence, R. I., 1982.

MATTSON H. F., Jr., SOLOMON G. [1] A new treatment of Bose—Chaudhuri codes, J. Soc. Indust. Appl. Math. **9**, 654—669 (1961). [Имеется перевод: МЭТТСОН Х., СОЛОМОН Г. Новая трактовка кодов Боуза—Чоудхури. — В кн.: Теория кодирования, М.: 1964, с. 7—29.]

MATTUCK A., TATE J. [1] On the inequality of Castelnuovo—Severi, Abh. Math. Sem. Univ. Hamburg **22**, 295—299 (1958).

MAXFIELD M. W. [1] The order of a matrix under multiplication (modulo m), Duke Math. J. **18**, 619—621 (1951).

MAXSON C. J. [1] A new characterization of finite prime fields, Canad. Math. Bull. **11**, 381—382 (1968).

MAZUR B. [1] Eigenvalues of Frobenius acting on algebraic varieties over finite fields, Proc. Symp. Pure Math., vol. 29, pp. 231—261, American Math. Society, Providence, R. I., 1975.

MCCANN K., WILLIAMS K. S. [1] On the residues of a cubic polynomial (mod p), Canad. Math. Bull. **10**, 29—38 (1967).

[2] The distribution of the residues of a quartic polynomial, Glasgow Math. J. **8**, 67—88 (1967).

[3] Cubic polynomials with the same residues (mod p), Proc. Cambridge Philos. Soc. **64**, 655—658 (1968).

MCCLELLAN J. H., PARKS T. W. [1] Eigenvalue and eigenvector decomposition of the discrete Fourier transform, IEEE Trans. Audio Electroacoust. **AU-20**, 66—74 (1972).

MCCLELLAN J. H., RADER C. M. [1] Number Theory in Digital Signal Processing, Prentice-Hall, Englewood Cliffs, N. J., 1979.

MCCLUSKEY E. J. [1] Introduction to the Theory of Switching Circuits, McGraw-Hill, New York, 1965.

MCCONNEL R. [1] Pseudo-ordered polynomials over a finite field, Acta Arith. **8**, 127—151 (1963).

[2] Function over finite fields preserving m-th powers, Duke Math. J. **36**, 465—472 (1969).

[3] Functions over finite fields satisfying coordinate ψ-conditions, Duke Math. J. **39**, 297—312 (1972).

MCCRIMMON K. [1] A note on finite division rings, Proc. Amer. Math. Soc. **23**, 598—600 (1969).

MCDONALD B. R. [1] Finite Rings with Identity, Dekker, New York, 1974.

MCELIECE R. J. [1] A generalization of difference sets, Canad. J. Math. **19**, 206—211 (1967).

[2] Factorization of polynomials over finite fields, Math. Comp. **23**, 861—867 (1969).

[3] Table of polynomials of period e over $GF(p)$, Math. Comp. **23**, microfiche suppl. C1—C6 (1969).

[4] On periodic sequences from $GF(q)$, J. Combinatorial Theory Ser.. A **10**, 80—91 (1971).
[5] Irreducible cyclic codes and Gauss sums, Combinatorics (M. Hall, Jr., and. J. H. van Lint, eds.), pp. 185—202, Reidel, Dordrecht—Boston, 1975.
[6] The Theory of Information and Coding, Encyclopedia of Math. and Its Appl., vol. 3, Addison-Wesley, Reading, Mass., 1977.
[7] Correlation properties of sets of sequences derived from irreducible cyclic codes, Information and Control **45**, 18—25 (1980).
MCELIECE R. J., RUMSEY H. [1] Euler products, cyclotomy, and coding, J. Number Theory **4**, 302—311 (1972).
MCELIECE R. J., SHEARER J. B. [1] A property of Euclid's algorithm and an application to Padé approximation, SIAM J. Appl. Math. **34**, 611—615 (1978).
MCGETTRICK A. D. [1] A result in the theory of Weierstrass elliptic functions, Proc. London Math. Soc. (3) **25**, 41—54 (1972).
[2] On the biquadratic Gauss sum, Proc. Cambridge Philos. Soc. **71**, 79—83 (1972).
MCLAIN K. E., EDGAR H. M. [1] A note on Golomb's «Cyclotomic polynomials and factorization theorems», Amer. Math. Monthly **88**, 753 (1981).
MEIJER H. G., DIJKSMA A. [1] On uniform distribution of sequences in $GF\{q, x\}$ and $GF\{q, x\}$, Duke Math. J. **37**, 507—514 (1970).
MENDELSOHN N. S. [1] Congruence relationship for integral recurrences, Canad. Math. Bull. **5**, 281—284 (1962).
[2] Algebraic construction of combinatorial designs, Congr. Numer. **13**, 157—168 (1975).
MENON P. K. [1] On Gauss's sum, J. Indian Math. Soc. **16**, 31—36 (1952).
[2] On certain sums connected with Galois fields and their applications to difference sets, Math. Ann. **154**, 341—364 (1964).
METROPOLIS N., NICOLETTI G., ROTA G.-C. [1] A new class of symmetric functions, Mathematical Analysis and Applications (L. Nachbin, ed.), Advances in Math. Suppl. Studies, vol. 7B, pp. 563—575, Academic Press, New York, 1981.
METSÄNKYLÄ R. [1] On kth power coset representatives mod p, Ann. Acad. Sci. Fenn. Ser. A I **557** (1973).
MEYER K. [1] Äquivalenz von quadratischen Formen über endlichen Körpern, Abh. Math. Sem. Univ. Hamburg **37**, 79—85 (1972).
MICHELSON A. M. [1] Computer implementation of decoders for several BCH codes, Proc. Symp. on Computer Processing in Communications (Polytechnic Inst. of Brooklyn, New York, 1969), pp. 401—413, Polytechnic Press, Brooklyn, N. Y., 1969.
MIGNOSI G. [1] Risoluzione apiristica della equazione generale cubica in un corpo numerico finito, Rend. Circ. Mat. Palermo **53**, 411—427 (1929).
[2] Sulla risoluzione apiristica delle equazioni algebriche in un corpo numerico finito, Rend. Accad. Sci. Fis. Mat. Napoli (3) **35**, 218—233 (1930).
[3] Eliminazione nei sistemi di equazioni algebriche in un corpo finito, Scritti matematici offerti a Luigi Berzolari, pp. 249—260, Istituto matematico della Università, Pavia, 1936.
[4] Risoluzione apiristica dei sitemi di equazioni algebriche nei corpi finiti, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **2**, 250—257 (1947).
[5] Estensione ai corpi finiti di una formula di Rados, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **7**, 216—219 (1949).
[6] Ancora sopra una estensione ai corpi finiti di una formula di Rados, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **7**, 284—289 (1949).
[7] Sulla enumerazione delle radici della più generale equazione algebrica in un corpo finito, Convegno Reticoli e Geometrie Proiettive (Palermo—Messina, 1957), pp. 99—108. Edizioni Cremonese, Rome, 1958.

MIGNOTTE M. [1] Suites récurrentes linéaires, Sém. Delange—Pisot—Poitou 1973/74, Théorie des Nombres, Exp. G14, Secrétariat Math., Paris, 1975.
[2] Un algorithme sur la décomposition des polynômes dans un corps fini, C. R. Acad. Sci. Paris Sér. A **280**, 137—139 (1975).
[3] Factorization des polynômes sur un corps fini, Astérisque, no. 38—39, pp. 149—157, Soc. Math. France, Paris, 1976.
[4] Algorithmes relatifs à la décomposition des polynômes, Theoret. Comput. Sci. **1**, 227—235 (1976).
[5] Calcul des racines d-ièmes dans un corps fini, C. R. Acad. Sci. Paris Sér. A **290**, 205—206 (1980).
MILLER J. C. P. [1] On factorisation, with a suggested new approach, Math. Comp. **29**, 155—172 (1975).
MILLER J. C. P., BROWN D. J. S. [1] An algorithm for evaluation of remote terms in a linear recurrence sequence, Comput. J. **9**, 188—190 (1966).
MILLER R. L. [1] Necklaces, symmetries and self-reciprocal polynomials, Discrete Math. **22**, 25—33 (1978).
MILLER R. L., REED I. S., TRUONG T. K. [1] A theorem for computing primitive elements in the field of complex integers of a characteristic Mersenne prime, IEEE Trans. Acoust. Speech Signal Process. **29**, 119—120 (1981).
MILLS W. H. [1] Polynomials with minimal value sets, Pacific J. Math. **14**, 225—241 (1964).
[2] Bounded consecutive residues and related problems, Proc. Symp. Pure Math., vol. 8, pp. 170—174, American Math. Society, Providence, R. I., 1965.
[3] The degree of factors of certain polynomials over finite fields, Proc. Amer. Math. Soc. **25**, 860—863 (1970).
[4] Continued fractions and linear recurrences, Math. Comp. **29**, 173—180 (1975).
MILLS W. H., ZIERLER N. [1] On a conjecture of Golomb, Pacific J. Math. **28**, 635—640 (1969).
MILNE J. S. [1] Étale Cohomology, Princeton Univ. Press, Princeton, N. J., 1980. [Имеется перевод: МИЛН ДЖ. Этальные когомологии. — М.: Мир, 1983.]
[2] Some estimates from étale cohomology, J. reine angew. Math. **328**, 208—220 (1981).
MILNE-THOMSON L. M. [1] The Calculus of Finite Differences, Macmillan, London, 1933.
MIN S. H. [1] On a system of congruences, J. London Math. Soc. **22**, 47—53 (1947).
[2] On systems of algebraic equations and certain multiple exponential sums, Quart. J. Math. **18**, 133—142 (1947).
MIRIMANOFF D. [1] Sur les congruences du troisième degré, L'Enseignement Math. **9**, 381—384 (1907).
MIRIMANOFF D., HENSEL K. [1] Sur la relation $\left(\frac{D}{p}\right) = (-1)^{n-h}$ et la loi de réciprocité, J. reine angew. Math. **129**, 86—87 (1905).
MITCHELL H. H. [1] On the generalized Jacobi—Kummer cyclotomic function, Trans. Amer. Math. Soc. **17**, 165—177 (1916).
[2] On the congruence $cx^\lambda + 1 \equiv dy^\lambda$ in a Galois field, Ann. of Math. (2) **18**, 120—131 (1917).
MITCHELL O. H. [1] Some theorems in numbers, Amer. J. Math. **4**, 25—38 (1881).
MOENCK R. T. [1] On the efficiency of algorithms for polynomial factoring, Math. Comp. **31**, 235—250 (1977).
MOHANTY N. C. [1] Binary and ternary signals with small cross correlations, Inform. Sci. **13**, 35—50 (1977).
MÖHRMANN K. H. [1] Erzeugung von binären Quasi-Zufallsfolgen hoher Taktfrequenz durch Multiplexen, Siemens Research and Development Re-

ports 3, no. 4, 218—224 (1974).
[2] Realisierung von Scramblern für PCM-Signale hoher Taktfrequenz, Siemens Research and Development Reports **6**, no. 1, 1—5 (1977).
MOISIL G. C. [1] L'emploi des imaginaires de Galois dans la théorie des mécanismes automatiques. I—V, VII—IX (Romanian. French summary), Com. Acad. R. P. Romîne **4**, 581—585, 587—589 (1954); ibid. **5**, 959—963 (1955); ibid. **6**, 505—508, 509—513, 621—623, 625—626, 1055—1058 (1956).
[2] Synthèse des schémas à relais idéaux, à l'aide des corps d'imaginaires de Galois (Romanian. French summary), Acad. R. P. Romîne. Bul. Sti. Sect. Sti, Mat. Fiz. **8**, 429—453 (1956).
[3] Sur la théorie algébrique de certains circuits électriques, J. Math. Pures Appl. (9) **36**, 313—324 (1957).
[4] The Algebraic Theory of Switching Circuits, Pergamon Press, Oxford, 1969.
MOISIL G. C., POPOVICI C. P. [1] Analyse et synthèse des schémas à commande directe, à l'aide des imaginaires de Galois (Romanian. French summary), Acad. R. P. Romîne. Bul. Sti. Sect. Sti: Mat. Fiz. **8**, 455—467 (1956).
MÖNNIG P. [1] Ein Beitrag zur Darstellung endlicher Körper, Math.-Phys. Semesterber. **17**, 46—56 (1970).
MONSKY P. [1] p-adic Analysis and Zeta Functions, Lectures in Math., Dept. of Math., Kyoto Univ., 1970.
MONTEL P. [1] Leçons sur les récurrences et leurs applications, Gauthier-Villars, Paris, 1957.
MONTGOMERY H. L. [1] Topics in Multiplicative Number Theory, Lecture Notes in Math., vol. 227, Springer-Verlag, Berlin—Heidelberg—New York, 1971. [Имеется перевод: МОНТГОМЕРИ Г. Мультипликативная теория чисел. — М.: Мир, 1974.]
[2] Distribution questions concerning a character sum, Topics in Number Theory (Debrecen, 1974), Colloq. Math. Soc. János Bolyai, vol. 13, pp. 195—203, North-Holland, Amsterdam, 1976.
MONTGOMERY H. L., VAUGHAN R. C. [1] Exponential sums with multiplicative coefficients, Invent. Math., **43**, 69—82 (1977).
MOORE E. H. [1] A doubly-infinite system of simple groups, Bull. New York Math. Soc. **3**, 73—78 (1893).
[2] A doubly-infinite system of simple groups, Math. Papers read at the Congress of Mathematics (Chicago, 1893), pp. 208—242, Chicago, 1896.
[3] A two-fold generalization of Fermat's theorem, Bull. Amer. Math. Soc. **2**, 189—199 (1896).
[4] The Subgroups of the Generalized Finite Modular Group, Decennial Publications, Chicago, 1903.
MORDELL L. J. [1] On a simple summation of the series $\sum_{s=0}^{n-1} e^{2s^2\pi i/n}$, Messenger of Math. **48**, 54—56 (1918).
[2] Three Lectures on Fermat's Last Theorem, Cambridge Univ. Press, Cambridge, 1921.
[3] On the reciprocity formula for the Gauss's sums in the quadratic field, Proc. London Math. Soc. (2) **20**, 289—296 (1922).
[4] On a sum analogous to a Gauss's sum, Quart. J. Math. **3**, 161—167 (1932).
[5] The number of solutions of some congruences in two variables, Math. Z. **37**, 193—209 (1933).
[6] Thoughts on number theory, J. London Math. Soc. **21**, 58—74 (1946).
[7] Note on the linear summetric congruence in n variables, Canad. J. Math. **5**, 433—438 (1953).
[8] Note on simultaneous quadratic congruences, Math. Scand. **5**, 21—26 (1957).
[9] On the number of solutions in incomplete residue sets of quadratic congruences, Arch. Math. **8**, 153—157 (1957).

[10] On Lehmer's congruence associated with cubes of Kloosterman's sums, J. London Math. Soc. **36**, 335—339 (1961).
[11] On a cubic congruence in three variables, Acta Arith. **8**, 1—9 (1962).
[12] The sign of the Gaussian sum, Illinois J. Math. **6**, 177—180 (1962).
[13] On a cyclotomic resolvent, Arch. Math. **13**, 486—487 (1962).
[14] On a special polynomial congruence and exponential sums, Calcutta Math. Soc. Golden Jubilee Commemoration Volume, Part I, pp. 29—32, Calcutta Math. Soc., Calcutta, 1963.
[15] On a cubic exponential sum in three variables, Amer. J. Math. **85**, 49—52 (1963).
[16] A congruence problem of E. G. Straus, J. London Math. Soc. **38**, 108—110 (1963).
[17] On a cubic congruence in three variables (III), J. London Math. Soc. **38**, 351—355 (1963).
[18] On a cubic exponential sum in two variables, J. London Math. Soc. **38**, 356—358 (1963).
[19] On the least residue and non-residue of a polynomial, J. London Math. Soc. **38**, 451—453 (1963).
[20] On a cubic congruence in three variables. II, Proc. Amer. Math. Soc. **14**, 609—614 (1963).
[21] On the congruence $ax^3 + by^3 + cz^3 + dxyz \equiv n \pmod{p}$, Duke Math. J. **31**, 123—126 (1964).
[22] Incomplete exponential sums and incomplete residue systems for congruences, Czechoslovak Math. J. **14**, 235—242 (1964).
[23] Diophantine Equations, Academic Press, London, 1969.
[24] Some exponential sums in several variables, Monatsh. Math. **73**, 348—353 (1969).
[25] Cubic polynomials with the same residues mod p, Proc. London Math. Soc. (3) **21**, 129—144 (1970).
[26] On some exponential sums related to Kloosterman sums, Acta Arith. **21**, 65—69 (1972).
[27] A finite evaluation of a special exponential sum, Proc. Cambridge Philos. Soc. **71**, 75—78 (1972).
[28] On rational functions representing all residues mod p, J. London Math. Soc. (2) **5**, 166—168 (1972).
[29] Rational functions representing all residues mod p. II, Proc. Amer. Math. Soc. **35**, 411—412 (1972).
[30] On Salié's sum, Glasgow Math. J. **14**, 25—26 (1973).
[31] Some exponential sums, Труды международной конференции по теории чисел (Москва, 1971), Труды Матем. инст. им. Стеклова, **132**, 30—34 (1973).
MORENO C. J. [1] Sur le problème de Kummer, L'Enseignement Math. (2) **20**, 45—51 (1974).
MORENO O. [1] Counting traces of powers over $GF(2^m)$, Cong. Numer. **29**, 673—679 (1980).
[2] On primitive elements of trace equal to 1 in $GF(2^m)$, Discrete Math. **41**, 53—56 (1982).
MORLAYE B. [1] Equations diagonales non homogènes sur un corps fini, C. R. Acad. Sci. Paris Sér. A **272**, 1545—1548 (1971).
[2] Démonstration élémentaire d'un théorème de Davenport et Hasse, L'Enseignement Math. (2) **18**, 269—276 (1972).
MORTIMER B. C., WILLIAMS K. S. [1] Note on a paper of S. Uchiyama, Canad. Math. Bull. **17**, 289—293 (1974).
MORTON P. [1] On the eigenvectors of Schur's matrix, J. Number Theory **12**, 122—127 (1980).
MOSES J. [1] Algebraic structures and their algorithms, Algorithms and Complexity (J. F. Traub, ed.), pp. 301—319, Academic Press, New York, 1976.

MOSSIGE S. [1] Table of irreducible polynomials over $GF(2)$ of degrees 10 through 20, Math. Comp. **26**, 1007—1009 (1972).

MOUSOURIS N., PORTER A. D. [1] The symmetric matrix equation $X_n' \dots X_1' A X_1 \dots X_n = B$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **62**, 126—130 (1977).

[2] The Hermitian matrix equation $U_n^* \dots U_1^* A U_1 \dots U_n = B$, Rend. Mat. (6) **11**, 387—392 (1978).

MULLEN G. L. [1] Equivalence classes of functions over a finite field, Acta Arith. **29**, 353—358 (1976).

[2] Permutation polynomials in several variables over finite fields, Acta Arith. **31**, 107—111 (1976).

[3] Equivalence classes of polynomials over finite fields, Acta Arith. **31**, 113—123 (1976).

[4] Equivalence classes of matrices over finite fields, Linear Algebra Appl. **27**, 61—68 (1979).

[5] Weak equivalence of functions over a finite field, Acta Arith. **35**, 259—272 (1979).

[6] Equivalence classes of matrices over a finite field, Internat. J. Math. and Math. Sci. **2**, 487—491 (1979).

[7] Local permutation polynomials over Z_p, Fibonacci Quart. **18**, 104—108 (1980).

[8] Local permutation polynomials in three variables over Z_p, Fibonacci Quart. **18**, 208—214 (1980).

[9] Equivalence classes of sets of functions over a finite field, Acta Arith. **36**, 323—329 (1980).

[10] Local permutation polynomials over a finite field, Norske Vid. Selsk. Skrifter **1981**, no. 1, 1—4.

[11] Permutation matrices and matrix equivalence over a finite field, Internat. J. Math. and Math. Sci. **4**, 503—512 (1981).

[12] Matrix equivalence over finite fields, Acta Arith. **41**, 133—139 (1982).

[13] Polynomials over finite fields which commute with linear permutations, Proc. Amer. Math. Soc. **84**, 315—317 (1982).

MULLER D. E. [1] Application of Boolean algebra to switching circuit design and error detection, IRE Trans. Electron. Comp. **EC-3**, 6—12 (1954).

MÜLLER W. B. [1] Über eine Klasse von durch Dickson-Polynome dargestellten Gruppen, Rings, Modules and Radicals (Keszthely, 1971), Colloq. Math. Soc. János Bolyai, vol. 6, pp. 361—376, North-Holland, Amsterdam, 1973.

MURAKAMI H., REED I. S. [1] Recursive realization of finite filters using finite field arithmetic, IEEE Trans. Information Theory **IT-23**, 232—242 (1977).

MUSKAT J. B. [1] On certain prime power congruences, Abh. Math. Sem. Univ. Hamburg **26**, 102—110 (1963).

[2] On the solvability of $x^e \equiv e \pmod{p}$, Pacific J. Math. **14**, 257—260 (1964).

[3] Criteria for solvability of certain congruences, Canad. J. Math. **16**, 343—352 (1964).

[4] The cyclotomic numbers of order fourteen, Acta Arith. **11**, 263—279 (1966).

[5] Reciprocity and Jacobi sums, Pacific J. Math. **20**, 275—280 (1967).

[6] On Jacobi sums of certain composite orders, Trans. Amer. Math. Soc. **134**, 483—502 (1968).

[7] Use of computers in cyclotomy, Computers in Number Theory (A. O. L. Atkin and B. J. Birch, eds.), pp. 141—147, Academic Press, London, 1971.

MUSKAT J. B., STREET A. P. [1] Sum-free cyclotomic classes in finite fields, Proc. Third Manitoba Conf. Numerical Math. (Winnipeg, Man., 1973), pp. 399—406, Utilitas Math., Winnipeg, Man., 1974.

MUSKAT J. B., WHITEMAN A. L. [1] The cyclotomic numbers of order twenty, Acta Arith. **17**, 185—216 (1970).
MUSKAT J. B., ZEE Y.-C. [1] Sign ambiguities of Jacobi sums, Duke Math. J. **40**, 313—334 (1973).
MUSSER D. R. [1] Multivariate polynomial factorization, J. Assoc. Comput. Mach. **22**, 291—308 (1975).
MYERSON G. [1] On the number of zeros of diagonal cubic forms, J. Number Theory **11**, 95—99 (1979).
[2] A combinatorial problem in finite fields. I, Pacific J. Math. **82**, 179—187 (1979).
[3] A combinatorial problem in finite fields. II, Quart. J. Math. (2) **31**, 219—231 (1980).
[4] The distribution of rational points on varieties defined over a finite field, Mathematika **28**, 153—159 (1981).
[5] Period polynomials and Gauss sums for finite fields, Acta Arith. **39**, 251—264 (1981).
MYKKELTVEIT J. [1] Nonlinear recurrences and arithmetic codes, Information and Control **33**, 193—209 (1977).
NADLER M., SENGUPTA A. [1] Shift-register code for indexing applications, Comm. Assoc. Comput. Mach. **2**, no. 10, 40—43 (1959).
NAGAHARA T., TOMINAGA H. [1] Elementary proofs of a theorem of Wedderburn and a theorem of Jacobson, Abh. Math. Sem. Univ. Hamburg **41**, 72—74 (1974).
NAGATA M. [1] On the number of solutions of $x_1^l + x_2^2 + \ldots + x_n^2 = a$ in a finite field (Japanese), Sûgaku **14**, 98—99 (1969/63).
[2] Field Theory, Dekker, New York, 1977.
NAGELL T. [1] On the solvability of some congruences, Norske Vid. Selsk. Forh. (Trondheim) **27**, 1—5 (1954).
NARKIEWICZ W. [1] Elementary and Analytic Theory of Algebraic Numbers, Monografie Mat., vol. 57, PWN, Warsaw, 1974.
[2] Uniform distribution of sequences of integers, Journées Arithmétiques 1980 (J. V. Armitage, ed.), London Math. Soc. Lecture Note Series, no. 56, pp. 202—210, Cambridge Univ. Press, Cambridge, 1982.
NASHIER B. S., RAJWADE A. R. [1] Determination of a unique solution of the quadratic partition for primes $p \equiv 1 \pmod 7$, Pacific J. Math. **72**, 513—521 (1977).
NATHANSON M. B. [1] Derivatives of binary sequences, SIAM J. Appl. Math. **21**, 407—412 (1971).
[2] Integrals of binary sequences, SIAM J. Appl. Math. **23**, 84—86 (1972)
[3] Shift dynamical systems over finite fields, Proc. Amer. Math. Soc. **34**, 591—594 (1972).
[4] Linear recurrences and uniform distribution, Proc. Amer. Math. Soc. **48**, 289—291 (1975).
[5] Difference operators and periodic sequences over finite modules, Acta Math Acad. Sci. Hungar. **28**, 219—224 (1976).
NEIKIRK L. I. [1] A geometric representation of the Galois field, Bull. Amer. Math. Soc. **14**, 323—325 (1908).
NEUMANN H. [1] On some finite non-desarguesian planes, Arch. Math. **6**, 36—40 (1954).
NEUMANN O. [1] Über die Kongruenz $ax^4 + 1 \equiv cz^2 \pmod p$, Monatsber Deutsch. Akad. Wiss. Berlin **11**, 699—703 (1969).
NEWMAN M. [1] Integral Matrices, Academic Press, New York, 1972.
NICHOLSON P. J. [1] Algebraic theory of finite Fourier transforms, J. Computer and Syst. Sci. **5**, 524—547 (1971).
NIEDERREITER H. [1] Permutation polynomials in several variables over finite fields, Proc. Japan Acad. **46**, 1001—1005 (1970).

[2] Orthogonal systems of polynomials in finite fields, Proc. Amer. Math. Soc. **28**, 415—422 (1971).
[3] Permutation polynomials in several variables, Acta Sci. Math. Szeged **33**, 53—58 (1972).
[4] Distribution of Fibonacci numbers mod 5^k, Fibonacci Quart. **10**, 373—374 (1972).
[5] Some new exponential sums with applications to pseudo-random numbers, Topics in Number Theory (Debrecen, 1974), Colloquia Math. Soc. János Bolyai, vol. 13, pp. 209—232, North-Holland, Amsterdam, 1976.
[6] On the cycle structure of linear recurring sequences, Math. Scand. **38**, 53—77 (1976).
[7] On the distribution of pseudo-random numbers generated by the linear congruential method. III, Math. Comp. **30**, 571—597 (1976).
[8] Weights of cyclic codes, Information and Control **34**, 130—140 (1977).
[9] Statistical tests for linear congruential pseudo-random numbers, COMPSTAT 1978: Proceedings in Computational Statistics (Leiden, 1978), pp. 398—404, Physica-Verlag, Vienna, 1978.
[10] Quasi-Monte Carlo methods and pseudo-random numbers, Bull. Amer. Math. Soc. **84**, 957—1041 (1978).
[11] Verteilung von Resten rekursiver Folgen, Arch. Math. **34**, 526—533 (1980).
[12] Statistical independence properties of Tausworthe pseudo-random numbers, Proc. Third Caribbean Conf. on Combinatorics and Computing (Cave Hill, Barbados, 1981), pp. 163—168, Univ. of the West Indies, Cave Hill, Barbados, 1981.
[13] Statistical tests for Tausworthe pseudo-random numbers, Probability and Statistical Inference (W. Grossmann, G. C. Pflug, and W. Wertz, eds.), pp. 265—274, Reidel, Dordrecht, 1982.
[14] Richard Dedekind and the development of the theory of finite fields, Abh. Braunschweig, Wissenschaftl. Gesellschaft **33**, 183—187 (1982).
NIEDERREITER H., LO S. K. [1] Permutation polynomials over rings of algebraic integers, Abh. Math. Sem. Univ. Hamburg **49**, 126—139 (1979).
NIEDERREITER H., ROBINSON K. H. [1] Bol loops of order pq, Math. Proc. Cambridge Philos. Soc. **89**, 241—256 (1981).
[2] Complete mappings of finite fields, J. Austral. Math. Soc. Ser. A **33**, 197—212 (1982).
NIEDERREITER H., SHIUE J.-S. [1] Equidistribution of linear recurring sequences in finite fields, Indag. Math. **80**, 397—405 (1977).
[2] Equidistribution of linear recurring sequences in finite fields. II, Acta Arith. **38**, 197—207 (1980).
NIVEN I. [1] Fermat's theorem for matrices, Duke Math. J. **15**, 823—826 (1948).
[2] Uniform distribution of sequences of integers, Trans. Amer. Math. Soc. **98**, 52—61 (1961).
NIVEN I., WARREN L. J. [1] A generalization of Fermat's theorem, Proc. Amer. Math. Soc. **8**, 306—313 (1957).
NÖBAUER W. [1] Über Gruppen von Restklassen nach Restpolynomidealen, Sitzungsber. Österr. Akad. Wiss. Abt. II **162**, 207—233 (1953).
[2] Über eine Gruppe der Zahlentheorie, Monatsh. Math. **58**, 181—192 (1954).
[3] Gruppen von Restklassen nach Restpolynomidealen in mehreren Unbestimmten, Monatsh. Math. **59**, 118—145 (1955).
[4] Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen, Monatsh. Math. **59**, 194—202 (1955).
[5] Bemerkungen über die Darstellung von Abbildungen durch Polynome und rationale Funktionen, Monatsh. Math. **68**, 138—142 (1964).
[6] Zur Theorie der Polynomtransformationen und Permutationspolynome, Math. Ann. **157**, 332—342 (1964).

[7] Über die Vollideale und Permutationspolynome eines Galoisfeldes, Acta Math. Acad. Sci. Hungar. **16**, 37—42 (1965).

[8] Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen, Monatsh. Math. **69**, 230—238 (1965).

[9] Polynome, welche für gegebene Zahlen Permutationspolynome sind, Acta Arith. **11**, 437—442 (1966).

[10] Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen, J. reine angew. Math. **231**, 215—219 (1968).

[11] Darstellungen von Permutationen durch Polynome und rationale Funktionen, Ber. Math. Forschungsinst. Oberwolfach, vol. 5, pp. 89—100, Bibliographisches Institut, Mannheim, 1971.

[12] Über Gruppen von Dickson-Polynomfunktionen und einige damit zusammenhängende zahlentheoretische Fragen, Monatsh. Math. **77**, 330—344 (1973).

NOMURA T., FUKUDA A. [1] Linear recurring planes and two-dimensional cyclic codes, Electron. Commun. Japan **54**, no. 3, 23—30 (1971).

NOMURA T., MIYAKAWA H., IMAI H., FUKUDA A. [1] A method of construction and some properties of planes having maximum area matrix, Electron. Commun. Japan **54**, no. 5, 18—25 (1971).

[2] Some properties of the $\gamma\beta$-plane and its extension to three-dimensional space, Electron, Commun. Japan **54**, no. 8, 27—34 (1971).

[3] A theory of two-dimensional linear recurring arrays, IEEE Trans. Information Theory **IT-18**, 775—785 (1972).

NORDON D. [1] Zéros non singuliers des formes quadratiques, C. R. Acad. Sci. Paris. Sér. A **277**, 295—297 (1973).

