Московский государственный технический университет
имени Н. Э. Баумана

А. В. Чашкин, Д. А. Жуков

ЭЛЕМЕНТЫ КОНЕЧНОЙ АЛГЕБРЫ

группы, кольца, поля, линейные пространства

Учебное пособие

Москва
ИЗДАТЕЛЬСТВО
МГТУ им. Н. Э. Баумана
2016

УДК 512.6
ББК 22.14
Ч-29

Издание доступно в электронном виде на портале *ebooks.bmstu.ru*
по адресу: `http://ebooks.bmstu.ru/catalog`

Факультет «Информатика и системы управления»
Кафедра «Информационная безопасность»

Рекомендовано редакционно-издательским советом МГТУ им. Н. Э. Баумана в качестве учебного пособия

Рецензенты:
профессор механико-математического факультета
МГУ им. М. В. Ломоносова *С. Б. Гашков*;
доцент факультета ВМК МГУ им. М. В. Ломоносова *М. А. Черепнев*

Чашкин, А. В.

Ч-29 Элементы конечной алгебры: группы, кольца, поля, линейные пространства: учебное пособие / А. В. Чашкин, Д. А. Жуков — Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. — 368 с. : ил.

ISBN 978-5-7038-4354-3

Учебное пособие основано на материалах лекций и семинаров, проводимых в МГТУ им. Н. Э. Баумана для студентов, специализирующихся в области защиты информации. В пособии рассмотрены основные алгебраические структуры и их свойства. Все утверждения снабжены подробными доказательствами и проиллюстрированы большим числом примеров. Основное внимание уделено конечным полям и линейным пространствам над конечными полями. Для чтения пособия достаточно уверенного владения математикой в объеме средней школы.

ISBN 978-5-7038-4354-3

УДК 512.6
ББК 22.14

Оглавление

Предисловие

Это учебное пособие основано на лекциях и семинарах, которые вот уже более десяти лет проводятся авторами в МГТУ им. Н. Э. Баумана для студентов, специализирующихся в области защиты информации, одной из составных частей которой является криптография. В современной криптографии активно используются результаты таких разделов математики, как теория вероятностей, теория чисел, теория сложности и т. д. В этом ряду одно из первых мест, безусловно, принадлежит алгебре, так как в основе подавляющего числа криптографических конструкций и методов лежат алгебраические структуры — группы, кольца, поля, линейные пространства. Изучению этих структур и посвящена настоящая книга.

Алгебра (как общая, так и линейная) давно является неотъемлемой частью подготовки инженеров и научных работников. Благодаря этому сейчас существует обширная и качественная учебная литература, посвященная тем разделам алгебры, которые традиционно изучаются в высших технических учебных заведениях и на математических и естественных факультетах университетов. Вместе с тем следует отметить, что эти разделы в основном имеют дело с «бесконечной» частью алгебры — с алгебраическими структурами, так или иначе связанными с полями действительных и комплексных чисел. «Конечной» части — конечным полям, линейным пространствам над конечными полями и т. п. — уделяется значительно меньше внимания, в то время как в современных задачах, имеющих дело с различными преобразованиями больших объемов информации, наиболее востребованы именно методы конечной алгебры. Такое положение было одной из главных причин, побудивших авторов к написа-

нию учебного пособия по алгебре, в котором основное внимание было бы уделено конечной алгебре и, в частности, конечным полям и линейным пространствам над конечными полями. При этом авторы стремились создать максимально независимое и подробное пособие, для чтения большей части которого достаточно уверенного владения математикой в объеме средней школы. В результате получилась книга с подробными доказательствами и большим числом разнообразных примеров, для работы с которой нет необходимости прибегать к дополнительной литературе[1)].

Книга состоит из девяти глав. Первая глава содержит простейшие сведения из теории множеств и носит в основном справочный характер. Вторая глава является простым введением в элементарную теорию чисел. Часть результатов второй главы обобщается в следующих главах для групп и колец и используется в качестве примеров появляющихся там общих конструкций и результатов. Материал третьей главы достаточно традиционен и содержится в большинстве начальных курсов алгебры — в ней изучаются группы и их основные свойства. В четвертой главе рассматриваются кольца. Значительная часть этой главы посвящена изучению колец многочленов над конечными полями. В частности, для любого простого p и любого натурального n доказывается существование поля из p^n элементов как поля вычетов многочленов по модулю неприводимого многочлена. В пятой и шестой главах подробно рассматриваются линейные пространства над конечными полями и их линейные преобразования. Рассматриваются методы решений систем линейных уравнений над конечными полями, изучаются циклические пространства. Материалы, составляющие четвертую, пятую и шестую главы, достаточно сильно отличаются от материалов, содержащихся в аналогичных разделах большинства курсов общей и линейной алгебры, где основное внимание уделяется кольцам многочленов и линейным пространствам над полями действительных и комплексных чисел. В этих главах, в частности, нет основной

[1)] Это ни в коем случае не рекомендация для работы с книгой, это возможность!

теоремы алгебры и теоремы о жордановой нормальной форме линейного оператора. Основная задача глав 4—6 — создать необходимые инструменты для изучения в восьмой главе конечных полей. В седьмой главе подробно изучаются конечные группы. Дается описание строения произвольной абелевой группы и, в частности, группы целых чисел с операцией умножения по составному модулю. В восьмой главе рассматриваются конечные поля, их структура, особенности выполнения в них арифметических операций и т. п. Доказывается единственность, с точностью до изоморфизма, поля из p^n элементов и устанавливается отсутствие других конечных полей. Не сильно преувеличивая, можно сказать, что восьмая глава является центром, вокруг которого построена книга. Причина этого в том исключительном положении, которое занимают конечные поля в создании и применении современных алгоритмов работы с дискретными данными. Наконец в девятой главе приводятся примеры таких алгоритмов: алгоритмы дискретного логарифмирования в конечных полях, алгоритм разложения на неприводимые множители многочлена над конечным полем и алгоритм исправления ошибок в примитивных БЧХ-кодах.

Авторы надеются, что настоящая книга позволит ее читателям продолжить изучение алгебраических структур и методов на более высоком уровне и, кроме того, облегчит знакомство как с другими областями математики, имеющими важные практические приложения, так и с самими приложениями.

Глава 1

Множества и отображения

Понятия «множества», «отношения», «отображения» и пр. являются базовыми для всей математики — и дискретной, и непрерывной. Они закладывают необходимую основу для всех дальнейших построений, зачастую весьма сложных. Алгебраические структуры на множествах являются основным объектом практически всех теоретических и прикладных математических дисциплин, в частности математической криптографии.

1.1. Множества

Понятие «множества» — одно из фундаментальных неопределяемых понятий математики. Под *множеством* понимают любую определенную совокупность объектов, называемых *элементами* множества. Элементы множества различны и отличимы друг от друга. Множества обычно обозначаются прописными буквами, а их элементы — строчными. Для некоторых особо важных множеств приняты стандартные обозначения: $\mathbb{N}$ — множество натуральных чисел, $\mathbb{Z}$ — целых, $\mathbb{Q}$ — рациональных, $\mathbb{R}$ — действительных, $\mathbb{C}$ — множество комплексных чисел.

Если объект x является элементом множества M, то говорят, что x принадлежит M (M содержит x) и используют обозначение $x \in M$. В противном случае говорят, что x не принадлежит M и пишут $x \notin M$. Например, $\sqrt{2} \notin \mathbb{Q}$ и $\sqrt{2} \in \mathbb{R}$. Множество M — *подмножество* множества N (M *содержится* в N, N *включает* M), если каждый элемент M есть элемент N. Это

свойство обозначается $M \subset N$ или $M \subseteq N$:

$$M \subset N \quad \Leftrightarrow \quad \forall\, x \in M : x \in N.$$

Например, $\mathbb{N} \subset \mathbb{Z}$. Два множества называются *равными*, если в них входят одни и те же элементы: $M = N \Leftrightarrow (M \subset N, N \subset M)$. *Пустое* множество $\varnothing$, не содержащее элементов, по определению является подмножеством любого множества: $\forall\, M\ \varnothing \subset M$. Если $M \subset N$, но $M \neq N$ и $M \neq \varnothing$, то M называется *собственным* подмножеством N.

Множество с конечным числом элементов называется *конечным*. Конечные множества могут быть описаны явным перечислением всех их элементов, при этом принято заключать их в фигурные скобки. Например, $M = \{2, 3, 5, 7\}$ — множество всех простых натуральных чисел, меньших 10. По нашему определению, множество является неупорядоченным объектом, в частности, $\{2, 3, 5, 7\} = \{5, 2, 7, 3\}$. Число элементов конечного множества M называют его *мощностью*. Оно обозначается $|M|$. Например, $|\varnothing| = 0$, но $|\{\varnothing\}| = 1$. Факт конечности M часто обозначается $|M| < \infty$, в противном случае используют запись $|M| = \infty$.

Над множествами обычно рассматриваются следующие операции:

1) *объединение* $M \cup N = \{x : x \in M$ или $x \in N\}$;

2) *пересечение* $M \cap N = \{x : x \in M$ и $x \in N\}$;

3) *разность* $M \setminus N = \{x : x \in M$ и $x \notin N\}$;

4) *симметрическая разность* $M \triangle N = (M \cup N) \setminus (M \cap N)$, причем легко убедиться, что также $M \triangle N = (M \setminus N) \cup (N \setminus M)$;

5) *дополнение* $\overline{M} = \{x : x \notin M\}$. Операция дополнения подразумевает некое универсальное множество U, такое, что $M \subset U$ и $\overline{M} = U \setminus M$.

Если $M \cap N = \varnothing$, то говорят, что M и N не пересекаются. Операции объединения и пересечения допускают обобщение: если I — некоторое множество, элементы которого используются как индексы, то

$$\bigcup_{i \in I} M_i = \{x : \exists\, i \in I\ \ x \in M_i\}, \qquad \bigcap_{i \in I} M_i = \{x : \forall\, i \in I\ \ x \in M_i\}.$$

Пусть U — универсальное множество и $M, N, K \subset U$ — произвольные подмножества. Нетрудно убедиться, что введенные операции над множествами обладают следующими свойствами:

1) идемпотентность: $M \cup M = M$, $M \cap M = M$;

2) коммутативность: $M \cup N = N \cup M$, $M \cap N = N \cap M$;

3) ассоциативность: $(M \cup N) \cup K = M \cup (N \cup K)$, $(M \cap N) \cap K = M \cap (N \cap K)$;

4) дистрибутивность: $(M \cup N) \cap K = (M \cup K) \cap (N \cup K)$, $(M \cap N) \cup K = (M \cap K) \cup (N \cap K)$;

5) поглощение: $(M \cup N) \cap M = M$, $(M \cap N) \cup M = M$;

6) свойство нуля: $M \cup \varnothing = M$, $M \cap \varnothing = \varnothing$;

7) свойство единицы: $M \cup U = U$, $M \cap U = M$;

8) инволютивность: $\overline{\overline{M}} = M$;

9) правила де Моргана: $\overline{M \cup N} = \overline{M} \cap \overline{N}$, $\overline{M \cap N} = \overline{M} \cup \overline{N}$.

Равенства $|M \cup N| = |M| + |N| - |M \cap N|$, $|M \setminus N| = |M| - |M \cap N|$, $|M \triangle N| = |M| + |N| - 2|M \cap N|$ и пр. легко следуют из определений.

1.2. Отношения на множествах

Если $a \in A$ и $b \in B$, то через (a, b) обозначим *упорядоченную пару*. Две упорядоченные пары (a, b) и (c, d) считаются равными тогда и только тогда, когда $a = c$ и $b = d$. Вообще говоря, $(a, b) \neq (b, a)$. *Прямым* или *декартовым* произведением двух множеств A и B называется множество всех различных упорядоченных пар, в которых первый элемент каждой пары из A, а второй — из B:

$$A \times B = \big\{(a, b) : a \in A, b \in B\big\}.$$

Степенью множества A называется его прямое произведение самого на себя: $A^n = A \times \ldots \times A$ (n раз). Очевидно, что для конечных множеств A и B справедливо $|A \times B| = |A| \cdot |B|$. Отсюда следует $|A^n| = |A|^n$.

Пусть A и B — два множества. Тогда произвольное подмножество R их прямого произведения $A \times B$ называется *отношением* из множества A в множество B (от англ. *relation* — от-

ношение), или, точнее, *бинарным отношением*. Для бинарных отношений принято использовать *инфиксную* форму записи: если $R \subset A \times B$, то пишут aRb в том и только в том случае, когда $(a, b) \in R$. Если $A = B$ и $R \subset A^2$, то говорят об отношении *на множестве* A. В качестве примера можно привести известные отношения $=$, $<$, $\leqslant$, определенные на множестве натуральных чисел. Обобщением бинарного отношения является n-арное отношение $R \subset A_1 \times \ldots \times A_n$, где множества A_i не обязательно различны. Далее рассматриваются только бинарные отношения, которые для краткости называются просто отношениями.

Пусть $R_1 \subset A \times B$, $R_2 \subset B \times C$ — отношения из A в B и из B в C соответственно. Тогда отношение

$$R_1 \circ R_2 = \big\{(a, c) : a \in A, c \in C : \exists\, b \in B \;\; aR_1b,\, bR_2c\big\}$$

называется *композицией* отношений R_1 и R_2.

Пусть $R \subset A^2$ — некоторое отношение на A. Тогда отношение $R^{-1} = \{(a, b) : (b, a) \in R\}$ называется *обратным* к отношению R, а отношение $\overline{R} = \{(a, b) : (a, b) \notin R\}$ — его *дополнением*. Отношение $\{(a, a) : a \in A\}$ называется *тождественным* или отношением *равенства* на A. Например, отношение $\neq$ является дополнением к отношению равенства на множестве $\mathbb{N}$.

Отношение $R \subset A^2$ называется *рефлексивным*, если для всех $a \in A$ выполнено aRa. Если для всех $a, b \in A$ из aRb следует bRa, то отношение R называется *симметричным*, а если для всех $a, b, c \in A$ из aRb, bRc следует aRc, то отношение R называется *транзитивным*.

Нетрудно убедиться в справедливости следующего утверждения.

Лемма 1.1. *Отношение R на множестве A является рефлексивным в том и только в том случае, когда оно содержит тождественное отношение. Отношение R симметрично тогда и только тогда, когда $R = R^{-1}$. Отношение R транзитивно тогда и только тогда, когда $R \circ R \subset R$.*

Рефлексивное, симметричное и транзитивное отношение называется *отношением эквивалентности*. Эквивалентность элементов a и b обозначается $a \sim b$.

Пусть $\sim$ — отношение эквивалентности на множестве A и $a \in A$. Подмножество $A_a^{\sim}$ множества A, состоящее из всех таких элементов $x \in A$, что $x \sim a$, называется *классом эквивалентности* элемента a.

Лемма 1.2. *Всякое отношение эквивалентности на множестве A определяет разбиение множества A на непустые классы эквивалентности. Различные классы эквивалентности не пересекаются: если $a \sim b$, то $A_a^{\sim} = A_b^{\sim}$, и если $a \not\sim b$, то $A_a^{\sim} \cap A_b^{\sim} = \varnothing$. Обратно, всякое разбиение множества A на непустые непересекающиеся подмножества определяет некоторое отношение эквивалентности на множестве A.*

Если $\sim$ — отношение эквивалентности на множестве A, то множество классов эквивалентности называется *фактор-множеством* множества A по эквивалентности $\sim$ и обозначается $A/\sim = \{A_a^{\sim} : a \in A\}$.

1.3. Отображения

Пусть R — отношение из A в B. Отношение R называется *однозначным* или *функциональным*, если для каждого элемента a из A из того, что aRb и aRc, следует $b = c$. Отношение R называется *тотальным*, или *всюду определенным* на A, если для каждого $a \in A$ найдется такой элемент $b \in B$, что выполнено aRb.

Однозначное всюду определенное[1)] на множестве A отношение $R \subset A \times B$ называется *отображением* или *функцией* из A в B. Для однозначных отношений (отображений) вместо записи aRb используется запись $b = R(a)$, а сами они обозначаются строчными латинскими или греческими буквами: f, g, φ, ψ и т. д. Для отображения f из A в B используется обозначение «$f : A \to$

[1)] Наряду со всюду определенными функциями важную роль в дискретной математике играют также функции *частичные* (однозначные нетотальные отношения). Однако далее они почти не встретятся, поэтому для удобства будем считать, что значения функции $f : A \to B$ определены на всем множестве A.

$\to B$». Множество A называется *областью определения*, а B — *областью значений* f. Если $b = f(a)$, то a называется *аргументом*, а b — *значением* функции f на аргументе a. *Сужением* функции $f : A \to B$ на множество $C \subset A$ называется функция $f|_C = \{(a, b) \in f : a \in C\}$.

Пример 1.1. Пусть N — произвольное множество, A — подмножество N. Функция $\chi_A(x) : N \to \{0, 1\}$ называется *характеристической* функцией множества A, если $\chi_A(x) = 1$ при $x \in A$ и $\chi_A(x) = 0$ при $x \notin A$. □

Множество $\operatorname{Im} f = \{f(a) : a \in A\} \subset B$ называется *образом* отображения f из A в B. Наряду с $\operatorname{Im} f$ для образа часто используется и обозначение $f(A)$. Множество $f^{-1}(b) = \{a \in A : b = f(a)\} \subset A$ называется *прообразом* элемента $b \in B$.

Отображение $f : A \to B$ называется *сюръективным* в случае $\operatorname{Im} f = B$, т. е. тогда, когда прообраз любого элемента из B непуст. Отображение f называется *инъективным*, когда из $a \neq a'$ следует $f(a) \neq f(a')$, т. е. все значения f на элементах из A различны. Инъективное и сюръективное отображение называется *биективным* или *взаимно однозначным*.

Отметим, что задание области определения и области значений отображения существенны для его определения. Так, отображения $f : \mathbb{N} \to \mathbb{N}$ и $g : \mathbb{R} \to \mathbb{R}$, будучи определены одним правилом $f(a) = a^3$ и $g(a) = a^3$, имеют разные свойства: f инъективно, но не сюръективно, а g — биекция. По определению, равенство двух отображений f, g означает совпадение областей определения и значений: $f : A \to B$ и $g : A \to B$, причем $f(a) = g(a)$ для всех $a \in A$.

Композицией, а также *суперпозицией* или *произведением*[1)] отображений $g : A \to B$ и $f : B \to C$ называется отображение $f \circ g : A \to C$, определяемое при каждом $x \in A$ равенством

$$(f \circ g)(x) = f(g(x)).$$

[1)] Определение композиции отображений является следствием определения композиции отношений, однако ввиду его особой важности мы дали его явно.

В дальнейшем вместо $f \circ g$ мы будем часто писать просто fg. Отметим, что композиция определена не для любых отображений f и g: область определения f должна совпадать с областью значений g.

Следующая теорема формулирует важнейшее свойство композиции отображений, которое неоднократно будет использовано ниже.

Теорема 1.1. *Композиция отображений ассоциативна. Точнее, если $h : A \to B$, $g : B \to C$ и $f : C \to D$ — три отображения, то $f \circ (g \circ h) = (f \circ g) \circ h$.*

Доказательство. Сравним значения отображений $f \circ (g \circ h) : A \to D$ и $(f \circ g) \circ h : A \to D$ на произвольном элементе $x \in A$. Согласно определению композиции,

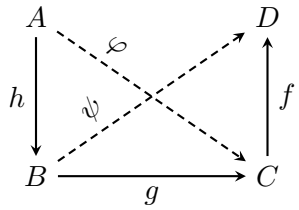
$$\big(f \circ (g \circ h)\big)(x) = f\big((g \circ h)(x)\big) = f\big(g\big(h(x)\big)\big).$$

С другой стороны,

$$\big((f \circ g) \circ h\big)(x) = (f \circ g)\big(h(x)\big) = f\big(g\big(h(x)\big)\big).$$

Сравнивая правые части двух последних равенств, убеждаемся в том, что $\big(f \circ (g \circ h)\big)(x) = \big((f \circ g) \circ h\big)(x)$ при любом x. Следовательно, отображения $f \circ (g \circ h)$ и $(f \circ g) \circ h$ совпадают согласно определению равенства отображений.

Приведенные рассуждения наглядно демонстрирует диаграмма, изображенная ниже на рисунке. Про подобные диаграммы



говорят, что они *коммутативны*: результат перехода от одной ее фиксированной вершины к другой не зависит от пути из ориентированных ребер. Так, пунктирное ребро φ соответствует

композиции $\varphi = g \circ h$, а результат перехода от A к C (согласно определению композиции) не зависит от того, сделать ли это сразу по пунктирному ребру, или через B по ребрам, помеченным h и g. Аналогично другое пунктирное ребро диаграммы задает отображение $\psi = f \circ g$. Ориентированный путь φ, f приводит из A туда же, куда и путь h, ψ (а также путь h, g, f), поэтому отображения $f \circ \varphi$ и $\psi \circ h$ равны. Теорема доказана.

Далее ввиду доказанной ассоциативности в выражениях вида $f \circ (g \circ h)$ будем опускать скобки и писать просто $f \circ g \circ h$. Заметим, что композиция отображений, вообще говоря, некоммутативна, т. е. $f \circ g \neq g \circ f$ даже в том случае, когда оба эти выражения имеют смысл (например $f, g : A \to A$). Однако если мы обозначим e_A отображение, переводящее каждый элемент $x \in A$ в себя (такое отображение называется *тождественным* или *единичным*), то очевидно получим $f \circ e_A = e_A \circ f = f$ для любого f из A в A.

Если композиция $f \circ g$ отображений $f : B \to A$ и $g : A \to B$ совпадает с тождественным отображением e_A, то говорят, что f — *левое обратное* отображение к g, а g — *правое обратное* к f. Если одновременно $f \circ g = e_A$ и $g \circ f = e_B$, то говорят, что отображение f — *обратное* к g, отображение g — *обратное* к f, и пишут, соответственно, $f = g^{-1}$ и $g = f^{-1}$. Отображение называется *обратимым* (слева, справа), если оно имеет (левое, правое) обратное отображение. Следующую простую теорему об обратимости отображений приведем без доказательства.

Теорема 1.2. *Отображение*: 1) *обратимо слева тогда и только тогда, когда оно инъективно*; 2) *обратимо справа тогда и только тогда, когда оно сюръективно*; 3) *обратимо тогда и только тогда, когда оно биективно.*

Пример 1.2. Пусть f отображает множество $A = \{0, 1, \ldots, 5\}$ в множество $B = \{0, 1, \ldots, 10\}$ по правилу $f(x) = 2x$, а g отображает B в A по правилу $g(x) = \lfloor x/2 \rfloor$. Легко видеть, что f инъективно, а g сюръективно. При этом $g \circ f = e_A$, и хотя композиция $f \circ g$ существует, она не равна e_B. □

Так как композиция биективных отображений биективна, то,

очевидно, имеет место следующее утверждение об обратимости композиции обратимых отображений.

Теорема 1.3. *Композиция обратимых отображений обратима.*

Пример 1.3. Рассмотрим множество целых чисел $\mathbb{Z}$ и его несобственное подмножество $2\mathbb{Z}$, состоящее из всех четных чисел. Нетрудно видеть, что отображение $f : \mathbb{Z} \to 2\mathbb{Z}$, действующее по правилу $f(n) = 2n$, является взаимно однозначным и обладает обратным $f^{-1} : 2\mathbb{Z} \to \mathbb{Z}$, действующим по правилу $f^{-1}(2n) = n$. Также взаимно однозначным будет сужение $f_{2\mathbb{Z}}$ отображения f на множество $2\mathbb{Z}$. Поэтому композиция $f_{2\mathbb{Z}} \circ f$, отображающая целые числа в множество $4\mathbb{Z}$, состоящее из всех целых кратных четырем, является обратимым отображением с обратным $g^{-1} : 4\mathbb{Z} \to \mathbb{Z}$, действующим по правилу $g(4n) = n$. □

Говорят, что множества A и B *равномощны*, если существует взаимно однозначное отображение A в B (очевидно, что одновременно существует и взаимно однозначное отображение B в A). Легко видеть, что два конечных множества равномощны, если их мощности равны. Поэтому никакое конечное множество не равномощно никакому своему собственному подмножеству. Для бесконечных множеств это не так.

Пример 1.4. В силу предыдущего примера множества $\mathbb{Z}$, $2\mathbb{Z}$ и $4\mathbb{Z}$ равномощны. □

1.4. Конечные множества и их мощности

Пусть $A = \{a_1, \ldots, a_n\}$ — конечное множество. Совокупность из k элементов множества A (не обязательно различных) называется *k-выборкой* множества A. Выборка называется *упорядоченной*, если каждому ее элементу поставлен в соответствие номер — натуральное число, не превосходящее k так, что разным элементам соответствуют разные числа. Упорядоченные выборки будем называть также *наборами*. Элементы упорядоченных выборок будем заключать в круглые скобки, а элементы неупорядоченных выборок — в фигурные скобки. Например,

(a_1, a_2, a_2) и (a_2, a_1, a_2) — две различные упорядоченные выборки, а $\{a_1, a_2, a_2\}$ и $\{a_2, a_1, a_2\}$ — одна и та же неупорядоченная выборка.

Перестановкой n-элементного множества $A = \{a_1, \ldots, a_n\}$ называется любой набор $(a_{i_1}, \ldots, a_{i_n})$, состоящий из элементов A, в котором каждый элемент из A встречается ровно один раз. Например, у трехэлементного множества $\{a_1, a_2, a_3\}$ существует ровно шесть различных перестановок:

$$(a_1, a_2, a_3), \quad (a_1, a_3, a_2), \quad (a_2, a_1, a_3),$$
$$(a_2, a_3, a_1), \quad (a_3, a_1, a_2), \quad (a_3, a_2, a_1).$$

Найдем число P_n различных перестановок n-элементного множества. Для этого из n-элементного множества будем последовательно выбирать элементы и формировать из них упорядоченную выборку: первый выбранный элемент станет первым элементом упорядоченной выборки, второй — вторым и т. д. Нетрудно видеть, что первый элемент можно выбрать n способами. Второй элемент будет выбираться из $(n-1)$ оставшихся элементов, поэтому его можно выбрать $(n-1)$ способом. Продолжая выбор, заметим, что после выбора первых k элементов останется $(n-k)$ невыбранных элементов. Следовательно, $(k+1)$-й элемент можно выбрать $(n-k)$ способами. Перемножив числа способов, которыми можно выбрать первый, второй, …, $(n-1)$-й и n-й элементы, получим величину, равную числу способов, которыми можно упорядочить n-элементное множество. Таким образом,

$$P_n = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!. \tag{1.1}$$

Размещением из n элементов по k называется произвольная перестановка k-элементного подмножества n-элементного множества. Для обозначения числа размещений из n элементов по k используется символ A_n^k. Рассуждениями, аналогичными приведенным выше при определении величины P_n, нетрудно показать, что

$$A_n^k = n(n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}. \tag{1.2}$$

Сочетанием из n элементов по k называется произвольное k-элементное подмножество n-элементного множества. Число сочетаний из n элементов по k обозначается через $\binom{n}{k}$ (иногда также используется символ C_n^k). Так как у одного k-элементного подмножества существует ровно $k!$ различных перестановок, то из (1.2) легко следует, что

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k(k-1)\cdot\ldots\cdot 2\cdot 1}. \qquad (1.3)$$

Из равенства (1.3) легко вытекают следующие часто используемые свойства сочетаний:

$$\binom{n}{k} = \binom{n}{n-k}, \qquad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \qquad (1.4)$$

Сочетанием с повторениями из n элементов по k называется неупорядоченная k-выборка n-элементного множества. Например, из трех элементов a_1, a_2 и a_3 можно составить шесть сочетаний с повторениями по два элемента:

$$a_1a_1, \quad a_1a_2, \quad a_1a_3, \quad a_2a_2, \quad a_2a_3, \quad a_3a_3.$$

Каждое сочетание с повторениями из n элементов по k однозначно определяется тем, сколько раз каждый элемент множества входит в рассматриваемое сочетание. Пусть в некоторое такое сочетание элемент a_i входит m_i раз, где $i = 1, 2, \ldots, n$. Этому сочетанию поставим в соответствие набор

$$\underbrace{1\ldots1}_{m_1}0\underbrace{1\ldots1}_{m_2}0\ldots\ldots0\underbrace{1\ldots1}_{m_n} \qquad (1.5)$$

из k единиц, сгруппированных в n блоков, и $n-1$ нулей, разделяющих эти блоки. В этом наборе первый блок из m_1 единиц соответствует элементу m_1, второй блок из m_2 единиц — элементу a_2, и т. д. Приведенным выше двухэлементным сочетаниям соответствуют следующие шесть наборов:

$$1100, \quad 1010, \quad 1001, \quad 0110, \quad 0101, \quad 0011.$$

Очевидно, что набор вида (1.5) однозначно определяет соответствующее ему сочетание с повторениями. Поэтому число H_n^k сочетаний с повторениями из n элементов по k равно числу наборов из k единиц и $n-1$ нулей. Каждый такой набор можно рассматривать как набор значений характеристической функции k-элементного подмножества $(n+k-1)$-элементного множества. Следовательно,

$$H_n^k = \binom{n+k-1}{k} = \frac{(n+k-1)!}{(n-1)!k!}.$$

Числа сочетаний $\binom{n}{k}$ называются также *биномиальными коэффициентами*, так как они появляются в формуле *бинома Ньютона*

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{1.6}$$

Справедливость равенства (1.6) следует из того, что после раскрытия скобок в выражении $(1+x)^n$ коэффициент при k-й степени переменной x будет равен числу способов, которыми можно выбрать k раз переменную x из n двучленов $(1+x)$.

Пример 1.5. В n-элементном множестве найдем число подмножеств четной и нечетной мощности. Очевидно, эти числа равны $\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k}$ и $\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1}$. Для вычисления этих сумм воспользуемся формулой бинома Ньютона. Подставляя в (1.6) вместо x единицу и минус единицу, получим тождества

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n, \qquad \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Вычисляя сумму и разность этих тождеств и деля результаты пополам, получаем, что

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = 2^{n-1}, \qquad \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1} = 2^{n-1}.$$

Таким образом, в n-элементном множестве существует ровно 2^{n-1} подмножеств четной мощности и столько же подмножеств нечетной мощности. □

Полезным средством при подсчете числа элементов различных множеств является *формула включений и исключений*, которая выражает мощность объединения множеств через мощности их пересечений. Для двух множеств эта формула выглядит достаточно просто:

$$|A \cup B| = |A| + |B| - |A \cap B|\,.$$

В общем случае справедлива следующая теорема.

Теорема 1.4. *Для любых конечных множеств $A_1, \ldots, A_n$ справедливо равенство*

$$\begin{aligned} |A_1 \cup \cdots \cup A_n| = \sum_{1 \leqslant i \leqslant n} |A_i| - \sum_{1 \leqslant i_1 < i_2 \leqslant n} |A_{i_1} \cap A_{i_2}| + \ldots \\ \cdots + (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |A_{i_1} \cap \cdots \cap A_{i_k}| + \ldots \\ \cdots + (-1)^{n+1} |A_1 \cap \ldots \cap A_n|. \end{aligned} \tag{1.7}$$

Доказательство. Пусть целое m не меньше нуля и не больше m. Допустим, что некоторый элемент a принадлежит ровно m множествам. Тогда a принадлежит $\binom{m}{2}$ попарным пересечениям множеств $A_1, \ldots, A_n$, $\binom{m}{3}$ тройным пересечениям этих множеств, и в общем случае $\binom{m}{k}$ пересечениям по k множеств. Следовательно, в сумме, стоящей в правой части (1.7), этот элемент будет учтен ровно

$$\binom{m}{1} - \binom{m}{2} + \cdots + (-1)^{k+1}\binom{m}{k} + \cdots + (-1)^{m+1}\binom{m}{m} \tag{1.8}$$

раз. Из (1.6) следует, что

$$\begin{aligned} (1-1)^m = 1 - \binom{m}{1} + \binom{m}{2} - \cdots + \\ \cdots + (-1)^k \binom{m}{k} + \cdots + (-1)^m \binom{m}{m}. \end{aligned}$$

Поэтому сумма (1.8) равна единице. Следовательно, в правой части (1.7) каждый элемент, принадлежащий объединению множеств A_i, учитывается ровно один раз, и поэтому вся сумма равна мощности объединения этих множеств. Теорема доказана.

Пример 1.6. Найдем число $N(n,m)$ сюръективных отображений n-элементного множества $A=\{a_1,\dots,a_n\}$ в m-элементное множество $B=\{b_1,\dots,b_m\}$. Каждое такое отображение f однозначно определяется набором образов

$$(f(a_1),\dots,f(a_n))=(b_{i_1},\dots,b_{i_n}) \tag{1.9}$$

всех элементов множества A, в котором встречается каждый элемент множества B. Легко видеть, что существует ровно m^n отображений (не обязательно сюръективных) множества A в множество B. Из всех таких отображений составим m подмножеств $N_1,\dots,N_m$, так, что N_i будет состоять из всех тех отображений, при которых элемент b_i не имеет прообраза в A, т. е. этот элемент отсутствует в наборе (1.8). Тогда $N(n,m)=$ $=m^n-|N_1\cup\dots\cup N_m|$, где мощность объединения находится при помощи формулы включений–исключений. Следовательно,

$$\begin{aligned}N(n,m)&=m^n-|N_1\cup\dots\cup N_m|=\\&=m^n-\sum_{1\leqslant i\leqslant m}|N_i|+\sum_{1\leqslant i_1<i_2\leqslant m}|N_{i_1}\cap N_{i_2}|-\dots\\&\quad\dots+(-1)^k\sum_{1\leqslant i_1<\dots<i_k\leqslant m}|N_{i_1}\cap\dots\cap N_{i_k}|+\dots\\&\quad\dots+(-1)^m|N_1\cap\dots\cap N_m|.\end{aligned}$$

Отображения из множества $N_{i_1}\cap\dots\cap N_{i_k}$ можно получить отображая элементы множества A в множество $\{b_{i_1},\dots,b_{i_k}\}$. Следовательно,

$$|N_{i_1}\cap\dots\cap N_{i_k}|=(m-k)^n.$$

Подставляя это равенство в предыдущую формулу и учитывая, что число различных множеств $N_{i_1}\cap\dots\cap N_{i_k}$ равно $\binom{m}{k}$, получаем искомое число

$$N(n,m)=\sum_{k=0}^{m}(-1)^k(m-k)^n\binom{m}{k}=\sum_{k=0}^{m}(-1)^k\frac{(m-k)^n m!}{k!(m-k)!}.$$

□

Задачи

1.1. Пусть $R = \{(a, b) : a, b \in \mathbb{N},\ a = b^2\}$. Какими свойствами обладает отношение R?

1.2. Доказать, что если $|A| = n$, то число различных бинарных отношений на множестве A равно 2^{n^2}. Сколько среди них рефлексивных, симметричных?

1.3. Привести примеры отношений: 1) не рефлексивного, но симметричного и транзитивного; 2) не симметричного, но рефлексивного и транзитивного; 3) не транзитивного, но симметричного и рефлексивного.

1.4. На множестве прямых на плоскости рассмотрим отношения: 1) параллельности прямых; 2) перпендикулярности прямых. Определить, будут ли эти отношения отношениями эквивалентности.

1.5. Доказать, что пересечение двух отношений эквивалентности на некотором множестве также является отношением эквивалентности на нем.

1.6. Отношение R на множестве A называется *антисимметричным*, если для любых $a, b \in A$ из aRb и bRa следует $a = b$. Рефлексивное, антисимметричное и транзитивное отношение называется отношением *частичного порядка* на множестве A и обозначается символом $\preccurlyeq$. Множество A с отношением $\preccurlyeq$ называется *частично упорядоченным*. Показать, что множество 2^X всех подмножеств конечного множества X с отношением включения «$\subseteq$» является частично упорядоченным и что всякое частично упорядоченное множество X изоморфно некоторой системе своих подмножеств, частично упорядоченной отношением включения.

1.7. Доказать, что если R — частичный порядок, то R^{-1} — также частичный порядок.

1.8. Отношение частичного порядка на множестве A, для которого любые два элемента сравнимы, т. е. $a \preccurlyeq b$ или $b \preccurlyeq a$ для любых $a, b \in \in A$, называется отношением *линейного порядка*. Доказать, что всякий частичный порядок на конечном множестве может быть продолжен до линейного порядка.

1.9. Привести пример линейного порядка на множестве $\mathbb{N} \times \mathbb{N}$.

1.10. Доказать леммы 1.1 и 1.2.

1.11. Доказать теорему 1.2 для отображений на конечных множествах.

1.12. Установить взаимно однозначное соответствие между множествами целых и рациональных чисел.

1.13. Найти сумму $\sum_{k=0}^{n} k\binom{n}{k}$.

1.14. Найти число n-элементных перестановок $(i_1, \ldots, i_n)$ множества $\{1, \ldots, n\}$ таких, что $k \neq i_k$ для $k = 1, \ldots, n$.

1.15. Найти число прямоугольных таблиц из n строк и m столбцов с элементами ± 1, у которых произведения всех элементов каждой строки и каждого столбца положительны.

1.16. За круглым столом сидят n человек. Сколькими способами из них можно выбрать k человек так, чтобы среди выбранных не было соседей.

1.17. Найти число натуральных решений уравнения $x_1 + \cdots + x_k = n$.

1.18. Сколько существует натуральных десятичных n-разрядных чисел, у которых цифры следуют в невозрастающем порядке?

1.19. Доказать, что

$$(x_1 + \cdots + x_k)^n = \sum_{m_1 + \cdots + m_k = n} \frac{n!}{m_1! \cdots m_k!}\, x_1^{m_1} \cdots x_k^{m_k}.$$

1.20. Выразить функцию $\chi_{A_1 \cup \cdots \cup A_n}(x)$ через функции $\chi_{A_i}(x)$.

1.21. Используя предыдущую задачу, доказать формулу включений-исключений.

Глава 2

Целые числа

Эта глава является кратким введением в элементарную теорию чисел. В ней содержатся простые и в то же время необходимые для изучения появляющихся далее алгебраических структур сведения о целых числах и их свойствах.

2.1. Делимость. Алгоритм Евклида

Будем говорить, что целое число a делится на целое число $b \neq 0$, если существует такое целое c, что $a = bc$. Если целое a делится на целое b, то число b будем называть *делителем* a, и будем говорить, что b делит a и обозначать это так: $b \mid a$. Очевидно, что для каждого $a \neq 0$ числа $\pm a$ и ± 1 являются делителями a. Такие делители будем называть *тривиальными*. Если b не делит a, то запишем $b \nmid a$.

Свойство одного числа делить другое задает на множестве целых чисел отношение делимости «$\mid$», которое, как нетрудно видеть, является транзитивным (если $b \mid a$ и $c \mid b$, то $c \mid a$) и обладает следующими простыми свойствами: если $a \mid b$ и $b \mid a$, то $a = \pm b$; если $c \mid a$ и $c \mid b$, то $c \mid a \pm b$; если $c \mid b$, то $c \mid ab$.

Доказываемая далее теорема играет фундаментальную роль при изучении свойств целых чисел и называется теоремой о делении с остатком.

Теорема 2.1. *Для любых целого a и натурального b найдутся, и притом единственные, такие целые q и r, что $a = qb + r$, где $0 \leqslant r < b$.*

Доказательство. Рассмотрим множество целых неотрицательных чисел вида $a - bk$, где k — целое. Пусть $r = a - bq$ — наименьший неотрицательный элемент этого множества. Тогда $0 \leqslant r < b$. Если это не так и $r = a - bq \geqslant b$, то неравенство $0 \leqslant a - (q+1)b < r$ противоречит минимальности r.

Докажем единственность указанного представления. Предположим, что $a = qb + r = q'b + r'$ и $0 \leqslant r < r' < b$. Отсюда $(q'-q)b = r'-r$, т. е. неотрицательное число $r'-r$ делится на b. С другой стороны $r' - r < b$. Противоречие. Следовательно, $r = r'$ и $(q' - q)b = 0$, т. е. $q = q'$. Теорема доказана.

Число r из теоремы 2.1 называется *остатком* от деления a на b, а число q — (не)полным *частным* или *целой частью* дроби $\frac{a}{b}$ и обозначается $\left\lfloor \frac{a}{b} \right\rfloor$.

Целое b, которое делит каждое из целых чисел $a_1, a_2, \ldots, a_n$, называется общим делителем этих чисел. Наибольшее число среди общих делителей чисел $a_1, a_2, \ldots, a_n$ называется их *наибольшим общим делителем* и обозначается символом $(a_1, a_2, \ldots, a_n)$ или НОД$(a_1, a_2, \ldots, a_n)$. Например, $(2, 4, 6) = 2$. Легко видеть, что если целые a и b не имеют нетривиальных общих делителей, то $(a, b) = 1$. Такие числа называются *взаимно простыми*.

Теорема 2.2 (Евклид). *Для любых двух натуральных a и b минимальное натуральное d, для которого справедливо равенство $d = ax + by$, где x и y целые, является наибольшим общим делителем чисел a и b.*

Доказательство. Рассмотрим множество $\{ax+by\}$ всех линейных комбинаций чисел a и b с различными целыми коэффициентами x и y. Пусть $d = ax_0+by_0$ — минимальное натуральное число этого множества. Покажем, что a делится на d. Для этого разделим a на d с остатком и представим его в виде $a = qd + r$, где $0 \leqslant r < d$. Тогда

$$\begin{aligned} r = a - qd &= a - q(ax_0 + by_0) = \\ &= a(1 - qx_0) - b(qy_0) = ax_1 + by_1, \end{aligned}$$

где $x_1 = 1-qx_0$ и $y_1 = -qy_0$. Так как d — минимальное натуральное число множества $\{ax+by\}$ и $r < d$, то $r = 0$ и, следовательно,

a делится на d. Аналогичным образом доказывается делимость на d числа b. Следовательно, d является общим делителем чисел a и b. Теперь покажем, что d будет наибольшим общим делителем. Действительно, если a и b делятся на $d \cdot d'$, где $d' > 1$, то в равенстве $d = ax_0 + by_0$ правая часть будет делиться на $d \cdot d'$, а левая не будет. Следовательно, $d = (a, b)$. Теорема доказана.

Рассмотрим алгоритм нахождения наибольшего общего делителя двух натуральных чисел a и b. Будем полагать, что $a > b$. Тогда $a = q_1 b + r_1$, где $0 \leqslant r_1 < b$. Легко видеть, что $(a, b) = (b, r_1)$. Поэтому вместо (a, b) будем искать (b, r_1). Продолжая подобные рассуждения, получим цепочку равенств

$$\begin{aligned}
a &= bq_1 + r_1, & (a,b) &= (b, r_1),\\
b &= r_1 q_2 + r_2, & (b, r_1) &= (r_1, r_2),\\
r_1 &= r_2 q_3 + r_3, & (r_1, r_2) &= (r_2, r_3), \qquad (2.1)\\
&\dots\dots\dots\dots\dots\dots & &\dots\dots\dots\dots\dots\dots\\
r_{n-2} &= r_{n-1} q_n + r_n, & (r_{n-2}, r_{n-1}) &= (r_{n-1}, r_n),\\
r_{n-1} &= r_n q_{n+1}, & (r_{n-1}, r_n) &= r_n,
\end{aligned}$$

в которой последний положительный остаток r_n и будет наибольшим общим делителем чисел a и b.

Приведенный алгоритм нахождения наибольшего общего делителя называется *алгоритмом Евклида*, а вычисление очередного остатка r_i называется i-м шагом этого алгоритма. Алгоритм (2.1) состоит из $(n+1)$ шагов, а если $r_n = 1$, то из n шагов, так как последнее деление на единицу можно не выполнять. Заметим, что остатки r_i в алгоритме Евклида убывают, оставаясь положительными, поэтому очевидно, что алгоритм остановится за конечное число шагов. Оценим число шагов в алгоритме Евклида. Для этого рассмотрим последовательность $\{a_n\}_{n=1}^{\infty}$, которая начинается с чисел

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \dots, \qquad (2.2)$$

и в которой каждый член, начиная с третьего, равен сумме двух предыдущих. Применяя алгоритм Евклида к числам a_{n+2}

и a_{n+1}, нетрудно убедиться, что для определения наибольшего общего делителя этих чисел потребуется ровно n шагов алгоритма и что $(a_{n+2}, a_{n+1}) = 1$. Например, для $n = 2$ наибольший общий делитель чисел $a_4 = 5$ и $a_3 = 3$ определяется за два шага:

$$5 = 3 \cdot 1 + 2,$$
$$3 = 2 \cdot 1 + 1.$$

Теперь покажем, что определение наибольшего общего делителя чисел a_{n+2} и a_{n+1} требует максимального количества шагов алгоритма Евклида среди всех пар натуральных чисел x и y, в которых меньшее число не превосходит a_{n+1}. Сделаем это индукцией по n. Далее везде полагаем, что $y < x$.

Если $y \leqslant a_1$, то $n = 0$ и $(x, y) = 1$ определяется без выполнения делений. Если $y \leqslant a_2 = 2$, то $n = 1$ и легко видеть, что (x, y) можно найти, выполнив только один шаг алгоритма Евклида. Два эти случая $(n = 0, 1)$ положим в основание индукции.

Предположим, что наибольший общий делитель любых натуральных x' и y' можно найти, выполнив самое большее n шагов алгоритма Евклида, если только $x' > y'$ и $y' \leqslant a_{n+1}$. Рассмотрим натуральные x и y такие, что $x > y$, $y \leqslant a_{n+2}$ и $n \geqslant 1$. Тогда $x = yq_1 + r_1$.

Если $r_1 \leqslant a_{n+1}$, то в силу предположения индукции наибольший общий делитель чисел y и r_1 можно найти, выполнив не более чем n делений, и, следовательно, для определения (x, y) потребуется выполнить не более чем $(n + 1)$ шагов алгоритма Евклида.

Пусть теперь $r_1 > a_{n+1}$. В этом случае $y = r_1q_2 + r_2$, где $r_2 \leqslant y - r_1 < a_{n+2} - a_{n+1} = a_n$. Следовательно, в силу предположения индукции наибольший общий делитель чисел r_1 и r_2 можно найти, выполнив не более чем $(n - 1)$ делений. Поэтому для определения (x, y) достаточно выполнить самое большее $(n + 1)$ шагов алгоритма Евклида.

Полученный результат сформулируем в виде следующей теоремы о сложности алгоритма Евклида.

Теорема 2.3. *Если меньшее из двух натуральных чисел не превосходит a_{n+1}, то наибольший общий делитель этих чисел*

можно найти, выполнив самое большее n шагов алгоритма Евклида. Вычисление наибольшего общего делителя чисел a_{n+2} и a_{n+1} требует выполнения ровно n шагов алгоритма Евклида.

Покажем, что при каждом натуральном k для членов последовательности (2.2) имеет место равенство

$$a_k = \frac{1}{\sqrt{5}}\Big(\alpha^{k+1} - \beta^{k+1}\Big), \tag{2.3}$$

в котором постоянные $\alpha = \frac{1+\sqrt{5}}{2}$ и $\beta = \frac{1-\sqrt{5}}{2}$ являются корнями уравнения $x^2 - x - 1 = 0$. Сделаем это индукцией по k. Так как $\alpha + \beta = 1$, $\alpha\beta = -1$, $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$ и $\alpha - \beta = \sqrt{5}$, то легко видеть, что

$$\alpha^2 - \beta^2 = (\alpha - \beta)(\alpha + \beta) = \sqrt{5},$$
$$\alpha^3 - \beta^3 = (\alpha - \beta)(\alpha^2 + \alpha\beta + \beta^2) = (\alpha - \beta)(\alpha + \beta + 1) = 2\sqrt{5}.$$

Поэтому $\frac{1}{\sqrt{5}}\Big(\alpha^2 - \beta^2\Big) = 1 = a_1$ и $\frac{1}{\sqrt{5}}\Big(\alpha^3 - \beta^3\Big) = 2 = a_2$. Таким образом, два первых члена последовательности (2.2) удовлетворяют равенству (2.3). Эти равенства положим в основание индукции.

Предположим, что равенство (2.3) также справедливо при всех k, не превосходящих некоторое m. Тогда из предположения индукции и равенства $a_{n+2} = a_{n+1} + a_n$ имеем

$$\begin{aligned} a_{m+2} &= a_{m+1} + a_m = \\ &= \frac{1}{\sqrt{5}}\Big(\alpha^{m+2} - \beta^{m+2}\Big) + \frac{1}{\sqrt{5}}\Big(\alpha^{m+1} - \alpha^{m+1}\Big) = \\ &= \frac{1}{\sqrt{5}}\Big(\alpha^{m+1}\big(\alpha + 1\big) - \beta^{m+1}\big(\beta + 1\big)\Big) = \frac{1}{\sqrt{5}}\Big(\alpha^{m+3} - \beta^{m+3}\Big). \end{aligned}$$

Равенство (2.3) доказано.

Воспользуемся теоремой 2.3 и равенством (2.3) для оценки числа шагов алгоритма Евклида, достаточного для нахождения наибольшего общего делителя натуральных чисел a и b. Допустим, что меньшее число b удовлетворяет неравенствам

$a_n < b \leqslant a_{n+1}$. Тогда из теоремы 2.3 следует, что для вычисления (a, b) потребуется не более n шагов. Величину n оценим при помощи (2.3). Из этого неравенства легко следует, что $a_n \geqslant \alpha^n$. Поэтому

$$\log_\alpha b > \log_\alpha a_n \geqslant \log_\alpha \alpha^n = n.$$

Так как $\left(\frac{1+\sqrt{5}}{2}\right)^5 > 10$, то, переходя к десятичным логарифмам, получим следующую оценку числа n:

$$n < \log_\alpha b = 5 \log_{\alpha^5} b < 5\log_{10} b.$$

Из полученного неравенства немедленно следует теорема Ламе о максимально возможном числе шагов в алгоритме Евклида.

Теорема 2.4 (Ламе). *Число шагов алгоритма Евклида при определении наибольшего общего делителя двух чисел не превосходит пятикратную длину десятичной записи меньшего из этих чисел.*

Заметим, что алгоритм Евклида можно использовать для вычисления целых x и y, удовлетворяющих равенству $(a, b) = ax + by$ (такие x, y называются *коэффициентами Безу* для чисел a, b). Для этого с помощью предпоследнего равенства из (2.1) надо выразить (a, b) через r_{n-1} и r_{n-2}. Затем в полученном равенстве вместо r_{n-1} надо подставить его выражение через r_{n-2} и r_{n-3}, и т. д. Рассмотрим этот алгоритм на следующем примере.

Пример 2.1. Ниже в левом столбце вычисляется наибольший общий делитель 73 и 14, а в правом находятся целые x и y, для которых $(73, 14) = 73x + 14y$:

$$\begin{aligned}
73 &= 14 \cdot 5 + 3, & 1 &= 3 - 2,\\
14 &= 3 \cdot 4 + 2, & 1 &= 3 - (14 - 3 \cdot 4),\\
3 &= 2 \cdot 1 + 1. & 1 &= (73 - 14 \cdot 5) - (14 - (73 - 14 \cdot 5)4) =\\
& & &= 73(1 + 4) - 14(5 + 1 + 20) =\\
& & &= 73 \cdot 5 - 14 \cdot 26.
\end{aligned}$$

Таким образом, $(73, 14) = 1$, $x = 5$, $y = -26$. □

Предложенный выше способ вычисления коэффициентов Безу можно условно разделить на два этапа: прямой ход (вычисление остатков r_i и неполных частных q_i при возрастающем i) и обратный ход (последовательное вычисление коэффициентов линейных комбинаций r_i и r_{i-1} при убывающем i). Это не всегда удобно, поскольку требует дополнительных затрат памяти на хранение r_i, q_i и рекурсию. Существует модификация алгоритма Евклида, свободная от этого недостатка.

Ее формулировка использует арифметические операции над упорядоченными наборами чисел, называемыми векторами. Подробнее о векторах мы расскажем в главе 5, а здесь просто будем пользоваться записью $q \cdot (x, y, z)$ для обозначения упорядоченной тройки (qx, qy, qz) и записью $(x, y, z) \pm (x', y', z')$ для тройки $(x \pm x', y \pm y', z \pm z')$, считая, как обычно, что умножение имеет более высокий приоритет, чем сложение и вычитание, а равенство упорядоченных наборов означает равенство всех их компонент.

Лемма 2.1 (Расширенный алгоритм Евклида)**.** *Пусть $a, b \in \mathbb{N}$ и $a > b$. Рассмотрим последовательность $(x_i, y_i, z_i) \in \mathbb{Z}^3$, $i = -1, 0, 1, 2, \ldots$, такую, что*

$$\begin{pmatrix} x_{-1} \\ y_{-1} \\ z_{-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ a \end{pmatrix}, \qquad \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ b \end{pmatrix}, \tag{2.4}$$

и

$$\begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} = \begin{pmatrix} x_{i-2} \\ y_{i-2} \\ z_{i-2} \end{pmatrix} - q_i \begin{pmatrix} x_{i-1} \\ y_{i-1} \\ z_{i-1} \end{pmatrix}, \tag{2.5}$$

где $q_i = \lfloor z_{i-2}/z_{i-1} \rfloor$. Тогда

1) *числа z_i, $i \geqslant 1$ совпадают с остатками, полученными на i-м шаге деления в алгоритме Евклида поиска* НОД(a, b) *(см.* (2.1)*);*

2) *при любом $i \geqslant -1$ выполнено равенство*

$$ax_i + by_i = z_i; \tag{2.6}$$

3) *если n — число делений с остатком в алгоритме Евклида, то $z_n = (a, b)$, причем x_n и y_n — искомые коэффициенты Безу линейной комбинации $ax_n + by_n = (a, b)$.*

Доказательство. 1. Равенство (2.5) показывает, что для третьей координаты вектора (x_i, y_i, z_i) выполнено $z_i = z_{i-2} - \lfloor z_{i-2}/z_{i-1} \rfloor z_{i-1}$, т. е. z_i является остатком от деления z_{i-2} на z_{i-1}. Поэтому последовательность $\{z_i\}$ совпадает с последовательностью $\{r_i\}$ остатков алгоритма Евклида для $r_{-1} = z_{-1} = a$, $r_0 = z_0 = b$.

2. Докажем искомое равенство по индукции. При $i = -1, 0$ оно верно в силу выбора начальных условий (2.4). Пусть $ax_{i-2} + by_{i-2} = z_{i-2}$ и $ax_{i-1} + by_{i-1} = z_{i-1}$. Тогда из (2.5) имеем

$$\begin{aligned} ax_i + by_i &= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = \\ &= (ax_{i-2} + by_{i-2}) - q_i(ax_{i-1} + by_{i-1}) = \\ &= z_{i-2} - q_i z_{i-1} = z_i. \end{aligned}$$

3. Искомое утверждение непосредственно следует из пп. 1—2. Лемма доказана.

Пример 2.2. Применим алгоритм леммы 2.1 к числам из примера 2.1. Вычисления, производимые этим алгоритмом, удобно сводить в таблицу:

1	0	1	−4	5	
0	1	−5	21	−26	
73	14	3	2	1	0

Два ее первых столбца являются начальными условиями (2.4). Согласно (2.5), каждый очередной столбец таблицы, имеющий номер $i \geqslant 1$, вычисляется как линейная комбинация двух стоящих слева от него столбцов с коэффициентами 1 и $(-q_i)$. Нижняя строка таблицы содержит остатки алгоритма Евклида. Вычисления оканчиваются, как только в нижней строке появился нуль. Тогда последний ненулевой остаток — это НОД$(73, 14)$, а над ним в таблице находятся коэффициенты Безу искомой линейной комбинации:

$$1 = (73, 14) = 73 \cdot 5 + 14 \cdot (-26).$$

Отметим, что объем дополнительной памяти для данного алгоритма весьма скромен: для проведения вычислений по формуле (2.5) достаточно всего 10 целочисленных переменных. □

Целое положительное b, которое делится на каждое из целых чисел $a_1, a_2, \ldots, a_n$, называется общим кратным этих чисел. Наименьшее положительное число среди общих кратных чисел $a_1, a_2, \ldots, a_n$ называется их *наименьшим общим кратным* и обозначается символом $\text{НОК}(a_1, a_2, \ldots, a_n)$. Например, $\text{НОК}(2, 4, 6) = 12$. Можно показать, что $\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab$ для любых натуральных a и b.

2.2. Разложение на простые множители

Натуральное число p называется *простым*, если у него есть ровно два различных натуральных делителя — единица и само число p. Среди первых тридцати натуральных чисел простыми являются

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29.$$

Из определения простого числа легко следует, что любое натуральное число можно разложить в произведение простых, например $12 = 2 \cdot 2 \cdot 3$. Покажем, что такое разложение единственно с точностью до порядка следования сомножителей. Сначала докажем две простые леммы.

Лемма 2.2. *Если произведение ab натуральных a и b делится на простое p, то хотя бы один из сомножителей также делится на p.*

Доказательство. Допустим, что утверждение леммы не верно. Тогда ни один из сомножителей не делится на p. Следовательно, $(a, p) = 1$ и $(b, p) = 1$, и из утверждения теоремы 2.2 следует, что найдутся такие целые x_1, x_2 и y_1, y_2, что

$$1 = x_1 a + x_2 p, \qquad 1 = y_1 b + y_2 p.$$

Перемножив эти равенства, получим, что

$$\begin{aligned} 1 &= (x_1 a + x_2 p)(y_1 b + y_2 p) = \\ &= (x_1 y_1) ab + p(x_2 y_1 b + x_1 y_2 a + x_2 y_2 p), \end{aligned}$$

т. е. в силу теоремы 2.2 числа ab и p взаимно просты. Противоречие. Лемма доказана.

Лемма 2.3. *Если произведение $a_1a_2\cdots a_n$ натуральных a_i делится на простое p, то хотя бы один из сомножителей также делится на p.*

Доказательство. Лемму докажем индукцией по числу сомножителей. Случай $n = 2$ доказан в предыдущей лемме. Допустим, утверждение леммы справедливо для любых произведений, содержащих не более k сомножителей. Тогда если произведение $(a_1a_2\cdots a_k)a_{k+1}$ делится на p, то из леммы 2.2 следует, что либо $a_1a_2\cdots a_k$, либо a_{k+1} делится на p. В первом случае утверждение леммы следует из предположения индукции. Во втором случае справедливость леммы очевидна. Лемма доказана.

Теперь можно доказать основную теорему арифметики о единственности разложения целого числа на простые сомножители.

Теорема 2.5. *Любое натуральное число единственным образом раскладывается в произведение простых сомножителей и притом единственным образом, с точностью до их порядка.*

Доказательство. Теорему докажем методом математической индукции. В основание индукции положим число 2, единственность разложения которого очевидна. Предположим, что каждое натуральное число, не превосходящее N, разлагается на простые множители единственным образом. Покажем, что из этого предположения следует единственность разложения числа $N + 1$. Действительно, если натуральное $N + 1$ имеет два различных разложения в произведение простых сомножителей, то

$$N + 1 = p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n} = q_1^{s_1}q_2^{s_2}\cdots q_m^{s_m},$$

где $p_1 < p_2 < \cdots < p_n$ и $q_1 < q_2 < \cdots < q_m$. Покажем, что $p_1 = q_1$. Так как простое p_1 делит произведение

$$\underbrace{q_1\cdots q_1}_{s_1\text{ раз}}\underbrace{q_2\cdots q_2}_{s_2\text{ раз}}\cdot\ldots\ldots\cdot\underbrace{q_m\cdots q_m}_{s_m\text{ раз}}, \tag{2.7}$$

то в силу леммы 2.3 число p_1 также делит один из его сомножителей. В (2.7) все сомножители — простые числа. Следовательно, p_1 совпадает с одним из них. Так как p_1 — минимальный простой делитель $N+1$, то легко видеть, что $p_1 = q_1$. Сокращая левую и правую части равенства (2.7) на p_1, получим

$$\frac{N+1}{p_1} = p_1^{k_1-1} p_2^{k_2} \cdots p_n^{k_n} = q_1^{s_1-1} q_2^{s_2} \cdots q_m^{s_m}. \tag{2.8}$$

По предположению индукции натуральное $(N+1)/p_1$ раскладывается на простые множители единственным образом. Поэтому в (2.8) $n = m$ и для каждого $i \in \{1, \ldots, n\}$ справедливы равенства $p_i = q_i$ и $k_i = s_i$. Теорема доказана.

2.3. Теорема Чебышёва

Нетрудно показать, что простых чисел бесконечно много. Если это не так, то найдется максимальное простое число n. Очевидно, что $n! = \prod_{k=1}^{n} k$ делится без остатка на каждое простое, и, следовательно, остаток от деления $n! + 1$ на каждое простое равен единице, т. е. $n! + 1$ не делится ни на одно из простых чисел. Поэтому либо $n! + 1$ само простое, либо содержит простой делитель, больший n. Получившееся противоречие доказывает бесконечность числа простых чисел.

Этот факт был известен еще Евклиду в III в. до н. э. Однако естественный вопрос о том, как часто среди натуральных чисел встречаются простые, долго оставался без ответа. Через $\pi(x)$ обозначим количество простых чисел, не превосходящих x. Если рассмотреть первые простые числа

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	199	211	223		

и вычислить разности между соседними, то можно заметить, что промежутки

1	2	2	4	2	4	2	4	6	2	6	4	2	4	6
6	2	6	4	2	6	4	6	8	4	2	4	2	4	14
4	6	2	10	2	6	6	4	6	6	2	10	8	12	12

между соседними простыми в среднем возрастают, поэтому можно предположить, что $\pi(n)/n \to 0$ с ростом n. Это действительно так. Более того, Гаусс и Лежандр, в конце XVIII в. независимо друг от друга численно изучавшие функцию $\pi(n)$ (количество вычисленных ими значений $\pi(n)$ исчислялось сотнями тысяч), предположили, что имеет место асимптотическое равенство[1)]

$$\pi(x) \sim \frac{x}{\ln x}, \tag{2.9}$$

но доказать это предположение не смогли. И только в самом конце XIX в. Адамар и Валле-Пуссен, также независимо и одновременно, установили справедливость равенства (2.9), называемого *асимптотическим законом распределения простых чисел.*

Отметим, что первое существенное продвижение в изучении распределения простых чисел было сделано П. Л. Чебышёвым, который в середине XIX в. нашел порядок роста функции $\pi(n)$, установив для нее достаточно близкие верхнюю и нижнюю оценки. Далее в теореме 2.6 докажем ослабленные оценки Чебышёва. Для этого потребуются простые неравенства

$$\frac{2^{2n}}{2n} < \binom{2n}{n} < 2^{2n}$$

для среднего биномиального коэффициента, справедливость которых при всех $n > 1$ легко следует из формулы бинома Ньютона.

Теорема 2.6 (Чебышёв). *Существуют такие постоянные c_1 и c_2, что для любого целого $n > 2$ справедливы неравенства*

$$c_1 \frac{n}{\log_2 n} \leqslant \pi(n) \leqslant c_2 \frac{n}{\log_2 n}.$$

[1)] Формула $a(n) \sim b(n)$ означает, что $\lim a(n)/b(n) = 1$ при $n \to \infty$.

Доказательство. Сначала получим верхнюю оценку функции $\pi(n)$. Для этого рассмотрим биномиальный коэффициент

$$\binom{2n}{n} = \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 2}. \tag{2.10}$$

Нетрудно видеть, что каждое простое число, которое больше n и не больше $2n$, присутствует в числителе правой части (2.10) и не сокращается ни с одним из множителей знаменателя, все множители которого не превосходят n. Поэтому коэффициент $\binom{2n}{n}$ делится на все простые числа, которые больше n и не больше $2n$. Всего таких чисел ровно $\pi(2n) - \pi(n)$. Так как $\binom{2n}{n} < 2^{2n}$, то справедливы неравенства

$$(n+1)^{\pi(2n)-\pi(n)} < \binom{2n}{n} < 2^{2n},$$

из которых после логарифмирования и несложных преобразований получим оценку разности значений функции π на четном аргументе $2n$ и его половине n:

$$\pi(2n) - \pi(n) < \frac{2n}{\log_2 n}. \tag{2.11}$$

Для степеней двойки последнее неравенство, очевидно, эквивалентно следующей рекуррентной оценке функции $\pi(n)$:

$$\pi(2^k) < \pi(2^{k-1}) + \frac{2^k}{k-1}. \tag{2.12}$$

Теперь, используя полученное рекуррентное неравенство, индукцией по k покажем, что

$$\pi(2^k) < \frac{4 \cdot 2^k}{k}. \tag{2.13}$$

В основание индукции положим очевидный случай $k = 3$. Далее в силу (2.12) при $k \geqslant 4$ имеем

$$\pi(2^k) < \pi(2^{k-1}) + \frac{2^k}{k-1} \leqslant \frac{4 \cdot 2^{k-1}}{k-1} + \frac{2^k}{k-1} = \frac{3 \cdot 2^k}{k-1} \leqslant \frac{4 \cdot 2^k}{k}.$$

Наконец, при $n \leqslant 2^k < 2n$ из последнего неравенства следует, что

$$\pi(n) \leqslant \pi(2^k) < \frac{4 \cdot 2^k}{k} < \frac{4 \cdot 2n}{\log_2 n}.$$

Верхняя оценка теоремы доказана.

Для доказательства нижней оценки теоремы снова воспользуемся биномиальным коэффициентом $\binom{2n}{n}$. Покажем, что в его разложении

$$\binom{2n}{n} = p_1^{k_1} \cdots p_i^{k_i} \cdots p_m^{k_m} \tag{2.14}$$

на простые множители каждый множитель $p_i^{k_i}$ не превосходит $2n$. Для этого определим степень $k(p)$, с которой простое число p входит в разложение числа $n!$ на простые множители. Нетрудно видеть, что среди первых n натуральных чисел ровно $\left\lfloor \frac{n}{p} \right\rfloor$ делятся на p, $\left\lfloor \frac{n}{p^2} \right\rfloor$ чисел делятся на p^2, $\left\lfloor \frac{n}{p^3} \right\rfloor$ чисел делятся на p^3 и т. д. Поэтому

$$k(p) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^i} \right\rfloor + \ldots. \tag{2.15}$$

Так как $\binom{2n}{n} = \frac{(2n)!}{n!n!}$, то степень вхождения числа p в разложение (2.14) равна разности степеней вхождения числа p в числитель и знаменатель. Из равенства (2.15) немедленно следует, что искомая величина равна сумме

$$\left(\left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \right) + \cdots + \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) + \ldots, \tag{2.16}$$

в которой только первые $\lfloor \log_p 2n \rfloor$ слагаемых могут быть отличны от нуля, так как $\left\lfloor \frac{2n}{p^i} \right\rfloor = 0$ при $p^i > 2n$. Теперь, учитывая неравенства $0 \leqslant \lfloor 2x \rfloor - 2\lfloor x \rfloor \leqslant 1$, получаем, что сумма (2.16), а следовательно, и степень k, с которой число p входит в (2.14), не превосходят величины $\lfloor \log_p 2n \rfloor$. Поэтому

$$p^k \leqslant p^{\lfloor \log_p 2n \rfloor} \leqslant p^{\log_p 2n} = 2n.$$

Таким образом, разложение (2.14) содержит не более $\pi(2n)$ сомножителей, каждый из которых не превосходит $2n$. Поэтому справедливы неравенства

$$\frac{2^{2n}}{2n} < \binom{2n}{n} \leqslant (2n)^{\pi(2n)},$$

из которых после логарифмирования и несложных преобразований получим нижнюю оценку функции π для четных аргументов:

$$\pi(2n) \geqslant \frac{2n}{\log_2 2n} - 1 \geqslant \frac{1}{2} \cdot \frac{2n}{\log_2 2n}.$$

Аналогичная оценка справедлива и для нечетных аргументов функции π. Действительно, так как каждое четное число бóльшее двух не является простым, то

$$\pi(2n-1) = \pi(2n) \geqslant \frac{1}{2} \cdot \frac{2n}{\log_2 2n} > \frac{1}{2} \cdot \frac{2n-1}{\log_2(2n-1)}$$

для любого $n \geqslant 2$. Теорема доказана.

2.4. Сравнения

Будем говорить, что целые a и b *сравнимы* по модулю натурального m, если совпадают их остатки от деления на m. Сравнимость a и b по модулю m будем обозначать равенством

$$a = b \pmod m,$$

которое называется *сравнением*. Легко видеть, что если целые a и b сравнимы по модулю m, то их разность $a - b$ делится на m и существует такое целое k, что[1)]

$$a = b + km.$$

Используя это равенство, покажем, что сравнения можно почленно складывать, вычитать и умножать.

[1)] Верно и обратное, поэтому $a = b \pmod m$ тогда и только тогда, когда найдется такое целое k, что $a = b + km$.

Пусть $a_1 = b_1 \pmod m$ и $a_2 = b_2 \pmod m$. В этом случае найдутся такие целые k_1 и k_2, что

$$a_1 = b_1 + k_1 m, \qquad a_2 = b_2 + k_2 m.$$

Тогда, так как

$$a_1 + a_2 = (b_1 + k_1 m) + (b_2 + k_2 m) = b_1 + b_2 + (k_1 + k_2)m,$$

то

$$a_1 + a_2 = b_1 + b_2 \pmod m.$$

Аналогичным образом из равенства

$$a_1 - a_2 = (b_1 + k_1 m) - (b_2 + k_2 m) = b_1 - b_2 + (k_1 - k_2)m$$

следует, что

$$a_1 - a_2 = b_1 - b_2 \pmod m.$$

Наконец, поскольку

$$a_1 a_2 = (b_1 + k_1 m)(b_2 + k_2 m) = b_1 b_2 + (b_1 k_2 + b_2 k_1 + k_1 k_2 m)m,$$

то

$$a_1 a_2 = b_1 b_2 \pmod m.$$

Если $a = b \pmod m$, то $ad = bd \pmod{md}$ для любого натурального d. Действительно, из того, что разность $b - a$ делится на m, легко следует, что $bd - ad$ делится на md. Аналогичным образом легко видеть, что если $m = m_1 d$, $a = a_1 d$ и $b = b_1 d$, то из сравнения $a = b \pmod m$ следует сравнение $a_1 = b_1 \pmod{m_1}$, т. е. обе части сравнения и модуль можно разделить на их общий делитель.

Пусть теперь $a = b \pmod{m_1}$ и $a = b \pmod{m_2}$. В этом случае $b - a$ делится на m_1 и m_2 и, следовательно, делится на их наименьшее общее кратное, т. е.

$$a = b \pmod{\text{НОК}(m_1, m_2)}.$$

Если $a = b \pmod{m_1 m_2}$, то найдется такое целое k, что

$$a = b + k(m_1 m_2) = b + (km_1)m_2 = b + (km_2)m_1.$$

Следовательно, a и b сравнимы по модулям m_1 и m_2. Отсюда видим, что из сравнения $a = b \pmod m$ следует сравнимость a и b по модулю, равному любому делителю m.

2.5. Классы вычетов

Сравнение чисел по модулю фиксированного натурального числа m определяет на множестве целых чисел отношение эквивалентности и разбивает это множество на классы эквивалентности, называемые классами вычетов по модулю m. Символом $[i]_m$ будем обозначать *класс вычетов*, состоящий из всех целых чисел, сравнимых с i по модулю m. Такое обозначение неоднозначно, например, $[8]_3$ и $[2]_3$ обозначают один и тот же класс, состоящий из чисел, сравнимых с двойкой по модулю три. Такая неоднозначность доставляет определенные неудобства, избежать которые можно, используя для обозначения классов вычетов минимальные неотрицательные элементы этих классов. Множество классов вычетов по модулю m будем обозначать символом $\mathbb{Z}_m$, т. е.

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Выше было установлено, что сравнения по одинаковому модулю можно складывать и умножать. Воспользуемся этим и определим в $\mathbb{Z}_m$ операции сложения и умножения классов вычетов, положив

$$[i]_m + [j]_m = [i+j]_m, \quad [i]_m[j]_m = [ij]_m. \tag{2.17}$$

Пример 2.3.

$$[5]_{10} + [6]_{10} = [11]_{10} = [1]_{10}, \quad [5]_{10}[6]_{10} = [30]_{10} = [0]_{10},$$
$$[5]_8 + [6]_8 = [11]_8 = [3]_8, \quad [5]_8[6]_8 = [30]_8 = [6]_8. \ \square$$

Введенные операции обладают многими свойствами, присущими операциям сложения и умножения целых чисел. Так, нетрудно показать, что для них справедливы законы ассоциативности

$$([i]_m + [j]_m) + [k]_m = [i]_m + ([j]_m + [k]_m),$$
$$([i]_m[j]_m)[k]_m = [i]_m([j]_m[k]_m),$$

коммутативности

$$[i]_m + [j]_m = [j]_m + [i]_m, \quad [i]_m[j]_m = [j]_m[i]_m,$$

закон дистрибутивности

$$([i]_m + [j]_m)[k]_m = [i]_m[k]_m + [j]_m[k]_m$$

и свойства сложения с нулем и умножения на единицу

$$[i]_m + [0]_m = [i]_m, \quad [i]_m[1]_m = [i]_m.$$

Операции (2.17) называются сложением и умножением по модулю m.

Часто бывает удобно, рассматривая классы вычетов, отождествлять сами классы вычетов и их минимальные неотрицательные элементы — использовать символ i как для целого числа из множества $\{0, 1, \ldots, m-1\}$, так и для класса $[i]_m$. Поэтому далее через $\mathbb{Z}_m$ будем обозначать не только множество классов вычетов по модулю m, но и множество $\{0, 1, \ldots, m-1\}$, подразумевая при этом, что его элементы, называемые также *вычетами*, складываются и умножаются по модулю m как соответствующие им классы. Если числа 5 и 6 рассматривать в качестве элементов $\mathbb{Z}_8$, то в соответствии с примером 2.3 их сумма равна 3, а произведение 6.

Любые m чисел, принадлежащие разным классам эквивалентности в $\mathbb{Z}_m$, называются *полной системой вычетов* по модулю m. Например, четные и нечетные числа образуют классы вычетов по модулю два, а пара $(3, 4)$ является полной системой вычетов по этому модулю.

Теорема 2.7. *Пусть* $(a, m) = 1$ *и* $\{x_1, \ldots, x_m\}$ *— полная система вычетов по модулю* m*. Тогда множество* $\{ax_i + b\}_{i=1}^m$*, где* b *— произвольное целое, будет полной системой вычетов.*

Доказательство. Допустим, что $ax_i + b = ax_j + b \pmod m$. Тогда в силу рассмотренных выше свойств сравнений $ax_i = ax_j \pmod m$ и, следовательно, $a(x_i - x_j) = km$. Так как a и m взаимно простые, то m должно делить разность $x_i - x_j$, что, очевидно, невозможно. Таким образом, все m различных чисел $ax_i + b$ попарно несравнимы по модулю m. Теорема доказана.

2.6. Решение сравнений

Будем говорить, что линейное сравнение $ax = b \pmod m$ *разрешимо* относительно переменной x, если существует такое целое n, что справедливо сравнение $an = b \pmod m$. Если n — решение рассматриваемого сравнения, то и $n + km$ при любом целом k также будет решением этого сравнения, т. е. решением сравнения будет класс вычетов по модулю m.

Теорема 2.8. *Сравнение $ax = b \pmod m$ разрешимо тогда и только тогда, когда (a, m) делит b. Если $d = (a, m)$ делит b, то на множестве $\mathbb{Z}_m$ сравнение имеет ровно d решений, сравнимых по модулю m/d.*

Доказательство. Пусть x_0 — решение сравнения и $(a, m) = d$. Тогда $a = a'd$ и $m = m'd$, где a' и m' — целые. Из равенства $ax_0 = b \pmod m$ следует, что $b = a'dx_0 - km'd = d(a'x_0 - km')$, где k — целое, т. е. d является делителем b.

Теперь покажем, что если d делит b, то решение существует. Из теоремы 2.2 следует, что существуют такие целые p и q, что $d = ap + mq$. Пусть $b = b'd$. Тогда $b = db' = a(pb') + m(qb')$ и, следовательно, $a(pb') = b \pmod m$. Таким образом, pb' — решение рассматриваемого сравнения.

Теперь найдем число решений системы на множестве $\mathbb{Z}_m$. Пусть $m = m'd$ и x_i и x_j — решения. Тогда $a'd(x_i - x_j) = 0 \pmod{m'd}$, или после сокращения на общий множитель d, $a'(x_i - x_j) = 0 \pmod{m'}$, где $(a', m') = 1$. Из последнего равенства следует, что m' делит $x_i - x_j$, т. е. x_i и x_j сравнимы по модулю m'. Поэтому если x_0 — минимальное неотрицательное решение, то решениями в $\mathbb{Z}_m$ будут также числа $x_0 + km'$, где $k = 1, \ldots, d - 1$. Теорема доказана.

Будем говорить, что число a *обратимо* по модулю m, если разрешимо сравнение $ax = 1 \pmod m$. Если это сравнение разрешимо, то его решение обозначим через a^{-1} и назовем *обратным* к a по модулю m. Из теоремы 2.8 легко извлекается необходимое и достаточное условие обратимости одного целого числа по модулю другого.

Теорема 2.9. *Число a обратимо по модулю m тогда и только тогда, когда $(a, m) = 1$. Если a обратимо по модулю m, то оно имеет единственное обратное по этому модулю.*

Пример 2.4. На множестве $\mathbb{Z}_{73}$ решим сравнение $14x = 1 \pmod{73}$. Так как $(14, 73) = 1$ (см. пример 2.1), то в силу теоремы 2.9 сравнение имеет единственное решение $14^{-1} \pmod{73}$. Для нахождения обратного воспользуемся найденным в примере 2.1 равенством $1 = 73 \cdot 5 - 14 \cdot 26$, из которого следует, что $14^{-1} = -26 = 47 \pmod{73}$. □

Пример 2.5. На множестве $\mathbb{Z}_{20}$ найдем все решения сравнения $8x = 12 \pmod{20}$. Так как $(8, 20) = 4$, 4 делит 12 и $20 = 4 \cdot 5$, то в силу теоремы 2.8 сравнение имеет четыре решения. Разделив элементы исходного сравнения на 4, получим новое сравнение $2x = 3 \pmod{5}$, имеющее на множестве $\mathbb{Z}_5$ единственное решение. Так как $(2, 5) = 1 = -2 \cdot 2 + 5$, то $2^{-1} = -2 = 3 \pmod{5}$. Следовательно, $x = 3 \cdot 3 = 4 \pmod{5}$ и $x_0 = 4 \pmod{20}$ — решение сравнения на $\mathbb{Z}_{20}$. Остальные три решения сравнимы с найденным x_0 по модулю 5. Поэтому $x_1 = 9, x_2 = 14, x_3 = 19$. □

2.7. Китайская теорема об остатках

Будем рассматривать системы линейных сравнений простейшего вида $x = a_i \pmod{p_i}$ с попарно взаимно простыми модулями p_i. Решение таких систем ниже полностью описывается в двух теоремах. Вторая из этих теорем называется китайской теоремой об остатках.

Теорема 2.10. *Пусть $p_1, \ldots, p_n$ — попарно взаимно простые положительные, $a_1, \ldots, a_n$ — целые. Система сравнений*

$$\left.\begin{aligned} x &= a_1 \pmod{p_1}, \\ x &= a_2 \pmod{p_2}, \\ &\cdots\cdots\cdots\cdots \\ x &= a_n \pmod{p_n}, \end{aligned}\right\} \tag{2.18}$$

имеет решение, причем все решения системы (2.18) сравнимы по модулю $p_1 p_2 \ldots p_n$.

Доказательство. Без ограничения общности будем считать, что в (2.18) каждое a_i принимает значение от 0 до $p_i - 1$. Поэтому легко видеть, что при фиксированных числах $p_1, \ldots, p_n$ существует ровно $M = p_1 \times \cdots \times p_n$ различных систем вида (2.18). Столько же существует и целых чисел, принадлежащих множеству $\mathbb{Z}_M$. Так как каждое число из $\mathbb{Z}_M$ является решением некоторой системы (2.18), то общее число решений систем (2.18) на множестве $\mathbb{Z}_M$ равно числу этих систем. Поэтому для доказательства теоремы достаточно показать, что в $\mathbb{Z}_M$ нет двух чисел, являющихся решениями одной и той же системы вида (2.18). Сделаем это методом от противного. Допустим, что некоторая система (2.18) имеет такие решения z и y, что $0 \leqslant y < z < M$. В этом случае разность $z - y$ удовлетворяет неравенствам

$$0 < z - y < M \tag{2.19}$$

и является решением системы сравнений

$$\left.\begin{aligned} x &= 0 \pmod{p_1}, \\ x &= 0 \pmod{p_2}, \\ &\ldots\ldots\ldots\ldots\ldots \\ x &= 0 \pmod{p_n}. \end{aligned}\right\} \tag{2.20}$$

Из (2.20) следует, что каждое p_i делит $z - y$ и, следовательно, входит в каноническое разложение $z - y$ на простые множители. Поэтому $z - y \geqslant M$, что противоречит (2.19). Таким образом, каждая система вида (2.18) имеет не более одного решения среди целых неотрицательных чисел из $\mathbb{Z}_M$. Теорема доказана.

Теперь найдем решение системы (2.18). Сделаем это в следующей теореме.

Теорема 2.11 (Китайская теорема об остатках)**.** *Пусть* $p_1, p_2, \ldots, p_n$ *— взаимно простые натуральные,* $a_1, \ldots, a_n$ *— целые,* $M = \prod_{i=1}^{n} p_i$*. Единственным решением системы сравнений*

$$\left.\begin{aligned} x &= a_1 \pmod{p_1}, \\ x &= a_2 \pmod{p_2}, \\ &\ldots\ldots\ldots\ldots\ldots \\ x &= a_n \pmod{p_n}, \end{aligned}\right\}$$

на множестве $\mathbb{Z}_M$ *является*

$$x_0 = a_1 M_1 N_1 + \cdots + a_i M_i N_i + \cdots + a_n M_n N_n \pmod{M}, \quad (2.21)$$

где $M_i = M/p_i$ *и* $N_i = M_i^{-1} \pmod{p_i}$ *для* $i = 1, 2, \ldots, n$.

Доказательство. Существование и единственность решения рассматриваемой системы на множестве $\mathbb{Z}_M$ следуют из предыдущей теоремы. Так как

$$x \pmod{p_i} = (x \pmod{M}) \pmod{p_i}$$

для любого x и каждого $i = 1, 2, \ldots, n$ и, кроме того, в силу условий теоремы справедливы равенства

$$M_j = 0 \pmod{p_i} \quad \text{при } i \neq j, \qquad M_i N_i = 1 \pmod{p_i},$$

то легко видеть, что x_0 действительно является решением рассматриваемой системы сравнений. Теорема доказана.

Пример 2.6. Решим систему сравнений

$$\left.\begin{aligned} x &= 1 \pmod 3, \\ x &= 2 \pmod 4, \\ x &= 3 \pmod 5. \end{aligned}\right\}$$

Нетрудно видеть, что $M = 60$, $M_1 = 20$, $M_2 = 15$, $M_3 = 12$. Кроме того, так как $M_1 = 2 \pmod 3$, $M_2 = 3 \pmod 4$ и $M_3 = 2 \pmod 5$, то $M_1^{-1} = 2 \pmod 3$, $M_2^{-1} = 3 \pmod 4$ и $M_3^{-1} = 3 \pmod 5$. Подставляя полученные значения в формулу (2.21), находим

$$x = 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 238 = 58 \pmod{60}.$$

Следовательно, число 58 является единственным решением рассматриваемой системы на множестве $\mathbb{Z}_{60}$. □

Китайская теорема об остатках является мощным средством, облегчающим вычисления с большими составными модулями.

Пример 2.7. Решим уравнение

$$x^3 + 12x + 15 = 0 \pmod{35}.$$

Из свойств сравнений следует, что решение рассматриваемого уравнения равносильно решению системы

$$\left.\begin{aligned} x^3 + 2x = 0 \pmod 5, \\ x^3 + 5x + 1 = 0 \pmod 7. \end{aligned}\right\}$$

Эту систему решим, последовательно подставляя в первое уравнение все элементы из $\mathbb{Z}_5$, а во второе — из $\mathbb{Z}_7$. В результате получим единственное решение, удовлетворяющее системе сравнений

$$\left.\begin{aligned} x = 0 \pmod 5, \\ x = 1 \pmod 7, \end{aligned}\right\}$$

решив которую, находим единственное решение исходного уравнения $x = 15 \pmod{35}$. □

2.8. Функция Эйлера

Функция $\varphi(m)$, равная количеству натуральных чисел, не превосходящих m и взаимно простых с m, называется *функцией Эйлера.* В следующей таблице представлены первые двенадцать значений этой функции:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	0	1	2	2	4	2	6	4	6	4	10	4

Легко видеть, что $\varphi(p) = p - 1$ для каждого простого p. Также несложно найти значение функции Эйлера для степени простого числа.

Лемма 2.4. *Пусть p — простое. Тогда $\varphi(p^k) = p^k - p^{k-1}$ для любого натурального k.*

Доказательство. Среди первых p^k натуральных чисел ровно p^{k-1} делится на p. Каждое из $p^k - p^{k-1}$ остальных чисел взаимно просто с p. Следовательно, $\varphi(p^k) = p^k - p^{k-1}$. Лемма доказана.

Лемма 2.5. *Для любых взаимно простых натуральных a и b справедливо равенство $\varphi(ab) = \varphi(a)\varphi(b)$.*

Доказательство. Каждое из $\varphi(ab)$ взаимно простых с ab и не превосходящих ab натуральных чисел взаимно просто одновременно с a и b. Все эти числа находятся в таблице

$$\begin{array}{rrcrcr}
1 & 2 & \cdots & i & \cdots & a \\
a+1 & a+2 & \cdots & a+i & \cdots & 2a \\
2a+1 & 2a+2 & \cdots & 2a+i & \cdots & 3a \\
\multicolumn{6}{c}{\dotfill} \\
ja+1 & ja+2 & \ldots & ja+i & \ldots & (j+1)a \\
\multicolumn{6}{c}{\dotfill} \\
(b-1)a+1 & (b-1)a+2 & \cdots & (b-1)a+i & \cdots & ba
\end{array}$$

из b строк и a столбцов. В каждой строке этой таблицы находится полная система вычетов по модулю a и, следовательно, $\varphi(a)$ чисел, взаимно простых с a. В каждом столбце таблицы все элементы одного столбца имеют одинаковые вычеты по модулю a. Таким образом, в таблице есть $\varphi(a)$ столбцов, полностью состоящих из чисел, взаимно простых с a. В силу взаимной простоты a и b и теоремы 2.7 в каждом из этих столбцов находится полная система вычетов по модулю b и, следовательно, $\varphi(b)$ чисел, взаимно простых с b. Следовательно, в таблице находится ровно $\varphi(a)\varphi(b)$ чисел, одновременно взаимно простых с a и b. Лемма доказана.

Теорема 2.12. *Если $m = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, то*

$$\varphi(m) = m\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \ldots \Big(1 - \frac{1}{p_n}\Big).$$

Доказательство. Из доказанных выше лемм 2.4 и 2.5 легко следует, что

$$\begin{aligned}
\varphi(p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_n^{k_n}) = \\
&= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-2}) \cdots (p_n^{k_n} - p_n^{k_n-1}).
\end{aligned}$$

Теорема доказана.

Пример 2.8. Найдем $\varphi(120)$. Так как $120 = 2^3 \cdot 3 \cdot 5$, то $\varphi(120) = 4 \cdot 2 \cdot 4 = 32$. □

Докажем имеющую многочисленные приложения классическую теорему элементарной теории чисел — теорему Эйлера.

Теорема 2.13 (Эйлер). *Если* $(a, n) = 1$, *то*

$$a^{\varphi(n)} = 1 \pmod{n}.$$

Доказательство. Будем полагать, что все встречающиеся далее числа принадлежат $\mathbb{Z}_n$. Пусть $a_1, a_2, \ldots, a_{\varphi(n)}$ — подмножество полной системы вычетов по модулю n, состоящее из всех взаимно простых с n вычетов. Такое множество называется *приведенной системой вычетов*. Если a взаимно просто с n, то в силу теоремы 2.7 числа $aa_1, aa_2, \ldots, aa_{\varphi(n)}$ образуют ту же самую приведенную систему вычетов, взятую, в общем случае, в другом порядке. Поэтому

$$\begin{aligned} a_1 \cdot a_2 \cdots a_{\varphi(n)} &= aa_1 \cdot aa_2 \cdots aa_{\varphi(n)} = \\ &= a^{\varphi(n)} a_1 \cdot a_2 \cdots a_{\varphi(n)} \pmod{n}. \end{aligned} \tag{2.22}$$

Сокращая в (2.22) одинаковые множители, приходим к равенству $a^{\varphi(n)} = 1 \pmod{n}$. Теорема доказана.

Простым следствием теоремы Эйлера является ее частный случай — малая теорема Ферма.

Теорема 2.14 (Ферма). *Если* $a \neq 0 \pmod{p}$, *то*

$$a^{p-1} = 1 \pmod{p}.$$

Пример 2.9. Воспользуемся малой теоремой Ферма для решения уравнения

$$x^{124} + 2x^4 + 1 = 0 \pmod{55}.$$

Так как в силу малой теоремы Ферма $x^4 = 1 \pmod{5}$ и $x^{10} = 1 \pmod{11}$ и, кроме того, $124 = 0 \pmod{4}$ и $124 = 4 \pmod{10}$, то решаемое уравнение равносильно системе

$$\left.\begin{aligned} 4 &= 0 \pmod{5}, \\ 3x^4 + 1 &= 0 \pmod{11}. \end{aligned}\right\}$$

Очевидно, что первое уравнение системы решений не имеет, и, следовательно, исходное уравнение также не имеет решений. □

Задачи

2.1. Доказать, что отношение делимости $a \mid b$ является отношением частичного порядка на множестве натуральных чисел. Построить диаграммы частично упорядоченных множеств делителей для чисел $n = 6, 12, 18, 24, 36$.

2.2. Показать, что если a делит c, b делит c и $(a, b) = 1$, то ab делит c.

2.3. Доказать, что

$$\left\lfloor \frac{\lfloor \frac{x}{k} \rfloor}{k^{i-1}} \right\rfloor = \left\lfloor \frac{x}{k^i} \right\rfloor$$

для любых натуральных x, k, i.

2.4. Доказать, что для любых натуральных $a_1, \ldots, a_n$ существуют такие целые $b_1, \ldots, b_n$, что $a_1 b_1 + \cdots + a_n b_n = (a_1, \ldots, a_n)$.

2.5. Доказать, что множество пар коэффициентов Безу для натуральных чисел a, b, т. е. множество всех таких целых $x, y \in \mathbb{Z}$, что $ax + by = (a, b)$, бесконечно. Как по одной известной паре коэффициентов Безу найти все остальные такие пары?

2.6. Доказать, что оба алгоритма из примера 2.1 и леммы 2.1 находят минимальные по модулю числа среди всех пар коэффициентов Безу.

2.7. Доказать, что существует пара коэффициентов Безу, которая удовлетворяет или неравенству $|x| \leqslant (a, b) \cdot \frac{b}{2}$, или неравенству $|y| \leqslant (a, b) \cdot \frac{a}{2}$.

2.8. Доказать, что
1) $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$;
2) $(k^a - 1, k^b - 1) = k^{(a,b)} - 1$ для любого натурального $k \neq 1$.

2.9. Найти все целые решения уравнений:

1) $83x + 115y = 1$; 2) $2015x - 1286y = 5$; 3) $426x + 125y = 14$.

2.10. Сформулировать и доказать критерий разрешимости в целых числах уравнения $a_1 x_1 + \cdots + a_n x_n = b$, где $a_i, b \in \mathbb{Z}$.

2.11. Сколько различных делителей имеет число $p_1^{n_1} \dots p_m^{n_m}$, где p_i — различные простые числа? Чему равна сумма всех его делителей?

2.12. (Теорема Вильсона) Доказать, что целое $p > 1$ является простым тогда и только тогда, когда $(p-1)! = -1 \pmod p$.

2.13. Показать, что если n — не простое число, то $(n-1)! = 0 \pmod n$ за исключением случая $n = 4$.

2.14. Найти вычет, обратный к вычету 777 по модулю 1000.

2.15. Решить уравнение $42x = 87$ в $\mathbb{Z}_{123}$.

2.16. Решить уравнение $x^{11} + 3x^4 + 4 = 0$ в $\mathbb{Z}_{420}$.

2.17. Доказать, что система сравнений

$$\left.\begin{aligned} x &= a_1 \pmod{m_1}, \\ x &= a_2 \pmod{m_2}, \end{aligned}\right\}$$

имеет решение тогда и только тогда, когда (m_1, m_2) делит $a_1 - a_2$, и это решение единственно на множестве $\mathbb{Z}_{\text{НОК}(m_1,m_2)}$.

2.18. Решить систему сравнений

$$\left.\begin{aligned} x &= 2 \pmod{18}, \\ x &= 8 \pmod{24}. \end{aligned}\right\}$$

2.19. Каким числом нулей оканчивается число 1000! в десятичной записи?

2.20. Доказать, что $(5n + 3m, 13n + 8m) = (n, m)$ для всех натуральных m, n.

2.21. Числа a_k (см. (2.2)), для которых было получено равенство (2.3), называются *числами Фибоначчи*. Доказать, что

1) $a_{k+m} = a_{k-1}a_m + a_k a_{m+1}$,
2) $(a_k, a_{k+1}) = 1$,
3) $\sum_{k=0}^{n} a_{2k+1} = a_{2n+2}$,
4) $\sum_{k=0}^{n} a_{2k} = a_{2n+1} - 1$,
5) $(a_k, a_m) = a_{(k,m)}$.

2.22. Найти число подмножеств в множестве чисел от 1 до k, в которые не входят соседние числа. Как связан ответ с числами Фибоначчи?

2.23. Доказать, что

$$\varphi(nm) = \varphi(n)\varphi(m)\frac{(n,m)}{\varphi\big((n,m)\big)}.$$

Глава 3

Группы

В этой главе начинается изучение одного из важнейших объектов современной математики — множества с заданной на нем бинарной операцией, удовлетворяющей нескольким определенным свойствам. Простейшими примерами таких множеств являются целые числа с операцией сложения, действительные числа без нуля с операцией умножения, все взаимнооднозначные отображения конкретного множества в себя с операцией композиции. Каждый такой объект называется группой. Группы образуют фундамент, на котором построены все остальные алгебраические структуры. В силу этого многие свойства групп наследуются более сложными структурами, такими как кольца, поля и линейные пространства, при этом достаточно часто задачи, связанные с этими алгебраическими структурами, сводятся к задачам, решаемым в рамках теории групп, основы которой закладываются ниже.

3.1. Определения и примеры

1. Понятие группы. *Бинарной операцией* на множестве M называется произвольное отображение множества упорядоченных пар элементов из M в само множество M. Как правило, факт применения бинарной операции к элементам x и y обозначают, связывая эти элементы при помощи символа операции, например: $x + y$, $x \times y$, $x \circ y$ и т. д. Бинарными операциями на множестве натуральных чисел будут операции сложения и умножения, на множестве целых чисел — сложение, вычитание и умноже-

ние. На множестве всех подмножеств множества M бинарными операциями будут объединение и пересечение, а на множестве функций $f : M \to M$ — композиция функций. Бинарная операция на множестве M не обязана быть бинарной операцией на произвольном подмножестве N этого множества. Например, сложение не будет бинарной операцией на множестве нечетных целых чисел. Если же бинарная операция остается таковой на подмножестве N, то будем говорить, что N *замкнуто* относительно этой бинарной операции. Среди всевозможных пар (множество, бинарная операция) будем рассматривать специальные пары — группы.

Множество G с определенной на нем бинарной операцией $\circ$, называется *группой* $(G, \circ)$, если:

(1) операция $\circ$ ассоциативна, т. е. $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$ для всех g_1, g_2, g_3 из G;

(2) существует *единичный* (*нейтральный*) *элемент* $e \in G$ такой, что $g \circ e = e \circ g = g$ для любого $g \in G$;

(3) для каждого элемента $g \in G$ существует *обратный элемент* $g^{-1} \in G$ такой, что $g \circ g^{-1} = g^{-1} \circ g = e$.

Нетрудно видеть, что группами будут множество целых чисел, множество рациональных чисел, множество действительных чисел и множество комплексных чисел, в которых в качестве групповой операции используется обычное сложение, а нейтральным элементом является нуль. Натуральные числа группу с операцией сложения не образуют, так как для пары $(\mathbb{N}, +)$ справедливо свойство (1), но не выполняются свойства (2) и (3) из определения группы. Множества $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ и $\mathbb{C} \setminus \{0\}$ образуют группы с операцией умножения. Единичным элементом в этих трех группах будет единица. Целые числа без нуля группу с операцией умножения не образуют, так как ни одно целое число, кроме единицы и -1, не имеет обратного относительно умножения.

Часто групповую операцию называют либо сложением, которое обозначают знаком «+», либо умножением, для которого используются знаки «×» или «·». В первом случае говорят об аддитивной форме записи группы, во втором — о мультипликатив-

ной форме. При использовании мультипликативной формы знак умножения часто опускают, так же как это делают при умножении чисел. Далее, как правило, будем использовать мультипликативную форму. При использовании аддитивной формы единичный элемент будем называть *нулевым*. Группа G называется *конечной*, если она состоит из конечного числа элементов. Это число называется *порядком* группы G и обозначается $|G|$.

Пример 3.1. Множество $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ образует группу с операцией сложения по модулю m. Нулевым (нейтральным) элементом в этой группе будет 0, а $m-k$ будет обратным элементом для k. □

Обозначим через $\mathbb{Z}_m^*$ множество натуральных чисел, не превосходящих m и взаимно простых с m. Например, $\mathbb{Z}_6^* = \{1, 5\}$, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, $\mathbb{Z}_{2^n}^* = \{1, 3, 5, \ldots, 2^n - 1\}$.

Пример 3.2. При простом p множество $\mathbb{Z}_p^*$ образует группу с операцией умножения по модулю p. Действительно, из равенства $ab = 0 \pmod p$ следует делимость ab на p, откуда в свою очередь в силу леммы 2.2 и простоты p следует делимость на p хотя бы одного из чисел a, b, что очевидно невозможно, так как $1 \leqslant a, b \leqslant p-1$. Таким образом, $ab \neq 0 \pmod p$, и, следовательно, множество $\mathbb{Z}_p^*$ замкнуто относительно умножения по модулю p. Очевидно, что 1 будет единичным элементом, а существование обратного для каждого элемента в $\mathbb{Z}_p^*$ следует из простоты p и теоремы 2.9 об обратимости по простому модулю. Аналогичным образом можно показать, что группой является и множество $\mathbb{Z}_m^*$ с операцией умножения по модулю m при составном m. □

Группа G называется *абелевой* (или коммутативной), если для любых элементов g_1 и g_2 из G справедливо равенство $g_1 g_2 = g_2 g_1$. Все упомянутые до сих пор группы абелевы.

Пример 3.3. Важным примером неабелевой группы является множество взаимно однозначных отображений произвольного множества M на себя с операцией композиции. Ранее было показано, что композиция ассоциативна (теорема 1.1). Замкнутость рассматриваемого множества отображений очевидна, так

как композиция двух биективных отображений снова будет биективным отображением. Единичным элементом в группе является тождественное преобразование, а существование обратных элементов следует непосредственно из биективности отображений. Если множество M состоит из конечного числа элементов, например из n, то группа взаимно однозначных отображений множества M на себя называется *симметрической группой* S_n *порядка* n, или группой подстановок на n элементах, а ее элементы называются *подстановками*. Если элементы множества M обозначить числами $1, 2, \ldots, n$, то подстановку, отображающую 1 в i_1, 2 в i_2 и т. д., можно представить в виде таблицы из двух строк, в первой строке которой находятся числа от 1 до n, а во второй их образы:

$$\begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n-1 & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_{n-1} & i_n \end{pmatrix}.$$

Для вычисления произведения двух подстановок надо найти композицию отображений. Например, в произведении подстановок $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ правая подстановка отображает 1 в 2, левая 2 в 1, и, следовательно, произведение оставляет 1 на месте. Определив аналогично образы для 2, 3 и 4, находим, что

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Перемножив эти подстановки в обратном порядке, видим, что

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Таким образом, группа S_4 не является абелевой. □

Конечную группу $G = \{g_1, g_2, \ldots, g_n\}$ можно задать при помощи таблицы умножения, в которой на пересечении i-й строки и j-го столбца стоит элемент, равный произведению $g_i g_j$ элементов g_i и g_j. Такая таблица называется *таблицей Кэли*, по имени английского математика XIX в. Артура Кэли, который первым в 1854 г. ввел в математику современное определение группы. До Кэли рассматривали только группы подстановок.

Пример 3.4. Для групп $\mathbb{Z}_4$ и $\mathbb{Z}_5^*$ таблицы Кэли выглядят следующим образом:

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

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

В приведенных выше таблицах Кэли групп $\mathbb{Z}_4$ и $\mathbb{Z}_5^*$ каждая линия (строка или столбец) состоит из различных элементов. Покажем, что подобное свойство справедливо для таблицы Кэли произвольной группы. Если в таблице какой-либо группы $G = \{g_1, g_2, \ldots, g_n\}$ в j-м столбце k-й и i-й элементы равны, то $g_k g_j = g_i g_j$. Умножив правую и левую части этого равенства справа на g_j^{-1}, придем к противоречию $g_k = g_i$. $\square$

Нетрудно заметить, что в каждой из рассмотренных выше групп есть ровно один единичный элемент, и любой элемент каждой группы имеет ровно один обратный. Покажем, что эти два свойства справедливы для любой группы.

Теорема 3.1. *В группе существует ровно один единичный элемент, и у каждого элемента существует ровно один обратный элемент.*

Доказательство. Допустим, что в некоторой группе G есть два единичных элемента e и e'. Тогда из свойств единичного элемента следует, что

$$e = e \cdot e' = e' \cdot e = e'.$$

Таким образом, $e = e'$.

Теперь допустим, что у элемента g есть два обратных элемента g_1 и g_2. Тогда из свойств обратного элемента следует, что

$$g_1 = g_1 \cdot e = g_1 \cdot (g \cdot g_2) = (g_1 \cdot g) \cdot g_2 = e \cdot g_2 = g_2.$$

Следовательно, $g_1 = g_2$. Теорема доказана.

Воспользуемся доказанной теоремой для нахождения обратного элемента произведения нескольких элементов группы. Так как

$$(g_1g_2)(g_2^{-1}g_1^{-1}) = g_1(g_2g_2^{-1})g_1^{-1} = g_1g_1^{-1} = e,$$

то единственным обратным элементом произведения g_1g_2 является произведение $g_2^{-1}g_1^{-1}$ обратных элементов сомножителей, взятых в обратном порядке. Нетрудно видеть, что аналогичная формула

$$(g_1g_2\cdots g_k)^{-1} = g_k^{-1}\cdots g_2^{-1}g_1^{-1}$$

справедлива для любого числа сомножителей.

2. Подгруппы. Подмножество H группы G называется *подгруппой* этой группы, если H является группой относительно операции группы G.

Пусть H — подгруппа группы G. Будем говорить, что элемент a сравним с элементом b по модулю подгруппы H

$$a = b \pmod{H},$$

если $ab^{-1} \in H$. Так как $(ab^{-1})^{-1} = ba^{-1} \in H$, то и элемент b сравним с a по модулю подгруппы H, т. е. из сравнения $a = b \pmod{H}$ следует сравнение $b = a \pmod{H}$. Поэтому можно говорить, что a и b сравнимы по модулю подгруппы H.

