серия: естетсвенные науки
математика
информатика

Журавлев Ю.И.
Флеров Ю.А.
Вялый М.Н.

Дискретный анализ. Основы высшей алгебры

МОСКВА
МЗ ПРЕСС

Ю. И. Журавлёв, Ю. А. Флёров,
М. Н. Вялый

Дискретный анализ. Основы высшей алгебры

**Издание второе,
исправленное и дополненное**

Рекомендовано Учебно-методическим объединением высших учебных заведений Российской Федерации по образованию в области прикладных математики и физики в качестве учебного пособия по курсу основ высшей алгебры

МЗ Пресс
Москва 2007

УДК 512.624
ББК 22.144
Ж91

Серия «Естественные науки. Математика. Информатика»

Редакционный совет серии:

Велихов Е. П.
Иванников В. П.
Кингсеп А. С.
Леванов Е. И.
Лобанов А. И. (ответственный секретарь серии)
Ризниченко Г. Ю.
Холодов А. С.
Шананин А. А.

Рецензенты:
Докт. физ.-мат. наук, проф. *В. К. Леонтьев* (ВЦ РАН)
Кафедра математики МИОО

Ю. И. Журавлёв и др.

Ж91 Дискретный анализ. Основы высшей алгебры — Изд. 2, испр. и доп. / Ю. И. Журавлёв, Ю. А. Флёров, М. Н. Вялый — М.: МЗ Пресс, 2007. — 224 с.

Эта книга является учебным пособием по основам высшей алгебры. Она написана на основе материалов курса «Дискретный анализ», проводимого многие годы для студентов ФУПМ МФТИ. В ней излагаются начала теории групп, теории колец и теории полей. Особое внимание уделено конечным полям. В качестве примера приложений конечных полей приводятся начальные сведения по теории кодов, исправляющих ошибки.

Для студентов, специализирующихся на прикладной математике и изучающих высшую алгебру.

ISBN 5–94073–101–5

УДК 512.624
ББК 22.144

©Ю. И. Журавлёв, 2007
©МЗ Пресс, 2007
©В. А. Музыченко,
дизайн обложек серии, 2007

Оглавление

Предисловие

Эта книга написана на основе курса лекций, прочитанных Ю. И. Журавлёвым для студентов факультета управления и прикладной математики Московского физико-технического института. Она посвящена введению в высшую алгебру. В ней рассматриваются основные алгебраические структуры: группы, кольца, поля. Курс лекций, который был положен в основу книги, является частью общего трехсеместрового курса «Дискретный анализ». Поэтому центральную роль в этом курсе играет теория конечных полей, которые являются одним из важнейших инструментов в комбинаторике и теоретической информатике. Одним из классических примеров приложения конечных полей является теория кодов, исправляющих ошибки. В книге дается краткое введение в эту теорию.

Книга содержит много задач. Часть из них — упражнения на понимание материала основной части книги, часть дает представление о дальнейших результатах в теории групп, колец и полей.

Книга предназначена для изучения основ высшей алгебры студентами младших курсов. Наиболее полезной она окажется для студентов, специализирующихся на прикладной математике.

Авторы благодарят всех, кто способствовал выходу этой книги. Особая благодарность — С. Едунову, А. Куракину, А. Мерзакреевой, Н. Пустовойтову и Д. Саянкину, которые взяли на себя нелегкий труд записи и расшифровки лекций.

Введение

Алгебра изучает множества и определенные на них операции. Она занимает центральное место в современной математике. Велика также роль алгебры в приложениях. Этот курс посвящен краткому введению в теорию основных алгебраических систем: групп, колец, полей. Основной темой является построение конечных полей. Эти удивительные объекты, возникающие из чисто алгебраического рассмотрения, играют большую роль в современной комбинаторике и информатике.

Мы приведем лишь один, но очень важный, пример использования конечных полей для решения комбинаторной задачи прикладного характера. Речь идет о теории кодов, исправляющих ошибки.

Появились эти коды в середине прошлого века, когда для передачи секретных сообщений (скажем, приказов в войска) стала активно использоваться радиосвязь. Сообщения нужно было шифровать, а из-за помех при передаче возможны ошибки, которые могут сделать расшифровку невозможной или бессмысленной (или того хуже: осмысленной, но ошибочной). Чтобы повысить надежность сообщения, можно передать каждый символ несколько раз. Скажем, если при передаче азбукой Морзе передавать каждую точку трижды и каждое тире трижды, то одна ошибка в передаче символа не мешает восстановлению исходного сообщения.

Но при таком способе кодирования передаваемых символов длина сообщения (и время передачи) увеличивается в три раза. Естественно возникает вопрос: как кодировать сообщение, чтобы сохранилась устойчивость к ошибкам и не сильно возрастала длина сообщения. Это и есть задача о построении кодов, исправляющих ошибки.

Сравнительно легко можно показать, что существуют «хорошие» коды, в которых нужно использовать немного дополнительных символов. Но для практических нужд одной теоремы существования мало: нужны явные конструкции кодов. Кроме того, естественным практическим требованием является простота декодирования передаваемых сообщений.

Удивительно, но вся теория построения хороших кодов оказывается тесно связанной с алгеброй. Изучив лишь самые основы этой науки, мы сможем построить только простейшие коды такого типа. Они, впрочем, оказываются весьма важными с практической точки зрения благодаря эффективным алгоритмам декодирования.

Этот пример использования алгебры является весьма показательным. Очень часто в комбинаторике встречается именно такая ситуация: можно сравнительно легко доказать, что объекты с некоторыми свойствами существуют (иногда даже, что почти все объекты удовлетворяют нужному свойству), но явно предъявить хотя бы один такой объект намного сложнее. И в очень многих случаях явные конструкции возникают из алгебры.

Несколько слов об истории. Алгебра прошла несколько этапов в своем развитии.

Сейчас решению линейных и квадратных уравнений обучают в средней школе, поэтому кажется, что решать их совсем просто. Но пока не появились буквенные обозначения, знаменитые a, b и c, все квадратные уравнения записывались словами. Представьте, что квадратное уравнение записано так: «возьми известное количество, два раза умноженное на неизвестное количество, добавь к этому второе известное количество, умноженное на неизвестное количество, добавь к этому третье известное количество, в сумме получишь ничего». Вот вам такая задачка, и будьте любезны найти это неизвестное количество. Древние египтяне с этой задачей справились именно в такой формулировке. Правда, учили этому много лет, но когда человек научался, он находил ответ точно в таком же виде, как формулируется задача. Потом на протяжении очень долгого времени делались попытки решить уравнения третьей и четвертой степени. В конце концов решения были получены; это весьма длинная и запутанная история (открыл один,

опубликовал другой, споры о приоритете и т. п.), но в результате мы с вами умеем решать эти уравнения. Далее возникла задача решения уравнения 5-й степени. И вот здесь начались сложности. Долгие безуспешные попытки найти формулу для решения уравнения 5-й степени закончились тем, что Абель доказал невозможность решения этой задачи в радикалах.

Потом появляется Галуа. Он погиб в возрасте 20 лет, но зато оставил после себя работу, которая предопределила развитие алгебры на много лет вперед. Созданные Галуа теории продолжают использоваться в современной математике.

Галуа предложил рассуждение, которое до сих пор является одним из основных средств рассуждений в алгебре. Представьте, что вам надо решить некоторую задачу. Задача сложная и никак не решается. Можно идти двумя путями: можно сесть и решать, решать, решать, ..., а можно пойти по другому пути. Например, пока не придумали мнимые числа, некоторые квадратные уравнения было нельзя решить, а вот когда ввели эту мнимую единичку, все сразу стало просто. Значит, второй способ состоит в том, чтобы расширить множество (чисел) так, чтобы у задачи появилось решение. Галуа предложил очень общий метод решения уравнений. Если они не решаются, надо расширить множество возможных решений, точно так же, как и в случае уравнения второй степени. И он предложил такие расширения, которые позволяют решать уравнения любой степени. Это так называемые расширения Галуа. Эта идея до настоящего времени является одной из основных в современной математике. Если что-то не решается, то, быть может, нужно не биться лбом в стенку, а рассмотреть возможные расширения.

Глава 1

Группы

1.1. Определение и простейшие свойства

Абстрактная современная алгебра отличается от школьной тем, что в ней рассматриваются произвольные операции, удовлетворяющие заданным свойствам (аксиомам).

Мы будем рассматривать только *бинарные операции*, когда операция применяется к двум элементам. Говорят, что на множестве M определена бинарная алгебраическая операция $*$, если для всяких двух его элементов a и b однозначно определен элемент $c = a * b$, называемый *произведением* элементов a и b (порядок операндов важен!). Примерами таких операций могут служить обычные операции сложения, вычитания или умножения на множестве действительных (или комплексных) чисел, операция умножения на множестве квадратных матриц данного порядка, операция композиции на множестве перестановок из n элементов, операция векторного умножения на множестве векторов трехмерного пространства.

Сам термин «произведение» подсказывает, что результат бинарной операции, примененной к элементам a и b, обозначается обычно $a \cdot b$ или даже ab. Это *мультипликативная* запись. Иногда используется *аддитивная* запись $a + b$, особенно в тех случаях, когда на одном множестве рассматриваются сразу две операции. Когда используется аддитивная запись, результат операции обычно называется *суммой*.

В общем случае операция применяется к упорядоченному набору из n элементов множества M (и называется тогда n-арной). Но нас такой общий случай интересовать не будет.

По определению алгебраическая операция отличается тем, что ее результат не выводит из множества M (говорят также, что M замкнуто относительно определенной на нём алгебраической операции). Этим алгебра принципиально отличается от математического анализа. В математическом анализе есть операции, которые выводят из множества. Например, операция нахождения производной непрерывной функции вовсе не обязательно дает непрерывную функцию. В алгебре такое исключено.

Рассмотрим несколько примеров алгебраических аксиом и задаваемых ими алгебраических структур.

Полугруппы. Имеется единственная аксиома $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Такое свойство называется *ассоциативностью*. Множество с одной операцией, от которой требуется только ассоциативность и ничего больше, называется *полугруппой*. Мы ими заниматься не будем. Полугруппы встречаются довольно часто. Например, они важны для одной из современных математических теорий — так называемой теории автоматов.

Пример 1.1. Пусть A — конечное множество. *Словом* в алфавите A называется конечная последовательность элементов A. Множество слов в алфавите A обозначается A^*. Для слов определена операция *конкатенации*: дописывание одного слова вслед за другим. Например, конкатенация aa и bb дает $aabb$. Множество слов с операцией конкатенации образует полугруппу. Действительно, результат конкатенации слов u, v, w в каждом из двух случаев $(uv)w$ и $u(vw)$ — это слово, которое получается последовательным выписыванием символов слова u, за которыми следуют символы слова v, за которыми следуют символы слова w.

Пример 1.2. *Отображение* множества X в множество Y ставит в соответствие каждому элементу множества X некоторый элемент множества Y (можно считать слова «отображение» и «функция» синонимами). Обычно отображение f множества X в множество Y обозначается как $f\colon X \to Y$, а записи

$f\colon x \mapsto y$ и $f(x) = y$ означают, что отображение f ставит в соответствие элементу x элемент y (y называется *образом* x). Если для каждого элемента y из множества Y существует хотя бы один элемент x из множества X такой, что $f\colon x \mapsto y$ (x в этом случае называется *прообразом* y), то отображение f называется *отображением на множество* Y.

На отображениях множества X в себя определена операция *композиции* (последовательного выполнения). Если f, g — два отображения, то их композиция $F = f \circ g$ задается формулой $F(x) = f(g(x))$. Отображения множества в себя с операцией композиции также образуют полугруппу:

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

Обратите внимание, что в обоих примерах порядок операндов существенен.

Моноиды. Следующая алгебраическая структура — это множество с такой операцией, для которой кроме ассоциативности требуется еще наличие *единицы*, т. е. такого элемента, произведение с которым слева и справа оставляет любой другой элемент неизменным. Дополнительно мы потребуем, чтобы единичный элемент был единственным. Итак, имеем две аксиомы:

M1: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (ассоциативность);

M2: (аксиома единицы) существует единственный единичный элемент e такой, что для любого x выполняется $e \cdot x = x \cdot e = x$.

Множество с ассоциативной и обладающей единицей операцией называется *моноидом*.

Рассмотренные выше примеры являются не только полугруппами, но и моноидами. В множестве слов единичным элементом относительно конкатенации является *пустое слово* (последовательность длины 0). В множестве отображений единичным элементом относительно композиции является *тождественное отображение*: $\mathrm{id}\colon x \mapsto x$.

Замечание 1.3. Поскольку результат операции, вообще говоря, зависит от порядка операндов, иногда бывают нужны

левые и *правые* единицы. Элемент e называется левой единицей, если для любого x выполнено $ex = x$. Аналогично, для правой единицы выполняется тождество $xe = x$.

Группы. Группа $G = \langle M, * \rangle$ — это такая пара из множества M и бинарной операции $*$ на этом множестве, что выполняются следующие свойства (аксиомы группы):

G1: $(x * y) * z = x * (y * z)$ (ассоциативность);

G2: (аксиома единицы) существует единственный единичный элемент e такой, что для любого x выполняется $e * x = x * e = x$;

G3: для любого элемента x существует ровно один *обратный элемент*, т. е. такой элемент y, для которого $y*x = x*y = e$ (обратный элемент обозначается x^{-1}).

Группы с добавленным свойством коммутативности операции $a*b = b*a$ называются *коммутативными* или *абелевыми* (по имени норвежского математика Абеля, который их изучал).

При использовании мультипликативной записи $x \cdot y$ или xy единичный элемент группы традиционно называется единицей и обозначается e или 1. При аддитивной записи единичный элемент называется нулем и обозначается 0. Вместо термина «обратный» при аддитивной записи используется термин «противоположный». Противоположный к элементу y обозначается $-y$. Аддитивная запись обычно (но далеко не всегда) используется для обозначения коммутативных операций.

Группа называется *конечной*, если в ней (а точнее — во множестве M) конечное число элементов, которое называется *порядком* группы.

Посмотрим на простейшие формальные следствия из групповых аксиом.

Первая аксиома группы означает независимость результата применения нескольких операций от расстановки скобок. По индукции можно распространить ее на сколь угодно длинные

выражения. Другими словами, если есть конечная последовательность элементов группы $a_1, a_2, \ldots, a_n$, то имеется однозначно определенный элемент группы

$$a_1 a_2 \ldots a_n,$$

который не зависит от того, в каком порядке расставлены скобки в этом выражении. Докажем это утверждение формально.

Будем доказывать индукцией по числу сомножителей n, что при любой расстановке скобок произведение элементов $a_1, \ldots, a_n$ равно $a_1(a_2(\ldots a_n)\ldots)$. Основание индукции $n = 3$ — это аксиома ассоциативности. Пусть утверждение доказано для произведений n элементов. Рассмотрим произведение $(n+1)$-го элемента. Оно имеет вид $L \cdot R$, где в L и R элементов не больше n. Поэтому по предположению индукции $L = a_1 \cdot L'$, а $L \cdot R = (a_1 \cdot L') \cdot R = a_1 \cdot (L' \cdot R)$. В $L' \cdot R$ всего n элементов, так что можно еще раз применить предположение индукции и вывести справедливость доказываемого утверждения для произведений $(n+1)$-го элемента.

Вторая и третья групповые аксиомы очень важны, потому что позволяют решать уравнения простейшего вида $ax = b$ и $xa = b$:

$$ax = b \quad \Leftrightarrow \quad a^{-1}ax = a^{-1}b \quad \Leftrightarrow \quad x = a^{-1}b,$$
$$xa = b \quad \Leftrightarrow \quad xaa^{-1} = ba^{-1} \quad \Leftrightarrow \quad x = ba^{-1}$$

(знаком $\Leftrightarrow$ обозначается равносильность утверждений).

Решения уравнений указанного вида в числах проходят в младших классах школы и дальнейшая школьная алгебра на них опирается. Если выполнены групповые аксиомы в какой-нибудь более сложной ситуации (скажем, для движений пространства), то некоторые привычные равенства останутся справедливыми. Обычно проверять групповые аксиомы проще, чем проверять разрешимость линейных уравнений (чтобы это почувствовать, попробуйте решить уравнение $ax = b$, где a — поворот вокруг оси z на 90° против часовой стрелки, b — поворот вокруг оси x на 90° по часовой стрелке).

Очень важно свойство *сократимости*: если взять два неравных элемента группы $a \neq b$ и умножить их на один и тот же элемент c, то снова получатся неравные элементы: $ac \neq bc$. Это совершенно очевидно: если $ac = bc$, то и $acc^{-1} = bcc^{-1}$, поэтому

$a = b$. Аналогичное свойство выполняется и для умножения слева.

В качестве еще одного примера использования групповых аксиом проверим полезное равенство $(ab)^{-1} = b^{-1}a^{-1}$, которое выражает обратный к ab элемент группы через обратные к a и b. Имеем

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e.$$

Здесь первое равенство получается после двух применений аксиомы ассоциативности, второе следует из определения обратного, третье — из аксиомы единицы, последнее — опять из определения обратного. Равенство $(ab)(b^{-1}a^{-1}) = e$ проверяется аналогично.

Свойство сократимости облегчает перечисление небольших групп. Операцию в конечной группе естественно задавать таблицей, строки которой индексированы первыми операндами[1)], столбцы — вторыми операндами, а в каждой клетке записан результат применения операции. Такая таблица называется *таблицей Кэли* (или *таблицей умножения*). Свойство сократимости означает, что в каждую строку и в каждый столбец таблицы Кэли каждый элемент группы входит не более одного раза. А поскольку число строк и число столбцов таблицы равно числу элементов группы, то можно утверждать, что каждый элемент группы входит в каждую строку и каждый столбец ровно один раз.

Для группы из двух элементов таблица будет выглядеть так:

$\cdot$	e	a
e	?	?
a	?	?

.

Три клетки заполняются по аксиоме единицы:

$\cdot$	e	a
e	e	a
a	a	?

.

С учетом свойства сократимости в четвертую клетку можно

[1)] Разумеется, чтобы записать таблицу на бумаге, нужно приписать всем элементам группы какие-то имена (символы).

поставить только e. Можно проверить, что таблица

$\cdot$	e	a
e	e	a
a	a	e

задает группу. Значит, существует единственная группа из двух элементов. Единственность здесь нельзя понимать буквально. Реализация группы может быть очень сложной: придавая разный смысл элементам e, a и групповой операции, можно получать содержательно разные примеры. Один из самых употребительных примеров группы второго порядка — множество чисел $\{-1, +1\}$ относительно операции умножения.

Аналогичный анализ можно проделать и для групп с тремя элементами. В этом случае также есть только одна группа.

Аксиома единицы оставляет незаполненными четыре клетки в таблице Кэли группы из трех элементов:

$\cdot$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

.

В центральной клетке не может стоять a. Если в ней стоит e, то приходим к противоречию со свойством сократимости: в третьем столбце второй строки должно стоять b, но в третьем столбце b уже есть. Получаем единственную возможность

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

Обратите внимание, что заполненные части первой строки и первого столбца таблицы Кэли совпадают с первой строкой и первым столбцом той части таблицы, которая выделена линиями (единичный элемент стоит первым). В дальнейшем при задании группы таблицей Кэли мы будем придерживаться этого соглашения — единичный элемент стоит первым — и будем опускать ту часть таблицы, которая лежит слева и сверху от линий.

Классическая реализация группы из двух элементов имеет вид: $e = 0$, $a = 1$, групповая операция — сложение по модулю 2 (суммируем и берем остаток от деления на 2). Аналогично для группы из трех элементов: $e = 0$, $a = 1$, $b = 2$, операция — сложение по модулю 3. Примеры групп из четырех, пяти и т. д. элементов получаются точно так же.

Из этих примеров можно увидеть, что для любого натурального n имеется хотя бы одна группа с n элементами. Сколько есть существенно разных групп с n элементами? Это трудная задача, которая до сих пор в общем случае не решена. (Точный смысл слов «существенно разных» — неизоморфных, см. ниже раздел 1.6.)

1.2. Примеры групп

Различных групп существует очень много, и они не обязательно конечные. Теория групп пронизывает сегодня всю математику: от геометрических доказательств до теории кодов, исправляющих ошибки. В этом разделе мы приводим основные примеры групп.

1.2.1. Примеры абелевых групп

Пример 1.4 (*числовые группы*). Все обычные числовые системы: целые $\mathbb{Z}$, рациональные $\mathbb{Q}$, действительные $\mathbb{R}$, комплексные числа $\mathbb{C}$ — образуют абелевы группы относительно сложения. Множество отличных от нуля чисел (рациональных $\mathbb{Q}^*$, действительных $\mathbb{R}^*$, комплексных $\mathbb{C}^*$) также образует группу относительно умножения. Проверка групповых аксиом во всех этих случаях не представляет труда.

Пример 1.5. Важный для нас пример абелевой группы — группа бинарных наборов длины n. *Бинарные наборы* — это последовательности из 0 и 1. Операция над ними — покомпонентное сложение по модулю 2. Суммой двух бинарных наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, $\alpha_i, \beta_i \in \{0, 1\}$ называется

$$\tilde{\alpha} \oplus \tilde{\beta} = ((\alpha_1 + \beta_1) \bmod 2,\ \ldots,\ (\alpha_n + \beta_n) \bmod 2)$$

(используем аддитивную запись групповой операции). Нулем этой группы является $\tilde{0} = (0, 0, \ldots, 0)$. Каждый ненулевой элемент совпадает со своим противоположным (напомним, что противоположный — это обратный элемент, когда используется аддитивная запись операции). Ассоциативность очевидна.

1.2.2. Группы преобразований

Пример 1.6. У отображения множества X в себя может не быть обратного относительно операции композиции отображений. Но если рассмотреть множество *взаимно однозначных отображений* множества X на себя (*биекций*), то оно относительно операции композиции отображений образует группу, которая обозначается $S(X)$. Отображение $\varphi\colon X \to X$ называется взаимно однозначным, если для любого элемента $x_1 \in X$ существует ровно один $x_2 \in X$ такой, что $\varphi\colon x_2 \mapsto x_1$. Отображение $\varphi^{-1}\colon X \to X$, задаваемое правилом $\varphi^{-1}\colon x_1 \mapsto x_2$, будет обратным к φ в группе $S(X)$.

Многие важные примеры групп — это группы биекций с дополнительными условиями. Их мы будем называть группами преобразований.

Пример 1.7. *Движения* пространства (преобразования, сохраняющие расстояние между точками), образуют группу относительно операции композиции отображений. Ясно, что композиция движений — движение, и обратное к движению — также движение.

Пример 1.8 (*матричные группы*). Матрицы с ненулевым определителем образуют группу относительно операции матричного умножения. Эта группа обозначается $GL(n)$ (n — размер матриц). Она имеет прямое отношение к группам преобразований, поскольку матрицами размера $n \times n$ записываются линейные преобразования n-мерного пространства, а матричное умножение соответствует композиции преобразований.

Выделяя матрицы специального вида, получаем новые примеры матричных групп. В частности, если ограничиться ортогональными матрицами, удовлетворяющими условию $X^T = X^{-1}$ (транспонированная матрица совпадает с обратной),

то получим группу $O(n)$, которая соответствует движениям n-мерного пространства, оставляющим на месте начало координат (*ортогональная группа*).

Мы ничего не сказали об элементах матриц. Это еще одна степень свободы при выборе матричных групп. От элементов матриц требуется немногое — их нужно складывать и умножать по обычным законам арифметики. Например, можно рассматривать группы матриц с рациональными, действительными или комплексными коэффициентами (важно понимать, что это совершенно разные группы!). Позже мы рассмотрим другие примеры алгебраических систем, допускающих такие операции. Пока будем считать (если не оговорено противное), что элементы матриц — действительные числа.

Пример 1.9 (*группа перестановок или симметрическая группа*). Это важный частный случай группы преобразований. По определению, $S_n = S(X)$, где $X = \{1, 2, \ldots, n\}$. Таким образом, *перестановки* — это взаимно однозначные отображения множества $\{1, 2, \ldots, n\}$ на себя.

Перестановки можно записывать в виде таблицы

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & i & \ldots & n \\ t_1 & t_2 & t_3 & \ldots & t_i & \ldots & t_n \end{pmatrix},$$

порядок столбцов которой несущественен.

В таких обозначениях легко написать произведение перестановок (композицию отображений):

$$\begin{pmatrix} t_1 & t_2 & t_3 & \ldots & t_i & \ldots & t_n \\ v_1 & v_2 & v_3 & \ldots & v_i & \ldots & v_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \ldots & i & \ldots & n \\ t_1 & t_2 & t_3 & \ldots & t_i & \ldots & t_n \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & 3 & \ldots & i & \ldots & n \\ v_1 & v_2 & v_3 & \ldots & v_i & \ldots & v_n \end{pmatrix}.$$

Заметьте, что произведение $\pi \circ \sigma$ — это перестановка, которая получается применением перестановки σ, а затем перестановки π. Такой порядок соответствует принятому порядку записи композиции функций: $(\pi \circ \sigma)(i) = \pi(\sigma(i)) = \pi(t_i) = v_i$.

Единица группы перестановок соответствует тождественному отображению

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & i & \ldots & n \\ 1 & 2 & 3 & \ldots & i & \ldots & n \end{pmatrix}.$$

Обратная перестановка

$$\begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & n \\ t_1 & t_2 & t_3 & \dots & t_i & \dots & t_n \end{pmatrix}^{-1} = \begin{pmatrix} t_1 & t_2 & t_3 & \dots & t_i & \dots & t_n \\ 1 & 2 & 3 & \dots & i & \dots & n \end{pmatrix}.$$

Группа перестановок S_n некоммутативна при $n \geqslant 3$. Вот простой пример, когда произведение перестановок трех элементов зависит от порядка множителей:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq$$
$$\neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \quad (1.1)$$

Перестановку также можно задать, указав ее *цикловое разложение*:

$$\pi = (i_1^1 i_2^1 \dots i_{k_1}^1)(i_1^2 i_2^2 \dots i_{k_2}^2) \dots (i_1^{c(\pi)} i_2^{c(\pi)} \dots i_{k_{c(\pi)}}^{c(\pi)}). \quad (1.2)$$

Внутри каждой пары скобок числа переставляются циклически: $\pi(i_1) = i_2$, $\pi(i_2) = i_3$, …, $\pi(i_k) = i_1$. Цикловое разложение определено с точностью до циклических сдвигов чисел внутри скобок. Часто используется сокращенная цикловая запись перестановки, при которой циклы длины 1 пропускаются. Тождественная перестановка при такой сокращенной записи выглядит как пара скобок: (). Цикловая запись более компактна. Вот, скажем, как выглядит формула (1.1) в цикловой записи:

$$(123) \circ (23) = (12) \neq (13) = (23) \circ (123).$$

1.2.3. Группы симметрии

Совокупность преобразований, совмещающих объект с самим собой, называется *группой симметрии объекта*.

Объекты могут быть разной природы: геометрические тела, молекулы, дифференциальные уравнения, функции и т. п. Главное, чтобы они не менялись при каких-либо преобразованиях. Преобразования бывают дискретными или непрерывными. Если преобразования дискретные и их конечное число, группа, естественно, оказывается конечной.

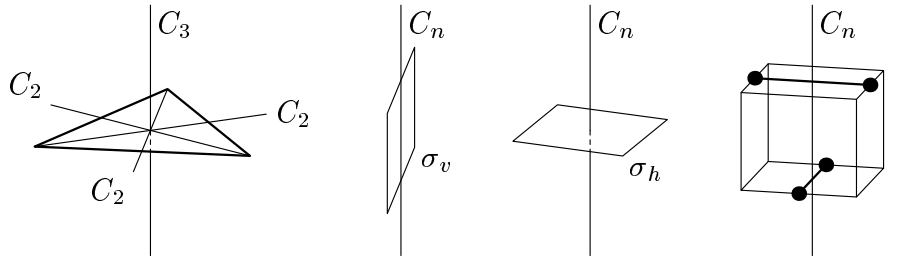


Рис. 1.1. а) Группа вращений правильного треугольника включает в себя ось третьего порядка C_3 и три оси второго порядка C_2.
б) Вертикальная зеркальная плоскость σ_v и горизонтальная σ_h.
в) «Молекула», имеющая зеркально-поворотную ось четвертого порядка S_4.

Группа симметрии молекулы состоит из конечного числа движений, под действием которых молекула переходит сама в себя. Все такие преобразования (элементы симметрии) оставляют на месте по крайней мере одну точку, поэтому такие группы называют точечными.

Пример 1.10 (*группа треугольника*). Примером точечной группы является группа треугольника D_3 (рис. 1.1 а). В данной группе два существенно разных элемента симметрии: ось третьего порядка C_3 и перпендикулярная ей ось второго порядка C_2. Из-за наличия оси третьего порядка появляется три оси второго порядка.

Всего в группе треугольника 6 элементов: тождественное преобразование, два поворота вокруг оси C_3 и три поворота вокруг осей C_2.

В общем случае в точечной группе могут быть только три вида элементов:

1: Поворот C_n на угол $2\pi/n$ вокруг оси n-го порядка.

2: Отражение σ_v в плоскости, проходящей через ось, или в плоскости σ_h, перпендикулярной оси. Индексы v, h ука-

зывают на вертикальную или горизонтальную плоскость в предположении, что ось n-го порядка является вертикальной, рис. 1.1 б).

3: Зеркальный поворот $S_{2n} = \sigma_h C_{2n}$, т. е. поворот с отражением в горизонтальной плоскости. Чтобы после поворота на 2π молекула возвратилась в исходное состояние, порядок зеркально-поворотной оси должен быть четным, рис. 1.1 в).

В пространственных группах, описывающих симметрию бесконечных пространственных кристаллов, к поворотам и отражениям добавляются трансляции (переносы) на постоянную решетки и их композиции с поворотами или отражениями. Пространственные группы могут быть как конечными, так и бесконечными.

Пример 1.11 (*группа диэдра или диэдральная группа*). Это группа симметрий правильной призмы (или правильного n-угольника). Она обозначается D_n. Легко понять, что в этой группе есть ось n-го порядка C_n и n перпендикулярных ей осей второго порядка C_2 (на рис. 1.2 изображены отдельно случай четного n и случай нечетного n).

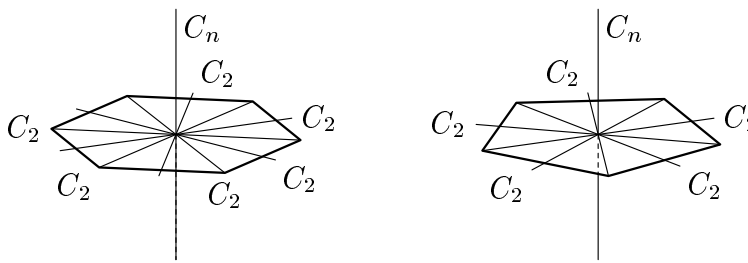


Рис. 1.2. Группы D_6 и D_5

В группе D_n всего $2n$ элементов: тождественное преобразование, $n-1$ поворот вокруг оси C_n и n поворотов вокруг осей C_2.

Пример 1.12. Обыкновенное дифференциальное уравнение

$$\frac{dy}{dx} = f\left(\frac{x}{y}\right)$$

инвариантно относительно преобразований растяжения

$$x \mapsto \lambda x,\ y \mapsto \lambda y, \quad \lambda \neq 0.$$

Такое уравнение называется однородным и решается с помощью перехода к новой переменной $z = y/x$. Все растяжения с разными λ образуют группу R, которая, очевидно, бесконечная и непрерывная. Чтобы задать преобразование из этой группы, требуется задать параметр λ. Количество параметров, необходимое для однозначного задания преобразования из непрерывной группы симметрии, называется размерностью и обозначается dim. В нашем примере $\dim R = 1$.

Пример 1.13 (*группы правильных многогранников*). Группа (правильного) многогранника состоит из *вращений* этого многогранника, совмещающих многогранник с самим собой. Вращения — это не все симметрии многогранника (среди которых могут быть, например, зеркальные отражения), а только повороты.

1.3. Циклические группы

Эти группы наиболее просто устроены. В *циклической группе* есть такой элемент (он называется *порождающим элементом* группы), что каждый элемент группы может быть получен (многократным) применением групповой операции к порождающему.

Чтобы разобраться с циклическими группами, введем несколько простых обозначений, которые понадобятся и в дальнейшем. Единицу мы будем обозначать как нулевую степень произвольного элемента: $e = a^0$. (Это просто полезное условное обозначение. Его можно считать определением a^0.) Далее, результат n-кратного применения операции к элементу a будем обозначать a^n:

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ раз}}.$$

В аддитивной записи та же самая степень обозначается na.

Проверим, что

$$(a^n)^{-1} = (a^{-1})^n \tag{1.3}$$

прямым вычислением (в нём мы используем, что a и a^{-1} коммутируют):

$$\big(\underbrace{a\cdot a\cdot\ldots\cdot a}_{n\text{ раз}}\big)\cdot\big(\underbrace{a^{-1}\cdot a^{-1}\cdot\ldots\cdot a^{-1}}_{n\text{ раз}}\big)=$$
$$=\big(\underbrace{(a\cdot a^{-1})\cdot\ldots\cdot(a\cdot a^{-1})}_{n\text{ раз}}\big)=e.$$

Равенство (1.3) позволяет однозначно понимать выражение a^{-n} ($-na$ в аддитивной записи) и дает определение отрицательной степени.

Все остальные свойства степени, к которым мы привыкли в обычной арифметике, здесь тоже сохраняются. Например:

$$a^n\cdot a^m=\big(\underbrace{a\cdot a\cdot\ldots\cdot a}_{n\text{ раз}}\big)\cdot\big(\underbrace{a\cdot a\cdot\ldots\cdot a}_{m\text{ раз}}\big)=\big(\underbrace{a\cdot a\cdot\ldots\cdot a}_{n+m\text{ раз}}\big)=a^{n+m}. \tag{1.4}$$

Так же легко получить еще одно привычное равенство

$$\big(a^n\big)^m=a^{nm}.$$

Теперь посмотрим на то, как устроены циклические группы. Есть два случая.

1. Все степени порождающего элемента различны. Группа состоит из элементов

$$\ldots,a^{-2},a^{-1},a^0,a^1,a^2,\ldots\ ,$$

а операция однозначно определена равенствами (1.3) – (1.4). По существу, это группа целых чисел по сложению. Это становится очевидным, если переписать предыдущую строчку в аддитивной записи

$$\ldots,-3a,-2a,-a,0,a,2a,3a,\ldots\ .$$

2. Две различные степени порождающего элемента совпадают:

$$a^{n+m}=a^n,\quad n,m\text{ — целые, }m\neq 0.$$

Но тогда

$$a^{n+m}=a^na^m=a^n,\ \text{т. е. } a^m=e.$$

Обозначим через q наименьшее натуральное m, для которого $a^m=e$ (это число называется *порядком элемента* a).

Докажем, что элементы циклической группы в этом случае — это $e = a^0$, a^1, $\ldots$, a^{q-1}, причем все перечисленные элементы различны. Действительно, если $a^t = a^l$, $1 \leqslant l < t \leqslant q-1$, то $a^{t-l} = e$ и приходим к противоречию с выбором q (так как $t - l < q$). Рассмотрим какой-нибудь элемент группы, он имеет вид a^n. Разделим n на q с остатком: $n = sq + m$, $0 \leqslant m < q$. Тогда

$$a^n = a^{sq+m} = a^{sq}a^m = \left(a^q\right)^s a^m = ea^m = a^m.$$

Циклическая группа из n элементов обозначается C_n.

Пример 1.14 (*корни из единицы*). Комплексное число z называется корнем из единицы порядка n, если $z^n = 1$. Можно проверить, что относительно умножения корни из единицы образуют группу, и эта группа циклическая.

Пример 1.15. Степени любого элемента a в любой группе образуют циклическую группу. Свойство ассоциативности в данном случае выполняется тривиально, единица — та же самая, что и в исходной группе. Согласно проделанным выше вычислениям, произведение степеней является степенью, обратный элемент также является степенью. Элемент a является порождающим. Обратите внимание, что каждый элемент исходной группы может породить свою группу. Группу, порожденную элементом a, мы будем обозначать $\langle a \rangle$.

1.4. Подгруппы

Предположим, что имеется некоторая группа G, и для какого-то подмножества элементов $H \subset G$ выполнены свойства

1: $e \in H$;

2: если $a, b \in H$, то $a \cdot b \in H$;

3: если $a \in H$, то $a^{-1} \in H$.

Такое множество H является группой относительно той же операции, что и в исходной группе. Ассоциативность проверять не надо, поскольку ассоциативна G, остальные групповые

аксиомы сразу следуют из приведенных выше свойств. Подмножество H, удовлетворяющее перечисленным выше свойствам, называется *подгруппой* G. Для указания на то, что H является подгруппой G мы будем использовать обозначение $H < G$.

Выше уже был приведен пример подгруппы — подгруппа, порожденная элементом группы.

Нам понадобится очень просто доказываемая теорема.

Теорема 1.16. *H — подгруппа группы G тогда и только тогда, когда для любых $a, b \in H$ выполнено $ab^{-1} \in H$. Формально это можно записать как*

$$H < G \;\Leftrightarrow\; ab^{-1} \in H \text{ для всех } a, b \in H.$$

Доказательство. Если H — подгруппа, то для любых $a, b \in H$ из свойств 3 и 2 подгруппы следует, что $ab^{-1} \in H$.

Теперь докажем необходимость. Пусть для любых $a, b \in H$ выполнено $ab^{-1} \in H$. Возьмем любой элемент $a \in H$. Тогда $e = a \cdot a^{-1} \in H$ (свойство 1). Выбрав пару $e, a \in H$, убеждаемся, что $ea^{-1} = a^{-1} \in H$ (свойство 3). Поскольку $(b^{-1})^{-1} = b$, то $ab = a(b^{-1})^{-1}$ и свойство 2 также выполнено. □

Вот пример использования теоремы 1.16.

Утверждение 1.17. *Пересечение подгрупп — подгруппа.*

Доказательство. Пусть $a, b \in H_1 \cap H_2$, где $H_1 < G$, $H_2 < G$. Тогда $ab^{-1} \in H_1$, $ab^{-1} \in H_2$. Значит, $ab^{-1} \in H_1 \cap H_2$. Из теоремы 1.16 следует, что $H_1 \cap H_2$ — подгруппа. □

Рассмотрим еще несколько конструкций подгрупп.

Пример 1.18. *Центром* группы G называется множество $C(G)$ тех ее элементов, которые коммутируют со всеми элементами группы:

$$C(G) = \{x \in G \mid \forall\, g \in G\ gx = xg\}.$$

Центр группы всегда не пуст ($e \in C(G)$). Если группа коммутативна, то $C(G) = G$. Докажем, что центр является подгруппой. Проверим выполнение свойств подгруппы для центра.