[2] Zéros communs non singuliers de deux formes quadratiques, Sém. Théorie des Nombres 1972—1973, Exp. 9, Univ. Bordeaux I, Talence, 1973.

[3] Zéros communs non singuliers de deux formes quadratiques, Acta Arith. **30**, 109—119 (1976).

NÖRLUND N. E. [1] Vorlesungen über Differenzenrechnung, Springer, Berlin, 1924.

NORTON K. K. [1] Upper bounds for kth power coset representatives modulo n, Acta Arith. **15**, 161—179 (1969).

[2] On the distribution of kth power residues and non-residues modulo n, J. Number Theory **1**, 398—418 (1969).

[3] Numbers with small prime factors, and the least kth power non-residue, Memoirs Amer. Math. Soc., no. 106, American Math. Society, Providence, R. I., 1971.

[4] On the distribution of power residues and non-residues, J. reine angew. Math. **254**, 188—203 (1972).

[5] On character sums and power residues, Trans. Amer. Math. Soc. **167**, 203—226 (1972); Erratum, ibid. **174**, 507 (1972).

[6] Bounds for sequences of consecutive power residues. I, Proc. Symp. Pure Math., vol. 24, pp. 213—220, American Math. Society, Providence, R. I., 1973.

NUSSBAUMER H. J. [1] Fast Fourier Transform and Convolution Algorithms, Springer-Verlag, Berlin—Heidelberg—New York, 1981. [Имеется перевод: НУССБАУМЕР Г. Быстрое преобразование Фурье и алгоритмы вычисления свертки. — М.: Радио и связь, 1985.]

NYMANN J. E. [1] Groups and fields in Z_n, Elemente der Math. **30**, 82—84 (1975).

O'CONNOR R. E. [1] Quadratic and linear congruence, Bull. Amer. Math. Soc. **45**, 792—798 (1939).

O'CONNOR R. E., PALL G. [1] The quaternion congruence $\bar{t}at \equiv b \pmod{g}$, Amer. J. Math. **61**, 487—508 (1939).

ODLYZKO A. M., STANLEY R. P. [1] Enumeration of power sums modulo a prime, J. Number Theory **10**, 263—272 (1978).

ODONI R. W. K. [1] The statistics of Weil's trigonometric sums, Proc. Cambridge Philos. Soc. **74**, 467—471 (1973).

OLSON L. D. [1] Hasse invariants and anomalous primes for elliptic curves with complex multiplication, J. Number Theory **8**, 397—414 (1976).

OLTRAMARE G. [1] Considérations générales sur les racines des nombres premiers, J. reine angew. Math. **45**, 303—344 (1853).

ONO T. [1] Gauss transforms and zeta-functions, Ann. of Math. (2) **91**, 332—361 (1970).

[2] A remark on Gaussian sums and algebraic groups, J. Math. Kyoto Univ. **13**, 139—142 (1973).

[3] On certain numerical invariants of mappings over finite fields. I, Proc. Japan Acad. Ser. A **56**, 342—347 (1980).

[4] On certain numerical invariants of mappings over finite fields. II, Proc. Japan Acad. Ser. A **56**, 397—400 (1980).

[5] On certain numerical invariants of mappings over finite fields. III, Proc. Japan Acad. Ser. A **56**, 441—444 (1980).

[6] On certain numerical invariants of mappings over finite fields. IV, Proc. Japan Acad. Ser. A **57**, 66—71 (1981).

[7] On certain numerical invariants of mappings over finite fields. V, Proc. Japan Acad. Ser. A **57**, 121—125 (1981).

[8] On a generalization of Jacobi sums, J. Fac. Sci. Univ. Tokyo Sect. IA **28**, 823—828 (1981).

ORE Ö. [1] Über höhere Kongruenzen, Norsk Mat. Forenings Skrifter Ser. I **1922**, no. 7.

[2] Über die Reduzibilität von algebraischen Gleichungen, Skrifter Norske Vid. Akad. Oslo 1923, no. 1.

[3] Note sur une identité dans la théorie des congruences supérieures, Rend. Circ. Mat. Palermo **48**, 37—40 (1924).

[4] Theory of non-commutative polynomials, Ann. of Math. (2) **34**, 480—508 (1933).

[5] On a special class of polynomials, Trans. Amer. Math. Soc. **35**, 559—584 (1933); Errata, ibid. **36**, 275 (1934).

[6] Contributions to the theory of finite fields, Trans. Amer. Math. Soc. **36** 243—274 (1934).

[7] Some studies on cyclic determinants, Duke Math. J. **18**, 343—354 (1951).

OSBORN R. [1] Tables of Primitive Roots of Odd Primes Less than 1000, Univ. of Texas Press, Austin, Tex., 1961.

PALEY R. E. A. C. [1] A theorem on characters, J. London. Math. Soc. **7**, 28—32 (1932).

[2] Theorems on polynomials in a Galois field, Quart. J. Math. **4**, 52—63 (1933).

[3] On orthogonal matrices, J. Math. Phys. **12**, 311—320 (1933).

PARKER E. T. [1] Orthogonal Latin squares, Proc. Nat. Acad. Sci. U. S. A. **45**, 859—862 (1959).

[2] Construction of some sets of mutually orthogonal Latin squares, Proc. Amer. Math. Soc. **10**, 946—949 (1959).

PARNAMI J. C., AGRAWAL M. K., RAJWADE A. R. [1] On the 4-power stufe of a field, Rend. Circ. Mat. Palermo (2) **30**, 245—254 (1981).

[2] A congruence relation between the coefficients of the Jacobi sum, Indian J. Pure Appl. Math. **12**, 804—806 (1981).

[3] Jacobi sums and cyclotomic numbers for a finite field, Acta Arith. **41**, 1—13 (1982).

PARSON L. A. [1] Generalized Kloosterman sums and the Fourier coefficients of cusp forms, Trans. Amer. Math. Soc. **217**, 329—350 (1976).

PATTERSON N. J. [1] The algebraic decoding of Goppa codes, IEEE Trans. Information Theory **IT-21**, 203—207 (1975).

PATTERSON S. J. [1] A cubic analogue of the theta series. I, II, J. reine angew. Math. **296**, 125—161, 217—220 (1977).
[2] On Dirichlet series associated with cubic Gauss sums, J. reine angew Math. **303/304**, 102—125 (1978).
[3] On the distribution of Kummer sums, J. reine angew. Math. **303/304**, 126—143 (1978).
[4] The distribution of general Gauss sums at prime arguments, Recent Progress in Analytic Number Theory (H. Halberstam and C. Hooley, eds.). vol. 2, pp. 171—182, Academic Press, London, 1981.
PAYNE S. E. [1] Linear transformations of a finite field, Amer. Math. Monthly **78**, 659—660 (1971).
PEARSON E. H., VANDIVER H. S. [1] On a new problem concerning trinomial congruences involving rational integers, Proc. Nat. Acad. Sci. U. S. A **39**, 1278—1285 (1953).
PELE R. L. [1] Some remarks on the vector subspaces of cyclic Galois extensions, Acta Math. Acad, Sci. Hungar. **20**, 237—240 (1969).
PELLEGRINO G. [1] Sui campi di Galois, di ordine dispari, che ammettono terne di elementi quadrati (non quadrati) consecutivi, Boll. Un. Mat. Ital (5) **17B**, 1482—1495 (1980).
[2] Sulle sostituzioni lineari, sui campi finiti di ordine dispari, che conservano oppure scambiano il carattere quadratico degli elementi transformati, Boll. Un. Mat. Ital. (6) **1B**, 211—223 (1982).
PELLET A.-E. [1] Sur les fonctions irréductibles suivant un module premier et une fonction modulaire, C. R. Acad. Sci. Paris. **70**, 328—330 (1870).
[2] Sur la décomposition d'une fonction entièrs en facteurs irréductibles suivant un module premier, C. R. Acad. Sci. Paris **86**, 1071—1072 (1878).
[3] Résolution d'une classe de congruences, C. R. Acad. Sci. Paris **88**, 417—418 (1879).
[4] Sur une classe d'équations dont toutes les racines peuvent s'exprimer linéairement en fonction de l'une d'elles, Bull. Sci. Math. (2) **4**, 262—265 (1880).
[5] Sur les fonctions irréductibles suivant un module premier, C. R. Acad. Sci. Paris **90**, 1339—1341 (1880).
[6] Méthode nouvelle pour diviser le cercle en parties égales, C. R. Acad. Sci. Paris **93**, 838—840 (1881).
[7] Sur les fonctions irréductibles suivant un module premier, C. R. Acad. Sci. Paris **93**, 1065—1066 (1881).
[8] Mémoire sur la théorie algébrique des équations, Bull. Soc. Math. France **15**, 61—103 (1887).
[9] Sur les fonctions réduites suivant un module premier, Bull. Soc. Math. France **17**, 156—167 (1889).
PEPIN T. [1] Sur diverses tentatives de démonstration du théorème de Fermat, C. R. Acad. Sci. Paris **91**, 366—368 (1880).
PERKINS J. C. [1] Rank r solutions to the matrix equation $XX^{\tau} = 0$ over a field of characteristic two, Math. Nachr. **48**, 69—76 (1971).
[2] Gauss sums and the matrix equation $XX^{\tau} = 0$ over fields of characteristic two, Acta Arith. **19**, 205—214 (1971).
PERKINS J. C., FULTON J. D. [1] Symmetric involutions over fields of characteristic 2, Duke Math. J. **38**, 697—702 (1971).
PERLIS S. [1] Normal bases of cyclic fields of prime-power degree, Duke Math. J. **9**, 507—517 (1942).
PERRIN R. [1] Sur la résolution des équations numériques au moyen des suites récurrentes, C. R. Acad. Sci. Paris **119**, 990—993 (1894).
PERRON O. [1] Bemerkungen über die Verteilung der quadratischen Reste, Math. Z. **56**, 122—130 (1952).
PETERSON W. W. [1] Encoding and error-correction procedures for the Bose—Chaudhuri codes, IRE Trans. Information Theory **IT-6**, 459—470 (1960).

[Имеется перевод: ПИТЕРСОН У. Кодирование и исправление ошибок для кодов Боуза—Чоудхури. — В кн.: Кибернетический сборник, вып. 6. — М.: Мир, 1963, с. 25—54.]

[2] Some new results on finite fields and their application to the theory of BCH codes, Proc. Conf. Combinatorial Math. and Its Appl. (Chapel Hill, N. C., 1967), pp. 329—334, Univ. of North Carolina Press, Chapel Hill, N. C., 1969.

PETERSON W. W., BROWN D. T. [1] Cyclic codes for error detection, Proc. IRE **49**, 228—235 (1961).

PETERSON W. W., WELDON E. J., Jr. [1] Error-Correcting Codes, 2nd, ed., M. I. T. Press, Cambridge, Mass., 1972. [Имеется перевод: ПИТЕРСОН У., УЭЛДОН Э. Коды, исправляющие ошибки. — М.: Мир, 1976.]

PETERSSON H. [1] Über die Entwicklungskoeffizienten der automorphen Formen, Acta Math. **58**, 169—215 (1932).

PETR K. [1] Über die Reduzibilität eines Polynoms mit ganzzahligen Koeffizienten nach einem Primzahlmodul, Časopis Pěst. Mat. Fys. **66**, 85—94 (1937).

PETTERSON E. L. [1] Eine Bedingung für die irreduziblen Faktoren von gewissen Polynomen modulo eines Primzahlprodukts, Jber. Deutsch. Math.-Verein. **45**, 169—172 (1935).

[2] Über einen Satz von Ö. Ore, J. reine angew. Math. **172**, 217—218 (1935).

[3] Über die Irreduzibilität ganzzahliger Polynome nach einem Primzahlmodul, J. reine angew. Math. **175**, 209—220 (1936).

PETTOROSSI A. [1] Derivation of an O ($k^2 \log n$) algorithm for computing order-k Fibonacci numbers from the O ($k^3 \log n$) matrix multiplication method, Inform. Process. Lett. **11**, no. 4—5, 172—179 (1980).

PETTOROSSI A., BURSTALL R. M. [1] Deriving very efficient algorithms for evaluating linear recurrence relations using the program transformation technique, Acta Informatica **18**, 181—206 (1982).

PICKERT G. [1] Projektive Ebenen, 2nd ed., Springer-Verlag, Berlin—Heidelberg—New York, 1975.

PIEPER H. [1] Variationen über ein zahlentheoretisches Thema von Carl Friedrich Gauss, Birkhäuser-Verlag, Basel, 1978.

PILZ G. [1] Near Rings: The Theory and Its Applications, North-Holland, Amsterdam, 1977.

PIUMA C. M. [1] Intorno ad una congruenza di modulo primo, Ann. Mat. Pura Appl. (2) **11**, 237—245 (1883).

PIZZARELLO G. [1] Sui polinomi in n indeterminate sopra un campo finito, Ricerca (Napoli) (4) **28**, no. 3, 3—7 (1977).

PLESKEN W. [1] Counting with groups and rings, J. reine angew. Math. **334**, 40—68 (1982).

PLESS V. [1] Power moment identities on weight distributions in error correcting codes, Information and Control **6**, 147—152 (1963).

[2] On the invariants of a vector subspace of a vector space over a field of characteristic two, Proc. Amer. Math. Soc. **16**, 1062—1067 (1965).

PLOTKIN M. [1] Binary codes with specified minimum distances, IRE Trans. Information Theory **IT-6**, 445—450 (1960). [Имеется перевод: ПЛОТКИН М. Двоичные коды с заданным минимальным расстоянием. — В ки.: Кибернетнческий сборник, вып. 7. — М.: ИЛ, 1963, с. 60—73.]

POCKLINGTON H. C. [1] The direct solution of the quadratic and cubic binomial congruences with prime moduli, Proc. Cambridge Philos. Soc. **19**, 57—59 (1917).

[2] Quadratic and higher reciprocity of modular polynomials, Proc. Cambridge Philos. Soc. **40**, 212—214 (1944).

POHLIG S. C., HELLMAN M. E. [1] An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, IEEE Trans. In-

formation Theory **IT-24**, 106—110 (1978).
POLKINGHORN F., Jr. [1] Decoding of double and triple error correcting Bose—Chaudhuri codes, IEEE Trans. Information Theory **IT-12**, 480—481 (1966).
POLLARD J. M. [1] The fast Fourier transform in a finite field, Math. Comp. **25**, 365—374 (1971). [Имеется перевод: ПОЛЛАРД ДЖ. М. Быстрое преобразование Фурье в конечном поле. — В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. — М.: Радио и связь, 1983, с. 147—155.]
[2] Implementation of number-theoretic transforms, Electron. Lett. **12**, 378—379 (1976).
[3] Monte Carlo methods for index computation (mod p), Math. Comp. **32**, 918—924 (1978).
PÓLYA G. [1] Über die Verteilung der quadratischen Reste und Nichtreste, Göttinger Nachr. **1918**, 21—29.
PÓLYA G., SZEGÖ G. [1] Aufgaben und Lehrsätze aus der Analysis. II, Springer, Berlin, 1925. [Имеется перевод: ПОЛИА Г., СЕГЕ Г. Задачи и теоремы из анализа, ч. 2. — М.: Наука, 1978.]
POPOVICI C. P. [1] Целочисленные полиномы, неприводимые по модулю p, Rev. Math. Pures Appl. **4**, 369—379 (1959).
[2] Irreducible polinomials modulo p (Romanian), Acad. R. P. Romîne Fil. Iasi Stud. Cerc. Sti. Mat. **11**, 13—23 (1960).
PORTER A. D. [1] Systems of bilinear and quadratic equations in a finite field, Ann. Mat. Pura Appl. (4) **68**, 21—29 (1965).
[2] Systems of one quadratic and two bilinear equations in a finite field, Publ. Math. Debrecen **13**, 117—121 (1966).
[3] Pairs of bilinear and quadratic equations in a finite field, Monatsh. Math. **70**, 155—160 (1966).
[4] Special equations in a finite field, Math. Nachr. **32**, 277—279 (1966).
[5] Trilinear equations in a finite field, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **40**, 361—365 (1966).
[6] Pairs of bilinear equations in a finite field, Canad. J. Math. **18**, 561—565 (1966).
[7] Some systems of equations in a finite field, Math. Z. **100**, 141—145 (1967).
[8] Orthogonal similarity for skew matrices in $GF(q)$, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **42**, 757—762 (1967).
[9] Generalized quadratic forms in $GF(q)$, Arch. Math. **19**, 615—620 (1968).
[10] The matric equation $AX_1 \ldots X_a = B$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **44**, 727—732 (1968).
[11] Simultaneous equations in a finite field, Publ. Math. Debrecen **16**, 99—110 (1969).
[12] Some partitions of a skew matrix, Ann. Mat. Pura Appl. (4) **82**, 115—120 (1969).
[13] Orthogonal similarity in a finite field, Math. Nachr. **40**, 327—331 (1969).
[14] Generalized bilinear forms in a finite field, Duke Math. J. **37**, 55—60 (1970).
[15] Systems of four equations with a matric application in a finite field, Portugal. Math. **31**, 121—131 (1972).
[16] A matrix form of an exponential sum, Rend. Mat. (6) **5**, 803—818 (1972).
[17] An exponential sum in a finite field, Publ. Math. Debrecen **20**, 53—62 (1973).
[18] The matric equation $A_1X_1 + \ldots + A_mX_m = B$ in $GF(q)$, J. Natur. Sci. and Math. **13**, 115—124 (1973).
[19] Some partitions of a rectangular matrix, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **56**, 667—671 (1974).
[20] Some partitions of a Hermitian matrix, Linear Algebra Appl. **12**, 231—239 (1975).
[21] Solvability of the matrix equation $AX = B$, Linear Algebra Appl. **13**, 177—184 (1976).
[22] Some partitions of a symmetric matrix, Math. Nachr. **84**, 179—183 (1978).

PORTER A. D., ADAMS J. [1] Similarity and orthogonal similarity in a finite field, Duke Math. J. **35**, 519—524 (1968).
PORTER A. D., HANSON L. A. [1] Unitary similarity of normal matrices in $GF(q)$, Math. Nachr. **49**, 351—357 (1971).
[2] Orthogonal similarity of normal matrices in $GF(q)$, Duke Math. J. **38**, 795—803 (1971).
PORTER A. D., MOUSOURIS N. [1] Ranked solutions of some matric equations, Linear and Multilinear Algebra **6**, 145—151 (1978).
[2] Ranked solutions of $AXC = B$ and $AX = B$, Linear Algebra Appl. **24**, 217—224 (1979).
[3] Ranked solutions of the matric equation $A_1X_1 = A_2X_2$, Internat. J. Math. and Math. Sci. **3**, 293—304 (1980).
[4] Exponential sums and rectangular partitions, Linear Algebra Appl. **29**, 347—355 (1980).
[5] Partitions of a symmetric matrix over a finite field, Linear and Multilinear Algebra **10**, 329—341 (1981).
PORTER A. D., RIVELAND A. A. [1] A generalized skew equation over a finite field, Math. Nachr. **69**, 291—296 (1975).
PRABHU K. A., BOSE N. K. [1] Number of irreducible q-ary polynomials in several variables with prescribed degrees, IEEE Trans. Circuits and Systems **CAS-26**, 973—975 (1979).
PRADHAN D. K. [1] A theory of Galois switching functions, IEEE Trans. Computers **C-27**, 239—248 (1978).
PRANGE E. [1] Cyclic error-correcting codes in two symbols, Tech. Note AFCRC-TN-57-103, Air Force Cambridge Research Center, Bedford, Mass., 1957.
[2] Some cyclic error-correcting codes with simple decoding algorithms, Tech. Note AFCRC-TN-58-156, Air Force Cambridge Research Center, Bedford, Mass., 1958.
PREPARATA F. P., SARWATE D. V. [1] Computational complexity of Fourier transforms over finite fields, Math. Comp. **31**, 740—751 (1977).
PREŠIĆ M. D. [1] A method for solving equations in finite fields, Mat. Vesnik **7**, 507—509 (1970).
RABER N. C. [1] A geometric approach to counting distribution of squares in a finite field, Geom. Dedicata **4**, 297—303 (1975).
RABIN M. O. [1] Probabilistic algorithms in finite fields, SIAM J. Computing **9**, 273—280 (1980).
RABUNG J. R., JORDAN J. H. [1] Consecutive power residues or nonresidues, Math. Comp. **24**, 737—740 (1970).
RADEMACHER H. [1] The Fourier coefficients of the modular invariant $J(\tau)$, Amer. J. Math. **60**, 501—512 (1938).
[2] Fourier expansions of modular forms and problems of partition, Bull. Amer. Math. Soc. **46**, 59—73 (1940).
RADOS G. [1] Zur Theorie der Congruenzen höheren Grades, J. reine angew. Math. **99**, 258—260 (1886).
[2] Sur une théorie des congruences à plusieurs variables, Ann. Sci. Ecole Norm. Sup. (3) **27**, 217—231 (1910).
[3] Sur la théorie des congruences de degré supérieur, Ann. Sci. Ecole Norm Sup. (3) **30**, 395—412 (1913).
[4] Ein Satz über Kongruenzen höheren Grades, Acta Lit. Scient. Univ. Hung. **1**, 1—5 (1922).
[5] Sur une identité remarquable de la théorie des congruences binomes, Rend. Circ. Mat. Palermo **46**, 308—314 (1922).
RAGHAVARAO D. [1] Constructions and Combinatorial Problems in Design of Experiments, Wiley, New York, 1971.
RAJWADE A. R. [1] Arithmetic on curves with complex multiplication by $\sqrt{-2}$, Proc. Cambridge Philos. Soc. **64**, 659—672 (1968).

[2] Arithmetic on curves with complex multiplication by the Eisenstein integers, Proc. Cambridge Philos. Soc. **65**, 59—73 (1969).
[3] On rational primes p congruent to 1 (mod 3 or 5), Proc. Cambridge Philos. Soc. **66**, 61—70 (1969).
[4] A note on the number of solutions N_p of the congruence $y^2 \equiv x^3 - Dx \pmod p$, Proc. Cambridge Philos. Soc. **67**, 603—606 (1970).
[5] The number of solutions of the congruence $y^2 \equiv x^6 - a \pmod p$, Indian J. Pure Appl. Math. **4**, 325—332 (1973).
[6] On the congruence $y^2 \equiv x^5 - a \pmod p$, Proc. Cambridge Philos. Soc. **74**, 473—475 (1973).
[7] Certain classical congruences via elliptic curves, J. London Math. Soc. (2) **8**, 60—62 (1974).
[8] Notes on the congruence $y^2 \equiv x^5 - a \pmod p$, L'Enseignement Math. (2) **21**, 49—56 (1975).
[9] The Diophantine equation $y^2 = x(x^2 + 21Dx + 112D^2)$ and the conjectures of Birch and Swinnerton-Dyer, J. Austral. Math. Soc. Ser. A **24**, 286—295 (1977).
ADJWADE A. R., PARNAMI J. C. [1] A new cubic character sum, Acta Arith. **40**, 347—356 (1982).
RAKTOE B. L. [1] Generalized combining of elements from finite fields, Ann. Math. Statist. **41**, 1763—1767 (1970).
RALSTON T. [1] On the distribution of squares in a finite field, Geom. Dedicata **8**, 207—212 (1979).
RANKIN R. A. [1] Modular Forms and Functions, Cambridge Univ. Press, Cambridge, 1977.
RAO C. R. [1] Factorial experiments derivable from combinatorial arrangements of arrays, J. Royal Statist. Soc. Suppl. **9**, 128—139 (1947).
RAO K. N. [1] A congruence equation in GF $[p^n, x]$ and some related arithmetical identities, Duke Math. J. **33**, 783—789 (1966).
[2] Some applications of Carlitz's η-sum, Acta Arith. **12**, 213—221 (1967).
[3] Algebras of quadratic residues (mod P) in $GF[p^n, x]$, Boll. Un. Mat. Ital. (4) **1**, 680—686 (1968).
RAUSSNITZ G. [1] Math. Natur. Ber. Ungarn **1**, 266—278 (1882/83).
RAUTER H. [1] Studien zur Theorie des Galoisschen Körpers über dem Körper der rationalen Funktionen einer Unbestimmten t mit Koeffizienten aus einem beliebigen endlichen Körper von p^{m_0} Elementen, J. reine angew. Math. **159**, 117—132 (1928); Bemerkungen, ibid. **159**, 228 (1928).
[2] Höhere Kreiskörper, J. reine angew. Math. **159**, 220—227 (1928).
RÉDEI L. [1] Über einige Mittelwertfragen im quadratischen Zahlenkörper, J. reine angew. Math. **174**, 15—55 (1936).
[2] Über einige merkwürdige Polynome in endlichen Körpern mit zahlentheoretischen Beziehungen, Acta Sci. Math. Szeged **11**, 39—54 (1946).
[3] Zur Theorie der Gleichungen in endlichen Körpern, Acta Sci. Math. Szeged **11**, 63—70 (1946).
[4] Über eindeutig umkehrbare Polynome in endlichen Körpern, Acta Sci. Math. Szeged **11**, 85—92 (1946).
[5] Über die Gleichungen dritten und vierten Grades in endlichen Körpern, Acta Sci. Math. Szeged **11**, 96—105 (1946).
[6] Bemerkung zu meiner Arbeit «Über die Gleichungen dritten und vierten Grades in endlichen Körpern», Acta Sci. Math. Szeged **11**, 184—190 (1947).
[7] Zwei Lückensätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gaussischen Summen, Acta Math. **79**, 273—290 (1947).
[8] Kurzer Beweis eines Satzes von Vandiver über endliche Körper, Publ. Math. Debrecen **1**, 99—100 (1949).

[9] A short proof of a theorem of Š. Schwarz concerning finite fields, Časopis Pěst. Mat. Fys. **75**, 211—212 (1950).

[10] Algebra, Geest & Portig, Leipzig, 1959; Pergamon Press, London, 1967.
[11] Lückenhafte Polynome über endlichen Körpern, Birkhäuser Verlag, Basel—Stuttgart, 1970; Akadémiai Kiadó, Budapest, 1973.

RÉDEI L., SZELE T. [1] Algebraisch-zahlentheoretische Betrachtungen über Ringe. I, Acta Math. **79**, 291—320 (1947).
[2] Algebraisch-zahlentheoretische Betrachtungen über Ringe. II, Acta Math. **82**, 209—241 (1950).

RÉDEI L., TURÁN P. [1] Zur Theorie der algebraischen Gleichungen über endlichen Körpern, Acta Arith. **5**, 223—225 (1959).

RÉDEI L., WEINERT H. J. [1] Ein Gleichverteilungssatz für Systemehomogener Linearformen modulo p, Acta Sci. Math. Szeged **27**, 41—43 (1966).

REDINBO G. R. [1] Finite field arithmetic on an array processor, IEEE Trans. Computers **C-28**, 461—471 (1979).

REE R. [1] Proof of a conjecture of S. Chowla, J. Number Theory **3**, 210—212 (1971): Erratum, ibid. **4**, 223 (1972).

REED I. S. [1] A class of multiple-error-correcting codes and the decoding scheme, IRE Trans. Information Theory **PGIT-4**, 38—49 (1954). [Имеется перевод: РИД И. С. Класс кодов с исправлением нескольких ошибок и схема декодирования. — В кн.: Кибернетический сборник, вып. 1. — М.: ИЛ, 1960, с. 189—205.]

REED I. S., SCHOLTZ R. A., TRUONG T. K., WELCH L. R. [1] The fast decoding of Reed—Solomon codes using Fermat theoretic transforms and continued fractions, IEEE Trans. Information Theory **IT-24**, 100—106 (1978).

REED I. S., SOLOMON G. [1] Polynomial codes over certain finite fields, J. Soc. Indust. Appl. Math. **8**, 300—304 (1960). [Имеется перевод: РИД И. С., СОЛОМОН Г. Полиномиальные коды над некоторыми конечными полями. — В кн.: Кибернетический сборник, вып. 7. — М.: ИЛ, 1963, с. 74—79.]

REED I. S., TRUONG T. K. [1] The use of finite fields to compute convolutions, IEEE Trans. Information Theory **IT-21**, 208—213 (1975).
[2] Convolutions over residue classes of quadratic integers, IEEE Trans. Information Theory **IT-22**, 468—475 (1976); Correction, ibid. **IT-23**, 544 (1977).
[3] Fast Mersenne-prime transforms for digital filtering, Proc. Inst. Electr. Engrs. **125**, 433—440 (1978).
[4] Simple proof of the continued fraction algorithm for decoding Reed—Solomon codes, Proc. Inst. Electr. Engrs. **125**, 1318—1320 (1978).

REED I. S., TRUONG T. K., MILLER R. L. [1] Fast algorithm for computing a primitive $2^{p+1}p$th root of unity in $GF[(2^p-1)^2]$, Electron. Lett. **14**, 493—494 (1978).
[2] Simple method for computing elements of order $2^k n$, where $n \mid 2^{p-1}-1$ and $2 \leqslant k \leqslant p+1$, in $GF[(2^p-1)^2]$, Electron. Lett. **14**, 697—698 (1978).
[3] Decoding of B. C. H. and R. S. codes with errors and erasures using continued fractions, Electron. Lett. **15**, 542—544 (1979).
[4] A new algorithm for computing primitive elements in the field of Gaussian complex integers modulo a Mersenne prime, IEEE Trans. Acoust. Speech Signal Process. **27**, 561—563 (1979).

REED I. S., TRUONG T. K., WELCH L. R. [1] The fast decoding of Reed—Solomon codes using Fermat transforms, IEEE Trans. Information Theory **IT-24**, 497—499 (1978).

REES D. [1] Note on a paper by I. J. Good, J. London Math. Soc. **21**, 169—172 (1946).

REICH D. [1] A p-adic fixed point formula, Amer. J. Math. **91**, 835—850 (1969).

REINER I. [1] On the number of matrices with given characteristic polynomial, Illinois J. Math. **5**, 324—329 (1961).