Пример 3.5. Множество целых чисел образует подгруппу в группе рациональных чисел с операцией сложения. Нетрудно видеть, что рациональные x и y сравнимы по модулю подгруппы целых чисел, если равны их дробные части. В свою очередь рациональные числа образуют подгруппу в группе действительных чисел с операцией сложения, и два действительных числа сравнимы по модулю подгруппы рациональных чисел, если их разность — рациональное число. □

Пример 3.6. Для любого целого m в группе целых чисел с операцией сложения подгруппой будет множество $m\mathbb{Z}$, состоящее из всех целых кратных m. Теперь покажем, что в $\mathbb{Z}$ нет подгрупп, отличных от подгрупп вида $m\mathbb{Z}$. Пусть H — подгруппа в $\mathbb{Z}$. Положим $m = \min(x - y)$, где минимум берется по всем парам целых чисел из H, в которых $x > y$. Так как $m \in H$,

то и все кратные m числа также лежат в H. Допустим, что в H найдется n, которое не делится на m. Тогда $n = km + r$, где $0 < r < m$. Но в этом случае $r = n - km < m$ также принадлежит H, что невозможно в силу выбора m. Следовательно, $H = m\mathbb{Z}$.□

Теорема 3.2. *Пусть G — группа, H и K — ее подгруппы. Тогда $H \cap K$ будет подгруппой группы G.*

Доказательство. Очевидно, что единичный элемент принадлежит множеству $H \cap K$. Поэтому для доказательства теоремы достаточно показать, что $H \cap K$ замкнуто относительно групповой операции и что для любого g из $H \cap K$ его обратный элемент также лежит в $H \cap K$. Пусть $g_1 \in H \cap K$ и $g_2 \in H \cap K$, тогда $g_1 g_2 \in H$ и $g_1 g_2 \in K$ и, следовательно, $g_1 g_2 \in H \cap K$. Таким образом, множество $H \cap K$ замкнуто относительно операции группы G. Если $g \in H \cap K$, то $g^{-1} \in H$ и $g^{-1} \in K$ и, следовательно, $g^{-1} \in H \cap K$. Теорема доказана.

Пример 3.7. В группе целых чисел пересечение подгрупп $6\mathbb{Z}$ и $4\mathbb{Z}$ состоит из всех целых, делящихся на 6 и 4. Следовательно, $6\mathbb{Z} \bigcap 4\mathbb{Z} = 12\mathbb{Z}$. Нетрудно видеть, что в общем случае для любых целых m и n справедливо равенство $m\mathbb{Z} \bigcap n\mathbb{Z} = \text{НОК}(m, n)\mathbb{Z}$. □

Для группы G и ее подгрупп H и K определим произведение

$$HK = \{x \in G \mid x = hk, \text{ где } h \in H, k \in K\}$$

этих подгрупп. Имеет место следующая теорема.

Теорема 3.3. *Пусть G — группа, H и K — ее подгруппы. Множество HK будет подгруппой группы G тогда и только тогда, когда $HK = KH$.*

Доказательство. Покажем достаточность условия $HK = KH$. Из этого условия следует, что для любых $k \in K$ и $h \in H$ найдутся такие $k' \in K$ и $h' \in H$, что $hk = k'h'$. Тогда

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2'k_1')k_2 = (h_1h_2')(k_1'k_2),$$

т. е. множество HK замкнуто относительно групповой операции. Аналогичным образом из условия $HK = KH$ следует существование обратного элемента $h'k'$ для произвольного hk:

$$e = (hk)(hk)^{-1} = (hk)(k^{-1}h^{-1}) = (hk)(h'k').$$

Следовательно, HK — группа.

Теперь установим необходимость условия $HK = KH$. Пусть HK — подгруппа в G. Тогда для произвольного произведения $h'k'$ элементов из H и K в HK лежит его обратный элемент hk. Поэтому

$$h'k' = ((h'k')^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1}.$$

Следовательно, $HK = KH$. Теорема доказана.

Так как в абелевой группе $hk = kh$ для любых ее элементов h и k, то из теоремы 3.3 вытекает следующее простое утверждение.

Следствие 3.1. *Пусть G — абелева группа, H и K — ее подгруппы. Тогда HK — подгруппа группы G.*

Пример 3.8. Нетрудно видеть, что в силу теоремы 2.2 при любых целых m и n произведением подгрупп $m\mathbb{Z}$ и $n\mathbb{Z}$ в группе $\mathbb{Z}$ будет подгруппа НОД$(m, n)\mathbb{Z}$. □

3. Полугруппы и моноиды. Множество G с определенной на нем ассоциативной бинарной операцией называется *полугруппой*.

Множество G с определенной на нем ассоциативной бинарной операцией называется *полугруппой с единицей* (или моноидом), если в нем существует единичный элемент.

Пример 3.9. Множество целых чисел $\mathbb{Z}$ с операцией умножения образует моноид, а множество $2\mathbb{Z}$ с той же операцией — лишь полугруппу. □

3.2. Группа подстановок

Напомним (см. пример 3.3), что множество взаимно однозначных отображений n-элементного множества $\{1, 2, \ldots, n\}$ на себя с операцией композиции называется симметрической группой S_n, ее элементы называются подстановками, и каждая подстановка π представляется в виде

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n-1 & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_{n-1} & i_n \end{pmatrix}, \qquad (3.1)$$

где $i_k = \pi(k)$ — образ элемента k. В (3.1) первая строка состоит из упорядоченных аргументов отображения π, а вторая — из их образов. Если аргументы подстановки π не упорядочивать, то ее можно представить $n!$ различными способами вида

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_k & \dots & i_{n-1} & i_n \\ j_1 & j_2 & \dots & j_k & \dots & j_{n-1} & j_n \end{pmatrix}, \tag{3.2}$$

где $j_k = \pi(i_k)$. Подстановка π из S_n называется *циклом* длины m, если найдутся такие $i_1, \dots, i_m$, что

$$\pi(i_1) = i_2,\ \pi(i_2) = i_3,\ \dots,\ \pi(i_{m-1}) = i_m,\ \pi(i_m) = i_1,$$
$$\pi(j) = j \text{ для всех } j \notin \{i_1, \dots, i_m\}.$$

Цикл будем представлять строкой $(i_1 \cdots i_k \cdots i_m)$, в которой каждый элемент является образом предыдущего, а первый элемент — образом последнего. Заметим, что для цикла длины m есть ровно m различных представлений. Например, цикл (12345) можно записать следующими способами:

$$(12345) = (23451) = (34512) = (45123) = (51234).$$

Циклы длины два называются *транспозициями*.

Пример 3.10. В группе S_3 все подстановки, кроме тождественной, являются циклами. Это три транспозиции (12), (13) и (23), и два цикла длины три (123) и (132). □

Циклы называются *непересекающимися* (или независимыми), если не пересекаются множества их элементов.

Пример 3.11. В S_3 все циклы пересекаются. В S_4 есть три пары непересекающихся транспозиций: (12) и (34), (13) и (24), и (14) и (23). В S_5 есть 15 пар непересекающихся транспозиций и 20 пар непересекающихся циклов, состоящих из транспозиции и цикла длины три. Так как три непересекающихся цикла неединичной длины содержат не менее шести различных элементов, то ни в S_4, ни в S_5 нет трех непересекающихся циклов. □

Пример 3.12. Рассмотрим произведение двух непересекающихся циклов. Так как перестановка столбцов в (3.2) не изменяет подстановку, то для любых непересекающихся циклов из равенств

$$
\begin{aligned}
&(i_1\, i_2\, \ldots\, i_k)(j_1\, j_2\, \ldots\, j_m) = \\
&\quad = \begin{pmatrix} i_1 & i_2 & \ldots & i_k & j_1 & j_2 & \ldots & j_m \\ i_2 & i_3 & \ldots & i_1 & j_1 & j_2 & \ldots & j_m \end{pmatrix} \begin{pmatrix} i_1 & i_2 & \ldots & i_k & j_1 & j_2 & \ldots & j_m \\ i_1 & i_2 & \ldots & i_k & j_2 & j_3 & \ldots & j_1 \end{pmatrix} = \\
&\quad = \begin{pmatrix} i_1 & i_2 & \ldots & i_k & j_1 & j_2 & \ldots & j_m \\ i_2 & i_3 & \ldots & i_1 & j_2 & j_3 & \ldots & j_1 \end{pmatrix} = \begin{pmatrix} j_1 & j_2 & \ldots & j_m & i_1 & i_2 & \ldots & i_k \\ j_2 & j_3 & \ldots & j_1 & i_2 & i_3 & \ldots & i_1 \end{pmatrix} = \\
&\quad = \begin{pmatrix} j_1 & j_2 & \ldots & j_m & i_1 & i_2 & \ldots & i_k \\ j_2 & j_3 & \ldots & j_1 & i_1 & i_2 & \ldots & i_k \end{pmatrix} \begin{pmatrix} j_1 & j_2 & \ldots & j_m & i_1 & i_2 & \ldots & i_k \\ j_1 & j_2 & \ldots & j_m & i_2 & i_3 & \ldots & i_1 \end{pmatrix} = \\
&\quad = (j_1\, j_2\, \ldots\, j_m)(i_1\, i_2\, \ldots\, i_k)
\end{aligned}
$$

следует, что эти циклы коммутируют. Более того, индукцией по числу сомножителей нетрудно показать, что произведение любого числа непересекающихся циклов не зависит от порядка сомножителей. □

Теорема 3.4. *Каждая нетождественная подстановка $\pi \in S_n$ представляется в виде произведения непересекающихся циклов, и притом единственным с точностью до порядка сомножителей образом.*

Доказательство. Так как подстановка π — взаимно однозначное отображение множества $\{1, 2, \ldots, n\}$ на себя, то для каждого элемента i этого множества найдется такое минимальное натуральное k_i, что $\pi^{k_i}(i) = i$. Воспользуемся этим свойством и разобъем множество $\{1, 2, \ldots, n\}$ на непересекающиеся упорядоченные наборы. Первый набор составим из элементов $1, \pi(1), \ldots, \pi^{k_1-1}(1)$. Если $k_1 < n$, то среди элементов, не попавших в первый набор, выберем минимальное i и второй набор составим из элементов $i, \pi(i), \ldots, \pi^{k_i-1}(i)$. Если $k_1 + k_i < n$, то построим третий набор и т. д. Допустим, что множество $\{1, 2, \ldots, n\}$ указанным способом разбито на непересекающиеся наборы $A_1, \ldots, A_s$, где $A_j = (i_j, \pi(i_j), \pi^2(i_j), \ldots, \pi^{k_{i_j}-1}(i_j))$.

Переместив в каждом наборе A_j первый элемент в конец, получим s новых наборов $A'_j = (\pi(i_j), \pi^2(i_j), \ldots, \pi^{k_{i_j}-1}(i_j), i_j)$, причем $A'_j = A_j$ тогда и только тогда, когда $k_j = 1$.

Так как i-й элемент $\pi^i(i_j)$ в A'_j является образом i-го элемента $\pi^{i-1}(i_j)$ из A_j, то столбцы в (3.1) можно упорядочить так, чтобы подстановка π выглядела следующим образом:

$$\begin{pmatrix} A_1 & A_2 & \ldots & A_j & \ldots & A_s \\ A'_1 & A'_2 & \ldots & A'_j & \ldots & A'_s \end{pmatrix}. \tag{3.3}$$

Теперь заметим, что возникшее в рассмотренном выше примере 3.12 равенство

$$(i_1\, i_2\, \ldots\, i_k)(j_1\, j_2\, \ldots\, j_m) = \begin{pmatrix} i_1 & i_2 & \ldots & i_k & j_1 & j_2 & \ldots & j_m \\ i_2 & i_3 & \ldots & i_1 & j_2 & j_3 & \ldots & j_1 \end{pmatrix}$$

легко обобщается на любое число непересекающихся сомножителей. Поэтому нетрудно видеть, что подстановка (3.3) является произведением непересекающихся циклов $(A_1)(A_2)\cdots(A_s)$. Единственность указанного представления следует из однозначности определения множеств A_j и A'_j. Теорема доказана.

Пример 3.13. Следуя доказательству теоремы 3.4, разложим подстановку в произведение непересекающихся циклов:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 3 & 1 & 7 & 5 & 8 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 3 & 5 & 7 & 8 & 6 \\ 2 & 4 & 1 & 3 & 7 & 8 & 6 & 5 \end{pmatrix} =$$
$$= (1\ 2\ 4)(3)(5\ 7\ 8\ 6) = (1\ 2\ 4)(5\ 7\ 8\ 6).$$

Записывая произведения циклов, часто пропускают циклы длины один, каждый из которых является тождественной подстановкой. Выше в последнем произведении так пропущен цикл (3). □

Теорема 3.5. *Каждая подстановка $\pi \in S_n$ представляется в виде произведения транспозиций.*

Доказательство. Из равенства

$$(1\,2\,3\,4\ldots k) = (1k)\cdots(14)(13)(12) \tag{3.4}$$

следует, что любой цикл разлагается в произведение транспозиций. А так как каждая подстановка представляется в виде произведения непересекающихся циклов, то очевидно, что ее можно представить и как произведение транспозиций. Теорема доказана.

Пример 3.14. Разложим в произведение транспозиций подстановку (1234)(12). Из равенства (3.4) легко следует, что

$$(1\,2\,3\,4)(12) = (14)(13)(12)(12) = (14)(13).$$

С другой стороны, (1234) = (2341), и поэтому

$$(1\,2\,3\,4)(12) = (2\,3\,4\,1)(12) = (21)(24)(23)(12).$$

Таким образом, представление подстановки в виде произведения транспозиций неоднозначно и разные представления могут состоять из разного числа транспозиций. □

Теорема 3.6. *Если подстановка $g \in S_n$ раскладывается двумя способами в произведение транспозиций*

$$\pi_1\pi_2\cdots\pi_k = g = \sigma_1\sigma_2\cdots\sigma_m, \tag{3.5}$$

то $k = m \pmod 2$. Величина $\operatorname{sgn} g = (-1)^k$ называется знаком подстановки g.

Доказательство. Пусть $i < j$ и $s < t$. Будем говорить, что транспозиция (ij) меньше транспозиции (st) (пишем $(ij) < (st)$), если $i < s$ или $i = s$ и $j < t$. Произведение транспозиций $\pi_1\pi_2\cdots\pi_k$ назовем упорядоченным, если $\pi_{r+1} < \pi_r$ для $r = 1, 2, \ldots, k-1$. Покажем, что любое произведение транспозиций можно перестроить в равное ему упорядоченное произведение. Сделаем это индукцией по числу сомножителей. В основание индукции положим произведения из двух сомножителей. У сомножителей могут совпадать минимальные элементы, максимальные элементы, максимальный элемент первого с минимальным элементом второго, транспозиции могут не пересекаться. Во всех этих случаях произведения можно упорядочить

следующим образом:

$$\begin{aligned}(12)(13) &= (23)(12), \quad (13)(23) = (23)(12),\\ (12)(23) &= (23)(13), \quad (12)(34) = (34)(12).\end{aligned} \tag{3.6}$$

Допустим, что любое произведение из k транспозиций можно упорядочить. Тогда в произвольном произведении $\pi_1\pi_2\cdots\pi_k\pi_{k+1}$ упорядочим k левых транспозиций. Если в преобразованном произведении $\pi'_1\pi'_2\cdots\pi'_k\pi_{k+1}$ транспозиции $\pi'_k\pi_{k+1}$ упорядочены ($\pi'_k > \pi_{k+1}$ или $\pi'_k = \pi_{k+1}$), то упорядочено и все произведение. Если нет, то упорядочиваем пару $\pi'_k\pi_{k+1}$ при помощи подходящего равенства из (3.6) и получаем новое произведение $\pi'_1\pi'_2\cdots\pi'_{k+1}$, правая транспозиция π'_{k+1} которого меньше правой транспозиции π_{k+1} исходного произведения. Если произведение $\pi'_1\pi'_2\cdots\pi'_{k+1}$ не упорядочено, то повторяем выполненные действия до тех пор, пока это возможно. Так как в каждом новом произведении правая транспозиция меньше правой транспозиции в предыдущем, то после конечного числа повторений выполнить очередное преобразование будет невозможно, т. е. произведение станет упорядоченным.

Теперь допустим, что для подстановки g из S_n справедливы равенства (3.5). Тогда

$$e = \pi_1\pi_2\cdots\pi_k\sigma_m^{-1}\cdots\sigma_2^{-1}\sigma_1^{-1}. \tag{3.7}$$

Упорядочим произведение в правой части (3.7) и удалим из него пары стоящих рядом одинаковых транспозиций. Очевидно, что четность числа транспозиций r в новом произведении $\pi'_1\pi'_2\cdots\pi'_r$ совпадает с четностью $k+m$. Пусть s — минимальный элемент, встречающийся в транспозициях нового произведения. В этом произведении выберем самую левую транспозицию с элементом s — пусть это будет (st), где $t > s$. Тогда транспозиции справа от (st) не содержат элемент t, а транспозиции слева от (st) не содержат элемент s. Поэтому все произведение отображает t в s, т. е. не может быть тождественным. Возникшее противоречие исчезает, если $r = 0$. Таким образом, $k + m = 0 \pmod 2$, и, следовательно, $k = m \pmod 2$. Теорема доказана.

Подстановка π называется *четной*, если $\operatorname{sgn}\pi = 1$, и *нечетной*, если $\operatorname{sgn}\pi = -1$. Очевидно, что тождественная подстановка является четной подстановкой. Кроме того, нетрудно показать, что

$$\operatorname{sgn}(\pi)\operatorname{sgn}(\pi') = \operatorname{sgn}(\pi\pi')$$

для любых подстановок π и π'. Из последнего равенства и четности тождественной подстановки следует, что $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$ для любой подстановки π. Таким образом, четные подстановки образуют в S_n подгруппу. Такая подгруппа называется *знакопеременной* группой A_n порядка n. Покажем, что A_n состоит из $n!/2$ элементов.

Пусть $\pi_1, \ldots, \pi_s$ — все четные подстановки в S_n, $\sigma_1, \ldots, \sigma_t$ — все нечетные подстановки в этой группе. Тогда подстановки $(12)\pi_1, \ldots, (12)\pi_s$ будут нечетными, и, следовательно, $t \geqslant s$. С другой стороны, четными будут подстановки $(12)\sigma_1, \ldots, (12)\sigma_t$, следовательно, $s \geqslant t$. Объединяя получившиеся неравенства, видим, что $s = t$, т. е. четные подстановки составляют ровно половину из $n!$ подстановок в S_n.

Пусть T — подмножество группы G, $\langle T\rangle$ — множество всех элементов из G, представимых в виде произведений элементов из T и обратных к ним. Множество $\langle T\rangle$ называется *системой образующих* (порождающих) элементов этой группы G, если $\langle T\rangle = G$.

Пример 3.15. $\mathbb{Z} = \langle 1\rangle$, $m\mathbb{Z} = \langle m\rangle$. □

Пример 3.16. Из теоремы 3.5 следует, что в S_n множество всех транспозиций является системой образующих. □

Пример 3.17. Множество всех циклов длины 3 является системой образующих в A_n при $n \geqslant 3$. Действительно, любое произведение четного числа транспозиций можно разбить на пары транспозиций так, что они имеют вид $(ij)(jk) = (ijk)$ или $(ij)(kl) = (ikj)(ikl)$. □

Подмножество T группы G называется *минимальной* системой образующих или *базисом* этой группы, если $G = \langle T\rangle$ и $G \neq \langle T'\rangle$ для любого собственного подмножества T' множе-

ства T. Можно легко убедиться, что минимальность системы T равносильна тому, что $x \notin \langle T \setminus \{x\}\rangle$ для всех $x \in T$.

Пример 3.18. Нетрудно видеть, что при $n \geqslant 3$ системы образующих из двух последних примеров не являются минимальными. Минимальную систему можно получить, если заметить, что $(ij) = (1i)(1j)(1i)$, откуда $S_n = \langle (1i) : i = 2, \dots, n\rangle$. Более того, $(23\dots n)(12)(23\dots n)^{-1} = (13)$, откуда по индукции следует, что $(1i) = (23\dots n)^{i-2}(12)(23\dots n)^{-(i-2)}$. Очевидно, что $(23\dots n)^{-1} = (23\dots n)^{n-2}$, $(12) \notin \langle (23\dots n)\rangle$ и $(23\dots n) \notin \langle (12)\rangle$. Таким образом, система $T = \{(12), (23\dots n)\}$ является минимальной порождающей S_n системой. □

Отметим, что минимальная система образующих группы G не обязательно имеет минимальную среди ее образующих систем мощность. Так, система $(12), (13), \dots, (1n)$ из предыдущего примера очевидно является минимальной в S_n (выбрасывание любой транспозиции делает ее неполной), однако число образующих системы $(12), (23\dots n)$ меньше.

3.3. Смежные классы и фактор-группы

1. Смежные классы и теорема Лагранжа. Рассмотрим произвольную группу $G = \{g_1, \dots, g_n, \dots\}$ и ее подгруппу $H = \{h_1, \dots, h_m, \dots\}$. *Левым смежным классом* группы G по подгруппе H называется множество $gH = \{gh_1, \dots, gh_m, \dots\}$, где g — фиксированный элемент группы G. *Правым смежным классом* группы G по подгруппе H называется множество $Hg = \{h_1g, \dots, h_mg, \dots\}$. Множество левых (правых) смежных классов называется левым (правым) *фактор-множеством* G/H группы G по подгруппе H. В абелевых группах левые и правые смежные классы совпадают, поэтому в случае абелевой группы говорят просто о смежных классах и фактор-множествах.

Пример 3.19. Смежными классами группы $\mathbb{Z}$ по подгруппе $3\mathbb{Z}$ будут: подгруппа $3\mathbb{Z}$; множество $1 + 3\mathbb{Z}$, состоящее из всех целых, сравнимых с единицей по $\pmod 3$; множество $2 + 3\mathbb{Z}$, состоящее из всех целых, сравнимых с двойкой по $\pmod 3$. Легко видеть, что фактор-множество $\mathbb{Z}/3\mathbb{Z}$ будет множеством $\mathbb{Z}_3$. □

Теорема 3.7. *Два левых (правых) смежных класса группы G по подгруппе H либо совпадают, либо не пересекаются.*

Доказательство. Покажем, что если два левых смежных класса группы G по подгруппе H имеют хотя бы один общий элемент, то тогда эти классы совпадают.

Допустим $g \in g_1H$ и $g \in g_2H$. Тогда в H найдутся такие элементы h_i и h_j, что $g = g_1h_i = g_2h_j$. Поэтому $g_1 = g_2h_jh_i^{-1}$ и, следовательно, для любого $g_1h_k \in g_1H$ справедливо равенство $g_1h_k = g_2(h_jh_i^{-1}h_k)$. Так как $h_jh_i^{-1}h_k \in H$, то $g_1h_k \in g_2H$, и, следовательно, $g_1H \subseteq g_2H$. Включение $g_2H \subseteq g_1H$ доказывается аналогично. Таким образом, $g_1H = g_2H$. Доказательство для правых смежных классов аналогично. Теорема доказана.

Теорема 3.8 (Лагранж)**.** *Порядок конечной группы делится на порядок любой ее подгруппы.*

Доказательство. Пусть G — конечная группа, H — подгруппа группы G. Каждый элемент группы G принадлежит некоторому левому смежному классу G по подгруппе H, причем каждый смежный класс состоит ровно из $|H|$ элементов. Поэтому $|G|$ равно числу смежных классов, умноженному на $|H|$. Теорема доказана.

Пусть g — произвольный элемент группы G. Произведение k элементов g называется k-й степенью g^k этого элемента. Из ассоциативности умножения легко следует, что

$$g^k g^l = g^l g^k = g^{l+k} \tag{3.8}$$

для любых натуральных l и k. Так как $(g^k)^{-1} = (g^{-1})^k$, то для упрощения вычислений положим $g^{-k} = (g^{-1})^k$.

Если G — конечная группа порядка n, то среди степеней $g, g^2, \ldots, g^n$ найдется такая степень k, что $g^k = e$. Допустим, что такой степени нет. Тогда среди n степеней g будет не более $n-1$ различных элементов G, и, следовательно, по крайней мере две степени, например g^s и g^t, где $s > t$, будут равны. Умножая левую и правую части равенства $g^t g^{s-t} = g^t$ слева на g^{-t}, приходим к равенству $g^{s-t} = e$, которое противоречит сделанному

предположению. Следовательно, одна из степеней $g, g^2, \ldots, g^n$ равна единичному элементу. Пусть k — минимальное натуральное, для которого $g^k = e$. Такое k называется *порядком* элемента g и обозначается обычно $|g|$, $o(g)$ или $\mathrm{ord}(g)$.

Множество $\{e, g, \ldots, g^{k-1}\}$ замкнуто относительно умножения, которое (см. (3.8)) коммутативно на нем. Это множество содержит единичный элемент e, и каждый его элемент $g^i \neq e$ имеет обратный g^{k-i}. Следовательно $\{e, g, \ldots, g^{k-1}\}$ является абелевой группой и подгруппой в G. Такая группа называется конечной циклической группой, порожденной элементом g, и обозначается $\langle g \rangle$. Элемент g называется *порождающим элементом* группы $\langle g \rangle$. В общем случае группа G называется *циклической* с порождающим элементом g и обозначается $\langle g \rangle$ или $\langle g \rangle_k$ для конечной группы порядка k, если каждый ее элемент является целой степенью g.

Пример 3.20. Легко видеть, что циклическими группами будут $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ и $\mathbb{Z}_5^* = \langle 2 \rangle = \langle 3 \rangle$. □

Из теоремы Лагранжа следует, что в конечной группе порядок каждого элемента делит порядок группы. Если n — порядок группы, k — порядок элемента g и $n = km$, то $g^n = (g^k)^m = e$. Таким образом, в конечной группе любой элемент в степени, равной порядку группы, равен единичному элементу. Простым следствием этого факта являются доказанные в главе 2 теорема Эйлера и малая теорема Ферма.

Пример 3.21. Рассмотрим группу G простого порядка p. Каждый неединичный элемент g этой группы порождает в ней циклическую подгруппу $\langle g \rangle$. Порядок этой подгруппы должен делить p, а так как p — простое, то порядок $\langle g \rangle$ равен p, т. е. $\langle g \rangle = G$. Следовательно, любая группа простого порядка будет циклической. □

Лемма 3.1. *Пусть в группе G с единичным элементом e выполнено равенство $g^k = e$ для некоторых $g \in G$ и $k \in \mathbb{N}$. Тогда число k нацело делится на порядок элемента g.*

Доказательство. Пусть $n = |g|$, тогда $g^n = e$ и $g^m \neq e$ для любого натурального $m < n$. Разделив k на n с остатком,

получим $k = nq + r$, где $0 \leqslant r < n$. Отсюда $g^k = g^{nq+r} = (g^n)^q g^r = g^r$. Так как по условию $g^k = e$, то и $g^r = e$. Но $r < n$, поэтому $r = 0$, иначе получим противоречие с определением порядка элемента g. Лемма доказана.

2. Фактор-группы. Пусть G — абелева группа, H — ее подгруппа. На фактор-множестве G/H введем операцию умножения, полагая, что

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Прежде всего отметим, что для любых h_i, h_j из H

$$\begin{aligned}((g_1h_i)H)((g_2h_j)H) &= (g_1h_i)(g_2h_j)H = \\ &= (g_1g_2)(h_ih_jH) = (g_1g_2)H,\end{aligned} \tag{3.9}$$

т. е. результат умножения не зависит от выбора представителей смежных классов. Следовательно, операция умножения определена корректно. Также заметим, что из ассоциативности групповой операции легко следует и ассоциативность введенного умножения. Далее, так как для любого $g \in G$

$$\begin{aligned}gHH &= HgH = gH, \\ gHg^{-1}H &= g^{-1}HgH = H,\end{aligned} \tag{3.10}$$

то фактор-множество G/H с такой операцией умножения будет группой, в которой единичным элементом является подгруппа H, а смежный класс $g^{-1}H$ является обратным к смежному классу gH. Оказывается, что для справедливости (3.9) и (3.10) группа G не обязательно должна быть абелевой. Нетрудно видеть, что для этого достаточно, чтобы подгруппа H была перестановочна с каждым элементом группы, т. е. $gH = Hg$ для любого $g \in G$[1)]. Такая подгруппа H называется *нормальной подгруппой* (обозначается $H \triangleleft G$), а фактор-множество по этой подгруппе — *фактор-группой* G/H группы G по нормальной подгруппе H. Таким образом, справедлива следующая теорема.

[1)] Равенство $gH = Hg$ эквивалентно равенству $gHg^{-1} = H$.

Теорема 3.9. *Фактор-множество группы G по нормальной подгруппе H является группой.*

Пример 3.22. Так как $\operatorname{sgn}\pi = \operatorname{sgn}\pi^{-1}$ для любой подстановки π из S_n, то множество $\pi A_n \pi^{-1}$ состоит только из четных подстановок. Следовательно, $\pi A_n \pi^{-1} = A_n$, т. е. A_n — нормальная подгруппа в S_n. Фактор-группа S_n/A_n состоит из двух смежных классов: подгруппы A_n и множества нечетных подстановок. □

Пример 3.23. В конце XIX в. американским изобретателем игр и головоломок Сэмюэлем Лойдом была предложена следующая задача, называемая игрой в «пятнашки». Квадратная коробочка разделена на 16 полей. В полях установлены 15 квадратных фишек, занумерованных числами от 1 до 15. Одно поле коробочки остается свободным. Ниже на рисунке слева изображено начальное расположение фишек в коробочке. За один ход можно передвинуть на свободное поле любую из соседних с ним фишек (например, на левом рисунке это фишки 12 и 15). Требуется получить из начального расположения фишек их расстановку, изображенную на рисунке справа.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Головоломка быстро стала очень популярной не в последнюю очередь благодаря обещанному за ее решение крупному вознаграждению. Обогатиться, однако, было невозможно: задача не имеет решения. Действительно, сопоставив свободному полю число 16, каждое расположение фишек можно представить некоторой перестановкой π из группы S_{16}. Перемещение фишки на свободное место означает перестановку ее номера с числом 16,

т. е. каждый ход является транспозицией и меняет $\operatorname{sgn}\pi$. Поэтому перестановки, получаемые четным числом ходов, должны иметь одинаковый знак. Чтобы пустое поле вернулось на прежнее место, число 16 должно переместиться вверх столько же раз, сколько и вниз, а влево столько же раз, сколько и вправо, т. е. количество ходов должно быть четным. Однако подстановки слева и справа на рисунке имеют разные знаки. □

3.4. Изоморфизмы групп

1. Изоморфизмы. Пусть G и H — группы с операциями $*$ и $\circ$ соответственно. Взаимно однозначное отображение $f : G \to H$ называется *изоморфизмом*, если равенство

$$f(a * b) = f(a) \circ f(b) \tag{3.11}$$

справедливо для любых элементов a и b из G. Про отображение, удовлетворяющее равенству (3.11), говорят, что оно сохраняет групповую операцию, а группы G и H, для которых существует изоморфизм, называются *изоморфными*. Для обозначения изоморфизма групп используется символ $\cong$.

Пример 3.24. Покажем, что $\mathbb{Z}_4 \cong \mathbb{Z}_5^*$. Обе группы являются циклическими: в $\mathbb{Z}_4$ порождающим элементом является 1, а в $\mathbb{Z}_5^*$ — 2. Изоморфизм f группы $\mathbb{Z}_4$ в группу $\mathbb{Z}_5^*$ определим, отобразив порождающий элемент в порождающий, т. е. положим $f(1) = 2$, а значения на оставшихся элементах группы $\mathbb{Z}_4$ зададим, используя свойство сохранения групповой операции:

$$\begin{aligned} f(2) &= f(1+1) = f(1) \cdot f(1) = 2 \cdot 2 = 4 \pmod 5, \\ f(3) &= f(2+1) = f(2) \cdot f(1) = 4 \cdot 2 = 3 \pmod 5, \\ f(0) &= f(3+1) = f(3) \cdot f(1) = 3 \cdot 2 = 1 \pmod 5. \end{aligned}$$

Непосредственной проверкой легко убедиться в том, что f действительно является изоморфизмом. □

Пример 3.25. Покажем, что $\mathbb{Z} \cong 2\mathbb{Z}$. Для этого зададим отображение $\mathbb{Z}$ в $2\mathbb{Z}$ по правилу $f(k) = 2k$. Очевидно, что такое отображение взаимно однозначно и, кроме того, сохраняет

групповую операцию, так как равенства

$$f(k+l) = 2(k+l) = 2k + 2l = f(k) + f(l)$$

справедливы для любых целых k и l. Следовательно, f является изоморфизмом. □

Пример 3.26. Рассмотрим функцию $f(x) = 2^x$, отображающую взаимнооднозначно множество $\mathbb{R}$ действительных чисел на множество $\mathbb{R}_+$ положительных действительных чисел. Легко видеть, что

$$f(x_1 + x_2) = 2^{x_1+x_2} = 2^{x_1} \cdot 2^{x_2} = f(x_1) \cdot f(x_2)$$

для любых действительных x_1 и x_2. Так как множество $\mathbb{R}$ с операцией сложения и множество $\mathbb{R}_+$ с операцией умножения являются группами, то функция $f(x) = 2^x$ устанавливает изоморфизм этих групп. □

Изоморфизмы, построенные в рассмотренных выше примерах, обладают несколькими общими свойствами. Так, например, нетрудно заметить, что каждый изоморфизм отображает единичный элемент одной группы в единичный элемент другой группы. Также нетрудно видеть, что в каждом из трех примеров выполняется равенство $f(g^{-1}) = f(g)^{-1}$, и кроме того, обратное отображение каждого из рассмотренных изоморфизмов само является изоморфизмом. Например в третьем примере такое обратное отображение задается функцией $\log_2 y$, которая отображает $\mathbb{R}_+$ в $\mathbb{R}$ и для которой равенство

$$\log_2(y_1 \cdot y_2) = \log_2 y_1 + \log_2 y_2$$

справедливо при всех положительных y_1, y_2. Это обстоятельство не является случайным. Покажем, что каждым из трех указанных свойств обладает любой изоморфизм $f : G \to H$ произвольных изоморфных групп G и H.

Теорема 3.10. *Пусть G и H — изоморфные группы с единичными элементами e и e'. Любой изоморфизм $f : G \to H$ обладает следующими свойствами:*

1) $f(e) = e'$;
2) $f(g^{-1}) = f(g)^{-1}$ *для каждого* $g \in G$;
3) *обратное отображение является изоморфизмом.*

Доказательство. Покажем, что изоморфизм f отображает единичный элемент e группы G в единичный элемент e' группы H, т. е. $f(e) = e'$. Действительно, из свойств единичного элемента следует, что $e * g = g * e = e$ для любого g из G, а из взаимной однозначности f следует, что для любого h из H в G найдется такой элемент g, что $h = f(g)$. Поэтому для любого h (и его прообраза g)

$$\begin{aligned} h \circ f(e) = f(g) \circ f(e) = f(g * e) = \\ = f(g) = f(e * g) = f(e) \circ f(g) = f(e) \circ h. \end{aligned}$$

Следовательно, $f(e)$ — единичный элемент.

Теперь покажем, что изоморфизм f отображает g^{-1} в элемент, являющийся обратным элементом к $f(g)$, т. е. $f(g^{-1}) = = f(g)^{-1}$. Для этого воспользуемся установленным выше свойством $f(e) = e'$ и определением обратного элемента:

$$\begin{aligned} f(g) \circ f(g^{-1}) = f(g * g^{-1}) = f(e) = \\ = e' = f(e) = f(g^{-1} * g) = f(g^{-1}) \circ f(g). \end{aligned} \tag{3.12}$$

Наконец покажем, что обратное отображение $f^{-1} : H \to G$ также является изоморфизмом. Так как f — взаимно однозначное отображение, то оно, очевидно, имеет обратное, которое также взаимно однозначно. Поэтому нам достаточно доказать справедливость равенства $f^{-1}(h_1 \circ h_2) = f^{-1}(h_1) * f^{-1}(h_2)$ для произвольных h_1 и h_2 из группы H. Пусть $g_1 = f^{-1}(h_1)$ и $g_2 = f^{-1}(h_2)$. Тогда

$$\begin{aligned} f^{-1}(h_1 \circ h_2) = f^{-1}(f(g_1) \circ f(g_2)) = \\ = f^{-1}(f(g_1 * g_2)) = g_1 * g_2 = f^{-1}(h_1) * f^{-1}(h_2). \end{aligned}$$

Таким образом, справедливость всех трех свойств установлена. Теорема доказана.

Среди всевозможных изоморфизмов различных групп отметим изоморфизмы группы на себя, называемые *автоморфизмами*. В частности, автоморфизмами группы G являются *сопряжения* $h_a : g \to aga^{-1}$ относительно произвольного элемента a группы. Нетрудно показать, что автоморфизмы произвольной группы G образуют группу относительно операции композиции. Такая группа называется *группой автоморфизмов* группы G и обозначается $\mathrm{Aut}(G)$. Все сопряжения группы G образуют подгруппу в группе $\mathrm{Aut}(G)$.

2. Теорема Кэли. Ранее было отмечено, что до середины XIX в. в математике рассматривались только группы подстановок. Распространив понятие группы на произвольное множество с бинарной операцией, Артур Кэли показал, что каждая конечная группа изоморфна некоторой подгруппе симметрической группы подходящего порядка.

Теорема 3.11 (Кэли)**.** *Любая конечная группа порядка n изоморфна некоторой подгруппе S_n.*

Доказательство. Рассмотрим множество взаимно однозначных отображений $H = \{f_a\}$ группы G в себя, действующих по правилу $f_a : g \to ag$. Такие отображения называются *сдвигами*. Рассматриваемое множество является группой относительно операции суперпозиции, так как суперпозиция ассоциативна, а из равенства

$$(f_a \circ f_b)(g) = f_a(f_b(g)) \tag{3.13}$$

легко следует, что для любого элемента a группы G и единичного элемента e этой группы

$$f_e \circ f_a = f_a \circ f_e = f_a, \quad f_a \circ f_{a^{-1}} = f_{a^{-1}} \circ f_a = f_e,$$

т. е. в группе H элемент f_e будет единичным элементом, а $f_{a^{-1}}$ — обратным к f_a.

Элементы группы H являются подстановками на n-элементном множестве элементов группы G. Следовательно, H — подгруппа группы S_n. Отображение $\varphi : a \to f_a$ определяет изоморфизм групп G и H, так как оно биективно и равенство

$$\varphi(ab) = f_{ab} = f_a \circ f_b = \varphi(a) \circ \varphi(b)$$

легко следует из (3.13). Теорема доказана.

Пример 3.27. Найдем в группе S_4 подгруппу, изоморфную группе $(\mathbb{Z}_5^*, \times)$. Отображения $f_a : g \to ag$, использованные в доказательстве теоремы 3.11, действуют на множестве $\mathbb{Z}_5^*$ следующим образом:

$$f_1 : \begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}1\\2\\3\\4\end{matrix}, \qquad f_2 : \begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}2\\4\\1\\3\end{matrix}, \qquad f_3 : \begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}3\\1\\4\\2\end{matrix}, \qquad f_4 : \begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}4\\3\\2\\1\end{matrix}.$$

Поэтому подгруппа группы S_4, изоморфная группе $(\mathbb{Z}_5^*, \times)$, состоит из тождественной подстановки f_1, двух циклов длины четыре $f_2 = (1243)$ и $f_3 = (1342)$ и произведения транспозиций $f_4 = (14)(23)$. □

3. Циклические группы. Среди всех конечных групп наиболее просто устроены циклические группы, в каждой из которых все элементы являются степенями одного порождающего элемента. Поэтому все конечные циклические группы одного порядка устроены одинаково. Точнее, справедлива следующая теорема.

Теорема 3.12. *Любая конечная циклическая группа порядка n изоморфна группе $(\mathbb{Z}_n, +)$.*

Доказательство. Пусть конечная циклическая группа порядка n порождается элементом g. Рассмотрим отображение $f : g^k \to k$. Тогда для любых элементов $g_1 = g^k$ и $g_2 = g^m$ группы G имеем:

$$f(g_1 g_2) = f(g^k g^m) = f(g^{k+m}) = [k+m]_n = \\ = [k]_n + [m]_n = f(g^k) + f(g^m) = f(g_1) + f(g_2).$$

Таким образом, f — изоморфизм. Теорема доказана.

Теорема 3.13. *Пусть m делит n. В любой конечной циклической группе порядка n существует единственная подгруппа порядка m. Все подгруппы циклической группы циклические.*

Доказательство. В силу теоремы 3.12 достаточно показать, что доказываемое свойство справедливо для $(\mathbb{Z}_n, +)$. Прежде всего отметим, что по крайней мере одна подгруппа порядка m существует. Эта подгруппа образована числами, делящимися на $d = n/m$: $0, d, \ldots, (m-1)d$, порождается элементом d и поэтому является циклической. Отсутствие других подгрупп следует из того, что по следствию теоремы Лагранжа для каждого элемента a такой подгруппы должно выполняться равенство $m \cdot a = 0 \pmod{n}$, т. е. каждый ее элемент должен делиться на d. В $\mathbb{Z}_n$ таких чисел ровно m, и все они принадлежат первой подгруппе. Теорема доказана.

Теорема 3.14. *В любой циклической группе порядка n существует ровно $\varphi(n)$ порождающих элементов.*

Доказательство. Снова воспользуемся теоремой 3.12. Покажем, что в $(\mathbb{Z}_n, +)$ порождающими элементами будут все числа, взаимно простые с n, и только они. В силу теоремы 2.2 взаимная простота чисел n и a эквивалентна существованию таких целых k и m, что $kn + ma = 1$. Из этого равенства следует, что

$$m \cdot a = 1 \pmod{n}. \tag{3.14}$$

Поэтому единица — порождающий элемент в $(\mathbb{Z}_n, +)$ — является суммой m элементов a. Следовательно, a — порождающий элемент в $(\mathbb{Z}_n, +)$. С другой стороны, если a — порождающий элемент, то единица должна быть суммой некоторого числа элементов a, т. е. должно существовать целое m, для которого справедливо (3.14), откуда в свою очередь следует взаимная простота n и a. Теорема доказана.

Простым следствием двух предыдущих теорем является следующее утверждение.

Теорема 3.15. *Пусть m делит n. В любой конечной циклической группе порядка n существует ровно $\varphi(m)$ элементов порядка m.*

Доказательство. Каждый элемент порядка m порождает подгруппу такого же порядка. Так как в циклической группе

есть только одна подгруппа порядка m, то все элементы порядка m принадлежат одной и той же подгруппе и являются ее порождающими элементами. Теорема доказана.

Теорема 3.16. *В циклической группе порядка n с порождающим элементом g для порядка элемента g^k справедливо равенство*

$$|g^k| = \frac{n}{(n,k)}.$$

Доказательство. Согласно теореме 3.12, достаточно доказать формулу в циклической группе $(\mathbb{Z}_n, +)$ с порождающим вычетом 1. Порядком произвольного вычета $k \in \mathbb{Z}_n$ является наименьшее натуральное решение x сравнения $x \cdot k = 0 \pmod{n}$. Все его целочисленные решения составляют множество $\{in/(n,k) : i \in \mathbb{Z}\}$ (см. доказательство теоремы 2.8). Наименьшим положительным из них будет $x = n/(n,k)$. Теорема доказана.

Из теоремы 3.16 легко извлекается следующее полезное утверждение.

Следствие 3.2. *Элемент g^k является порождающим элементом циклической группы $\langle g \rangle_n$ тогда и только тогда, когда $(n,k) = 1$.*

Пример 3.28. Если g — элемент некоторой (не обязательно циклической или коммутативной) группы, имеющий порядок 18, то порядок элемента g^{15} равен $\frac{18}{(18,15)} = 6$. □

Пример 3.29. Рассмотрим уравнение $z^8 = g^{12}$ в циклической группе $G = \langle g \rangle_{20}$. Каждый элемент $z \in G$ имеет представление вида $z = g^x$ при некотором $x \in \mathbb{Z}_{20}$, откуда $z^8 = g^{8x} = g^{12}$. Последнее равенство равносильно сравнению $8x = 12 \pmod{20}$. В примере 2.5 были найдены все его решения $x = 4, 9, 14, 19$. Поэтому элементы g^4, g^9, g^{14}, g^{19} являются решениями исходного уравнения в группе G, и других решений в G у него нет. Аналогичным образом нетрудно установить, что уравнение $z^a = g^b$ в группе $\langle g \rangle_n$ либо не имеет решений, когда $(a,n) \nmid b$, либо имеет ровно (a,n) решений в противном случае. Отметим, что и этот пример основан на теоремах 2.8 и 3.12. □

4. Прямое произведение групп. *Внешним прямым произведением* $G_1 \times \cdots \times G_k$ групп $G_1, \ldots, G_k$ называется множество всех упорядоченных наборов $(g_1, \ldots, g_k)$ длины k, где $g_i \in G_i$, с определенной на этом множестве покомпонентной операцией умножения

$$(g_1, \ldots, g_k)(g'_1, \ldots, g'_k) = (g_1 g'_1, \ldots, g_k g'_k),$$

в которой умножение по i-й компоненте является умножением в G_i. Легко видеть, что такое умножение ассоциативно, множество $G_1 \times \cdots \times G_k$ замкнуто относительно этого умножения, содержит единичный элемент $e = (e_1, \ldots, e_k)$, составленный из единичных элементов групп $G_1, \ldots, G_k$, и для каждого набора $g = (g_1, \ldots, g_k)$ существует такой обратный набор $g^{-1} = (g_1^{-1}, \ldots, g_k^{-1})$, что $gg^{-1} = g^{-1}g = e$. Таким образом, внешнее прямое произведение групп само является группой.

Пример 3.30. Перечислим все подгруппы в прямом произведении $\mathbb{Z}_4 \times \mathbb{Z}_9$ групп $\mathbb{Z}_4$ и $\mathbb{Z}_9$. Группа $\mathbb{Z}_4 \times \mathbb{Z}_9$ состоит из 36 пар (a, b), где $a \in \mathbb{Z}_4$, $b \in \mathbb{Z}_9$, и поэтому порядки ее нетривиальных подгрупп содержатся среди чисел $2, 3, 4, 6, 9, 12, 18$. Покажем, что для каждого из этих чисел найдется единственная подгруппа соответствующего порядка. Так как групповыми операциями в $\mathbb{Z}_4$ и $\mathbb{Z}_9$ являются сложения по $\bmod 4$ и $\bmod 9$, то для $\mathbb{Z}_4 \times \mathbb{Z}_9$ будем использовать аддитивную форму записи. Пусть k — порядок элемента $(1, 1)$, тогда $k(1, 1) = (k, k) = (0, 0)$. Последнее равенство эквивалентно тому, что $k = 0 \pmod 4$ и $k = 0 \pmod 9$. Из китайской теоремы об остатках следует, что k кратно 36. Следовательно, $\mathbb{Z}_4 \times \mathbb{Z}_9$ — циклическая группа с порождающим элементом $(1, 1)$. Поэтому в силу теоремы 3.13 о циклических группах $\mathbb{Z}_4 \times \mathbb{Z}_9$ содержит ровно по одной подгруппе порядка $2, 3, 4, 6, 9, 12, 18$. Нетрудно видеть, что такими подгруппами будут $2\mathbb{Z}_4 \times \{0\}$, $\{0\} \times 3\mathbb{Z}_9$, $\mathbb{Z}_4 \times \{0\}$, $2\mathbb{Z}_4 \times 3\mathbb{Z}_9$, $\{0\} \times \mathbb{Z}_9$, $\mathbb{Z}_4 \times 3\mathbb{Z}_9$ и $2\mathbb{Z}_4 \times \mathbb{Z}_9$.

Заметим, что все приведенные выше рассуждения применимы и к группе $\mathbb{Z}_9 \times \mathbb{Z}_4$. Следовательно, $\mathbb{Z}_4 \times \mathbb{Z}_9 \cong \mathbb{Z}_9 \times \mathbb{Z}_4$. □

Некоторые свойства группы $\mathbb{Z}_4 \times \mathbb{Z}_9$ из рассмотренного примера справедливы для любых внешних прямых произведений

групп. Можно легко показать, что $G_1 \times G_2 \cong G_2 \times G_1$ для любых G_1 и G_2, и если H_i — подгруппа в G_i, то $H_1 \times H_2$ будет подгруппой в $G_1 \times G_2$.

Пример 3.31. Пусть p и q — различные простые, $A = \langle a \rangle$ и $B = \langle b \rangle$ — циклические группы порядков p и q. Покажем, что прямое произведение $A \times B$ также будет циклической группой. Повторяя рассуждения из предыдущего примера, найдем порядок k элемента (a, b). Так как $(a, b)^k = (a^k, b^k) = (e, e)$, то $k = 0 \pmod p$ и $k = 0 \pmod q$. Из китайской теоремы об остатках следует, что k кратно pq. Следовательно, $A \times B$ — циклическая группа порядка pq. □

Теорема 3.17. *Пусть $n = q_1 q_2 \cdots q_k$, где все q_i попарно взаимно простые. Тогда*

$$\mathbb{Z}_n \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}, \quad \mathbb{Z}_n^* \cong \mathbb{Z}_{q_1}^* \times \mathbb{Z}_{q_2}^* \times \cdots \times \mathbb{Z}_{q_k}^*.$$

Доказательство. Для каждого a из $\mathbb{Z}_n$ и каждого i из $\{1, 2, \ldots, k\}$ положим $a_i = a \pmod{q_i}$. Из китайской теоремы об остатках следует, что отображение $f(a) = (a_1, a_2, \ldots, a_k)$ из $\mathbb{Z}_n$ в $\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$ будет взаимно однозначным. Сравнения можно складывать, поэтому

$$\begin{aligned} f(a+b) &= (a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k) = \\ &= (a_1, a_2, \ldots, a_k) + (b_1, b_2, \ldots, b_k) = f(a) + f(b) \end{aligned}$$

для любых a и b из $\mathbb{Z}_n$. Таким образом, f — изоморфизм из группы $\mathbb{Z}_n$ в группу $\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$.

Далее заметим, что если a взаимно просто с n, то оно взаимно просто и с любым его делителем. Поэтому если $a \in \mathbb{Z}_n^*$, то $a_i \in \mathbb{Z}_{q_i}^*$. Верно и обратное, если все a_i взаимно просты с n, то и соответствующее им a из $\mathbb{Z}_n$ будет взаимно просто с n. Следовательно, если $a_i \in \mathbb{Z}_{q_i}^*$ при каждом i из $\{1, 2, \ldots, k\}$, то $a \in \mathbb{Z}_n$. Теперь из китайской теоремы об остатках следует, что отображение $f(a) = (a_1, a_2, \ldots, a_k)$ из $\mathbb{Z}_n^*$ в $\mathbb{Z}_{q_1}^* \times \mathbb{Z}_{q_2}^* \times \cdots \times \mathbb{Z}_{q_k}^*$ будет взаимно однозначным. Так как сравнения можно умножать, то

$$f(ab) = (a_1 b_1, a_2 b_2, \ldots, a_k b_k) =$$

$$= (a_1, a_2, \ldots, a_k)(b_1, b_2, \ldots, b_k) = f(a)f(b)$$

для любых a и b из $\mathbb{Z}_n^*$. Следовательно, f — изоморфизм из группы $\mathbb{Z}_n^*$ в группу $\mathbb{Z}_{q_1}^* \times \mathbb{Z}_{q_2}^* \times \cdots \times \mathbb{Z}_{q_k}^*$. Теорема доказана.

Лемма 3.2. *Пусть $g \in G$, $h \in H$. Тогда порядок элемента (g, h) в прямом произведении $G \times H$ групп G и H равен наименьшему общему кратному* $\mathrm{НОК}\big(|g|, |h|\big)$ *порядков элемента g и элемента h.*

Доказательство. Положим $n = |(g, h)|$ и $N = \mathrm{НОК}\big(|g|, |h|\big)$. Тогда $(g, h)^n = (g^n, h^n) = (e_G, e_H)$, и по лемме 3.1 имеем, что число n делится и на $|g|$, и на $|h|$. Следовательно, n делится на N.

С другой стороны, $(g, h)^N = (g^N, h^N) = (e_G, e_H)$ в силу делимости N на $|g|$ и $|h|$, откуда следует, что N делится на n. Поэтому $n = N$. Лемма доказана.

Следствие 3.3. *Пусть $g = (g_1, \ldots, g_k) \in G_1 \times \ldots \times G_k$, тогда*

$$|g| = \mathrm{НОК}\big(|g_1|, \ldots, |g_k|\big).$$

3.5. Гомоморфизмы групп

Пусть G и H — группы с операциями $*$ и $\circ$ соответственно. Отображение $f : G \to H$ называется *гомоморфизмом* группы G в группу H, если $f(a * b) = f(a) \circ f(b)$ для всех элементов a и b группы G. *Ядром гомоморфизма* f называется множество $\mathrm{Ker}\, f = \{g \in G \mid f(g) = e\}$. Нетрудно видеть, что всякий изоморфизм является гомоморфизмом, ядро которого состоит только из единичного элемента.

Пример 3.32. Отображение $f : \mathbb{Z} \to \mathbb{Z}_2$, определенное равенством $f(k) = [k]_2$, является гомоморфизмом с ядром $2\mathbb{Z}$. Действительно, равенство

$$f(k + m) = [k + m]_2 = [k]_2 + [m]_2 = f(k) + f(m)$$

справедливо для любых целых k и m, а каждое четное l отображается в нулевой элемент группы $\mathbb{Z}_2$: $f(l) = [l]_2 = [0]_2$. □

Теорема 3.18. *Пусть $f : G \to H$ — гомоморфизм группы G в группу H с ядром K. Тогда K — нормальная подгруппа в G.*

Доказательство. Покажем, что ядро K гомоморфизма f образует подгруппу в G. Для любых $k_1, k_2 \in K$ и единичного элемента e' группы H имеем

$$f(k_1k_2) = f(k_1) \cdot f(k_2) = e' \cdot e' = e',$$

т. е. $k_1k_2 \in K$ и ядро гомоморфизма замкнуто относительно групповой операции. Единичный элемент e группы G принадлежит ядру гомоморфизма, так как при $k \in K$

$$e' = f(k) = f(k \cdot e) = f(k) \cdot f(e) = e' \cdot f(e) = e'.$$

Для каждого k из K и его обратного k^{-1} справедливы равенства

$$e' = f(kk^{-1}) = f(k) \cdot f(k^{-1}) = e' \cdot f(k^{-1}) = f(k^{-1}).$$

Следовательно, $k^{-1} \in K$. Таким образом K — подгруппа группы G. Так как для каждого g из G

$$\begin{aligned} f(gKg^{-1}) &= f(g) \cdot f(K) \cdot f(g^{-1}) = \\ &= f(g) \cdot f(g^{-1}) = f(gg^{-1}) = f(e) = e', \end{aligned}$$

то K — нормальная подгруппа. Теорема доказана.

Укажем два простых, но важных свойства гомоморфизмов. Первое состоит в том, что для любого гомоморфизма f группы G в группу H и каждого элемента $g \in G$ имеет место равенство $f(g^{-1}) = f(g)^{-1}$. Доказательство этого факта дословно повторяет рассуждения, приведенные в доказательстве теоремы 3.10 (последовательность равенств (3.12)) о свойствах изоморфизмов. Второе свойство заключается в том, что если $f(g_1) = f(g_2)$, то g_1 и g_2 принадлежат одному и тому же смежному классу группы G по ядру гомоморфизма f. Действительно, так как

$$f(g_2^{-1}g_1) = f(g_2^{-1})f(g_1) = f(g_2)^{-1}f(g_1) = f(g_1)^{-1}f(g_1) = e',$$

где e' — единичный элемент группы H, то $g_2^{-1}g_1 \in \operatorname{Ker} f$ или $g_1 \in g_2\operatorname{Ker} f$. Очевидно, что верно и обратное свойство: если элементы g_1 и g_2 принадлежат одному и тому же смежному классу группы G по ядру гомоморфизма f, то $f(g_1) = f(g_2)$. Из принадлежности g_1 и g_2 одному и тому же смежному классу следует существование такого элемента ядра h, что $g_1 = g_2h$. Тогда

$$f(g_1) = f(g_2h) = f(g_2)f(h) = f(g_2)e' = f(g_2).$$

Легко видеть, что образ гомоморфизма $\operatorname{Im} f = \{f(g) \mid g \in G\}$ является подгруппой в H (в отличие от ядра не обязательно нормальной).

Пример 3.33. Выясним, какие группы могут быть образами гомоморфизмов группы S_3. Из теоремы 3.18 следует, что необходимым условием существования гомоморфизма является наличие в S_3 нормальной подгруппы, являющейся ядром гомоморфизма. Будем рассматривать гомоморфизмы, ядра которых не совпадают с самой группой S_3 и состоят более чем из одного элемента. Нетрудно видеть, что в группе S_3 есть три подгруппы $H_1 = \{e, (12)\}$, $H_2 = \{e, (13)\}$ и $H_3 = \{e, (23)\}$ порядка два, и одна подгруппа порядка три — знакопеременная группа $A_3 = \{e, (123), (132)\}$, являющаяся нормальной подгруппой в S_3.

Ни одна из подгрупп порядка два не является нормальной. Убедиться в этом можно прямой проверкой, которую выполним для подгруппы H_1. Действительно, так как $(132)(12)(123) = = (13)$, то $(132)H_1(132)^{-1} \neq H_1$. Аналогичные неравенства можно получить и для подгрупп H_2 и H_3. Таким образом, нет ни одного гомоморфизма группы S_3, ядром которого является подгруппа порядка два.

Теперь построим гомоморфизм f с ядром A_3. Для этого воспользуемся равенством $\operatorname{sgn}(\pi)\operatorname{sgn}(\pi') = \operatorname{sgn}(\pi\pi')$, справедливым для любых подстановок π и π'. Очевидно, что отображение $f : \pi \to \operatorname{sgn}(\pi)$ сохраняет групповую операцию и, следовательно, является гомоморфизмом S_3 в группу $G = \{1, -1\}$ с операцией умножения. Также легко видеть, что f отображает четные подстановки в 1 — единичный элемент G, т. е. A_3 — ядро f. Так как A_3 единственная нетривиальная нормальная подгруппа

в S_3, то любой нетривиальный гомоморфный образ группы S_3 изоморфен группе G. $\square$

В следующей теореме рассмотренный выше пример обобщается на произвольную группу и любую ее нормальную подгруппу.

Теорема 3.19. *Пусть K — нормальная подгруппа в G. Тогда существует гомоморфизм $f : G \to G/K$, ядром которого является подгруппа K.*

Доказательство. Рассмотрим отображение $f : g \to gK$, ставящее в соответствие элементу g смежный класс, которому он принадлежит. Так как подгруппа K нормальна в G, то

$$f(g_1g_2) = g_1g_2K = g_1g_2KK = g_1Kg_2K = f(g_1)f(g_2)$$

для любых g_1 и g_2 из G. Следовательно, f сохраняет групповую операцию и поэтому является гомоморфизмом. Теорема доказана.

Теорема 3.20. *Пусть $f : G \to H$ — гомоморфизм группы G в группу H с ядром K. Тогда $G/K \cong \mathrm{Im}f$.*

Доказательство. Рассмотрим отображение $\varphi : gK \to f(g)$, ставящее в соответствие смежному классу gK образ элемента g при гомоморфизме f. Из свойства сохранения операции гомоморфизмом следует, что

$$\begin{aligned}\varphi(g_1K \cdot g_2K) = \varphi(g_1g_2K) = f(g_1g_2) = \\ = f(g_1)f(g_2) = \varphi(g_1K)\varphi(g_2K)\end{aligned}$$

для любых g_1 и g_2 из G. Поэтому φ сохраняет групповую операцию и, таким образом, является гомоморфизмом.

Теперь покажем, что φ — биективное отображение. Так как $\mathrm{Im}\varphi = \mathrm{Im}f$ в силу определения φ, то оно сюръективно. Покажем инъективность φ. Действительно, если найдутся g_1 и g_2 такие, что $\varphi(g_1K) = \varphi(g_2K)$, то

$$f(g_1) = \varphi(g_1K) = \varphi(g_2K) = f(g_2),$$

и, следовательно, элементы g_1, g_2 принадлежат одному и тому же смежному классу группы G по K, т. е. $g_1K = g_2K$. Таким образом, $\varphi(g_1K) \neq \varphi(g_2K)$, если $g_1K \neq g_2K$. Теорема доказана.

Задачи

3.1. Определить, образует ли группу множество с указанной операцией, и если оно является группой, то найти ее порядок и выяснить, абелева она или нет, циклическая она или нет; если циклическая, то найти число ее образующих:

1) все взаимнооднозначные отображения $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ относительно операции композиции отображений;

2) все булевы функции двух аргументов относительно операции $f \vee g$;

3) все булевы функции двух аргументов относительно операции $f \oplus g$;

4) все необратимые по умножению вычеты из $\mathbb{Z}_{1024}$ относительно сложения вычетов;

5) все необратимые по умножению вычеты из $\mathbb{Z}_{216}$ относительно сложения вычетов.

3.2. Пусть x, y — элементы некоммутативной группы G. Доказать, что порядки элементов xy и yx совпадают.

3.3. Доказать, что если $xy = yx$ и $\langle x\rangle \cap \langle y\rangle = e$, то порядок элемента xy равен наименьшему общему кратному порядков элементов x и y. Показать на примере, что каждого из условий $xy = yx$ и $\langle x\rangle \cap \langle y\rangle = e$ в отдельности недостаточно.

3.4. Пусть $\alpha = (01)(23)(456)(769)$, $\beta = (0423)(196758)$. Найти знаки и порядки подстановок α, β. Определить, коммутируют ли они. Вычислить α^{-1} и β^{2014}. Решить уравнение $\alpha x = \beta$. Решить уравнение $x^2 = \alpha$.

3.5. (Эквивалентное определение знака подстановки) Пусть π — некоторая подстановка из S_n. Доказать, что ее знак удовлетворяет равенству

$$\operatorname{sgn}(\pi) = \prod_{1 \leqslant i < j \leqslant n} \frac{j - i}{\pi(j) - \pi(i)}.$$

3.6. Найти при $n = 3, 4, \ldots, 12$ максимальный порядок элемента в группе S_n и число элементов максимального порядка.

3.7. Найти при $n = 3, 4, \ldots, 12$ максимальный порядок элемента в группе A_n и число элементов максимального порядка.

3.8. Пусть $n \geqslant 3$. Доказать, что $A_n = \langle T \rangle$, где T — множество, состоящее из циклов:

1) $(123), (124), \ldots, (12n)$,

2) $(123), (234), \ldots, (n-2, n-1, n)$.

Являются ли эти множества минимальными порождающими группу A_n системами?

3.9. Пусть число $n \in \mathbb{N}$ является произведением двух различных простых чисел. Показать, что сравнение $x^{1+\varphi(n)} = x \pmod{n}$ справедливо для всех вычетов $x \in \mathbb{Z}_n$, а не только для обратимых по модулю n (следствие теоремы Эйлера, на котором основана корректность системы RSA).

3.10. Пусть G — группа порядка n, H — ее подгруппа, и элемент $g \in G$ таков, что $g^k \in H$, причем $(k, n) = 1$. Доказать, что $g \in H$.

3.11. Перечислить все неизоморфные группы порядка 4.

3.12. Существует ли в группе A_n минимальная образующая система из двух элементов?

3.13. Найти $\sum_{m|n} \varphi(m)$.

3.14. Пусть G — циклическая группа порядка 600 с образующим элементом a.

1) Найти порядок элемента $a^{70} \in G$ и число элементов из G порядков $16, 20, 100$;

2) найти число подрупп группы G;

3) решить уравнения $x^{70} = 1$ и $x^{85} = a^{100}$ в группе G, определить, множество решений какого из них образует подгруппу в G;

4) построить изоморфизм между группой G и группой $H = (\mathbb{Z}_{600}, +)$.

3.15. Показать, что автоморфизмы произвольной группы образуют группу относительно операции композиции.

3.16. Показать, что сдвиги группы G образуют подгруппу в группе $\mathrm{Aut}(G)$.

3.17. Показать, что сопряжения группы G образуют подгруппу в группе $\mathrm{Aut}(G)$.

3.18. Найти группы $\mathrm{Aut}(\mathbb{Z})$, $\mathrm{Aut}(\mathbb{Z}_5)$, $\mathrm{Aut}(\mathbb{Z}_6)$.

3.19. Найти число автоморфизмов конечной циклической группы порядка n.

3.20. Показать, что при изоморфизме групп образ любого элемента имеет тот же порядок, что и прообраз, подгруппы переходят в подгруппы (того же порядка), а системы образующих — в системы образующих.

3.21. Пусть G — конечная группа, H и K — ее подгруппы. Показать, что $|H \cap K| \cdot |HK| = |H| \cdot |K|$.

3.22. Пусть $\varphi : G \to H$ — гомоморфизм. Доказать, что порядок x делится на порядок $\varphi(x)$ для всех $x \in G$.

3.23. Показать, что композиция гомоморфизмов будет гомоморфизмом.

3.24. Пусть $\varphi : G \to H$ и $\psi : H \to K$ — гомоморфизмы группы G в группу H и группы H в группу K. Показать, что

$$\operatorname{Ker}(\psi \circ \varphi)/\operatorname{Ker}\varphi \cong \operatorname{Ker}\psi.$$

3.25. Построить все возможные гомоморфизмы $f : \langle a\rangle_{60} \to \langle b\rangle_{40}$. Указать среди них все такие, что $|\operatorname{Ker} f| = 6$.

3.26. Найти все гомоморфизмы $f : \langle a\rangle_{10} \to S_4$ и $g : S_4 \to \langle a\rangle_{10}$.

3.27. Найти все нормальные подгруппы H в группе подстановок S_4, построить фактор-группы S_4/H.

3.28. На примере группы A_4 показать, что нормальная подгруппа H_1 нормальной подгруппы H_2 группы G не обязательно является нормальной в G.

3.29. Выяснить, для каких групп G отображение $f : G \to G$, определенное правилом: 1) $f(x) = x^2$; 2) $f(x) = x^{-1}$, является гомоморфизмом. При каком условии оно является изоморфизмом?

3.30. Пусть $H_1 \triangleleft G$, $H_2 \triangleleft G$ и $H_1 \cap H_2 = e$. Доказать справедливость равенства $x_1x_2 = x_2x_1$ для всех $x_i \in H_i$.

Глава 4

Кольца

В этой главе вводятся алгебраические структуры с двумя операциями — кольца и поля. Кольцом называется множество с двумя заданными на нем бинарными операциями, удовлетворяющими некоторым определенным свойствам и называемыми сложением и умножением. Поле представляет собой важный частный случай кольца, в котором операция умножения подчиняется дополнительным требованиям. Примерами кольца и поля являются, соответственно, целые и действительные числа с операциями сложения и умножения. Ниже рассматриваются основные свойства произвольных колец. После этого подробно изучаются кольца многочленов. Эти кольца играют важную роль при подробном изучении полей в восьмой главе.

4.1. Кольца и поля

Множество $\mathbb{K}$ с определенными на нем бинарными операциями сложения $+$ и умножения $\cdot$ называется *кольцом*, если:

(1) множество $\mathbb{K}$ с операцией $+$ является абелевой группой;

(2) множество $\mathbb{K}$ с операцией $\cdot$ является полугруппой;

(3) для всех a, b и c из множества $\mathbb{K}$ выполняются законы дистрибутивности:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Группа $(\mathbb{K}, +)$ называется аддитивной группой кольца, а ее единичный элемент — нулевым элементом кольца. Нулевой элемент

кольца обозначается символом 0. Полугруппа $(\mathbb{K}, \cdot)$ называется мультипликативной полугруппой кольца.

Кольцо $\mathbb{K}$ называется *кольцом с единицей*, если существует такой элемент 1, что $a \cdot 1 = 1 \cdot a = a$ для любого $a \in \mathbb{K}$. Кольцо называется конечным, если оно состоит из конечного числа элементов.

Пример 4.1. Множество целых чисел с обычными операциями сложения и умножения является кольцом с единицей, а множество $2\mathbb{Z}$ четных целых чисел с такими же операциями — кольцом без единицы. Конечным кольцом с единицей будет множество $\mathbb{Z}_m$ с операциями сложения и умножения по модулю m, а конечным кольцом без единицы — множество четных элементов из $\mathbb{Z}_{2m}$ с операциями сложения и умножения по модулю $2m$. □

Пример 4.2. Обозначим через $\mathbb{Z}[\sqrt{2}]$ все числа, которые можно получить из целых чисел и $\sqrt{2}$ при помощи сложений и умножений. Это множество состоит из чисел вида $a + b\sqrt{2}$, где a, b — целые, и с обычными операциями сложения и умножения является кольцом с единицей. □

Подмножество L кольца $\mathbb{K}$ называется *подкольцом*, если оно замкнуто относительно сложения и умножения, т. е.

$$\text{если } a, b \in L, \text{ то } a + b \in L \text{ и } ab \in L.$$

Пример 4.3. Множество $2\mathbb{Z}$ является подкольцом в $\mathbb{Z}$, $2\mathbb{Z}_{2m}$ — подкольцом в $\mathbb{Z}_{2m}$, $\mathbb{Z}$ — подкольцом в $\mathbb{Z}[\sqrt{2}]$ и кольце $\mathbb{R}$ действительных чисел. □

Пример 4.4. Из примера 3.6 на с. 57 легко следует, что в кольце целых чисел все подкольца имеют вид $m\mathbb{Z}$. □

Кольцо называется *коммутативным*, если операция умножения коммутативна. Все кольца в рассмотренных выше примерах коммутативные. Пример некоммутативного кольца можно найти на с. 150.

Выполняя действия над элементами произвольных колец, будем использовать ряд соглашений и свойств, позволяющих упростить выкладки и имеющих очевидные аналогии в кольце целых чисел. Обратный элемент по сложению к элементу a

будем обозначать $-a$. Сумму элементов a и $-b$ будем обозначать как $a-b$, введя по сути дополнительную операцию вычитания.

Теорема 4.1. *Пусть $\mathbb{K}$ — кольцо. Для любых его элементов a и b*

$$a0 = 0a = 0, \quad a(-b) = (-a)b = -(ab), \quad (-a)(-b) = ab.$$

Если $\mathbb{K}$ — кольцо с единицей, то

$$(-1)a = -a, \quad (-1)(-1) = 1.$$

Доказательство. Так как $a + 0 = a$ для любого a, то

$$a^2 + 0 = a^2 = a(a+0) = a^2 + a0 \Rightarrow a0 = 0.$$

Аналогичным образом устанавливается равенство $0a = 0$. Далее, используя предыдущее свойство, видим, что

$$0 = a0 = a(b-b) = ab + a(-b) \Rightarrow -ab = a(-b). \tag{4.1}$$

Так как $-(-b) = b$, то, подставляя это равенство в (4.1), приходим к равенству $(-a)(-b) = ab$. В свою очередь из этого равенства легко следует, что $(-1)a = -a$ и $(-1)(-1) = 1$. Теорема доказана.

Кольцо $\mathbb{K}$ называется *кольцом без делителей нуля* или *целостным*, если из равенства $ab = 0$ следует либо $a = 0$, либо $b = 0$. Ненулевые элементы $a, b \in \mathbb{K}$ называются *делителями нуля* в кольце $\mathbb{K}$, если $ab = 0$. Например, кольцо $\mathbb{Z}_6$ содержит делители нуля (это вычеты $2, 3, 4$), а в кольце $\mathbb{Z}_5$ их нет.

Лемма 4.1. *В кольце без делителей нуля выполняется закон сокращения*: *если $c \neq 0$ и $ac = bc$, то $a = b$.*

Доказательство. Из равенства $ac = bc$ следует, что $(a-b)c = 0$, и так как $c \neq 0$ и в кольце нет делителей нуля, то $a - b = 0$, т. е. $a = b$. Лемма доказана.

Пусть $\mathbb{K}$ — кольцо с единицей 1. Тогда элемент $x \in \mathbb{K}$ называется *обратимым* (по умножению), если в $\mathbb{K}$ найдется такой элемент x^{-1}, что $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Элемент x^{-1} в этом случае называется (мультипликативным) *обратным* к x. Из теоремы 4.1 очевидно, что нулевой элемент 0 любого кольца необратим, так как $0 \neq 1$.

В отличие от обратимости по сложению, не каждый элемент кольца обратим по умножению. Если $a, b \in \mathbb{K}$ — делители нуля, т. е. $ab = 0$, то ни a, ни b не имеют обратного в $\mathbb{K}$: из предположения $1 = a^{-1}a$ домножением обеих частей этого равенства на b немедленно получаем $b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$.

Рассмотрим множество всех обратимых по умножению элементов кольца $\mathbb{K}$:

$$\mathbb{K}^* = \{x \in \mathbb{K} : \exists\, x^{-1} \in \mathbb{K}\}.$$

Например, $(\mathbb{Z}_6)^* = \{1, 5\}$. Обозначение $\mathbb{K}^*$ полностью согласуется с введенным ранее на с. 54 обозначением $\mathbb{Z}_m^*$ для множества взаимно простых с m вычетов и обобщает его на произвольное кольцо: по теореме 2.9 вычет $[x]$ кольца $\mathbb{Z}_m$ имеет обратный вычет тогда и только тогда, когда представляющее его целое число x взаимно просто с m.

Лемма 4.2. *Пусть $\mathbb{K}$ — произвольное кольцо с единицей, не обязательно коммутативное. Тогда множество $\mathbb{K}^*$ является группой относительно умножения кольца $\mathbb{K}$.*

Доказательство. Ясно, что единица 1 кольца $\mathbb{K}$ лежит в множестве $\mathbb{K}^*$, так как $1^{-1} = 1$ в силу равенства $1 \cdot 1 = 1$, и является его единичным элементом. Ассоциативность умножения следует из аксиом кольца.

Далее, множество $\mathbb{K}^*$ замкнуто относительно умножения. Действительно, пусть элементы x и y обратимы, тогда

$$(xy) \cdot (y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = 1, \quad (y^{-1}x^{-1}) \cdot (xy) = 1,$$

а это означает, что произведение xy также обратимо и $(xy)^{-1} = y^{-1}x^{-1}$.

Наконец, в силу тождества $(x^{-1})^{-1} = x$ обратный к элементу $x \in \mathbb{K}^*$ элемент также лежит в $\mathbb{K}^*$. Лемма доказана.

Группа $\mathbb{K}^*$ называется *мультипликативной группой* кольца $\mathbb{K}$. Например, $\mathbb{Z}^* = \{1, -1\}$.

Коммутативное кольцо с единицей $1 \neq 0$, в котором каждый ненулевой элемент обратим по умножению, называется *полем*. Множество ненулевых элементов поля замкнуто относительно операции умножения, так как если произведение двух ненулевых элементов a и b равно нулю, то цепочка равенств

$$a = a(bb^{-1}) = (ab)b^{-1} = 0b^{-1} = 0$$

немедленно приводит к противоречию с условием $a \neq 0$. Таким образом, в поле нет делителей нуля, а все его ненулевые элементы образуют коммутативную группу, которая называется *мультипликативной группой поля*. Воспользуемся этим свойством и дадим новое, независимое от понятия кольца определение поля.

Множество $\mathbb{F}$ с определенными на нем бинарными операциями сложения $+$ и умножения $\cdot$ называется *полем*, если:

(1) множество $\mathbb{F}$ с операцией сложения является абелевой группой $(\mathbb{F}, +)$ и эта группа называется *аддитивной группой поля*, а ее нулевой элемент 0 — *нулевым элементом* (нулем) поля;

(2) множество $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ с операцией умножения является абелевой группой $(\mathbb{F}^*, \cdot)$ и эта группа называется *мультипликативной группой поля*, а ее единичный элемент — *единичным элементом* (единицей) поля;

(3) для всех a, b и c из множества $\mathbb{F}$ выполняются законы дистрибутивности:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Нетрудно видеть, что полями являются множества $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ с обычными для этих множеств операциями сложения и умножения. Поле называется *конечным*, если оно состоит из конечного числа элементов.

К основным арифметическим операциям в поле относятся сложение, вычитание, умножение и деление. Под вычитанием $a - b$, как и в кольце, понимается сложение с аддитивным обратным, т. е. $a + (-b)$. Аналогично деление $\frac{a}{b}$ определяется как умножение на мультипликативный обратный элемент $a \cdot b^{-1}$, где $b \neq 0$.

Пример 4.5. Обозначим через $\mathbb{Q}[\sqrt{2}]$ все числа, которые можно получить из рациональных чисел и $\sqrt{2}$ при помощи сложений и умножений. Это множество состоит из чисел вида $a + b\sqrt{2}$, где a, b — рациональные. Так как

$$(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \cdot \sqrt{2}\right) = 1,$$

то каждый ненулевой элемент в $\mathbb{Q}[\sqrt{2}]$ имеет обратный по умножению и поэтому $\mathbb{Q}[\sqrt{2}]$ с обычными операциями сложения и умножения является полем. Про поле $\mathbb{Q}[\sqrt{2}]$ говорят, что оно получено расширением поля рациональных чисел при помощи корня уравнения $x^2 - 2 = 0$. Аналогичным образом можно сказать, что поле комплексных чисел является расширением $\mathbb{R}[i]$ поля действительных чисел при помощи корня уравнения $x^2 + 1 = 0$. □

Теорема 4.2. *Конечное коммутативное кольцо без делителей нуля является полем.*

Доказательство. Для доказательства теоремы достаточно показать, что в конечном коммутативном кольце без делителей нуля есть единичный элемент и каждый ненулевой элемент такого кольца имеет обратный по умножению.

Пусть a — произвольный ненулевой элемент коммутативного кольца без делителей нуля, $a_1, a_2, \ldots, a_n$ — все его ненулевые элементы. Если среди произведений $aa_1, aa_2, \ldots, aa_n$ найдутся два равных, например $aa_i = aa_j$, то равенства

$$a(a_i - a_j) = aa_i - aa_j = 0$$

приводят к противоречию с отсутствием делителей нуля. Поэтому все произведения aa_i различны и среди этих произведений найдется произведение aa_j, равное a. В этом случае из равенства $aa_j = aa_ja_j$ следует, что $a(a_j - a_j^2) = 0$ или $a_j = a_j^2$. Отсюда для любого ненулевого a_i справедливы равенства

$$a_ia_j = a_ia_j^2 = (a_ia_j)a_j = a_j(a_ia_j),$$

а так как все произведения $a_j a_1, a_j a_2, \ldots, a_j a_n$ различны, то a_j является единичным элементом.

Теперь заметим, что среди произведений $aa_1, aa_2, \ldots, aa_n$ найдется произведение aa_k, равное единичному элементу. Следовательно, $a^{-1} = a_k$, т. е. каждый ненулевой элемент коммутативного кольца без делителей нуля имеет обратный по умножению. Теорема доказана.

Следствие 4.1. *При простом p множество $\mathbb{Z}_p$ с операциями сложения и умножения по модулю p является полем*[1)].

4.2. Морфизмы колец

1. Изоморфизм колец. Пусть $(\mathbb{K}, +, \cdot)$ и $(\mathbb{K}', \oplus, \odot)$ — кольца. Взаимно однозначное отображение $f : \mathbb{K} \to \mathbb{K}'$ называется *изоморфизмом*, если оно сохраняет операции, т. е. равенства

$$f(a+b) = f(a) \oplus f(b), \quad f(ab) = f(a) \odot f(b)$$

справедливы для любых a и b из $\mathbb{K}$. Для обозначения изоморфизма колец используется символ $\cong$.

Пример 4.6. Отображение $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, преобразующее $a + b\sqrt{2}$ в $a - b\sqrt{2}$, является изоморфизмом кольца $\mathbb{Z}[\sqrt{2}]$. □

Прямой суммой $\mathbb{K}_1 \otimes \cdots \otimes \mathbb{K}_m$ колец $\mathbb{K}_1, \ldots, \mathbb{K}_m$ называется множество всех упорядоченных наборов $(a_1, \ldots, a_m)$ длины m, где $a_i \in \mathbb{K}_i$, с определенными на этом множестве покомпонентными операциями умножения и сложения

$$(a_1, \ldots, a_m)(a'_1, \ldots, a'_m) = (a_1 a'_1, \ldots, a_m a'_m),$$
$$(a_1, \ldots, a_m) + (a'_1, \ldots, a'_m) = (a_1 + a'_1, \ldots, a_m + a'_m),$$

в которых умножение и сложение по i-й компоненте является умножением и сложением в $\mathbb{K}_i$. Такие операции на множестве

[1)] Отметим, что этот факт следует независимо от теоремы 4.2 также из расширенного алгоритма Евклида и результатов раздела 2.4.

$\mathbb{K}_1 \otimes \cdots \otimes \mathbb{K}_m$ ассоциативны, и для них справедливы законы дистрибутивности, а само множество является абелевой группой относительно операции сложения и полугруппой относительно операции умножения. Поэтому прямая сумма $\mathbb{K}_1 \otimes \cdots \otimes \mathbb{K}_m$ является кольцом с нулевым элементом $0 = (0, \ldots, 0)$, составленным из нулевых элементов колец $\mathbb{K}_1, \ldots, \mathbb{K}_m$. Если каждое кольцо $\mathbb{K}_i$ является кольцом с единицей, то и $\mathbb{K}_1 \otimes \cdots \otimes \mathbb{K}_m$ будет кольцом с единицей $(1, \ldots, 1)$, состоящей из единиц колец $\mathbb{K}_i$.

Пример 4.7. Прямая сумма $\mathbb{R} \otimes \mathbb{R}$ является коммутативным кольцом с единицей, но не является полем. □

Пример 4.8. Прямая сумма $\mathbb{Z}_n \otimes \mathbb{Z}_m$ является коммутативным кольцом с единицей. □

Следующее утверждение является очевидным следствием теоремы 3.17 и поэтому приводится без доказательства.

Теорема 4.3. *Пусть $n = q_1 q_2 \cdots q_k$, где все q_i попарно взаимно простые. Тогда*

$$\mathbb{Z}_n \cong \mathbb{Z}_{q_1} \otimes \mathbb{Z}_{q_2} \otimes \cdots \otimes \mathbb{Z}_{q_k}.$$

Как и теорему 2.11, теорему 4.3 часто называют китайской теоремой об остатках.

2. Гомоморфизм колец. Пусть $(\mathbb{K}, +, \cdot)$ и $(\mathbb{K}', \oplus, \odot)$ — кольца. Отображение $f : \mathbb{K} \to \mathbb{K}'$ называется *гомоморфизмом*, если оно сохраняет операции, т. е. равенства

$$f(a + b) = f(a) \oplus f(b), \quad f(ab) = f(a) \odot f(b)$$

справедливы для любых a и b из $\mathbb{K}$. *Ядром гомоморфизма* f называется множество

$$\operatorname{Ker} f = \{a \in \mathbb{K} \mid f(a) = 0\}.$$

Легко видеть, что ядро гомоморфизма $f : \mathbb{K} \to \mathbb{K}'$ будет подкольцом в $\mathbb{K}$.

Пример 4.9. Гомоморфизмом кольца $\mathbb{Z}$ в кольцо $\mathbb{Z}_m$ будет отображение $f : a \to [a]_m$. Ясно, что $\operatorname{Ker} f = m\mathbb{Z}$ является подкольцом в $\mathbb{Z}$. □

Следующая теорема легко следует из свойств гомоморфизмов групп. Эту теорему, как и сформулированную выше теорему 4.3, приведем без доказательства, которое оставляем читателю в качестве несложного упражнения.

Теорема 4.4. *Если $f : \mathbb{K} \to \mathbb{K}'$ гомоморфизм колец $\mathbb{K}$ и $\mathbb{K}'$, то*:

1) $f(0) = 0$;
2) $f(-a) = -f(a)$ *для любого* $a \in \mathbb{K}$.

Подмножество I кольца $\mathbb{K}$ называется (двусторонним) *идеалом*, если оно является подгруппой аддитивной группы кольца и $ab \in I$ и $ba \in I$ для любого $a \in I$ и любого $b \in \mathbb{K}$. Про идеал говорят, что он выдерживает умножение на любой элемент кольца. Если $b \in \operatorname{Ker} f$, то для любого $a \in \mathbb{K}$

$$f(ab) = f(a)f(b) = f(a) \cdot 0 = 0, \quad f(ba) = f(b)f(a) = 0 \cdot f(a) = 0.$$

Поэтому $ab \in \operatorname{Ker} f$ и $ba \in \operatorname{Ker} f$. Следовательно, ядро гомоморфизма является идеалом в $\mathbb{K}$.

Выше было отмечено, что в кольце целых чисел каждое подкольцо имеет вид $m\mathbb{Z}$. Так как $m\mathbb{Z}$ состоит из всех целых кратных m, то легко видеть, что $m\mathbb{Z}$ будет идеалом в $\mathbb{Z}$, т. е. каждое подкольцо в $\mathbb{Z}$ является идеалом. В общем случае это не так, например, целые числа в $\mathbb{Z}[\sqrt{2}]$ образуют подкольцо, но не идеал. С другой стороны, аналоги идеалов в кольце целых чисел существуют в произвольном коммутативном кольце. Так как для любого такого кольца $\mathbb{K}$ и любых его элементов a, x, y

$$ax + ay = a(x + y), \quad (ax)y = a(xy),$$

то $a\mathbb{K}$ будет идеалом в $\mathbb{K}$. Такой идеал называют *главным идеалом*, порожденным элементом a. Если каждый идеал I кольца $\mathbb{K}$ главный, т. е. существует порождающий его элемент $a \in I$, такой, что $I = a\mathbb{K}$, то кольцо $\mathbb{K}$ называется *кольцом главных идеалов*.

Пример 4.10. Кольца $\mathbb{Z}$ и $\mathbb{Z}_m$ при любом $m \in \mathbb{N}$ являются кольцами главных идеалов. □

4.3. Фактор-кольца

В произвольном кольце $\mathbb{K}$ любой идеал I является подгруппой аддитивной абелевой группы этого кольца. Поэтому в силу теоремы 3.9 фактор-множество $\mathbb{K}/I$, элементы которого складываются по правилу

$$(a+I)+(b+I)=(a+b)+I, \tag{4.2}$$

будет абелевой группой. На этом фактор-множестве введем операцию умножения, полагая, что

$$(a+I)(b+I)=ab+I. \tag{4.3}$$

Эта операция ассоциативна, что легко следует из ассоциативности умножения в $\mathbb{K}$, а так как для любых i_1, i_2 из I

$$\begin{aligned}((a+i_1)+I)((b+i_2)+I) &= (a+i_1)(b+i_2)+I = \\ &= ab+i_1b+ai_2+I = ab+I,\end{aligned}$$

то результат умножения не зависит от выбора представителей смежных классов. Следовательно, операция умножения определена корректно, и фактор-множество $\mathbb{K}/I$ будет полугруппой относительно этой операции. Для операций сложения и умножения на $\mathbb{K}/I$ справедливы законы дистрибутивности, что нетрудно видеть из следующих равенств:

$$\begin{aligned}(a+I)((b+I)+(c+I)) &= (a+I)((b+c)+I)) = \\ &= a(b+c)+I = \\ &= ab+ac+I = ab+I+ac+I = \\ &= (a+I)(b+I)+(a+I)(c+I).\end{aligned}$$

Таким образом, фактор-множество $\mathbb{K}/I$ с операциями (4.2) и (4.3) будет кольцом. Оно называется *фактор-кольцом* кольца $\mathbb{K}$ по идеалу I. Подводя итог, видим, что аналог теоремы 3.9 для групп и их нормальных подгрупп имеет место для колец и их идеалов.

Теорема 4.5. *Фактор-множество кольца $\mathbb{K}$ по идеалу I является кольцом.*

Две следующие теоремы о гомоморфизмах колец делают отмеченную аналогию между нормальными подгруппами и идеалами более полной.

Теорема 4.6. *Пусть I — идеал в кольце $\mathbb{K}$. Тогда существует гомоморфизм $f : \mathbb{K} \to \mathbb{K}/I$, ядром которого является идеал I.*

Доказательство. Рассмотрим отображение $f : a \to a + I$, ставящее в соответствие элементу a смежный класс, которому он принадлежит. Так как

$$\begin{aligned} f(a_1 + a_2) &= a_1 + a_2 + I = a_1 + a_2 + I + I = \\ &= a_1 + I + a_2 + I = f(a_1) + f(a_2), \\ f(a_1 a_2) &= a_1 a_2 + I = (a_1 + I)(a_2 + I) = f(a_1) f(a_2) \end{aligned}$$

для любых a_1 и a_2 из $\mathbb{K}$, то f сохраняет операции и поэтому является гомоморфизмом. Теорема доказана.

Теорема 4.7. *Пусть $f : \mathbb{K} \to \mathbb{K}'$ — гомоморфизм кольца $\mathbb{K}$ в кольцо $\mathbb{K}'$ с ядром I. Тогда $\mathbb{K}/I \cong \mathrm{Im} f$.*

Доказательство. Рассмотрим отображение $\varphi : a + I \to f(a)$, ставящее в соответствие смежному классу $a + I$ образ элемента a при гомоморфизме f. Из свойства сохранения операции гомоморфизмом следует, что

$$\begin{aligned} \varphi((a_1 + I) + (a_2 + I)) &= \varphi((a_1 + a_2) + I) = f(a_1 + a_2) = \\ &= f(a_1) + f(a_2) = \varphi(a_1 + I) + \varphi(a_2 + I), \\ \varphi((a_1 + I)(a_2 + I)) &= \varphi(a_1 a_2 + I) = f(a_1 a_2) = \\ &= f(a_1) f(a_2) = \varphi(a_1 + I)\varphi(a_2 + I) \end{aligned}$$

для любых a_1 и a_2 из $\mathbb{K}$. Поэтому φ сохраняет операции и, таким образом, является гомоморфизмом.

Теперь покажем, что φ — биективное отображение. Так как $\mathrm{Im}\varphi = \mathrm{Im} f$ в силу определения φ, то оно сюръективно. Покажем

инъективность φ. Действительно, если найдутся a_1 и a_2 такие, что $\varphi(a_1 + I) = \varphi(a_2 + I)$, то

$$f(a_1) = \varphi(a_1 + I) = \varphi(a_2 + I) = f(a_2),$$

и, следовательно, элементы a_1 и a_2 принадлежат одному и тому же смежному классу кольца $\mathbb{K}$ по идеалу I, т. е. $a_1 + I = a_2 + I$. Таким образом, $\varphi(a_1 + I) \neq \varphi(a_2 + I)$, если $a_1 + I \neq a_2 + I$. Теорема доказана.

4.4. Кольцо многочленов

1. Основные свойства. Пусть $\mathbb{K}$ — кольцо, x — переменная, n — целое неотрицательное. Выражение

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0$$

с коэффициентами $a_0, a_1, \ldots, a_n$ из кольца $\mathbb{K}$ назовем *многочленом* $a(x)$ *над кольцом* $\mathbb{K}$ степени n относительно переменной x, если $a_n \neq 0$. Степень многочлена $a(x)$ обозначим через $\deg a(x)$.

Суммой многочлена $a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ степени n и многочлена $b(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ степени m называется многочлен $c_r x^r + c_{r-1} x^{r-1} + \cdots + c_0$, где $c_i = a_i + b_i$ и $r = \max(n, m)$. *Произведением* этих многочленов называется многочлен $d_k x^k + d_{k-1} x^{k-1} + \cdots + d_0$, где $d_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i$ и $k = n + m$. Нетрудно проверить, что определенные так сумма и произведение многочленов удовлетворяют свойству дистрибутивности и другим аксиомам кольца.

Значением $a(\alpha)$ многочлена $a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ на элементе $\alpha \in \mathbb{K}$ называется такой элемент β кольца $\mathbb{K}$, что $\beta = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_0$. *Корнем* многочлена $a(x)$ называется элемент $\alpha \in \mathbb{K}$, для которого $a(\alpha) = 0$.

Будем говорить, что многочлен $a(x)$ *делится* на многочлен $b(x) \neq 0$, если существует такой многочлен $c(x)$, что $a(x) = b(x)c(x)$. Если многочлен $a(x)$ делится на многочлен $b(x)$, то многочлен $b(x)$ будем называть *делителем* $a(x)$, и будем говорить также, что $b(x)$ делит $a(x)$ (обозначение $b(x) \mid a(x)$).

Множество, состоящее из всех многочленов любой конечной степени над $\mathbb{K}$ называется *кольцом многочленов* $\mathbb{K}[x]$. Нетрудно показать, что $\mathbb{K}[x]$ будет кольцом, содержащим кольцо $\mathbb{K}$. Более того, если $\mathbb{K}$ — кольцо без делителей нуля, то и $\mathbb{K}[x]$ будет кольцом без делителей нуля. Действительно, если произведение многочлена $a(x)$ степени n и многочлена $b(x)$ степени m равно нулю, то равен нулю и коэффициент $a_n b_m$ при старшей степени произведения, что, очевидно, невозможно, так как a_n и b_m элементы кольца без делителей нуля.

Если кольцо коэффициентов $\mathbb{K}$ является полем, то в кольце многочленов над $\mathbb{K}$ справедлива теорема об однозначности деления с остатком, аналогичная теореме о делении с остатком в кольце целых чисел.

Теорема 4.8. *Пусть $\mathbb{F}$ — некоторое поле. Тогда для любых многочленов $a(x), b(x) \in \mathbb{F}[x]$, где $\deg b(x) > 0$, существуют и притом единственные многочлены $q(x), r(x) \in \mathbb{F}[x]$, такие, что*

$$a(x) = b(x) \cdot q(x) + r(x), \quad \deg r(x) < \deg b(x). \tag{4.4}$$

Многочлен $r(x)$ называется *остатком*, а $q(x)$ — *неполным частным* при делении $a(x)$ на $b(x)$.

Доказательство. Обозначим $n = \deg a(x)$, $m = \deg b(x)$, и пусть $a(x) = \sum_{i=0}^{n} a_i x^i$, $b(x) = \sum_{i=0}^{m} b_i x^i$. Можно считать, что $n > m > 0$, так как все остальные случаи либо сводятся к этому, либо являются тривиальными. Заметим, что старшие коэффициенты a_n, b_m не равны нулю, поэтому существует $b_m^{-1} \in \mathbb{F}$. Обозначим $\tilde{a}(x) = a(x) - b(x) \cdot a_n b_m^{-1} x^{n-m} \in \mathbb{F}[x]$. Коэффициент при x^n в разности $a(x) - b(x) \cdot a_n b_m^{-1} x^{n-m}$ равен $a_n - b_m \cdot a_n b_m^{-1} = 0$, поэтому $\deg \tilde{a}(x) < n$. Получили равенство

$$a(x) = b(x) \cdot a_n b_m^{-1} x^{n-m} + \tilde{a}(x), \quad \deg \tilde{a}(x) < n.$$

Применив по индукции эти рассуждения к $\tilde{a}(x)$ и $b(x)$, найдем такие $\tilde{q}(x), r(x) \in \mathbb{F}[x]$, для которых $\tilde{a}(x) = b(x) \cdot \tilde{q}(x) + r(x)$, причем $\deg \tilde{q} < n - m$ и $\deg r < m$. Тогда $q(x) = a_n b_m^{-1} x^{n-m} + \tilde{q}(x)$ и $r(x)$ дают искомое представление (4.4).

Теперь докажем единственность представления (4.4). Допустим, что

$$a = bq + r = bq' + r', \quad 0 \leqslant \deg r < \deg b, \quad 0 \leqslant \deg r' < \deg b.$$

Тогда $b(q-q') = r'-r$. Но $\deg(r'-r) < \deg b$, а $\deg b(q-q') \geqslant \deg b$ при $q - q' \neq 0$. Противоречия не будет только в случае, когда $q = q'$ и $r = r'$. Теорема доказана.

Пусть $\mathbb{F}$ — поле. Если коэффициент при старшей степени многочлена над полем $\mathbb{F}$ равен единице, то многочлен называется *нормированным.* Без доказательства приведем следующее очевидное утверждение.

Теорема 4.9. *Пусть $\mathbb{F}$ — поле. Тогда $\mathbb{F}[x]$ — коммутативное кольцо с единицей и без делителей нуля.*

Применяя в кольце многочленов теорему о делении с остатком, можно легко убедиться, что если $\mathbb{F}$ — поле, то $\mathbb{F}[x]$ — кольцо главных идеалов. Доказательство этого факта аналогично доказательству того, что каждый идеал кольца $\mathbb{Z}$ главный.

Любой многочлен $c(x)$, который делит многочлены $a(x)$ и $b(x)$, называется общим делителем этих многочленов. Нормированный многочлен наибольшей степени среди общих делителей многочленов $a(x)$ и $b(x)$ называется их *наибольшим общим делителем* (сокращенно НОД) и обозначается символом $(a(x), b(x))$. Многочлены, не имеющие общих делителей ненулевой степени, называются *взаимно простыми*. Легко видеть, что $(a(x), b(x)) = 1$ для любых взаимно простых многочленов $a(x)$ и $b(x)$.

Теорема 4.10. *Пусть $\mathbb{F}$ — поле. Тогда для любых ненулевых многочленов $a(x)$ и $b(x)$ над полем $\mathbb{F}$ ненулевой нормированный многочлен минимальной степени $d(x)$, удовлетворяющий равенству*

$$d(x) = a(x)s(x) + b(x)t(x), \tag{4.5}$$

где $s(x)$ и $t(x)$ — многочлены над $\mathbb{F}$, является наибольшим общим делителем многочленов $a(x)$ и $b(x)$.

Доказательство. Покажем, что $a(x)$ делится на $d(x)$. Представим $a(x)$ в виде $a(x) = p(x)d(x)+q(x)$, где $\deg q(x) < \deg d(x)$. Тогда

$$q(x) = a(x) - p(x)d(x) = a(x) - p(x)(a(x)s(x) + b(x)t(x)) = \\ = a(x)(1 - p(x)s(x)) - b(x)(p(x)t(x)) = a(x)s'(x) + b(x)t'(x),$$

где $s'(x) = 1-p(x)s(x)$ и $t'(x) = -p(x)t(x)$. Так как $d(x)$ — ненулевой нормированный многочлен минимальной степени, удовлетворяющий (4.5), то $q(x) = 0$ и, следовательно, $a(x)$ делится на $d(x)$. Аналогичным образом доказывается делимость на $d(x)$ многочлена $b(x)$. Следовательно, $d(x)$ является общим делителем многочленов $a(x)$ и $b(x)$. Теперь покажем, что $d(x)$ будет наибольшим общим делителем. Действительно, если $a(x)$ и $b(x)$ делятся на $d(x)d'(x)$, где $\deg d'(x) > 0$, то в (4.5) правая часть будет делиться на $d(x)d'(x)$, а левая не будет. Следовательно, $d(x) = (a(x), b(x))$. Теорема доказана.

Многочлен $p(x)$ называется *неприводимым* над полем $\mathbb{F}$, если из равенства $p(x) = a(x)b(x)$, где $a(x), b(x) \in \mathbb{F}[x]$, следует $\deg a(x) = 0$ или $\deg b(x) = 0$. Из определения неприводимого многочлена легко следует, что любой многочлен можно представить в виде произведения неприводимых многочленов, например, в $\mathbb{Z}_2[x]$ имеет место равенство

$$x^4 + x = x(x + 1)(x^2 + x + 1).$$

Лемма 4.3. *Если произведение $a(x)b(x)$ многочленов $a(x)$ и $b(x)$ над полем $\mathbb{F}$ делится на неприводимый многочлен $p(x)$, то хотя бы один из сомножителей также делится на $p(x)$.*

Доказательство. Допустим, что утверждение леммы неверно. Тогда ни один из сомножителей не делится на $p(x)$. Следовательно, $(a(x), p(x)) = 1$ и $(b(x), p(x)) = 1$, и из теоремы 4.10 следует, что найдутся такие многочлены $s_1(x), s_2(x)$ и $t_1(x), t_2(x)$, что

$$1 = s_1(x)a(x) + s_2(x)p(x), \qquad 1 = t_1(x)b(x) + t_2(x)p(x).$$

Перемножив эти равенства, получим

$$\begin{aligned}1 &= (s_1(x)a(x) + s_2(x)p(x)) \cdot (t_1(x)b(x) + t_2(x)p(x)) = \\ &= (s_1(x)t_1(x)) \cdot a(x)b(x) + \\ &\quad + (s_2(x)t_1(x)b(x) + s_1(x)t_2(x)a(x) + s_2(x)t_2(x)p(x)) \cdot p(x),\end{aligned}$$

т. е. в силу теоремы 4.10 многочлены $a(x)b(x)$ и $p(x)$ взаимно просты. Противоречие. Лемма доказана.

Лемма 4.4. *Если произведение $a_1(x)a_2(x)\cdots a_n(x)$ многочленов $a_i(x)$ над полем $\mathbb{F}$ делится на неприводимый многочлен $p(x)$, то хотя бы один из сомножителей также делится на $p(x)$.*

Доказательство. Лемму докажем индукцией по числу сомножителей. Случай $n = 2$ доказан в предыдущей лемме. Допустим, утверждение леммы справедливо для любых произведений, содержащих не более k сомножителей. Тогда если произведение $(a_1(x)a_2(x)\cdots a_k(x))a_{k+1}(x)$ делится на $p(x)$, то из леммы 4.3 следует, что либо $a_1(x)a_2(x)\cdots a_k(x)$, либо $a_{k+1}(x)$ делится на $p(x)$. В первом случае утверждение леммы следует из предположения индукции. Во втором случае справедливость леммы очевидна. Лемма доказана.

Теорема 4.11. *Каждый нормированный многочлен над полем $\mathbb{F}$ единственным, с точностью до порядка следования сомножителей, образом раскладывается в произведение нормированных неприводимых многочленов.*

Доказательство. Далее все многочлены считаем нормированными. Теорему докажем методом математической индукции. В основание индукции положим многочлены степени 1, единственность разложения которых очевидна. Предположим, что каждый многочлен, степень которого не превосходит n, разлагается на неприводимые множители единственным образом. Покажем, что из этого предположения следует единственность разложения любого многочлена степени $n+1$. Действительно, если некоторый многочлен $t(x)$ степени $n+1$ имеет два различных разложения в произведение неприводимых сомножителей, то

$$t(x) = p_1^{k_1}(x)p_2^{k_2}(x)\cdots p_n^{k_n}(x) = q_1^{s_1}(x)q_2^{s_2}(x)\cdots q_m^{s_m}(x).$$

Покажем, что $p_1(x)$ совпадает с одним из многочленов $q_i(x)$. Так как неприводимый многочлен $p_1(x)$ делит произведение

$$\underbrace{q_1(x)\cdots q_1(x)}_{s_1 \text{ раз}}\underbrace{q_2(x)\cdots q_2(x)}_{s_2 \text{ раз}}\cdot\ldots\ldots\cdot\underbrace{q_m(x)\cdots q_m(x)}_{s_m \text{ раз}}, \tag{4.6}$$

то в силу леммы 4.4 многочлен $p_1(x)$ также делит один из его сомножителей. В (4.6) все сомножители — неприводимые многочлены. Следовательно, $p_1(x)$ совпадает с одним из них. Без ограничения общности будем полагать, что $p_1(x) = q_1(x)$. Сокращая левую и правую части равенства (4.6) на $p_1(x)$, получим

$$p_1^{k_1-1}(x)p_2^{k_2}(x)\cdots p_n^{k_n}(x) = q_1^{s_1-1}(x)q_2^{s_2}(x)\cdots q_m^{s_m}(x). \tag{4.7}$$

По предположению индукции многочлен $t(x)/p_1(x)$ раскладывается на неприводимые множители единственным образом. Поэтому в (4.7) $n = m$ и для каждого $i \in \{1,\ldots,n\}$ справедливы равенства $p_i(x) = q_i(x)$ и $k_i = s_i$. Теорема доказана.