Очевидно, что для любого $g \in G$

$$ge = eg. \qquad \text{(свойство 1)}$$

Если $x_1, x_2 \in C(G)$, то из ассоциативности умножения получаем

$$g(x_1x_2) = x_1gx_2 = (x_1x_2)g. \qquad \text{(свойство 2)}$$

Наконец, если $x \in C(G)$, то умножим равенство $gx = xg$ слева на x^{-1}, получим $x^{-1}gx = x^{-1}xg = g$. Умножая полученное равенство на x^{-1} справа, получим $x^{-1}g = gx^{-1}$, значит, $x^{-1} \in C(G)$. Это свойство 3 из определения подгруппы.

Введем одно полезное обозначение. Пусть A, B — подмножества элементов группы G. Тогда «умножение» подмножества A на подмножество B дает подмножество AB элементов группы, состоящее из всех попарных произведений ab, $a \in A$, $b \in B$. При умножении одноэлементного подмножества $\{x\}$ фигурные скобки для краткости записи опускаются.

Пример 1.19. *Нормализатором* $N(S)$ подмножества $S \subset G$ элементов группы G называется множество таких ее элементов g, что выполнено равенство $Sg = gS$. Нормализатор $N(S)$ всегда не пуст ($e \in N(S)$). Если группа коммутативна, то $N(S) = G$.

Доказательство того, что нормализатор любого подмножества является подгруппой, аналогично предыдущему примеру.

А теперь перейдем к некоторой конструкции, которая в алгебре и в огромном букете математических направлений, вырастающих из алгебры, играет огромную роль. Рассмотрим как происходит принятие решений в некоторых сложных ситуациях. Скажем, министр хочет знать как обстоят дела в министерстве. Вся информация может представлять собой стопку бумаги в десятки тысяч листов. Никакой человек не сможет оперативно обрабатывать такие объемы информации. Поэтому по запросу министра вся информация не предоставляется ему в чистом виде, а обобщается (агрегируется). По-научному это называется «принцип агрегирования информации». Весь огромный объем информации представляется в виде отдельных сообщений, которые объединяются в группы, и этим группам присваиваются новые названия. И в результате получается уже другая информация. Мы рассмотрим простейший пример такого рода на основе групп: будем агрегировать или обобщать по отношению к данной подгруппе.

Далеко не сразу можно понять, что приводимая ниже теорема имеет отношение к описанной выше ситуации.

Рассмотрим некоторую подгруппу H группы G, а также некоторый элемент группы $x \in G$. Множество xH в соответствии со введенным выше обозначением является множеством тех элементов группы G, которые получаются из элементов подгруппы H умножением на x слева:

$$xH = \{xh \mid h \in H\}.$$

Множество xH называется *смежным классом по подгруппе* H с представителем (смежного класса) x. Поскольку умножение на x произошло слева, то говорят, что это *левый смежный класс*. Если же умножать на x справа, то получится *правый смежный класс*. Если операция некоммутативна, эти классы могут различаться. Для коммутативной группы всегда выполнено равенство $xH = Hx$. В этом случае можно просто говорить о смежном классе. Имеет место очень важная теорема.

Теорема 1.20 (теорема о смежных классах). *Смежные классы xH и yH либо не пересекаются, либо совпадают.*

Доказательство. Предположим, что у двух смежных классов нашелся общий элемент z. Тогда $z = xh_i = yh_j$. Отсюда получаем $x = y(h_j h_i^{-1}) \in yH$, $y = x(h_i h_j^{-1}) \in xH$, т. е. представитель одного класса принадлежит другому.

Дальше всё просто. Пусть $w \in xH$, т. е. $w = xh'$. Но $x = yh_x$, значит, $w = y(h_x h') \in yH$. Таким образом, $xH \subseteq yH$. Совершенно аналогично доказывается включение в противоположную сторону. Значит, $xH = yH$. Мы доказали, что смежные классы совпадают, если у них есть хотя бы один общий элемент. □

Пример 1.21. Рассмотрим группу $\mathbb{R}^2$, которая состоит из пар действительных чисел с операцией покомпонентного сложения:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

(используем здесь аддитивную запись). В этой группе есть подгруппа R, состоящая из пар $(x, 0)$, $x \in \mathbb{R}$ (проверку свойств подгруппы оставляем читателю в качестве полезного упражнения).

Смежными классами будут множества $R_a = \{(x, y) \mid y = a, x \in \mathbb{R}\}$. Это очевидно, так как пары с совпадающей второй компонентой отличаются на элемент из R:

$$(x_1, a) = (x_2, a) + (x_1 - x_2, 0).$$

Пример 1.22. Рассмотрим некоммутативную группу S_3 и в ней подгруппу $H = \langle(12)\rangle$ (используем сокращенную цикловую запись перестановок). Запишем смежные классы по этой подгруппе

H :	()	(12)
$(23)H$:	(23)	(132)
$(13)H$:	(13)	(123)

Поскольку элемент g группы G принадлежит смежному классу gH по подгруппе H, то вся группа G разбивается на объединение смежных классов по H (в данном случае левых, хотя то же самое верно и для правых смежных классов):

$$G = \dot{\bigcup_i} g_i H.$$

Количество смежных классов группы G по подгруппе H называется *индексом подгруппы* и обозначается через $(G : H)$. (Если смежных классов по H бесконечно много, то H называется подгруппой бесконечного индекса.)

Докажем, что если H конечна, то количество элементов во всех смежных классах одинаково, т. е. $|g_i H| = |g_j H|$ для любых $g_j, g_j \in G$.

Рассмотрим отображение $L_a\colon h \mapsto ah$, которое каждому элементу h подгруппы H ставит в соответствие элемент ah смежного класса aH. Это взаимно однозначное отображение (по свойству сократимости из $ah_1 = ah_2$ следует $h_1 = h_2$), поэтому $|H| = |aH|$ (т. е. количество элементов H совпадает с количеством элементов aH). Поскольку вся группа представлена в виде объединения смежных классов, то количество элементов в группе будет равно количеству элементов в каждом смежном классе, умноженному на количество смежных классов по подгруппе (индекс H в группе G). Итак, мы доказали важную теорему.

Теорема 1.23 (теорема Лагранжа). *Пусть H — подгруппа группы G. Тогда порядок H является делителем порядка G:*

$$|G| = (G : H) \cdot |H|.$$

В каком смысле нужно понимать это равенство? Для бесконечных групп его трактовка требует дополнительных уточнений[2)]. Мы будем понимать его в следующем смысле: если любые два сомножителя в равенстве конечны, то конечен и третий множитель, и выполняется указанное соотношение.

В чем прелесть доказанного утверждения? Если у вас спросят, сколько различных подгрупп у группы порядка 17, то можно мгновенно ответить: две. Единичная подгруппа, состоящая только из единичного элемента, и сама группа. Эти тривиальные или *несобственные* группы являются подгруппами. А нетривиальных подгрупп у группы порядка 17 быть не может, поскольку число 17 — простое.

Следствие 1.24. *Группа простого порядка не имеет нетривиальных подгрупп.*

Теорема 1.25. *Порядок любого элемента есть делитель порядка группы.*

Почему так получается? По теореме Лагранжа порядок любой подгруппы делит порядок группы. Осталось вспомнить, что степени любого элемента образуют группу.

Отсюда следует, что если порядок группы G — простое число n, то G — циклическая группа, и любой элемент G, отличный от единицы, является порождающим для G. Действительно, возьмем любой элемент $g \in G$, не равный единице. Порядок g должен быть делителем порядка группы, поэтому он равен n. Таким образом, все степени любого элемента исчерпывают всю группу.

Замечание 1.26. Обращение теоремы Лагранжа неверно: существуют такие группы порядка n, что в них нет подгрупп порядка k, где $k \mid n$. Простейший пример приведен в задаче 1.31 е).

[2)] Равенство будет выполняться для кардинальных чисел, которые задаются соответствующими множествами.

Теперь посмотрим, какие подгруппы есть у циклических групп. Обозначим через $\mathbb{Z}$ аддитивную группу целых чисел (группу целых чисел относительно сложения) — единственную бесконечную циклическую группу. В следующем далее рассуждении мы используем аддитивную запись групповой операции. Пусть H — нетривиальная подгруппа группы $\mathbb{Z}$, а d — наименьшее положительное число, принадлежащее H. Докажем, что H имеет вид

$$H = \{nd \mid n \in \mathbb{Z}\} = d\mathbb{Z}. \tag{1.5}$$

Действительно пусть $y \in H$. Разделим y на d с остатком: $y = nd+r$, $0 \leqslant r < d$. Так как $y \in H$, $nd \in H$, то и $r = y-nd \in H$. Значит, $r = 0$. Итак, любой элемент нашей подгруппы имеет вид nd.

Отметим еще один факт

Теорема 1.27. *Всякая подгруппа циклической группы — циклическая.*

В доказательстве мы чуть-чуть забежим вперед.

Доказательство. Если G — бесконечная циклическая группа, то она изоморфна $\mathbb{Z}$ (об изоморфизме см. следующий раздел), а мы уже нашли все подгруппы $\mathbb{Z}$ и доказали, что они циклические. Если G — конечная циклическая группа с порождающим элементом a и $H < G$, то пусть n — наименьшее положительное число, такое что $a^n \in H$. Легко проверяется что $b = a^n$ порождает H, аналогично тому, что мы раньше сделали с $\mathbb{Z}$ — все степени b будут принадлежать H, а не кратных n степеней в H опять не будет в силу выбора n. □

Используя теорему Лагранжа, можно определять порядок группы по порядку подгруппы и числу классов смежности.

Пример 1.28. Найдем порядок групп правильных многогранников. Из геометрических соображений ясно, что вращение многогранника должно быть поворотом вокруг оси, проходящей через его центр. Вершины многогранника переходят при вращении в вершины, причем пара вершин, соединенных ребром (соседние вершины), переходит в пару соседних вершин.

Если вращение многогранника g оставляет на месте вершину A, то ось поворота проходит через центр многогранника

и вершину A. Угол поворота определяется из того, что соседние с A вершины должны переходить в себя. Такие повороты образуют циклическую подгруппу H_A, порядок которой равен числу соседей у вершины многогранника.

Элементы g_1, g_2 принадлежат одному смежному классу по подгруппе H_A тогда и только тогда, когда $g_1^{-1}g_2$ принадлежит H_A. Если $g_1(A) = g_2(A)$, то $(g_1^{-1}g_2)(A) = A$. Верно и обратное. Поэтому сопряженный класс по подгруппе H_A образуют те вращения многогранника, которые переводят вершину A в некоторую вершину B.

Можно проверить, что любая пара вершин любого правильного многогранника совмещается вращением. Поэтому, если обозначить через G группу вращений многогранника, через n — число вершин, а через k — число ребер, выходящих из одной вершины, то $|H_A| = k$, $(G : H_A) = n$. По теореме Лагранжа $|G| = (G : H_A)|H_A| = nk$.

Приведем порядки групп для правильных многогранников, сосчитанные указанным способом:

многогранник	n	k	$\lvert G\rvert$
тетраэдр	4	3	12
куб	8	3	24
октаэдр	6	4	24
додекаэдр	20	3	60
икосаэдр	12	5	60

1.5. Задание группы порождающими и соотношениями

Мы уже привели много примеров групп. Определялись эти группы в основном путем явного описания множества и операции на нём (в случае конечных групп это можно сделать, скажем, с помощью таблицы Кэли). Далее мы рассмотрим другие способы задания группы. Например, ниже будет доказана теорема Кэли (теорема 1.37, с. 37), которая утверждает, что всякую конечную группу можно задать как подгруппу группы перестановок. Можно также строить группы из уже имеющихся. Например, в предыдущем разделе были приведены

примеры центра и нормализатора, см. также ниже конструкцию прямого произведения групп в примере 1.35.

В этом разделе мы рассмотрим задание группы порождающими и соотношениями.

Пусть есть подмножество S группы G. Пересечение подгрупп является подгруппой (утверждение 1.17). Возьмем пересечение всех подгрупп группы G, содержащих подмножество S. Это наименьшая подгруппа группы G, содержащая множество S. Она называется *подгруппой, порожденной* S (обозначается $\langle S\rangle$). По определению подгруппы, в $\langle S\rangle$ входит единица, элементы S, обратные к ним, все возможные произведения элементов S и их обратных по 2, 3, 4, и т. д. сомножителей.

Говорят, что группа G *порождается* множеством M своих элементов, если $G = \langle M\rangle$. Множество M в таком случае называется *множеством порождающих*. Например, из формулы (1.2) на с. 19 следует, что группа перестановок S_n порождается множеством циклов $(i_1 i_2 \dots i_k)$ всех возможных длин.

Основная идея задания группы порождающими и соотношениями состоит в том, чтобы указать (небольшое, обычно конечное) количество элементов группы, которое порождает группу (). Все остальные элементы группы записываются как произведения степеней порождающих. Конечно, не все такие выражения дают различные элементы. Часть равенств следует непосредственно из групповых аксиом (например, всегда $(ab)^{-1} = b^{-1}a^{-1}$). Помимо этого могут выполняться дополнительные равенства. Их можно задать, указав такое множество *соотношений* между порождающими (равенств), что все другие равенства следуют из соотношений и групповых аксиом.

Мы не будем давать формального определения задания группы порождающими и соотношениями. Ограничимся тем, что приведем два примера.

Пример 1.29 (*циклическая группа*). Один порождающий элемент a и одно соотношение $a^n = 1$. Ясно, что любое выражение, составленное из a, с учетом соотношения $a^n = 1$ равно a^k, $0 \leqslant k \leqslant n-1$. С другой стороны, все a^k, $0 \leqslant k \leqslant n-1$, различны. Иначе выполнялось бы соотношение $a^s = 1$, $1 \leqslant s < n$,

что невозможно. Строгое доказательство последнего утверждения уже требует введения дополнительного формализма, поэтому ограничимся нестрогим объяснением: поскольку *существует* циклическая группа C_n порядка n, в которой $a^s \neq 1$ при $1 \leqslant s < n$, то соотношение $a^s = 1$ *не следует* из соотношения $a^n = 1$. Последнее рассуждение называется построением *модели*.

Пример 1.30 (*диэдральная группа*). Группа D_n ($n \geqslant 3$) имеет ось n-го порядка C_n и перпендикулярную ей ось второго порядка C_2. Обозначим поворот на $2\pi/n$ вокруг C_n через r, а поворот на угол π вокруг C_2 через p. Очевидно, что

$$r^n = 1, \quad p^2 = 1. \tag{1.6}$$

Заметим, что если повернуть n-угольник на угол $2\pi/n$, ось второго порядка перейдет в другую ось второго порядка. Это означает, что

$$(pr)^2 = 1. \tag{1.7}$$

Три соотношения (1.6), (1.7) порождают группу диэдра. Действительно, из (1.7) следует, что $prp = r^{-1}$. Значит,

$$pr^k p = pr^{k-1}pprp = pr^{k-1}pr^{-1} = \ldots = r^{-k}\,,$$

поэтому любое произведение элементов p и r равно такому произведению, в котором p встречается не более одного раза. С учетом (1.6) таких выражений $1+3(n-1)$ штук: $1 = p^0 = r^0$, r^k, pr^k, $r^k p$, где $1 \leqslant k \leqslant n-1$. Но из (1.7) следует, что $rp = pr^{-1}$, поэтому

$$r^k p = r^{k-1}pr^{-1} = \ldots = pr^{-k} = pr^{n-k}.$$

Итак в группе, порожденной соотношениями (1.6), (1.7), не более $2n$ элементов. Поэтому она совпадает с D_n (опять используем рассуждение с моделью).

Уже из этих примеров видно, что анализ группы, заданной порождающими и соотношениями, труден. Более того, оказывается, что не существует алгоритма, который бы проверял по системе порождающих и соотношений, что заданная ими группа нетривиальна (отлична от единичной группы).

1.6. Изоморфизм и гомоморфизм

У этих слов есть общая часть: «морфизм». В математике есть общее понятие морфизма, однако нам понадобятся только изоморфизмы и гомоморфизмы.

Много информации о группе можно получить из таблицы Кэли (таблицы умножения) группы

$$\begin{array}{|cccc|}\hline e & g_1 & \dots & g_{n-1} \\ g_1 & g_1^2 & \dots & g_1 g_{n-1} \\ \dots & & & \\ g_{n-1} & g_{n-1}g_1 & \dots & g_{n-1}^2 \\ \hline\end{array}.$$

Как уже объяснялось выше, в каждой строке таблицы умножения элементы попарно различны, и в каждом столбце элементы также попарно различны (любая строка и любой столбец образуют перестановку элементов группы).

Алгебраические свойства группы отражаются в таблице Кэли. Скажем, если группа коммутативна, то таблица Кэли симметрична; если все элементы имеют порядок 2, то на диагонали стоят единичные элементы группы, и т. д.

Пусть для сравнительно большой группы, скажем, порядка 20, выписана таблица умножения. Занумеруем теперь элементы этой группы в другом порядке и напишем еще одну таблицу умножения. Глядя на эти таблицы, трудно понять, задают ли они одинаковую группу. И как вообще понимать утверждение «две группы одинаковы»?

С алгебраической точки зрения группы «одинаковы», если они изоморфны.

Пусть есть отображение $\varphi\colon G \to G'$ группы $\langle G, * \rangle$ в группу $\langle G', \circ \rangle$.

Отображение φ называется *изоморфизмом*, если

1) отображение φ взаимно однозначно;

2) отображение φ сохраняет операцию, т. е. образ произведения равняется произведению образов: $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

Рассмотрим некоторые свойства изоморфизма.

1) Изоморфизм сохраняет единицу: $\varphi(e) = e'$. Доказательство: для любого $a \in G$ имеем $a*e = e*a = a$. Тогда по второму свойству изоморфизма $\varphi(a) \circ \varphi(e) = \varphi(e) \circ \varphi(a) = \varphi(a)$.

Заметим, что в этом рассуждении мы использовали оба свойства из определения изоморфизма. Применяя второе свойство, мы можем раскрыть равенство $\varphi(a * e) = \varphi(e * a) = \varphi(a)$. Согласно первому свойству $\varphi(a)$ пробегает всю группу G', если a пробегает всю группу G.

2) Образ обратного элемента — обратный элемент к образу: $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Этот факт следует из равенства

$$\varphi(a) \circ \varphi(a^{-1}) = \varphi(a * a^{-1}) = \varphi(e) = e',$$

которое и означает, что обратный к образу a элемент есть образ обратного: $\varphi(a)^{-1} = \varphi(a^{-1})$.

3) Обратное отображение φ^{-1} является изоморфизмом. Взаимная однозначность обратного отображения очевидна, а сохранение операции получается так:

$$\varphi^{-1}(a \circ b) = \varphi^{-1}\big(\varphi(\varphi^{-1}(a)) \circ \varphi(\varphi^{-1}(b))\big) = \\ = \varphi^{-1}\big(\varphi(\varphi^{-1}(a) * \varphi^{-1}(b))\big) = \varphi^{-1}(a) * \varphi^{-1}(b).$$

4) Композиция изоморфизмов является изоморфизмом:

$$\psi(\varphi(a \cdot b)) = \psi(\varphi(a) \cdot \varphi(b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b)).$$

Здесь для простоты записи операции во всех трех группах обозначены одинаково.

Пример 1.31. У бесконечной циклической группы $\langle a \rangle$ есть два порождающих элемента: a и a^{-1}. Никаких других порождающих нет. Степени любого элемента, отличного от a и a^{-1}, не перечислят все элементы группы. Поэтому любая бесконечная циклическая группа изоморфна $\mathbb{Z}$. Для установления изоморфизма достаточно перевести $a \mapsto 1$, тогда $a^n \mapsto n$.

Тем самым утверждение, которое мы сделали в теореме о циклических группах, полностью обосновано.

Пример 1.32. Рассмотрим теперь две циклические группы A, B с одинаковым количеством элементов, скажем, n. Порождающий элемент группы A обозначим a, порождающий элемент группы B обозначим b. Как уже говорилось выше, любой элемент A представляется в виде a^k, $0 \leqslant k < n$. То же верно и для группы B. Рассмотрим отображение $\varphi\colon A \to B$,

которое задается правилом $\varphi\colon a^k \mapsto b^k$. Это взаимно однозначное отображение. Более того, это изоморфизм, так как операция сохраняется:

$$\varphi(a^s \cdot a^r) = \varphi(a^{s+r}) = b^{s+r} = b^s \cdot b^r = \varphi(a^s) \cdot \varphi(a^r).$$

Итак, любые две циклические группы с одинаковым числом элементов изоморфны. Поэтому нет нужды различать их, когда используются только свойства групповой операции.

Пример 1.33. Рассмотрим пример изоморфизма неабелевых групп. Докажем, что $D_3 \cong S_3$. Каждый элемент группы симметрий треугольника переводит треугольник в себя. Значит, вершины треугольника переходят в вершины. Пронумеруем вершины треугольника числами 1, 2, 3 и сопоставим элементу $g \in D_3$ перестановку $v(g) \in S_3$ чисел, которая задается перестановкой соответствующих вершин треугольника. Например, $v(e) = ()$ — каждая вершина остается на месте. Из построения ясно, что композиции элементов D_3 соответствует композиция соответствующих перестановок. С другой стороны, образы трех точек однозначно определяют движение плоскости. Поэтому разным элементам D_3 соответствуют разные перестановки. Поскольку $|D_3| = |S_3| = 6$, указанное выше отображение $v\colon D_3 \to S_3$ — изоморфизм.

Пример 1.34. Среди правильных многогранников есть двойственные: куб двойственен октаэдру, а додекаэдр — икосаэдру. В частности, центры граней куба являются вершинами октаэдра, а центры граней додекаэдра — вершинами икосаэдра (это можно проверить и непосредственно). Поскольку центры граней при вращении переходят в центры граней, получаем из этого наблюдения изоморфизм группы куба и группы октаэдра, а также группы додекаэдра и группы икосаэдра.

Пример 1.35. По двум группам G, H можно построить группу, которая называется *прямым произведением* групп G и H и обозначается $G \times H$. Элементами $G \times H$ являются все пары (g, h), где $g \in G$, $h \in H$. Операция в $G \times H$ — это покомпонентное выполнение операций в G и H:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2).$$

Относительно такой операции $G \times H$ является группой: ассоциативность очевидна, единицей $G \times H$ является пара (e_G, e_H) (здесь e_G — единица группы G, а e_H — единица группы H), обратным к (g, h) — элемент (g^{-1}, h^{-1}).

Порядок сомножителей в прямом произведении не важен, потому что $G \times H \cong H \times G$. Изоморфизм задается отображением, меняющим компоненты местами: $\varphi\colon (g, h) \mapsto (h, g)$. Взаимная однозначность и сохранение групповой операции очевидны.

Пример 1.36. Изоморфизм группы с самой собой называется *автоморфизмом*. Тривиальный пример автоморфизма — тождественное отображение. Автоморфизмы группы G образуют относительно композиции группу, которая называется группой автоморфизмов. Важным примером автоморфизмов являются *внутренние автоморфизмы*, которые имеют вид

$$x \mapsto gxg^{-1},$$

где g — некоторый фиксированный элемент группы. Автоморфизмы, не являющиеся внутренними, называются *внешними*. Внутренние автоморфизмы также образуют группу относительно композиции. Если группа G коммутативна, то единственный ее внутренний автоморфизм — тождественное отображение. Для некоммутативных групп существуют нетривиальные внутренние автоморфизмы.

Проверим, что $\varphi\colon x \mapsto gxg^{-1}$ действительно является автоморфизмом. Взаимная однозначность: пусть $\varphi(x) = \varphi(y)$, т. е. $gxg^{-1} = gyg^{-1}$. Умножая это равенство слева на g^{-1}, а справа на g, получаем $x = y$. Сохранение операции также проверяется прямым вычислением:

$$\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y).$$

Теорема 1.37 (теорема Кэли). *Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.*

Доказательство. Пусть $n = |G|$ — порядок группы G. Для элемента a группы G рассмотрим отображение $L_a\colon G \to G$, определяемое формулой $L_a\colon g \mapsto ag$. Мы «сдвигаем» каждый элемент на a, поэтому отображение L_a называется сдвигом

на a. Как уже говорилось, L_a — взаимно однозначное отображение G на себя. Перенумеровав элементы G числами от 1 до n, можно считать L_a перестановкой из S_n.

Если $\{e = g_1, g_2, \dots g_n\}$ — все элементы группы G, то множество перестановок $\{L_{g_1}, L_{g_2}, \dots L_{g_n}\}$ образует подгруппу S_n. Действительно,

$$L_{g_1}(L_{g_2}(g)) = g_1 g_2 g = L_{g_1 g_2}(g), \tag{1.8}$$

аналогично $L_g^{-1} = L_{g^{-1}}$.

Отображение $L\colon a \mapsto L_a$ является изоморфизмом. Оно взаимно однозначно по построению, а второе свойство изоморфизма получается из (1.8).

Итак, построен изоморфизм G и подгруппы группы перестановок S_n. □

Группа всех перестановок устроена достаточно сложно, так что большой пользы от теоремы Кэли нет. Скорее ее нужно воспринимать как утверждение о сложности структуры подгрупп группы перестановок.

Теперь перейдем к гомоморфизмам.

Отображение $\varphi\colon G \to G'$, где $\langle G, * \rangle$, $\langle G', \circ \rangle$ — две группы, называется *гомоморфизмом*, если $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

Гомоморфизм не обязательно взаимно однозначен. Группа G' не обязательно является полным образом группы G, может так быть, что $\mathrm{Im}(G) = \varphi(G) \subset G'$, т. е. образ будет собственным подмножеством G'.

Свойства гомоморфизма:

1) $\varphi(e) = e'$.

2) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

3) Композиция гомоморфизмов — гомоморфизм.

Доказательства аналогичны доказательствам для изоморфизма.

4) $\varphi(G) = H' < G'$, т. е. гомоморфный образ группы есть группа.

Докажем это свойство, проверив групповые аксиомы. Единица e' принадлежит H'. Пусть $\varphi(x), \varphi(y) \in H'$. Тогда $\varphi(x * y) = \varphi(x) \circ \varphi(y) \in H'$. Наконец, $\varphi(x^{-1}) = \varphi(x)^{-1}$, поэтому $\varphi(x)^{-1} \in H'$.

Следовательно, H' — группа, а раз она группа, то она подгруппа G'.

Пример 1.38. Из линейной алгебры известно, что определитель произведения матриц равен произведению определителей: $\det(AB) = \det(A)\det(B)$. Поэтому отображение

$$\det\colon GL(\mathbb{R}, n) \to \mathbb{R}^*, \quad \det\colon A \mapsto \det(A)$$

является гомоморфизмом группы $GL(\mathbb{R}, n)$ невырожденных матриц порядка n с действительными элементами в мультипликативную группу действительных чисел, отличных от 0.

Пример 1.39. *Транспозицией* называется перестановка, которая меняет местами ровно два элемента. Всякая перестановка является произведением транспозиций. Для доказательства этого утверждения нужно разложить перестановку на циклы и выразить каждый цикл в виде произведения транспозиций:

$$(i_1 i_2 i_3 \dots i_k) = (i_1 i_k) \circ (i_1 i_{k-1}) \circ \dots \circ (i_1 i_4) \circ (i_1 i_3) \circ (i_1 i_2).$$

Знаком $\operatorname{sgn}(\pi)$ перестановки π назовем число $(-1)^{n+k}$, где n — число элементов в перестановке, k — число циклов в цикловом разложении перестановки, включая циклы длины 1. Перестановка называется *четной*, если ее знак равен $+1$, в противном случае она называется *нечетной*. Легко видеть, что тождественная перестановка $()$ — четная, ее знак $(-1)^{n+n} = +1$.

Перестановку можно разложить в произведение транспозиций разными способами. Но оказывается, что четность числа транспозиций в любом разложении перестановки π не зависит от выбора разложения: четные перестановки разлагаются в четное число транспозиций; нечетные — в нечетное. Доказать это можно индукцией по длине записи перестановки в виде произведения транспозиций. Основание индукции — тождественная перестановка (произведение 0 транспозиций). Для индуктивного перехода осталось проверить, что умножение перестановки на транспозицию (jk) меняет количество циклов на 1: увеличивает, если j и k входят в один цикл; уменьшает, если j и k входят в разные циклы. Действительно, запишем

произведения в обоих случаях (используем цикловую запись):

$$(jk) \circ (AjBkC) = (AkC)(Bj),$$
$$(jk) \circ (jA)(kB) = (jAkB)$$

(на месте заглавных букв могут стоять любые последовательности чисел, отличных от j, k).

Рассмотрим отображение $\operatorname{sgn}\colon \pi \mapsto \operatorname{sgn}(\pi)$. Это гомоморфизм группы S_n в группу $\{\pm 1\}$, которая есть просто-напросто циклическая группа порядка 2 в мультипликативной записи. В самом деле, раз четность числа транспозиций, произведением которых записывается перестановка, не зависит от выбора произведения, то при перемножении перестановок четности числа транспозиций складываются по модулю 2, а знаки перестановок перемножаются.

1.7. Нормальные подгруппы

Особенно важную роль в теории групп играют те подгруппы, для которых левые и правые смежные классы совпадают. Такие подгруппы называются *нормальными*; их также называют нормальными делителями или инвариантными подгруппами.

Более формально, подгруппа H группы G называется нормальной, если для любого элемента $g \in G$ выполняется равенство $gH = Hg$. Для отношения «быть нормальной подгруппой» используется специальное обозначение $H \lhd G$.

Очевидно, что подгруппа, состоящая из одного-единственного элемента e, — нормальная подгруппа, $e \lhd G$, что сама группа также является нормальной подгруппой: $G \lhd G$, а также, что у коммутативной группы все подгруппы нормальны.

Теперь рассмотрим менее тривиальный пример.

Пусть G — группа и H — ее подгруппа индекса 2 (напомним, что индекс подгруппы $(G : H)$ — это количество смежных классов по этой подгруппе). Вся группа разбивается на два смежных класса по H. Поскольку один из них — это сама подгруппа H, то в другой смежный класс входят все остальные элементы группы G. Обозначим этот класс H'. По определению смежного класса $H' = g'H$, где $g' \notin H$. Аналогично

для правых смежных классов: один из классов это снова H, а второй это $H'' = Hg''$, где $g'' \notin H$. Конечно, $H' = H'' = G \setminus H$ — ведь и в тот, и в другой класс входят в точности те элементы группы, которые не принадлежат H.

Следовательно, любая подгруппа индекса 2 будет нормальной. Отсюда получим нетривиальный пример нормальной подгруппы.

Пример 1.40. Рассмотрим группу S_3 и ее подгруппу $H = \langle (123) \rangle < G$. Легко видеть, что H — циклическая подгруппа порядка 3 группы S_3. Следовательно, ее индекс равен 2 и $H \lhd G$.

Пример 1.41. Рассмотрим прямое произведение $G_1 \times G_2$ групп G_1 и G_2. Легко видеть, что множества $G_1 \times \{e_2\} = \{(g, e_2) \mid g \in G_1\}$ и $\{e_1\} \times G_2 = \{(e_1, g) \mid g \in G_2\}$ являются подгруппами $G_1 \times G_2$. Эти подгруппы нормальны, как показывает следующее вычисление:

$$(g_1, g_2) \cdot (G_1 \times \{e_2\}) = \{(g, g_2) \mid g \in G_1\} = (G_1 \times \{e_2\}) \cdot (g_1, g_2)$$

(аналогично для $\{e_1\} \times G_2$).

Утверждение 1.42. *Пересечение нормальных подгрупп — нормальная подгруппа.*

Доказательство. Пусть $N_1 \lhd G$, $N_2 \lhd G$, $N = N_1 \cap N_2$. Для любого $g \in G$ имеем $gN \subseteq gN_1 = N_1 g$, $gN \subseteq gN_2 = N_2 g$. Если $x \in N_1 g \cap N_2 g$, то $xg^{-1} \in N_1 \cap N_2 = N$. Таким образом, $gN \subseteq Ng$. Аналогично доказывается, что $Ng \subseteq gN$. Поэтому $gN = Ng$. □

Выше было показано, что гомоморфный образ подгруппы является подгруппой. Следует иметь в виду, что гомоморфизм не сохраняет, вообще говоря, свойство «быть нормальной подгруппой».

Пример 1.43. Рассмотрим циклическую группу $C_4 = \langle a \rangle$ и ее подгруппу $C_2 = \langle a^2 \rangle$ индекса 2. Поскольку C_4 абелева, то $C_2 \lhd C_4$ (все подгруппы абелевой группы нормальны). Теперь рассмотрим гомоморфизм

$$\varphi\colon C_4 \to S_4, \qquad \varphi\colon a \mapsto (1234).$$

Легко видеть, что $\varphi(\langle a^2\rangle) = \langle (13)(24)\rangle$. Эта подгруппа не является нормальной в S_4, что видно из вычисления

$$(12)\circ(13)(24) = (1324) \neq (1423) = (13)(24)\circ(12).$$

Тут использовано, что подгруппа порядка 2 нормальна тогда и только тогда, когда она лежит в центре группы, т. е. ее неединичный элемент перестановочен со всеми элементами группы.

Чтобы взглянуть на нормальные подгруппы по-другому, рассмотрим сопряженные элементы.

1.8. Сопряженные элементы

Будем называть элемент b группы G *сопряженным* с элементом a посредством элемента g, если $b = gag^{-1}$.

Выбирая различные элементы g, будем получать различные, вообще говоря, элементы, сопряженные с элементом a. Отношение сопряженности будем обозначать $\sim$.

Перечислим свойства отношения сопряженности.

1) $a \sim a$. Каждый элемент сопряжен сам с собой (посредством элемента e).

2) Из $a \sim b$ следует $b \sim a$. Если b получается из a сопряжением посредством элемента g, то a получается из b сопряжением посредством g^{-1}.

3) Из $a \sim b$, $b \sim c$ следует $a \sim c$. Проверяется прямым вычислением: из $b = gag^{-1}$, $c = hbh^{-1}$ следует

$$c = hbh^{-1} = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}. \qquad (1.9)$$

Что можно сказать об отношениях, для которых выполнены свойства 1) – 3)? Каждое такое отношение разбивает множество на классы, внутри которых отношение выполняется между любыми двумя элементами, а на парах элементов, принадлежащих разным классам, отношение не выполняется. Такие отношения называются *отношениями эквивалентности*. Свойство 1) называется *рефлексивностью* отношения, свойство 2) — *симметричностью*, свойство 3) — *транзитивностью*.

Отношение сопряженности разбивает группу на *классы сопряженных элементов* (все элементы внутри одного класса

сопряжены друг с другом, а элементы из разных классов не сопряжены).

Пример 1.44. Если G коммутативна, то каждый ее элемент является классом сопряженных элементов: $gxg^{-1} = xgg^{-1} = x$.

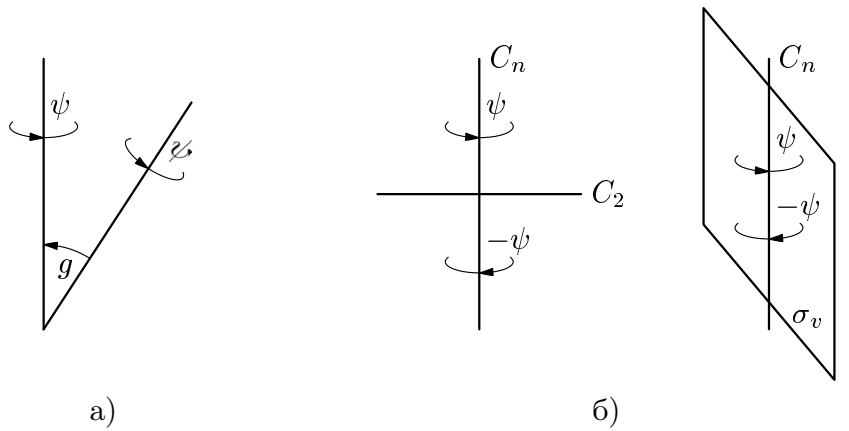
Искать классы сопряженных элементов, исходя из определения, довольно сложно. Нужно выбрать элемент группы b и вычислять для каждого элемента группы g выражение gbg^{-1}. Для групп преобразований есть более простой способ, который мы кратко проиллюстрируем на примерах, предоставляя читателю восстановить детали рассуждений самостоятельно.

Рассмотрим, например, группу движений. Из геометрических соображений ясно, что движения a и b сопряжены ($a = gbg^{-1}$), когда это одно и то же преобразование, выполненное в двух разных системах координат (преобразованием g^{-1} перешли в старую систему координат, применили b, вернулись преобразованием g в новую систему координат и получили преобразование a, которое в старой системе координат записывается так же, как b в новой). В частности, движение xax^{-1}, сопряженное с поворотом a вокруг прямой ℓ, является поворотом на такой же угол вокруг той прямой ℓ_x, в которую переходит прямая ℓ при движении x ($\ell_x = x(\ell)$).

В силу этих рассуждений повороты на один и тот же угол вокруг двух разных осей сопряжены, если в группе есть преобразование g, переводящее одну ось в другую, как показано на рис. 1.3 а). Если речь идет о поворотах вокруг одной оси на одинаковые по абсолютной величине углы ψ, $-\psi$ (но в разные стороны), то преобразований g может быть всего два: ось второго порядка C_2, перпендикулярная данной оси C_n, или зеркальная плоскость σ_v, проходящая через ось, рис. 1.3 б). Ось C_n в этих двух случаях называется *двусторонней*.

Пример 1.45. Найдем сопряженные элементы в группе диэдра D_n. Ответ зависит от четности n. Как и в примере 1.30, обозначим поворот на $2\pi/n$ вокруг C_n через r, а поворот на угол π вокруг C_2 через p.

Заметим, что повороты вокруг оси C_n на разные по абсолютной величине углы не сопряжены друг с другом. А повороты на одинаковые углы, но в противоположных направлениях



а) б)

Рис. 1.3.

сопряжены, так как есть перпендикулярная оси C_n ось C_2. Повороты на угол π вокруг осей C_2 сопряжены тогда и только тогда, когда эти оси можно совместить симметрией диэдра.

В случае нечетного n любые две оси C_2 можно совместить поворотом вокруг C_n. Поэтому все элементы вида pr^k сопряжены. Итого получаем $k+2$ классов сопряженных элементов в D_{2k+1}:

$$\{e\},\ \{r, r^{-1}\},\ \ldots,\ \{r^k, r^{-k}\},\ \{p, pr, pr^2, \ldots, pr^{2k}\}.$$

В случае четного n поворотом вокруг C_n можно совместить либо те оси, которые проходят через пару противоположных вершин, либо те, которые проходят через середины противоположных сторон (см. рис. 1.2 а) на с. 21). Поскольку вершины переходят в вершины, между собой эти оси совместить нельзя. Поэтому получаем $k+3$ классов сопряженных элементов в D_{2k}:

$$\{e\},\ \{r, r^{-1}\},\ \ldots,\ \{r^{k-1}, r^{-k+1}\},\ \{r^k\},$$
$$\{pr, pr^3, \ldots, pr^{2k-1}\},\ \{p, pr^2, \ldots, pr^{2k-2}\}.$$

Пример 1.46. Найдем классы сопряженных элементов для группы перестановок S_n. Каждой перестановке сопоставим цикловой тип $(c_1, c_2, \ldots, c_n)$, где c_i — количество циклов длины i в цикловом разложении. Другой способ задать цикловой тип — указать разбиение числа n в (неупорядоченную) сумму натуральных слагаемых.