RELLA T. [1] Lineare Operatoren in endlichen Kongruenzkörpern, Monatsh. Math. Phys. **32**, 139—150 (1922).
RETTER C. T. [1] Decoding Goppa codes with a BCH decoder, IEEE Trans. Information Theory **IT-21**, 112 (1975).
RHIN G. [1] Quelques résultats métriques dans un corps de séries formelles sur un corps fini, Sém. Delange—Pisot—Poitou 1967/68, Théorie des Nombres, Exp. 21, Secrétariat Math., Paris, 1969.
[2] Généralisation d'un théorème de I. M. Vinogradov à un corps de séries formelles sur un corps fini, C. R. Acad. Sci. Paris Sér. A **272**, 567—569 (1971).
[3] Répartition modulo 1 dans un corps de séries formelles sur un corps fini, Dissertationes Math. **95** (1975).
RIBENBOIM P. [1] Polynomials whose values are powers, J. reine angew. Math. **268/269**, 34—40 (1974).
[2] 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York—Heidelberg—Berlin, 1979.
RICE B. [1] Some good fields and rings for computing number-theoretic transforms, IEEE Trans. Acoust. Speech Signal Process. **27**, 432—433 (1979).
[2] Winograd convolution algorithms over finite fields, Congr. Numer. **29**, 827—857 (1980).
RICHALET J. [1] Operational calculus for finite rings, IEEE Trans. Circuit Theory **CT-12**, 558—570 (1965).
RIEGER G. J. [1] Sur les nombres de Cullen, Sém. Théorie des Nombres 1976—1977, Exp. 16, Univ. Bordeaux I, Talence, 1977.
[2] Bemerkungen über gewisse nichtlineare Kongruenzen, Elemente der Math **32**, 113—115 (1977).
[3] Über Lipschitz-Folgen, Math. Scand. **45**, 168—176 (1979).
RITT J. F. [1] Prime and composite polynomials, Trans. Amer. Math. Soc. **23**, 51—66 (1922).
[2] Permutable rational functions, Trans. Amer. Math. Soc. **25**, 399—448 (1923).
RIVELAND A. A., PORTER A. D. [1] The skew matric equation $X_n' \dots X_1' A X_1 \dots X_n = B$, Rend. Mat. (6) **9**, 633—638 (1976).
[2] The skew matrix equation $X_n' \dots X_1' A X_1 \dots X_n = B$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **60**, 751—755 (1976).
RIVLIN T. J. [1] The Chebyshev Polynomials, Wiley, New York, 1974.
ROBERT A. [1] Elliptic Curves, Lecture Notes in Math., vol. 326, Springer-Verlag Berlin—Heidelberg—New York, 1973.
ROBINSON A. [1] Introduced to Model Theory and to the Metamathematics of Algebra, North-Holland, Amsterdam, 1963.
ROBINSON D. W. [1] The Fibonacci matrix modulo m, Fibonacci Quart. **1**, no. 2, 29—36 (1963).
[2] A note on linear recurrent sequences modulo m, Amer. Math. Monthly **73**, 619—621 (1966).
[3] Iteration of the modular period of a second order linear recurrent sequence, Acta Arith. **22**, 249—256 (1972/73).
[4] The rank and period of a linear recurrent sequence over a ring, Fibonacci Quart. **14**, 210—214 (1976).
ROBINSON S. F. [1] Theorems on Brewer sums, Pacific J. Math. **25**, 587—596 (1968).
ROCCI E. [1] Sulla distribuzione dei residui quadratici di un numero primo nella serie naturale, Giorn. Mat. Battaglini **65**, 112—134 (1927).
RODEMICH E. R., RUMSEY H. [1] Primitive trinomials of high degree, Math. Comp. **22**, 863—865 (1968).
ROGERS K. [1] Cyclotomic polynomials and division rings, Monatsh. Math. **69**, 239—242 (1965).
[2] An elementary proof of a theorem of Jacobson, Abh. Math. Sem. Univ. Hamburg **35**, 223—229 (1971); Berichtigung, ibid. **37**, 268 (1972).

ROGERS L. J. [1] On the analytic representation of heptagrams, Proc. London Math. Soc. **22**, 37—52 (1890).

[2] Note on functions proper to represent a substitution of a prime number of letters, Messenger of Math. (2) **21**, 44—47 (1891).

ROHRBACH H. [1] Die Charaktere der binären Kongruenzgruppen mod p^2, Schr. Math. Sem. Inst. Angew. Math. Univ. Berlin **1**, 33—94 (1932).

ROQUETTE P. [1] Riemannsche Vermutung in Funktionenkörpern, Arch. Math. **4**, 6—16 (1953).

[2] Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts, J. reine angew. Math. **191**, 199—252 (1953).

ROSATI L. A. [1] Sul numero dei punti di una superficie cubica in uno spazio lineare finito, Boll. Un. Mat. Ital. (3) **11**, 412—418 (1956).

ROSENBERG I. G. [1] Sums of Legendre symbols. I, II (Czech), Sb. Vysoké. Učení Tech. Brno **1962**, no. 1—2, 183—190; no. 3—4, 311—314.

[2] Polynomial functions over finite rings, Glasnik Mat. (3) **10**, 25—33 (1975).

[3] Characteristic polynomials in *GF* (2) of zero-one inequalities and equations, Utilitas Math. **7**, 323—343 (1975).

ROSENBERGER G. [1] Über Tschebyscheff-Polynome, Nicht-Kongruenzuntergruppen der Modulgruppe und Fibonacci-Zahlen, Math. Ann. **246**, 193—203 (1980).

ROTA G.-C. [1] On the foundations of combinatorial theory, I. Theory of Moebius functions, Z. Wahrscheinlichkeitstheorie **2**, 340—368 (1964).

ROTH H. H. [1] Linear binary shift register circuits utilizing a minimum number of mod-2 adders, IEEE Trans. Information Theory **IT-11**, 215—220 (1965).

RUDEANU S. [1] L'emploi des imaginaires de Galois dans la théorie des mécanismes automatiques. X (Romanian. French summary), Acad. R. P. Romîne. Stud. Cerc. Mat. **9**, 217—287 (1958).

RUDOLPH L. D. [1] A class of majority-logic decodable codes, IEEE Trans. Information Theory **IT-13**, 305—307 (1967).

RUTHERFORD D. E. [1] Modular Invariants, Cambridge Tracts in Math. and Math. Physics, no. 27, Cambridge Univ. Press, London, 1932.

RYSER H. J. [1] Combinatorial Mathematics, Carus Math. Monographs, no. 14, Math. Assoc. of America, New York, 1963. [Имеется перевод: РАЙЗЕР Г. ДЖ. Комбинаторная математика. — М.: Мир, 1966.]

[2] Symmetric designs and related configurations, J. Combinatorial Theory Ser. A **12**, 98—111 (1972).

[3] The existence of symmetric block designs, J. Combinatorial Theory Ser. A **32**, 103—105 (1982).

SACHAR H. [1] The F_p span of the incidence matrix of a finite projective plane, Geom. Dedicata **8**, 407—415 (1979).

SAKATA S. [1] General theory of doubly periodic arrays over an arbitrary finite field and its applications, IEEE Trans. Information Theory **IT-24**, 719—730 (1978).

[2] On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals, IEEE Trans. Information Theory **IT-27**, 556—565 (1981).

SALIÉ H. [1] Über die Kloostermanschen Summen $S(u, v; q)$, Math. Z. **34**, 91—109 (1932).

[2] Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen, Math. Z. **36**, 263—278 (1933).

[3] Über die Verteilung der quadratischen Reste, Math. Z. **37**, 594—602 (1933).

SAMPSON J. H., WASHNITZER G. [1] Numerical equivalence and the zeta-function of a variety, Amer. J. Math. **81**, 735—748 (1959).

SANSONE G. [1] La risoluzione apiristica delle congruenze biquadratiche, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (6) **6**, 573—578 (1927).

[2] Nuove formule risolutive delle congruenze cubiche, Rend. Accad. Sci. Fis. Mat. Napoli (4) **35**, 54—81 (1929).
[3] La risoluzione apiristica delle congruenze cubiche, Ann. Mat. Pura Appl. (4) **6**, 127—160 (1929).
[4] Sul problema della risoluzione apiristica delle congruenze di grado qualunque rispetto ad un modulo primo, e la risoluzione apiristica delle congruenze di quarto grado, Mem. Accad. Naz. Lincei (6) **3**, 220—260 (1929).
[5] La risoluzione apiristica delle congruenze cubiche, Ann. Mat. Pura Appl. (4) **7**, 1—32 (1930).
SÁRKÖZY A. [1] Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions. IV, Acta Math. Acad. Sci. Hungar. **30**, 155—162 (1977).
SARWATE D. V. [1] On the complexity of decoding Goppa codes, IEEE Trans. Information Theory **IT-23**, 515—516 (1977).
[2] Semi-fast Fourier transforms over $GF(2^m)$, IEEE Trans. Computers **C-27**, 283—285 (1978).
SATO M., YORINAGA M. [1] Numerical experiments on a conjecture of B. C. Mortimer and K. S. Williams, Proc. Japan Acad. **49**, 791—794 (1973).
SCARPIS U. [1] Intorno alla risoluzione per radicali di un'equazione algebrica in un campo di Galois, Periodico di Mat. (3) **9**, 73—79 (1912).
[2] Successioni ricorrenti in un campo di Galois, Ann. Mat. Pura Appl. (3) **18**, 245—286 (1912).
[3] Intorno all'interpretazione della Teoria di Galois in un campo di razionalità finito, Ann. Mat. Pura Appl. (3) **23**, 41—60 (1914).
SCHAAR M. [1] Mémoire sur la théorie des résidus quadratiques, Acad. Roy. Sci. Lettres Beaux Arts Belgique **24** (1850).
SCHANUEL S. H. [1] An extension of Chevalley's theorem to congruences modulo prime powers, J. Number Theory **6**, 284—290 (1974).
SCHMID H. L. [1] Relationen zwischen verallgemeinerten Gaußschen Summen, J. reine angew. Math. **176**, 189—191 (1937).
[2] Kongruenzzetafunktionen in zyklischen Körpern, Abh. Preuss. Akad. Wiss. Math.-Naturw. Kl. **1941**, no. 14, 1—30.
SCHMID H. L., TEICHMÜLLER O. [1] Ein neuer Beweis für die Funktionalgleichung der L-Reihen, Abh. Math. Sem. Univ. Hamburg **15**, 85—96 (1943).
SCHMIDT F. K. [1] Allgemeine Körper im Gebiet der höheren Kongruenzen, Dissertation, Freiburg i. Br., 1925.
[2] Zur Zahlentheorie in Körpern von der Charakteristik p, Sitzungsber. Phys.-Med. Soz. Erlangen **58/59**, 159—172 (1926/27).
[3] Analytische Zahlentheorie in Körpern der Charakteristic p, Math. Z. **33**, 1—32 (1931).
SCHMIDT W. M. [1] Zur Methode von Stepanov, Acta Arith. **24**, 347—367 (1973).
[2] A lower bound for the number of solutions of equations over finite fields, J. Number Theory **6**, 448—480 (1974).
[3] Equations over Finite Fields: An Elementary Approach, Lecture Notes in Math., vol. 536, Springer-Verlag, Berling—Heidelberg—New York, 1976.
SCHNEIDER P. [1] On the values of the zeta function of a variety over a finite field, Compositio Math. **46**, 133—143 (1982).
SCHOLEFIELD P. H. R. [1] Shift registers generating maximum-length sequences, Electronic Technology **37**, 389—394 (1960).
SCHÖNEMANN T. [1] Ueber die Congruenz $x^2 + y^2 \equiv 1 \pmod{p}$, J. reine angew. Math. **19**, 93—112 (1839).
[2] Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben, J. reine angew. Math. **19**, 289—308 (1839).
[3] Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, J. reine angew. Math. **31**, 269—325 (1846).

[4] Über einige von Herrn Dr. Eisenstein aufgestelle Lehrsätze, J. reine angew. Math. **40**, 185—187 (1850).

SCHÖNHAGE A. [1] Schnelle Berechnung von Kettenbruchentwicklungen, Acta Informatica **1**, 139—144 (1971).

[2] Schnelle Multiplikation von Polynomen über Körpern der Charakteristik **2**, Acta Informatica **7**, 395—398 (1977).

SCHÖNHEIM J. [1] Formules pour résoudre la congruence $x^2 \equiv a \pmod{P}$ dans des cas encore inconnus et leur application pour déterminer directement des racines primitives de certains nombres premiers (Romanian. French summary), Acad. R. P. Romîne Fil. Cluj. Stud. Cerc. Mat. Fiz. **7**, no. 1—4, 51 (1956).

[2] On linear and nonlinear single-error-correcting q-nary perfect codes, Information and Control **12**, 23—26 (1968).

SCHUPFER F. [1] Su due proposizioni di teoria dei numeri, Rend. Mat. e Appl. (5) **5**, 246—251 (1946).

SCHUR I. [1] Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$, Jber. Deutsch. Math.-Verein. **25**, 114—117 (1916).

[2] Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pòlya: Über die Verteilung der quadratischen Reste und Nichtreste, Göttinger Nachr. **1918**, 30—36.

[3] Über die Gaußschen Summen, Göttinger Nachr. **1921**, 147—153.

[4] Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen, Sitzungsber. Preuß. Akad. Wiss. Berlin Math.-Naturwiss. Kl. **1923**, 123—134.

SCHWARZ Š. [1] Contribution à la réductibilité des polynômes dans la théorie des congruences, Věstnik Královské České Spol. Nauk. Třida Matemat. — Přirodověd. **1939**, no. 7, 1—7.

[2] A contribution to the arithmetic of finite filds (Slovak), Prirodoved. Priloha Techn. Obzoru Sloven. **1**, no. 8, 75—81 (1940).

[3] Sur le nombre des racines et des facteurs irréductibles d'une congruence donnée, Časopis Pěst. Mat. Fys. **69**, 128—145 (1940).

[4] A contribution to the reducibility of binomial congruences (Slovak), Časopis. Pěst. Mat. Fys. **71**, 21—31 (1946).

[5] On Waring's problem for finite fields, Quart. J. Math. **19**, 123—128 (1948).

[6] On the equation $a_1x_1^k + a_2x_2^k + \ldots + a_kx_k^k + b = 0$ in finite fields, Quart. J. Math. **19**, 160—163 (1948).

[7] On the reducibility of binomial congruences and on the bound of the least integer belonging to a given exponent mod p, Časopis Pěst. Mat. Fys. **74**, 1—16 (1949).

[8] On equations of the form $c_1x_1^k + \ldots + c_sx_s^k = c$ in finite fields (Slovak), Časopis Pěst. Mat. Fys. **74**, 175—176 (1949).

[9] On universal forms in finite fields, Časopis Pěst. Mat. Fys., **75**, 45—50 (1950).

[10] On a type of universal forms in discretely normed fields, Acta Sci. Math. Szeged **17**, 5—19 (1956).

[11] On the reducibility of polynomials over a finite field, Quart. J. Math. (2) **7**, 110—124 (1956).

[12] Об одном классе многочленов над конечным полем, Mat.—Fyz. Časopis Sloven. Akad. Vied **10**, 68—80 (1960).

[13] О числе неприводимых факторов данного многочлена над конечным полем, Czechoslovak Math. J. **11**, 213—225 (1961).

[14] Замечание об алгебраических уравнениях над конечным полем, Mat.-Fyz. Časopis Sloven. Akad. Vied, **122**,24—229 (1962).

[15] On a system of congruences. A remark on the preceding paper of Sedláček

(Slovak), Mat.-Fyz. Časopis Sloven Akad. Vied **13**, 103—104 (1963).
SCHWERING K. [1] Zur Theorie der arithmetischen Functionen, welche von Jacobi $\psi(\alpha)$ genannt werden, J. reine angew. Math. **93**, 334—337 (1882).
SCOGNAMIGLIO G. [1] Algebre di matrici atte a rappresentare campi di Galois, Giorn. Mat. Battaglini (6) **2**, 37—48 (1964).
SCORZA G. [1] La risoluzione apiristica delle congruenze binomie e la formula di interpolazione di Lagrange, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (6) **3**, 390—394 (1926).
SCOTT W. R. [1] Group Theory, Prentice-Hall, Englewood Cliffs, N. J., 1964.
SEDLÁČEK J. [1] Some remarks on the problem of W. Mnich (Czech), Mat.-Fys. Časopis Sloven.Acad. Vied **13**, 97—102 (1963).
SEGRE B. [1] Sui k-archi nei piani finiti di caratteristica due, Rev. Math. Pures Appl. **2**, 289—300 (1957).
[2] Le geometrie di Galois, Ann. Mat. Pura Appl. (4) **48**, 1—97, (1959).
[3] Sulla teoria delle equazioni e delle congruenze algebriche. I, II, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **27**, 155—161, 303—311 (1959).
[4] Sistemi di equazioni nei campi di Galois, Convegno Teoria dei Gruppi Finiti e Applicazioni (Florence, 1960), pp. 66—80, Edizioni Cremonese, Rome, 1960.
[5] Sul numero delle soluzioni di un qualsiasi sistema di equazioni algebriche sopra un campo finito, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **28**, 271—277 (1960).
[6] Lectures on Modern Geometry, Edizioni Cremonese, Rome, 1961.
[7] Geometry and algebra in Galois spaces, Abh. Math. Sem. Univ. Hamburg **25**, 129—139 (1962).
[8] Ovali e curve σ nei piani di Galois di caratteristica due, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **32**, 785—790 (1962).
[9] Intorno ad una congettura di Lang e Weil, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **34**, 337—339 (1963).
[10] Arithmetische Eigenschaften von Galois-Räumen. I, Math. Ann. **154**, 195—256 (1964).
[11] Forme e geometrie hermitiane, con particolare riguardo al caso finito, Ann. Mat. Pura Appl. (4) **70**, 1—201 (1965).
SEGRE B., BARTOCCI U. [1] Ovali ed altre curve nei piani di Galois di caratteristica due, Acta Arith. **18**, 423—449 (1971).
SELBERG A. [1] Über die Fourierkoeffizienten elliptischer Modulformen negativer Dimension, Neuvième Congrès des Mathématiciens Scandinaves (Helsinki, 1938), pp. 320—322, Merc. Kirjapaino, Helsinki, 1939.
[2] On the estimation of Fourier coefficients of modular forms, Proc. Symp. Pure Math., vol. 8, pp. 1—15, American Math. Society, Providence, R. I., 1965.
SELFRIDGE J. L., NICOL C. A., VANDIVER H. S. [1] On diophantine equations which have no solutions, Proc. Nat. Acad. Sci. U. S.A. **42**,264—266 (1956).
SELMER E. S. [1] The diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85**, 203—362 (1951).
[2] On Newton's equations for the power sums, Nordisk Tidskr. for Informationsbehandling (BIT) **6**, 158—160 (1966).
[3] Linear Recurrence Relations over Finite Fields, Univ. of Bergen, 1966.
SENGENHORST P. [1] Über Körper der Charakteristik p, Math. Z. **24**, 1—39 (1926); Bemerkungen, ibid. **26**, 495 (1927).
SEROUSSI G., LEMPEL A. [1] Factorization of symmetric matrices and trace-orthogonal bases in finite fields, SIAM J. Computing **9**, 758—767 (1980).
SERRE J.-P. [1] Cours d'arithmétique, Presses Univ. de France, Paris, 1970. [Имеется перевод: СЕРР Ж.-П. Курс арифметики. — М.: Мир, 1972.]
[2] Valeurs propres des endomorphismes de Frobenius (d'après P. Deligne),

Séminaire Bourbaki 1973/74, Exp. 446, Lecture Notes in Math., vol. 431, pp. 190—204, Springer-Verlag, Berlin—Heidelberg—New York, 1975.

[3] Majorations des sommes exponentielles, Astérisque, no. 41—42, pp. 111—126, Soc. Math. France, Paris. 1977.

SERRET J.-A. [1] Cours d'algèbre supérieure, 2nd ed., Mallet-Bachelier, Paris, 1854.

[2] Course d'algèbre supérieure, 3rd ed., Gauthier-Villars, Paris, 1866. [Имеется перевод: СЕРРЕ И.-А. Курс высшей алгебры. — С.-Пб., М.: Изд. М. О. Вольф, 1897.]

[3] Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modulaire irréductible, Mém. Acad. Sci. Inst. de France **35**, 617—688 (1866).

[4] Détermination des fonctions entières irréductibles, suivant un module premier, dans le cas où le degré est égal au module, J. Math. Pures Appl. (2) **18**, 301—304 (1873).

[5] Sur les fonctions entières irréductibles suivant un module premier, dans le cas où le degré est une puissance du module, J. Math. Pures Appl. (2) **18**, 437—451 (1873).

SHADER L. E. [1] Arithmetical functions associated with unitary divisors in $GF[q, x]$. I, II, Ann. Mat. Pura Appl. (4) **86**, 79—85, 87—97 (1970).

[2] On the number of solutions of congruences and equations in $GF[q, x]$, Portugal. Math. **30**, 181—190 (1971).

[3] On the number of solutions of a congruence in $GF[q, x]$, Portugal. Math. **32**, 9—16 (1973).

[4] Closed form expressions for several Rammanujan sums, Portugal. Math. **32**, 147—153 (1973).

SHAH A. P. [1] Fibonacci sequence modulo m, Fibonacci Quart. **6**, 139—141 (1968).

SHANKS D. [1] Two theorems of Gauss, Pacific J. Math. **8**, 609—612 (1958).

[2] Five number-theoretic algorithms, Proc. Second Manitoba Conf. on Numerical Math. (Winnipeg, Man., 1972), pp. 51—70, Utilitas Math., Winnipeg, Man., 1973.

SHANNON C. E. [1] A mathematical theory of communication, Bell System Tech. J. **27**, 379—423, 623—656 (1948). [Имеется перевод: ШЕННОН К. Математическая теория связи. — В кн.: К. Шеннон. Работы по теории информации и кибернетике. — М.: ИЛ, 1963, с. 243—332.]

SHANNON C. E., WEAVER W. [1] A Mathematical Theory of Communication, Univ. of Illinois Press, Urbana, Ill., 1949.

SHEHADEH N. M. [1] On the distribution of the coefficients of some polynomials, SIAM J. Appl. Math. **16**, 958—963 (1968).

SHIMURA G. [1] Introduction to the Arithmetic Theory of Automorphic Functions, Princeton Univ. Press. Princeton, N. J., 1971. [Имеется перевод: ШИМУРА Г. Введение в арифметическую теорию автоморфиых функций. — М.: Мир, 1973.]

SHIMURA G., TANIYAMA Y. [1] Complex Multiplication of Abelian Varieties and Its Applications to Number Theory, Math. Society of Japan, Tokyo, 1961.

SHIRATANI K. [1] On the Gauss—Hecke sums, J. Math. Soc. Japan **16**, 32—38 (1964).

SHIUE J.-S. [1] A remark of a paper by Bundschuh, Tamkang J. Math. **4**, 129—130 (1973).

SHIUE J.-S., HU M. H. [1] Some remarks on the uniform distribution of a linear recurrence of the second order, Tamkang J. Math. **4**, 101—103 (1973).

SHIUE J.-S., SHEU T. L. [1] On the periodicity of linear recurrence of second order in commutative rings, Tamkang J. Math. **4**, 105—107 (1973).

SHIVA S. G. S., ALLARD P. E. [1] A few useful details about a known technique

for factoring $1 + X^{2q-1}$, IEEE, Trans. Information Theory **IT-16**, 234—235 (1970).

SHRIKHANDE S. S. [1] The impossibility of certain symmetrical balanced incomplete block design, Ann. Math. Statist. **21**, 106—111 (1950).

SIEGEL C. L. [1] Über die analytische Theorie der quadratischen Formen, Ann. of Math. (2) **36**, 527—606 (1935).

[2] Generalization of Waring's problem to algebraic number fields, Amer. J. Math. **66**, 122—136 (1944).

[3] Über das quadratische Reziprozitätsgesetz in algebraischen Zahlkörpern, Göttinger Nachr. **1960**, no. 1, 1—16.

SILVA J. A. [1] A theorem on cyclic matrices, Duke Math. J. **18**, 821—825 (1951).

[2] Representation of arithmetic functions in $GF[p^n, x]$ with values in an arbitrary field, Duke Math. J. **19**, 31—44 (1952).

SIMMONS G. [1] On the number of irreducible polynomials of degree d over $GF(p)$, Amer. Math. Monthly **77**, 743—745 (1970).

SIMS C. C. [1] The role of algorithms in the teaching of algebra, Topics in Algebra (M. F. Newman, ed.), Lecture Notes in Math., vol. 697, pp. 95—107, Springer-Verlag, Berlin—Heidelberg—New York, 1978.

SINGER J. [1] A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. **43**, 377—385 (1938).

SINGH S. [1] Bounds of cubic residues in A. P., Indian J. Pure Appl. Math. **1**, 265—268 (1970).

[2] The number of decompositions of an integer as a sum of two squares in $GF(p^n)$, Indian J. Pure Appl. Math. **4**, 606—611 (1973).

[3] Stufe of a finite field, Fibonacci Quart. **12**, 81—82 (1974).

[4] Analysis of each integer as sum of two cubes in a finite integral domain, Indian J. Pure Appl. Math. **6**, 29—35 (1975).

[5] Bound for the solutions of a Diophantine equation in prime Galois fields, Indian J. Pure Appl. Math. **8**, 1428—1430 (1977).

[6] Integer points on special hyper-elliptic curves in $GF(p)$, Indian J. Pure Appl. Math. **10**, 1213—1215 (1979).

SINGH S., RAJWADE A. R. [1] The number of solutions of the congruence $y^2 \equiv x^4 - a \pmod{p}$, L'Enseignement Math. (2) **20**, 265—273 (1974).

SINGLETON R. C. [1] Maximum distance q-nary codes, IEEE Trans. Information Theory **IT-10**, 116—118 (1964).

SINGMASTER D. [1] On polynomial functions (mod m), J. Number Theory **6**, 345—352 (1974).

SKOLEM T. [1] Zwei Sätze über kubische Kongruenzen, Norske Vid. Selsk, Forh. 10, 89—92 (1937).

[2] Die Anzahl der Wurzeln der Kongruenz $x^3 + ax + b \equiv 0 \pmod{p}$ für die verschiedenen Paare a, b, Norske Vid. Selsk. Forh. **14**, 161—164 (1942).

[3] Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist, Avh. Norske Vid. Akad. Oslo I **1942**, no. 4.

[4] The general congruence of 4th degree modulo p, p prime, Norsk Mat. Tidsskr. **34**, 73—80 (1952).

[5] On a certain connection between the discriminant of a polynomial and the number of its irreducible factors (mod p), Norsk Mat. Tidsskr. **34**, 81—85 (1952).

[6] Remarks on proofs by cyclotomic formulas of reciprocity laws for power residues, Math. Scand. **9**. 229—242 (1961).

SLEPIAN D. [1] A note on two binary signaling alphabets, IRE Trans. Information Theory **IT-2**, 84—86 (1956).

[2] A class of binary signaling alphabets, Bell System Tech. J. **35**, 203—234 (1956). [Имеется перевод: СЛЕПЯН Д. Класс двоичных сигнальных алфавитов. — В кн.: Теория передачи сообщений. — М: ИЛ, 1957, с. 82—113.]

[3] Some further theory of group codes, Bell System Tech. J. **39**, 1219—1252 (1960).

[4] Key Papers in the Development of Information Theory, IEEE Press, New York, 1974.

SLOANE N. J. A. [1] A survey of constructive coding theory, and a table of binary codes of highest known rate, Discrete Math. 3, 265—294 (1972). [Имеется перевод: СЛОЭН Н. ДЖ. А. Обзор конструктивной теории кодирования и таблица двоичных кодов с наибольшими известными скоростями. — В кн.: Кибернетический сборник, нов. сер., вып. 10. — М.: Мир, 1973, с. 5—32.]
[2] Error-correcting codes and cryptography, The Mathematical Gardner (D. A. Klarner, ed.), pp. 346—382, Prindle, Weber & Schmidt, Boston, 1981.
SMALL C. [1] Waring's problem mod n, Amer. Math. Monthly **84**, 12—25 (1977).
[2] Sums of powers in large finite fields, Proc. Amer. Math. Soc. **65**, 35—36 (1977).
[3] Solution of Waring's problem mod n, Amer. Math. Monthly **84**, 356—359 (1977).
SMITH C., HOGGATT V. E., Jr. [1] Primitive periods of generalized Fibonacci sequences, Fibonacci Quart. **14**, 343—347 (1976).
SMITH H. J. S. [1] Report on the theory of numbers. Part II, Report of the British Association for 1860, pp. 120—169; Collected Math. Papers, vol. 1, pp. 93—162, Chelsea, New York, 1965.
SMITH R. A. [1] The circle problem in an arithmetic progression, Canad. Math. Bull. **11**, 175—184 (1968).
[2] The distribution of rational points on hypersurfaces defined over a finite field, Mathematika **17**, 328—332 (1970).
[3] On n-dimensional Kloosterman sums, C. R. Math. Rep. Acad. Sci. Canada **1**, 173—176 (1979).
[4] On n-dimensional Kloosterman sums, J. Number Theory **11**, 324—343 (1979).
[5] A generalization of Kuznietsov's identity for Kloosterman sums, C. R. Math. Rep. Acad. Sci. Canada **2**, 315—320 (1980).
[6] Estimates for exponential sums, Proc. Amer. Math. Soc. **79**, 365—368 (1980).
SMITS T. H. M. [1] On the group of units of $GF(q)[x]/(a(x))$, Indag. Math. **44**, 355—358 (1982).
SNAPPER E. [1] Quadratic spaces over finite fields and codes, J. Combinatorial Theory Ser. A **27**, 263—268 (1979).
SOMER L. [1] Problem E 2377, Amer. Math. Monthly **79**, 906 (1972); Solution, ibid. **81**, 282—283 (1974).
[2] Fibonacci-like groups and periods of Fibonacci-like sequences, Fibonacci Quart. **15**, 35—41 (1977).
[3] The divisibility properties of primary Lucas recurrences with respect to primes, Fibonacci Quart. **18**, 316—334 (1980).
[4] Possible periods of primary Fibonacci-like sequences with respect to a fixed odd prime, Fibonacci Quart. **20**, 311—333 (1982).
SPACKMAN K. W. [1] Simultaneous solutions to diagonal equations over finite fields, J. Number Theory **11**, 100—115 (1979).
[2] On the number and distribution of simultaneous solutions to diagonal congruences, Canad. J. Math. **33**, 421—436 (1981).
SPEISER A. [1] Die Zerlegung von Primzahlen in algebraischen Zahlkörpern, Trans. Amer. Math. Soc. **23**, 173—178 (1922).
SPERBER S. [1] p-adic hypergeometric functions and their cohomology, Duke Math. J. **44**, 535—589 (1977).
[2] Congruence properties of the hyperkloosterman sum, Compositio Math. **40**, 3—33 (1980).
[3] On the L-functions associated with certain exponential sums, J. Number Theory **12**, 141—153 (1980).
SPRINGER T. A. [1] Note on quadratic forms in characteristic 2, Nieuw Arch. Wisk. (3) **10**, 1—10 (1962).
[2] The zeta function of a cuspidal representation of a finite group $GL_n(k)$, Lie Groups and Their Representations (I. M. Gelfand, ed.), pp. 645—648, Akadémiai Kiadó, Budapest, 1975.

[3] Caractères quadratiques de groupes abéliens finis et sommes de Gauss, Colloque sur les Formes Quadratiques (Montpellier, 1975), Bull. Soc. Math. France Suppl. Mém. **48**, 103—115 (1976).

[4] Trigonometric sums, Green functions of finite groups and representations of Weyl groups, Invent. Math. **36**, 173—207 (1976).

SRINIVASAN B. [1] Representations of Finite Chevalley Groups, Lecture Notes in Math., vol. 764, Springer-Verlag, Berlin—Heidelberg—New York, 1979.

STAHNKE W. [1] Primitive binary polynomials, Math. Comp. **27**, 977—980 (1973).

STANLEY T. E. [1] A note on the sequence of Fibonacci numbers, Math. Mag. **44**, 19—22 (1971).

[2] Some remarks on the periodicity of the sequence of Fibonacci numbers, Fibonacci Quart. **14**, 52—54 (1976).

STARK H. M. [1] On the Riemann hypothesis in hyperelliptic function fields, Proc. Symp. Pure Math., vol. 24, pp. 285—302, American Math. Society, Providence, R. I., 1973.