Лемма 4.5 (теорема Безу). *Многочлен $f(x)$ над полем $\mathbb{F}$ делится на двучлен $x-\alpha$, где $\alpha \in \mathbb{F}$, тогда и только тогда, когда $f(\alpha) = 0$. Значение многочлена $f(x)$ в точке α равно остатку от деления $f(x)$ на $x-\alpha$.*

Доказательство. Если многочлен $f(x)$ делится на $x-\alpha$, то $f(x) = h(x)(x-\alpha)$. Тогда $f(\alpha) = h(\alpha)(\alpha-\alpha) = 0$. С другой стороны, $f(x) = h(x)(x-\alpha)+\beta$, и если $f(\alpha) = 0$, то легко видеть, что $\beta = 0$. Следовательно, $f(x)$ делится на $x-\alpha$. Лемма доказана.

Теорема 4.12. *Многочлен f степени n над полем $\mathbb{F}$ имеет в поле $\mathbb{F}$ не более n корней.*

Доказательство. Теорему докажем индукцией по степени многочлена. Очевидно, что ненулевой многочлен нулевой степени не имеет корней. Этот случай ($\deg f = 0$) положим в основание индукции. Допустим, что утверждение теоремы справедливо для всех многочленов степени не более k. Пусть $\deg f = k+1$.

Если многочлен $f(x)$ в поле $\mathbb{F}$ не имеет корней, то утверждение теоремы очевидно. Пусть α — корень многочлена $f(x)$. Тогда в силу леммы 4.5 многочлен $f(x)$ делится на $x-\alpha$, т. е. $f(x)=h(x)(x-\alpha)$, где многочлен k-й степени $h(x)$ по предположению индукции имеет в $\mathbb{F}$ не более k корней. Следовательно, f имеет в поле $\mathbb{F}$ не более $k+1$ корней. Теорема доказана.

При доказательстве теорем 4.8—4.12 было существенно, что множество коэффициентов $\mathbb{K}$ является полем. В случае, когда $\mathbb{K}$ не является полем, все они, вообще говоря, неверны.

Действительно, пусть, например, $\mathbb{K}=\mathbb{Z}_6$. Кольцо $\mathbb{Z}_6[x]$ является ассоциативным, коммутативным кольцом с единицей, но, как и $\mathbb{Z}_6$, содержит делители нуля: например, $2x\cdot 3x=0$.

В рассматриваемом кольце для x^2 и $2x$ не существует таких многочленов $q(x)$ и $r(x)$, что $x^2=2x\cdot q(x)+r(x)$ и $\deg r<$ $<\deg 2x=1$, иначе для старшего коэффициента $a\in\mathbb{Z}_6$ частного $q(x)$ должно быть выполнено равенство $2a=1$, но вычет 2 необратим в $\mathbb{Z}_6$. А для многочленов $2x^3$ и $2x^2+2x+1$ таких пар (q,r) несколько:

$$\begin{aligned}2x^3&=(2x^2+2x+1)(x+5)+x+1=\\&=(2x^2+2x+1)(4x+2)+4x+4.\end{aligned}$$

Таким образом, в $\mathbb{Z}_6[x]$ неверна и теорема о делении с остатком.

Многочлен x^2+3x+2 имеет в $\mathbb{Z}_6$ четыре корня $x=1,2,4,5$, что больше, чем его степень. В кольце $\mathbb{Z}_6[x]$ он также неоднозначно разлагается на неприводимые множители: $x^2+3x+2=$ $=(x+1)(x+2)=(x+4)(x+5)$.

Наконец, равенство $(2x^2+x)(3x+1)+(2x+1)(x^2+x+1)=1$ иллюстрирует неприменимость теоремы 4.10 в кольце $\mathbb{Z}_4[x]$: оба многочлена $a(x)=2x^2+x=x(2x+1)$ и $b(x)=2x+1$ делятся на $b(x)$, однако нормированного делителя максимальной степени у них нет. Таким образом, кольца $\mathbb{K}[x]$ и $\mathbb{F}[x]$ имеют серьезные отличия.

2. Евклидовы кольца. Формулировки и доказательства утверждений о разложении в кольце многочленов очень похожи на аналогичные формулировки и доказательства в кольце целых

чисел. Это не случайно, так как оба эти кольца являются евклидовыми кольцами. Целостное кольцо (без делителей нуля) $\mathbb{K}$ называется *евклидовым*, если каждому его ненулевому элементу a поставлено в соответствие целое неотрицательное число $\Delta(a)$ так, что:

(1) $\Delta(ab) \geqslant \Delta(a)$ для всех $a, b \neq 0$ из $\mathbb{K}$;

(2) для всех $a, b \neq 0$ из $\mathbb{K}$ существуют такие $q, r \in \mathbb{K}$, что

$$a = qb + r \quad \text{и} \quad \Delta(r) < \Delta(b) \text{ или } r = 0.$$

В кольце целых чисел значение $\Delta(a)$ совпадает с $|a|$, а в кольце многочленов равно степени многочлена.

В целостном кольце необратимый элемент p называется *простым*, если не существует таких необратимых элементов a и b, что $p = ab$. На множестве ненулевых элементов целостного кольца отношение делимости определяется аналогично отношениям делимости в кольце целых чисел и кольце многочленов. *Наибольшим общим делителем* элементов a и b целостного кольца называется их общий делитель, делящийся на все общие делители этих элементов. Нетрудно показать, что в евклидовом кольце для любых ненулевых элементов a и b существует их наибольший общий делитель, обладающий такими же свойствами, что и наибольшие общие делители в $\mathbb{Z}$ и $\mathbb{F}[x]$.

Целостное кольцо называется *факториальным*, если каждый его ненулевой элемент a можно представить в виде произведения

$$a = bp_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \tag{4.8}$$

где b — обратимый элемент, а различные простые элементы $p_1, p_2, \ldots, p_n$ определены однозначно с точностью до обратимых множителей. В кольце $\mathbb{Z}$ есть ровно два обратимых элемента 1 и -1, поэтому каждое число p_i, являющееся простым элементом кольца $\mathbb{Z}$ в разложении (4.8) целого числа a, определено с точностью до множителя ± 1. Следуя доказательствам утверждений данного раздела, нетрудно показать, что любое евклидово кольцо является факториальным.

4.5. Арифметика многочленов

Из доказательства теоремы 4.8 извлекается известный со школы алгоритм деления многочленов в столбик (уголком).

Пример 4.11. Рассмотрим многочлены $a(x) = x^5+2x^4+2x^3+$ $+x+1$ и $b(x) = x^4+x^2+2x+2$ над полем $\mathbb{Z}_3$ и найдем неполное частное $q(x)$ и остаток $r(x)$ от деления $a(x)$ на $b(x)$. При делении в столбик удобно записывать не сами многочлены, а только их коэффициенты, объединенные в упорядоченный набор, называемый вектором[1)]. Так, например, многочлен $a(x)$ представляется вектором `122011`. Соответствие между многочленами и векторами их коэффициентов взаимно однозначно, если договориться записывать старшие коэффициенты слева. Для сравнения приведем деление $a(x)$ на $b(x)$ в стандартной записи и в векторной, которая, очевидно, более компактна:

$$\begin{array}{l|l}
x^5+2x^4+2x^3\qquad\quad+x+1 & x^4+x^2+2x+2 \\
\underline{x^5\qquad\quad+x^3+2x^2+2x} & x+2 \\
\qquad 2x^4\ +x^3\ +x^2+2x+1 & \\
\qquad \underline{2x^4\qquad\quad+2x^2\ +x+1} & \\
\qquad\qquad\quad x^3+2x^2\ +x &
\end{array}
\qquad
\begin{array}{l|l}
\texttt{122011} & \texttt{10122} \\
\underline{\texttt{10122}} & \texttt{12} \\
\texttt{21121} & \\
\underline{\texttt{20211}} & \\
\texttt{1210} &
\end{array}$$

Таким образом, $q(x) = x+2 = \texttt{12}$ и $r(x) = x^3+2x^2+x = \texttt{1210}$. Следовательно,

$$x^5+2x^4+2x^3+x+1 = (x^4+x^2+2x+2)(x+2)+x^3+2x^2+x,$$

или $\texttt{122011} = \texttt{10122}\cdot\texttt{12}+\texttt{1210}$ в векторной записи.

Ниже, тоже в векторной форме, приведено умножение и сложение полученных многочленов, которые можно считать про-

[1)] Векторам и векторным пространствам посвящена глава 5. Здесь мы не будем забегать вперед и ссылаться на пример 5.5, векторное представление многочлена будет пока использоваться нами только в целях укорочения его записи. Арифметика таких «векторов» является арифметикой просто переобозначенных по-другому многочленов.

веркой правильности деления:

$$\begin{array}{r} \times\ 10122 \\ \underline{\qquad\ 12} \\ 20211 \\ \underline{10122\ \ } \\ 121101 \end{array} \qquad \begin{array}{r} +\ 121101 \\ \underline{\qquad\ 1210}. \\ 122011 \end{array}$$

□

Полезно знать, что умножение и деление в столбик являются не наилучшими по числу затраченных операций в поле коэффициентов алгоритмами. Их широкая распространенность обусловлена главным образом простотой реализации и привычностью (данью традициям). Начиная со второй половины XX в. было разработано много альтернативных методов[1)] (алгоритмы Карацубы, Тоома, Шёнхаге — Штрассена, Фюрера и пр.). Для многочленов большой степени их сложность гораздо меньше, чем у умножения — деления в столбик.

Далее для удобства будем использовать введенную выше векторную запись

$$a(x) = (\mathtt{a_n a_{n-1} \dots a_1 a_0}) = \sum_{i=0}^{n} a_i x^i$$

многочлена $a(x) \in \mathbb{F}[x]$ уже без пояснений, особенно когда из контекста ясно, что вектор является вектором коэффициентов некоторого многочлена.

Пример 4.12 (схема Горнера)**.** Удобный способ вычисления значения многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}[x]$ в точке $x = \alpha \in \mathbb{F}$ вытекает из следующего равенства:

$$f(\alpha) = ((\ldots (((a_n\alpha + a_{n-1})\alpha + a_{n-2})\alpha + a_{n-3}) \ldots)\alpha + a_1)\alpha + a_0,$$

полученного последовательным вынесением за скобки общих множителей одночленов. Он сводится к рекуррентному вычислению последовательности

$$b_0 = a_n, \quad b_1 = b_0\alpha + a_{n-1}, \quad \ldots \quad b_i = b_{i-1}\alpha + a_{n-i}, \quad i \leqslant n. \tag{4.9}$$

[1)] См. [5, 23, 29, 30].

По индукции нетрудно установить, что ее последний член b_n является искомым значением $f(\alpha)$. Также легко видеть, что элементы последовательности $\{b_i\}$ совпадают с коэффициентами неполного частного $q(x)$, вычисляемого при делении в столбик $f(x)$ на $x-\alpha$ (b_0 является старшим коэффициентом, а b_{n-1} — свободным членом $q(x)$). Результат работы принято записывать таблицей вида

	$\mathtt{a_n}$	$\mathtt{a_{n-1}}$	$\mathtt{a_{n-2}}$	$\ldots$	$\mathtt{a_1}$	$\mathtt{a_0}$
α	$\mathtt{b_0}$	$\mathtt{b_1}$	$\mathtt{b_2}$	$\ldots$	$\mathtt{b_{n-1}}$	$\mathtt{b_n} = \mathtt{f}(\alpha)$

.

Из (4.9) следует мнемоническое правило: каждый элемент ее нижней строки (начиная с b_1) равен сумме соседа сверху с произведением соседа слева на α. По теореме Безу данное вычисление значения $f(\alpha)$ является одновременно вычислением остатка от деления $f(x)$ на $x-\alpha$ и, как оказывается, заодно и неполного частного.

В качестве примера найдем значение многочлена $f(x) = x^8 + 4x^7 + 2x^5 + x^4 + x^3 + 3x + 2$ в точке $x = 3$ над полем $\mathbb{Z}_5$:

	1	4	0	2	1	1	0	3	2
3	1	2	1	0	1	4	2	4	4

.

Таким образом, $f(3) = 4$. Попутно мы установили, что (в векторной записи) $\mathtt{140211032} = \mathtt{12101424} \cdot \mathtt{12} + \mathtt{4}$.

Схема Горнера использует $n = \deg f$ сложений и n умножений коэффициентов в поле $\mathbb{F}$. Можно показать[1)], что данное число операций является минимально возможным для любого алгоритма, находящего $f(\alpha)$ и не использующего деление в поле $\mathbb{F}$. Таким образом, схема Горнера оптимальна для вычисления $f(x)$ в одной точке. Для вычисления значений $f(x)$ одновременно в m точках при большом m существуют способы с меньшей сложностью, чем независимое вычисление в каждой точке по отдельности, например, быстрое преобразование Фурье[2)]. □

[1)] См. [1, с. 227—232].

[2)] См. [3, 5, 23, 30].

Из теоремы 4.8 о делении с остатком в кольце многочленов $\mathbb{F}[x]$, где $\mathbb{F}$ — поле, следует, что для вычисления НОД многочленов можно применять те же способы, что и для вычисления НОД в кольце $\mathbb{Z}$ (см. с. 30—32). В частности, аналогично лемме 2.1 доказывается следующее утверждение, в котором, как и ранее, запись $(X, Y, Z) - Q(X', Y', Z')$ означает упорядоченную тройку $(X - QX', Y - QY', Z - QZ')$, только уже не чисел, а многочленов.

Лемма 4.6. *Пусть* $a(x), b(x) \in \mathbb{F}[x]$, $\deg a(x) \geqslant \deg b(x)$ *и* $b(x) \neq 0$. *Рассмотрим последовательность троек многочленов* (X_i, Y_i, Z_i) *над полем* $\mathbb{F}$, *такую, что* $(X_{-1}, Y_{-1}, Z_{-1}) = (1, 0, a(x))$, $(X_0, Y_0, Z_0) = (0, 1, b(x))$ *и*

$$\begin{pmatrix} X_i \\ Y_i \\ Z_i \end{pmatrix} = \begin{pmatrix} X_{i-2} \\ Y_{i-2} \\ Z_{i-2} \end{pmatrix} - Q_i \begin{pmatrix} X_{i-1} \\ Y_{i-1} \\ Z_{i-1} \end{pmatrix}$$

при $i \geqslant 1$, *где* $Q_i = \lfloor Z_{i-2}/Z_{i-1} \rfloor$ — *неполное частное от деления многочлена* Z_{i-2} *на* Z_{i-1}. *Тогда существует наименьшее такое* $n \geqslant 0$, *что* $Z_{n+1} = 0$, *и многочлен* Z_n *является с точностью до постоянного нормирующего множителя наибольшим общим делителем многочленов* $a(x)$ *и* $b(x)$. *Более того,* $a \cdot X_i + b \cdot Y_i = Z_i$ *при всех* $i \geqslant -1$. *В частности,*

$$a \cdot X_n + b \cdot Y_n = Z_n. \tag{4.10}$$

Многочлены последовательности $Z_1, \ldots, Z_n$ из леммы 4.6 — это остатки алгоритма Евклида. Значит, на последнем шаге имеем $Z_n \mid \text{НОД}(a, b)$ и $\text{НОД}(a, b) \mid Z_n$. Остаток от деления даже нормированных многочленов не обязательно нормирован, а НОД, по нашему определению, должен иметь старший коэффициент 1. Поэтому если $c \in \mathbb{F}$, $c \neq 0$ — старший коэффициент многочлена $Z_n(x)$, то делением обеих частей (4.10) на c получаем равенство

$$a \cdot \frac{X_n}{c} + b \cdot \frac{Y_n}{c} = \frac{Z_n}{c} = \text{НОД}(a, b), \tag{4.11}$$

гарантированное нам теоремой 4.10. Отметим, что равенству (4.5) теоремы 4.10 удовлетворяет бесконечное число пар многочленов $s(x), t(x) \in \mathbb{F}[x]$. Многочлены $s(x)$ и $t(x)$ (в частности многочлены X_n/c и Y_n/c), как и в случае целочисленной линейной комбинации, называются *коэффициентами Безу*.

Справедливо следующее утверждение.

Лемма 4.7. *Степени найденных алгоритмом леммы* 4.6 *коэффициентов X_n/c и Y_n/c являются наименьшими из всех возможных степеней коэффициентов Безу s, t для многочленов a, b в равенстве* (4.5).

Пример 4.13. Найдем НОД и коэффициенты Безу для многочленов $a(x) = x^5 + 2x^4 + 2x^3 + x + 1 = \mathtt{122011}$ и $b(x) = x^4 + x^2 + 2x + 2 = \mathtt{10122}$ над полем $\mathbb{Z}_3$ аналогично тому, как сделали это для чисел в примере 2.2. Первый шаг леммы 4.6 (деление с остатком $Z_{-1} = a$ на $Z_0 = b$) был проделан в примере 4.11. Отсюда $Q_1 = \mathtt{12}$, $X_1 = \mathtt{1} - \mathtt{12} \cdot \mathtt{0} = \mathtt{1}$ и $Y_1 = \mathtt{0} - \mathtt{12} \cdot \mathtt{1} = \mathtt{21}$. Переходим к шагу $i = 2$. Поделив с остатком Z_0 на Z_1, получаем $Q_2 = \mathtt{11}$, $Z_2 = \mathtt{112}$ и $\mathtt{10122} = \mathtt{1210} \cdot \mathtt{11} + \mathtt{112}$, откуда $X_2 = \mathtt{0} - \mathtt{11} \cdot \mathtt{1} = \mathtt{22}$, $Y_2 = \mathtt{1} - \mathtt{11} \cdot \mathtt{21} = \mathtt{100}$. Действуя и далее подобным образом, заполним таблицу:

1	0	1	22	122	2102	
0	1	21	100	2221	11220	
122011	10122	1210	112	11	2	0

В данном случае число делений n оказалось равно 4 (так как $Z_5 = 0$, $Z_4 \neq 0$). В силу $\deg Z_4 = 0$ многочлены $a(x)$ и $b(x)$ взаимно просты. Из последнего столбца таблицы по формуле (4.10) имеем

$$\mathtt{122011} \cdot \mathtt{2102} + \mathtt{10122} \cdot \mathtt{11220} = \mathtt{2}.$$

Найденный многочлен $Z_4 = \mathtt{2}$ не нормирован, следовательно, поделив обе части последнего равенства на его старший коэффициент $c = \mathtt{2}$, получим

$$a(x) \cdot \mathtt{1201} + b(x) \cdot \mathtt{22110} = \big(a(x), b(x)\big) = \mathtt{1}. \tag{4.12}$$

Таким образом, многочлены $x^3 + 2x^2 + 1$ и $2x^4 + 2x^3 + x^2 + x$ являются искомыми коэффициентами Безу. □

Лемма 4.8. *Пусть* $a(x), b(x) \in \mathbb{F}[x]$ *и* $\deg b(x) \leqslant \deg a(x) \leqslant N$. *Тогда число операций поля* $\mathbb{F}$, *потраченное для вычисления наибольшего общего делителя* $\big(a(x), b(x)\big)$ *и коэффициентов Безу алгоритмом леммы* 4.6, *не превосходит по порядку величины* N^2.

Доказательство. Действительно, из равенств

$$Z_{-1} = Q_1 Z_0 + Z_1, \quad Z_0 = Q_2 Z_1 + Z_2, \quad \ldots \quad Z_{n-2} = Q_n Z_{n-1} + Z_n$$

следует, что

$$Z_{-1} = Z_{n-1} \prod_{i=1}^{n} Q_i + h(x),$$

где $h(x)$ — некоторый многочлен, степень которого строго меньше $N = \deg Z_{-1}$. Поэтому

$$\deg \prod_{i=1}^{n} Q_i = \sum_{i=1}^{n} \deg Q_i = \deg \frac{Z_{-1} - h}{Z_{n-1}} \leqslant N.$$

Чтобы найти коэффициенты представления $Z_{i-2} = Q_i Z_{i-1} + Z_i$, достаточно $\mathcal{O}(\deg Z_{i-2} \cdot \deg Q_i)$ операций поля $\mathbb{F}$ при использовании деления в столбик. Последовательность степеней остатков алгоритма Евклида монотонно убывает: $\deg Z_i < \deg Z_{i-1}$. Отсюда следует, что сложность вычисления всех коэффициентов последнего ненулевого остатка Z_n не превосходит по порядку величины

$$\sum_{i=1}^{n} \deg Z_{i-2} \cdot \deg Q_i < N \sum_{i=1}^{n} \deg Q_i \leqslant N^2.$$

Аналогично получаются квадратичные оценки сложности и для нахождения X_n, Y_n. Лемма доказана.

Пример 4.14. Найдем все неприводимые многочлены над полем $\mathbb{Z}_2$, степень которых не превосходит четырех.

Из определения неприводимого многочлена следует, что все многочлены первой степени неприводимы. Над полем $\mathbb{Z}_2$ их имеется всего два: это многочлены $f_1(x) = x$ и $f_2(x) = x + 1$.

Среди многочленов второй степени и выше уже есть приводимые, например $x^n = x^{n-1} \cdot x$. Тем не менее для многочленов степени 2 и 3 имеется очень простой способ проверки приводимости. Его дает вышеупомянутая теорема Безу: если $f \in \mathbb{F}[x]$ и $\deg f \leqslant 3$, то многочлен f неприводим над $\mathbb{F}$ в том и только в том случае, когда он не имеет корней в поле $\mathbb{F}$. В самом деле, если $f = gh$ — приводим, то $\deg g, h \geqslant 1$, что в сочетании с неравенством $\deg f \leqslant 3$ дает $\deg g = 1$ или $\deg h = 1$, а многочлен первой степени всегда имеет корень в поле коэффициентов. Осталось выбрать среди всех нормированных многочленов степени 2, а именно среди многочленов

$$x^2, \quad x^2 + 1, \quad x^2 + x, \quad x^2 + x + 1$$

те, у которых нет корней в $\mathbb{Z}_2$. Таким, а значит неприводимым, будет единственный многочлен $f_3(x) = x^2 + x + 1$.

Вместо того, чтобы перебирать все нормированные многочлены третьей степени[1)] (а их всего $2^3 = 8$), заметим, что 0 — корень многочленов с нулевым свободным членом и только их, а единица является корнем многочлена из $\mathbb{Z}_2[x]$ тогда и только тогда, когда число слагаемых в нем четно. Из восьми многочленов третьей степени только два имеют нечетное число одночленов и одновременно ненулевой свободный член, это многочлены $f_4(x) = x^3 + x + 1$ и $f_5(x) = x^3 + x^2 + 1$.

Из шестнадцати многочленов 4-й степени только четыре не имеют корней в $\mathbb{Z}_2$:

$$x^4 + x + 1, \quad x^4 + x^2 + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1.$$

Теперь, однако, этого недостаточно для неприводимости: приводимый многочлен 4-й степени может являться произведением

[1)] Легко видеть, что число нормированных многочленов степени n над конечным полем $\mathbb{F}_q$ равно q^n, а число всех многочленов степени n равно $(q-1)q^n$ (старший коэффициент не может быть нулем).

двух неприводимых многочленов 2-й степени и не иметь корней в поле коэффициентов. Так как неприводимый многочлен 2-й степени у нас один, то приводимый многочлен 4-й степени без корней в $\mathbb{Z}_2$ также единственен и является его квадратом, в частности это многочлен $(x^2+x+1)^2 = x^4+x^2+1$. Значит, остальные многочлены $f_6(x) = x^4+x+1$, $f_7(x) = x^4+x^3+1$ и $f_8(x) = x^4+x^3+x^2+x+1$ неприводимы. Иных неприводимых многочленов, кроме $f_1, \ldots, f_8$, в заданном диапазоне степеней нет. □

Результаты вычислений примера 4.14 составляют часть приводимой ниже таблицы неприводимых над $\mathbb{Z}_2$ многочленов степени не больше 5.

Таблица

Неприводимые многочлены над $\mathbb{Z}_2$ степени $\leqslant 5$		
	полином	векторное представление
степень 1	x $x+1$	`10` `11`
степень 2	x^2+x+1	`111`
степень 3	x^3+x+1 x^3+x^2+1	`1011` `1101`

степень 4	x^4+x+1
	x^4+x^3+1
	$x^4+x^3+x^2+x+1$
		`10011`
		`11001`
		`11111`

степень 5	x^5+x^2+1
	x^5+x^3+1
	$x^5+x^3+x^2+x+1$
	$x^5+x^4+x^2+x+1$
	$x^5+x^4+x^3+x+1$
	$x^5+x^4+x^3+x^2+1$
		`100101`
		`101001`
		`101111`
		`110111`
		`111011`
		`111101`

Пусть f — многочлен степени n. Покажем, что f неприводим тогда и только тогда, когда он не делится ни на какой неприводимый многочлен степени $\left\lfloor \frac{n}{2} \right\rfloor$ и менее. Действительно, если

f неприводим, то он не делится ни на какой многочлен меньшей степени, в том числе неприводимый. Если же f приводим, то $f = gh$, где $\deg g \geqslant 1$ и $\deg h \geqslant 1$. Так как $\deg g + \deg h = n$, то степень одного из многочленов g и h не превышает $n/2$. Пусть для определенности это многочлен g. Если он неприводим, то мы нашли у многочлена f искомый неприводимый множитель степени не более $n/2$. В случае, когда g приводим, в качестве искомого множителя можно взять любой неприводимый множитель g — он имеется, так как каждый многочлен разлагается в произведение неприводимых, и степень этого множителя не превосходит $\deg g \leqslant n/2$.

Поэтому для проверки многочлена степени n на приводимость достаточно проверить его делимость на каждый неприводимый многочлен степени не выше $n/2$: если он не делится ни на один из них, то он неприводим[1)]. Для этого можно воспользоваться заранее вычисленной таблицей неприводимых многочленов. Например, таблица на с. 113 позволяет проверять на неприводимость все многочлены над $\mathbb{Z}_2$ вплоть до 11-й степени.

Пример 4.15. Проверим многочлен $f(x) = x^9 + x^4 + 1$ на неприводимость над $\mathbb{Z}_2$. Так как $f(0) \neq 0$ и $f(1) \neq 0$, то $f(x)$ не делится ни на x, ни на $x + 1$. Делимость на остальные неприводимые многочлены проверим делением с остатком. В результате получим следующие равенства:

$$\begin{aligned}
1000010001 &= 111 \cdot 11011101 + 10,\\
1000010001 &= 1011 \cdot 1011110 + 11,\\
1000010001 &= 1101 \cdot 1110111 + 10,\\
1000010001 &= 10011 \cdot 100111 + 1000,\\
1000010001 &= 11001 \cdot 111100 + 1101,\\
1000010001 &= 11111 \cdot 110000 + 00001.
\end{aligned}$$

Ни один из шести остатков не равен нулю, т. е. $f(x)$ не делится ни на какой неприводимый многочлен степени 4 и менее, поэтому $f(x)$ неприводим. □

[1)] Имеются и более эффективные способы проверки приводимости, основанные на строении конечных полей, см. пример 8.7.

Пример 4.16. Найдем число неприводимых нормированных многочленов второй степени над полем $\mathbb{Z}_{19}$. Нормированный многочлен второй степени из $\mathbb{Z}_{19}[x]$ имеет вид $x^2 + ax + b$, где $a, b \in \mathbb{Z}_{19}$ произвольны. Легко видеть, что существует ровно $19^2 = 361$ таких многочленов. Если нормированный многочлен приводим, то он представляется произведением

$$x^2 + ax + b = (x + c)(x + d) \tag{4.13}$$

двух нормированных двучленов, где коэффициенты c, d лежат в поле $\mathbb{Z}_{19}$ и не обязательно различны. Значит, число приводимых нормированных многочленов равно числу различных представлений вида (4.13). Если $c \neq d$, то имеется $\binom{19}{2} = \frac{19 \cdot 18}{2} = 171$ таких произведений, так как $(x+c)(x+d) = (x+d)(x+c)$. Если $c = d$, то их ровно 19. Следовательно, число неприводимых нормированных многочленов равно разности числа всех нормированных многочленов и числа приводимых нормированных многочленов[1)], т. е. равно $19^2 - (\binom{19}{2} + 19) = 171$. □

Аналогично нетрудно установить, что в кольце $\mathbb{Z}_p[x]$ имеется ровно $p^2 - \binom{p+1}{2} = \binom{p}{2} = \frac{p^2-p}{2}$ неприводимых нормированных многочленов второй степени, а значит при достаточно больших p вероятность неприводимости наугад выбранного нормированных квадратного трехчлена близка к $\frac{1}{2}$. В следующем разделе мы убедимся, что найти точное число неприводимых нормированных многочленов степени n даже для больших значений n достаточно просто.

4.6. Число неприводимых многочленов

Число нормированных неприводимых над полем $\mathbb{Z}_p$ многочленов степени n из $\mathbb{Z}_p[x]$ обозначим через $N(p, n)$. Найдем это число, установив ключевой результат — лемму 4.9 — при помощи метода производящих функций[2)].

[1)] Можно было сразу заметить, что число приводимых многочленов вида (4.13) равно числу сочетаний с повторениями из 19 по 2.

[2)] Ниже утверждение леммы 4.9 будет получено без использования производящих функций в разделе 8.2.

Лемма 4.9. *Для последовательности $N(p,n)$ справедливо рекуррентное равенство*

$$p^n = \sum_{m \mid n} mN(p,m). \tag{4.14}$$

Доказательство. Пусть $p_{1m}, p_{2m}, \ldots, p_{N(p,m)m}$ — все неприводимые нормированные многочлены степени m. Нетрудно видеть, что, раскрывая скобки в произведении

$$\prod_{m=1}^{\infty} \prod_{k=1}^{N(p,m)} \left(1 + p_{km} + (p_{km})^2 + \cdots + (p_{km})^l + \ldots\right), \tag{4.15}$$

получим сумму всевозможных произведений неприводимых многочленов, причем каждое произведение встретится в этой сумме ровно один раз. Так как каждый нормированный многочлен единственным образом раскладывается в произведение неприводимых нормированных многочленов, то в рассматриваемой сумме будет содержаться ровно p^n произведений степени n. Каждому неприводимому многочлену степени m поставим в соответствие одночлен x^m, а произведению (4.15) — произведение

$$\begin{aligned}\prod_{m=1}^{\infty} \prod_{k=1}^{N(p,m)} \left(1 + x^m + (x^m)^2 + \ldots + (x^m)^l + \cdots\right) = \\ = \prod_{m=1}^{\infty} \left(\frac{1}{1-x^m}\right)^{N(p,m)}.\end{aligned} \tag{4.16}$$

Так как существует ровно p^n многочленов степени n, у которых коэффициент при x^n равен единице, то легко видеть, что в ряду, получившемся после раскрытия скобок в (4.16), коэффициент при x^n будет равен p^n. Следовательно,

$$\frac{1}{1-px} = \prod_{m=1}^{\infty} \left(\frac{1}{1-x^m}\right)^{N(p,m)}. \tag{4.17}$$

Логарифмируя правую и левую части (4.17), получим новое равенство

$$\ln \frac{1}{1-px} = \sum_{m=1}^{\infty} N(p,m) \ln \frac{1}{1-x^m}.$$

Теперь, применяя формулу $\ln \frac{1}{1-x} = \sum_{n=1}^{\infty} \frac{1}{n} x^n$, разложим в ряд правую и левую части последнего равенства:

$$\sum_{n=1}^{\infty} \frac{1}{n} p^n x^n = \sum_{m=1}^{\infty} \sum_{k=1}^{\infty} \frac{1}{k} N(p,m) x^{km} = \sum_{n=1}^{\infty} \left(\sum_{km=n} \frac{1}{k} N(p,m) \right) x^n.$$

Приравнивая в получившемся равенстве коэффициенты при n-й степени x, находим

$$\frac{1}{n} p^n = \sum_{km=n} \frac{1}{k} N(p,m) = \sum_{m \mid n} \frac{m}{n} N(p,m).$$

Лемма доказана.

Для того чтобы из равенства (4.14) в явном виде выразить функцию $N(p,n)$, воспользуемся формулой обращения Мёбиуса, которую докажем далее в лемме 4.11. Сначала определим *функцию Мёбиуса*

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1; \\ (-1)^k, & \text{если } n \text{ — произведение } k \text{ простых чисел;} \\ 0, & \text{если } n \text{ делится на квадрат простого числа,} \end{cases}$$

и покажем, что имеет место следующее утверждение.

Лемма 4.10. *Справедливо равенство*

$$\sum_{m \mid n} \mu(m) = \begin{cases} 1, & \textit{если } n = 1; \\ 0, & \textit{если } n > 1. \end{cases} \tag{4.18}$$

Доказательство. Если $n = 1$, то единица является единственным делителем, и, следовательно, $\mu(1) = 1$. При $n > 1$ представим n в виде произведения простых чисел: $n = p_1^{q_1} \cdots p_r^{q_r}$. Легко видеть, что в сумме (4.18) нужно учитывать только делители без кратных множителей. Поэтому

$$\sum_{m \mid n} \mu(m) = \sum_{k=0}^{r} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant r} \mu(p_{i_1} \cdots p_{i_k}) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = 0.$$

Лемма доказана.

Лемма 4.11 (Обращение Мёбиуса)**.** *Функции $f(n)$ и $h(n)$, определенные на множестве целых положительных чисел, удовлетворяют равенству*

$$f(n) = \sum_{m \mid n} h(m) \quad \text{при всех } n \in \mathbb{N} \tag{4.19}$$

тогда и только тогда, когда

$$h(n) = \sum_{m \mid n} \mu\Big(\frac{n}{m}\Big) f(m) \quad \text{при всех } n \in \mathbb{N}. \tag{4.20}$$

Доказательство. Покажем, что из (4.19) следует (4.20). Для этого прежде всего заметим, что

$$\sum_{m \mid n} \mu\Big(\frac{n}{m}\Big) f(m) = \sum_{m \mid n} \mu(m) f\Big(\frac{n}{m}\Big),$$

так как суммы, стоящие в обеих частях равенства, отличаются только порядком следования слагаемых. Затем в правую часть последнего равенства вместо $f(m)$ подставим правую часть равенства (4.19). Меняя в получившейся двойной сумме порядок суммирования и применяя лемму 4.10, получим следующую цепочку равенств:

$$\begin{aligned}
\sum_{m \mid n} \mu(m) f\Big(\frac{n}{m}\Big) &= \sum_{m \mid n} \mu(m) \sum_{k \mid \frac{n}{m}} h(k) = \\
&= \sum_{m \mid n} \sum_{k \mid \frac{n}{m}} \mu(m) h(k) = \sum_{km \mid n} \mu(m) h(k) = \\
&= \sum_{k \mid n} \sum_{m \mid \frac{n}{k}} \mu(m) h(k) = \sum_{k \mid n} h(k) \sum_{m \mid \frac{n}{k}} \mu(m) = h(n).
\end{aligned}$$

Таким образом, справедливость равенства (4.20) установлена. Обратное утверждение доказывается аналогично. Лемма доказана.

Теорема 4.13. *Для числа $N(p, n)$ неприводимых многочленов степени n справедливо равенство*

$$N(p, n) = \frac{1}{n} \sum_{m \mid n} \mu\Big(\frac{n}{m}\Big) p^m.$$

Доказательство. Из леммы 4.9 следует, что первое равенство леммы 4.11 справедливо при $f(n) = p^n$ и $h(n) = nN(p, n)$ для всех натуральных n. Поэтому утверждение теоремы следует непосредственно из леммы 4.11. Теорема доказана.

4.7. Кольцо остатков и поле многочленов

Множество многочленов из $\mathbb{Z}_p[x]$ степени не выше $n-1$ с операциями сложения и умножения по модулю многочлена $h(x)$ степени n является кольцом. Оно называется *кольцом остатков* по модулю $h(x)$ и обозначается $\mathbb{Z}_p[x]/h(x)$. Нетрудно видеть, что кольцо $\mathbb{Z}_p[x]/h(x)$ изоморфно фактор-кольцу $\mathbb{K}/I$ кольца $\mathbb{K} = \mathbb{Z}_p[x]$ по идеалу $I = h\mathbb{K}$, образованному всеми многочленами из $\mathbb{Z}_p[x]$, кратными многочлену $h(x)$: элемент $a \in \mathbb{Z}_p[x]/h(x)$ представляет смежный класс $a + I \subset \mathbb{Z}_p[x]$. Очевидно, что кольцо $\mathbb{Z}_p[x]/h(x)$ состоит из p^n элементов, где $n = \deg h(x)$. Также нетрудно видеть, что $\mathbb{Z}_p[x]/h(x)$ содержит в себе $\mathbb{Z}_p$ как подкольцо и является коммутативным кольцом с единицей. Более того, справедлива следующая теорема.

Теорема 4.14. *Пусть p — простое и $h(x)$ — многочлен из $\mathbb{Z}_p[x]$ степени n. Тогда фактор-кольцо $\mathbb{Z}_p[x]/h(x)$ является полем из p^n элементов в том и только в том случае, когда $h(x)$ неприводим над полем $\mathbb{Z}_p$.*

Доказательство. Кольцо $\mathbb{Z}_p[x]/h(x)$ является коммутативным кольцом с единицей и состоит из p^n элементов. Поэтому достаточно показать, что любой ненулевой элемент этого кольца имеет обратный по умножению, если $h(x)$ неприводим. Так как $(f(x), h(x)) = 1$ для любого ненулевого $f(x)$ из $\mathbb{Z}_p[x]/h(x)$, то в силу теоремы 4.10 найдутся такие многочлены $s(x)$ и $t(x)$, что $1 = s(x)f(x) + t(x)h(x)$. Поэтому $f(x)s(x) = 1 \pmod{h(x)}$, т. е. $f(x)$ имеет обратный элемент в $\mathbb{Z}_p[x]/h(x)$.

С другой стороны, если $h(x) = a(x)b(x)$, то $a(x)$ и $b(x)$ являются делителями нуля в кольце $\mathbb{Z}_p[x]/h(x)$ в силу равенства $a(x) \cdot b(x) = 0 \pmod{h(x)}$. Поэтому если многочлен $h(x)$

приводим над $\mathbb{Z}_p$, то кольцо $\mathbb{Z}_p[x]/h(x)$ не является полем. Теорема доказана.

Теорема 4.15. *Для любого простого p и любого натурального n существует конечное поле из p^n элементов.*

Доказательство. Существование поля из p^n элементов для простого p и натурального n легко следует из теоремы 4.14 и существования в $\mathbb{Z}_p[x]$ неприводимого над $\mathbb{Z}_p$ многочлена любой степени n. В свою очередь существование такого многочлена является простым следствием теоремы 4.13 о числе неприводимых многочленов. Действительно, по определению функции Мёбиуса $\mu(\frac{n}{m}) \geqslant -1$ при всех $m \mid n$. Следовательно,

$$N(p,n) = \frac{1}{n}\sum_{m|n}\mu\Big(\frac{n}{m}\Big)p^m \geqslant$$

$$\geqslant \frac{1}{n}\left(\mu(1)\cdot p^n + \sum_{m|n,\ m\neq n}(-1)\cdot p^m\right) \geqslant \frac{1}{n}\left(p^n - \sum_{m=0}^{n-1} p^m\right) =$$

$$= \frac{1}{n}\left(p^n - \frac{p^n-1}{p-1}\right) = \frac{p^{n+1}-2p^n+1}{n(p-1)} \geqslant \frac{1}{n(p-1)} > 0,$$

так как $p^{n+1} \geqslant 2p^n$ в силу того, что $p \geqslant 2$. Мы доказали, что при всех натуральных n и при всех простых p величина $N(p,n)$ положительна. Кроме того, $N(p,n)$ — целое число. Значит, $N(p,n) \geqslant 1$ и неприводимый многочлен степени n найдется в $\mathbb{Z}_p[x]$ при всех n и p. Теорема доказана.

Пример 4.17. Найдем асимптотику числа $N(p,n)$ неприводимых над $\mathbb{Z}_p$ многочленов при $n \to \infty$ и фиксированном простом p. Оценим $N(p,n)$ сверху и снизу функциями с одинаковым асимптотическим поведением. Так, из теоремы 4.13 очевидно следует, что, во-первых, $N(p,n) \leqslant p^n/n$ при всех n и p. Во-вторых,

$$N(p,n) \geqslant \frac{1}{n}\left(p^n - np^{n/2}\right),$$

так как у числа n не больше n делителей, и наибольший сре-

ди них (отличный от n) не превосходит $n/2$. Отсюда следует[1], что $N(p,n) \sim p^n/n$ при $n \to \infty$. $\square$

Замечание 4.1. Отметим, что из того, что $N(p,n) \to \infty$ при $n \to \infty$, не следует, что $N(p,n) > 0$ при всех n, а только при достаточно больших n. Иными словами, теорема 4.15 не является следствием рассмотренного выше примера.

Замечание 4.2. Пусть $n > 1$ и $h(x) = a_n x^n + \ldots + a_1 x + a_0$ — произвольный многочлен над $\mathbb{Z}_p$, не обязательно неприводимый. Рассмотрим фактор-кольцо $\mathbb{K} = \mathbb{Z}_p[x]/h(x)$ и его элемент — вычет[2] $[x] = [x]_h$. Подставим $[x]$ в многочлен $h(x)$ в качестве аргумента — это действие корректно, так как поле $\mathbb{Z}_p$ коэффициентов многочлена $h(x)$ изоморфно вложено[3] в $\mathbb{K}$:

$$\begin{aligned} h([x]) &= a_n[x]^n + a_{n-1}[x]^{n-1} + \ldots + a_1[x] + a_0 = \\ &= [a_n][x]^n + [a_{n-1}][x]^{n-1} + \ldots + [a_1][x] + [a_0] = \\ &= [a_n x^n + \ldots + a_1 x + a_0] = [f(x)] = [0]. \end{aligned}$$

Мы видим, что значение $h([x])$ является нулем кольца $\mathbb{K}$. Таким образом, каким бы ни был многочлен h, вычет $[x]$ является его *корнем* в кольце остатков по модулю h и вдобавок самым «просто устроенным» корнем среди всех остатков. Поэтому определение корня многочлена, данное на стр. 98, может быть естественным образом обобщено с кольца его коэффициентов на другие алгебраические структуры.

---

[1] Напомним, что запись $f_n \sim g_n$ при $n \to \infty$ означает, что существует предел $\lim_{n\to\infty} f_n/g_n = 1$. Согласно известной теореме из анализа (мажоритарный признак сходимости последовательностей), если последовательности a_n, b_n и c_n таковы, что $a_n \sim c_n$ и $a_n \leqslant b_n \leqslant c_n$ при всех n, начиная с некоторого n_0, то $b_n \sim a_n$ и $b_n \sim c_n$.

[2] Элементы кольца остатков $\mathbb{Z}_p[x]/h(x)$ иногда обозначаются $[g]_h$ по аналогии с вычетами из $\mathbb{Z}_n$ (стр. 41), чтобы подчеркнуть, по какому модулю берется вычет g. Также запись в квадратных скобках используется вместо обозначающей остаток по модулю записи $g \pmod n$ или $g \pmod h$ для компактности, например $[-5]_3 = 1$. Обычно, однако, квадратные скобки и индексы к ним опускаются, когда модуль и природа аргумента ясны из контекста.

[3] Изоморфизм $\mathbb{Z}_p$ с подкольцом в $\mathbb{K}$ определен равенством $\varphi(a) = [a]_h$.

Теорема 4.14 позволяет задавать конечные поля в явном виде и выполнять в этих полях операции сложения и умножения. Для задания поля из p^n элементов выберем в $\mathbb{Z}_p[x]$ неприводимый над $\mathbb{Z}_p$ многочлен n-й степени $h(x)$. Элементы поля будем представлять в виде упорядоченных наборов $(a_{n-1},\dots,a_0)$ длины n с элементами из $\mathbb{Z}_p$. При этом операция сложения выполняется покомпонентно, а для умножения элементов $a = (a_{n-1},\dots,a_0)$ и $b = (b_{n-1},\dots,b_0)$ надо вычислить произведение $r(x) = r_{n-1}x^{n-1} + \dots + r_0$ многочленов $a(x) = a_{n-1}x^{n-1} + \dots + a_0$ и $b(x) = b_{n-1}x^{n-1} + \dots + b_0$ по модулю многочлена $h(x)$ и в качестве произведения ab взять набор $(r_{n-1},\dots,r_0)$ коэффициентов многочлена $r(x)$.

Пример 4.18. Построим поле $\mathbb{F}$ из 27 элементов. Для этого понадобится неприводимый нормированный многочлен третьей степени из $\mathbb{Z}_3[x]$. Так как любой приводимый многочлен третьей степени над $\mathbb{Z}_3$ имеет корень в $\mathbb{Z}_3$, то многочлен $x(x+1)(x+2)+1 = x^3+2x+1$ будет неприводимым над $\mathbb{Z}_3$. Поэтому в качестве поля $\mathbb{F}$ можно взять фактор-кольцо $\mathbb{Z}_3[x]/(x^3+2x+1)$. Элементы такого поля удобно представлять наборами коэффициентов многочленов $a_2x^2+a_1x+a_0$ из $\mathbb{Z}_3[x]/(x^3+2x+1)$, т. е. наборами вида $(a_2a_1a_0)$, где $a_i \in \mathbb{Z}_3$. Найдем сумму и произведение элементов $(\mathtt{111})$ и $(\mathtt{220})$. Легко видеть, что $(\mathtt{111}) + (\mathtt{220}) = (\mathtt{001})$. Далее, так как

$$(x^2+x+1)(2x^2+2x) = 2x^4+x^3+x^2+2x = \\ = (x^3+2x+1)(2x+1)+(x+2),$$

то $(\mathtt{111})\cdot(\mathtt{220}) = (\mathtt{012})$. □

4.8. Китайская теорема об остатках для многочленов

Доказательство теоремы 4.14 указывает удобный способ нахождения обратного элемента в $\mathbb{K} = \mathbb{Z}_p[x]/h(x)$ не только в том случае, когда многочлен $h(x)$ неприводим, но и когда этот многочлен приводим, а кольцо $\mathbb{K}$ не является полем. В частности,

$f(x) \in \mathbb{K}$ обратим, т. е. $f(x) \in \mathbb{K}^*$, тогда и только тогда, когда найдутся многочлены $s(x), t(x)$ такие, что в кольце $\mathbb{Z}_p[x]$ выполнено равенство

$$s(x)f(x) + t(x)h(x) = 1. \tag{4.21}$$

Установить такие $s(x), t(x)$ или доказать их отсутствие, а значит и необратимость $f(x)$, помогает алгоритм Евклида (см. с. 109).

Действительно, для любых многочленов $f(x), h(x) \in \mathbb{Z}_p[x]$ этот алгоритм находит нормированный наибольший общий делитель $d(x) = (f, h)$ и коэффициенты Безу $s'(x), t'(x)$, так что

$$s'(x)f(x) + t'(x)h(x) = d(x).$$

Если $d(x) \neq 1$, то это противоречит равенству (4.21), так как его левая часть делится на $d(x)$, а значит $f(x) \notin \mathbb{K}^*$. Иначе, рассмотрев остатки от деления обеих частей (4.21) на $h(x)$, имеем $s(x)f(x) = 1 \pmod{h(x)}$, а значит $f^{-1}(x) = s(x) \pmod{h(x)}$.

Пример 4.19. Полученное на с. 110 в кольце $\mathbb{Z}_3[x]$ тождество

$$\mathtt{122011} \cdot \mathtt{1201} + \mathtt{10122} \cdot \mathtt{22110} = \mathtt{1}$$

показывает, что вычет $f(x) = \mathtt{10122}$ обратим в кольце $\mathbb{K} = \mathbb{Z}_3[x]/h(x)$, где $h(x) = \mathtt{122011}$, причем $f^{-1}(x) = \mathtt{22110}$. Нетрудно также убедиться, что $\text{НОД}\,(\mathtt{122011}, \mathtt{1111}) = \mathtt{101} \neq \mathtt{1}$, поэтому вычет $\mathtt{1111}$ не имеет обратного в $\mathbb{K}$. Так как $\mathtt{122011} = \mathtt{101} \cdot \mathtt{1211}$, где многочлены $a(x) = \mathtt{101}$ и $b(x) = \mathtt{1211}$ неприводимы над $\mathbb{Z}_3$, то делителями нуля в $\mathbb{K}$ будут кратные $a(x)$ или $b(x)$ вычеты, и других делителей нуля в $\mathbb{K}$ нет. □

Другой способ производить арифметические действия в фактор-кольце $\mathbb{K} = \mathbb{Z}_p[x]/h(x)$ при составном модуле $h(x)$ описан ниже в данном разделе. Он основан на строении кольца $\mathbb{K}$, и в его основе лежит следующая теорема, называемая китайской теоремой об остатках для многочленов.

Теорема 4.16. *Пусть $m_1(x), \ldots, m_n(x)$ — попарно взаимно простые многочлены над полем $\mathbb{F}$, $M(x) = m_1(x) \cdots m_n(x)$ — их произведение, $a_1(x), \ldots, a_n(x)$ — такие многочлены над полем $\mathbb{F}$,*

что $\deg a_i(x) < \deg m_i(x)$. *Единственным решением системы сравнений*

$$\left.\begin{aligned} b(x) &= a_1(x) \pmod{m_1(x)},\\ b(x) &= a_2(x) \pmod{m_2(x)},\\ &\dots\dots\dots\dots\dots\dots\dots\\ b(x) &= a_n(x) \pmod{m_n(x)}, \end{aligned}\right\} \tag{4.22}$$

в кольце $\mathbb{F}[x]/M(x)$ *является многочлен*

$$b_0(x) = \Bigl(\sum_{i=1}^{n} a_i(x)M_i(x)N_i(x)\Bigr) \pmod{M(x)}, \tag{4.23}$$

где $M_i(x) = M(x)/m_i(x)$ *и* $N_i(x)M_i(x) = 1 \pmod{m_i(x)}$ *для* $i = 1, 2, \dots, n$.

Доказательство. Допустим, что система (4.22) имеет два различных решения $c(x)$ и $d(x) \in \mathbb{F}[x]/M(x)$. В этом случае их разность $\hat{b}(x) = c(x) - d(x) \neq 0$ удовлетворяет неравенствам

$$0 \leqslant \deg \hat{b}(x) < \deg M(x) \tag{4.24}$$

и является решением системы сравнений

$$\left.\begin{aligned} \hat{b}(x) &= 0 \pmod{m_1},\\ \hat{b}(x) &= 0 \pmod{m_2},\\ &\dots\dots\dots\dots\dots\dots\\ \hat{b}(x) &= 0 \pmod{m_n}. \end{aligned}\right\} \tag{4.25}$$

Из (4.25) следует, что каждое $m_i(x)$ делит $c(x) - d(x)$ и, следовательно, входит в разложение $c(x) - d(x)$ на неприводимые многочлены. Поэтому $\deg(c(x) - d(x)) \geqslant \deg M(x)$, что противоречит (4.24). Таким образом, каждая система вида (4.22) имеет не более одного решения в кольце $\mathbb{F}[x]/M(x)$.

Найдем это решение. Прежде всего отметим, что многочлены $M_i(x)$ и $m_i(x)$ взаимно простые. Поэтому в силу теоремы 4.10 существует такой многочлен $N_i(x)$, что

$$M_i(x)N_i(x) = 1 \pmod{m_i(x)}.$$

Так как

$$b(x) \pmod{m_i(x)} = (b(x) \pmod{M(x)}) \pmod{m_i(x)}$$

для любого $b(x)$ и каждого $i = 1, 2, \ldots, n$, и, кроме того, в силу условий теоремы

$$M_j(x) = 0 \pmod{m_i(x)} \quad \text{при } i \neq j,$$

то легко видеть, что многочлен $b_0(x)$, определяемый формулой (4.23), действительно является решением рассматриваемой системы сравнений. Теорема доказана.

Пример 4.20. Найдем решение системы над полем $\mathbb{Z}_5$:

$$\left.\begin{aligned} b(x) &= 4 \pmod{x+1}, \\ b(x) &= 1 \pmod{x+2}, \\ b(x) &= 2 \pmod{x+3}. \end{aligned}\right\}$$

Очевидно, что двучлены $x+1$, $x+2$ и $x+3$ попарно взаимно просты. Тогда по теореме 4.16 имеем

$$b(x) = 4 \cdot M_1 \cdot N_1 + 1 \cdot M_2 \cdot N_2 + 2 \cdot M_3 \cdot N_3 \pmod{M(x)},$$

где $M(x) = (x+1)(x+2)(x+3) = x^3 + x^2 + x + 1$ и

$$\begin{aligned} M_1(x) &= (x+2)(x+3) = x^2 + 1, \\ M_2(x) &= (x+1)(x+3) = x^2 + 4x + 3, \\ M_3(x) &= (x+1)(x+2) = x^2 + 3x + 2. \end{aligned}$$

Как следует из доказательства теоремы 4.16, многочлен N_i является обратным к многочлену M_i по модулю m_i, а каждый многочлен m_i в данном случае имеет вид $x - a$ для некоторого $a \in \mathbb{Z}_5$. Поэтому можно воспользоваться теоремой Безу и найти

$$\begin{aligned} M_1(x) &= M(-1) = 2 \pmod{x+1}, \\ M_2(x) &= M(-2) = 4 \pmod{x+2}, \\ M_3(x) &= M(-3) = 2 \pmod{x+3}, \end{aligned}$$

откуда в силу изоморфизма $\mathbb{Z}_5[x]/(x-a) \cong \mathbb{Z}_5$ следует, что $N_1 = N_3 = 2^{-1} = 3 \pmod 5$ и $N_2 = 4^{-1} = 4 \pmod 5$. Отсюда получаем ответ

$$\begin{aligned} b(x) &= 4\cdot 3\cdot (x+2)(x+3) + 1\cdot 4\cdot (x+1)(x+3) + \\ &\qquad + 2\cdot 3\cdot (x+1)(x+2) = \\ &= 2(x^2+1) + 4(x^2+4x+3) + (x^2+3x+2) = 2x^2+4x+1. \end{aligned}$$

Таким образом, $b(x) = 2x^2+4x+1$ является единственным решением системы в кольце $\mathbb{Z}_5[x]/M(x)$, а в кольце $\mathbb{Z}_5[x]$ система имеет бесконечно много решений вида $b(x) + c(x)\cdot M(x)$, где $c(x)$ — произвольный многочлен из кольца $\mathbb{Z}_5[x]$. Проверить найденный ответ можно также с помощью теоремы Безу: нетрудно видеть, что действительно $b(-1) = 4$, $b(-2) = 1$, $b(-3) = 2$. □

Пример 4.21. Решим в кольце многочленов $\mathbb{Z}_2[x]$ систему сравнений

$$\left.\begin{aligned} b(x) &= \mathtt{10} \pmod{\mathtt{111}},\\ b(x) &= \mathtt{101} \pmod{\mathtt{1101}},\\ b(x) &= \mathtt{1111} \pmod{\mathtt{10011}}. \end{aligned}\right\}$$

Многочлены $m_1(x) = \mathtt{111} = x^2+x+1$, $m_2(x) = \mathtt{1101} = x^3+x^2+1$, $m_3(x) = \mathtt{10011} = x^4+x+1$ неприводимы над $\mathbb{Z}_2$ (см. с. 113) и, следовательно, взаимно просты. Применим теорему 4.16. Последовательно находим:

$$M(x) = \mathtt{1001010101}, \quad M_1(x) = \mathtt{11000111},$$

$$M_2(x) = \mathtt{1111001}, \quad M_3(x) = \mathtt{100011}.$$

Далее находим $M_1(x) = \mathtt{11} (\mathrm{mod}\, m_1(x))$, $M_2(x) = \mathtt{110} (\mathrm{mod}\, m_2(x))$ и $M_3(x) = \mathtt{101} (\mathrm{mod}\, m_3(x))$. Отсюда

$$\begin{aligned} N_1(x) &= M_1(x)^{-1} = \mathtt{10} \pmod{m_1(x)},\\ N_2(x) &= M_2(x)^{-1} = \mathtt{10} \pmod{m_2(x)},\\ N_3(x) &= M_3(x)^{-1} = \mathtt{1011} \pmod{m_3(x)}. \end{aligned}$$

Последние равенства были получены с помощью алгоритма Евклида. Подставляя полученные значения в формулу (4.23), находим

$$\begin{aligned} b(x) &= a_1(x)\cdot M_1(x)\cdot N_1(x) + a_2(x)\cdot M_2(x)\cdot N_2(x) + \\ &\qquad + a_3(x)\cdot M_3(x)\cdot N_3(x) = \\ &= a_1(x)\cdot \mathtt{110001110} + a_2(x)\cdot \mathtt{11110010} + a_3(x)\cdot \mathtt{101111101} = \\ &= \mathtt{110110111101} = \mathtt{1000011} (\mathrm{mod}\, M(x)). \end{aligned}$$

Следовательно, многочлен $b(x) = \mathtt{1000011}$ является единственным решением рассматриваемой системы в кольце $\mathbb{Z}_2[x]/M(x)$. Множество ее решений в кольце $\mathbb{Z}_2[x]$ выражается формулой $b(x) = \mathtt{1000011} + c(x)\cdot M(x)$, где $c(x) \in \mathbb{Z}_2[x]$ — произвольный многочлен. □

Китайская теорема об остатках для кольца многочленов (теорема 4.16) имеет следствие, аналогичное теореме 3.17 для колец числовых вычетов (и аналогично доказываемое), которое удобно формулировать на языке изоморфизмов и прямых сумм.

Теорема 4.17. *Пусть $g(x)$ и $h(x)$ — произвольные многочлены положительной степени из $\mathbb{Z}_p[x]$. Если $g(x)$ и $h(x)$ взаимно просты, то фактор-кольцо $\mathbb{Z}_p[x]/f(x)$, где $f(x) = g(x)\cdot h(x)$, изоморфно прямой сумме фактор-колец $\mathbb{Z}_p[x]/g(x)$ и $\mathbb{Z}_p[x]/h(x)$.*

Заметим, что если $(g, h) \neq 1$, то последнее утверждение, вообще говоря, неверно.

Итак, пусть $M(x) = m_1(x)\cdots m_n(x)$ — разложение многочлена $M(x) \in \mathbb{Z}_p[x]$ в произведение различных взаимно простых многочленов $m_i(x)$. Тогда, применяя по индукции теорему 4.17, получим

$$\mathbb{Z}_p[x]/M(x) \cong \mathbb{Z}_p[x]/m_1(x) \otimes \cdots \otimes \mathbb{Z}_p[x]/m_n(x). \tag{4.26}$$

Каждый элемент $b(x)$ кольца $\mathbb{Z}_p[x]/M(x)$ однозначно определяется системой остатков $a_1(x), \ldots, a_n(x)$ по формулам (4.22) и (4.23). Для сокращения запишем это одним из двух следующих способов:

$$b = [a_1, \ldots, a_n]_{m_1,\ldots,m_n} \quad \text{или} \quad b = [a_1, \ldots, a_n]_M,$$

причем будем опускать внешние индексы в случае, когда из контекста ясно, по какой системе взаимно простых делителей какого многочлена представлен вычет b. Данное представление гомоморфно (сохраняет обе операции кольца $\mathbb{Z}_p[x]/M$), т. е. если $b = [a_1, \ldots, a_n]$ и $b' = [a'_1, \ldots, a'_n]$, то

$$b + b' = [a_1 + a'_1, \ldots, a_n + a'_n], \qquad b \cdot b' = [a_1 \cdot a'_1, \ldots, a_n \cdot a'_n].$$

Подчеркнем, что здесь в i-й компоненте $a_i \circ a'_i$ упорядоченного набора $[a_1 \circ a'_1, \ldots, a_n \circ a'_n]$ используется операция $\circ \in \{+, \cdot\}$ кольца $\mathbb{Z}_p[x]/m_i$. Будем называть такое представление вычетов кольца $\mathbb{Z}_p[x]/M(x)$ *представлением системой остатков*.

Представление многочленов системой остатков имеет много полезных следствий. Изоморфизм колец (4.26) влечет изоморфизм их мультипликативных групп. В частности, элемент $b = [a_1, \ldots, a_n]$ обратим по умножению тогда и только тогда, когда обратимы все a_i, причем $b^{-1} = [a_1^{-1}, \ldots, a_n^{-1}]$, где обратный к a_i вычет берется в кольце $\mathbb{Z}_p[x]/m_i$. При всяком $l \in \mathbb{Z}$ справедливо и более общее свойство $b^l = [a_1^l, \ldots, a_n^l]$. Поэтому (лемма 3.2) мультипликативный порядок элемента $b \in (\mathbb{Z}_p[x]/M)^*$ равен наименьшему общему кратному порядков элементов $a_i \in$ $\in (\mathbb{Z}_p[x]/m_i)^*$.

Пример 4.22. Как мы убедились в примере 4.20, над полем $\mathbb{Z}_5$ справедливо равенство $2x^2 + 4x + 1 = [4, 1, 2]_{x+1, x+2, x+3}$. Легко также видеть, что $3x + 2 = [4, 1, 3]$. Поэтому разность $2x^2 + x + 4$ многочленов $2x^2 + 4x + 1$ и $3x + 2$ представляется системой остатков

$$[4, 1, 2] - [4, 1, 3] = [4 - 4, 1 - 1, 2 - 3] = [0, 0, 4],$$

а их произведение $[4, 1, 2] \cdot [4, 1, 3] = [4 \cdot 4, 1 \cdot 1, 2 \cdot 3] = [1, 1, 1]$ равно единице, т. е. эти многочлены являются взаимно обратными вычетами в кольце $\mathbb{Z}_5[x]/(x + 1)(x + 2)(x + 3)$. □

Пример 4.23. Рассмотрим кольцо вычетов $\mathbb{Z}_n$ по составному модулю $n = ab$, где $a, b > 1$. Если $(a, b) = 1$, то, согласно теореме 4.3, $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \otimes \mathbb{Z}_b$. Следовательно, $\mathbb{Z}_{ab}^* \cong \mathbb{Z}_a^* \times \mathbb{Z}_b^*$. Число обратимых по модулю n вычетов совпадает с порядком группы $\mathbb{Z}_n^*$ и равно $\varphi(n)$, где φ — функция Эйлера. Число элементов

в прямом произведении $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ равно $\varphi(a)\varphi(b)$. Таким образом, мы убедились в мультипликативности функции Эйлера, т. е. в равенстве $\varphi(ab) = \varphi(a)\varphi(b)$ при $(a, b) = 1$, независимо от леммы 2.5. □

Пример 4.24. Порядок мультипликативной группы кольца $\mathbb{Z}_{91} \cong \mathbb{Z}_7 \otimes \mathbb{Z}_{13}$ равен $\varphi(91) = \varphi(7) \cdot \varphi(13) = 6 \cdot 12 = 72$. Поэтому $x^{72} = 1 \pmod{91}$ для любого $x \in \mathbb{Z}_{91}^*$ по теореме Эйлера (теорема 2.13). Воспользуемся изоморфизмом $\mathbb{Z}_{91}^* \cong \mathbb{Z}_7^* \times \mathbb{Z}_{13}^*$ и рассмотрим элемент $x = (x_1, x_2) \in \mathbb{Z}_7^* \times \mathbb{Z}_{13}^*$. Заметим, что $x_1^6 = 1 \pmod 7$ и $x_2^{12} = 1 \pmod{13}$, поэтому порядки элементов $x_1 \in \mathbb{Z}_7^*$ и $x_2 \in \mathbb{Z}_{13}^*$ являются делителями чисел 6 и 12 соответственно. Порядок элемента $x = (x_1, x_2)$ равен наименьшему общему кратному порядков элементов x_1 и x_2, причем $\text{НОК}(6, 12) = 12$. Следовательно, в данном случае теорема Эйлера может быть немного усилена: в действительности $x^{12} = 1 \pmod{91}$ для любого x взаимно простого с 91.

Аналогичным образом нетрудно установить, что $x^{\psi(n)} = 1 \pmod n$, где $\psi(n)$ равно наименьшему общему кратному чисел $\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1}$, если $n = p_1^{k_1} \dots p_s^{k_s}$ и $(x, n) = 1$. □

Пример 4.25. В примере 4.21 было показано, что

$$\texttt{1000011} = [\texttt{10},\ \texttt{101},\ \texttt{1111}]_{M(x)},$$

где $M(x) = \texttt{111} \cdot \texttt{1101} \cdot \texttt{10011} = \texttt{1001010101}$. Порядок мультипликативной группы $\mathbb{K}^*$ кольца $\mathbb{K} = \mathbb{Z}_p[x]/M(x)$ равен $3 \cdot 7 \times$ $\times 15 = 315$ в силу неприводимости многочленов $\texttt{111}, \texttt{1101}, \texttt{10011}$. Нетрудно убедиться, что порядки элементов $\texttt{10}$, $\texttt{101}$ и $\texttt{1111}$ в мультипликативных группах полей $\mathbb{Z}_p[x]/(\texttt{111})$, $\mathbb{Z}_p[x]/(\texttt{1101})$ и $\mathbb{Z}_p[x]/(\texttt{10011})$ равны 3, 7 и 5 соответственно. Поэтому порядок элемента $\texttt{1000011} \in \mathbb{K}^*$ равен $\text{НОК}(3, 7, 5) = 105$ и является максимально возможным в $\mathbb{K}^*$. □

Аналогичные китайской теореме об остатках утверждения справедливы для многих колец и идеалов[1)]. Подобные факты ценны тем, что помогают свести изучение составного кольца, например кольца $\mathbb{Z}_{p_1^{k_1} \dots p_s^{k_s}}$, к изучению более просто[2)] устро-

[1)] См., например [23].

[2)] Строению кольца $\mathbb{Z}_n$ посвящен раздел 7.5.

енных колец типа $\mathbb{Z}_{p^k}$. В частности, справедливо, что $\mathbb{Z}_{300} \cong$ $\cong \mathbb{Z}_{2^2} \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_{5^2}$, однако $\mathbb{Z}_{300} \ncong \mathbb{Z}_{15} \otimes \mathbb{Z}_{20}$.

Теорема 4.18 (интерполяционная теорема Лагранжа)**.** *Пусть* $\mathbb{F}$ *— поле,* $f(x) \in \mathbb{F}[x]$ *и* $x_0, x_1, \ldots, x_n \in \mathbb{F}$, $x_i \neq x_j$ *— попарно различные элементы поля* $\mathbb{F}$. *Пусть* $\deg f = n$ *и известны значения многочлена* f *в* $n+1$ *точках:*

$$f(x_0) = y_0,\ f(x_1) = y_1, \ldots,\ f(x_n) = y_n,$$

тогда

$$f(x) = \sum_{i=0}^{n} y_i \frac{(x-x_0)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_n)}{(x_i-x_0)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)}. \tag{4.27}$$

Равенство (4.27) называется *интерполяционной формулой Лагранжа*, а многочлен в его правой части — *интерполяционным полиномом Лагранжа*.

Доказательство. По теореме Безу $f(x_i) = y_i$ тогда и только тогда, когда

$$f(x) = y_i \pmod{(x-x_i)}. \tag{4.28}$$

Многочлены $m_i(x) = x - x_i$ попарно взаимно просты, поэтому, применяя к системе равенств (4.28) при $0 \leqslant i \leqslant n$ китайскую теорему об остатках, можно найти $f(x)$. Действительно, в обозначениях теоремы 4.16

$$a_i(x) = y_i \in \mathbb{F},\ M(x) = \prod_{k=0}^{n}(x-x_k),\ M_i(x) = \prod_{k\neq i}^{n}(x-x_k) = \frac{M(x)}{x-x_i},$$

причем $N_i(x)M_i(x) = 1 \pmod{(x-x_i)}$, откуда с учетом того, что $M_i(x) = M_i(x_i) \pmod{(x-x_i)}$ и $M_i(x_i) \neq 0$, следует, что $N_i(x) =$ $= M_i(x_i)^{-1}$, т. е. многочлен $N_i(x)$ является некоторой константой из $\mathbb{F}$. Применяя формулу (4.23), имеем

$$f(x) = \sum_{i=0}^{n} y_i \frac{M_i(x)}{M_i(x_i)} = \sum_{i=0}^{n} y_i \prod_{j\neq i} \frac{x-x_j}{x_i-x_j},$$

так как степень каждого ее слагаемого $a_i(x)M_i(x)N_i(x)$ строго меньше степени многочлена $M(x)$. Под делением в поле, как обычно, понимается умножение делимого на обратный к делителю элемент. Теорема доказана.

Следствие 4.2. *Любой многочлен степени n над полем $\mathbb{F}$ однозначно определяется своими значениями в $n+1$ различных точках поля $\mathbb{F}$.*

Последнее утверждение имеет естественное ограничение: в поле $\mathbb{F}$ должно быть не менее $n+1$ элементов.

Пример 4.26. Найдем многочлен $f(x)$ наименьшей степени над полем $\mathbb{Z}_7$, принимающий значения $2, 6, 3$ в точках $1, 2, 3$ соответственно. Из формулы (4.27) получаем

$$f(x) = 2\cdot\frac{(x-2)(x-3)}{(1-2)(1-3)} + 6\cdot\frac{(x-1)(x-3)}{(2-1)(2-3)} + 3\cdot\frac{(x-1)(x-2)}{(3-1)(3-2)} =$$
$$= (x^2+2x+6) + (x^2+3x+3) + 5(x^2+4x+2) = 4x+5,$$

где деление в поле $\mathbb{Z}_7$ — это умножение на обратный вычет. □

Задачи

4.1. Будет ли множество $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ с обычными операциями сложения и умножения кольцом? Полем?

4.2. Показать, что любой гомоморфизм поля будет либо изоморфизмом, либо будет отображать все элементы поля в нулевой элемент.

4.3. Доказать, что над полем $\mathbb{F}$ множество всех линейных функций вида $ax+b$, $a \neq 0$ образует группу относительно операции суперпозиции. Найти ее порядок при $|\mathbb{F}| = q$ и исследовать ее структуру (коммутативность, цикличность, система образующих и пр.).

4.4. Доказать, что если идеал кольца содержит обратимый элемент, то он совпадает со всем кольцом.

4.5. Образуют ли идеал необратимые элементы кольца 1) $\mathbb{Z}$, 2) $\mathbb{Z}_n$, 3) $\mathbb{Z}_p[x]$, 4) $\mathbb{R}[x]$, 5) $\mathbb{C}[x]$?

4.6. Доказать, что при любых простом p, натуральном n и $h(x) \in \mathbb{Z}_p[x]$ все идеалы в кольцах $\mathbb{Z}$, $n\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Z}_p[x]$ и $\mathbb{Z}_p[x]/h(x)$ — главные.

4.7. Доказать, что кольцо $\mathbb{Z}[x]$ и кольцо $\mathbb{Z}_2[x, y]$, состоящее из всевозможных многочленов от двух переменных x, y с коэффициентами из $\mathbb{Z}_2$, не являются кольцами главных идеалов.

4.8. На стр. 97 была отмечена схожесть идеалов с нормальными подгруппами. Показать, что аналогично тому, как образ гомоморфизма групп является подгруппой (не обязательно нормальной), так и образ гомоморфизма колец является подкольцом (но уже не обязательно идеалом).

4.9. Найти все гомоморфизмы колец 1) $\mathbb{Z} \to m\mathbb{Z}$, 2) $2\mathbb{Z} \to 2\mathbb{Z}$, 3) $2\mathbb{Z} \to 3\mathbb{Z}$, 4) $\mathbb{Z}_n \to \mathbb{Z}_m$.

4.10. Останется ли верной теорема 4.8, если $\mathbb{F}$ — кольцо без делителей нуля, не являющееся полем?

4.11. Доказать леммы 4.6 и 4.7.

4.12. Доказать теорему 4.17.

4.13. Определить, изоморфны ли фактор-кольца $\mathbb{Z}_2[x]/(x^3+1)$ и $\mathbb{Z}_2[x]/(x^3+x+1)$.

4.14. Пусть $f(x) = \sum_{k=0}^{n} a_k x^k$ — неприводимый многочлен над $\mathbb{Z}_2$. Показать, что многочлен $\sum_{k=0}^{n} a_k x^{n-k}$ неприводим.

4.15. Найти число правильных несократимых дробей со знаменателем $f(x) = x^8 + x^7 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$.

4.16. Найти с помощью расширенного алгоритма Евклида для кольца многочленов обратный вычет к вычету $x^4 + x^3 + 2$ в кольце $\mathbb{Z}_3[x]/f(x)$, где $f(x) = x^6 + 2x^3 + x^2 + 2$.

4.17. Доказать, что если многочлен $f(x)$ неприводим над $\mathbb{Z}_p$, то многочлен $f(ax+b)$ также неприводим при всех $a, b \in \mathbb{Z}_p$, $a \neq 0$.

4.18. Показать, что в целостном кольце наибольший общий делитель определен однозначно с точностью до обратимого множителя.

4.19. Показать, что в евклидовом кольце для любых ненулевых элементов a и b существует их наибольший общий делитель d, который можно представить в виде $d = au + bv$, где u и v — элементы кольца.

4.20. Доказать факториальность произвольного евклидова кольца.

4.21. Показать, что всякое евклидово кольцо является кольцом главных идеалов.

4.22. В кольце $2\mathbb{Z}$ привести примеры элементов с неединственным разложением на простые элементы.

4.23. Является ли определенная на стр. 129 функция $\psi(n)$ мультипликативной, т. е. верно ли, что $\psi(ab) = \psi(a)\psi(b)$ при $(a, b) = 1$?

4.24. Доказать, что функция Мёбиуса $\mu(n)$ так же, как и функция Эйлера $\varphi(n)$, мультипликативна, т. е. что $\mu(ab) = \mu(a)\mu(b)$ для всех взаимно простых натуральных a и b. Доказать, что при всех $n \in \mathbb{N}$

$$\varphi(n) = n\sum_{m|n}\frac{\mu(m)}{m}, \qquad \sum_{m|n}\mu(m)\varphi(m) = \begin{cases}1, n = 1,\\ 0, n \geqslant 2.\end{cases}$$

4.25. Доказать мультипликативный вариант формулы Мёбиуса (ср. с леммой 4.11): функции $f : \mathbb{N} \to \mathbb{R}$ и $h : \mathbb{N} \to \mathbb{R}$ удовлетворяют равенству $f(n) = \prod_{m|n} h(m)$ при всех $n \in \mathbb{N}$ тогда и только тогда, когда при всех $n \in \mathbb{N}$ выполнено равенство

$$h(n) = \prod_{m|n} f(m)^{\mu\left(\frac{n}{m}\right)}.$$

Данное утверждение справедливо и для функций $f, h : \mathbb{N} \to G$, где G — произвольная абелева группа с операцией, обозначаемой умножением.

4.26. Доказать, что произведение всех нормированных неприводимых над $\mathbb{Z}_p$ многочленов степени n равно $\prod_{m|n}(x^{p^m} - x)^{\mu\left(\frac{n}{m}\right)}$.

4.27. (Обобщенная китайская теорема об остатках.) Пусть $\mathbb{K}$ — коммутативное кольцо с единицей, а $I, J \subset \mathbb{K}$ — такие его идеалы, что $I + J = \mathbb{K}$. Доказать, что произведение IJ является тогда пересечением $I \cap J$, а также что $\mathbb{K}/(IJ) \cong \mathbb{K}/I \otimes \mathbb{K}/J$. Более того, изоморфизм $\varphi : \mathbb{K}/I \otimes \mathbb{K}/J \to \mathbb{K}/(IJ)$ можно задать равенством $\varphi(x, y) = ix + jy$, где элементы $i \in I$, $j \in J$ таковы, что $i + j = 1$.

Глава 5

Линейные пространства

Возникшая при взаимодействии физики, геометрии и математического анализа теория линейных (векторных) пространств успешно используется практически во всех непрерывных разделах современной математики. Не менее эффективно линейные пространства можно использовать и при изучении дискретных объектов, в частности конечных полей. В этой главе вводятся основные понятия теории линейных пространств и устанавливается ряд ее фундаментальных результатов, необходимых для различных приложений этой теории.

5.1. Линейные пространства и их свойства

Множество $\mathbb{V}$ с операциями сложения и умножения на элементы поля $\mathbb{F}$ называется *линейным (векторным) пространством над полем* $\mathbb{F}$, если:

(1) $\mathbb{V}$ — абелева группа относительно операции сложения;

(2) $\alpha(\boldsymbol{v}+\boldsymbol{w}) = \alpha\boldsymbol{v} + \alpha\boldsymbol{w}$ для любых $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{V}$ и $\alpha \in \mathbb{F}$;

(3) $(\alpha+\beta)\boldsymbol{v} = \alpha\boldsymbol{v} + \beta\boldsymbol{v}$ для любых $\boldsymbol{v} \in \mathbb{V}$ и $\alpha, \beta \in \mathbb{F}$;

(4) $(\alpha\beta)\boldsymbol{v} = \alpha(\beta\boldsymbol{v})$ для любых $\boldsymbol{v} \in \mathbb{V}$ и $\alpha, \beta \in \mathbb{F}$;

(5) $1\boldsymbol{v} = \boldsymbol{v}$ для любого $\boldsymbol{v} \in \mathbb{V}$ и единицы 1 поля $\mathbb{F}$.

Элементы линейного пространства называются *векторами*, нейтральный элемент группы называется *нулевым вектором*.

Рассмотрим некоторые примеры линейных пространств.

Пример 5.1. На множестве наборов из $\mathbb{F}^n$ введем две операции: операцию покомпонентного сложения «+», отображающую

наборы $\boldsymbol{u}$ и $\boldsymbol{v}$ в их сумму $\boldsymbol{u}+\boldsymbol{v}$, и операцию покомпонентного умножения «$\cdot$» набора на константу из $\mathbb{F}$. Для i-х разрядов суммы $\boldsymbol{u}+\boldsymbol{v}$ и произведения $\alpha\cdot\boldsymbol{u}$ $(i=1,2,\ldots,n)$ положим

$$(\boldsymbol{u}+\boldsymbol{v})_i = u_i + v_i, \quad (\alpha\cdot\boldsymbol{u})_i = \alpha u_i.$$

Легко видеть, что множество $\mathbb{F}^n$ с операциями «$+$» и «$\cdot$» будет линейным пространством, в котором нулевым элементом будет нулевой набор $\mathbf{0}=(0,\ldots,0)$. *Скалярным произведением* $(\boldsymbol{x},\boldsymbol{y})$ векторов $\boldsymbol{x},\boldsymbol{y}$ из $\mathbb{F}^n$ называется величина

$$(\boldsymbol{x},\boldsymbol{y}) = x_1y_1 + \ldots + x_iy_i + \ldots + x_ny_n.$$

Векторы называются *ортогональными*, если их скалярное произведение равно нулю. Отметим, что линейную функцию с нулевым свободным членом $\alpha_1x_1+\ldots+\alpha_nx_n$ можно рассматривать как скалярное произведение вектора ее коэффициентов $\boldsymbol{\alpha}=(\alpha_1,\ldots,\alpha_n)$ и вектора переменных $\boldsymbol{x}=(x_1,\ldots,x_n)$. □

Пример 5.2. Поле $\mathbb{Z}_3[x]/(x^3+2x+1)$ из примера 4.18 образует линейное пространство над своим подмножеством — полем $\mathbb{Z}_3$ с операцией сложения «$+$», и операцией умножения «$\cdot$» на элементы из $\mathbb{Z}_3$. □

Пусть $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k \in \mathbb{V}$, $\alpha_1,\ldots,\alpha_k \in \mathbb{F}$. Вектор $\alpha_1\boldsymbol{x}_1+\cdots+$ $+\alpha_k\boldsymbol{x}_k$ называется *линейной комбинацией* векторов $\boldsymbol{x}_i$ с коэффициентами α_i. Множество всех линейных комбинаций векторов $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k$ называется *линейной оболочкой* этих векторов и обозначается $\langle\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k\rangle$. Легко видеть, что линейная оболочка любых векторов $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k$ будет линейным пространством.

Если линейное пространство $\mathbb{V}$ совпадает с линейной оболочкой конечного числа векторов, то пространство называется *конечномерным*, в противном случае пространство называется *бесконечномерным*.

Пример 5.3. На множестве $\mathbb{F}^\infty$, состоящем из бесконечных наборов вида

$$(\alpha_1,\alpha_2,\ldots,\alpha_i,\ldots),$$

где $\alpha_i \in \mathbb{F}$, введем операции покомпонентного сложения и покомпонентного умножения набора на константу из $\mathbb{F}$, так же как

и в примере 5.1. Нетрудно видеть, что множество $\mathbb{F}^\infty$ с такими операциями будет бесконечномерным линейным пространством. □

Векторы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ называются *линейно зависимыми*, если в поле $\mathbb{F}$ найдутся такие одновременно не равные нулю элементы $\alpha_1, \ldots, \alpha_k$, что линейная комбинация векторов $\boldsymbol{x}_i$ с коэффициентами α_i равна нулевому набору: $\alpha_1\boldsymbol{u}_1 + \ldots + \alpha_k\boldsymbol{u}_k = \boldsymbol{0}$. Если при любых одновременно не равных нулю элементах α_i линейная комбинация векторов $\boldsymbol{x}_i$ с коэффициентами α_i не равна нулевому набору, то векторы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ называются *линейно независимыми.*

Легко видеть, что для линейной оболочки векторов справедливы следующие простые свойства:

$\langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_i, \ldots, \boldsymbol{x}_j, \ldots, \boldsymbol{x}_k \rangle = \langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_j, \ldots, \boldsymbol{x}_i, \ldots, \boldsymbol{x}_k \rangle$ для любых i, j;

$\langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \rangle = \langle \boldsymbol{x}_1, \ldots, \alpha\boldsymbol{x}_k \rangle$ для любого ненулевого α;

$\langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \rangle = \langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{k-1}, \boldsymbol{x}_{k-1} + \boldsymbol{x}_k \rangle$.

Из этих свойств следует, что для любого ненулевого α_i и произвольных $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_k$

$$\begin{aligned} &\langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_i, \ldots, \boldsymbol{x}_k \rangle = \\ &\quad = \langle \boldsymbol{x}_1, \ldots, \alpha_1\boldsymbol{x}_1 + \cdots + \alpha_i\boldsymbol{x}_i + \cdots + \alpha_k\boldsymbol{x}_k, \ldots, \boldsymbol{x}_k \rangle. \end{aligned} \tag{5.1}$$

Лемма 5.1. *Пусть $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ и $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ — линейно независимые системы векторов, и каждый $\boldsymbol{y}_i \in \langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \rangle$. Тогда $m \leqslant n$.*

Доказательство. Допустим, утверждение леммы неверно и $m > n$. Без ограничения общности будем полагать, что $\boldsymbol{y}_1$ зависит от $\boldsymbol{x}_1$, т. е. в равенстве $\boldsymbol{y}_1 = \sum_{i=1}^{n} \alpha_{1,i}\boldsymbol{x}_i$ коэффициент $\alpha_{1,1}$ отличен от нуля. В системе векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ вектор $\boldsymbol{x}_1$ заменим вектором $\boldsymbol{y}_1$. Из (5.1) следует, что $\langle \boldsymbol{y}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \rangle = \langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \rangle$. Среди векторов $\boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ и $\boldsymbol{y}_2, \ldots, \boldsymbol{y}_m$ найдем пару $\boldsymbol{x}_i, \boldsymbol{y}_j$, в которой $\boldsymbol{y}_j$ зависит от $\boldsymbol{x}_i$. Пусть такую пару образуют векторы $\boldsymbol{x}_2$ и $\boldsymbol{y}_2$. В системе векторов $\boldsymbol{y}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ вектор $\boldsymbol{x}_2$ заменим вектором $\boldsymbol{y}_2$. И снова из (5.1) следует, что $\langle \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{x}_3, \ldots, \boldsymbol{x}_n \rangle =$

$= \langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \rangle$. Будем проводить такие замены, пока это возможно. Предположим, что это сделано s раз и в результате получена система векторов $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s, \boldsymbol{x}_{s+1}, \ldots, \boldsymbol{x}_n$, линейная оболочка которой совпадает с $\langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \rangle$. Следующую замену нельзя сделать по одной причине — среди векторов $\boldsymbol{x}_{s+1}, \ldots, \boldsymbol{x}_n$ и $\boldsymbol{y}_{s+1}, \ldots, \boldsymbol{y}_m$ нельзя найти пару векторов $\boldsymbol{x}_i, \boldsymbol{y}_j$, в которой вектор $\boldsymbol{y}_j$ зависит от $\boldsymbol{x}_i$. Следовательно, все векторы $\boldsymbol{y}_{s+1}, \ldots, \boldsymbol{y}_m$ зависят только от векторов $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$, т. е. справедливо включение

$$\langle \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m \rangle \subseteq \langle \boldsymbol{y}_1, \ldots, \boldsymbol{y}_s \rangle,$$

где $s \leqslant n < m$. Очевидно, что это включение противоречит линейной независимости векторов $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$. Таким образом, $m \leqslant n$. Лемма доказана.

Пусть $\mathbb{V}$ — произвольное линейное пространство. Система векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ называется *базисом* в $\mathbb{V}$, если эти векторы линейно независимы и их линейная оболочка совпадает с $\mathbb{V}$. Например, в рассмотренном в примере 5.1 пространстве $\mathbb{F}^n$ базисом будет следующая система векторов E_n:

$$\begin{aligned}
\boldsymbol{e}_1 &= (1, 0, 0, \ldots, 0, 0), \\
\boldsymbol{e}_2 &= (0, 1, 0, \ldots, 0, 0), \\
\boldsymbol{e}_3 &= (0, 0, 1, \ldots, 0, 0), \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\boldsymbol{e}_n &= (0, 0, 0, \ldots, 0, 1),
\end{aligned}$$

в которой каждый из векторов содержит ровно одну единичную компоненту. Базис E_n называется *стандартным базисом* в $\mathbb{F}^n$.

Так как конечномерное линейное пространство $\mathbb{V}$ совпадает с линейной оболочкой конечного числа векторов, то отсюда и из леммы 5.1 легко получаем следующее утверждение.

Теорема 5.1. *В каждом конечномерном линейном пространстве $\mathbb{V}$ найдется базис. Все базисы $\mathbb{V}$ состоят из одинакового числа векторов.*

Будем говорить, что векторы $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ *порождают* линейное пространство $\mathbb{V}$, если $\mathbb{V} = \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \rangle$. Очевидно, что любое линейное пространство порождается своим базисом, но не

всякая система векторов, порождающая линейное пространство, является базисом этого пространства. Например, система векторов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n, \boldsymbol{e}_1+\boldsymbol{e}_2$ порождает пространство $\mathbb{F}^n$, но не является его базисом.

Число векторов в базисе пространства $\mathbb{V}$ называется *размерностью* пространства $\mathbb{V}$ и обозначается через $\dim \mathbb{V}$. Пространство размерности k часто называют k-мерным пространством.

Из леммы 5.1 и теоремы 5.1 легко извлекаются следующие простые и полезные утверждения.

Лемма 5.2. *При $m > k$ в k-мерном линейном пространстве любые m векторов линейно зависимы.*

Лемма 5.3. *В k-мерном линейном пространстве любые k линейно независимых векторов являются базисом этого пространства.*

Пример 5.4. Найдем число различных базисов в $\mathbb{Z}_p^n$. Прежде всего заметим, что каждый базис в $\mathbb{Z}_p^n$ состоит ровно из n векторов. Это легко следует из леммы 5.1 и существования базиса E_n.

В $\mathbb{Z}_p^n$ выберем n линейно независимых векторов. Сделаем это, последовательно выбирая векторы из $\mathbb{Z}_p^n$ так, чтобы выбранный на очередном шаге вектор не принадлежал линейной оболочке ранее выбранных векторов. Первый вектор $\boldsymbol{v}_1$ можно выбрать p^n-1 способами: подойдет любой ненулевой вектор. Второй вектор $\boldsymbol{v}_2$ можно выбрать $p^n - p$ способами: подойдет любой вектор, отличный от $\alpha\boldsymbol{v}_1$, где $\alpha \in \mathbb{Z}_p$. На k-м шаге можно выбрать любой вектор, не принадлежащий линейной оболочке векторов $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-1}$. Так как линейная оболочка $\langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-1} \rangle$ состоит из p^{k-1} векторов, то вектор $\boldsymbol{v}_k$ можно выбрать $p^n - p^{k-1}$ способами. Таким образом, все n векторов можно выбрать

$$(p^n - 1)(p^n - p) \cdot \ldots \cdot (p^n - p^k) \cdot \ldots \cdot (p^n - p^{n-1}) \qquad (5.2)$$

способами. Следовательно, число различных базисов в $\mathbb{Z}_p^n$ равно произведению (5.2). $\square$

Очевидно, что каждый вектор $\boldsymbol{v}$, лежащий в k-мерном пространстве $\mathbb{V}$, представляется в виде линейной комбинации

$$\boldsymbol{v} = \alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_k \boldsymbol{v}_k \tag{5.3}$$

базисных векторов $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ этого пространства. Величины α_i называются *координатами* вектора $\boldsymbol{v}$ в базисе $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$. Нетрудно видеть, что представление (5.3) единственно. Действительно, допустим, что найдутся две различные линейные комбинации базисных векторов, каждая из которых равна вектору $\boldsymbol{v}$. Тогда

$$\alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_k \boldsymbol{v}_k = \beta_1 \boldsymbol{v}_1 + \cdots + \beta_k \boldsymbol{v}_k.$$

Вычисляя разность этих линейных комбинаций, получаем, что

$$(\alpha_1 - \beta_1)\boldsymbol{v}_1 + \cdots + (\alpha_k - \beta_k)\boldsymbol{v}_k = \boldsymbol{0},$$

причем среди коэффициентов $\alpha_i - \beta_i$ обязательно найдется хотя бы один, не равный нулю. Следовательно, векторы $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ линейно зависимы, т. е. эти векторы не образуют базис в $\mathbb{V}$. Противоречие.

Лемма 5.4. *При $m < k$ в k-мерном линейном пространстве любые m линейно независимых векторов можно дополнить до базиса пространства.*

Доказательство. В k-мерном линейном пространстве $\mathbb{V}$ рассмотрим линейно независимые векторы $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$. Так как $m < k$, то в $\mathbb{V}$ найдется вектор $\boldsymbol{v}$, не являющийся линейной комбинацией векторов $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$. Положим $\boldsymbol{v}_{m+1} = \boldsymbol{v}$. Если $m + 1 = n$, то в силу леммы 5.3 система $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m+1}$ будет базисом в $\mathbb{V}$. Если $m + 1 < k$, то в $\mathbb{V}$ найдется новый вектор $\boldsymbol{v}$, не являющийся линейной комбинацией векторов $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m+1}$, который вместе с этими векторами образует линейно независимую систему. Повторяя эту процедуру в общей сложности $k - m$ раз, получим базис пространства $\mathbb{V}$, в котором содержатся векторы $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$. Лемма доказана.

Линейные пространства $\mathbb{V}$ и $\mathbb{W}$ над полем $\mathbb{F}$ называются *изоморфными*, если существует такое взаимно однозначное отображение $\varphi : \mathbb{V} \to \mathbb{W}$, что:

(*i*) $\varphi(\boldsymbol{x}+\boldsymbol{y}) = \varphi(\boldsymbol{x}) + \varphi(\boldsymbol{y})$ для всех $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{V}$;
(*ii*) $\varphi(\alpha\boldsymbol{x}) = \alpha\varphi(\boldsymbol{x})$ для всех $\alpha \in \mathbb{F}$ и $\boldsymbol{x} \in \mathbb{V}$.
Отображение $\varphi : \mathbb{V} \to \mathbb{W}$ называется *изоморфизмом*, а факт изоморфизма пространств $\mathbb{V}$ и $\mathbb{W}$ обозначается через $\mathbb{V} \cong \mathbb{W}$.

Пример 5.5. Пусть $\mathbb{V} = \{f \in \mathbb{F}[x] : \deg f < n\}$ — множество, состоящее из всех многочленов степени $n-1$ и менее с коэффициентами из поля $\mathbb{F}$. Оно очевидно замкнуто относительно операций сложения многочленов и их умножения на константы из поля $\mathbb{F}$[1)]. Также из свойств кольца $\mathbb{F}[x]$ следуют свойства (1)—(5) определения на с. 134. Таким образом, $\mathbb{V}$ образует линейное пространство над $\mathbb{F}$, причем $\dim \mathbb{V} = n$. Оно изоморфно пространству $\mathbb{F}^n$ из примера 5.1. □

Пример 5.6. Множество $\mathbb{F}[x]$ всех многочленов над полем $\mathbb{F}$ относительно операций предыдущего примера изоморфно пространству $\mathbb{W}$ всевозможных бесконечных последовательностей элементов из $\mathbb{F}$, имеющих конечное число ненулевых членов. Изоморфизм $\varphi : \mathbb{F}[x] \to \mathbb{W}$ ставит в соответствие многочлену $\alpha_0 + \ldots + \alpha_n x^n$ набор его коэффициентов $(\alpha_0, \ldots, \alpha_n, 0, 0, \ldots)$, дополненный нулями. □

Из определения изоморфизма легко следует, что изоморфизм $\varphi : \mathbb{V} \to \mathbb{W}$ отображает нулевой вектор пространства $\mathbb{V}$ в нулевой вектор пространства $\mathbb{W}$ и что композиция изоморфизмов $\varphi : \mathbb{V} \to \mathbb{W}$ и $\psi : \mathbb{W} \to \mathbb{U}$ является изоморфизмом пространства $\mathbb{V}$ в пространство $\mathbb{U}$.

Теорема 5.2. *Два линейных конечномерных пространства $\mathbb{V}$ и $\mathbb{W}$ над полем $\mathbb{F}$ изоморфны тогда и только тогда, когда их размерности совпадают.*

Доказательство. Покажем, что произвольное k-мерное линейное пространство $\mathbb{V}$ над полем $\mathbb{F}$ изоморфно линейному пространству $\mathbb{F}^k$ наборов длины k из примера 5.1. Пусть $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ — базис пространства $\mathbb{V}$ и $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ — стандартный базис пространства $\mathbb{F}^k$. Так как каждый вектор $\boldsymbol{x}$ из $\mathbb{V}$ единственным

[1)] Степень суммы многочленов не превосходит наибольшей степени слагаемых, степень многочлена αf не превосходит степени f при любом $\alpha \in \mathbb{F}$.

образом представляется в виде суммы $\boldsymbol{x} = x_1\boldsymbol{v}_1 + \cdots + x_k\boldsymbol{v}_k$ и любая сумма такого вида принадлежит $\mathbb{V}$, то отображение $\varphi : \mathbb{V} \to \mathbb{F}^k$, определяемое равенством

$$\varphi(x_1\boldsymbol{v}_1 + \cdots + x_k\boldsymbol{v}_k) = (x_1, \ldots, x_k),$$

является взаимно однозначным. Для такого отображения и любых векторов $\boldsymbol{x} = x_1\boldsymbol{v}_1 + \cdots + x_k\boldsymbol{v}_k$ и $\boldsymbol{y} = y_1\boldsymbol{v}_1 + \cdots + y_k\boldsymbol{v}_k$ из пространства $\mathbb{V}$

$$\begin{aligned}\varphi(\boldsymbol{x} + \boldsymbol{y}) &= \varphi((x_1\boldsymbol{v}_1 + \cdots + x_k\boldsymbol{v}_k) + (y_1\boldsymbol{v}_1 + \cdots + y_k\boldsymbol{v}_k)) = \\ &= \varphi((x_1 + y_1)\boldsymbol{v}_1 + \cdots + (x_k + y_k)\boldsymbol{v}_k) = \\ &= (x_1 + y_1, \ldots, x_k + y_k) = \\ &= (x_1, \ldots, x_k) + (y_1, \ldots, y_k) = \varphi(\boldsymbol{x}) + \varphi(\boldsymbol{y}).\end{aligned}$$

Также легко видеть, что для любого α из $\mathbb{F}$ и любого $\boldsymbol{x}$ из $\mathbb{V}$

$$\begin{aligned}\varphi(\alpha\boldsymbol{x}) &= \varphi(\alpha x_1\boldsymbol{v}_1 + \cdots + \alpha x_k\boldsymbol{v}_k) = \\ &= (\alpha x_1, \ldots, \alpha x_k) = \alpha(x_1, \ldots, x_k) = \alpha\varphi(\boldsymbol{x}).\end{aligned}$$

Таким образом, $\mathbb{V} \cong \mathbb{F}^k$.

Рассмотрим изоморфизм φ пространства $\mathbb{V}$ в пространство $\mathbb{F}^k$ и изоморфизм ψ пространства $\mathbb{F}^k$ в пространство $\mathbb{U}$. Так как композиция изоморфизмов является изоморфизмом, то композиция $\psi \circ \varphi$ будет изоморфизмом $\mathbb{V}$ в $\mathbb{U}$. Следовательно, любые два линейных k-мерных пространства $\mathbb{V}$ и $\mathbb{U}$ над полем $\mathbb{F}$ изоморфны.

Теперь покажем, что если $k \neq m$, то никакое k-мерное пространство $\mathbb{V}$ над полем $\mathbb{F}$ неизоморфно никакому m-мерному пространству $\mathbb{U}$ над тем же полем. В силу доказанного выше для этого достаточно показать, что $\mathbb{F}^k$ неизоморфно $\mathbb{F}^m$. Пусть $m > k$. Допустим, что существует изоморфизм $\varphi : \mathbb{F}^m \to \mathbb{F}^k$ и $\varphi(\boldsymbol{e}_1), \ldots, \varphi(\boldsymbol{e}_m)$ — образ стандартного базиса $\mathbb{F}^m$. Тогда в силу леммы 5.2 найдется ненулевой набор коэффициентов $\alpha_1, \ldots, \alpha_m$, для которого

$$\alpha_1\varphi(\boldsymbol{e}_1) + \cdots + \alpha_m\varphi(\boldsymbol{e}_m) = \boldsymbol{0}.$$

В этом случае приходим к противоречию со свойствами изоморфизма, так как

$$\varphi(\alpha_1\boldsymbol{e}_1 + \cdots + \alpha_m\boldsymbol{e}_m) = \alpha_1\varphi(\boldsymbol{e}_1) + \cdots + \alpha_m\varphi(\boldsymbol{e}_m) = \boldsymbol{0},$$

т. е. φ отображает ненулевой вектор $\alpha_1\boldsymbol{e}_1 + \cdots + \alpha_m\boldsymbol{e}_m$ из $\mathbb{F}^m$ в нулевой вектор пространства $\mathbb{F}^k$, что, очевидно, невозможно. Следовательно, пространства $\mathbb{F}^k$ и $\mathbb{F}^m$ неизоморфны. Теорема доказана.

Пусть $\mathbb{V}$ — линейное пространство над полем $\mathbb{F}$, $\mathbb{V}' \subseteq \mathbb{V}$. Множество $\mathbb{V}'$ называется *линейным подпространством* пространства $\mathbb{V}$, если:

(1) сумма $\boldsymbol{x} + \boldsymbol{y} \in \mathbb{V}'$ для всех $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{V}'$;

(2) $\alpha\boldsymbol{x} \in \mathbb{V}'$ для всех $\alpha \in \mathbb{F}$ и для всех $\boldsymbol{x} \in \mathbb{V}'$.

Пример 5.7. Пространство $\mathbb{W}$, рассмотренное выше в примере 5.6, является бесконечномерным подпространством пространства $\mathbb{F}^\infty$ из примера 5.3. □

Пример 5.8. Найдем число различных k-мерных подпространств в $\mathbb{Z}_p^n$. Каждое такое подпространство определяется базисом, состоящим из k линейно независимых векторов. Повторяя рассуждения из примера 5.4, видим, что число таких базисов равно

$$(p^n - 1)(p^n - p) \cdot \ldots \cdot (p^n - p^{k-1}).$$

При этом в каждом подпространстве существует

$$(p^k - 1)(p^k - p) \cdot \ldots \cdot (p^k - p^{k-1})$$

различных базисов. Следовательно, число различных k-мерных подпространств в $\mathbb{Z}_p^n$ равно

$$\frac{(p^n - 1)(p^n - p) \cdot \ldots \cdot (p^n - p^{k-1})}{(p^k - 1)(p^k - p) \cdot \ldots \cdot (p^k - p^{k-1})}. \quad \square$$

Пусть $\mathbb{U}$ — подпространство пространства $\mathbb{V}$ над полем $\mathbb{F}$. Так как $\mathbb{U}$ и $\mathbb{V}$ абелевы группы, то $\mathbb{U}$, очевидно, будет подгруппой в $\mathbb{V}$, и существует фактор-группа $\mathbb{V}/\mathbb{U}$ группы $\mathbb{V}$ по подгруппе $\mathbb{U}$. Непосредственной проверкой свойств (2)—(5) определения

линейного пространства нетрудно убедиться в том, что фактор-группа $\mathbb{V}/\mathbb{U}$ будет линейным пространством над $\mathbb{F}$. Такое пространство называется *фактор-пространством* пространства $\mathbb{V}$ по подпространству $\mathbb{U}$.

5.2. Линейные операторы

Пусть $\mathbb{V}$ и $\mathbb{U}$ — линейные пространства над полем $\mathbb{F}$. Отображение $\mathcal{A} : \mathbb{V} \to \mathbb{U}$ называется *линейным оператором*, если

$$\begin{aligned} \mathcal{A}(\boldsymbol{v} + \boldsymbol{w}) &= \mathcal{A}(\boldsymbol{v}) + \mathcal{A}(\boldsymbol{w}), \\ \mathcal{A}(\alpha\boldsymbol{v}) &= \alpha\mathcal{A}(\boldsymbol{v}) \end{aligned} \tag{5.4}$$

для любых $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{V}$ и любого $\alpha \in \mathbb{F}$.

Пусть $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ — базис в $\mathbb{V}$, $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$ — базис в $\mathbb{U}$. Тогда для любого вектора $\boldsymbol{x} = x_1\boldsymbol{v}_1 + \ldots + x_n\boldsymbol{v}_n$ из первого пространства в силу свойств (5.4) выполнено равенство

$$\mathcal{A}(\boldsymbol{x}) = \mathcal{A}(x_1\boldsymbol{v}_1 + \ldots + x_n\boldsymbol{v}_n) = x_1\mathcal{A}(\boldsymbol{v}_1) + \ldots + x_n\mathcal{A}(\boldsymbol{v}_n). \tag{5.5}$$

Следовательно, значение линейного оператора однозначно определяется его значениями на векторах базиса. С другой стороны, рассмотрим образы базисных векторов $\boldsymbol{v}_i$, выразив их через элементы базиса в $\mathbb{U}$:

$$\mathcal{A}(\boldsymbol{v}_i) = v_{1i}\boldsymbol{u}_1 + v_{2i}\boldsymbol{u}_2 + \cdots + v_{mi}\boldsymbol{u}_m, \quad i = 1, 2, \ldots, n. \tag{5.6}$$

Подставив равенства (5.6) в (5.5), видим, что

$$\begin{aligned} \mathcal{A}(\boldsymbol{x}) &= x_1\mathcal{A}(\boldsymbol{v}_1) + \ldots + x_n\mathcal{A}(\boldsymbol{v}_n) = \\ &= x_1(v_{11}\boldsymbol{u}_1 + \cdots + v_{m1}\boldsymbol{u}_m) + \ldots \\ &\qquad \cdots + x_n(v_{1n}\boldsymbol{u}_1 + \cdots + v_{mn}\boldsymbol{u}_m) = \\ &= (v_{11}x_1 + \cdots + v_{1n}x_n)\boldsymbol{u}_1 + \ldots \\ &\qquad \cdots + (v_{m1}x_1 + \cdots + v_{mn}x_n)\boldsymbol{u}_m. \end{aligned} \tag{5.7}$$

Если $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y} = y_1\boldsymbol{u}_1 + \cdots + y_m\boldsymbol{u}_m$, то из (5.7) следует, что

$$y_i = v_{i1}x_1 + v_{i2}x_2 + \cdots + v_{im}x_n, \quad i = 1, 2, \ldots, m. \tag{5.8}$$

Очевидно и обратное: если отображение $\mathcal{A}(\boldsymbol{x}) = \boldsymbol{y}$ задано формулами (5.8), то оно является линейным оператором. Функции $y_1, \ldots, y_m$ называются его *компонентами*.