Аналогично тому, как был рассмотрен случай сопряжения в группах движений, перестановка gag^{-1} получается применением перестановки g ко всем числам в разложении перестановки a на независимые циклы (перенумерации элементов). Действительно, g^{-1} возвращает исходную нумерацию, далее применяем a, после чего возвращаемся к новой нумерации с помощью g.

Цикловой тип от нумерации, очевидно, не зависит, поэтому сопряженные перестановки имеют одинаковый цикловой тип. Верно и обратное: если две перестановки имеют одинаковый цикловой тип, то можно найти взаимно однозначное соответствие между элементами их циклов, сохраняющее порядок в циклах. Это соответствие и есть та перестановка, сопряжение с помощью которой переводит первую перестановку во вторую.

Читателю рекомендуется проследить за этим рассуждением на конкретном примере. Скажем, перестановка (12)(34) сопряжена с (13)(24) посредством (1342).

Проверим, что если H — подгруппа, то множество

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

также является подгруппой. По теореме 1.16 достаточно доказать, что для любых $a = gh_1g^{-1}$, $b = gh_2g^{-1}$ $(h_1, h_2 \in H)$ выполняется $ab^{-1} \in gHg^{-1}$:

$$ab^{-1} = gh_1g^{-1}\bigl(gh_2g^{-1}\bigr)^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = \\ = g(h_1h_2^{-1})g^{-1} \in gHg^{-1}.$$

Подгруппу gHg^{-1} называют *подгруппой, сопряженной с H посредством элемента g*.

В некоторых случаях $gHg^{-1} = H$ для любого элемента $g \in G$. Умножая это равенство на g справа, получаем $gH = Hg$. Тем самым, мы получили новое определение нормальной подгруппы (нормальная подгруппа совпадает со всеми своими сопряженными). Другими словами, условия

1) $gH = Hg$ для любого $g \in G$,

2) $H = gHg^{-1}$ для любого $g \in G$

равносильны.

Если есть отображение $\varphi\colon X \to X$ некоторого множества на себя, то любое подмножество $Y \subseteq X$, для которого выполнено условие $\varphi(Y) \subseteq Y$, называется *инвариантным* подмножеством (относительно φ). Нормальная подгруппа в силу второго ее определения инвариантна относительно всех внутренних автоморфизмов (см. пример 1.36). Отсюда и второе название нормальной подгруппы — *инвариантная подгруппа*.

Отметим также, что нормальная подгруппа вместе с каждым элементом содержит весь класс сопряженных с ним элементов. Верно и обратное: если подгруппа содержит полные классы сопряженных элементов, то она является нормальной.

1.9. Действия групп. Лемма Бернсайда

Действием группы G на множестве X называется гомоморфизм $\varphi\colon G \to S(X)$ группы G в группу $S(X)$ биекций множества X (взаимно однозначных отображений множества X на себя). Говорят также, что группа G действует на множестве X. Если ясно, о каком действии идет речь, то $\varphi(g)(x)$ записывают как $g(x)$. Элементы множества X будем называть точками, чтобы отличать их от элементов группы G.

Фактически действия групп уже появлялись в предыдущих разделах. Сейчас мы вернемся к этим примерам.

Пример 1.47 (*действие левыми сдвигами*). Как уже говорилось при доказательстве теоремы Кэли, левый сдвиг на g — это преобразование $L_g(h) = gh$. При доказательстве теоремы Кэли мы проверили по сути, что $L\colon G \to S(G)$ — гомоморфизм и, более того, $L(G) \cong G$. Поэтому любая группа действует на себе самой умножением слева.

Конечно, можно определить аналогичное действие правыми сдвигами.

Пример 1.48 (*действие сопряжениями*). Группа действует на себе самой сопряжениями. По определению,

$$\varphi(g)(x) = gxg^{-1}.$$

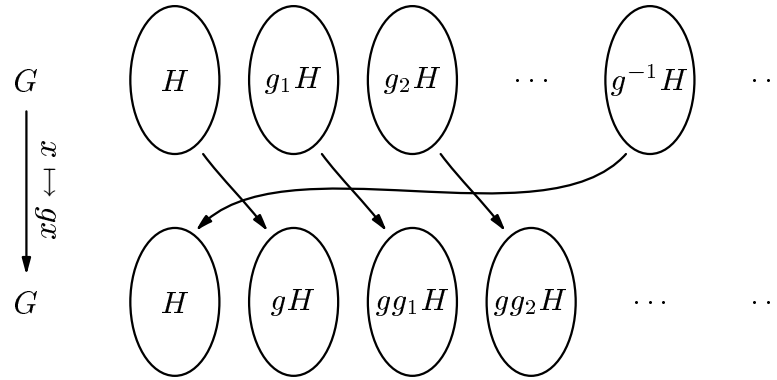


Рис. 1.4.

Фактически уже было доказано, что это гомоморфизм (формула (1.9) на с. 42).

Пример 1.49 (*действие на классах смежности*). Посмотрим более внимательно на действие группы левыми сдвигами. Пусть есть подгруппа H группы G. По теореме 1.20 группа G разбивается на классы смежности по подгруппе H, как показано на рис. 1.4. Там же можно увидеть, что происходит при умножении на некоторый элемент g группы G. Из ассоциативности умножения следует, что умножение на g сохраняет классы смежности по H: образ $g(g_1H)$ класса смежности g_1H является классом смежности с представителем gg_1. Более того, образы различных смежных классов различны. Действительно, если $g(g_1H) = g(g_2H)$, то $gg_1h_1 = gg_2h_2$, $h_1, h_2 \in H$, т. е. $g_1 = g_2h$, $h = h_2h_1^{-1} \in H$, а значит $g_1H = g_2H$.

Таким образом мы получаем действие группы на множестве классов смежности (см. рис. 1.5).

Действия из примера 1.49 в некотором смысле исчерпывают все возможные действия групп.

Зафиксируем некоторое действие и будем писать $g(x)$ для обозначения образа точки x при действии элемента g. Для любого $x \in X$ определим множество элементов группы G, оставляющих точку x неподвижной: $G_x = \{g \in G \mid g(x) = x\}$. Множество G_x называется *стабилизатором* точки x.

Утверждение 1.50. *Стабилизатор G_x — подгруппа G.*

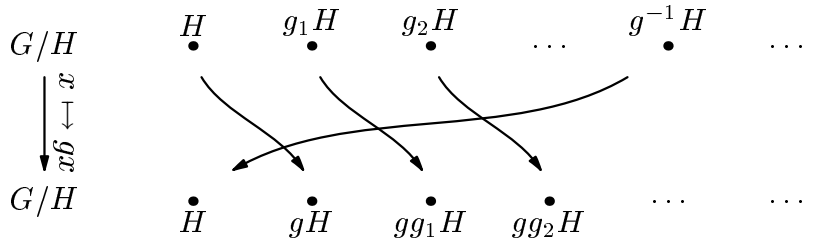


Рис. 1.5.

Доказательство. Проверим свойства подгруппы. Во-первых, $e \in G_x$, так как $e(x) = x$ (при гомоморфизме единичный элемент переходит в единичный, а единичный элемент в группе $S(X)$ — тождественное отображение). Во-вторых, так как $g(g^{-1}(x)) = x$, то из $g \in G_x$ следует $g^{-1} \in G_x$. В-третьих, если $g, h \in G_x$, то и $gh \in G_x$, поскольку $g(h(x)) = g(x) = x$. □

Орбитой действия называется множество образов некоторой точки x: $O_x = \{x' \in X \mid x' = g(x), g \in G\}$.

Утверждение 1.51. *Орбиты действия разбивают точки множества X на классы эквивалентности.*

Доказательство. Проверим свойства отношения эквивалентности.

Рефлексивность: $e(x) = x$, так как при гомоморфизме единичный элемент переходит в единичный.

Симметричность: если $y \in O_x$, то $x \in O_y$, так как из $y = g(x)$ следует $x = g^{-1}(y)$.

Транзитивность: если $y \in O_x$, $z \in O_y$, то $z \in O_x$, так как из $y = g_1(x)$, $z = g_2(y)$ следует $z = (g_1 g_2)(x)$. □

Между смежными классами по стабилизатору G_x и точками орбиты x существует естественное взаимно однозначное соответствие (мы уже его фактически использовали при подсчете порядка группы многогранника в примере 1.28, с. 30).

Утверждение 1.52. *Отображение φ: $y \to \{g \in G \mid g(x) = y\}$ сопоставляет каждой точке орбиты O_x класс смежности по стабилизатору G_x. Это соответствие взаимно однозначно.*

Доказательство. Вначале докажем, что образом любой точки при отображении φ является класс смежности. Условие $g(x) = h(x)$ равносильно условию $h^{-1}(g(x)) = x$, которое означает, что $h^{-1}g \in G_x$ и потому $g \in hG_x$.

Из определения φ ясно, что прообраз класса gG_x при отображении φ определен однозначно: это $y = g(x)$.

Осталось доказать, что образ орбиты при отображении φ — всё множество смежных классов по G_x. Это очевидно: класс смежности gG_x является образом точки $g(x)$ при отображении φ. □

Следствие 1.53. *Число элементов в орбите равно индексу стабилизатора*: $|O_x| = (G : G_x)$.

Действие называется *транзитивным*, если у него ровно одна орбита (любую точку можно перевести в любую действием элемента группы). Доказанные выше утверждения означают, что все транзитивные действия являются, в сущности, действиями группы на смежных классах по некоторой ее подгруппе (стабилизатору точки). В частности, если $H < G$, то существует такое действие G (действие сдвигами на смежных классах), для которого H — стабилизатор некоторой точки.

Лемма 1.54 (лемма Бернсайда). *Пусть конечная группа G действует на конечном множестве X. Количество орбит действия дается формулой:*

$$\frac{1}{|G|}\sum_{g\in G}|X_g|, \tag{1.10}$$

где $X_g = \{x \in X \mid gx = x\}$ — множество неподвижных точек g.

Доказательство. Обозначим через N количество таких пар (g, x), что $g(x) = x$. Подсчитаем число N двумя способами.

Вначале просуммируем мощности стабилизаторов всех элементов $x \in X$. Стабилизаторы точек из орбиты точки x, состоящей из s точек, дадут вклад $s|G_x| = (G : G_x)|G_x| = |G|$ (по следствию 1.53 мощность орбиты равна индексу стабилизатора). Т. е. каждая орбита дает вклад $|G|$ в число N. Поэтому N равно числу орбит, умноженному на $|G|$.

По-другому число N можно посчитать, суммируя количество неподвижных точек $|X_g|$ по всем g. Приравняв два полученных выражения и разделив на $|G|$, получаем искомую формулу (1.10). □

Лемма Бернсайда часто применяется в перечислительной комбинаторике. Приведем один простой пример.

Пример 1.55 (*подсчет ожерелий*). Ожерелье состоит из 12 бусин черного или белого цвета, которые жестко закреплены на круглом кольце через равные расстояния. Ожерелья разные, если их нельзя совместить движением. Сколько есть разных ожерелий?

Занумеруем местá бусин в порядке их следования вдоль кольца и для каждого места укажем цвет бусины. Получили множество N из 2^{12} «помеченных» ожерелий. На этом множестве действует диэдральная группа D_{12} и те «помеченные» ожерелья, которые попадают в одну орбиту, задают одинаковое в смысле нашей задачи ожерелье. Так что задача свелась к подсчету числа орбит.

Подсчитаем число орбит, пользуясь леммой Бернсайда. Прежде всего заметим, что сопряженные элементы группы дают одинаковый вклад в формулу (1.10): если $h = ugu^{-1}$ и $g(x) = x$, то $h(u(x)) = u(g(x)) = u(x)$, поэтому $u(X_g) = X_h$.

С другой стороны, если $g(x) = x$, то и $g^k(x) = x$. Поэтому неподвижные точки при действии g остаются неподвижными и при действии группы $\langle g \rangle$.

Теперь разберем все возможные случаи.

$g = e$. Для тождественного отображения неподвижными точками будут все $2^{12} = 4096$ «помеченных» ожерелий.

g — поворот на $\pm 2\pi/12$, $\pm 5 \cdot 2\pi/12$. Группа $\langle g \rangle$ действует транзитивно на множестве $\{1, \ldots, 12\}$ (1 и 5 взаимно просты с 12). Поэтому неподвижными точками будут только 2^1 «помеченных» ожерелий, в которых все бусины одинакового цвета. Этот случай дает вклад в формулу (1.10) в размере $4 \cdot 2^1 = 8$.

g — поворот на $\pm 2 \cdot 2\pi/12$. На четных и нечетных местах должны стоять бусины одинакового цвета, поэтому общий вклад этого случая $2 \cdot 2^2 = 8$.

Рассуждая аналогично, находим, что вклад случая, когда g — повороты на $\pm 3 \cdot 2\pi/12$ равен $2 \cdot 2^3 = 16$, вклад случая, когда g — повороты на $\pm 4 \cdot 2\pi/12$ равен $2 \cdot 2^4 = 32$, а вклад случая, когда g — поворот на $6 \cdot 2\pi/12$ равен $2^6 = 64$.

Осталось рассмотреть два случая: когда g — поворот на угол π вокруг диагонали 12-угольника, в этом случае общий вклад равен $6 \cdot 2^7 = 768$; а также когда g — поворот на угол π вокруг середины противоположных сторон 12-угольника, в этом случае общий вклад равен $6 \cdot 2^6 = 384$.

Собирая эти вычисления вместе, получаем ответ:

$$\frac{1}{24}\Big(4096 + 8 + 8 + 16 + 32 + 64 + 768 + 384\Big) = \frac{5376}{24} = 224.$$

1.10. Факторгруппы

Прежде чем давать формальное определение факторгруппы, объясним, что хотелось бы получить. Переход от множества к классам эквивалентности этого множества по некоторому отношению эквивалентности называется *факторизацией*. Мы хотим факторизовать группу по подгруппе, т. е. перейти к множеству классов смежности по этой подгруппе. В случае произвольной подгруппы факторизация по классам смежности переводит группу в более общий объект — действие группы на множестве. Но иногда это действие можно представить как действие некоторой новой *факторгруппы* на себе самой сдвигами. Другими словами, в этом случае можно рассматривать классы смежности по подгруппе как элементы некоторой группы. Конечно, мы теряем при факторизации какую-то информацию о группе, но зато полученная факторгруппа будет проще, изучать ее легче и т. д.

Оказывается, что факторизация дает группу только в случае нормальных подгрупп. Рассмотрим вначале пример, когда факторизация не дает группу.

Пример 1.56 (*продолжение примера* 1.22). Составим таблицу действия группы S_3 на смежных классах по подгруппе $H = \langle(12)\rangle$ (смежные классы разделены линиями):

	H	$(23)H$	$(13)H$
$()$	H	$(23)H$	$(13)H$
(12)	H	$(13)H$	$(12)H$
(23)	$(23)H$	H	$(13)H$
(132)	$(23)H$	$(13)H$	H
(13)	$(13)H$	$(23)H$	H
(123)	$(13)H$	H	$(23)H$

Как видим, разные элементы одного смежного класса действуют на смежные классы по-разному. Поэтому из такого действия нельзя получить бинарную операцию на множестве смежных классов.

Теперь рассмотрим случай нормальной подгруппы $H \lhd G$. Пусть G/H — совокупность смежных классов G по H. Обозначение подсказывает, что мы «делим» G на H. Отсюда еще одно название нормальной подгруппы — нормальный делитель. Чтобы получить группу, на множестве G/H необходимо ввести операцию. Сделаем это таким образом: $(xH) \cdot (yH) = (xyH)$.

Прежде всего нужно проверить, что данное выше определение корректно. Другими словами, произведение двух классов смежности должно не зависеть от выбора представляющих классы элементов x, y. (В противном случае никакой операции на G/H мы бы не получили.)

Пусть $x' = xh_1$, $y' = yh_2$. Тогда $(x'H)\cdot(y'H) = (xh_1yh_2)H = (xyh_3)H = (xyH)$ (в среднем равенстве мы использовали нормальность подгруппы H).

Теперь докажем, что множество G/H относительно введенной операции является группой.

1) Ассоциативность очевидна, так как выполняется в группе G.

2) Поскольку $(xH) \cdot (eH) = (eH) \cdot (xH) = (xH)$, подгруппа H (точнее, смежный класс eH, но это и есть сама подгруппа) является единичным элементом.

3) Класс $x^{-1}H$ — обратный к xH относительно введенной операции: $(x^{-1}H) \cdot (xH) = (x^{-1}xH) = (eH)$.

Итак, G/H относительно операции умножения смежных классов является группой. Она называется *факторгруппой* G

по подгруппе H. Заметим, что если G конечна, то и все ее подгруппы конечны, поэтому

$$|G/H| = \frac{|G|}{|H|} = (G : H).$$

Элемент факторгруппы G/H обычно задается указанием представителя $x \in G$ класса смежности xH. Чтобы не путать элементы группы и элементы факторгруппы, используются различные обозначения: $(xH) = \bar{x} = [x] = \{x\}$.

Рассмотрим примеры факторгрупп.

Пример 1.57. $G/G \cong \{e\}$. Мы забываем про группу всё, кроме того, что в ней есть единица.

Пример 1.58. $G/\{e\} = G$. Здесь мы всё запомнили о группе.

Естественно, у нас возникают и промежуточные случаи.

Пример 1.59. Возьмем в аддитивной группе целых чисел $\mathbb{Z}$ подгруппу $3\mathbb{Z} \lhd \mathbb{Z}$. Построим факторгруппу $\mathbb{Z}/3\mathbb{Z}$. Во-первых, в этой группе есть нулевой элемент $\bar{0}$ (здесь естественно использовать аддитивную запись):

$$\bar{0} = 0 + 3\mathbb{Z},$$

далее берем смежный класс, порожденный элементом 1,

$$\bar{1} = 1 + 3\mathbb{Z},$$

то же самое для элемента $2 \in \mathbb{Z}$

$$\bar{2} = 2 + 3\mathbb{Z}.$$

Получаем факторгруппу $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ с операцией сложения, определенной следующей таблицей (в сокращенной форме):

$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{1}$

Теперь мы можем забыть, что классы смежности — это множества чисел, и работать с группой из трех элементов. (Эта группа называется группой вычетов по модулю 3, и мы ее уже один раз построили на с. 15.)

В продолжение этого примера заметим, что если $G = \langle a \rangle$ — циклическая группа, то факторгруппа G/H по любой подгруппе $H < G$ будет также циклической: ясно, что $\overline{a^n} = (\bar{a})^n$.

Пример 1.60 (*продолжение примера* 1.41). Имеют место изоморфизмы $(G \times H)/(G \times \{e\}) \cong H$, $(G \times H)/(\{e\} \times H) \cong G$. Читателю предлагается построить эти изоморфизмы самостоятельно.

1.11. Ядро гомоморфизма

Напомним, что гомоморфизм — это отображение одной группы в другую, сохраняющее произведение. Пусть $\langle G, \cdot \rangle$ и $\langle G', \circ \rangle$ — группы, а φ — гомоморфизм группы G в группу G'. *Ядром гомоморфизма* называется множество $\operatorname{Ker} \varphi = \{g \in G \mid \varphi(g) = e'\}$. Т. е. ядро гомоморфизма — это множество элементов группы G, отображающихся в единицу группы G'. Пусть $a \in \operatorname{Ker} \varphi$, $b \in \operatorname{Ker} \varphi$, тогда и $ab \in \operatorname{Ker} \varphi$ (если два элемента принадлежат ядру гомоморфизма, то и их произведение принадлежит гомоморфизму), так как

$$\varphi(ab) = \varphi(a) \circ \varphi(b) = e' \circ e' = e'.$$

Обратный к элементу, принадлежащему ядру, также принадлежит ядру:

$$\varphi(a^{-1}) \circ \varphi(a) = \varphi(a^{-1} \cdot a) = \varphi(e) = e'.$$

Значит ядро является подгруппой G.

Пример 1.61. Рассмотрим отображение $\varphi\colon \mathbb{Z} \to \langle a \rangle$ аддитивной группы целых чисел $\mathbb{Z}$ в конечную циклическую группу $\langle a \rangle$, порожденную элементом a, которое задается формулой:

$$\varphi\colon n \mapsto a^n.$$

Очевидно, что это гомоморфизм. Что же будет ядром гомоморфизма φ? Пусть q — минимальное положительное число, для которого $a^q = e$. Тогда $\operatorname{Ker} \varphi = \{lq \mid l \in \mathbb{Z}\}$ (доказательство аналогично тому рассуждению, с помощью которого были найдены все подгруппы циклической группы в теореме 1.27).

Пример 1.62. Рассмотрим мультипликативную группу положительных чисел с операцией умножения $(\mathbb{R}_+^*, \cdot)$, а также

$(\mathbb{R}, +)$ — аддитивную группу действительных чисел. Отображение $\varphi\colon a \mapsto \ln a$ является гомоморфизмом в силу известного свойства логарифма. Поскольку $\operatorname{Ker}\varphi = \{1\}$, этот гомоморфизм является изоморфизмом.

Теорема 1.63 (теорема о гомоморфизме групп). *Пусть* $\varphi\colon G \to G'$ *— гомоморфизм с ядром* $\operatorname{Ker}\varphi = K$. *Тогда* $K \lhd G$ *и* $G/K \cong \varphi(G)$.

Обратно, если $K \lhd G$, *то существуют группа* G', *а именно* G/K, *и гомоморфизм* $\pi\colon G \to G'$ $(\pi\colon G \to G/K)$ *такие, что* $\operatorname{Ker}\pi = K$.

Т. е. гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма. Звучит немного угрожающе, но разобраться с этой теоремой несложно.

Доказательство. Докажем, что ядро гомоморфизма является нормальной подгруппой. Возьмем $h \in \operatorname{Ker}\varphi$ и проверим, что $\varphi(g^{-1}hg) = e'$:

$$\varphi(g^{-1}hg) = \varphi(g^{-1}) \circ \varphi(h) \circ \varphi(g) = \varphi(g)^{-1} \circ \varphi(g) = e'.$$

Определим отображение $\tilde{\varphi}\colon G/K \to G'$ так, что образом смежного класса по K является образ при гомоморфизме φ любого элемента из этого класса, т. е. $\tilde{\varphi}\colon (gK) \mapsto \varphi(g)$.

Это определение корректно, так как из $g_1 = g_2x$, $x \in K$, следует $\varphi(g_1) = \varphi(g_2x) = \varphi(g_2) \circ \varphi(x) = \varphi(g_2) \circ e' = \varphi(g_2)$. Значит, образы представителей смежного класса по K при гомоморфизме φ одинаковы.

Далее,

$$\tilde{\varphi}\big((g_1K) \cdot (g_2K)\big) = \tilde{\varphi}\big((g_1g_2K)\big) = \\ = \varphi(g_1g_2) = \varphi(g_1) \circ \varphi(g_2) = \tilde{\varphi}\big((g_1K)\big) \circ \tilde{\varphi}\big((g_2K)\big).$$

Мы доказали, что образ произведения равен произведению образов. Следовательно, $\tilde{\varphi}$ — гомоморфизм. Докажем, что $\tilde{\varphi}$ не только гомоморфизм, но и изоморфизм. Для этого нужно доказать, что отображение $\tilde{\varphi}$ взаимно однозначно. Действительно, из $\tilde{\varphi}\big(g_1K)\big) = \tilde{\varphi}\big((g_2K)\big)$ следует $\varphi(g_1) = \varphi(g_2)$, откуда получаем $\varphi(g_1^{-1}g_2) = e'$. Значит, $g_1^{-1}g_2 \in K$, т. е. $g_1K = g_2K$.

Очевидно, что $\operatorname{Im}\tilde{\varphi} = \operatorname{Im}\varphi$ (образ отображения $\tilde{\varphi}$ совпадает с образом отображения φ). Поэтому $\tilde{\varphi}$ — искомый изоморфизм G/K и $\varphi(G) = \operatorname{Im}\varphi$.

Обратное утверждение в теореме совершенно тривиально. Пусть $K \lhd G$. Построим гомоморфизм $\pi\colon G \to G/K$ формулой $\pi\colon g \mapsto (gK)$. Тогда $\operatorname{Ker}\pi = K$. Этот гомоморфизм называется естественным (или каноническим) гомоморфизмом. Если у вас возникает задача построить гомоморфизм, ядро которого задано, то нужно просто брать элементы и отображать в смежный класс по той группе, которая объявлена ядром. □

Следствие 1.64. *Если* $\operatorname{Ker}\varphi = \{e\}$, *то* $G \cong \varphi(G)$.

Следствие 1.64 удобно использовать при доказательстве того, что некоторое отображение φ является изоморфизмом: достаточно проверить тривиальность ядра и *сюръективность* отображения φ. Отображение $\varphi\colon G \to H$ называется сюръективным, если оно является отображением на H. Напомним, что это в точности означает, что у каждого элемента $h \in H$ есть хотя бы один прообраз (такой элемент $g \in G$, что $\varphi(g) = h$).

Пример 1.65. Пусть $\mathbb{Z}[x]$ — аддитивная группа полиномов от x с целыми коэффициентами. Теперь возьмем множество $H = \{(x-3)f(x) \mid f(x) \in \mathbb{Z}[x]\}$ — множество полиномов, у которых есть множитель $x - 3$. Очевидно, $H \lhd \mathbb{Z}[x]$ (любая подгруппа коммутативной группы нормальна). Как построить факторгруппу?

Рассмотрим гомоморфизм $\varphi\colon f(x) \mapsto f(3)$, который каждому многочлену ставит в соответствие его значение в точке 3. В ноль отобразятся только элементы из H. Таким образом, $\mathbb{Z}[x]/H \cong \mathbb{Z}$.

Пример 1.66 (*продолжение примера* 1.38). В ядро гомоморфизма $\det\colon GL(\mathbb{R}, n) \to \mathbb{R}^*$ входят матрицы с определителем 1. Группа таких матриц обозначается $SL(\mathbb{R}, n)$. Она является нормальной подгруппой $GL(\mathbb{R}, n)$.

Пример 1.67 (*продолжение примера* 1.39). В ядро гомоморфизма $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ входят четные перестановки. Группа четных перестановок называется *знакопеременной группой*

(или альтернирующей группой) и обозначается A_n. Она является нормальной подгруппой в S_n.

Замечание 1.68. Если $H \lhd G$, то $|G| = |H| \cdot |G/H|$ (считаем группы конечными). Поэтому между элементами G и множеством пар (h, f), где $h \in H$, $f \in G/H$, существует взаимно однозначное соответствие. Однако было бы ошибкой думать, что $G \cong H \times (G/H)$. Простейший пример, когда такого изоморфизма нет, — группа S_3. Как мы видели в примере 1.40, группа $H = \langle(123)\rangle$ является нормальной подгруппой S_3. Подгруппа H — циклическая группа C_3 порядка 3. Факторгруппа S_3/H состоит из двух элементов, а потому изоморфна циклической группе C_2. Но $S_3 \ncong C_3 \times C_2$ (группа $C_3 \times C_2$ коммутативная, а S_3 — нет).

1.12. Абелевы группы

В этом разделе мы полностью опишем структуру *конечно порожденных* абелевых групп. Группа A называется конечно порожденной, если она порождается конечным множеством своих элементов: $A = \langle B\rangle$, $|B| < \infty$.

При работе с абелевыми группами удобнее использовать аддитивную запись. Поэтому (а также по более важным причинам) прямые произведения абелевых групп называются *прямыми суммами*.

Дадим определение прямой суммы абелевых групп, переписав с необходимыми изменениями в обозначениях определение прямого произведения из примера 1.35.

Прямой суммой абелевых групп A_1, A_2 называется группа $A_1 \oplus A_2$, элементами которой являются все пары (x_1, x_2), где $x_1 \in A_1$, $x_2 \in A_2$. Групповая операция в $A_1 \oplus A_2$ — это покомпонентное выполнение операций в A_1 и A_2: $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$.

Аналогично определяется прямая сумма нескольких групп A_1, A_2, …, A_n, которая обозначается $A_1 \oplus A_2 \oplus \ldots \oplus A_n$. Это множество наборов $(x_1, \ldots, x_n)$, где $x_i \in A_i$, а групповая операция на нём — покомпонентное сложение

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Проверка групповых аксиом не составляет труда: нулевым элементов группы $A_1 \oplus A_2 \oplus \ldots \oplus A_n$ является набор $(0_1, \ldots, 0_n)$; ассоциативность непосредственно вытекает из ассоциативности операций в компонентах; элемент, противоположный элементу $(x_1, \ldots, x_n)$, записывается как $(-x_1, \ldots, -x_n)$.

Прямая сумма n экземпляров одной и той же группы A обозначается A^n. Мы уже встречали прямые суммы абелевых групп в примерах: группа из примера 1.5 есть не что иное, как C_2^n, а группа из примера 1.21 и была обозначена как $\mathbb{R}^2$.

Основные примеры абелевых групп — циклическая группа C_n порядка n и циклическая группа $\mathbb{Z}$ бесконечного порядка, которая есть просто аддитивная группа целых чисел.

Теорема 1.69. *Любая конечно порожденная абелева группа изоморфна прямой сумме циклических групп.*

Замечание 1.70. Не все абелевы группы конечно порождены. Например, группа рациональных чисел $\mathbb{Q}$ относительно сложения не является конечно порожденной. Рассмотрим подгруппу $\langle a_1, a_2, \ldots, a_n \rangle$, порожденную конечным набором рациональных чисел a_1, a_2, $\ldots$, a_n. Любой элемент этой группы выражается как линейная комбинация чисел a_i с целыми коэффициентами:

$$x = x_1 a_1 + \cdots + x_n a_n. \tag{1.11}$$

Поэтому знаменатель несократимой записи x не превосходит произведения знаменателей a_i, которое мы обозначим N. Поэтому число $(N+1)^{-1}$ не принадлежит группе $\langle a_1, a_2, \ldots, a_n \rangle$.

Для построения изоморфизма из теоремы 1.69 удобно выделить структуру прямой суммы «внутри» группы A. Для этого введем новые понятия суммы подгрупп и прямой суммы подгрупп.

Абелева группа $A = A_1 + A_2 + \cdots + A_n$, порожденная подгруппами A_1, A_2, $\ldots$, A_n называется *суммой подгрупп* (или *разложением группы на подгруппы*). Если при этом для любого элемента $a \in A$ существует единственный набор таких $a_i \in A_i$, что $a = a_1 + a_2 + \cdots + a_n$, то группа $A_1 + A_2 + \cdots + A_n$ называется *прямым разложением группы на подгруппы* (или прямой суммой).

Утверждение 1.71. *Если $A = A_1 + A_2 + \dots + A_n$ — прямое разложение абелевой группы, то $A \cong A_1 \oplus A_2 \oplus \dots \oplus A_n$.*

Доказательство. Искомый изоморфизм имеет вид

$$\varphi\colon a \mapsto (a_1, a_2, \dots, a_n), \quad \text{где } a = a_1 + a_2 + \dots + a_n.$$

В силу определения прямого разложения отображение φ корректно определено и взаимно однозначно. Проверим, что φ сохраняет операцию: если $a = a_1 + a_2 + \dots + a_n$, где $a_i \in A_i$, а $b = b_1 + b_2 + \dots + b_n$, где $b_i \in A_i$, то $a + b = (a_1 + b_1) + (a_2 + b_2) + \dots + (a_n + b_n)$ (здесь использована коммутативность), т. е. $\varphi(a + b) = (a_1 + b_1, a_2 + b_2, \dots) = (a_1, \dots, a_n) + (b_1, \dots, b_n) = \varphi(a) + \varphi(b)$. □

Замечание 1.72. В случае неабелевых групп существование разложения в произведение подгрупп не гарантирует, что группа изоморфна прямому произведению подгрупп. Пусть $H \lhd G$, $K < G$, $H \cap K = \{e\}$ и $HK = G$. В этом случае говорят, что группа разлагается в *полупрямое произведение* подгрупп H и K (обозначение $G = H \leftthreetimes K$). Для полупрямых произведений не выполняется аналог утверждения 1.71. Например,

$$S_3 = \langle (123) \rangle \leftthreetimes \langle (12) \rangle \ncong C_3 \times C_2.$$

(сравни с замечанием 1.68).

Теперь разберемся, какие соотношения могут быть между порождающими конечно порожденной абелевой группы $A = \langle a_1, a_2, \dots, a_n \rangle$. Поскольку группа коммутативна, любое соотношение можно записать в виде

$$c_1 a_1 + c_2 a_2 + \dots + c_n a_n = 0, \quad c_1, \dots, c_n \in \mathbb{Z}, \tag{1.12}$$

объединяя все слагаемые вида a_i. Соотношение (1.12) будем задавать набором $\boldsymbol{c} = (c_1, \dots, c_n)$ его коэффициентов. Если $\boldsymbol{c}_1, \dots, \boldsymbol{c}_k$ — соотношения, то $x_1 \boldsymbol{c}_1 + \dots + x_k \boldsymbol{c}_k$, $x_i \in \mathbb{Z}$, — также соотношение, которое мы будем называть *следствием* соотношений $\boldsymbol{c}_1, \dots, \boldsymbol{c}_k$ (здесь + обозначает покомпонентную сумму целочисленных наборов). Поэтому множество всех соотношений между порождающими группы A является подгруппой R группы $\mathbb{Z}^n$. Поскольку каждый элемент группы A можно записать в виде целочисленной комбинации порождающих, то неудивительно следующее утверждение.

Утверждение 1.73. *Во введенных выше обозначениях* $A \cong \mathbb{Z}^n/R$.

Пример 1.74. Пусть $A = C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_r}$. Обозначим через a_i порождающий элемент группы C_{n_i}. Множество $\{a_i\}$ порождает A. По определению прямой суммы

$$c_1a_1 + c_2a_2 + \cdots + c_na_n = 0$$

тогда и только тогда, когда $c_i = y_in_i$, $y_i \in \mathbb{Z}$. Значит, соотношения образуют подгруппу D в $\mathbb{Z}^n$, содержащую те наборы из n целых чисел, в которых i-й элемент набора делится на n_i. Смежный класс по подгруппе D состоит из множества наборов, имеющих заданный набор остатков от деления на n_i, поэтому факторгруппа $\mathbb{Z}^n/D$ изоморфна $C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_r}$.

Доказательство утверждения 1.73. Пусть элемент $a \in A$ двумя способами выражен через порождающие:

$$a = c_1a_1 + c_2a_2 + \cdots + c_na_n = c'_1a_1 + c'_2a_2 + \cdots + c'_na_n.$$

Тогда

$$(c_1 - c'_1)a_1 + (c_2 - c'_2)a_2 + \cdots + (c_n - c'_n)a_n = 0,$$

т. е. $\boldsymbol{c}-\boldsymbol{c}' \in R$. Разумеется, верно и обратное. Поэтому каждому $a \in A$ можно сопоставить класс смежности $\rho(a)$ группы $\mathbb{Z}^n$ по подгруппе R, который состоит из тех $\boldsymbol{c} = (c_1, \ldots, c_n)$, для которых

$$a = c_1a_1 + c_2a_2 + \cdots + c_na_n. \tag{1.13}$$

Отображение ρ является искомым изоморфизмом. Складывая соотношения (1.13), убеждаемся, что ρ сохраняет операции. Единственным прообразом класса $\boldsymbol{c} + R$ является $c_1a_1 + \cdots + c_na_n$. □

Следующий шаг — описание подгрупп группы $\mathbb{Z}^n$.

Лемма 1.75. *Пусть* $R < \mathbb{Z}^n$. *Тогда* $R \cong \mathbb{Z}^m$, $0 \leqslant m \leqslant n$.

Подгруппой $\mathbb{Z}^0$ будем по определению считать подгруппу, состоящую из одного нуля.

Доказательство. Индукция по n. Основание индукции $n = 1$ было уже разобрано выше (см. вывод формулы (1.5) на с. 30).

Теперь предположим, что утверждение леммы доказано при всех $n' < n$. В подгруппе $R < \mathbb{Z}^n$ выделим подгруппу

$$R_0 = \{x \in R : x_n = 0\}.$$

Поскольку R_0 изоморфна подгруппе $\mathbb{Z}^{n-1}$ (равные нулю последние компоненты можно опустить), то по предположению индукции $R \cong \mathbb{Z}^k$, $0 \leqslant k \leqslant n-1$.

Если $R_0 = R$, утверждение леммы доказано.

В противном случае рассмотрим подмножество $\tilde{R}_n$ целых чисел, состоящее из последних компонент элементов $r \in R$. Это множество является подгруппой $\mathbb{Z}$, поэтому имеет вид $\langle d \rangle$ (формула (1.5)). Выберем $r = (r_1, r_2, \ldots, r_{n-1}, d) \in R$, у которого последняя компонента равна d.

Докажем, что $R = R_0 + \langle r \rangle$ — прямое разложение. Для любого $r' \in R$ найдется не более одного целого числа t, для которого $r' - tr \in R_0$. Поскольку последние компоненты всех элементов R кратны d, такое число t обязательно найдется. Тогда $r' - tr \in R_0$, поэтому r' представляется в виде суммы элемента R_0 и элемента из подгруппы $\langle r \rangle$, и это представление однозначно определено.

Итак, по утверждению 1.71,

$$R \cong R_0 \oplus \langle r' \rangle \cong \mathbb{Z}^k \oplus \mathbb{Z} \cong \mathbb{Z}^m,$$

где $0 \leqslant m \leqslant n$. □

Отметим очевидное следствие из доказанной леммы.

Следствие 1.76. *Для любой конечно порожденной абелевой группы существует такой конечный набор соотношений $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k$, что всякое соотношение $\boldsymbol{c}$ между порождающими является следствием $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k$.*

Итак, из утверждения 1.73 и леммы 1.75 вытекает, что любую конечно порожденную абелеву группу с n порождающими элементами можно задать целочисленной матрицей размера $m \times n$, $m \leqslant n$,

$$M = \begin{pmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \\ \ldots \\ \boldsymbol{c}_m \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ c_{m1} & c_{m2} & \ldots & c_{mn} \end{pmatrix}.$$

Любой матрице M указанного вида соответствует группа

$$A(M) = \mathbb{Z}^n / \langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m \rangle.$$

Некоторым матрицам соответствует одна и та же группа. Чтобы описать матрицы, которые задают изоморфные группы, введем понятие элементарного преобразования матрицы.

Элементарное преобразование целочисленной матрицы — это одно из следующих преобразований:

- прибавление к элементам одной строки соответствующих элементов другой строки, умноженных на одно и то же целое число;
- прибавление к элементам одного столбца соответствующих элементов другого столбца, умноженных на одно и то же целое число;
- перестановка строк;
- перестановка столбцов;
- умножение элементов некоторой строки или столбца на -1.