STEINITZ E. [1] Algebraische Theorie der Körper, J. reine angew. Math. **137**, 167—309 (1910).

STEMMLER R. M. [1] The easier Waring problem in algebraic number fields, Acta Arith. **6**, 447—468 (1961).

STEPHENS N. M. [1] On a conjecture of Chowla and Chowla, J. Number Theory **9**, 276—277 (1977).

[2] Dirichlet characters and polynomials, Bull. London Math. Soc. **11**, 52—54 (1979).

STERN M. A. [1] Bemerkungen über höhere Arithmetik, J. reine angew. Math. **6**, 147—158 (1830).

STERN T. E., FRIEDLAND B. [1] Application of modular sequential circuits to single error-correcting p-nary codes, IRE Trans. Information Theory **IT-5**, 114—123 (1959).

STEVENS H. [1] Linear homogeneous equations over finite rings, Canad. J. Math. **16**, 532—538 (1964).

STEVENS H., KUTY L. [1] Applications of an elementary theorem to number theory, Arch. Math. **19**, 37—42 (1968).

STEVENS W. L. [1] The completely orthogonalized Latin square, Ann. of Eugenics **9**, 82—93 (1939).

STICKELBERGER L. [1] Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann. **37**, 321—367 (1890).

[2] Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verhandl. Ersten Intern. Math.-Kongr. (Zürich, 1897), pp. 182—193, Teubner, Leipzig, 1898.

STORER T. [1] Cyclotomy and Difference Sets, Markham, Chicago, 1967.

[2] On the unique determination of the cyclotomic numbers for Galois fields and Galois domains, J. Combinatorial Theory **2**, 296—300 (1967).

[3] Mixed cyclotomy, prime-power circulants, and cyclotomy modulo $p = ef + 1$ for composite e, J. Number Theory **1**, 280—290 (1969).

[4] Extensions of cyclotomic theory, Proc. Symp. Pure Math., vol. 20, pp. 123—134, American Math. Society, Providence, R. I., 1971.

STRASSEN V. [1] Berechnungen in partiellen Algebren endlichen Typs, Computing **11**, 181—196 (1973).

[2] Computational complexity over finite fields, SIAM J. Computing **5**, 324—331 (1976).

STREET A. P., WALLIS W. D. [1] Combinatorial Theory: An Introduction, Charles Babbage Research Centre, Winnipeg, Man., 1977.

STREET A. P., WHITEHEAD E. G., Jr. [1] Sum-free sets, difference sets and cyclotomy, Combinatorial Mathematics (D. A. Holton, ed.), Lecture Notes in Math., vol. 403, pp. 109—124, Springer-Verlag, Berlin—Heidelberg—New York, 1974.

SUGIMOTO E. [1] A short note on new indexing polynomials of finite fields, Information and Control **41**, 243—246 (1979).
SUGIYAMA Y. KASAHARA M., HIRASAWA S., NAMEKAWA T. [1] A method for solving key equation for decoding Goppa codes, Information and Control **27**, 87—99 (1975).
[2] Further results on Goppa codes and their applications for constructing efficient binary codes, IEEE Trans. Information Theory **IT-22**, 518—526 (1976).
SURBÖCK F., WEINRICHTER H. [1] Interlacing properties of shift-register sequences with generator polynomials irreducible over $GF(p)$, IEEE Trans. Information Theory **IT-24**, 386—389 (1978).
SWAN R. G. [1] Factorization of polynomials over finite fields, Pacific J. Math. **12**, 1099—1106 (1962).
SWIFT J. D. [1] Construction of Galois fields of characteristic two and irreducible polynomials, Math. Comp. **14**, 99—103 (1960).
SWINNERTON-DYER H. P. F. [1] The conjectures of Birch and Swinnerton-Dyer, and of Tate, Proc. Conf. Local Fields (Driebergen, 1966), pp. 132—157, Springer-Verlag, Berlin—Heidelberg—New York, 1967.
[2] The zeta function of a cubic surface over a finite field, Proc. Cambridge Philos. Soc. **63**, 55—71 (1967).
[3] Applications of algebraic geometry to number theory, Proc. Symp. Pure Math., vol. 20, pp. 1—52, American Math. Society, Providence, R. I., 1971.
SZALAY M. [1] On the distribution of primitive roots mod p (Hungarian), Mat. Lapok **21**, 357—362 (1970).
[2] On the distribution of the primitive roots of a prime, J. Number Theory **7**, 184—188 (1975).
SZÉKELY I., MUREŞAN T. [1] Interpolation with respect to a prime modulus (Romanian), Bul. Sti. Inst. Politehn. Cluj **8**, 105—109 (1965).
SZELE T. [1] An elementary proof of the fundamental theorem for finite fields (Hungarian), Mat. Lapok **7**, 249—254 (1956).
SZYMICZEK K. [1] Sums of powers of generators of a finite field, Colloq. Math. **20**, 59—63 (1969).
TÄCKLIND S. [1] Über die Periodizität der Lösungen von Differenzenkongruenzen, Ark. Mat. Astr. Fys. **30A**, not. 22 (1944).
TAKAHASHI I. [1] Switching functions constructed by Galois extension fields, Information and Control **48**, 95—108 (1981).
TAMARKINE J., FRIEDMANN A. [1] Sur les congruences du second degré et les nombres de Bernoulli, Mat. Ann. **62**, 409—412 (1906).
TANAKA H., KASAHARA M., TEZUKA Y., KASAHARA Y. [1] Computation over Galois fields using shiftregisters, Information and Control 13,75—84(1968).
TANIYAMA Y. [1] Distribution of positive 0-cycles in absolute classes of an algebraic variety with finite constant field, Sci. Papers Coll. Gen. Ed. Univ. Tokyo **8**, 123—137 (1958).
TANNER H. W. L. [1] On the binomial equation $x^p - 1 = 0$: Quinquisection, Proc. London Math. Soc. **18**, 214—234 (1887).
[2] On some square roots of unity for a prime modulus, Messenger of Math. (2) **21**, 139—144 (1892).
[3] On complex primes formed with the fifth roots of unity, Proc. London Math. Soc. **24**, 223—272 (1893).
TARRY G. [1] Le problème des 36 officiers, C. R. Assoc. Francaise Avancement Sci. Nat. **1**, 122—123 (1900); ibid. **2**, 170—203 (1901).
TATE J. [1] Algebraic cycles and poles of zeta functions, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), pp. 93—110, Harper and Row, New York, 1965.
[2] The arithmetic of elliptic curves, Invent. Math. **23**, 179—206 (1974).

TAUSWORTHE R. C. [1] Random numbers generated by linear recurrence modulo two, Math. Comp. **19**, 201—209 (1965). [Имеется перевод: ТАУСВОРТ Р. Случайные числа, порождаемые линейными рекуррентными соотношениями по модулю 2 — В кн.: Кибернетический сборник, нов. сер., вып. 16. — М.: Мир, 1979, с. 62—79.]
TAYLOR D. E. [1] Some classical theorems on division rings, L'Enseignement Math. (2) **20**, 293—298 (1974).
TAYLOR M. J. [1] Local Gauss sums, Sém. Théorie des Nombres 1978—79, Exp. 8, Univ. Bordeaux I, Talence, 1979.
[2] Adams operations, local root numbers, and the Galois module structure of rings of integers, Proc. London Math. Soc. (3) **39**, 147—175 (1979).
TAZAWA M. [1] A theorem on congruence, Tôhoku Math. J. **32**, 354—356 (1930).
TEICHMÜLLER O. [1] Differentialrechnung bei Charakteristik p, J. reine angew. Math. **175**, 89—99 (1936).
TERJANIAN G. [1] Sur les corps finis, C. R. Acad. Sci. Paris Sér. A **262**, 167—169 (1966).
THAYSE A. [1] Differential calculus for functions from $(GF(p))^n$ into $GF(p)$, Phillips Res. Rep. **29**, 560—586 (1974).
THOMAS A. D. [1] Zeta-Functions: An Introduction to Algebraic Geometry, Research Notes in Math., no. 12, Pitman, London, 1977.
THOUVENOT S. [1] Propriétés arithmétiques déductibles d'une présentation simplifiée de la formule du binome, C. R. Acad. Sci. Paris **254**, 1550—1552 (1962).
THOUVENOT S., CHÂTELET F. [1] Au sujet des congruences de degré supérieur à deux, L'Enseignement Math. (2) **13**, 89—98 (1967).
TIETÄVÄINEN A. [1] On the non-trivial solvability of some systems of equations in finite fields, Ann. Univ. Turku Ser. AI **71** (1964).
[2] On the non-trivial solvability of some equations and systems of equations in finite fields, Ann. Acad. Sci. Fenn. Ser. AI **360** (1965).
[3] On systems of linear and quadratic equations in finite fields, Ann. Acad. Sci. Fenn. Ser. AI **382** (1965).
[4] On the trace of a polynomial over a finite field, Ann. Univ. Turku Ser. AI **87** (1966).
[5] On non-residues of a polynomial, Ann. Univ. Turku Ser. AI **94** (1966).
[6] On systems of equations in finite fields, Ann. Acad. Sci. Fenn. Ser. AI **386** (1966).
[7] On the solvability of equations in incomplete finite fields, Ann. Univ. Turku Ser. AI **102** (1967).
[8] On pairs of additive equations, Ann. Univ. Turku Ser. AI **112** (1967).
[9] On diagonal forms over finite fields, Ann. Univ. Turku Ser. AI **118**, no. 1 (1968).
[10] On the distribution of the residues of a polynomial, Ann. Univ. Turku Ser. AI **120** (1968).
[11] On a homogeneous congruence of odd degree, Ann. Univ. Turku Ser. AI **131** (1969).
[12] On a problem of Chowla and Shimura, J. Number Theory **3**, 247—252 (1971).
[13] Note on Waring's problem (mod p), Ann. Acad. Sci. Fenn. Ser. AI **554** (1973).
[14] On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math. **24**, 88—96 (1973).
[15] A short proof for the nonexistence of unknown perfect codes over $GF(q)$, $q > 2$, Ann. Acad. Sci. Fenn. Ser. AI **580** (1974).
[16] Proof of a conjecture of S. Chowla, J. Number Theory **7**, 353—356 (1975).
TIETZE U. P. [1] Zur Theorie quadratischer Formen über Körpern der Charakteristik 2, J. reine angew. Math. **268/269**, 388—390 (1974).
TONELLI A. [1] Bemerkung über die Auflösung quadratischer Congruenzen, Göttinger Nachr. **1891**, 344—346.
TORNHEIM L. [1] Sums of n-th powers in fields of prime characteristic, Duke Math. J. **4**, 359—362 (1938).

T'U K. C. [1] The structure of Q-matrices and the reducibility of polynomials over a Galois field (Chinese), Acta Math. Sinica **17**, 46—59 (1974).
[2] Canonical forms of a class of ternary forms over GF (2) (Chinese), Acta Math. Sinica **23**, 1—10 (1980).
TURYN R. [1] Sequences with small correlation, Error Correcting Codes (H. B. Mann, ed.), pp. 195—228, Wiley, New York, 1968.
UCHIYAMA S. [1] Sur les polynômes irréductibles dans un corps fini. I, Proc. Japan Acad. **30**, 523—527 (1954).
[2] Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini, Proc. Japan Acad. **30**, 930—933 (1954).
[3] Note on the mean value of $V(f)$, Proc. Japan Acad. **31**, 199—201 (1955).
[4] Sur les polynômes irréductibles dans un corps fini. II, Proc. Japan Acad. **31**, 267—269 (1955).
[5] Note on the mean value of $V(f)$. II, Proc. Japan Acad. **31**, 321—323 (1955).
[6] Note on the mean value of $V(f)$. III, Proc. Japan Acad. **32**, 97—98 (1956).
[7] On a multiple exponential sum, Proc. Japan Acad. **32**, 748—749 (1956).
[8] On a conjecture of K. S. Williams, Proc. Japan Acad. **46**, 755—757 (1970).
ULBRICH K.-H. [1] Über Endomorphismen, deren Minimalpolynom mit dem charakteristischen Polynom übereinstimmt, J. reine angew. Math. **299/300**, 385—387 (1978).
URBANEK F. J. [1] An O (log n) algorithm for computing the nth element of the solution of a difference equation, Inform. Process. Lett. **11**, no. 2, 66—67 (1980).
USPENSKY J. V., HEASLET M. A. [1] Elementary Number Theory, McGraw-Hill, New York, 1939.
VAIDA D. [1] L'emploi des imaginaires de Galois dans la théorie des mécanismes automatiques. VI (Romanian. French summary), Acad. R. P. Romîne. Bul. Sti. Sect. Mat. Fiz. **8**, 21—29 (1956).
VAIDYANATHASWAMY R. [1] The quadratic reciprocity of polynomials modulo p, J. Indian Math. Soc. **17**, 185—196 (1928).
[2] The algebra of cubic residues, J. Indian Math. Soc. (N. S.) **21**, 57—66 (1957).
VAJDA S. [1] Patterns and Configurations in Finite Spaces, Hafner, New York, 1967.
[2] The Mathematics of Experimental Design, Hafner, New York, 1967.
VAN DER CORPUT J. G. [1] Sur un certain système de congruences. I, II, Indag. Math. **1**, 168—176, 254—259 (1939).
VAN DER WAERDEN B. L. [1] Noch eine Bemerkung zu der Arbeit «Zur Arithmetik der Polynome» von U. Wegner in Math. Ann. 105, S. 628—631, Math. Ann. **109**, 679—680 (1934).
[2] Algebra, vol. 1, 7th ed., Springer-Verlag, Berlin—Heidelberg—New York, 1966. [Имеется перевод 8-го издания (1971): ВАН ДЕР ВАРДЕН Б. Л. Алгебра. — М.: Наука, 1979, с. 15—296.]
[3] Algebra, vol. 2, 5th ed., Springer-Verlag, Berlin—Heidelberg—New York, 1967. [Имеется перевод: ВАН ДЕР ВАРДЕН Б. Л. Алгебра. — М.: Наука, 1979, с. 297—607.]
VAN DE VOOREN-VAN VEEN J. [1] On the number of irreducible equations of degree n in $GF(p)$ and the decomposability of the cyclotomic polynomials in $GF(p)$ (Dutch), Simon Stevin **31**, 80—82 (1957).
VANDIVER H. S. [1] Note on trinomial congruences and the first case of Fermat's last theorem, Ann. of Math. (2) **27**, 54—56 (1925).
[2] Algorithms for the solution of the quadratic congruence, Amer. Math. Monthly **36**, 83—86 (1929).
[3] Some theorems in finite field theory with applications to Fermat's last theorem, Proc. Nat. Acad. Sci. U. S. A. **30**, 362—367 (1944).
[4] On trinomial congruences and Fermat's last theorem, Proc. Nat. Acad. Sci. U. S. A. **30**, 368—370 (1944).
[5] New types of relations in finite field theory. I, II, Proc. Nat. Acad. Sci.

U. S. A. **31**, 50—54, 189—194 (1945).
[6] On the number of solutions of certain non-homogeneous trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **31**, 170—175 (1945).
[7] On the number of solutions of some general types of equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **32**, 47—52 (1946).
[8] On classes of diophantine equations of higher degrees which have no solutions, Proc. Nat. Acad. Sci. U. S. A. **32**, 101—106 (1946).
[9] Cyclotomy and trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **32**, 317—319 (1946).
[10] On some special trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **32**, 320—326 (1946).
[11] Limits for the number of solutions of certain general types of equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **33**, 236—242 (1947).
[12] Applications of cyclotomy to the theory of nonhomogeneous equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **34**, 62—66 (1948).
[13] Congruence methods as applied to diophantine analysis, Math. Mag. **21**, 185—192 (1948).
[14] Cyclotomic power characters and trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **34**, 196—203 (1948).
[15] Quadratic relations involving the numbers of solutions of certain types of equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **35**, 681—685 (1949).
[16] On a generalization of a Jacobi exponential sum associated with cyclotomy, Proc. Nat. Acad. Sci. U. S. A. **36**, 144—151 (1950).
[17] On cyclotomy and extensions of Gaussian type quadratic relations involving numbers of solutions of conditional equations in finite fields, Proc. Nat. Acad. Sci. U. S. A. **38**, 981—991 (1952).
[18] New types of trinomial congruence criteria applying to Fermat's last theorem, Proc. Nat. Acad. Sci. U. S. A. **40**, 248—252 (1954).
[19] On trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **40**, 1008—1010 (1954).
[20] On the properties of certain trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **41**, 651—653 (1955).
[21] Relation of the theory of certain trinomial equations in a finite field to Fermat's last theorem, Proc. Nat. Acad. Sci. U. S. A. **41**, 770—775 (1955).
[22] On cyclotomic relations and trinomial equations in a finite field, Proc. Nat. Acad. Sci. U. S. A. **41**, 775—780 (1955).
[23] Diophantine equations in certain rings, Proc. Nat. Acad. Sci. U. S. A. **42**, 656—665 (1956); Errata, ibid. **43**, 252—253 (1957).
[24] The rapid computing machine as an instrument in the discovery of new relations in the theory of numbers, Proc. Nat. Acad. Sci. U. S. A. **44**, 459—464 (1958).
[25] On distribution problems involving the number of solutions of certain trinomial congruences, Proc. Nat. Acad. Sci. U. S. A. **45**, 1635—1641 (1959).

VAN LINT J. H. [1] Coding Theory, Lecture Notes in Math., vol. 201, Springer-Verlag, Berlin—Heidelberg—New York, 1971.
[2] Combinatorial Theory Seminar Eindhoven University of Technology, Lecture Notes in Math., vol. 382, Springer-Verlag, Berlin—Heidelberg—New York, 1974.
[3] Recent results on perfect codes and related topics, Combinatorics, Part 1: Theory of Designs, Finite Geometry and Coding Theory, Math. Centre Tracts, no. 55, pp. 158—178, Math. Centrum, Amsterdam, 1974.
[4] A survey of perfect codes, Rocky Mountain J. Math. **5**, 199—224 (1975).

VAN LINT J. H., RYSER H. J. [1] Block designs with repeated blocks, Discrete Math. **3**, 381—396 (1972).

VAN METER R. G. [1] The number of solutions of certain systems of equations in a finite field, Duke Math. J. **38**, 365—377 (1971).

[2] Generalized k-linear equations over a finite field, Math. Nachr. **53**, 63—67 (1972).

[3] The number of solutions of certain equations over a finite field, Portugal. Math. **32**, 119—124 (1973).

VARNUM E. C. [1] Polynomial determination in a field of integers modulo p, J. Computing Systems **1**, 57—70 (1953).

VAUGHAN R. C. [1] The Hardy—Littlewood Method, Cambridge Univ. Press, Cambridge, 1981.

VAUGHAN T. P. [1] Polynomials and linear transformations over finite fields, J. reine angew. Math. **267**, 179—206 (1974).

[2] Linear transformations of a finite field, Linear Algebra Appl. **8**, 413—426 (1974).

VEBLEN O., BUSSEY W. H. [1] Finite projective geometries, Trans. Amer. Math. Soc. **7**, 241—259 (1906).

VEBLEN O., WEDDERBURN J. H. M. [1] Non-Desarguesian and non-Pascalian geometries, Trans. Amer. Math. Soc. **8**, 379—388 (1907).

VEBLEN O., YOUNG J. W. [1] Projective Geometry, 2 vols., Ginn & Co., Boston, 1938.

VEGH E. [1] Pairs of consecutive primitive roots modulo a prime, Proc. Amer. Math. Soc. **19**, 1169—1170 (1968).

[2] Primitive roots modulo a prime as consecutive terms of an arithmetic progression, J. reine angew. Math. **235**, 185—188 (1969).

[3] Arithmetic progressions of primitive roots of a prime. II, J. reine angew. Math. **244**, 108—111 (1970).

[4] A new condition for consecutive primitive roots of a prime, Elemente der Math. **25**, 113 (1970).

[5] A note on the distribution of the primitive roots of a prime, J. Number Theory **3**, 13—18 (1971).

[6] Arithmetic progressions of primitive roots of a prime. III, J. reine angew. Math. **256**, 130—137 (1972).

VENKATARAYUDU T. [1] The algebra of the eth power residues, J. Indian Math. Soc. **3**, 73—81 (1938).

VERNER L. [1] A singular series in characteristic p, Bull. Acad. Polon. Sci. Sér. Sci. Math. **26**, 957—961 (1978).

[2] A singular series in characteristic p, Bull. Acad. Polon. Sci. Sér. Sci. Math. **27**, 147—151 (1979).

VILANOVA K. [1] О некоторых трехчленных уравнениях над конечными полями. Труды Универс. Дружбы народов, т. 21, № 2, 1967, с. 17—31.

VINCE A. [1] The Fibonacci sequence modulo N, Fibonacci Quart. **16**, 403—407 (1978).

[2] Period of a linear recurrence, Acta Arith. **39**, 303—311 (1981).

VINSON J. [1] The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence, Fibonacci Quart. **1**, no. 2, 37—45 (1963).

VIRY G. [1] Factorisation des polynômes à plusieurs variables à coefficients entiers, RAIRO Inform. Théor. **12**, 305—318 (1978).

[2] Factorisation des polynômes à plusieurs variables, RAIRO Inform. Théor. **14**, 209—223 (1980).

VOGT W. G., BOSE N. K. [1] A method to determine whether two polynomials are relatively prime, IEEE Trans. Automatic Control **AC-15**, 379—380 (1970).

VON AMMON U., TRÖNDLE K. [1] Mathematische Grundlagen der Codierung, Oldenbourg, Munich, 1974.

VON GROSSCHMID L. [1] Generalization of a theorem of Lagrange. Contribution to the theory of the distribution of quadratic residues (Hungarian), Math. és Termész. Ért. **36**, 165—191 (1918).

VON NEUMANN J., GOLDSTINE H. H. [1] A numerical study of a conjecture of Kummer, Math. Tables Aids Comput. **7**, 133—134 (1953).

VON SCHRUTKA L. [1] Ein Beweis für die Zerlegbarkeit der Primzahlen von der Form $6n + 1$ in ein einfaches und ein dreifaches Quadrat, J. reine angew. Math. **140**, 252—265 (1911).

VON STERNECK R. D. [1] Über die Anzahl inkongruenter Werte, die eine ganze Funktion dritten Grades annimmt, Sitzungsber. Wien Abt. II, **116**, 895—904 (1907).

WADE L. I. [1] Certain quantities transcendental over $GF(p^n, x)$. I, II, Duke Math. J. **8**, 701—720 (1941); ibid. **10**, 587—594 (1943).

[2] Remarks on the Carlitz ψ-functions, Duke Math. J. **13**, 71—78 (1946).

[3] Transcendence properties of the Carlitz ψ-functions, Duke Math. J. **13**, 79—85 (1946).

WAGNER C. G. [1] On the factorization of some polynomial analogues of binomial coefficients, Arch. Math. **24**, 50—52 (1973).

[2] Linear pseudo-polynomials over $GF[q, x]$, Arch. Math. **25**, 385—390 (1974).

[3] Polynomials over $GF(q, x)$ with integral-valued differences, Arch. Math. **27**, 495—501 (1976).

WALKER G. L. [1] Fermat's theorem for algebras, Pacific J. Math. **4**, 317—320 (1954).

WALL D. D. [1] Fibonacci series modulo m, Amer. Math. Monthly **67**, 525—532 (1960).

WALLIS W. D., STREET A. P., WALLIS J. S. [1] Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Lecture Notes in Math., vol. 292, Springer-Verlag, Berling—Heidelberg—New York, 1972.

WALUM H. [1] Some averages of character sums, Pacific J. Math. **16**, 189—192 (1966).

WAMSLEY J. W. [1] On a condition for commutativity of rings, J. London Math. Soc. (2) **4**, 331—332 (1971).

WAN Z., YANG B. [1] Notes on finite geometries and the construction of PBIB designs. III. Some «Anzahl» theorems in unitary geometry over finite fields and their applications, Sci. Sinica **13**, 1006—1007 (1964).

[2] Studies in finite geometries and the construction of incomplete block designs. III. Some «Anzahl» theorems in unitary geometry over finite fields and their applications (Chinese), Acta Math. Sinica **15**, 533—544 (1965); Chinese Math. Acta **7**, 252—264 (1965).

WANG P. S. [1] Factoring multivariate polynomials over algebraic number fields, Math. Comp. **30**, 324—336 (1976).

[2] An improved multivariate polynomial factoring algorithm, Math. Comp. **32**, 1215—1231 (1978).

WANG P. S., ROTHSCHILD L. P. [1] Factoring multivariate polynomials over the integers, Math. Comp. **29**, 935—950 (1975).

WANG Y. [1] A note on the least primitive root of a prime, Sci. Record (N. S.) **3** 174—179 (1959).

[2] On the least primitive root of a prime (Chinese), Acta Math. Sinica **9**, 432—441 (1959); Sci. Sinica **10**, 1—14 (1961).

[3] Estimation and application of character sums (Chinese), Shuxue Jinzhan **7** 78—83 (1964).

WARD M. [1] The algebra of recurring series, Ann. of Math. (2) **32**, 1—9 (1931)

[2] The characteristic number of a sequence of integers satisfying a linear recursion relation, Trans. Amer. Math. Soc. **33**, 153—165 (1931).

[3] The distribution of residues in a sequence satisfying a linear recursion relation, Trans. Amer. Math. Soc. **33**, 166—190 (1931).

[4] Some arithmetical properties of sequences satisfying a linear recursion relation, Ann. of Math. (2) **32**, 734—738 (1931).

[5] The arithmetical theory of linear recurring series, Trans. Amer. Math. Soc. **35** 600—628 (1933).

[6] Note on the period of a mark in a finite field, Bull. Amer. Math. Soc **40**, 279—281 (1934).

[7] An arithmetical property of recurring series of the second order, Bull. Amer. Math. Soc. **40**, 825—828 (1934).
[8] Note on an arithmetical property of recurring series, Math. Z. **39**, 211—214 (1935).
[9] An enumerative problem in the arithmetic of linear recurring series, Trans. Amer. Math. Soc. **37**, 435—440 (1935).
[10] On the factorization of polynomials to a prime modulus, Ann. of Math. (2) **36**, 870—874 (1935).
[11] The null divisors of linear recurring series, Duke Math. J. **2**, 472—476 (1936).
[12] Linear divisibility sequences, Trans. Amer. Math. Soc. **41**, 276—286 (1937).
[13] Arithmetic functions on rings, Ann. of Math. (2) **38**, 725—732 (1937).
[14] The law of apparition of primes in a Lucasian sequence, Trans. Amer. Math. Soc. **44**, 68—86 (1938).
[15] Arithmetical properties of sequences in rings, Ann. of Math. (2) **39**, 210—219 (1938).
[16] Memoir on elliptic divisibility sequences, Amer. J. Math. **70**, 31—74 (1948).
WARNING E. [1] Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, Abh. Math. Sem. Univ. Hamburg **11**, 76—83 (1936).
WATERHOUSE W. C. [1] Abelian varieties over finite fields, Ann. Sci. Ecole Norm. Sup. (4) **2**, 521—560 (1969).
[2] The sign of the Gaussian sum, J. Number Theory **2**, 363 (1970).
[3] The normal basis theorem, Amer. Math. Monthly **86**, 212 (1979).
WATERHOUSE W. C., MILNE J. S. [1] Abelian varieties over finite fields, Proc. Symp. Pure Math., vol. 20, pp. 53—64, American Math. Society, Providence, R. I., 1971.
WATSON E. J. [1] Primitive polynomials (mod 2), Math. Comp. **16**, 368 (1962).
WATSON G. L. [1] Cubic congruences, Mathematika **11**, 142—150 (1964).
WEBB W. A. [1] On the representation of polynomials over finite fields as sums of powers and irreducibles, Rocky Mountain J. Math. **3**, 23—29 (1973).
[2] Numerical results for Waring's problem in $GF[q, x]$, Math. Comp. **27**, 193—196 (1973).
[3] Waring's problem in $GF[q, x]$, Acta Arith. **22**, 207—220 (1973).
[4] Uniformly distributed functions in $GF[q, x]$ and $GF\{q, x\}$, Ann. Mat. Pura Appl. (4) **95**, 285—291 (1973).
WEBB W. A., LONG C. T. [1] Distribution modulo p^h of the general linear second order recurrence, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **58**, 92—100 (1975).
WEBER H. [1] Ueber die mehrfachen Gaussischen Summen, J. reine angew. Math. **74**, 14—56 (1872).
[2] Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist, Math. Ann. **20**, 301—329 (1882).
[3] Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie, Math. Ann. **43**, 521—549 (1893).
[4] Lehrbuch der Algebra, vol. 1, Vieweg, Braunschweig, 1895.
[5] Lenrbuch der Algebra, vol. 2, Vieweg, Braunschweig, 1896.
[6] Über Abel's Summation endlicher Differenzenreihen, Acta Math. **27**, 225—233 (1903).
WEDDERBURN J. H. M. [1] A theorem on finite algebras, Trans. Amer. Math. Soc. **6**, 349—352 (1905).
WEGNER U. [1] Über die ganzzahligen Polynome, die für unendlich viele Primzahlmoduln Permutationen liefern. Dissertation, Berlin, 1928.
[2] Über ein algebraisches Problem, Math. Ann. **105**, 779—785 (1931).
[3] Über einen Satz von Dickson, Math. Ann. **105**, 790—792 (1931).
[4] Über das Verhalten der Potenzsummen der Wurzeln einer algebraischen Gleichung hinsichtlich ihrer Gruppe, J. reine angew. Math. **173**, 185—190 (1935).