Таким образом, выбрав базисы в пространствах $\mathbb{V}$ и $\mathbb{U}$, линейный оператор из $\mathbb{V}$ в $\mathbb{U}$ можно рассматривать как отображение из $\mathbb{F}^n$ в $\mathbb{F}^m$, все компоненты которого являются линейными функциями с нулевыми свободными членами. Каждый такой оператор будем называть линейным (n, m)-оператором.

Суммой линейных операторов $\mathcal{A} : \mathbb{V} \to \mathbb{U}$ и $\mathcal{B} : \mathbb{V} \to \mathbb{U}$ называется такой оператор $(\mathcal{A} + \mathcal{B}) : \mathbb{V} \to \mathbb{U}$, что

$$(\mathcal{A} + \mathcal{B})(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{B}(\boldsymbol{x})$$

для каждого $\boldsymbol{x} \in \mathbb{V}$. Очевидно, что сумма линейных операторов также будет линейным оператором. Второе равенство в (5.4) определяет произведение линейного оператора и элемента поля, над которым определено линейное пространство. Нетрудно показать, что множество линейных операторов $\mathcal{A}$ из $\mathbb{V}$ в $\mathbb{U}$ с указанными операциями сложения и умножения на элементы поля является линейным пространством, размерность которого равна произведению размерностей пространств $\mathbb{V}$ и $\mathbb{U}$.

Композицией $\mathcal{B} \circ \mathcal{A}$ линейного оператора $\mathcal{A} : \mathbb{V} \to \mathbb{U}$ и линейного оператора $\mathcal{B} : \mathbb{U} \to \mathbb{W}$ называется такой оператор $\mathcal{C} : \mathbb{V} \to \mathbb{W}$, что

$$\mathcal{C}(\boldsymbol{x}) = \mathcal{B}(\mathcal{A}(\boldsymbol{x})) \tag{5.9}$$

для каждого $\boldsymbol{x}$ из $\mathbb{V}$.

Покажем, что композиция линейных операторов является линейным оператором. Рассмотрим композицию $\mathcal{C}(\boldsymbol{x}) = \mathcal{B}(\mathcal{A}(\boldsymbol{x}))$, зафиксировав базисы в пространствах $\mathbb{V}, \mathbb{U}, \mathbb{W}$. Пусть в этом случае компоненты операторов $\mathcal{A}$ и $\mathcal{B}$ определяются следующими равенствами:

$$a_i = a_{i1}x_1 + \ldots + a_{ij}x_j + \ldots + a_{in}x_n, \quad i = 1, 2, \ldots, m; \tag{5.10}$$

$$b_i = b_{i1}y_1 + \ldots + b_{ij}y_j + \ldots + b_{im}y_m, \quad i = 1, 2, \ldots, k, \tag{5.11}$$

где $n = \dim \mathbb{V}$, $m = \dim \mathbb{U}$, $k = \dim \mathbb{W}$. Выразим компоненты c_i оператора $\mathcal{C}$ через коэффициенты операторов $\mathcal{B}$ и $\mathcal{A}$. Для

этого компоненты оператора $\mathcal{A}$ из (5.10) подставим в (5.11) вместо переменных $y_1, \ldots, y_m$. В результате при $i = 1, 2, \ldots, k$ для i-компоненты $\mathcal{C}$ получим

$$\begin{aligned} c_i &= b_{i1}(a_{11}x_1 + \ldots + a_{1t}x_t + \ldots + a_{1n}x_n) + \ldots \\ &\quad \ldots + b_{im}(a_{m1}x_1 + \ldots + a_{mt}x_t + \ldots + a_{mn}x_n) = \\ &= (b_{i1}a_{11} + \ldots + b_{it}a_{t1} + \ldots + b_{im}a_{m1})x_1 + \ldots \\ &\quad \ldots + (b_{i1}a_{1n} + \ldots + b_{it}a_{tn} + \ldots + b_{im}a_{mn})x_n. \end{aligned}$$

Следовательно, каждая компонента c_i оператора $\mathcal{C}$ является линейной функцией, для j-го коэффициента которой справедливо равенство

$$c_{ij} = b_{i1}a_{1j} + \ldots + b_{it}a_{tj} + \ldots + b_{im}a_{mj}. \tag{5.12}$$

Таким образом, композиция линейных операторов является линейным оператором.

Оператор $\mathcal{E} : \mathbb{V} \to \mathbb{V}$ называется *тождественным*, если $\mathcal{E}(\boldsymbol{x}) = \boldsymbol{x}$ для каждого $\boldsymbol{x}$ из $\mathbb{V}$. Легко видеть, что тождественный оператор является линейным. Оператор $\mathcal{A} : \mathbb{V} \to \mathbb{V}$ называется *обратимым* или *невырожденным*, если существует *обратный* оператор $\mathcal{A}^{-1}$ такой, что

$$\mathcal{A}^{-1}(\mathcal{A}(\boldsymbol{x})) = \mathcal{A}(\mathcal{A}^{-1}(\boldsymbol{x})) = \mathcal{E}(\boldsymbol{x}).$$

В силу теоремы 1.2 оператор невырожден тогда и только тогда, когда он биективен. Нетрудно показать, что оператор, обратный к линейному невырожденному оператору, также будет линейным. Поэтому (см. теорему 1.3) множество всех невырожденных операторов $\mathcal{A} : \mathbb{V} \to \mathbb{V}$ образует группу относительно операции композиции. Тождественный оператор $\mathcal{E}$ является ее единичным элементом. Эта группа называется *общей линейной группой* пространства $\mathbb{V}$ и обозначается $\mathrm{GL}(\mathbb{V})$ или $\mathrm{GL}(n, \mathbb{F})$, если $\mathbb{V} = \mathbb{F}^n$. Также отметим, что множество всех операторов $\mathcal{A} : \mathbb{V} \to \mathbb{V}$ образует кольцо операторов с операциями суммы и композиции, мультипликативной группой которого является группа $\mathrm{GL}(\mathbb{V})$.

Ядром линейного оператора $\mathcal{A} : \mathbb{V} \to \mathbb{U}$ называется множество всех таких $\boldsymbol{x} \in \mathbb{V}$, для которых $\mathcal{A}(\boldsymbol{x}) = \mathbf{0}$. Ядро оператора

$\mathcal{A}$ обозначается через $\operatorname{Ker}\mathcal{A}$. *Образом* оператора $\mathcal{A}$ называется множество всех таких $\boldsymbol{y} \in \mathbb{U}$, что $\boldsymbol{y} = \mathcal{A}(\boldsymbol{x})$. Образ оператора $\mathcal{A}$ обозначается через $\operatorname{Im}\mathcal{A}$. Нетрудно показать, что ядро и образ любого линейного оператора являются линейными подпространствами в $\mathbb{V}$ и $\mathbb{U}$ соответственно. Размерность образа линейного оператора $\mathcal{A}$ называется его *рангом* и обозначается через $\operatorname{rank}\mathcal{A}$.

Теорема 5.3. *Пусть* $\dim\mathbb{V} = n$. *Для любого определенного на* $\mathbb{V}$ *линейного оператора* $\mathcal{A}$

$$n = \dim\operatorname{Ker}\mathcal{A} + \dim\operatorname{Im}\mathcal{A}.$$

Доказательство. Пусть векторы $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ образуют базис в $\operatorname{Ker}\mathcal{A}$. Произвольным образом дополним этот базис до базиса всего пространства $\mathbb{V}$. Новые базисные векторы обозначим через $\boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_n$. Теперь для доказательства теоремы достаточно показать, что образ оператора $\mathcal{A}$ порождается векторами $\mathcal{A}(\boldsymbol{v}_{k+1}), \ldots, \mathcal{A}(\boldsymbol{v}_n)$, т. е.

$$\operatorname{Im}\mathcal{A} = \langle\mathcal{A}(\boldsymbol{v}_{k+1}), \ldots, \mathcal{A}(\boldsymbol{v}_n)\rangle.$$

Прежде всего убедимся, что векторы $\mathcal{A}(\boldsymbol{v}_{k+1}), \ldots, \mathcal{A}(\boldsymbol{v}_n)$ линейно независимы. Действительно, если это не так, то найдутся такие одновременно не равные нулю постоянные $\alpha_{k+1}, \ldots, \alpha_n$, что

$$\alpha_{k+1}\mathcal{A}(\boldsymbol{v}_{k+1}) + \ldots + \alpha_n\mathcal{A}(\boldsymbol{v}_n) = \boldsymbol{0}.$$

Откуда, используя линейность оператора $\mathcal{A}$, легко получаем, что

$$\begin{aligned}\boldsymbol{0} &= \alpha_{k+1}\mathcal{A}(\boldsymbol{v}_{k+1}) + \ldots + \alpha_n\mathcal{A}(\boldsymbol{v}_n) = \\ &= \mathcal{A}(\alpha_{k+1}\boldsymbol{v}_{k+1} + \ldots + \alpha_n\boldsymbol{v}_n),\end{aligned}$$

т. е. вектор $(\alpha_{k+1}\boldsymbol{v}_{k+1} + \ldots + \alpha_n\boldsymbol{v}_n)$ принадлежит ядру оператора $\mathcal{A}$. Противоречие с выбором векторов $\boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_n$. Следовательно, векторы $\mathcal{A}(\boldsymbol{v}_{k+1}), \ldots, \mathcal{A}(\boldsymbol{v}_n)$ линейно независимы.

Теперь покажем, что каждый вектор из образа $\mathcal{A}$ выражается в виде линейной комбинации векторов $\mathcal{A}(\boldsymbol{v}_{k+1}), \ldots, \mathcal{A}(\boldsymbol{v}_n)$. Для этого произвольный вектор $\boldsymbol{\alpha}$ из $\mathbb{V}$ разложим по базису $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ и применим к этому вектору оператор $\mathcal{A}$:

$$\mathcal{A}(\boldsymbol{\alpha}) = \mathcal{A}(\alpha_1\boldsymbol{v}_1 + \ldots + \alpha_n\boldsymbol{v}_n) =$$

$$= \mathcal{A}(\alpha_1 \boldsymbol{v}_1 + \ldots + \alpha_k \boldsymbol{v}_k) + \mathcal{A}(\alpha_{k+1}\boldsymbol{v}_{k+1} + \ldots + \alpha_n \boldsymbol{v}_n) =$$
$$= \alpha_{k+1}\mathcal{A}(\boldsymbol{v}_{k+1}) + \ldots + \alpha_n \mathcal{A}(\boldsymbol{v}_n).$$

Таким образом, любой элемент из $\operatorname{Im}\mathcal{A}$ выражается в виде линейной комбинации векторов $\mathcal{A}(\boldsymbol{v}_{k+1}), \ldots, \mathcal{A}(\boldsymbol{v}_n)$. Так как эти векторы линейно независимы, то они образуют базис в $\operatorname{Im}\mathcal{A}$. Следовательно, $\dim \operatorname{Im}\mathcal{A} = n - k$. Теорема доказана.

Пусть $\dim \mathbb{V} = n$ и $\mathcal{A} : \mathbb{V} \to \mathbb{V}$. Если $\dim \operatorname{Ker}\mathcal{A} = 0$, то линейный оператор $\mathcal{A}$ биективен. Действительно, из теоремы 5.3 следует сюръективность $\mathcal{A}$. Если найдутся такие неравные $\boldsymbol{a}$ и $\boldsymbol{b}$, что $\mathcal{A}(\boldsymbol{a}) = \mathcal{A}(\boldsymbol{b})$, то $\mathcal{A}(\boldsymbol{a} - \boldsymbol{b}) = \boldsymbol{0}$, что очевидно противоречит равенству $\dim \operatorname{Ker}\mathcal{A} = 0$, т. е. $\mathcal{A}$ инъективен. Таким образом, оператор $\mathcal{A}$ невырожден тогда и только тогда, когда его ранг равен n.

5.3. Матрицы

Далее полагаем, что во всех рассматриваемых пространствах зафиксированы базисы. Пусть $\mathbb{V}$ — n-мерное линейное пространство над полем $\mathbb{F}$, $\mathbb{U}$ — m-мерное линейное пространство над тем же полем. Удобным средством описания линейных операторов из $\mathbb{V}$ в $\mathbb{U}$ являются матрицы. *Матрицей линейного* (n, m)*-оператора* $\mathcal{A} = (a_1, \ldots, a_m)$ с компонентами

$$\begin{aligned}
a_1 &= a_{11}x_1 \ + a_{12}\,x_2 \ + \ldots\ldots \ + a_{1n}\,x_n,\\
a_2 &= a_{21}x_1 \ + a_{22}\,x_2 \ + \ldots\ldots \ + a_{1n}\,x_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_m &= a_{m1}x_1 + a_{m2}x_2 \ + \ldots\ldots \ + a_{mn}x_n
\end{aligned}$$

называется прямоугольная таблица из m строк и n столбцов

$$\mathbf{A} = \begin{pmatrix}
a_{11} & \cdots & a_{1j} & \cdots & a_{1n}\\
\ldots & \ldots & \ldots & \ldots & \ldots\\
a_{i1} & \ldots & a_{ij} & \ldots & a_{in}\\
\ldots & \ldots & \ldots & \ldots & \ldots\\
a_{m1} & \cdots & a_{mj} & \cdots & a_{mn}
\end{pmatrix}, \tag{5.13}$$

составленная из коэффициентов a_{ij} оператора $\mathcal{A}$. Величины a_{ij} называются элементами матрицы (5.13). Матрицу из m строк и n столбцов с элементами из поля $\mathbb{F}$ будем называть (m,n)-*матрицей* $\mathbf{A} = (a_{ij})$ над полем $\mathbb{F}$ или матрицей размера $m \times n$ над полем $\mathbb{F}$. Если $m = n$, то (n,n)-матрицу будем называть *квадратной* матрицей порядка n, или просто матрицей порядка n. В частности, легко видеть, что матрицей тождественного оператора будет квадратная матрица $\mathbf{E}_n = (e_{ij})$, элементы которой определяются равенством

$$e_{ij} = \begin{cases} 1, & \text{при } i = j, \\ 0, & \text{при } i \neq j. \end{cases}$$

Матрица $\mathbf{E}_n$ называется *единичной* матрицей порядка n.

Матрица $\mathbf{A}^{\mathrm{T}} = (a_{ij}^{\mathrm{t}})$ размера $m \times n$ называется *транспонированной матрицей* к матрице $\mathbf{A} = (a_{ij})$ размера $n \times m$, если $a_{ij}^{\mathrm{t}} = a_{ji}$. Легко видеть, что для любой матрицы $\mathbf{A}$ справедливо равенство $\left(\mathbf{A}^{\mathrm{T}}\right)^{\mathrm{T}} = \mathbf{A}$. Квадратная матрица $\mathbf{A}$ называется *симметрической*, если $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$, и *кососимметрической*, если $\mathbf{A}^{\mathrm{T}} = -\mathbf{A}$.

Пример 5.9. Если $\mathbf{A} = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix}$, то $\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} 0 & 3 \\ 1 & 4 \\ 2 & 5 \end{pmatrix}$. □

Определим операцию умножения матрицы на элемент поля и операции сложения и умножения матриц. Сделаем это так, чтобы матрица произведения $\alpha\mathcal{A}$ элемента α и оператора $\mathcal{A}$ была равна произведению α и матрицы $\mathbf{A}$ оператора $\mathcal{A}$, матрица суммы $\mathcal{A} + \mathcal{B}$ линейных операторов $\mathcal{A}$ и $\mathcal{B}$ была равна сумме матриц этих операторов, а матрица композиции $\mathcal{B} \circ \mathcal{A}$ линейных операторов $\mathcal{B}$ и $\mathcal{A}$ — произведению матриц этих операторов.

Произведением элемента α и матрицы $\mathbf{A}$ называется такая матрица $\mathbf{C} = (c_{ij})$, что $c_{ij} = \alpha a_{ij}$. Очевидно, что матрица $\mathbf{C}$ является матрицей оператора $\alpha\mathcal{A}$.

Суммой $\mathbf{A} + \mathbf{B}$ двух (m,n)-матриц $\mathbf{A} = (a_{ij})$ и $\mathbf{B} = (b_{ij})$ называется такая (m,n)-матрица $\mathbf{C} = (c_{ij})$, что $c_{ij} = a_{ij} + b_{ij}$. Нетрудно видеть, что матрица суммы двух линейных операторов равна сумме матриц этих операторов.

Произведением $\mathbf{BA}$ (k,m)-матрицы $\mathbf{B}=(b_{ij})$ и (m,n)-матрицы $\mathbf{A}=(a_{ij})$ называется такая (k,n)-матрица $\mathbf{C}=(c_{ij})$, что[1)]

$$c_{ij}=b_{i1}a_{1j}+\ldots+b_{it}a_{tj}+\ldots+b_{im}a_{mj}.$$

Если матрицы $\mathbf{B}$ и $\mathbf{A}$ являются матрицами операторов $\mathcal{B}$ и $\mathcal{A}$, заданных равенствами (5.10) и (5.11), то из определения произведения матриц и равенства (5.12) легко следует, что матрица $\mathbf{BA}$ действительно будет матрицей композиции $\mathcal{B}\circ\mathcal{A}$.

Множество (m,n)-матриц над полем $\mathbb{F}$ с указанными операциями сложения и умножения на элементы поля образует линейное пространство размерности mn над $\mathbb{F}$. Нетрудно показать, что это пространство матриц изоморфно линейному пространству соответствующих матрицам операторов.

Если рассматривать набор $\boldsymbol{x}$ из $\mathbb{F}^n$ в качестве матрицы, состоящей из единственного столбца высоты n, то из определения матриц легко следует, что значение линейного (n,m)-оператора $\mathcal{A}$ на наборе $\boldsymbol{x}$ можно найти, вычислив произведение $\mathbf{A}\boldsymbol{x}$ матрицы этого оператора и набора $\boldsymbol{x}$. Далее, говоря о произведении $\mathbf{A}\boldsymbol{x}$, набор $\boldsymbol{x}$ будем иногда называть *вектором-столбцом* для того, чтобы подчеркнуть его «вертикальное» положение в этом произведении.

Пример 5.10. В линейном пространстве над полем $\mathbb{Z}_5$ рассмотрим оператор $\mathcal{A}=(a_1,a_2)$ с компонентами $a_1=x_1+x_2$ и $a_2=x_1+2x_2+3x_3$. Найдем его значение при $x_1=x_2=x_3=1$. Сделаем это, умножив матрицу оператора $\mathcal{A}$ на вектор-столбец (111):

$$\mathcal{A}(111)=\begin{pmatrix}1&1&0\\1&2&3\end{pmatrix}\begin{pmatrix}1\\1\\1\end{pmatrix}=\begin{pmatrix}2\\1\end{pmatrix}.$$

Следовательно, образом вектора (111) является вектор (21), т. е. $a_1(x_1,x_2,x_3)=2$, $a_2(x_1,x_2,x_3)=1$. Аналогичный результат получается после вычисления $\mathcal{A}(1,1,1)$ по формулам его компонент. □

[1)] Заметим, что элемент c_{ij} равен скалярному произведению i-й строки матрицы $\mathbf{B}$ и j-го столбца матрицы $\mathbf{A}$.

Как и при вычислении композиции линейных операторов, произведение $\mathbf{BA}$ матриц $\mathbf{B}$ и $\mathbf{A}$ определено не всегда, а только в том случае, когда число столбцов матрицы $\mathbf{B}$ равно числу строк матрицы $\mathbf{A}$. Поэтому легко видеть, что произведения $\mathbf{AB}$ и $\mathbf{BA}$ матриц $\mathbf{B}$ и $\mathbf{A}$ определены одновременно только для квадратных матриц одного порядка. Отметим, что операция умножения квадратных матриц не коммутативна, т. е. найдутся такие матрицы $\mathbf{A}$ и $\mathbf{B}$ одного порядка, что $\mathbf{AB} \neq \mathbf{BA}$.

Пример 5.11. Рассмотрим две треугольные матрицы второго порядка $\mathbf{A} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ и $\mathbf{B} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ с элементами из $\mathbb{Z}_2$. Для произведений $\mathbf{AB}$ и $\mathbf{BA}$ этих матриц справедливы равенства

$$\mathbf{AB} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\mathbf{BA} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Следовательно, $\mathbf{AB} \neq \mathbf{BA}$. □

Непосредственно из определений операции умножения и сложения матриц следует, что каждая из этих операций ассоциативна, и кроме того, эти операции связаны законами дистрибутивности: для любой матрицы $\mathbf{A}$ размера $m \times n$, любых матриц $\mathbf{B}$ и $\mathbf{C}$ размера $n \times k$ и любой матрицы $\mathbf{D}$ размера $k \times l$ справедливы равенства

$$\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}, \qquad (\mathbf{B} + \mathbf{C})\mathbf{D} = \mathbf{BD} + \mathbf{CD}.$$

Отсюда следует, что множество квадратных матриц одного порядка образует некоммутативное кольцо с единицей, которое, очевидно, изоморфно кольцу соответствующих матрицам операторов.

Матрицы можно разбивать на блоки — матрицы меньших размеров и при условии подходящего выбора размеров блоков выполнять поблочное сложение и умножение матриц. Например, рассмотрим разбитые на четыре блока (m, n)-матрицу $\mathbf{A}$ и (n, k)-матрицу $\mathbf{B}$:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{A}_{21} & \mathbf{A}_{22} \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} \mathbf{B}_{11} & \mathbf{B}_{12} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \end{pmatrix}.$$

Если размеры блоков $\mathbf{A}_{it}$ и $\mathbf{B}_{tj}$ таковы, что произведения $\mathbf{A}_{it}\mathbf{B}_{tj}$ определены для всех $1 \leqslant i, t, j \leqslant 2$, то для произведения $\mathbf{C} = \mathbf{AB}$ справедливо равенство

$$\mathbf{C} = \begin{pmatrix} \mathbf{A}_{11}\mathbf{B}_{11} + \mathbf{A}_{12}\mathbf{B}_{21} & \mathbf{A}_{11}\mathbf{B}_{12} + \mathbf{A}_{12}\mathbf{B}_{22} \\ \mathbf{A}_{21}\mathbf{B}_{11} + \mathbf{A}_{22}\mathbf{B}_{21} & \mathbf{A}_{21}\mathbf{B}_{12} + \mathbf{A}_{22}\mathbf{B}_{22} \end{pmatrix}.$$

С каждой матрицей свяжем три линейных пространства: пространство строк, пространство столбцов и ортогональное пространство. *Пространством строк* матрицы $\mathbf{A}$ называется линейное пространство $\mathbb{A}$, порожденное строками этой матрицы. Пространство строк матрицы $\mathbf{A}$ будем обозначать также через $\langle\mathbf{A}\rangle$. Если $\mathbb{A}$ — пространство строк матрицы $\mathbf{A}$, то матрица $\mathbf{A}$ называется *порождающей* матрицей пространства $\mathbb{A}$. *Пространством столбцов* матрицы $\mathbf{A}$ называется линейное пространство, порожденное столбцами этой матрицы. Легко видеть, что для любой матрицы $\mathbf{A}$ пространство ее столбцов совпадает с пространством строк транспонированной матрицы. Поэтому пространство столбцов матрицы $\mathbf{A}$ будем обозначать через $\langle\mathbf{A}^{\mathrm{T}}\rangle$ и $\mathbb{A}^{\mathrm{T}}$. *Ортогональным пространством* матрицы $\mathbf{A}$ называется линейное пространство $\mathbb{A}^{\perp}$, состоящее из всех тех векторов $\boldsymbol{v}$, для которых $\mathbf{A}\boldsymbol{v} = \mathbf{0}$. Матрицу, столбцы которой образуют базис ортогонального пространства матрицы $\mathbf{A}$, назовем матрицей, ортогональной к $\mathbf{A}$, и обозначим через $\mathbf{A}^{\perp}$. Заметим, что ортогональная матрица в общем случае определена не однозначно.

Нетрудно видеть, что ядро и образ любого линейного оператора $\mathcal{A}$ совпадают с ортогональным пространством и пространством столбцов матрицы $\mathbf{A}$ этого оператора, т. е.

$$\mathbb{A}^{\perp} = \operatorname{Ker}\mathcal{A}, \qquad \mathbb{A}^{\mathrm{T}} = \operatorname{Im}\mathcal{A}. \tag{5.14}$$

Поэтому из теоремы 5.3 вытекает следующее утверждение.

Теорема 5.4. *Для любой матрицы $\mathbf{A}$, состоящей из n столбцов, справедливо равенство*

$$\dim\mathbb{A}^{\perp} + \dim\mathbb{A}^{\mathrm{T}} = n.$$

Введем три элементарных преобразования строк произвольной матрицы: (1) умножение i-й строки матрицы на ненулевую константу; (2) перестановку i-й и j-й строк матрицы; (3) прибавление i-й строки матрицы к ее j-й строке. Если матрица $\mathbf{B}$ получена из матрицы $\mathbf{A}$ при помощи элементарных преобразований строк, то будем говорить, что эти матрицы *эквивалентны*. Эквивалентность матриц $\mathbf{A}$ и $\mathbf{B}$ будем обозначать через $\mathbf{A} \sim \mathbf{B}$.

Теорема 5.5. *Для любых эквивалентных матриц* $\mathbf{A}$ *и* $\mathbf{B}$ *их ортогональные пространства совпадают, т. е.* $\mathbb{A}^\perp = \mathbb{B}^\perp$.

Доказательство. Очевидно, что при умножении компоненты линейного преобразования на ненулевую константу и при перестановке компонент линейного оператора его ядро не изменяется. Поэтому в силу первого равенства в (5.14) элементарные преобразования 1-го и 2-го типов над строками матрицы не изменяют ее. Следовательно, для доказательства теоремы достаточно показать, что третье элементарное преобразование строк также не изменяет ортогонального пространства.

Рассмотрим линейное пространство $\mathbb{V}$, порожденное векторами $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$, и линейное пространство $\mathbb{V}'$, порожденное векторами $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_k$. Будем полагать, что вторая система получена из первой прибавлением ее i-го вектора к j-му, т. е. $\boldsymbol{v}'_t = \boldsymbol{v}_t$ при $t \neq j$ и $\boldsymbol{v}'_j = \boldsymbol{v}_i + \boldsymbol{v}_j$. Легко видеть, что в этом случае $\boldsymbol{v}_j = \boldsymbol{v}'_j - \boldsymbol{v}'_i$.

Докажем равенство $\mathbb{V}^\perp = (\mathbb{V}')^\perp$. Для этого рассмотрим произвольный вектор $\boldsymbol{u}$ из пространства $\mathbb{V}^\perp$. Очевидно, что $(\boldsymbol{u}, \boldsymbol{v}_t) = 0$ для каждого вектора $\boldsymbol{v}_t$ первой системы. Поэтому

$$0 = (\boldsymbol{u}, \boldsymbol{v}_j) + (\boldsymbol{u}, \boldsymbol{v}_i) = (\boldsymbol{u}, \boldsymbol{v}_j + \boldsymbol{v}_i) = (\boldsymbol{u}, \boldsymbol{v}'_j).$$

Следовательно, $\boldsymbol{u} \in (\boldsymbol{v}')^\perp$, и, таким образом, пространство $\mathbb{V}^\perp$ содержится в пространстве $(\mathbb{V}')^\perp$. С другой стороны, если $\boldsymbol{u} \in (\mathbb{V}')^\perp$, то $(\boldsymbol{u}, \boldsymbol{v}'_t) = 0$ для каждого вектора $\boldsymbol{v}'_t$ второй системы. Поэтому

$$0 = (\boldsymbol{u}, \boldsymbol{v}'_j) - (\boldsymbol{u}, \boldsymbol{v}'_i) = (\boldsymbol{u}, \boldsymbol{v}'_j - \boldsymbol{v}'_i) = (\boldsymbol{u}, \boldsymbol{v}_j).$$

Следовательно, $\boldsymbol{u} \in \mathbb{V}^\perp$, и пространство $(\mathbb{V}')^\perp$ содержится в пространстве $\mathbb{V}^\perp$. Таким образом, $\mathbb{V}^\perp = (\mathbb{V}')^\perp$. Теорема доказана.

Теорема 5.6. *Для любой (m,n)-матрицы* $\mathbf{A}$ *справедливо равенство*

$$\dim \mathbb{A} = \dim \mathbb{A}^{\mathrm{T}}. \tag{5.15}$$

Число (5.15) называется *рангом* матрицы $\mathbf{A}$ и обозначается через $\operatorname{rank} \mathbf{A}$.

Доказательство. Пусть $\dim \mathbb{A} = k$. Без ограничения общности будем полагать, что первые k строк матрицы $\mathbf{A}$ линейно независимы, а остальные $m-k$ строк матрицы являются их линейными комбинациями. При помощи элементарных преобразований строк преобразуем матрицу $\mathbf{A}$ в эквивалентную ей матрицу $\mathbf{B}$, в которой только первые k строк не будут нулевыми. Для этого из каждой из последних $m-k$ строк матрицы $\mathbf{A}$ надо вычесть равную ей линейную комбинацию первых k строк. В силу предыдущей теоремы $\mathbb{A}^{\perp} = \mathbb{B}^{\perp}$. Так как все ненулевые компоненты столбцов матрицы $\mathbf{B}$ сосредоточены в ее первых k строках, то легко видеть, что размерность пространства столбцов матрицы $\mathbf{B}$ не превосходит k. Таким образом, из предыдущих рассуждений и теоремы 5.4 имеем

$$\dim \mathbb{A}^{\mathrm{T}} = n - \dim \mathbb{A}^{\perp} = n - \dim \mathbb{B}^{\perp} = \dim \mathbb{B}^{\mathrm{T}} \leqslant k = \dim \mathbb{A}.$$

Следовательно, $\dim \mathbb{A}^{\mathrm{T}} \leqslant \dim \mathbb{A}$. Применяя приведенные рассуждения к матрице $\mathbf{A}^{\mathrm{T}}$, получаем неравенство $\dim \mathbb{A}^{\mathrm{T}} \geqslant \dim \mathbb{A}$. Теорема доказана.

Теорему 5.6 можно переформулировать так: у любой матрицы ранг системы ее строк совпадает с рангом системы ее столбцов и равен рангу задаваемого ею оператора.

Теперь рассмотрим вопрос о том, как, зная матрицу оператора в одном базисе, найти матрицу этого оператора в другом базисе. Пусть $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ и $\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n$ — два базиса n-мерного пространства $\mathbb{V}$, и векторы второго базиса выражаются через векторы первого следующими формулами

$$\left.\begin{aligned} \boldsymbol{v}'_1 &= a_{11}\boldsymbol{v}_1 + a_{12}\,\boldsymbol{v}_2 + \ldots + a_{1n}\,\boldsymbol{v}_n, \\ \boldsymbol{v}'_2 &= a_{21}\boldsymbol{v}_1 + a_{22}\,\boldsymbol{v}_2 + \ldots + a_{2n}\,\boldsymbol{v}_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \boldsymbol{v}'_n &= a_{n1}\boldsymbol{v}_1 + a_{n2}\,\boldsymbol{v}_2 + \cdots + a_{nn}\,\boldsymbol{v}_n. \end{aligned}\right\} \tag{5.16}$$

В этом случае будем говорить, что переход от первого базиса ко второму задается матрицей

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{pmatrix}, \tag{5.17}$$

столбцы которой являются наборами координат векторов второго базиса в первом и которая называется *матрицей перехода* от базиса $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ к базису $\boldsymbol{v}'_1, \boldsymbol{v}'_2, \dots, \boldsymbol{v}'_n$.

Рассмотрим в пространстве $\mathbb{V}$ произвольный вектор $\boldsymbol{x}$ и его координаты $(u_1, \dots, u_n)$ и $(u'_1, \dots, u'_n)$ в этих базисах. Тогда

$$\begin{aligned} \boldsymbol{x} &= u_1\boldsymbol{v}_1 + u_2\boldsymbol{v}_2 + \dots + u_n\boldsymbol{v}_n, \\ \boldsymbol{x} &= u'_1\boldsymbol{v}'_1 + u'_2\boldsymbol{v}'_2 + \dots + u'_n\boldsymbol{v}'_n. \end{aligned}$$

Найдем формулы, выражающие набор координат $\boldsymbol{u} = (u_1, \dots, u_n)$ вектора $\boldsymbol{x}$ в первом базисе через его координаты $\boldsymbol{u}' = (u'_1, \dots, u'_n)$ во втором базисе. Для этого в правой части последнего равенства вместо векторов $\boldsymbol{v}'_i$ подставим соответствующие формулы из (5.16) и соберем вместе слагаемые с одинаковыми множителями $\boldsymbol{v}_i$. В результате имеем

$$\begin{aligned} \boldsymbol{x} &= u'_1\boldsymbol{v}'_1 + u'_2\boldsymbol{v}'_2 + \dots + u'_n\boldsymbol{v}'_n = \\ &= u'_1(a_{11}\boldsymbol{v}_1 + a_{12}\,\boldsymbol{v}_2 + \dots + a_{1n}\,\boldsymbol{v}_n) + \\ &\quad + u'_2(a_{21}\boldsymbol{v}_1 + a_{22}\,\boldsymbol{v}_2 + \dots + a_{2n}\,\boldsymbol{v}_n) + \\ &\qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &\quad + u'_n(a_{n1}\boldsymbol{v}_1 + a_{n2}\,\boldsymbol{v}_2 + \dots + a_{nn}\,\boldsymbol{v}_n) = \\ &= (u'_1a_{11} + u'_2a_{21} + \dots + u'_na_{n1})\boldsymbol{v}_1 + \\ &\quad + (u'_1a_{12} + u'_2a_{22} + \dots + u'_na_{n2})\boldsymbol{v}_2 + \\ &\qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &\quad + (u'_1a_{1n} + u'_2a_{2n} + \dots + u'_na_{nn})\boldsymbol{v}_n. \end{aligned}$$

Сравнивая последнюю сумму с координатами вектора $\boldsymbol{x}$ в базисе

$\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$, видим, что

$$\begin{aligned} u_1 &= a_{11}u'_1 + a_{21}u'_2 + \ldots + a_{n1}u'_n, \\ u_2 &= a_{12}u'_1 + a_{22}u'_2 + \ldots + a_{n2}u'_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u_n &= a_{1n}u'_1 + a_{2n}u'_2 + \ldots + a_{nn}u'_n. \end{aligned} \tag{5.18}$$

Равенства (5.18) можно записать в матричной форме — умножая матрицу перехода $\mathbf{A}$ на вектор-столбец $\boldsymbol{u}'$:

$$\mathbf{A}\boldsymbol{u}' = \boldsymbol{u}.$$

Пусть $\mathbf{B}$ — матрица линейного оператора $\mathcal{B} : \mathbb{V} \to \mathbb{V}$ в базисе $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$. Найдем матрицу $\mathbf{B}'$ этого оператора в базисе $\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n$. Для этого потребуется понятие обратной матрицы. Квадратная матрица $\mathbf{A}^{-1}$ называется *обратной матрицей* квадратной матрицы $\mathbf{A}$, если

$$\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{E}.$$

Не каждая квадратная матрица имеет обратную матрицу. Подробно обратные матрицы будут рассмотрены ниже в разделе 6.2. Здесь же достаточно того очевидного факта (легко следующего из изоморфизма кольца квадратных матриц и кольца соответствующих операторов), что матрица любого невырожденного оператора имеет обратную. Легко видеть, что линейный оператор с матрицей $\mathbf{A}$ из (5.17) невырожден, так как ранг этой матрицы равен n. Поэтому матрица $\mathbf{A}^{-1}$ существует.

Если $\mathbf{A}\boldsymbol{u}' = \boldsymbol{u}$, $\mathbf{B}'\boldsymbol{u}' = \boldsymbol{w}'$ и $\mathbf{B}\boldsymbol{u} = \boldsymbol{w}$, то $\mathbf{A}\boldsymbol{w}' = \boldsymbol{w}$. Следовательно, $\mathbf{B}\mathbf{A}\boldsymbol{u}' = \boldsymbol{w} = \mathbf{A}\boldsymbol{w}'$. Умножив на матрицу $\mathbf{A}^{-1}$ правую и левую стороны последнего равенства, видим, что

$$\mathbf{A}^{-1}\mathbf{B}\mathbf{A}\boldsymbol{u}' = \mathbf{A}^{-1}\mathbf{A}\boldsymbol{w}' = \boldsymbol{w}'.$$

Таким образом, произведение $\mathbf{A}^{-1}\mathbf{B}\mathbf{A}$, где $\mathbf{A}$ — матрица перехода от базиса $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ к базису $\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n$, будет матрицей $\mathbf{B}'$ оператора $\mathcal{B}$ в базисе $\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n$.

Заметим, что так как $\mathbf{B}' = \mathbf{A}^{-1}\mathbf{B}\mathbf{A}$, то, очевидно, что справедливо и равенство $\mathbf{B} = \mathbf{A}\mathbf{B}'\mathbf{A}^{-1}$. Поэтому нетрудно показать, что матрица $\mathbf{A}^{-1}$ будет матрицей перехода от базиса $\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n$ к базису $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$.

5.4. Определители

Будем рассматривать функции вида $f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) = y$, где $\boldsymbol{a}_i$ — вектор из n-мерного линейного пространства $\mathbb{F}^n$, а y — элемент поля $\mathbb{F}$. Функция f называется *полилинейной* (линейной по каждому своему аргументу), если

$$\begin{aligned} f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i + \boldsymbol{a}'_i, \ldots, \boldsymbol{a}_n) &= \\ &= f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) + f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}'_i, \ldots, \boldsymbol{a}_n), \\ f(\boldsymbol{a}_1, \ldots, \lambda\boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) &= \lambda f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) \end{aligned}$$

для каждого $i \in \{1, \ldots, n\}$ и каждого $\lambda \in \mathbb{F}$. Функция f называется *кососимметрической*, если для всех $1 \leqslant i \neq j \leqslant n$

$$f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_n) = -f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n).$$

Покажем, что каждая полилинейная функция f, обращающаяся в нуль, если среди ее аргументов есть два одинаковых, является кососимметрической. Для этого вычислим значение f, полагая, что при любом $k \neq i, j$ ее k-й аргумент равен вектору $\boldsymbol{a}_k$, а i-й и j-й аргументы равны сумме $\boldsymbol{a}_i + \boldsymbol{a}_j$. В этом случае

$$\begin{aligned} 0 &= f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i + \boldsymbol{a}_j, \ldots, \boldsymbol{a}_i + \boldsymbol{a}_j, \ldots, \boldsymbol{a}_n) = \\ &= f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) + f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_n) + \\ &\quad + f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) + f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_n) = \\ &= f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_n) + f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n). \end{aligned}$$

Следовательно,

$$f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_n) = -f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n),$$

и f — кососимметрическая функция. Верно и обратное — значение кососимметрической функции с двумя одинаковыми аргументами равно нулю. Действительно, если $\boldsymbol{a}_i = \boldsymbol{a}_j = \boldsymbol{a}$, то

$$\begin{aligned} f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}_n) &= f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_n) = \\ &= -f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_j, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) = \\ &= -f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}_n). \end{aligned}$$

Таким образом,

$$f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}_n) = -f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}_n) = 0.$$

Часто оказываются полезными функции $f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$, позволяющие разделять линейно зависимые и линейно независимые системы векторов. В линейных пространствах над полем действительных чисел такой естественной функцией векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ является ориентированный объем $V(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ параллелепипеда, построенного на этих векторах. Нетрудно показать, что $V(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ — полилинейная функция, и эта функция равна нулю, если среди ее аргументов есть два одинаковых вектора[1)].

Пример 5.12. В двумерном действительном пространстве $\mathbb{R}^2$ найдем площадь параллелограмма $ABCD$, построенного на векторах $(1, 0)$ и $(1, 2)$. Поместив вершину A в начало координат, получим координаты остальных вершин: $B = A + (1, 0) = (1, 0)$, $C = A + (1, 2) = (1, 2)$, $D = A + (1, 0) + (1, 2) = (2, 2)$. Очевидно, что $ABCD$ — параллелограмм с основанием $|AB| = 1$ и высотой $|CB| = 2$, и его площадь равна 2. Такой же результат нетрудно получить, пользуясь полилинейностью двумерного объема:

$$\begin{aligned} V((1,0),(1,2)) &= V((1,0),(1,0)+(0,2)) = \\ &= V((1,0),(1,0)) + V((1,0),(0,2)) = \\ &= 0 + 2V((1,0),(0,1)) = 0 + 2 = 2. \quad \square \end{aligned}$$

Для n-мерного линейного пространства над произвольным полем $\mathbb{F}$ найдем функцию f, обладающую свойствами, аналогичными указанным выше свойствам объема. Эта функция должна быть полилинейной и кососимметрической. Покажем, что среди таких функций есть функции, равные нулю, если их аргументы линейно зависимы, и не равные нулю в противном случае.

Будем полагать, что векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ заданы своими координатами в базисе $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$. Сначала рассмотрим случай трех векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$, заданных координатами в базисе

[1)] См., например, [15].

$\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$. Воспользовавшись полилинейностью искомой функции f, получим следующие равенства:

$$\begin{aligned} f(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3) &= f\Big(\sum_{i=1}^{3} a_{1i}\boldsymbol{v}_i, \sum_{j=1}^{3} a_{2j}\boldsymbol{v}_j, \sum_{k=1}^{3} a_{3k}\boldsymbol{v}_k\Big) = \\ &= \sum_{i=1}^{3} a_{1i} f\Big(\boldsymbol{v}_i, \sum_{j=1}^{3} a_{2j}\boldsymbol{v}_j, \sum_{k=1}^{3} a_{3k}\boldsymbol{v}_k\Big) = \\ &= \sum_{i=1}^{3} a_{1i} \sum_{j=1}^{3} a_{2j} f\Big(\boldsymbol{v}_i, \boldsymbol{v}_j, \sum_{k=1}^{3} a_{3k}\boldsymbol{v}_k\Big) = \\ &= \sum_{i=1}^{3} a_{1i} \sum_{j=1}^{3} a_{2j} \sum_{k=1}^{3} a_{3k} f(\boldsymbol{v}_i, \boldsymbol{v}_j, \boldsymbol{v}_k) = \\ &= \sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} a_{1i} a_{2j} a_{3k} f(\boldsymbol{v}_i, \boldsymbol{v}_j, \boldsymbol{v}_k). \end{aligned}$$

Затем из последней суммы удалим все слагаемые с нулевыми множителями f. Так как такими будут все с двумя равными аргументами, то в результате получим равенство

$$\begin{aligned} &\sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} a_{1i} a_{2j} a_{3k} f(\boldsymbol{v}_i, \boldsymbol{v}_j, \boldsymbol{v}_k) = \\ &\qquad = \sum_{1 \leqslant i \neq j \neq k \neq i \leqslant 3} a_{1i} a_{2j} a_{3k} f(\boldsymbol{v}_i, \boldsymbol{v}_j, \boldsymbol{v}_k), \end{aligned}$$

в правой части которого в каждом слагаемом индексы i, j и k попарно различны. Поэтому каждый из этих индексов представим как результат действия подстановки $\pi = \begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$ из симметрической группы S_3 на единицу, двойку или тройку, после чего снова воспользуемся кососимметричностью функции f, чтобы в каждом слагаемом упорядочить ее аргументы — векторы $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$. При этом величина $f(\boldsymbol{v}_{\pi(1)}, \boldsymbol{v}_{\pi(2)}, \boldsymbol{v}_{\pi(3)})$ совпадает с $f(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$, если знак подстановки π совпадает со знаком тождественной подстановки, т. е. π является четной, и совпадает с

величиной $-f(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$, если подстановка π является нечетной. Таким образом,

$$\sum_{1\leqslant i\neq j\neq k\neq i\leqslant 3} a_{1i}a_{2j}a_{3k}f(\boldsymbol{v}_i, \boldsymbol{v}_j, \boldsymbol{v}_k) = \\ = \sum_{\pi\in S_3} a_{1\pi(1)}a_{2\pi(2)}a_{3\pi(3)}f(\boldsymbol{v}_{\pi(1)}, \boldsymbol{v}_{\pi(2)}, \boldsymbol{v}_{\pi(3)}) = \\ = \sum_{\pi\in S_3} a_{1\pi(1)}a_{2\pi(2)}a_{3\pi(3)}\operatorname{sgn}\pi \cdot f(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3).$$

Объединяя получившиеся равенства и вынося $f(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ из-под знака суммирования видим, что

$$f(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3) = f(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) \sum_{\pi\in S_3} \operatorname{sgn}\pi \cdot a_{1\pi(1)}a_{2\pi(2)}a_{3\pi(3)}. \quad (5.19)$$

Формула (5.19) легко обобщается на n векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$, заданных координатами в базисе $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$. Нетрудно показать, что имеет место равенство

$$f(\boldsymbol{a}_1,\boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \\ = f(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) \sum_{\pi\in S_n} \operatorname{sgn}\pi \cdot a_{1\pi(1)}a_{2\pi(2)}\cdots a_{n\pi(n)}. \quad (5.20)$$

Из равенства (5.20) видно, что любая полилинейная кососимметрическая функция f однозначно определяется своим значением на базисных[1)] векторах $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$, т. е. для полного определения функции f достаточно задать ее значение на векторах $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$.

Далее рассмотрим наиболее интересный частный случай равенства (5.20), в котором векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ задаются координатами в стандартном базисе $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$, и при этом значение $f(\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n)$ полилинейной кососимметрической функции f на векторах этого базиса равно единице. Такую функцию

[1)] Подчеркнем, что равенство (5.20) выполнено не только в случае, когда $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ — базис, но и когда векторы $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ линейно зависимы, причем a_{ij} являются уже не координатами, а просто коэффициентами линейных комбинаций.

назовем *определителем* системы векторов и обозначим символом $\det$. В этом случае равенство (5.20) записывается в виде

$$\det(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \sum_{\pi \in S_n} \operatorname{sgn}\pi \cdot a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}. \qquad (5.21)$$

Пример 5.13. Для трех векторов (5.21) превращается в формулу

$$\det(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3) = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + \\ + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31},$$

слагаемые в правой части которой упорядочены в соответствии с лексикографическим порядком на множестве вторых строк (ijk) подстановок $\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$ из S_3. $\square$

В следующей теореме покажем, что функция $\det$ разделяет линейно зависимые и линейно независимые системы векторов, т. е. является искомой функцией.

Теорема 5.7. *В линейном n-мерном пространстве для любых векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$*

$$\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \begin{cases} = 0, & \text{если } \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \text{ линейно зависимы;} \\ \neq 0, & \text{если } \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \text{ линейно независимы.} \end{cases}$$

Доказательство. Допустим, что векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ линейно зависимы и $\boldsymbol{a}_n = \sum_{i=1}^{n-1} \lambda_i \boldsymbol{a}_i$. Тогда

$$\det(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \det\Big(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{n-1}, \sum_{i=1}^{n-1} \lambda_i \boldsymbol{a}_i\Big) = \\ = \sum_{i=1}^{n-1} \lambda_i \det(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{n-1}, \boldsymbol{a}_i) = 0,$$

так как в последней сумме каждый определитель содержит два одинаковых аргумента.

Пусть теперь векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ линейно независимы. В этом случае векторы стандартного базиса $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ можно

выразить через векторы $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$. Пусть $\boldsymbol{e}_i = \sum_{j=1}^{n} e_{ij}\boldsymbol{a}_j$. Из свойств функции det и равенства (5.20) видим, что

$$\begin{aligned} 1 &= \det(\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n) = \\ &= \det(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) \sum_{\pi \in S_n} \operatorname{sgn}\pi \cdot e_{1\pi(1)} e_{2\pi(2)} \cdots e_{n\pi(n)}. \end{aligned}$$

Следовательно, $\det(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) \neq 0$. Теорема доказана.

Определителем $\det \mathbf{A}$ квадратной матрицы $\mathbf{A} = (a_{ij})$ называется определитель системы ее строк

$$\det \mathbf{A} = \sum_{\pi \in S_n} \operatorname{sgn}\pi \cdot a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}. \tag{5.22}$$

Пример 5.14. Как и в предыдущем примере, легко видеть, что

$$\begin{aligned} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = & a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + \\ & + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}. \end{aligned}$$ □

Из теоремы 5.7 легко следует, что если ранг квадратной матрицы совпадает с ее порядком, то ее определитель отличен от нуля, а если ранг меньше порядка, то определитель равен нулю.

Из сказанного выше видно, что определитель квадратной матрицы — это полилинейная кососимметрическая функция строк матрицы, которая равна единице на единичной матрице.

Пример 5.15. Следующее равенство справедливо в силу линейности определителя по первой строке:

$$\begin{aligned} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} \det \begin{pmatrix} 1 & 0 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} + \\ + a_{12} \det \begin{pmatrix} 0 & 1 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} + a_{13} \det \begin{pmatrix} 0 & 0 & 1 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}. \end{aligned}$$ □ (5.23)

5.5. Свойства определителей

В этом разделе перечислим основные свойства определителей, обеспечивающие успешное применение последних в решении различных задач линейной алгебры.

1) Пусть $\mathbf{A}$ — квадратная матрица порядка n, $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ — ее строки, $\mathbf{A}'$ — матрица размера $(n-1) \times n$, получающаяся из $\mathbf{A}$ удалением первой строки. Тогда в силу полилинейности и кососимметричности определителя

$$\det \begin{pmatrix} \boldsymbol{a}_1 + \lambda_2 \boldsymbol{a}_2 + \cdots + \lambda_n \boldsymbol{a}_n \\ \mathbf{A}' \end{pmatrix} = \\ = \det \begin{pmatrix} \boldsymbol{a}_1 \\ \mathbf{A}' \end{pmatrix} + \lambda_2 \det \begin{pmatrix} \boldsymbol{a}_2 \\ \mathbf{A}' \end{pmatrix} + \cdots + \lambda_n \det \begin{pmatrix} \boldsymbol{a}_n \\ \mathbf{A}' \end{pmatrix} = \det \mathbf{A},$$

так как при $i = 2, \ldots, n$ в матрице $\begin{pmatrix} \boldsymbol{a}_i \\ \mathbf{A}' \end{pmatrix}$ есть две одинаковые строки, и, следовательно, определитель каждой такой матрицы равен нулю. Очевидно, что установленное равенство справедливо не только для первой строки. Поэтому *если к любой строке квадратной матрицы прибавить линейную комбинацию других ее строк, то определитель матрицы не изменится.*

2) Покажем, что определитель произведения двух квадратных матриц равен произведению их определителей.

Теорема 5.8. *Для любых квадратных матриц* $\mathbf{A}$ *и* $\mathbf{B}$ *одного порядка*

$$\det \mathbf{AB} = \det \mathbf{A} \cdot \det \mathbf{B}.$$

Доказательство. Пусть $\mathbf{C} = \mathbf{AB}$, a_{ji} — элемент, стоящий на пересечении j-й строки и i-го столбца в матрице $\mathbf{A}$, $\boldsymbol{b}_i$ — i-я строка матрицы $\mathbf{B}$, $\boldsymbol{c}_j$ — j-я строка матрицы $\mathbf{C}$. Тогда

$$\boldsymbol{c}_j = \sum_{i=1}^{n} a_{ji} \boldsymbol{b}_i,$$

т. е. j-я строка матрицы $\mathbf{C}$ является линейной комбинацией строк матрицы $\mathbf{B}$ с коэффициентами, взятыми из j-й строки

матрицы $\mathbf{A}$. Поэтому для вычисления значения определителя строк матрицы $\mathbf{C}$ можно воспользоваться формулой (5.20):

$$\begin{aligned}\det \mathbf{AB} = \det \mathbf{C} = \det(\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n) = \\ = \det(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) \sum_{\pi \in S_n} \operatorname{sgn} \pi a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)} = \\ = \det \mathbf{B} \cdot \det \mathbf{A} = \det \mathbf{A} \cdot \det \mathbf{B}.\end{aligned}$$

Теорема доказана.

3) Пусть $\mathbf{A}$ и $\mathbf{A}'$ — матрицы оператора $\mathcal{A} : \mathbb{V} \to \mathbb{V}$ в базисах $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ и $\boldsymbol{v}'_1, \boldsymbol{v}'_2, \ldots, \boldsymbol{v}'_n$ пространства $\mathbb{V}$, $\mathbf{B}$ — матрица перехода от первого базиса ко второму. Так как $\mathbf{A}' = \mathbf{B}^{-1}\mathbf{AB}$, то в силу теоремы 5.8

$$\begin{aligned}\det \mathbf{A}' = \det(\mathbf{B}^{-1}\mathbf{AB}) = \det \mathbf{B}^{-1} \cdot \det \mathbf{A} \cdot \det \mathbf{B} = \\ = \det(\mathbf{B}^{-1}\mathbf{B}) \cdot \det \mathbf{A} = \det \mathbf{E} \cdot \det \mathbf{A} = \det \mathbf{A}.\end{aligned} \tag{5.24}$$

Таким образом, определитель матрицы оператора не зависит от выбора базиса, и поэтому можно говорить об *определителе* линейного оператора. Для вычисления определителя линейного оператора надо в пространстве выбрать базис и найти определитель матрицы оператора в этом базисе.

4) Найдем значение определителя транспонированной матрицы $\mathbf{A}^{\mathrm{T}} = (a^{\mathrm{t}}_{ij})$. Так как $\operatorname{sgn} \pi = \operatorname{sgn} \pi^{-1}$, то поменяем порядок суммирования и перейдем к элементам матрицы $\mathbf{A}$. В результате получим равенства

$$\begin{aligned}\det \mathbf{A}^{\mathrm{T}} = \sum_{\pi \in S_n} \operatorname{sgn} \pi \cdot a^{\mathrm{t}}_{1\pi(1)} a^{\mathrm{t}}_{2\pi(2)} \cdots a^{\mathrm{t}}_{n\pi(n)} = \\ = \sum_{\pi \in S_n} \operatorname{sgn} \pi \cdot a^{\mathrm{t}}_{1\pi^{-1}(1)} a^{\mathrm{t}}_{2\pi^{-1}(2)} \cdots a^{\mathrm{t}}_{n\pi^{-1}(n)} = \\ = \sum_{\pi \in S_n} \operatorname{sgn} \pi \cdot a_{\pi^{-1}(1)1} a_{\pi^{-1}(2)2} \cdots a_{\pi^{-1}(n)n}.\end{aligned}$$

Далее в каждом слагаемом последней суммы упорядочим множители по возрастанию первого индекса:

$$\sum_{\pi \in S_n} \operatorname{sgn} \pi \cdot a_{\pi^{-1}(1)1} a_{\pi^{-1}(2)2} \cdots a_{\pi^{-1}(n)n} =$$

$$= \sum_{\pi \in S_n} \operatorname{sgn} \pi \cdot a_{\pi^{-1}(\pi(1))\pi(1)} a_{\pi^{-1}(\pi(2))\pi(2)} \cdots a_{\pi^{-1}(\pi(n))\pi(n)} =$$
$$= \sum_{\pi \in S_n} \operatorname{sgn} \pi \cdot a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}.$$

Таким образом, из (5.22) следует, что

$$\det \mathbf{A}^{\mathrm{T}} = \det \mathbf{A}, \tag{5.25}$$

и определитель любой квадратной матрицы $\mathbf{A}$ является полилинейной кососимметрической функцией столбцов этой матрицы. В следующем примере используем это свойство определителей для разложения определителей из правой части равенства примера 5.15.

Пример 5.16. Для первого определителя из правой части (5.23) имеем:

$$\det \begin{pmatrix} 1 & 0 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix} +$$
$$+ \det \begin{pmatrix} 0 & 0 & 0 \\ a_{21} & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix} + \det \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} =$$
$$= \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix} = \det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}.$$

Переставляя столбцы во втором и третьем определителях так, чтобы их первые строки совпали с первой строкой первого определителя, видим, что справедливы равенства:

$$\det \begin{pmatrix} 0 & 1 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = -\det \begin{pmatrix} 1 & 0 & 0 \\ a_{22} & a_{21} & a_{23} \\ a_{32} & a_{31} & a_{33} \end{pmatrix} = -\det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix},$$
$$\det \begin{pmatrix} 0 & 0 & 1 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = (-1)^2 \det \begin{pmatrix} 1 & 0 & 0 \\ a_{23} & a_{21} & a_{22} \\ a_{33} & a_{31} & a_{32} \end{pmatrix} = \det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}.$$

Подставляя найденные формулы в (5.23), приходим к равенству

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}\det\begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} - \\ - a_{12}\det\begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13}\det\begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix},$$

являющемуся частным случаем следствия (5.25) и доказываемой ниже в теореме 5.9 формулы разложения определителя по столбцу. □

5) В квадратной матрице $\mathbf{A}$ порядка n удалим i-ю строку и j-й столбец. Определитель получившейся квадратной матрицы порядка $n-1$ называется *минором* $\mathbf{M}_{ij}$ матрицы $\mathbf{A}$. Произведение $(-1)^{i+j}\mathbf{M}_{ij}$ называется *алгебраическим дополнением* $\mathbf{A}_{ij}$ элемента a_{ij} матрицы $\mathbf{A}$.

Теорема 5.9. *Пусть* $\mathbf{A}$ *— квадратная матрица порядка* n*. Тогда для любого* $j \in \{1, 2, \ldots, n\}$ *справедливо равенство*

$$\det \mathbf{A} = \sum_{i=1}^{n} a_{ij}\mathbf{A}_{ij}. \tag{5.26}$$

Равенство (5.26) *называется разложением определителя по* j*-у столбцу.*

Доказательство. Перечислим несколько простых фактов о матрицах и их определителях, совокупность которых позволит легко доказать настоящую теорему.

1. Из равенства (5.22) легко следует, что

$$\det\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & a_{n2} & \ldots & a_{nn} \end{pmatrix} = a_{11}\det\begin{pmatrix} a_{22} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \ldots & a_{nn} \end{pmatrix} = a_{11}\mathbf{A}_{11}. \tag{5.27}$$

2. Преобразуем матрицу $\mathbf{A}$ в матрицу $\mathbf{A}(ij)$, передвинув ее i-ю строку на место первой строки, а j-й столбец на место первого столбца. Для перестановки строк нужно последовательно

выполнить $i-1$ транспозицию строк — поменять i-ю строку местами с $i-1$-й, затем с $i-2$-й и далее совершать такие перестановки со всеми предшествующими строками вплоть до первой. Аналогичные действия надо проделать и над столбцами. Поэтому в силу кососимметричности определителя

$$\det \mathbf{A}(ij) = (-1)^{i+j-2}\det \mathbf{A} = (-1)^{i+j}\det \mathbf{A}. \tag{5.28}$$

3. Если i-я строка и j-й столбец квадратной матрицы $\mathbf{A}$ содержат единственный ненулевой элемент a_{ij}, то в силу (5.27) и (5.28)

$$\det \mathbf{A} = a_{ij}(-1)^{i+j}\mathbf{M}_{ij} = a_{ij}\mathbf{A}_{ij}. \tag{5.29}$$

4. Воспользуемся линейностью определителя матрицы по первому столбцу и представим определитель матрицы $\mathbf{A}$ в виде суммы n определителей:

$$\det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix} +$$
$$+ \det \begin{pmatrix} 0 & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix} + \dots + \det \begin{pmatrix} 0 & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}. \tag{5.30}$$

5. Используя линейность определителя по первой строке, первый определитель из суммы в правой части равенства (5.30) представим в виде суммы

$$\det \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix} + \det \begin{pmatrix} 0 & a_{12} & 0 & \dots & 0 \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix} + \dots$$
$$\dots + \det \begin{pmatrix} 0 & 0 & \dots & 0 & a_{1n} \\ 0 & a_{22} & \dots & a_{2\,n-1} & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \cdots & a_{nn-1} & a_{nn} \end{pmatrix}$$

n определителей, из которых только первый отличен от нуля. Поэтому

$$\det\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix} = \det\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix} = a_{11}\mathbf{A}_{11}.$$

6. Повторив рассуждения из предыдущего пункта для i-го слагаемого из суммы в правой части равенства (5.30), видим, что

$$\det\begin{pmatrix} 0 & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix} = a_{i1}\mathbf{A}_{i1}.$$

7. Из (5.30) и последнего равенства следует, что справедлива формула разложения определителя по первому столбцу:

$$\det\mathbf{A} = \sum_{i=1}^{n} a_{i1}\mathbf{A}_{i1}.$$

8. Нетрудно видеть, что рассуждения п.п. 4—7 справедливы для произвольного столбца определителя. Таким образом

$$\det\mathbf{A} = \sum_{i=1}^{n} a_{ij}\mathbf{A}_{ij}.$$

Теорема доказана.

Из теоремы 5.9 и равенства (5.25) немедленно следует формула *разложения определителя по i-й строке*:

$$\det\mathbf{A} = \sum_{j=1}^{n} a_{ij}\mathbf{A}_{ij}. \tag{5.31}$$

6) Из теоремы 5.9 легко следует, что определитель любой верхнетреугольной ($a_{ij} = 0$ при $i > j$) матрицы $\mathbf{A}$ равен произ-

ведению ее диагональных элементов:

$$\det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix} = a_{11}a_{22}\cdots a_{nn}. \tag{5.32}$$

Равенство (5.32) позволяет достаточно просто вычислять определители больших матриц. Чтобы воспользоваться формулой (5.32), покажем, что произвольная матрица может быть преобразована в верхнетреугольную при помощи двух элементарных преобразований: (2) перестановки строк; (3′) прибавлении к i-й строке линейной комбинации остальных строк. Заметим, что первое из этих преобразований умножает определитель матрицы на -1, а второе, по свойству 1), определитель матрицы не изменяет.

Рассмотрим произвольную квадратную матрицу

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \tag{5.33}$$

порядка n. Если все элементы первого столбца равны нулю, то $\det \mathbf{A} = 0$. Если это не так, то в первом столбце найдется ненулевой элемент a_{i1}. В матрице $\mathbf{A}$ из каждой j-й строки (при $j \neq i$) вычтем i-ю строку, умноженную на $a_{j1}a_{i1}^{-1}$, и переставим первую и i-ю строки (при $i \neq 1$). В результате получим новую матрицу

$$\mathbf{A}' = \begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ 0 & a'_{22} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a'_{n2} & \cdots & a'_{nn} \end{pmatrix},$$

определитель которой либо равен определителю исходной матрицы, либо, если $a_{11} = 0$, отличается от него множителем -1. Проделав аналогичные преобразования с последними $n-1$ строками матрицы $\mathbf{A}'$, либо обнаружим, что первые два столбца матрицы $\mathbf{A}'$ линейно зависимы, т. е. $\det \mathbf{A}' = 0$, либо получим новую

матрицу

$$\mathbf{A}'' = \begin{pmatrix} a''_{11} & a''_{12} & a''_{13} & \cdots & a''_{1n} \\ 0 & a''_{22} & a''_{23} & \cdots & a''_{2n} \\ 0 & 0 & a''_{33} & \cdots & a''_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & a''_{n3} & \cdots & a''_{nn} \end{pmatrix}.$$

Повторив в общей сложности подобные преобразования не более $n-1$ раз, придем к верхнетреугольной матрице, определитель которой равен определителю исходной матрицы, умноженному на $(-1)^k$, где k — общее число сделанных перестановок строк.

Пример 5.17. Вычислим определитель матрицы $\mathbf{A}$ с коэффициентами из $\mathbb{Z}_5$. Преобразуем эту матрицу к верхнетреугольному виду:

$$\mathbf{A} = \begin{pmatrix} 0 & 2 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 3 & 4 & 1 & 1 \\ 2 & 2 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 2 & 2 & 3 \\ 3 & 4 & 1 & 1 \\ 2 & 2 & 2 & 1 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 2 & 2 & 3 \\ 0 & 3 & 2 & 1 \\ 0 & 3 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 2 & 2 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Определитель последней матрицы равен $12 = 2 \pmod 5$, при этом строки переставлялись ровно один раз на первом шаге. Следовательно, $\det \mathbf{A} = -2 = 3$. $\square$

7) Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные квадратные матрицы порядков m и n соответственно. Покажем, что

$$\det \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} = \det \mathbf{A} \cdot \det \mathbf{B}. \tag{5.34}$$

Последовательно раскладывая определитель матрицы $\begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{E}_n \end{pmatrix}$ по последним n строкам, видим, что ее определитель равен определителю матрицы $\mathbf{A}$. Аналогичным образом находим, что опре-

делитель матрицы $\begin{pmatrix} \mathbf{E}_m & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}$ равен $\det \mathbf{B}$. Следовательно,

$$\det \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} = \det \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{E}_n \end{pmatrix} \begin{pmatrix} \mathbf{E}_m & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} =$$
$$= \det \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{E}_n \end{pmatrix} \cdot \det \begin{pmatrix} \mathbf{E}_m & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} = \det \mathbf{A} \cdot \det \mathbf{B}.$$

Теперь покажем, что равенство (5.34) является частным случаем равенства

$$\det \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} = \det \mathbf{A} \cdot \det \mathbf{B} \tag{5.35}$$

с произвольной матрицей $\mathbf{C}$. Прежде всего заметим, что если $\det \mathbf{B} = 0$, то строки матрицы в (5.35) линейно зависимы, и, следовательно, ее определитель равен нулю. Если же $\det \mathbf{B} \neq 0$, то строки матрицы $\mathbf{B}$ линейно независимы, и каждая строка матрицы $\mathbf{C}$ является линейной комбинацией строк матрицы $\mathbf{B}$. В этом случае справедливость равенства (5.35) следует из свойства определителей, установленного в п. 1).

8) Матрица $\widehat{\mathbf{A}} = (\widehat{a}_{ij})$ называется *присоединенной матрицей* квадратной матрицы $\mathbf{A}$, если ее ij-й элемент $\widehat{a}_{ij}$ равен алгебраическому дополнению[1)] $\mathbf{A}_{ji}$ матрицы $\mathbf{A}$.

Пример 5.18. Для матрицы $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ над полем $\mathbb{Z}_5$ найдем присоединенную матрицу $\widehat{\mathbf{A}}$. Так как $\mathbf{A}_{11} = 4$, $\mathbf{A}_{12} = -3 = 2$, $\mathbf{A}_{21} = -2 = 3$ и $\mathbf{A}_{22} = 1$, то $\widehat{\mathbf{A}} = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$. Далее легко видеть, что $\det \mathbf{A} = 3$ и

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

т. е. $\mathbf{A}\widehat{\mathbf{A}} = \det \mathbf{A} \cdot \mathbf{E}$. □

[1)] Подчеркнем, что присоединенная матрица является не матрицей алгебраических дополнений, а транспонированной к ней.

Покажем, что произвольная матрица $\mathbf{A}$ и ее присоединенная матрица $\widehat{\mathbf{A}}$ связаны соотношениями

$$\mathbf{A}\widehat{\mathbf{A}} = \det \mathbf{A} \cdot \mathbf{E} = \widehat{\mathbf{A}}\mathbf{A}. \tag{5.36}$$

Прежде всего заметим, что из двух равенств в (5.36) достаточно доказать одно, второе равенство будет простым следствием первого и (5.25). Поэтому ограничимся доказательством левого равенства.

Нетрудно видеть, что сумма в правой части равенства (5.31) является произведением i-й строки матрицы $\mathbf{A}$ и i-го столбца присоединенной матрицы $\widehat{\mathbf{A}}$:

$$\det \mathbf{A} = \sum_{j=1}^{n} a_{ij}\mathbf{A}_{ij} = \sum_{j=1}^{n} a_{ij}\widehat{\mathbf{A}}_{ji}.$$

Таким образом, для доказательства (5.36) достаточно показать, что произведение i-й строки $\mathbf{A}$ и j-го столбца $\widehat{\mathbf{A}}$ равно нулю при $i \neq j$.

В матрице $\mathbf{A}$ заменим i-ю строку ее j-й строкой и разложим определитель новой матрицы $\mathbf{A}'$ по i-й строке. Так как алгебраические дополнения элементов i-й строки новой матрицы совпадают с соответствующими алгебраическими дополнениями матрицы $\mathbf{A}$, то

$$\det \mathbf{A}' = \sum_{k=1}^{n} a_{jk}\mathbf{A}_{ik}.$$

С другой стороны, i-я и j-я строки в матрице $\mathbf{A}'$ одинаковы. Следовательно, определитель матрицы $\mathbf{A}'$ равен нулю. Таким образом, при $i \neq j$ приходим к равенствам

$$\sum_{k=1}^{n} a_{jk}\widehat{\mathbf{A}}_{ki} = \sum_{k=1}^{n} a_{jk}\mathbf{A}_{ik} = 0,$$

которые завершают доказательство (5.36).

Из (5.36) следует, что каждая матрица $\mathbf{A} = (a_{ij})$ с ненулевым определителем имеет обратную матрицу, найти которую можно

по формуле[1)]

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}^{-1} = \begin{pmatrix} \frac{\mathbf{A}_{11}}{\det \mathbf{A}} & \frac{\mathbf{A}_{21}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{n1}}{\det \mathbf{A}} \\ \frac{\mathbf{A}_{12}}{\det \mathbf{A}} & \frac{\mathbf{A}_{22}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{n2}}{\det \mathbf{A}} \\ \dots & \dots & \dots & \dots \\ \frac{\mathbf{A}_{1n}}{\det \mathbf{A}} & \frac{\mathbf{A}_{2n}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{nn}}{\det \mathbf{A}} \end{pmatrix}. \quad (5.37)$$

Пример 5.19. Для матрицы $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ над $\mathbb{Z}_5$ из предыдущего примера найдем обратную матрицу. Так как $\det \mathbf{A} = 3$, $3^{-1} = 2 \pmod 5$ и $\widehat{\mathbf{A}} = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$, то

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 2 \cdot 4 & 2 \cdot 3 \\ 2 \cdot 2 & 2 \cdot 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}. \square$$

Пример 5.20. Обобщая предыдущий пример, получаем

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \quad \square$$

Нахождение обратных матриц по формуле (5.37) слишком трудоемко для матриц больших порядков, и поэтому эта формула имеет в основном теоретический интерес. Подробнее обратные матрицы и способы их вычисления будут рассмотрены ниже в разделе 6.2.

9) Рассмотрим важный пример вычисления определителя имеющей многочисленные приложения *матрицы Вандермонда*

$$V_n = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix} \quad (5.38)$$

с элементами из поля $\mathbb{F}$.

[1)] Здесь и далее дробь $\frac{a}{b}$ используется для обозначения произведения ab^{-1}.

Лемма 5.5. *Для определителя матрицы Вандермонда V_n справедливо равенство*

$$\det V_n = \prod_{1 \leqslant j < i \leqslant n} (x_i - x_j). \tag{5.39}$$

Доказательство. Лемму докажем индукцией по n. В основание индукции положим очевидный случай $n = 2$. Допустим, что утверждение леммы верно при $n \leqslant m$. Покажем, что оно справедливо и при $n = m + 1$.

Прежде всего заметим, что если $x_i = x_j$, то матрица V_{m+1} будет содержать два одинаковых столбца, и, следовательно, ее определитель будет равен нулю. Поэтому в этом случае равенство (5.39) верно. Далее будем полагать, что все x_i различны.

В матрице V_{m+1} заменим x_{m+1} переменной x, после чего определитель разложим по последнему столбцу. Нетрудно видеть, что в этом случае определитель преобразованной матрицы будет многочленом степени m от x:

$$D(x) = \det \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ x_1 & x_2 & \dots & x_m & x \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^m & x_2^m & \dots & x_m^m & x^m \end{pmatrix} = d_m x^m + \ldots + d_1 x + d_0,$$

где коэффициент d_m — определитель матрицы V_m. Многочлен $D(x)$ имеет ровно m корней — $x_1, \ldots, x_m$. Поэтому

$$D(x) = d_m (x - x_1)(x - x_2) \cdots (x - x_m),$$

где $d_m \in \mathbb{F}$. Так как по предположению индукции имеет место равенство $d_m = \prod_{1 \leqslant j < i \leqslant m} (x_i - x_j)$, то

$$\begin{aligned} \det V_{m+1} &= D(x_{m+1}) = \\ &= \prod_{1 \leqslant j < i \leqslant m} (x_i - x_j) \prod_{1 \leqslant j \leqslant m} (x_{m+1} - x_j) = \prod_{1 \leqslant j < i \leqslant m+1} (x_i - x_j). \end{aligned}$$

Лемма доказана.

Из леммы 5.5 следует, что определитель матрицы Вандермонда отличен от нуля тогда и только тогда, когда все x_i в (5.38) различны.

Задачи

5.1. Доказать эквивалентность двух следующих определений базиса линейного векторного пространства:

1) множество векторов V является базисом пространства $\mathbb{V}$, если векторы V линейно независимы и $\mathbb{V}$ является линейной оболочкой V;

2) множество векторов V является базисом пространства $\mathbb{V}$, если $\mathbb{V}$ является линейной оболочкой V и не является линейной оболочкой никакого его собственного подмножества V'.

5.2. Определить, является ли каждое из указанных множеств линейным пространством, и если является, то найти его размерность, мощность и указать базис:

1) все булевы функции трех аргументов относительно операции $f \vee g$ (над полем $\mathbb{Z}_2$);

2) все булевы функции трех аргументов относительно операции $f \oplus g$;

3) множество матриц размера 3×3 с элементами из $\mathbb{Z}_7$;

4) все симметрические матрицы размера 3×3 с элементами из $\mathbb{Z}_7$;

5) все кососимметрические матрицы размера 3×3 с элементами из $\mathbb{Z}_7$;

6) множество всех многочленов двух переменных степени не более 3 с коэффициентами из $\mathbb{Z}_7$.

5.3. Найти число векторов из пространства $\mathbb{Z}_3^{12}$, ортогональных вектору $\boldsymbol{u} = \mathtt{102002220101}$. Привести пример ненулевого вектора этого пространства, ортогонального самому себе.

5.4. Найти число k-мерных подпространств пространства $\mathbb{Z}_2^n$, содержащих данный вектор.

5.5. Как изменится матрица перехода от одного базиса к другому, если:

1) поменять местами два вектора первого базиса;

2) поменять местами два вектора второго базиса;

3) записать векторы обоих базисов в обратном порядке?

5.6. Найти матрицу перехода от базиса $1, x, x^2, \ldots, x^n$ к базису $1, x-a, (x-a)^2, \ldots, (x-a)^n$ пространства многочленов степени не выше n над полем действительных чисел.

5.7. Найти число различных линейных операторов f, действующих из пространства $\mathbb{Z}_2^n$ в пространство $\mathbb{Z}_2^m$. Сколько из них имеет полный ранг (то есть $\dim \operatorname{Im} f = m$)?

5.8. Найти число различных матриц порядка n над $\mathbb{Z}_p$, p — простое, имеющих ранг m.

5.9. Найти число различных линейных операторов $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, которые переводят фиксированный вектор $\boldsymbol{u} \neq 0$ в нулевой вектор.

5.10. Пусть $\mathbb{V}_1, \mathbb{V}_2$ — произвольные линейные подпространства в некотором пространстве размерности n над полем $\mathbb{F}$. Доказать, что их сумма

$$\mathbb{V}_1 + \mathbb{V}_2 = \left\{ \boldsymbol{x}_1 + \boldsymbol{x}_2 : \boldsymbol{x}_1 \in \mathbb{V}_1, \boldsymbol{x}_2 \in \mathbb{V}_2 \right\}$$

и пересечение $\mathbb{V}_1 \cap \mathbb{V}_2$ также являются подпространствами. Привести пример подпространств $\mathbb{V}_1$ и $\mathbb{V}_2$, объединение которых $\mathbb{V}_1 \cup \mathbb{V}_2$ не является подпространством.

5.11. Пусть $\mathbb{V}_1 = \langle \mathtt{12011}, \mathtt{21102}, \mathtt{12121} \rangle$, $\mathbb{V}_2 = \langle \mathtt{20210}, \mathtt{02001}, \mathtt{11012} \rangle$ над полем $\mathbb{Z}_3$. Найти $\dim(\mathbb{V}_1 + \mathbb{V}_2)$, $\dim(\mathbb{V}_1 \cap \mathbb{V}_2)$ и указать базисы в пространствах $\mathbb{V}_1 + \mathbb{V}_2$ и $\mathbb{V}_1 \cap \mathbb{V}_2$.

5.12. Пусть $\mathbb{V}_1$ и $\mathbb{V}_2$ — подпространства пространства $\mathbb{V}$. Показать, что

$$\dim(\mathbb{V}_1 + \mathbb{V}_2) = \dim \mathbb{V}_1 + \dim \mathbb{V}_2 - \dim(\mathbb{V}_1 \cap \mathbb{V}_2).$$

5.13. Пусть $\mathbb{V}$ — линейное пространство и $\mathbb{U}$ — его произвольное подпространство. Доказать, что $(\mathbb{U}^\perp)^\perp = \mathbb{U}$.

5.14. Привести пример такого подпространства $\mathbb{U}$ в линейном конечномерном пространстве над конечным полем, что $\mathbb{U}^\perp = \mathbb{U}$.

5.15. Показать, что существует ровно одна полилинейная функция $f : (\mathbb{Z}_2^n)^n \to \mathbb{Z}_2$, равная нулю на линейно зависимых аргументах и равная единице в противном случае.

5.16. Найти число различных полилинейных кососимметрических функций $f : (\mathbb{Z}_p^n)^n \to \mathbb{Z}_p$, p — простое, равных нулю на линейно зависимых аргументах и неравных нулю в противном случае.

5.17. Показать, что для любых квадратных матриц $\mathbf{A}$ и $\mathbf{B}$ одинакового порядка

$$\det(\mathbf{A} + \mathbf{B}) \leqslant \det \mathbf{A} + \det \mathbf{B}.$$

5.18. Пусть $\mathbf{A}$ — квадратная матрица порядка n и ранга k. Найти ранг присоединенной матрицы $\widehat{\mathbf{A}}$.

5.19. Показать, что если в квадратной матрице есть строка из единиц, то сумма всех алгебраических дополнений этой матрицы равна ее определителю.

5.20. Матрица H_n над $\mathbb{R}$ порядка 2^n называется матрицей Адамара, если $H_1 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ и $H_{k+1} = \begin{pmatrix} H_k & H_k \\ -H_k & H_k \end{pmatrix}$. Найти $\det H_n$ и H_n^{-1}.

5.21. Воспользовавшись методом индукции, указать способ вычисления произведения $H_n\boldsymbol{x}$ матрицы H_n на произвольный действительный вектор-столбец $\boldsymbol{x}$ длины 2^n, использующий по порядку не более $n2^n$ операций с действительными числами.

5.22. Доказать, что матрица Адамара обладает максимальным (по модулю) определителем среди всех матриц порядка 2^n над $\mathbb{R}$ с элементами ± 1.

5.23. Матрица $F_n = (f_{ij})$ над $\mathbb{C}$ порядка n называется матрицей дискретного преобразования Фурье, если $f_{ij} = \xi_n^{(i-1)(j-1)}$, где ξ_n — первообразный корень n-й степени из единицы ($\xi_n^n = 1$ и $\xi_n^k \neq 1$ при $0 < k < n$). Найти $\det F_n$ и F_n^{-1}.

Глава 6

Пространства с операторами

В этой главе рассматриваются различные вопросы, связанные с решением систем линейных уравнений, и изучается структура линейных пространств с заданными на них линейными операторами. Материал этой главы существенным образом используется далее в восьмой и девятой главах при изучении конечных полей и алгоритмов. С таким, ориентированным на конечные поля, «прикладным» характером данной главы связан ряд особенностей, основная из которых порождена тем, что при вычислениях в конечных полях отсутствуют ошибки округления. Поэтому в излагаемых ниже методах решения линейных систем вопросы точности не рассматриваются, и точность этих методов в «бесконечной» линейной алгебре может оказаться неудовлетворительной.

6.1. Системы линейных уравнений

Над полем $\mathbb{F}$ рассмотрим систему из m линейных уравнений

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}\,x_2 \,+ \ldots + a_{1n}\,x_n = b_1, \\ a_{21}x_1 + a_{22}\,x_2 \,+ \ldots + a_{2n}\,x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}\,x_2 + \ldots + a_{mn}x_n = b_m \end{array}\right\} \qquad (6.1)$$

с коэффициентами a_{ij}, свободными членами b_i и с n неизвестными x_i. Эту систему можно записать в виде матричного урав-

нения

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \tag{6.2}$$

с (m, n)-матрицей $\mathbf{A} = (a_{ij})$, составленной из коэффициентов функций системы (6.1), вектором-столбцом свободных членов $\boldsymbol{b} = (b_i)$ и вектором-столбцом неизвестных $\boldsymbol{x} = (x_i)$. Матричное уравнение называется *согласованным,* если оно имеет хотя бы одно решение. Далее будем изучать решения уравнения (6.2), а следовательно, и решения системы (6.1).

Прежде всего выясним, в каких случаях уравнение (6.2) согласовано. Для этого из матрицы $\mathbf{A}$ и вектора $\boldsymbol{b}$ рассматриваемого уравнения составим новую матрицу $(\mathbf{A} \,|\, \boldsymbol{b})$, добавив к матрице $\mathbf{A}$ в качестве нового столбца вектор $\boldsymbol{b}$ и отделив его при этом от $\mathbf{A}$ вертикальной линией. Получившаяся матрица

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

называется *расширенной матрицей* уравнения (6.2) (а также и системы (6.1)). Имеет место следующий критерий согласованности матричного уравнения.

Теорема 6.1 (Кронекера — Капелли)**.** *Уравнение* $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ *с* (m, n)*-матрицей* $\mathbf{A}$ *имеет решение тогда и только тогда, когда ранг матрицы* $\mathbf{A}$ *равен рангу расширенной матрицы* $(\mathbf{A}|\boldsymbol{b})$.

Доказательство. Если $\operatorname{rank} \mathbf{A} = \operatorname{rank} (\mathbf{A} \,|\, \boldsymbol{b})$, то вектор $\boldsymbol{b}$ является линейной комбинацией столбцов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ матрицы $\mathbf{A}$, т. е.

$$\boldsymbol{b} = \alpha_1 \boldsymbol{a}_1 + \cdots + \alpha_n \boldsymbol{a}_n. \tag{6.3}$$

Так как равенство (6.3) эквивалентно матричному равенству $\mathbf{A}\boldsymbol{\alpha} = \boldsymbol{b}$, то очевидно, что вектор $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ будет решением уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$.

С другой стороны, если вектор-столбец $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ является решением уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$, то, очевидно, справедливо равенство (6.3), из которого немедленно следует равенство рангов матриц $\mathbf{A}$ и $(\mathbf{A} \,|\, \boldsymbol{b})$. Теорема доказана.

Теорема 6.2. *Если уравнение* $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ *с* (m, n)*-матрицей* $\mathbf{A}$ *имеет хотя бы одно решение, то все решения этого уравнения образуют смежный класс пространства* $\mathbb{F}^n$ *по ортогональному пространству матрицы* $\mathbf{A}$*.*

Доказательство. Допустим, что уравнение $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ имеет решение $\boldsymbol{x}_0$. В этом случае для доказательства теоремы достаточно показать, что любой вектор, лежащий с вектором $\boldsymbol{x}_0$ в одном смежном классе пространства $\mathbb{F}^n$ по ортогональному пространству матрицы $\mathbf{A}$, является решением уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$, и наоборот, любое решение рассматриваемого уравнения принадлежит тому же смежному классу пространства $\mathbb{F}^n$ по ортогональному пространству матрицы $\mathbf{A}$, что и вектор $\boldsymbol{x}_0$.

Рассмотрим ортогональное пространство $\mathbb{A}^\perp$ матрицы $\mathbf{A}$. Для каждого вектора $\boldsymbol{v}$ из пространства $\mathbb{A}^\perp$ справедливы равенства

$$\mathbf{A}(\boldsymbol{x}_0 + \boldsymbol{v}) = \mathbf{A}\boldsymbol{x}_0 + \mathbf{A}\boldsymbol{v} = \boldsymbol{b} + \mathbf{0} = \boldsymbol{b}.$$

Следовательно, вектор $\boldsymbol{x}_0 + \boldsymbol{v}$ является решением уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$. С другой стороны, если $\boldsymbol{y}$ — решение рассматриваемого уравнения, то

$$\mathbf{A}(\boldsymbol{y} - \boldsymbol{x}_0) = \mathbf{A}\boldsymbol{y} - \mathbf{A}\boldsymbol{x}_0 = \boldsymbol{b} - \boldsymbol{b} = \mathbf{0}.$$

Поэтому, $\boldsymbol{y} - \boldsymbol{x}_0 \in \mathbb{A}^\perp$. Следовательно, $\boldsymbol{y}$ принадлежит тому же смежному классу пространства $\mathbb{F}^n$ по $\mathbb{A}^\perp$, что и вектор $\boldsymbol{x}_0$. Теорема доказана.

Из доказанной теоремы следует, что для нахождения всех решений уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ достаточно решить две задачи: 1) найти хотя бы одно решение $\boldsymbol{x}_0$ этого уравнения, такое решение называется *частным*; 2) найти ортогональное пространство матрицы $\mathbf{A}$.

Ортогональное пространство матрицы $\mathbf{A}$ является решением *однородного* уравнения $\mathbf{A}\boldsymbol{x} = \mathbf{0}$ (соответствующая этому уравнению система линейных уравнений также называется *однородной*), а базис этого пространства называется *фундаментальной системой решений* уравнения (6.2) (и системы (6.1)).

Решения задач 1) и 2) рассматриваются в двух следующих разделах.

6.2. Обращение невырожденных матриц

Квадратная матрица $\mathbf{A}$ называется *невырожденной* , если ее строки линейно независимы. Из равенства (5.25) и теоремы 5.7 следует, что столбцы невырожденной матрицы также линейно независимы.

Лемма 6.1 (Алгоритм Гаусса)**.** *Квадратную невырожденную матрицу при помощи элементарных преобразований строк можно преобразовать в единичную матрицу.*

Доказательство. Теорему докажем индукцией по порядку матрицы. В основание индукции положим очевидный случай матрицы первого порядка. Далее предположим, что утверждение теоремы верно для всех невырожденных матриц, порядок которых не превосходит $(n-1)$. Рассмотрим произвольную невырожденную матрицу

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \tag{6.4}$$

порядка n. Так как матрица невырождена, то в ее первом столбце найдется хотя бы один ненулевой элемент. В матрице $\mathbf{A}$ переставим строки так, чтобы после перестановки первый элемент первой строки стал ненулевым. После этого умножим первую строку матрицы на константу из $\mathbb{F}$ так, чтобы ее первый элемент стал равным единице. Затем из каждой строки вычтем первую

строку, умноженную на первый элемент уменьшаемой строки. В результате получим новую матрицу

$$\mathbf{A}' = \begin{pmatrix} 1 & a'_{12} & \cdots & a'_{1n} \\ 0 & a'_{22} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a'_{n2} & \cdots & a'_{nn} \end{pmatrix},$$

в которой в первом столбце ненулевой элемент встречается только один раз — в первой строке, где он равен единице. Так как последние $(n-1)$ строк матрицы $\mathbf{A}'$ линейно независимы, то, следовательно, матрица, получающаяся из матрицы $\mathbf{A}'$ удалением первой строки и первого столбца, будет невырожденной матрицей порядка $(n-1)$, и по предположению индукции эту матрицу можно преобразовать в единичную матрицу при помощи элементарных преобразований строк. Легко видеть, что аналогичные преобразования, выполненные над последними $(n-1)$ строками матрицы $\mathbf{A}'$, преобразуют ее в матрицу

$$\mathbf{A}'' = \begin{pmatrix} 1 & a'_{12} & \cdots & a'_{1n} \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

в которой на пересечении последних $(n-1)$ строк и последних $(n-1)$ столбцов стоит единичная матрица. Теперь из первой строки матрицы $\mathbf{A}''$ вычтем вторую строку, умноженную на a'_{12}, третью строку, умноженную на a'_{13}, и т. д. вплоть до последней строки, умноженной на a'_{1n}. Очевидно, что в результате получим единичную матрицу. Лемма доказана.

Вместе с элементарными преобразованиями строк будем также рассматривать и аналогичные элементарные преобразования столбцов. Легко видеть, что справедливо следующее утверждение.

Лемма 6.2. *Квадратную невырожденную матрицу при помощи элементарных преобразований столбцов можно преобразовать в единичную матрицу.*

Заметим, что применение первого элементарного преобразования строк к данной матрице, т. е. умножение ее i-й строки на константу α, сводится к умножению этой матрицы на единичную матрицу, в которой вместо единицы на пересечении i-й строки и i-го столбца стоит α, применение второго элементарного преобразования к сводится к умножению матрицы слева на единичную матрицу с переставленными i-й и j-й строками, а применение третьего элементарного преобразования — к умножению слева на единичную матрицу с дополнительной единицей, стоящей на пересечении j-й строки и i-го столбца. Например, для перестановки первой и четвертой строк нижнетреугольной матрицы четвертого порядка имеем

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

а для прибавления к первой строке этой матрицы ее четвертой строки —

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Таким образом, для каждой невырожденной матрицы $\mathbf{A}$ найдется матрица $\mathbf{B}$, являющаяся произведением матриц, соответствующих выполненным элементарным преобразованиям строк, и такая, что $\mathbf{BA} = \mathbf{E}$.

Аналогичным образом можно показать, что каждое элементарное преобразование столбцов матрицы эквивалентно умножению этой матрицы справа на соответствующую ему матрицу. Поэтому в силу леммы 6.2 для каждой невырожденной матрицы $\mathbf{A}$ найдется матрица $\mathbf{C}$, являющаяся произведением матриц, соответствующих элементарным преобразованиям столбцов, преобразующих $\mathbf{A}$ в единичную матрицу, такая, что $\mathbf{AC} = \mathbf{E}$. Так как

$$\mathbf{C} = (\mathbf{BA})\mathbf{C} = \mathbf{B}(\mathbf{AC}) = \mathbf{B},$$

то $\mathbf{C} = \mathbf{B} = \mathbf{A}^{-1}$, т. е. каждая невырожденная матрица порядка n имеет единственную *обратную* матрицу $\mathbf{A}^{-1}$ такую, что

$$\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{E}_n.$$

Отметим, что множество невырожденных матриц одного порядка образует группу с операцией умножения[1)].

Из сказанного выше следует простой способ обращения невырожденной матрицы $\mathbf{A}$. Сначала элементарными преобразованиями строк матрица $\mathbf{A}$ преобразуется в единичную матрицу, или, что эквивалентно, матрица $\mathbf{A}$ умножается слева на некоторую матрицу $\mathbf{B}$ такую, что $\mathbf{BA} = \mathbf{E}$. Затем аналогичные преобразования производим над единичной матрицей, т. е. умножаем единичную матрицу на ту же матрицу $\mathbf{B}$ и, следовательно, имеем $\mathbf{BE} = \mathbf{B}$. Очевидно, что матрица, получившаяся из единичной матрицы, будет обратной к матрице $\mathbf{A}$.

Пример 6.1. Применим сформулированный выше алгоритм обращения невырожденных матриц к матрице $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ над $\mathbb{Z}_3$. Элементарные преобразования над обращаемой и единичной матрицами будем выполнять одновременно, разделив эти матрицы вертикальной линией. Легко видеть, что справедливы следующие соотношения:

$$\left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right).$$

Таким образом, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. □

[1)] Этот факт, так же как и существование обратной матрицы, является следствием изоморфизма колец матриц и операторов.

6.3. Решение линейных матричных уравнений

1. Систематические матрицы. Матрица $\mathbf{A}$ называется *систематической*, если она состоит из двух блоков — единичной матрицы порядка m и следующей за ней матрицы размера $m \times (n-m)$, т. е.

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & a_{1\,m+1} & \cdots & a_{1n} \\ 0 & 1 & \dots & 0 & 0 & a_{2\,m+1} & \cdots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 1 & a_{m\,m+1} & \cdots & a_{mn} \end{pmatrix}. \tag{6.5}$$

Покажем, что произвольную матрицу простыми преобразованиями строк и столбцов можно превратить в систематическую. Имеет место следующее утверждение.

Лемма 6.3. *Любую матрицу при помощи элементарных преобразований строк, удаления нулевых строк и перестановки столбцов можно преобразовать в систематическую матрицу.*

Доказательство. Рассмотрим (m,n)-матрицу $\mathbf{A}$ ранга k. Переставим строки и столбцы этой матрицы так, чтобы в новой матрице первые k строк и столбцов были линейно независимы. Затем из каждой из последних $m-k$ строк матрицы $\mathbf{A}$ вычтем равную ей линейную комбинацию первых k строк. В преобразованной матрице $\mathbf{A}'$ последние k строк станут нулевыми. Удалим эти строки. Далее рассмотрим матрицу $\mathbf{A}_k$, состоящую из первых k столбцов матрицы $\mathbf{A}'$. Очевидно, что эта матрица будет невырожденной. Следовательно, найдется последовательность элементарных преобразований строк R, переводящая матрицу $\mathbf{A}_k$ в единичную матрицу порядка k. Легко видеть, что эта же последовательность R преобразует матрицу $\mathbf{A}'$ в эквивалентную ей систематическую матрицу. Лемма доказана.

Матрицы $\mathbf{A}$ и $\mathbf{B}$ называются *перестановочно эквивалентными*, если матрицу $\mathbf{A}$ можно преобразовать в матрицу $\mathbf{B}$ элементарными преобразованиями строк и перестановкой столбцов.

Заметим, что любая (m,n)-матрица $\mathbf{B}$ ранга k может быть получена перестановкой столбцов из подходящей (m,n)-матрицы $\mathbf{A}$ ранга k с первыми k линейно независимыми столбцами.

Следовательно, любая (m, n)-матрица ранга k перестановочно эквивалентна некоторой систематической (k, n)-матрице.

Для преобразования матрицы в перестановочно эквивалентную ей систематическую матрицу удобно использовать модификацию приведенного в предыдущем разделе алгоритма преобразования невырожденной матрицы в единичную. Отличие модификации от исходного алгоритма состоит только в том, что при выполнении очередного шага алгоритма над произвольной матрицей может возникнуть ситуация, когда преобразуемый на этом шаге столбец будет равен линейной комбинации предыдущих столбцов. В этом случае преобразуемый столбец надо просто пропустить и продолжить выполнение алгоритма со следующим столбцом. Заканчивается выполнение алгоритма удалением нулевых строк (если такие строки появятся) и перестановкой пропущенных столбцов в конец матрицы.

Пример 6.2. Преобразуем указанную далее матрицу $\mathbf{A}$ над $\mathbb{Z}_3$ в перестановочно эквивалентную ей систематическую матрицу $\mathbf{A}'$. Применяя для этого описанный выше алгоритм, последовательно получим пять приведенных ниже матриц. Первые четыре матрицы эквивалентны матрице $\mathbf{A}$, а последняя, являющаяся систематической, — перестановочно эквивалентна:

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 2 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

На первом шаге алгоритма первая строка матрицы $\mathbf{A}$ прибавлена к ее второй строке. На втором шаге вторая строка новой

матрицы прибавлена к удвоенной третьей и четвертой строкам. Легко видеть, что в полученной матрице третий столбец является линейной комбинацией первых двух столбцов. Поэтому на третьем шаге третий столбец оставлен без изменений, преобразован четвертый столбец — третья строка матрицы удвоена и прибавлена ко второй. На четвертом шаге к первой строке прибавляются удвоенные вторая и третья строки. Наконец на последнем шаге переставлены третий и четвертый столбцы, а последняя строка, состоящая только из нулей, удалена. Полученная в результате преобразований матрица является систематической. □

2. Решение однородного уравнения. Приведем алгоритм, который находит базис ортогонального пространства произвольной (m, n)-матрицы.

Сначала рассмотрим частный случай — опишем алгоритм, решающий данную задачу для систематической матрицы. Для этого систематической матрице $\mathbf{A} = \left(\mathbf{E}_m \widetilde{\mathbf{A}}\right)$ поставим в соответствие (n, m)-матрицу $\mathbf{A}' = \begin{pmatrix} -\widetilde{\mathbf{A}} \\ \mathbf{E}_{n-m} \end{pmatrix}$, которая состоит из двух блоков — матрицы $-\widetilde{\mathbf{A}}$ и находящейся под ней единичной матрицы порядка $(n-m)$. Легко видеть, что для произведения $\mathbf{A}\mathbf{A}'$ справедливы равенства:

$$\mathbf{A}\mathbf{A}' = \left(\mathbf{E}_m \widetilde{\mathbf{A}}\right) \begin{pmatrix} -\widetilde{\mathbf{A}} \\ \mathbf{E}_{n-m} \end{pmatrix} = \left(\widetilde{\mathbf{A}} - \widetilde{\mathbf{A}}\right) = \mathbf{0}.$$

Таким образом, пространство $\mathbb{A}'^{\mathrm{T}}$, порожденное столбцами матрицы $\mathbf{A}'$, входит в ортогональное пространство матрицы $\mathbf{A}$. Так как размерность этого пространства равна $n-m$, а размерность пространства строк матрицы $\mathbf{A}$ равна m, т. е. $\dim \mathbb{A}'^{\mathrm{T}} + \dim \mathbb{A} = n$, то из теоремы 5.4 легко следует, что $\mathbb{A}^{\perp} = \mathbb{A}'^{\mathrm{T}}$. Таким образом, в качестве базиса ортогонального пространства матрицы $\mathbf{A}$ можно взять столбцы матрицы $\mathbf{A}'$.

Приведенный алгоритм очевидным образом модифицируется в алгоритм нахождения базиса ортогонального пространства произвольной матрицы. Матрицу $\mathbf{A}$ надо преобразовать в

перестановочно эквивалентную ей систематическую матрицу $\mathbf{B}$. При этом следует запомнить все выполненные в процессе преобразования перестановки столбцов — действующую на множестве столбцов подстановку $\pi \in S_n$. Затем для матрицы $\mathbf{B}$ описанным выше способом строится матрица $\mathbf{B}'$, столбцы которой порождают ортогональное пространство матрицы $\mathbf{B}$. Наконец на строки матрицы $\mathbf{B}'$ действуем подстановкой π^{-1}, восстанавливая исходный порядок координат. Полученная матрица $\mathbf{C}$ будет порождать ортогональное пространство исходной матрицы $\mathbf{A}$.

Пример 6.3. Для матрицы $\mathbf{A}$ из рассмотренного выше примера 6.2 построим матрицу, порождающую ее ортогональное пространство. Сначала преобразуем матрицу $\mathbf{A}$ в перестановочно эквивалентную ей систематическую матрицу $\mathbf{B}$. Из примера 6.2 имеем

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 2 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

При преобразовании $\mathbf{A}$ в $\mathbf{B}$ переставлялись третий и четвертый столбцы. Для матрицы $\mathbf{B}$ легко находим порождающую ее ортогональное пространство матрицу $\mathbf{B}'$: умножая матрицу $\widetilde{\mathbf{B}} = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ на -1, получаем матрицу $\begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$, к которой снизу приписываем единичную матрицу третьего порядка. Затем в матрице $\mathbf{B}'$ выполняем обратную к ранее выполненной перестановку строк — снова меняем местами третью и четвертую строки. В результате имеем

$$\mathbf{B}' = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 1 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Непосредственной проверкой легко убедиться в справедливости равенства $\mathbf{AC} = \mathbf{0}$, и так как $\operatorname{rank}\mathbf{C} + \operatorname{rank}\mathbf{A} = 6$, то $\mathbf{C}$ — искомая матрица. □

Используя приведенный в предыдущем разделе алгоритм обращения невырожденных матриц, можно легко решить уравнение $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ с невырожденной квадратной матрицей $\mathbf{A}$. Для решения этого уравнения достаточно обратить матрицу $\mathbf{A}$ и умножить найденную матрицу $\mathbf{A}^{-1}$ на вектор $\boldsymbol{b}$. Действительно, умножая матрицу $\mathbf{A}^{-1}$ на левую и правую части рассматриваемого уравнения, видим, что

$$\mathbf{A}^{-1}\boldsymbol{b} = \mathbf{A}^{-1}\mathbf{A}\boldsymbol{x} = \mathbf{E}\boldsymbol{x} = \boldsymbol{x}.$$

Следовательно, решением уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ с невырожденной матрицей $\mathbf{A}$ является вектор $\mathbf{A}^{-1}\boldsymbol{b}$. Рассмотрим простой пример.

Пример 6.4. Решим над $\mathbb{Z}_3$ матричное уравнение

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Матрица из этого уравнения была обращена в примере 6.1. Используя его результат, имеем

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}.$$

Таким образом, решением рассматриваемого уравнения является вектор-столбец (121). □

Заметим, что для решения уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ с невырожденной матрицей $\mathbf{A}$ необязательно эту матрицу обращать. Достаточно выполнить над вектором $\boldsymbol{b}$ действия, преобразующие матрицу $\mathbf{A}$ в единичную матрицу.

Пример 6.5. Решим уравнение $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$, в котором матрица $\mathbf{A}$ такая же, как и в предыдущем примере, а вектор $\boldsymbol{b}$ равен

(110). Элементарные преобразования над матрицей $\mathbf{A}$ и вектором $\boldsymbol{b}$ будем выполнять одновременно, добавив вектор $\boldsymbol{b}$ к столбцам матрицы $\mathbf{A}$. Выполняя такие же преобразования, как и в примере 6.1, видим, что

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Следовательно, $\boldsymbol{x} = (201)$. □

Рассмотренный выше алгоритм нахождения базиса ортогонального пространства матрицы позволяет показать, что любое подпространство линейного пространства является в некотором смысле аналогом нормальных подгрупп и идеалов, а любой линейный оператор — аналогом гомоморфизма. Точнее, справедливо следующее утверждение.

Теорема 6.3. *Для любого подпространства $\mathbb{U}$ конечномерного пространства $\mathbb{V}$ найдется такой линейный оператор $\mathcal{A} : \mathbb{V} \to \mathbb{V}$, что $\mathbb{U} = \operatorname{Ker} \mathcal{A}$.*

Доказательство. Зафиксируем в n-мерном пространстве $\mathbb{V}$ базис V. Пусть $k = \dim \mathbb{U}$, векторы $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ образуют базис в $\mathbb{U}$ и являются строками матрицы $\mathbf{U}$. Пусть, далее, векторы $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{n-k}$ образуют базис ортогонального пространства матрицы $\mathbf{U}$ и являются строками матрицы $\mathbf{U}'$. Так как строки матрицы $\mathbf{U}$ образуют базис ортогонального пространства матрицы $\mathbf{U}'$, то подпространство $\mathbb{U}$ будет ядром оператора $\mathcal{A}$, матрицей которого в базисе V является $\mathbf{U}'$. Теорема доказана.

3. Общий случай. Теперь приведем алгоритм нахождения решения согласованного уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ в общем случае с ненулевой правой частью. Для этого сначала найдем частное решение этого уравнения в случае, когда матрица $\mathbf{A} = (\mathbf{E}_m \mathbf{B})$ систематическая. Такое решение находится легко. Например, из равенств

$$(\mathbf{E}_m\mathbf{B})\begin{pmatrix}\boldsymbol{b}\\ \mathbf{0}\end{pmatrix} = \mathbf{E}_m\boldsymbol{b} + \mathbf{B0} = \boldsymbol{b}$$

следует, что вектор $\begin{pmatrix}\boldsymbol{b}\\ \mathbf{0}\end{pmatrix}$ будет частным решением рассматриваемого уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$.