Лемма 1.77. *Пусть M' получена из M последовательностью элементарных преобразований. Тогда $A(M) \cong A(M')$.*

Доказательство. Так как отношение изоморфизма транзитивно, лемму достаточно проверить для матриц, связанных одним элементарным преобразованием. Очевидно, что перестановка строк не влияет на $A(M)$, равно как и умножение на -1.

Перестановка столбцов приводит к перестановке порождающих, что дает изоморфную группу (изоморфизм переставляет компоненты, см. пример 1.35).

Рассмотрим прибавление кратного строки. Пусть

$$M = \begin{pmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \\ \ldots \\ \boldsymbol{c}_m \end{pmatrix}, \quad M' = \begin{pmatrix} \boldsymbol{c}'_1 \\ \boldsymbol{c}_2 \\ \ldots \\ \boldsymbol{c}_m \end{pmatrix}, \quad \boldsymbol{c}'_1 = \boldsymbol{c}_1 + t\boldsymbol{c}_2, \quad t \in \mathbb{Z}.$$

Тогда $\boldsymbol{c}_1 = \boldsymbol{c}'_1 - t\boldsymbol{c}_2$, поэтому $\langle \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m \rangle = \langle \boldsymbol{c}'_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m \rangle$.

Теперь рассмотрим прибавление кратного столбца. Пусть

$$M = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{pmatrix}, \quad M' = \begin{pmatrix} c'_{11} & c_{12} & \dots & c_{1n} \\ c'_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c'_{m1} & c_{m2} & \dots & c_{mn} \end{pmatrix},$$

где $c'_{i1} = c_{i1} + tc_{i2}$, $t \in \mathbb{Z}$. Обозначим порождающие группы $A(M)$ через $a_1, a_2, \dots, a_n$, а порождающие группы $A(M')$ через $a'_1, a'_2, \dots, a'_n$. Построим такой изоморфизм $\varphi\colon A(M) \to A(M')$, что

$$\varphi(a_1) = a'_1,\ \varphi(a_2) = ta'_1 + a'_2,\ \varphi(a_3) = a'_3,\ \dots,\ \varphi(a_n) = a'_n. \tag{1.14}$$

Поскольку φ должен сохранять операции, образ любого элемента $A(M)$ определен условиями (1.14):

$$\varphi(x_1a_1 + x_2a_2 + \dots + x_na_n) = x_1\varphi(a_1) + x_2\varphi(a_2) + \dots + x_n\varphi(a_n). \tag{1.15}$$

Проверим, что формула (1.15) корректно задает отображение из $A(M)$ в $A(M')$. Пусть

$$(x_1 - y_1, \dots, x_n - y_n) = \sum_{j=1}^{m} \lambda_j \boldsymbol{c}_j,\ \lambda_j \in \mathbb{Z},$$

т. е. $x = x_1a_1 + x_2a_2 + \dots + x_na_n = y_1a_1 + y_2a_2 + \dots + y_na_n = y$ в группе A. Тогда

$$\sum_{j=1}^{m} \lambda_j \boldsymbol{c}'_j = ((x_1 - y_1) + t(x_2 - y_2), x_2 - y_2, \dots, x_n - y_n),$$

поэтому

$$(x_1 - y_1)a'_1 + t(x_2 - y_2)a'_1 + (x_2 - y_2)a'_2 + \dots + (x_n - y_n)a'_n = \\ = (x_1 - y_1)\varphi(a_1) + (x_2 - y_2)\varphi(a_2) + \dots + (x_n - y_n)\varphi(a_n) = 0,$$

так что $\varphi(x) = \varphi(y)$.

Обратное отображение задается формулами

$$\varphi^{-1}(a'_1) = a_1,\ \varphi^{-1}(a'_2) = -ta_1 + a_2,\ \varphi^{-1}(a'_3) = a_3,\ \dots \\ \dots, \varphi^{-1}(a'_n) = a_n,$$

корректность которых доказывается аналогично. □

Для доказательства теоремы 1.69 мы применим следующую теорему.

Теорема 1.78 (нормальная форма Смита). *Целочисленную матрицу M размера $m \times n$, $m \leqslant n$, можно привести элементарными преобразованиями к такому виду, что все элементы вне главной диагонали равны* 0, *а для диагональных элементов m_{ii} выполняется условие*: m_{ii} *делит* $m_{(i+1)(i+1)}$.

Доказательство. Если матрица состоит из одних нулей, то утверждение теоремы справедливо.

Пусть в M есть ненулевые элементы. Будем применять к M элементарные преобразования до тех пор, пока можно уменьшить минимальную абсолютную величину ненулевого элемента матрицы. Затем перестановками строк и столбцов (и умножением строк на -1) добьемся, чтобы m_{11} стал положительным элементом с минимальной абсолютной величиной среди элементов матрицы.

Докажем, что все ненулевые элементы матрицы делятся на m_{11}. Пусть m_{i1} не делится на m_{11}. Разделим m_{i1} на m_{11} с остатком: $m_{i1} = qm_{11} + r$. Если вычесть из i-й строки первую строку, умноженную на q, то $m'_{i1} = r$, т. е. мы уменьшили минимальную абсолютную величину ненулевых элементов матрицы. Аналогично рассуждаем для элементов первой строки.

Пусть теперь m_{ij} не делится на m_{11}, т. е. $m_{ij} = qm_{11} + r$, $0 < r < m_{11}$. Как уже доказано, $m_{i1} = am_{11}$, $m_{1j} = bm_{11}$. И в этом случае элементарными преобразованиями матрицы можно уменьшить минимальную абсолютную величину ненулевых элементов матрицы. Вычтем из i-й строки первую строку, умноженную на $(a-1)$, а затем из j-го столбца вычтем первый столбец, умноженный на $q-(a-1)b$. После этих преобразований (i,j)-й элемент матрицы будет равен r, как показывают вычисления (приводим только минор матрицы, образованный первой и i-й строкой и первым и j-м столбцом):

$$\begin{pmatrix} m_{11} & bm_{11} \\ am_{11} & qm_{11}+r \end{pmatrix} \to \begin{pmatrix} m_{11} & bm_{11} \\ m_{11} & (q-(a-1)b)m_{11}+r \end{pmatrix} \to$$
$$\to \begin{pmatrix} m_{11} & (b-q+(a-1)b)m_{11} \\ m_{11} & r \end{pmatrix}.$$

Поскольку все ненулевые элементы матрицы делятся на m_{11}, можно элементарными преобразованиями сделать равными нулю все элементы первого столбца и первой строки, за исключением m_{11} (вычитая подходящие кратные первой строки или первого столбца). После этого матрица приобретает вид

$$M = \begin{pmatrix} m_{11} & 0 \\ 0 & M' \end{pmatrix},$$

где все ненулевые элементы матрицы M' делятся на m_{11}, а размер M' меньше, чем у исходной матрицы.

К матрице M' можно применить такие же преобразования, какие были применены к M и т. д. В конце концов получим требуемую форму матрицы. □

Доказательство теоремы 1.69. Пусть A — конечно порожденная абелева группа. Представим ее в виде $A \cong A(M)$. В силу леммы 1.77 и теоремы 1.78 можно считать, что матрица M диагональная. Если $M = 0$, то $A \cong \mathbb{Z}^n$. В противном случае обозначим ненулевые диагональные элементы матрицы M через n_i, $1 \leqslant i \leqslant k$, соответствующие столбцам M порождающие элементы обозначим через a_i. Соотношение вида $\sum_i x_i a_i = 0$ является следствием соотношений из диагональной матрицы M тогда и только тогда, когда $n_i \mid x_i$. Последнее означает, что $x_i a_i = 0$. Это означает, что разложение любого элемента группы в сумму порождающих однозначно. Поэтому, пользуясь утверждением 1.71, получаем, что группа A изоморфна прямой сумме циклических групп $\langle a_i \rangle$. □

Анализ структуры конечных абелевых групп можно продолжить. Для этого необходимы некоторые факты из элементарной теории чисел. В главе 2 эти факты будут выведены из более общей теории. Заметим, что доказательства этих фактов не используют утверждений из данного раздела, так что порочного круга в рассуждениях можно не опасаться.

Из следствия 2.43 вытекает, что если p, q — взаимно простые числа, то $C_{pq} \cong C_p \oplus C_q$. Поэтому можно построить такое разложение конечно порожденной абелевой группы в прямую сумму циклических, в котором все слагаемые — группы порядка p^k, где p — простое число (*примарные компоненты*).

Оказывается, что набор порядков примарных компонент определен однозначно.

Теорема 1.79. *Любая конечная абелева группа изоморфна прямой сумме циклических групп порядков p^k, p — простое, причем количество примарных компонент порядка p^k одинаково для любого разложения в прямую сумму.*

Доказательство. Первая часть теоремы, как уже сказано, вытекает из теоремы 1.69 и следствия 2.43. Осталось доказать вторую часть. В этом доказательстве мы используем основную теорему арифметики об однозначности разложения целого числа на простые множители (следствие из теоремы 2.39, доказываемой в следующей главе).

Итак, пусть имеется конечная абелева группа A. Ее можно разложить в прямую сумму примарных компонент:

$$A \cong C_{p_1}^{k_{11}} \oplus C_{(p_1)^2}^{k_{12}} \oplus \cdots \oplus C_{(p_1)^{s_1}}^{k_{1s_1}} \oplus \cdots \oplus C_{p_r}^{k_{r1}} \oplus \cdots \oplus C_{(p_r)^{s_r}}^{k_{rs_r}}. \quad (1.16)$$

Выберем одно из чисел p_i и докажем, что числа k_{ij} не зависят от выбора разложения (1.16). Повторяя это рассуждение для всех простых делителей порядка группы, получим отсюда утверждение теоремы. Для простоты обозначений полагаем $p_i = p$, $k_{ij} = k_j$, $s_i = s$.

Возведение в степень $\varphi_n \colon x \mapsto nx$ является гомоморфизмом абелевой группы, так как $n(x+y) = nx + ny$. Обозначим через $A^{(n)}$ образ A при гомоморфизме возведения в n-ю степень. Порядок группы $|A| = p^{a_0}q$, где $p \nmid q$. Из основной теоремы арифметики следует, что число a_0 определено однозначно. Обозначим $a_t = |A^{(p^t q)}|$, $1 \leqslant t < a_0$. В определении чисел a_t не использовалось никакого разложения вида (1.16). Поэтому, если мы выразим k_j через a_t, то тем самым докажем, что числа k_j также не зависят от выбора разложения.

Докажем, что

$$(A_1 \oplus A_2)^{(n)} \cong A_1^{(n)} \oplus A_2^{(n)}. \quad (1.17)$$

Каждый элемент $x \in (A_1 \oplus A_2)^{(n)}$ имеет вид (nx_1, nx_2), где $x_1 \in A_1$, $x_2 \in A_2$. Отображение $\alpha \colon x \mapsto (nx_1, nx_2)$ задает искомый изоморфизм. Прежде всего нужно проверить корректность. Если $nx = ny$, где $x = x_1 + x_2$, $y = y_1 + y_2$, $x_1, y_1 \in A_1$, $x_2, y_2 \in A_2$, то по определению прямой суммы

$nx_1 = nx_2$, $ny_1 = ny_2$. Таким образом, отображение α корректно определено (не зависит от выбора представителя класса смежности). Проверим, что α сохраняет операцию:

$$\begin{aligned}\alpha\big((nx_1, nx_2) + (ny_1, ny_2)\big) &= \alpha(nx_1 + ny_1, nx_2 + ny_2) = \\ &= (nx_1 + ny_1, nx_2 + ny_2) = (nx_1, nx_2) + (ny_1, ny_2) = \\ &= \alpha(nx_1, nx_2) + \alpha(ny_1, ny_2).\end{aligned}$$

Из определения ясно, что α является взаимно однозначным отображением.

По индукции можно доказать, что соотношение (1.17) выполняется и для прямой суммы нескольких слагаемых.

Чтобы выразить a_t через k_j, найдем образы циклических групп при гомоморфизмах возведения в степень.

Если n делится на m, то для любого $x \in C_m$ выполнено $nx = 0$ (порядок элемента делит порядок группы). Значит, в этом случае $C_m^{(n)}$ — единичная группа. С другой стороны, если n взаимно просто с m, то для любого $x \in C_m$ выполнено $nx \neq 0$. Это означает, что ядро гомоморфизма возведения в степень в этом случае нулевое и $C_m^{(n)} = C_m$.

Пусть $n = p^t$, $m = p^k$. Если $t < k$, то $C_m^{(n)} = C_{p^{k-t}}$ (кратные p^t имеют вид $p^t ua$, $0 \leqslant u < p^{k-t} - 1$, a — порождающий C_m). Если $t \geqslant k$, то $C_m^{(n)}$ — единичная, так как n делит порядок группы.

Из разложения (1.16) и изоморфизма (1.17) получаем

$$A^{(p^t q)} \cong C_p^{k_{t+1}} \oplus C_{p^2}^{k_{t+2}} \oplus \cdots \oplus C_{p^{s-t}}^{k_s}.$$

Порядок группы равен произведению порядков прямых слагаемых. Поэтому получаем систему уравнений

$$\begin{aligned}k_1 + 2k_2 + 3k_3 + \cdots + ik_i + (i+1)k_{i+1} + \cdots + sk_s &= a_0, \\ k_2 + 2k_3 + \cdots + (i-1)k_i + ik_{i+1} + \cdots + (s-1)k_s &= a_1, \\ &\cdots \\ k_i + 2k_{i+1} + \cdots + (s-i+1)k_s &= a_i, \\ &\cdots \\ k_s &= a_{s-1},\end{aligned}$$

из которой k_j однозначно выражаются через a_t. □

1.13. Задачи

Некоторые из предлагаемых ниже задач очень просты и получаются немедленным применением приведенных в основном тексте рассуждений. Но есть и сложные задачи, которые требуют привлечения новых идей.

1.1. Является ли ассоциативной операция $*$ на множестве положительных действительных чисел, задаваемая формулой

$$x * y = \frac{xy}{x+y} \ ?$$

1.2. Построить пример неассоциативной бинарной операции, для которой выполняются аксиома единицы и аксиома обратного элемента.

1.3. Доказать, что конечное множество G, в котором определена ассоциативная алгебраическая операция и каждое из уравнений $ax = b$, $ya = b$ для любых a и b из G имеет в G единственное решение, будет группой.

1.4. Пусть в полугруппе G есть правая единица e (для любого $x \in G$ выполнено $xe = x$) и для любого $x \in G$ есть правый обратный x^{-1} ($x \cdot x^{-1} = e$). Доказать, что тогда G — группа (в частности, единица в ней единственна и для каждого элемента обратный тоже единственен).

1.5. Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

1) целые числа относительно сложения;

2) четные числа относительно сложения;

3) целые числа, кратные данному натуральному числу n, относительно сложения;

4) степени данного действительного числа a, $a \neq 0, \pm 1$, с целыми показателями относительно умножения;

5) неотрицательные целые числа относительно сложения;

6) нечетные целые числа относительно сложения;

7) целые числа относительно вычитания;

8) рациональные числа относительно сложения;

9) рациональные числа относительно умножения;

10) рациональные числа, отличные от нуля, относительно умножения;

11) положительные рациональные числа относительно умножения;

12) положительные рациональные числа относительно деления;

13) двоично-рациональные числа, т. е. рациональные числа, знаменатели которых, — степени числа 2 с целыми неотрицательными показателями, относительно сложения;

14) все рациональные числа, знаменатели которых равны произведениям простых чисел из данного множества M (конечного или бесконечного) с целыми неотрицательными показателями (лишь конечное число которых может быть отлично от нуля), относительно сложения;

15) корни n-й степени из единицы (как действительные, так и комплексные) относительно умножения;

16) корни всех целых положительных степеней из единицы относительно умножения;

17) матрицы порядка n с действительными элементами относительно умножения;

18) невырожденные матрицы порядка n с действительными элементами относительно умножения;

19) матрицы порядка n с целыми элементами относительно умножения;

20) матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения;

21) матрицы порядка n с целыми элементами и определителем, равным ± 1 относительно умножения;

22) матрицы порядка n с действительными элементами относительно сложения;

23) перестановки чисел $1, 2, \ldots, n$ относительно композиции перестановок;

24) четные перестановки чисел $1, 2, \ldots, n$ относительно композиции перестановок;

25) нечетные перестановки чисел $1, 2, \ldots, n$ относительно композиции перестановок;

26) взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t, затем s);

27) преобразования множества M, т. е. взаимно однозначные отображения этого множества на себя, относительно композиции отображений;

28) векторы n-мерного линейного пространства $\mathbb{R}^n$ относительно сложения;

29) параллельные переносы трехмерного пространства $\mathbb{R}^3$ относительно композиции движений;

30) повороты трехмерного пространства $\mathbb{R}^3$ вокруг прямых, проходящих через данную точку O относительно композиции движений;

31) все движения трехмерного пространства $\mathbb{R}^3$ относительно композиции движений;

32) положительные действительные числа относительно операции $a * b = a^b$;

33) положительные действительные числа относительно операции $a * b = a^2b^2$;

34) действительные многочлены степени не выше n от неизвестного x и нулевой многочлен относительно сложения;

35) действительные многочлены степени n от переменной x относительно сложения;

36) действительные многочлены любых степеней (включая 0) от переменной x относительно сложения;

37) отрезок $[0, 1]$ с операцией $\oplus$, где $\alpha \oplus \beta$ — дробная часть $\alpha + \beta$;

38) множество функций вида

$$y = \frac{ax + b}{cx + d}, \quad \text{где } a, b, c, d \in \mathbb{R} \text{ и } ad - bc \neq 0.$$

1.6. Доказать, что множество $A_1(\mathbb{R})$ так называемых аффинных преобразований $\varphi_{a,b}\colon x \mapsto ax + b$ $(a, b \in \mathbb{R};\ a \neq 0)$ вещественной прямой $\mathbb{R}$ образует группу с законом умножения $\varphi_{a,b}\varphi_{c,d} = \varphi_{ac,ad+b}$. В группе $A_1(\mathbb{R})$ содержится подгруппа $GL(1, \mathbb{R})$, оставляющая точку $x = 0$ на месте, и подгруппа «чистых сдвигов» $x \mapsto x + b$.

1.7. В любой ли группе выполняются тождества

а) $(ab)^{-1}(ab^{-1}a^{-1})^{-1}a = e$,

б) $(aba^{-1}b^{-1})(bab^{-1}a^{-1})^{-1} = e$?

1.8. Для любых трех элементов a, b, c группы G выполняется равенство

$$abc = cba.$$

Верно ли, что группа коммутативная?

1.9. Пусть в группе G выполняется тождество $a \cdot a = e$. Доказать, что G — коммутативная.

1.10*. Доказать, что группа корней n-й степени из единицы является единственной мультипликативной группой n-го порядка с комплексными элементами.

1.11*. Найти все (с точностью до изоморфизма) группы порядка а) 3; б) 4; в) 6. Выписать таблицы умножения этих групп и представить эти группы в виде групп перестановок.

1.12. Доказать, что группы 1) – 4) задачи 1.5 изоморфны между собой.

1.13*. Доказать, что:

а) симметрическая группа S_n при $n > 1$ порождается транспозициями $(1\,2)$, $(1\,3)$, $\ldots$, $(1\,n)$;

б) знакопеременная группа A_n при $n > 2$ порождается множеством всех тройных циклов $(i\,j\,k)$;

в) знакопеременная группа A_n при $n > 2$ порождается тройными циклами: $(1\,2\,3)$, $(1\,2\,4)$, $(1\,2\,n)$.

1.14. Найти минимальное количество перестановок n элементов, порождающих группу S_n, $n \geqslant 3$.

1.15. Найти порядок элемента

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} \in S_6.$$

1.16. Существует ли в S_6 элемент порядка 8?

1.17. Циклична ли группа $C_2 \times C_5$?

1.18. В циклической группе $\langle a \rangle$ порядка n найти все элементы g, удовлетворяющие условию $g^k = e$, и все элементы порядка k при

а) $n = 24$, $k = 6$;

б) $n = 100$, $k = 20$;

в) $n = 100$, $k = 5$;

г) $n = 360$, $k = 30$;

д) $n = 360$, $k = 12$;

е) $n = 360$, $k = 7$.

1.19. Пусть $G = \langle a \rangle$ — конечная циклическая группа порядка n. Доказать утверждения:

а) для любого делителя d числа n существует единственная подгруппа H группы G, имеющая порядок d;

б) порождающими подгруппы H порядка d являются все элементы порядка d группы G. В частности, $H = \langle a^{n/d} \rangle$.

1.20. Доказать, что если элемент x группы G имеет бесконечный порядок, то $x^k = x^m$ тогда и только тогда, когда $k = m$.

1.21. Доказать, что если e — единица и a — элемент порядка n группы G, то $a^k = e$ тогда и только тогда, когда k делится на n.

1.22. Найти порядок элемента x^k, если порядок элемента x равен n.

1.23. Доказать утверждения:

а) если элементы a и b группы G перестановочны (коммутируют), т. е.

$$ab = ba \qquad (1^\circ)$$

и имеют конечные взаимно простые порядки r и s, то их произведение ab имеет порядок rs;

б) если элементы a и b группы G перестановочны, имеют конечные порядки r и s и пересечение порожденных ими циклических подгрупп содержит лишь единицу e, т. е.

$$\langle a \rangle \cap \langle b \rangle = \langle e \rangle, \qquad (2^\circ)$$

то порядок произведения ab равен наименьшему общему кратному r и s. Показать на примерах, что для справедливости последнего утверждения каждого из условий (1°) и (2°) в отдельности недостаточно и что условие (1°) не является следствием условия (2°), даже для взаимно простых порядков элементов a и b;

в) если порядки r и s элементов a и b взаимно просты, то условие (2°) выполняется;

г) показать на примере, что без условия (2°) порядок произведения ab не определяется однозначно порядками сомножителей a и b.

1.24. Пусть $G = \langle a \rangle$ — циклическая группа порядка n. Доказать, что:

а) если n и k взаимно просты, то в G существует корень $\sqrt[k]{a}$, т. е. a является k-й степенью некоторого элемента из G и обратно;

б) в группе нечетного порядка все элементы являются квадратами.

1.25. Пусть порядок элемента x группы G есть число pq, где p и q — взаимно просты. Доказать, что в группе G найдутся такие элементы u и v, что выполняются равенства

$$uv = vu, \quad u^p = e, \quad v^q = e.$$

1.26*. Доказать, что если в конечной группе G порядка n для каждого делителя d числа n уравнение $x^d = e$ имеет не более d решений, то группа G — циклическая.

1.27*. *Показателем* группы назовем наименьшее общее кратное порядков ее элементов. Доказать, что группа циклическая тогда и только тогда, когда показатель равен порядку группы.

1.28. Какие из групп задачи 1.5 являются подгруппами других из этих групп?

1.29. Доказать, что любая бесконечная группа имеет бесконечное число подгрупп.

1.30. Найти с точностью до изоморфизма все группы, которые изоморфны любой своей неединичной подгруппе.

1.31. Найти все подгруппы:

а) циклической группы порядка 6;

б) циклической группы порядка 24;

в) четверной группы (задача 1.11);

г) симметрической группы S_3.

д) Какие из подгрупп группы S_3 являются нормальными делителями?

е) Доказать, что знакопеременная группа четвертой степени A_4 не имеет подгруппы шестого порядка. Таким образом, группа G порядка n для некоторых k, делящих n, может не иметь подгрупп порядка k.

1.32. Найти все подгруппы группы G порядка 8, все элементы которой, кроме единицы e, имеют порядок 2.

1.33. Найти все подгруппы циклической группы порядка p^n, где p — простое число.

1.34. Найти смежные классы

а) аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу d;

б) аддитивной группы действительных чисел по подгруппе целых чисел;

в) аддитивной группы комплексных чисел по подгруппе целых гауссовых чисел, т. е. чисел вида $m + ni$, $m, n \in \mathbb{Z}$;

г) аддитивной группы векторов плоскости (выходящих из начала координат) по подгруппе векторов, лежащих на оси Ox;

д) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе чисел, равных по модулю единице;

е) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе положительных действительных чисел;

ж) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе действительных чисел;

з) симметрической группы S_n по подгруппе перестановок, оставляющих число n на месте.

1.35. Доказать, что

а) если H — конечное множество элементов группы G и произведение двух любых элементов из H снова лежит в H, то $H < G$;

б) если все элементы множества H группы G имеют конечные порядки и произведение двух любых элементов из H снова лежит в H, то H будет подгруппой группы G.

1.36. Найти центр у группы обратимых действительных матриц размера $n \times n$.

1.37. Сколько подгрупп второго порядка имеет группа S_5?

1.38. Есть ли подгруппа индекса 2 в A_n?

1.39. Периодической частью группы G называется множество всех ее элементов конечного порядка. Доказать, что периодическая часть коммутативной группы является подгруппой.

1.40. Доказать, что если в коммутативной группе G есть элементы бесконечного порядка, и все они содержатся в подгруппе H, то $H = G$.

1.41*. Доказать, что подгруппа H индекса два любой группы G содержит квадраты всех элементов группы G.

1.42*. Доказать, что при $n > 1$ знакопеременная группа A_n является единственной подгруппой индекса два в симметриче-

ской группе S_n. Привести пример конечной группы, содержащей несколько подгрупп индекса два.

1.43. Доказать, что:

а) группа положительных действительных чисел по умножению изоморфна группе всех действительных чисел по сложению;

б) группа положительных рациональных чисел по умножению не изоморфна группе всех рациональных чисел по сложению.

1.44. Доказать, что в коммутативной группе множество элементов, порядки которых делят фиксированное число, является подгруппой. Верно ли это утверждение для некоммутативной группы?

1.45. Доказать, что группа G' является гомоморфным образом конечной циклической группы G тогда и только тогда, когда G' также циклическая и ее порядок делит порядок группы G.

1.46. Доказать, что если группа G гомоморфно отображена на группу G', причем $a \mapsto a'$, то

а) порядок a делится на порядок a';

б) порядок G делится на порядок G'.

1.47. Доказать, что порядок любой нечетной перестановки в S_n четен.

1.48. Найти все гомоморфные отображения а) циклической группы C_n в себя; б) C_6 в C_{18}; в) C_{18} в C_6; г) C_{12} в C_{15}; д) C_6 в C_{25}.

1.49. Доказать, что аддитивную группу рациональных чисел нельзя гомоморфно отобразить на аддитивную группу целых чисел.

1.50. Пусть p — простое число. Изоморфны ли группы C_{p^2} и $C_p \times C_p$?

1.51. Изоморфны ли группы а) $C_{18} \times C_{20}$ и $C_{12} \times C_{30}$; б) $C_{18} \times C_{20}$ и $C_{36} \times C_{10}$?

1.52. Сколько подгрупп, изоморфных C_4, содержится в $C_{12} \times C_{18}$?

1.53*. Доказать, что:

а) группа тетраэдра изоморфна группе четных перестановок четырех элементов;

б) группы куба и октаэдра изоморфны группе всех перестановок четырех элементов;

в) группы додекаэдра и икосаэдра изоморфны группе четных перестановок пяти элементов.

1.54. Пусть в конечной группе G выполняется тождество $a \cdot a = e$. Доказать, что эта группа изоморфна группе подмножеств конечного множества относительно операции симметрической разности: $A \oplus B = (A \setminus B) \cup (B \setminus A)$.

1.55. Сколько есть разных ожерелий из 2 красных, 2 зеленых и 2 желтых бусин? (Определение разных ожерелий см. в примере 1.55.)

1.56. Является ли нормальной подгруппа симметрической группы S_n, которая содержит все перестановки, оставляющие число n на месте?

1.57. Является ли нормальной подгруппой в S_{10} группа перестановок, которые каждое четное число оставляют на месте?

1.58. Доказать, что в любой группе перестановок, содержащей хотя бы одну нечетную перестановку:

а) число четных перестановок равно числу нечетных;

б) четные перестановки образуют нормальный делитель;

в) все простые группы перестановок n элементов (где $n > 2$) содержатся в знакопеременной группе A_n (*простой* называется группа, не имеющая нормальных делителей, кроме себя самой и единичной подгруппы).

1.59. Доказать, что центр группы G (пример 1.18 на с. 25) является нормальным делителем.

1.60. Элемент $aba^{-1}b^{-1}$ называется *коммутатором* элементов a и b группы G. Доказать, что группа K, порожденная коммутаторами всех пар элементов группы, является нормальной подгруппой K группы G. Эта подгруппа называется *коммутантом* G.

1.61. Доказать, что любая четная перестановка является коммутатором некоторых перестановок. Найти коммутант симметрической группы S_n.

1.62. Привести пример группы, в которой коммутант не совпадает с множеством коммутаторов.

1.63. Пусть G — группа всех собственных движений трехмерного пространства, H — подгруппа параллельных переносов, K — подгруппа вращений, оставляющих неподвижной

точку O. Доказать, что

а) H является нормальным делителем G, а K — нет;

б) факторгруппа G/H изоморфна K.

1.64. Доказать, что нормальный делитель группы G, имеющий конечный индекс k, содержит все элементы группы G, порядки которых взаимно просты с k. Показать на примере, что для подгруппы H, не являющейся нормальным делителем, утверждение может быть неверным.

1.65. Доказать, что факторгруппа G/H тогда и только тогда коммутативна, когда H содержит коммутант K группы G.

1.66. Доказать, что во всякой группе элементы x и yxy^{-1} имеют один и тот же порядок.

1.67. Доказать, что для любых элементов a, b и c группы G:

а) элементы ab и ba имеют одинаковый порядок;

б) элементы abc, bca и cab имеют одинаковый порядок.

1.68. Построить пример группы, в которой есть такие элементы a, b, c, что abc и cba имеют разный порядок.

1.69*. Доказать, что:

а) четверная группа V (задача 1.11) является нормальным делителем симметрической группы S_4;

б) факторгруппа S_4/V изоморфна симметрической группе S_3.

1.70*. Найти число перестановок симметрической группы S_n, коммутирующих с данной перестановкой σ.

1.71*. Доказать, что если пересечение двух нормальных делителей H_1 и H_2 группы G содержит лишь единицу e, то $h_1h_2 = h_2h_1$ для всех элементов $h_1 \in H_1$, $h_2 \in H_2$.

1.72. Пусть в группе G подгруппа $N(a)$ является нормализатором элемента a. Показать, что для любого $x \in G$ нормализатором элемента xax^{-1} будет $xN(a)x^{-1}$.

1.73. Пусть $N = N(H)$ — нормализатор подгруппы H в группе G. Дано правое разложение G по $N(H)$:

$$G = Nx_1 \dot\cup Nx_2 \dot\cup \ldots \dot\cup Nx_i \dot\cup \ldots$$

Доказать, что все множества

$$x_1Hx_1^{-1}, x_2Hx_2^{-1}, \ldots, x_iHx_i^{-1}, \ldots$$

различны и что всякое множество, сопряженное с H, совпадает с одним из $x_iHx_i^{-1}$ $(i = 1, 2, \dots)$.

1.74. Доказать, что

а) нормализатор $N(a)$ содержит подгруппу $\langle a\rangle$ в качестве нормального делителя;

б) число элементов группы G, сопряженных с a, равно индексу нормализатора $N(a)$ в G.

1.75. Доказать, что

а) нормализатор $N(H)$ подгруппы H в группе G содержит подгруппу H в качестве нормального делителя;

б) число подгрупп группы G, сопряженных с H, равно индексу нормализатора $N(H)$ в G.

1.76. Доказать, что:

а) число элементов группы G, сопряженных с данным элементом, делит порядок группы G;

б) число подгрупп группы G, сопряженных с данной подгруппой, делит порядок группы G.

1.77. Пусть x — элемент конечной группы G и k — число элементов, сопряженных с x в G; пусть k' — число элементов, сопряженных с x^n в G. Доказать, что k' — делитель числа k.

1.78. Пусть H — подгруппа индекса 2 в группе G, K — класс сопряженных в G элементов и $K \subset H$. Доказать, что K является либо классом сопряженных в H элементов, либо объединением двух классов сопряженных в H элементов, состоящих из одинакового числа элементов.

1.79. Найти число перестановок симметрической группы S_n, сопряженных с данной перестановкой σ.

1.80*. Конечная группа G имеет порядок p^n, где p — простое число. Доказать, что G имеет нетривиальный центр (содержащий более одного элемента).

1.81*. Доказать, что любой нормальный делитель A знакопеременной группы A_n степени $n \geqslant 5$, содержащий хотя бы один тройной цикл, совпадает с A_n.

1.82*. а) Найти все классы сопряженных элементов группы икосаэдра;

б) доказать, что группа икосаэдра является простой (т. е. не имеет нормальных делителей, отличных от самой группы и единичной подгруппы).

1.83*. Доказать, что знакопеременная группа пятой степени является простой.

1.84. Доказать, что факторгруппа симметрической группы S_n по знакопеременной группе A_n изоморфна факторгруппе аддитивной группы целых чисел по подгруппе четных чисел.

1.85. Построить факторгруппу

а) аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу d;

б) аддитивной группы целых чисел, кратных 3, по подгруппе чисел, кратных 15;

в) аддитивной группы целых чисел, кратных 4, по подгруппе чисел, кратных 24;

г) мультипликативной группы действительных чисел, отличных от нуля, по подгруппе положительных чисел;

д) аддитивной группы комплексных чисел по подгруппе целых гауссовых чисел;

е) аддитивной группы векторов плоскости (выходящих из начала координат) по подгруппе векторов, лежащих на оси Ox;

ж) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе действительных чисел.

1.86. Пусть G_n — аддитивная группа векторов n-мерного линейного пространства и H_k — подгруппа векторов k-мерного подпространства, $0 \leqslant k \leqslant n$. Доказать, что факторгруппа G_n/H_k изоморфна G_{n-k}.

1.87. Пусть G — мультипликативная группа всех комплексных чисел, отличных от 0, и H — множество всех чисел из G, лежащих на действительной и мнимой осях.

а) Доказать, что H — подгруппа группы G.

б) Найти смежные классы группы G по подгруппе H.

в) Доказать, что факторгруппа G/H изоморфна мультипликативной группе U всех комплексных чисел, равных по модулю 1.

1.88*. Пусть

G — мультипликативная группа комплексных чисел, отличных от 0,

H — множество чисел из G, лежащих на n лучах, выходящих из 0 под равными углами, причем один из этих лучей совпадает с положительной действительной полуосью.

K — аддитивная группа всех действительных чисел,

Z — аддитивная группа целых чисел,
D — мультипликативная группа положительных чисел,
U — мультипликативная группа комплексных чисел, равных по модулю 1,
U_n — мультипликативная группа корней n-й степени из 1.
Доказать, что

а) $K/Z \cong U$; б) $G/D \cong U$; в) $G/U \cong D$;
г) $U/U_n \cong U$; д) $G/U_n \cong G$; е) $H < G$ и $G/H \cong U$;
ж) $H/D \cong U_n$; з) $H/U_n \cong D$.

1.89. Для мультипликативных групп невырожденных квадратных матриц порядка n доказать утверждения:

а) факторгруппа группы действительных матриц по подгруппе матриц с определителем, равным 1, изоморфна мультипликативной группе действительных чисел, отличных от 0;

б) факторгруппа группы действительных матриц по подгруппе матриц с определителем, равным ± 1, изоморфна мультипликативной группе положительных чисел;

в) факторгруппа группы действительных матриц по подгруппе матриц с положительными определителями является циклической группой второго порядка;

г) факторгруппа группы комплексных матриц по подгруппе матриц с определителями, по модулю равными 1, изоморфна мультипликативной группе положительных чисел;

д) факторгруппа группы комплексных матриц по подгруппе матриц с положительными определителями изоморфна мультипликативной группе комплексных чисел, по модулю равных 1.

1.90. Доказать, что в факторгруппе $\mathbb{Q}/\mathbb{Z}$ ($\mathbb{Q}$ — аддитивная группа рациональных чисел, $\mathbb{Z}$ — аддитивная группа целых чисел):

а) каждый элемент имеет конечный порядок;

б) для каждого натурального n имеется в точности одна подгруппа порядка n.

1.91. Доказать, что

а) симметрическая группа S_3 имеет шесть внутренних автоморфизмов и ни одного внешнего, причем группа автоморфизмов изоморфна S_3;

б) четверная группа V (задача 1.11) имеет один внутренний автоморфизм (тождественный) и пять внешних, причем группа автоморфизмов изоморфна S_3.

1.92. Доказать, что для любой группы G множество всех внутренних автоморфизмов является нормальной подгруппой в группе всех автоморфизмов группы G.

1.93*. Существуют ли у S_6 внешние автоморфизмы?

1.94. Доказать, что группа внутренних автоморфизмов группы G изоморфна факторгруппе группы G по ее центру.

1.95. Доказать, что группа всех автоморфизмов некоммутативной группы не может быть циклической.

1.96. Доказать, что факторгруппа некоммутативной группы по ее центру (пример 1.18 на с. 25) не может быть циклической.

1.97*. Доказать, что если порядок конечной группы G делится на простое число p, то G содержит элемент порядка p (теорема Коши).

1.98*. Пусть p — простое число. Группа G называется p-группой, если порядки всех ее элементов конечны и равны некоторым степеням числа p. Доказать, что конечная группа G тогда и только тогда будет p-группой, когда ее порядок равен степени числа p.

1.99. Доказать, что группа порядка p^2, где p — простое число, коммутативна.

1.100. Найти число классов сопряженности и число элементов в каждом классе для некоммутативной группы порядка p^3, где p — простое число.

1.101. Доказать, что:

а) аддитивная группа векторов n-мерного линейного пространства есть прямая сумма n подгрупп векторов одномерных подпространств, натянутых на векторы любого базиса пространства;

б) аддитивная группа комплексных чисел есть прямая сумма подгрупп действительных и чисто мнимых чисел;

в) мультипликативная группа действительных чисел есть прямое произведение подгруппы положительных чисел и подгруппы чисел ± 1;

г) мультипликативная группа комплексных чисел есть прямое произведение подгрупп положительных чисел и чисел, по

модулю равных единице.

1.102. Доказать, что если $G = A + B_1 = A + B_2$ — прямые разложения абелевой группы G и $B_1 \subseteq B_2$, то $B_1 = B_2$.

1.103. Доказать, что прямое разложение $G = H + K$ абелевой группы G существует тогда и только тогда, когда существует гомоморфное отображение G на подгруппу H, сохраняющее на месте все элементы из H.

1.104. Доказать, что если $G = A + B$ — прямое разложение группы G, то факторгруппа G/A изоморфна B.

1.105. Пусть $G = A_1 + A_2 + \cdots + A_s$ разложение абелевой группы G в прямую сумму подгрупп и $x = a_1 + a_2 + \cdots + a_s$, $a_k \in A_k$, $k = 1, 2, \ldots, s$, — соответствующее разложение элемента x в сумму компонент. Доказать, что:

а) группа G тогда и только тогда имеет конечный порядок n, когда каждая подгруппа A_k имеет конечный порядок n_k, $k = 1, 2, \ldots, s$, причем $n = n_1 n_2 \ldots n_s$.