WEIL A. [1] Sur les fonctions algébriques à corps de constantes fini, C. R. Acad. Sci. Paris **210**, 592—594 (1940).
[2] On the Riemann hypothesis in function fields, Proc. Nat. Acad. Sci. U. S. A. **27**, 345—347 (1941).
[3] Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. Ind., no. 1041, Hermann, Paris, 1948.
[4] Variétés abéliennes et courbes algébriques, Actualités Sci. Ind., no. 1064, Hermann, Paris, 1948.
[5] On some exponential sums, Proc. Nat. Acad. Sci. U. S. A. **34**, 204—207 (1948).
[6] Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc. **55**, 497—508 (1949).
[7] Jacobi sums as «Grössencharaktere», Trans. Amer. Math. Soc. **73**, 487—495 (1952).
[8] Footnote to a recent paper, Amer. J. Math. **76**, 347—350 (1954).
[9] Abstract versus classical algebraic geometry, Proc. International Congress of Math. (Amsterdam, 1954), vol. 3, pp. 550—558, North-Holland, Amsterdam, 1956.
[10] Sommes de Jacobi et caractères de Hecke, Göttinger Nachr. **1974**, 1—14.
[11] La cyclotomie jadis et naguère, L'Enseignement Math. (2) **20**, 247—263 (1974).
WEINBERGER P. J., ROTHSCHILD L. P. [1] Factoring polynomials over algebraic number fields, ACM Trans. Math. Software **2**, 335—350 (1976).
WEINSTEIN L. [1] The hyper-Kloosterman sum, L'Enseignement Math. (2) **27**, 29—40 (1981).
WEISSINGER J. [1] Theorie der Divisorenkongruenzen, Abh. Math. Sem. Univ. Hamburg **12**, 115—126 (1938).
WELCH L. R., SCHOLTS R. A. [1] Continued fractions and Berlekamp's algorithm, IEEE Trans. Information Theory **IT-25**, 19—27 (1979).
WELLS C. [1] Groups of permutation polynomials, Monatsh. Math. **71**, 248—262 (1967).
[2] The number of solutions of a system of equations in a finite field, Acta Arith. **12**, 421—424 (1967).
[3] A generalization of the regular representation of finite abelian groups, Monatsh, Math. **72**, 152—156 (1968).
[4] Generators for groups of permutation polynomials over finite fields, Acta Sci. Math. Szeged **29**, 167—176 (1968).
[5] The degrees of permutation polynomials over finite fields, J. Combinatorial Theory **7**, 49—55 (1969).
[6] Polynomials over finite fields which commute with translations, Proc. Amer. Math. Soc. **46**, 347—350 (1974).
WELLS J., MUSKAT J. B. [1] On the number of solutions of certain trinomial congruences, Math. Comp. **19**, 483—487 (1965).
WENDT E. [1] Arithmetische Studien über den «letzten» Fermatschen Satz, welcher aussagt, dass die Gleichung $a^n = b^n + c^n$ für $n > 2$ in ganzen Zahlen nicht auflösbar ist, J. reine angew. Math. **113**, 335—347 (1894).
WENG L.-J. [1] Decomposition of m-sequences and its applications, IEEE Trans. Information Theory **IT-17**, 457—463 (1971).
WERTHEIM G. [1] Anfangsgründe der Zahlenlehre, Vieweg, Braunschweig, 1902.
WESSELKAMPER T. C. [1] Divided difference methods for Galois switching functions, IEEE Trans. Computers **C-27**, 232—238 (1978).
[2] The algebraic representation of partial functions, Discrete Appl. Math. **1**, 137—142 (1979).
[3] The algebraic representation of partial functions, Proc. Ninth Internat. Symp. on Multiple-Valued Logic (Bath. 1979), pp. 290—293, IEEE, Long Beach, Cal., 1979.
WESTERN A. E. [1] An extension of Eisenstein's law of reciprocity. I, II, Proc. London Math. Soc. (2) **6**, 16—28, 265—297 (1908).

[2] Some criteria for the residues of eighth and other powers, Proc. London Math. Soc. (2) **9**, 244—272 (1911).
WESTERN A. E., MILLER J. C. P. [1] Tables of Indices and Primitive Roots, Royal Soc. Math. Tables, vol. 9, Cambridge Univ. Press, London, 1968.
WHAPLES G. [1] Additive polynomials, Duke Math. J. **21**, 55—65 (1954).
WHITEMAN A. L. [1] On a theorem of higher reciprocity, Bull. Amer. Math. Soc. **43**, 567—572 (1937).
[2] A note on Kloosterman sums, Bull. Amer. Math. Soc. **51**, 373—377 (1945).
[3] Theorems analogous to Jacobsthal's theorem, Duke Math. J. **16**, 619—626 (1949).
[4] Theorems on quadratic partitions, Proc. Nat. Acad. Sci. U. S. A. **36**, 60—66 (1950).
[5] Finite Fourier series and cyclotomy, Proc. Nat. Acad. Sci. U. S. A. **37**, 373—378 (1951).
[6] Cyclotomy and Jacobsthal sums, Amer. J. Math. **74**, 89—99 (1952).
[7] Finite Fourier series and equations in finite fields, Trans. Amer. Math. Soc. **74**, 78—98 (1953).
[8] The sixteenth power residue character of 2, Canad. J. Math. **6**, 364—373 (1954).
[9] The cyclotomic numbers of order sixteen, Trans. Amer. Math. Soc. **86**, 401—413 (1957).
[10] The cyclotomic numbers of order twelve, Acta Arith. **6**, 53—76 (1960).
[11] The cyclotomic numbers of order ten, Proc. Symp. Appl. Math., vol. 10, pp. 95—111, American Math. Society, Providence, R. I., 1960.
[12] A family of difference sets, Illinois J. Math. **6**, 107—121 (1962).
[13] A theorem of Brewer on character sums, Duke Math. J. **30**, 545—552 (1963).
[14] Theorems on Brewer and Jacobsthal sums. I, Proc. Symp. Pure Math., vol. 8, pp. 44—55, American Math. Society, Providence, R. I., 1965.
[15] Theorems on Brewer and Jacobsthal sums. II, Michigan Math. J. **12**, 65—80 (1965).
WHYBURN C. T. [1] The distribution of r-th powers in finite fields, J. reine angew. Math. **245**, 183—187 (1970).
[2] An elementary note on character sums, Duke Math. J. **37**, 307—310 (1970).
WILEY F. B. [1] Proof of the finiteness of the modular covariants of a system of binary forms and cogredient points, Trans. Amer. Math. Soc. **15**, 431—438 (1914).
WILLETT M. [1] The minimum polynomial for a given solution of a linear recursion, Duke Math. J. **39**, 101—104 (1972).
[2] The index of an m-sequence, SIAM J. Appl. Math. **25**, 24—27 (1973).
[3] On a theorem of Kronecker, Fibonacci Quart. **14**, 27—29 (1976).
[4] Characteristic m-sequences, Math. Comp. **30**, 306—311 (1976).
[5] Factoring polynomials over a finite field, SIAM J. Appl. Math. **35**, 333—337 (1978).
[6] Arithmetic in a finite field, Math. Comp. **35**, 1353—1359 (1980).
WILLIAMS H. C. [1] Some algorithms for solving $x^q \equiv N \pmod{p}$, Proc. Third Southeastern Conf. on Combinatorics, Graph Theory, and Computing (Boca Raton, Fla., 1972), pp. 451—462, Utilitas Math., Winnipeg, Man., 1972.
[2] Primality testing on a computer, Ars Combinatoria **5**, 127—185 (1978).
WILLIAMS H. C., ZARNKE C. R. [1] Some algorithms for solving a cubic congruence modulo p, Utilitas Math. **6**, 285—306 (1974).
WILLIAMS K. S. [1] On the number of solutions of a congruence, Amer. Math. Monthly **73**, 44—49 (1966).
[2] On the least non-residue of a quartic polynomial, Proc. Cambridge Philos. Soc. **62**, 429—431 (1966).
[3] Eisenstein's criteria for absolute irreducibility over a finite field, Canad. Math. Bull. **9**, 575—580 (1966).
[4] On general polynomials, Canad. Math. Bull. **10**, 579—583 (1967).
[5] On extremal polynomials, Canad. Math. Bull. **10**, 585—594 (1967).

[6] Pairs of consecutive residues of polynomials, Canad. J. Math. **19**, 655—666 (1967).
[7] A sum of fractional parts, Amer. Math. Monthly **74**, 978—980 (1967).
[8] Note on pairs of consecutive residues of polynomials, Canad. Math. Bull. **11**, 79—83 (1968).
[9] On exceptional polynomials, Canad. Math. Bull. **11**, 279—282 (1968).
[10] Quadratic polynomials with the same residues, Amer. Math. Monthly **75**, 969—973 (1968).
[11] Polynomials with irreducible factors of specified degree, Canad. Math. Bull. **12**, 221—223 (1969).
[12] Small solutions of the congruence $ax^2 + by^2 \equiv c \pmod{k}$, Canad. Math. Bull. **12**, 311—320 (1969).
[13] On two conjectures of Chowla, Canad. Math. Bull. **12**, 545—565 (1969).
[14] Note on factorable polynomials, Canad. Math. Bull. **12**, 589—595 (1969).
[15] Distinct values of a polynomial in subsets of a finite field, Canad. J. Math. **21**, 1483—1488 (1969).
[16] Finite transformation formulae involving the Legendre symbol, Pacific J. Math. **34**, 559—568 (1970).
[17] On a result of Libri and Lebesgue, Amer. Math. Monthly **77**, 610—613 (1970).
[18] A distribution property of the solutions of a congruence modulo a large prime, J. Number Theory **3**, 19—32 (1971).
[19] Note on the Kloosterman sum, Proc. Amer. Math. Soc. **30**, 61—62 (1971).
[20] A class of character sums, J. London Math. Soc. (2) **3**, 67—72 (1971).
[21] On Salié's sum, J. Number Theory **3**, 316—317 (1971).
[22] Note on Salié's sum, Proc. Amer. Math. Soc. **30**, 393—394 (1971).
[23] Small solutions of the congruence $a_1x_1^{l_1} + a_2x_2^{l_2} + a_0 \equiv 0 \pmod{p}$, Proc. Cambridge Philos. Soc. **70**, 409—412 (1971).
[24] Note on the number of solutions of $f(x_1) = f(x_2) = \ldots = f(x_r)$ over a finite field, Canad. Math. Bull. **14**, 429—432 (1971).
[25] Note on Dickson's permutation polynomials, Duke Math. J. **38**, 659—665 (1971).
[26] Products of polynomials over a finite field, Delta (Waukesha) **3**, no. 2, 35—37 (1972).
[27] Exponential sums over $GF(2^n)$, Pacific J. Math. **40**, 511—519 (1972).
[28] The Kloosterman sum revisited, Canad. Math. Bull. **16**, 363—365 (1973).
[29] Elementary treatment of quadratic partition of primes $p \equiv 1 \pmod{7}$, Illinois J. Math. **18**, 608—621 (1974).
[30] Note on a cubic character sum, Aequationes Math. **12**, 229—231 (1975).
[31] On Euler's criterion for cubic nonresidues, Proc. Amer. Math. Soc. **49**, 277—283 (1975).
[32] Note on cubics over $GF(2^n)$ and $GF(3^n)$, J. Number Theory **7**, 361—365 (1975).
[33] Note on a result of Kaplan, Proc. Amer. Math. Soc. **56**, 34—36 (1976).
[34] A rational octic reciprocity law, Pacific J. Math. **63**, 563—570 (1976).
[35] Note on Brewer's character sum, Proc. Amer. Math. Soc. **71**, 153—154 (1978).
[36] Remark on an assertion of Chowla, Norske Vid. Selsk. Skrifter **1979**, no. 1, 3—4.
[37] Problem E 2760, Amer. Math. Monthly **86**, 128 (1979); Solution, ibid. **87**, 223—224 (1980).
[38] Evaluation of character sums connected with elliptic curves, Proc. Amer. Math. Soc. **73**, 291—299 (1979).
WILLIAMS W. L. G. [1] Fundamental system of formal modular seminvariants of the binary cubic, Trans. Amer. Math. Soc. **22**, 56—79 (1921).
[2] On the formal modular invariants of binary forms, J. Math. Pures Appl. (9) **4**, 169—192 (1925).

[3] Fundamental systems of formal modular protomorphs of binary forms, Trans. Amer. Math. Soc. **28**, 183—197 (1926).
[4] Formal modular invariants of forms in q variables, Proc. International Math. Congress (Toronto, 1924), vol. 1, pp. 347—359, Univ. of Toronto Press, Toronto, 1928.
[5] A summation theorem in the theory of numbers, Trans. Roy. Soc. Canada (3) **26**, 35—37 (1932).
WILSON R. M. [1] An existence theory for pairwise balanced designs. I, II, J. Combinatorial Theory Ser. A. **13**, 220—245, 246—273 (1972).
[2] An existence theory for pairwise balanced desings. III — Proof of the existence conjectures, J. Combinatorial Theory Ser. A **18**, 71—79 (1975).
WILSON T. C., SHORTT J. [1] An O (log n) algorithm for computing general order-k Fibonacci numbers, Inform. Process. Lett. **10**, no. 2, 68—75 (1980).
WINOGRAD S. [1] Some bilinear forms whose multiplicative complexity depends on the field of constants, Math. Systems Theory **10**, 169—180 (1977).
[2] On multiplication in algebraic extension fields, Theoret. Comput. Sci. **8**, 359—377 (1979).
WINTER D. J. [1] The Structure of Fields, Springer-Verlag, New York — Heidelberg — Berlin, 1974.
WITT E. [1] Über die Kommutativität endlicher Schiefkörper, Abh. Math. Sem. Univ. Hamburg **8**, 413 (1931).
[2] Über eine Invariante quadratischer Formen mod 2, J. reine angew. Math. **193**, 119—120 (1954).
WOLFMANN J. [1] Un problème d'extrémum dans les espaces vectoriels binaires, Ann. Discrete Math. **9**, 261—264 (1980).
WOLFOWITZ J. [1] Coding Theorems of Information Theory, Prentice-Hall, Englewood Cliffs, N. J., 1961. [Имеется перевод: ВОЛЬФОВИЦ ДЖ. Теоремы кодирования теории информации. — М.: Мир, 1967.]
WOLKE D. [1] Eine Bemerkung über das Legendre-Symbol, Monatsh. Math. **77**, 267—275 (1973).
WYLER O. [1] On second-order recurrences, Amer. Math. Monthly **72**, 500—506 (1965).
WYMAN B. F. [1] What is a reciprocity law?, Amer. Math. Monthly **79**, 571—586 (1972).
YALAVIGI C. C. [1] A conjecture of J. H. Halton, Math. Education Ser. A **4**, 125—126 (1970).
[2] Fibonacci series modulo m, Math. Education Ser. A **7**, 48—54 (1973).
YALAVIGI C. C., KRISHNA H. V. [1] Periodic lengths of the generalized Fibonacci sequence modulo p, Fibonacci Quart. **15**, 150—152 (1977).
YALE R. B. [1] Error correcting codes and linear recurring sequences, Report 34-77, M. I. T. Lincoln Laboratory, Lexington, Mass., 1958.
YAMADA T. [1] On the Davenport — Hasse curves, J. Math. Soc. Japan **20**, 403—410 (1968).
YAMAMOTO K. [1] On Gaussian sums with biquadratic residue characters, J. reine angew. Math. **219**, 200—213 (1965).
[2] On a conjecture of Hasse concerning multiplicative relations of Gaussian sums, J. Combinatorial Theory **1**, 476—489 (1966).
[3] On Jacobi sums and difference sets, J. Combinatorial Theory **3**, 146—181 (1967).
[4] The gap group of multiplicative relationships of Gaussian sums, Symposia Math., vol. 15, pp. 427—440, Academic Press, London, 1975.
YAMAMOTO Y., NAGANUMA M., DOI K. [1] Experimental integer theory (Japanese), Sûgaku **18**, 95—103 (1966).
YAMAUCHI M. [1] Some identities on the character sum containing $x(x-1)(x-\lambda)$, Nagoya Math. J. **42**, 109—113 (1971).
YIN K. Z. [1] An inversion formula for switching functions (Chinese), J. Math. Res. Exposition **1981**, no. 1, 63—68.

YOKOYAMA A. [1] On the Gaussian sum and the Jacobi sum with its application, Tôhoku Math. J. (2) **16**, 142—153 (1964).

YOSHIDA H. [1] On an analogue of the Sato conjecture, Invent. Math. **19**, 261—277 (1973).

YOUNG F. H. [1] Analysis of shift register counters, J. Assoc. Comput. Mach **5**, 385—388 (1958).

ZADEH L. A., DESOER C. A. [1] Linear System Theory, McGraw-Hill, New York, 1963. [Имеется перевод: ЗАДЕ Л., ДЕЗОЕР Ч. Теория линейных систем. Метод пространства состояний. — М.: Наука, 1970.]

ZADEH L. A., POLAK E. [1] System Theory, McGraw-Hill, New York 1969.

ZANE B. [1] Uniform distribution modulo m of monomials, Amer. Math. Monthly **71**, 162—164 (1964).

ZASSENHAUS H. [1] Über endliche Fastkörper, Abh. Math. Sem. Univ. Hamburg **11**, 187—220 (1936).

[2] A group-theoretic proof of a theorem of Maclagan — Wedderburn, Proc. Glasgow Math. Assoc. **1**, 53—63 (1952).

[3] The quadratic law of reciprocity and the theory of Galois fields, Proc. Glasgow Math. Assoc. **1**, 64—71 (1952).

[4] Über die Fundamentalkonstruktionen der endlichen Körpertheorie, Jber. Deutsch. Math.-Verein. **70**, 177—181 (1968).

[5] On Hensel factorization. I, J. Number Theory **1**, 291—311 (1969).

[6] On Hensel factorization. II, Symposia Math., vol. 15, pp. 499—513, Academic Press, London, 1975.

[7] A remark on the Hensel factorization method, Math. Comp. **32**, 287—292 (1978).

ZECKENDORF E. [1] Représentation graphique des suites récurrentes modulo p et premiers résultats, Bull. Soc. Roy. Sci. Liège **45**, 13—25 (1976).

ZEE Y.-C. [1] The Jacobi sums of orders thirteen and sixty and related quadratic decompositions, Math. Z. **115**, 259—272 (1970).

[2] The Jacobi sums of order twenty-two, Proc. Amer. Math. Soc. **28**, 25—31 (1971).

ZETTERBERG L.-H. [1] Cyclic codes from irreducible polynomials for correction of multiple errors, IRE Trans. Information Theory **IT-8**, 13—21 (1962). [Имеется перевод: ЦЕТТЕРБЕРГ Л. Х. Циклические коды, исправляющие кратные ошибки и построенные с помощью неприводимых полиномов. — В кн.: Теория кодирования. — М.: Мир, 1964, с. 40—64.]

ZIERLER N. [1] Several binary-sequence generators, Tech. Report no. 95, M. I. T. Lincoln Laboratory, Lexington, Mass., 1955.

[2] On the theorem of Gleason and Marsh, Proc. Amer. Math. Soc. **9**, 236—237 (1958).

[3] On a variation of the first-order Reed — Muller codes, Report 34-80, M. I. T. Lincoln Laboratory, Lexington, Mass., 1958.

[4] Linear recurring sequences, J. Soc. Indust. Appl. Math. **7**, 31—48 (1959). [Имеется перевод: ЦИРЛЕР Н. Линейные возвратные последовательности. — В кн.: Кибернетический сборник, вып. 6. — М.: ИЛ, 1963, с. 55—79.]

[5] Linear recurring sequences and error-correcting codes, Error Correcting Codes (H. B. Mann, ed.), pp. 47—59, Wiley, New York, 1968.

[6] Primitive trinomials whose degree is a Mersenne exponent, Information and Control **15**, 67—69 (1969).

[7] On $x^n + x + 1$ over $GF(2)$, Information and Control **16**, 502—505 (1970).

[8] Trinomials with non conjugate roots of the same prime order, J. Combinatorial Theory Ser. A **11**, 307—309 (1971).

[9] A conversion algorithm for logarithms on $GF(2^n)$, J. Pure Appl. Algebra **4**, 353—356 (1974).

ZIERLER N., BRILLHART J. [1] On primitive trinomials (mod 2), Information and Control **13**, 541—554 (1968).

[2] On primitive trinomials (mod 2). II, Information and Control **14**, 566—569 (1969).

ZIERLER N., MILLS W. H. [1] Products of linear recurring sequences, J. Algebra **27**, 147—157 (1973).

ZIMMER H. G. [1] An elementary proof of the Riemann hypothesis for an elliptic curve over a finite field, Pacific J. Math. **36**, 267—278 (1971).

[2] Computational Problems, Methods, and Results in Algebraic Number Theory, Lecture Notes in Math., vol. 262, Springer-Verlag, Berlin — Heidelberg — New York, 1972.

ZSIGMONDY K. [1] Zur Theorie der Potenzreste, Monatsh. Math. Phys. **3**, 265—284 (1892).

[2] Ueber die Anzahl derjenigen ganzen ganzzahligen Functionen *n*ten Grades von x, welche in Bezug auf einen gegebenen Primzahlmodul eine vorgeschriebene Anzahl von Wurzeln besitzen, Sitzungsber. Wien Abt. II **103**, 135—144 (1894).

[3] Ueber wurzellose Congruenzen in Bezug auf einen Primzahlmodul, Monatsh. Math. Phys. **8**, 1—42 (1897).

АБДУЛЛАЕВ И. [1] Эллиптические кривые и представление чисел кватернарными квадратичными формами. — Докл. АН УзССР, № 1, 1973, с. 3—4.

[2] Эллиптические кривые и представление чисел некоторыми квадратичными формами с четырьмя переменными. — Изв. АН УзССР. Серия физ.-мат. наук., т. **18**, № 1, 1974, с. 59—60.

АБДУЛЛАЕВ И., КОГАН Л. А. [1] Эллиптические кривые и представление чисел положительными квадратичными формами. — Докл. АН УзССР, № 6, 1971, с. 3—4.

АВАНЕСОВ Э. Т. [1] О проблеме В. Мниха. — Mat.-Fiz. Časopis Sloven. Akad. Vied, т. **15**, 1965, с. 280—284.

АЙЗЕНБЕРГ Н. Н., СЕМИОН И. В., ЦИТКИН А. И. [1] Полиномиальные представления логических функций. — Автоматика и выч. техн., № 2, 1971, с. 6—13.

АКУЛИНИЧЕВ Н. М. [1] Оценки рациональных тригонометрических сумм специального вида. — Докл. АН СССР, т. **161**, № 4, 1965, с. 743—745.

АЛАДОВ Н. С. [1] О распределении квадратичных и неквадратичных вычетов простого числа p в ряду 1, 2, ..., $p-1$. — Матем. сборник, т. **18**, вып. 1, 1896, с. 61—75.

АНАНИАШВИЛИ Г. Г., ВАРШАМОВ Р. Р., ГОРОВОЙ В. П., ПАРХОМЕНКО П. П. [1] К вопросу разложимости полиномов над полем GF (2). — Сообщ. АН ГССР, т. **41**, № 1, 1966, с. 129—134.

АНДРИАНОВ А. Н. [1] Представление чисел некоторыми квадратичными формами в связи с теорией эллиптических кривых. — Изв. АН СССР. Серия Матем., т. **29**, № 1, 1965, с. 227—238.

АНДРУХАЕВ Х. М. [1] Об одной сумме типа Клоостермана — В кн.: Некоторые вопросы теории полей. — Изд. Сарат. универс.: Саратов, 1964, с. 60—66.

[2] Обобщение сумм Клостермана на поле Гаусса и их оценки. — Научн. труды Краснодарского пед. инст., вып. 118, 1969, с. 29—40.

АРАКЕЛОВ В. А., ВАРШАМОВ Р. Р. [1] К исследованию алгебраической структуры периодических рекуррентных последовательностей. — Изв. АН АрмССР. Серия матем., т. **6**, № 5, 1971, с. 379—385.

АРАКЕЛОВ В. А., ТЕНЕНГОЛЬЦ Г. М. [1] Некоторые свойства рекурреитных периодических последовательностей. — Труды ВЦ АН АрмССР и Ереванского гос. университета. Матем. вопросы киберн. и выч. техн., вып. 6, 1970, с. 18—28.

АРХИПОВ Г. И., КАРАЦУБА А. А., ЧУБАРИКОВ В. Н. [1] Кратные тригонометрические суммы. — Труды Матем. института им. В. А. Стеклова, т. **151**, 1980, с. 1—128.

БАБАЕВ Г., ИСМОИЛОВ Д. [1] О числе решений одной пары сравнений. — Докл. АН ТаджССР, т. **22**, № 7, 1979, с. 404—407.

БАССАЛЫГО Л. А. [1] Замечание о быстром умножении многочленов над полями Галуа. — Пробл. передачи информ., т. **14**, № 1, 1978, с. 101—102.

БЛОХ Э. Л. [1] О методе декодирования для кодов Боуза — Чоудхури, исправляющих тройные ошибки. — Изв. АН СССР. Серия техн. киберн., № 3, 1964, с. 30—37.

БОРЕВИЧ З. И., ШАФАРЕВИЧ И. Р. [1] Теория чисел. — М.: Наука, 1985.

БУХШТАБ А. А. [1] О числах арифметнческой прогрессии, у которых все простые множители малы по порядку роста. — Докл. АН СССР, т. **67**, № 1, 1949, с. 5—9.

ВАРШАМОВ Р. Р. [1] Оценка числа сигналов в кодах с коррекцией ошибок. — Докл. АН СССР, т. **117**, № 5, 1957, с. 739—741.

[2] Об одной теореме из теории приводимости полиномов. — Докл. АН СССР, т. **156**, № 6, 1964, с. 1308—1311.

[3] Об одном линейном операторе в поле Галуа и его приложении. — Studia Sci. Hungar., v. 8, № 1—2, 1973, p. 5—19.

[4] Некоторые вопросы конструктивной теории приводимости полиномов над конечными полями. — В кн.: Проблемы кибернетики, вып. 27. — М.: Физматгиз, 1973, с. 127—134; исправления: вып. 28, с. 280.

[5] Операторные подстановки в поле Галуа и их приложение. — Докл. АН СССР, т. **211**, № 4, 1973, с. 768—771.

ВАРШАМОВ Р. Р., АНАНИАШВИЛИ Г. Г. [1] К теорни приводимости полиномов в конечиом поле. — В ки.: Абстрактная и структурная теория построения релейных устройств. (под ред. М. А. Гаврилова). — М.: Наука, 1966, с. 134—138.

ВАРШАМОВ Р. Р., АНТОНЯН А. М. [1] Об одном методе синтеза неприводимых полиномов над конечными полями. — Докл. АН АрмССР, т. **66**, № 4, 1978, с. 197—199.

ВАРШАМОВ Р. Р., ГАМКРЕЛИДЗЕ Л. И. [1] Об одном методе построения примитивных полиномов над конечными полями. — Сообщ. АН ГССР, т. **99**, № 1, 1980, с. 61—64.

ВАРШАМОВ Р. Р., ГАРАКОВ Г. А. [1] К теории самодвойственных полиномов над полем Галуа. Матем. вопр. киберн. и вычисл. техн. — Труды ВЦ АН АрмССР и Ереван. гос. унив., вып. 6, 1970, с. 5—17.

ВАРШАМОВ Р. Р., ОСТИАНУ В. М. [1] Примененне теории конечных полей к теории корректирующих кодов и синтезу надежных релейных структур. — В кн.: Теория конечных и вероятностных автоматов. — М.: Наука, 1965, с. 376—378.

ВАСИЛЬЕВ Ю. Л. [1] О негрупповых плотио упакованных кодах. — В кн.: Проблемы кибернетики, вып. 8. — М.: Физматгиз, 1962, с. 337—339.

ВАСИЛЬЕВ Ю. П. [1] Описание конечных полей с помощью ЭВМ. — Кибернетика (Киев), № 5, 1979, с. 133—135.

ВИНОГРАДОВ А. И. [1] О кубической сумме Гаусса. — Изв. АН СССР. Серия матем., т. **31**, № 1, 1967, с. 123—148.

ВИНОГРАДОВ И. М. [1] Sur la distribution des résidus et des nonrésidus des puissances. — Журн. физ.-матем. общ. при Пермском гос. унив., № 1, 1918, с. 94—98.

[2] On a general theorem conserning the distribution of the residue and nonresidues of powers. — Trans. Amer. Math. Soc., v. **29**, 1927, p. 209—217.

[3] On the bound of the least non-residue of n-th powers. — Trans. Amer. Math. Soc., v. **29**, 1927, 218—226.

[4] Об одной тригонометрической сумме и ее приложениях в теории чисел. — Докл. АН СССР, № 5, 1933, с. 195—204.

[5] О некоторых тригоиометрических суммах и их приложениях. — Докл. АН СССР, № 6, 1933, с. 249—254.

[6] Новые приложения тригонометрических сумм. — Докл. АН СССР, т. **1**,

№ 1, 1934, с. 10—14.
[7] Новые асимптотические выражения. — Докл. АН СССР, т. **1**, № 2, 1934, с. 49—51.
[8] Некоторые теоремы о распределенни индексов и первообразных корней. Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **5**, 1934, с. 87—93.
[9] Тригонометрические суммы, зависящие от составного модуля. — Докл. АН СССР, т. **1**, № 5, 1934, с. 225—229.
[10] Новые теоремы о распределении квадратичных вычетов. — Докл. АН СССР, т. **1**, № 6, 1934, с. 289—290.
[11] Новые теоремы о распределении первообразных корней. —Докл. АН СССР, т. **1**, № 7, 1934, с. 366—369.
[12] Новое усовершенствование метода оценки двойных сумм. — Докл. АН СССР, т. **73**, № 4, 1950, с. 635—638.
ВОРОБЬЕВ Н. Н. [1] Числа Фибоначчи. — М.: Наука, 1969.
ВОРОНОЙ Г. Ф. [1] О целых алгебраических числах, зависящих от корня уравнения третьей степени. — СПб, изд. Акад. наук, 1894; см. также: Собр. соч. в 3-х томах, т. 1, Киев, изд. АН УССР, 1952, с. 25—195.
[2] Об одном свойстве дискриминанта целых функций. Verhandl. Dritten Intern. Math.-Kong. (Heidelberg, 1904), p. 186—189, Teubner, Leipzig, 1905; см. также Собр. соч. в 3-х томах, т. 3, Киев: изд. АН УССР, 1953, с. 12—15.
ГАБИДУЛИН Е. М. [1] О кодах, инвариантных относительно линейных преобразований. — Радиотехн. и электроника, т. **11**, 1966, с. 433—438.
ГАНТМАХЕР Ф. Р. [1] Теория матриц. — М.: Наука, 1967.
ГАРАКОВ Г. А. [1] Алгоритм определения неприводимых двоичных полиномов и их показателей. — Изв. АН АрмССР, серия физ.-мат. наук, т. **17**, № 5, 1964, с. 7—16.
[2] Об одном свойстве первообразных элементов поля Z_p^*. — Докл. АН АрмССР, т. **46**, № 5, 1968, с. 213—216.
[3] Таблицы неприводимых полиномов над полем $GF(p)$ ($p \leqslant 11$). — Матем. вопр. киберн. и выч. техн. — Труды ВЦ АН АрмССР и Ереван. гос. унив., вып. 6, 1970, с. 112—142.
ГЕЛЬФАНД С. И. [1] О неприводимых многочленах над конечным полем. — Успехи мат. наук, т. **24**, № 1 (1969), с. 193—194.
[2] Представления полной линейной группы над конечным полем. — Матем. сборник, т. **83**. вып. 1, 1970, с. 15—41.
ГЕЛЬФОНД А. О. [1] Исчисление конечных разностей. — М.: Наука, 1967.
ГЕЛЬФОНД А. О., ЛИННИК Ю. В. [1] Элементарные методы в аналитической теории чисел. — М.: Физматгиз, 1962.
ГОППА В. Д. [1] Декодирование и диофантовы приближения. — Пробл. управл. и теор. информации, т. **5**, 1976, с. 195—206.
[2] Коды на алгебраических кривых. — Докл. АН СССР, т. **259**, № 6, 1981, с. 1289—1290.
ГОРБОВ А. Н., ШМИДТ Р. А. [1] Резольвента Клейна для уравнения 5-й степени над полем характеристики, делящей 5!. — Зап. науч. семинаров ЛОМИ АН СССР, т. **46**, 1974, с. 36—40.
ГРЕБЕНЮК Д. Г. [1] О целых алгебраических числах, зависящих от неприводимого уравнения 4-й степени. — Бюлл. Ср.-Аз. гос. унив., Ташкент, т. **11**, 1925, с. 19—43.
[2] Применение комплексных чисел Вороного к решению сравнений четвертой степени. — Труды Инст. матем. им. Романовского АН УзССР, вып. **26**, 1962, с. 57—80.
ГРУШКО И. И. [1] Об одном подходе к вопросу о корректирующих возможностях групповых кодов. — Радиотехн. и электр., т. **9**, вып. 10, 1964, с. 1749—1756.
ДЕМЬЯНОВ В. Б. [1] О представлении нуля формами вида $\sum_{i=1}^{m} a_i X_i^n$. — Докл. АН СССР, т. **105**, № 2, 1955, с. 203—205.