Далее рассмотрим уравнение с несистематической (m, n)-матрицей $\mathbf{A}$ ранга m, в которой первые m столбцов линейно независимы. Легко видеть, что при помощи только элементарных преобразований строк матрица $\mathbf{A}$ может быть преобразована в эквивалентную ей систематическую матрицу $\mathbf{B}$. Ранее было показано (с. 182), что выполнение любого элементарного преобразования строк квадратной матрицы сводится к умножению этой матрицы слева на некоторую матрицу определенного вида. Аналогичное утверждение справедливо и для матриц произвольных размеров. Например, легко видеть, что умножение произвольной (m, n)-матрицы $\mathbf{A}$ слева на квадратную матрицу порядка m, получающуюся из единичной матрицы того же порядка добавлением единицы на пересечение i-й строки и j-го столбца, соответствует добавлению к i-й строке матрицы $\mathbf{A}$ ее j-й строки. Следовательно, для любой (m, n)-матрицы $\mathbf{A}$ ранга m, в которой первые m столбцов линейно независимы, найдется квадратная матрица $\mathbf{C}$ порядка m, умножение на которую слева преобразует матрицу $\mathbf{A}$ в эквивалентную ей систематическую матрицу $\mathbf{B}$. Так как

$$\mathbf{B}\boldsymbol{x} = \mathbf{CA}\boldsymbol{x} = \mathbf{C}\boldsymbol{b},$$

то одновременное выполнение над строками матрицы $\mathbf{A}$ и над координатами вектора $\boldsymbol{b}$ элементарных преобразований, переводящих $\mathbf{A}$ в $\mathbf{B}$, преобразует уравнение $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ в уравнение $\mathbf{B}\boldsymbol{x} = \mathbf{C}\boldsymbol{b}$, решения которого совпадают с решениями исходного уравнения. Так как матрица $\mathbf{B}$ систематическая, то вектор-столбец $(\boldsymbol{b}', \mathbf{0})$, где $\boldsymbol{b}' = \mathbf{C}\boldsymbol{b}$, будет частным решением уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$. Очевидным образом приведенный алгоритм можно использовать и для решений уравнений с произвольными матрицами.

Пример 6.6. Найдем все решения уравнения

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_6 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 1 \end{pmatrix}. \tag{6.6}$$

Решения однородного уравнения с такой же матрицей, как и в (6.6), были найдены в примере 6.3, где, в частности, был найден ранг этой матрицы, равный трем. Поэтому для определения всех решений уравнения (6.6) надо определить, будет ли это уравнение согласованным, и если оно согласовано, то найти какое-нибудь его частное решение. Сделаем это описанным выше способом. Элементарные преобразования над строками матрицы и координатами вектора будем выполнять одновременно, добавив в матрицу коэффициентов в качестве дополнительного столбца вектор свободных членов. Из двух следующих преобразований

$$\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right),$$

которые аналогичны двум первым преобразованиям из примера 6.2, видно, что ранг расширенной матрицы равен четырем. Таким образом, система (6.6) решений не имеет. □

Пример 6.7. Поменяем вектор в правой части (6.6) и найдем все решения нового уравнения

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_6 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \tag{6.7}$$

Для этого над расширенной матрицей системы (6.7) выполним первые четыре преобразования из примера 6.2. Эти преобразования состоят в следующем: 1) первую строку расширенной матрицы прибавим к ее второй строке; 2) вторую строку новой матрицы прибавим к удвоенной третьей и четвертой строкам; 3) третью строку матрицы удвоим и прибавим ко второй строке; 4) к первой строке прибавим удвоенные вторую и третью строки. В результате этих преобразований получим последовательность эквивалентных матриц

$$\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 & 2 \\ 0 & 0 & 0 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccccc|c} 1 & 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right),$$

последняя из которых с точностью до перестановки двух столбцов является систематической. Легко видеть, что ранг матрицы нового уравнения

$$\begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_6 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 2 \\ 0 \end{pmatrix}$$

равен рангу расширенной матрицы. Следовательно, решение существует. В матрице нового уравнения сумма первого, второго и удвоенного четвертого столбцов равна вектору, стоящему в правой части этого уравнения. Поэтому вектор (110200) будет частным решением последнего уравнения, а следовательно, и

уравнения (6.7). Наконец каждое решение этих уравнений является суммой найденного частного решения и некоторого вектора из ортогонального пространства матрицы из (6.6), которое было найдено в примере 6.3. Следовательно, каждое решение уравнения (6.7) представляется в виде суммы

$$(110200) + \lambda_1(121000) + \lambda_2(020010) + \lambda_3(010201),$$

где λ_1, λ_2 и λ_3 — произвольные константы из $\mathbb{Z}_3$. □

4. Формулы Крамера. Снова рассмотрим уравнение $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ с невырожденной квадратной матрицей $\mathbf{A}$. Из (5.37) следует, что для его решения $\boldsymbol{x} = \mathbf{A}^{-1}\boldsymbol{b}$ справедливо равенство

$$\begin{pmatrix} x_1 \\ \dots \\ x_j \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} \frac{\mathbf{A}_{11}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{i1}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{n1}}{\det \mathbf{A}} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{\mathbf{A}_{1j}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{ij}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{nj}}{\det \mathbf{A}} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{\mathbf{A}_{1n}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{in}}{\det \mathbf{A}} & \dots & \frac{\mathbf{A}_{nn}}{\det \mathbf{A}} \end{pmatrix} \begin{pmatrix} b_1 \\ \dots \\ b_i \\ \dots \\ b_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n b_i \frac{\mathbf{A}_{i1}}{\det \mathbf{A}} \\ \dots\dots \\ \sum_{i=1}^n b_i \frac{\mathbf{A}_{ij}}{\det \mathbf{A}} \\ \dots\dots \\ \sum_{i=1}^n b_i \frac{\mathbf{A}_{in}}{\det \mathbf{A}} \end{pmatrix}. \tag{6.8}$$

С другой стороны, пусть $\mathbf{A}_j$ — матрица, полученная из матрицы $\mathbf{A}$ заменой ее j-го столбца столбцом свободных членов $\boldsymbol{b}$. Так как $\det \mathbf{A} = \sum_{i=1}^n a_{ij}\mathbf{A}_{ij}$, то, разложив $\det \mathbf{A}_j$ по j-у столбцу, получим

$$\det \mathbf{A}_j = \det \begin{pmatrix} a_{11} & \dots & b_1 & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & b_i & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & b_n & \dots & a_{nn} \end{pmatrix} = \sum_{i=1}^n b_i \mathbf{A}_{ij}. \tag{6.9}$$

Сравнивая (6.8) с (6.9), видим, что

$$x_j = \frac{\det \mathbf{A}_j}{\det \mathbf{A}}, \qquad j = 1, 2, \dots, n. \tag{6.10}$$

Таким образом, для нахождения i-й компоненты решения уравнения $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ с невырожденной квадратной матрицей $\mathbf{A}$ следует: 1) в матрице $\mathbf{A}$ заменить i-й столбец вектором $\boldsymbol{b}$; 2) вычислить определитель новой матрицы; 3) разделить найденный определитель на определитель матрицы $\mathbf{A}$.

Формулы (6.10) называются *формулами Крамера*. Вычисление определителей даже для матриц относительно небольших порядков достаточно трудоемкая задача. Поэтому формулы Крамера имеют более теоретическое, нежели прикладное значение.

6.4. Инвариантные подпространства

1. Циклические подпространства. Будем рассматривать n-мерное линейное пространство $\mathbb{V}$ над полем $\mathbb{F}$ вместе с определенным на этом пространстве линейным оператором $\mathcal{A} : \mathbb{V} \to \mathbb{V}$. Подпространство $\mathbb{U} \subseteq \mathbb{V}$ называется *инвариантным относительно оператора* $\mathcal{A}$, если $\mathcal{A}(\mathbb{U}) \subseteq \mathbb{U}$. Если $\boldsymbol{v} \in \operatorname{Ker}\mathcal{A}$, то $\mathcal{A}(\boldsymbol{v}) = \mathbf{0} \in \operatorname{Ker}\mathcal{A}$. Следовательно, ядро оператора является его инвариантным пространством. Так как $\mathcal{A}(\boldsymbol{v}) \in \operatorname{Im}\mathcal{A}$ для любого $\boldsymbol{v}$, то образ оператора также будет его инвариантным пространством.

Пусть $\boldsymbol{v}$ — вектор из $\mathbb{V}$. Найдем минимальное инвариантное подпространство $\mathbb{U}$, содержащее $\boldsymbol{v}$. Действуя на $\boldsymbol{v}$ оператором $\mathcal{A}$, получим последовательность векторов $\boldsymbol{v}, \mathcal{A}(\boldsymbol{v}), \ldots, \mathcal{A}^i(\boldsymbol{v}), \ldots$. Если в этой последовательности первые k векторов линейно независимы, а вектор $\mathcal{A}^k(\boldsymbol{v})$ является линейной комбинацией

$$\mathcal{A}^k(\boldsymbol{v}) = a_{k-1}\mathcal{A}^{k-1}(\boldsymbol{v}) + a_{k-2}\mathcal{A}^{k-2}(\boldsymbol{v}) + \cdots + a_1\mathcal{A}(\boldsymbol{v}) + a_0\boldsymbol{v} \quad (6.11)$$

предыдущих, то векторы $\boldsymbol{v}, \mathcal{A}(\boldsymbol{v}), \ldots, \mathcal{A}^{k-1}(\boldsymbol{v})$ образуют базис инвариантного пространства, так как они линейно независимы и для любой линейной комбинации $v_0\boldsymbol{v}+v_1\mathcal{A}(\boldsymbol{v})+\cdots+v_{k-1}\mathcal{A}^{k-1}(\boldsymbol{v})$ этих векторов их образ

$$\begin{aligned}\mathcal{A}(v_0\boldsymbol{v} + v_1\mathcal{A}(\boldsymbol{v}) + \cdots + v_{k-1}\mathcal{A}^{k-1}(\boldsymbol{v})) &= \\ = v_0\mathcal{A}(\boldsymbol{v}) + v_1\mathcal{A}^2(\boldsymbol{v}) + \cdots + v_{k-2}\mathcal{A}^{k-1}(\boldsymbol{v}) + v_{k-1}\mathcal{A}^k(\boldsymbol{v}) &= \\ = v_{k-1}a_0\boldsymbol{v} + (v_0 + v_{k-1}a_1)\mathcal{A}(\boldsymbol{v}) + (v_1 + v_{k-1}a_2)\mathcal{A}^2(\boldsymbol{v}) + \ldots & \\ \cdots + (v_{k-2} + v_{k-1}a_{k-1})\mathcal{A}^{k-1}(\boldsymbol{v})) &\end{aligned}$$

также является их линейной комбинацией. Вектор $\boldsymbol{v}$ называется *циклическим* вектором, порождающим пространство $\mathbb{U}$. Про-

странство с циклическим вектором называется *циклическим* пространством.

Пример 6.8. В примере 4.18 на с. 122 было построено поле $\mathbb{F}$ из 27 элементов — поле $\mathbb{Z}_3[x]/(x^3+2x+1)$ вычетов по модулю неприводимого над $\mathbb{Z}_3$ многочлена x^3+2x+1. Нетрудно показать, что элементы $f(x)$ этого поля составляют трехмерное линейное пространство $\mathbb{V}$ над полем $\mathbb{Z}_3$ с базисом $1, x, x^2$, а отображение $\mathcal{A}: f(x) \to xf(x)$ будет линейным оператором. Так как $\mathcal{A}(1) = x, \mathcal{A}(x) = x^2$ и $\mathcal{A}(x^2) = x+2$, то $\mathbb{V}$ с действующим на нем оператором $\mathcal{A}$ будет циклическим пространством, порожденным циклическим вектором 1. □

В циклическом пространстве $\mathbb{U}$ с циклическим вектором $\boldsymbol{v}$, для которого справедливо (6.11), матрицей оператора $\mathcal{A}$ в базисе $V = \{\boldsymbol{v}, \mathcal{A}(\boldsymbol{v}), \ldots, \mathcal{A}^{k-1}(\boldsymbol{v})\}$ будет матрица

$$\mathbf{A}_V = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix}. \tag{6.12}$$

В справедливости (6.12) легко убедиться, последовательно умножив матрицу $\mathbf{A}_V$ на базисные векторы-столбцы:

$$\begin{aligned} \boldsymbol{v} &= (1,0,0,\ldots,0,0), \\ \mathcal{A}(\boldsymbol{v}) &= (0,1,0,\ldots,0,0), \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathcal{A}^{k-1}(\boldsymbol{v}) &= (0,0,0,\ldots,0,1). \end{aligned}$$

Далее будем рассматривать многочлены из $\mathbb{F}[t]$, в которые вместо переменной t будем подставлять оператор $\mathcal{A}$. Легко видеть, что значение $f(\mathcal{A})$ многочлена $f(t)$ на операторе $\mathcal{A}$ также будет линейным оператором. Так как степени любого оператора $\mathcal{A}$ коммутируют, $\mathcal{A}^m\mathcal{A}^n = \mathcal{A}^{m+n} = \mathcal{A}^n\mathcal{A}^m$, то нетрудно показать, что коммутирует и произведение произвольных многочленов $f(t)$ и $h(t)$, т. е. что выполняется равенство

$$f(\mathcal{A})h(\mathcal{A}) = h(\mathcal{A})f(\mathcal{A}). \tag{6.13}$$

Действительно, если $f(t) = f \cdot t^k$, где $f \in \mathbb{F}$, то равенство (6.13) очевидно:

$$f\mathcal{A}^k(h_n\mathcal{A}^n + \cdots + h_0\mathcal{E}) = f\mathcal{A}^k h_n\mathcal{A}^n + \cdots + f\mathcal{A}^k h_0\mathcal{E} = \\ = h_n\mathcal{A}^n f\mathcal{A}^k + \cdots + h_0\mathcal{E}f\mathcal{A}^k = (h_n\mathcal{A}^n + \cdots + h_0\mathcal{E})f\mathcal{A}^k.$$

Теперь для произвольного $f(t)$ имеем

$$(f_m\mathcal{A}^m + \cdots + f_0\mathcal{E})h(\mathcal{A}) = f_m\mathcal{A}^m h(\mathcal{A}) + \cdots + f_0\mathcal{E}h(\mathcal{A}) = \\ = h(\mathcal{A})f_m\mathcal{A}^m + \cdots + h(\mathcal{A})f_0\mathcal{E} = h(\mathcal{A})(f_m\mathcal{A}^m + \cdots + f_0\mathcal{E}).$$

Равенство (6.13) доказано.

Отметим еще одно простое свойство рассматриваемых многочленов: если пространство $\mathbb{U}$ инвариантно относительно оператора $\mathcal{A}$, то оно также инвариантно и относительно оператора $f(\mathcal{A})$ при любом многочлене f.

2. Аннуляторы и минимальные многочлены векторов. Ненулевой многочлен $f(t)$ называется *аннулятором* вектора $\boldsymbol{v}$ (говорим, что $f(t)$ аннулирует $\boldsymbol{v}$), если $f(\mathcal{A})(\boldsymbol{v}) = \mathbf{0}$. Из (6.11) следует, что многочлен $t^k - a_{k-1}t^{k-1} - \cdots - a_1 t - a_0$ будет аннулятором вектора $\boldsymbol{v}$. Отметим, что аннулятор вектора $\boldsymbol{v}$ аннулирует и вектор $\mathcal{A}(\boldsymbol{v})$.

Нормированный аннулятор вектора $\boldsymbol{u}$ минимальной степени называется *минимальным многочленом* этого вектора. Так как в конечномерном пространстве любой ненулевой вектор порождает циклическое подпространство, то в силу предыдущих рассуждений у каждого вектора найдется минимальный многочлен. Более того, справедливо следующее утверждение.

Лемма 6.4. *В конечномерном пространстве каждый вектор обладает единственным минимальным многочленом.*

Доказательство. Существование минимального многочлена показано выше. Допустим, что у некоторого вектора $\boldsymbol{u}$ есть два различных минимальных многочлена f и h. Тогда разность $f - h$ этих многочленов будет ненулевым многочленом меньшей степени, который аннулирует вектор $\boldsymbol{u}$. Противоречие. Лемма доказана.

Лемма 6.5. *Минимальный многочлен вектора $\boldsymbol{u}$ делит каждый аннулятор этого вектора.*

Доказательство. Допустим, что минимальный многочлен m вектора $\boldsymbol{u}$ не делит его аннулятор f. Тогда, разделив с остатком f на m, видим, что

$$\begin{aligned} f(\mathcal{A})(\boldsymbol{u}) &= q(\mathcal{A})(m(\mathcal{A})(\boldsymbol{u})) + r(\mathcal{A})(\boldsymbol{u}) = \\ &= q(\mathcal{A})(\mathbf{0}) + r(\mathcal{A})(\boldsymbol{u}) = r(\mathcal{A})(\boldsymbol{u}) = \mathbf{0}, \end{aligned}$$

где степень r меньше степени m и r аннулирует $\boldsymbol{u}$. Противоречие. Лемма доказана.

Лемма 6.6. *Если взаимно простые многочлены p и q одновременно аннулируют вектор $\boldsymbol{u}$, то $\boldsymbol{u}$ — нулевой вектор.*

Доказательство. Из взаимной простоты p и q следует существование таких f и h, что $1 = f(t)p(t) + h(t)q(t)$. Тогда

$$\begin{aligned} \mathcal{E}(\boldsymbol{u}) &= (f(\mathcal{A})p(\mathcal{A}) + h(\mathcal{A})q(\mathcal{A}))(\boldsymbol{u}) = \\ &= f(\mathcal{A})(p(\mathcal{A})(\boldsymbol{u})) + h(\mathcal{A})(q(\mathcal{A})(\boldsymbol{u})) = \\ &= f(\mathcal{A})(\mathbf{0}) + h(\mathcal{A})(\mathbf{0}) = \mathbf{0}, \end{aligned}$$

т. е. $\boldsymbol{u} = \mathbf{0}$. Лемма доказана.

Лемма 6.7. *Если произведение p_1p_2 взаимно простых многочленов p_1 и p_2 аннулирует вектор $\boldsymbol{u}$, то $\boldsymbol{u}$ можно представить в виде суммы $\boldsymbol{u}_1 + \boldsymbol{u}_2$, где многочлен p_1 аннулирует вектор $\boldsymbol{u}_1$, а многочлен p_2 — вектор $\boldsymbol{u}_2$.*

Доказательство. Существуют такие многочлены q_1 и q_2, что $1 = q_1(t)p_1(t) + q_2(t)p_2(t)$. Тогда

$$\boldsymbol{u} = q_1(\mathcal{A})p_1(\mathcal{A})(\boldsymbol{u}) + q_2(\mathcal{A})p_2(\mathcal{A})(\boldsymbol{u})$$

и в силу предыдущей леммы

$$\begin{aligned} p_2(\mathcal{A})(q_1(\mathcal{A})p_1(\mathcal{A})(\boldsymbol{u})) &= q_1(\mathcal{A})(p_1(\mathcal{A})p_2(\mathcal{A})(\boldsymbol{u})) = q_1(\mathcal{A})(\mathbf{0}) = \mathbf{0}, \\ p_1(\mathcal{A})(q_2(\mathcal{A})p_2(\mathcal{A})(\boldsymbol{u})) &= q_2(\mathcal{A})(p_1(\mathcal{A})p_2(\mathcal{A})(\boldsymbol{u})) = q_2(\mathcal{A})(\mathbf{0}) = \mathbf{0}. \end{aligned}$$

Положим $\boldsymbol{u}_1 = q_2(\mathcal{A})p_2(\mathcal{A})(\boldsymbol{u})$ и $\boldsymbol{u}_2 = q_1(\mathcal{A})p_1(\mathcal{A})(\boldsymbol{u})$. Лемма доказана.

Покажем, что имеет место и «обратное» утверждение.

Лемма 6.8. *Если минимальный многочлен p_1 вектора $\boldsymbol{u}_1$ и минимальный многочлен p_2 вектора $\boldsymbol{u}_2$ взаимно просты, то произведение p_1p_2 будет минимальным многочленом суммы $\boldsymbol{u}_1 + \boldsymbol{u}_2$.*

Доказательство. Пусть q — минимальный многочлен суммы $\boldsymbol{u}_1 + \boldsymbol{u}_2$. Тогда

$$\begin{aligned}\mathbf{0} &= p_1q(\mathcal{A})(\boldsymbol{u}_1 + \boldsymbol{u}_2) = qp_1(\mathcal{A})(\boldsymbol{u}_1) + p_1q(\mathcal{A})(\boldsymbol{u}_2) = \\ &= q(\mathcal{A})(p_1(\mathcal{A})(\boldsymbol{u}_1)) + p_1q(\mathcal{A})(\boldsymbol{u}_2) = \\ &= q(\mathcal{A})(\mathbf{0}) + p_1q(\mathcal{A})(\boldsymbol{u}_2) = p_1q(\mathcal{A})(\boldsymbol{u}_2).\end{aligned}$$

Следовательно, p_2 делит произведение p_1q и поэтому в силу взаимной простоты p_1 и p_2 делит q. Аналогично устанавливается делимость q на p_1. Так как q — многочлен минимальной степени, делящийся на взаимно простые p_1 и p_2, то $q = p_1p_2$. Лемма доказана.

Индукцией по числу взаимно простых многочленов нетрудно установить справедливость следующих обобщений лемм 6.7 и 6.8.

Лемма 6.9. *Если произведение $\prod_{i=1}^m p_i$ взаимно простых многочленов p_i аннулирует вектор $\boldsymbol{u}$, то $\boldsymbol{u}$ можно представить в виде суммы $\sum_{i=1}^m \boldsymbol{u}_i$, в которой многочлен p_i аннулирует вектор $\boldsymbol{u}_i$.*

Лемма 6.10. *Если минимальные многочлены p_i векторов $\boldsymbol{u}_i$ взаимно просты, $i = 1, \ldots, m$, то произведение $\prod_{i=1}^m p_i$ будет минимальным многочленом суммы $\sum_{i=1}^m \boldsymbol{u}_i$.*

3. Аннуляторы и минимальные многочлены пространств. Ненулевой многочлен f называется *аннулятором* пространства $\mathbb{U}$ относительно действующего на нем оператора $\mathcal{A}$, а также *аннулятором* оператора $\mathcal{A}$ на пространстве $\mathbb{U}$, если f аннулирует все векторы этого пространства. Нормированный аннулятор

пространства $\mathbb{U}$ минимальной степени называется *минимальным многочленом* этого пространства или *минимальным многочленом* оператора $\mathcal{A}$ на пространстве $\mathbb{U}$. Из доказательства леммы 6.4 легко следует единственность минимального многочлена любого конечномерного пространства, а из доказательства леммы 6.5 — делимость всех аннуляторов пространства на его минимальный многочлен. Нетрудно видеть, что минимальный многочлен любого конечномерного пространства должен делиться на минимальный многочлен каждого вектора пространства и поэтому будет наименьшим общим кратным минимальных многочленов векторов произвольного базиса этого пространства. Отсюда легко следует, что минимальный многочлен циклического пространства равен минимальному многочлену его циклического вектора, а минимальный многочлен любого подпространства делит минимальный многочлен всего пространства.

Будем говорить, что пространство $\mathbb{V}$ является *суммой* $\mathbb{V} = \sum_{i=1}^{m} \mathbb{U}_i$ своих подпространств $\mathbb{U}_1, \ldots, \mathbb{U}_m$, если каждый вектор $\boldsymbol{v}$ из $\mathbb{V}$ можно представить в виде суммы

$$\boldsymbol{v} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_m \tag{6.14}$$

векторов $\boldsymbol{u}_1 \in \mathbb{U}_1, \ldots, \boldsymbol{u}_m \in \mathbb{U}_m$. Если каждый вектор $\boldsymbol{v}$ из $\mathbb{V}$ представляется в виде суммы (6.14) единственным образом, то говорят, что пространство $\mathbb{V}$ разлагается в *прямую сумму* $\mathbb{V} = \bigoplus_{i=1}^{m} \mathbb{U}_i$ своих подпространств $\mathbb{U}_1, \ldots, \mathbb{U}_m$. Из единственности представления (6.14) следует, что объединение базисов $U_i = \{\boldsymbol{u}_{i1}, \ldots, \boldsymbol{u}_{ik_i}\}$ прямых слагаемых $\mathbb{U}_i$ будет базисом V пространства $\mathbb{V}$. Отметим следующий простой, но важный факт: если все прямые слагаемые $\mathbb{U}_i$ являются инвариантными подпространствами, то матрица $\mathbf{A}_V$ оператора $\mathcal{A}$ в базисе V будет иметь блочно-диагональный вид

$$\mathbf{A}_V = \begin{pmatrix} \mathbf{A}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{A}_m \end{pmatrix}, \tag{6.15}$$

где $\mathbf{A}_1, \ldots, \mathbf{A}_m$ — матрицы оператора $\mathcal{A}$ на инвариантных пространствах $\mathbb{U}_1, \ldots, \mathbb{U}_m$ в базисах $U_1, \ldots, U_m$. Такое представле-

ние оператора $\mathcal{A}$ в базисе V позволяет сводить изучение оператора $\mathcal{A}$ на пространстве $\mathbb{V}$ к нескольким более простым задачам — изучению этого оператора на пространствах $\mathbb{U}_i$ меньшей размерности. В связи с этим выясним, при каких условиях пространство с оператором разлагается в прямую сумму своих инвариантных подпространств. Оказывается, такое разложение тесно связано с видом минимального многочлена пространства. В частности, из перечисленных выше свойств минимальных многочленов следует, что минимальный многочлен прямой суммы подпространств равен наименьшему общему кратному минимальных многочленов прямых слагаемых. Имеет место и «обратное» утверждение.

Теорема 6.4. *Пусть $\prod_{i=1}^{m} p_i$ — разложение на взаимно простые множители минимального многочлена p пространства $\mathbb{U}$ с оператором $\mathcal{A}$. Тогда $\mathbb{U}$ единственным с точностью до порядка слагаемых образом разлагается в прямую сумму $\bigoplus_{i=1}^{m} \mathbb{U}_i$, где $\mathbb{U}_i$ — инвариантное подпространство с минимальным многочленом p_i.*

Доказательство. В силу леммы 6.9 каждый вектор $\boldsymbol{u}$ пространства $\mathbb{U}$ можно представить в виде суммы

$$\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_i + \cdots + \boldsymbol{u}_m, \tag{6.16}$$

в которой многочлен p_i аннулирует вектор $\boldsymbol{u}_i$. Очевидно, что для каждого $i = 1, 2, \ldots, m$ вектор $\boldsymbol{u}_i$ лежит в ядре оператора $p_i(\mathcal{A})$, ядро является инвариантным пространством и его минимальным многочленом будет делитель многочлена p_i.

Покажем, что представление (6.16) единственно для каждого $\boldsymbol{u}$ из $\mathbb{U}$. Для этого достаточно установить, что любая сумма (6.16), в которой не все слагаемые нулевые, не равна нулевому вектору. Предположим, что это не так и такая сумма $\boldsymbol{u}_{i_1} + \cdots + \boldsymbol{u}_{i_k} = \boldsymbol{0}$ из k ненулевых векторов нашлась. Тогда минимальным многочленом такой суммы, с одной стороны, будет тождественная единица, а с другой — произведение минимальных многочленов векторов $\boldsymbol{u}_{i_j}$ (в силу леммы 6.10). Полученное противоречие доказывает единственность представления (6.16),

из которого в свою очередь немедленно следует разложение $\mathbb{U}$ в прямую сумму $\bigoplus_{i=1}^{m} \operatorname{Ker} p_i(\mathcal{A})$. Единственность установленного разложения следует из однозначности определения ядер операторов $p_i(\mathcal{A})$.

Теперь заметим, что p_i аннулирует пространство $\operatorname{Ker} p_i(\mathcal{A})$ и поэтому обязан быть минимальным многочленом m_i этого пространства, так как в противном случае делитель $m_i \prod_{j\neq i} p_j$ многочлена $\prod_{j=1}^{m} p_j$ будет аннулятором пространства $\mathbb{U}$. Теорема доказана.

Пространство с минимальным многочленом равным степени неприводимого многочлена называется *примарным* пространством. Теорема 6.4 утверждает, что каждое пространство однозначно раскладывается в прямую сумму своих инвариантных примарных подпространств. В свою очередь каждое примарное пространство можно представить в виде прямой суммы примарных циклических пространств, и в общем случае такое представление не единственно.

Теорема 6.5. *Примарное пространство можно представить в виде прямой суммы примарных циклических подпространств.*

Доказательство. Теорему докажем индукцией по размерности пространства. В основание индукции положим одномерные пространства, для которых утверждение теоремы тривиально. Допустим, что теорема справедлива для каждого примарного пространства размерности не больше $n-1$.

Пусть p — неприводимый многочлен степени r. В примарном пространстве $\mathbb{V}$ размерности n с минимальным многочленом p^m найдем вектор $\boldsymbol{u}_1$, минимальный многочлен которого совпадает с минимальным многочленом p^m пространства $\mathbb{V}$, т. е. $p^m(\mathcal{A})(\boldsymbol{u}_1) = \mathbf{0}$ и $p^{m-1}(\mathcal{A})(\boldsymbol{u}_1) \neq \mathbf{0}$. Пусть $\mathbb{U}_1$ — порожденное этим вектором примарное циклическое подпространство в $\mathbb{V}$. Если $\mathbb{U}_1 = \mathbb{V}$, то $\mathbb{V}$ — циклическое пространство, и в этом случае теорема доказана.

Пусть теперь $\mathbb{U}_1$ не совпадает с $\mathbb{V}$. По предположению индукции, фактор-пространство $\overline{\mathbb{V}}$ пространства $\mathbb{V}$ по подпростран-

ству $\mathbb{U}_1$ можно представить в виде прямой суммы $\bigoplus_{i=2}^{k} \overline{\mathbb{U}}_i$ примарных циклических подпространств. Будем полагать, что для каждого $i \in \{2, \ldots, k\}$ подпространство $\overline{\mathbb{U}}_i$ порождается циклическим вектором $\boldsymbol{u}_i + \mathbb{U}_1$ и их минимальный многочлен (вектора и подпространства) равен p^{m_i}, где $m_i \leqslant m$. Так как $\deg p = r$, то $\dim \overline{\mathbb{U}}_i = m_i r$. Покажем, что в каждом смежном классе $\overline{\mathbb{U}}_i$ найдется вектор $\boldsymbol{u}_i + \boldsymbol{v}_i$, где $\boldsymbol{v}_i \in \mathbb{U}_1$, минимальный многочлен которого также равен p^{m_i}.

Так как $p^{m_i}(\mathcal{A})(\boldsymbol{u}_1) \in \mathbb{U}_1$, то этот вектор является линейной комбинацией векторов $\mathcal{A}^j(\boldsymbol{u}_1)$ и поэтому найдется такой многочлен f_i, что $p^{m_i}(\mathcal{A})(\boldsymbol{u}_1) = f_i(\mathcal{A})(\boldsymbol{u}_1)$. Из равенства $p^{m-m_i} p^{m_i}(\mathcal{A})(\boldsymbol{u}_1) = \boldsymbol{0}$, следует, что многочлен p^{m-m_i} аннулирует вектор $f_i(\mathcal{A})(\boldsymbol{u}_1)$. Поэтому многочлен f_i должен делиться на p^{m_i}, т. е. его можно представить в виде произведения $f_i = p^{m_i} \tilde{f}_i$. Положим $\boldsymbol{v}_i = -\tilde{f}_i(\mathcal{A})(\boldsymbol{u}_1)$. Тогда

$$\begin{aligned} p^{m_i}(\mathcal{A})(\boldsymbol{u}_i + \boldsymbol{v}_i) &= p^{m_i}(\mathcal{A})(\boldsymbol{u}_i) + p^{m_i}(\mathcal{A})(\boldsymbol{v}_i) = \\ &= f_i(\mathcal{A})(\boldsymbol{u}_1) + p^{m_i}(\mathcal{A})(-\tilde{f}_i(\mathcal{A})(\boldsymbol{u}_1)) = \\ &= f_i(\mathcal{A})(\boldsymbol{u}_1) - f_i(\mathcal{A})(\boldsymbol{u}_1) = 0. \end{aligned}$$

Таким образом, p^{m_i} аннулирует вектор $\boldsymbol{u}_i + \boldsymbol{v}_i$. Теперь убедимся в том, что p^{m_i} будет минимальным многочленом этого вектора. Если это не так, то из равенства $p^{m_i-1}(\mathcal{A})(\boldsymbol{u}_i + \boldsymbol{v}_i) = \boldsymbol{0}$ легко следует, что $p^{m_i-1}(\mathcal{A})(\boldsymbol{u}_i + \boldsymbol{v}) \in \mathbb{U}_1$ для любого $\boldsymbol{v}$ из $\mathbb{U}_1$. Но в этом случае многочлен p^{m_i-1} аннулирует подпространство $\overline{\mathbb{U}}_i$, что противоречит минимальности многочлена p^{m_i} для $\overline{\mathbb{U}}_i$. Таким образом, каждый вектор $\boldsymbol{u}_i + \boldsymbol{v}_i$ порождает в пространстве $\mathbb{V}$ инвариантное циклическое подпространство $\mathbb{U}_i$ размерности $m_i r$.

По предположению индукции, каждый элемент фактор-пространства $\overline{\mathbb{V}}$ однозначно представляется в виде суммы $(\boldsymbol{u}_2 + \mathbb{U}_1) + \\ + \cdots + (\boldsymbol{u}_k + \mathbb{U}_1)$ векторов подпространств $\overline{\mathbb{U}}_2, \ldots, \overline{\mathbb{U}}_k$. Отсюда легко следует, что каждый вектор $\boldsymbol{w}$ из $\mathbb{V}$ можно представить в виде сумы векторов $\boldsymbol{w}_i$ из $\mathbb{U}_i$. Поэтому для доказательства теоремы достаточно показать, что для любых одновременно неравных нулю векторов $\boldsymbol{w}_i \in \mathbb{U}_i$ сумма $\sum_{i=1}^{k} \boldsymbol{w}_i$ не равна нулевому

вектору. Действительно, если $\sum_{i=1}^{k} \boldsymbol{w}_i = \mathbf{0}$, то из предположения индукции и равенств

$$\sum_{i=2}^{k}(\boldsymbol{w}_i + \mathbb{U}_1) = \sum_{i=2}^{k} \boldsymbol{w}_i + \sum_{i=2}^{k} \mathbb{U}_1 = -\boldsymbol{w}_1 + \mathbb{U}_1 = \mathbb{U}_1$$

следует, что все $\boldsymbol{w}_i$ равны нулю. Теорема доказана.

Объединяя теоремы 6.4 и 6.5, видим, что справедливо следующее утверждение.

Теорема 6.6. *Пространство с действующим на нем оператором можно представить в виде прямой суммы примарных циклических подпространств.*

4. Теорема Гамильтона — Кэли. Рассмотрим вопрос о нахождении инвариантных примарных подпространств в пространствах с операторами. Пусть в пространстве $\mathbb{V}$ с базисом $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ действует оператор $\mathcal{A}$ с матрицей $\mathbf{A}$. Прежде всего заметим, если f — минимальный многочлен оператора $\mathcal{A}$, то матрица $\mathbf{A}$ будет корнем f, и этот многочлен можно назвать *минимальным* многочленом матрицы $\mathbf{A}$. Поэтому если минимальный многочлен $f = \prod_{i=1}^{m} p_i$, где $(p_i, p_j) = 1$, известен, то в соответствии с теоремой 6.4 для нахождения инвариантных пространств $\mathbb{U}_i$ достаточно найти ортогональные пространства матриц $p_i(\mathbf{A})$. Таким образом, задачу нахождения инвариантных примарных подпространств в общем случае можно свести к нахождению минимального многочлена пространства и разложению этого многочлена на взаимно простые множители. Найти минимальный многочлен можно с помощью алгоритма, рассматриваемого в двух следующих примерах.

Пример 6.9. Пусть в трехмерном пространстве $\mathbb{V}$ над полем $\mathbb{Z}_3$ действует оператор $\mathcal{A}$ с матрицей $\mathbf{A} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Найдем минимальный многочлен пространства $\mathbb{V}$. Так как степень минимального многочлена циклического пространства равна размерности пространства, то в силу теоремы 6.6 степень минимального многочлена любого пространства не превосходит его

размерности. Поэтому минимальный многочлен пространства $\mathbb{V}$ будем искать в виде многочлена $a_0 + a_1 t + a_2 t^2 + a_3 t^3$ с неизвестными коэффициентами a_i. Так как этот многочлен аннулирует матрицу $\mathbf{A}$,

$$\mathbf{A}^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{A}^3 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

то справедливо матричное равенство

$$a_0 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} + \\ + a_2 \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + a_3 \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

которое, очевидно, эквивалентно системе из девяти линейных уравнений

$$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 1 & 2 & 1 & 2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}. \tag{6.17}$$

Нетрудно видеть, что для матрицы из системы (6.17) справедливы эквивалентности

$$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 1 & 2 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Поэтому фундаментальная система решений системы (6.17) состоит из векторов $(1\,2\,1\,0)$ и $(1\,0\,0\,1)$, соответствующих многочленам $1+2t+t^2$ и $1+t^3$, первый из которых и будет минимальным многочленом оператора $\mathcal{A}$. $\square$

Пример 6.10. Пусть в трехмерном пространстве $\mathbb{V}$ над полем $\mathbb{Z}_3$ действует оператор $\mathcal{A}$ с матрицей $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}$. Найдем минимальный многочлен $m_{\mathbb{V}}(t)$ пространства $\mathbb{V}$. Минимальный многочлен будем искать как наименьшее общее кратное минимальных многочленов стандартного базиса этого пространства. Пусть $m_{\mathbb{V}}(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3$. Тогда матрица $m_{\mathbb{V}}(\mathbf{A}) = a_0\mathbf{E} + a_1\mathbf{A} + a_2\mathbf{A}^2 + a_3\mathbf{A}^3$ аннулирует пространство $\mathbb{V}$ и, в частности, вектор $(1\,0\,0)$ этого пространства. Подставляя

$$\mathbf{A}^2 = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{A}^3 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}$$

в $m_{\mathbb{V}}(\mathbf{A})$ и умножая получившуюся матрицу на вектор $(1\,0\,0)$, видим, что

$$a_0 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \\ + a_2 \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Последнее равенство эквивалентно уравнению

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

фундаментальная система решений которого состоит из векторов $(2\,1\,0\,0)$, $(2\,0\,1\,0)$ и $(2\,0\,0\,1)$, соответствующих многочленам $2 + t$, $2 + t^2$ и $2 + t^3$, первый из которых будет минимальным многочленом оператора вектора $(1\,0\,0)$.

Выполнив аналогичные вычисления для векторов $(0\,1\,0)$ и $(0\,0\,1)$, найдем их минимальные многочлены $1 + t + t^2$ и $1 + t$.

Таким образом,

$$m_{\mathbb{V}}(t) = \text{НОК}(2+t, 1+t+t^2, 1+t) = \\ = (1+t+t^2)(1+t) = (t-1)^2(t-2). \square$$

Если в двух рассмотренных выше примерах продолжить вычисления и найти инвариантные подпространства, то окажется, что в обоих пространствах есть одномерные инвариантные подпространства. В первом примере такое подпространство задается вектором $(0\,0\,1)$, а во втором — вектором $(1\,1\,1)$. Нахождение одномерных инвариантных подпространств — важная практическая задача[1)]. Поэтому рассмотрим ее подробнее. Найдем одномерные инвариантные подпространства (в том случае, когда такие подпространства существуют). Если $\mathbb{U}$ — одномерное инвариантное подпространство, то оно состоит из всех векторов вида $\alpha\boldsymbol{u}$, где $\boldsymbol{u}$ — некоторый вектор из $\mathbb{V}$, а α — произвольный элемент поля $\mathbb{F}$. Очевидно, что $\mathcal{A}(\boldsymbol{u}) = \lambda\boldsymbol{u}$ для некоторого λ из поля $\mathbb{F}$. Вектор $\boldsymbol{u}$ называется *собственным вектором* оператора $\mathcal{A}$, а элемент λ — *собственным значением* этого оператора, отвечающим собственному вектору $\boldsymbol{u}$. Так как

$$(\lambda\mathbf{E} - \mathbf{A})\boldsymbol{u} = \lambda\mathbf{E}\boldsymbol{u} - \mathbf{A}\boldsymbol{u} = \lambda\boldsymbol{u} - \lambda\boldsymbol{u} = \mathbf{0}, \tag{6.18}$$

то вектор $\boldsymbol{u}$ лежит в ортогональном пространстве матрицы $\lambda\mathbf{E} - \mathbf{A}$, и, следовательно, эта матрица вырождена, а ее определитель $\det(\lambda\mathbf{E} - \mathbf{A})$ равен нулю. Если t — независимая переменная, то определитель $\det(t\mathbf{E} - \mathbf{A})$ будет элементом кольца $\mathbb{F}[t]$, корни которого в силу равенства (6.18) будут собственными значениями оператора $\mathcal{A}$. Многочлен $\det(t\mathbf{E} - \mathbf{A})$ называется *характеристическим многочленом* матрицы $\mathbf{A}$, а так как определитель матрицы оператора не зависит от выбора базиса (см. (5.24)), то многочлен $\det(t\mathbf{E} - \mathbf{A})$ также называется *характеристическим многочленом* оператора $\mathcal{A}$. Вычислив корни λ_i характеристического уравнения и найдя ортогональные пространства матриц $\lambda_i\mathbf{E} - \mathbf{A}$, можно найти все одномерные инвариантные пространства.

[1)] Особое значение она имеет в пространствах над полями комплексных и действительных чисел.

Пример 6.11. Рассмотрим двумерное пространство над полем $\mathbb{Z}_3$. Пусть в этом пространстве зафиксирован базис $E = \{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ и действует оператор $\mathcal{A}$ с матрицей $\mathbf{A} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ в выбранном базисе. Тогда его характеристический многочлен

$$\det\left(\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} - \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\right) = \det\begin{pmatrix} t-2 & 2 \\ 0 & t-1 \end{pmatrix} = (t-1)(t-2)$$

имеет два корня $\lambda_1 = 1$ и $\lambda_2 = 2$. Так как

$$\lambda_1\mathbf{E} - \mathbf{A} = \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}, \quad \lambda_2\mathbf{E} - \mathbf{A} = \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix},$$

то у оператора $\mathcal{A}$ в базисе E будет два собственных вектора: $\boldsymbol{u}_1 = (1\,2)$ с собственным значением 1, и $\boldsymbol{u}_2 = (1\,0)$ с собственным значением 2. Легко видеть, что двучлен $t-1$ будет минимальным многочленом вектора $\boldsymbol{u}_1$, а двучлен $t-2$ — минимальным многочленом вектора $\boldsymbol{u}_2$. Поэтому в силу леммы 6.8 характеристический многочлен $(t-1)(t-2)$ будет и минимальным многочленом $\mathcal{A}$.

Матрицей оператора $\mathcal{A}$ в базисе $U = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ будет диагональная матрица $\mathbf{A}_U = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Так как

$$(\mathbf{A}_U - \mathbf{E})(\mathbf{A}_U - 2\mathbf{E}) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \mathbf{0},$$

то матрица $\mathbf{A}_U$ будет корнем своего характеристического многочлена. □

Пример 6.12. Рассмотрим трехмерное линейное пространство $\mathbb{V}$ из примера 6.8. Это пространство состоит из элементов поля $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$, и на нем действует линейный оператор $\mathcal{A}$ умножения на x. Нетрудно видеть, что $\mathcal{A}(1) = x, \mathcal{A}^2(1) = x^2$ и $\mathcal{A}^3(1) = \mathcal{A}(x^2) = x + 2$. Поэтому

$$(t^3 + 2t + 1)(\mathcal{A})(1) = \mathcal{A}^3(1) + 2\mathcal{A}(1) + \mathcal{E}(1) = 0.$$

Следовательно, многочлен t^3+2t+1 аннулирует вектор 1. Далее видим, что

$$\begin{aligned}(t^3+2t+1)(\mathcal{A})(x) &= (t^3+2t+1)(\mathcal{A})(\mathcal{A}(1)) = \\ &= t(t^3+2t+1)(\mathcal{A})(1) = 0, \\ (t^3+2t+1)(\mathcal{A})(x^2) &= (t^3+2t+1)(\mathcal{A})(\mathcal{A}^2(1)) = \\ &= t^2(t^3+2t+1)(\mathcal{A})(1) = 0,\end{aligned}$$

т. е. t^3+2t+1 аннулирует базис $\{1, x, x^2\}$ пространства $\mathbb{V}$ и, следовательно, все $\mathbb{V}$. Так как многочлен t^3+2t+1 неприводим, то он будет минимальным многочленом $\mathbb{V}$.

В соответствии с (6.12) матрицей $\mathbf{A}_V$ оператора $\mathcal{A}$ в базисе V из векторов-столбцов $1 = (100), x = (010), x^2 = (001)$ будет матрица $\begin{pmatrix}0 & 0 & 2\\ 1 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$, и, следовательно, эта матрица будет корнем многочлена t^3+2t+1.

Вычисляя характеристический многочлен

$$\det(t\mathbf{E}-\mathbf{A}_V) = \det\begin{pmatrix}t & 0 & 1\\ 2 & t & 2\\ 0 & 2 & t\end{pmatrix} = t^3+2t+1$$

матрицы $\mathbf{A}_V$, видим, что он совпадает с минимальным многочленом $\mathcal{A}$, и поэтому матрица $\mathbf{A}_V$ будет корнем своего характеристического многочлена. □

В двух последних примерах минимальные и характеристические многочлены совпадали. В n-мерном пространстве тождественный оператор $\mathcal{E}$ с характеристическим многочленом $(t-1)^n$ и минимальным многочленом $t-1$ показывает, что эти многочлены совпадают не всегда. В общем случае характеристический многочлен делится на минимальный. Это следует из доказываемой далее теоремы Гамильтона — Кэли.

Теорема 6.7 (Гамильтон — Кэли)**.** *Минимальный многочлен линейного оператора делит его характеристический многочлен.*

Доказательство. В силу теорем 6.4 и 6.5 пространство $\mathbb{V}$ с действующим на нем оператором $\mathcal{A}$ можно представить в виде прямой суммы $\bigoplus_{i=1}^{m} \mathbb{U}_i$ инвариантных примарных циклических подпространств $\mathbb{U}_i$. Из (6.15) следует существование базиса V, в котором матрица оператора $\mathcal{A}$ будет иметь блочно-диагональный вид:

$$\mathbf{A}_V = \begin{pmatrix} \mathbf{A}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{A}_m \end{pmatrix},$$

где $\mathbf{A}_1, \ldots, \mathbf{A}_m$ — матрицы этого оператора на инвариантных пространствах $\mathbb{U}_1, \ldots, \mathbb{U}_m$. Следовательно, определитель

$$\det(t\mathbf{E} - \mathbf{A}_V) = \det \begin{pmatrix} t\mathbf{E} - \mathbf{A}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & t\mathbf{E} - \mathbf{A}_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & t\mathbf{E} - \mathbf{A}_m \end{pmatrix}$$

будет характеристическим многочленом $f_{\mathcal{A}}$ оператора $\mathcal{A}$. Из последнего равенства немедленно следует, что

$$f_{\mathcal{A}}(t) = \det(t\mathbf{E} - \mathbf{A}_V) = \prod_{i=1}^{m} \det(t\mathbf{E} - \mathbf{A}_i). \tag{6.19}$$

Покажем, что характеристический многочлен f оператора $\mathcal{A}$ на каждом циклическом подпространстве $\mathbb{U}$ равен минимальному многочлену этого подпространства. Пусть $\boldsymbol{v}$ — циклический вектор в $\mathbb{U}$. Допустим, что векторы $\boldsymbol{v}, \mathcal{A}(\boldsymbol{v}), \ldots, \mathcal{A}^{k-1}(\boldsymbol{v})$ линейно независимы и

$$\mathcal{A}^k(\boldsymbol{v}) = a_{k-1}\mathcal{A}^{k-1}(\boldsymbol{v}) + a_{k-2}\mathcal{A}^{k-2}(\boldsymbol{v}) + \cdots + a_1\mathcal{A}(\boldsymbol{v}) + a_0\boldsymbol{v}.$$

Тогда $m(t) = t^k - a_{k-1}t^{k-1} - a_{k-2}t^{k-2} - \cdots - a_1 t - a_0$ — минимальный многочлен $\mathbb{U}$. Возьмем матрицу оператора $\mathcal{A}$ в базисе

$\boldsymbol{v}, \mathcal{A}(\boldsymbol{v}), \ldots, \mathcal{A}^{k-1}(\boldsymbol{v})$ и найдем характеристический многочлен

$$f(t) = \det(t\mathbf{E} - \mathbf{A}) = \det \begin{pmatrix} t & 0 & \cdots & 0 & -a_0 \\ -1 & t & \cdots & 0 & -a_1 \\ 0 & -1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t - a_{k-1} \end{pmatrix}.$$

Для вычисления определителя к его первой строке прибавим вторую, умноженную на t, затем третью, умноженную на t^2, и т. д. В конце прибавим последнюю строку, умноженную на t^{k-1}. В результате получим определитель

$$\det \begin{pmatrix} 0 & 0 & \cdots & 0 & m(t) \\ -1 & t & \cdots & 0 & -a_1 \\ 0 & -1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t - a_{k-1} \end{pmatrix},$$

раскладывая который по первой строке видим, что

$$f(t) = (-1)^{k+1}(-1)^{k-1}m(t) = m(t).$$

Таким образом, если $m_{\mathcal{A}}$ — минимальный многочлен $\mathcal{A}$ на пространстве $\mathbb{V}$, m_i — минимальный многочлен подпространства $\mathbb{U}_i$, то из свойств минимальных многочленов и (6.19) следуют равенства

$$m_{\mathcal{A}} = \text{НОК}(m_1, \ldots, m_m), \qquad f_{\mathcal{A}} = m_1 \times \ldots \times m_m,$$

из которых в свою очередь легко следует делимость $f_{\mathcal{A}}$ на $m_{\mathcal{A}}$. Теорема доказана.

Теорему Гамильтона — Кэли можно переформулировать в терминах матриц и их характеристических многочленов. Нетрудно видеть, что на этом языке она превращается в следующее утверждение.

Теорема 6.8 (Гамильтон — Кэли)**.** *Каждая квадратная матрица является корнем своего характеристического многочлена.*

Докажем теорему Гамильтона — Кэли еще раз. В новом прямом доказательстве не будем использовать теорему о разложении пространства в прямую сумму инвариантных примарных циклических подпространств. Вместо этого воспользуемся равенством (5.36), утверждающим, что произведение произвольной матрицы $\mathbf{M}$ и ее присоединенной матрицы $\widehat{\mathbf{M}}$ равно единичной матрице, умноженной на $\det \mathbf{M}$.

Доказательство. Пусть $\mathbf{A}$ — квадратная матрица порядка n с элементами из поля $\mathbb{F}$, t — независимая переменная, $\mathbf{B}$ — присоединенная матрица матрицы $t\mathbf{E}-\mathbf{A}$. Определитель матрицы $t\mathbf{E}-\mathbf{A}$ является многочленом n-й степени из $\mathbb{F}[t]$, а элементы матрицы $\mathbf{B}$ — минорами $(n-1)$-го порядка матрицы $t\mathbf{E}-\mathbf{A}$ и, следовательно, многочленами $(n-1)$-й степени из $\mathbb{F}[t]$. Поэтому

$$\begin{aligned}\det(t\mathbf{E}-\mathbf{A}) &= t^n + d_{n-1}t^{n-1} + d_{n-2}t^{n-2} + \cdots + d_1 t + d_0,\\ \mathbf{B} &= \mathbf{B}_{n-1}t^{n-1} + \mathbf{B}_{n-2}t^{n-2} + \cdots + \mathbf{B}_1 t + \mathbf{B}_0,\end{aligned}$$

где $\mathbf{B}_{n-1}, \mathbf{B}_{n-2}, \ldots, \mathbf{B}_1, \mathbf{B}_0$ — матрицы с элементами из поля $\mathbb{F}$. В силу равенства (5.36)

$$\mathbf{B}(t\mathbf{E}-\mathbf{A}) = (\det(t\mathbf{E}-\mathbf{A}))\mathbf{E}.$$

Тогда

$$\begin{aligned}(\mathbf{B}_{n-1}t^{n-1} + \mathbf{B}_{n-2}t^{n-2} + \cdots + \mathbf{B}_1 t + \mathbf{B}_0)(t\mathbf{E}-\mathbf{A}) =\\ = (t^n + d_{n-1}t^{n-1} + d_{n-2}t^{n-2} + \cdots + d_1 t + d_0)\mathbf{E}.\end{aligned} \tag{6.20}$$

Приравнивая коэффициенты при одинаковых степенях t в правой и левой частях (6.20) приходим к равенствам

$$\begin{aligned}\mathbf{B}_{n-1} &= \mathbf{E},\\ \mathbf{B}_{n-2} - \mathbf{B}_{n-1}\mathbf{A} &= d_{n-1}\mathbf{E},\\ \mathbf{B}_{n-3} - \mathbf{B}_{n-2}\mathbf{A} &= d_{n-2}\mathbf{E},\\ &\cdots\cdots\cdots\cdots\\ \mathbf{B}_0 - \mathbf{B}_1\mathbf{A} &= d_1\mathbf{E},\\ -\mathbf{B}_0\mathbf{A} &= d_0\mathbf{E}.\end{aligned}$$

Умножив первое из этих равенств справа на $\mathbf{A}^n$, второе на $\mathbf{A}^{n-1}$ и т. д., получим новые равенства

$$\begin{aligned}
\mathbf{B}_{n-1}\mathbf{A}^n &= \mathbf{A}^n,\\
\mathbf{B}_{n-2}\mathbf{A}^{n-1} - \mathbf{B}_{n-1}\mathbf{A}^n &= d_{n-1}\mathbf{A}^{n-1},\\
\mathbf{B}_{n-3}\mathbf{A}^{n-2} - \mathbf{B}_{n-2}\mathbf{A}^{n-1} &= d_{n-2}\mathbf{A}^{n-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\mathbf{B}_0\mathbf{A} - \mathbf{B}_1\mathbf{A}^2 &= d_1\mathbf{A},\\
-\mathbf{B}_0\mathbf{A} &= d_0\mathbf{E},
\end{aligned}$$

сложив которые получим равенство

$$\mathbf{0} = \mathbf{A}^n + d_{n-1}\mathbf{A}^{n-1} + d_{n-2}\mathbf{A}^{n-2} + \cdots + d_1\mathbf{A} + d_0\mathbf{E},$$

в правой части которого видим характеристический многочлен матрицы $\mathbf{A}$, где вместо переменной t стоит сама матрица $\mathbf{A}$. Теорема доказана.

Дополним теорему Гамильтона — Кэли следующим простым утверждением.

Лемма 6.11. *Пусть* $\prod_{i=1}^m p_i^{k_i}$, $\prod_{i=1}^m p_i^{l_i}$ — *разложения на неприводимые множители характеристического и минимального многочленов оператора* $\mathcal{A}$. *Тогда* $\operatorname{Ker} p_i^{k_i}(\mathcal{A}) = \operatorname{Ker} p_i^{l_i}(\mathcal{A})$ *для каждого* i.

Доказательство. Если $k_i = l_i$ для каждого i, то утверждение леммы тривиально. Поэтому далее без ограничения общности будем полагать, что $k_1 > l_1$. Если $\operatorname{Ker} p_1^{k_1}(\mathcal{A}) \neq \operatorname{Ker} p_1^{l_1}(\mathcal{A})$, то существует такой вектор $\boldsymbol{v}$, что его аннулирует $p_1^{k_1}$ и не аннулирует $p_1^{l_1}$. При $m = 1$ существование $\boldsymbol{v}$ противоречит минимальности многочлена $p_1^{l_1}$. При $m > 1$ ненулевой вектор $\boldsymbol{u} = p_1^{l_1}(\mathcal{A})(\boldsymbol{v})$ аннулируется двумя взаимно простыми многочленами $p_1^{k_1-l_1}$ и $\prod_{i=2}^m p_i^{l_i}$. Следовательно, в силу леммы 6.6 $\boldsymbol{u} = \mathbf{0}$. Противоречие. Лемма доказана.

Теорема Гамильтона — Кэли и лемма 6.11 показывают, что для нахождения инвариантных примарных подпространств не

обязательно находить минимальный многочлен пространства. Вместо него можно воспользоваться характеристическим многочленом, который относительно легко вычисляется в пространствах небольшой размерности.

Пример 6.13. Рассмотрим трехмерное пространство $\mathbb{V}$ над полем $\mathbb{Z}_3$. Пусть в этом пространстве зафиксирован базис $E = \{\boldsymbol{e}_1, \boldsymbol{e}_2\, \boldsymbol{e}_3\}$ и действует оператор $\mathcal{A}$ с матрицей $\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix}$ в выбранном базисе. Тогда у его характеристического многочлена

$$\det \begin{pmatrix} t-1 & 1 & 2 \\ 0 & t-2 & 1 \\ 1 & 1 & t-1 \end{pmatrix} = (t-1)^2(t-2)$$

есть корень $\lambda_1 = 1$ кратности два и простой корень $\lambda_2 = 2$. Вычисляя $(t-1)^2(\mathbf{A})$, видим, что

$$(\mathbf{A}-\mathbf{E})^2 = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 2 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 2 \end{pmatrix}.$$

Следовательно, столбцы ортогональной матрицы $\begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$ образуют базис $\{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ двумерного инвариантного подпространства. Вычислив аналогичным образом

$$(t-2)(\mathbf{A}) = \mathbf{A} - 2\mathbf{E} = \begin{pmatrix} 2 & 2 & 1 \\ 0 & 0 & 2 \\ 2 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

находим одномерное инвариантное подпространство, порожденное собственным вектором $\boldsymbol{u}_3 = (1\,2\,0)$. Так как

$$\mathbf{A}\boldsymbol{u}_1 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = 2\boldsymbol{u}_1 + \boldsymbol{u}_2,$$

$$\mathbf{A}\boldsymbol{u}_2 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 2\boldsymbol{u}_1$$

и $\mathbf{A}\boldsymbol{u}_3 = 2\boldsymbol{u}_3$, то матрица $\begin{pmatrix} 2 & 2 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ будет матрицей оператора $\mathcal{A}$ в базисе $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$. □

5. Циклические пространства. Далее будем рассматривать циклические пространства и их минимальные многочлены. Из доказательства теоремы Гамильтона — Кэли следует, что степень минимального многочлена циклического пространства совпадает с его размерностью. Дадим простое независимое доказательство этого факта.

Лемма 6.12. *Если* $\mathbb{U}$ *— циклическое пространство, то степень его минимального многочлена равна его размерности.*

Доказательство. Пусть $\boldsymbol{u}$ — циклический вектор, порождающий $\mathbb{U}$. Допустим, что степень минимального многочлена m пространства $\mathbb{U}$ меньше его размерности n, т. е.

$$m(\mathcal{A}) = a_{n-1}\mathcal{A}^{n-1} + a_{n-2}\mathcal{A}^{n-2} + \cdots + a_1\mathcal{A} + a_0\mathcal{E}.$$

Тогда для каждого вектора из пространства $\mathbb{U}$, в том числе и для циклического вектора $\boldsymbol{u}$, справедливо равенство

$$a_{n-1}\mathcal{A}^{n-1}(\boldsymbol{u}) + a_{n-2}\mathcal{A}^{n-2}(\boldsymbol{u}) + \cdots + a_1\mathcal{A}(\boldsymbol{u}) + a_0\boldsymbol{u} = \mathbf{0},$$

из которого немедленно следует линейная зависимость векторов $\mathcal{A}^{n-1}(\boldsymbol{u}), \ldots, \mathcal{A}(\boldsymbol{u}), \boldsymbol{u}$, что, очевидно, противоречит цикличности вектора $\boldsymbol{u}$. Следовательно, степень m равна n. Лемма доказана.

Заметим, что степень минимального многочлена пространства не превосходит степени характеристического многочлена, и, следовательно, размерности пространства.

В трех следующих леммах покажем, что верно обращение леммы 6.12 — пространство будет циклическим, если его размерность равна степени его минимального многочлена.

Лемма 6.13. *Если в пространстве* $\mathbb{U}$ *найдется такой вектор* $\boldsymbol{u}$*, что степень его минимального многочлена равна размерности* $\mathbb{U}$*, то* $\boldsymbol{u}$ *— циклический вектор и* $\mathbb{U}$ *— циклическое пространство.*

Доказательство. Пусть $k = \dim \mathbb{U}$ и степень минимального многочлена $\boldsymbol{u}$ равна k. Если векторы $\boldsymbol{u}, \mathcal{A}(\boldsymbol{u}), \ldots, \mathcal{A}^{k-1}(\boldsymbol{u})$ линейно зависимы, то найдутся такие не равные одновременно нулю элементы $a_0, a_1, \ldots, a_{k-1}$, что

$$a_{k-1}\mathcal{A}^{k-1}(\boldsymbol{u}) + a_{k-2}\mathcal{A}^{k-2}(\boldsymbol{u}) + \cdots + a_1\mathcal{A}(\boldsymbol{u}) + a_0\boldsymbol{u} = \boldsymbol{0}. \quad (6.21)$$

В этом случае

$$(a_{k-1}t^{k-1} + a_{k-2}t^{k-2} + \cdots + a_1t + a_0)(\mathcal{A})(\boldsymbol{u}) = \boldsymbol{0},$$

т. е. многочлен степени меньшей k аннулирует вектор $\boldsymbol{u}$. Противоречие. Следовательно векторы $\boldsymbol{u}, \mathcal{A}(\boldsymbol{u}), \ldots, \mathcal{A}^{k-1}(\boldsymbol{u})$ линейно независимы и $\mathbb{U}$ порождается вектором $\boldsymbol{u}$. Лемма доказана.

Лемма 6.14. *Если размерность примарного пространства* $\mathbb{U}$ *равна степени его минимального многочлена, то* $\mathbb{U}$ *— циклическое пространство.*

Доказательство. Пусть p^k — минимальный многочлен $\mathbb{U}$. В силу леммы 6.13 пространство $\mathbb{U}$ будет циклическим, если найдется такой вектор $\boldsymbol{u}$, что его минимальным многочленом будет многочлен p^k. Допустим, что такого вектора нет. Тогда из леммы 6.5 следует, что каждый вектор в $\mathbb{U}$ аннулируется многочленом p^{k-1}, т. е. p^{k-1} будет аннулятором $\mathbb{U}$. Противоречие. Лемма доказана.

Лемма 6.15. *Если размерность пространства* $\mathbb{U}$ *равна степени его минимальноого многочлена, то* $\mathbb{U}$ *— циклическое пространство.*

Доказательство. Лемму докажем индукцией по размерности пространства. В основание индукции положим очевидный случай пространства единичной размерности. Предположим, что лемма верна для всех пространств размерности не

более n. Пусть p — минимальный многочлен $(n+1)$-мерного пространства $\mathbb{U}$. Если p является степенью неприводимого многочлена, то в силу леммы 6.14 пространство $\mathbb{U}$ будет циклическим. Если p разлагается в произведение p_1p_2 взаимно простых многочленов меньшей степени, то в силу теоремы 6.4 пространство $\mathbb{U}$ разлагается в прямую сумму подпространств $\mathbb{U}_1$ и $\mathbb{U}_2$, сумма размерностей которых равна $n+1$ и, очевидно, совпадает с суммой степеней их минимальных многочленов p_1 и p_2. Так как степень минимального многочлена подпространства не превосходит его размерности, то $\deg p_i = \dim \mathbb{U}_i$ для $i = 1, 2$. Поэтому из предположения индукции следует, что в $\mathbb{U}_1$ и $\mathbb{U}_2$ найдутся циклические векторы $\boldsymbol{u}_1$ и $\boldsymbol{u}_2$ с минимальными многочленами p_1 и p_2. В свою очередь из леммы 6.10 следует, что минимальным многочленом суммы $\boldsymbol{u}_1 + \boldsymbol{u}_2$ будет произведение p_1p_2. А так как $\deg p_1p_2 = \dim \mathbb{U}$, то в силу леммы 6.13 вектор $\boldsymbol{u}_1 + \boldsymbol{u}_2$ будет циклическим вектором в $\mathbb{U}$. Лемма доказана.

Объединяя утверждения лемм 6.12 и 6.15, получаем следующую полезную теорему.

Теорема 6.9. *Пусть $\mathcal{A}$ — линейный оператор в конечномерном пространстве $\mathbb{U}$. Пространство $\mathbb{U}$ будет циклическим относительно $\mathcal{A}$ тогда и только тогда, когда его размерность равна степени его минимального многочлена.*

Нетрудно видеть, что утверждение теоремы 6.9 можно переформулировать следующим образом.

Теорема 6.10. *Пространство с оператором будет циклическим тогда и только тогда, когда его минимальный и характеристический многочлены совпадают.*

Пример 6.14. Вернемся к трехмерному пространству $\mathbb{V}$ с действующим на нем оператором $\mathcal{A}$ из примера 6.13. Так как $\mathcal{A}(\boldsymbol{u}_1) = 2\boldsymbol{u}_1 + \boldsymbol{u}_2$, то подпространство $\langle \boldsymbol{u}_1, \boldsymbol{u}_2 \rangle$ будет циклическим с циклическим вектором $\boldsymbol{u}_1$ и минимальным многочленом $(t-1)^2$. Поэтому $\mathbb{V}$ также будет циклическим пространством с циклическим вектором $\boldsymbol{u}_1 + \boldsymbol{u}_3$ и минимальным многочленом $(t-1)^2(t-2)$. $\square$

Задачи

6.1. Найти все идеалы кольца верхнетреугольных матриц размера 2×2 с элементами из: 1) $\mathbb{Z}$; 2) $\mathbb{Z}_p$.

6.2. Доказать, что квадратные матрицы размера $n \times n$, в каждой строке и каждом столбце которых одна единица, а остальные элементы — нули, с операцией умножения образуют группу, изоморфную группе S_n.

6.3. Решить над полем $\mathbb{Z}_5$ систему уравнений

$$\left(\begin{array}{ccccc|c} 0 & 1 & 3 & 2 & 1 & 4 \\ 2 & 2 & 0 & 1 & 4 & 0 \\ 3 & 0 & 2 & 4 & 3 & 1 \\ 4 & 3 & 1 & 4 & 2 & 3 \end{array}\right).$$

6.4. Решить систему уравнений над полем $\mathbb{Z}_5[x]/(x^2+x+2)$:

$$\left.\begin{array}{l} (3x+2)\alpha + (4x+1)\beta = 2x+3, \\ (2x+4)\alpha + (3x+4)\beta = x+4. \end{array}\right\}$$

6.5. Даны матрицы над полем $\mathbb{Z}_3$:

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}; \quad \mathbf{B} = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}; \quad \mathbf{C} = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{pmatrix}.$$

Найти их определители и ранги. Найти присоединенные и обратные к ним матрицы (если они обратимы). Вычислить $\det \mathbf{C}^{2015}$. Выяснить, коммутируют ли матрицы $\mathbf{A}$ и $\mathbf{B}$. Решить матричное уравнение $\mathbf{AXB} = \mathbf{B}^3$.

6.6. Найти все целые решения уравнения:
1) $10x_1+2x_2+12x_3+8x_4+14x_5 = 2$; 2) $3x_1+5x_2+7x_3+9x_4+11x_5 = 15$.

6.7. Привести пример линейного оператора над полем $\mathbb{Z}_3$, ядром которого является линейная оболочка векторов `12011` и `21102`.

6.8. Найти какой-либо базис пространства, ортогонального пространству $\mathbb{V} = \langle \mathtt{12011}, \mathtt{21102} \rangle \subset \mathbb{Z}_3^5$.

6.9. Известно, что линейный оператор f над полем $\mathbb{Z}_3$ переводит векторы стандартного базиса $\boldsymbol{e}_1 = \mathtt{10000}$, …, $\boldsymbol{e}_5 = \mathtt{00001}$ в векторы `121`, `022`, `221`, `101`, `212` соответственно. Найти ядро и образ оператора f. Найти образ вектора $f(\mathtt{20112})$ и полный прообраз вектора `210`.

6.10. Пусть A — подмножество, не обязательно являющееся подпространством, в некотором линейном пространстве $\mathbb{V}$. Будем называть множество $A^\perp = \{\boldsymbol{x} \in \mathbb{V} : \boldsymbol{x} \perp A\}$, состоящее из векторов, ортогональных каждому вектору из A, ортогональным к A. Является ли $A^\perp$ подпространством в $\mathbb{V}$?

6.11. Оценить сложность метода Гаусса (в худшем случае) для системы линейных уравнений с квадратной матрицей размера $n \times n$.

6.12. Показать, что линейный оператор невырожден тогда и только тогда, когда свободный член его минимального многочлена отличен от нуля.

6.13. Пусть многочлен p_i аннулирует вектор $\boldsymbol{v}_i$, $i = 1, \ldots, k$. Показать, что многочлен $\text{НОК}(p_1, \ldots, p_k)$ аннулирует любую линейную комбинацию векторов $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$.

6.14. Оператор $\mathcal{A}$ действует в k-мерном пространстве и имеет k собственных векторов $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ с попарно различными собственными значениями. Показать, что собственные векторы линейно независимы и в базисе $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ матрица оператора $\mathcal{A}$ диагональна.

6.15. В пространстве $\mathbb{Z}_3^3$ действует линейный оператор $\mathcal{A}$ с матрицей $\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Указать два различных разложения $\mathbb{Z}_3^3$ в прямую сумму циклических подпространств.

6.16. Пусть $\mathcal{A}$ — линейный оператор и $f(t)$ — многочлен. Показать на примере, что инвариантное относительно оператора $f(\mathcal{A})$ пространство не обязательно инвариантно относительно $\mathcal{A}$. Доказать, что пространство $\operatorname{Ker} f(\mathcal{A})$ инвариантно относительно $\mathcal{A}$ при любом $f(t)$.

6.17. Доказать, что минимальный многочлен циклического пространства совпадает с минимальным многочленом его циклического вектора.

6.18. Пусть $\mathbb{V}$ — примарное циклическое пространство с минимальным многочленом p^k. Найти все инвариантные подпространства в $\mathbb{V}$.

6.19. Используя примеры 6.9 и 6.10, сформулировать и обосновать алгоритм вычисления минимального многочлена пространства. Оценить число операций над элементами поля, выполняемых при работе этого алгоритма.

6.20. Пусть $\mathcal{D}$ — оператор дифференцирования в пространстве $\mathbb{V}$ многочленов над $\mathbb{R}$ степени не выше трех. Показать, что этот оператор линейный. Найти его ранг, минимальный и характеристический

многочлены. Разложить $\mathbb{V}$ в прямую сумму инвариантных примарных циклических подпространств.

6.21. Решить предыдущую задачу для оператора дифференцирования в пространстве многочленов над $\mathbb{R}$ степени не выше n.

6.22. Пусть $\mathcal{A}$ — оператор умножения на x в пространстве многочленов из $\mathbb{Z}_2[x]/(x^4+x+1)$. Показать, что этот оператор линейный. Найти его ранг, минимальный и характеристический многочлены. Разложить пространство в прямую сумму инвариантных примарных циклических подпространств.

6.23. Решить предыдущую задачу для оператора умножения на x в пространстве многочленов из:
1) $\mathbb{Z}_2[x]/(x^5+x^2+1)$; 2) $\mathbb{Z}_2[x]/(x^5+x^3+1)$; 3) $\mathbb{Z}_2[x]/(x^n-1)$.

6.24. Пусть оператор $\mathcal{A}$ действует в пространстве многочленов над $\mathbb{Z}_5$ степени не выше четырех и отображает многочлен f в набор его остатков от деления на многочлены $x, x+1, x+2, x+3$. Будет ли этот оператор линейным? Если будет, то найти его ранг и ядро.

6.25. Пусть оператор $\mathcal{A}: \mathbb{Z}_5^5 \to \mathbb{Z}_5^5$ отображает коэффициенты многочлена f над $\mathbb{Z}_5$ степени не выше четырех в набор его остатков от деления на многочлены $x, x+1, x+2, x+3, x+4$. Будет ли этот оператор линейным? Если будет, то найти его ранг, минимальный и характеристический многочлены. Разложить пространство $\mathbb{Z}_5^5$ в прямую сумму инвариантных примарных циклических подпространств и выяснить, единственно ли полученное разложение. Указать базис пространства, в котором матрица оператора имеет наиболее простой вид.

6.26. Пусть степень минимального многочлена примарного пространства $\mathbb{V}$ равна его размерности. Доказать, что $\mathbb{V}$ нельзя представить в виде прямой суммы двух инвариантных подпространств.

Глава 7

Структура конечных групп

В этой главе для произвольной конечной группы устанавливаются критерии существования в этой группе подгруппы данного порядка. Затем на основе полученных результатов показывается, что конечная группа является прямым произведением своих подгрупп специального вида. В конце главы подробно изучается структура мультипликативной группы кольца $\mathbb{Z}_m$.

7.1. Действие группы на множестве

Будем говорить, что *группа G действует на множестве X*, если каждому элементу g группы G поставлено в соответствие взаимно однозначное отображение $\varphi(g)$ множества X в себя так, что $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ для любых g_1 и g_2 из G. Иначе говоря, группа G действует на множестве X, если определен гомоморфизм φ группы G в множество взаимно однозначных отображений множества X в себя. Рассматривая далее действие группы G на множестве X, будем опускать символ гомоморфизма и будем рассматривать элементы группы G непосредственно как преобразования множества X: результат действия элемента g группы G на элементе x множества X будем обозначать через $g(x)$.

Пусть группа G действует на множестве X. *Стабилизатором* элемента x_0 из X называется множество $\mathrm{St}(x_0) = \{g \in \in G \,|\, g(x_0) = x_0\}$. *Орбитой элемента* x_0 из X называется множество $\mathrm{Or}(x_0) = \{x \in X \,|\, x = g(x_0), \text{где } g \in G\}$, число элементов орбиты называется ее длиной. Орбита единичной длины называется *неподвижной* (*или стационарной*) *точкой*.

Пример 7.1. G — произвольная конечная группа, H — ее подгруппа. Пусть подгруппа H действует сдвигами на множестве элементов группы G, т. е. элемент h подгруппы H преобразует элемент g группы G в произведение hg. В этом случае элементы группы G образуют $|G|/|H|$ орбит, каждая из которых является смежным классом группы G по подгруппе H, и для каждого $g \in G$ его стабилизатор состоит только из единичного элемента. □

Пример 7.2. Рассмотрим действие сопряжениями подгруппы $\langle(12)\rangle$ группы S_3 на множестве всех элементов этой группы. Напомним, что при сопряжениях элемент h подгруппы H преобразует элемент g группы G в произведение hgh^{-1}. Так как

$$(12)(12)(12) = (12), \quad (12)(13)(12) = (23), \quad (12)(23)(12) = (13)$$
$$(12)(123)(12) = (132), \quad (12)(132)(12) = (123), \quad (12)e(12) = e,$$

то множество элементов группы S_3 распадается на две неподвижные точки $\{e\}$ и $\{(12)\}$ и две двухэлементные орбиты $\{(13),(23)\}$ и $\{(123),(132)\}$. Стабилизатором элементов e и (12) будет подгруппа $\langle(12)\rangle$, а стабилизаторы остальных элементов состоят из одного единичного элемента. □

Покажем, что при действии группы G на множестве X стабилизатор любого элемента x является подгруппой в группе G. Для этого достаточно установить, что множество $\mathrm{St}(x)$ замкнуто относительно групповой операции, единичный элемент группы G принадлежит $\mathrm{St}(x)$ и вместе с любым элементом $g \in \mathrm{St}(x)$ элемент g^{-1} также принадлежит $\mathrm{St}(x)$. Замкнутость множества $\mathrm{St}(x)$ следует из того, что если g_1 и g_2 принадлежат $\mathrm{St}(x)$, то

$$g_1g_2(x) = g_1(g_2(x)) = g_1(x) = x,$$

и поэтому произведение g_1g_2 также принадлежит $\mathrm{St}(x)$. Принадлежность единичного элемента группы G стабилизатору элемента x очевидна, так как единичный элемент оставляет на месте все элементы множества X. Таким образом осталось показать, что если элемент g принадлежит стабилизатору x, то вместе с ним в стабилизаторе x присутствует и его обратный элемент g^{-1}.

Действительно, так как для любого $x \in X$ и любого $g \in \mathrm{St}(x)$ справедливы равенства

$$x = g^{-1}g(x) = g^{-1}(g(x)) = g^{-1}(x),$$

то $g^{-1} \in \mathrm{St}(x)$. Таким образом, $\mathrm{St}(x)$ — подгруппа группы G.

Теорема 7.1. *Пусть конечная группа G действует на конечном множестве X. Тогда для любого x из X*

$$|\mathrm{Or}(x)| \cdot |\mathrm{St}(x)| = |G|.$$

Доказательство. Покажем, что длина орбиты произвольного элемента x из X равна числу смежных классов группы G по подгруппе $\mathrm{St}(x)$. Для этого достаточно показать, что элементы из одного смежного класса переводят x в один и тот же элемент множества X, а элементы из разных смежных классов — в разные элементы множества X.

Если g_1 и g_2 лежат в одном и том же смежном классе группы G по подгруппе $\mathrm{St}(x)$, то $g_2 = g_1 s$, где $s \in \mathrm{St}(x)$. Поэтому

$$g_2(x) = g_1 s(x) = g_1(s(x)) = g_1(x),$$

т. е. элементы из одного и того же смежного класса группы G по подгруппе $\mathrm{St}(x)$ отображают x в один и тот же элемент множества X. Теперь покажем, что элементы из разных смежных классов группы G по подгруппе $\mathrm{St}(x)$ отображают x в разные элементы множества X. Допустим, что $g_1(x) = g_2(x)$, тогда

$$x = g_1^{-1}g_1(x) = g_1^{-1}(g_1(x)) = g_1^{-1}(g_2(x)) = g_1^{-1}g_2(x),$$

и, следовательно, $g_1^{-1}g_2 \in \mathrm{St}(x)$. Но тогда в $\mathrm{St}(x)$ найдется такой элемент s, что $g_2 = g_1 s$ и поэтому g_1 и g_2 лежат в одном и том же смежном классе группы G по подгруппе $\mathrm{St}(x)$.

Так как число смежных классов группы G по подгруппе $\mathrm{St}(x)$ равно $|G|/|\mathrm{St}(x)|$, а длина орбиты элемента x равна числу смежных классов группы G по подгруппе $\mathrm{St}(x)$, то $|\mathrm{Or}(x)| \cdot |\mathrm{St}(x)| = |G|$. Теорема доказана.

Пример 7.3. Пусть G — произвольная конечная группа, $\{H_i\}$ — множество всех ее подгрупп. Будем говорить, что группа G действует сопряжениями на $\{H_i\}$, если элемент g группы G преобразует подгруппу H в gHg^{-1}. Прежде всего заметим, что поскольку в каждой группе G для любых элементов h_i, h_j и h из ее подгруппы H

$$gh_ig^{-1} \cdot gh_jg^{-1} = gh_ih_jg^{-1}, \quad geg^{-1} = e, \quad ghg^{-1} \cdot gh^{-1}g^{-1} = e,$$

то множество gHg^{-1} также будет подгруппой в G. Кроме того, если $h_i \in H_i$ и $\notin H_j$, то $gh_ig^{-1} \in gH_ig^{-1}$ и $gh_ig^{-1} \notin gH_jg^{-1}$, т. е. сопряжение элементом g является инъективным преобразованием конечного множества подгрупп группы G в себя, и, следовательно, является подстановкой на этом множестве. Таким образом, действие группы сопряжениями на множестве подгрупп определено корректно.

Рассмотрим группу S_3 и действие этой группы сопряжениями на множестве всех ее *несобственных* (отличных от $\{e\}$ и самой группы) подгрупп. Таких подгрупп в S_3 ровно четыре — три подгруппы $H_1 = \{e, (12)\}$, $H_2 = \{e, (13)\}$ и $H_3 = \{e, (23)\}$ порядка два и одна подгруппа $H_4 = \{e, (123), (132)\}$ порядка три. Так как сопряжения оставляют единичный элемент на месте и

$$\begin{array}{lll} (12)(12)(12) = (12), & (13)(12)(13) = (23), & (23)(12)(23) = (13) \\ (12)(13)(12) = (23), & (13)(13)(13) = (13), & (23)(13)(23) = (12) \\ (12)(23)(12) = (13), & (13)(23)(13) = (12), & (23)(23)(23) = (23), \end{array}$$

то легко видеть, что

$$\begin{array}{lll} (12)H_1(12) = H_1, & (13)H_1(13) = H_3, & (23)H_1(23) = H_2 \\ (12)H_2(12) = H_3, & (13)H_2(13) = H_2, & (23)H_2(23) = H_1 \\ (12)H_3(12) = H_2, & (13)H_3(13) = H_1, & (23)H_3(23) = H_3. \end{array}$$

Откуда в свою очередь видно, что подгруппы H_1, H_2 и H_3 образуют орбиту длины три, а стабилизатором каждой подгруппы является сама подгруппа. Подгруппа H_4 является единственной подгруппой порядка три. Поэтому она образует самостоятельную орбиту, а ее стабилизатором будет вся группа S_3. □

Пример 7.4. Рассмотрим действие сопряжениями подгруппы H_1 на множестве нетривиальных подгрупп группы S_3. Из предыдущего примера видно, что это множество разбивается на две орбиты $\{H_1\}$ и $\{H_4\}$ единичной длины и одну орбиту длины два из подгрупп H_2 и H_3. Стабилизатором подгрупп H_1 и H_4 будет подгруппа H_1, а стабилизатор подгрупп H_2 и H_3 состоит только из единичного элемента. □

Нормализатором $N(H)$ подгруппы H группы G называется стабилизатор этой подгруппы при действии группы G сопряжениями на множестве своих подгрупп, т. е.

$$N(H) = \{g \in G \,|\, gHg^{-1} \subseteq H\}.$$

Очевидно, что нормализатор является подгруппой группы G и подгруппа H является нормальной подгруппой в своем нормализаторе.

Центром Z группы G называется множество таких ее элементов, каждый из которых коммутирует со всеми элементами G, т. е.

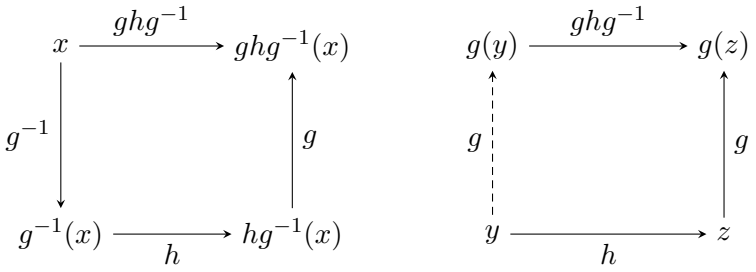
$$Z(G) = \{z \in G \,|\, gz = zg \quad \forall g \in G\}.$$

Легко видеть, что центр является коммутативной нормальной подгруппой группы G и состоит из неподвижных точек действия группы G сопряжениями на множестве ее элементов: $Z(G) = \{z \in G \,|\, gzg^{-1} = z \quad \forall g \in G\}$. Неформально можно сказать, что размер центра является мерой «коммутативности» группы — чем больше центр, тем больше в группе коммутирующих элементов, например $Z(G) = G$ для любой абелевой группы G. Элементы a, b группы G называются *сопряженными*, если они лежат в одной орбите при действии G на себя сопряжениями, т. е. если найдется такой элемент $g \in G$, что $a = gbg^{-1}$. Элемент g в этом случае называется *сопрягающим* a с b, а орбита — *классом сопряженности*. Нетрудно убедиться, что сопряженность является отношением эквивалентности на элементах группы G.

Пример 7.5. Группа подстановок S_2 коммутативна, поэтому $Z(S_2) = S_2$. Найдем центр некоммутативной группы S_3. В

примере 7.3 были вычислены произведения вида gzg^{-1} для всех транспозиций g, z из S_3, откуда видно, что для любой транспозиции z найдется такая транспозиция g, что $gzg^{-1} \neq z$, т. е. $gz \neq zg$. Иными словами, никакая транспозиция из S_3 не коммутирует со всеми элементами группы. Легко видеть, что это верно и для циклов длины 3, например $(12)(123)(12) = (132) \neq (123)$. Таким образом, $Z(S_3) = \{e\}$. Из двух следующих примеров следует, что $Z(S_n) = \{e\}$ при всех $n \geqslant 3$. $\square$

Пример 7.6. Рассмотрим подстановку $f = ghg^{-1}$, сопряженную в группе S_n с подстановкой h. Результат ее применения $f(x) = g\big(h\big(g^{-1}(x)\big)\big)$ к элементу $x \in \{1, \ldots, n\}$ можно представить коммутативной диаграммой, приведенной ниже на рисунке слева. Подобные диаграммы уже встречались нам ранее при ис-



следовании композиции отображений (см. диаграмму на с. 15). Отображения g, h, g^{-1} являются биекциями, поэтому элементы $y = g^{-1}(x)$ и $z = h(y)$ определяются по x, g и h однозначно. Перерисуем нашу диаграмму с использованием новых обозначений y, z и того факта, что равенство $y = g^{-1}(x)$ равносильно $x = g(y)$ (на рисунке справа). Пунктирное ребро соответствует подстановке $g = (g^{-1})^{-1}$, обратной к g^{-1}.

Полученная на рисунке справа диаграмма также является коммутативной. Она показывает, что если подстановка h переводит элемент y в некоторый элемент z (не обязательно отличный от y), то подстановка ghg^{-1} переводит элемент $g(y)$ в $g(z)$. Отсюда следует, что *сопряженная подстановка ghg^{-1} получается применением сопрягающей ее с h подстановки g ко всем числам из разложения подстановки h на независимые циклы.*

Например, если $g = (1234567)$ и $h = (12)(34)(567)$, то для нахождения разложения ghg^{-1} на независимые циклы не обязательно искать подстановку g^{-1} и находить ее композицию с g и h: так как $g(1) = 2$, $g(2) = 3$, $\ldots$, $g(7) = 1$, то $ghg^{-1} = = (23)(45)(671)$. $\square$

Пусть разложение подстановки g из симметрической группы S_n на независимые циклы состоит из k_i циклов длины i, где $i = = 1, \ldots, n$ и $k_1 + 2k_2 + \ldots + nk_n = n$. Назовем упорядоченный набор $t_g = (k_1, k_2, \ldots, k_n)$ *типом* подстановки g. Каждая транспозиция имеет тип $(0, 1, 0, \ldots, 0)$, а тождественная подстановка является единственной подстановкой типа $(n, 0, \ldots, 0)$ в S_n.

Подстановка $g = (12)(345) \in S_5$ имеет тип $(0, 1, 1, 0, 0)$. Каждое из 5! произведений $(i_1 i_2)(i_3 i_4 i_5)$, где i_j — попарно различные числа от 1 до 5, определяет некоторую подстановку h того же типа, что и g.

Так как $(i_1 i_2) = (i_2 i_1)$ и $(i_3 i_4 i_5) = (i_4 i_5 i_3) = (i_5 i_3 i_4)$, то имеется всего $2 \cdot 3 = 6$ различных способов записи подстановки h. Поэтому группа S_5 содержит всего $5!/6 = 20$ подстановок, тип которых совпадает с типом подстановки g.

Аналогичные рассуждения позволяют получить общую формулу

$$\bigl|\{g \in S_n : t_g = (k_1, k_2, \ldots, k_n)\}\bigr| = \frac{n!}{\prod_{i=0}^{n} i^{k_i} k_i!} \qquad (7.1)$$

для числа подстановок типа $(k_1, k_2, \ldots, k_n)$ в S_n. Действительно, каждый цикл длины i может быть записан i способами независимо от остальных циклов той же длины, причем k_i независимых циклов одинаковой длины можно переставить $k_i!$ способами, не изменяя их произведения.

Пример 7.7. Рассмотрим действие группы S_n сопряжениями на множестве всех своих элементов. Тогда стабилизатором $\mathrm{St}(h)$ подстановки h будет множество всех таких g из S_n, что $ghg^{-1} = = h$ (что равносильно $gh = hg$), т. е. множество всех подстановок, коммутирующих с h. Орбита $\mathrm{Or}(h)$ подстановки h состоит из всех сопряженных с ней подстановок.

Пример 7.6 показывает, что сопряженными в группе S_n могут быть только подстановки с одинаковой цикловой структу-

рой, т. е. подстановки одного типа. Более того, любые две подстановки одного типа действительно сопряжены, так как для любых двух упорядоченных наборов, состоящих из n различных чисел множества $\{1, 2, \ldots, n\}$, найдется подстановка, переводящая один из них в другой. Например, последовательность 351462 является образом последовательности 123456 при подстановке $g = (13)(4)(256)$, поэтому $ghg^{-1} = (351)(462) = (135)(246)$ при $h = (123)(456)$. Таким образом, орбита $\mathrm{Or}(h)$ содержит все подстановки того же типа, что и h.

Поэтому по теореме 7.1 с учетом (7.1) получаем, что число всех подстановок, коммутирующих с подстановкой h типа $(k_1, k_2, \ldots, k_n)$, равно

$$|\mathrm{St}(h)| = \frac{n!}{|\mathrm{Or}(h)|} = \prod_{i=0}^{n} i^{k_i} k_i!. \tag{7.2}$$

Отсюда следует, что коммутировать с h будут все возможные произведения независимых циклов, входящих в ее разложение, и только они. Заметим также, что $|\mathrm{Or}(h)| = 1$ только когда подстановка h тождественная. Во всех остальных случаях выражение (7.2) строго меньше, чем $n!$, поэтому h коммутирует не со всеми подстановками из S_n.

Таким образом, число орбит (классов сопряженных элементов), на которые распадается группа S_n при действии сопряжением на своих элементах, равно числу различных типов подстановок, т. е. числу неотрицательных решений $(k_1, k_2, \ldots, k_n)$ уравнения $k_1 + 2k_2 + \ldots + nk_n = n$. В частности, группа S_4 состоит из пяти орбит: орбита тождественной подстановки с длиной 1, орбита подстановки $(1)(2)(34)$ длины $4!/(2! \cdot 2) = 6$, орбита подстановки $(12)(34)$ длины $4!/(2! \cdot 2^2) = 3$, орбита подстановки $(1)(234)$ длины $4!/3 = 8$ и орбита подстановки (1234) длины $4!/4 = 6$. □

Пример 7.8. Покажем, что в каждой группе G порядка p^n, где p — простое и $n \geqslant 1$, центр $Z(G)$ будет нетривиальной ($Z(G) \neq \{e\}$) подгруппой. Для этого рассмотрим действие группы G сопряжениями на множестве ее элементов. При таком действии p^n элементов группы распадаются на орбиты, сумма длин которых равна p^n. Из теоремы 7.1 следует, что длины всех орбит

делят порядок группы и поэтому являются степенями p. Следовательно, число неподвижных точек (это число больше нуля, так как неподвижной точкой будет единичный элемент) кратно p, т. е. центр группы состоит не менее чем из p элементов. □

Пример 7.9. Воспользуемся предыдущим примером и покажем, что любая группа G порядка p^2 абелева. Каждая такая группа имеет нетривиальный центр Z, порядок которого равен либо p^2, либо p. Если $|Z| = p^2$, то G совпадает со своим центром и является абелевой. Если же $|Z| = p$, то фактор-группа G/Z будет циклической. Пусть aZ — порождающий элемент этой фактор-группы. Тогда произвольный элемент группы G представляется в виде произведения $a^k z$, где $z \in Z$ и $a^p = e$. В этом случае для любых $a^k z_1$ и $a^l z_2$ из равенств

$$a^k z_1 \cdot a^l z_2 = a^k a^l z_1 z_2 = a^l a^k z_2 z_1 = a^l z_2 \cdot a^k z_1$$

следует перестановочность этих элементов и, следовательно, коммутативность всей группы G, что, очевидно, противоречит рассматриваемому случаю $|Z| = p$. □

7.2. Теоремы Силова

Пусть группа G состоит из $p^n m$ элементов, где p — простое и $(p, m) = 1$. Подгруппа из p^n элементов называется силовской p-подгруппой группы G.

Теорема 7.2 (первая теорема Силова)**.** *Пусть группа G состоит из $p^n m$ элементов, где p — простое и $(p, m) = 1$. Тогда в G существует силовская p-подгруппа.*

Доказательство. Рассмотрим множество M, состоящее из всех p^n-элементных подмножеств группы G. Это множество состоит из

$$\binom{p^n m}{p^n} = \prod_{k=0}^{p^n-1} \frac{p^n m - k}{p^n - k} \tag{7.3}$$

различных подмножеств. Покажем, что ни одна из дробей в правой части (7.3) не делится на p. Для этого заметим, что если

числитель дроби $\frac{p^n m-k}{p^n-k}$ делится на p^r, то на p^r обязательно делится и число k. В этом случае положим $k = p^r k'$, где k' на p не делится. Тогда

$$\frac{p^n m - k}{p^n - k} = \frac{p^n m - p^r k'}{p^n - p^r k'} = \frac{p^{n-r} m - k'}{p^{n-r} - k'},$$

и так как $r < n$, то легко видеть, что рассматриваемая дробь действительно не делится на p. Следовательно не делится на p и произведение дробей — число элементов множества M.

Теперь рассмотрим действие группы G на множестве M, при котором каждый элемент g группы G преобразует подмножество $\{g_1, g_2, \ldots, g_{p^n}\}$ в подмножество $\{gg_1, gg_2, \ldots, gg_{p^n}\}$. В результате такого действия группы G множество M разобьется на орбиты, сумма длин которых равна $\binom{p^n m}{p^n}$. Так как $\binom{p^n m}{p^n}$ не делится на p, то среди орбит обязательно найдется по крайней мере одна, число элементов в которой также не делится на p. Далее заметим, что каждая орбита множества M состоит не менее чем из m элементов. Это следует из того, что в объединении всех подмножеств, составляющих одну орбиту, обязательно присутствуют все элементы группы G, в то время как каждое подмножество состоит ровно из p^n элементов.

Наконец рассмотрим подмножество x из M, длина орбиты которого не делится на p. В силу теоремы 7.1 для x справедливо равенство

$$|\mathrm{Or}(x)| \cdot |\mathrm{St}(x)| = p^n m.$$

Так как в левой части этого равенства первый множитель не меньше m и при этом не делится на p, то второй множитель равен p^n. Таким образом, стабилизатор подмножества x состоит ровно из p^n элементов и, следовательно, является искомой подгруппой группы G. Теорема доказана.

Теорема 7.3 (вторая теорема Силова)**.** *Пусть группа G состоит из $p^n m$ элементов, где p — простое и $(p, m) = 1$. Тогда все силовские p-подгруппы группы G сопряжены.*

Доказательство. Пусть группа G состоит из $p^n m$ элементов, где $(p, m) = 1$. Предположим, что S и S' — две силовские

p-подгруппы группы G. Рассмотрим действие подгруппы S' на фактор-множестве G/S, при котором элемент g подгруппы S' преобразует смежный класс $\{g_1, g_2, \ldots, g_{p^n}\}$ в смежный класс $\{gg_1, gg_2, \ldots, gg_{p^n}\}$. Порядок подгруппы S' равен p^n, поэтому в силу теоремы 7.1 длины всех орбит в G/S являются степенями числа p. Фактор-множество G/S состоит из m смежных классов, и так как m не делится на p, то среди орбит должна найтись хотя бы одна неподвижная точка (длина орбиты равна $p^0 = 1$). Пусть смежный класс aS является такой неподвижной точкой. Тогда $gaS = aS$ для любого g из S'. Домножив правую и левую части последнего равенства на a^{-1}, получим, что $gaSa^{-1} = aSa^{-1}$ для любого g из S'. Так как aSa^{-1} является подгруппой группы G и умножение этой подгруппы на элементы S' не выводит за пределы aSa^{-1}, то $S' \subseteq aSa^{-1}$. Теперь, учитывая, что S и S' имеют один и тот же порядок, заключаем, что $S' = aSa^{-1}$. Теорема доказана.

Теорема 7.4 (третья теорема Силова)**.** *Пусть группа G состоит из $p^n m$ элементов, где p — простое и $(p, m) = 1$. Тогда число силовских p-подгрупп группы G сравнимо с единицей по модулю p.*

Доказательство. Пусть M — множество всех силовских p-подгрупп группы G. Все силовские p-подгруппы группы G сопряжены в силу теоремы 7.3, и поэтому любую силовскую p-подгруппу S' можно представить в виде aSa^{-1}, где S — некоторая фиксированная силовская p-подгруппа, а a — элемент группы G. Рассмотрим действие подгруппы S на множестве M, при котором элемент a подгруппы S преобразует подгруппу $S' = \{g_1, g_2, \ldots, g_{p^n}\}$ в сопряженную подгруппу $aS'a^{-1} = \{ag_1a^{-1}, ag_2a^{-1}, \ldots, ag_{p^n}a^{-1}\}$. Покажем, что при таком действии в M существует единственная неподвижная точка — подгруппа S.

Допустим, что некоторая подгруппа S' является неподвижной точкой рассматриваемого действия. Тогда $gS'g^{-1} \subseteq S'$ для любого $g \in S$. Следовательно, подгруппа S содержится в нормализаторе подгруппы S'. Очевидно, что и подгруппа S' также содержится в своем нормализаторе. Поэтому S и S' являются

силовскими p-подгруппами нормализатора подгруппы S', и, следовательно, эти подгруппы сопряжены в силу теоремы 7.3, т. е. в нормализаторе S' найдется такой элемент a, что $aS'a^{-1} = S$. Теперь заметим, что S' — нормальная подгруппа в своем нормализаторе, т. е. $gS'g^{-1} = S'$ для любого элемента g из нормализатора S', в том числе и для элемента a из предыдущего равенства. Таким образом, из двух последних равенств заключаем, что $S = S'$. Следовательно, при рассматриваемом действии подгруппы S на множестве M в этом множестве существует единственная неподвижная точка — подгруппа S.

Порядок подгруппы S равен p^n, и поэтому в силу теоремы 7.1 длины всех орбит в M являются степенями числа p. Так как среди этих орбит есть только одна орбита длины $p^0 = 1$, то число элементов в M сравнимо с единицей по модулю p. Теорема доказана.

Теорема 7.5. *Пусть группа G состоит из $p^n m$ элементов, где p — простое и $(p, m) = 1$. Число силовских p-подгрупп группы G делит порядок этой группы.*

Доказательство. Рассмотрим действие группы G сопряжениями на множестве всех ее силовских p-подгрупп. Так как все силовские p-подгруппы сопряжены, то все они попадают в одну орбиту, длина которой в силу теоремы 7.1 является делителем порядка группы G. Таким образом, число силовских p-подгрупп является делителем порядка группы. Теорема доказана.

Пример 7.10. Рассмотрим группу G из 15 элементов. Из первой теоремы Силова следует, что в этой группе есть подгруппы из трех и пяти элементов. Так как три и пять — простые числа, то все эти подгруппы будут циклическими. Из третьей теоремы Силова следует, что количество трехэлементных подгрупп равно одному из чисел 1, 4, 7, 10, 13 и при этом в силу теоремы 7.5 делит 15, т. е. совпадает с одним из чисел 1, 3, 5. Очевидно, что в G есть ровно одна подгруппа $A = \langle a \rangle$ порядка три. Аналогичным образом можно показать, что в G содержится ровно одна подгруппа $B = \langle b \rangle$ порядка пять. Из второй теоремы Силова следует, что эти подгруппы нормальные. Так как порядки

подгрупп A и B взаимно просты, то эти подгруппы пересекаются только по единичному элементу. Покажем, что элементы таких подгрупп A и B коммутируют. Так как $a^k b^m a^{-k} = b^s$ и $b^m a^{-k} b^{-m} = a^t$, то

$$a^{k+t} = a^k(b^m a^{-k} b^{-m}) = (a^k b^m a^{-k})b^{-m} = b^{s-m} \;\Rightarrow$$
$$\Rightarrow \quad a^k b^m a^{-k} b^{-m} = e \quad \Rightarrow \quad a^k b^m = b^m a^k.$$

Поэтому, начиная с тривиального тождества $(ab)^1 = a^1 b^1$ и предполагая справедливость равенства $(ab)^{k-1} = a^{k-1} b^{k-1}$, из цепочки равенств

$$(ab)^k = (ab)^{k-1} ab = a^{k-1} b^{k-1} ab = a^{k-1} ab^{k-1} b = a^k b^k$$

индукцией по k заключаем, что $(ab)^k = a^k b^k$. Следовательно, $(ab)^3 = a^3 b^3 = b^3 \neq e$ и $(ab)^5 = a^5 b^5 = a^2 \neq e$. Произведение $ab \neq e$ лежит в группе из 15 элементов, и поэтому его порядок d должен быть отличным от единицы делителем 15. Но $d \neq 3, 5$. Тогда $d = 15$ и G — циклическая группа. Таким образом, любая группа порядка 15 является циклической. □

7.3. Прямые произведения групп

Напомним, что для групп $G_1, \ldots, G_k$ их внешним прямым произведением $G_1 \times \cdots \times G_k$ называется множество всех упорядоченных наборов $(g_1, \ldots, g_k)$ длины k, где $g_i \in G_i$, с определенной на этом множестве покомпонентной операцией умножения

$$(g_1, \ldots, g_k)(g'_1, \ldots, g'_k) = (g_1 g'_1, \ldots, g_k g'_k),$$

в которой умножение по i-й компоненте является умножением в группе G_i.

Будем говорить, что группа G является *внутренним прямым произведением* $H_1 H_2 \cdots H_n$ своих нормальных подгрупп $H_1, H_2, \ldots, H_n$, если любой элемент $g \in G$ единственным образом представляется в виде $g = h_1 h_2 \cdots h_n$, где $h_i \in H_i$.

Пример 7.11. В абелевой группе $\mathbb{Z}_7^*$ есть две циклические подгруппы $\langle 2\rangle = \{1, 2, 4\}$ и $\langle 6\rangle = \{1, 6\}$. Так как в $\mathbb{Z}_7^*$

$$1 = 1 \cdot 1, \quad 2 = 2 \cdot 1, \quad 3 = 4 \cdot 6, \quad 4 = 4 \cdot 1, \quad 5 = 2 \cdot 6, \quad 6 = 1 \cdot 6,$$

то все шесть произведений ab, где $a \in \langle 2\rangle$ и $b \in \langle 6\rangle$ различны и представляют все элементы $\mathbb{Z}_7^*$. Следовательно, группа $\mathbb{Z}_7^*$ является внутренним прямым произведением своих нормальных подгрупп $\langle 2\rangle$ и $\langle 6\rangle$. □

Пример 7.12. Рассмотрим циклическую группу $G = \langle a\rangle$ порядка pq, где p и q — простые числа. В G есть две подгруппы порядков p и q — это подгруппа $G^q = \langle a^q\rangle$ и подгруппа $G^p = \langle a^p\rangle$, которые пересекаются только по единичному элементу. Покажем, что любой элемент $g \in G$ единственным образом представляется в виде произведения $(a^q)^k(a^p)^m$, где $0 \leqslant k < p$ и $0 \leqslant m < q$. Так как таких произведений ровно pq, то достаточно показать, что все они различны. Допустим, это не так и два произведения равны: $(a^q)^{k_1}(a^p)^{m_1} = (a^q)^{k_2}(a^p)^{m_2}$. Тогда из этого равенства и коммутативности группы G следует, что $(a^q)^{k_1-k_2} = (a^p)^{m_2-m_1}$, $|k_1 - k_2| < p$ и $|m_2 - m_1| < q$. Последнее равенство возможно только в том случае, когда $(a^q)^{k_1-k_2} = e$, т. е. разность k_1-k_2 должна быть кратна p, что, очевидно, невозможно в силу неравенства $|k_1 - k_2| < p$. Таким образом, группа G является внутренним прямым произведением своих нормальных подгрупп G^q и G^p. □

Из примеров 3.31 и 7.12 следует, что при простых p и q циклическая группа порядка pq является внутренним прямым произведением подгрупп порядка p и q и изоморфна внешнему прямому произведению этих подгрупп. В следующей теореме покажем, что это частный случай более общей ситуации.