б) элемент тогда и только тогда имеет конечный порядок p, когда каждая его компонента a_k имеет конечный порядок p_k, $k = 1, 2, \ldots, s$, причем p равно наименьшему общему кратному чисел p_1, p_2, $\ldots$, p_s.

в) группа G тогда и только тогда является конечной циклической, когда все прямые слагаемые A_k — конечные циклические группы, причем их порядки попарно взаимно просты.

1.106. Разложить в прямую сумму примарных компонент циклическую группу порядка: а) 6; б) 12; в) 60; г) 900.

1.107*. Доказать неразложимость в прямую сумму двух ненулевых подгрупп:

а) аддитивной группы целых чисел;

б) аддитивной группы рациональных чисел;

в) циклической группы порядка p^n, p — простое.

1.108*. Пусть G — ненулевая конечная абелева группа (с аддитивной записью операции). Доказать утверждения:

а) если порядки всех элементов из G делят произведение pq взаимно простых чисел p и q, то G разлагается в прямую сумму подгрупп A и B, где порядки всех элементов из A делят p, а из B — делят q, причем одна из подгрупп A или B может оказаться нулевой;

б) для группы G имеет место разложение $G = A_1 + A_2 + \ldots + A_s$ в прямую сумму ненулевых подгрупп, порядок элемен-

тов A_i — степень простого числа p_i, причем все p_i различны: $p_i \neq p_j$ при $i \neq j$;

в) группа A_k, относящаяся к простому числу p_k, состоит из всех элементов группы G, порядки которых равны степеням числа p^k, что однозначно определяет разложение из пункта б).

1.109. Найти все (с точностью до изоморфизма) абелевы группы следующих порядков:

а) 3; б) 4; в) 6; г) 8; д) 9; е) 12; ж) 16; з) 24; и) 30; к) 36; л) 48; м) 60; н) 63; о) 72; п) 100.

1.110*. Разложить в прямую сумму примарных циклических и бесконечных циклических подгрупп факторгруппу $\mathbb{Z}^3/H$, где x_1, x_2, x_3 — порождающие $\mathbb{Z}^3$, а порождающие H заданы соотношениями

а) $\begin{cases} y_1 = 7x_1 + 2x_2 + 3x_3, \\ y_2 = 21x_1 + 8x_2 + 9x_3, \\ y_3 = 5x_1 - 4x_2 + 3x_3, \end{cases}$ б) $\begin{cases} y_1 = 4x_1 + 5x_2 + 3x_3, \\ y_2 = 5x_1 + 6x_2 + 5x_3, \\ y_3 = 8x_1 + 7x_2 + 9x_3, \end{cases}$

в) $\begin{cases} y_1 = 5x_1 + 5x_2 + 2x_3, \\ y_2 = 11x_1 + 8x_2 + 5x_3, \\ y_3 = 17x_1 + 5x_2 + 8x_3, \end{cases}$ г) $\begin{cases} y_1 = 6x_1 + 5x_2 + 7x_3, \\ y_2 = 8x_1 + 7x_2 + 11x_3, \\ y_3 = 6x_1 + 5x_2 + 11x_3, \end{cases}$

д) $\begin{cases} y_1 = 4x_1 + 5x_2 + x_3, \\ y_2 = 8x_1 + 9x_2 + x_3, \\ y_3 = 4x_1 + 6x_2 + 2x_3, \end{cases}$ е) $\begin{cases} y_1 = 2x_1 + 6x_2 - 2x_3, \\ y_2 = 2x_1 + 8x_2 - 4x_3, \\ y_3 = 4x_1 + 12x_2 + 4x_3, \end{cases}$

ж) $\begin{cases} y_1 = 6x_1 + 5x_2 + 4x_3, \\ y_2 = 7x_1 + 6x_2 + 9x_3, \\ y_3 = 5x_1 + 4x_2 - 4x_3, \end{cases}$ з) $\begin{cases} y_1 = 1x_1 + 2x_2 + 3x_3, \\ y_2 = 2x_1, \\ y_3 = 3x_1, \end{cases}$

и) $\begin{cases} y_1 = 4x_1 + 7x_2 + 3x_3, \\ y_2 = 2x_1 + 3x_2 + 2x_3, \\ y_3 = 6x_1 + 10x_2 + 5x_3, \end{cases}$ к) $\begin{cases} y_1 = 2x_1 + 3x_2 + 4x_3, \\ y_2 = 5x_1 + 5x_2 + 6x_3, \\ y_3 = 2x_1 + 6x_2 + 9x_3. \end{cases}$

1.111. Доказать, что является циклической конечная абелева группа G, порядок которой равен:

а) произведению двух различных простых чисел p и q;

б) произведению различных простых чисел $p_1, p_2, \ldots, p_s$;

в) найти все подгруппы абелевой группы G, порядок которой удовлетворяет условию пункта б), и найти число этих

подгрупп;

г) доказать, что для любого делителя k порядка n конечной абелевой группы G существуют подгруппа и факторгруппа группы G, имеющие порядок k.

1.112. Пусть G — ненулевая конечная абелева группа, все ненулевые элементы которой имеют один и тот же порядок p (элементарная группа). Доказать утверждения:

а) число p является простым;

б) группа G разлагается в прямую сумму конечного числа циклических подгрупп порядка p и имеет порядок p^k, где k — число этих слагаемых;

в) любая ненулевая подгруппа H группы G сама будет элементарной и является прямым слагаемым в некотором прямом разложении $G = H + K$ группы G;

г) число подгрупп порядка p^s элементарной группы G порядка p^k, $k \geqslant s > 0$, равно

$$\frac{(p^k-1)(p^k-p)(p^k-p^2)\dots(p^k-p^{s-1})}{(p^s-1)(p^s-p)(p^s-p^2)\dots(p^s-p^{s-1})}.$$

1.113. Доказать, что конечная абелева группа G порождается ее элементами максимального порядка.

Глава 2

Кольца

Перейдем теперь к рассмотрению более сложной алгебры — алгебры с двумя операциями. Операции будем всегда обозначать как сложение и умножение, хотя к обычным сложению и умножению они могут не иметь никакого отношения.

2.1. Определение кольца и простейшие свойства

Кольцо — это множество R с двумя бинарными операциями сложения $+$ и умножения $\cdot$ такими, что

R1: относительно сложения R — коммутативная группа (которая называется *аддитивной группой кольца*);

R2: умножение ассоциативно;

R3: $a\cdot(b+c) = a\cdot b+a\cdot c$; $(b+c)\cdot a = b\cdot a+c\cdot a$ (*дистрибутивность* умножения относительно сложения слева и справа).

Если в кольце имеется единичный элемент для умножения, то кольцо называется *кольцом с единицей*. Мы будем обозначать единицу через 1, несмотря на двусмысленность такого обозначения. Если умножение коммутативно, то такое кольцо называется *коммутативным кольцом*.

Замечание 2.1. В литературе встречается другое определение кольца, в котором опущена аксиома ассоциативности R2.

В таких книгах кольца с ассоциативным умножением называются ассоциативными. Нам удобнее использовать более узкое понятие кольца.

Замечание 2.2. Когда рассматриваются кольца с единицей, почти всегда исключается вырожденный случай $0 = 1$. Далее всегда предполагается, что в кольцах с единицей $0 \neq 1$.

Обратного элемента по второй операции (умножению) в кольце может и не быть. Поэтому уравнение $ax = b$ может не иметь решений в кольце.

Классический пример кольца — это множество целых чисел с операциями сложения и умножения. Обозначается кольцо целых чисел через $\mathbb{Z}$. Обратного элемента по умножению нет для всех целых чисел, за исключением ± 1. Другой важный пример кольца — кольцо многочленов — подробно рассматривается ниже (раздел 2.2).

Из аксиом кольца следует довольно много тривиальных следствий. Приведем здесь только самые необходимые, и будем вводить остальные по мере надобности.

Утверждение 2.3. *В любом кольце* $a(b - c) = ab - ac$.

Это утверждение означает, что дистрибутивность выполняется и для вычитания (сложения с противоположным, т. е. обратным относительно сложения).

Доказательство. $a(b - c) + ac = a(b - c + c) = ab$. □

Конечно, выполняется также и равенство $(b-c)a = ba-ca$.

Утверждение 2.4. *В любом кольце* $a \cdot 0 = 0$.

Доказательство. $a \cdot 0 = a(b - b) = ab - ab = 0$. □

Выполняется также и аналогичное равенство при умножении на 0 слева: $0 \cdot a = 0$.

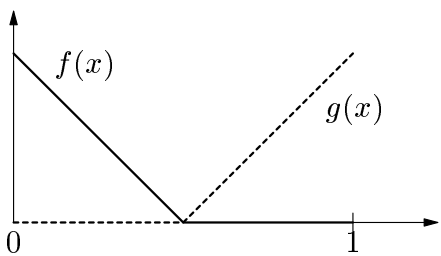
Для чисел и многочленов выполняется такое свойство: если произведение двух элементов равно нулю, то хотя бы один элемент равен нулю. В общем случае это свойство может не выполняться. Давайте рассмотрим некоторые примеры.

Пример 2.5. Множество целых чисел с операциями сложения и умножения по модулю 4. Более точно, мы рассматриваем

операции на множестве вычетов по модулю 4, т. е. не различаем числа, разность которых делится на 4. Относительно этих операций множество из четырех различных вычетов по модулю 4, т. е. $\{0, 1, 2, 3\}$, образует кольцо. И в этом кольце произведение двух не равных нулю элементов может быть нулевым: $2 \cdot 2 = 0$.

Пример 2.6. Прямым обобщением предыдущего примера является *кольцо вычетов по модулю* n, где n — натуральное число. Элементами этого кольца, которое мы будем обозначать $\mathbb{Z}_n$, являются числа $0, 1, \ldots, n-1$. Сложение и умножение в этом кольце определяются как сложение и умножение по модулю n. Аналогично предыдущему примеру можно заметить, что если число $n = ab$ — составное, то $ab = 0$ в $\mathbb{Z}_n$. Оказывается, что если n — простое, то произведение ненулевых элементов в $\mathbb{Z}_n$ обязательно отлично от 0. Доказательство этого утверждения будет приведено ниже (см. раздел 2.7).

Пример 2.7. Есть еще один важный пример — кольцо непрерывных функций на отрезке $[0, 1]$ с обычными операциями поточечного сложения и умножения функций: $(f + g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x)g(x)$. Нулем этого кольца является функция, тождественно равная нулю. Рассмотрим две ненулевых функции f, g, графики которых изображены на рисунке. Очевидно, что произведение этих функций тождественно равно нулю.



Пример 2.8. По двум кольцам R_1, R_2 можно определить их *прямую сумму* $R_1 \oplus R_2$ аналогично прямому произведению групп, которое было определено в примере 1.35 и прямой сумме абелевых групп, которая была определена в разделе 1.12.

Кольцо $R_1 \oplus R_2$ состоит из всевозможных пар (r_1, r_2), где $r_1 \in R_1$, $r_2 \in R_2$. Операции определяются так:

$$(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2'),$$
$$(r_1, r_2) \cdot (r_1', r_2') = (r_1 \cdot r_1', r_2 \cdot r_2')$$

(для простоты обозначений мы используем одни и те же символы для операций в обоих кольцах).

Проверка аксиом кольца для прямой суммы колец выполняется механически. По сложению это группа, которая есть прямое произведение аддитивных групп колец R_1 и R_2. Ассоциативность умножения и дистрибутивность проверяются покомпонентно.

В прямой сумме колец несложно построить пару ненулевых элементов, произведение которых равно нулю. Используем утверждение 2.4:

$$(a, 0) \cdot (0, b) = (a \cdot 0, 0 \cdot b) = (0, 0).$$

Ненулевые элементы кольца, произведение которых равно нулю, имеют специальное название — *делители нуля*. Технически бывает удобно различать левые и правые делители нуля. Элемент $a \in R$ называется правым (левым) делителем нуля, если для некоторого $b \in R$ выполняется $ba = 0$ ($ab = 0$).

Наличие делителей нуля в кольцах является крайне неприятным эффектом. Поэтому выделяется класс колец без делителей нуля. Коммутативные кольца без делителей нуля называются *целостными кольцами* (или областями целостности). Как правило, мы будем рассматривать целостные кольца, поскольку они дают важные для приложений примеры.

2.2. Кольцо многочленов

Возьмем какой-нибудь коммутативное кольцо R с единицей (например, целые, рациональные, действительные, комплексные числа и т. д.). Построим кольцо многочленов $R[x]$ с коэффициентами из R (иногда говорят об алгебре многочленов над R). *Многочлен* — это формальное выражение

$$A = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d, \quad a_i \in R, a_d \neq 0. \qquad (2.1)$$

Число d называется *степенью* многочлена (2.1) и обозначается $\deg A$. Есть еще один исключительный многочлен — 0. Его нельзя представить в виде (2.1). Степень нулевого многочлена обычно полагают неопределенной, но часто ее можно считать равной $-\infty$.

Что такое x^k в формуле (2.1)? Это, конечно, просто переменная x, возведенная в некоторую степень. Но ничего об этой переменной нам знать не нужно, она используется в записи исключительно для наглядности. Правильнее даже считать, что многочлен — это финитная последовательность элементов кольца R (последовательность коэффициентов):

$$a_0, a_1, \ldots, a_n, \ldots$$

Здесь слово «*финитная*» означает, что все элементы последовательности, начиная с некоторого места, равны 0. (Если этого не требовать, то мы получим другое интересное кольцо — кольцо степенных рядов, которое играет важную роль в комбинаторике под названием производящих функций.) Заметьте, что нуль включается в такое описание на общих основаниях.

Сложение многочленов определяется формулой

$$\begin{aligned}(a_0 + a_1x + \cdots + a_dx^d) + (b_0 + b_1x + \cdots + b_dx^d) = \\ = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_d + b_d)x^d \quad (2.2)\end{aligned}$$

(если степени разные, к многочлену меньшей степени нужно добавить слагаемые с нулевыми коэффициентами), а умножение — формулой

$$\begin{aligned}(a_0 + a_1x + \cdots + a_dx^d)(b_0 + b_1x + \cdots + b_kx^k) = \\ = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots = \sum_{i=0}^{d+k} x^i \sum_{j=0}^{i} a_jb_{i-j} \quad (2.3)\end{aligned}$$

(в которой отсутствующие коэффициенты также полагаются равными нулю — в полном соответствии со второй интерпретацией многочленов). Эти формулы можно получить, если потребовать коммутативности, ассоциативности и дистрибутивности сложения и умножения многочленов. С левыми частями написанных выражений нужно действовать так, как учили в 7-м классе: раскрыть скобки и привести подобные.

Итак, $R[x]$ — это множество финитных последовательностей элементов R с операциями, задаваемыми формулами (2.2) и (2.3).

Утверждение 2.9. *$R[x]$ является коммутативным кольцом с единицей.*

Доказательство. Из формул (2.2) и (2.3) очевидно, что $0 = (0, \dots)$ и $1 = (1, 0, \dots)$ будут соответственно нулем и единицей в $R[x]$.

Из определения сложения (коэффициенты складываются по отдельности при разных степенях) видно, что коммутативность и ассоциативность сложения следуют из коммутативности и ассоциативности сложения в R. Противоположный многочлен (обратный относительно сложения) получается переменой знаков у всех коэффициентов. Поэтому по сложению многочлены образуют группу.

Коммутативность умножения очевидна из симметрии формулы (2.3), которой определяется умножение.

Дистрибутивность также легко проверяется по формуле для умножения: подставим в формулу вместо b_j выражение $c_j + d_j$ и затем воспользуемся дистрибутивностью в кольце R, получим:

$$\sum_{j=0}^{i} a_j b_{i-j} = \sum_{j=0}^{i} a_j (c_{i-j} + d_{i-j}) = \sum_{j=0}^{i} a_j c_{i-j} + \sum_{j=0}^{i} a_j d_{i-j}.$$

Это и есть дистрибутивность.

Проверим ассоциативность умножения многочленов непосредственным вычислением:

$$A(BC) = \sum_{i=0} a_i x^i \left(\sum_j \Big(\sum_{k+s=j} b_k c_s \Big) x^j \right) =$$

$$= \sum_{i=0} \left(\sum_{r+j=i} a_r \Big(\sum_{k+s=j} b_k c_s \Big) \right) x^i = \sum_{i=0} \left(\sum_{r+k+s=i} a_r b_k c_s \right) x^i =$$

$$= \sum_{i=0} \left(\Big(\sum_{r+k=j} a_r b_k \Big) \sum_{j+s=i} c_s \right) x^i = \left(\sum_j \Big(\sum_{r+k=j} a_r b_k \Big) x^j \sum_s c_s x^s \right) =$$

$$= (AB)C. \quad (2.4)$$

Если вы внимательно посмотрите на эту выкладку, то поймете, что ассоциативность умножения многочленов следует из ассоциативности сложения натуральных чисел. Заметьте также, что верхние индексы в этой выкладке не указывались. Они в ней не играют никакой роли — на самом деле мы проверили ассоциативность в более широком кольце степенных рядов. □

Может показаться непонятным, зачем нужны такие сложные выкладки в этом доказательстве. Если смотреть на многочлен, как на функцию из R в R, задаваемую формулой (2.1), то свойства кольца, включая ассоциативность, очевидны.

Но такое понимание многочленов будет для нас слишком ограничительным. Возьмем, скажем, кольцо из двух элементов $F = \{0, 1\}$ со сложением и умножением по модулю 2. Функции $x \mapsto x$ и $x \mapsto x^2$ в этом кольце совпадают. А многочлены x и x^2 над этим кольцом различны по определению, данному выше (одному соответствует последовательность коэффициентов $(0, 1, 0, \dots)$, а другому — $(0, 0, 1, 0, \dots)$).

Однако для целых, рациональных, действительных или комплексных чисел определение многочленов как функций, задаваемых формулой (2.1), равносильно данному выше определению. Ниже мы обсудим этот вопрос подробнее (см. пример 3.21 из раздела 3.4).

А пока рассмотрим простые алгебраические свойства колец многочленов.

Утверждение 2.10. *Если в R нет делителей нуля, то для $f, g \neq 0$ выполнено* $\deg(fg) = \deg f + \deg g$.

Доказательство: коэффициент при старшей степени произведения равен произведению коэффициентов при старших степенях сомножителей. Исключительный случай 0 покрывается той же формулой, если полагать степень 0 равной $-\infty$.

Следствие 2.11. *Если в R нет делителей нуля, то и в $R[x]$ нет делителей нуля.*

Используя формулу для степени произведения многочленов, можно найти и *делители единицы* в кольце многочленов, как еще называют *обратимые элементы* относительно умножения.

Следствие 2.12. *Обратимые элементы в кольце многочленов $R[x]$ над целостным кольцом R — это константы (многочлены степени 0), обратимые в кольце R.*

2.3. Изоморфизмы и гомоморфизмы колец

Эти операции вводятся по аналогии с группами. Теперь требуется сохранение обеих операций. Если есть кольцо R с операциями $+$, $\cdot$ и кольцо R' с операциями $\oplus$, $\otimes$, то *гомоморфизмом* называется отображение $\varphi\colon R \to R'$, сохраняющее обе операции:

$$\varphi(r_1 + r_2) = \varphi(r_1) \oplus \varphi(r_2),$$
$$\varphi(r_1 \cdot r_2) = \varphi(r_1) \otimes \varphi(r_2).$$

Изоморфизм колец — это взаимно однозначный гомоморфизм. Так же, как и в случае групп, изоморфные кольца «одинаковы» с алгебраической точки зрения.

Совершенно без изменений доказывается теорема о том, что гомоморфная область кольца есть кольцо. По первой операции всё повторяется дословно, ассоциативность умножения проверяется так же, как и ассоциативность сложения. Проверка дистрибутивности осуществляется прямым вычислением:

$$\begin{aligned}\varphi(a) \otimes (\varphi(b) \oplus \varphi(c)) &= \varphi(a) \otimes \varphi(b + c) = \\ &= \varphi(a \cdot (b + c)) = \varphi(a \cdot b + a \cdot c) = \varphi(a \cdot b) \oplus \varphi(a \cdot c) = \\ &= \varphi(a) \otimes \varphi(b) \oplus \varphi(a) \otimes \varphi(c).\end{aligned}$$

2.4. Идеалы

Группы можно факторизовать («делить») по нормальным подгруппам. Аналогичное действие в случае колец основано на понятии идеала.

Что такое *идеал*? Это подмножество кольца, которое по сложению является коммутативной подгруппой. Кроме того, идеал удовлетворяет очень сильному условию по умножению.

Если использовать образы из физики, то идеал — это подмножество «с очень сильным потенциалом». Если взять произвольный элемент i, принадлежащий идеалу I, и умножить его на любой элемент кольца $r \in R$, то произведение также должно принадлежать идеалу: $r \cdot i \in I$ (свойство «втягивания»).

В частности, идеал I является кольцом относительно тех же операций, что и исходное кольцо R. Это пример *подкольца*, т. е. такого подмножества кольца, которое является подгруппой по сложению и замкнуто относительно операции умножения.

Умножение в кольце не обязательно коммутативно. Поэтому, как и в случае смежных классов по подгруппе, нужны два технических понятия: если умножение берется слева, то это левый идеал, а если справа, то — правый. Если выполняются оба условия (как всегда будет в коммутативном случае), говорят о двустороннем идеале или просто идеале.

Технически более удобно слегка иное определение идеала. При изучении теории групп была доказана простая теорема о том, что подмножество группы является подгруппой тогда и только тогда, когда вместе с элементами a и b содержит элемент ab^{-1}. Поэтому вместо условия, что I — подгруппа, можно использовать условие $a-b \in I$ (так представляется ab^{-1} в аддитивной записи). Итак, подмножество $I \in R$ называется *левым идеалом*, если выполняются два следующих условия:

1) если $a, b \in I$, то $a - b \in I$;

2) если $a \in I$, $r \in R$, то $ra \in I$.

Аналогично определяются правые и двусторонние идеалы.

Оказывается, что идеалы в теории колец и в дальнейших теориях играют первостепенную роль. Для начала посмотрим на примеры идеалов.

Пример 2.13. Возьмем кольцо целых чисел $\mathbb{Z}$. Выберем в нем фиксированный элемент n, и рассмотрим все его кратные, т. е. множество $n\mathbb{Z} = \{rn \mid r \in \mathbb{Z}\}$. Это множество — идеал, что легко проверить из определения.

Нетрудно также убедиться, что любой идеал в $\mathbb{Z}$ имеет вид $n\mathbb{Z}$. Действительно, пусть $I \subseteq \mathbb{Z}$ — идеал. Если $I = \{0\}$, то $I = 0\mathbb{Z}$. В противном случае I содержит положительные числа (так как идеал — подгруппа аддитивной группы $\mathbb{Z}$). Пусть n —

наименьшее положительное число, принадлежащее I. Докажем, что $I = n\mathbb{Z}$. В силу определения идеала $I \supseteq n\mathbb{Z}$. С другой стороны, если a принадлежит идеалу I то остаток r от деления a на n принадлежит I, так как $r = a - qn$. Но тогда, если a не принадлежит идеалу $n\mathbb{Z}$, то $r \neq 0$ и $r < n$, что противоречит выбору n.

Это простое рассуждение будет обобщено ниже (см. теорему 2.27).

Пример 2.14. То же самое можно сделать и с многочленами: зафиксировать какой-нибудь многочлен $\varphi(x)$ и умножить его на всевозможные многочлены. Получим идеал $\varphi(x)R[x] = \{\psi(x)\varphi(x) \mid \psi(x) \in R[x]\}$.

Приведенные примеры легко обобщить. По элементу $a \in R$ коммутативного кольца R можно построить множество

$$(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\},$$

которое, как легко проверить, является идеалом. Этот идеал называется *главным идеалом, порожденным элементом* a. Если в кольце есть единица, то главный идеал можно записать в таком же виде, как в предыдущих примерах:

$$(a) = \{ra \mid r \in R\}.$$

Главные идеалы можно определить иначе. Заметим, что пересечение идеалов также идеал. Поэтому для любого подмножества S кольца R можно определить наименьший идеал, содержащий S, как пересечение всех идеалов, содержащих S. Этот идеал называется *идеалом, порожденным множеством* S (обозначается (S)). В общем случае главным идеалом, порожденным элементом a, можно назвать идеал, порожденный множеством $\{a\}$.

Кольца, в которых все идеалы, отличные от самого кольца, — главные, называются *кольцами главных идеалов*. Примеры колец главных идеалов, обобщающие кольцо целых чисел, приводятся ниже в разделе 2.7.

Поскольку идеалы в теории колец играют роль, аналогичную роли нормальных подгрупп в теории групп, естественно проверить справедливость следующего утверждения.

Утверждение 2.15. *Ядро любого гомоморфизма колец является двусторонним идеалом.*

Доказательство. Пусть $\varphi\colon R_1 \to R_2$ — гомоморфизм колец, $I = \operatorname{Ker}\varphi = \{x \mid \varphi(x) = 0\}$ — ядро этого гомоморфизма. Поскольку гомоморфизм колец является и гомоморфизмом их аддитивных групп, то I — подгруппа по сложению. Осталось проверить, что для любого $r \in R_1$ и $a \in I$ выполнено $ra \in I$, $ar \in I$. Из свойств гомоморфизма следует, что $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0$. Аналогично $\varphi(ar) = 0$. □

2.5. Кольца классов вычетов

Так же, как мы раскладывали группу на смежные классы по нормальной подгруппе, мы будем раскладывать кольцо по идеалам. Возьмем какой-нибудь элемент кольца r и рассмотрим суммы этого элемента со всеми элементами идеала. Получим, конечно, смежный класс по идеалу как аддитивной подгруппе кольца. Но теория колец очень долго развивалась совершенно независимо от теории групп, поэтому в ней возникла своя терминология. В данном случае смежные классы называются *классами вычетов по модулю идеала* I, или, более кратко, классами вычетов по I. Поскольку по сложению кольцо — группа, то для классов вычетов выполняются все теоремы о смежных классах.

Пример 2.16. Рассмотрим кольцо целых чисел и вычеты по идеалу $n\mathbb{Z}$, описанному в примере 2.13. Получим такие множества:

$$\begin{aligned} 0 + n\mathbb{Z} &= \{rn \mid r \in \mathbb{Z}\} = \bar{0}, \\ 1 + n\mathbb{Z} &= \{1 + rn \mid r \in \mathbb{Z}\} = \bar{1}, \\ &\dots \\ (n-1) + n\mathbb{Z} &= \{n - 1 + rn \mid r \in \mathbb{Z}\} = \overline{n-1}. \end{aligned}$$

Следующий шаг состоит в том, чтобы доказать, что совокупность классов вычетов снова образует кольцо. Это верно, если идеал — двусторонний. (Аналогично тому, как классы смежности по подгруппе образуют группу лишь в том случае, когда левые смежные классы совпадают с правыми).

Операции над классами вычетов определяются аналогично операциям над смежными классами. Однако из-за наличия двух операций возникают некоторые тонкости.

Докажем несколько простых соотношений. (Предполагаем ниже, что рассматриваются двусторонние идеалы, хотя часть утверждений верна и для односторонних идеалов.)

Пусть у нас есть два элемента, которые принадлежат одному классу вычетов по модулю двустороннего идеала I. Это означает, что $a = r + i_1$, $b = r + i_2$, $i_1, i_2 \in I$. Такие элементы называются *сравнимыми*, отношение сравнимости обозначается $a \equiv b \pmod I$ (иногда для краткости I не пишут), читается «a сравнимо с b по модулю идеала I».

Непосредственно из определения следует

Утверждение 2.17. *$a \equiv b \pmod I$ равносильно $a - b \in I$.*

Доказательство. Предположим, что $a = r + i_1$, $b = r + i_2$. Тогда $a - b = i_1 - i_2 \in I$. И наоборот: если $a - b = i \in I$, то $a = b + i \in b + I$, значит, $a \equiv b$. □

Из этого простого утверждения следует весьма полезный вывод: сравнение по модулю идеала в большой степени похоже на обычное равенство.

Утверждение 2.18. *Если $a_1 \equiv a_2$, $b_1 \equiv b_2$, то $a_1 + b_1 \equiv a_2 + b_2$ и $a_1 b_1 \equiv a_2 b_2$.*

Доказательство. Разность двух элементов, принадлежащих идеалу, принадлежит идеалу; произведение элемента идеала на любой другой элемент принадлежит идеалу. Поэтому

1) Пусть $a_1 - a_2 \in I$, $b_1 - b_2 \in I$, тогда $(a_1 + b_1) - (a_2 + b_2) \in I$, т. е. $a_1 + b_1 \equiv a_2 + b_2$.

2) $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2) b_2 \in I$ (здесь использовано, что идеал — двусторонний). □

Теперь определим сумму и произведение классов вычетов $\bar r_1 = r_1 + I$, $\bar r_2 = r_2 + I$:

$$\bar r_1 + \bar r_2 = \overline{r_1 + r_2} = r_1 + r_2 + I, \tag{2.5}$$

$$\bar r_1 \cdot \bar r_2 = \overline{r_1 r_2} = r_1 r_2 + I. \tag{2.6}$$

Нужно доказать корректность введенных операций, т. е. независимость результата операции от выбора представителя класса вычетов. Это немедленно следует из утверждения 2.18.

Действительно, если

$$r_1 + I = \bar{r}_1 = r'_1 + I,$$
$$r_2 + I = \bar{r}_2 = r'_2 + I,$$

то $r_1 \equiv r'_1$, $r_2 \equiv r'_2$, и по утверждению 2.18 получаем $r_1 + r_2 \equiv r'_1 + r'_2$, $r_1 r_2 \equiv r'_1 r'_2$. Это и значит, что сумма и произведение представителей классов вычетов принадлежат одному и тому же классу вычетов, который не зависит от выбора представителей. Поэтому результаты операций, определенных (2.5), (2.6), не зависят от выбора представителей классов вычетов.

Утверждение 2.19. *Совокупность классов вычетов с операциями, определенными равенствами* (2.5), (2.6), *образует кольцо.*

Это кольцо и называется *кольцом классов вычетов* (обозначение R/I).

Доказательство. Для доказательства мы построим гомоморфизм исходного кольца на совокупность классов вычетов и воспользуемся доказанным ранее утверждением, что образ кольца при гомоморфизме является кольцом.

Возьмем исходное кольцо R и разложим его по идеалу I, получим множество классов вычетов R/I. Строим отображение $\varphi\colon R \to R/I$ следующим образом $\varphi\colon r \mapsto \bar{r} = r + I$. Проверим, что это — гомоморфизм:

$$\varphi(r_1 + r_2) = r_1 + r_2 + I = \overline{r_1 + r_2} = \overline{r_1} + \overline{r_2} = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = r_1 r_2 + I = \overline{r_1 r_2} = \overline{r_1} \cdot \overline{r_2} = \varphi(r_1)\varphi(r_2),$$

т. е. операции сохраняются. Сюръективность очевидна: класс вычетов $r + I$ является образом элемента r. □

Теорема 2.20 (теорема о гомоморфизме колец). *Пусть* $\varphi\colon R_1 \to R_2$ *— гомоморфизм колец. Тогда кольцо классов вычетов по модулю ядра гомоморфизма изоморфно гомоморфному образу кольца*: $R_1/\operatorname{Ker}\varphi \cong \varphi(R_1)$.

Доказательство. Изоморфизм устанавливается естественным образом:

$$\alpha\colon \{r\} \mapsto \varphi(r). \tag{2.7}$$

Здесь $r \in R_1$, $\{r\}$ — класс вычетов по модулю $I = \operatorname{Ker}\varphi$.

Отображение (2.7) определено корректно, так как если $r_1 \equiv r_2 \pmod I$, то $\varphi(r_1 - r_2) = 0$, т. е. $\varphi(r_1) = \varphi(r_2)$. Очевидно, что α сюръективно (оно переводит в $\varphi(r)$ класс вычетов $\{r\}$). Проверим свойства гомоморфизма:

$$\alpha(\{r_1\} + \{r_2\}) = \alpha(\{r_1 + r_2\}) = \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = \\ = \alpha(\{r_1\}) + \alpha(\{r_2\}),$$

$$\alpha(\{r_1\} \cdot \{r_2\}) = \alpha(\{r_1 \cdot r_2\}) = \varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2) = \\ = \alpha(\{r_1\}) \cdot \alpha(\{r_2\}).$$

Ядро этого гомоморфизма нулевое, так как $\varphi(r) = 0$ означает $r \in I$, т. е. $\{r\} = 0$. Значит, α — изоморфизм. □

Теперь мы подходим к самому главному для нашего дальнейшего изложения вопросу: можно ли так выбрать идеал, чтобы кольцо классов вычетов было «совсем хорошим»? Например, хотелось бы иметь возможность решать в кольце классов вычетов линейные уравнения. Для этого кольцо классов вычетов должно обладать некоторыми дополнительными свойствами, которые мы укажем в следующем разделе.

2.6. Тела и поля, максимальные идеалы

Введем еще два алгебраических понятия: тело и поле.

Тело — это такое кольцо, ненулевые элементы которого образуют группу относительно умножения, т. е. выполняются дополнительные свойства:

1) существует единичный элемент относительно умножения 1, для любого другого элемента a выполнено $a \cdot 1 = 1 \cdot a = a$;

2) для $a \neq 0$ существует обратный элемент a^{-1}, для которого $a^{-1} \cdot a = a \cdot a^{-1} = 1$.

Отсюда следует разрешимость уравнения $a \cdot x = b$ при $a \neq 0$.

Утверждение 2.21. *В теле нет делителей нуля*: *из* $ab = 0$ *следует* $a = 0$ *или* $b = 0$.

Доказательство. В любом кольце $a \cdot 0 = 0$ (утверждение 2.4). Значит, у 0 нет обратного. Но если $a \neq 0$, $b \neq 0$, то у ab есть обратный $b^{-1}a^{-1}$. □

Поле — это коммутативное тело. Другими словами, ненулевые элементы поля образуют относительно умножения абелеву группу. Более подробное определение поля таково: полем называется множество F с двумя бинарными операциями (сложение и умножение), которые удовлетворяют следующим свойствам:

F1: Относительно сложения F является абелевой группой.

F2: Относительно умножения $F^* = F \setminus \{0\}$ является абелевой группой. (Здесь 0 обозначает нулевой элемент относительно сложения.)

F3: Аксиома дистрибутивности: $a(b + c) = ab + ac$.

Обратите внимание, что аксиомы поля позволяют выполнять арифметические операции аналогично тому, как это делается с числами. И неудивительно: рациональные, действительные и комплексные числа дают самые простые и самые важные примеры полей. Но этими примерами возможные поля далеко не исчерпываются. Один из важных способов построения полей состоит в переходе от коммутативного кольца к кольцу классов вычетов по модулю некоторого идеала.

Как же выбрать идеал так, чтобы кольцо классов вычетов по этому идеалу было полем?

Для этого нам потребуется еще одно понятие — *максимальный идеал*. Идеал I называется максимальным в кольце R, если не существует такого идеала $I' \neq R$, что $I \subset I' \subset R$.

Теорема 2.22. *Кольцо классов вычетов* R/I *коммутативного кольца с единицей есть поле тогда и только тогда, когда* I *— максимальный идеал.*

Доказательство. Коммутативное кольцо является полем тогда и только тогда в нём разрешимы уравнения $ax = b$, $a \neq 0$.

Пусть I — максимальный идеал. Рассмотрим уравнение

$$\bar{a} \cdot \bar{x} = \bar{b}, \quad \bar{a} \neq \bar{0}, \tag{2.8}$$

а $\bar{b}$ — произвольный элемент из кольца R/I, т. е. класс вычетов $b + I$, $b \in R$. Докажем, что такое уравнение разрешимо.

Проверим, что множество $I' = \{(r \cdot a) + i \mid r \in R, i \in I\}$ является идеалом. Для этого достаточно доказать, что разность двух элементов остается в этом множестве и произведения любого элемента этого множества на произвольные элементы кольца остаются в этом множестве:

$$(r_1 \cdot a + i_1) - (r_2 \cdot a + i_2) = (r_1 - r_2) \cdot a + (i_1 - i_2) \in I',$$
$$r \cdot (r' \cdot a + i) = (rr')a + (ri) \in I'.$$

Следующий шаг: $I \subset I'$. Действительно, для элемента $i \in I$ имеем представление в виде $0 \cdot a + i$. Почему это включение строгое? В I' есть элемент $1 \cdot a + 0 = a \notin I$ (условие $\bar{a} \neq \bar{0}$ означает просто-напросто, что $a \notin I$). Следовательно, $I' = R$, т. е. любой элемент кольца, в том числе и b, представим в виде $b = r \cdot a + i$. В некотором смысле мы нашли явное решение уравнения (2.8): $\bar{x} = \bar{r}$. Этим доказана достаточность.

Доказательство необходимости несложно, но это рассуждение часто вызывает некоторое непонимание. Поэтому проведем его максимально подробно. Пусть разрешимы любые уравнения вида (2.8). Нужно доказать, что I — максимальный идеал.

Что означает разрешимость уравнения (2.8)? В точности разрешимость сравнения $ax \equiv b \pmod{I}$, которая равносильна по доказанному выше утверждению 2.17 условию $ax - b \in I$.

Рассмотрим такой идеал I', что $I \subset I'$. Выберем элемент a такой, что $a \in I'$ и $a \notin I$. Поскольку $ax - b \in I \subset I'$ и $a \in I'$, то $ax \in I'$. Поэтому (идеал замкнут относительно вычитания) $b \in I'$. Поскольку b — произвольный элемент кольца R, приходим к выводу, что $I' = R$. □

Эта изящная теорема, легко и просто доказываемая, позволила в свое время осуществить гигантский прорыв, поскольку с ее помощью строится огромное количество объектов, в которых можно решать линейные уравнения.

2.7. Евклидовы кольца

Далее мы будем искать максимальные идеалы в специальных кольцах, которые называются евклидовыми.

По определению, коммутативное кольцо R называется *евклидовым*, если для него выполнены следующие свойства.

E1: Кольцо R — целостное (т. е. в нём нет делителей нуля: из $ab = 0$ следует, что $a = 0$ или $b = 0$).

E2: Для каждого ненулевого элемента кольца определена числовая характеристика — норма, которая принимает целые неотрицательные значения. Т. е. *норма* — это такое отображение $N\colon R \setminus \{0\} \to \mathbb{Z}$, что $N(r) \geqslant 0$.

E3: Возможность деления с остатком означает, что для любых элементов a, b кольца, $b \neq 0$, существуют такие q, r, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$. Элемент r называется остатком от деления a на b. Это основное свойство нормы. Собственно, отсюда и возник термин «евклидово». Дело в том, что в дошедших до нас рукописях термин «деление с остатком» впервые появляется в сочинениях Евклида.

E4: Норма произведения двух ненулевых сомножителей больше либо равна норме любого из сомножителей. Формально: для любых $a, b \in R$, $a \neq 0$, $b \neq 0$ выполнено $N(ab) \geqslant \geqslant \max(N(a), N(b))$.