[2] Пары квадратичных форм над полным дискретно-нормированным полем с конечным полем классов вычетов. — Изв. АН СССР. Сер. матем., т. 20, № 3, 1956, с. 307—324.

ДОБРУШИН Р. Л. [1] Survey of Soviet research in information theory, IEEE Trans, Information theory, v. **IT-18**, 1972, p. 703—724.

ДЫНЬКИН В. Н., АГАРОНОВ Д. А. [1] Метод разложения полиномов в конечном поле. — Пробл. передачи информ., т. **6**, вып. 3, 1970, с. 82—86.

ЕЛИСТРАТОВ И. В. [1] О числе решений некоторых уравнений в конечных полях. — В кн.: Труды молодых ученых. — Саратов: изд. Сарат. унив., 1964, с. 27—30.

[2] О числе решений некоторых уравнений в конечных полях. — В кн.: Некоторые вопросы теории полей. — Саратов: Изд. Сарат. унив., 1964, с. 48—69.

[3] Об элементарном доказательстве теоремы Хассе. — В кн.: Исследования по теории чисел, вып. 1. — Саратов: Изд. Сарат. унив., 1966, с. 21—26.

[4] Число классов и расположение нулей $Z(u)$-функции. — Волжский матем. сборник, вып. 4, 1966, с. 58—65.

[5] Некоторые вопросы теории алгебраических функций. — В кн.: Исследования по теории чисел, вып. 4. — Саратов: Изд. Сарат. унив., 1972, с. 17—34.

[6] Оценка числа решений некоторого уравнения в конечном поле. — Докл. АН ТаджССР, т. 17, № 8, 1974, с. 3—6.

[7] Элементарный подход к оценке рациональных тригонометрических сумм. Литов. матем. сборник, т. **17**, № 2, 1977, с. 91—110.

ЖМУДЬ Э. М. [1] Об одном инварианте квадратичных форм над полем Галуа характеристики 2. — Вестн. Харьков. госуд. универ., № 177, Прикл. матем. и мех., вып. 44, 1979, с. 77—86.

ЗИНОВЬЕВ В. А., ЛЕОНТЬЕВ В. К. [1] Несуществование совершенных кодов над полями Галуа. — Пробл. управл. и теор. информ., т. **2**, № 2, 1973, с. 123—132.

ИВАНОВ И. И. [1] О двух сравнениях. — Журн. Ленингр. Физ.-мат. общ., т. 1, 1926, с. 37—38.

ИПАТОВ В. П. [1] К теории троичных последовательностей с идеальными периодическими автокорреляционными свойствами. — Радиотехн. и электрон., т. **25**, 1980, с. 723—727.

ИСКОВСКИХ В. А. [1] Проверка гипотезы Римана для некоторых локальных дзета-функций. Успехи матем. наук, т. **28**, вып. 3, 1973, с. 171—182.

КАЛУЖНИН Л. А. [1] La structure des p-groupes de Sylow des groupes symétriques finis. — Ann. Sci. Ecole Norm. Sup. v. (3) **65**, 1948, 239—276.

КАРАЦУБА А. А. [1] Проблема Тэри для систем уравнений. — Матем. сб., т. **55**, вып. 2, 1961, с. 209—220.

[2] О системах сравнений. — Изв. АН СССР. Серия. матем., т. **29**, № 4, 1965, с. 935—944.

[3] Асимптотические формулы для некоторого класса тригонометрических сумм. — Докл. АН СССР, т. **169**, № 1 1966, с. 9—11.

[4] Теоремы о среднем и полные тригонометрические суммы. — Изв. АН СССР, серия матем., т. **30**, № 1, 1966, с. 183—206.

[5] Об оценках полных тригонометрических сумм. — Матем. заметки, т. **1**, вып. 2, 1967, с. 199—208.

[6] Суммы характеров и первообразные корни в конечных полях. — Докл. АН СССР, т. **180**, № 6, 1968, с. 1287—1289.

[7] О тригонометрических суммах. — Докл. АН СССР, т. **189**, № 1, 1969, с. 31—34.

[8] Об оценках сумм характеров. — Изв. АН СССР. Серия матем., т. **34**, № 1, 1970, с. 20—30.

[9] Об оценках снизу сумм характеров от многочленов. — Матем. заметки, т. **14**, вып. 1, 1973, с. 67—72.

КЛЯЧКО А. А. [1] Группы моноидромии полиномиальных отображений. — В кн: Исследования по теории чисел, вып. 6. — Саратов: Изд. Сарат. унив.,

1975, с. 82—91.
КНИЖНЕРМАН Л. А., СОКОЛИНСКИЙ В. З. [1] Некоторые оценки рациональных тригонометрических сумм и сумм символов Лежандра. — Успехи матем. наук, т. **34**, вып. 3, 1979, с. 199—200.
КОЗЕЛ П. Т., ШАКЛЕИНА Т. А. [1] Число изотропных подпространств в пространстве с ортогональной метрикой. Вестн. Белорус. гос. унив., сер. 1, № 1, 1975, с. 11—15.

КОРОБОВ Н. М. [1] Распределение невычетов и первообразных корней в рекуррентных рядах. — Докл. АН СССР, т. **88**, № 4, 1953, с. 603—606.

[2] Оценки тригонометрических сумм и их приложения. Успехи матем. наук, т. **13**, вып. 4, 1958, с. 185—192.

[3] Об оценке рациональных тригонометрических сумм. Докл. АН СССР, т. **118**, №, 2, 1958, с. 231—232.
[4] О нулях функции $\zeta(s)$. — Докл. АН СССР, т. **118**, № 3, 1958, с. 431—432.
[5] Двойные тригонометрические суммы и их приложения к оценке рациональных сумм. — Матем. заметки, т. **6**, вып. 1, 1969, с. 25—34.
[6] Оценка суммы символов Лежандра.— Докл. АН СССР, т. 196, № 4, 1971, с. 764—767.
[7] О полных системах сравнений. — Acta Arith., v. **21**, 1972, p. 357—366.
КОРОБОВ Н. М., МИТЬКИН Д. А. [1] О нижних оценках полных тригонометрических сумм. — Вестн. Моск. гос. унив., сер. матем. и мех., 1977, № 5, с. 54—57.
КУЗНЕЦОВ В. Н. [1] Z-функции одного класса Артин—Шрайеровых накрытий, — Матем. зап. Уральск. унив., т. **10**, № 1, 1976, с. 24—36.
КУЗНЕЦОВ Н. В. [1] Гипотеза Петерсона для параболических форм веса нуль и гипотеза Линника. Суммы сумм Клостермана. Матем. сб., т. **111**, вып. 3, 1980, с. 334—383.
КУРБАТОВ В. А. [1] О полиномах, которые дают подстановки для бесконечно многих простых чисел. — Ученые зап. Свердловск. гос. пединст., т. 4, 1947, с. 79—121.
[2] Обобщенные теоремы Шура относительно одного класса алгебраических функций. — Матем. сб., т. 21, вып. 1, 1947, с. 133—141.
[3] О группе монодромии одной алгебраической функции. — Матем. сб., т. **25**, вып. 1, 1949, с. 51—94.
КУРБАТОВ В. А., СТАРКОВ Н. Г. [1] Об аналитическом представлении подстановок. — Уч. записки Свердловск. гос. пединст., т. **31**, 1965, с. 151—158.
ЛАБУНЕЦ В. Г., СИТНИКОВ О. П. [1] Гармонический анализ булевых функций и функций k-значной логики над конечными полями. — Изв. АН СССР, серия техн. киберн., № 1, 1975, с. 141—148.
ЛЕБЕДЕВ С. С. [1] Об оценке одной тригонометрической суммы. — Вестн. Моск. гос. унив., сер. матем., мех., № 3, 1961, с. 22—28.
ЛЕНСКОЙ Д. Н. [1] К арифметике многочленов над конечным полем. — Волжск. матем. сб., вып. 4, 1966, с. 155—159.
[2] К арифметике многочленов над конечным полем II. — В кн.: Исследования по теории чисел, вып. 1. — Саратов; изд. Саратовск. унив., 1966, с. **27—34**.
ЛИННИК Ю. В. [1] Некоторые замечания об оценке тригонометрических сумм. — Успехи матем. наук, т. **14**, вып. 3, 1959, с. 153—160.
[2] Additive problemes and eigenvalues of the modular operators. International Congress of Math. (Stockholm, 1962), Institut Mittag—Leffler, 1963, p. 270—284.
ЛИТВЕР Е. Л., ЮДИНА Г. Е. [1] Первообразные корни для простых чисел первого миллиона и их степеней. — Матем. анализ и его прилож., вып. 3. — Ростов-на-Дону: изд. Ростовск. унив., 1971, с. 106—109.
ЛЬВОВ И. В. [1] Одно приложение теоремы Шевалле—Варнинга в теории колец. — Матем. зап. Урал. гос. унив., т. **11**, вып. 1, 1978, с. 110—124.

МАЗУР Л. Е. [1] О последовательных вычетах и невычетах многочленов. — Матем. заметки, т. 7, вып. 1, 1970, с. 97—107.
МАЛЫШЕВ А. В. [1] Обобщение сумм Клостермана и их оценки. — Вестн. Ленингр. унив., сер. матем., мех. и астрон., № 13, вып. 3, 1960, с. 59—75.
[2] О суммах Гаусса и суммах Клостермана. — Докл. АН СССР, т. **133**, № 5, 1960, с. 1017—1020.
[3] О представлении целых чисел положительными квадратичнымн формами. — Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **65**, 1962.
[4] О коэффициентах Фурье модулярных форм. Зап. научн. семинара Ленингр. отделен. Матем. инст. им. Стеклова АН СССР, т. 1, 1966, с. 140—163.
МАНИН Ю. И. [1] О сравнениях третьей степени по простому модулю. — Изв. АН СССР сер. матем., т. **20**, № 5, 1956, с. 673—678.
[2] Об арифметнке рациональных поверхностей. — Докл. АН СССР, т. **152**, № 1, 1963, с. 47—49.
[3] Соответствия, мотивы и моноидальные преобразования. Матем. сб., т. **77**, вып. 4, 1968, с. 475—507.
[4] Кубические формы. Алгебра, геометрия, арифметика. — М.: Наука, 1972.
[5] What is the maximum number of points on a curve over F_2? — J. Fac. Sci. Univ. Tokyo Sect. IA, v. **28**, 1981, p. 715—720.
МАРКОВИЧ О. Ф. [1] Исследование особой суммы в системах варинговского типа методом элементариого сглаживания. — Труды Куйбыш. пед. инст., т. **215**, 1978, с. 30—37.
МАРКУШЕВИЧ А. И. [1] Возвратные последовательности.— М.: Наука, 1975.
МАТВЕЕВА М. В. [1] О решении уравиений третьей степени в поле характеристики 3. — Пробл. передачи информ., т. 4, вып. 4, 1968, с. 76—78.
МИРОНЧИКОВ Е. Т. [1] Класс кодов, исправляющих двойные ошибки, и их реализация. — Авт., телем. и прибор., № 3, 1963, с. 251—255.
МИТЬКИН Д. А. [1] К оценке рациональной тригонометрической суммы с простым знаменателем. — Вести. Моск. унив., сер. 1 матем., механика, № 5, 1972, с. 50—58.
[2] Оценка суммы символов Лежандра от многочленов четной степени. — Матем. заметки, т. 14, вып. 1, 1973, с. 73—81.
[3] Об оценках снизу сумм символов Лежандра и тригонометрических сумм. — Успехи матем. наук, т. 30, вып. 5, 1975, с. 214.
[4] Сушествование рациональных точек на гиперэллиптической кривой иад простым коиечным полем. — Вести. Моск. унив., сер. матем., механика, т. **30**, № 6, 1975, с. 86—90.
[5] Об оценках рациональиых тригонометрических сумм специального вида. — Докл. АН СССР, т. **224**, № 4, 1975, с. 760—763.
МИХАЙЛЮК М. В. [1] О сложности вычисления элементарных симметрических функций в конечиых полях. — Докл. АН СССР, т. **244**, № 5, 1979, с. 1072—1076.
[2] Вычисление базиса симметрических функций в конечных полях. — Матем. заметки, т. **30**, вып. 2, 1981, с. 291—304.
МОРОЗ Б. З. [1] О распределении степенных вычетов и невычетов. — Вестн. Ленингр. унив., сер. матем., мех. и астрон., т. **16**, № 19, 1961, с. 164—169.
МУРЗАЕВ Е. А. [1] О выделении кратиых множителей многочленов над коиечными коммутативными полями. — Волжск. матем. сб., вып. 5, 1966, с. 255—259.
НАЗАРОВ И. А. [1] Математический аппарат анализа и синтеза линейиых многотактных кодирующих схем. — Изв. Ленингр. электротех. инст., т. **39**, 1959 с. 153—162.
НЕЧАЕВ В. И. [1] Группа неособенных матриц иад конечным полем и рекуррентные последовательности. — Докл. АН СССР, т. **152**, № 2, 1963, с. 275—277.

[2] Неулучшаемая оценка тригонометрических сумм для рекуррентных функций с непостоянными коэффициентами. — Докл. АН СССР, т. **154**, № 3, 1964, с. 520—522.
[3] Линейные рекуррентные сравнения с периодическими коэффициентами. — Матем. заметки, т. 3, вып. 6, 1968, с. 625—632.
[4] Рекуррентные последовательности. — Учен. зап. Московск. пед. инст., т. 375, 1971, с. 103—123.
[5] Тригонометрические суммы для рекуррентных последовательностей элементов конечного поля. — Матем. заметки, т. 11, вып. 5, 1972, с. 597—607.
[6] Тригонометрические суммы для рекуррентных последовательностей. — Докл. АН СССР, т. 206, № 4, 1972, с. 811—814.
[7] Оценка полной рациональной тригонометрической суммы. — Матем. заметки, т. 17, вып. 6, 1975, с. 839—849.
НЕЧАЕВ В. И., ПОЛОСУЕВ А. М. [1] О распределении невычетов и первообразных корней в последовательности, удовлетворяющей конечноразностному уравнению с полиномиальными коэффициентами. — Вестн. Моск. унив., сер. матем., мех., № 6, 1964, с. 75—84.
НЕЧАЕВ В. И., СТЕПАНОВА Л. Л. [1] Распределение невычетов и первообразных корней в рекуррентных последовательностях над полем алгебраических чисел. — Успехи матем. наук, т. 20, вып. 3, 1965, с. 197—203.
НЕЧАЕВ В. И., ТОПУНОВ В. Л. [1] Оценка модуля полных рациональных тригонометрических сумм третьей и четвертой степени. — Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **158**, 1981, с. 125—129.
НИСНЕВИЧ Л. Б. [1] О числе точек алгебраического многообразия в простом конечном поле. Докл. АН СССР, т. **99**, № 1, 1954, с. 17—20.
ПАВЛОВ А. И., ПОХОДЗЕЙ Б. Б. [1] Псевдослучайные числа, порождаемые линейными рекуррентными соотношениями над конечным полем. — Журн. вычисл. матем. и мат. физ., т. 19, № 4, 1979, с. 836—842.
ПЕРЕЛЬМУТЕР Г. И. [1] Оценка одной суммы с простыми числами. — Докл. АН СССР, т. **144**, № 1, 1962, с. 48—51.
[2] О некоторых суммах с характерами. Успехи матем. наук, т. **18**, вып. 2, 1963, с. 145—149.
[3] О проблеме оценки некоторых арифметических сумм. — В кн.: Некоторые вопросы теории полей. — Саратов: изд. Саратов. унив., 1964, с. 6—15.
[4] О некоторых суммах и связанных с ними многообразиях. — В кн.: Труды молодых ученых. — Саратов: изд. Сарат. унив., 1964, с. 69—72.
[5] Z-функция одного класса кубических поверхностей. — В кн.: Исследования по теории чисел, вып. 1. — Саратов: изд. Саратов. унив., 1966, с. 49—58.
[6] Рациональность L-функций одного класса алгебраических многообразий. — В кн.: Исследования по теории чисел, вып. 1. — Саратов: изд. Сарат. унив., 1966, с. 59—62.
[7] О наименьшем невычете полинома вдоль алгебраической кривой. — В кн.: Исследования по теории чисел, вып. 3. — Саратов: Изд. Сарат. унив., 1969, с. 64—68.
[8] Об одной гипотезе К. Вильямса. — Докл. АН СССР, т. **184**, № 2, 1969, с. 282—284.
[9] Оценка суммы вдоль алгебраической кривой. — Матем. заметки, т. **5**, вып. 3, 1969, с. 373—380.
[10] Оценка многократной суммы с символом Лежандра для кубического полинома. — В кн.: Исследования по теории чисел, вып. 6. — Саратов: Изд. Сарат. унив., 1975, с. 129—131.
[11] Оценка многократной суммы с символом Лежандра. — Матем. заметки, т. **18**, вып. 3, 1975, с. 421—427.
[12] Оценка многократной суммы с символом Лежандра для полинома нечетной степени. — Матем. заметки, т. **20**, вып. 6, 1976, с. 815—824.
ПЕРЕЛЬМУТЕР Г. И., ПОСТНИКОВ А. Г. [1] О числе решений одного сравнения. — Acta Arith., v. **21**, 1972, p. 103—110.

ПИМЕНОВ Н. В. [1] О колеблемости знака остатка в формуле для числа точек алгебраической кривой. — Укр. матем. журнал, т. **28**, № 4, 1976, с. 546—551.

ПОЛОСУЕВ А. М. [1] Некоторые арифметические свойства рекуррентных функций с переменными коэффициентами. — Матем. заметки, т. 1, вып. 1, 1967, с. 45—52.

ПОСТНИКОВ А. Г. [1] Эргодическне вопросы теории сравнений и теории диофантовых приближений. — Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **82**, 1966.

ПОСТНИКОВ А. Г., СТЕПАНОВ С. А. [1] К теории сумм Якобсталя. — Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **142**, 1976, с. 208—214.

ПРОСКУРИН Н. В. [1] Формулы суммирования для общих сумм Клостермана. Зап. научн. семинаров Ленингр. отдел. Матем. инст. им. Стеклова АН СССР, т. **82**, 1979, с. 103—135.

[2] О гипотезе Ю. В. Линника. — Зап. научн. семинаров Ленингр. отдел. Матем. инст. им. Стеклова АН СССР, т. **91**, 1979, с. 94—118.

[3] Общие суммы Клостермана. — Препринт ЛОМИ ,R-3-80, Ленннгр. отдел. Матем. инст. им. Стеклова АН СССР, Л., 1980.

РАДЧЕНКО А. Н., ФИЛИППОВ В. И. [1] Сдвигающие регистры с логической обратной связью и их использование в качестве счетных и кодирующих устройств. — Автом. и телемех., т. **20**, № 11, 1959, с. 1507—1514.

[2] Логическая обратная связь в сдвигающих регистрах. — Авт., телем. и прибор., № 3, 1960, с. 257—267.

РЕШЕТУХА И. В. [1] Один вопрос теории кубических вычетов. — Матем. заметки, т. 7, вып. 4, 1970, с. 469—476.

[2] Обобщенные суммы для характеров и их применения к законам взаимности. — Укр. матем. журнал, т. **23**, № 2, 1971, с. 270—276.

САГАЛОВИЧ Ю. Л. [1] Последовательности максимальной длины как коды состояний автомата. — Пробл. передачи информ.: т. 12, вып. 4, 1976, с. 70—73.

СЕГАЛ Б. И. [1] Суммы характеров и их применение. — Изв. АН СССР, серия матем., т. 5, № 4—5, 1941, с. 401—410.

СЕРГЕЕВ Е. А. [1] Расщепление полиномов $f_n(x)$ над конечными полями. — Научн. труды Кубанск, гос. унив., вып. 166, 1973, с. 20—33.

СОКОЛОВСКИЙ А. В. [1] Оценка снизу в «большом решете». — Зап. научн. семинаров Ленинград. отдел. Матем. инст. им. Стеклова АН СССР, т. **91**, 1979, с. 125—133.

СТЕПАНОВ С. А. [1] О числе точек гиперэллиптической кривой над простым конечным полем. Изв. АН СССР. Серия матем., т. 33, № 5, 1969, с. 1171—1181.

[2] Elemantary method in the theory of congruences for a prime modulus.— Acta Arith., v. **17**, 1970, p. 231—247.

[3] Об оценке сумм Вейля с простым знаменателем. — Изв. АН СССР, серия матем., т. **34**, № 5, 1970, с. 1015—1037. Замечания к этой работе там же, т. **35**, № 4, 1971, с. 965—966.

[4] Об оценке сумм Клостермана. — Изв. АН СССР, серия матем., т. **35**, № 2, 1971, с. 308—323.

[5] Об оцеике рациональных тригонометрических сумм с простым знаменателем. — Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **112**, 1971, с. 346—371.

[6] An elemenraty proof of the Hasse—Weil theorem for hyperelliptic curves. — J. Numbet Theory, v. **4**, 1972, p. 118—143.

[7] Сравнении с двумя неизвестными. — Изв. АН СССР, серия матем., т. **36**, № 4, 1972, с. 683—711.

[8] Конструктивный метод в теории уравнений над конечными полями (доклад на Междуиар. конфер. по теории чисел, Москва, сент. 1971). — Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **132**, 1973, с. 237—246.

[9] Рациональные точки алгебраических кривых над конечными полями. — В кн.: Актуальные проблемы аналитической теории чисел. Труды летн. школы по аналит. теор. чисел, Минск, 1972. — Минск: Наука, и техн., 1974, с. 223—243.
[10] Элементарный метод в теории уравнений над конечными полями. Proc. International Congress Math., Vancouver, B. C. 1974, vol 1, pp. 383—391, Canad. Math. Congress, Montreal, Que., 1975.
[11] Об оценках снизу неполных сумм характеров от многочленов. — Труды Матем. инст. В. А. Стеклова АН СССР, т. **143**, 1977, с. 175—177.
[12] Уравнения над конечными полями. — Матем. заметки, т. 21, вып. 2, 1977, с. 271—279.
[13] Элементарный метод в теории алгебраических чисел. — Матем. заметки, т. **24**, вып. 3, 1978, с. 425—431.
[14] К доказательству соотношений Давенпорта—Хассе. — Матем. заметки, т. **27**, вып. 1, 1980, с. 3—6.
СТЕЧКИН С. Б. [1] Оценка полной рациональной тригонометрической суммы.— Труды Матем. инст. им. В. А. Стеклова АН СССР, т. **143**, 1977, с. 188—207.
ТУШКИНА Т. А. [1] Численный эксперимент по вычислению инварианта Хассе для некоторых кривых. — Изв. АН СССР, серия матем., т. 29, № 5, 1965, с. 1203—1204.
УДАЛОВ А. П., СУПРУН Б. А. [1] Избыточное кодирование при передаче информации двоичными кодами. — М.: Связь, 1964.
УСОЛЬЦЕВ Л. П. [1] Оценки больших уклонений в некоторых задачах на неполную систему вычетов. — Докл. АН СССР, т. 143, № 3, 1962, с. 539—542.
ФОМЕНКО О. М. [1] Применение формулы редукции Айхлера к представлению чисел квадратичными формами. — Матем. заметки, т. 9, вып. 1, 1971, с. 71—76.
ЧЕБЫШЁВ П. Л. [1] Теория сравнений. — С-Пб.: тип. Имп. акад. наук, 1849; см. также: Полн. собр. соч., т. 1, М.—Л.: Изд. АН СССР, 1944, с. 10—172.
ЧУБАРИКОВ В. Н. [1] О кратных рациональных тригонометрических суммах и кратных интегралах.— Матем. заметки, т. **20**, вып. 1, 1976, с. 61—68.
ШАТУНОВСКИЙ С. О. [1] Об условиях существования n неравных корней сравнения n-й степени по простому модулю. — Изв. физ.-мат. общества, Казань, (2), т. **12**, 1902, с. 33—49.
ШПАРЛИНСКИЙ И. Е. [1] Распределение невычетов и первообразных корней в рекуррентных последовательностях. — Матем. заметки, т. **24**, вып. 5, 1978, с. 603—613.

Дополнительная литература

AGOU S. [1*] Degré minimum des polynômes $f\left(\sum_{i=1}^{m} a_i x^{p^{r_i}}\right)$ sur les corps finis de caractéristique $p > m$. — Pacif. J. Math., v. **102**, 1982, no 1, p. 1—8.
[2*] Sur l'irréductibilité des trinômes $x^{p+1} - ax - b$ sur les corps finis F_{p^s}. — Acta Arithmetica, v. **44**, 1984, no 4, p. 343—355.
[3*] Sur la factorisation des polynômes $x^{p^{2r}+p^r+p^r} - ax^{p^r+1} - bx - c$ sur les corps finis F_{p^s}. — Manuscripta math., v. **58**, 1987, no 1/2, p. 141—154.
BAKER R. C. [1*] Small solutions of congruences. — Mathematika, v. **30**, 1983, no 2, p. 164—188.
BARKER H. A. [1*] Sums and products tables for Galois fields. — Ant. J. Math. Educ. Sci. and Technol., v. **17**, 1986, no 4, p. 473—485.

BEARD J. T. B., Jr., SUE H. M. [1*] Non-splitting unitary perfect polynomials over GF (q). — Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Natur., v. **66**, 1979, no 3, p. 179—185.

BREMSER P. S. [1*] A generalization of Gaussian sums to vector spaces over finite fields. — Lin. Alg. and Appl., v. **81**, 1986, p. 35—45.

BROWKIN J. [1*] On forms over p-adic fields. — Bull. Acad. Polon. Sci., Sèr. sci. math. astr. et phys., v. **14**, 1966, no 9, p. 489—492.

[2*] On system of congruences. — Bull. Pol. Acad. Sci. Math., v. **31**, 1983, no 5—8, p. 219—226.

BURKE J. R. [1*] A notion of density and essential components in $GF[p, x]$. — Acta Arithmetica, v. **44**, 1984, no 4, p. 299—306.

CALMET J. [1*] Algebraic algorithms in GF (q). — Discr. Math., v. **56**, 1985, no 2—3, p. 101—109.

CALMET J., LOOS R. [1*] Deterministic factorization of integral polynomials. — Let. Notes Comput. Sci., v. **144**, 1982, p. 117—125.

CAR M. [1*] Sommes de carrés dans $F_q[x]$. — Rozpr. Mat., 1983, no 215.

[2*] Sommes de deux carrés dans $F_q[x]$ et probleme diviseur. — Ann. Fac. Sci. Toulouse Math., v. **5**, 1983, no 2, p. 89—108.

[3*] Polynômes de $F_q[x]$ ayant un diviseur de degré donné. — Acta Arithm., v. **43**, 1984, no 2, p. 131—154.

[4*] Sommes de carrés de polynômes irréductibles dans $F_q[x]$. — Acta Arithm., v. **44**, 1984, no 4, p. 307—321.

[5*] Ensembles de polynômes irréductibles et théorèmes de densité. — Acta Arithm. v. **44**, 1984, no 4, p. 323—342.

[6*] Polynômes irréductibles de $F_q[x]$ de la forme $M + N$ ou N est norme d'un polynôme de $F_{q^2}[x]$. — Rozpr. Mat., 1984, no 238.

[7*] Le théorème de Chen pour $F_q[x]$. — Rozpr. mat., 1984, no 223.

[8*] Sommes de puissances et d'irréductibles dans $F_q[x]$. — Acta Arithm., v. **44**, 1984, no 1, p. 7—34.

[9*] Sommes d'un carrè t d'un polynôme irréductible dans $F_q[x]$. — Ann. Fac. Sci. Toulouse Math., v. **6**, 1984, no 3—4, p. 185—213.

CHENG C. L. [1*] Formulas for the solutions of quadratic equations over GF (2^m). — IEEE Trans. Inform. Theory, v. **28**, 1982, no 5, p. 792—794.

CLAASEN H. L. [1*] More on the group of units in $GF(q)[x]/(a(x))$. — Delft. Progr. Rept., v. **8**, 1983, no 4, p. 274—291.

COHEN H., LENSTRA H. W., Jr. [1*] Primality testing and Jacobi sums. — Math. Comput., v. **42**, 1984, no 165, p. 297—330.

COHEN S. D. [1*] Quadratic residues and character sums over fields of square order. — J. Number Theory, v. **18**, 1984, no 3, p. 391—395.

[2*] Primitive roots and powers among values of polynomials over finite fields. — J. Rein. Angew. Math., v. **350**, 1984, p. 137—151.

[3*] Consequtive primitive roots in a finite field. — Proc. Amer. Math. Soc. v. **93**, 1985, no 2, p. 189—197.

[4*] Consequtive primitive root in a finite field. II. — Proc. Amer. Math. Soc., v. **94**, 1985, no 4, p. 605—611.

COPPERSMITH D. [1*] Fast evaluation of logarithms in fields of characteristic two. — IEEE Trans. Inf. Theory, v. **30**, 1984, no 4, p. 587—594.

COPPERSMITH D., ODLYZKO A. M., SCHROEPPEL R. [1*] Discrete algorithms in $GF(p)$. — Algorithmica, v. **1**, 1986, no 1, p. 1—15.

DE VROEDT C. [1*] A formula for the weight of the product of a set of vectors belonging to the n-dimensional vector space over $GF(q)$. — Delft. Progr. Rept., v. **8**, 1983, no 3, p. 195—199.

EFFINGER G. [1*] A Goldbach theorem for polynomials of low degree over odd finite fields. — Acta Arithm., v. **42**, 1983, no 4, p. 329—365.

EGAMI S. [1*] The distribution of residue classes modulo p in an algebraic number field. — Tsucuba J. Math., v. **4**, 1980, p. 9—13.