Теорема 7.6. *Пусть группа G является внутренним прямым произведением $H_1H_2\cdots H_n$ своих нормальных подгрупп $H_1, H_2, \ldots, H_n$. Тогда*

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

Доказательство. Покажем, что $H_i \cap H_j = e$ для всех i и j. Если это не так и $g \in H_i \cap H_j$, то элемент g можно представить двумя разными способами в виде произведений элементов нормальных подгрупп. Рассматривая g как элемент подгруппы H_i, получим произведение

$$g = e_1 \cdots e_{i-1} g e_{i+1} \cdots e_j \cdots e_n, \tag{7.4}$$

где $e_t = e$ — элемент подгруппы H_t. Рассматривая g как элемент подгруппы H_j, получим второе произведение

$$g = e_1 \cdots e_i \cdots e_{j-1} g e_{j+1} \cdots e_n, \tag{7.5}$$

где $e_t = e$ — элемент подгруппы H_t. Если $g \neq e$, то равенства (7.4) и (7.5) противоречат единственности представления каждого элемента группы G в виде произведения $h_1 \cdots h_i \cdots h_n$, где $h_i \in H_i$. Следовательно, $H_i \cap H_j = e$ для всех i и j.

Теперь легко видеть, что для любых $h_i \in H_i$ и $h_j \in H_j$

$$\begin{aligned} h_i h_j h_i^{-1} h_j^{-1} &= h_i (h_j h_i^{-1} h_j^{-1}) = h_i h_i' \in H_i, \\ h_i h_j h_i^{-1} h_j^{-1} &= (h_i h_j h_i^{-1}) h_j^{-1} = h_j' h_j^{-1} \in H_j. \end{aligned}$$

Следовательно, $h_i h_j h_i^{-1} h_j^{-1} = e$ и $h_i h_j = h_j h_i$, т. е. элементы из разных нормальных подгрупп коммутируют. Используя это свойство, нетрудно показать, что для умножения произведений $h_1 \cdots h_i \cdots h_n$ и $h_1' \cdots h_i' \cdots h_n'$, состоящих из элементов h_i, h_i', попарно пересекающихся только по единичному элементу нормальных подгрупп H_i, можно воспользоваться равенством

$$(h_1 \cdots h_i \cdots h_n)(h_1' \cdots h_i' \cdots h_n') = h_1 h_1' \cdots h_i h_i' \cdots h_n h_n'. \tag{7.6}$$

Зададим отображение φ группы $G = H_1 H_2 \cdots H_n$ в прямое произведение $H_1 \times H_2 \times \cdots \times H_n$ ее нормальных подгрупп равенством

$$\varphi(h_1 h_2 \cdots h_n) = (h_1, h_2, \ldots, h_n). \tag{7.7}$$

Взаимная однозначность этого отображения следует из единственности представления каждого элемента группы G в виде

произведения $h_1h_2\cdots h_n$. Пусть $g = h_1h_2\cdots h_n$ и $g' = h'_1h'_2\cdots h'_n$ — произвольные элементы группы G. Тогда в силу свойства (7.6)

$$\begin{aligned}\varphi(gg') &= \varphi((h_1h_2\cdots h_n)(h'_1h'_2\cdots h'_n)) = \\ &= \varphi(h_1h'_1h_2h'_2\cdots h_nh'_n) = (h_1h'_1, h_2h'_2, \ldots, h_nh'_n) = \\ &= (h_1, h_2, \ldots, h_n)(h'_1, h'_2, \ldots, h'_n)) = \varphi(g)\varphi(g'),\end{aligned}$$

т. е. φ сохраняет групповую операцию и, следовательно, является изоморфизмом. Теорема доказана.

Говоря далее о разложении группы в *прямое произведение ее нормальных подгрупп*, как правило, не будем различать внешние и внутренние произведения, так как эти произведения изоморфны, а использованный в доказательстве теоремы 7.6 изоморфизм (7.7) позволяет все технические действия во внешних и внутренних произведениях проводить совершенно идентичным образом.

Теорема 7.7. *Группа G порядка $p_1^{k_1}\cdots p_n^{k_n}$ является прямым произведением своих силовских p_i-подгрупп тогда и только тогда, когда эти подгруппы нормальны в G.*

Доказательство. Необходимость следует из того простого факта, что любой множитель в прямом произведении является нормальной подгруппой произведения. Для группы $G = H_1\times \times\cdots\times H_n$ и ее прямого множителя H_i это следует из равенств

$$\begin{aligned}&(h_1, \ldots, h_i, \ldots, h_n)(e_1, \ldots, H_i, \ldots, e_n)(h_1^{-1}, \ldots, h_i^{-1}, \ldots, h_n^{-1}) = \\ &\quad = (h_1h_1^{-1}, \ldots, h_iH_ih_i^{-1}, \ldots, h_nh_n^{-1}) = (e_1, \ldots, H_i, \ldots, e_n),\end{aligned}$$

где $h_t \in H_t$ и e_t — единичный элемент H_t.

Докажем достаточность. Сначала покажем, что каждый элемент g группы G единственным образом представляется в виде $g = h_1h_2\cdots h_n$, где $h_i \in H_i$ и H_i — нормальная силовская подгруппа порядка $p_i^{k_i}$. Если это не так, то в силу того, что в G есть ровно $p_1^{k_1}\cdots p_n^{k_n}$ произведений вида $h_1h_2\cdots h_n$, в G найдется такой элемент g, что

$$h'_1\ldots h'_i\cdots h'_n = g = h''_1\ldots h''_i\cdots h''_n,$$

где $h'_i, h''_i \in H_i$ и $h'_j \neq h''_j$ хотя бы для одного j. Так как $H_i \bigcap H_j = e$ (если $g \in H_i \bigcap H_j$ и $g \neq e$, то порядок элемента g будет кратен $p_i p_j$, что, очевидно, невозможно), то в силу (7.6)

$$e = h''_1 h'^{-1}_1 \cdots h''_i h'^{-1}_i \cdots h''_n h'^{-1}_n = h_1 \cdots h_i \cdots h_n,$$

причем среди элементов $h_i = h''_i h'^{-1}_i$ есть хотя бы один неединичный элемент h_j. Так как $h_i \in H_i$, то его порядок d_i равен $p_i^{m_i}$. Положим $d = \prod_{i \neq j} d_i$. Тогда (см. (7.6))

$$e = (h_1 \ldots h_i \cdots h_j \cdots h_n)^d = h_1^d \ldots h_i^d \cdots h_j^d \cdots h_n^d = h_j^d.$$

С другой стороны, d и d_j взаимно просты, и поэтому $h_j^d \neq e$. Пришли к противоречию, из которого следует, что все $p_1^{k_1} \cdots p_n^{k_n}$ произведений вида $h_1 \cdots h_n$, где $h_i \in H_i$, представляют различные элементы группы G. Следовательно, G является внутренним прямым произведением своих силовских p_i-подгрупп. Теперь достаточность условия теоремы легко следует из теоремы 7.6. Теорема доказана.

7.4. Конечные абелевы группы

Коммутативность накладывает сильные ограничения на возможную структуру группы. Одно из таких ограничений состоит в том, что любая подгруппа абелевой группы является нормальной. Из этого факта и теоремы 7.7 легко извлекается следующая простая теорема[1)].

Теорема 7.8. *Каждая конечная абелева группа является прямым произведением своих силовских p-подгрупп.*

Пример 7.13. Рассмотрим абелеву G группу порядка $n = p_1 \cdots p_k$, где p_i — различные простые числа. Из теоремы 7.8 и простоты порядков всех силовских подгрупп группы G следует, что G является прямым произведением циклических подгрупп

[1)] Полезно сравнить эту и следующую теоремы с теоремами о строении конечномерных линейных пространств из раздела 6.4.

с взаимно простыми порядками: $G = \langle g_1\rangle \times \cdots \times \langle g_k\rangle$, где $|\langle g_i\rangle| = p_i$. Положим $n_i = n/p_i$. Покажем, что порядок произведения $g = g_1 \cdots g_k$ равен n. Для этого достаточно убедиться в том, что $g^{n_i} \neq e$ при $i = 1, \ldots, k$. Покажем, что это так для $i = 1$. В этом случае $n_1 = p_2 \cdots p_k$ и $g_i^{n_1} = e$ при $i = 2, \ldots, k$ так как $g_i^{p_i} = e$ и p_i делит n_1, и $g_1^{n_1} \neq e$, так как n_1 и p_1 взаимно просты. Тогда в силу коммутативности группы G

$$g^{n_1} = g_1^{n_1} g_2^{n_1} \cdots g_k^{n_1} = g_1^{n_1} \neq e.$$

Таким образом, порядок элемента g совпадает с порядком группы, т. е. G — циклическая группа. Следовательно, циклическая группа порядка $n = p_1 \cdots p_k$, где p_i — различные простые числа, является единственной, с точностью до изоморфизма, коммутативной группой данного порядка. □

Группу порядка p^n, где p — простое, будем называть *примарной* группой, или *p-группой*.

Далее рассмотрим абелевы p-группы, в прямое произведение которых разлагается произвольная абелева группа. Оказывается, каждая такая группа имеет достаточно жесткую внутреннюю структуру. Эту структуру опишем в следующей теореме.

Теорема 7.9. *Каждая конечная абелева p-группа является прямым произведением циклических групп.*

Доказательство. Покажем, что любая абелева группа порядка p^n является прямым произведением своих циклических подгрупп. Сделаем это индукцией по n. В основание индукции положим очевидный случай $n = 1$. Допустим, что при всех $n < m$ утверждение теоремы справедливо. Рассмотрим произвольную абелеву группу G порядка p^m и выберем в ней элемент g максимального порядка. Если порядок g равен p^m, то утверждение теоремы очевидно, так как в этом случае G будет циклической группой. Далее полагаем, что порядок элемента g равен p^k, где $k < m$. Фактор-группа $H = G/\langle g\rangle$ состоит из p^{m-k} элементов и по предположению индукции является прямым произведением

$$H = H_1 \times \cdots \times H_i \times \cdots \times H_r \tag{7.8}$$

циклических подгрупп

$$H_i = \langle h_i\langle g\rangle\rangle = \{\langle g\rangle, h_i\langle g\rangle, \ldots, h_i^j\langle g\rangle, \ldots, h_i^{p^{k_i}-1}\langle g\rangle\},$$

где $h_i \in G$, $|H_i| = p^{k_i}$, $k_i \leqslant k$ и $k_1 + \cdots + k_r = m - k$. Из равенства (7.8) и теоремы 7.6 следует, что любой элемент $h\langle g\rangle$ группы H можно единственным образом представить в виде произведения

$$h\langle g\rangle = h_1^{t_1}\langle g\rangle \cdots h_i^{t_i}\langle g\rangle \cdots h_r^{t_r}\langle g\rangle = h_1^{t_1} \cdots h_i^{t_i} \cdots h_r^{t_r}\langle g\rangle, \qquad (7.9)$$

где $0 \leqslant t_i < p^{k_i}$.

Так как $h_i^{p^{k_i}}\langle g\rangle = \langle g\rangle$, то найдется такое s_i, что $h_i^{p^{k_i}} = g^{s_i}$. Порядок элемента h_i в группе G не превосходит p^k. Поэтому из равенств

$$g^{p^k} = e = h_i^{p^k} = h_i^{p^{k_i}\cdot p^{k-k_i}} = g^{s_i\cdot p^{k-k_i}}$$

следует, что произведение $s_i p^{k-k_i}$ кратно p^k. Значит, существует такое l_i, что $s_i p^{k-k_i} = l_i p^k$ или $s_i = l_i p^{k_i}$. Положим $g_i = h_i g^{-l_i}$. Нетрудно видеть, что $\langle h_i\langle g\rangle\rangle = \langle g_i\langle g\rangle\rangle$, и поэтому $g_i^l \notin \langle g\rangle$ при $0 < l < p^{k_i}$. А так как

$$g_i^{p^{k_i}} = \left(h_i g^{-l_i}\right)^{p^{k_i}} = h_i^{p^{k_i}} g^{-l_i p^{k_i}} = g^{s_i} g^{-s_i} = e,$$

то каждая циклическая группа $G_i = \langle g_i\rangle$ будет в группе G такой подгруппой порядка p^{k_i}, которая пересекается с $\langle g\rangle$ только по единичному элементу. Заметим, что равенство

$$g_1^{t_1} \cdots g_i^{t_i} \cdots g_r^{t_r} = g^t \quad (\text{или } g_1^{t_1} \cdots g_i^{t_i} \cdots g_r^{t_r} g^{-t} = e) \qquad (7.10)$$

возможно только в том случае, когда t и все t_i равны нулю. Действительно, из (7.10) и определения элементов g_i следует соотношение

$$\begin{aligned} h_1^{t_1} \cdots h_i^{t_i} \cdots h_r^{t_r} &= (g_1 g^{l_1})^{t_1} \cdots (g_i g^{l_i})^{t_i} \cdots (g_r g^{l_r})^{t_r} = \\ &= g_1^{t_1} \cdots g_i^{t_i} \cdots g_r^{t_r} g^{l_1 t_1 + \cdots + l_r t_r} = g^{t + l_1 t_1 + \cdots + l_r t_r} \in \langle g\rangle, \end{aligned}$$

которое в силу (7.9) возможно только тогда, когда все t_i равны нулю. Но $g_1^0 \cdots g_i^0 \cdots g_r^0 = e$, т. е. t также равно нулю. Отсюда

следует, что все $p^{k_1+\cdots+k_r+k} = p^m$ произведений $g_1^{t_1}\cdots g_i^{t_i}\cdots g_r^{t_r}g^t$ являются различными элементами G, т. е. каждый элемент G единственным образом представляется в виде такого произведения. Следовательно,

$$G = G_1 \times \cdots \times G_i \times \cdots \times G_r \times \langle g\rangle.$$

Теорема доказана.

Пример 7.14. Воспользуемся доказанной теоремой и покажем, что в любой абелевой группе порядка p^n для любого $m < n$ найдется подгруппа из p^m элементов. Заметим, что это верно для циклических групп. В циклической группе G с порождающим элементом g требуемую подгруппу будет порождать элемент $g^{p^{n-m}}$. Пусть теперь G — произвольная абелева группа порядка p^n. Тогда $G = G_1\times\cdots\times G_r$, где $|G_i| = p^{n_i}$ и $n_1+\cdots+n_r = n$. Очевидно, что существуют такие $m_1,\ldots,m_r$, что $m_i \leqslant n_i$ и $m_1 + \cdots + m_r = m$. Выбирая в группах G_i подгруппы H_i порядка p^{m_i}, видим, что произведение $H_1 \times \cdots \times H_r$ будет подгруппой порядка p^m в группе G. □

Теорема 7.10. *Если конечная абелева p-группа G разлагается двумя способами в прямое произведение циклических подгрупп*

$$G = A_1 \times \cdots \times A_r = B_1 \times \cdots \times B_s,$$

где $|A_1| \geqslant |A_2| \geqslant \cdots \geqslant |A_r|$ и $|B_1| \geqslant |B_2| \geqslant \cdots \geqslant |B_s|$, то $r = s$ и $|A_i| = |B_i|$ для всех $i \in \{1, 2, \ldots, r\}$.

Доказательство. Для группы из p элементов утверждение теоремы очевидно. Допустим, что при всех $n < m$ утверждение теоремы также справедливо. Рассмотрим абелеву группу G порядка p^m, которая разлагается двумя способами

$$G = \langle a_1\rangle \times \cdots \times \langle a_r\rangle = \langle b_1\rangle \times \cdots \times \langle b_s\rangle \tag{7.11}$$

в прямое произведение циклических подгрупп $\langle a_i\rangle$ и $\langle b_j\rangle$, где

$$\begin{aligned} &|\langle a_i\rangle| = p^{k_i},\ \ k_1 \geqslant k_2 \geqslant \cdots \geqslant k_u > k_{u+1} = \cdots = k_r = 1,\\ &|\langle b_j\rangle| = p^{n_j},\ \ n_1 \geqslant n_2 \geqslant \cdots \geqslant n_v > n_{v+1} = \cdots = n_s = 1. \end{aligned} \tag{7.12}$$

Легко видеть, что множество $G^p = \{g^p \mid g \in G\}$ является подгруппой группы G. Из (7.11), (7.12) и теоремы 7.6 следует, что произвольный элемент g группы G можно представить в виде двух произведений

$$a_1^{t_1} \cdots a_i^{t_i} \cdots a_r^{t_r} = g = b_1^{d_1} \cdots b_j^{d_j} \cdots b_s^{d_s}, \tag{7.13}$$

где $0 \leqslant t_i < p^{k_i}$ и $0 \leqslant d_j < p^{n_j}$, причем для каждого g существует единственный набор показателей $t_1, \ldots, t_r$ и единственный набор показателей $d_1, \ldots, d_s$, для которых справедливо (7.13). В свою очередь из (7.12) и (7.13) следует, что произвольный элемент g^p подгруппы G^p также можно представить в виде двух произведений

$$(a_1^p)^{t_1} \cdots (a_i^p)^{t_i} \cdots (a_u^p)^{t_u} = g^p = (b_1^p)^{d_1} \cdots (b_j^p)^{d_j} \cdots (b_v^p)^{d_v}, \tag{7.14}$$

где $0 \leqslant t_i < p^{k_i - 1}$, $0 \leqslant d_j < p^{n_j - 1}$, и для каждого g^p существует единственный набор показателей $t_1, \ldots, t_r$ и единственный набор показателей $d_1, \ldots, d_s$, для которых справедливо (7.14). Отсюда при помощи теоремы 7.6 немедленно получаем, что

$$G^p = \langle a_1^p \rangle \times \cdots \times \langle a_u^p \rangle = \langle b_1^p \rangle \times \cdots \times \langle b_v^p \rangle,$$

где $|\langle a_i \rangle| = p^{k_i - 1}$ и $|\langle b_j \rangle| = p^{n_j - 1}$. Так как $|G^p| = p^{m-r+u} = p^{m-s+v} \leqslant p^{m-1}$, то по предположению индукции $u = v$, $k_i - 1 = n_i - 1$ для $i \in \{1, \ldots, u\}$ и, следовательно, $r = s$ и $k_i = n_i$ для $i \in \{1, \ldots, r\}$. Теорема доказана.

Если конечная абелева p-группа G разлагается в прямое произведение своих циклических подгрупп $G_1 \times \cdots \times G_r$, то порядки $p^{k_1}, \ldots, p^{k_r}$ этих подгрупп называются *инвариантами*, или *инвариантными делителями* группы G. В следующей теореме покажем, что любая конечная абелева p-группа определяется своими инвариантами с точностью до изоморфизма.

Теорема 7.11. *Конечные абелевы p-группы изоморфны тогда и только тогда, когда они имеют одинаковые инварианты.*

Доказательство. Пусть $A = \langle a_1\rangle \times \cdots \times \langle a_r\rangle$, $|\langle a_i\rangle| = p^{k_i}$, $A \cong B$ и $\varphi : A \to B$ — изоморфизм A в B. Так как каждый элемент A однозначно представляется в виде произведения $a_1^{t_1}a_2^{t_2}\cdots a_r^{t_r}$, то очевидно, что и каждый элемент B однозначно представляется в виде произведения $\varphi(a_1)^{t_1}\varphi(a_2)^{t_2}\cdots\varphi(a_r)^{t_r}$, и, следовательно, $B = \langle\varphi(a_1)\rangle \times \cdots \times \langle\varphi(a_r)\rangle$. Таким образом, $p^{k_1}, \ldots, p^{k_r}$ — инварианты группы B, т. е. инварианты групп A и B совпадают.

Пусть теперь абелевы группы A и B имеют одинаковые инварианты. Тогда $A = \langle a_1\rangle \times \cdots \times \langle a_r\rangle$, $B = \langle b_1\rangle \times \cdots \times \langle b_r\rangle$ и $\langle a_i\rangle \cong \langle b_i\rangle$. Если отображение $\varphi_i : \langle a_i\rangle \to \langle b_i\rangle$ — изоморфизм $\langle a_i\rangle$ в $\langle b_i\rangle$, то легко видеть, что отображение $\varphi(x_1, \ldots, x_r) = (\varphi_1(x_1), \ldots, \varphi_r(x_r))$ будет изоморфизмом группы A в группу B. Теорема доказана.

Пример 7.15. Найдем все неизоморфные абелевы группы порядка 16. Так как $16 = 8 \cdot 2 = 4 \cdot 4 = 4 \cdot 2 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 2$, то любая абелева группа порядка 16 изоморфна одной из следующих групп:

$$\mathbb{Z}_{16}, \quad \mathbb{Z}_8 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_4,$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2. \quad \square$$

Объединяя теоремы 7.8 и 7.10, видим, что справедливо следующее утверждение, достаточно точно описывающее структуру конечной абелевой группы.

Теорема 7.12. *Каждая конечная абелева группа является прямым произведением циклических p-подгрупп. Любые два произведения состоят из одинакового числа множителей одного порядка.*

Как и в случае p-групп, порядки множителей в разложении конечной абелевой группы G в произведение циклических p-подгрупп называются *инвариантами* группы G. Нетрудно видеть, что имеет место следующая теорема, доказательство которой почти дословно повторяет доказательство теоремы 7.11.

Теорема 7.13. *Конечные абелевы группы изоморфны тогда и только тогда, когда они имеют одинаковые инварианты.*

Пример 7.16. Частный случай теоремы 7.13 был рассмотрен выше в примере 7.13, где было показано, что все абелевы группы с простыми несовпадающими инвариантами $p_1, \ldots, p_k$ изоморфны. □

Пример 7.17. Рассмотрим абелеву группу G порядка $3 \cdot 10^3$ с инвариантами $5^2, 5, 3, 2^2, 2$. Эту группу можно представить в виде произведения $G_{25} \times G_5 \times G_3 \times G_4 \times G_2$, где G_i — циклическая подгруппа порядка i. Так как

$$G_{25} \times G_5 \times G_3 \times G_4 \times G_2 \cong (G_{25} \times G_3 \times G_4) \times (G_5 \times G_2),$$

то, повторяя рассуждения примера 7.13, можно показать, что G является прямым произведением двух циклических подгрупп, чьи порядки равны 300 и 10. □

Пример 7.18. Перечислим все неизоморфные абелевы группы порядка 100. Так как $100 = 25 \cdot 4 = 25 \cdot 2 \cdot 2 = 5 \cdot 5 \cdot 4 = 5 \cdot 5 \cdot 2 \cdot 2$, то любая абелева группа порядка 100 изоморфна одной из следующих групп:

$$\begin{aligned} &\mathbb{Z}_{25} \times \mathbb{Z}_4, \quad \mathbb{Z}_{25} \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_4, \\ &\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2. \end{aligned} \tag{7.15}$$

Заметим, что

$$\begin{aligned} &\mathbb{Z}_{25} \times \mathbb{Z}_4 \cong \mathbb{Z}_{100}, && \mathbb{Z}_{25} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_{50} \times \mathbb{Z}_2, \\ &\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \cong \mathbb{Z}_{20} \times \mathbb{Z}_5, && \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_{10} \times \mathbb{Z}_{10}, \end{aligned}$$

т. е. каждую из групп в (7.15) можно представить в виде произведения меньшего числа циклических сомножителей. □

Обобщим рассуждения из примера 7.17 на произвольную абелеву группу G с инвариантами

$$\begin{array}{ll} p_1^{n_{11}},\ p_1^{n_{12}},\ p_1^{n_{13}}, \ldots,\ p_1^{n_{1m_1}}, & n_{11} \geqslant n_{12} \geqslant n_{13} \geqslant \ldots \geqslant n_{1m_1}, \\ p_2^{n_{21}},\ p_2^{n_{22}},\ p_2^{n_{23}}, \ldots,\ p_2^{n_{2m_2}}, & n_{21} \geqslant n_{22} \geqslant n_{23} \geqslant \ldots \geqslant n_{2m_2}, \\ \multicolumn{2}{c}{\dotfill} \\ p_k^{n_{k1}},\ p_k^{n_{k2}},\ p_k^{n_{k3}}, \ldots,\ p_k^{n_{km_k}}, & n_{k1} \geqslant n_{k2} \geqslant n_{k3} \geqslant \ldots \geqslant n_{km_k}. \end{array}$$

Положим $m = \max(m_1, \ldots, m_k)$. Можно считать, что все m_i равны m. Если это не так, то к инвариантам с основанием p_i добавим $m - m_i$ единиц. Группа G разлагается в прямое произведение

$$G_{11} \times G_{12} \times \cdots \times G_{1m} \times \cdots \times G_{k1} \times G_{k2} \times \cdots \times G_{km} \qquad (7.16)$$

своих циклических p_i-подгрупп G_{ij} порядка $p_i^{n_{ij}}$ (подгруппы, соответствующие добавленным к инвариантам единицам, будут тривиальными единичными подгруппами). Объединяя в (7.16) подгруппы с одинаковыми вторыми индексами, получим новое представление

$$(G_{11} \times G_{21} \times \cdots \times G_{k1}) \times \cdots \times (G_{1m} \times G_{2m} \times \cdots \times G_{km})$$

группы G. Так как при $s \neq t$ порядки подгрупп G_{si} и G_{ti} взаимно просты, то для каждого $i = 1, 2, \ldots, m$ произведение

$$G_{1i} \times G_{2i} \times \cdots \times G_{ki}$$

будет циклической подгруппой G_i порядка $q_i = p_1^{n_{1i}} p_2^{n_{2i}} \cdots p_k^{n_{ki}}$, причем q_{i+1} будет делить q_i для $i = 1, \ldots, m-1$.

Таким образом, произвольную абелеву группу G можно представить в виде произведения

$$G = G_1 \times G_2 \times \cdots \times G_m$$

ее циклических подгрупп G_i, где порядок подгруппы G_{i+1} делит порядок подгруппы G_i. Порядок подгруппы G_1 называется *показателем группы* G. В группе с показателем q максимальный порядок элемента равен q, и порядок каждого элемента группы делит q. Легко видеть, что абелева группа является циклической тогда и только тогда, когда ее порядок и показатель равны.

Следующая теорема является обращением теоремы Лагранжа для абелевых групп и обобщением примера 7.14.

Теорема 7.14. *Пусть m делит n. В абелевой группе порядка n существует подгруппа порядка m.*

Доказательство. Рассмотрим абелеву группу G порядка $n = p_1^{n_1} \cdots p_k^{n_k}$. Эта группа является прямым произведением $G_1 \times \cdots \times G_k$ своих силовских p_i-подгрупп G_i. Каждый делитель m порядка группы n представим в виде произведения $p_1^{m_1} \cdots p_k^{m_k}$, где $m_i \in \{0, 1, \ldots, n_i\}$ и $m_i \leqslant n_i$. Из разобранного выше примера 7.14 следует, что в каждой подгруппе G_i порядка $p_i^{n_i}$ найдется подгруппа H_i порядка $p_i^{m_i}$. Поэтому прямое произведение $H_1 \times \cdots \times H_k$ этих подгрупп будет подгруппой порядка m в группе G. Теорема доказана.

Теперь покажем, что утверждение теоремы 7.14 нельзя обобщить на неабелевы группы. Для этого рассмотрим симметрическую группу S_5. Порядок этой группы равен 120, а максимальный порядок ее элемента равен шести. Таким элементом, например, будет произведение двух циклов (123)(45). Ранее в примере 7.10 на с. 231 было показано, что любая группа порядка 15 является циклической. Следовательно, в S_5 нет подгруппы порядка 15, хотя $120 = 15 \cdot 8$.

7.5. Группа $\mathbb{Z}_n^*$

Из доказанной в главе 3 теоремы 3.17 следует, что группа $\mathbb{Z}_n^*$ при $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, где все p_i различные простые, изоморфна прямому произведению

$$\mathbb{Z}^*_{p_1^{k_1}} \times \mathbb{Z}^*_{p_2^{k_2}} \times \cdots \times \mathbb{Z}^*_{p_m^{k_m}}. \tag{7.17}$$

В приводимых далее леммах перечисляются все циклические группы $\mathbb{Z}_n^*$. Эти леммы позволят полностью описать структуру всех множителей в (7.17).

Лемма 7.1. *При каждом простом p группа $\mathbb{Z}_p^*$ — циклическая.*

Доказательство. Пусть m — показатель группы $\mathbb{Z}_p^*$. Так как порядок каждого элемента группы делит ее показатель, то каждый элемент $\mathbb{Z}_p^*$ является корнем двучлена $x^m - 1$. С другой стороны, двучлен $x^m - 1$ в поле $\mathbb{Z}_p$ имеет не более m корней.

Следовательно, $m = p - 1$ и $\mathbb{Z}_p^*$ — циклическая группа. Лемма доказана.

Лемма 7.2. *При любом простом p группа $\mathbb{Z}_{p^2}^*$ — циклическая. Более того, среди порождающих ее элементов существует элемент h, удовлетворяющий равенству $h^{p-1} = 1 + np$, где целое n не делится на p.*

Доказательство. Покажем, что в качестве требуемого элемента h можно взять либо порождающий элемент g группы $\mathbb{Z}_p^*$, либо элемент $g + p$.

Рассмотрим элемент $g+tp$, где $t \in \{0, 1\}$, и пусть d — порядок этого элемента в группе $\mathbb{Z}_{p^2}^*$. Нетрудно видеть, что $(g + tp)^d = g^d \pmod p$. Кроме того, из равенства $(g + tp)^d = 1 \pmod{p^2}$ следует, что $(g + tp)^d = 1 \pmod p$. Поэтому $g^d = 1 \pmod p$, и, следовательно, d должно делится на $p - 1$, т. е. либо $d = p - 1$, либо $d = p(p-1)$ в силу того, что $|\mathbb{Z}_{p^2}^*| = p(p-1)$. Таким образом для того, чтобы показать, что $g + tp$ является порождающим элементом в группе $\mathbb{Z}_{p^2}^*$, достаточно показать, что $d \neq p - 1$.

Так как g — порождающий элемент группы $\mathbb{Z}_p^*$, то найдется целое m, для которого $g^{p-1} = 1 + mp$. Тогда

$$(g + tp)^{p-1} = g^{p-1} + \binom{p-1}{1} tpg^{p-2} + \sum_{k=2}^{p-1} \binom{p-1}{k} (tp)^k g^{p-1-k} =$$

$$= 1 + p(m - tg^{p-2}) + p^2 tg^{p-2} + \sum_{k=2}^{p-1} \binom{p-1}{k} (tp)^k g^{p-1-k}.$$

Каждое произведение, стоящее под знаком суммы в последнем равенстве, делится на p^2. Следовательно, найдется такое целое k, что

$$(g + tp)^{p-1} = 1 + p(m - tg^{p-2}) + kp^2 = 1 + p(m - tg^{p-2} + kp).$$

Теперь покажем, что по крайней мере при одном из двух возможных значений t величина $n = m - tg^{p-2} + kp$ не делится на p. Если m не делится на p, то полагаем $t = 0$. Тогда $n = m+kp$ и легко видеть, что n не делится на p. Если же m делится на p,

то полагаем $t = 1$. В этом случае $n = m - g^{p-2} + kp$. Так как g и p взаимно простые, то g^{p-2} не делится на p. Поэтому n также не делится на p.

Таким образом, найдется t, равное нулю или единице, при котором $n = m - tg^{p-2} + kp$ не делится на p, и, следовательно, произведение pn не делится на p^2. Поэтому

$$(g + tp)^{p-1} = 1 + np \neq 1 \pmod{p^2},$$

т. е. $h = g + tp$ является порождающим элементом в группе $\mathbb{Z}^*_{p^2}$ и $h^{p-1} = 1 + pn$, где n не делится на p. Лемма доказана.

Лемма 7.3. *Если p — простое нечетное, то при каждом натуральном k группа $\mathbb{Z}^*_{p^k}$ — циклическая.*

Доказательство. Покажем, что при $k > 2$ порождающим элементом в группе $\mathbb{Z}^*_{p^k}$ будет порождающий элемент h группы $\mathbb{Z}^*_{p^2}$, указанный в лемме 7.2. Пусть d — порядок элемента h в группе $\mathbb{Z}^*_{p^k}$. Тогда из равенства $h^d = 1 \pmod{p^k}$ следует, что $h^d = 1 \pmod{p^2}$. Поэтому d должно делиться на $p(p-1)$, т. е. d равно произведению $p^s(p-1)$. Покажем, что это равенство возможно только при $s = k - 1$.

Из леммы 7.2 следует, что $h^{p-1} = 1 + np$, где n не делится на p. Тогда, учитывая, что $\binom{p}{i}$ делится на p при $i \neq 0, p$,

$$h^{p(p-1)} = (1 + np)^p = 1 + \binom{p}{1} np + \sum_{i=2}^{p} \binom{p}{i} (np)^i = \\ = 1 + np^2 + n'p^3 = 1 + p^2(n + n'p) = 1 + p^2 n_1,$$

где очевидно n_1 на p не делится[1)]. Возводя аналогичным образом получившееся равенство $h^{p(p-1)} = 1 + p^2 n_1$ в степени $p, p^2, \ldots$, легко видеть, что для любого натурального s справедливо равенство

$$h^{p^s(p-1)} = 1 + p^{s+1} n_s,$$

[1)] Последнее равенство со свойством $p \nmid n_1$ справедливо только при $p > 2$, поэтому и лемма 7.3 неверна для единственного четного простого числа $p = 2$, — см. далее лемму 7.5 и ср. с леммой 7.2.

где n_s не делится на p. Следовательно,

$$h^{p^{k-2}(p-1)} \neq 1 \pmod{p^k}.$$

Таким образом порядок h в группе $\mathbb{Z}_{p^k}^*$ равен $p^{k-1}(p-1)$, т. е. этот элемент является порождающим элементом группы. Лемма доказана.

Пример 7.19. Рассмотрим группу $\mathbb{Z}_9^*$. В $\mathbb{Z}_3^*$ порождающим элементом является 2. Так как $2^2 = 4 \pmod 9$, то 2 — порождающий элемент в $\mathbb{Z}_9^*$. □

Пример 7.20. Найдем порождающий элемент в группе $\mathbb{Z}_{19^2}^*$. Так как $2^6 - 1$ и $2^9 - 1$ не делятся на 19, то 2 будет порождающим элементом в $\mathbb{Z}_{19}^*$. Теперь проверим, выполняется ли равенство $2^{18} = 1 \pmod{19^2}$. Так как $19^2 = 361$ и

$$2^{18} - 1 = (2^9 - 1)(2^9 + 1) = 511 \cdot 513,$$

то легко видеть, что ни 511, ни 513 не делятся на 361. Также легко видеть, что 511 и 513 не могут одновременно делиться на 19. Следовательно, $2^{18} \neq 1 \pmod{19^2}$, и 2 является порождающим элементом в $\mathbb{Z}_{19^2}^*$. □

Лемма 7.4. *Если p — простое нечетное, то при каждом натуральном k группа $\mathbb{Z}_{2p^k}^*$ — циклическая.*

Доказательство. Прежде всего заметим, что группа $\mathbb{Z}_{2p^k}^*$ состоит из $(p-1)p^{k-1}$ натуральных чисел, каждое из которых нечетно, не делится на p и меньше, чем $2p^k$.

Пусть g — порождающий элемент группы $\mathbb{Z}_{p^k}^*$. Если g нечетное число, то g принадлежит группе $\mathbb{Z}_{2p^k}^*$. Его порядок в этой группе обозначим через d. Тогда из равенства $g^d = 1 \pmod{2p^k}$ следует, что

$$g^d = 1 + 2p^k \cdot n = 1 + p^k \cdot 2n = 1 \pmod{p^k}.$$

Таким образом, $d = (p-1)p^{k-1}$, и, следовательно, g будет порождающим элементом в группе $\mathbb{Z}_{2p^k}^*$.

Если g — четное, то нечетным будет число $g + p^k$, вычет которого по четному модулю $2p^k$ очевидно принадлежит группе $\mathbb{Z}^*_{2p^k}$. Пусть d — порядок этого вычета в группе $\mathbb{Z}^*_{2p^k}$. Тогда из равенства $(g + p^k)^d = 1 \pmod{2p^k}$ и четности g следует, что

$$1 + 2p^k \cdot n = (g + p^k)^d = g^d + \sum_{i=1}^{d} \binom{d}{i} p^{ki} g^{d-i} = g^d + 2p^k \cdot m,$$

т. е. $g^d = 1 \pmod{p^k}$. Таким образом, $d = (p-1)p^{k-1}$, и, следовательно, вычет числа $g + p^k$ по модулю $2p^k$ будет порождающим элементом в группе $\mathbb{Z}^*_{2p^k}$.

Вообще говоря, утверждение леммы 7.4 сразу следует из разложения (7.17) и леммы 7.3, так как при нечетном p

$$\mathbb{Z}^*_{2p^k} \cong \mathbb{Z}^*_2 \times \mathbb{Z}^*_{p^k} \cong \{1\} \times \mathbb{Z}^*_{p^k} \cong \mathbb{Z}^*_{p^k}.$$

Однако доказательство с явным указанием порождающего элемента группы $\mathbb{Z}^*_{2p^k}$, как это было сделано в предыдущих леммах, дает дополнительную полезную информацию об этой группе. Лемма доказана.

Лемма 7.5. *При $k \geqslant 3$ группа $\mathbb{Z}^*_{2^k}$ не является циклической и изоморфна прямому произведению группы порядка 2 и циклической группы порядка 2^{k-2}.*

Доказательство. Преобразуя разность $5^{2^{k-2}} - 1$ по формуле разности квадратов, приходим к равенству

$$5^{2^{k-2}} - 1 = (5^{2^0} - 1) \prod_{i=0}^{k-3} (5^{2^i} + 1) = 4 \cdot \prod_{i=0}^{k-3} (5^{2^i} + 1),$$

в правой части которого первый множитель равен 4, а остальные $k - 2$ четные. Таким образом, разность $5^{2^{k-2}} - 1$ делится на 2^k, и, следовательно, $5^{2^{k-2}} = 1 \pmod{2^k}$.

Теперь рассмотрим разность $5^{2^{k-3}} - 1$. Так как $5 = 1 \pmod 4$, то и $5^n = 1 \pmod 4$ при любом натуральном n. Поэтому в правой части равенства

$$5^{2^{k-3}} - 1 = 4 \prod_{i=0}^{k-4} (5^{2^i} + 1)$$

ни один из сомножителей вида $(5^{2^i}+1)$ не делится на 4, и, следовательно, все произведение не делится на 2^k. Таким образом, порядок 5 в группе $\mathbb{Z}_{2^k}^*$ больше, чем 2^{k-3} и, следовательно, равен 2^{k-2}.

Далее заметим, что $5^n \neq -5 \pmod{2^k}$ ни при каком n, так как в этом случае также справедливо равенство $5^n = -5 \pmod 4$, которое, очевидно, противоречит равенствам $5^n = 1 \pmod 4$ и $-5 = 3 \pmod 4$. Поэтому все числа вида $(-1)^i 5^j$, где $i = 0, 1$ и $j = 1, \ldots, 2^{k-2}$, различны по модулю 2^k, и так как все эти числа нечетные, то они образуют группу $\mathbb{Z}_{2^k}^*$.

Теперь легко видеть, что отображение $\varphi : \mathbb{Z}_{2^k}^* \to \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$, преобразующее число $(-1)^i 5^j$ в пару чисел (i, j), является изоморфизмом, т. е. $\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$. Лемма доказана.

Лемма 7.6. *Пусть $n = m_1 m_2$, где m_1 и m_2 взаимно простые и не равные 2. Тогда группа $\mathbb{Z}_n^*$ не является циклической.*

Доказательство. Прежде всего заметим, что в силу теоремы 3.17 группа $\mathbb{Z}_{m_1 m_2}^*$ изоморфна прямому произведению $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$. Так как $m_1, m_2 > 2$, то группы $\mathbb{Z}_{m_1}^*$ и $\mathbb{Z}_{m_2}^*$ состоят из четного числа элементов, и поэтому каждая из этих групп имеет элемент порядка 2. Следовательно, в $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$ найдутся два различных элемента второго порядка, что невозможно в циклической группе. Лемма доказана.

Собирая вместе результаты доказанных лемм 7.1—7.6, получаем следующую теорему, позволяющую с учетом (7.17) исчерпывающе описать структуру мультипликативной группы кольца вычетов по модулю n.

Теорема 7.15. *Группа $\mathbb{Z}_n^*$ является циклической тогда и только тогда, когда $n = 2, 4$, или $n = p^k$, или $n = 2p^k$, где p — нечетное простое, k — произвольное натуральное. При $k \geqslant 3$ группа $\mathbb{Z}_{2^k}^*$ не является циклической, однако $\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$.*

Пример 7.21. Теорема 7.12 показывает, что абелева группа $\mathbb{Z}_{63000}^*$ разлагается в прямое произведение своих циклических

p-подгрупп. Воспользуемся результатами этого раздела и найдем явный вид этого произведения. Так как $63000 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7$, то

$$\mathbb{Z}^*_{63000} \cong \mathbb{Z}^*_{2^3} \times \mathbb{Z}^*_{3^2} \times \mathbb{Z}^*_{5^3} \times \mathbb{Z}^*_7. \tag{7.18}$$

Имеем $\mathbb{Z}^*_{2^3} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}^*_{3^2} \cong \mathbb{Z}^*_7 \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ и $\mathbb{Z}^*_{5^3} \cong \mathbb{Z}_{100} \cong$ $\cong \mathbb{Z}_4 \times \mathbb{Z}_{25}$ по леммам 7.1—7.5. Таким образом,

$$\mathbb{Z}^*_{63000} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}, \tag{7.19}$$

и инвариантами группы $\mathbb{Z}^*_{63000}$ являются $5^2, 3, 3, 2^2, 2, 2, 2, 2$. Следовательно, максимальный порядок ее элементов (показатель группы), совпадающий с наименьшим общим кратным ее инвариантов, равен $5^2 \cdot 3 \cdot 2^2 = 300$.

Найти любой конкретный элемент, порядок которого делит 300, можно с помощью порождающих элементов циклических разложений групп $\mathbb{Z}^*_{2^3}, \mathbb{Z}^*_{3^2}, \mathbb{Z}^*_{5^3}, \mathbb{Z}^*_7$ и китайской теоремы об остатках. □

Пример 7.22. Изоморфизмы (7.18) и (7.19) помогают и решать уравнения в $\mathbb{Z}^*_{63000}$, и легко находить число их корней, не решая явно. Например, сравнение $x^2 = 1 \pmod{63000}$ имеет $2^5 = 32$ корня, так как в циклических группах порядка 2 и 4 уравнение $x^2 = 1$ имеет по 2 корня, а в циклических группах порядка 3 и 25 только один (единицу группы). Одним из искомых корней будет, например, вычет x, равный 5 по модулю 2^3 и (-1) по модулям 3^2, 5^3 и 7. Его явный вид $x = 15749 \pmod{63000}$ можно найти по формуле теоремы 2.11 (стр. 45). □

Задачи

7.1. Почему мощность любого класса сопряженных элементов конечной группы делит ее порядок? Перечислить все группы, имеющие ровно три класса сопряженных элементов.

7.2. Пусть подстановки $f, h \in S_n$ имеют тип $(k_1, k_2, \ldots, k_n)$. Найти число сопрягающих их подстановок, то есть число таких g, что $f = ghg^{-1}$.

7.3. Пусть подстановка $\pi \in S_n$ имеет тип $(k_1, k_2, \ldots, k_n)$ и пусть $m = k_1 + k_2 + \ldots + k_n$. Доказать, что $\operatorname{sgn}(\pi) = (-1)^{n-m}$.

7.4. Привести пример двух четных подстановок, сопряженных в группе S_n и не сопряженных в группе A_n.

7.5. Найти число орбит в группах S_5, A_5, S_6, A_6, S_7 и A_7 при их действии сопряжением на себя.

7.6. Найти число неизоморфных групп порядков $2, 3, 4, 5, 6, 7, 8$.

7.7. Найти число неизоморфных групп порядков $35, 65, 77, 175$.

7.8. Пусть группа G имеет порядок p_1p_2, где p_1, p_2 — различные простые числа, такие, что $p_1 = 1 \pmod{p_2}$. Доказать, что $G = \langle a, b\rangle$, где порядки элементов a и b равны p_1 и p_2 соответственно, причем $bab^{-1} = c$, где c — образующий элемент подгруппы $\langle a\rangle$.

7.9. При каких значениях m, n группа $\langle a\rangle_m \times \langle b\rangle_n$ — циклическая?

7.10. Пусть $G = \langle a\rangle_{12} \times \langle b\rangle_{30}$. Найти максимальный порядок элемента в G. Сколько различных подгрупп в G имеет порядок 6? Найти число различных гомоморфизмов $\varphi : G \to \langle c\rangle_{18}$ и $\psi : \langle c\rangle_{18} \to G$.

7.11. Пусть $Z(G)$ — центр некоммутативной группы G. Доказать, что фактор-группа $G/Z(G)$ не может быть циклической.

7.12. Пусть G — произвольная группа. Доказать, что группа $G/Z(G)$ изоморфна группе всех сопряжений G.

7.13. Показать, что в группе порядка p^k, где p — простое, существует нормальная подгруппа порядка p^{k-1}.

7.14. Найти все нормальные подгруппы в симметрической группе S_4 и построить все гомоморфизмы $\varphi : S_4 \to S_4$.

7.15. Найти число неизоморфных абелевых групп порядков $8, 9, 48, 60, 900, 1000$.

7.16. Доказать теорему Коши: если порядок конечной группы G делится на простое число p, то в G существует элемент порядка p.

7.17. Показать, что в группе порядка p^k, где p — простое, для любого $m < k$ существует подгруппа порядка p^m.

7.18. Найти число силовских 2-подгрупп и 3-подгрупп в группе S_4.

7.19. Для простого p найти порядок силовской p-подгруппы в группе S_n.

7.20. Для простого p найти число силовских p-подгрупп в S_p.

7.21. Пусть p, q — простые, $p < q$ и $q-1$ не делится на p. Доказать, что любая группа порядка pq коммутативна.

7.22. Для простого p в некоммутативной группе порядка p^3 найти число классов сопряженности и число элементов в каждом таком классе.

7.23. Доказать, что центр прямого произведения групп G и H равен произведению центров, т. е. $Z(G \times H) = Z(G) \times Z(H)$.

7.24. В группе G найти максимальный порядок элемента и число элементов максимального порядка, если: 1) $G = \mathbb{Z}^*_{256}$; 2) $G = \mathbb{Z}^*_{2310}$; 3) $G = \mathbb{Z}^*_{40000}$.

7.25. Решить уравнение $x^{95} = 1$ в кольце $\mathbb{Z}_{30030}$.

7.26. Доказать, что показатель любой абелевой группы равен максимальному порядку ее элементов.

7.27. Разложить в прямое произведение циклических p-подгрупп циклическую группу порядка: 1) 12; 2) 24; 3) 60; 4) 900.

7.28. Пусть T — множество всех элементов максимального порядка конечной абелевой группы G. Доказать, что $G = \langle T \rangle$.

7.29. Показать, что если в конечной коммутативной группе порядок каждого неединичного элемента равен p, p — простое, то группа изоморфна группе $\mathbb{Z}_p^k$.

7.30. Пусть A — подмножество элементов группы G. Множество $N(A)$ всех элементов $g \in G$ таких, что $gAg^{-1} = A$, называется *нормализатором* множества A. Показать, что $N(A)$ — подгруппа в G.

7.31. Найти нормализатор $N(H)$ подгруппы H в группе S_4, если: 1) $H = \langle (12) \rangle$; 2) $H = \langle (1234) \rangle$; 3) $H = \{e, (12)(34), (13)(24), (14)(23)\}$.

Глава 8

Конечные поля

В этой главе подробно изучаются конечные поля, их основные свойства, внутренняя структура. Рассмотрены особенности выполнения вычислений с элементами конечных полей.

8.1. Мультипликативная группа поля

Из доказанной в предыдущей главе леммы 7.1 следует цикличность мультипликативной группы поля $\mathbb{Z}_p$. Ниже покажем, что циклической будет мультипликативная группа любого конечного поля. Сделаем это, в отличии от доказательства леммы 7.1, не используя понятие показателя группы.

Лемма 8.1. *В группе G порядка n, где $n = p_1^{k_1} \dots p_r^{k_r}$ — разложение числа n на простые множители, элемент $h \in G$ имеет порядок n, т.е. является порождающим в G, тогда и только тогда, когда выполнено условие*

$$h^{n/p_i} \neq 1 \qquad \text{для всех} \quad i = 1, \dots, r. \tag{8.1}$$

Доказательство. Необходимость. Если хотя бы для одного значения i неравенство (8.1) превращается в равенство, то порядок элемента h строго меньше, чем n, так как из $h^{n/p_i} = 1$ следует, что порядок h делит n/p_i.

Для доказательства достаточности воспользуемся теоремой Лагранжа. Заметим, что порядок элемента h является делителем числа $n = |G|$, а значит имеет вид $p_1^{x_1} \dots p_r^{x_r}$, где $0 \leqslant x_i \leqslant k_i$ при всех i. Из условия (8.1) следует, что при каждом $i = 1, \dots, r$

порядок h не делит $p_1^{k_1}\dots p_{i-1}^{k_{i-1}}p_i^{k_i-1}p_{i+1}^{k_{i+1}}\dots p_s^{k_s}$, откуда $x_i = k_i$. Следовательно, $|h| = n$ и элемент h — порождающий в G. Лемма доказана.

Теорема 8.1. *Мультипликативная группа конечного поля циклическая.*

Доказательство. Рассмотрим поле $\mathbb{F}_q$, состоящее из q элементов. Пусть $q-1 = p_1^{k_1}\cdots p_r^{k_r}$ — разложение числа $q-1 = |\mathbb{F}_q^*|$ на простые множители. При каждом i многочлен $x^{(q-1)/p_i} - 1$ имеет в мультипликативной группе поля $\mathbb{F}_q$ не более $(q-1)/p_i$ корней, поэтому для каждого i в этой группе найдется элемент g_i такой, что

$$g_i^{(q-1)/p_i} \neq 1. \tag{8.2}$$

Положим $h_i = g_i^{(q-1)/p_i^{k_i}}$, $h = \prod_{i=1}^r h_i$ и покажем, что h будет порождающим элементом в $\mathbb{F}_q^*$. По лемме 8.1 для этого достаточно доказать, что $h^{(q-1)/p_i} \neq 1$ для каждого i. Сделаем это только для $i = 1$, так как легко видеть, что доказательства для разных значений i аналогичны.

Так как группа $\mathbb{F}_q^*$ абелева, то $h^{(q-1)/p_1} = \prod_{i=1}^r h_i^{(q-1)/p_1}$. Далее заметим, что произведение $((q-1)/p_i^{k_i})\cdot(q-1)/p_1$ кратно $q-1$, если $i \neq 1$. Поэтому

$$h_i^{(q-1)/p_1} = 1 \quad \text{при} \quad i \neq 1. \tag{8.3}$$

Теперь найдем порядок элемента h_1. Так как $h_1^{p_1^{k_1}} = g_i^{q-1} = 1$, то порядок элемента h_1 равен p_1^s, где $s \leqslant k_1$. Но из неравенства (8.2) следует, что $h_1^{p_1^{k_1-1}} = g_1^{(q-1)/p_1} \neq 1$. Поэтому порядок элемента h_1 равен $p_1^{k_1}$. Учитывая, что $(q-1)/p_1$ не делится на $p_1^{k_1}$, то заключаем, что

$$h_1^{(q-1)/p_1} \neq 1. \tag{8.4}$$

Из (8.3) и (8.4) следует, что $h^{(q-1)/p_1} \neq 1$. Теорема доказана.

Пример 8.1. Покажем, что в поле $\mathbb{Z}_3[x]/(x^3+2x+1)$ из примера 4.18 порождающим элементом мультипликативной группы

будет элемент $x = (010)$. Используя равенство[1)] $x^3 = x+2$, легко находим все степени x:

$$
\begin{array}{llll}
x^0 = (001), & x^7 = (122), & x^{14} = (020), & x^{21} = (101), \\
x^1 = (010), & x^8 = (202), & x^{15} = (200), & x^{22} = (022), \\
x^2 = (100), & x^9 = (011), & x^{16} = (021), & x^{23} = (220), \\
x^3 = (012), & x^{10} = (110), & x^{17} = (210), & x^{24} = (221), \\
x^4 = (120), & x^{11} = (112), & x^{18} = (121), & x^{25} = (201). \ \square \\
x^5 = (212), & x^{12} = (102), & x^{19} = (222), & \\
x^6 = (111), & x^{13} = (002), & x^{20} = (211), &
\end{array}
$$

Образующий элемент мультипликативной группы поля $\mathbb{F}_q$ (т. е. имеющий порядок $q-1 = |\mathbb{F}_q^*|$) называется *примитивным* элементом этого поля. Теорема 8.1 утверждает, что примитивный элемент есть в любом конечном поле. Более того, поле порядка q содержит ровно $\varphi(q-1)$ примитивных элементов, т. к. циклическая группа порядка $(q-1)$ имеет ровно $\varphi(q-1)$ образующих (см. теорему 3.14).

Пусть α — примитивный элемент поля $\mathbb{F}_q$ и β — ненулевой элемент этого поля. Минимальное неотрицательное число i, для которого $\beta = \alpha^i$, называется *индексом* или *дискретным логарифмом* элемента β по основанию α и обозначается $i = \log_\alpha \beta$. В примере 8.1 фактически построена таблица логарифмов поля $\mathbb{F}_{27} = \mathbb{Z}_3[x]/(x^3+2x+1)$ по основанию $\alpha = x$. Из нее, например, следует, что $\log_\alpha(\alpha^2+\alpha) = 10$.

Все примитивные элементы поля можно легко получить, зная один из них. Действительно, по теореме 3.16 в группе, образованной элементом α порядка n, порядок элемента α^x равен $n/(n,x)$ и, следовательно, совпадает с порядком α тогда и только тогда, когда n и x взаимно просты. Например, зная, что вычет $\alpha = 2$ является примитивным в поле $\mathbb{Z}_{13}$, получаем, что

[1)] Строго говоря, надо было написать $[x]^3 = [x] + [2]$, так как это равенство вычетов, но мы, начиная с этого момента, опускаем лишние скобки, чтобы они не загромождали запись. Равенство $x^4 = (120)$ следует из того, что $x^4 = x \cdot x^3 = x(x+2) = x^2 + 2x$, откуда $x^5 = x(x^2+2x) = x^3 + 2x^2 = 2x^2 + x + 2 = (212)$, и т. д.

вычеты $2^5 = 6$, $2^7 = 11$ и $2^{11} = 7$ также являются примитивными, и других примитивных элементов в $\mathbb{Z}_{13}$ нет.

Пример 8.2. В поле $\mathbb{F}_{128}$ любой элемент $\alpha \neq 0, 1$ является примитивным, так как порядок его мультипликативной группы $|\mathbb{F}_{128}^*| = 127$ — простое число (см. пример 3.21). □

Указать конкретный примитивный элемент в конечном поле $\mathbb{F}_q$ часто помогает проверка неравенств леммы 8.1 в группе $G = \mathbb{F}_q^*$. Так, для доказательства примитивности элемента $x \in \mathbb{Z}_3[x]/(x^3 + 2x + 1)$ из примера 8.1 достаточно было проверить, что $x^2 \neq 1$ и $x^{13} \neq 1$. Для этого, вообще говоря, не нужно строить всю таблицу логарифмов.

Пример 8.3. Найдем какой-либо примитивный элемент в $\mathbb{Z}_{113}$. Число 113 является простым (оно не делится ни на одно из простых чисел $2, 3, 5, 7$, меньших $\sqrt{113}$), поэтому $\mathbb{Z}_{113}$ — конечное поле и по этой причине содержит примитивные элементы. Разложим на простые множители порядок его мультипликативной группы $113 - 1 = 112 = 2^4 \cdot 7$ и проверим выполнение условия (8.1). Претендентов на примитивность $\alpha \in \mathbb{Z}_{113}^*$ будем перебирать в порядке возрастания[1)]. Отметим, что при наших вычислениях можно легко обойтись без калькулятора и компьютера. Действительно, возьмем вычет $\beta = 2$ и возведем его в степень $112/2 = 56$:

$$2^{2^3 \cdot 7} = 128^8 = 15^8 = (15^2)^4 = 225^4 = (-1)^4 = 1 \pmod{113}.$$

Следовательно, вычет $\beta = 2$ не примитивен. Попутно мы нашли,

[1)] Один из результатов аналитической теории чисел, выходящий за рамки данного курса, гласит, что если справедлива расширенная гипотеза Римана, то наименьший примитивный корень из $\mathbb{Z}_p$ при всяком простом p не превосходит величины $a \log^b p$, где a и b — некоторые константы, не зависящие от p. Значит, в предположении, что гипотеза верна, перебор малых вычетов из $\mathbb{Z}_p$ должен дать положительный результат. Расширенная гипотеза Римана утверждает, что все комплексные нули z_0 функции $L_\chi(z) = \sum_{n=1}^{\infty} \chi(n)/n^z$, называемой рядом Дирихле, которые находятся в полосе $0 < \operatorname{Re} z_0 < 1$ комплексной плоскости $\mathbb{C}$, должны лежать на прямой $\operatorname{Re} z_0 = \frac{1}{2}$. Гипотеза в настоящий момент не доказана, но нули функций $L_\chi(z)$ численно проверены для астрономически больших значений $\operatorname{Im} z_0$.

что его порядок равен 28, так как $2^4 \neq 1 \pmod{113}$ и $2^{14} \neq 1 \pmod{113}$.

Перейдем к следующему вычету $\alpha = 3$. Действуя аналогичным образом, видим, что

$$\begin{aligned} 3^{2^3 \cdot 7} &= (3^7)^{2^3} = (243 \cdot 3^2)^8 = (17 \cdot 9)^8 = 153^8 = 40^8 = \\ &= (40^2)^4 = 1600^4 \stackrel{\circ}{=} 18^4 = 324^2 = 98^2 = (-15)^2 = 15^2 = \\ &= 225 = -1 \neq 1 \pmod{113}. \end{aligned}$$

При этом честно поделить с остатком нам пришлось всего один раз на шаге, отмеченном значком $\stackrel{\circ}{=}$ (а можно было заметить, что $1600 = 1130 + 470 = 470 = 18 \pmod{113}$). Все остальные приведения по модулю 113, которые мы выполняли на каждом шаге, свелись к одному-двум вычитаниям числа 113 из текущего результата. Указанный способ[1)] значительно проще честного возведения в степень с последующим взятием остатка, так как $3^{56} = 523\,347\,633\,027\,360\,537\,213\,511\,521$.

Наконец,

$$\begin{aligned} 3^{2^4} &= (3^4)^4 = 81^4 = (-32)^4 = (2 \cdot 16)^4 = (4 \cdot 256)^2 = \\ &= (4 \cdot 30)^2 = 7^2 = 49 \neq 1 \pmod{113}. \end{aligned}$$

Таким образом, мы доказали, что вычет 3 примитивен. □

Пример 8.4. В силу взаимной простоты чисел 7 и $26 = |\mathbb{F}_{27}^*|$ элемент α^7, так же как и элемент α, будет примитивным в поле $\mathbb{F}_{27}$ из примера 8.1. Найдем дискретный логарифм элемента $\alpha^{10} = \alpha^2 + \alpha$ по основанию α^7. Это нетрудно сделать, зная, что $\log_\alpha \alpha^{10} = 10$. Действительно, равенство $(\alpha^7)^i = \alpha^{10}$ равносильно сравнению $7i = 10 \pmod{26}$. Его наименьшим положительным решением будет $i = 10 \cdot 7^{-1} = 10 \cdot 15 = 20 \pmod{26}$, поэтому $\log_{\alpha^7} \alpha^{10} = 20$. □

Обобщая это простое наблюдение на произвольное конечное поле $\mathbb{F}_q$ и его примитивные элементы α, γ, получим равенство

$$\log_\gamma \beta = \frac{\log_\alpha \beta}{\log_\alpha \gamma}, \tag{8.5}$$

[1)] Модификация бинарного возведения в степень, см. [16].

где β — произвольный элемент из $\mathbb{F}_q^*$, а под делением понимается умножение на обратный вычет по модулю $q-1$. Равенство (8.5) является дискретным аналогом известной формулы перехода под знаком логарифма к другому основанию над полем $\mathbb{R}$. Оно показывает, что, зная логарифм по одному примитивному основанию, его нетрудно найти и по всем остальным. Вычислению дискретных логарифмов посвящен раздел 9.3.

8.2. Разложение $x^{p^n} - x$ на множители

При изучении конечных полей особую роль играет двучлен $x^{p^n} - x$. Ниже в теореме 8.2 найдено разложение этого двучлена на неприводимые над $\mathbb{Z}_p$ множители. Далее это разложение позволит легко установить структуру и основные свойства любого конечного поля.

Лемма 8.2. *Пусть p — простое, $g(x)$ — произвольный многочлен над полем $\mathbb{Z}_p$. Тогда*

$$(g(x))^p = g(x^p).$$

Доказательство. Так как p простое, то в правой части равенства

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

все коэффициенты $\binom{p}{k}$ при $k \neq 0, p$ делятся на p. Поэтому

$$(a+b)^p = a^p + b^p \tag{8.6}$$

для любых a и b из $\mathbb{Z}_p$. Используя равенство (8.6) в качестве основания индукции, индукцией по числу слагаемых нетрудно показать, что

$$(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p \tag{8.7}$$

для любого n и любых $a_1, \ldots, a_n \in \mathbb{Z}_p$. Так как $a^p = a$ для каждого a из $\mathbb{Z}_p$, то для любого многочлена $g(x)$

$$\begin{aligned}(g(x))^p &= (g_n x^n + \cdots + g_1 x + g_0)^p = \\ &= (g_n x^p)^n + \cdots + (g_1 x)^p + (g_0)^p = \\ &= g_n (x^p)^n + \cdots + g_1 x^p + g_0 = g(x^p).\end{aligned}$$

Лемма доказана.

Следствие 8.1. *Для всех целых неотрицательных n, простых p и любого многочлена $g(x) \in \mathbb{Z}_p[x]$ выполнено равенство* $\big(g(x)\big)^{p^n} = g(x^{p^n})$.

Формальной производной многочлена $f(x) = a_n x^n + \cdots + a_1 x + a_0$ называется многочлен $f'(x) = n a_n x^{n-1} + \cdots + a_1$. Заметим, что преобразование многочлена в его формальную производную является линейным преобразованием. Используя это свойство, нетрудно показать, что для формальной производной произведения двух многочленов справедлива формула Лейбница

$$\big(f(x)h(x)\big)' = f'(x)h(x) + f(x)h'(x). \tag{8.8}$$

Действительно, для одночленов $f(x) = ax^n$ и $h(x) = bx^m$ равенство (8.8) очевидно, поэтому по линейности оно верно и для случая $f(x) = a_n x^n + \ldots + a_1 x + a_0$ и $h(x) = bx^m$, откуда следует его справедливость для многочленов $f(x)$ и $h(x)$ общего вида.

По индукции из (8.8) получаем следующий способ вычисления производной произведения m многочленов:

$$(f_1 \cdot \ldots \cdot f_m)' = \sum_{i=1}^{m} f_i' \cdot \prod_{j \neq i} f_j,$$

откуда следует равенство $\big(f^m\big)' = m f^{m-1} \cdot f'$.

Теорема 8.2. *Для всех простых p и целых неотрицательных n*

$$x^{p^n} - x = \prod h(x), \tag{8.9}$$

где произведение берется по всем нормированным неприводимым над $\mathbb{Z}_p$ многочленам из $\mathbb{Z}_p[x]$, степени которых делят n.

Доказательство. Пусть $h(x)$ — неприводимый многочлен степени m. Так как $\mathbb{Z}_p[x]/h(x)$ является полем, которое состоит из p^m элементов, то в мультипликативной группе этого поля порядок любого элемента, в том числе и одночлена x, является делителем числа $p^m - 1$, и, следовательно,

$$x^{p^m} = x \pmod{h(x)}. \tag{8.10}$$

Представим n в виде $n = km+r$, где $0 \leqslant r < m$. Тогда, учитывая равенство (8.10), имеем

$$x^{p^n} = x^{p^{km+r}} = \left(x^{p^{km}}\right)^{p^r} = x^{p^r} \pmod{h(x)}. \tag{8.11}$$

Если n делится на m, т. е. $r = 0$, то в силу предыдущего равенства

$$x^{p^n} - x = 0 \pmod{h(x)},$$

и, следовательно, двучлен $x^{p^n} - x$ делится на многочлен $h(x)$.

Теперь предположим, что двучлен $x^{p^n} - x$ делится на $h(x)$ и n не делится на m, т. е. $r > 0$. В этом случае

$$x^{p^n} - x = 0 \pmod{h(x)},$$

и из (8.11) следует равенство

$$x^{p^r} = x \pmod{h(x)}.$$

Далее заметим, что в силу леммы 8.2 для любого элемента g поля $\mathbb{Z}_p[x]/h(x)$ из предыдущего равенства следует, что

$$(g(x))^{p^r} = g(x^{p^r}) = g(x) \pmod{h(x)}.$$

Таким образом, порядок любого элемента поля $\mathbb{Z}_p[x]/h(x)$ не превосходит $p^r - 1$. Так как $r < m$, то в этом поле нет порождающего элемента, что противоречит теореме 8.1.

Поэтому двучлен $x^{p^n} - x$ является произведением всех неприводимых многочленов, степени которых делят n. Пусть $h(x)$ — один из таких многочленов. Покажем, что $x^{p^n} - x$ не делится на

$(h(x))^2$. Для этого рассмотрим формальную производную произведения квадрата $h(x)$ и произвольного многочлена $g(x)$. Легко видеть, что

$$\begin{aligned}\big(h(x)^2 g(x)\big)' &= 2h(x)h'(x)g(x) + h(x)^2 g'(x) = \\ &= h(x)(2h'(x)g(x) + h(x)g'(x)).\end{aligned}$$

Поэтому производная произведения $(h(x))^2 g(x)$ либо делится на $h(x)$, либо равна нулю (если $2h'(x)g(x) + h(x)g'(x) = 0$). Дифференцируя $x^{p^n} - x$, легко находим, что производная этого двучлена равна минус единице. Таким образом, в разложении $x^{p^n} - x$ на неприводимые многочлены нет кратных множителей. Следовательно,

$$x^{p^n} - x = \prod h(x),$$

где произведение берется по всем неприводимым многочленам, степени которых делят n. Теорема доказана.

Пример 8.5. В $\mathbb{Z}_2[x]$ при $n = 3$ равенство (8.9) принимает вид

$$x^{2^3} - x = x(x+1)(x^3 + x^2 + 1)(x^3 + x + 1). \square$$

Из теоремы 8.2 легко извлекается доказанное на с. 116 с использованием метода производящих функций рекуррентное равенство для числа $N(p, m)$ неприводимых над $\mathbb{Z}_p$ многочленов степени m:

$$p^n = \sum_{m \mid n} mN(p, m).$$

Пример 8.6. Чтобы проиллюстрировать это утверждение, найдем число неприводимых многочленов степени 15 над $\mathbb{Z}_2$ с помощью теоремы 8.2, независимо от результатов раздела 4.6. Обозначим через $F_i(x)$ произведение всех различных неприводимых над $\mathbb{Z}_2$ многочленов, степень которых равна i. Тогда, согласно (8.9),

$$x^{2^{15}} - x = F_1(x)F_3(x)F_5(x)F_{15}(x),$$

причем $F_1(x)F_3(x) = x^{2^3} - x$ и $F_1(x)F_5(x) = x^{2^5} - x$. Отсюда

$$F_{15}(x) = \frac{x^{2^{15}} - x}{(F_1F_3)(F_1F_5)} \cdot F_1 = \frac{x^{2^{15}} - x}{(x^{2^3} - x)(x^{2^5} - x)} \cdot (x^2 - x).$$

Следовательно, степень многочлена $F_{15}(x)$ равна $2^{15} - 2^3 - 2^5 + 2 = 32730$. Зная эту степень, можно найти число сомножителей в F_{15}, не выписывая сам многочлен F_{15} явно. Очевидно, что оно равно $32730/15 = 2182$. Таким образом, $N(2, 15) = 2182$ при $p = 2$. □

Теорема 8.2 исключительно важна для теории конечных полей и многочленов над конечными полями. Приведем еще один пример ее применения.

Пример 8.7. Используем двучлены $x^{p^m} - x$ для проверки неприводимости. Пусть $f = f(x) \in \mathbb{Z}_p[x]$ — многочлен, который мы хотим проверить на неприводимость, и пусть $n = \deg f$. Очевидно, что f приводим в том и только в том случае, когда он имеет неприводимый делитель $g = g(x)$ степени $r \leqslant \lfloor n/2 \rfloor$. С другой стороны, как мы убедились выше, каждый неприводимый над $\mathbb{Z}_p$ многочлен степени r является делителем двучлена $x^{p^r} - x$. Отсюда получаем простой тест (не)приводимости: многочлен f приводим, если он не взаимно прост с одним из двучленов $x^{p^r} - x$ при $1 \leqslant r \leqslant \lfloor n/2 \rfloor$. В противном случае f неприводим.

На рис. 8.1 представлена возможная реализация этого алгоритма на псевдокоде. Она использует подпрограмму `gcd` вычисления НОД двух многочленов, подпрограмму `deg`, определяющую степень многочлена, и две вспомогательные переменные — целочисленную r и переменную D типа «многочлен».

```
1. D = x ;
2. for( r = 1 ; r ⩽ ⌊n/2⌋ ; r++ ) {
3.   D = D^p (mod f) ;
4.   if( deg gcd(D − x, f) > 0 ) print «f приводим»;}
5. print «f неприводим»
```

Рис. 8.1

В обоснование ее корректности отметим, что (g, h) равен $(g \bmod h, h)$ для всех $g, h \in \mathbb{Z}_p[x]$, поэтому для сокращения вычислений переменная D на очередном шаге цикла 2—4 вместо

самого одночлена x^{p^r} содержит его остаток от деления на f. Поэтому на каждом шаге цикла происходит проверка взаимной простоты многочлена f с многочленом $x^{p^r} - x$, то есть со всеми неприводимыми многочленами степени r (и, возможно, некоторых меньших степеней, а именно остальных делителей числа r).

Оценим сложность предложенного алгоритма. Самым трудоемким является вычисление НОД в строке 4. «Школьная» реализация алгоритма Евклида требует для нахождения НОД двух многочленов степени не выше n около n^2 операций в поле их коэффициентов. При использовании эффективных алгоритмов деления многочленов и «быстрой» реализации алгоритма Евклида[1)] их число снижается до $\mathcal{O}(n \log^2 n)$. Шаги 3 и 4 будут повторены не более $\lfloor n/2 \rfloor$ раз. Таким образом, общая сложность алгоритма даже при «наивной» реализации составляет не более $\mathcal{O}(n^3)$ операций в $\mathbb{Z}_p$ и может быть снижена до $\mathcal{O}(n^2 \log^2 n)$. Для больших n это существенно лучше, чем последовательное деление $f(x)$ на все неприводимые многочлены степеней до $\lfloor n/2 \rfloor$ включительно: уже только размер таблицы неприводимых многочленов растет не медленнее, чем c^n для некоторой константы $c > 1$ (см. пример 4.17), а значит табличный способ экспоненциален. Тем не менее он удобен тем, что однажды построенную таблицу можно использовать многократно.

В заключение заметим, что данный алгоритм легко может быть улучшен: вычислять НОД в строке 4 можно не при всех r, а только начиная с $r = \lfloor n/4 \rfloor + 1$. Например, для многочлена f степени 20 достаточно проверить его взаимную простоту только с двучленами $x^{p^r} - x$ для $r = 6, 7, 8, 9, 10$, так как, например, двучлен $x^{p^5} - x$ делит $x^{p^{10}} - x$. □

Замечание 8.1. Количество неприводимых над $\mathbb{Z}_p$ многочленов степени n асимптотически равно p^n/n, как было показано в разделе 4.7. Отсюда следует, что доля неприводимых среди всех нормированных многочленов степени n примерно равна $1/n$. Это наблюдение дает простой вероятностный алгоритм построения неприводимого многочлена заданной степени n: выбрать его наугад из p^n нормированных многочленов степени n

[1)] См. [5, 9, 29, 30].

и проверить на неприводимость, используя, скажем, метод примера 8.7. Если выбранный многочлен окажется приводимым, то проверить другой случайный многочлен и т.д. Среднее число итераций при этом равно n, и поэтому данный вероятностный метод полиномиален, но в худшем случае оно может оказаться и бóльшим. Детерминированные полиномиальные алгоритмы для этой задачи появились только в 80-х годах XX века. На данный момент лучшим из них является метод Шоупа. Самый быстрый вероятностный алгоритм принадлежит ему же[1)].

Теперь сформулируем два простых, но важных свойства формальной производной многочлена над конечным полем, на которые будем опираться в дальнейшем в разделах 8.5 и 9.1.

Лемма 8.3. *Пусть $f(x) \in \mathbb{Z}_p[x]$. Тогда $f'(x) = 0$ в том и только в том случае, когда найдется такой многочлен $g(x) \in \in \mathbb{Z}_p[x]$, что $f(x) = g(x^p)$.*

Доказательство. Предположим, что $f(x) = g(x^p) = (g(x))^p$ (лемма 8.2), тогда многочлен имеет вид $f(x) = \sum_{i=0}^{n} a_i x^{pi}$, где $n = \deg g$, $a_i \in \mathbb{Z}_p$. Отсюда имеем

$$f'(x) = \sum_{i=1}^{n} a_i \cdot pi \cdot x^{pi-1} = \sum_{i=1}^{n} a_i \cdot 0 \cdot x^{pi-1} = 0,$$

так как в кольце $\mathbb{Z}_p[x]$ сумма любых p одинаковых слагаемых равна нулю.

С другой стороны, если $f(x) = \sum_{i=0}^{n} b_i x^i$ и $f'(x) = 0$, то все коэффициенты многочлена $f'(x)$ нулевые. Согласно определению производной, коэффициент при x^{i-1} в $f'(x)$ равен $i \cdot b_i$. Нетрудно убедиться, что $i \cdot b = 0$ при $i \geqslant 0$ и $b \in \mathbb{Z}_p$ тогда и только тогда, когда $i = 0 \bmod p$ или $b = 0$. Поэтому $b_i = 0$ при всех $i = 0, \ldots, n$, не кратных p. Следовательно, $f(x) = g(x^p)$ для некоторого $g(x) \in \mathbb{Z}_p[x]$. Лемма доказана.

Лемма 8.4. *Пусть $f(x) \in \mathbb{Z}_p[x]$. Тогда в разложении многочлена $f(x)$ в произведение неприводимых над $\mathbb{Z}_p$ делителей отсутствуют кратные множители тогда и только тогда, когда он взаимно прост со своей производной.*

[1)] Эти алгоритмы см. в [31] и [32].

Доказательство. В одну сторону утверждение было уже получено при доказательстве теоремы 8.2: если $(f, f') = 1$, то в разложении f отсутствуют кратные множители.

Предположим теперь, что $(f, f') \neq 1$. В этом случае существует неприводимый многочлен h, делящий одновременно и f, и f'. Поэтому $f = ah$, $f' = bh$, где $a, b \in \mathbb{Z}_p[x]$. Дифференцируя $f = ah$, получаем

$$f' = (ah)' = a'h + ah' = bh,$$

откуда следует, что h делит произведение ah'. При этом не может случиться так, что $ah' = 0$, иначе $h' = 0$ и по лемме 8.3 многочлен h является степенью некоторого другого многочлена, что противоречит его неприводимости. Кроме того, $\deg h' < \deg h$ и поэтому $h \nmid h'$. Но $h \mid ah'$, следовательно, $h \mid a$, откуда $a = \hat{a}h$ и $f = ah = \hat{a}h^2$, т. е. в разложении f присутствуют кратные множители. Лемма доказана.

8.3. Структура конечного поля

1. Характеристика поля. Сумму k одинаковых элементов x поля $\mathbb{F}$ будем обозначать через $k \cdot x$. *Характеристикой поля* $\mathbb{F}$ называется минимальное натуральное число m, для которого $m \cdot \mathbf{1} = \mathbf{0}$, а если такого числа нет, то говорят, что характеристика поля равна нулю. Характеристика любого конечного поля является простым числом. Действительно, если это не так и существует конечное поле $\mathbb{F}$ характеристики $m = ks$, то в силу дистрибутивности

$$(k \cdot \mathbf{1})(s \cdot \mathbf{1}) = (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{k \text{ единиц}})(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{s \text{ единиц}}) =$$
$$= (\underbrace{\mathbf{1} + \cdots\cdots\cdots + \mathbf{1}}_{k \times s \text{ единиц}}) = (ks) \cdot \mathbf{1} = \mathbf{0},$$

откуда следует, что в $\mathbb{F}$ есть делители нуля, что, как было показано выше (с. 91), невозможно.

Подмножество $\mathbb{F}'$ элементов поля $\mathbb{F}$ называется *подполем* поля $\mathbb{F}$, если $\mathbb{F}'$ замкнуто и является полем относительно операций

поля $\mathbb{F}$. Если $\mathbb{F}'$ — подполе поля $\mathbb{F}$, то $\mathbb{F}$ называется *расширением* поля $\mathbb{F}'$. Поле называется *простым*, если оно не имеет собственного подполя. Очевидно, что при любом простом p поле $\mathbb{Z}_p$ будет простым, и порядок любого простого поля будет простым числом. Также нетрудно видеть, что в любом конечном поле существует простое подполе, порожденное его единичным элементом, и других простых подполей в нем нет.

Пример 8.8. В рассмотренном выше поле $\mathbb{Z}_3[x]/(x^3+2x+1)$ из примера 8.1 его единица порождает поле $\mathbb{Z}_3$, которое и будет простым подполем исходного поля. □

Два поля $\mathbb{F}$ и $\mathbb{F}'$ называются *изоморфными*, если существует такое взаимно однозначное отображение φ поля $\mathbb{F}$ в поле $\mathbb{F}'$, что $\varphi(ab)=\varphi(a)\varphi(b)$ и $\varphi(a+b)=\varphi(a)+\varphi(b)$ для любых элементов a и b поля $\mathbb{F}$.

Лемма 8.5. *Пусть p — простое. Любое конечное поле $\mathbb{F}$ из p элементов изоморфно полю $\mathbb{Z}_p$.*

Доказательство. Пусть $\mathbf{1}$ — единица поля $\mathbb{F}$. Любой элемент поля $\mathbb{F}$ можно представить в виде $k\mathbf{1}$ — суммы k единиц этого поля. Очевидно, что $n\mathbf{1}=[n]_p\mathbf{1}$ при любом n из $\mathbb{N}$. Тогда для отображения φ из $\mathbb{F}$ в $\mathbb{Z}_p$, заданного равенством $\varphi(n\mathbf{1})=n$, и для любых k и m из $\{0,1,\ldots,p-1\}$ справедливо равенство

$$\begin{aligned}\varphi(k\mathbf{1}+m\mathbf{1}) &= \varphi((k+m)\mathbf{1}) = \varphi([k+m]_p\mathbf{1}) = \\ &= [k+m]_p = [k]_p+[m]_p = \varphi(k\mathbf{1})+\varphi(m\mathbf{1}).\end{aligned}$$

Аналогичное равенство имеет место для умножения:

$$\begin{aligned}\varphi(k\mathbf{1}\cdot m\mathbf{1}) &= \varphi((k\cdot m)\mathbf{1}) = \varphi([k\cdot m]_p\mathbf{1}) = \\ &= [k\cdot m]_p = [k]_p\cdot[m]_p = \varphi(k\mathbf{1})\cdot\varphi(m\mathbf{1}).\end{aligned}$$

Следовательно, φ — изоморфизм. Лемма доказана.

2. Корни неприводимых многочленов. Далее будем вычислять значения многочленов из $\mathbb{Z}_p[x]$ на элементах полей характеристики p, рассматривая одночлены ax^k, где $a\in\mathbb{Z}_p$, как сумму a одночленов x^k. В свете леммы 8.5 будем также отождествлять простые подполя полей характеристики p с полем $\mathbb{Z}_p$.

Теорема 8.3. *Любое конечное поле $\mathbb{F}$ характеристики p состоит из p^n элементов, где n — целое неотрицательное, и*

$$x^{p^n} - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha). \tag{8.12}$$

Доказательство. В поле $\mathbb{F}$ характеристики p существует простое подполе $\mathbb{F}'$ из p элементов, порожденное единичным элементом. Легко проверить, что поле $\mathbb{F}$ будет линейным конечномерным пространством над своим простым подполем $\mathbb{F}'$, и поэтому число элементов в поле $\mathbb{F}$ будет натуральной степенью числа элементов в его простом подполе $\mathbb{F}'$.

Теперь равенство (8.12) легко следует из единственности разложения многочлена над полем на множители, леммы 4.5 и того, что каждый ненулевой элемент поля $\mathbb{F}$ в степени, равной порядку мультипликативной группы, равен единице, т. е. является корнем двучлена $x^{p^n-1} - 1$. Теорема доказана.

Пример 8.9. Поле $\mathbb{F}$ из примера 8.1 является трехмерным линейным пространством над полем $\mathbb{Z}_3$. Его элементы $1 = (001), x = (010)$ и $x^2 = (100)$ образуют базис. Каждый элемент из $\mathbb{F}$ является простым корнем двучлена $x^{27} - x$, а каждый элемент из $\mathbb{F}^*$ — корнем $x^{26} - 1$. □

Теорема 8.4. *В любом поле $\mathbb{F}$ из p^n элементов каждый элемент поля является простым корнем неприводимого над $\mathbb{Z}_p$ многочлена, степень которого делит n.*

Доказательство. Каждый элемент поля $\mathbb{F}$ является корнем двучлена $x^{p^n} - x$, который в силу теоремы 8.2 разлагается в произведение всех нормированных неприводимых над $\mathbb{Z}_p$ многочленов, степени которых делят n. Так как $x^{p^n} - x$ не имеет кратных множителей, то каждый элемент поля $\mathbb{F}$ будет простым корнем одного из этих неприводимых над $\mathbb{Z}_p$ многочленов. Теорема доказана.

Пример 8.10. Рассмотрим произвольное поле $\mathbb{F}$ из 27 элементов. По крайней мере одно такое поле характеристики 3 существует, оно было рассмотрено в примере 8.1. В $\mathbb{F}$ найдутся изоморфное $\mathbb{Z}_3$ простое подполе $\mathbb{F}'$ и элемент α — корень неприводимого над $\mathbb{Z}_3$ многочлена $x^3 + 2x + 1$. Поле $\mathbb{F}$ будет трехмерным

линейным пространством над подполем $\mathbb{F}'$, элементы которого можно обозначить $0, 1, 2$. Здесь 0 и 1 являются нейтральными по сложению и умножению элементами в $\mathbb{F}'$, а значит, и в $\mathbb{F}$; элемент $2 = 1 + 1$ является третьим в простом подполе. Так как $\alpha^3 = \alpha + 2$, то, повторяя вычисления примера 8.1, находим все степени α (ниже выписаны наборы коэффициентов (a, b, c) линейных комбинаций $a\alpha^2 + b\alpha + c$ над полем $\mathbb{F}'$, представляющих элементы $\alpha^k \in \mathbb{F}^*$):

$$\begin{array}{llll}
\alpha^0 = (001), & \alpha^7 = (122), & \alpha^{14} = (020), & \alpha^{21} = (101), \\
\alpha^1 = (010), & \alpha^8 = (202), & \alpha^{15} = (200), & \alpha^{22} = (022), \\
\alpha^2 = (100), & \alpha^9 = (011), & \alpha^{16} = (021), & \alpha^{23} = (220), \\
\alpha^3 = (012), & \alpha^{10} = (110), & \alpha^{17} = (210), & \alpha^{24} = (221), \\
\alpha^4 = (120), & \alpha^{11} = (112), & \alpha^{18} = (121), & \alpha^{25} = (201). \\
\alpha^5 = (212), & \alpha^{12} = (102), & \alpha^{19} = (222), & \\
\alpha^6 = (111), & \alpha^{13} = (002), & \alpha^{20} = (211), &
\end{array} \tag{8.13}$$

Из этой таблицы нетрудно видеть, что элементы α^2, α и 1 образуют базис пространства $\mathbb{F}$ над $\mathbb{F}'$, и каждый элемент поля $\mathbb{F}$ можно однозначно представить набором координат в этом базисе. Сравнивая таблицы (8.13) и (8.1), несложно показать, что $\mathbb{F}$ — произвольное поле из 27 элементов, — изоморфно полю $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$. Это не случайный факт, а частный случай общей ситуации, рассматриваемой ниже в теореме 8.8. □

Теорема 8.5. *Пусть поле $\mathbb{F}$ состоит из p^n элементов, а его элемент α — корень неприводимого над $\mathbb{Z}_p$ многочлена степени n. Тогда любой элемент поля $\mathbb{F}$ единственным образом представляется линейной комбинацией элементов $1, \alpha, \ldots, \alpha^{n-1}$ с коэффициентами из его простого подполя.*

Доказательство. Прежде всего заметим, что существует ровно p^n различных линейных комбинаций из элементов $1, \alpha, \ldots, \alpha^{n-1}$ с коэффициентами из простого подполя, и каждая линейная комбинация является элементом поля $\mathbb{F}$. Более того, среди этих линейных комбинаций нет двух, равных одному и тому же

элементу поля $\mathbb{F}$, так как в противном случае разность двух равных линейных комбинаций будет ненулевой линейной комбинацией, равной нулевому элементу поля. Нетрудно показать, что существование такой линейной комбинации равносильно тому, что α будет корнем многочлена степени не больше $n-1$, что, очевидно, противоречит тому, что α является корнем неприводимого многочлена степени n. Теорема доказана.

Теорема 8.5 показывает, что поле $\mathbb{F}$ из p^n элементов с простым подполем $\mathbb{F}_p$ можно представить как множество многочленов $\mathbb{F}_p[\alpha]$, где α — корень неприводимого над $\mathbb{Z}_p$ многочлена $h(x)$ степени n, со сложением и умножением по модулю многочлена $h(\alpha)$.

Пример 8.11. Построим поле $\mathbb{Z}_2[\alpha]$ из 16 элементов, добавив к полю $\mathbb{Z}_2$ корень α неприводимого над $\mathbb{Z}_2$ многочлена x^4+x+1 и все те элементы, которые можно получить из 0, 1 и α при помощи операций сложения и умножения. Легко видеть, что $\mathbb{Z}_2[\alpha]$ состоит из различных многочленов f от α с коэффициентами из $\mathbb{Z}_2$. А так как $\alpha^4 = \alpha+1$, то каждая степень α большая трех будет линейной комбинацией первых четырех степеней. Таким образом, $\mathbb{Z}_2[\alpha]$ содержит ровно 16 элементов и является линейным пространством над $\mathbb{Z}_2$, порожденным элементами $\alpha^3, \alpha^2, \alpha, 1$. Если произведение $f(\alpha)\cdot g(\alpha)$ разделить с остатком на $\alpha^4+\alpha+1$, то

$$f(\alpha)\cdot g(\alpha) = (\alpha^4+\alpha+1)\cdot q(\alpha) + r(\alpha) = r(\alpha)$$

для любых $f(\alpha)$ и $g(\alpha)$. Поэтому умножение в $\mathbb{Z}_2[\alpha]$ определим как умножение многочленов по модулю многочлена $\alpha^4+\alpha+1$.

Про поле $\mathbb{Z}_2[\alpha]$ будем говорить, что оно получено *расширением* поля $\mathbb{Z}_2$ элементом α. Покажем, что $\mathbb{Z}_2[\alpha]$ действительно будет полем. Для этого проверим единственное нетривиальное в данном случае свойство поля — установим существование обратного по умножению для каждого ненулевого элемента $f(\alpha)$. Так как $\alpha^4+\alpha+1$ и $f(\alpha)$ взаимно простые, то в силу теоремы 4.10 найдутся такие многочлены $s(\alpha)$ и $t(\alpha)$, что $1 = s(\alpha)(\alpha^4+\alpha+1) + t(\alpha)f(\alpha)$, причем степени $s(\alpha)$ и $t(\alpha)$ не превосходят трех (если это не так, то вместо многочленов $s(\alpha)$ и

$t(\alpha)$ можно взять их остатки от деления на $\alpha^4+\alpha+1$). Поэтому

$$t(\alpha)f(\alpha) = 1 + s(\alpha)(\alpha^4+\alpha+1) = 1 + s(\alpha)\cdot 0 = 1,$$

и $t(\alpha)$ будет обратным элементом по умножению для $f(\alpha)$. Таким образом, $\mathbb{Z}_2[\alpha]$ — поле из 16 элементов.

Так как $\alpha^3 \neq 1$ и $\alpha^5 = \alpha^2+\alpha \neq 1$, то α будет порождающим элементом мультипликативной группы поля. Представляя элементы поля $\mathbb{Z}_2[\alpha]$ наборами их коэффициентов в базисе $(\alpha^3, \alpha^2, \alpha, 1)$, видим, что степени α в этом поле выглядят следующим образом:

$$\begin{array}{lll}
\alpha^0 = (0001), & \alpha^5 = (0110), & \alpha^{10} = (0111),\\
\alpha^1 = (0010), & \alpha^6 = (1100), & \alpha^{11} = (1110),\\
\alpha^2 = (0100), & \alpha^7 = (1011), & \alpha^{12} = (1111),\\
\alpha^3 = (1000), & \alpha^8 = (0101), & \alpha^{13} = (1101),\\
\alpha^4 = (0011), & \alpha^9 = (1010), & \alpha^{14} = (1001).
\end{array} \qquad (8.14)$$

□

Теорема 8.6. *В любом поле $\mathbb{F}$ из p^n элементов для любого m, являющегося делителем n, существует единственное подполе из p^m элементов. Других подполей в поле $\mathbb{F}$ нет.*

Доказательство. Если $\mathbb{F}'$ — подполе поля $\mathbb{F}$, то $\mathbb{F}$ будет линейным пространством над своим подполем $\mathbb{F}'$. В этом случае найдется натуральное k такое, что $p^n = |\mathbb{F}'|^k$. Очевидно, что последнее равенство возможно только в том случае, когда $n = km$.

Теперь покажем, что если m делит n, то в $\mathbb{F}$ существует подполе из p^m элементов. Рассмотрим множество N элементов поля $\mathbb{F}$, являющихся корнями всех неприводимых многочленов, степени которых равны m или делят m. Из теоремы 8.4 следует, что каждый из этих элементов является корнем двучлена $x^{p^m} - x$. Покажем, что сумма и произведение любых двух элементов из N также принадлежат этому множеству. Если $a^{p^m} - a = 0$ и $b^{p^m} - b = 0$, то в силу равенства (8.6), справедливого, очевидно,

в любом поле характеристики p,

$$(a+b)^{p^m} - (a+b) = (a^{p^m} + b^{p^m}) - (a+b) = \\ = (a^{p^m} - a) + (b^{p^m} - b) = 0,$$

т. е. сумма $a+b$ принадлежит N. Аналогичная цепочка равенств имеет место и для произведения ab:

$$(ab)^{p^m} - ab = a^{p^m} b^{p^m} - ab = ab - ab = 0.$$

Таким образом множество N замкнуто относительно сложения и умножения. Также нетрудно видеть, что если a является корнем двучлена $x^{p^m} - x$, то и его обратные элементы по сложению и умножению будут корнями этого двучлена. Следовательно, N является полем.

Наконец заметим, что мультипликативная группа подполя будет подгруппой мультипликативной группы поля. Поэтому единственность подполя из p^m элементов в поле из p^n элементов легко следует из теоремы 3.13. Теорема доказана.

Пример 8.12. В поле $\mathbb{Z}_2[\alpha]$ из предыдущего примера есть два нетривиальных подполя — простое подполе $\mathbb{Z}_2$ и подполе из четырех элементов, состоящее из нуля, единицы и элементов α^5 и α^{10}. Из таблицы 8.14 степеней α видно, что ненулевые элементы второго подполя связаны равенством $\alpha^{10} + \alpha^5 = 1$. □

3. Изоморфные поля. Пусть α — произвольный элемент поля из p^n элементов. Элементы $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{k-1}}$, где $\alpha^{p^k} = \alpha$, называются *сопряженными* с α. Так как в поле из p^n элементов $\alpha^{p^n} = \alpha$, то α имеет не более $n-1$ сопряженных элементов.

Теорема 8.7. *Если α — корень неприводимого над $\mathbb{Z}_p$ многочлена $h(x)$ степени k, то корнями этого многочлена являются все элементы, сопряженные с α, и других корней многочлен $h(x)$ не имеет.*

Доказательство. Так как $(h(x))^p = h(x^p)$, то очевидно, что любой элемент, сопряженный с α, будет корнем многочлена $h(x)$. Поэтому для доказательства теоремы достаточно показать, что все элементы $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{k-1}}$ различны. Допустим, что это

не так и $\alpha^{p^m} = \alpha$ при $m < k$. Тогда α будет корнем многочлена $x^{p^m} - x$ и, в силу теоремы 8.2, будет также корнем неприводимого многочлена $g(x)$ степени t, где t является делителем m. Разделив неприводимый многочлен $h(x)$ на $g(x)$, получим, что $h(x) = g(x)f(x) + r(x)$, где $r(x) \neq 0$ и $\deg r(x) < t \leqslant m < k$. Так как $h(\alpha) = 0$ и $g(\alpha) = 0$, то очевидно, что и $r(\alpha) = 0$. Вместе с α корнями многочлена $r(x)$ должны быть и все элементы, сопряженные с α, т. е. число корней многочлена $r(x)$ не меньше m, что, очевидно, невозможно, так как его степень строго меньше m. Таким образом, сделанное предположение ложно и $m = k$. Теорема доказана.

Пусть $\mathbb{F}$ — поле из p^n элементов, α — элемент этого поля. Нормированный многочлен $f(x)$ из $\mathbb{Z}_p[x]$ называется *минимальным многочленом* элемента α, если $f(\alpha) = 0$ и степень многочлена f минимальна среди всех многочленов положительной степени из $\mathbb{Z}_p[x]$, для которых α является корнем. Из леммы 8.2 и доказательства теоремы 8.5 легко следует, что для любого α существует единственный минимальный многочлен, этот многочлен является неприводимым над $\mathbb{Z}_p[x]$, и его корнями в $\mathbb{F}$ являются вместе с α все элементы, сопряженные с α. Минимальный многочлен элемента α обозначается $m_\alpha(x)$.

Пример 8.13. Найдем минимальный многочлен элемента (212) поля $\mathbb{F}$ из примера 8.10. Так как элемент (212) является пятой степенью примитивного элемента α, то с (212) $= \alpha^5$ будут сопряжены два элемента $(\alpha^5)^3 = \alpha^{15}$ и $(\alpha^5)^9 = \alpha^{45} = \alpha^{19}$. Поэтому

$$m_{(212)}(x) = (x - \alpha^5)(x - \alpha^{15})(x - \alpha^{19}).$$

Раскрывая скобки и приводя подобные слагаемые при помощи таблицы (8.13), находим минимальный многочлен:

$$\begin{aligned} m_{(212)}(x) &= (x - \alpha^5)(x - \alpha^{15})(x - \alpha^{19}) = \\ &= x^3 - (\alpha^5 + \alpha^{15} + \alpha^{19})x^2 + (\alpha^{20} + \alpha^{24} + \alpha^8)x - \alpha^{13} = \\ &= x^3 - x^2 + x - 2 = x^3 + 2x^2 + x + 1. \quad \square \end{aligned}$$

Пример 8.14. Покажем, что мультипликативные порядки всех корней неприводимого многочлена совпадают.

Действительно, согласно теореме 8.7, все корни неприводимого многочлена $f(x) \in \mathbb{Z}_p[x]$ сопряжены. В частности, если β, γ — корни $f(x)$ в поле $\mathbb{F}_{p^n}$, то найдется такое целое k, что $\gamma = \beta^{p^k}$. В циклической группе $\langle\beta\rangle$, образованной элементом β, порядок элемента β^{p^k} равен $|\beta|/(|\beta|, p^k)$, где $|\beta|$ — порядок элемента β. Одновременно порядки элементов β и β^{p^k} должны быть делителями порядка p^n-1 мультипликативной группы $\mathbb{F}^*_{p^n}$. Но любой делитель числа p^n-1 взаимно прост с числом p^k. Поэтому $(|\beta|, p^k) = 1$ и $|\beta^{p^k}| = |\beta|$. □

Теорема 8.8. *Любые два конечных поля, состоящие из одного и того же числа элементов, изоморфны.*

Доказательство. Пусть p — простое, $h(x)$ — нормированный неприводимый над $\mathbb{Z}_p$ многочлен степени n из $\mathbb{Z}_p[x]$. Покажем, что произвольное поле из p^n элементов изоморфно полю $\mathbb{Z}_p[x]/h(x)$.

В силу леммы 8.5 далее без ограничения общности будем полагать, что простое подполе поля $\mathbb{F}$ совпадает с полем $\mathbb{Z}_p$. В поле $\mathbb{F}$ выберем элемент α, являющийся корнем многочлена $h(x)$. Покажем, что отображение

$$\varphi : \sum_{i=0}^{n-1} a_i\alpha^i \to \sum_{i=0}^{n-1} a_i x^i$$

поля $\mathbb{F}$ в поле $\mathbb{Z}_p[x]/h(x)$ будет искомым изоморфизмом. Очевидно, что φ взаимнооднозначно, линейно и в силу своей линейности сохраняет операцию сложения. Поэтому для доказательства теоремы достаточно показать, что φ сохраняет умножение. Каждый элемент $a = \sum_{i=0}^{n-1} a_i\alpha^i$ поля $\mathbb{F}$ будем рассматривать как многочлен $a(\alpha)$ относительно α. В силу законов дистрибутивности умножение элементов $a = \sum_{i=0}^{n-1} a_i\alpha^i$ и $b = \sum_{i=0}^{n-1} b_i\alpha^i$ поля $\mathbb{F}$ производится так же, как и умножение многочленов. Поэтому справедливо равенство

$$ab = a(\alpha)b(\alpha) = c(\alpha)h(\alpha) + r(\alpha),$$

где $r(\alpha)$ — остаток от деления многочлена $a(\alpha)b(\alpha)$ на многочлен $h(\alpha)$. Так как $h(\alpha)=0$, то $ab=r(\alpha)$. Поэтому

$$\varphi(a(\alpha))\varphi(b(\alpha))=a(x)b(x)=r(x)=\varphi(r(\alpha)),$$

т. е. φ действительно сохраняет умножение. Теорема доказана.

Конечные поля, отличные от полей $\mathbb{Z}_p$, впервые появились в работе французского математика Эвариста Галуа в 1830 г. в виде множества корней двучлена $x^{p^n}-x$. Сейчас любое конечное поле называется полем Галуа, и для поля из p^n элементов часто используется единое обозначение $GF(p^n)$.

4. Примитивные многочлены. Многочлен $h(x)$ из $\mathbb{Z}_p[x]$ называется *примитивным многочленом*, если он является минимальным многочленом примитивного элемента поля из p^n элементов. Из примера 8.14 следует примитивность всех корней примитивного многочлена. Поэтому в силу теорем 8.7 и 3.14 справедливо следующее утверждение.

Теорема 8.9. *В кольце $\mathbb{Z}_p[x]$, где p — простое, существует ровно $\varphi(p^n-1)/n$ примитивных многочленов степени n.*

Пример 8.15. Так как $\varphi(15)=8$, то в $\mathbb{Z}_2[x]$ существует ровно два примитивных многочлена четвертой степени. В то же время из теоремы 4.13 следует существование в $\mathbb{Z}_2[x]$ трех неприводимых многочленов четвертой степени. Таким образом, один из этих трех неприводимых многочленов не является примитивным. Найдем такой многочлен. Для этого воспользуемся полем $\mathbb{Z}_2[\alpha]$ из примера 8.11, где α — корень неприводимого многочлена x^4+x+1. Среди 15 ненулевых элементов поля $\mathbb{Z}_2[\alpha]$ непримитивными будут следующие степени α: $0,3,5,6,9,10,12$. Из этих степеней 5-я и 10-я будут корнями единственного неприводимого многочлена второй степени x^2+x+1, а нулевая степень — корнем $x+1$. Следовательно, четыре оставшиеся степени $3,6,9,12$ — корни искомого многочлена

$$f(x)=x^4+f_3x^3+f_2x^2+f_1x+f_0. \tag{8.15}$$

Подставив в (8.15) вместо переменной x его корни $\alpha^3, \alpha^6, \alpha^9$ и α^{12}, получим систему из четырех линейных уравнений с четырьмя неизвестными:

$$\left.\begin{aligned}
(\alpha^3)^4 + f_3\,(\alpha^3)^3 + f_2\,(\alpha^3)^2 + f_1\,(\alpha^3) + f_0 = 0,\\
(\alpha^6)^4 + f_3\,(\alpha^6)^3 + f_2\,(\alpha^6)^2 + f_1\,(\alpha^6) + f_0 = 0,\\
(\alpha^9)^4 + f_3\,(\alpha^9)^3 + f_2\,(\alpha^9)^2 + f_1\,(\alpha^9) + f_0 = 0,\\
(\alpha^{12})^4 + f_3(\alpha^{12})^3 + f_2(\alpha^{12})^2 + f_1(\alpha^{12}) + f_0 = 0.
\end{aligned}\right\} \qquad (8.16)$$

Так как многочлен $f(x)$ неприводим над $\mathbb{Z}_2$, то его свободный член равен единице. Поэтому в (8.16) вместо f_0 подставим единицу, после чего из системы удалим последнее уравнение — для нахождения трех оставшихся коэффициентов достаточно трех уравнений. В результате получим (учитывая, что $1 = -1$ в поле $\mathbb{Z}_2$) новую систему

$$\left.\begin{aligned}
f_3\,\alpha^9 + f_2\,\alpha^6 + f_1\,\alpha^3 = 1 + \alpha^{12} = \alpha^{11},\\
f_3\,\alpha^3 + f_2\,\alpha^{12} + f_1\,\alpha^6 = 1 + \alpha^9 = \alpha^7,\\
f_3\,\alpha^{12} + f_2\,\alpha^3 + f_1\,\alpha^9 = 1 + \alpha^6 = \alpha^{13}.
\end{aligned}\right\}$$

Для решения последней системы воспользуемся формулами Крамера. Вычислив необходимые для этого определители

$$\det\begin{pmatrix} \alpha^9 & \alpha^6 & \alpha^3 \\ \alpha^3 & \alpha^{12} & \alpha^6 \\ \alpha^{12} & \alpha^3 & \alpha^9 \end{pmatrix} = \det\begin{pmatrix} \alpha^{11} & \alpha^6 & \alpha^3 \\ \alpha^7 & \alpha^{12} & \alpha^6 \\ \alpha^3 & \alpha^3 & \alpha^9 \end{pmatrix} =$$

$$= \det\begin{pmatrix} \alpha^9 & \alpha^{11} & \alpha^3 \\ \alpha^3 & \alpha^7 & \alpha^6 \\ \alpha^{12} & \alpha^3 & \alpha^9 \end{pmatrix} = \det\begin{pmatrix} \alpha^9 & \alpha^6 & \alpha^{11} \\ \alpha^3 & \alpha^{12} & \alpha^7 \\ \alpha^{12} & \alpha^3 & \alpha^3 \end{pmatrix} = \alpha^{11}$$

и подставив найденные значения в (6.10), видим, что все коэффициенты искомого многочлена равны единице. Таким образом, $f(x) = x^4 + x^3 + x^2 + x + 1$. □

5. Нормальный базис. Покажем, что в поле $GF(p^n)$ найдется такой элемент α, что все элементы $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$, сопряженные с ним, образуют базис поля $GF(p^n)$, рассматриваемого как линейное пространство $\mathbb{F}^n$ над его простым подполем $\mathbb{F}$. Такой базис называется *нормальным* базисом поля.