Утверждение 2.23. *Евклидово кольцо является кольцом с единицей.*

Доказательство. Выберем такой ненулевой элемент e' евклидова кольца R, что $N(e')$ принимает минимально возможное положительное значение (здесь существенно, что значения норм элементов целые неотрицательные, поэтому минимум достигается). Разделим произвольный элемент a на e' с остатком: $a = qe' + r$. По свойству E3 верно одно из двух: либо $N(r) < < N(e')$, либо $r = 0$. Первое невозможно в силу минимальности нормы e'. Значит, $a = qe'$. Итак, все элементы кольца кратны e' (делятся без остатка). В частности, это верно и для самого

e': $e' = ee'$. Но тогда для любого $a \in R$ имеем $ae' = aee'$, т. е. $e'(a - ae) = 0$. Поскольку кольцо R целостное и $e' \neq 0$, получаем $a - ae = 0$. Значит, e является единицей кольца R. $\square$

Рассмотрим два основных примера евклидовых колец.

Пример 2.24. Кольцо $\mathbb{Z}$ целых чисел — евклидово. Норма — это модуль числа. Свойства 1, 4 очевидны. Возможность деления с остатком тоже проверяется без труда: для $a, b \in \mathbb{Z}$, $b > 0$, обозначим $q = \max\{s \mid a \geqslant sb\}$. Заметим, что $qb + b > a$. Поэтому если $a \neq qb$, то для $r = a - qb$ выполнено $r < b$. Для $b < 0$ полагаем $q = \max\{s \mid -a \geqslant s(-b)\}$, свойства остатка проверяются аналогично.

Пример 2.25. Пусть F — некоторое поле. Оказывается, что кольцо многочленов $F[x]$ над полем F — евклидово. Норма — это степень многочлена.

По следствию 2.11 в кольце $F[x]$ нет делителей 0, так как их нет в поле F (см. утверждение 2.21).

По утверждению 2.10 степень произведения двух ненулевых многочленов равна сумме степеней сомножителей, отсюда следует свойство 4 из определения евклидова кольца.

Делить многочлены с остатком можно «в столбик», как учат в школе делить обычные целые числа. Формально возможность деления с остатком можно проверить по индукции. Пусть мы рассматриваем деление с остатком на многочлен $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_d x^d$, $g_d \neq 0$. Для многочленов f степени меньше d имеем представление $f = 0 \cdot g + f$, $\deg f < \deg g$. Это база индукции. Теперь предположим, что мы умеем делить с остатком на g многочлены степени меньше n. Рассмотрим многочлен степени n:

$$f(x) = f_0 + f_1 x + \cdots + f_n x^n, \ f_n \neq 0.$$

Многочлен $\tilde{f} = f - f_n g_d^{-1} x^{n-d} g$ имеет степень, меньшую n, поэтому его можно разделить с остатком на g:

$$\tilde{f} = hg + r, \ \deg r < \deg g.$$

Но тогда

$$f = \tilde{f} + f_n g_d^{-1} x^{n-d} g = (h + f_n g_d^{-1} x^{n-d}) g + r.$$

Значит, f также можно разделить на g с остатком.

Замечание 2.26. В определении деления с остатком мы не требовали единственности неполного частного и остатка. Это требование не нужно для доказательства основных свойств евклидовых колец. Отметим, однако, что для кольца многочленов, как и для кольца целых чисел, неполное частное и остаток определены однозначно.

Действительно, пусть $f = q_1 g + r_1 = q_2 g + r_2$. Тогда $(q_1 - q_2)g + (r_2 - r_1) = 0$. Из этой формулы сразу получаем, что $q_1 = q_2$, так как $\deg r_i < \deg g$. Но тогда и $r_1 = r_2$.

Далее мы рассматриваем только евклидовы кольца.

Теорема 2.27. *Евклидовы кольца — это кольца главных идеалов.*

Обратное, вообще говоря, неверно.

Доказательство. Пусть $I \subset R$ — идеал. Предположим, что элемент $a \in I$ имеет наименьшую норму среди всех ненулевых элементов идеала. Теперь возьмем любой другой элемент идеала b и разделим его на a с остатком: $b = qa + r$, $N(r) < N(a)$. Но $r = b - qa \in I$, поэтому в силу минимальности нормы a получаем, что $r = 0$, т. е. $b = qa$. Таким образом, $I = (a)$. □

Пусть a, b — два элемента (евклидова) кольца R. *Наибольшим общим делителем a и b* называют такой элемент d, что $a = qd$, $b = rd$, и для любого общего делителя d' ($a = q'd'$, $b = r'd'$) выполнено $d = d'd''$ для какого-то $d'' \in R$. Наибольших общих делителей в смысле данного определения может быть много. Скажем, 5 и -5 являются наибольшими общими делителями чисел 10 и 15 в кольце $\mathbb{Z}$.

Пусть d_1 и d_2 — два наибольших общих делителя. Тогда по определению $d_1 = d'd_2 = d'd''d_1$, т. е. $d'd'' = 1$. Мы видим, что наибольшие общие делители отличаются на множитель, для которого в кольце есть обратный. И наоборот, если d — наибольший общий делитель, а ε — *обратимый* элемент (делитель единицы), то εd — также наибольший общий делитель. Действительно, если $a = qd$, $b = rd$, то $a = (q\varepsilon^{-1})(\varepsilon d)$, $b = (r\varepsilon^{-1})(\varepsilon d)$; если $d = d'd''$, то $\varepsilon d = (\varepsilon d')d''$.

Итак, наибольшие общие делители отличаются множителями, которые являются делителями единицы.

Два элемента кольца называются *ассоциированными*, если они различаются делителями единицы: $a \sim b$ равносильно $a = \varepsilon b$, ε — делитель единицы. Ассоциированность является отношением эквивалентности. Несложная проверка этого утверждения оставляется читателю в качестве упражнения.

Мы будем обозначать наибольший общий делитель через (a, b) и понимать под этим традиционным обозначением *любой* из наибольших общих делителей.

Теорема 2.28. *Наибольший общий делитель двух элементов евклидова кольца можно представить как линейную комбинацию элементов a, b с коэффициентами из кольца*: $(a, b) = \tilde{r}a + \tilde{q}b$, $\tilde{r}, \tilde{q} \in R$.

Доказательство. Рассмотрим множество I, состоящее из всех элементов кольца вида $ra + qb$, $r, q \in R$. Проверим, что это множество — идеал:

$$(r_1a + q_1b) - (r_2a + q_2b) = (r_1 - r_2)a + (q_1 - q_2)b \in I,$$
$$r(r'a + q'b) = (rr')a + (rq')b \in I.$$

Поскольку кольцо евклидово, то этот идеал — главный, т. е. $I = (d)$.

Докажем, что d — наибольший общий делитель a, b. Во-первых, поскольку $a = ea + 0b \in I$, $b = 0a + eb \in I$, получаем $a = sd$, $b = td$. Во-вторых, поскольку $d \in I$, его можно представить в виде $d = \tilde{r}a + \tilde{q}b$. Значит, если $a = q'd'$, $b = r'd'$, то

$$d = \tilde{r}q'd' + \tilde{q}r'd' = (\tilde{r}q' + \tilde{q}r')d'.$$

Как уже было показано, любой другой наибольший общий делитель $\tilde{d}$ отличается от d на множитель ε, который является делителем единицы. Поэтому $\tilde{d} = (\varepsilon\tilde{r})a + (\varepsilon\tilde{q})b$. □

Замечание 2.29. Обозначение (a, b) двусмысленно: так обозначается не только наибольший общий делитель элементов a, b, но и идеал, порожденный элементами a, b (наименьший идеал, содержащий эти элементы). В случае евклидовых колец эта двусмысленность не существенна, поскольку идеал (a, b) является главным идеалом, порожденным наибольшим общим делителем (a, b).

Элементы евклидова кольца R называются *взаимно простыми*, если их наибольший общий делитель равен единице.

Частным случаем теоремы 2.28 является **основная теорема теории делимости**: если числа n и m взаимно просты, то можно подобрать два таких целых x и y, что $xn + ym = 1$. Ясно также, что из теоремы 2.28 следует, что для любых двух целых n, m можно подобрать такие целые числа x, y, что $xn + ym = (n, m)$. Используя эти утверждения, можно определить порядок элемента в циклической группе C_n и описать все порождающие элементы C_n.

Утверждение 2.30. *Пусть m — целое число. Тогда порядок $\bar{m}$ в аддитивной группе $\mathbb{Z}_n$ вычетов по модулю n равен $d = n/(n, m)$.*

Доказательство. Во-первых, $d\bar{m} = \overline{dm} = \overline{n \cdot (m/(n,m))} = \bar{0}$. Во-вторых, если $s\bar{m} = \bar{0}$, $s \neq 0$, то $sm = tn$. Так как $(n, m) = xn + ym$, то $s(n, m) = sxn + sym$ делится на n. Но тогда $s(n, m) \geqslant n$ и $s \geqslant d$. □

Следствие 2.31. *В аддитивной группе $\mathbb{Z}_n$ порождающими элементами являются в точности те вычеты x, для которых $(n, x) = 1$.*

Вернемся к общей теории. Пусть есть три элемента a, b, c целостного кольца с единицей и $a = bc$. Рассмотрим идеалы (a), (b), т. е. все кратные a и все кратные b. Имеет место

Утверждение 2.32. $(a) \subseteq (b)$.

Доказательство. Возьмем какой-нибудь элемент из идеала (a). Он может быть представлен в виде $ad = b(cd) \in (b)$. □

Если элемент b ассоциирован с a, т. е. $b = a \cdot \varepsilon$, то $a = b \cdot \varepsilon^{-1}$. Следовательно, $(a) \subseteq (b)$, $(b) \subseteq (a)$ и поэтому $(a) = (b)$. Другими словами, если два элемента различаются делителем единицы, то они порождают одинаковые идеалы.

Элемент b называется *собственным делителем* ненулевого элемента a, если $a = bc$ и c необратим.

Утверждение 2.33. *Пусть b — собственный делитель a. Тогда a не является делителем b, т. е. $b \neq ad$.*

(Значит, $b \notin (a)$ и потому $(a) \subset (b)$.)

Доказательство. От противного. Пусть $a = bc$. Предположим, что $b = ad$. Тогда $a = a(cd)$ и $a(1 - cd) = 0$. Так как мы рассматриваем кольца без делителей нуля, то по крайней мере один из сомножителей в левой части равен 0. Поскольку $a \neq 0$, то $1 = cd$. Элемент d — обратный к c, приходим к противоречию. □

Лемма 2.34. *Если $a \neq 0$ разлагается в произведение собственных делителей bc, то $N(b) < N(a)$.*

Доказательство. Разделим b на a с остатком: $b = qa + r$. Поскольку b — собственный делитель, то $r \neq 0$, $N(r) < N(a)$. Но $a = bc$. Поэтому $b = qcb + r$, т. е. $r = b(1 - qc) \neq 0$. Следовательно, $N(a) > N(r) \geqslant N(b)$ (норма произведения не меньше нормы ненулевого сомножителя). □

Попутно, для завершения картины, выведем из этой леммы еще одну несложную теорему. Элемент кольца называется *простым*, если у него нет собственных делителей, а он сам не является делителем единицы.

Теорема 2.35. *Каждый элемент евклидова кольца разлагается в произведение простых элементов и делителя единицы.*

Доказательство. Индукция по величине нормы. В качестве базы индукции рассмотрим утверждение теоремы для элементов с минимальной нормой. Очевидно, что они простые: в противном случае они имели бы собственные делители, и эти делители имели бы меньшую норму.

Предположим, что утверждение теоремы верно для всех значений нормы, меньших либо равных некоторому числу m. Возьмем следующее значение нормы $m+s$, т. е. наименьшее из значений нормы, бóльших m (существенное отличие от стандартной индукции здесь в том, что никто не утверждает, что значения норм идут подряд). Пусть $N(a) = m + s$. Если a — простой элемент, то утверждение выполняется. Если a — не простой, то он разлагается в произведение собственных делителей, норма которых меньше нормы a: $a = bc$, $N(b) < N(a)$, $N(c) < N(a)$. Для b, c утверждение справедливо в силу предположения индукции, значит оно справедливо и для a. □

Мы уже доказали (утверждение 2.33) что непростой элемент не может породить максимальный идеал (равносильная форма: всякий главный максимальный идеал порождается простым элементом). Верно и обратное:

Теорема 2.36. *Простой элемент p порождает максимальный идеал (p).*

Доказательство. По теореме 2.22 идеал является максимальным тогда и только тогда, когда кольцо классов вычетов по этому идеалу является полем, т. е. разрешимо уравнение $\bar{a}\bar{x} = \bar{b}$, $\bar{a} \neq \bar{0}$. Докажем, что в кольце $R/(p)$ такое уравнение обязательно разрешимо.

Рассмотрим наибольший общий делитель (a, p). Так как p — простой, его делители — только единицы и он сам. Но a на p не делится ($\bar{a} \neq \bar{0}$, значит, $a \notin (p)$). Поэтому (a, p) — делитель единицы. По теореме 2.28 единицу можно представить в виде линейной комбинации a и p:

$$1 = ar + pq.$$

Докажем, что $\overline{rb}$ — решение уравнения $\bar{a}\bar{x} = \bar{b}$. Так как $b = 1 \cdot b = (ar + pq)b = a(rb) + p(qb)$, то

$$\overline{a(rb) + p(qb)} = \bar{b} \;\Rightarrow\; \bar{a}\overline{rb} + \bar{p}\overline{qb} = \bar{b} \;\Rightarrow\; \bar{a}\overline{rb} = \bar{b}.$$

Итак, мы доказали, что любое линейное уравнение разрешимо, значит, кольцо классов вычетов $R/(p)$ — поле, а потому идеал (p) — максимален. □

В евклидовых кольцах существует простой способ нахождения наибольшего общего делителя и решения уравнения $xa + yb = (a, b)$, который называется *расширенным алгоритмом Евклида*.

Утверждение 2.37. *Для любых элементов a, b, q евклидова кольца выполнено $(a, b) = (a - qb, b)$.*

Доказательство. Пусть d — общий делитель a и b, т. е. $a = a'd$, $b = b'd$. Тогда $a - qb = a'd - qb'd = (a' - qb')d$, так что d является общим делителем $a - qb$ и b. И наоборот, если $a - qb = cd$, $b = b'd$, то $a = qb + cd = (qb' + c)d$. Значит, множество общих делителей для пар a, b и $a - qb, b$ одинаково. □

Утверждение 2.38. *Решениями однородного линейного уравнения с двумя переменными $ax + by = 0$ с коэффициентами из евклидова кольца R (a и b не равны одновременно нулю) являются*

$$x = t\frac{b}{d},\ y = -t\frac{a}{d}, \quad d = (a, b),\ t \in R.$$

Доказательство. Разделив обе части уравнения на наибольший общий делитель (a, b), получим равносильное уравнение, коэффициенты которого взаимно просты. Поэтому достаточно решить уравнение $ax + by = 0$ со взаимно простыми коэффициентами.

Если $(a, b) = 1$, то по теореме 2.28 для некоторых $u, v \in R$ выполнено $au + bv = 1$. Умножим равенство $ax + by = 0$ на u:

$$u(ax + by) = ua + uby = (1 - bv)x + uby = x + b(by - vx) = 0.$$

Таким образом, $x = tb$ при некотором $t \in R$. Но тогда $by = -ax = -tab$ и $y = -ta$. С другой стороны, любая пара $(tb, -ta)$ является решением уравнения $ax + by = 0$. □

Расширенный алгоритм Евклида работает следующим образом. Вначале вычисляется последовательность остатков (собственно алгоритм Евклида):

$$a_i = q_{i+1}a_{i+1} + a_{i+2}, \quad a_0 = a,\ a_1 = b,$$

пока $a_{i+2} \neq 0$. Последние числа в этой последовательности $a_t = q_{t+1}a_{t+1}$, a_{t+1}, причем $a_{t+1} = (a_0, a_1) = (a, b)$.

Почему алгоритм Евклида работает конечное число шагов и дает правильный ответ? Нормы элементов a_i уменьшаются при $i \geqslant 1$, поскольку каждый следующий элемент является остатком от деления на предыдущий. Значит, после конечного числа шагов остаток станет нулю. Корректность ответа следует из утверждения 2.37:

$$(a_0, a_1) = (a_1, a_2) = \cdots = (a_t, a_{t+1}) = a_{t+1}\,.$$

Вторая часть алгоритма (расширенный алгоритм Евклида) строит последовательность пар x_i, y_i, начиная с $x_t = -1$, $y_t = q_{t+1} + 1$ по следующим рекуррентным формулам

$$x_i = y_{i+1}, \qquad y_i = x_{i+1} - q_{i+1}y_{i+1}.$$

По индукции проверяется, что

$$x_i a_i + y_i a_{i+1} = (a_0, a_1). \tag{2.9}$$

Это верно при $i = t$, так как

$$x_t a_t + y_t a_{t+1} = -q_{t+1} a_{t+1} + (q_{t+1} + 1) a_{t+1} = a_{t+1} = (a_0, a_1).$$

Если (2.9) верно при $i + 1$, то оно верно и при i:

$$\begin{aligned} x_i a_i + y_i a_{i+1} &= y_{i+1} a_i + (x_{i+1} - q_{i+1} y_{i+1}) a_{i+1} = \\ &= y_{i+1}(q_{i+1} a_{i+1} + a_{i+2}) + (x_{i+1} - q_{i+1} y_{i+1}) a_{i+1} = \\ &= x_{i+1} a_{i+1} + y_{i+1} a_{i+2} = (a_0, a_1). \end{aligned}$$

Пара (x_0, y_0), полученная в результате работы второй части алгоритма, будет решением уравнения $ax + by = (a, b)$. Остальные решения отличаются от этого на решение однородного уравнения, так как если $ax_0 + by_0 = (a, b)$ и $ax + by = (a, b)$, то $(ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0) = 0$. Поэтому общее решение линейного неоднородного уравнения имеет вид

$$x = x_0 + t\frac{b}{d},\ y = y_0 - t\frac{a}{d} \quad d = (a, b),\ t \in R.$$

2.8. Основная теорема арифметики

Одним из следствий теоремы 2.36 является то, что в кольце классов вычетов по модулю (p), где (p) — простой идеал, нет делителей нуля (выше было доказано, что их нет в любом теле). Из этого факта получается важное усиление теоремы 2.35.

Теорема 2.39. *Каждый элемент евклидова кольца однозначно разлагается в произведение простых элементов с точностью до делителей единицы. Это означает, что если есть два разложения в произведение простых*

$$a = \varepsilon p_1 p_2 \dots p_n = \delta q_1 q_2 \dots q_m$$

(ε, δ — делители единицы), то $n = m$ и существует такая перестановка индексов σ, что $p_i = \varepsilon_i q_{\sigma(i)}$, где ε_i — делители единицы.

Доказательство. Индукция по длине кратчайшего разложения в произведение простых.

База индукции: $n = 0$, делители единицы. Пусть делитель единицы ε является произведением простых элементов $q_1 q_2 \dots q_m$. Тогда q_1 — делитель единицы, так как $\varepsilon^{-1} q_2 \dots q_m$ является обратным к q_1. Но это противоречит определению простоты. Значит, $m = 0$.

Пусть утверждение теоремы выполнено для всех элементов кольца, которые разлагаются в произведение не более чем n простых. Рассмотрим два разложения на простые:

$$\varepsilon p_1 p_2 \dots p_n p_{n+1} = \delta q_1 q_2 \dots q_m, \quad m \geqslant n.$$

Поскольку в кольце вычетов по модулю (p_{n+1}) нет делителей нуля, один из сомножителей в правой части должен делиться на p_{n+1}. С точностью до перенумерации элементов можно считать, что это — q_m. Из простоты p_{n+1}, q_m вытекает, что $p_{n+1} = \varepsilon_{n+1} q_m$. Значит,

$$\varepsilon \varepsilon_{n+1} p_1 p_2 \dots p_n = \delta q_1 q_2 \dots q_{m-1}.$$

Осталось применить предположение индукции к этим разложениям. □

Кольцо целых чисел $\mathbb{Z}$ евклидово (см. пример 2.24). Делителями единицы в этом кольце являются ± 1. Поэтому из теоремы 2.39 вытекает следствие, известное как **основная теорема арифметики:** всякое положительное целое число разлагается в произведение простых чисел однозначно с точностью до перестановки множителей.

Замечание 2.40. Кольца, в которых любой элемент однозначно в смысле теоремы 2.39 разлагается на простые множители, называются *факториальными*. Теорема 2.39 утверждает, что все евклидовы кольца факториальны. Обратное неверно. Можно, например, доказать, что кольцо многочленов от двух переменных $\mathbb{Q}[x, y]$ является факториальным. Но это кольцо не является евклидовым, потому что не является кольцом главных идеалов. Многочлены, у которых свободный член равен 0, образуют в этом кольце идеал и легко проверить, что этот идеал не является главным.

2.9. Китайская теорема об остатках

В этом разделе мы приведем еще одно важное следствие общей теории евклидовых колец.

Теорема 2.41. *Для взаимно простых элементов p_1, p_2 евклидова кольца R имеет место изоморфизм колец $R/(p_1p_2) \cong R/(p_1) \oplus R/(p_2)$.*

Доказательство. Рассмотрим гомоморфизм

$$\varphi\colon R \to R/(p_1) \oplus R/(p_2), \quad \varphi\colon r \mapsto (\{r\}_1, \{r\}_2),$$

где $\{r\}_i$ обозначает класс вычетов по модулю p_i.

Теорема 2.28 утверждает, что в кольце найдутся такие элементы x_1, x_2, для которых $x_1p_1 + x_2p_2 = (p_1, p_2) = 1$. Из этого равенства следует, что $\overline{p_1}$ является делителем единицы в $R/(p_2)$, а $\overline{p_2}$ является делителем единицы в $R/(p_1)$.

Пусть $r = y_1p_1 = y_2p_2 \in \operatorname{Ker}\varphi$. Тогда $\overline{y_1p_1} = \overline{y_2p_2} = \bar{0}$ в $R/(p_1)$. Поскольку $\overline{p_2}$ — делитель единицы, то $\overline{y_2} = \bar{0}$, т. е. $y_2 = ap_1$. Значит, $r = ap_1p_2$. Поэтому ядро гомоморфизма φ совпадает с (p_1p_2).

При этом гомоморфизм φ сюръективен, так как для любой пары классов вычетов $(\{r_1\}_1, \{r_2\}_2)$ найдется элемент кольца $s = r_1 + (r_2 - r_1)x_1p_1 = r_2 - (r_2 - r_1)x_2p_2$, который отображается в эту пару при гомоморфизме φ.

Осталось применить теорему о гомоморфизме колец. □

Теорема 2.41 имеет очевидные следствия для колец вычетов, циклических групп и колец вычетов по модулю идеалов кольца многочленов.

Следствие 2.42. *Если p, q — взаимно простые числа, то $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$.*

Следствие 2.43. *Если p, q — взаимно простые числа, то $C_{pq} \cong C_p \oplus C_q$.*

Следствие 2.44. *Пусть K — поле. Если многочлены $f, g \in K[x]$ взаимно просты, то $K[x]/(fg) \cong K[x]/(f) \oplus K[x]/(g)$.*

Приведем еще один пример использования китайской теоремы об остатках. Функция Эйлера $\varphi(n)$ равна количеству

натуральных чисел, меньших n и взаимно простых с n (т. е. количеству обратимых элементов кольца вычетов $\mathbb{Z}_n$).

Теорема 2.45. *Функция $\varphi(n)$ мультипликативна, т. е. если $(n, m) = 1$, то $\varphi(nm) = \varphi(n)\varphi(m)$.*

Доказательство. Обратимые элементы в кольце $\mathbb{Z}_n \oplus \mathbb{Z}_m$ — это те элементы, у которых в каждой компоненте — обратимый элемент. Значит, количество обратимых элементов в кольце $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$ равно количеству пар (x, y), где x — обратимый в $\mathbb{Z}_n$, а y — обратимый в $\mathbb{Z}_m$. □

2.10. Задачи

2.1. Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

а) целые числа $\mathbb{Z}$;

б) четные числа;

в) целые числа, кратные данному числу d (рассмотреть в частности, случай $d = 0$);

г) рациональные числа $\mathbb{Q}$;

д) действительные числа $\mathbb{R}$;

е) комплексные числа $\mathbb{C}$;

ж) действительные числа вида $x + y\sqrt{2}$, где $x, y \in \mathbb{Z}$;

з) действительные числа вида $x + y\sqrt[3]{2}$, где $x, y \in \mathbb{Q}$;

и) комплексные числа вида $n + mi$, где $n, m \in \mathbb{Z}$ (гауссовы числа);

к) множество комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Q}$;

л) матрицы порядка n с целыми элементами относительно сложения и умножения матриц;

м) матрицы порядка n с действительными элементами относительно сложения и умножения матриц;

н) функции с действительными значениями, непрерывные на отрезке $[-1, +1]$ относительно обычных сложения и умножения функций;

о) многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения;

п) многочлены от одного неизвестного x с действительными коэффициентами относительно обычных операций;

р) матрицы вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными или действительными a, b относительно сложения и умножения матриц;

с) Образуют ли кольцо все тригонометрические полиномы

$$a_0 + \sum_{k=1}^{n} a_k \cos(kx) + b_k \sin(kx)$$

с действительными коэффициентами? Выяснить то же для полиномов одних косинусов $a_0 + \sum_{k=1}^{n} a_k \cos(kx)$ и одних синусов $a_0 + \sum_{k=1}^{n} a_k \sin(kx)$.

2.2. Образует ли кольцо относительно обычных операций сложения и умножения

а) множество рациональных чисел, в несократимой записи которых знаменатели делят фиксированное натуральное число $n \in \mathbb{N}$;

б) множество рациональных чисел, в несократимой записи которых знаменатели не делятся на фиксированное простое число p;

в) множество рациональных чисел, в несократимой записи которых знаменатели являются степенями фиксированного простого числа p;

г) числа вида $x + y\sqrt[3]{2}$, где $x, y \in \mathbb{Q}$ (для определенности берется действительное значение корня);

д) множество комплексных чисел вида $a_1 z_1 + a_2 z_2 + \ldots + a_n z_n$, где a_1, a_2, $\ldots$, a_n — действительные числа, а z_1, z_2, $\ldots$, z_n — комплексные корни n-й степени из 1;

е) множество комплексных чисел вида $\frac{m+in\sqrt{D}}{2}$, где D — фиксированное целое число, свободное от квадратов (не делящееся на квадрат простого числа), n, m — целые числа одинаковой четности.

2.3. Образует ли указанное множество матриц кольцо относительно матричного сложения и умножения:

а) множество действительных симметрических матриц порядка n;

б) множество действительных ортогональных матриц порядка n;

в) множество верхних треугольных матриц порядка n;

г) множество матриц вида $\begin{pmatrix} m & n \\ Dn & m \end{pmatrix}$, где D — фиксированное целое число, $n, m \in \mathbb{Z}$;

д) множество матриц вида $\begin{pmatrix} m & n \\ Dn & m \end{pmatrix}$, где D — фиксированный элемент некоторого кольца K; $n, m \in K$;

е) множество матриц вида $\frac{1}{2}\begin{pmatrix} m & n \\ Dn & m \end{pmatrix}$, где D — фиксированное целое число, свободное от квадратов (не делящееся на квадрат простого числа), n, m — целые числа одинаковой четности;

ж) множество комплексных матриц вида $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$;

з) множество вещественных матриц вида

$$\begin{pmatrix} x & -y & z & t \\ y & x & -t & z \\ -z & t & x & y \\ -t & -z & -y & x \end{pmatrix}.$$

2.4. Образует ли следующее множество функций кольцо относительно обычных операций сложения и умножения функций:

а) множество функций действительного переменного на отрезке $[a, b]$;

б) множество функций действительного переменного, имеющих вторую производную на интервале (a, b);

в) множество рациональных функций действительного переменного;

г) множество непрерывных периодических функций действительного переменного;

д) множество функций действительного переменного, обращающихся в 0 на некотором подмножестве $D \subseteq \mathbb{R}$;

е) множество функций, определенных на некотором множестве D и принимающих значение в некотором кольце K.

2.5. В множестве многочленов от переменного t с обычным сложением в качестве умножения рассматривается операция суперпозиции, заданная правилом $(f \circ g)(t) = f(g(t))$. Является ли это множество кольцом относительно заданных операций?

2.6. Образует ли кольцо множество всех подмножеств некоторого множества относительно симметрической разности и пересечения, рассматриваемых как сложение и умножение соответственно?

2.7. Является ли кольцом множество трехмерных векторов относительно операций векторного сложения и векторного умножения?

2.8. Доказать, что в кольце с единицей выполняются тождества

$$\text{а)}\ -ab = (-1)ab, \qquad \text{б)}\ (-1)\cdot(-1) = 1.$$

2.9. Какие из колец в задачах 2.1 – 2.7 содержат делители нуля?

2.10. Доказать, что если a^k — делитель нуля, то и a — делитель нуля.

2.11. Доказать, что все диагональные матрицы, т. е. матрицы вида

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix},$$

порядка $n \geqslant 2$ с действительными коэффициентами относительно обычных операций сложения и умножения матриц образуют коммутативное кольцо с делителями нуля.

2.12. Доказать, что в кольце квадратных матриц порядка n с элементами из некоторого поля делителями нуля являются вырожденные матрицы, и только они. (Матрица называется вырожденной, если ее определитель равен 0).

2.13. Найти все делители нуля кольца $\mathbb{Z} \oplus \mathbb{Z}$ (определение прямой суммы колец см. на с. 87).

2.14. Доказать, что все обратимые элементы кольца с единицей образуют группу относительно умножения.

2.15. Найти обратимые элементы в кольцах с единицей из задач 2.1 – 2.7.

2.16. Доказать, что из равенства $ax = ay$ для данного элемента a и любых элементов x и y кольца следует равенство $x = y$ тогда и только тогда, когда a не является делителем нуля.

2.17. Показать, что матрицы порядка $n \geqslant 2$ с элементами из некоторого поля, в которых все строки, начиная со второй, состоят из нулей, образуют кольцо относительно матричного сложения и умножения, в котором всякий элемент, отличный от нуля, будет правым делителем нуля. Какие матрицы в этом кольце не будут левыми делителями нуля?

2.18. Элемент a кольца R называется *нильпотентным*, если $a^m = 0$ для некоторого натурального m. Для коммутативного кольца R доказать, что а) если a — нильпотентный, то для любого $r \in R$ элемент ra — также нильпотентный; б) если a, b — нильпотентные, то $a + b$ — также нильпотентный.

2.19. Найти все обратимые элементы, все делители нуля и все нильпотентные элементы в кольцах а) $\mathbb{Z}_{p^n}$, где p — простое число; б) кольцо верхних треугольных матриц над полем; в) кольцо $M_2[\mathbb{R}]$ матриц второго порядка с действительными элементами; г) кольцо всех функций, определенных на некотором множестве S и принимающих значения в поле K.

2.20. Пусть R — конечное кольцо. Доказать, что

а) если R не содержит делителей нуля, то оно имеет единицу и все его ненулевые элементы обратимы;

б) если R имеет единицу, то каждый его элемент, имеющий односторонний обратный, обратим;

в) если R имеет единицу, то всякий левый делитель нуля является правым делителем нуля;

Верно ли утверждение в) для колец без единицы?

2.21. Доказать, что в кольце с единицей и без делителей нуля каждый элемент, имеющий односторонний обратный, является обратимым.

2.22. Пусть R — кольцо с единицей, $x, y \in R$. Доказать, что

а) если произведения xy и yx обратимы, то элементы x и y также обратимы;

б) если R без делителей нуля и произведение xy обратимо, то элементы x и y также обратимы;

в) если R конечно и произведение xy обратимо, то элементы x и y также обратимы;

г) без дополнительных предположений о кольце R из обратимости произведения xy не следует обратимость элементов x и y.

2.23. Пусть R — кольцо с единицей и S — его подкольцо.

а) Верно ли, что $1 \in S$?

б) Может ли подкольцо S иметь единицу e, отличную от 1 — единицы кольца R?

2.24. Показать, что в кольце с единицей коммутативность сложения вытекает из остальных аксиом кольца.

2.25. Проверить, что равенства $0 \cdot a = a \cdot 0 = 0$ можно доказать, не используя коммутативности сложения. Доказать, что в кольце, содержащем хотя бы один элемент c, не являющийся делителем нуля, коммутативность сложения вытекает из остальных аксиом кольца.

2.26. Привести примеры колец матриц, в которых есть несколько правых или левых единиц.

2.27. Доказать, что если все элементы коммутативного кольца R имеют общий делитель a, то это кольцо обладает единицей.

2.28. Указать коммутативное кольцо с единицей, содержащее элемент $a \neq 0$ с одним из следующих свойств:

а) $a^2 = 0$;

б) для данного целого числа $n > 1$ выполнены условия $a^n = 0$, $a^k \neq 0$, если $0 < k < n$.

2.29. Пусть R — коммутативное кольцо с единицей и $R\langle x\rangle$ — множество всех формальных степенных рядов $\sum_{k=0}^{\infty} a_k x^k$, $a_k \in R$. Введем обычные операции сложения и умножения рядов:

$$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (a_k + b_k) x^k,$$

$$\Big(\sum_{k=0}^{\infty} a_k x^k\Big) \cdot \Big(\sum_{k=0}^{\infty} b_k x^k\Big) = \sum_{k=0}^{\infty} (c_k) x^k, \quad \text{где } c_k = \sum_{j=0}^{k} a_j b_{k-j}\,.$$

Показать, что:

а) $R\langle x\rangle$ — коммутативное кольцо с единицей;

б) $R\langle x\rangle$ содержит подкольцо, изоморфное R;

в) если R не имеет делителей нуля, то это верно и для $R\langle x\rangle$;

г) если R — поле, то $\sum_{k=0}^{\infty} a_k x^k$ тогда и только тогда будет обратимым элементом кольца $R\langle x\rangle$, когда $a_0 \neq 0$.

2.30. Пусть R — множество всех чисел вида $a + b\sqrt{-3}$, где $a, b \in \mathbb{Z}$. Показать, что R — кольцо с единицей, в котором разложение на простые множители существует, но не однозначно. В частности, показать, что в двух разложениях $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ сомножители являются простыми, причем 2 не ассоциировано с $1 \pm \sqrt{-3}$.

2.31*. Доказать, что все конечные суммы $\sum a_k 2^{r_k}$ с целыми коэффициентами a_k и неотрицательными двоично рациональными r_k относительно обычных операций сложения и умножения чисел образуют коммутативное кольцо с единицей и без делителей нуля, в котором не существует разложения на простые множители.

2.32. Доказать изоморфизм следующих колец: кольца комплексных чисел вида $\frac{m+in\sqrt{D}}{2}$, где D — фиксированное целое число, свободное от квадратов (не делящееся на квадрат простого числа), n, m — целые числа одинаковой четности относительно обычных операций сложения и умножения, и кольца матриц вида $\frac{1}{2}\begin{pmatrix} m & n \\ Dn & m \end{pmatrix}$, где D — то же самое число, n, m — целые числа одинаковой четности, относительно матричного сложения и умножения.

2.33. Доказать изоморфизм следующих колец: кольцо комплексных матриц вида $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$ относительно матричного сложения и умножения и кольцо действительных матриц вида

$$\begin{pmatrix} x & -y & z & t \\ y & x & -t & z \\ -z & t & x & y \\ -t & -z & -y & x \end{pmatrix}.$$

относительно матричного сложения и умножения.

2.34. Пусть R — кольцо, состоящее из всех действительных функций $f(x)$, определенных на всей числовой прямой, с обычными операциями сложения и умножения, и c — действительное число. Доказать, что:

а) отображение $\varphi[f(x)] = f(c)$ есть гомоморфное отображение кольца R на поле $\mathbb{R}$ действительных чисел;

б) ядро $\operatorname{Ker}\varphi$ гомоморфизма φ есть идеал в R;

в) факторкольцо $R/\operatorname{Ker}\varphi$ изоморфно полю действительных чисел $\mathbb{R}$.

2.35. *Алгебра кватернионов* $\mathbb{H}$ — это множество

$$\mathbb{H} = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_i \in \mathbb{R}\}$$

с операциями покомпонентного сложения

$$(a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k)$$

и умножения, которое определяется таблицей умножения «мнимых единиц»

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

и условием дистрибутивности.

а) Сопряженным кватерниону $h = a_0 + a_1 i + a_2 j + a_3 k$ называется кватернион $\bar{h} = a_0 - a_1 i - a_2 j - a_3 k$. Проверить, что $h\bar{h}$ — действительное число (кватернион вида $a + 0i + 0j + 0k$). Это число называется *квадратом нормы* кватерниона.

б) Проверить, что кватернионы образуют тело.

в) Проверить, что любой кватернион нормы 1 можно записать в виде $h = \cos(\theta/2) + \sin(\theta/2)v$, где «мнимая часть» кватерниона v является единичным вектором в трехмерном евклидовом пространстве с ортонормированным базисом i, j, k. Кватерниону h сопоставим вращение трехмерного пространства вокруг оси, задаваемой вектором v, на угол θ.

Доказать, что построенное соответствие является гомоморфизмом: произведению кватернионов соответствует композиция соответствующих им вращений.

2.36. Доказать, что алгебра матриц вида $\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$ с действительными a, b, c, d и $i = \sqrt{-1}$ изоморфна алгебре кватернионов $\mathbb{H}$.

2.37. Доказать, что алгебра действительных матриц вида

$$\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

изоморфна алгебре кватернионов $\mathbb{H}$.

2.38. Пусть (n) — идеал, порожденный целым числом $n > 1$ в кольце многочленов с целыми коэффициентами $\mathbb{Z}[x]$. Доказать, что факторкольцо $\mathbb{Z}[x]/(n)$ изоморфно кольцу $\mathbb{Z}_n[x]$ многочленов над кольцом $\mathbb{Z}_n$ вычетов по модулю n.

2.39. Пусть R и S — кольца с единицей, $\varphi\colon R \to S$ — гомоморфизм.

а) Верно ли, что образ единицы кольца R является единицей кольца S?

б) Верно ли утверждение а), если гомоморфизм φ сюръективен?

2.40. Гомоморфизм $\varphi\colon R \to S$ колец R и S с единицами 1 и e называется *унитарным*, если $\varphi(1) = e$. Найти

а) все унитарные гомоморфизмы кольца $\mathbb{Z}$ и кольца многочленов $\mathbb{Z}[x]$ в произвольное кольцо R с единицей;

б) все гомоморфизмы кольца $\mathbb{Z}$ и кольца многочленов $\mathbb{Z}[x]$ в произвольное кольцо R.

2.41. Пусть K — поле и f пробегает множество всех многочленов степени 2 из $K[x]$. Разбить на классы попарно изоморфных колец совокупность колец $K[x]/(f)$, если а) $K = \mathbb{C}$; б) $K = \mathbb{R}$; в) $K = \mathbb{Q}$; г) K — конечное поле.

