Лидл Р., Нидеррайтер Г.

Конечные поля

Том 1-2

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Л55

Лидл Р.
Л55 Конечные поля: Том 1-2 / Лидл Р., Нидеррайтер Г. – М.: Книга по Требованию, 2013. – 812 с.

ISBN 978-5-458-31991-1

Монография известных математиков (Австралия, Австрия), отражающая многочисленные связи классического раздела алгебры - теория конечных полей - с комбинаторикой, теорией кодирования, теорией автоматов. Изложение отличается простотой и ясностью, большим числом (около 600) примеров и упражнений, имеются комментарии исторического характера. Книга входит в известную энциклопедию математики и её приложений (под. ред. Дж.-К. Роты); ряд её томов переведён в издательствах "Мир" И "Наука".Русское издание выходит в двух томах.Для математиков-прикладников, инженеров-исследователей, аспирантов и студентов университетов.

ISBN 978-5-458-31991-1

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

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

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*