Теорема 8.10. *В поле $GF(p^n)$ существует нормальный базис.*

Доказательство. В пространстве $\mathbb{F}^n$ рассмотрим линейный оператор $\mathcal{A} : \alpha \to \alpha^p$, линейность которого является простым следствием справедливых для любых α, β из $\mathbb{F}^n$ и любого a из $\mathbb{F}$ равенств

$$\mathcal{A}(\alpha + \beta) = \mathcal{A}(\alpha) + \mathcal{A}(\beta),$$
$$\mathcal{A}(a\alpha) = a\mathcal{A}(\alpha),$$

которые в свою очередь легко следуют из леммы 8.2.

Заметим, что $\mathcal{A}^n(\alpha) = \alpha^{p^n} = \alpha$. Поэтому $(x^n - 1)(\mathcal{A})(\alpha) = 0$ для каждого α. Таким образом, двучлен $x^n - 1$ является аннулятором каждого элемента из $\mathbb{F}^n$, а следовательно, и всего пространства $\mathbb{F}^n$ с действующим на нем оператором $\mathcal{A}$. Если окажется, что $x^n - 1$ не только аннулятор, но еще и минимальный многочлен n-мерного пространства $\mathbb{F}^n$, то в силу теоремы 6.9 это пространство будет циклическим, т. е. в нем найдется базис

$$\alpha, \mathcal{A}(\alpha), \mathcal{A}^2(\alpha), \ldots, \mathcal{A}^{n-1}(\alpha), \tag{8.17}$$

порождаемый некоторым вектором α. Так как $\mathcal{A}^k(\alpha) = \alpha^{p^k}$, то базис (8.17) будет нормальным базисом поля $GF(p^n)$.

Таким образом, для доказательства теоремы достаточно установить, что двучлен $x^n - 1$ будет минимальным многочленом пространства $\mathbb{F}^n$. В свою очередь $x^n - 1$ будет минимальным многочленом, если для любого многочлена $a(x) = a_0 + a_1 x + \\ + \cdots + a_{n-1}x^{n-1}$ меньшей степени в поле $GF(p^n)$ найдется такой элемент α, что

$$a(x)(\mathcal{A})(\alpha) = a_0\alpha + a_1\alpha^p + \cdots + a_{n-1}\alpha^{p^{n-1}} \neq 0. \tag{8.18}$$

Допустим, что это не так, и в поле $GF(p)$ найдутся такие одновременно не равные нулю $b_0, \ldots, b_{n-1}$, что

$$b_0\beta + b_1\beta^p + \cdots + b_{n-1}\beta^{p^{n-1}} = 0 \quad \text{для каждого } \beta \in GF(p^n). \tag{8.19}$$

Пусть α_0 — порождающий элемент мультипликативной группы поля $GF(p^n)$. Из предположения (8.19) следует, что равенство

$$\begin{aligned} 0 &= b_0\alpha_0^k + b_1(\alpha_0^k)^p + \cdots + b_{n-1}(\alpha_0^k)^{p^{n-1}} = \\ &= b_0\alpha_0^k + b_1(\alpha_0^p)^k + \cdots + b_{n-1}(\alpha_0^{p^{n-1}})^k \end{aligned} \tag{8.20}$$

справедливо при $k = 0, 1, \ldots, n-1$. Переписывая равенства (8.20) в матричной форме, видим, что они эквивалентны равенству

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_0^p & \ldots & \alpha_0^{p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{n-1} & (\alpha_0^p)^{n-1} & \ldots & (\alpha_0^{p^{n-1}})^{n-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{8.21}$$

с матрицей Вандермонда. Так как $\alpha_0^{p^i} \neq \alpha_0^{p^j}$ при $0 \leqslant i \neq j \leqslant n-1$, то в силу леммы 5.5 матрица Вандермонда невырождена, и, следовательно, (8.21) справедливо только если все $b_i = 0$. Полученное противоречие гарантирует, что в поле $GF(p^n)$ для любого многочлена, степень которого меньше n, найдется элемент α, удовлетворяющий неравенству (8.18). Следовательно, $x^n - 1$ будет минимальным многочленом $\mathbb{F}^n$. Теорема доказана.

Пример 8.16. Пусть $\mathbb{F}$ — рассмотренное в примере 8.10 на с. 267 поле из 27 элементов с примитивным элементом α. Так как

$$\begin{aligned} \alpha^1 &= (\texttt{010}), \qquad \alpha^3 = (\texttt{012}), \qquad \alpha^9 = (\texttt{011}), \\ \alpha^2 &= (\texttt{100}), \qquad \alpha^6 = (\texttt{111}), \qquad \alpha^{18} = (\texttt{121}), \end{aligned}$$

то легко видеть, что элементы $\alpha, \alpha^3, \alpha^{3^2}$ не образуют нормальный базис в $\mathbb{F}$, в то время как элементы $\alpha^2, (\alpha^2)^3, (\alpha^2)^{3^2}$ такой базис образуют. □

8.4. Арифметика в конечных полях

В практических приложениях теории конечных полей приходится производить вычисления в конкретном поле, обычно представленном как поле вычетов по какому-либо модулю. Первые

примеры данного раздела посвящены развитию навыков подобных вычислений в простейших случаях и могут быть без ущерба пропущены подготовленным читателем. Еще несколько примеров иллюстрируют полученные в предыдущих разделах общие свойства полей и многочленов над ними, которые часто помогают такие вычисления значительно упростить.

Разберем сначала вопросы о примитивных многочленах и примитивных элементах в полях-расширениях.

Пример 8.17. Неприводимый над $\mathbb{Z}_3$ многочлен

$$f(x) = x(x+1)(x+2) + 1 = x^3 + 2x + 1$$

из примера 4.18 является примитивным, и, как показывает пример 8.1 и замечание 4.2, любой ненулевой элемент поля $\mathbb{F}_{27} = \mathbb{Z}_3[x]/f(x)$ представляется степенью вычета $\alpha = x$ (порядок которого в группе $\mathbb{F}_{27}^*$ равен 26) и α — корень многочлена $f(x)$. Полученная при этом таблица, сопоставляющая каждому ненулевому вычету его логарифм по «основанию» α, называется *таблицей дискретных логарифмов* поля $\mathbb{Z}_3[x]/f(x)$.

Отметим, что для доказательства примитивности элемента $\alpha = x$ и, как следствие, многочлена $f(x)$, не обязательно было строить всю таблицу целиком: по лемме 8.1 достаточно было лишь проверить, что $x^2 \neq 1 \pmod f$ и что $x^{13} \neq 1 \pmod f$. Первое из этих неравенств очевидно. Второе можно проверить, например, поделив x^{13} на $f(x)$ в столбик: $x^{13} = 2 \pmod f$. □

Корень многочлена большой степени имеет, вообще говоря, большой порядок. В таком случае деление в столбик или составление таблицы логарифмов слишком громоздки и значительно проще произвести несколько приведений по модулю, как в примере 8.3.

Пример 8.18. Покажем, что многочлен $f(x) = x^9 + x^4 + 1$ примитивен над $\mathbb{Z}_2$. Он неприводим (см. пример 4.15 на с. 114). Также это следует из его взаимной простоты с двучленами $x^{2^3} - x$ и $x^{2^4} - x$ (пример 8.7), в чем нетрудно убедиться непосредственно. Так как $2^9 - 1 = 511 = 7 \cdot 73$, где 7 и 73 — простые числа, и очевидно $x^7 \neq 1 \pmod f$, то достаточно проверить, что $x^{73} \neq 1$

(mod f). Вычислим остаток x^{73}:

$$\begin{aligned}
x^{73} &= \left(x^9\right)^8 \cdot x = \left(x^4+1\right)^8 \cdot x = \left(x^{16}+1\right)^4 \cdot x = \\
&= \left(x^9 \cdot x^7 + 1\right)^4 \cdot x = \left((x^4+1)\cdot x^7 + 1\right)^4 \cdot x = \\
&= \left(x^{11}+x^7+1\right)^4 \cdot x = \left(x^7+x^6+x^2+1\right)^4 \cdot x = \\
&= \left(x^{14}+x^{12}+x^4+1\right)^2 \cdot x = \\
&= \left(x^5(x^4+1)+x^3(x^4+1)+x^4+1\right)^2 \cdot x = \\
&= \left(x^9+x^5+x^7+x^3+x^4+1\right)^2 \cdot x = \\
&= \left(x^4+1+x^5+x^7+x^3+x^4+1\right)^2 \cdot x = \\
&= \left(x^7+x^5+x^3\right)^2 \cdot x = \left(x^{14}+x^{10}+x^6\right) \cdot x = \\
&= \left(x^5(x^4+1)+(x^5+x)+x^6\right) \cdot x = \\
&= \left(x^6+x^4+x+1\right) \cdot x = \\
&= x^7+x^5+x^2+x \neq 1 \pmod{(x^9+x^4+1)}.
\end{aligned}$$

Здесь мы неоднократно воспользовались тем, что $x^9 = x^4+1$ (mod f), а также леммой 8.2. Таким образом, многочлен f примитивен. □

Пример 8.18 наглядно показывает, что число битовых операций (в общем случае операций в поле коэффициентов) по модулю многочлена f пропорционально числу его ненулевых коэффициентов. Поэтому с точки зрения сложности вычислений в поле остатков по модулю f выгоднее тот многочлен, у которого больше нулевых членов. Таблицы таких многочленов составлены для весьма значительных степеней и могут быть найдены в специальной литературе.

Перейдем теперь к арифметическим операциям в полях-расширениях.

Пример 8.19. Найдем обратный к вычету $g(x) = x^7 + x^6 + x^3 + x + 1$ по модулю многочлена $f(x) = x^9 + x^4 + 1 \in \mathbb{Z}_2[x]$. Мы уже доказали примитивность многочлена $f(x)$ в примере 8.18, следовательно, вычет $g(x) \neq 0$ обратим по модулю $f(x)$. Чтобы найти g^{-1} (mod f), воспользуемся расширенным алгоритмом Евклида из леммы 4.6 (ниже многочлены представлены в

векторной записи, а таблица алгоритма, приведенная в конце примера, транспонирована). В этой таблице первые два столбца отведены под коэффициенты Безу, третий — столбец остатков, четвертый — неполные частные очередного шага. На последнем шаге получаем, что

$$(1101011)\cdot f+(100100110)\cdot g=(1),$$

или, в алгебраической форме,

$$(x^6+x^5+x^3+x+1)\cdot f+(x^8+x^5+x^2+x)\cdot g=1.$$

Рассмотрев остатки от деления на f обеих частей этого равенства, находим, что $(x^8+x^5+x^2+x)\cdot g=1 \pmod f$, то есть $g^{-1}(x)=x^8+x^5+x^2+x \pmod{f(x)}$.

1	0	1000010001	
0	1	11001011	111
1	111	1100000	10
10	1111	1011	1110
11101	1011101	10	101
1101011	100100110	1	

Аналогично находятся обратные и к другим элементам рассматриваемого поля $\mathbb{Z}_2[x]/f(x)$. □

В случае, когда поле $\mathbb{Z}_p[x]/f(x)$ относительно небольшое, а количество вычислений с его элементами велико, операции по модулю многочлена f удобно осуществлять не непосредственно, как в предыдущем примере, а сводить их к поиску по вспомогательной таблице. Таблица Кэли для этих целей подходит плохо, так как ее размер, равный квадрату порядка группы, требует относительно большого объема памяти. Компромиссным решением является таблица логарифмов (или ее часть), построенная на основе свойства цикличности мультипликативной группы $(\mathbb{Z}_p[x]/f)^*$ и имеющая линейный, относительно ее порядка, размер. Проиллюстрируем этот подход несколькими примерами.

Пример 8.20. Построим таблицу дискретных логарифмов поля $\mathbb{F}_8 = \mathbb{Z}_2[x]/(x^3 + x + 1)$.

Многочлен $f(x) = x^3 + x + 1$ неприводим над $\mathbb{Z}_2$ (см. с. 113). Поэтому группа $\mathbb{F}_8^* = (\mathbb{Z}_2[x]/f)^*$ — циклическая, то есть существует такой вычет $\alpha \in \mathbb{F}_8^*$, что $\mathbb{F}_8^* = \langle\alpha\rangle_7$. В силу того что $|\mathbb{F}_8^*| = 7$ — простое число, многочлен $f(x)$ примитивен. Поэтому для удобства будем считать, что α является его корнем x в $\mathbb{F}_8$, хотя в $\mathbb{F}_8$ есть и другие примитивные элементы. Каждый элемент β нашего поля имеет как минимум три представления — он является вычетом по модулю f, вектором линейного векторного пространства $\mathbb{F}_8$ размерности 3 над простым подполем $\mathbb{Z}_2$, и, наконец, если $\beta \neq 0$, то он является некоторой степенью элемента α: существует такое число $k = \log_\alpha \beta$, $0 \leqslant k \leqslant 6$, что $\beta = \alpha^k$. Первые два представления связаны очевидным образом: вектором, представляющим какой-либо элемент поля, является набор коэффициентов соответствующего многочлена как вычета по модулю f (старшие коэффициенты записываются, как обычно, слева). В частности, $\alpha = [x] = (\mathtt{010})$ и $\alpha^0 = [1] = (\mathtt{001})$.

Найдем представления остальных элементов поля $\mathbb{F}_8$. Для этого будем последовательно рассматривать подряд идущие степени α и вычислять их остатки по модулю f. Так, очевидно, $\alpha^2 = [x^2] = (\mathtt{100})$. Однако при $k = 3$ многочлен x^3 не является вычетом по модулю f, и необходимо найти его остаток. Вместо деления с остатком можно заметить, что $\alpha^3 + \alpha + 1 = 0$ (так как α — корень f), откуда

$$\alpha^3 = \alpha + 1. \tag{8.22}$$

Следовательно, $\alpha^3 = [x^3] = [x + 1] = \alpha + 1 = (\mathtt{011})$. Далее,

$$\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = (\mathtt{110}).$$

Здесь мы сложили ранее найденные векторные представления $\alpha^2 = (\mathtt{100})$ и $\alpha = (\mathtt{010})$. Применяя тождество (8.22), также находим

$$\begin{aligned}\alpha^5 = \alpha \cdot \alpha^4 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \\ = \alpha^2 + \alpha + 1 = (\mathtt{111}) = [x^2 + x + 1].\end{aligned}$$

Наконец,

$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \\ = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1 = (\texttt{101}) = [x^2 + 1].$$

В заключение можно произвести проверку того, что $\alpha^7 = 1$. Действительно, $\alpha^7 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = 1$. Результаты наших вычислений занесем в таблицу:

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$		
-	000	$[0]$
1	001	$[1]$
α	010	$[x]$
α^2	100	$[x^2]$
α^3	011	$[x + 1]$
α^4	110	$[x^2 + x]$
α^5	111	$[x^2 + x + 1]$
α^6	101	$[x^2 + 1]$

Нулевой вычет, не являющийся элементом группы $\mathbb{F}_8^*$ и не имеющий дискретного логарифма по основанию α, включен в таблицу для полноты картины (вместо его мультипликативного представления стоит прочерк). Третий столбец нашей таблицы — столбец вычетов — не несет никакой дополнительной информации по сравнению со вторым, и поэтому в дальнейшем будем его отбрасывать (однако отметим, что он иллюстрирует теорему 8.5).

Чем полезна такая таблица? При осуществлении аддитивных операций удобно пользоваться векторным представлением элемента поля, а мультипликативных — его дискретным логарифмом, так как $\alpha^i \cdot \alpha^j = \alpha^{i+j}$ и $\alpha^i / \alpha^j = \alpha^{i-j}$. Иначе говоря, вместо умножения двух элементов можно просто сложить их логарифмы, а вместо деления — вычесть (и привести по модулю порядка группы). Таблица же позволяет быстро переходить от одного представления к другому.

Пусть, например, надо вычислить $\alpha^3 + \alpha^4$. По таблице устанавливаем, что $\alpha^3 = (\texttt{011})$ и $\alpha^4 = (\texttt{110})$. Складывая соответствующие векторы, получаем $(\texttt{011}) + (\texttt{110}) = (\texttt{101})$. Из таблицы

видим, что вектор (101) представляет элемент α^6. Таким образом[1)], $\alpha^3 + \alpha^4 = \alpha^6$.

Другой пример. Предположим, что нам требуется найти векторное представление произведения (011) · (111). Из таблицы следует, что (011) $= \alpha^3$ и (111) $= \alpha^5$, поэтому

$$(011) \cdot (111) = \alpha^3 \cdot \alpha^5 = \alpha^8 = \alpha \cdot \alpha^7 = \alpha$$

и $\alpha = (010)$. Следовательно, (011) · (111) = (010).

Пусть, наконец, нам надо найти обратный вычет $(110)^{-1}$. Тогда опять-таки по таблице устанавливаем, что $(110)^{-1} = \left(\alpha^4\right)^{-1} = \alpha^{-4} = \alpha^{7-4} = \alpha^3 = (011)$. Алгоритм Евклида не потребовался! □

Замечание 8.2. Тех же самых результатов можно было достичь, выписывая остатки от деления одночленов x^k, $0 \leqslant k \leqslant 6$, на неприводимый многочлен $x^3 + x + 1$. Однако при больших значениях степени неприводимого многочлена наш подход оптимальнее, т. к. при таком подходе используется меньше операций над элементами поля. Произведенные выше вычисления α^k можно рассматривать и как доказательство (неоптимальное) примитивности многочлена $x^3 + x + 1$.

В примере 8.11 на с. 269 было построено поле из 16 элементов путем расширения поля $\mathbb{Z}_2$ корнем α неприводимого над $\mathbb{Z}_2$ примитивного многочлена x^4+x+1. Там же для всех ненулевых элементов этого поля были найдены логарифмы по основанию элемента α. Приведем эти логарифмы здесь в более компактной форме:

1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
0	0	1	0	0	1	1	0	1	0	1	1	1	1	0
0	1	0	0	1	1	0	1	0	1	1	1	1	0	0
1	0	0	0	1	0	0	1	1	0	1	0	1	1	1

· (8.23)

[1)] Это можно было установить, и просто умножив обе части равенства (8.22) на α^3.

Для построения поля из 16 элементов можно было выбрать и другой примитивный многочлен четвертой степени $x^4 + x^3 + 1$ из $\mathbb{Z}_2[x]$ и аналогично построить таблицу логарифмов в поле $\mathbb{Z}_2[x]/(x^4 + x^3 + 1)$ по основанию его корня — вычета α. Как нетрудно убедиться, она будет отличаться от приведенной выше таблицы. Поэтому при вычислениях в конечном поле необходимо указывать способ его построения (примитивный многочлен и примитивный элемент). Выше было доказано, что поля $\mathbb{Z}_2[x]/(x^4+x+1)$ и $\mathbb{Z}_2[x]/(x^4+x^3+1)$ изоморфны; читателю рекомендуется построить этот изоморфизм явно, основываясь на доказательстве теоремы 8.8.

Пример 8.21. Вычислим значение выражения

$$\left(\frac{\alpha^4 + \alpha^7 + \alpha^8 + \alpha^{14}}{\alpha^2 + \alpha^{10} + \alpha^5 \cdot \alpha^6} + \alpha^3\right)^{2015},$$

где α — примитивный элемент поля $\mathbb{F}_{16} = \mathbb{Z}_2[x]/(x^4 + x + 1)$.

Для этого воспользуемся приведенной выше таблицей (8.23). Сначала вычислим числитель и знаменатель дроби, заменяя элементы $\alpha^4, \alpha^7, \alpha^8, \alpha^{14}$ и α^2, α^{10}, $\alpha^{11} = \alpha^5 \cdot \alpha^6$ их векторными представлениями:

$$\begin{array}{ll} \texttt{0011} & = \alpha^4 \\ \texttt{1011} & = \alpha^7 \\ \texttt{0101} & = \alpha^8 \\ \texttt{1001} & = \alpha^{14} \\ \hline \texttt{0100} & = \alpha^2, \end{array} \qquad \begin{array}{ll} \texttt{0100} & = \alpha^2 \\ \texttt{0111} & = \alpha^{10} \\ \texttt{1110} & = \alpha^{11} \\ \hline \texttt{1101} & = \alpha^{13}. \end{array}$$

Отсюда $\alpha^4 + \alpha^7 + \alpha^8 + \alpha^{14} = \alpha^2$ и $\alpha^2 + \alpha^{10} + \alpha^{11} = \alpha^{13}$. Таким образом, значение дроби равно $\alpha^2/\alpha^{13} = \alpha^{-11} = \alpha^4$.

Далее, $\alpha^4 + \alpha^3 = \alpha^7$. Наконец, возведем α^7 в степень $2015 = 15 \cdot 134 + 5$ и получим ответ $\alpha^{7 \cdot 2015} = (\alpha^{15})^{7 \cdot 134} \cdot (\alpha^7)^5 = 1 \cdot \alpha^5 = \alpha^5$. □

Пример 8.22. Для элемента α^5 из поля $\mathbb{Z}_2[x]/(x^4 + x + 1)$ найдем минимальный многочлен над простым подполем.

Простым подполем поля $\mathbb{F}_{16}$ является поле $\mathbb{F}_2$, его характеристика равна $p = 2$. Воспользуемся теоремой 8.7 и свойствами

сопряженных элементов. Найдем все сопряженные с α^5 элементы. Для этого рассмотрим последовательность

$$\alpha^{5\cdot 2^i}, \qquad i = 0, 1, \ldots .$$

Прямым вычислением убеждаемся, что она содержит всего два различных члена, α^5 и α^{10}, так как $\alpha^{20} = \alpha^5$ (период последовательности равен двум). Следовательно, искомый многочлен не имеет других корней, кроме α^5 и α^{10}. Отсюда

$$\begin{aligned} m_{\alpha^5}(x) = m_{\alpha^{10}}(x) &= (x - \alpha^5)(x - \alpha^{10}) = \\ &= x^2 + (\alpha^5 + \alpha^{10})x + \alpha^5\alpha^{10} = x^2 + x + 1. \end{aligned}$$

В последнем вычислении мы воспользовались таблицей (8.23), чтобы найти $\alpha^5 + \alpha^{10} = 1$. □

Пример 8.23. Найдем минимальный многочлен $m_{\alpha^5}(x)$ из предыдущего примера другим способом — применим метод неопределенных коэффициентов. Из теорем 8.2 и 8.7 следует, что степень минимального многочлена любого элемента поля $\mathbb{F}_{2^4}$ не превосходит четырех, поэтому искомый многочлен имеет вид

$$m_{\alpha^5}(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4, \quad a_i \in \mathbb{Z}_2.$$

Подставив вместо аргумента в $m_{\alpha^5}(x)$ его корень $x = \alpha^5$, получим

$$m_{\alpha^5}(\alpha^5) = a_0 + a_1\alpha^5 + a_2\alpha^{10} + a_3\alpha^0 + a_4\alpha^5 = 0.$$

Последнее равенство можно переписать в векторном виде, используя векторное представление элементов поля $\mathbb{F}_{16}$ над простым подполем (см. таблицу (8.23)):

$$a_0\begin{pmatrix}0\\0\\0\\1\end{pmatrix} + a_1\begin{pmatrix}0\\1\\1\\0\end{pmatrix} + a_2\begin{pmatrix}0\\1\\1\\1\end{pmatrix} + a_3\begin{pmatrix}0\\0\\0\\1\end{pmatrix} + a_4\begin{pmatrix}0\\1\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}.$$

Получаем однородную систему линейных уравнений над простым подполем:

$$\left(\begin{array}{ccccc|c} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{array}\right),$$

откуда находим

$$\left(\begin{array}{ccccc|c} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{array}\right),$$

применяя метод раздела 6.2. Последняя матрица систематическая, поэтому общее решение системы имеет вид

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \tag{8.24}$$

где $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_2$ — произвольны. Последнее равенство задает целое семейство многочленов над $\mathbb{Z}_2$, корнем которых является α^5. Ненулевым многочленом наименьшей степени среди них, очевидно, является многочлен с коэффициентами $\lambda_1 = 1, \lambda_2 = \lambda_3 = 0$. Заметим, что это можно было сказать заранее, не выписывая общее решение (8.24), из-за того, что свободная переменная λ_i с меньшим номером отвечает за меньшую степень одночлена в $m_{\alpha^5}(x)$. Таким образом, искомым ответом является первый базисный вектор (11100) найденной фундаментальной системы решений, кодирующий многочлен $1 + x + x^2$. $\square$

Подчеркнем, что метод решения примера 8.23 является достаточно общим и удобным: чтобы найти минимальный многочлен $m_\beta(x)$ элемента $\beta \in \mathbb{F}_{p^n}$ над простым подполем $\mathbb{F}_p$, достаточно решить систему линейных уравнений над $\mathbb{F}_p$, которая получается из уравнения с неопределенными коэффициентами $m_\beta(\beta) = 0$, если заменить в нем все множители из $\mathbb{F}_{p^n}$ их векторными представлениями над $\mathbb{F}_p$. При этом набор коэффициентов многочлена $m_\beta(x)$ автоматически получится равным первому из базисных векторов в ортогональном пространстве этой системы, если элементарные преобразования при ее решении производить так, чтобы в конце главными оказались те переменные, которые соответствуют младшим коэффициентам $m_\beta(x)$, а свободными — те, которые соответствуют старшим.

Пример 8.24. Нам уже известны все неприводимые многочлены небольшой степени над полем $\mathbb{Z}_2$ (см. с. 113). На основании этого запишем равенства

$$x^4 + x = x \cdot (x+1)(x^2+x+1) = \prod_{\beta \in \mathbb{F}_4} (x - \beta),$$

$$x^8 + x = x \cdot (x+1)(x^3+x+1)(x^3+x^2+1) = \prod_{\beta \in \mathbb{F}_8} (x - \beta),$$

$$\begin{aligned} x^{16} + x &= x \cdot (x+1)(x^2+x+1)(x^4+x+1) \cdot \\ &\quad \cdot (x^4+x^3+1)(x^4+x^3+x^2+x+1) = \\ &= (x-0)(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)\dots(x-\alpha^{14}), \end{aligned}$$

являющиеся частным случаем равенств (8.9) и (8.12). Действуя аналогичным примеру 8.22 или примеру 8.23 образом, нетрудно найти минимальные многочлены для всех элементов поля $\mathbb{F}_{16} = \mathbb{Z}_2[x]/(x^4+x+1)$. В результате можно составить таблицу элементов этого поля с указанием их минимальных многочленов:

0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0
0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0
0	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1
x	m_1	m_3	m_3	m_5	m_3	m_2	m_5	m_4	m_3	m_5	m_2	m_4	m_5	m_4	m_4

Минимальные многочлены в последней строке данной таблицы для компактности записи занумерованы следующим образом:

$$\overbrace{(x+1)}^{m_1(x)}\ \overbrace{(x^2+x+1)}^{m_2(x)}\ \overbrace{(x^4+x+1)}^{m_3(x)}$$

$$\overbrace{(x^4+x^3+1)}^{m_4(x)}\ \overbrace{(x^4+x^3+x^2+x+1)}^{m_5(x)},$$

а сама таблица наглядно демонстрирует разбиение циклической

группы $\mathbb{F}_{16}^*$ на классы сопряженных элементов:

$$\langle\alpha\rangle = \underbrace{\{\,1\,\}}_{m_1(x)} \cup \underbrace{\{\alpha^5, \alpha^{10}\}}_{m_2(x)} \cup \underbrace{\{\alpha, \alpha^2, \alpha^4, \alpha^8\}}_{m_3(x)} \cup \underbrace{\{\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}\}}_{m_4(x)} \cup \underbrace{\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}}_{m_5(x)}. \tag{8.25}$$

Заметим также, что $m_1(x) \cdot m_2(x) \cdot \ldots \cdot m_5(x) = x^{15} + 1$. $\square$

Пример 8.25. Согласно теореме 8.6, поле $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ содержит подполя $\mathbb{F}_2$ и $\mathbb{F}_{2^2}$ и не содержит других собственных подполей. Ее доказательство указывает возможный способ нахождения элементов, лежащих в $\mathbb{F}_2$ и $\mathbb{F}_{2^2}$. Так, подполе $\mathbb{F}_{2^2}$ состоит из корней уравнения $x^4 + x = 0$, а $\mathbb{F}_2$ — из корней уравнения $x^2 + x = 0$. Иными словами, $\mathbb{F}_4$ и $\mathbb{F}_2$ состоят из корней неприводимых делителей двучленов $x^4 + x$ и $x^2 + x$, которые сами являются делителями двучлена $x^{16} + x$. Отсюда с учетом уже найденных минимальных многочленов для элементов $\mathbb{F}_{16}$ находим, что $\mathbb{F}_4 = \{0, 1, \alpha^5, \alpha^{10}\}$ и $\mathbb{F}_2 = \{0, 1\}$ (последнее очевидно).

Альтернативный и значительно более удобный способ основан на строении группы $\mathbb{F}_{16}^* = \langle\alpha\rangle$. Как циклическая группа 15-го порядка, она содержит единственную подгруппу порядка $3 = |\mathbb{F}_4^*|$, и это подгруппа $\langle\alpha^5\rangle$. Значит, $\mathbb{F}_4^* = \langle\alpha^5\rangle$, откуда $\mathbb{F}_4 = \{0\} \cup \mathbb{F}_4^* = \{0, 1, \alpha^5, \alpha^{10}\}$. $\square$

Вернемся к вопросу нахождения числа неприводимых многочленов над простым полем. Ранее уже были предложены два подхода к решению этой задачи (теорема 4.13 и пример 8.6). Разберем третий метод, основанный на строении конечного поля, похожий на них, но имеющий немного другое обоснование.

Пример 8.26. Найдем число неприводимых многочленов степени 12 над $\mathbb{Z}_2$.

Заметим, что каждый неприводимый над $\mathbb{Z}_2$ многочлен степени n является минимальным для некоторых n элементов поля $\mathbb{F}_{2^n}$ согласно результатам раздела 8.2. Эти n элементов сопряжены, имеют одинаковый порядок и не лежат ни в каком собственном подполе поля $\mathbb{F}_{2^n}$. Таким образом, все элементы

поля $\mathbb{F}_{2^n}$, не входящие в подполя, разбиваются на непересекающиеся равномощные подмножества D_i, каждое из которых является множеством корней одного неприводимого многочлена степени n (корни минимальных многочленов меньших степеней лежат в подполях). Следовательно, число элементов $M = \sum_i |D_i|$, не входящих в подполя поля $\mathbb{F}_{2^n}$, и число N неприводимых многочленов степени n связаны равенством $N = \frac{M}{n}$.

Осталось найти число M. Напомним, что $\mathbb{F}_{2^a} \subset \mathbb{F}_{2^b}$ тогда и только тогда, когда $a \mid b$ (теорема 8.6). На рис. 8.2 слева приведена так называемая *решетка подполей* поля $\mathbb{F}_{2^{12}}$. Она представляет собой граф, вершины которого соответствуют подполям, а ребра — отношению $\mathbb{F}_{2^a} \subset \mathbb{F}_{2^b}$ (транзитивные ребра опущены). По теореме 8.6 решетка подполей поля $\mathbb{F}_{p^n}$ всегда совпадает с решеткой делителей числа n.

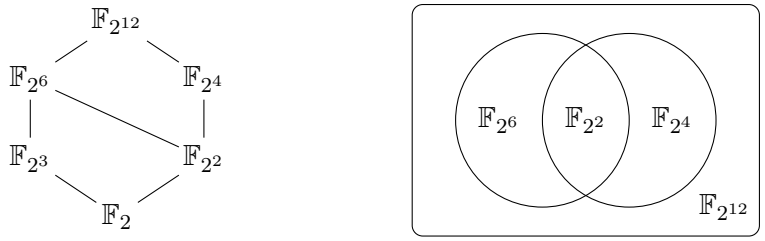


Рис. 8.2

Справа на этом же рисунке приведена диаграмма максимальных подполей в $\mathbb{F}_{2^{12}}$. Отсюда, применяя принцип включений и исключений, находим

$$M = 2^{12} - 2^4 - 2^6 + 2^2 = 4020,$$

поэтому существует ровно $\frac{4020}{12} = 335$ двоичных неприводимых многочленов степени 12. □

Пример 8.27. На с. 275 было введено понятие нормального базиса поля и доказано его существование в любом конечном поле. Одно из основных применений нормальных базисов — упрощение вычислений в конечных полях. В частности, возведение элемента в степень, равную характеристике поля, в нормальном

базисе равносильно циклическому сдвигу вектора координат этого элемента в нем. Действительно, пусть $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ — нормальный базис поля $\mathbb{F}_{p^n}$ и

$$\beta = b_0\alpha + b_1\alpha^p + b_2\alpha^{p^2} + \ldots + b_{n-1}\alpha^{p^{n-1}},$$

где $b_i \in \mathbb{F}_p$, — разложение элемента β по этому базису. Тогда, учитывая, что $\alpha^{p^n} = \alpha$, имеем

$$\begin{aligned}\beta^p &= \left(b_0\alpha + b_1\alpha^p + \ldots + b_{n-1}\alpha^{p^{n-1}}\right)^p = \\ &= b_0\alpha^p + b_1\alpha^{p^2} + \ldots + b_{n-2}\alpha^{p^{n-1}} + b_{n-1}\alpha^{p^n} = \\ &= b_{n-1}\alpha + b_0\alpha^p + b_1\alpha^{p^2} + \ldots + b_{n-2}\alpha^{p^{n-1}}.\end{aligned}$$

Таким образом, координаты p-й степени элемента с координатами $(b_0, b_1, \ldots, b_{n-1})$ равны $(b_{n-1}, b_0, b_1, \ldots, b_{n-2})$. На большинстве современных процессоров для подобного преобразования вектора, умещающегося в одно машинное слово, достаточно всего одного такта работы, а схемная реализация циклического сдвига вообще не требует функциональных элементов. Таким образом, вычисление степеней $\beta^p, \beta^{p^2}, \ldots$ — очень эффективная операция в нормальном базисе. Остальные степени можно вычислить по формулам $\beta^{pi} = (\beta^i)^p$ и $\beta^{pi+j} = \beta^{pi}\beta^j$ при $j < p$, хотя умножение в нормальном базисе — уже не столь простая операция. □

Пример 8.28. В примере 8.16 был рассмотрен нормальный базис B поля $\mathbb{F}_{27} = \mathbb{Z}_3[x]/(x^3 + 2x + 1)$, состоящий из элементов $\alpha^2, \alpha^6, \alpha^{18}$.

Согласно предыдущему примеру, если элемент β имеет в базисе B координаты (012), то $\beta^3 = (201)$. Чтобы найти координаты элементов β и β^3 в стандартном базисе B', то есть в базисе $\alpha^2, \alpha, 1$, можно воспользоваться матрицей перехода $\mathbf{A}$ от B' к B, введенной на с. 154. Обратная к ней матрица $\mathbf{A}^{-1}$ будет матрицей перехода от B к B', она позволяет по координатам вектора в базисе B найти его координаты в базисе B'. Учитывая, что

$\alpha^2 = (\mathtt{100})$, $\alpha^6 = (\mathtt{111})$ и $\alpha^{18} = (\mathtt{121})$ (это устанавливается легко), имеем

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix}, \qquad \mathbf{A}^{-1} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix},$$

применив метод раздела 6.2. Следовательно, в стандартном базисе $\beta = \mathbf{A}(012)^{\mathrm{T}} = (020)^{\mathrm{T}}$ и $\beta^3 = \mathbf{A}(201)^{\mathrm{T}} = (021)^{\mathrm{T}}$. Подчеркнем, что при вычислениях нам не потребовалась таблица дискретных логарифмов из примера 8.10. При ее наличии задача становится тривиальной, так как $\beta = \alpha^{14}$ и $\beta^3 = \alpha^{14\cdot 3} = \alpha^{16}$. Также заметим, что матрицы $\mathbf{A}$ и $\mathbf{A}^{-1}$ вычисляются единожды, а применять их для возведения различных элементов в степени 3 и 9 можно многократно. $\square$

Пример 8.29. Рассмотрим фактор-кольцо $\mathbb{K} = \mathbb{Z}_2[x]/(h)$, где $h(x) = (x^3 + x + 1)(x^4 + x + 1) \in \mathbb{Z}_2[x]$. Очевидно, что $|\mathbb{K}| = 2^7 = 128$. Исследуем структуру мультипликативной группы $\mathbb{K}^*$. Для этого воспользуемся китайской теоремой об остатках (теорема 4.17): кольцо $\mathbb{K}$ изоморфно прямой сумме колец $\mathbb{K}_1 = \mathbb{Z}_2[x]/(x^3 + x + 1)$ и $\mathbb{K}_2 = \mathbb{Z}_2[x]/(x^4 + x + 1)$. В силу неприводимости над $\mathbb{Z}_2$ многочленов $f(x) = x^3 + x + 1$ и $g(x) = x^4 + x + 1$, кольца $\mathbb{K}_1$ и $\mathbb{K}_2$ являются полями, состоящими из $2^3 = 8$ и $2^4 = 16$ элементов соответственно. Следовательно, их мультипликативные группы — циклические с порядками $8 - 1 = 7$ и $16 - 1 = 15$. Из изоморфизма колец следует изоморфизм их мультипликативных групп:

$$\mathbb{K} \cong \mathbb{K}_1 \otimes \mathbb{K}_2 \quad \Rightarrow \quad \mathbb{K}^* \cong \mathbb{K}_1^* \times \mathbb{K}_2^*.$$

В частности, мультипликативная группа $\mathbb{K}^*$ — циклическая как прямое произведение двух циклических групп $\mathbb{K}_1^*, \mathbb{K}_2^*$ взаимно простых порядков, и $|\mathbb{K}^*| = |\mathbb{K}_1^*|\cdot|\mathbb{K}_2^*| = 7\cdot 15 = 105$. Образующим элементом группы $\mathbb{K}^*$ будет элемент прямого произведения $\alpha = (\alpha_1, \alpha_2)$, где α_1, α_2 — примитивные элементы полей $\mathbb{K}_1$ и $\mathbb{K}_2$.

Нетрудно видеть, что f и g — примитивные многочлены. Следовательно, $\alpha_1 = x \pmod f$ и $\alpha_2 = x \pmod g$. Представление остатками из китайской теоремы дает нам равенство $x =$

$= [x, x]_{f,g}$. Поэтому корень $x \in \mathbb{K}$ многочлена $h(x)$ является образующим элементом в $\mathbb{K}^*$.

Таким образом, получен пример приводимого и заведомо непримитивного многочлена h, корень которого тем не менее является образующим в мультипликативной группе $(\mathbb{Z}_2[x]/(h))^*$. $\square$

Многие важные задачи теории конечных полей решаются практически без вычислений в них. Так, в приложениях встречаются задачи, в которых требуется оценить или найти точное число решений некоторого уравнения, не решая его, или по элементу поля-расширения необходимо установить степень его минимального многочлена, не находя сам этот многочлен, или выяснить, сопряжены ли два каких-то элемента поля. Разберем несколько примеров на эту тему.

Пример 8.30. Найдем корни многочлена $f(x) = x^3+x^2+x+1$ в поле $\mathbb{F}_{3^9}$. Выясним сначала, приводим или нет этот многочлен над простым подполем $\mathbb{F}_3$. При проверке сразу убеждаемся, что $0, 1 \in \mathbb{F}_3$ — не корни $f(x)$, а двойка является корнем. Значит, $f(x)$ приводим и делится на $x - 2 = x + 1 \in \mathbb{F}_3[x]$. Поделив, например, в столбик, находим

$$x^3 + x^2 + x + 1 = (x^2 + 1) \cdot (x + 1).$$

Квадратичный множитель $x^2 + 1$ не имеет корней в $\mathbb{F}_3$ и, следовательно, неприводим.

Перебором найдены все решения (а именно $x = 2$) данного уравнения в простом подполе. Кроме поля $\mathbb{F}_3$ и поля $\mathbb{F}_{3^3}$ в поле $\mathbb{F}_{3^9}$ нет других собственных подполей ($1, 3, 9$ — это все делители числа 9). Следовательно, элементы из $\mathbb{F}_{3^9} \setminus \mathbb{F}_3$ являются корнями всевозможных неприводимых многочленов 3-й и 9-й степени из $\mathbb{F}_3[x]$ и только их. Так как ни один из этих многочленов не делится на многочлен $x^2 + 1$, то $f(x)$ не имеет корней среди элементов множества $\mathbb{F}_{3^9} \setminus \mathbb{F}_3$. Таким образом, единственным решением уравнения является $x = 2$. $\square$

Пример 8.31. Найдем число решений уравнения $x^7 + x^5 + x^3 + x^2 + 1 = 0$ в поле $\mathbb{F}_{2^6}$.

Заметим, что ответ зависит от разложения левой части уравнения на неприводимые множители. Действительно, если многочлен $f(x) = x^7 + x^5 + x^3 + x^2 + 1$ неприводим, то решений нет, так как никакой неприводимый над $\mathbb{Z}_2$ многочлен 7-й степени не делит двучлен $x^{2^6} - x$, а каждый элемент поля $\mathbb{F}_{2^6}$ является корнем этого двучлена.

Если же f делится на некоторый неприводимый многочлен g степени k, где k — делитель числа 6, то каждый из k корней многочлена g одновременно и является корнем многочлена f, и лежит в поле $\mathbb{F}_{2^6}$. Нетрудно видеть, что данный многочлен f является произведением двух неприводимых многочленов g_1, g_2, таких, что $\deg g_1 = 3$ и $\deg g_2 = 4$. Таким образом, данное уравнение имеет три решения.

Обобщая вышесказанное, получаем, что число различных решений уравнения $f(x) = 0$ в поле $\mathbb{F}_{p^n}$ равно степени наибольшего общего делителя многочленов $f(x)$ и $x^{p^n} - x$ над $\mathbb{Z}_p$ (без учета их кратности). Из условия задачи нетрудно установить, что $(f, x^{2^6} - x) = x^3 + x + 1$. $\square$

Пример 8.32. Пусть α — примитивный элемент поля $\mathbb{F}_{2^{12}}$. Найдем степень минимального многочлена элемента α^{546} над простым подполем $\mathbb{F}_2$, не вычисляя сам многочлен явно.

Мы уже пользовались следствием теоремы о строении поля-расширения (см. пример 8.26): если элемент α^k лежит в поле $\mathbb{F}_{p^m}$ и не лежит ни в каком его собственном подполе, то степень минимального многочлена $m_{\alpha^k}(x) \in \mathbb{Z}_p[x]$ равна m. Осталось узнать, в какое подполе попал данный элемент. Оказывается, что это легко можно установить по его порядку.

Действительно, согласно теореме 3.16,

$$|\alpha^{546}| = \frac{|\alpha|}{(|\alpha|, 546)} = \frac{2^{12} - 1}{(2^{12} - 1, 546)} = \frac{4095}{(4095, 546)} = \frac{4095}{273} = 15.$$

Следовательно, элемент α^{546} образует циклическую подгруппу 15-го порядка в $\mathbb{F}^*_{2^{12}}$. Эта подгруппа является группой $\mathbb{F}^*_{2^4}$, так как иных подгрупп порядка 15 в поле $\mathbb{F}_{2^{12}}$ нет в силу цикличности его мультипликативной группы. Следовательно, элемент

α^{546} лежит в поле $\mathbb{F}_{2^4} \subset \mathbb{F}_{2^{12}}$ и не лежит ни в каком его подполе (порядки элементов подполей поля $\mathbb{F}_{2^4}$ являются делителями числа $3 = |\mathbb{F}_{2^2}^*|$). Поэтому $\deg m_{\alpha^{546}} = 4$. $\square$

Пример 8.33. Выясним, являются ли сопряженными элемент $\beta = \alpha^{546}$ из предыдущего примера и элемент $\gamma = \alpha^{273}$ в поле $\mathbb{F}_{2^{12}}$. Сделать это можно по определению: если найдется такое i, что $\beta^{2^i} = \gamma$, то β и γ сопряжены. Равенство $\beta^{2^i} = \gamma$ равносильно сравнению

$$546 \cdot 2^i = 273 \bmod 2^{12} - 1.$$

Решению уравнений такого типа посвящен раздел 9.3. Однако в данном случае применять никакие специальные алгоримы не требуется, т. к. по теореме о строении поля $\mathbb{F}_{2^{12}}$ неизвестное i не превосходит числа 12 и потому может быть найдено полным перебором (более того, i должно делить 12).

Вместо перебора можно применить еще одну хитрость. Представим дискретный логарифм b элемента $\beta = \alpha^b$ из поля $\mathbb{F}_{2^n}$ в позиционной двоичной системе счисления:

$$b = b_0 + 2b_1 + 2^2 b_2 + \ldots + 2^{n-1} b_{n-1}, \quad b_i \in \{0, 1\}.$$

Заметим, что

$$\beta^2 = \alpha^{2b} = \alpha^{2b_0 + 2^2 b_1 + \ldots + 2^n b_{n-1}} = \alpha^{b_{n-1} + 2b_0 + 2^2 b_1 + \ldots + 2^{n-1} b_{n-2}}$$

в силу того, что $|\alpha| = 2^n - 1$. Иными словами, двоичная запись $\overline{(b_{n-1}, b_0, b_1, \ldots, b_{n-2})}_2$ логарифма элемента β^2 оказалась равна циклическому сдвигу двоичной записи $\overline{(b_0, b_1, \ldots, b_{n-1})}_2$ логарифма элемента β на один разряд (ср. с примером 8.27). То же самое верно и для элемента β^{2^2}, и т. д.

Отсюда следует простое правило: в поле характеристики 2 сопряжены те и только те элементы, двоичные записи логарифмов которых по основанию примитивного элемента поля переходят друг в друга циклическими сдвигами. Множества таких чисел принято называть *циклотомическими классами*. В частности, легко видеть, что

$$546 = \overline{(001000100010)}_2, \quad 273 = \overline{(000100010001)}_2,$$

откуда заключаем, что β и γ сопряжены, причем $i = 3$. В циклотомическом классе числа 546 всего четыре числа (включая его само), поэтому α^{546} сопряжен с четырьмя элементами поля $\mathbb{F}_{2^{12}}$. Следовательно, его минимальный многочлен имеет степень 4 (доказали независимо от предыдущего примера). $\square$

Пример 8.34. Разбиение (8.25) мультипликативной группы поля $\mathbb{F}_{16}$ на классы сопряженных элементов равносильно следующему разбиению множества всех целых чисел от 0 до 14 на циклотомические классы:

$$\{0\} \cup \{5, 10\} \cup \{1, 2, 4, 8\} \cup \{7, 11, 13, 14\} \cup \{3, 6, 9, 12\},$$

или, более наглядно, в двоичной системе:

$$\{0000\} \cup \{0101, 1010\} \cup \{0001, 0010, 0100, 1000\} \cup \\ \cup \{0111, 1011, 1101, 1110\} \cup \{0011, 0110, 1100, 1001\}. \quad \square$$

Пример 8.35. Циклотомический класс числа 9 по основанию $2^6 - 1 = 63$ состоит всего из трех чисел: $9 \cdot 2^0 = 9$, $9 \cdot 2 = 18$ и $9 \cdot 2^2 = 36$, так как $9 \cdot 2^3 = 9 \bmod 63$. Поэтому элемент α^9, где α — примитивный элемент поля $\mathbb{F}_{2^6}$, лежит в подполе $\mathbb{F}_{2^3}$. Следовательно, $\deg m_{\alpha^9}(x) = 3$. $\square$

8.5. Порядки многочленов

Пусть $f(x) \in \mathbb{Z}_p[x]$ и пусть $f(0) \neq 0$, т. е. свободный член у многочлена $f(x)$ не равен нулю. Тогда наименьшее натуральное число n, при котором двучлен $x^n - 1$ делится на $f(x)$, называется *порядком*[1)] многочлена $f(x)$ (а также иногда его *периодом*, или *экспонентой*) и обозначается $\operatorname{ord} f$:

$$\operatorname{ord} f = \min\bigl\{n \in \mathbb{N} : f(x) \mid x^n - 1\bigr\}.$$

[1)] В теории регистров сдвига с линейной обратной связью над конечным полем (Linear Feedback Shift Register, LFSR) рассматриваются также порядки многочленов с нулевым свободным членом. Если $f(0) = 0$, то многочлен $f(x)$ однозначно представим в виде $f(x) = x^r g(x)$, где $r \geqslant 1$ и $g(0) \neq 0$. Тогда порядком многочлена f по определению является порядок многочлена g. Далее такие многочлены рассматривать не будем.

Пример 8.36. Порядок многочлена $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ равен трем, так как $x^2 + x + 1 \nmid x - 1, x^2 - 1$ и $x^2 + x + 1 \mid x^3 - 1$. $\square$

Нетрудно заметить, что данное выше определение порядка многочлена равносильно следующему: порядок многочлена $f(x)$ совпадает с порядком его корня x в мультипликативной группе кольца $\mathbb{Z}_p[x]/f(x)$. Действительно, $x^n = 1 \pmod{f(x)}$ тогда и только тогда, когда $f(x) \mid x^n - 1$.

Из предположения $f(0) \neq 0$ следует, что $f(x)$ и его корень x взаимно просты, поэтому $x \in (\mathbb{Z}_p[x]/f(x))^*$. Отсюда следует корректность определения порядка многочлена: обратимый вычет x имеет конечный мультипликативный порядок, который к тому же является делителем порядка группы $(\mathbb{Z}_p[x]/f(x))^*$ по теореме Лагранжа. Далее, как и раньше, порядок элемента a в конечной группе будем обозначать $|a|$.

В случае, когда многочлен $f(x)$ неприводим над $\mathbb{Z}_p$, факторкольцо $\mathbb{Z}_p[x]/f(x)$ является полем $\mathbb{F}$ из p^m элементов, где $m = \deg f$. В этом поле многочлен $f(x)$ имеет m различных сопряженных корней, причем вычет x является одним из них при условии $m > 1$. Порядки всех корней одинаковы, как было установлено в примере 8.14, и потому равны $\operatorname{ord} f$. Для неприводимого многочлена степени $m = 1$ с одним ненулевым корнем это очевидно.

Выше мы убедились, что все конечные поля одинакового порядка изоморфны между собой. Таким образом, получаем следующую теорему.

Теорема 8.11. *Пусть $\mathbb{F}$ — поле из p^m элементов, $m \geqslant 1$, и $f(x) \neq x$ — неприводимый над $\mathbb{Z}_p$ многочлен степени m. Тогда $\operatorname{ord} f = |\beta|$ для любого корня β из сопряженных в поле $\mathbb{F}$ корней многочлена f.*

Отметим, что в этом утверждении важна неприводимость многочлена $f(x)$. Оно остается верным и для любого поля $\mathbb{F}'$, содержащего поле $\mathbb{F} = \mathbb{F}_{p^m}$.

Следствие 8.2. *Порядок любого неприводимого над $\mathbb{Z}_p$ многочлена степени m является делителем числа $p^m - 1$.*

Следствие 8.3. *Многочлен степени m над $\mathbb{Z}_p$ является примитивным тогда и только тогда, когда его порядок равен $p^m - 1$.*

Последнее следствие можно считать эквивалентным определением примитивного многочлена.

Пример 8.37. Как было установлено выше, имеются всего три неприводимых многочлена 4-й степени над $\mathbb{Z}_2$. Это многочлены $x^4 + x + 1$, $x^4 + x^3 + 1$ и $x^4 + x^3 + x^2 + x + 1$. Из таблицы минимальных многочленов элементов поля $\mathbb{F}_{16}$ на с. 287 имеем, что первые два из них являются примитивными, так как порядок их корней равен 15. У последнего же многочлена порядок корня α^3 равен 5, поэтому $\operatorname{ord}(x^4+x^3+x^2+x+1) = 5$ (см. также пример 8.15). □

Пример 8.38. Воспользовавшись разложением на множители числа

$$2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31,$$

можно найти количество неприводимых многочленов f степени 10 над $\mathbb{Z}_2$, имеющих конкретный порядок. При этом $\operatorname{ord} f$ делит $2^{10} - 1$. У числа $2^{10} - 1$, как и у всякого числа, являющегося произведением трех различных простых чисел, имеется восемь делителей, два из которых тривиальны. В данном случае делители составляют множество $A = \{1, 3, 11, 31, 33, 93, 341, 1023\}$, причем $\operatorname{ord} f \in A$.

Для всякого $d \in A$ в поле $\mathbb{F}_{2^{10}}$ содержится $\varphi(d)$ элементов порядка d, каждый из которых является корнем некоторого неприводимого многочлена. Порядок этого многочлена совпадает с порядком корня, а степень — с порядком расширения того подполя поля $\mathbb{F}_{2^{10}}$, в котором лежит его корень, т. е. является делителем числа 10. Поле $\mathbb{F}_{2^{10}}$ содержит подполя $\mathbb{F}_2$, $\mathbb{F}_{2^2}$ и $\mathbb{F}_{2^5}$. Других собственных подполей в нем нет. Порядки мультипликативных групп подполей $\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^5}$ равны $1, 3, 31$ соответственно. Поэтому многочлены с порядками $1, 3, 31$ (и их нетривиальными делителями, если бы они были) имеют степени $1, 2, 5$. Все остальные многочлены с порядками из множества $A \setminus \{1, 3, 31\} = \{11, 33, 93, 341, 1023\}$ имеют степень 10.

Итак, многочлен порядка d и степени m имеет m корней (порядка d каждый), поле-расширение содержит всего $\varphi(d)$ таких элементов, и каждый из них является корнем одного многочлена, следовательно, число различных неприводимых многочленов порядка d равно $\frac{\varphi(d)}{m}$ (сравните с примером 8.26). Поэтому существует $\frac{\varphi(11)}{10} = 1$ многочлен порядка 11 и

$$\frac{\varphi(33)}{10} = 2, \quad \frac{\varphi(93)}{10} = 6, \quad \frac{\varphi(341)}{10} = 30, \quad \frac{\varphi(1023)}{10} = 60$$

многочленов степени 10 порядка $33, 93, 341, 1023$ соответственно. $\square$

Заметим, что из рассмотренного только что примера следует простое комбинаторное объяснение интересного факта из теории чисел: если p — простое и m — наименьшее натуральное число, при котором число d является делителем числа $p^m - 1$, то $\varphi(d)$ нацело делится на m.

Выше в примере 8.37 мы воспользовались готовой таблицей дискретных логарифмов и минимальных многочленов поля $\mathbb{F}_{16}$. Если же такой таблицы нет или ее построение слишком громоздко, то порядок неприводимого многочлена можно найти тем же способом, что и порядок элемента x произвольной конечной группы G в случае, когда известно разложение числа $|G|$ на простые множители, а для возведения x в степень в группе G имеется эффективный алгоритм. (См. также посвященный идейно близкому методу раздел 9.4.)

Действительно, если $f \in \mathbb{Z}_p[x]$ — неприводим, $n = \operatorname{ord} f$ и $m = \deg f$, то n делит число $p^m - 1$ (следствие 8.2). Разложим число $p^m - 1$ на простые множители (это наиболее трудный при больших m этап метода; для его облегчения для чисел такого вида составлены специальные таблицы делителей):

$$p^m - 1 = p_1^{r_1} \dots p_k^{r_k}, \qquad r_i \geqslant 1.$$

Тогда $n = p_1^{s_1} \dots p_k^{s_k}$, где $0 \leqslant s_i \leqslant r_i$. Для каждого $i = 1, \dots, k$ найдем вычеты $x^{(p^m-1)/p_i}$ по модулю $f(x)$. Если при этом окажется, что

$$x^{(p^m-1)/p_i} \neq 1 \pmod{f(x)},$$

то число n делится на $p_i^{r_i}$, а значит $s_i = r_i$ (см. доказательство леммы 8.1 и теоремы 8.1). Иначе $s_i < r_i$. В последнем случае, чтобы найти s_i, надо выяснить, будет ли делиться число n на числа $p_i^{r_i-1}, p_i^{r_i-2}, \ldots, p_i$. Это можно сделать, вычисляя вычеты

$$x^{(p^m-1)/p_i^2}, \quad x^{(p^m-1)/p_i^3}, \quad \ldots, \quad x^{(p^m-1)/p_i^{r_i}} \pmod{f(x)}$$

и сравнивая их с единицей. Производя такие действия для каждого простого делителя p_i числа $p^m - 1$, найдем все неизвестные s_i и искомое число n.

Для иллюстрации этого метода приведем пример.

Пример 8.39. Нетрудно убедиться в том, что многочлен $f(x) = x^4 + x^2 + 2x + 1$ взаимно прост с двучленом $x^{3^2} - x$ и, следовательно, неприводим над $\mathbb{Z}_3$. Найдем его порядок.

Пусть n — порядок многочлена f. Тогда n является делителем числа $p^m - 1 = 3^4 - 1 = 80 = 5 \cdot 2^4$ и, следовательно, имеет вид $n = 5^{s_1} \cdot 2^{s_2}$. Для нахождения s_1 и s_2 нам необходимо вычислить $x^{80/5} = x^{16} \pmod{f}$ и $x^{80/2} = x^{40} \pmod{f}$. Вычисления будем производить в поле $\mathbb{F} = \mathbb{F}_{81} = \mathbb{Z}_3[x]/f(x)$.

Очевидно, что $x^4 = 2x^2 + x + 2 = \texttt{0212} \pmod{f}$. Тогда

$$\begin{aligned} x^{16} &= (x^4)^3 x^4 = (2x^2 + x + 2)^3 x^4 = (2x^6 + x^3 + 2)x^4 = \\ &= (2x^2 \cdot x^4 + x^3 + 2)x^4 = (2x^2(2x^2 + x + 2) + x^3 + 2)x^4 = \\ &= (x^4 + 2x^3 + x^2 + x^3 + 2)x^4 = (x^4 + x^2 + 2)x^4 = \\ &= (2x^2 + x + 2 + x^2 + 2)x^4 = (x + 1)x^4 = \\ &= (x + 1)(2x^2 + x + 2) = 2x^3 + 2 \pmod{f(x)}. \end{aligned}$$

Так как $x^{16} \neq 1 \pmod{f}$, то n делится на 5, т. е. $s_1 = 1$. Далее, $x^{40} = (x^{20})^2$, где

$$\begin{aligned} x^{20} &= x^{16}x^4 = (2x^3 + 2)(2x^2 + x + 2) = \\ &= x^5 + 2x^4 + x^3 + x^2 + 2x + 1 = \\ &= (2x^3 + x^2 + 2x) + 2(2x^2 + x + 2) + x^3 + x^2 + 2x + 1 = \\ &= (2 + 1)x^3 + (1 + 1 + 1)x^2 + (2 + 2 + 2)x + (1 + 1) = \\ &= 2 \pmod{f(x)}. \end{aligned}$$

Имеем $x^{20} = 2 \neq 1 \pmod f$ и $x^{40} = 2^2 = 1 \pmod f$. Следовательно, n делится на 8 и не делится на 16, т. е. $s_2 = 3$. Таким образом, $\operatorname{ord} f = 5 \cdot 8 = 40$. $\square$

Теперь рассмотрим ряд утверждений, позволяющих находить порядки приводимых многочленов.

Лемма 8.6. *Пусть многочлены $f(x), g(x) \in \mathbb{Z}_p[x]$ взаимно просты. Тогда порядок их произведения равен наименьшему общему кратному их порядков*:

$$\operatorname{ord}(fg) = \operatorname{НОК}\bigl(\operatorname{ord} f, \operatorname{ord} g\bigr).$$

Доказательство. Величина $\operatorname{ord}(f \cdot g)$ равна порядку вычета x в кольце $\mathbb{Z}_p[x]/(f \cdot g)$. Из условия $(f, g) = 1$ по китайской теореме об остатках (теорема 4.17 на с. 127) следует, что это кольцо является прямой суммой:

$$\mathbb{Z}_p[x]/(fg) \cong \mathbb{Z}_p[x]/f \otimes \mathbb{Z}_p[x]/g.$$

В частности, вычет $x \pmod{(fg)}$ представляется парой вычетов $[x, x]_{f,g}$. Следовательно, его порядок в группе обратимых по модулю fg вычетов равен порядку этой пары $[x, x]$ в группе

$$(\mathbb{Z}_p[x]/f \otimes \mathbb{Z}_p[x]/g)^* = (\mathbb{Z}_p[x]/f)^* \times (\mathbb{Z}_p[x]/g)^*,$$

который в свою очередь равен наименьшему общему кратному порядков вычетов $x \pmod f$ и $x \pmod g$ по лемме 3.2. Лемма доказана.

Следствие 8.4. *Пусть $f_1(x), \ldots, f_k(x) \in \mathbb{Z}_p[x]$ и $(f_i, f_j) = 1$ при $i \neq j$. Тогда*

$$\operatorname{ord}(f_1 \cdot \ldots \cdot f_k) = \operatorname{НОК}\bigl(\operatorname{ord} f_1, \ldots, \operatorname{ord} f_k\bigr).$$

Лемма 8.7. *Двучлен $x^a - 1$ делит двучлен $x^b - 1$ тогда и только тогда, когда a делит b. Это справедливо над любым полем.*

Доказательство. Необходимость. Воспользуемся формулой суммы геометрической прогрессии $y^c - 1 = (y-1)(y^{c-1} + \ldots + y + 1)$. Пусть $a \mid b$. Тогда найдется такое c, что $b = ac$, и поэтому

$$x^b - 1 = (x^a)^c - 1 = (x^a - 1)\big(x^{(c-1)a} + x^{(c-2)a} + \ldots + x^{2a} + x^a + 1\big),$$

то есть $x^a - 1 \mid x^b - 1$.

Достаточность. Пусть $x^a - 1 \mid x^b - 1$. Следовательно, $b \geqslant a$. Рассмотрим деление с остатком двучлена $x^b - 1$ на двучлен $x^a - 1$:

$$\begin{aligned} x^b - 1 &= (x^a - 1)x^{b-a} + x^{b-a} - 1 = \\ &= (x^a - 1)(x^{b-a} + x^{b-2a}) + x^{b-2a} - 1 = \\ &= (x^a - 1)(x^{b-a} + x^{b-2a} + x^{b-3a}) + x^{b-3a} - 1 = \ldots = \\ &= (x^a - 1)\Big(\sum_{i=1}^{s} x^{b-i\cdot a}\Big) + x^{b-sa} - 1. \end{aligned}$$

Процесс деления закончится на таком шаге s, что $0 \leqslant b - sa < a$. Из условия $x^a - 1 \mid x^b - 1$ следует, что остаток равен нулю, то есть $x^{b-sa} - 1 = 0$. Отсюда имеем $b - sa = 0$. Значит, $a \mid b$. Лемма доказана.

Лемма 8.8. *Пусть $f(x) \in \mathbb{Z}_p[x]$, $f(0) \neq 0$ и $a \in \mathbb{N}$. Двучлен $x^a - 1$ без остатка делится на многочлен $f(x)$ тогда и только тогда, когда число a делится на его порядок* $\operatorname{ord} f$.

Доказательство. Обозначим $n = \operatorname{ord} f$. Пусть $n \mid a$. Тогда $x^n - 1 \mid x^a - 1$ согласно лемме 8.7. Кроме того, $f \mid x^n - 1$ по определению порядка. Отсюда следует, что $f \mid x^a - 1$.

Теперь предположим, что $f \mid x^a - 1$. Тогда из определения порядка $n = \operatorname{ord} f$ следует, что $n \leqslant a$. Разделим a на n с остатком: $a = qn + r$, где $0 \leqslant r < n$. Двучлен $x^a - 1$ можно тогда представить в виде

$$x^a - 1 = x^{qn+r} - 1 = (x^{qn} - 1)x^r + (x^r - 1).$$

Из последнего равенства с учетом того, что многочлен f делит двучлены $x^a - 1$ и $x^{qn} - 1$, следует, что f делит $x^r - 1$. В случае, когда $r > 0$, это противоречит определению n в силу неравенства $r < n$. Значит, $r = 0$. Лемма доказана.

Отметим, что многочлены f, g в лемме 8.6 и многочлен f в лемме 8.8 могут быть любыми — как приводимыми, так и неприводимыми.

Пример 8.40. Рассмотрим многочлен $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. Ранее было установлено, что $\operatorname{ord} f = 5$. Найдем теперь порядок многочлена f^3.

Пусть $n = \operatorname{ord} f^3$. Так как $x^n - 1$ делится на f^3, а значит и на f, то n делится на 5 по лемме 8.8. Кроме того, так как $x^5 - 1$ делится на f, то многочлен $(x^5 - 1)^4 = x^{20} - 1$ делится на f^4, а значит и на f^3 (здесь мы воспользовались леммой 8.2). Применив лемму 8.8 теперь к многочленам f^3 и $x^{20} - 1$, получим, что n является делителем числа $20 = 2^2 \cdot 5$.

Так как $5 \mid n$ и $n \mid 2^2 \cdot 5$, то искомое n имеет вид $n = 2^k \cdot 5$, где $0 \leqslant k \leqslant 2$. Если $k < 2$, например, $k = 1$, то двучлен $x^{10} - 1 = (x^5 - 1)^2$ должен делиться на f^3. Однако это невозможно в силу неприводимости f: двучлен $x^5 - 1$ делится на f и не делится на f^2. Альтернативный аргумент: многочлен f не имеет кратных корней в поле $\mathbb{F}_{16} = \mathbb{Z}_2[x]/f$, значит кратность каждого корня многочлена f^3 в этом поле равна трем; однако кратность корней двучлена $x^{2^k \cdot 5} - 1 = (x^5 - 1)^{2^k}$ не превосходит 2^k, и поэтому $f^3 \nmid x^{2^k \cdot 5} - 1$ при $k < 2$. Таким образом, $\operatorname{ord} f^3 = 20$. □

Обобщение метода предыдущего примера с многочленов над полем $\mathbb{Z}_2$ на многочлены над $\mathbb{Z}_p$ позволяет получить следующую полезную формулу для порядка такого многочлена, который является степенью неприводимого.

Лемма 8.9. *Пусть $f(x) \in \mathbb{Z}_p[x]$ — неприводимый многочлен, отличный от x, и пусть $m \in \mathbb{N}$. Тогда $\operatorname{ord}(f^m) = p^s \cdot \operatorname{ord}(f)$, где s — наименьшее целое число, удовлетворяющее неравенству $p^s \geqslant m$.*

Доказательство. Обозначим $n = \operatorname{ord} f$ и $N = \operatorname{ord}(f^m)$. Число N делится на n по лемме 8.8, так как $f^m \mid x^N - 1$, а значит и $f \mid x^N - 1$. Далее, двучлен $x^n - 1$ делится на $f(x)$, и потому $(x^n - 1)^m$ делится на $f^m(x)$. А значит, двучлен $(x^n - 1)^{p^s} = x^{np^s} - 1$ также будет делиться на многочлен $f^m(x)$ при условии, что $p^s \geqslant m$.

Положим $s = \lceil \log_p m \rceil$. По лемме 8.8 из того, что f^m делит $x^{np^s} - 1$ получаем, что N делит np^s. В силу того, что $n \mid N$ и $N \mid np^s$, число N имеет вид $N = np^k$, где $0 \leqslant k \leqslant s$. Осталось выяснить, чему равно k.

Рассмотрим теперь фактор-кольцо $\mathbb{F} = \mathbb{Z}_p[x]/f(x)$, которое в силу неприводимости f является полем. Многочлен f имеет столько корней в $\mathbb{F}$, какова его степень, причем кратность каждого его корня равна единице. Заметим, что по следствию 8.2 число $n = \operatorname{ord} f$ не делится на p. Следовательно, двучлен $x^n - 1$ не имеет кратных делителей, как следует из леммы 8.4. Поэтому все его корни из поля $\mathbb{F}$ простые, так же как простыми являются и все корни многочлена f. Более того, так как n делит число $|\mathbb{F}^*|$, то двучлен $x^n - 1$ имеет именно столько корней в поле $\mathbb{F}$, какова его степень, то есть n. Значит, кратность каждого корня многочлена f^m и каждого корня многочлена $(x^n - 1)^m$ в этом поле равна m.

Итак, двучлен $(x^n - 1)^{p^k} = x^{np^k} - 1$ имеет корни кратности p^k. Многочлен f^m делит $x^{np^k} - 1$ и имеет корни кратности m. Сравнивая кратности корней, получаем, что $m \leqslant p^k$. Поэтому $k = s$ и $N = np^s$. Лемма доказана.

В кольце $\mathbb{Z}_p[x]$ всякий многочлен $f(x)$ положительной степени единственным с точностью до порядка множителей образом раскладывается в произведение степеней неприводимых многочленов (см. теорему 4.11, такое разложение по аналогии с разложением целых чисел в произведение степеней простых часто называют каноническим):

$$f(x) = f_1^{m_1}(x) \cdot \ldots \cdot f_k^{m_k}(x). \tag{8.26}$$

Если $f(0) \neq 0$, то в разложении (8.26) отсутствует неприводимый многочлен x. Порядок каждого неприводимого делителя $f_i(x)$ можно найти методом, аналогичным методу из примера 8.39. Зная $\operatorname{ord} f_i$, можно определить $\operatorname{ord} f_i^{m_i}$ по лемме 8.9. Наконец, применяя по индукции к взаимно простым делителям $f_i^{m_i}$ лемму 8.6, получим $\operatorname{ord} f$. Все вместе это дает следующее выражение для порядка произвольного многочлена над полем $\mathbb{Z}_p$.

Теорема 8.12. *Пусть многочлен $f(x) \in \mathbb{Z}_p[x]$ имеет положительную степень и ненулевой свободный член. Рассмотрим его каноническое разложение* (8.26) *в кольце $\mathbb{Z}_p[x]$, где $m_i \in \mathbb{N}$, а $f_1(x), \ldots, f_k(x)$ — различные нормированные неприводимые над $\mathbb{Z}_p$ многочлены, отличные от x. Тогда*

$$\operatorname{ord} f = p^s \cdot \operatorname{НОК}\bigl(\operatorname{ord} f_1, \ldots, \operatorname{ord} f_k\bigr), \tag{8.27}$$

где s — наименьшее целое число, удовлетворяющее неравенству $p^s \geqslant \max(m_1, \ldots, m_k)$.

Пример 8.41. Найдем порядок многочлена

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

В рассмотренных выше примерах было установлено, что

$$\begin{aligned} &\operatorname{ord}(x^2 + x + 1) = 3, \quad \operatorname{ord}(x^4 + x + 1) = 15, \\ &\operatorname{ord}(x^4 + x^3 + x^2 + x + 1) = 5, \\ &\operatorname{ord}(x^4 + x^3 + x^2 + x + 1)^3 = 20. \end{aligned}$$

По теореме 8.12 получаем, что порядок многочлена f равен $\operatorname{НОК}(3, 15, 20) = 2^2 \cdot \operatorname{НОК}(3, 15, 5) = 60$. Отметим, что $\operatorname{ord} f$ не делит число $2^{\deg f} - 1 = 2^{18} - 1$. Это означает, что в общем случае для приводимых многочленов следствие 8.2 не выполняется. □

Пример 8.42. Рассмотрим последовательность $\{a_n\}_{n=0}^{\infty}$ над полем $\mathbb{Z}_3$, заданную линейным рекуррентным равенством

$$a_{n+3} = a_{n+1} + 2a_n, \quad a_n \in \mathbb{Z}_3, \quad n \geqslant 0, \tag{8.28}$$

с начальными условиями $a_0 = a_1 = 0$, $a_2 = 1$. Эта последовательность является периодической, так как при любом фиксированном n тремя ее членами a_n, a_{n+1}, a_{n+2} все последующие ее члены определяются однозначно по формуле (8.28), а число различных наборов (a_n, a_{n+1}, a_{n+2}) над конечным полем конечно. Найдем период последовательности T, для чего рассмотрим последовательность $\boldsymbol{a}_n \in \mathbb{Z}_3[x]/f(x)$ вычетов по модулю $f(x) = x^3 + 2x + 1$, такую, что

$$\boldsymbol{a}_{n+1}(x) = x\boldsymbol{a}_n(x) \pmod{(x^3 + 2x + 1)}.$$

Заметим, что $x^3\boldsymbol{a}(x) = x\boldsymbol{a}(x) + 2\boldsymbol{a}(x) \pmod{(x^3 + 2x + 1)}$ при любом $\boldsymbol{a}(x)$, поэтому $x^3\boldsymbol{a}_n(x) = x\boldsymbol{a}_n(x) + 2\boldsymbol{a}_n(x)$, что равносильно

$$\boldsymbol{a}_{n+3}(x) = \boldsymbol{a}_{n+1}(x) + 2\boldsymbol{a}_n(x).$$

Положив $\boldsymbol{a}_n(x) = b_n x^2 + c_n x + d_n = (b_n, c_n, d_n)$, где $b_n, c_n, d_n \in \mathbb{Z}_3$, перепишем последнее равенство в векторном виде

$$\begin{pmatrix} b_{n+3} \\ c_{n+3} \\ d_{n+3} \end{pmatrix} = \begin{pmatrix} b_{n+1} \\ c_{n+1} \\ d_{n+1} \end{pmatrix} + 2 \begin{pmatrix} b_n \\ c_n \\ d_n \end{pmatrix}.$$

Сравнивая компоненты векторов этого равенства с (8.28), убеждаемся, что $a_n = b_n$ для всех n, если совпадают начальные члены последовательностей $\{a_n\}$ и $\{b_n\}$. Как нетрудно видеть, последнее выполняется при $\boldsymbol{a}_0(x) = 1$. Более того, период последовательности $\{a_n\}$ совпадает с периодом последовательности $\{\boldsymbol{a}_n\}$. В силу того, что $\boldsymbol{a}_n = x^n \pmod{f(x)}$, период последовательности $\{\boldsymbol{a}_n\}$ равен порядку многочлена $f(x)$. В примере 8.1 была доказана его примитивность, поэтому $T = \operatorname{ord} f = 26$.

Многочлен, вектор коэффициентов которого совпадает с вектором коэффициентов линейного рекуррентного уравнения (после перенесения всех его членов в левую часть), называется его *характеристическим* многочленом. Так, многочлен $f(x) = x^3 + 2x + 1$ является характеристическим для уравнения (8.28). Применяя аналогичные рассуждения к уравнению

$$a_{n+4} + a_{n+2} + 2a_{n+1} + a_n = 0 \tag{8.29}$$

с начальными условиями $a_0 = a_1 = a_2 = 0$, $a_3 = 1$ и его характеристическому многочлену $x^4 + x^2 + 2x + 1$ и учитывая, что в примере 8.39 уже был найден его порядок, устанавливаем, что период последовательности (8.29) равен 40. Очевидно, что период линейной рекуррентной последовательности максимален тогда и только тогда, когда ее характеристический многочлен примитивен. □

Порядок многочлена является важным понятием теории циклических помехоустойчивых кодов и теории псевдослучайных

последовательностей над конечным полем. Формула (8.27) сводит вычисление порядка многочлена к его разложению на неприводимые множители. В начале следующей главы будет показано, как это можно сделать достаточно эффективно.

Задачи

8.1. Выяснить, какие из перечисленных колец являются полями: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_7[x]$, $\mathbb{Z}_7[x]/(x+1)$, $\mathbb{Z}_7[x]/(x^2+1)$, множество матриц вида $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ с коэффициентами из $\mathbb{R}$, множество матриц такого же вида, но с коэффициентами из $\mathbb{Z}_5$, $\mathbb{Z}_7$.

8.2. Привести пример бесконечного поля конечной характеристики. (Указание: рассмотреть множество рациональных дробей над конечным полем $\mathbb{F}$.)

8.3. Пусть $\boldsymbol{x}$, $\boldsymbol{y}$ и $\boldsymbol{z}$ — линейно независимые векторы линейного векторного пространства над конечным полем $\mathbb{F}_q$, состоящим из q элементов. Найти все значения q, при которых векторы $\boldsymbol{x}+\boldsymbol{y}$, $\boldsymbol{x}+\boldsymbol{z}$ и $\boldsymbol{y}+\boldsymbol{z}$ будут линейно зависимы.

8.4. Доказать, что неприводимый над полем $GF(q)$ многочлен степени n остается неприводимым над его расширением $GF(q^m)$ тогда и только тогда, когда n и m взаимно просты.

8.5. Пусть многочлен $f(x)$ неприводим над $GF(q)$ и $\deg f = n$. Доказать, что над полем $GF(q^m)$, $m>1$ многочлен $f(x)$ разлагается на (n,m) неприводимых сомножителей одинаковой степени $\frac{n}{(n,m)}$.

8.6. Разложить многочлен $x^{256}+x^{128}+1 \in \mathbb{Z}_2[x]$ на неприводимые множители.

8.7. Определить, является ли многочлен $x^6+x^4+x^2+x+1 \in \mathbb{Z}_2[x]$ примитивным. Найти какой-либо примитивный многочлен степени 7 над полем $\mathbb{Z}_2$.

8.8. Пусть $m,n \in \mathbb{N}$. Найти наибольший общий делитель многочленов $x^{p^m}-x$ и $x^{p^n}-x$.

8.9. Найти наибольший общий делитель двучленов x^a-x и x^b-x, где $a,b \in \mathbb{N}$.

8.10. Построить решетки подполей в полях $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^8}$, $\mathbb{F}_{2^{18}}$, $\mathbb{F}_{2^{30}}$. Сколько элементов каждого такого поля не лежит ни в одном из его подполей? Как связано это число с числом неприводимых многочленов степени $4, 6, 8, 18, 30$ над полем $\mathbb{Z}_2$?

8.11. Описать все конечные поля, решетка подполей которых является деревом.

8.12. Построить таблицы дискретных логарифмов в полях $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9$, $\mathbb{F}_{16}$, $\mathbb{F}_{25}$, $\mathbb{F}_{27}$. Указать все примитивные элементы и подполя. Для всех элементов найти их минимальные многочлены над простыми подполями.

8.13. Найти минимальное поле характеристики 3, в котором многочлен $f(x) \in \mathbb{Z}_3[x]$ раскладывается на линейные множители, если: 1) $f(x) = x^3+x+2$; 2) $f(x) = x^4+2x^3+x+2$; 3) $f(x) = x^5+x^2+2x+1$. В каждом случае указать все корни многочлена $f(x)$ в этом поле и их кратности.

8.14. Выяснить, в каких подполях поля $\mathbb{F}_{2^{12}}$ лежит элемент α^{260}, где α — примитивный элемент поля $\mathbb{F}_{2^{12}}$. Найти степень его минимального многочлена $m_{\alpha^{260}}(x) \in \mathbb{Z}_2[x]$, не вычисляя сам многочлен явно.

8.15. Пусть $\alpha \in \mathbb{F}_{64}$ — корень многочлена $f(x) = x^6 + x^4 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. Найти минимальный многочлен элемента α^{18} разными способами.

8.16. Построить поле $GF(16)$ двумя способами: используя примитивный многочлен степени 4 над полем $GF(2)$ и используя примитивный многочлен степени 2 над полем $GF(4)$. Установить изоморфизм между двумя полученными полями.

8.17. Пусть $\mathbb{F}$ — конечное поле и $\mathbb{F}'$ — подполе в $\mathbb{F}$. Нормированный многочлен $m(x)$ с коэффициентами из $\mathbb{F}'$ называется *минимальным многочленом* элемента $\alpha \in \mathbb{F}$, если $m(\alpha) = 0$ и степень многочлена $m(x)$ минимальна среди всех многочленов положительной степени над $\mathbb{F}'$, для которых α является корнем. Это определение является естественным обобщением понятия минимального многочлена над простым подполем (см. с. 272) на произвольное подполе. Воспользовавшись решением предыдущей задачи, найти минимальные над $GF(4)$ многочлены для всех элементов поля $GF(16)$ и сравнить полученный результат с примерами 8.24, 8.34 и теоремой 8.2.

8.18. Найти порядок многочлена над полем $\mathbb{Z}_2$:
1) $x^2 + x + 1$; 2) $(x^2 + x + 1)^2$; 3) $(x^2 + x + 1)^2(x^4 + x + 1)$.

8.19. Найти количество и степени неприводимых множителей в разложении следующих двучленов над полем $\mathbb{Z}_2$:
1) $x^{21} + 1$; 2) $x^{23} + 1$; 3) $x^{45} + 1$; 4) $x^{63} + 1$; 5) $x^{84} + 1$.
Для каждого из них указать минимальное поле характеристики 2, над которым он разлагается на линейные множители.

8.20. Найти $\sum_{1\leqslant i_1<i_2<i_3\leqslant 125}\alpha_{i_1}\alpha_{i_2}\alpha_{i_3}$, где $\alpha_{i_j}\in GF(5^3)$.

8.21. Пусть p и r — различные простые числа. Доказать, что многочлен $\frac{x^r-1}{x-1}$ раскладывается над $\mathbb{Z}_p$ на различные неприводимые многочлены, каждый из которых имеет степень, равную порядку вычета $p \pmod r$ в группе $\mathbb{Z}_r^*$.

8.22. Пусть α и β — примитивные элементы поля $GF(p^n)$. Будет ли их произведение примитивным элементом?

8.23. Пусть $x^{p^n} = x \bmod f(x)$, где $f(x)$ — многочлен степени n над полем $\mathbb{Z}_p$. Является ли $f(x)$ неприводимым?

8.24. Найти период последовательности $\{a_n\}_{n=0}^{\infty}$ над полем $\mathbb{Z}_3$, если $a_{n+5}+a_{n+4}+a_{n+3}+2a_n=0$, где $a_0=\ldots=a_3=0$, $a_4=1$.

8.25. Пусть k — делитель p^n-1. Многочлен $Q_k(x)=\prod_{\alpha_i}(x-\alpha_i)$, где произведение берется по всем корням k-й степени из единицы в поле $GF(p^n)$, имеющим порядок k, называется *k-круговым* многочленом над $GF(p^n)$. Доказать, что $Q_k(x)\in GF(p)[x]$.

8.26. Доказать, что $x^k-1=\prod_{m|k}Q_m(x)$.

8.27. Доказать, что $Q_k(x)=\prod_{m|k}(x^m-1)^{\mu(k/m)}$.

8.28. Доказать, что $Q_{kp}(x)=Q_k(x^p)$ при всех натуральных k и простых p.

8.29. Доказать, что круговые многочлены $Q_{19}(x)$ и $Q_{27}(x)$ неприводимы над полем $GF(2)$. Совпадают ли они?

8.30. Показать, что многочлен $f(x)$ степени n неприводим над $\mathbb{Z}_p$ тогда и только тогда, когда $f(x)$ делит $x^{p^n}-x$ и при этом взаимно прост с каждым из двучленов вида $x^{p^{n/p_i}}-x$, где p_i — простой делитель числа n (см. пример 8.7).

8.31. Доказать, что элементы $\alpha,\alpha^p,\ldots,\alpha^{p^{n-1}}$ образуют нормальный базис поля $GF(p^n)$ тогда и только тогда, когда многочлены x^n-1 и $\alpha x^{n-1}+\alpha^p x^{n-2}+\ldots+\alpha^{p^{n-2}}x+\alpha^{p^{n-1}}$ взаимно просты.

Глава 9

Алгоритмы

Эта глава является небольшим введением в современные приложения конечной алгебры. В ней рассматриваются примеры алгоритмов, находящих решения алгебраических задач разной природы. Эти задачи условно можно отнести к одному из трех видов. Задачи первого вида естественным образом возникают в самой алгебре, такова задача разложения многочлена на неприводимые множители, и затем появляются в качестве составных частей решений многочисленных прикладных задач. Задачи второго вида лежат на стыке алгебры и ее приложений. Ярким примером такой задачи является задача логарифмирования в конечном поле, которая интересна и как чисто математическая, и как криптографическая задача. Наконец, к третьему виду можно отнести задачи, в которых алгебраические конструкции являются средством для решения практических задач, возникающих за пределами математики. К таким задачам относится задача передачи информации при наличии помех, в основе решения которой лежат коды, исправляющие ошибки.

9.1. Свободные от квадратов многочлены

С помощью алгоритма Берлекемпа можно эффективно раскладывать многочлен на неприводимые множители над небольшим конечным полем. В основе этого метода лежит китайская теорема об остатках для кольца многочленов (см. теорему 4.17 на с. 127) и ее очевидное следствие, которое сформулируем в виде следующей теоремы.

Теорема 9.1. *Пусть p — простое число и*

$$f(x) = f_1^{n_1}(x) \cdot \ldots \cdot f_k^{n_k}(x) \tag{9.1}$$

— разложение многочлена $f(x) \in \mathbb{Z}_p[x]$ в произведение степеней различных многочленов $f_i(x)$, неприводимых над $\mathbb{Z}_p$. Тогда

$$\mathbb{Z}_p[x]/f(x) \cong \mathbb{Z}_p[x]/f_1^{n_1}(x) \otimes \cdots \otimes \mathbb{Z}_p[x]/f_k^{n_k}(x).$$

Нам также потребуется обозначение

$$a = [a_1, \ldots, a_k] = [a_1, \ldots, a_k]_{f_1^{n_1}, \ldots, f_k^{n_k}} \tag{9.2}$$

для системы остатков, представляющей элемент $a(x)$ факторкольца $\mathbb{Z}_p[x]/f(x)$ так, что

$$\left.\begin{array}{c} a(x) = a_1(x) \pmod{f_1^{n_1}(x)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a(x) = a_k(x) \pmod{f_k^{n_k}(x)} \end{array}\right\},$$

введенное нами ранее в разделе 4.8.

Рассмотрим вначале многочлены $f(x)$ одного частного вида, у которых все показатели степеней n_i в разложении (9.1) равны единице. Они называются *свободными от квадратов*. Иными словами, многочлен свободен от квадратов, если квадрат любого его нетривиального делителя не является его делителем.

Итак, предположим, что $f(x) = f_1(x) \cdot \ldots \cdot f_k(x)$, и установим способ нахождения всех неприводимых над $\mathbb{Z}_p$ делителей f_i. Согласно теореме 9.1 и теореме 4.14 (с. 119), в разложении

$$\mathbb{Z}_p[x]/f(x) \cong \mathbb{Z}_p[x]/f_1(x) \otimes \cdots \otimes \mathbb{Z}_p[x]/f_k(x) \tag{9.3}$$

каждое из фактор-колец $\mathbb{Z}_p[x]/f_i$ является полем. Множество вычетов-констант $\{h \in \mathbb{Z}_p[x]/f_i \mid \deg h = 0\}$ является его единственным простым подполем, изоморфным полю $\mathbb{Z}_p$. При доказательстве теоремы 8.6 (с. 270) было отмечено, что элемент поля-расширения лежит в подполе порядка p^m тогда и только тогда, когда он является корнем двучлена $x^{p^m} - x$. Отсюда следует важное наблюдение, что принадлежность вычета h простому подполю поля $\mathbb{Z}_p[x]/f_i$ эквивалентна условию $h^p = h$.

В разложении (9.3) неизвестны и число множителей k, и сами множители f_i. Найдем сначала k. Рассмотрим множество

$$\mathbb{V} = \Big\{\, g \in \mathbb{Z}_p[x]/f \;\Big|\; g = [g_1, \ldots, g_k], \quad \text{где } \deg g_i = 0 \text{ для всех } g_i \in \mathbb{Z}_p[x]/f_i \,\Big\}, \tag{9.4}$$

состоящее из тех многочленов g, остатки которых от деления на *все* неприводимые делители f_i являются константами[1)]. Из свойств представления $g = [g_1, \ldots, g_k]$ (см. с. 127) следует, что множество $\mathbb{V} \subset \mathbb{Z}_p[x]/f$ является линейным векторным пространством размерности k над $\mathbb{Z}_p$ (оно часто называется пространством или алгеброй Берлекемпа):

$$\alpha \in \mathbb{Z}_p, \quad g, \hat{g} \in \mathbb{V} \quad \Rightarrow \quad g + \hat{g} \in \mathbb{V}, \quad \alpha g \in \mathbb{V}, \quad g \cdot \hat{g} \in \mathbb{V}.$$

Кроме того, $\deg g_i = 0$ тогда и только тогда, когда $g_i^p = g_i$. Поэтому система вычетов $[g_1^p, \ldots, g_k^p] = [g_1, \ldots, g_k]$, представляющая g^p в случае, когда $\deg(g \pmod{f_i}) = 0$, одновременно представляет и g. Значит,

$$g \in \mathbb{V} \;\Leftrightarrow\; g^p = g \;\Leftrightarrow\; g^p - g = 0.$$

Пусть $n = \deg f$. Тогда произвольный вычет $g \in \mathbb{Z}_p[x]/f$ имеет вид

$$g(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}, \quad a_i \in \mathbb{Z}_p.$$

Следовательно, в силу леммы 8.2 (см. с. 258) $g^p(x) = g(x^p) = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_{n-1} x^{(n-1)p}$. Приводя подобные слагаемые при неизвестных a_j, получим равносильное условию $g \in \mathbb{V}$ равенство

$$g^p - g = a_0 \cdot 0 + a_1(x^p - x) + a_2(x^{2p} - x^2) + \ldots \\ \ldots + a_{n-1}(x^{(n-1)p} - x^{n-1}) \equiv 0 \pmod{f}. \tag{9.5}$$

[1)] Из того, что все остатки некоторого многочлена при делении на f_i, $i = 1, \ldots, k$ являются константами, не следует, что сам многочлен является константой по модулю f. Это справедливо только в случае, когда все остатки одинаковы.

Обозначим через $r_j(x)$ остаток от деления двучлена $x^{jp} - x^j$ на $f(x)$:

$$r_j(x) = r_{0,j} + r_{1,j}x + \cdots + r_{n-1,j}x^{n-1}, \quad r_{ij} \in \mathbb{Z}_p.$$

Тогда уравнение (9.5) можно переписать как $\sum_{j=0}^{n-1} a_j r_j(x) = 0$, или, перегруппировав члены, в виде

$$\begin{aligned}(a_0 \cdot 0 + a_1 r_{0,1} + a_2 r_{0,2} + \cdots + a_{n-1} r_{0,n-1}) + \\ + x(a_0 \cdot 0 + a_1 r_{1,1} + a_2 r_{1,2} + \cdots + a_{n-1} r_{1,n-1}) + \ldots \\ \ldots + x^i(a_0 \cdot 0 + a_1 r_{i,1} + a_2 r_{i,2} + \cdots + a_{n-1} r_{i,n-1}) + \ldots = 0.\end{aligned}$$

Приравнивая каждый коэффициент многочлена в левой части этого равенства к нулю, получим однородную систему линейных уравнений над $\mathbb{Z}_p$:

$$\begin{pmatrix} 0 & r_{0,1} & r_{0,2} & \ldots & r_{0,n-1} \\ 0 & r_{1,1} & r_{1,2} & \ldots & r_{1,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & r_{n-1,1} & r_{n-1,2} & \ldots & r_{n-1,n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \qquad (9.6)$$

Обозначим ее матрицу размера $n \times n$, состоящую из коэффициентов $r_{i,j}$, через $\mathbf{R}$. Отметим, что матрица $\mathbf{R}$ однозначно определяется многочленом f.

Лемма 9.1. *Число неприводимых делителей k свободного от квадратов многочлена f степени n удовлетворяет равенству*

$$k = n - \operatorname{rank} \mathbf{R},$$

где $\mathbf{R} = \mathbf{R}_{n\times n}$ — матрица, j-й столбец которой является столбцом коэффициентов остатка $r_j(x) = x^{jp} - x^j \pmod{f(x)}$, $j = 0, 1, \ldots, n-1$.

Доказательство. Из определения пространства $\mathbb{V}$ и китайской теоремы об остатках следует, что $k = \dim \mathbb{V}$. Ранее мы убедились, что $g \in \mathbb{V}$ тогда и только тогда, когда $\mathbf{R}\boldsymbol{a} = \mathbf{0}$, где $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ — вектор коэффициентов вычета g. Иначе

говоря, подпространство $\mathbb{V}$ является ортогональным пространством матрицы $\mathbf{R}$. Поэтому k равно размерности пространства решений системы (9.6) и искомое утверждение является тривиальным следствием теоремы 5.3 (с. 146) об образе и ядре линейного оператора. Лемма доказана.

Таким образом, получен еще один способ проверки неприводимости свободного от квадратов многочлена над конечным полем: многочлен неприводим, если его матрица остатков $\mathbf{R}$ имеет ранг $n-1$. Это условие эквивалентно линейной независимости многочленов $r_1, \ldots, r_{n-1}$.

Найти ранг матрицы $\mathbf{R}$ можно, например, методом Гаусса из раздела 6.2. Попутно с рангом метод Гаусса позволяет найти еще и некоторую фундаментальную систему решений (ФСР) однородной системы $\mathbf{R}\boldsymbol{a} = \mathbf{0}$, т. е. базис подпространства $\mathbb{V}$. Покажем, что любую ФСР системы (9.6) можно использовать для разложения $f(x)$ на множители.

Действительно, пусть $k > 1$, а $B = \{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_k\}$ — какой-либо базис в ортогональном пространстве $\mathbb{V}$ матрицы $\mathbf{R}$. Каждый базисный многочлен $\boldsymbol{e}_j = \boldsymbol{e}_j(x)$ имеет два представления. Во-первых,

$$\boldsymbol{e}_j = \sum_{l=0}^{n-1} b_{j,l} x^l = (b_{j,0}, b_{j,1}, \ldots, b_{j,n-1})$$

как вычет кольца $\mathbb{Z}_p[x]/f$, где $b_{j,l} \in \mathbb{Z}_p$ и младшие коэффициенты векторной записи многочлена, как и везде выше в этом разделе, расположены слева. Во-вторых, как элемент прямого произведения (9.3) он представляется также системой остатков

$$\boldsymbol{e}_j = [e_1^j, \ldots, e_k^j] = [e_1^j, \ldots, e_k^j]_{f_1,\ldots,f_k}$$

по неприводимым делителям, где $e_i^j \in \mathbb{Z}_p[x]/f_i$. Первое представление нам известно после решения системы (9.6), второе — нет, как неизвестны и сами f_i. Однако известно, что все остатки e_i^j по каждому модулю f_i имеют нулевую степень, т. е. являются константами из $\mathbb{Z}_p$ в силу того, что $\boldsymbol{e}_j \in \mathbb{V}$.

Заметим также, что вне зависимости от многочлена f первый столбец матрицы $\mathbf{R} = \mathbf{R}(f)$ всегда нулевой. Это означает, что пространство $\mathbb{V}$ обязательно содержит все вычеты нулевой степени из $\mathbb{Z}_p[x]/f$, что следует непосредственно из определения $\mathbb{V}$. Поэтому без ограничения общности рассуждений можно считать, что первый среди найденных методом Гаусса базисных многочленов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ будет единичным:

$$\boldsymbol{e}_1(x) \equiv 1 = (1, 0, 0, \ldots, 0) = [1, 1, \ldots, 1]_{f_1, f_2, \ldots, f_k}.$$

Данное решение (как и любая другая константа кольца $\mathbb{Z}_p[x]/f$, в чем убедимся далее) не дает никаких сведений о делителях f и отбрасывается. Все остальные решения $\boldsymbol{e}_2, \ldots, \boldsymbol{e}_k$ при $k > 1$ линейно независимы с $\boldsymbol{e}_1$ и являются нетривиальными многочленами. Для дальнейшей работы может понадобиться каждый из них.

Пусть $g \in \mathbb{Z}_p[x]/f$ и пусть $g \neq 0$. Тогда $(f, g) \neq f$, так как $\deg g < \deg f$. В силу неприводимости f_i многочлены g и $f = f_1 f_2 \ldots f_k$ могут быть не взаимно просты тогда и только тогда, когда g делится на некоторые из многочленов f_i. Рассмотрим систему остатков многочлена $g = [g_1, \ldots, g_k]_{f_1, \ldots, f_k}$. Получаем, что $(f, g) \neq 1$ тогда и только тогда, когда существует такое i, что $g_i = 0$. В силу $(f, g) \neq f$ должно также существовать такое j, что $g_j \neq 0$. Многочлен g называется в этом случае *f-разлагающим*, так как он позволяет разложить f на множители $d = (f, g)$ и f/d, причем $d \neq 1$ и $f/d \neq 1$. Очевидно, что $d = \prod_{i: g_i = 0} f_i$ и $f/d = \prod_{i: g_i \neq 0} f_i$.

Ключевым является наблюдение, что в $\mathbb{V}$ содержится много f-разлагающих многочленов. Действительно, пусть $a \in \mathbb{Z}_p$. Тогда константе a соответствует вычет $a \in \mathbb{V} \subset \mathbb{Z}_p[x]/f$, который можно представить системой остатков $[a, \ldots, a]_{f_1, \ldots, f_k}$. При различных многочленах $g(x)$ из $\mathbb{Z}_p[x]/f$ неприводимый делитель f_i может делить как $d(x) = (f(x), g(x) - a)$, так и $f(x)/d(x)$. Рассмотрим разность $g(x) - a$ и ее систему остатков:

$$g(x) - a = [g_1, \ldots, g_k] - [a, \ldots, a] = [g_1 - a, \ldots, g_k - a].$$

Если $g \in \mathbb{V}$, то для каждого остатка g_i существует такое $a \in \mathbb{Z}_p$,

зависящее от i, что $g_i = a$. При таком (и только таком) значении a разность $g_i - a$ равна нулю, и, следовательно, многочлен $g(x) - a$ делится на f_i. Поэтому разность $g(x) - a$ является f-разлагающим многочленом при условии, что $g(x) \neq a$. Это заведомо так, например, в случае, когда $g(x) \in B \setminus \{\boldsymbol{e}_1\}$ в силу линейной независимости многочленов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$.

Линейная независимость векторов базиса B оказалась, таким образом, полезным свойством. Следующее утверждение основано на втором свойстве базиса — линейной полноте. Оно показывает, что любые два неприводимых делителя могут быть отделены друг от друга вычислением НОД многочленов $f(x)$ и $\boldsymbol{e}(x) - a$ при подходящем выборе базисного многочлена $\boldsymbol{e}(x)$ и константы a: один из них войдет в НОД, а другой — нет.

Лемма 9.2. *Пусть $i, j \in \{1, \ldots, k\}$, $i \neq j$ — произвольные индексы. Тогда найдется такое s, $2 \leqslant s \leqslant k$, что $e_i^s \neq e_j^s$. Иными словами, фундаментальная система решений B содержит нетривиальный вектор $\boldsymbol{e}_s$, остатки которого по модулю f_i и по модулю f_j различны.*

Доказательство. Докажем лемму от противного. Фиксируем i, j и предположим, что $e_i^s = e_j^s$ для всех $s = 1, \ldots, k$ (базисный вектор $\boldsymbol{e}_1$ также обладает этим свойством). Тогда и остатки любой линейной комбинации $\lambda_1 \boldsymbol{e}_1 + \ldots + \lambda_k \boldsymbol{e}_k$ при делении на f_i и f_j также совпадают. Однако из (9.3) следует, что пространство $\mathbb{V}$ содержит вычеты с разными остатками. Получили противоречие с тем, что $\mathbb{V}$ — линейная оболочка B. Лемма доказана.

Итак, для любых $i \neq j$ найдется хотя бы одно $s = s(i, j)$, такое, что константы $\boldsymbol{e}_s \pmod{f_i}$ и $\boldsymbol{e}_s \pmod{f_j}$ различны. Пусть $\boldsymbol{e}_s = a \pmod{f_i}$, где $a \in \mathbb{Z}_p$. Тогда пара многочленов $f(x)$ и $\boldsymbol{e}_s(x) - a$ имеет нетривиальный общий делитель $d = (f, \boldsymbol{e}_s - a)$, который делится на f_i и не делится на f_j. Возможно, впрочем, что d делится и на некоторый многочлен f_m такой, что $m \neq \neq i, j$, но для пары i, m по доказанному утверждению найдется свой индекс s' и своя константа a'. Следовательно, перебирая константы $a \in \mathbb{Z}_p$ с индексами $s = 2, \ldots, k$ и вычисляя $(f, \boldsymbol{e}_s - a)$,

можно отделить все множители f_i друг от друга. При этом на следующем шаге разложения вместо f удобно использовать его делители d и f/d, найденные ранее.

Резюмируя все сказанное выше, полученный метод нахождения неприводимых множителей можно условно разделить на три этапа (см. рис. 9.1).

Алгоритм Берлекемпа

Вход: свободный от квадратов многочлен $f(x) \in \mathbb{Z}_p[x]$
Выход: список его неприводимых делителей $f_1, \ldots, f_k$

1. Найти матрицу остатков $\mathbf{R} = \mathbf{R}(f)$.
2. Найти базис $B = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k\}$ ортогонального пространства матрицы $\mathbf{R}$.
3. Используя базис B, разложить f на множители вычислением НОД с многочленами $\boldsymbol{e}_s - a$.

Рис. 9.1

Реализация первых двух этапов очевидна и предоставляется читателю в качестве упражнения. Они используют вычисление остатков по модулю f (например, делением «в столбик») и метод Гаусса.

Псевдокод одной из возможных реализаций последнего этапа приведен на рис. 9.2. Поясним работу этой подпрограммы. На каждом ее шаге множество найденных нетривиальных делителей f объединено в список S. Список выбран в качестве основной структуры данных потому, что сложность добавления (или выбрасывания) нового члена списка независима от его длины.

Вначале (строка 1) список делителей S содержит только сам многочлен f. Еще потребуется вспомогательный список S_{tmp} промежуточных делителей текущего шага.

Программа перебирает базисные векторы $\boldsymbol{e}_2, \ldots, \boldsymbol{e}_k$. Фиксируем очередной вектор $\boldsymbol{e}_s$ (строка 2). Пока вспомогательный

Вспомогательная процедура: разложить f с помощью B

Вход: $f \in \mathbb{Z}_p[x]$, базис $B = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k\}$ в $\mathbb{V}$
Вспомогательная память: списки делителей S и S_{tmp}
Выход: $S = \{f_1, \ldots, f_k\}$, где f_i неприводимы, $\prod_{i=1}^{k} f_i = f$

```
1.   S = {f} ;
2.   for( s = 2 ; s ⩽ k ; s++ )
3.   {
4.     S_tmp = S ;
5.     while ( S_tmp ≠ ∅ )
6.     {
7.       F(x) = Очередной множитель(S_tmp) ;
8.       S_tmp = S_tmp \ {F(x)} ;
9.       a = 0 ;
10.       while ( a ⩽ p − 1 )
11.       {
12.         d(x) = НОД(F(x), e_s(x) − a) ;
13.         if( d = 1 ) a++ ;
14.         else
15.           if( d = F ) a = p ;
16.           else
17.           {
18.             S = S \ {F(x)} ;
19.             S = S ∪ {d(x), F(x)/d(x)} ;
20.             if( |S| = k ) return S ;
21.             else
22.             {
23.               a++ ;
24.               F(x) = F(x)/d(x) ;
25.             }
26.           }
27.       }
28.     }
29.   }
```

Рис. 9.2

список ранее найденных нетривиальных делителей f непуст, возьмем очередной делитель F и выбросим его из S_{tmp} (строки 7—8). Начнем перебирать всевозможные константы a из основного поля (цикл в строке 10). Для данных $\boldsymbol{e}_s$, F и a вычислим НОД d многочленов $\boldsymbol{e}_s - a$ и F (строка 12). В зависимости от значения d возможны следующие варианты. Либо $\boldsymbol{e}_s - a$ и F взаимно просты — это означает, что многочлен $\boldsymbol{e}_s - a$ не является F-разлагающим, но, возможно, будет им при другом значении a. Либо $d = F$ — такое возможно, когда все остатки многочлена $\boldsymbol{e}_s$ по модулю всех неприводимых делителей F одинаковы и равны a. В этом случае дальнейший перебор констант a бесполезен («неудачный» $\boldsymbol{e}_s$), и надо перейти к следующему делителю или даже к следующему базисному вектору, если список делителей исчерпан, — возможно, с ним повезет больше. Этой цели служит присваивание $a = p$ в строке 15, которое выводит из цикла строки 10.