2.42. Найти с точностью до изоморфизма: а) все кольца с единицей, б) все кольца, у которых аддитивная группа — циклическая порядка n.

2.43. Доказать, что любое гомоморфное отображение поля P в кольцо R является или изоморфным отображением на некоторое поле, входящее в R как подкольцо (так называемое вложение P в R), или отображением всех элементов из P в нуль из R.

2.44. Пусть $\mathbb{Z}$ — кольцо целых чисел и R — любое кольцо с единицей e. Доказать, что отображение $\varphi\colon n \mapsto ne$ есть гомоморфное отображение $\mathbb{Z}$ в R. Найти образ $\varphi(\mathbb{Z})$ кольца $\mathbb{Z}$ при этом гомоморфизме.

2.45. Будут ли следующие множества подгруппами аддитивной группы, подкольцами или идеалами указанных ниже колец:

а) множество $n\mathbb{Z}$ чисел, кратных числу $n > 1$, в кольце $\mathbb{Z}$ целых чисел;

б) множество $\mathbb{Z}$ целых чисел в кольце $\mathbb{Z}[x]$ многочленов с целыми коэффициентами;

в) множество $n\mathbb{Z}[x]$ многочленов, коэффициенты которых кратны числу $n > 1$, в кольце $\mathbb{Z}[x]$ многочленов с целыми коэффициентами;

г) множество $\mathbb{N}$ натуральных чисел в кольце $\mathbb{Z}$ целых чисел;

д) множество $\mathbb{Z}$ целых чисел в кольце $\mathbb{Z}[i]$ целых гауссовых чисел, т. е. чисел вида $m + ni$ с целыми $m, n \in \mathbb{Z}$;

е) множество E чисел $a + ai$ в кольце $\mathbb{Z}[i]$ целых гауссовых чисел;

ж) множество C чисел вида $x(1 + i)$ в кольце $\mathbb{Z}[i]$ целых гауссовых чисел, где x пробегает всё кольцо $\mathbb{Z}[i]$;

з) множество $\mathbb{Z}[x]$ многочленов с целыми коэффициентами в кольце $\mathbb{Q}[x]$ многочленов над полем $\mathbb{Q}$ рациональных чисел;

и) множество I многочленов, не содержащих членов с x^k для всех $k < n$, где $n > 1$, в кольце $\mathbb{Z}[x]$ многочленов с целыми коэффициентами;

к) множество I многочленов с четными свободными членами в кольце $\mathbb{Z}[x]$ многочленов с целыми коэффициентами;

л) множество I многочленов с четными старшими коэффициентами в кольце $\mathbb{Z}[x]$ многочленов с целыми коэффициентами.

2.46. При каких n все необратимые элементы кольца $\mathbb{Z}_n$ образуют идеал?

2.47. Доказать, что пересечение любого множества идеалов коммутативного кольца R является идеалом.

2.48. Доказать, что множество I_S непрерывных функций, обращающихся в 0 на фиксированном подмножестве $S \subseteq [a, b]$, является идеалом в кольце функций, непрерывных на $[a, b]$. Верно ли, что всякий идеал этого кольца имеет вид I_S для некоторого S?

2.49. Доказать, что в кольце $M_n(\mathbb{Z})$ матриц порядка n над кольцом $\mathbb{Z}$ подкольцо $M_n(2\mathbb{Z})$ является двусторонним идеалом.

2.50. Доказать, что любой ненулевой идеал в кольце $M_n(\mathbb{Z})$ матриц порядка n над кольцом $\mathbb{Z}$ совпадает с $M_n(k\mathbb{Z})$ для некоторого $k \in \mathbb{N}$.

2.51. Доказать, что в кольце $M_n(R)$ матриц порядка n с элементами из произвольного кольца R идеалами являются в точности множества матриц, элементы которых принадлежат фиксированному идеалу кольца R.

2.52. Доказать, что в кольце матриц над полем всякий двусторонний идеал либо нулевой, либо совпадает со всем кольцом.

2.53. Найти все идеалы кольца верхних треугольных матриц порядка 2 с целыми элементами.

2.54. Пусть I и J — множества матриц вида

$$\begin{pmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & l & 2m \\ 0 & 0 & 2n \\ 0 & 0 & 0 \end{pmatrix}$$

с целыми $g, h, k, \ldots$. Доказать, что I является двусторонним идеалом в кольце R верхних треугольных матриц над $\mathbb{Z}$, J есть идеал кольца I, но J не является идеалом кольца R.

2.55. Пусть R — коммутативное кольцо с единицей. Доказать, что:

а) обратимый элемент (т. е. делитель единицы) не может быть делителем нуля;

б) обратимый элемент имеет единственный обратный элемент;

в) если λ, μ обратимы, то a делится на b тогда и только тогда, когда $a\lambda$ делится на $b\mu$;

г) главный идеал (a), порожденный элементом a из R тогда и только тогда отличен от R, когда a необратим.

2.56. Пусть R — коммутативное кольцо с единицей и без делителей нуля. Доказать, что элементы a и b тогда и только тогда ассоциированы, когда каждый из них делится на другой.

2.57. Доказать, что идеал (M), порожденный непустым множеством $M \subseteq R$ состоит из всех конечных сумм вида:

а) $\sum r_k a_k$, $r_k \in R$, $a_k \in M$, если R имеет единицу;

б) $\sum r_k a_k + \sum n_k a_k$, $r_k \in R$, $a_k \in M$, $n_k \in \mathbb{Z}$, если R не имеет единицы.

2.58. Суммой идеалов $I_1, I_2, \ldots, I_k$ коммутативного кольца R называется множество I всех элементов x из R, представимых в виде $x = x_1 + x_2 + \cdots + x_k$, $x_j \in I_j$, $j = 1, 2, \ldots, k$. Пишут $I = I_1 + I_2 + \cdots + I_k$. Если для любого x из I указанное представление единственно, то сумма I называется прямой суммой идеалов I_j. В этом случае пишут $I = I_1 \oplus I_2 \oplus \ldots \oplus I_k$. Доказать, что:

а) сумма любого конечного числа идеалов есть идеал;

б) сумма двух идеалов тогда и только тогда будет прямой суммой, когда пересечение идеалов содержит только нуль.

2.59. Доказать, что если $I = I_1 \oplus I_2$ — прямая сумма идеалов I_1, I_2, то произведение любого элемента из I_1 на любой элемент из I_2 равно нулю.

2.60. Пусть $R = I_1 \oplus I_2$ — разложение коммутативного кольца R с единицей e в прямую сумму ненулевых идеалов I_1, I_2. Доказать, что если $e = e_1 + e_2$, $e_1 \in I_1$, $e_2 \in I_2$, то e_1, e_2 будут единицами соответственно в I_1, I_2, но не в R.

2.61. Какие из колец в задачах 2.1 – 2.7 являются полями?

2.62. Доказать, что конечное коммутативное кольцо без делителей нуля, содержащее более одного элемента, является полем.

2.63. Квадратная матрица называется скалярной, если ее элементы на главной диагонали равны между собой, а вне главной диагонали — равны нулю. Показать, что скалярные матрицы порядка n с действительными элементами относительно матричных сложения и умножения образуют поле, изоморфное полю действительных чисел.

2.64. Показать, что матрицы вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a и b — действительные числа, образуют поле, изоморфное полю комплексных чисел.

2.65. Доказать,что числа вида $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ образуют поле, причем каждый элемент этого поля представляется в указанном виде однозначно. Найти элемент, обратный числу $x = 1 - \sqrt[3]{2} + 2\sqrt[3]{4}$ (берется действительное значение корня).

2.66. Доказать, что числа вида $\mathbb{Q}[\sqrt[3]{5}] = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} \mid a, b, c \in \mathbb{Q}\}$ образуют поле, причем каждый элемент этого поля представляется в указанном виде однозначно. Найти элемент,

обратный числу $x = 2 + 3\sqrt[3]{5} - 2\sqrt[3]{25}$ (берется действительное значение корня).

2.67. Пусть α — корень многочлена $f(x)$ степени $n > 1$ с рациональными коэффициентами, неприводимого над полем $\mathbb{Q}$ рациональных чисел. Доказать, что множество $Q(\alpha)$ чисел вида

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \quad a_0, \ldots, a_{n-1} \in \mathbb{Q},$$

образует поле, причем каждый элемент этого поля представляется в указанном виде однозначно. Говорят, что это поле получено присоединением числа α к полю рациональных чисел.

2.68. В поле, полученном присоединением к полю рациональных чисел корня α многочлена $f(x) = x^3 + 4x^2 + 2x - 6$ найти число, обратное числу $\beta = 3 - \alpha + \alpha^2$.

2.69. Доказать, что поле матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, с рациональными a и b изоморфно полю $\mathbb{Q}[\sqrt{2}]$.

2.70. Какие из следующих множеств матриц образуют поле относительно обычных матричных операций:

а) $\left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \mid x, y \in \mathbb{Q} \right\}$, где $n \in \mathbb{Z}$ фиксировано;

б) $\left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$, где $n \in \mathbb{Z}$ фиксировано;

в) $\left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \mid x, y \in \mathbb{Z}_p \right\}$, где $p = 2, 3, 5, 7$?

2.71. Доказать, что при любом изоморфизме числовых полей подполе рациональных чисел отображается тождественно. В частности, поле рациональных чисел допускает лишь тождественное изоморфное отображение в себя.

2.72. Доказать, что поле $\mathbb{R}$ не имеет автоморфизмов, отличных от тождественного.

2.73. Найти все автоморфизмы поля $\mathbb{C}$, при которых каждое действительное число переходит в себя.

2.74. Имеет ли поле $\mathbb{Q}[\sqrt{2}]$ нетождественные автоморфизмы?

2.75. При каких $m, n \in \mathbb{Z} \setminus \{0\}$ поля $\mathbb{Q}[\sqrt{m}]$ и $\mathbb{Q}[\sqrt{n}]$ изоморфны?

2.76. Доказать, что для любого автоморфизма φ поля K множество элементов, неподвижных относительно φ, является подполем.

2.77. Существует ли поле, строго содержащее поле комплексных чисел?

2.78. Найти наибольший общий делитель чисел $a^n - 1$ и $a^m - 1$.

2.79. Найти наибольший общий делитель многочленов $f(x) = x^3 + x^2 + 1$, $g(x) = x^2 + x + 1$ а) над полем вычетов по модулю 3; б) над полем рациональных чисел.

2.80. Найти наибольший общий делитель многочленов $f(x) = 5x^3 + x^2 + 5x + 1$, $g(x) = 5x^2 + 6x + 1$ а) над полем вычетов по модулю 5 (при этом каждый коэффициент a надо понимать как кратное ae единицы e указанного поля или заменить коэффициенты их наименьшими неотрицательными вычетами по модулю 5); б) над полем рациональных чисел.

2.81. Найти наибольший общий делитель многочленов $f(x) = x^4 + 1$, $g(x) = x^3 + x + 1$ над полем вычетов по модулю а) 3; б) 5.

2.82. Доказать, что

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\dots\Big(1 - \frac{1}{p_k}\Big),$$

где $\varphi(n)$ — функция Эйлера (число обратимых элементов кольца $\mathbb{Z}_n$), а p_1, p_2, …, p_k — все различные простые делители числа n.

2.83. Найти все такие целые n, для которых группа обратимых элементов кольца $\mathbb{Z}/(2^n)$ является циклической.

2.84*. Доказать, что группа обратимых элементов кольца $\mathbb{Z}/(p^n)$ является циклической для любого простого $p \geqslant 3$.

2.85. Доказать, что

а) кольцо целых гауссовых чисел $\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\}$ евклидово;

б) кольцо комплексных чисел вида $\mathbb{Z}[i\sqrt{3}] = \{m + in\sqrt{3} \mid m, n \in \mathbb{Z}\}$ не является евклидовым;

в) кольцо комплексных чисел вида

$$\Big\{\frac{m + in\sqrt{3}}{2} \mid m, n \in \mathbb{Z};\ m - n \text{ четно}\Big\}$$

является евклидовым.

2.86. Пусть $\mathbb{Z}[i]$ — кольцо целых гауссовых чисел, I — множество всех чисел $m + ni$ с четными m и n.

а) Показать, что I — идеал в $\mathbb{Z}[i]$;

б) найти смежные классы $\mathbb{Z}[i]$ по I;

в) в факторкольце $\mathbb{Z}[i]/I$ найти делители нуля и показать этим, что $\mathbb{Z}[i]/I$ не является полем.

2.87. Доказать, что факторкольцо $\mathbb{Z}[i]/(3)$ кольца целых гауссовых чисел $\mathbb{Z}[i]$ по главному идеалу $(3) = 3\mathbb{Z}[i]$ есть поле из девяти элементов.

2.88. Доказать, что факторкольцо $\mathbb{Z}[i]/(n)$ кольца целых гауссовых чисел $\mathbb{Z}[i]$ по главному идеалу $(n) = n\mathbb{Z}[i]$ тогда и только тогда будет полем, когда n — простое число, не равное сумме двух квадратов целых чисел.

2.89. Доказать, что кольцо $\mathbb{Z}[x]$ не является кольцом главных идеалов.

2.90. Пусть $K[x, y]$ — кольцо многочленов от двух переменных x, y над полем K, I — множество всех многочленов этого кольца без свободного члена. Доказать, что:

а) I является идеалом, но не является главным идеалом;

б) факторкольцо $K[x, y]/I$ изоморфно полю K.

2.91. Эндоморфизмом группы называется гомоморфизм этой группы в себя. На множестве эндоморфизмов коммутативной группы G определим операцию умножения как композицию эндоморфизмов, а операцию сложения — по правилу

$$(\varphi + \psi)(a) = \varphi(a) + \psi(a).$$

Доказать, что множество эндоморфизмов коммутативной группы с определенными выше операциями сложения и умножения образует кольцо.

2.92. Доказать, что

а) кольцо эндоморфизмов циклической группы порядка n изоморфно кольцу $\mathbb{Z}_n$;

б) группа автоморфизмов циклической группы порядка n изоморфна группе обратимых элементов кольца $\mathbb{Z}_n$.

2.93. Доказать, что всякое кольцо с единицей изоморфно вкладывается в кольцо эндоморфизмов своей аддитивной группы. (Изоморфное вложение — гомоморфизм с нулевым ядром.)

2.94. (Еще одна версия китайской теоремы об остатках). Пусть A — коммутативное кольцо с единицей. Доказать, что если I_1 и I_2 — идеалы в A и $I_1+I_2 = A$, то для любых элементов $x_1, x_2 \in A$ существует такой элемент $x \in A$, что $x - x_1 \in I_1$, $x - x_2 \in I_2$.

2.95*. В кольце выполнено тождество $x^3 = x$. Доказать, что такое кольцо коммутативно.

Глава 3

Конечные поля или поля Галуа

В этой главе мы рассмотрим *конечные поля*, т. е. поля, в которых есть лишь конечное число элементов. Они также называются *полями Галуа*, в честь Э. Галуа, который их первым изучил.

Оказывается, все поля Галуа можно получить факторизацией по некоторому идеалу кольца целых чисел или кольца многочленов.

3.1. Поле вычетов по модулю простого числа

Сначала рассмотрим кольцо целых чисел. Возьмем произвольное простое число p и построим идеал $(p) = \{np \mid n \in \mathbb{Z}\}$, т. е. возьмем все кратные p.

Кольцо $\mathbb{Z}/p\mathbb{Z}$ вычетов по модулю этого идеала описано в примере 2.16. Напомним, что оно состоит из p элементов

$$\begin{aligned}
\bar{0} &= 0 + p\mathbb{Z} = \{rp \mid r \in \mathbb{Z}\},\\
\bar{1} &= 1 + p\mathbb{Z} = \{1 + rp \mid r \in \mathbb{Z}\},\\
&\dots\\
\overline{p-1} &= (p-1) + p\mathbb{Z} = \{p - 1 + rp \mid r \in \mathbb{Z}\}.
\end{aligned}$$

Поскольку $\mathbb{Z}$ — евклидово, а p — простое, по теореме 2.36 кольцо $\mathbb{Z}/p\mathbb{Z}$ является полем. Это поле вычетов по модулю p и есть простейшее поле Галуа, которое мы далее будем обозначать $GF(p)$. Операции сложения и умножения в этом поле — это

сложение и умножение целых чисел по модулю p. Скажем, чтобы найти $\bar{x} + \bar{y}$, необходимо вычислить $z = (x + y) \bmod p$, класс вычетов $\bar{z}$ и будет результатом сложения $\bar{x}$ и $\bar{y}$. Ясно также, что можно брать и любые другие представители тех же самых классов вычетов: результат сложения по модулю p не изменится.

Поля $GF(p)$ — это конечный аналог числовых полей, более точно, — поля рациональных чисел. Чтобы увидеть это, введем понятие *характеристики поля*. Рассмотрим в некотором поле F множество кратных единицы:

$$\begin{aligned} &1 = 1, \\ &2 = 1 + 1, \\ &\dots \\ &k = \underbrace{1 + 1 + \dots + 1}_{k \text{ раз}}, \\ &\dots \end{aligned}$$

Если порядок 1 в аддитивной группе поля бесконечен, то характеристика поля F по определению равна 0. В этом случае все кратные единицы различны. В поле F выполнимы все арифметические действия, поэтому из этих кратных единицы мы можем построить произведения $n \cdot k^{-1}$ и противоположные к ним (обратные относительно сложения). Арифметические операции с этими числами выполняются так же, как с обыкновенными дробями, это легко проверить, используя свойства операций сложения и умножения в поле. Поэтому, добавляя к построенным выше элементам поля элемент 0, мы получаем в поле F подполе, которое изоморфно полю рациональных чисел $\mathbb{Q}$.

Если порядок 1 в аддитивной группе поля конечен, то он и есть по определению характеристика поля $\operatorname{char} F$. Повторяя описанную выше процедуру добавления к кратным единицы «дробей», «противоположных чисел» и 0, мы получим подполе поля F, содержащее $\operatorname{char} F$ элементов. Нетрудно видеть, что оно изоморфно кольцу классов вычетов $\mathbb{Z}$ по модулю $(\operatorname{char} F)$. Но $(nm) \subset (n)$, поэтому чтобы кольцо классов вычетов по модулю p было полем, необходимо (и достаточно, как было показано выше), чтобы p было простым числом.

Итак, мы показали неформально справедливость следующих утверждений.

Утверждение 3.1. *Если характеристика поля не равна нулю, то она — простое число.*

Утверждение 3.2. *В каждом поле F есть либо подполе, изоморфное $\mathbb{Q}$, либо подполе, изоморфное $GF(p)$, $p = \operatorname{char} F$.*

Читателю предлагается построить строгие доказательства этих утверждений, следуя намеченному выше плану.

Замечание 3.3. Не нужно думать, что все поля положительной характеристики конечны. Вот простейший пример бесконечного поля положительной характеристики. Пусть $\Bbbk$ — произвольное поле. Построим новое поле $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$. По определению, элементами этого поля, т. е. рациональными функциями, являются отношения многочленов (т. е. дроби) $r = p/q$, где $p, q \in \Bbbk[x]$, причем $q \neq 0$. По определению, $p_1/q_1 = p_2/q_2$, если $p_1 q_2 = p_2 q_1$. Отсюда следует, что для любого d выполняется равенство $(dp)/(dq) = p/q$. Поэтому дроби можно приводить к общему знаменателю, что дает возможность их складывать: $p/q + u/v = (pv)/(qv) + (qu)/(qv) = (pv + qu)/qv$. Умножение дробей определяется естественным образом: $(p/q) \cdot (u/v) = (pu)/(qv)$. Отметим, что $\Bbbk[x] \subset k(x)$ — каждый многочлен p отождествляется с дробью $p/1$. Ясно, что эта конструкция действительно дает поле. Если в качестве $\Bbbk$ взять конечное поле $GF(q)$ характеристики p, то мы придем к бесконечному полю $GF(q)(x)$, которое также имеет характеристику p.

3.2. Автоморфизм Фробениуса

Конечное поле имеет положительную характеристику, причем эта характеристика — простое число. Вычисления в поле положительной характеристики сильно упрощаются следующей леммой.

Лемма 3.4. *В поле характеристики $p > 0$ выполнено тождество*

$$(a + b)^p = a^p + b^p. \tag{3.1}$$

Доказательство. В любом коммутативном кольце верна формула для бинома

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

Чтобы доказать (3.1), достаточно проверить, что все $\binom{p}{k}$, $k \notin \{0, p\}$, делятся на p. Запишем формулу для биномиального коэффициента:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p\cdot(p-1)\cdot\ldots\cdot 1}{k!(p-k)!}\,.$$

Так как p — простое число, а кольцо целых чисел — евклидово, числитель дроби делится на p, а знаменатель — нет. В самом деле, разлагая сомножители знаменателя в произведение простых, видим, что каждый простой делитель знаменателя не превосходит максимума из k и $p-k$, т. е. меньше p. □

Аналогичная формула для умножения $(ab)^p = a^p b^p$ верна для любого поля по очевидным причинам. Поэтому отображение $x \mapsto x^p$ является гомоморфизмом поля характеристики p в себя. Ядро этого гомоморфизма нулевое, так как в поле есть только два идеала — идеал, состоящий из одного элемента 0, и само поле. Действительно, если I — идеал в поле, $a \in I$, $a \neq 0$, то и всякий другой ненулевой элемент поля x принадлежит идеалу I, поскольку является кратным a: $x = (xa^{-1})a$. Раз ядро гомоморфизма нулевое, то отображение *инъективно* (по определению это означает, что образы всех элементов различны). Таким образом, приходим к интересному следствию леммы 3.4 для конечных полей.

Следствие 3.5. *Отображение конечного поля характеристики p, задаваемое формулой $x \mapsto x^p$, является автоморфизмом поля.*

Действительно, инъективное отображение конечного поля в себя является биективным (взаимно однозначным).

Автоморфизм $x \mapsto x^p$ называется автоморфизмом Фробениуса.

3.3. Неприводимые многочлены

Как было показано выше, кольцо многочленов над полем F — евклидово. Простые элементы этого кольца называются *неприводимыми многочленами* (над F). В этом разделе мы рассмотрим неприводимые многочлены над полями комплексных, действительных и рациональных чисел, а также над полем вычетов $GF(p)$.

Начнем с того, что проверим справедливость известных школьных фактов о корнях многочленов для колец многочленов с коэффициентами в произвольном поле.

Утверждение 3.6. *Остаток от деления многочлена f на многочлен первой степени $x - a$ равен $f(a)$. В частности, f делится на $(x - a)$ тогда и только тогда, когда a является корнем f,* т. е. $f(a) = 0$.

Доказательство. Разделим f с остатком на $x - a$, остаток должен иметь степень 0: $f = q \cdot (x - a) + b$. Подставляя вместо x элемент a, получаем $f(a) = b$. □

То же самое утверждение можно сформулировать иначе. Рассмотрим гомоморфизм

$$\mathrm{Ev}_a \colon F[x] \to F,$$

который определяется вычислением значения многочлена при $x = a$: $\mathrm{Ev}_a \colon f \mapsto f(a)$. У этого гомоморфизма есть ядро: те многочлены, для которых a является корнем. Тогда наше утверждение в точности означает, что $\operatorname{Ker} \mathrm{Ev}_a = (x-a)$ (идеал, порожденный $x - a$).

Можно доказать это утверждение, не обращаясь к делению с остатком. Действительно, отображение $f(x) \mapsto f(x + a)$ также является гомоморфизмом колец. Более того, оно взаимно однозначно: обратное отображение задается формулой $f(x) \mapsto f(x-a)$. Значит, это автоморфизм кольца многочленов. Но тогда наше утверждение достаточно доказать при $a = 0$, а в этом случае оно очевидно.

Полезным следствием утверждения 3.6 является следующая лемма.

Лемма 3.7. *Многочлен степени d имеет не более d корней.*

Достаточно вспомнить, что при умножении многочленов степени складываются, и учесть, что многочлены $x-a$ и $x-b$ взаимно просты при $a \neq b$. Отсюда получаем очень важное утверждение:

Лемма 3.8. *Если два многочлена степени не выше d как функции различны, то их значения совпадают не более чем в d точках.*

Можно применить предыдущую лемму к разности многочленов. Эта лемма показывает, что многочлены «сильно отличаются один от другого». Именно это свойство многочленов лежит в основе многих их применений в комбинаторике и в теоретической информатике.

Можно также заметить, что корни в лемме 3.7 могут быть и кратными (по определению, a — корень кратности k означает, что f делится на $(x-a)^k$ и не делится на $(x-a)^{k+1}$).

Теперь посмотрим, какие многочлены неприводимы над полем комплексных чисел $\mathbb{C}$.

Теорема 3.9 (основная теорема алгебры). *Всякий многочлен положительной степени над полем $\mathbb{C}$ имеет корень.*

Хотя эта теорема и называется основной теоремой алгебры, доказывать ее мы не будем, поскольку ее доказательство относится скорее к анализу, чем к алгебре. (Простое доказательство основной теоремы алгебры см., например, в [5].)

Из теоремы 3.9 и утверждения 3.6 вытекает, что над полем $\mathbb{C}$ неприводимы только многочлены первой степени. (Многочлен первой степени неприводим над любым полем, так как при умножении многочленов их степени складываются, а многочлены нулевой степени обратимы.)

Следующий пример — поле действительных чисел $\mathbb{R}$. Чтобы перейти от поля $\mathbb{C}$ к полю $\mathbb{R}$, заметим, что отображение $z \mapsto \bar{z}$, сопоставляющее каждому комплексному числу z сопряженное число $\bar{z}$, является изоморфизмом поля $\mathbb{C}$ на себя (автоморфизмом) и переводит поле $\mathbb{R}$ в себя. Отсюда вытекает, что для всякого $p \in \mathbb{C}[x]$ и всякого $\alpha \in \mathbb{C}$ имеет место формула:

$$\overline{p(\alpha)} = \bar{p}(\bar{\alpha}), \tag{3.2}$$

где $\bar{p}$ получается из p комплексным сопряжением коэффициентов. Пусть теперь $p \in \mathbb{R}[x] \subset \mathbb{C}[x]$ — многочлен степени > 1, не имеющий действительных корней (при наличии действительных корней p приводим). Многочлен p имеет комплексный корень α. Так как $p = \bar{p}$, то из формулы (3.2) получаем, что $p(\bar{\alpha}) = \bar{p}(\bar{\alpha}) = \overline{p(\alpha)} = \bar{0} = 0$. Из утверждения 3.6 получаем, что взаимно простые многочлены $x - \alpha$ и $x - \bar{\alpha}$ делят p. Но тогда p делится и на их произведение $q = (x - \alpha)(x - \bar{\alpha})$, которое принадлежит $\mathbb{R}[x]$.

Следовательно, над полем $\mathbb{R}$ неприводимы:

а) многочлены первой степени;

б) те многочлены второй степени, которые не имеют корней в $\mathbb{R}$ (многочлены с отрицательным дискриминантом).

Все прочие многочлены над $\mathbb{R}$ приводимы.

Гораздо сложнее обстоит дело с многочленами над полем рациональных чисел $\mathbb{Q}$. Мы ограничимся лишь тем, что докажем существование неприводимых над $\mathbb{Q}$ многочленов произвольной степени.

Если q — ненулевой многочлен с рациональными коэффициентами степени n, то, приводя коэффициенты к общему знаменателю, можно записать: $q = \alpha(a_0 + a_1 x + \cdots + a_n x^n) = = \alpha q_0$, где все коэффициенты a_i — целые числа, не имеющие нетривиального общего делителя, $a_n > 0$, $\alpha \in \mathbb{Q}$. Легко видеть, что многочлен q_0 и число α определены однозначно. Будем называть q_0 *примитивным многочленом*, соответствующим многочлену q.

Лемма 3.10 (Гаусс). $(uv)_0 = u_0 v_0$.

Доказательство. В сущности, нужно доказать, что если у каждого из многочленов $u_0, v_0 \in \mathbb{Z}[x]$ коэффициенты взаимно просты в совокупности, то у их произведения $u_0 v_0$ коэффициенты так же взаимно просты в совокупности. Для доказательства построим гомоморфизм кольца $\mathbb{Z}[x]$ на кольцо $GF(p)[x]$, который называется *редукцией многочлена* по модулю p. Редукция f_p многочлена f получается приведением по модулю p каждого из коэффициентов f. Посмотрев на формулы для суммы и произведения многочленов, видим, что редукция действительно является гомоморфизмом.

Предположим, что у коэффициентов $u_0 v_0$ есть общий простой делитель p. Тогда $(u_0 v_0)_p$ и для редукций по модулю p имеем $(u_0)_p (v_0)_p = 0$. Поскольку в кольце $GF(p)[x]$ нет делителей нуля (лемма 2.11), то одна из редукций $(u_0)_p$, $(v_0)_p$ равна 0. Это противоречит примитивности u_0, v_0. □

Таким образом, вопрос о приводимости многочлена над полем рациональных чисел сводится к вопросу о разложении на множители меньшей степени многочлена с целыми коэффициентами. В этом направлении имеется следующее достаточное условие неприводимости:

Теорема 3.11 (критерий Эйзенштейна). *Если для многочлена $q = a_0 + a_1 x + \cdots + a_n x^n$ с целыми коэффициентами существует такое простое число p, что $p \nmid a_n$, $p \mid a_i$ при $i = 0, \ldots, n-1$, $p^2 \nmid a_0$, то этот многочлен неприводим.*

Доказательство. Предположим, что q приводимый многочлен: $q = uv$. Тогда $q_p = u_p v_p$. По условию теоремы $q_p = a x^n$, $a \neq 0$. Значит, $u_p = b x^k$, $v_p = c x^m$, где $k < n$ и $m < n$. Поэтому все коэффициенты многочленов u и v, кроме старших, делятся на p, а тогда свободный член многочлена q, (т. е. a_0), равный $u_0 v_0$, делится на p^2, что противоречит условию. □

Пример 3.12. Многочлен $2x^4 - 6x^3 + 15x^2 + 21$ неприводим над полем $\mathbb{Q}$. Достаточно взять $p = 3$ и применить критерий Эйзенштейна.

Пример 3.13. Для всякого $n > 0$ многочлен $x^n - 2$ неприводим над $\mathbb{Q}$. Достаточно взять $p = 2$ и применить критерий Эйзенштейна. Отсюда вытекает, что над полем рациональных чисел существуют неприводимые многочлены любой степени.

Теперь перейдем к самому важному для нас случаю многочленов над полем $GF(p)$. Начнем с примеров.

Пример 3.14. Найдем все неприводимые многочлены степеней 2, 3, 4 над полем $GF(2)$. В этом поле есть два элемента 0 и 1, операции — сложение и умножение по модулю 2.

Вторая степень: $x^2 + ax + b$. Ясно, что $b \neq 0$, так как в противном случае имеется разложение на нетривиальные делители $x^2 + ax = x(x + a)$. Значит, неприводимый многочлен

степени 2 имеет вид $x^2 + ax + 1$. Поскольку многочленов первой степени всего два: x и $x + 1$, а делимость на первый мы уже исключили, то осталось исключить делимость на $x + 1$. Это делается аналогично предыдущему случаю: после замены $y = x+1$ остается проверить, что свободный член в разложении по степеням y не равен 0. Этот свободный член равен значению многочлена при $x = 1$ (в нашем поле $-1 = 1$). Поэтому получаем условие $1 + a + 1 \neq 0$, т. е. $a \neq 0$.

Итак, неприводимый многочлен степени 2 единственный: $x^2 + x + 1$.

Третья степень: $x^3 + ax^2 + bx + 1$ (свободный член не равен нулю, иначе имеем делитель x).

Исключим делимость на $x + 1$, получаем условие $a + b \neq 0$. Т. е. имеем два решения $a = 0$, $b = 1$ и $a = 1$, $b = 0$.

Соответственно, имеем два неприводимых многочлена степени 3:

$$x^3 + x^2 + 1,$$
$$x^3 + x + 1.$$

Для четвертой степени исключение делимости на x и $x + 1$ приводит к многочленам вида $x^4+ax^3+bx^2+cx+1$, $a+b+c = 1$ (напомним, что коэффициенты мы складываем по модулю 2). Всего есть 4 варианта, которые дают 3 решения:

a	b	c	многочлен	
0	0	1	$x^4 + x + 1$	
0	1	0	$x^4 + x^2 + 1$	приводимый
1	0	0	$x^4 + x^3 + 1$	
1	1	1	$x^4 + x^3 + x^2 + x + 1$	

Откуда взялся еще один приводимый многочлен? В таблице указаны многочлены, у которых нет делителей степени 1. Но многочлен 4-й степени может разлагаться в произведение двух неприводимых многочленов 2-й степени. Неприводимый многочлен 2-й степени единственный, поэтому получаем единственное исключение

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1$$

(для возведения в степень, равную характеристике поля, у нас есть простая формула (3.1)).

Используя неприводимые многочлены, можно строить конечные поля.

Рассмотрим поле $GF(p) = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$, с операциями сложения и умножения по модулю простого числа p. Возьмем многочлен n-й степени

$$P(x) = a_n x^n + \cdots + a_1 x + a_0$$

с коэффициентами из этого поля ($a_i \in GF(p)$, $0 \leqslant i \leqslant n$), неприводимый над полем $GF(p)$. Разложим кольцо многочленов над полем $GF(p)$ по идеалу, порожденному $P(x)$. Получим совокупность остатков от деления на $P(x)$, которая образует поле (поскольку кольцо многочленов евклидово, идеал $(P(x))$ — максимальный). Элементы этого поля будем обозначать $\{r(x)\} = \{f \in GF(p)[x] \mid f(x) = r(x) + Q(x)P(x), Q \in GF(p)[x]\}$.

Построенное поле является полем Галуа, т. е. в нем содержится конечное число элементов. Действительно, разных элементов этого поля, т. е. классов вычетов, имеется столько же, сколько есть разных остатков от деления на $P(x)$. А в остатке от деления на $P(x)$ может быть любой многочлен степени не выше $n-1$. Такой многочлен можно записать как $b_0+b_1x+\ldots+ +b_{n-1}x^{n-1}$, где в качестве коэффициентов можно подставлять любые элементы поля $GF(p)$. Поэтому число элементов равно p^n. Соответствующее поле Галуа называется расширением n-й степени поля $GF(p)$ и обозначается $GF(p^n)$. Обратите внимание на то, что в этом обозначении не используется многочлен $P(x)$, с помощью которого мы построили поле. Это не случайно. Верна следующая теорема.

Теорема 3.15. *Любое конечное поле изоморфно какому-нибудь полю Галуа $GF(p^n)$. Любые два поля, содержащие p^n элементов, изоморфны.*

Теорема 3.16. *Для любой степени n и для любого простого p существует неприводимый полином степени n над $GF(p)$.*

Эти две теоремы в совокупности полностью описывают все конечные поля. Другими словами их можно сформулировать так: любое поле содержит p^n элементов, где p — простое, и для каждого простого p и натурального n есть ровно одно (с точностью до изоморфизма) поле $GF(p^n)$.

Доказательства этих теорем приводятся ниже. Сейчас заметим только, что нам потребуется строить поля расширением не только простого поля вычетов $GF(p)$, но и произвольного конечного поля. Конструкция такого расширения дословно совпадает с приводимой выше конструкцией расширения поля $GF(p)$.

3.4. Линейная алгебра над конечным полем

Начнем с того, что введем векторные пространства над конечным полем.

Абстрактное *векторное пространство* можно определить над любым полем F. Это множество V, на котором заданы следующие операции: сложение $+\colon V \times V \to V$ и умножение на «число» $F \times V \to V$. Свойства этих операций таковы (здесь мы обозначаем элементы поля греческими буквами, а элементы векторного пространства — латинскими, умножение на число обозначаем точкой $\cdot$, хотя почти всегда в дальнейшем точка будет опускаться):

L1: V — коммутативная группа по сложению;

L2: $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$, $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$ (дистрибутивность);

L3: $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$ (композиция умножений на два числа совпадает с умножением на произведение этих чисел);

L4: $1 \cdot v = v$.

Нулевой вектор (единичный элемент в группе сложения векторного пространства) будем обозначать 0.

Пример 3.17. Пусть $V = F^n$ — множество последовательностей длины n, составленных из элементов поля F. Сложение и умножение на число определим покомпонентно: для $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\tilde{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$, где $\alpha_i \in F$, $\beta_i \in F$,

по определению имеем

$$\tilde{\alpha} + \tilde{\beta} = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n),$$
$$\alpha \cdot \tilde{\alpha} = (\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n).$$

Легко проверить выполнение всех свойств из определения векторного пространства.

Построенное в этом примере пространство называется *n-мерным координатным пространством над полем F*.

Аналогично случаю колец (см. выше), из определения векторного пространства сразу следует дистрибутивность относительно вычитания: $\alpha \cdot v - \beta \cdot v = (\alpha - \beta) \cdot v$, так как

$$(\alpha - \beta) \cdot v + \beta \cdot v = (\alpha - \beta + \beta) \cdot v = \alpha \cdot v.$$

Отсюда получаем, что $0 \cdot v = 0$, так как

$$0 \cdot v = (1 - 1) \cdot v = v - v = 0,$$

и $-v = (-1) \cdot v$ так как

$$v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 - 1) \cdot v = 0 \cdot v = 0.$$

Множество векторов V' векторного пространства V назовем *порождающим*, если каждый вектор пространства является *линейной комбинацией* векторов из V', т. е. для любого $v \in V$ справедливо равенство вида

$$v = \sum_{i=1}^{m} \alpha_i v_i, \quad \alpha_i \in F,\ v_i \in V'.$$

Пространство V называется *конечномерным*, если в нем существует конечное порождающее множество.

Множество векторов V' называется *линейно независимым*, если из $\sum_{i=1}^{k} \alpha_i v_i = 0$, где $\alpha_i \in F$, $v_i \in V$, следует, что $\alpha_i = 0$ для всех i.

Совокупность векторов V' называется *базисом*, если она одновременно является и порождающим, и линейно независимым множеством.

Легко понять, что базис существует в любом конечномерном векторном пространстве V. Выберем какое-нибудь конечное порождающее множество V'. Среди подмножеств V', которые являются порождающими для V, выберем минимальное

по включению подмножество B. Это и будет базис. Действительно, если

$$\sum_{i=1}^{k} \alpha_i b_i = 0, \quad \alpha_i \in F,\ \alpha_j \neq 0,\ v_i \in B,$$

то $B \setminus \{b_j\}$ также порождающее: для любого $v \in V$ имеем

$$v = \sum_{i=1}^{m} \beta_i b_i = \sum_{i \neq j} \beta_i b_i - \frac{\beta_j}{\alpha_j} \sum_{i \neq j} \alpha_i b_i = \sum_{i \neq j} \left(\beta_i - \alpha_i \frac{\beta_j}{\alpha_j} \right) b_i.$$

Это противоречит минимальности.