EXPONENTIALSUMMEN (KLOOSTERMAN'SCHE SUMMEN). — Tagungsber. Math. Forschungsinst. Oberwolfach., 1984, no 19, 1—14.
GERTH F. [1*] An application of matrices over finite fields to algebraic number theory. — Math. Comput., v. **41**, 1983, no 163, p. 229—234.
GOLDFELD D., SARNAK P. [1*] Sums of Kloosterman sums. — Anvent. Math., v. **71**, 1983, no 2, p. 243—250.
GRYTCZUK A., TROPAK B. [1*] On the equation $\varphi_n(x, y) = 0$ in the Z_p field. — Zesz. Nauk., WSI. w Zielonej Górze, 1981, no 55, p. 15—18.
GUERRA L., UGHI E. [1*] On the distribution of Legendre symbols in Galois fields. — Discr. Math., v. **42**, 1982, no 2—3, p. 197—208.
HEATH-BROWN D. R. [1*] Multiple exponential sum to modulus p^2. — Canad Math. Bull., v. **28**, 1985, no 4, p. 394—396.
HELLEGOUARCH J. [1*] Loi de réciprocité critère de primalité dans $F_q[t]$. — Math. Repts. Acad. Sci. Can., v. **8**, 1986, no 5, p. 291—296.
HELLESETH T. [1*] On the covering radius of cyclic linear codes. — Discr. Appl. Math., v. **11**, 1985, p. 157—173.
HELLMAN M., REYNERI J. M. [1*] Fast computation of discrete logarithms in *GF* (*q*). — Adv. Criptol. Proc. Crypt. 82: Workshop Theory and Appl. Cryptogr. Techn., Santa Barbara, Calif., 23—25 Aug. 1982, N.-Y., London, 1983, p. 3—19.
HENSLEY D. [1*] Dirichlet theorem for the ring of polynomials over *GF* (2). — Pacific J. Math., v. **123**, 1986, no **1**, p. 93—101.
HINZ J. [1*] The average order of magnitude of least primitive roots in algebraic number fields. — Mathematika., v. **30**, 1983, no 1, p. 11—25.
[2*] Character sums in algebraic number field. — J. Number Theory, v. **17**, 1983, no 1, p. 52—70.
[3*] Character sums and primitive roots in algebraic number fields. — Monatsh Math., v. **95**, 1983, no 4, p. 275—286.
[4*] Über die Verteilung von primen primitiven Wurzlen in algebraischen Zahlkörpern. — Monatsh. Math., v. 100, 1985, no 4, p. 259—275.
HUDSON R. H. [1*] On the first occurrence of certain patterns of quadratic residues and non-residues. — Israel J. Math., v. **44**, 1983, no 1, p. 23—32.
[2*] A note on *k*-th power nonresidues. — Manuscripta Math., v. **42**, 1983, p. 285—288.
HUDSON R. H., WILLIAMS K. S. [1*] Binomial coefficients and Jacobi sums. — Trans. Amer. Math. Soc., v. **281**, 1984, no 2, p. 431—505.
HUXLEY M. N. [1*] A note on polynomial congruences. — Recent Progr. Anal. Numb. Theory, 1981, p. 193—196.
KALTOFEN E. [1*] Factorization of polynomials. — Computing., 1982, Suppl. no 4, p. 95—113.
[2*] Fast parallel absolute irreducibility testing. — J. Symb. Comput., 1985, no 1, p. 57—67.
KAMINSKI M. [1*] A lower bound for polynomial multiplication. — Theor. Comput. Sci., v. **40**, 1985. no 2—3, p. 319—322.
KASHIWAGI H., MORIUCHI T. [1*] A fast method fot arithmetic modulo a polynomial over *GF* (2) and its applications. — Conrt. Sci. and Technol. Progr. Soc. Proc. 8-th Trienni. World Congr. Int. Fed. Autom. Contr., Kyoto, 1981, v. **1**, Oxford, 1982, p. 237—242.
KASHIWAGI H., UCHIMURA T. [1*] A simple method for obtaining primitive pentanomials over *GF* (2). — Trans. Soc. Instr. Contr., Eng., v. **18**, 1982, no 7, p. 747—750.
KATRE S. A., RAJWADE A. R. [1*] Complete solution of the cyclotomic problem in F_q for any prime modulus m, $q = p^k$, $p \equiv 1 \pmod{m}$. — Acta Arithm., v. **45**, 1985, no 3, p. 183—199.

[2*] Unique determination of cyclotomic numbers of order five. — Manuscr. Math., v. **53**, 1985, no 1—2, p. 65—75.
KOH K. [1*] On the matrix ring over a finite field. — Linear Algebra and Appl., v. **66**, 1985, p. 195—197.
LEMPEL A., SEROUSSI G., WINOGRAD S. [1*] On the complexity of multiplication in finite fields. — Theor. Comput. Sci., v. **22**, 1983, no 3, 285—296.
LEMPEL A., SEROUSSI G., ZIV J. [1*] On the power of straight-line computations in finite fields. — IEEE Trans. Inf. Theory, v. **28**, 1982, no 6, p. 875—880.
LENSTRA A. K. [1*] Factorization of polynomials. — SIGSAM Bull., v. **18**, 1984, no 2, p. 16—18.
[2*] Factoring multivariate polynomials over finite fields. — J. Comput. Syst. Sci., v. **30**, 1985, no 2, p. 235—248.
LEWIS D. J. [1*] Cubic homogeneous polynomials over p-adic number fields. — Ann. Math., v. **56**, 1952, no 3, p. 473—478.
LIDL R., NIEDERREITER H. [1*] Introduction to finite fields and their applications. — Cambrige University Press, 1986.
LOXTON J. H., VAUGHAN R. C. [1*] The estimation of complete exponential sums. — Canad. Math. Bull., v. 28, 1985, No 4, p. 440—454.
MONZINGO M. G. [1*] On elementary evaluation of Jacobsthal sum. — J. Number Theory, v. **22**, 1986, no 1, p. 21—25.
MUKHOPADHYAY A. [1*] On the probability that the determinant of an $n \times n$ matrix over a finite field vanished. — Discrete Math., v. **51**, 1984, no 3, p. 311—315.
MUSKAT J. B., WILLIAMS K. S. [1*] Cyclotomy of order twelve over $GF(p^2)$, $p^2 \equiv 1 \pmod{12}$. — Carleton Math. Ser., 1985, no 217.
NAGELL T. [1*] Introduction to number theory. — Stockholm: Almqvist and Wiksell, 1951.
NARANJANI A. M. [1*] On Dirichlet characters of polynomial. — Acta Arithm., v. **43**, 1984, no 3, p. 245—251.
NIEDERREITER H. [1*] Distribution properties of feedback shift register sequences. — Проблемы управления и информ., т. **15**, 1986, № 1, с. 19—33.
NÖBAUER R. [1*] Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen. — Acta Arithm., v. **45**, 1985, no 2, p. 171—181.
[2*] Über die minimale Fixpunktanzahl von Dickson-Permutationen auf Galoisfeldern. — Monatsh. Math., v. 101, 1986, no 3, p. 193—210.
OBERST U., DÜR A. [1*] A constructive characterization of all optimal linear codes. — Lect. Notes Math., 1985, no 1146, p. 176—213.
ODONI R. W. K. [1*] Trigonometric sums of Heilbronn's type. — Math. Proc. Cambrige Phil. Soc., v. **98**, 1985, no 3, p. 389—396.
[2*] A note on trigonometric sums in several variables. — Math. Proc. Cambrige Phil. Soc., v. **99**, 1985, no 2, p. 189—193.
ORZECH M. [1*] Form of low degree in finite fields. — Bull. Austral. Math. Soc., v. **29**, 1984, p. 45—58.
OZEKI M. [1*] On certain generalized Gaussian sums. — Proc. Jap. Acad., A58, 1982, no 5, p. 223—226.
PEI D. J., WANG C. C., OMURA J. K. [1*] Normal basis of finite field $GF(2^m)$. — IEEE Trans. Inform. Theory, v. **32**, 1986, no 2, p. 285—287.
SCHMIDT W. M. [1*] On cubic polynomials. I. Hua's estimate of exponential sums. — Monatsh. Math., v. **93**, 1982, no 1, p. 63—74.
[2*] On cubic polynomials. 2. Multiple exponential sums. — Monatsh. Math., v. **93**, 1982, no 2, p. 141—168.
[3*] Bounds for exponential sums. — Acta Arithm., v. **44**, 1984, no 3. p. 281—297.
SIVARAMAKRISHAN R., VIJAYAN B. K. [1*] On certain exponential and character sums. — Lect. Notes. Math., 1982, no 938, p. 138—156.
SMALL C. [1*] Diagonal equations over large finite fields. — Canad. J. of

Math., v. **36**, 1984, no 2, p. 249—262.
SMEETS B. [1*] On the number of polynomials over *GF* (2) that factor in 2, 3 and 4 prime polynomials. — BIT (Dan.), v. **25**, 1985, no 4, p. 667—674.
SMITS T. H. M. [1*] On the group of units of *GF* (*q*) [*x*]/(*a* (*x*)). — Delft. Progr. Rept., v. **6**, 1981, no 4, p. 231—235.
[2*] On the group of units of *GF* (*q*) [*x*]/(*a* (*x*)). — Proc. Kon. Ned. Akad. Wetensch., **A85**, 1982, no 3, p. 355—358.
SNAPPER E. [1*] Finite fields, integral matrices, and Diophantine equations. — Journ. of Algebra, v. **97**, 1985, no 1, p. 267—277.
SPACKMAN K. W. [1*] Linearly requrring solution sequences for equation over finite fields. — J. Number Theory, v. **18**, 1983, no 2, p. 209—218.
STOHR K.-O., VOLOCH F. [1*] Weierstrass points and curves over finite fields. — Proc. London Math. Soc., v. **52**, 1986, no 1, p. 1—19.
TAPPE J. [1*] Remarks on generalized cyclic codes. — Bayrenth. Math. Schr., 1984, no 16, p. 143—150.
TERJANIAN G. [1*] Un contre-exemple à une conjecture d'Artin. — Compt. Rend. Acad. Sci., t. **262**, 1966, p. 612.
TIETÄVÄINEN A. [1*] Lower bounds for the maximum moduli of certain character sums. — J. London. Math. Soc., v. **29**, 1984, no 2, p. 204—210.
TODOROW J., JANICKE O. [1*] Darstellung mehrwertiger Funktionen durch Reihenentwicklung nach orthogonalen Funktionensystemen über endlichen Körpern. — Z. Elek. Inf. und Energietechn., B. **13**, 1983, no 1, S. 69—80.
TSFASMAN M. A., VLADUTS S. G., ZINK Th. [1*] Modular curves, Shimura curves and Goppa codes better than Varshamov—Gilbert bound. — Math. Nachr., B. **104**, 1982, S. 15—28.
VAN DER GATHEN J. [1*] Irreducibility of multivariate polynomials. — J. Comput. and Syst. Sci., v. **31**, 1985, no 2, p. 225—264.
VAN DER GATHEN J., KALTOFEN E. [1*] Factorization of multivariate polynomials over finite fields. — Math. Comp., v. **45**, 1985, no 171, p. 251—261.
ZEITLER H. [1*] Rechnen in endlichen Körpern. — Elem. Math., v. **38**, 1983, no **4**, p. 89—93.

АРХИПОВ Г. И. [1*] О значении особого ряда в проблеме Гильберта—Камке. — Докл. АН СССР, т. **259**, 1981, № 2, с. 265—267.
[2*] О проблеме Гильберта—Камке. — Изв. АН СССР, сер. матем., т. **48**, 1984, № 1, с. 3—52.
АРХИПОВ Г. И., КАРАЦУБА А. А. [1*] О локальном представлении нуля формой. — Изв. АН СССР, сер. матем., т. **45**, 1981, № 3, с. 948—961.
[2*] О представлении нуля формой в поле *p*-адических чисел. — Докл. АН СССР, т. **262**, 1982, № 1, с. 11—13.
[3*] Об одной задаче теории сравнений. — Успехи матем. наук, т. **37**, 1982, № 5 (227), с. 161—162.
АРХИПОВ Г. И., КАРАЦУБА А. А., ЧУБАРИКОВ В. Н. [1*] Кратные тригонометрические суммы и их приложения. — Изв. АН СССР, сер. матем., т. **44**, 1980, № 4, с. 723—781.
[2*] Особые случаи теории кратных тригонометрических сумм. — Изв. АН СССР, сер. матем., т. **47**, 1983, № 4, с. 707—784.
АРХИПОВ Г. И., ЧУБАРИКОВ В. Н. [1*] Об арифметических условиях разрешимости нелинейных систем диофантовых уравнений. — Докл. АН СССР, т. **284**, 1985, № 1, с. 6—21.
БРОНШТЕЙН Б. С. [1*] Неограниченность сумматорной функции одного обобщенного характера. — Уч. Зап. МГУ, сер. мат., т. 7, 1954, с. 212—220.
ВАРШАМОВ Р. Р. [1*] Общий метод синтеза неприводимых полиномов над полями Галуа. — Докл. АН СССР, т. **275**, 1984, № 5, с. 41—44.
ВАРШАМОВ Р. Р., КОЖЕВНИКОВ Ю. А. [1*] Решение на ЭВМ задач построения полиномов в поле вычетов по модулю 2. — Сб. научн. трудов,

М., 1962. с. 170—175.
ВАРШАМОВ Р. Р., ТЕНЕНГОЛЬЦ Г. М. [1*] Об одном классе циклических кодов. — Проблемы кибери., т. 22. М.: Наука, 1970, с. 157—166.
ВИНОГРАДОВ И. М. [1*] Избранные труды. — М.: Изд. АН СССР, 1952.
[2*] Метод тригонометрических сумм в теории чисел. — М.: Наука, 1971.
ВИШНЕВЕЦКИЙ А. Л. [1*] О цикличности расширениых кодов Гоппы. — Пробл. передачи информ., т. **18**, 1982, № 3, с. 14—18.
[2*] (L, g)-коды и бинарные формы. — Пробл. передачи информ., т. **19**, 1983, № 4, с. 23—30.
ВЛЭДУЦ С. Г., КАЦМАН Г. Л., ЦФАСМАН М. А. [1*] Модулярные кривые и коды с полиномиальной сложностью построения. — Пробл. передачи ииформ., т. **20**, 1984, № 1, с. 47—55.
ГЛАЗУНОВ Н. М. [1*] О равнораспределенности значенний сумм Клостермана. — Докл. АН УССР, 1983, А, № 2, с. 9—12.
ГОЛУБЕВА Е. П. [1*] Связь сумм Салье с распределением целых точек на гиперболоидах. — Зап. научн. сем. ЛОМИ, т. **116**, 1982, с. 56—62.
ГОППА В. Я. [1*] Новый класс линейных корректирующих кодов. — Пробл. передачи информ., т. 6, 1970, № 3, с. 24—30.
[2*] Рационаальные представления кодов и (L, g)-коды: — Пробл. передачи информ., т. **7**, 1971, № 3, с. 41—49.
ГРИГОРЬЕВ Д. Ю. [1*] Разложение миогочленов над конечиым полем и решение систем алгебраических уравнений. — Зап. иаучн. сем. ЛОМИ АН СССР, т. **137**, 1984, с. 20—74.
ДЕМЬЯНОВ В. Б. [1*] О кубических формах в дискретно нормированных полях. — Докл. АН СССР, т. **74**, 1950, № 5, с. 889—891.
ДУМЕР И. И., ЗИНОВЬЕВ В. А. [1*] Некоторые новые максимальные коды над полем Галуа GF (4). — Пробл. передачи информ., т. **14**, 1978, № 3, с. 24—34.
ЕЛИСТРАТОВ И. В. [1*] Об оценках тригоиометрических сумм. — В кн.: Исслед. по теор. чисел, вып. 6, Саратов: изд. Сар. унив., 1976, с. 38—49.
[2*] Об оценках сумматорных функций возмущенных характеров Дирихле. — В кн. Иссл. по теор. чисел, вып. 7, Саратов: йзд. Сар. ун., 1978, с. 29—58.
ЕРШОВ Ю. Л. [1*] Об элементарных теориях локальных полей. — Алгебра и логика, т. 4, 1965, вып. 2, с. 5—30.
КАЛУЖНИН Л. А. [1*] Введение в общую алгебру. — М.: Наука, 1973.
КАРАЦУБА А. А. [1*] Оценки тригонометрических сумм особого вида и их приложение. — Докл. АН СССР, т. **137**, 1961, № 3, с. 513—514.
[2*] Аиалог проблемы Варинга. — Вестник МГУ, 1962, № 1, с. 38—46.
[3*] Проблема Вариига для сравнения по модулю, равному степени простого числа. — Вестник МГУ, 1962, № 4, с. 28—38.
[4*] Системы сравнений и уравиения Варинговского типа. — Докл. АН СССР, т. 165, 1965, № 2, с. 274—276.
[5*] Об одной асимптотической формуле. — Труды Моск. матем. общ., т. 18, 1968, с. 77—82.
[6*] Распределеиие степенных вычетов и иевычетов в аддитивных последовательностях. — Докл. АН СССР, т. 196, 1971, № 4, с. 759—760.
[7*] Об одиой арифметической сумме. — Докл. АН СССР, т. **199**, 1971, № 4, с. 770—772.
[8*] Об одиой системе сравиений. — Матем. заметки, т. **19**, 1976, № 3, с. 389—392.
[9*] О распределении зиачеиий иеглавиых характеров. — Труды Матем. инст. им. Стеклова АН СССР, т. **142**, 1976, с. 156—164.
[10*] Основы аналитической теории чисел. — М.: Наука, 1983.
[11*] Метод тригоиометрических сумм И. М. Виноградова. — Труды Матем. иист. им. Стеклова АН СССР, т. **163**, 1984, с. 97—103.
КАРГАПОЛОВ М. И., МЕРЗЛЯКОВ Ю. И. [1*] Основы теории групп. — М.: Наука, 1972.
КИСЛОВСКАЯ Н. М. [1*] Циклические последовательности иад конечиым

полем — В сб. Динамич. системы и теория приближений. Владивосток, 1979, с. 129—132.

КОНЯГИН С. В. [1*] О числе решений сравнения n-й степени с одним неизвестным. — Матем. сбори., 1979, № 2, с. 171—187.

КОСТРИКИН А. И. [1*] Введение в алгебру. — М.: Наука, 1977.

КУЗНЕЦОВ В. Н. [1*] Z-функции иекоторых Артии—Шрайеровых накрытий. — В кн. Иссл. по теор. чисел, вып. 5, Саратов: изд. Сар. унив. 1975, с. 74—81.

[2*] К гипотезе Э. Бомбьери. — В кн. Исслед. по теории чисел, вып. 5, Саратов: изд. Сарат. уиив., 1975, с. 81—93.

[3*] К вопросу оценки двумерных тригонометрических сумм. — В ки. Исслед. по теории чисел, вып. 6, Саратов: изд. Сарат. унив., 1975, с. 92—100.

КУРБАТОВ В. А. [1*] О симметрической группе поля. — Уч. зап. Свердл. гос. пед. иист., вып. 8, 1952, с. 23—31.

КУРОШ А. Г. [1*] Курс высшей алгебры. — М.: Наука, 1975.

[2*] Теория групп. — М.: Наука, 1967.

КЮРЕГЯН М. К. [1*] Разложеиие полиномов иад конечными полями. — Докл. АН АрмССР, т. **81**, 1985, № 2, с. 69—73.

[2*] Об одном методе построеиия иеприводимых полиномов над полями Галуа. — Докл. АН АрмССР, т. **83**, 1986, № 2, с. 58—61.

МАЗУР Л. Е. [1*] О некоторых кодах, исправляющих несимметрнческие ошибки. — Пробл. передачи информ., т. **10**, 1974, № 4, с. 40—46.

МАРЕНИЧ Е. Е. [1*] О числе неприводимых миогочлеиов над конечным полем. — В кн.: Математическая физика. — М.: Моск. гос. пед. ин-т им. Ленииа, 1986, с. 92—95.

МИТЬКИН Д. А. [1*] О величиие сумм характеров от многочленов. — Матем. заметки, т. **31**, 1982, № 6, с. 827—835.

[2*] Об оцеиках и асимптотических формулах для рациоиальных тригонометрических сумм, близких к полным. — Матем. сборник, т. **122**, 1983, № 4, с. 527—545.

[3*] Многочлеиы с минимальным множеством значений и уравнеиие $f(x) = f(y)$ в простом конечиом поле. — Матем. заметки, т. **38**, 1985, № 1, с. 3—14.

[4*] Об элемеитарием доказательстве оценки А. Вейля для рациональных тригоиометрических сумм с простым зиамеиателем. — Изв. вузов. Математика, 1986, № 6, с. 14—17.

МИШИНА А. П., ПРОСКУРЯКОВ И. В. [1*] Высшая алгебра. — М.: Физматгиз, 1962.

МУРЗАЕВ Е. А. [1*] Об одном методе установления признаков неприводимостн полиномов. — Уч. зап. Сарат. гос. пед. иист., вып. 23, 1956, с. 107—114.

[2*] Об одиом алгоритме для выделения корией многочлена, удовлетворяющих заданному рациоиальиому соотношеиию, и его прнложениях к разложеиию миогочленов на неприводимые множителн. — В кн. Исслед. по теории чисел, вып. 1. Саратов, 1966, с. 35—48.

НЕЧАЕВ В. И. [1*] Линейиые сравнения по степенн простого идеала и линейиые рекуррентные последовательиостн. — Уч. зап. Моск. педаг. иист., т. **375**, 1971, с. 124—132.

ПЕРЕЛЬМУТЕР Г. И. [1*] Об особых точках иормальных иакрытий Артина—Шрайера. — В кн. Иссл. по теории чисел, вып. 6, Саратов, 1976, с. 119—128.

[2*] Оценка двумериой суммы символов Лежаидра. — В кн.: Иссл. по теории чисел, вып. 8, Саратов, 1982, с. 88—92.

ПОСТНИКОВ А. Г. [1*] Введеиие в аиалитическую теорию чисел. — М. Наука, 1971.

ПОСТНИКОВ М. М. [1*] Теория Галуа. — М.: Физматгиз, 1963.

ПОСТНИКОВА Л. П. [1*] Тригонометрические суммы и теория сравнений

по простому модулю. — М.: Изд. МГПИ им. Леннна, 1973.
СЕЙТЕНОВ С. М. [1*] Элементарная теория решеток подполей конечных полей. — В сб. Некоторые вопросы алгебраической теории чисел и конструктивных моделей. — Алма—Ата, 1985, с. 71—80.
СИДЕЛЬНИКОВ В. М. [1*] О спектре весов двоичных кодов Боуза—Чоудхури—Хоквингема. — Пробл. передачи ннформ., т. 7, 1971, № 1, с. 14—22.
[2*] Об экстремальных многочленах, используемых при оцеиках мощности кода. — Пробл. передачи информ., т. **16**, 1980, № 3, с. 17—30.
СИДОРЕНКО В. Р. [1*] Верхняя граница мощности q-ичных кодов. — Пробл. передачи информ., т. **11**, 1975, № 3, с. 14—20.
СКОРНЯКОВ Л. А. [1*] Элементы алгебры. — М.: Наука, 1980.
СОБОЛЬ И. М. [1*] О распределении точек в кубе и приближенном вычислении интегралов. — Журн. выч. мат. и мат. физ., т. 7, 1967, № 4, с. 784—802.
[2*] Многомерные квадратурные формулы и функции Хаара. — М.: Наука, 1969.
СТЕПАНОВ С. А. [1*] Об оценке рациональных тригонометрических сумм вдоль кривой. — Докл. АН СССР, т. 277, 1984, № 5, с. 1077—1082.
[2*] Рацноиальные тригоиометрические суммы вдоль кривой. — Зап. иаучн. сем. ЛОМИ АН СССР, т. **134**, 1984, с. 232—251.
[3*] О числе неприводимых в $\mathbb{F}_q[x]$ многочленов специального вида. — Успехи матем. наук, т. **40**, 1985, № 4, с. 199—200.
[4*] Рациональные тригонометрические суммы на «алгебраическом многообразии». — Матем. заметки, т. **39**, 1986, № 2, с. 161—174.
[5*] Об оценке рациональных тригонометрических сумм иа алгебраическнх многообразиях. — Докл. АН СССР, т. **286**, 1986, № 2, с. 298—301.
СТЕЧКИН С. Б. [1*]. Об оценке сумм Гаусса. — Матем. заметки, т. **17**, 1975, № 4, с. 579—588.
СУШКЕВИЧ А. К. [1*] Основы высшей алгебры. — М.—Л.: ГИТТЛ, 1941.
ФАДДЕЕВ Д. К. [1*] Лекции по алгебре. — М.: Наука, 1984.
ЦФАСМАН М. А. [1*] Коды Гоппы, лежащие выше граннцы Варшамова—Гильберта — Пробл. передачи информ., т. **18**, 1982, № 3, с. 3—6.
ЧУБАРИКОВ В. Н. [1*] Асимптотическая формула средиего зиачення кратиой тригонометрической суммы. — Матем. заметки, т. **23**, 1978, № 6, 799—816.
[2*] Об асимптотических формулах для интеграла И. М. Виноградова и его обобщений. — Труды Матем. иист. им. Стеклова АН СССР, т. **157**, 1981, с. 214—232.
[3*] Кратные тригоиометрические суммы с простыми числами. — Докл. АН СССР, т. **278**, 1984, № 2, с. 302—304.
ШМИДТ О. Ю. [1*] Абстрактная теория групп. М.: ОНТИ, 1933 (а также в кн.: Шмидт О. Ю.. Избранные труды (Математнка). М.: Изд. АН СССР, 1959).
ШПАРЛИНСКИЙ И. Е. [1*] Распределеиие дробиых долей рекуррентных последовательностей. — Журн. выч. мат. и мат. физ., т. **21**, 1981, № 6, с. 1588—1591.
[2*] О некоторых свойствах линейных циклических кодов. — Пробл. передачи информ., т. **19**, 1983, № 3, с. 106—110.
[3*] О скорости сходнмости интерполяциоиного процесса Ньютона и мощности некоторых кодов. — Усп. матем. наук, т. **39**, 1984, № 2, с. 205—206.
[4*] О коэффициеитах примитивиых многочленов. — Матем. заметки, т. **38**, 1985, № 6, с. 810—815.
[5*] О весовых спектрах некоторых кодов. — Пробл. передачи информ., т. **22**, 1986, № 2, с. 43—48.

Указатель обозначений

$\mathbb{C}$	множество комплексных чисел
$\mathbb{N}$	множество натуральных (целых положительных) чисел
$\mathbb{Q}$	множество рациональных чисел
$\mathbb{R}$	множество действительных чисел
$\mathbb{Z}$	множество целых чисел
$\{ah \mid h \in H\}$	множество произведений ah, где $h \in H$
A^{T}	транспонированная матрица для матрицы A
$\det(A)$	определитель матрицы A
$\dim(V)$	размерность векторного пространства V
$e(t)$	$e^{2\pi i t}$, где $t \in \mathbb{R}$
$\operatorname{Im} z$	мнимая часть комплексного числа z
$\log a$	натуральный логарифм числа a
$\max\{k_1, \ldots, k_n\}$	наибольшее из чисел $k_1, \ldots, k_n$
$\min\{k_1 \ldots, k_n\}$	наименьшее из чисел $k_1, \ldots, k_n$
$\operatorname{Re} z$	действительная часть комплексного числа z
$\operatorname{rg}(A)$	ранг матрицы A
$(s_1, s_2, \ldots, s_n)$	n-набор, или упорядоченное множество из n элементов $s_1, s_2, \ldots, s_n$
S^n	множество всех n-наборов вида $(s_1, \ldots, s_n)$, где $s_i \in S$, $1 \leqslant i \leqslant n$
$S_1 \times \ldots \times S_n$	множество всех n-наборов вида $(s_1, \ldots, s_n)$, где $s_i \in S_i$, $1 \leqslant i \leqslant n$
$\operatorname{Tr}(A)$	след матрицы $A = (a_{ij})_{1 \leqslant i,\ j \leqslant n}$, т. е. $a_{11} + \ldots + a_{nn}$
$\bar{z}$	комплексное число, сопряженное с числом z (т. е. $z = a - bi$, если $z = a + bi$, $a, b \in \mathbb{R}$)
$\lvert z \rvert$	абсолютная величина числа $z \in \mathbb{R}$ или модуль числа $z \in \mathbb{C}$ (т. е. $\lvert z \rvert = \sqrt{a^2 + b^2}$, если $z = a + bi$, $a, b \in \mathbb{R}$)
НОД $(k_1, \ldots, k)$	наибольший общий делитель чисел $k_1, \ldots, k_n$

НОК $(k_1, \ldots, k_n)$ наименьшее общее кратное чисел $k_1, \ldots, k_n$

$\sum_{a \in A} f(a)$ сумма значений $f(a)$ по всем $a \in A$

$\square$ конец доказательства, примера или замечания

$\Longleftrightarrow$ необходимо и достаточно, чтобы...