Во всех остальных случаях многочлен $\boldsymbol{e}_s - a$ будет F-разлагающим, и мы переходим к строкам 18—24. Здесь мы имеем два нетривиальных делителя d и F/d, которые добавим к списку S, и при этом выбросим F из S. Список S_{tmp} играет роль списка старых делителей, а список S — вновь найденных, причем S_{tmp} обновляется всякий раз при смене вектора базиса. После увеличения списка S необходимо проверить, совпадает ли его длина $|S|$ с k (строка 20). Если да, т. е. число делителей f равно размерности пространства $\mathbb{V}$, то все они различны и неприводимы (лемма 9.1). Следовательно, получен искомый ответ.

Если $|S| < k$, то следует продолжить вычисления со следующего значения a. При этом для всех значений $b > a$ остатки многочлена $\boldsymbol{e}_s - b$ по модулю всех неприводимых делителей F, входящих в d, будут заведомо не равны нулю (но только для данного $\boldsymbol{e}_s$). Поэтому имеет смысл упростить вычисления НОД, понизив степень многочлена F делением на d (строка 24). Здесь мы пользуемся очевидным свойством: остатки многочлена $\boldsymbol{e}_s - b$ по модулю неприводимых делителей многочлена F/d совпадают с остатками по модулю тех неприводимых делителей F, которые не входят в d, но входят в F/d.

Таким образом, данная подпрограмма всегда заканчивает свою работу и выходит из цикла в строке 20. Ее корректность следует из леммы 9.2. По ее окончании список S содержит все неприводимые делители многочлена f.

Пример 9.1. Многочлен $f(x) = x^7+x^6+2x^5+x^4+2x^2+2x+2$ с коэффициентами из поля $\mathbb{Z}_3$ разложим в произведение неприводимых над этим полем многочленов. При помощи алгоритма Евклида нетрудно убедиться, что многочлен $f(x)$ взаимно прост со своей производной $f'(x) = x^6+x^4+x^3+x+2$, и следовательно, свободен от квадратов.

Поэтому для разложения $f(x)$ на неприводимые множители можно воспользоваться изложенным выше алгоритмом Берлекемпа. В соответствии с этим алгоритмом сначала найдем многочлены $r_j(x)$:

$$\begin{aligned}
&r_0(x) \equiv 0;\\
&r_1(x) = x^3 - x \quad = \texttt{0001020} \pmod f,\\
&r_2(x) = x^6 - x^2 \;= \texttt{1000200} \pmod f,\\
&r_3(x) = x^9 - x^3 \;= \texttt{2022212} \pmod f,\\
&r_4(x) = x^{12} - x^4 = \texttt{2122010} \pmod f,\\
&r_5(x) = x^{15} - x^5 = \texttt{2001120} \pmod f,\\
&r_6(x) = x^{18} - x^6 = \texttt{0211120} \pmod f.
\end{aligned}$$

При этом удобно использовать вспомогательный многочлен $y(x)$ для вычета x^{jp} по модулю f и вычислять $x^{(j+1)p} = x^{jp} \cdot x^p$ как $y(x) \cdot x^p$ по модулю f. Из коэффициентов $r_{i,j}$ найденных многочленов составим матрицу

$$\mathbf{R} = \begin{pmatrix}
0 & 0 & 1 & 2 & 2 & 2 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 2\\
0 & 0 & 0 & 2 & 2 & 0 & 1\\
0 & 1 & 0 & 2 & 2 & 1 & 1\\
0 & 0 & 2 & 2 & 0 & 1 & 1\\
0 & 2 & 0 & 1 & 1 & 2 & 2\\
0 & 0 & 0 & 2 & 0 & 0 & 0
\end{pmatrix}$$

и найдем базис ее ортогонального пространства. Для этого элементарными преобразованиями строк преобразуем ее в матрицу

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 \end{pmatrix},$$

которая перестановочно эквивалентна систематической. Последняя матрица имеет полный ранг, поэтому $\operatorname{rank}\mathbf{R} = 4$ и $k = n - \operatorname{rank}\mathbf{R} = 7 - 4 = 3$. Следовательно, исходный многочлен $f(x)$ разлагается в произведение трех различных неприводимых над $\mathbb{Z}_3$ многочленов. Воспользовавшись последней матрицей, находим также базис B в $\mathbb{V} = \operatorname{Ker}\mathbf{R}$:

$$\texttt{1000000}, \quad \texttt{0210010}, \quad \texttt{0010101}.$$

Для дальнейшей работы (деление многочленов с остатком) коэффициенты этих векторов удобнее переписать в обратном порядке, чтобы старшие разряды оказались слева:

$$\begin{aligned} \boldsymbol{e}_1 &= \texttt{0000001} \equiv 1, \\ \boldsymbol{e}_2 &= \texttt{0100120} = x^5 + x^2 + 2x, \\ \boldsymbol{e}_3 &= \texttt{1010100} = x^6 + x^4 + x^2. \end{aligned}$$

Найдя базис $B = \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ в $\mathbb{V}$, переходим к финальной стадии алгоритма. Список делителей многочлена f вначале положим состоящим только из него самого, т. е. $S = \{f\}$. Будем вычислять наибольшие общие делители f и $\boldsymbol{e}_i - a$ для всех $a \in \mathbb{Z}_3$ и всех базисных многочленов $\boldsymbol{e}_i$, начиная со второго. Имеем $a = 0$ и $(f, \boldsymbol{e}_2) = 1$. Но уже на следующем шаге, при $a = 1$, получаем общий делитель $d = (f, \boldsymbol{e}_2 - 1) = x^2 + x + 2 = \texttt{112}$, откуда $f/d = \texttt{100121}$ и $S = \{F_1, F_2\}$, где $F_1(x) = x^2 + x + 2$, $F_2(x) = x^5 + x^2 + 2x + 1$ — нетривиальный список делителей многочлена $f(x)$. Число делителей $|S|$ пока еще меньше k, поэтому продолжаем вычисления.

Так как $(F_1, \boldsymbol{e}_2 - 2)$ и $(F_2, \boldsymbol{e}_2 - 2)$ тривиальны, то переходим к следующему, последнему базисному вектору $\boldsymbol{e}_3$. Вычисляя наибольшие общие делители $\boldsymbol{e}_3 - a$ с очередным членом списка S,

имеем $(F_1, \boldsymbol{e}_3) = (F_2, \boldsymbol{e}_3) = 1$, но $(F_2, \boldsymbol{e}_3 - 1) = x^3 + 2x + 1$, $F_2/(F_2, \boldsymbol{e}_3 - 1) = x^2 + 1$. После этого шага список делителей f содержит многочлены $x^2 + x + 2$, $x^2 + 1$ и $x^3 + 2x + 1$. Сравнивая их количество с найденным ранее числом делителей $k = 3$, убеждаемся, что получен окончательный ответ:

$$f(x) = (x^2 + x + 2)(x^2 + 1)(x^3 + 2x + 1)$$

или $\mathtt{11210222} = \mathtt{112} \cdot \mathtt{101} \cdot \mathtt{1021}$ в векторной записи. Нетрудно проверить, что каждый из найденных множителей неприводим. □

Замечание 9.1. Сложность последней части алгоритма существенно зависит от найденного базиса. Базис в свою очередь зависит от способа решения системы $\mathbf{R}\boldsymbol{a} = \mathbf{0}$. Так, в нашем примере, как нетрудно убедиться, мы получили $\boldsymbol{e}_2 = [1, 2, 2]_{f_1, f_2, f_3}$ и $\boldsymbol{e}_3 = [2, 2, 1]_{f_1, f_2, f_3}$, где $f_1 = \mathtt{112}$, $f_2 = \mathtt{101}$, $f_3 = \mathtt{1021}$. «Китайские» векторные представления $[1, 2, 2]$ и $[2, 2, 1]$ содержат много совпадающих координат и совсем не содержат нулей, поэтому нами было произведено достаточно много вычитаний и делений. При другой последовательности элементарных преобразований строк матрицы $\mathbf{R}$ можно было получить, например, базис $\boldsymbol{e}'_2 = [0, 1, 2]$, $\boldsymbol{e}'_3 = [0, 1, 0]$. В этом базисе уже первые три шага алгоритма $(f, \boldsymbol{e}'_2) = f_1$, $(f, \boldsymbol{e}'_2 - 1) = f_2$, $(f, \boldsymbol{e}'_2 - 2) = f_3$ дадут полное разложение, и другой базисный вектор даже не потребуется.

Лемма 9.3. *Сложность предложенного алгоритма разложения свободного от квадратов многочлена над $\mathbb{Z}_p$ на неприводимые множители составляет $\mathcal{O}(n^3 + pkn^2)$ арифметических операций в поле $\mathbb{Z}_p$.*

Доказательство. На первом шаге (см. рис. 9.1) требуется вычислить $n-1$ остатков по модулю многочлена степени n. Если вычисления проводить независимо делением в столбик, то на это потребуется $(n-1) \cdot \mathcal{O}(n^2) = \mathcal{O}(n^3)$ операций, хотя возможны и другие способы[1)]. Решение однородной системы с нахождением

[1)] См. [23, 29, 30].

базиса на втором шаге также имеет сложность $\mathcal{O}(n^3)$, если применить метод Гаусса. Наконец, в худшем случае на последнем шаге мы переберем все $k-1$ нетривиальных базисных векторов $\boldsymbol{e}_s$ и для каждого из них все p констант a из поля $\mathbb{Z}_p$ (рис. 9.2). Для каждой из $(k-1)p$ таких пар $(\boldsymbol{e}_s, a)$ состоится менее k вычислений НОД с делителями $F(x)$, причем $\sum_{F\in S} \deg F(x) = n$. Сложность этого равна $\mathcal{O}(n^2)$, откуда получаем искомое. Вычислительные эксперименты[1)] показывают, что в среднем $k \approx \log n$. Из-за перебора констант $a \in \mathbb{Z}_p$ на третьем шаге алгоритм будет эффективен лишь для сравнительно небольших значений p, т. е. только для небольших полей. Лемма доказана.

9.2. Алгоритм Берлекемпа. Общий случай

Осталось выяснить, что делать с несвободным от квадратов многочленом. В этом разделе мы покажем, как нахождение разложения многочлена

$$f(x) = f_1^{n_1}(x) \cdot \ldots \cdot f_k^{n_k}(x) \tag{9.7}$$

сводится к нахождению разложения некоторого многочлена, не имеющего кратных неприводимых множителей.

Пусть $a(x) \mid b(x)$. Под кратностью делителя $a(x)$ будем понимать такое натуральное число r, что $a^r \mid b$ и $a^{r+1} \nmid b$.

Лемма 9.4. *Пусть $h(x)$ — неприводимый делитель многочлена $f(x) \in \mathbb{Z}_p[x]$, имеющий кратность $r > 0$ в разложении (9.7). Тогда кратность $h(x)$ как делителя НОД $f(x)$ и его производной $f'(x)$ равна $r-1$ в случае, когда $p \nmid r$, и равна r, когда $p \mid r$.*

Доказательство. Если r — кратность h как делителя многочлена f, то $f = h^r \cdot g$ и $(g, h) = 1$. Тогда

$$f' = rh^{r-1}g + h^r g' = h^{r-1}(rg + hg'),$$

откуда $h^{r-1} \mid f'$.

[1)] См. [16].

Первый случай. Если $p \mid r$, то $rg \equiv 0$ и $f' = h^r g'$. Поэтому h^r делит (f, f'), а h^{r+1} не делит (f, f'), так как не делит f. Отметим, что, вообще говоря, кратность h как делителя f' может оказаться больше его кратности как делителя f.

Второй случай. Если $p \nmid r$, то $rg \neq 0$ и $h \nmid rg$. Поэтому $h \nmid (rg + hg')$, и, следовательно, h^r не делит f', откуда $h^r \nmid (f, f')$. Лемма доказана.

Пусть $A = \{i \mid p \text{ делит } n_i\}$ — множества номеров тех неприводимых делителей $f_i(x)$, кратности которых в разложении (9.7) делятся на p, $B = \{i \mid p \text{ не делит } n_i\}$ — множества номеров тех неприводимых делителей $f_i(x)$, кратности которых в разложении (9.7) не делятся на p. Положим

$$a(x) = \prod_{i \in A} f_i^{n_i}(x), \quad b(x) = \prod_{i \in B} f_i^{n_i}(x).$$

Тогда $f(x) = a(x)b(x)$. Так как степени всех неприводимых делителей $a(x)$ кратны p, то $a(x) = (g(x))^p = g(x^p)$, где $g(x) \in \mathbb{Z}_p[x]$. Значит, $a'(x) = 0$, откуда

$$f'(x) = (a(x) \cdot b(x))' = a'(x)b(x) + a(x)b'(x) = a(x)b'(x).$$

Если $f'(x) = 0$, то $B = \varnothing$ и $f(x) = a(x)$. В этом случае задача разложения многочлена $f(x) = (g(x))^p$ сводится к нахождению разложения многочлена $g(x)$, имеющего меньшую степень.

Если $f'(x) \neq 0$, то из леммы 9.4 следует, что

$$(f, f') = (ab, ab') = a(b, b') = a(x) \cdot \prod_{i \in B} f_i^{n_i - 1}(x).$$

Поэтому многочлен $\frac{f}{(f', f)} = \prod_{i \in B} f_i(x)$ свободен от квадратов, и к нему можно применить метод разложения на множители из предыдущего раздела. Это позволит найти неприводимые делители $f_i(x)$ для всех $i \in B$. После этого их кратности n_i можно определить пробными делениями, и в результате мы получим многочлен $b(x)$. По частному $a(x) = f(x)/b(x)$ легко находится такой многочлен $g(x)$, что $a(x) = g(x^p)$. Если $g(x)$ отличен

от константы, то, применив к нему и его производной предыдущие рассуждения, по индукции получим все неприводимые делители $f_i(x)$, $i \in A$. Кратность каждого такого делителя многочлена $g(x)$ умножим на p и получим его кратность как делителя $f(x)$. С учетом уже найденного разложения многочлена $b(x)$ это даст нам искомое представление (9.7) целиком.

Факторизация многочлена

(рекурсивный алгоритм Берлекемпа)

Вход: $f \in \mathbb{Z}_p[x]$

Выход: (S, N), где $S = \{f_1, \ldots, f_k\}$, $N = \{n_1, \ldots, n_k\}$, где $f_1^{n_1} \ldots f_k^{n_k} = f$

1. $S = \{f_1, \ldots f_m\} =$ ДелителиСвобОтКв $\big(f/(f, f')\big)$;
2. for($j = 1$; $j \leqslant m$; j++)
3. { $n_j = 1$;
4. while ($f_j^{n_j+1} \mid f$) n_j++ ; }
5. $N = \{n_1, \ldots, n_m\}$; $S' = \varnothing$; $N' = \varnothing$;
6. $g = \Big(f/(f_1^{n_1} \ldots f_m^{n_m})\Big)^{1/p}$;
7. if ($\deg g > 0$) then
8. $(S', N') =$ Факторизация многочлена (g) ;
9. return $(S \cup S', N \cup p \cdot N')$;

Рис. 9.3

На рис. 9.3 представлена схема этого рекурсивного алгоритма. Результатом его работы с произвольным многочленом f над $\mathbb{Z}_p$ будет список S всех неприводимых делителей f и список их кратностей N.

Теорема 9.2. *Алгоритм Берлекемпа* (*рис.* 9.3) *работает корректно и находит полное разложение произвольного многочлена $f(x) \in \mathbb{Z}_p[x]$ на множители.*

Доказательство. Вначале (строка 1) вычисляется производная f', наибольший общий делитель (f, f') и частное $f/(f, f')$.

К свободному от квадратов многочлену $f/(f,f')$ применяется описанный выше метод разложения на множители (см. рис. 9.1). Если $f'=0$, то $f/(f,f')=1$, $S=N=\varnothing$, $m=0$ и можно сразу переходить к строке 7 при $g(x)=\big(f(x)\big)^{1/p}$. В строках 2—4 пробным делением f вычисляются кратности его неприводимых делителей. В строке 6 не требуется извлечение корня степени p, так как коэффициенты многочлена $g(x)$ содержатся среди коэффициентов многочлена $a(x)=f/(f_1^{n_1}\dots f_m^{n_m})$. Строка 8 содержит рекурсивный вызов процедуры поиска неприводимых делителей и их кратностей у многочлена $g(x)$. Ответом являются объединения списков делителей и списков кратностей, при этом каждый элемент списка N' надо умножить на p.

Таким образом, искомое утверждение следует из корректности процедуры разложения свободного от квадратов многочлена, т. е. из лемм 9.1 и 9.2. Теорема доказана.

Замечание 9.2. Лемма 9.3 показывает, что при небольших p алгоритм Берлекемпа полиномиален. Таким образом, кольцо целых чисел и кольцо многочленов над малым конечным полем имеют фундаментальное различие: многочлены можно сравнительно легко разлагать на множители, в то время как для целых чисел никаких полиномиальных алгоритмов разложения неизвестно до сих пор, хотя детерминированный полиномиальный способ проверки простоты числа недавно был обнаружен[1)].

Пример 9.2. Применим рекурсивный алгоритм Берлекемпа к разложению над полем $\mathbb{Z}_3$ многочлена

$$\begin{aligned} f(x) &= x^{17}+2x^{16}+2x^{15}+2x^{14}+\\ &\qquad +x^{12}+2x^{11}+x^9+2x^7+x^4+x^2+x+2=\\ &= \texttt{122201201020010112}. \end{aligned}$$

Так как $f'(x)=2x^{16}+2x^{15}+x^{13}+x^{10}+2x^6+x^3+2x+1$ и

$$\begin{aligned} (f,f') &= \texttt{101101101202101}=\\ &= x^{14}+x^{12}+x^{11}+x^9+x^8+x^6+2x^5+2x^3+x^2+1, \end{aligned}$$

[1)] См., например, [9].

то

$$\frac{f}{(f,f')} = \mathtt{1212} = x^3 + 2x^2 + x + 2.$$

Раскладывая последний (заведомо свободный от квадратов) многочлен на неприводимые множители, получаем $x^3+2x^2+x+2 = (x+2)(x^2+1)$. Найдем кратность $x+2$ и x^2+1 как делителей многочлена f. Для двучлена $x+2 = x-1$ удобно воспользоваться схемой Горнера (в конце очередной строки остаток от деления на этот двучлен выделен жирным шрифтом):

	1	2	2	2	0	1	2	0	1	0	2	0	0	1	0	1	1	2
1	1	0	2	1	1	2	1	1	2	2	1	1	1	2	2	0	1	**0**
1	1	1	0	1	2	1	2	0	2	1	2	0	1	0	2	2	**0**	
1	1	2	2	0	2	0	2	2	1	2	1	1	2	2	1	**0**		
1	1	0	2	2	1	1	0	2	0	2	0	1	0	2	**0**			
1	1	1	0	2	0	1	1	0	0	2	2	0	0	**2**				

Из этой таблицы следует, что искомая кратность равна 4 и что

$$\frac{f(x)}{(x+2)^4} = \mathtt{10221102020102} = \\ = x^{13} + 2x^{11} + 2x^{10} + x^9 + x^8 + 2x^6 + 2x^4 + x^2 + 2.$$

Делением последнего многочлена на x^2+1 убеждаемся, что его кратность равна двум, и получаем многочлен

$$\frac{f(x)}{(x+2)^4(x^2+1)^2} = \mathtt{1002000002} = x^9 + 2x^6 + 2.$$

Его производная равна нулю, поэтому он является полным кубом:

$$\frac{f(x)}{(x+2)^4(x^2+1)^2} = (x^3 + 2x^2 + 2)^3.$$

Разлагая стоящее в скобках выражение на множители, получим $x^3 + 2x^2 + 2 = (x+1)(x^2+x+2)$. Отсюда окончательно имеем

$$f(x) = (x^2+1)^2(x+1)^3(x^2+x+2)^3(x+2)^4. \qquad \square$$

Замечание 9.3. Данный пример приведен исключительно для иллюстрации алгоритма разложения на множители. На практике все делители небольшой степени проще находить схемой Горнера и пробным делением на многочлены из таблицы неприводимых многочленов. Минимальная степень, начиная с которой алгоритм Берлекемпа становится выгоднее полного перебора неприводимых делителей, зависит от его реализации. Эта тема выходит за рамки данного курса, интересующийся вопросами оптимизации читатель найдет все необходимое в энциклопедических библиографиях книг, приведенных в списке литературы[1)].

9.3. Логарифмирование. Метод согласования

Пусть α — примитивный элемент поля $\mathbb{F}_q$, $q = p^n$, и β — ненулевой элемент этого поля. Теорема 8.1 показывает, что уравнение

$$\alpha^x = \beta \tag{9.8}$$

имеет решение при всех таких α, β. Напомним, что минимальное неотрицательное решение уравнения (9.8) называется *индексом*, или *дискретным логарифмом* элемента β по основанию α, и обозначается $\log_\alpha \beta$. Такой x фактически является вычетом из $\mathbb{Z}_{q-1}$. Задача нахождения $\log_\alpha \beta$ называется задачей дискретного логарифмирования в поле $\mathbb{F}_q$.

В полях действительных и комплексных чисел известны многочисленные эффективные способы вычисления логарифмов по произвольному основанию, базирующиеся в основном на методе последовательных приближений (деление отрезка, метод Ньютона, разложение специальных функций в ряды и т.п.). Они позволяют вычислить логарифм с любой наперед заданной точностью и небольшим числом операций в поле. В случае конечного поля ситуация принципиально иная. Метод последовательных приближений неприменим в нем из-за отсутствия аксиомы Архимеда и невозможности определить антисимметричное, тран-

[1)] См., например, [7, 20, 30].

зитивное и связное бинарное отношение, согласованное с какой-нибудь операцией. Несмотря на многолетние усилия многих специалистов, полиномиальные алгоритмы для задачи дискретного логарифмирования до сих пор неизвестны. Это привело к широкому использованию функции α^x в различных криптографических протоколах и схемах.

Тем не менее известно немало методов, позволяющих найти $\log_\alpha \beta$ значительно быстрее, чем полным перебором. Наиболее сильные из них, основанные на решете числового поля, имеют субэкспоненциальную сложность, но требуют глубокой подготовки в области аналитической теории чисел и выходят за рамки данного курса[1)]. Здесь мы изложим только два особенно простых для реализации метода.

Первый алгоритм называется *методом согласования*. Рассмотрим решение x уравнения (9.8) как целое неотрицательное число, меньшее $q-1$. Положим $a = \lceil \sqrt{q-1} \rceil$ и рассмотрим две последовательности элементов поля $\mathbb{F}_q$:

$$A = \left\{ \alpha^{ai} \;\middle|\; 0 \leqslant i < a \right\} \quad \text{и} \quad B = \left\{ \beta \cdot \alpha^{-j} \;\middle|\; 0 \leqslant j < a \right\}.$$

Лемма 9.5. *Множества A и B имеют непустое пересечение.*

Доказательство. Равенство $\alpha^x = \beta$ выполнено при некотором x, где $0 \leqslant x < q-1$. Любое число x из промежутка $0 \leqslant x < q-1$, разделив с остатком на a, можно представить в виде

$$x = ai + j, \tag{9.9}$$

где $0 \leqslant i, j < a$. Это следует из того, что $a^2 = \lceil \sqrt{q-1} \rceil^2 \geqslant q-1$. Из (9.9) имеем

$$\alpha^{ai+j} = \beta,$$

откуда $(\alpha^a)^i = \beta\alpha^{-j}$. Отметим, что по теореме о делении целых чисел с остатком представление $x \leftrightarrow (i, j)$ однозначно. Лемма доказана.

[1)] Обзор таких методов можно найти в [9].

С практической точки зрения положительные степени α удобнее для расчетов, чем отрицательные. Поэтому от представления (9.9) перейдем к представлению $x = ai' - j'$ с помощью биекции $i' = i + 1$, $j' = a - j$. Отсюда $(\alpha^a)^{i'} = \beta\alpha^{j'}$, а значит и пересечение множеств

$$A' = \{\alpha^{ai'} \mid 1 \leqslant i' \leqslant a\} \quad \text{и} \quad B' = \{\beta \cdot \alpha^{j'} \mid 1 \leqslant j' \leqslant a\}$$

также непусто. Резюмируя сказанное, получаем следующий алгоритм (см. рис. 9.4).

Алгоритм согласования

Вход: $\alpha, \beta \in \mathbb{F}_q$
Выход: $x \in \mathbb{Z}_{q-1}$, где $\alpha^x = \beta$

1. Присвоить $a = \lceil \sqrt{q-1} \rceil$ и найти α^a
2. Составить таблицу $A' = \{(i, \alpha^{ai}) : 1 \leqslant i \leqslant a\}$
3. Отсортировать A' по ключу α^{ai}
4. for($j = 1$; $j \leqslant a$; j++) if($\beta\alpha^j = \alpha^{ai}$) break;
5. return $x = ai - j \pmod{q-1}$;

Рис. 9.4

Лемма 9.6. *Сложность метода согласования не превосходит* $\mathcal{O}(\sqrt{q}\log q)$.

Доказательство. Таблица A' шага 2 имеет размер $\mathcal{O}(\sqrt{q})$. Все степени α^{ai} элемента α^a можно последовательно вычислить за a умножений в поле $\mathbb{F}_q$, используя равенство $\alpha^{a(i+1)} = \alpha^{ai} \cdot \alpha^a$. Поэтому общая сложность шагов инициализации не превосходит по порядку величины $\sqrt{q}$.

На шаге 3 применяется алгоритм быстрой сортировки массива A' длины a со сложностью $\mathcal{O}(a \log a)$. На шаге 4 мы перебираем элементы последовательности B', проверяя, входит ли очередной элемент в A'. Поиск элемента в упорядоченном массиве

длины a требует по порядку не более $\log a$ операций (в отличие от a операций в неупорядоченном). В худшем случае потребуется a попыток, поэтому общая сложность есть $\mathcal{O}(a \log a) = = \mathcal{O}(\sqrt{q} \log q)$. Шаг 4 может быть заменен построением и сортировкой таблицы B' с последующим поиском коллизий в ней и A'.

Таким образом, наиболее ресурсоемкими частями метода являются сортировка и поиск (при использовании медленных алгоритмов сортировки, например пузырьковой сортировки, метод согласования может оказаться даже хуже полного перебора). Объем дополнительной памяти, требуемой алгоритму, не превышает $\mathcal{O}(\sqrt{q})$ элементов поля $\mathbb{F}_q$. Лемма доказана.

Метод согласования был предложен советским математиком А. О. Гельфондом в 1962 г. В зарубежной литературе он более известен как метод Шенкса.

Пример 9.3. Рассмотрим поле $\mathbb{F}_{81} = \mathbb{Z}_3[x]/(x^4 + x + 2)$. Корень α многочлена $f(x) = x^4 + x + 2$ является его примитивным элементом. Для элементов поля будем, как обычно, использовать следующие обозначения:

$$a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = [a_3x^3 + a_2x^2 + a_1 + a_0]_{f(x)} = (\mathtt{a_3a_2a_1a_0}),$$

где $a_i \in \mathbb{Z}_3$, опуская иногда лишние скобки.

Найдем логарифм элемента $\beta = 2\alpha^2 + 1 = \mathtt{0201}$ методом согласования.

Имеем $a = \lceil\sqrt{80}\rceil = 9$ и $\alpha^9 = \alpha^3 + \alpha^2 + \alpha = \mathtt{1110}$. Здесь и далее при вычислении степеней применяется модификация бинарного алгоритма и тождество $\alpha^4 = 2\alpha + 1 = \mathtt{0021}$. Составим таблицу A':

$$\begin{aligned}
\alpha^9 &= \mathtt{1110},\\
\alpha^{18} &= \mathtt{1110} \cdot \mathtt{1110} = \mathtt{1020},\\
\alpha^{27} &= \mathtt{1020} \cdot \mathtt{1110} = \mathtt{1210},\\
\alpha^{36} &= \mathtt{1210} \cdot \mathtt{1110} = \mathtt{2221},\\
\alpha^{45} &= \mathtt{2221} \cdot \mathtt{1110} = \mathtt{0120},
\end{aligned}$$

$$\alpha^{54} = \mathtt{0120} \cdot \mathtt{1110} = \mathtt{0110},$$
$$\alpha^{63} = \mathtt{0110} \cdot \mathtt{1110} = \mathtt{2022},$$
$$\alpha^{72} = \mathtt{2022} \cdot \mathtt{1110} = \mathtt{2101},$$
$$\alpha^{81} = \alpha = \mathtt{0010}.$$

При этом использовались полезные тождества $\alpha^5 = 2\alpha^2 + \alpha = \mathtt{0210}$ и $\alpha^6 = 2\alpha^3 + \alpha^2 = \mathtt{2100}$. После лексикографической сортировки по второму столбцу получаем модифицированную таблицу A':

α^9	1110
α^{18}	1020
α^{27}	1210
α^{36}	2221
α^{45}	0120
α^{54}	0110
α^{63}	2022
α^{72}	2101
α^{81}	0010

$\rightarrow$

α^{81}	0010
α^{54}	0110
α^{45}	0120
α^{18}	1020
α^9	1110
α^{27}	1210
α^{63}	2022
α^{72}	2101
α^{36}	2221

.

Перейдем к вычислению элементов последовательности $B' = \{\beta \cdot \alpha^j\}$. Вначале убеждаемся, что $\beta = \mathtt{0201} \notin A'$, поэтому значение $j = a$ не подходит. При $j = 1$ получаем $\beta \cdot \alpha = \mathtt{0201} \times \mathtt{0010} = \mathtt{2010} \notin A'$. При $j = 2$ нас также ждет неудача, ибо $\beta \cdot \alpha^2 = (\beta\alpha)\alpha = \mathtt{2010} \cdot \mathtt{0010} = \mathtt{0112} \notin A'$. Далее продолжаем аналогично:

$$\beta \cdot \alpha^3 = \mathtt{0112} \cdot \mathtt{0010} = \mathtt{1120} \notin A',$$
$$\beta \cdot \alpha^4 = \mathtt{1120} \cdot \mathtt{0010} = \mathtt{1221} \notin A',$$
$$\beta \cdot \alpha^5 = \mathtt{1221} \cdot \mathtt{0010} = \mathtt{2201} \notin A',$$
$$\beta \cdot \alpha^6 = \mathtt{2201} \cdot \mathtt{0010} = \mathtt{2022} \in A'.$$

Получили совпадение: $\beta\alpha^6 = \alpha^{63}$. Отсюда $\beta = \alpha^{63-6} = \alpha^{57}$, значит, искомый логарифм $\log_\alpha \beta = \log_\alpha(2\alpha^2 + 1)$ равен 57. $\square$

9.4. Метод Полига — Хеллмана — Нечаева

Снова рассмотрим уравнение (9.8) в поле $\mathbb{F}_q$. Допустим, что $q-1 = p^k n$, где $(p,n) = 1$. Так как p делит $q-1$, то элемент $\gamma = \alpha^{(q-1)/p}$ порождает подгруппу

$$C = C(p) = \{1, \gamma, \gamma^2, \ldots, \gamma^{p-1}\} = \langle\gamma\rangle,$$

— множество решений уравнения $x^p = 1$ в поле $\mathbb{F}_q$. Если p невелико и элемент x содержится в C, то показатель $z \in \mathbb{Z}_p$, для которого выполняется $x = \gamma^z$, легко может быть найден, например, с помощью перебора или поиска в таблице C. На этом свойстве и основан наш следующий алгоритм.

Представим решение уравнения (9.8), взятое по модулю p^k, в виде

$$x = \log_\alpha \beta = x_0 + x_1 p + \ldots + x_{k-1} p^{k-1} \pmod{p^k}, \qquad (9.10)$$

где $x_i \in \mathbb{Z}_p$. Такое представление однозначно, так как фактически является записью остатка целого числа x, взятого по модулю p^k, в позиционной системе счисления с основанием p.

Разряды x_i представления (9.10) можно последовательно определить, сочетая возведение обеих частей уравнения $\alpha^x = \beta$ в подходящую степень с поиском логарифма в сравнительно малой подгруппе $C(p)$. Действительно, заметим, что в силу равенства $\alpha^{np^k} = 1$

$$(\alpha^x)^{np^{k-1}} = \alpha^{(x_0 + x_1 p + \ldots + x_{k-1}p^{k-1})\cdot np^{k-1}} = (\alpha^{x_0})^{np^{k-1}}.$$

Отсюда, вспоминая, что $\alpha^x = \beta$, получаем уравнение

$$\beta^{np^{k-1}} = \left(\alpha^{np^{k-1}}\right)^{x_0},$$

решение которого x_0 находим перебором $x_0 = 0, 1, \ldots, p-1$ или с помощью таблицы логарифмов группы $C(p) = \langle\alpha^{(q-1)/p}\rangle$.

Далее, $(\alpha^{x-x_0})^{np^{k-2}} = \alpha^{x_1 np^{k-1}}$, откуда

$$\left(\frac{\beta}{\alpha^{x_0}}\right)^{np^{k-2}} = \left(\alpha^{np^{k-1}}\right)^{x_1}.$$

Из последнего уравнения, зная x_0, находим x_1, и т. д. Значение x_{i+1} находим из уравнения

$$\left(\frac{\beta}{\alpha^{x_0+x_1p+\ldots+x_ip^i}}\right)^{np^{k-i-2}} = \left(\alpha^{np^{k-1}}\right)^{x_{i+1}}, \qquad (9.11)$$

которое справедливо в силу того, что

$$\beta = \alpha^x = \alpha^{x_0+x_1p+\ldots+x_ip^i} \cdot \alpha^{x_{i+1}p^{i+1}+\ldots+x_{k-1}p^{k-1}}.$$

Наши вычисления фактически сводятся к пошаговому нахождению остатков $x \pmod p$, $x \pmod{p^2}$, $\ldots$, $x \pmod{p^i}$ дискретного логарифма x. Основная работа при этом заключается в делении промежуточного числа $\beta/\alpha^{x_0+x_1p+\ldots+x_{i-1}p^{i-1}}$ на $\alpha^{x_ip^i}$, где значение x_i найдено на предыдущем шаге, с последующим возведением результата в степень. На последнем шаге мы узнаем, чему равен остаток $x \pmod{p^k}$. Так как умножение, деление и возведение степень в конечном поле осуществляются достаточно просто, то алгоритм эффективен.

Повторив указанные действия со всеми простыми делителями p_i числа

$$q - 1 = p_1^{k_1} \ldots p_r^{k_r},$$

получим систему сравнений

$$\left.\begin{aligned} x &= z_1 \pmod{p_1^{k_1}}, \\ &\ldots\ldots\ldots\ldots\ldots \\ x &= z_r \pmod{p_r^{k_r}}, \end{aligned}\right\} \qquad (9.12)$$

где z_j удовлетворяет сравнению (9.10) при $p = p_j$, $j = 1, \ldots, r$. Остается применить к полученной системе формулу (2.21) китайской теоремы об остатках и получить x. Схема алгоритма приведена ниже на рис. 9.5.

В следующей лемме оценим сложность приведенного алгоритма.

Лемма 9.7. *Если $q - 1 = p_1^{k_1} \ldots p_r^{k_r}$, то число операций в поле $\mathbb{F}_q$, которые потратит алгоритм Полига — Хеллмана —*

Нечаева, по порядку не превысит величины

$$\sum_{j=1}^{r} k_j(\log q + p_j).$$

Доказательство. Сложность шага 1 очевидно не превосходит по порядку $\sum_{j=1}^{r}(\log q + p_j)$.

На шаге 2 для нахождения очередного разряда числа z_j требуется возвести в степень (вычислить $\alpha^{-x_i p^i}$), умножить на промежуточное значение величины $\beta\alpha^{-x_0 - x_1 p - \ldots - x_{i-1}p^{i-1}}$, снова возвести в степень np^{k-i-2} и пройти по таблице $C(p)$. Возведение в степень $s < q$ требует $\mathcal{O}(\log s) = \mathcal{O}(\log q)$ умножений и должно быть повторено k_i раз. Поиск в таблице размера p имеет в среднем сложность $\mathcal{O}(p)$ (простой перебор), при специальном упорядочении таблицы сложность может быть еще уменьшена. При фиксированном j имеем всего $\mathcal{O}\big(k_j(\log q + p_j)\big)$ операций.

На последнем, третьем шаге арифметика поля $\mathbb{F}_q$ не используется. Для решения системы (9.12) в целых числах достаточно выполнить $\mathcal{O}(r^2)$ операций. Лемма доказана.

Алгоритм Полига—Хеллмана—Нечаева

Вход: $\alpha, \beta \in \mathbb{F}_q$, $q - 1 = p_1^{k_1} \ldots p_r^{k_r}$
Выход: $x \in \mathbb{Z}_{q-1}$, где $\alpha^x = \beta$

1. Составить таблицы логарифмов $C(p_j)$ в подгруппах порядков $(q-1)/p_j$, $j = 1, \ldots, r$.
2. Для каждого $j = 1, \ldots, r$ с помощью $C(p_j)$ найти разряды числа $z_j = x \pmod{p_j^{k_j}}$, применяя по индукции формулу (9.11).
3. Решить систему (9.12).

Рис. 9.5

Замечание 9.4. К недостаткам алгоритма Полига — Хеллмана — Нечаева можно отнести необходимость разложения $q-1$ на множители. Однако в случае, когда каждый простой делитель числа $q-1$ не превосходит величины $\log^{\mathcal{O}(1)} q$, — такие q иногда называют *гладкими* (smooth) числами, — сложность алгоритма оказывается полиномиальной по длине записи q. Если же $q-1$ имеет большой простой делитель, то сложность экспоненциальна. Также отметим, что алгоритм эффективно распараллеливается.

Пример 9.4. Проиллюстрируем метод Полига — Хеллмана — Нечаева вычислением того же дискретного логарифма, что был ранее получен методом согласования в примере 9.3.

Возьмем $\beta = \mathtt{0201}$ в поле $\mathbb{F}_{81} = \mathbb{Z}_3[x]/(x^4 + x + 2)$. Так как $|\mathbb{F}_{81}^*| = 80 = 2^4 \cdot 5$, то нам потребуются таблицы подгрупп порядков 2 и 5 в $\mathbb{F}_{81}^*$. Они образованы соответственно элементами α^{40} и α^{16}, причем α^{40} лежит в простом подполе. Получаем

$$C(2) = \mathbb{Z}_3^* = \{1, 2\} = \{\mathtt{0001}, \mathtt{0002}\}.$$

Далее находим $\gamma = \alpha^{16} = 2\alpha^3 + \alpha + 2 = \mathtt{2012}$ и элементы циклической подгруппы $\langle\gamma\rangle$:

$$C(5) = \big\{1 = \mathtt{0001},\ \gamma = \mathtt{2012},\ \gamma^2 = \mathtt{1202},\ \gamma^3 = \mathtt{0222},\ \gamma^4 = \mathtt{0202}\big\}.$$

Рассмотрим простой делитель 2 и вычислим остаток логарифма $x = \log_\alpha \beta$ по модулю $2^4 = 16$. Имеем $x = \overline{(x_3x_2x_1x_0)}_2 = {} = 8x_3 + 4x_2 + 2x_1 + x_0$, где $x_i \in \{0, 1\}$, и находим младший разряд x_0 из уравнения

$$\beta^{5\cdot 2^3} = \beta^{40} = \alpha^{40x_0}.$$

Для этого вычисляем $\beta^{40} = (2\alpha^2 + 1)^{40} = \mathtt{0002}$, откуда заключаем, что $x_0 = 1$.

Формула (9.11) показывает, что для наших вычислений может потребоваться деление на величину $\alpha^{x_i p^i}$, если $x_i \neq 0$. Поэтому заранее найдем α^{-1} и несколько первых его квадратов:

$$\alpha^4 + \alpha + 2 = 0 \quad \Rightarrow \quad 1 = \alpha^4 + \alpha \quad \Rightarrow \quad \alpha^{-1} = \alpha^3 + 1 = \mathtt{1001},$$

$$\alpha^{-2} = \texttt{1001} \cdot \texttt{1001} = \texttt{1101},$$
$$\alpha^{-4} = \texttt{1101} \cdot \texttt{1101} = \texttt{1112}.$$

Теперь из (9.11) при $i = 0$ получим уравнение для следующего разряда x_1:

$$\left(\frac{\beta}{\alpha^{x_0}}\right)^{40/2} = \left(\frac{\beta}{\alpha}\right)^{20} = \left(\alpha^{40}\right)^{x_1}. \tag{9.13}$$

Вычислим $\beta/\alpha = \beta \cdot \alpha^{-1} = \texttt{0201} \cdot \texttt{1001} = \texttt{1021}$, затем $(\beta/\alpha)^{20} = \texttt{0001}$. Тогда из (9.13) получаем $(\alpha^{40})^{x_1} = 1$, откуда $x_1 = 0$.

Переходим к разряду x_2, учитывая, что $x = x_3 \cdot 2^3 + x_2 \cdot 2^2 + 1$:

$$\left(\frac{\beta}{\alpha^{x_0+2x_1}}\right)^{40/2^2} = \left(\frac{\beta}{\alpha}\right)^{10} = \left(\alpha^{40}\right)^{x_2}.$$

Из $(\beta/\alpha)^{10} = \texttt{0001}$ следует $x_2 = 0$. Наконец,

$$\left(\frac{\beta}{\alpha^{x_0+2x_1+4x_2}}\right)^{40/2^3} = (\beta/\alpha)^5 = \left(\alpha^{40}\right)^{x_3},$$

откуда $x_3 = 1$, поскольку $(\beta/\alpha)^5 = (\alpha^3 + 2\alpha + 1)^5 = \texttt{0002}$. Итогом всех этих вычислений является равенство

$$x = \overline{(1001)}_2 = 9 \pmod{16}.$$

Теперь переходим к простому делителю $p = 5$. Формула

$$\beta^{2^4} = (2\alpha^2 + 1)^{16} = \alpha^{16 \cdot x \pmod 5}$$

вместе с таблицей $C(5)$ дает $x = 2 \pmod 5$, так как $\beta^{16} = \texttt{1202} = \gamma^2$.

Решая систему

$$\left.\begin{aligned} x &= 9 \pmod{16} \\ x &= 2 \pmod 5 \end{aligned}\right\},$$

находим

$$\begin{aligned} x &= 9 \cdot 5 \cdot (5^{-1} \pmod{16}) + 2 \cdot 16 \cdot (16^{-1} \pmod 5) = \\ &= 9 \cdot 5 \cdot 13 + 2 \cdot 16 \cdot 1 = 617 = 57 \pmod{80}. \end{aligned}$$

Таким образом, мы подтвердили полученный ранее ответ. □

Замечание 9.5. Оба изложенных метода логарифмирования (Гельфонда и Полига — Хеллмана — Нечаева) являются универсальными в том смысле, что они применимы не только в мультипликативной группе конечного поля, но и вообще в любой конечной группе. Идея метода согласования находит еще более широкое применение, например в декодировании линейных кодов, криптоанализе (атака «встречей посередине») и пр.

9.5. Коды, исправляющие ошибки

Рассмотрим следующую задачу. По каналу связи из пункта A в пункт B передается информация в виде последовательности слов длины n из символов поля $\mathbb{F}_q$. Под воздействием внешних факторов в каждом передаваемом слове $\boldsymbol{v}$ произвольным образом могут измениться не более t символов. Такое изменение слова $\boldsymbol{v}$ можно рассматривать как его покомпонентное сложение со словом $\mathbf{c}$, содержащим не более t ненулевых компонент и называемым *вектором ошибок*. Для безошибочной передачи информации можно поступить следующим образом. Надо ограничить множество передаваемых слов так, чтобы любые два передаваемых слова $\boldsymbol{v}_i$ и $\boldsymbol{v}_j$ отличались друг от друга не менее чем в $2t+1$ компонентах. Такое множество слов называется *кодом* длины n с минимальным расстоянием $2t+1$. В этом случае в пункте B для извлечения переданной информации из полученного слова $\boldsymbol{u}$ достаточно найти кодовое слово, отличающееся от $\boldsymbol{u}$ в минимальном числе компонент. Поиск такого слова называется *декодированием*. В теории кодирования рассматриваются задачи построения и декодирования кодов. Основная трудность состоит в том, что по ряду причин необходимо использовать коды большой длины и с большим минимальным расстоянием, и поэтому для декодирования таких кодов нужен простой алгоритм, сложность которого не превосходит полинома небольшой степени от n и t. Очевидно, что существуют тривиальные алгоритмы построения кода и его декодирования. Для построения кода G с расстоянием $2t+1$ достаточно начать с одноэлементного кода и последовательно добавлять в него элементы так, чтобы новый

добавляемый элемент отличался от уже принадлежащих коду не менее чем в $2t+1$ компонентах. Для декодирования полученного слова $\boldsymbol{u}$ можно последовательным перебором элементов G (или перебором векторов ошибок с не более чем t ненулевыми компонентами, если их меньше, чем число элементов в G) найти ближайший к $\boldsymbol{u}$ элемент кода. Легко видеть, что оба этих алгоритма в общем случае имеют экспоненциальную относительно n сложность. И если с такой сложностью построения кода можно смириться — один раз перебрать и затем много раз использовать, — то для декодирования это неприемлемо.

Эффективное решение указанных задач, построение и декодирование кодов при больших длинах и расстояниях, оказалось возможным благодаря использованию алгебраических структур — конечных полей и линейных пространств. Далее рассматриваются алгоритмы построения и декодирования примитивных БЧХ-кодов, составляющих основу современной алгебраической теории кодирования. Эти коды были открыты в 1959 г. А. Хоквингемом и независимо от него в 1960 г. Р. К. Боузом и Д. К. Рой-Чоудхури. Они предложили простую и эффективную конструкцию, позволяющую строить коды с различными минимальными расстояниями. Впоследствии эта конструкция была обобщена, и построенные на ее основе коды стали называться кодами Боуза — Чоудхури — Хоквингема или кратко БЧХ-кодами.

Пусть $\mathbb{F}_q^n$ — линейное n-мерное пространство над полем $\mathbb{F}_q$ из q элементов. *Расстоянием Хемминга* $d(\boldsymbol{x}, \boldsymbol{y})$ между векторами $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\mathbb{F}_q^n$ называется число компонент, в которых эти векторы не совпадают. *Весом* $\|\boldsymbol{x}\|$ вектора $\boldsymbol{x}$ из $\mathbb{F}_q^n$ называется число ненулевых координат этого вектора. Нетрудно видеть, что

$$d(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|. \tag{9.14}$$

Подмножество $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$ множества векторов из $\mathbb{F}_q^n$ называется *q-ичным кодом длины n с минимальным расстоянием d*, если для любых двух его элементов $\mathbf{g}_i$ и $\mathbf{g}_j$ расстояние Хемминга между ними не меньше d и найдутся два элемента, расстояние между которыми равно d. Множество $C_t = \{\mathbf{c} \in \in \mathbb{F}_q^n \mid \|\mathbf{c}\| \leqslant t\}$ называется множеством ошибок веса не более t,

а его элементы — векторами ошибок или ошибками. Ненулевые компоненты вектора $\mathbf{c}$ из C_t указывают положение ошибок, а их величины называются *значениями ошибок*. Будем говорить, что код G *исправляет* t *независимых ошибок*, если для суммы $\boldsymbol{v} = \mathbf{g} + \mathbf{c}$ любого $\mathbf{g} \in G$ и любого $\mathbf{c} \in C_t$

$$d(\boldsymbol{v}, \mathbf{g}) < d(\boldsymbol{v}, \mathbf{g}_i) \text{ для всех } \mathbf{g}_i \in G, \text{ таких, что } \mathbf{g}_i \neq \mathbf{g}.$$

Легко видеть, что код G исправляет t ошибок тогда и только тогда, когда его минимальное расстояние d не меньше $2t + 1$. Если $\boldsymbol{v} = \mathbf{g}+\mathbf{c}$ и вес $\mathbf{c}$ равен k, то будем говорить, что в векторе $\mathbf{g}$ произошло k ошибок. Отображение $\mathcal{D} : \boldsymbol{v} = \mathbf{g}+\mathbf{c} \to \mathbf{g}$ называется *декодированием* кода G, или исправлением ошибок в векторе $\boldsymbol{v}$.

Код G называется *линейным* (n, k)*-кодом*, если он является k-мерным подпространством в $\mathbb{F}_q^n$.

Теорема 9.3. *В каждом линейном коде G минимальное расстояние d равно минимальному весу его ненулевого элемента*:

$$d = \min_{\mathbf{g} \neq \mathbf{0}, \mathbf{g} \in G} \|\mathbf{g}\|.$$

Доказательство. Так как нулевой набор всегда принадлежит линейному коду, то очевидно, что минимальное расстояние не превосходит веса минимального ненулевого элемента. Допустим, что $d < \min \|\mathbf{g}\|$. В этом случае в G найдутся два элемента $\mathbf{g}_1$ и $\mathbf{g}_2$, расстояние между которыми меньше d. Следовательно,

$$\|\mathbf{g}_1 - \mathbf{g}_2\| = d(\mathbf{g}_1, \mathbf{g}_2) < d.$$

С другой стороны, разность $\mathbf{g}_1 - \mathbf{g}_2$ обязательно принадлежит G. Поэтому $\|\mathbf{g}_1 - \mathbf{g}_2\| \geqslant d$. Пришли к противоречию. Теорема доказана.

Пространство многочленов степени не выше $n-1$ над полем $\mathbb{F}_q$ изоморфно пространству $\mathbb{F}_q^n$. Задающее такой изоморфизм отображение ψ ставит в соответствие многочлену v вектор его коэффициентов $\boldsymbol{v}$. Этот изоморфизм позволяет при конструировании кодов использовать развитую теорию многочленов над конечными полями. Код G называется *полиномиальным кодом*

длины n с *порождающим многочленом* $h(x)$, если множество многочленов, соответствующих элементам кода G, состоит из всех тех многочленов степени не выше $n-1$, каждый из которых без остатка делится на многочлен $h(x)$. Такими кодами являются рассматриваемые ниже примитивные коды Боуза — Чоудхури — Хоквингема.

Пусть $n = q^m - 1$, α — примитивный элемент поля $GF(q^m)$, $h(x)$ — наименьшее общее кратное минимальных многочленов элементов $\alpha, \alpha^2, \ldots, \alpha^{2t}$ поля $GF(q^m)$. *Примитивным БЧХ-кодом* G длины n с конструктивным расстоянием $2t+1$ и порождающим многочленом $h(x)$ будем называть идеал $h(x)\mathbb{F}_q[x]/(x^n-1)$ кольца $\mathbb{F}_q[x]/(x^n-1)$.

Теорема 9.4. *Минимальное расстояние примитивного БЧХ-кода не меньше его конструктивного расстояния.*

Доказательство. Пусть G — примитивный БЧХ-код длины $n = q^m - 1$ с конструктивным расстоянием $2t+1$, $h(x)$ — его порождающий многочлен. Для доказательства теоремы достаточно показать, что никакой многочлен из $\mathbb{F}_q[x]/(x^n-1)$ с не более чем $2t$ ненулевыми коэффициентами не делится на $h(x)$. Допустим, что утверждение теоремы не верно, и такой многочлен $g(x) = h(x)\tilde{g}(x) = \sum_{j=1}^{2t} g_j x^{i_j}$ существует. Тогда среди его корней будут элементы $\alpha, \alpha^2, \ldots, \alpha^{2t}$, и, следовательно, имеет место система уравнений

$$\left.\begin{array}{rcrcrcl} g_{i_1}\alpha^{i_1} & + & g_{i_2}\alpha^{i_2} & + & \ldots & + & g_{i_{2t}}\alpha^{i_{2t}} = 0, \\ g_{i_1}(\alpha^2)^{i_1} & + & g_{i_2}(\alpha^2)^{i_2} & + & \ldots & + & g_{i_{2t}}(\alpha^2)^{i_{2t}} = 0, \\ \ldots & & \ldots & & \ldots & & \ldots \\ g_{i_1}(\alpha^{2t})^{i_1} & + & g_{i_2}(\alpha^{2t})^{i_2} & + & \ldots & + & g_{i_{2t}}(\alpha^{2t})^{i_{2t}} = 0, \end{array}\right\}$$

которая в матричной записи выглядит следующим образом:

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \ldots & \alpha^{i_{2t}} \\ \alpha^{i_1\cdot 2} & \alpha^{i_2\cdot 2} & \ldots & \alpha^{i_{2t}\cdot 2} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^{i_1\cdot 2t} & \alpha^{i_2\cdot 2t} & \ldots & \alpha^{i_{2t}\cdot 2t} \end{pmatrix} \begin{pmatrix} g_{i_1} \\ g_{i_2} \\ \ldots \\ g_{i_{2t}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \ldots \\ 0 \end{pmatrix}. \qquad (9.15)$$

Так как

$$\det\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{2t}} \\ \alpha^{i_1\cdot 2} & \alpha^{i_2\cdot 2} & \dots & \alpha^{i_{2t}\cdot 2} \\ \dots & \dots & \dots & \dots \\ \alpha^{i_1\cdot 2t} & \alpha^{i_2\cdot 2t} & \dots & \alpha^{i_{2t}\cdot 2t} \end{pmatrix} =$$

$$= \alpha^{i_1}\alpha^{i_2}\cdots\alpha^{i_{2t}}\det\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{2t}} \\ \dots & \dots & \dots & \dots \\ \alpha^{i_1\cdot(2t-1)} & \alpha^{i_2\cdot(2t-1)} & \dots & \alpha^{i_{2t}\cdot(2t-1)} \end{pmatrix} \neq 0,$$

то в силу леммы 5.5 матрица в (9.15) невырождена и, следовательно, это уравнение не имеет ненулевых решений. Противоречие. Теорема доказана.

Пример 9.5. Найдем порождающий многочлен $h(x)$ троичного примитивного БЧХ-кода длины 26, исправляющего три ошибки. В качестве поля из 27 элементов возьмем построенное в примере 8.10 поле $\mathbb{Z}_3[\alpha]$, где α — корень примитивного многочлена x^3+2x+1. Напомним, что в этом поле степени α выглядят следующим образом:

$$\begin{array}{llll} \alpha^0 = (001), & \alpha^7 = (122), & \alpha^{14} = (020), & \alpha^{21} = (101), \\ \alpha^1 = (010), & \alpha^8 = (202), & \alpha^{15} = (200), & \alpha^{22} = (022), \\ \alpha^2 = (100), & \alpha^9 = (011), & \alpha^{16} = (021), & \alpha^{23} = (220), \\ \alpha^3 = (012), & \alpha^{10} = (110), & \alpha^{17} = (210), & \alpha^{24} = (221), \\ \alpha^4 = (120), & \alpha^{11} = (112), & \alpha^{18} = (121), & \alpha^{25} = (201). \\ \alpha^5 = (212), & \alpha^{12} = (102), & \alpha^{19} = (222), & \\ \alpha^6 = (111), & \alpha^{13} = (002), & \alpha^{20} = (211), & \end{array} \tag{9.16}$$

Так как $x^3 + 2x + 1$ является минимальным многочленом для α и α^3, а минимальные многочлены α^2 и α^6 совпадают, то для нахождения $h(x)$ надо найти минимальные многочлены элементов α^2, α^4 и α^5. Используя равенства (9.16), последовательно находим эти многочлены:

$$
\begin{aligned}
m_{\alpha^2}(x) &= (x-\alpha^2)(x-\alpha^6)(x-\alpha^{18}) = \\
&= x^3 - (\alpha^2+\alpha^6+\alpha^{18})x^2 + (\alpha^8+\alpha^{20}+\alpha^{24})x - \alpha^{26} = \\
&= x^3 - 2x^2 + x - 1 = x^3 + x^2 + x + 2; \\
m_{\alpha^4}(x) &= (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{10}) = \\
&= x^3 - (\alpha^4+\alpha^{10}+\alpha^{12})x^2 + (\alpha^{14}+\alpha^{16}+\alpha^{22})x - \alpha^{26} = \\
&= x^3 - 2x^2 - 1 = x^3 + x^2 + 2; \\
m_{\alpha^5}(x) &= (x-\alpha^5)(x-\alpha^{15})(x-\alpha^{19}) = \\
&= x^3 - (\alpha^5+\alpha^{15}+\alpha^{19})x^2 + (\alpha^{20}+\alpha^{24}+\alpha^{28})x - \alpha^{13} = \\
&= x^3 - x^2 + x - 2 = x^3 + 2x^2 + x + 1.
\end{aligned}
$$

Умножая x^3+2x+1 на найденные минимальные многочлены x^3+x^2+x+2, x^3+x^2+2 и x^3+2x^2+x+1, находим порождающий многочлен

$$h(x) = x^{12} + x^{11} + 2x^6 + x^3 + 2x^2 + 2x + 1 \tag{9.17}$$

троичного примитивного БЧХ-кода длины 26, исправляющего три ошибки. □

Построим алгоритм исправления ошибок в примитивных БЧХ-кодах. Для этого найдем вектор ошибок $\mathbf{c}$, если известна сумма $\boldsymbol{v} = \mathbf{g} + \mathbf{c}$. Прежде всего заметим, что так как $g(\alpha^i) = 0$ для $1 \leqslant i \leqslant 2t$, то

$$v(\alpha^i) = g(\alpha^i) + c(\alpha^i) = c(\alpha^i),$$

и, следовательно, значение многочлена v на α^i зависит только от многочлена ошибок c. Для $1 \leqslant i \leqslant 2t$ положим $v(\alpha^i) = S_i$. Набор $S = (S_1, S_2, \ldots, S_{2t})$ называется *синдромом* многочлена v (или синдромом вектора $\boldsymbol{v}$).

Допустим, что многочлен ошибок c содержит ровно $r \leqslant t$ ненулевых слагаемых и равен $\sum_{i=1}^{r} c_{j_i} x^{j_i}$. Для $i = 1, \ldots, r$ введем *локаторы ошибок* $X_i = \alpha^{j_i}$, при этом величину c_{j_i} ошибки, соответствующей локатору X_i, обозначим через Y_i. Нетрудно видеть, что первые r компонент синдрома S многочлена v выражаются

через локаторы и величины ошибок следующим образом:

$$\begin{pmatrix} X_1 & X_2 & \dots & X_r \\ X_1^2 & X_2^2 & \dots & X_r^2 \\ \dots & \dots & \dots & \dots \\ X_1^r & X_2^r & \dots & X_r^r \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ \dots \\ Y_r \end{pmatrix} = \begin{pmatrix} Y_1X_1 + \dots + Y_rX_r \\ Y_1X_1^2 + \dots + Y_rX_r^2 \\ \dots \\ Y_1X_1^r + \dots + Y_rX_r^r \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ \dots \\ S_r \end{pmatrix}. \tag{9.18}$$

Как и в (9.15), матрица в левой части равенства (9.18) невырождена. Поэтому если известны локаторы ошибок X_i, то величины ошибок Y_i можно найти из (9.18).

Для нахождения локаторов ошибок воспользуемся *многочленом локаторов ошибок*

$$\begin{aligned} \Lambda(x) &= (1 - xX_1)(1 - xX_2)\dots(1 - xX_r) = \\ &= \Lambda_r x^r + \Lambda_{r-1}x^{r-1} + \dots + \Lambda_1 x + 1. \end{aligned}$$

Если многочлен $\Lambda(x)$ известен, то, вычислив его корни, можно определить позиции ошибок. Так как переменная x может принимать не более чем n различных значений, то корни $\Lambda(x)$ можно найти, последовательно вычисляя значения $\Lambda(x)$ на всех элементах поля $GF(q^m)$. Для этого достаточно выполнить в общей сложности $\mathcal{O}(tn)$ действий над элементами поля $GF(q^m)$.

Сначала для каждого $i = 1, \dots, r$ и каждого $j = 1, \dots, r$ умножим многочлен локаторов ошибок на произведение $Y_iX_i^{r+j}$ и подставим вместо переменной x его корень X_i^{-1}. В результате получим систему равенств

$$\Lambda_r Y_i X_i^j + \Lambda_{r-1} Y_i X_i^{j+1} + \dots + \Lambda_1 Y_i X_i^{r+j-1} + Y_i X_i^{r+j} = 0, \tag{9.19}$$

где $i = 1, \dots, r$ и $j = 1, \dots, r$. Суммируя при фиксированном j равенства из (9.19) по всем i от 1 до r, получим, что для каждого $j = 1, \dots, r$

$$\begin{aligned} &\sum_{i=1}^{r} (\Lambda_r Y_i X_i^j + \Lambda_{r-1} Y_i X_i^{j+1} + \dots + Y_i X_i^{r+j}) = \\ &\quad = \Lambda_r \sum_{i=1}^{r} Y_i X_i^j + \Lambda_{r-1} \sum_{i=1}^{r} Y_i X_i^{j+1} + \dots + \sum_{i=1}^{r} Y_i X_i^{r+j} = 0. \end{aligned}$$

Так как суммы, умножаемые в последнем равенстве на коэффициенты Λ_i, являются компонентами синдрома, то

$$\Lambda_r S_j + \Lambda_{r-1} S_{j+1} + \cdots + \Lambda_1 S_{r+j-1} + S_{r+j} = 0, \quad j = 1, \ldots, r. \quad (9.20)$$

Из равенств (9.20) составим систему уравнений относительно коэффициентов Λ_i. В матричной форме эта система имеет следующий вид:

$$\begin{pmatrix} S_1 & S_2 & \ldots & S_r \\ S_2 & S_3 & \ldots & S_{r+1} \\ \ldots & \ldots & \ldots & \ldots \\ S_r & S_{r+1} & \ldots & S_{2r-1} \end{pmatrix} \begin{pmatrix} \Lambda_r \\ \Lambda_{r-1} \\ \ldots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_{r+1} \\ -S_{r+2} \\ \ldots \\ -S_{2r} \end{pmatrix}. \quad (9.21)$$

Пусть $\mathbf{S}_r$ — матрица из (9.21) и $r \leqslant l \leqslant t$. Покажем, что матрица $\mathbf{S}_l$ невырождена, если $l = r$, и вырождена, если $l > r$. Для того чтобы убедиться в этом, достаточно представить матрицу $\mathbf{S}_l$ в виде произведения

$$\begin{pmatrix} S_1 & S_2 & \ldots & S_l \\ S_2 & S_3 & \ldots & S_{l+1} \\ \ldots & \ldots & \ldots & \ldots \\ S_l & S_{l+1} & \ldots & S_{2l-1} \end{pmatrix} =$$

$$= \begin{pmatrix} Y_1X_1 & Y_2X_2 & \ldots & Y_lX_l \\ Y_1X_1^2 & Y_2X_2^2 & \ldots & Y_lX_l^2 \\ \ldots & \ldots & \ldots & \ldots \\ Y_1X_1^l & Y_2X_2^l & \ldots & Y_lX_l^l \end{pmatrix} \begin{pmatrix} 1 & X_1 & \ldots & X_1^{l-1} \\ 1 & X_2 & \ldots & X_2^{l-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & X_l & \ldots & X_l^{l-1} \end{pmatrix},$$

в котором левый множитель также можно представить в виде произведения

$$\begin{pmatrix} Y_1X_1 & Y_2X_2 & \ldots & Y_lX_l \\ Y_1X_1^2 & Y_2X_2^2 & \ldots & Y_lX_l^2 \\ \ldots & \ldots & \ldots & \ldots \\ Y_1X_1^l & Y_2X_2^l & \ldots & Y_lX_l^l \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_l \\ \ldots & \ldots & \ldots & \ldots \\ X_1^{l-1} & X_2^{l-1} & \ldots & X_l^{l-1} \end{pmatrix} \begin{pmatrix} Y_1X_1 & 0 & \ldots & 0 \\ 0 & Y_2X_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & Y_lX_l \end{pmatrix}.$$

Таким образом, видим, что матрица $\mathbf{S}_l$ является произведением трех квадратных матриц, две из которых невырождены тогда и только тогда, когда различны все X_i, а третья — диагональная матрица, невырождена тогда и только тогда, когда все X_i и Y_i отличны от нуля[1)]. Следовательно, матрица $\mathbf{S}_l$ невырождена тогда и только тогда, когда все X_i различны и все Y_i отличны от нуля, т. е. когда $l = r$.

Теперь можно сформулировать алгоритм декодирования примитивного БЧХ-кода. Пусть БЧХ-код длины $n = q^m - 1$ исправляет t ошибок. Тогда для декодирования вектора $\boldsymbol{v}$ выполняем следующие действия.

1. Вычисляя значения $v(\alpha), v(\alpha^2), \ldots, v(\alpha^{2t})$, находим компоненты синдрома $S_1, S_2, \ldots, S_{2t}$ и полагаем $r = t$.

2. Составляем матрицу

$$\mathbf{S}_r = \begin{pmatrix} S_1 & S_2 & \ldots & S_r \\ S_2 & S_3 & \ldots & S_{r+1} \\ \ldots & \ldots & \ldots & \ldots \\ S_r & S_{r+1} & \ldots & S_{2r-1} \end{pmatrix}$$

и определяем, вырождена эта матрица или нет.

3. Если матрица $\mathbf{S}_r$ вырождена, то уменьшаем r на единицу и возвращаемся к п. 2. Если матрица $\mathbf{S}_r$ невырождена, то определяем, что число ошибок равно r, и переходим к следующему пункту.

4. Решая матричное уравнение

$$\begin{pmatrix} S_1 & S_2 & \ldots & S_r \\ S_2 & S_3 & \ldots & S_{r+1} \\ \ldots & \ldots & \ldots & \ldots \\ S_r & S_{r+1} & \ldots & S_{2r-1} \end{pmatrix} \begin{pmatrix} \Lambda_r \\ \Lambda_{r-1} \\ \ldots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_{r+1} \\ -S_{r+2} \\ \ldots \\ -S_{2r} \end{pmatrix},$$

находим коэффициенты Λ_i многочлена локаторов ошибок.

5. Последовательно вычисляя на всех элементах поля $GF(q^m)$ значения многочлена

$$\Lambda(x) = \Lambda_r x^r + \Lambda_{r-1} x^{r-1} + \cdots + \Lambda_1 x + 1,$$

[1)] Для выполнения при $t \geqslant l > r$ указанных матричных равенств положим $Y_i = 0$ при $r < i \leqslant t$, а индексы позиций фиктивных ошибок j_i для $r < i \leqslant t$ выберем произвольными.

находим его корни $x_1, \ldots, x_r$, обращая которые, находим локаторы ошибок $X_1, \ldots, X_r$. Затем из равенств $X_i = \alpha^{j_i}$ определяем позиции ошибок j_i.

6. Решая матричное уравнение

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_r \\ X_1^2 & X_2^2 & \ldots & X_r^2 \\ \ldots & \ldots & \ldots & \ldots \\ X_1^r & X_2^r & \cdots & X_r^r \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ \ldots \\ Y_r \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ \ldots \\ S_r \end{pmatrix},$$

находим величины ошибок $Y_1, \ldots, Y_r$.

7. Пусть, как и ранее, $\boldsymbol{e}_j$ — j-й базисный вектор стандартного базиса. Вычисляя разность

$$\boldsymbol{v} - \sum_{i=1}^{r} Y_i \boldsymbol{e}_{j_i},$$

находим кодовый вектор $\mathbf{g}$.

Приведенный алгоритм декодирования называется алгоритмом Питерсона — Горенстейна — Цирлера. Нетрудно видеть, что для реализации этого алгоритма достаточно выполнить $\mathcal{O}(t^4 + nt)$ действий над элементами поля $GF(q^m)$.

Пример 9.6. Рассмотрим работу алгоритма на примере исправления ошибок в векторе $\boldsymbol{v} = (01222222222222222222222222)$ троичным БЧХ-кодом длины 26 с построенным в предыдущем примере порождающим многочленом (9.17).

1. Вычисляя при помощи (9.16) значения многочлена

$$v(x) = x^{24} + 2x^{23} + 2x^{22} + \cdots + 2x^2 + 2x + 2$$

на элементах $\alpha, \alpha^2, \alpha^4$ и α^5, найдем первую, вторую, четвертую и пятую компоненты синдрома:

$$S_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \alpha, \qquad S_2 = \begin{pmatrix} 2 \\ 0 \\ 2 \end{pmatrix} = \alpha^8,$$

$$S_4 = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \alpha^{25}, \quad S_5 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \alpha^{10}.$$

Далее находим $S_3 = (S_1)^3 = \alpha^3$ и $S_6 = (S_2)^3 = \alpha^{24}$.

2—3. Положим $r = 3$. Так как

$$\det \begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix} = \det \begin{pmatrix} \alpha & \alpha^8 & \alpha^3 \\ \alpha^8 & \alpha^3 & \alpha^{25} \\ \alpha^3 & \alpha^{25} & \alpha^{10} \end{pmatrix} = \\ = \alpha^{14} + \alpha^{10} + \alpha^{10} - \alpha^9 - \alpha^0 - \alpha^{24} = 0,$$

то заключаем, что произошло не более двух ошибок. Положим $r = 2$. Так как

$$\det \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} = \det \begin{pmatrix} \alpha & \alpha^8 \\ \alpha^8 & \alpha^3 \end{pmatrix} = \alpha^4 - \alpha^{16} \neq 0,$$

то заключаем, что произошло две ошибки.

4. Найдем коэффициенты многочлена локаторов ошибок. Для этого решим матричное уравнение

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_3 \\ -S_4 \end{pmatrix},$$

преобразуя левую часть расширенной матрицы уравнения в единичную. Так как

$$\left(\begin{array}{cc|c} \alpha & \alpha^8 & -\alpha^3 \\ \alpha^8 & \alpha^3 & -\alpha^{25} \end{array}\right) \sim \left(\begin{array}{cc|c} \alpha & \alpha^8 & \alpha^{16} \\ \alpha^8 & \alpha^3 & \alpha^{12} \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & \alpha^7 & \alpha^{15} \\ 1 & \alpha^{21} & \alpha^4 \end{array}\right) \sim \\ \sim \left(\begin{array}{cc|c} 1 & \alpha^7 & \alpha^{15} \\ 0 & \alpha^{21} - \alpha^7 & \alpha^4 - \alpha^{15} \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & \alpha^7 & \alpha^{15} \\ 0 & \alpha^3 & \alpha^{23} \end{array}\right) \sim \\ \sim \left(\begin{array}{cc|c} 1 & \alpha^7 & \alpha^{15} \\ 0 & 1 & \alpha^{20} \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & \alpha^{15} - \alpha \\ 0 & 1 & \alpha^{20} \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & \alpha^{23} \\ 0 & 1 & \alpha^{20} \end{array}\right),$$

то $\Lambda_2 = \alpha^{23}$ и $\Lambda_1 = \alpha^{20}$.

5. Вычисляя значения многочлена $\Lambda(x) = \alpha^{23}x^2 + \alpha^{20}x + 1$ на всех ненулевых элементах поля $\mathbb{Z}_3[\alpha]$, найдем его корни $x_1 = \alpha$ и $x_2 = \alpha^2$. Обращая корни, находим локаторы ошибок $X_1 = \alpha^{25}$ и $X_2 = \alpha^{24}$, которые, очевидно, соответствуют двум левым позициям.

6. Для определения значений ошибок Y_1 и Y_2 решим матричное уравнение $\begin{pmatrix} X_1 & X_2 \\ X_1^2 & X_2^2 \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \end{pmatrix}$. Так как

$$\left(\begin{array}{cc|c} \alpha^{25} & \alpha^{24} & \alpha \\ \alpha^{24} & \alpha^{22} & \alpha^8 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & \alpha^{25} & \alpha^2 \\ 1 & \alpha^{24} & \alpha^{10} \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|c} 1 & \alpha^{25} & \alpha^2 \\ 0 & \alpha^{24}-\alpha^{25} & \alpha^{10}-\alpha^2 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & \alpha^{25} & \alpha^2 \\ 0 & \alpha^{14} & \alpha \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|c} 1 & \alpha^{25} & \alpha^2 \\ 0 & 1 & \alpha^{13} \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & \alpha^2-\alpha^{12} \\ 0 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 2 \end{array}\right),$$

то $Y_1 = 1$ и $Y_2 = 2$. Следовательно, в векторе ошибок $\mathbf{c}$ последние 24 компоненты равны нулю, первая компонента равна двум, а вторая — единице.

7. Вычитая из полученного вектора $\boldsymbol{v}$ найденный вектор ошибок $\mathbf{c}$:

$$\begin{aligned} \boldsymbol{v} - \mathbf{c} &= (012222222222222222222222) - \\ &\quad - (120000000000000000000000) = \\ &= (222222222222222222222222), \end{aligned}$$

находим искомый элемент кода $\mathbf{g}$, у которого каждая компонента равна 2. □

Задачи

9.1. Показать, что если $\mathbb{F}_q$ — конечное поле нечетной характеристики, то элемент $\alpha \in \mathbb{F}_q^*$ имеет в $\mathbb{F}_q$ квадратный корень β, т. е. такой элемент, что $\beta^2 = \alpha$, тогда и только тогда, когда $\alpha^{(q-1)/2} = 1$. Как можно его вычислить?

9.2. Доказать, что $\alpha = 2$ является примитивным элементом поля $\mathbb{Z}_{101}$ и найти логарифм вычета 59 по основанию α.

9.3. Найти логарифм элемента $\alpha^3 + \alpha^2 + 1$ по основанию примитивного элемента α поля $\mathbb{F}_{81} = \mathbb{F}_3[x]/(x^4 + x + 2)$ из примера 9.3.

9.4. Решить уравнение $2^x = 195 \pmod{19^2}$.

9.5. Решить уравнение $3^x = 132 \pmod{257}$.

9.6. Пусть $q-1=p_1^{k_1}\dots p_r^{k_r}$. Построить алгоритм, решающий задачу дискретного логарифмирования в поле $\mathbb{F}_q$, число операций которого по порядку не превосходит $\sum_{j=1}^{r} k_j(\log q+\sqrt{p_j}\log_2 p_j)$.

9.7. Многочлены $x^8+x^6+x^4+x^3+1$ и $x^{12}+x^7+x^5+x^4+x^3+x^2+$ $+1$ разложить на неприводимые множители над полем $\mathbb{Z}_2$ с помощью алгоритма Берлекемпа.

9.8. Доказать неприводимость над $\mathbb{Z}_3$ многочлена x^3+2x^2+x+1 с помощью алгоритма Берлекемпа.

9.9. Доказать, что число f-разлагающих многочленов в определенном на с. 311 пространстве $\mathbb{V}$ равно $p^k-(p-1)^k-1$. Получить отсюда, что взятая наугад линейная комбинация векторов базиса B в $\mathbb{V}$ будет f-разлагающей с вероятностью не менее $1/p$.

9.10. Пусть многочлен $f\in\mathbb{Z}_p[x]$ свободен от квадратов и $g(x)\in$ $\in\mathbb{Z}_p[x]/f$, причем $\deg g\geqslant 1$. Пусть $g^p=g\pmod f$. Доказать, что

$$f(x)=\prod_{a\in\mathbb{Z}_p}\bigl(f(x),g(x)-a\bigr),$$

причем правая часть этого равенства является нетривиальным разложением $f(x)$ на взаимно простые множители. Останется ли верным это утверждение, если f не свободен от квадратов?

9.11. Пусть $f=f_1\cdots f_k$ — свободный от квадратов многочлен степени n над полем $\mathbb{Z}_p$, множители f_i неприводимы и $n_i=\deg f_i$. Положим $M=\text{НОК}(n_1,\dots,n_k)$ и $T(x)=x+x^p+x^{p^2}+\ldots+x^{p^M}$. Пусть $T_i(x)=T(x^i)\pmod{f(x)}$. Показать, что по крайней мере один из многочленов $T_1(x),\dots,T_{n-1}(x)$ является f-разлагающим.

9.12. Пусть G — линейный (n,k)-код. Матрица из $n-k$ строк и n столбцов называется *проверочной матрицей* кода G, если ее строки образуют базис ортогонального пространства кода G. Показать, что матрица $\mathbf{H}$ будет проверочной матрицей линейного кода с минимальным расстоянием не меньшим d тогда и только тогда, когда ее любые $d-1$ столбцов линейно независимы.

9.13. Написать проверочную матрицу двоичного БЧХ-кода длины 15, исправляющего две ошибки.

9.14. Найти порождающий многочлен и размерность двоичного БЧХ-кода длины 15, исправляющего три ошибки.

9.15. Пусть $q^m-1=ab$, α — порождающий элемент поля $GF(q^m)$. Показать, что минимальное расстояние полиномиального кода длины b, порожденного многочленом $\text{НОК}(m_{\alpha^a}(x),m_{\alpha^{2a}}(x),\dots,m_{\alpha^{2ta}}(x))$, не меньше, чем $2t+1$.

9.16. Код G называется *циклическим*, если вместе с каждым своим элементом $(g_1, g_2, g_3, \ldots, g_n)$ код G содержит и его циклический сдвиг $(g_2, g_3, \ldots, g_n, g_1)$. Показать, что любой примитивный БЧХ-код — циклический.

9.17. Найти порождающий многочлен двоичного $(21, 11)$-кода, исправляющего две ошибки.

9.18. Показать, что существует исправляющий шесть ошибок двоичный полиномиальный $(80, 40)$-код. Для этого кода описать алгоритм построения порождающего многочлена и алгоритм исправления ошибок.

9.19. При передаче по каналу с помехами кодового слова двоичного кода БЧХ длины 15 с корнями в поле $\mathbb{Z}_2[x]/(x^4 + x^3 + 1)$, исправляющего три ошибки, получено слово $\boldsymbol{v} = (011000000111101)$. Декодировать его.

9.20. Пусть G — примитивный двоичный БЧХ-код. Доказать, что если $\mathbf{g} \in G$, то и $\overline{\mathbf{g}} \in G$, где вектор $\overline{\mathbf{g}}$ отличается от $\mathbf{g}$ во всех разрядах.

9.21. Привести пример примитивного двоичного кода БЧХ, истинное минимальное расстояние которого строго больше конструктивного.

9.22. Пусть $V(\mathbf{g}) = \mathbf{g} + C_t$. Показать, что множества $V(\mathbf{g})$ и $V(\mathbf{g}')$ не пересекаются при различных $\mathbf{g}, \mathbf{g}' \in G$, если G — примитивный двоичный код БЧХ длины $n = 2^m - 1$, иправляющий одну $(t = 1)$ ошибку. Показать, что $\bigcup_{\mathbf{g}\in G} V(\mathbf{g}) = \mathbb{Z}_2^{2^m-1}$.

9.23. Найти максимальное n, для которого существует двоичный линейный код длины n, исправляющий одну ошибку, проверочная матрица которого содержит ровно три строки.

9.24. Пусть G — линейный (n, k)-код. Матрица $\mathbf{A} = \mathbf{A}_{k\times n}$ называется его *порождающей матрицей*, если ее строки образуют базис в G. Найти число различных порождающих матриц (n, k)-кода.

9.25. Показать, что у всякого линейного (n, k)-кода найдется систематическая порождающая матрица. Используя это, доказать, что для любого (n, k)-кода с минимальным расстоянием d выполнено неравенство $d \leqslant n - k + 1$, называемое неравенством Синглтона.

Литература

1. *Абрамов С. А.* Лекции о сложности алгоритмов. Москва: МЦНМО, 2009. 256 с.
2. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. Москва: Мир, 1987. 416 с.
3. *Андерсон Дж. А.* Дискретная математика и комбинаторика. Москва: Вильямс, 2004. 960 с.
4. *Алексеев В. Б.* Теорема Абеля в задачах и решениях. Москва: МЦНМО, 2001. 192 с.
5. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. Москва: Мир, 1979. 536 с.
6. *Берлекэмп Э.* Алгебраическая теория кодирования. Москва: Мир, 1971. 479 с.
7. *Болотов А. А., Гашков С.Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. Москва: Комкнига, 2011. 328 с.
8. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. Москва: Мир, 1986. 576 с.
9. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. Москва: МЦНМО, 2003. 328 с.
10. *Винберг Э. Б.* Начала алгебры. Москва: МЦНМО, 1998. 192 с.
11. *Винберг Э. Б.* Курс алгебры. Москва: Факториал, 2002. 544 с.
12. *Виноградов И. М.* Основы теории чисел. Москва — Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. 176 с.

13. *Гашков С. Б.* Современная элементарная алгебра в задачах и решениях. Москва: МЦНМО, 2006. 328 с.
14. *Гельфанд И. М.* Лекции по линейной алгебре. Москва: МЦНМО, 1998. 320 с.
15. *Зорич В. А.* Математический анализ. Т. 1. Москва: МЦНМО, 2002. 664 с.
16. *Кнут Д.* Искусство программирования. Т. 2. Москва: Вильямс, 2001. 788 с.
17. *Коблиц Н.* Курс теории чисел и криптографии. Москва: ТВП, 2001. 254 с.
18. *Кострикин А. И.* Введение в алгебру. Ч. 3. Основные структуры алгебры. Москва: Физматлит, 2001. 272 с.
19. Сборник задач по алгебре: учеб. пособие под ред. А. И. Кострикина. Москва: Факториал, 1995. 454 с.
20. *Лидл Р., Нидеррайтер Г.* Конечные поля. Москва: Мир, 1988. 822 с.
21. *Мендельсон Э.* Введение в математическую логику. Москва: Наука, 1984. 320 с.
22. *Нечаев В. И.* Элементы криптографии (основы теории защиты информации). Москва: Высшая школа, 1999. 109 с.
23. *Ноден П., Китте К.* Алгебраическая алгоритмика. Москва: Мир, 1999. 720 с.
24. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. Москва: Мир, 1976. 594 с.
25. *Проскуряков И. В.* Сборник задач по линейной алгебре. Москва: Лаборатория базовых знаний, 2003. 384 с.
26. *Фаддеев Д. К.* Лекции по алгебре. Москва: Наука, 1984. 416 с.
27. *Фрид Э.* Элементарное введение в абстрактную алгебру. Москва: Мир, 1979. 261 с.
28. *Чашкин А. В.* Дискретная математика. Москва: Академия, 2012. 352 с.
29. *Cohen H.* A course in computational algebraic number theory. Berlin: Springer-Verlag, 1993. 534 p.
30. *von zur Gathen J., Gerhard J.* Modern computer algebra. 3rd ed. Cambridge University Press, 2013. 808 p.

31. *Shoup V.* New algorithms for finding irreducible polynomials over finite fields // Math. Comp. 54, 1990, pp. 435–447.
32. *Shoup V.* Fast construction of irreducible polynomials over finite fields // J. Symbolic Comput. 17, 1994, pp. 371–391.

Приложение А. Примитивные элементы поля $\mathbb{Z}_p$

Таблица первых 195 простых чисел. Во втором столбце перечислены простые числа p, в третьем — минимальные примитивные корни $\alpha_{\min}$ из $\mathbb{Z}_p$.

n	p_n	α
1	2	1
2	3	2
3	5	2
4	7	3
5	11	2
6	13	2
7	17	3
8	19	2
9	23	5
10	29	2
11	31	3
12	37	2
13	41	6
14	43	3
15	47	5
16	53	2
17	59	2
18	61	2
19	67	2
20	71	7
21	73	5
22	79	3
23	83	2
24	89	3
25	97	5
26	101	2
27	103	5
28	107	2
29	109	6
30	113	3

n	p_n	α
31	127	3
32	131	2
33	137	3
34	139	2
35	149	2
36	151	6
37	157	5
38	163	2
39	167	5
40	173	2
41	179	2
42	181	2
43	191	19
44	193	5
45	197	2
46	199	3
47	211	2
48	223	3
49	227	2
50	229	6
51	233	3
52	239	7
53	241	7
54	251	6
55	257	3
56	263	5
57	269	2
58	271	6
59	277	5
60	281	3

n	p_n	α
61	283	3
62	293	2
63	307	5
64	311	17
65	313	10
66	317	2
67	331	3
68	337	10
69	347	2
70	349	2
71	353	3
72	359	7
73	367	6
74	373	2
75	379	2
76	383	5
77	389	2
78	397	5
79	401	3
80	409	21
81	419	2
82	421	2
83	431	7
84	433	5
85	439	15
86	443	2
87	449	3
88	457	13
89	461	2
90	463	3

n	p_n	α
91	467	2
92	479	13
93	487	3
94	491	2
95	499	7
96	503	5
97	509	2
98	521	3
99	523	2
100	541	2
101	547	2
102	557	2
103	563	2
104	569	3
105	571	3
106	577	5
107	587	2
108	593	3
109	599	7
110	601	7
111	607	3
112	613	2
113	617	3
114	619	2
115	631	3
116	641	3
117	643	11
118	647	5
119	653	2
120	659	2
121	661	2
122	673	5
123	677	2
124	683	5
125	691	3

n	p_n	α
126	701	2
127	709	2
128	719	11
129	727	5
130	733	6
131	739	3
132	743	5
133	751	3
134	757	2
135	761	6
136	769	11
137	773	2
138	787	2
139	797	2
140	809	3
141	811	3
142	821	2
143	823	3
144	827	2
145	829	2
146	839	11
147	853	2
148	857	3
149	859	2
150	863	5
151	877	2
152	881	3
153	883	2
154	887	5
155	907	2
156	911	17
157	919	7
158	929	3
159	937	5
160	941	2

n	p_n	α
161	947	2
162	953	3
163	967	5
164	971	6
165	977	3
166	983	5
167	991	6
168	997	7
169	1009	11
170	1013	3
171	1019	2
172	1021	10
173	1031	14
174	1033	5
175	1039	3
176	1049	3
177	1051	7
178	1061	2
179	1063	3
180	1069	6
181	1087	3
182	1091	2
183	1093	5
184	1097	3
185	1103	5
186	1109	2
187	1117	2
188	1123	2
189	1129	11
190	1151	17
191	1153	5
192	1163	5
193	1171	2
194	1181	7
195	1187	2

Приложение B. Разложение на простые множители чисел вида $p^n - 1$

$$
\begin{aligned}
2^2 - 1 &= 3 \\
2^3 - 1 &= 7 \\
2^4 - 1 &= 15 &&= 3 \cdot 5 \\
2^5 - 1 &= 31 \\
2^6 - 1 &= 63 &&= 3^2 \cdot 7 \\
2^7 - 1 &= 127 \\
2^8 - 1 &= 255 &&= 3 \cdot 5 \cdot 17 \\
2^9 - 1 &= 511 &&= 7 \cdot 73 \\
2^{10} - 1 &= 1023 &&= 3 \cdot 11 \cdot 31 \\
2^{11} - 1 &= 2047 &&= 23 \cdot 89 \\
2^{12} - 1 &= 4095 &&= 3^2 \cdot 5 \cdot 7 \cdot 13 \\
2^{13} - 1 &= 8191 \\
2^{14} - 1 &= 16383 &&= 3 \cdot 43 \cdot 127 \\
2^{15} - 1 &= 32767 &&= 7 \cdot 31 \cdot 151 \\
2^{16} - 1 &= 65535 &&= 3 \cdot 5 \cdot 17 \cdot 257 \\
2^{17} - 1 &= 131071 \\
2^{18} - 1 &= 262143 &&= 3^3 \cdot 7 \cdot 19 \cdot 73 \\
2^{19} - 1 &= 524287 \\
2^{20} - 1 &= 1048575 &&= 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41 \\
2^{21} - 1 &= 2097151 &&= 7^2 \cdot 127 \cdot 337 \\
2^{22} - 1 &= 4194303 &&= 3 \cdot 23 \cdot 89 \cdot 683 \\
2^{23} - 1 &= 8388607 &&= 47 \cdot 178481 \\
2^{24} - 1 &= 16777215 &&= 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241 \\
2^{25} - 1 &= 33554431 &&= 31 \cdot 601 \cdot 1801 \\
2^{26} - 1 &= 67108863 &&= 3 \cdot 2731 \cdot 8191 \\
2^{27} - 1 &= 134217727 &&= 7 \cdot 73 \cdot 262657 \\
2^{28} - 1 &= 268435455 &&= 3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127 \\
2^{29} - 1 &= 536870911 &&= 233 \cdot 1103 \cdot 2089 \\
2^{30} - 1 &= 1073741823 &&= 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331 \\
2^{31} - 1 &= 2147483647 \\
2^{32} - 1 &= 4294967295 &&= 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \\
2^{33} - 1 &= 8589934591 &&= 7 \cdot 23 \cdot 89 \cdot 599479 \\
2^{34} - 1 &= 17179869183 &&= 3 \cdot 131071 \cdot 43691 \\
2^{35} - 1 &= 34359738367 &&= 31 \cdot 71 \cdot 127 \cdot 122921
\end{aligned}
$$

$$
\begin{aligned}
2^{36}-1 &= 68719476735 &&= 3^3\cdot 5\cdot 7\cdot 13\cdot 19\cdot 37\cdot 73\cdot 109\\
2^{37}-1 &= 137438953471 &&= 223\cdot 616318177\\
2^{38}-1 &= 274877906943 &&= 3\cdot 174763\cdot 524287\\
2^{39}-1 &= 549755813887 &&= 7\cdot 79\cdot 121369\cdot 8191\\
2^{40}-1 &= 1099511627775 &&= 3\cdot 5^2\cdot 11\cdot 17\cdot 31\cdot 41\cdot 61681\\
2^{41}-1 &= 2199023255551 &&= 164511353\cdot 13367\\
2^{42}-1 &= 4398046511103 &&= 3^2\cdot 7^2\cdot 43\cdot 127\cdot 337\cdot 5419\\
2^{43}-1 &= 8796093022207 &&= 431\cdot 2099863\cdot 9719\\
2^{44}-1 &= 17592186044415 &&= 3\cdot 5\cdot 23\cdot 89\cdot 397\cdot 683\cdot 2113\\
2^{45}-1 &= 35184372088831 &&= 7\cdot 31\cdot 73\cdot 151\cdot 631\cdot 23311\\
2^{46}-1 &= 70368744177663 &&= 3\cdot 47\cdot 178481\cdot 2796203\\
2^{47}-1 &= 140737...355327 &&= 2351\cdot 4513\cdot 13264529
\end{aligned}
$$

$$
\begin{aligned}
3^2-1 &= 8 &&= 2^3\\
3^3-1 &= 26 &&= 2\cdot 13\\
3^4-1 &= 80 &&= 2^4\cdot 5\\
3^5-1 &= 242 &&= 2\cdot 11^2\\
3^6-1 &= 728 &&= 2^3\cdot 7\cdot 13\\
3^7-1 &= 2186 &&= 2\cdot 1093\\
3^8-1 &= 6560 &&= 2^5\cdot 5\cdot 41\\
3^9-1 &= 19682 &&= 2\cdot 13\cdot 757\\
3^{10}-1 &= 59048 &&= 2^3\cdot 11^2\cdot 61\\
3^{11}-1 &= 177146 &&= 2\cdot 23\cdot 3851\\
3^{12}-1 &= 531440 &&= 2^4\cdot 5\cdot 7\cdot 13\cdot 73\\
3^{13}-1 &= 1594322 &&= 2\cdot 797161\\
3^{14}-1 &= 4782968 &&= 2^3\cdot 547\cdot 1093\\
3^{15}-1 &= 14348906 &&= 2\cdot 11^2\cdot 13\cdot 4561\\
3^{16}-1 &= 43046720 &&= 2^6\cdot 5\cdot 17\cdot 41\cdot 193\\
3^{17}-1 &= 129140162 &&= 2\cdot 1871\cdot 34511\\
3^{18}-1 &= 387420488 &&= 2^3\cdot 7\cdot 13\cdot 19\cdot 37\cdot 757\\
3^{19}-1 &= 1162261466 &&= 2\cdot 1597\cdot 363889\\
3^{20}-1 &= 3486784400 &&= 2^4\cdot 5^2\cdot 11^2\cdot 61\cdot 1181\\
3^{21}-1 &= 10460353202 &&= 2\cdot 13\cdot 1093\cdot 368089\\
3^{22}-1 &= 31381059608 &&= 2^3\cdot 23\cdot 67\cdot 661\cdot 3851\\
3^{23}-1 &= 94143178826 &&= 2\cdot 47\cdot 1001523179\\
3^{24}-1 &= 282429536480 &&= 2^5\cdot 5\cdot 7\cdot 13\cdot 41\cdot 73\cdot 6481\\
3^{25}-1 &= 847288609442 &&= 2\cdot 11^2\cdot 8951\cdot 391151
\end{aligned}
$$

$$
\begin{aligned}
5^2 - 1 &= 24 &&= 2^3 \cdot 3\\
5^3 - 1 &= 124 &&= 2^2 \cdot 31\\
5^4 - 1 &= 624 &&= 2^4 \cdot 3 \cdot 13\\
5^5 - 1 &= 3124 &&= 2^2 \cdot 11 \cdot 71\\
5^6 - 1 &= 15624 &&= 2^3 \cdot 3^2 \cdot 7 \cdot 31\\
5^7 - 1 &= 78124 &&= 2^2 \cdot 19531\\
5^8 - 1 &= 390624 &&= 2^5 \cdot 3 \cdot 13 \cdot 313\\
5^9 - 1 &= 1953124 &&= 2^2 \cdot 19 \cdot 31 \cdot 829\\
5^{10} - 1 &= 9765624 &&= 2^3 \cdot 3 \cdot 11 \cdot 71 \cdot 521\\
5^{11} - 1 &= 48828124 &&= 2^2 \cdot 12207031\\
5^{12} - 1 &= 244140624 &&= 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601\\
5^{13} - 1 &= 1220703124 &&= 2^2 \cdot 305175781\\
5^{14} - 1 &= 6103515624 &&= 2^3 \cdot 3 \cdot 29 \cdot 449 \cdot 19531\\
5^{15} - 1 &= 30517578124 &&= 2^2 \cdot 11 \cdot 31 \cdot 71 \cdot 181 \cdot 1741\\
5^{16} - 1 &= 152587890624 &&= 2^6 \cdot 3 \cdot 13 \cdot 17 \cdot 313 \cdot 11489\\
5^{17} - 1 &= 762939453124 &&= 2^2 \cdot 409 \cdot 466344409\\
5^{18} - 1 &= 381469...65624 &&= 2^3 \cdot 3^3 \cdot 7 \cdot 19 \cdot 31 \cdot 829 \cdot 5167\\
5^{19} - 1 &= 190734...28124 &&= 2^2 \cdot 191 \cdot 6271 \cdot 3981071\\
5^{20} - 1 &= 953674...40624 &&= 2^4 \cdot 3{\cdot}11{\cdot}13{\cdot}41{\cdot}71{\cdot}521{\cdot}9161
\end{aligned}
$$

$$
\begin{aligned}
7^2 - 1 &= 48 &&= 2^4 \cdot 3\\
7^3 - 1 &= 342 &&= 2 \cdot 3^2 \cdot 19\\
7^4 - 1 &= 2400 &&= 2^5 \cdot 3 \cdot 5^2\\
7^5 - 1 &= 16806 &&= 2 \cdot 3 \cdot 2801\\
7^6 - 1 &= 117648 &&= 2^4 \cdot 3^2 \cdot 19 \cdot 43\\
7^7 - 1 &= 823542 &&= 2 \cdot 3 \cdot 29 \cdot 4733\\
7^8 - 1 &= 5764800 &&= 2^6 \cdot 3 \cdot 5^2 \cdot 1201\\
7^9 - 1 &= 40353606 &&= 2 \cdot 3^3 \cdot 19 \cdot 37 \cdot 1063\\
7^{10} - 1 &= 282475248 &&= 2^4 \cdot 3 \cdot 11 \cdot 191 \cdot 2801\\
7^{11} - 1 &= 1977326742 &&= 2 \cdot 3 \cdot 1123 \cdot 293459\\
7^{12} - 1 &= 13841287200 &&= 2^5 \cdot 3^2 \cdot 5^2 \cdot 13 \cdot 19 \cdot 43 \cdot 181\\
7^{13} - 1 &= 96889010406 &&= 2 \cdot 3 \cdot 16148168401\\
7^{14} - 1 &= 678223072848 &&= 2^4 \cdot 3 \cdot 29 \cdot 113 \cdot 911 \cdot 4733\\
7^{15} - 1 &= 474756...09942 &&= 2 \cdot 3^2 \cdot 19 \cdot 31 \cdot 2801 \cdot 159871\\
7^{16} - 1 &= 332329...69600 &&= 2^7 \cdot 3 \cdot 5^2 \cdot 17 \cdot 1201 \cdot 169553\\
7^{17} - 1 &= 232630...87206 &&= 2 \cdot 3 \cdot 14009 \cdot 2767631689\\
7^{18} - 1 &= 162841...10448 &&= 2^4{\cdot}3^3{\cdot}19{\cdot}37{\cdot}43{\cdot}1063{\cdot}117307
\end{aligned}
$$

Приложение C. Неприводимые и примитивные многочлены

Ниже приведены векторы коэффициентов неприводимых многочленов над $\mathbb{Z}_2$, $\mathbb{Z}_3$ и $\mathbb{Z}_5$. Непримитивные многочлены обозначены *курсивом*. Старшие разряды расположены слева.

Многочлены над $\mathbb{Z}_2$ степени $n = 2, 3, 4, 5, 6, 7, 8, 9$

$n = 2$

111

$n = 3$

1011	1101		

$n = 4$

10011	11001	*11111*	

$n = 5$

100101	101001	101111	110111
111011	111101		

$n = 6$

1000011	*1001001*	*1010111*	1011011
1100001	1100111	1101101	1110011
1110101			

$n = 7$

10000011	10001001	10001111	10010001
10011101	10100111	10101011	10111001
10111111	11000001	11001011	11010011
11010101	11100101	11101111	11110001
11110111	11111101		

$n = 8$

100011011	100011101	100101011	100101101
100111001	*100111111*	101001101	101011111
101100011	101100101	101101001	101110001
101110111	*101111011*	110000111	*110001011*
110001101	*110011111*	*110100011*	110101001
110110001	*110111101*	111000011	111001111
111010111	*111011101*	111100111	*111110011*
111110101	*111111001*		

$n = 9$

1000000011	1000010001	*1000010111*	1000011011
1000100001	1000101101	1000110011	*1001001011*
1001011001	1001011111	*1001100101*	1001101001
1001101111	1001110111	1001111101	1010000111
1010010101	*1010011001*	1010100011	1010100101
1010101111	1010110111	1010111101	1011001111
1011010001	1011011011	1011110101	1011111001
1100000001	1100010011	1100010101	1100011111
1100100011	1100110001	1100111011	*1101001001*
1101001111	1101011011	1101100001	1101101011
1101101101	1101110011	1101111111	1110000101
1110001111	*1110100001*	1110110101	1110111001
1111000111	1111001011	1111001101	1111010101
1111011001	1111100011	1111101001	1111111011

Многочлены над $\mathbb{Z}_3$ степени $n = 2, 3, 4, 5, 6$

$n = 2$

101	112	122

$n = 3$

1021	*1022*	*1102*	*1112*	1121	1201
1211	*1222*				

$n = 4$

10012	10022	*10102*	*10111*	*10121*	*10202*
11002	*11021*	*11101*	*11111*	11122	11222
12002	*12011*	*12101*	12112	*12121*	12212

$n = 5$

100021	*100022*	*100112*	100211	101011	*101012*
101102	*101122*	101201	101221	102101	*102112*
102122	*102202*	102211	*102221*	*110002*	*110012*
110021	110101	110111	*110122*	111011	111121
111211	*111212*	112001	*112022*	*112102*	112111
112201	*112202*	120001	120011	*120022*	*120202*
120212	120221	*121012*	121111	*121112*	*121222*
122002	122021	122101	*122102*	*122201*	*122212*

$n = 6$

1000012	1000022	*1000111*	*1000121*	*1000201*
1001012	*1001021*	*1001101*	*1001122*	*1001221*
1002011	1002022	*1002101*	*1002112*	*1002211*
1010201	1010212	1010222	*1011001*	*1011011*
1011022	1011122	*1012001*	1012012	*1012021*
1012112	*1020001*	*1020101*	1020112	1020122
1021021	*1021102*	1021112	*1021121*	*1022011*
1022102	*1022111*	1022122	1100002	*1100012*
1100111	1101002	*1101011*	*1101101*	1101112
1101212	*1102001*	*1102111*	*1102121*	*1102201*
1102202	*1110001*	*1110011*	1110122	1110202
1110221	1111012	*1111021*	*1111111*	1111112
1111222	*1112011*	*1112201*	1112222	1120102
1120121	1120222	1121012	1121102	*1121122*
1121212	*1121221*	*1122001*	*1122002*	*1122122*
1122202	*1122221*	1200002	*1200022*	*1200121*
1201001	*1201111*	*1201121*	*1201201*	1201202
1202002	*1202021*	*1202101*	1202122	1202222
1210001	*1210021*	1210112	1210202	*1210211*
1211021	*1211201*	1211212	*1212011*	1212022
1212121	1212122	1212212	1220102	*1220111*
1220212	*1221001*	*1221002*	*1221112*	1221202
1221211	1222022	1222102	*1222112*	*1222211*
1222222				

Многочлены над $\mathbb{Z}_5$ степени $n = 2, 3, 4$

$n = 2$

102	*103*	*111*	112	123	*124*
133	*134*	*141*	142		

$n = 3$

1011	*1014*	*1021*	*1024*	1032	1033
1042	1043	*1101*	1102	1113	*1114*
1131	*1134*	*1141*	1143	*1201*	1203
1213	*1214*	1222	1223	1242	*1244*
1302	*1304*	*1311*	1312	1322	1323

1341 1343 1403 *1404* *1411* 1412
1431 *1434* 1442 *1444*

$n = 4$

10002 *10003* *10014* *10024* *10034* *10044*
10102 *10111* 10122 10123 10132 10133
10141 *10203* *10221* *10223* *10231* *10233*
10303 *10311* *10313* *10341* *10343* *10402*
10412 10413 *10421* *10431* 10442 10443
11004 11013 11023 *11024* 11032 *11041*
11042 *11101* 11113 *11114* *11124* *11133*
11142 11202 11212 *11213* *11221* *11222*
11234 *11244* *11301* 11303 *11321* 11342
11344 *11402* *11411* *11414* *11441* 11443
12004 12013 *12014* *12021* 12022 12033
12042 *12102* *12121* 12123 *12131* *12134*
12201 12203 *12211* 12222 *12224* 12302
12311 *12312* *12324* 12332 *12333* *12344*
12401 *12414* *12422* 12433 *12434* *12443*
13004 13012 13023 *13031* 13032 13043
13044 *13102* *13121* *13124* *13131* 13133
13201 13203 13232 *13234* *13241* 13302
13314 13322 *13323* *13334* *13341* *13342*
13401 *13413* 13423 *13424* *13432* *13444*
14004 *14011* 14012 14022 14033 *14034*
14043 *14101* *14112* *14123* *14134* 14143
14144 14202 *14214* *14224* *14231* *14232*
14242 *14243* *14301* 14303 14312 *14314*
14331 *14402* *14411* 14413 *14441* *14444*

Предметный указатель

Н

О

П

P

C

T