$a \equiv b \pmod{n}$ a сравнимо с b по модулю n 15

$\langle a \rangle$ циклическая группа, порожденная элементом a 15, 17

aH левый смежный класс группы по подгруппе H (содержащий элемент a) 18

(a) главный идеал кольца, порожденный элементом a 26

$[a]$, $a + J$ класс вычетов кольца по модулю идеала J 26

$[A_0, A_1, \ldots, A_s]$ непрерывная дробь, представляющая рациональную функцию 290

A_q знакопеременная группа степени q 450

$AG(2, K)$ аффинная плоскость над полем K 619

$AG(m, \mathbb{F}_q)$ конечная аффинная (или евклидова) геометрия 631

$\left(\frac{c}{p}\right)$ символ Лежандра 242

$C^{\perp}$ дуальный (или ортогональный) код для линейного кода C 598

$\deg(f)$ степень многочлена f 34, 45

$D(f)$ дискриминант многочлена f 53

$\det(T)$ определитель линейного оператора T 80

$\det(f)$ определитель квадратичной формы f 344

$D_n^{(r)}$ ганкелев определитель 547

$d(\mathbf{x}, \mathbf{y})$ расстояние Хэмминга между векторами $\mathbf{x}$ и $\mathbf{y}$ 591

d_C минимальное расстояние линейного кода C 592

E^n множество корней n-й степени из единицы над полем K 84

$E(\psi)$ сумма Эйзенштейна 325

$E_s(\psi; a)$ обобщениая сумма Эйзенштейна 326

$E_p(r)$ 363

$E^{(n)}(f)$ n-я гиперпроизводная многочлена f 372

$\mathbb{F}_p$ поле Галуа порядка p (p — простое число) 28

f' производная многочлена f 43

$\mathbb{F}_q$ поле Галуа порядка $q = p^n$ (p простое, $n \in \mathbb{N}$) 68

$\mathbb{F}_q^*$ мультипликативная группа иенулевых элементов конечного поля $\mathbb{F}_q$ 69

f^* многочлен, возвратный (двойственный) к многочлену f 114

$\mathbb{F}_q[[x]]$ кольцо формальных степенных рядов над полем $\mathbb{F}_q$ 518

$f_1(x) \vee \ldots \vee f_h(x)$ 542
$(G, *)$ группа с операцией $*$ 13
$|G|$ порядок конечной группы G 16
$(G : H)$ индекс подгруппы H в группе G 18
G/H факторгруппа группы G по нормальной подгруппе H 22
$GF(p)$ поле Галуа порядка p (p — простое число) 28
$GF(q)$ поле Галуа порядка $q = p^n$ (p простое, $n \in \mathbb{N}$) 68
$G^\wedge$ множество (группа) характеров группы G 236
$G(\psi, \chi)$ сумма Гаусса 243
$g_k(x, a)$ многочлен Диксона 447
$GL(r, \mathbb{F}_q)$ общая линейная группа невырожденных $r \times r$-матриц над полем $\mathbb{F}_q$ 455
$g_k^{(i)}(x_1, \ldots, x_n, a)$ многочлен Диксона от n переменных 472
$H_n(a)$ сумма Якобсталя 285
$I(n, q; x)$ произведение всех нормированных неприводимых многочленов степени n из $\mathbb{F}_q[x]$ 122
$I_n(a)$ 285
$J(\lambda_1, \ldots, \lambda_h)$ сумма Якоби 257
$J_0(\lambda_1, \ldots, \lambda_h)$ 257
$\mathrm{Ker}(f)$ ядро гомоморфизма f 21, 28
$K(M)$ расширение поля K, полученное присоединением элементов множества M 47
$\bar{K}$ алгебраическое замыкание поля K 59
K^n n-круговое поле над K 84
$K(\chi; a, b)$ сумма Клостермана 280
K_r кратная сумма Клостермана 313
$K(\psi, \chi; a, b)$ обобщенная сумма Клостермана 327
$[L : K]$ степень поля L над K 48
$L_1(x) \otimes L_2(x)$ символическое произведение q-многочленов 148
$L(V, f; t)$ L-функция многообразия V 416
$M(d_1, \ldots, d_n)$ 357
$N(b)$ нормализатор элемента b группы 22
$N(S)$ нормализатор подмножества S группы 22
$\binom{n}{k}$ биномиальный коэффициент 60
$N_{F/K}(\alpha)$ норма элемента α поля F над подполем K 77
$N_q(n)$ число нормированных неприводимых многочленов степени n в $\mathbb{F}_q[x]$ 121
$N(f(x_1, \ldots, x_n) = b$ число решений уравнения $f(x_1, \ldots, x_n) = b$ в $\mathbb{F}_q^n$ 346
$\mathrm{ord}(f)$ порядок многочлена f над конечным полем 110
$PG(2, K)$ проективная плоскость над полем K 619
$PG(m, \mathbb{F}_q)$ конечное проективное пространство, или проективная геометрия 628
$Q_n(x)$ n-круговой многочлен 85

$(R, +, \cdot)$	кольцо с операциями $+$ и $\cdot$ 24
R/J	факторкольцо кольца R по идеалу J 27
$R[x]$	кольцо многочленов над кольцом R 34
$R[x_1, \ldots, x_n]$	кольцо многочленов от n переменных над кольцом R 44
$R(f, g)$	результант многочленов f и g 54
$[s]$	класс эквивалентности элемента s (класс вычетов по модулю n, если речь идет о сравнениях по модулю n) 15, 16
$\langle S \rangle$	подгруппа группы, порожденная ее подмножеством S 17
S_q	симметрическая группа степени q 449
$S(f(x))$	530
$S(\mathbf{y})$	синдром вектора $\mathbf{y}$ 594
$\mathrm{Tr}_{F/K}(\alpha)$	след элемента α поля F над подполем K 74
$\mathrm{Tr}_F(\alpha)$	абсолютный след элемента α поля F 74
$\lvert T \rvert$	мощность конечного множества T 334
$\lfloor t \rfloor$	наибольшее целое число, не превосходящее $t \in \mathbb{R}$ 363
$v(b)$	специальная целочисленная функция на конечном поле 345
$V(f)$	число различных значений многочлена f 456
$w(\mathbf{x})$	вес Хэмминга вектора $\mathbf{x}$ 591
Z_n	группа классов вычетов по модулю n 16
$Z/(n)$	кольцо вычетов по модулю n 27
$Z(V; t)$	дзета-функция на многообразии V 412
НОД $(f_1, \ldots, f_n)$	наибольший общий делитель многочленов $f_1, \ldots, f_n$ 36
НОК $(f_1, \ldots, f_n)$	наименьшее общее кратное многочленов $f_1, \ldots, f_n$ 37, 38
$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$	дискриминант элементов $\alpha_1, \ldots, \alpha_m$ поля F над подполем K 81, 82
η	квадратичный характер 242
$\Lambda_k(a)$	сумма Бревера 316
$\mu(n)$	функция Мёбиуса 120
$\sigma_k(x_1, \ldots, x_n)$	k-й элементарный симметрический многочлен 46
$\varphi(n)$	функция Эйлера 19, 59
$\Phi_q(f)$	аналог функции Эйлера для многочленов 157
χ	характер, сопряженный с характером χ 236
χ_0	тривиальный аддитивный характер 240
χ_1	канонический аддитивный характер 240
χ_b	аддитивный характер, определяемый равенством $\chi_b(c) = \chi_1(bc)$ 240
ψ_0	тривиальный мультипликативный характер 241
ψ_i	мультипликативный характер, определяемый ра-

венством $\psi_j(g^k) = e^{2\pi i j k/(q-1)}$ (g — примитивный элемент поля $\mathbb{F}_q$) 241

$\overset{\circ}{\prod}$ композиция отображений 20

$\prod_{d|n}$ произведение, распространяющееся на все натуральные делители d числа n 120

$\sum_{d|n}$ сумма, распространяющаяся на все натуральные делители d числа n 120

автоморфизм группы (automorphism of a group) 20
— — внутренний (inner) 20
— поля F над подполем K (of F over K) 73
— Фробениуса (Frobenius) 99
алгоритм Берлекэмпа (Berlekamp algorithm) 192
— Берлекэмпа—Месси (Berlekamp—Massey) 550
— декодирования (decoding) 593, 611
— деления (division) 35
— диагонализации (diagonalization) 208
— для определения цикловой суммы ЛМС (procedure for determining the cycle sum of an LMS) 652
— Евклида (Euclidian algorithm) 37
— Миньотта (Mignotte) 570
— разложения в непрерывную дробь (continued fraction) 289
— Цассенхауза (Zassenhaus) 205
алфавит входной (input alphabet) 643
— выходной (output) 643
аннулятор подгруппы (annihilator of a subgroup) 239
ассоциативность (associativity) 13, 24

базис поля F над подполем K (basis of F over K) 74
— — автодуальный (self-dual) 79
— — дуальный (dual, complementary) 78
— — нормальный (normal) 79, 669
— — — дуальный (dual) 669
— — полиномиальный (polynomial) 79
— — следоортогональный (trace-orthogonal) 100
башня расширений полей (chain of extension fields) 76
бином (binomial) 160
блок (block) 632
— элементарный (elementary) 651
блок-схема (block design) 631
— уравновешенная неполная (balanced incomplete) 632
(v, k, λ)-блок-схема 632

вектор кодовый (code vector) 589
— начального состояния (initial state) 498
— n-го состояния (n-th state) 498
— ошибок (error vector, error word) 591
— перестановочный полиномиальный (permutation polynomial) 486
— циклический (cyclic) 80
векторы ортогональные (orthogonal vectors) 598
вес Хэмминга (Hamming weight) 591
вход ЛМС (input of a LMS) 644
выход ЛМС (output of a LMS) 644

геометрия аффинная конечная (finite affine geometry) 631
— евклидова (euclidean) 631
— проективная (projective) 628
— — конечная (finite) 628
гиперплоскость (hyperplane) 628
гиперпроизводная (hyperderivative) 372
гипотеза Римана (Riemann hypothesis) 406
— Римана—Вейля (Riemann — Weil) 414
гомоморфизм (homomorphism) 20, 28
— на (on) 20
граница Варшамова—Гилберта (Gilbert—Warshamov bound) 597

— Плоткина (Plotkin) 597
— Синглетона (Singleton) 661
— Хэмминга (Hamming) 596
группа (group) 13
— абелева (abelian, commutative) 13
— аддитивная (additive) 13
— бесконечная (infinite) 16
— Бетти—Матье (Betti—Mathieu) 455
— Галуа (Galois) 99
— классов вычетов по модулю n (of integers modulo n) 16
— коммутативная (commutative, abelian) 13
— конечная (finite) 16
— общая линейная (general linear) 502
— циклическая (cyclic) 15
группоид (groupoid) 56
группы изоморфные (isomorphic groups) 20

двучлен (binomial) 160
декодирование в ближайшее кодовое слово (nearest neighbor decoding) 591
деление углом (long division) 35
делитель единицы (divisor of the identity, unit) 31
— многочлена (of a polynomial) 35
— наибольший общий (greatest common) 36
— нормальный группы (normal subgroup) 21
— элемента (of an element) 31
детерминаит квадратичной формы (determinant of quadratic form) 344
децимация (decimation) 575
дискриминаит многочлена (discriminant of a polynomial) 53
— элемеитов поля F над подполем K (of elements of F over K) 81
дистрибутивность (distributivity) 24
длина кода (length of a code) 589
дополнение бинарное (binary complement) 537

единица (identity, unity element) 13, 25

закои взаимности квадратичный (law of quadratic reciprocity) 255
замкиутость операции (closure property of an operation) 13
замыкаиие алгебраическое (algebraic closure) 59
значение многочлеиа от x при $x = c$ (polynomial expression in c) 33
— начальное рекуррентной последовательности (initial value of a recurring sequence) 495
— ошибки (error value) 612

идеал (ideal) 26
— главный (principal) 26
— максимальный (maximal) 31
— порожденный элементом (generated by an element) 26
— простой (prime) 31
изоморфизм группы (isomorphism of a group) 20
индекс подгруппы в группе (index of a subrgoup in a group) 18
— (элемента) 667

касательная (tangent) 624
квадрат латинский (latin square) 55, 637
— магический (magic) 666
квадраты латинские ортогональные (orthogonal latin squares) 637
класс смежный (coset) 18, 493
— сопряженности (conjugacy class) 23
— эквивалентности (equivalence class) 15
классы вычетов по модулю идеала J (residue classes modulo J) 26
— — по модулю n (equvalence classes modulo n) 16
код бинариый (binary code) 589
— — Хэмминга (Hamming) 596
— БЧХ (Боуза—Чоудхури—Хоквингема) (BCH-code) 609
— — в узком смысле (narrow sense) 609
— — примитивный (primitive) 609
— групповой (group) 589
— дуальный (dual, orthogonal) 598
— исправляющий t ошибок (t error correcting) 591
— линейный (linear) 589
— ортогональный (dual, orthogonal) 598
— реверсивный (reversible) 663
— Рида—Соломона (Reed—Solomon) 609
— с общей проверкой на четиость (parity-check) 590
— с повторением (repetition) 590
— систематический (systematic) 589
— совершенный (perfect) 661
— цнклический (cyclic) 601
— — максимальный (maximal) 603
— — укорочеиный (shortened) 604
кольцо (ring) 24

— без делителей нуля (ring with no zero divisors) 25
— вычетов (residue class ring, factor ring) 27
— главных идеалов (principal ideal domain) 31
— евклидово (euclidean ring) 57
— коммутативное (commutative ring) 24
— конечное (finite ring) 25
— многочленов (polynomial ring) 35
— полиномиально полное (polynomially complete ring) 474
— положительной характеристики (ring of positive characteristic) 29
— с делением неассоциативное (nonassociative division ring) 658
— с единицей (ring with identity) 24
— с однозначным разложением (unique factorization domain) 58
— тернарное (ternary ring) 657
— факториальное (unique factorization domain) 58
— характеристики 0 (ring of characteristic 0) 29
— целостное (integral domain) 24
— целых алгебраических чисел (ring of algebraic integers) 255
композиция многочленов (composition of polynomials) 148
— отображений (of maps) 20
компонента вынужденная (forced component) 648
— свободная (free) 648
коника (conic) 624
— вырожденная (degenerate) 624
— невырожденная (nondegenerate) 624
константа (constant) 34
конфигурация тактическая (tactical configuration) 632
координаты однородные (homogeneous coordinates) 621
корень многочлена (root, zero of a polynomial) 42
— — кратный (multiple) 43
— — q-первообразный над $\mathbb{F}_{q^m}$ (q-primitive over $\mathbb{F}_{q^m}$) 154
— — простой (simple) 43
— первообразный по модулю p (primitive root modulo p) 97
— n-й степени из единицы (n-th root of unity) 84
— — — — — первообразный (primitive) 85
коэффициент многочлена старший (leading coefficient of a polynomial) 24
— полиномиальный (polynomial) 364
— формального степенного ряда (of formal power series) 516
кратное аффинное многочлена (affine multiple of a polynomial) 144
— наименьшее общее (least common multiple) 37
кратность корня (multiplicity of a root) 43
кривая алгебраическая (algebraic curve) 455, 666
— эллиптическая (elliptic) 408
критерий подполя (subfield criterion) 68
— Эрмита (Hermite's) 439

лемма Артина (Artin lemma) 79
лидер смежного класса (coset leader) 593
ЛМС (линейная модулярная система) (LMS) 644
логарифм Якоби (Jacobi's logarithm) 104, 668
локатор ошибки (error-location number) 606

матрица Адамара (Hadamard matrix) 640
— — нормализованная (normalized) 641
— из многочленов (of polynomials) 205
— — — невырожденная (nonsingular) 205
— — — нормализованная (normalized) 208
— — — унимодулярная (unimodular) 205
— инволютивная (involutory) 398
— инцидентности (incidence) 633
— квадратичной формы (coefficient matrix of quadratic form) 342
— кодирующая (generator) 590
— кососимметрическая (skew-symmetric) 396
— порождающая (generator) 590
— — — каноническая (canonical) 590
— проверочная (parity-check) 589
— сопровождающая (companion) 90, 132
— стандартная (canonical generator) 590
— характеристическая (characterizing) 644
— — основная (characteristic) 644
— эрмитова (Hermitian) 397
матрицы из многочленов эквивалентные (equivalent matrices of polynomials) 206
— подобные (similar) 666

метод Кронекера (Kronecker's method) 61
многочлен (polynomial) 33, 44
— абсолютно неприводимый (absolutely irreducible) 369, 455
— аннулирующий (annihilate) 80
— q-ассоциированный (conventional q-associate) 148
— аффинный кратный (affine multiple) 144
— без кратных неприводимых сомножителей (with no repeated factors) 188
— возвратный (reciprocal) 114
— — характеристический (characteristic) 521
— вполне перестановочный (complete mapping) 481
— — разлагающийся (split) 52
— вычетный (residue) 475
— двойственный (reciprocal) 114
— делящий g (dividing g) 35
— делящийся на g (divisible by g) 35
— Диксона (Dickson) 447, 472
— допустимый (admissible) 490
— исключительный (exceptional) 456
— квазиперестановочный (crude permutation) 481, 490
— квазисамовозвратный (quasi-self-reciprocal) 169
— кратный (multiple) 35
— n-круговой (nth cyclotomic) 85
— линеаризованный (linearized) 139
— — q-ассоциизованный (q-associate) 148
— локаторов ошибки (error-locator) 613
— минимальный (minimal) 48, 80, 525
— неприводимый (irreducible) 38, 117
— иормированный (monic) 34
— нулевой (zero) 34
— однородный (homogeneous) 45, 338
— от перемеиных $x_1, \ldots, x_n$ (in $x_1, \ldots, x_n$) 44
— перестановочный (permitation) 438, 462
— — локальный (local) 487
— — по модулю p (modulo p) 491
— подпримитивный (subprimitive) 170
— порождающий (generator) 603
— постоянный (constant) 34
— приведенный (monic) 34
— приводимый (reducible) 38
— примитивный (primitive) 116
— проверочный (parity-check) 603
— f-разлагающий (f-reducing) 189
— самовозвратный (self-reciprocal) 169
— символически делящий g (symbolically dividing g) 149
— — делящийся на g (divisible by g) 149
— — неприводимый (irreducible) 151
— симметрический (symmetric) 45
— — элементарный k-й (kth elementary) 46
— унитарный (monic) 34
— факторизуемый (factoriable) 172
— характеристический (characteristic) 74, 80, 132, 507
— n-циклотомический (nth cyclotomic) 85
q-многочлен (q-polynomial) 139
— аффинный (affine) 144
— минимальный (minimal) 155
многочлены q-ассоциированные (q-associates) 148
— взаимно простые (relatively prime polynomials) 37
— — — попарно (pairwise) 37
— допустимые эквивалентные (admissible equivalent) 491
— перестановочные эквивалентные (permutational equivalent) 473
множество разиостное (difference set) 635
— Зиигера (Singer) 658
моноид (monoid) 56

НОД (наибольший общий делитель) (gcd) 36
НОК (наименьшее общее кратное) (lcm 37
норма (norm) 77
нормализатор (normalizer) 22
нуль кольца (zero element of a ring) 24
— многочлена (root, zero of a polynomial) 42, 64
нуль-пространство матрицы (null space of a matrix) 190
нумератор весов кода (weight enumerator of a code) 598

область целостности (integral domain) 24
образ гомоморфиый (homomorphic image) 20
образующий циклической группы (generator of cyclic group) 15
овал (oval) 625
— регулярный (regular) 664
— трансляционный (translation) 664
операция бинарная (binar operation) 12
определитель ганкелев (Hankel determinant) 547

— квадратичной формы (of quadratic form) 344
— линейного оператора (of linear operator) 80
отношение инцидентности (incidence relation) 617
— сравнимости по модулю n (congruence modulo n) 16
— эквивалентности (equivalence relation) 15

переменная (indeterminate) 33
период последовательности (period of a sequence) 498
— — минимальный (least) 498
k-плоскости параллельные (parallel k-flats) 631
плоскость аффинная (affine plane) 618
— дезаргова (Desargusian) 622
— недезаргова (non-Desargusian) 622
— проективная (projective) 617
— — конечная (finite) 617
— Фано (Fano) 617
k-плоскость (k-flat) 628
— бесконечно удаленная (at infinity) 631
подгруппа (subgroup) 17
— нормальная (normal) 21
— порожденная множеством (generated by a set) 17
— — элементом (generated by an element) 17
— собственная (nontrivial) 17
— тривиальная (trivial) 17
подкольцо (subring) 26
поднятие характера (character lifting) 248
подполе (subfield) 44
— простое (prime) 46
— собственное (proper) 46
— тела (of division ring) 92
— — максимальное (maximal) 93
подпространства аффинные параллельные (parallel affine subspaces) 335
показатель, которому принадлежит число a по модулю p (multiplicative order of a modulo p) 111
поле (field) 24
— алгебраических функций (of algebraic functions) 265
— Галуа (Galois) 28, 68
— конечное (finite) 27
— n-круговое (nth cyclotomic) 84
— разложения (splitting) 52
— рациональных функций (of rational functions) 369
— совершенное (perfect) 99
— n-циклотомическое (nth cyclotomic) 84
— эллиптических функций (of elliptic functions) 408
полином (polynomial) 33
полугруппа (semigroup) 56
полуполе (semifield) 658
порядок группы (order of a group) 16
— кольца (of a ring) 25
— конечной проективной плоскости (of finite projective plane) 618
— многочлена (of a polynomial) 110
— — приведенный (integral order, subexponent of a polynomial) 168
— состояния ЛМС (of state of a LMS) 649
последовательность де Бройна (de Bruijn sequence) 581
— линейная рекуррентная (linear requrring) 495
— — — неоднородная (inhomogeneous) 495
— — — однородная (homogeneous) 495
— максимального периода (maximal period) 514
— периодическая (ultimately periodic) 498
— порожденная импульсом (impulse response) 503
— псевдослучайная (pseudonoise) 572
— равномерно распределенная (uniformly distributed, equidistributed) 578
— Фибоначчи (Fibonacci) 566
— характеристическая (characteristic) 576
— чисто периодическая (periodic) 499
m-последовательность (m-sequence) 572
почти-поле (near-field) 657
предпериод (preperiod) 499
преобразование Фурье дискретное (discrete Fourier transform) 227
приведение многочлена по модулю f (reduction of a polynomial modulo f) 40
принцип двойственности (principle of duality) 617
— подстановки (of substitution) 42
присоединение элемента кольцевое (ring adjunction of an element) 57
проблема Варинга (Waring's problem) 177, 401
— Гольдбаха (Goldbach's) 177
произведение многочленов (product of polynomials) 34
— символическое (symbolic) q-многочленов 148
— скалярное (dot) 598

— характеров (of characters) 236
— элементов группы (of elements of a group) 13
производная (derivative) 43
пространство аннулируемое матрицы (null space of a matrix) 190
— внутренних состояний (state) 644
— входов (input) 644
— выходов (output) 644
— проективное (projective) 628
— — конечное (finite) 628
m-пространство (m-space) 628
процедура Ченя (Chien search) 614
прямая (line) 617
— бесконечно удаленная (at infinity) 620
прямые параллельные (parallel lines) 620

разбиение множества (partition of a set) 15
разложение многочлена на множители (factorization of a polynomial) 39
— — каноническое (canonical) 39
— p-чичное числа m (representation of m to base p) 364
— q-многочлена символическое (symbolic factorization) 151
размерность кода (dimension of a code) 589
— пространства (of a space) 628
разрядка (decimation) 575
расстояние конструктивное (designed distance) 609
— минимальное (minimum) 592
— Хэмминга (Hamming) 591
расширение поля (field extension) 46
— — алгебраическое (algebraic) 47
— — конечное (finite) 48
— — нормальное (normal) 49
— — полученное присоединением элементов множества M (obtained by adjoining the elements in M) 47
— — простое (simple) 47
— — трансцендентное (transcendental) 59
— — циклическое (cyclic) 99
регистр сдвига с обратной связью (feedback shift register) 496
рефлексивность (reflexivity) 15
ряд степенной формальный (formal power series) 516

секущая (secant) 624
символ входной (input symbol) 643
— выходной (output) 643
— информационный (message) 588
— контрольный (control) 588
— Лежандра (Legendre) 242
— проверочный (control) 588
симметричность (symmetry) 15
синдром вектора (syndrome of a vector) 593
система алгебраическая (algebraic system) 13
— Веблена—Веддербёрна (Veblen—Wedderburn) 657
— линейная модулярная (ЛМС) (linear modular) 644
— ортогональная (orthogonal) 462
— полная детерминированная с конечным числом состояний (complete deterministic finite-state) 643
— троек Штейнера (Steiner triple) 633
след (trace) 74
— абсолютный (absolute) 74
слова ортогональные (orthogonal words) 598
слово кодовое (code word) 588
— шумовое (error word, error vector) 591
сложение в кольце (addition in a ring) 25
соответствие (correspondence) 490
соотношение Дэвенпорта—Хассе (Davenport—Hasse relation) 263
— линейное рекуррентное (linear recurrence) 495
— — — неоднородное (inhomogeneous) 495
— — — однородное (homogeneous) 495
соотношения ортогональности для характеров (orthogonality relations for characters) 238
состояние внутреннее (state) 643, 644
— — регистра сдвига на n-м такте (nth state vector) 498
спектр перестановочный (простой) ((prime) permutation spectrum) 490
степень многочлена (degree of polynomial) 45
— — формальная (formal) 54
— поля F над подполем K (degree of F over K) 48
— рациональной функции (degree of a rational function) 291
— элемента θ поля над подполем K (degree of θ over K) 48
— n-я характера χ (nth power of χ) 236
— — элемента a (n-th power of a) 14
структура алгебраическая (algebraic structure) 13
— кольцевая, индуцированная отображением φ (ring strusture induced

by φ) 28
— цикловая (cycle) 575
сумма Бревера (Brewer sum) 316, 449
— Вейля (Weil) 269
— Гаусса (Gaussian) 243
— значений характера (character) 235
— Клостермана (Cloosterman) 280, 490
— — кратная (multiple) 313
— — обобщенная (generalized) 327
— многочленов (of polynomials) 33
— Салье (Salie) 313
— тригонометрическая (exponential) 243
— — неполная (incomplete) 309
— цикловая (cycle) 650
— Эйзенштейна (Eisenstein) 325
— — обобщенная (generalized) 326
— экспоненциальная (exponential) 243
— элементов группы (of elements of a group) 13
— Якоби (Jacobi) 257
— Якобсталя (Jacobsthal) 285
сумматор (adder) 496, 644
схема (design) 631
— декодирования (decoding scheme) 588
— инцидентности (tactical configuration) 632
— — симметричная (symmetric) 632
— кодирования (coding scheme) 588
t-схема (t-design) 658

таблица групповой операции (group operation table) 16
— индексов (index) 89
— Кэли (Cayley) 16
тело (skew field, division ring) 24
теорема Варнинга (Warning's theorem) 333
— Веддербёрна (Wedderburn's) 92
— Вейля (Weil) 275
— Вильсона (Wilson's) 60
— Гамильтона—Кэли (Cayley—Hamilton) 80
— Дезарга (Desargue's) 620
— Дэвенпорта—Хасса (Davenport—Hasse) 248
— Кёнига—Радоша (König—Rados) 330
— китайская об остатках (chinese remainder) 60, 62
— об однозначном разложении на множители (unique factorization) 39
— о гомоморфизме (homomorphism) 22, 28
— — нормальном базисе (normal basis) 81
— — симметрических многочленах (on symmetric polynomials) основная (fundamental) 39
— Паппа (Pappus) 620
— Ферма малая (Fermat's little) 60
— четности Штикельбергера (Stickelberger's parity) 225
— Шевалле (Chevaley's) 333
— Штикельбергера (Stickelberger's) 253

тождество Мак-Вильямс (MacWilliams identity) 599
точка (point) 617
— рациональная (rational) 455
точки коллинеарные (collinear points) 620
транзитивность (transitivity) 15
— нормы (of norm) 78
— следа (of trace) 76
трехчлен (trinomial) 163
триггер (flip-flop) 496, 644

увеличитель (constant adder) 496
умножение (multiplication) 25
— символическое (symbolic) 148
уравнение гиперэллиптическое (hyperelliptic equation) 410
— диагональное (diagonal) 355
— классов сопряженности (class) 23
— k-линейное (k-linear) 393
— мультилинейное (linear) 393
— проверочное (parity check) 588
— разностное (difference) 495
усилитель (constant multiplier) 496, 644

факторгруппа (factor group, quotient group) 22
факторкольцо (factor ring, residue class ring) 27
форма (form) 338
— квадратичная (quadratic) 341
— — бинарная (binary) 342
— — диагональная (diagonal) 343
— — невырожденная (nondegenerate) 344, 350
— — представляющая элемент (representing an element) 343
— нормализованная (normalized) 443
— норменная (norm) 391
— приведенная (reduced) непрерывной дроби (of continued fraction) 291
— рациональная каноническая (rational canonical) 651
формула бинома (binomial theorem) 60
— Варинга (Waring's formula) 46

— Ньютона (Newton's formula) 46
— обращения Мёбиуса (Moebius inversion formula) 120
— полной реакции (general response formula) 647
формы квадратичные эквивалентные (equivalent quadratic forms) 342
функция автокорреляционная (autocorrelation function) 580
— весовая кода (weight enumerator) 598
— выхода (output function) 643
— импульсная (impulse response sequence) 503
— индексная (index function) 667
— кросс-корреляционная (cross-correlation function) 579
— Мёбиуса (Moebius function) 120
— мультипликативная (multiplicative function) 246
— переходная (next-state function) 643
— производящая (generating function) 515
— следующего состояния (next-state function) 643
— Эйлера (Euler's function) 19, 59
— экспоненциальная (exponential function) 667
L-функция (L-function) 446

характер (character) 236
— аддитивный (additive) 240
— — канонический (canonical) 240
— квадратичный (quadratic) 242
— мультипликативный (multiplicative) 241
— нетривиальный (nontrivial) 236
— сопряженный (conjugate) 236
— тривиальный (trivial) 236
характеристика кольца (characteristic of a ring) 29

центр группы (center of a group) 23
V-цепь (V-chain) 483
цикл (cycle) 630

четырехвершинник полный (complete quadrangle) 622

число среднее решений уравнения (average number of solutions of an equation) 339
— циклотомическое (cyclotomic) 305
члеи многочлена (term of a polynomial) 45
— цикловый (cycle) 650

элемент алгебраический (algebraic element) 47
— бесконечного порядка (of infinite order) 17
— блок-схемы (variety) 632
— единичный (identity, unity element) 13, 25
— задержки (delay element) 496, 644
— образующий простого расширения поля (defining element of a simple extension of field) 47
— обратимый (unit) 31
— обратный (inverse element) 13
— порождающий простого расширения поля (defining element of a simple field extension) 47
— примитивный (primitive element) 69
— простой (prime element) 31
— трансцендентный (transcendental element) 59
элементы ассоциированные (associate elements) 31
— бинарные (binary) 29
— сопряженные (conjugate) 20
— — относительно подполя K (with respect to K) 72
— сравнимые по модулю $n(J)$ (congruent modulo $n(J)$) 15, 26
— эквивалентные (equivalent) 15
эндоморфизм (endomorphism) 20
эпиморфизм (epimorphism) 20

ядро гомоморфизма (kernel of homomorphism) 21, 28

Содержание т. 1

Глава 1. Алгебраические основы

§ 1. Группы. § 2. Кольца и поля. § 3. Многочлены. § 4. Расширение полей. Комментарии. Упражнения.

Глава 2. Строение конечных полей

§ 1. Характеризация конечных полей. § 2. Корни неприводимых многочленов. § 3. Следы, нормы и базисы. § 4. Корни из единицы и круговые многочлены. § 5. Представление элементов конечных полей. § 6. Теорема Веддербёрна. Комментарии. Упражнения.

Глава 3. Многочлены над конечными полями

§ 1. Порядки многочленов и примитивные многочлены. § 2. Неприводимые многочлены. § 3. Построение неприводимых многочленов. § 4. Линеаризованные многочлены. § 5. Двучлены и трехчлены. Комментарии. Упражнения.

Глава 4. Разложение многочленов на множители

§ 1. Разложение многочленов над малыми конечными полями. § 2. Разложение многочленов над большими конечными полями. § 3. Вычисление корней многочленов. Комментарии. Упражнения.

Глава 5. Тригонометрические суммы

§ 1. Характеры. § 2. Суммы Гаусса. § 3. Суммы Якобн. § 4. Суммы значений характеров с полиномиальными аргументами. § 5. Дальнейшие результаты о суммах значений характеров. Комментарии. Упражнения.

Глава 6. Уравнения над конечными полями

§ 1. Элементарные результаты о числе решений. § 2. Квадратичные формы. § 3. Диагональные уравнения. § 4. Метод Степанова—Шмидта. Комментарии. Упражнения.

ОГЛАВЛЕНИЕ

Глава 7. Перестановочные многочлены 437
§ 1. Критерии перестановочности многочленов 438
§ 2. Примеры перестановочных многочленов 441
§ 3. Группы перестановочных многочленов 449
§ 4. Исключительные многочлены 455
§ 5. Перестановочные многочлены от нескольких переменных 462
Комментарии 473
Упражнения 488

Глава 8. Линейные рекуррентные последовательности 494
§ 1. Регистры сдвига с обратной связью. Свойства периодичности . . . 495
§ 2. Импульсная функция. Характеристический многочлен 503
§ 3. Производящие функции 515
§ 4. Минимальный многочлен 524
§ 5. Семейства линейных рекуррентных последовательностей 530
§ 6. Характеризация линейных рекуррентных последовательностей . . 547
§ 7. Распределение элементов в линейных рекуррентных последовательностях 555
Комментарии 566
Упражнения 580

Глава 9. Приложения конечных полей 586
§ 1. Линейные коды 587
§ 2. Циклические коды 601
§ 3. Конечные геометрии 616
§ 4. Приложения к комбинаторике 631
§ 5. Линейные модулярные системы 642
Комментарии 653
Упражнения 661

Глава 10. Таблицы 667
§ 1. Вычисления в конечных полях 667
§ 2. Таблицы неприводимых многочленов 670
Комментарии 670
Таблицы 673

ЛИТЕРАТУРА 694
УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ 806
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ 811
СОДЕРЖАНИЕ Т. 1 819

Уважаемый читатель!

Ваши замечания о содержании книги, ее оформлении, качестве перевода и другие просим присылать по адресу: 129820, Москва, И-110, ГСП, 1-й Рижский пер., д. 2, издательство «Мир».