Утверждение 3.18. *Каждый элемент конечномерного векторного пространства однозначно представляется в виде линейной комбинации элементов базиса.*

Доказательство. Действительно, если есть два представления в виде линейной комбинации векторов из базиса

$$v = \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \beta_i v_i,$$

то, вычитая одну из другой, получаем

$$0 = v - v = \sum_{i=1}^{n} \alpha_i v_i - \sum_{i=1}^{n} \beta_i v_i = \sum_{i=1} (\alpha_i v - \beta_i v) = \sum_{i=1}^{n} (\alpha_i - \beta_i) v.$$

По определению линейной независимости отсюда следует, что для всех i выполняется равенство $\alpha_i - \beta_i = 0$, т. е. $\alpha_i = \beta_i$. $\square$

Таким образом, каждому элементу векторного пространства с конечным базисом однозначно соответствует набор коэффициентов разложения по этому базису

$$v \leftrightarrow (\alpha_1, \ldots, \alpha_n).$$

Если ввести понятие изоморфизма векторных пространств аналогично изоморфизмам групп и колец (биекция, сохраняющая операции), то можно сказать, что разложение по базису задает изоморфизм между конечномерным пространством V и координатным пространством F^n.

Теорема 3.19. *Число элементов в любых двух базисах конечномерного пространства одинаково.*

Другими словами, координатные пространства F^n и F^m неизоморфны при $n \neq m$.

По теореме 3.19 число элементов в базисе не зависит от выбора базиса и называется *размерностью* пространства.

Мы выведем теорему 3.19 из следующей леммы, использующей понятие эквивалентных систем векторов. Две системы векторов $y_1, \ldots, y_l \in V$ и $z_1, \ldots, z_m \in V$ назовем *эквивалентными*, если каждый вектор одной из систем выражается в виде линейной комбинации векторов из второй системы. Ясно, что это действительно отношение эквивалентности: подставив в линейную комбинацию вместо векторов одной системы их выражения в виде линейных комбинаций векторов другой системы, можно раскрыть скобки, привести подобные и получить линейную комбинацию векторов второй системы. Отсюда вытекает транзитивность. Симметричность и рефлексивность очевидны из определения.

Лемма 3.20 (лемма о замене). *Пусть $y_1, \ldots, y_l$ — система из линейно независимых векторов и все векторы y_i выражаются как линейные комбинации векторов системы $z_1, \ldots, z_m$. Тогда существует эквивалентная системе $z_1, \ldots, z_m$ система, содержащая $y_1, y_2, \ldots, y_l$ и какие-то $m - l$ векторов из системы $z_1, \ldots, z_m$.*

Следствием этой леммы является неравенство $l \leqslant m$. К двум базисам лемму о замене можно применять в две стороны (так как любые векторы выражаются в виде линейной комбинации векторов из базиса, и базисные векторы линейно независимы). Поэтому получаем два неравенства $l \leqslant m$, $m \leqslant l$, т. е. $m = l$. Но это и есть утверждение теоремы.

Значит, осталось доказать лемму о замене.

Доказательство леммы о замене. Будем доказывать индукцией по l.

База индукции: $l = 1$. Условие леммы означает, что

$$y_1 = \sum_{i=1}^{m} \alpha_i z_i, \tag{3.3}$$

причем не все коэффициенты равны 0 (поясним на всякий случай: система из одного вектора 0 является по определению

линейно зависимой). Считаем без ограничения общности, что первый коэффициент α_1 не равен 0. Тогда

$$-\alpha_1 z_1 = -y_1 + \sum_{i=2}^{m} \alpha_i v_i, \quad \text{т. е.} \quad z_1 = \alpha_1^{-1} y_1 + \sum_{i=2}^{m} (-\alpha_1^{-1}\alpha_i) z_i. \tag{3.4}$$

Системы $y_1, z_2, \ldots, z_m$ и $z_1, z_2, \ldots, z_m$ в силу (3.3) и (3.4) эквивалентны.

Индуктивный переход. Пусть лемма доказана для $l < s$. Рассмотрим линейно независимую систему $y_1, \ldots, y_s$. Ее подсистема $y_1, \ldots, y_{s-1}$ также линейно независима. Поэтому, перенумеровав векторы в системе $z_1, \ldots, z_m$), можно считать, что системы $y_1, \ldots, y_{s-1}, z_s, \ldots, z_m$ и $z_1, \ldots, z_m$ эквивалентны. Но тогда

$$y_s = \sum_{i=1}^{s-1} \alpha_i y_i + \sum_{i=s}^{m} \beta_i z_i, \tag{3.5}$$

причем хотя бы один из коэффициентов β_i отличен от нуля (иначе из (3.5) получалась бы линейная зависимость между векторами системы $y_1, \ldots, y_s$). Можно без ограничения общности предположить, что $\beta_s \neq 0$. Тогда

$$z_s = \beta_s^{-1} y_s + \sum_{i=1}^{s-1} (-\beta_s^{-1}\alpha_i) y_i + \sum_{i=s+1}^{m} (-\beta_s^{-1}\beta_i) z_i. \tag{3.6}$$

Системы $y_1, \ldots, y_{s-1}, z_s, \ldots, z_m$ и $y_1, \ldots, y_s, z_{s+1}, \ldots, z_m$ в силу (3.5) и (3.6) эквивалентны. Значит, эквивалентны и системы $y_1, \ldots, y_s, z_{s+1}, \ldots, z_m$ и $z_1, \ldots, z_m$. □

Пример 3.21. Многочлены степени не выше d с коэффициентами из поля F образуют линейное пространство над полем F размерности $d+1$. Очевидно, что многочлены 1, x, x^2, …, x^d образуют базис в этом пространстве. Но можно указать и другие интересные базисы для пространства многочленов. В частности, если в поле F больше d элементов, то для любого набора $a_0, \ldots, a_d$ из различных элементов поля существуют такие многочлены $f_0, \ldots, f_d$, что $f_i(a_i) = 1$ и $f_i(a_j) = 0$ при $i \neq j$. Многочлены $f_0, \ldots, f_d$ образуют базис. Действительно, многочлен $f = \sum_{i=0}^{d} \alpha_i f_i = 0$ принимает в каждой точке a_i значение α_i. Поэтому линейная зависимость между такими

многочленами $\alpha_0 f_0 + \alpha_1 f_1 + \cdots + \alpha_d f_d = 0$ означает, что все α_i равны 0.

Выпишем явно выражения для многочленов f_i:

$$f_0 = \frac{(x-a_1)(x-a_2)\dots(x-a_d)}{(a_0-a_1)(a_0-a_2)\dots(a_0-a_d)},$$
$$f_1 = \frac{(x-a_0)(x-a_2)\dots(x-a_d)}{(a_1-a_0)(a_1-a_2)\dots(a_1-a_d)},$$
$$\dots,$$
$$f_d = \frac{(x-a_0)(x-a_1)\dots(x-a_{d-1})}{(a_d-a_0)(a_d-a_1)\dots(a_d-a_{d-1})}$$

Коэффициенты разложения многочлена f по этому базису равны значениям многочлена в точках $a_0, \dots, a_d$, а само разложение по этому базису называется *интерполяционной формулой Лагранжа*:

$$f = \sum_{i=0}^{d} f(a_i) f_i \ . \tag{3.7}$$

Как следствие, получаем, что многочлен степени d над полем F однозначно определяется своими значениями, если $|F| > d$. В частности, над любым бесконечным полем кольцо функций, представимых многочленами, изоморфно кольцу многочленов над этим полем, определенному как в разделе 2.2.

Замечание 3.22. Можно доказать и обратное: если в поле не более d элементов, то некоторый многочлен степени не выше d тождественно равен 0, см. ниже следствие 3.36.

Применим теперь линейную алгебру к изучению конечных полей.

Лемма 3.23. *Поле характеристики p является векторным пространством над полем $GF(p)$.*

Операция сложения в поле дает операцию сложения в векторном пространстве. Как уже показано, поле F характеристики p содержит подполе кратных 1, изоморфное $GF(p)$. Это позволяет определить умножение элементов F («векторов»)

на элементы $GF(p)$ («числа») как умножение в поле F. Аксиомы векторного пространства выполняются в силу свойств арифметических операций в поле.

Следствие 3.24. *В конечном поле p^n элементов, p — простое, n — натуральное.*

Теперь рассмотрим поле $GF(p^n)$, построенное как кольцо вычетов по модулю некоторого неприводимого многочлена $f(x)$ степени n над $GF(p)$. Мы описали элементы этого поля с помощью многочленов степени $n-1$ с коэффициентами из $GF(p)$: элемент $\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}\}$ поля $GF(p^n)$ соответствует тому классу вычетов, в который входят многочлены, дающие при делении на $f(x)$ остаток $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$.

Теорема 3.25. *Элементы $\{1\}$, $\{x\}$, …, $\{x^{n-1}\}$ образуют базис $GF(p^n)$.*

В частности, $GF(p^n)$ — векторное пространство размерности n над полем $GF(p)$.

Доказательство. Любой остаток представим в виде линейной комбинации указанных векторов:

$$\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}\} = a_0\{1\} + a_1\{x\} + \cdots + a_{n-1}\{x^{n-1}\}.$$

И обратно, пусть

$$b_0\{1\} + b_1\{x\} + \cdots + b_{n-1}\{x^{n-1}\} = 0.$$

Это означает, что многочлен $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ делится на многочлен n-й степени $f(x)$. Поскольку при умножении ненулевых многочленов их степени складываются, это возможно лишь при $b_0 + b_1x + \cdots + b_{n-1}x^{n-1} = 0$. Значит, система $\{1\}$, $\{x\}$, …, $\{x^{n-1}\}$ линейно независима. □

Замечание 3.26. Разумеется, построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных в этом разделе теорем справедливы не только в случае конечных полей. Например, возьмем поле действительных чисел и неприводимый над $\mathbb{R}$ многочлен $x^2 + 1$. Построим поле $\mathbb{R}/(x^2+1)$, оно является векторным пространством над $\mathbb{R}$. Элементы $\{1\}$, $\{x\}$ образуют базис этого пространства. Значит, каждый элемент можно представить

в виде $a\{1\} + b\{x\}$. Легко проверить, что полученное поле изоморфно полю комплексных чисел $\mathbb{C}$, один из возможных изоморфизмов задается соответствием $1 \mapsto 1$, $\{x\} \mapsto i$.

Лемма 3.27. *Если поле $GF(p^n)$ содержит поле $GF(p^k)$, то k делит n.*

Доказательство. Аналогично доказательству леммы 3.23. Если $F_1 \subset F_2$, то элементы F_2 можно умножать на элементы из F_1, а также складывать. Поэтому F_2 является векторным пространством над полем F_1 размерности d. Значит, в нем $|F_1|^d$ элементов. Таким образом $p^n = (p^k)^d$, что и означает делимость n на k. □

Замечание 3.28. Справедливо и обращение леммы 3.27. Оно следует из единственности поля $GF(p^n)$ (см. ниже раздел 3.8) и существования неприводимого многочлена степени k над любым конечным полем (см. второе доказательство теоремы 3.16 на с. 159).

3.5. Корни многочленов над конечным полем

Теперь будем решать уравнения в конечном поле. Рассмотрим поле $GF(p^n)$, а в нём — какой-нибудь элемент β, и будем интересоваться многочленами, для которых этот элемент является корнем.

Определение 3.29. Многочлен $m(x)$ называется *минимальной функцией* для β, если $m(x)$ — нормированный[1)] многочлен минимальной степени, для которого β является корнем.

Другими словами, должны выполняться три свойства:

а) $m(\beta) = 0$;

б) $f(\beta) \neq 0$ при $f(x) \neq 0$, $\deg f(x) < \deg m(x)$;

в) коэффициент при старшей степени в $m(x)$ равен 1.

[1)] У нормированного многочлена старший коэффициент равен 1. Всякий многочлен можно нормировать, умножив его на обратный к старшему коэффициенту, при этом множество корней не изменяется.

Пример 3.30. Пусть поле представлено как кольцо классов вычетов по модулю неприводимого многочлена $a(x) = a_0 + \\ + a_1 x + \cdots + a_n x^n$. Для класса вычетов $\{x\}$ полином $a_n^{-1} a(x)$ является минимальной функцией. Действительно, $\{x\}$ является его корнем:

$$a_0\{1\} + a_1\{x\} + \cdots + a_n\{x\}^n = \{a_0 + a_1 x + \cdots + a_n x^n\} = \{0\},$$

т. е. $\{x\}$ — корень $a(x)$, но тогда $\{x\}$ является корнем и $a_n^{-1} a(x)$. Докажем минимальность. Предположим, что существует многочлен $b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$, для которого

$$b_0\{1\} + b_1\{x\} + \cdots + b_{n-1}\{x\}^{n-1} = \\ = b_0\{1\} + b_1\{x\} + \cdots + b_{n-1}\{x^{n-1}\} = \{0\}.$$

Это равенство задает линейную зависимость между $\{1\}$, $\{x\}$, $\{x^2\}$, $\ldots \{x^{n-1}\}$, которые образуют базис поля как векторного пространства над $GF(p)$. Поэтому все $b_i = 0$.

Приведем несколько простых свойств минимальных функций.

Утверждение 3.31. *$m(x)$ — неприводимый многочлен.*

Доказательство. Предположим, что $m(x) = m_1(x)\, m_2(x)$, причем $\deg m_i(x) > 0$, поскольку многочлены нулевой степени — константы — образуют группу обратимых элементов в кольце многочленов над полем. Но $m(\beta) = 0$, поэтому хотя бы один из множителей $m_1(\beta)$ или $m_2(\beta)$ также должен равняться нулю (в поле делителей нуля нет). Значит, один из сомножителей имеет корень β, а его степень меньше степени $m(x)$. Это противоречит минимальности $m(x)$. □

Утверждение 3.32. *Пусть $m(x)$ — минимальная функция для β, и β также является корнем многочлена $f(x)$. Тогда $f(x)$ делится на $m(x)$.*

Доказательство. Разделим $f(x)$ на $m(x)$ с остатком: $f(x) = \\ = u(x)m(x) + v(x)$, $\deg v < \deg m$. Подставляя в это равенство β, получаем $0 = f(\beta) = u(\beta)m(\beta) + v(\beta) = v(\beta)$. Т. е. β является корнем $v(x)$, что противоречит минимальности $m(x)$. □

Следствие 3.33. *Для каждого β есть ровно одна минимальная функция.*

Действительно, пусть минимальных функций две. Они взаимно делят друг друга, а значит, различаются на обратимый множитель (константу). Поскольку минимальная функция нормирована, эта константа равна 1, т. е. функции совпадают.

Утверждение 3.34. *Для каждого $\beta \in GF(p^n)$ существует минимальная функция и ее степень не превосходит n.*

Доказательство. Рассмотрим следующие элементы поля: 1, β, β^2, …, β^n, их $n+1$ штука, а размерность $GF(p^n)$ как векторного пространства над $GF(p)$ равна n. Значит, эти элементы линейно зависимы, т. е. существуют такие коэффициенты $c_0, \ldots, c_n$, что

$$c_0 + c_1\beta + \cdots + c_n\beta^n = 0.$$

Следовательно, β — корень многочлена $c_0+c_1x+\cdots+c_nx^n$. Значит, минимальной функцией для β какой-нибудь будет нормированный неприводимый делитель этого многочлена. □

Теорема 3.35. *Любой ненулевой элемент поля $GF(p^n)$ является корнем многочлена $x^{p^n-1}-1$.*

Доказательство. Ненулевые элементы поля образуют группу по умножению, порядок этой группы равен p^n-1. Порядок любого элемента (т. е. порядок циклической подгруппы, порожденной этим элементом) по теореме Лагранжа делит порядок группы. Возьмем произвольный элемент α, обозначим его порядок через k. Тогда $p^n-1 = kq$, $\alpha^k = 1$, откуда получаем

$$\alpha^{p^n-1} - 1 = \alpha^{kq} - 1 = (\alpha^k)^q - 1 = 1^q - 1 = 0. \qquad \square$$

Следствие 3.36. *Все элементы поля $GF(p^n)$, не исключая нуля, являются корнями многочлена $x^{p^n} - x$.*

Доказательство. Вынесем x за скобку:

$$x^{p^n} - x = x(x^{p^n-1} - x).$$

У правого множителя корнями будут все ненулевые элементы, а у левого — 0. □

Теорема 3.37. *Многочлен $x^n - 1$ делится на $x^m - 1$ тогда и только тогда, когда n делится на m.*

Доказательство. Пусть $n = mk$. Сделаем замену переменных: $x^m = y$. Тогда $x^n - 1 = y^k - 1$, а $x^m - 1 = y - 1$. Делимость очевидна, поскольку 1 является корнем $y^k - 1$.

Предположим, что n не делится на m, т. е. $n = km + r$, $0 < r < m$. Запишем тождество

$$x^n - 1 = \frac{x^r(x^{mk} - 1)(x^m - 1)}{x^m - 1} + x^r - 1 = \\ = \frac{x^r(x^{mk} - 1)}{x^m - 1}(x^m - 1) + x^r - 1.$$

Последнее выражение задает результат деления $x^n - 1$ на $x^m - 1$ с остатком, поскольку $x^{mk} - 1$ делится на $x^m - 1$ по доказанному выше. Остаток $x^r - 1 \neq 0$ в силу сделанных предположений. Поэтому в этом случае $x^n - 1$ не делится на $x^m - 1$. □

Эта теорема дает нам возможность раскладывать некоторые многочлены $x^n - 1$. Например, пусть мы работаем в характеристике 2 (где $+1 = -1$), разложим $x^{15} + 1$:

$$x^{15} + 1 = (x^3 + 1)(x^{12} + x^9 + x^6 + x^3 + 1).$$

Продолжить это разложение помогает следующая теорема.

Теорема 3.38. *Все неприводимые многочлены n-й степени над $GF(p)$ являются делителями $x^{p^n} - x$.*

Доказательство. Если $n = 1$, то нужно проверить, что $x - a$, где $a \in GF(p)$, является делителем $x^p - x$. Это очевидно при $a = 0$. В остальных случаях нужно проверить, что a — корень многочлена $x^{p-1} - 1$, что уже сделано выше в теореме 3.35.

При $n > 1$ строим по неприводимому многочлену $f(x)$ степени n поле $GF(p^n)$. Тогда многочлен $f(x)$ имеет в $GF(p^n)$ корень $\{x\}$ и, более того, нормированный $f(x)$ является минимальной функцией для $\{x\}$, поскольку степени $\{x\}$ образуют базис в $GF(p^n)$. С другой стороны, $\{x\}$ является корнем уравнения $x^{p^n-1} - 1$. По утверждению 3.32 о минимальной функции многочлен $x^{p^n-1} - 1$ делится на $f(x)$. □

Используя эту теорему, мы можем завершить разложение $x^{15} - 1$:

$$x^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Теорема 3.39. *Любой неприводимый делитель многочлена* $x^{p^n-1}-1$ *имеет степень, не превосходящую* n.

Доказательство. Пусть φ — неприводимый многочлен степени k, который является делителем $x^{p^n}-x$. Кратные φ образуют максимальный идеал в кольце $GF(p)[x]$, поэтому кольцо вычетов по этому идеалу является полем. Поле можно рассматривать как векторное пространство над $GF(p)$, базисом этого пространства является набор степеней $\{1\}$, $\{x\}$, $\ldots$, $\{x^{k-1}\}$. Далее будем обозначать $\{x\}=\alpha$. Поскольку $x^{p^n}-x$ делится на φ, то в кольце вычетов по модулю идеала (φ) получаем $\alpha^{p^n}-\alpha=0$.

Любой элемент построенного поля есть линейная комбинация базисных элементов:

$$\beta = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}.$$

Возведем и левую, и правую части этого равенства в степень p^n, получим

$$\begin{aligned}\beta^{p^n} &= (a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1})^{p^n} = \\ &= a_0^{p^n} + a_1^{p^n}\alpha^{p^n} + \cdots + a_{k-1}^{p^n}(\alpha^{k-1})^{p^n} = \\ &= a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1} = \beta.\end{aligned}$$

Отсюда получаем соотношение $\beta^{p^n}-\beta=0$, значит, β — корень уравнения $x^{p^n}-x=0$. Но у этого уравнения не более чем p^n различных корней, а в построенном нами поле — p^k элементов. Каждый элемент поля является корнем, следовательно $p^n \geqslant p^k$, т. е. $n \geqslant k$. □

Утверждение 3.40. *Пусть некоторый элемент* β *конечного поля имеет порядок* ℓ, *а минимальная функция* $m(x)$ *этого элемента имеет степень* k. *Тогда* p^k-1 *делится на* ℓ, *а если* $r<k$, *то* p^r-1 *не делится на* ℓ.

Доказательство. По сути это прямое следствие только что доказанной теоремы.

По неприводимому многочлену k-й степени $m(x)$ можно построить поле из p^k элементов. Ненулевые элементы этого поля, в том числе и β, являются корнями уравнения $x^{p^k-1}-1=0$,

т. е. $\beta^{p^k-1} - 1 = 0$, $\beta^{p^k-1} = 1$. Это доказывает первую часть утверждения.

Вторая часть доказывается от противного. Предположим, что $p^r - 1$ делится на ℓ и $r < k$. Тогда β — корень уравнения $x^{p^r} - 1 = 0$. Так как $m(x)$ — минимальная функция для β, то $x^{p^r} - 1$ делится на $m(x)$ (утверждение 3.32). Получается, что мы нашли неприводимый делитель многочлена $x^{p^r} - 1$ степени k. Но $k > r$, что противоречит доказанной выше теореме 3.39. □

Следующая теорема нужна нам для того, чтобы раскладывать многочлены на множители.

Теорема 3.41. *Пусть $\beta \in GF(p^n)$ — корень неприводимого многочлена $\varphi(x)$ степени n с коэффициентами из $GF(p)$. Тогда β, β^p, …, $\beta^{p^{n-1}}$ все различны и исчерпывают список корней этого многочлена.*

Т. е. чтобы получить все корни неприводимого многочлена, достаточно найти один из них и возводить его последовательно в степень p.

Доказательство. Вначале докажем, что если β — корень $\varphi(x)$, то β^p — тоже корень.

Как было показано выше, $a^p = a$ для всех $a \in GF(p)$. Поэтому для любого многочлена $f(x)$ с коэффициентами из $GF(p)$ выполняется равенство

$$f(x)^p = f(x^p). \tag{3.8}$$

Действительно, возведение в степень p сохраняет операции сложения и умножения (см. выше раздел 3.2). Поэтому

$$(a_0 + a_1x + \cdots + a_kx^k)^p = a_0^p + a_1^px^p + a_2^px^{2p} + \cdots + a_k^px^{kp} = \\ = a_0 + a_1(x^p) + a_2(x^p)^2 + \cdots + a_k(x^p)^k.$$

Если $\varphi(\beta) = 0$, то и $\varphi(\beta)^p = 0$. Из (3.8) получаем, что и $\varphi(\beta^p) = 0$.

Итак, мы доказали, что β, β^p, …, $\beta^{p^{n-1}}$ — корни многочлена $\varphi(x)$. Осталось доказать, что они все различны, тогда из леммы 3.7 будет следовать, что мы нашли все корни многочлена $\varphi(x)$.

Предположим, что $\beta^{p^\ell} = \beta^{p^k}$, причем без ограничения общности $\ell \leqslant k$. Мы знаем, что $\beta^{p^n} = \beta$. С другой стороны, поскольку

$$\beta^{p^n} = \beta^{p^k \cdot p^{n-k}} = \left(\beta^{p^k}\right)^{p^{n-k}} = \left(\beta^{p^\ell}\right)^{p^{n-k}} = \beta^{p^{n-k+\ell}},$$

то β — корень уравнения $x^{p^{n-k+\ell}-1} - 1 = 0$. Из теоремы 3.38 получаем $n - k + \ell \geqslant n$, так что $\ell \geqslant k$. Другими словами, $\ell = k$ и все выписанные выше корни различны. □

Пример 3.42. Рассмотрим $GF(2)$ и неприводимый над этим полем многочлен четвертой степени x^4+x^3+1. Найдем его корни. Для этого строим расширение $GF(2^4)$ как кольцо вычетов по модулю идеала, образованного всеми кратными этого многочлена. Один корень получаем немедленно: $\{x\}$. Теперь по теореме 3.41 можно выписать остальные: $\{x^2\}$, $\{x^4\} = \{x^3+1\}$, $\{x^8\} = \{x^6+1\} = \{x^3+x^2+x\}$, так как $\{x^5\} = \{x^4+x\} = \{x^3+x+1\}$, $\{x^6\} = \{x^4+x^2+x\} = \{x^3+1+x^2+x\}$.

Таким образом, если мы решаем уравнение $f(x) = 0$, где f — неприводимый многочлен, то нужно построить по идеалу (f) поле. Первый корень есть сразу, это $\{x\}$. Остальные получаются применением теоремы 3.41. В общем случае для решения уравнения нужно уметь раскладывать многочлен на неприводимые множители.

3.6. Мультипликативная группа поля

Если в поле Галуа убрать нулевой элемент, то остальные элементы по умножению образуют группу, которая называется мультипликативной группой поля. Оказывается, что это не просто коммутативная группа, а циклическая группа. Другими словами, в ней есть порождающий элемент, и все остальные получаются возведением в степень этого порождающего.

Пример 3.43. Возьмем поле $GF(2)$ и его расширение четвертой степени. Как сказано выше (но пока не доказано), расширение четвертой степени можно строить с помощью любого из трех неприводимых многочленов. Удобнее всего это сделать, если взять многочлен $x^4 + x + 1$. Будем задавать элементы

степень α	$1,\ x, x^2, x^3$
$\alpha =$	$(0,\ 1,\ 0,\ 0)$
$\alpha^2 =$	$(0,\ 0,\ 1,\ 0)$
$\alpha^3 =$	$(0,\ 0,\ 0,\ 1)$
$1 + \alpha = \alpha^4 =$	$(1,\ 1,\ 0,\ 0)$
$\alpha + \alpha^2 = \alpha^5 =$	$(0,\ 1,\ 1,\ 0)$
$\alpha^2 + \alpha^3 = \alpha^6 =$	$(0,\ 0,\ 1,\ 1)$
$\alpha^3 + \alpha + 1 = \alpha^3 + \alpha^4 = \alpha^7 =$	$(1,\ 1,\ 0,\ 1)$
$1 + \alpha^2 = \alpha + 1 + \alpha^2 + \alpha = \alpha^8 =$	$(1,\ 0,\ 1,\ 0)$
$\alpha + \alpha^3 = \alpha^9 =$	$(0,\ 1,\ 0,\ 1)$
$\alpha^2 + 1 + \alpha = \alpha^2 + \alpha^4 = \alpha^{10} =$	$(1,\ 1,\ 1,\ 0)$
$\alpha + \alpha^2 + \alpha^3 = \alpha^{11} =$	$(0,\ 1,\ 1,\ 1)$
$1 + \alpha + \alpha^2 + \alpha^3 = \alpha^2 + \alpha^3 + \alpha^4 = \alpha^{12} =$	$(1,\ 1,\ 1,\ 1)$
$1 + \alpha^2 + \alpha^3 = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = \alpha^{13} =$	$(1,\ 0,\ 1,\ 1)$
$1 + \alpha^3 = \alpha + \alpha^3 + \alpha^4 = \alpha^{14} =$	$(1,\ 0,\ 0,\ 1)$
$1 = \alpha + \alpha^4 = \alpha^{15} =$	$(1,\ 0,\ 0,\ 0)$

Таблица 3.1. Мультипликативная группа поля $GF(2^4)$.

расширения наборами коэффициентов многочлена, который получается в остатке при делении на $x^4 + x + 1$, записывая их в порядке возрастания степеней.

Порождающим является элемент $\alpha = x$, который в силу нашего соглашения записывается как $(0, 1, 0, 0)$. Посчитаем последовательность степеней α. Результаты вычислений приведены в таблице 3.1.

Имея такую таблицу, очень просто производить умножение:

$$(x^3 + x + 1) \cdot (x^2 + x + 1) = x^2,$$
$$(1, 1, 0, 1) \cdot (1, 1, 1, 0) = (0, 0, 1, 0),$$
$$\alpha^7 \alpha^{10} = \alpha^{17} = \alpha^2.$$

Теорема 3.44. *Мультипликативная группа любого конечного поля циклическая.*

Для доказательства этой теоремы нам потребуется дополнительная лемма о конечных абелевых группах.

Лемма 3.45. *Пусть m — максимальный порядок элемента в конечной абелевой группе G. Тогда порядок любого элемента G делит m.*

Доказательство. Группа G по теореме 1.79 однозначно разлагается в прямую сумму примарных компонент — циклических групп, порядки которых являются степенями простых чисел. Для каждого простого делителя p_i порядка группы найдем примарную компоненту $\langle a\rangle \cong C_{p^{k_i}}$ максимального порядка p^{k_i}. Обозначим произведение чисел p^{k_i} через M. По построению любого $x \in G$ выполняется $x^M = e$, т. е. порядок x делит M. С другой стороны, произведение всех порождающих выбранных примарных компонент $a_1 a_2 \dots$ имеет порядок M, поскольку наименьшее общее кратное взаимно простых чисел равно произведению этих чисел. Поэтому $m = M$. □

Доказательство теоремы 3.44. Пусть m — максимальный порядок элемента в мультипликативной группе поля.

По доказанной выше лемме 3.45, каждый ненулевой элемент поля является корнем уравнения $x^m = 1$. Но у многочлена степени m не более m корней. Поэтому m равен числу ненулевых элементов поля. Но это и означает, что мультипликативная группа поля циклическая: существует такой элемент, что его порядок совпадает с порядком группы (и тогда все элементы группы являются степенями этого элемента). □

Мультипликативная группа простого поля характеристики p обозначается $GF(p)^*$. Ее порождающие элементы *первообразными корнями по модулю p*. Найдем наименьшие первообразные корни по модулям некоторых простых чисел.

$p = 2$. Группа $GF(p)^*$ состоит из одного элемента $\bar{1}$, он же является первообразным корнем.

$p = 3$. Первообразный корень $\bar{2}$ — единственный неединичный элемент $GF(p)^*$.

$p = 5$. Поскольку $(\bar{2})^2 = \bar{4}$, порядок $\bar{2}$ равен 4. Других вариантов нет, поскольку порядок элемента — делитель порядка группы. Значит, $\bar{2}$ — первообразный корень.

$p = 7$. Снова $(\bar{2})^2 = \bar{4} \neq \bar{1}$. Но у $p-1 = 6$ есть еще один делитель 3, а $(\bar{2})^3 = \bar{8} = \bar{1}$. Поэтому порядок $\bar{2}$ равен 3. Поскольку $(\bar{3})^2 = \bar{9} \neq \bar{1}$, $(\bar{3})^3 = \overline{27} \neq \bar{1}$, $\bar{3}$ — первообразный корень.

Вычисления можно продолжить. Приведем небольшую таблицу первообразных корней.

модуль p	3	5	7	11	13	17	19	23	29	31	37	41
первообразный корень mod p	$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{2}$	$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{2}$	$\bar{7}$

3.7. Существование поля из p^n элементов

Теперь можно вернуться к вопросу о существовании конечного поля заданного размера. В этом разделе мы всюду полагаем $q = p^n$, где p — простое. Мы докажем существование поля из q элементов, откуда будет следовать и теорема 3.16 о существовании неприводимого многочлена степени n над полем $GF(p)$. Более того, мы это сделаем двумя способами. Вначале докажем существование поля из p^n элементов, откуда выведем существование неприводимого многочлена степени n над $GF(p)$. Затем мы рассмотрим другое рассуждение, которое вначале устанавливает существование неприводимого многочлена степени n над $GF(p)$, откуда уже следует существование поля из p^n элементов (факторкольца по модулю неприводимого многочлена степени n).

Начнем с того, что построим поле характеристики p, над которым многочлен $x^q - x$ разлагается на линейные множители (т. е. имеет q корней). Будем строить цепочку полей

$$F_0 \subset F_1 \subset \dots$$

по следующему индуктивному правилу. Поле F_0 — это поле вычетов $GF(p)$. Пусть поле F_k уже построено. Если в разложении многочлена $x^q - x$ на неприводимые множители над F_k встретился неприводимый множитель f_k степени большей, чем 1, то строим новое поле $F_{k+1} = F_k[x]/(f_k)$. В противном случае построение закончено.

Заметим, что в разложении многочлена $x^q - x$ над полем F_{k+1} больше неприводимых множителей, чем в разложении

над полем F_k. Значит, построенная выше цепочка конечна (поскольку число неприводимых множителей многочлена не превосходит его степени). Но тогда над последним в этой цепочке полем F_m многочлен $x^q - x$ разлагается на линейные множители по построению.

Корни многочлена $x^q - x$ в поле F_m образуют искомое подполе из q^n элементов.

Вначале разберемся, почему эти корни действительно образуют подполе. Отображение $x \mapsto x^q$ является n-й итерацией автоморфизма Фробениуса, который был описан выше в разделе 3.2. Поэтому $(x+y)^q = x^q + y^q$, $(xy)^q = x^q y^q$. Отсюда получаем замкнутость множества корней многочлена $x^q - x$ относительно сложения и умножения. 0 и 1 принадлежат множеству корней по очевидным причинам. Но тогда множество корней замкнуто и относительно взятия обратных как по сложению, так и по умножению, поскольку поле конечно.

Может ли так случиться, что у многочлена $x^q - x$ в поле F_m различных корней меньше, чем q? Поскольку этот многочлен разлагается на линейные множители, это означало бы наличие кратных корней, т. е. множителей вида $(x-a)^r$, $r > 1$.

Чтобы исключить такую возможность, нам потребуется использовать понятие *производной* многочлена над полем F. Производная константы равна 0 по определению, производная x^n определяется как nx^{n-1} (здесь n означает элемент поля коэффициентов F, который равен сумме n единиц поля). Кроме того, потребуем линейности производной: для любых $\alpha, \beta \in F$, $f, g \in F[x]$ это означает выполнение равенства

$$(\alpha f + \beta g)' = \alpha f' + \beta g',$$

где штрихом обозначена производная. По линейности можно определить производную для любого многочлена, зная производные одночленов и констант.

Утверждение 3.46 (формула Лейбница). *Для любых многочленов f, g выполнено $(fg)' = f'g + fg'$.*

Доказательство. Если один из сомножителей равен 1, то $(f \cdot 1)' = f' = f' \cdot 1 + f \cdot 1'$ (производная константы — нуль).

Для мономов x^n, x^k имеем

$$(x^n \cdot x^k)' = (n+k) \cdot x^{n+k-1} = nx^{n-1}x^k + kx^n x^{k-1} = \\ = (x^n)'x^k + x^n(x^k)'.$$

В остальных случаях формула выполняется в силу линейности производной. □

Утверждение 3.47. *Пусть f и f' взаимно просты. Тогда f не имеет кратных корней.*

Доказательство. Предположим противное: $f = g^2 h$. Тогда по формуле Лейбница $f' = 2g'gh + g^2 h'$. Значит, g является общим делителем f и f'. Пришли к противоречию. □

Вычислим производную нашего многочлена $x^q - x$:

$$(x^q - x)' = qx^{q-1} - 1 = -1.$$

В последнем равенстве мы учли, что $q = p^n = 0$ в поле характеристики p. Теперь из утверждения 3.47 получаем, что у многочлена $x^q - x$ над полем F_m кратных корней нет. Значит, построенное нами поле корней этого многочлена содержит ровно $q = p^n$ элементов.

Первое доказательство теоремы 3.16. Чтобы доказать существование неприводимого многочлена степени n над полем $GF(p)$, рассмотрим поле $GF(p^n)$ из p^n элементов. Мультипликативная группа этого поля циклическая по теореме 3.44, значит, есть такой элемент $\alpha \in GF(p^n)$, степени которого совпадают со всеми ненулевыми элементами поля.

По утверждению 3.31 минимальная функция $m(\alpha)$ — неприводимый многочлен. Докажем, что ее степень равна n. Обозначим $d = \deg m(\alpha)$. Все степени α (т. е. все элементы поля) принадлежат d-мерному подпространству с базисом 1, α, α^2, α^3, …, α^{d-1}, в котором p^d элементов. Значит, $d = n$. □

Как обещано в начале этого раздела, докажем теперь существование неприводимого многочлена степени n над полем $GF(p)$, не опираясь на существование поля из p^n элементов. Это рассуждение дает независимый способ доказательства существования поля из p^n элементов.

Будем доказывать существование нормированного (старший коэффициент 1) неприводимого многочлена. Для нормированных многочленов выполняется аналог основной теоремы арифметики: каждый нормированный многочлен однозначно разлагается на произведение степеней неприводимых многочленов. Действительно, разложение в евклидовом кольце однозначно с точностью до умножения на делители единицы (обратимые элементы). В случае кольца многочленов над полем обратимые элементы — это константы (многочлены степени 0). Выбор старшего коэффициента устраняет произвол в выборе сомножителей.

Мы выведем существование неприводимых нормированных многочленов степени n над полем $GF(p)$ из рекуррентной формулы для числа d_n неприводимых нормированных многочленов степени n.

Лемма 3.48. $\sum\limits_{m|n} m d_m = p^n$.

Доказательство. Каждому неприводимому нормированному многочлену сопоставим формальную переменную f_{in}, где n — степень многочлена, $i = 1, \dots, d_n$. Поскольку всякий нормированный многочлен однозначно раскладывается в произведение степеней неприводимых нормированных, то произвольному нормированному многочлену степени n однозначно сопоставлен моном

$$f_{i_1 n_1}^{s_1} \dots f_{i_r n_r}^{s_r}, \quad \text{причем } \sum_{j=1}^{r} n_r s_r = n.$$

Поэтому все нормированные многочлены перечисляются формальным бесконечным произведением

$$\prod_{i,n} \Big(\sum_{k=0}^{\infty} f_{in}^k \Big) = \sum f_{i_1 n_1}^{s_1} \dots f_{i_r n_r}^{s_r}. \tag{3.9}$$

В последнем выражении мы раскрыли скобки и переписали бесконечное произведение в виде формального ряда. Равенство (3.9) — это другой способ сказать, что каждый нормированный многочлен однозначно разлагается в произведение неприводимых нормированных.

Теперь сделаем замену переменных $f_{in} = t^n$, которая делает все многочлены одной степени «одинаковыми». Приведение подобных в правой части равенства (3.9) даст ряд от переменной t. Коэффициент при t^n в этом ряде равен числу нормированных многочленов степени n, которое равно p^n. Действительно, нормированный многочлен степени n однозначно задается своими коэффициентами $a_0, \ldots, a_{n-1}$ (так как старший коэффициент равен 1).

Что произойдет с левой частью равенства (3.9) после замены переменных? Все неприводимые многочлены степени n дадут одинаковый множитель (сумму бесконечной геометрической прогрессии со знаменателем t^n). Поэтому равенство (3.9) превращается в

$$\prod_n \Big(\sum_{k=0}^{\infty} t^{nk} \Big)^{d_n} = \sum_{n=0}^{\infty} p^n t^n. \tag{3.10}$$

Применим формулу для суммы бесконечной геометрической прогрессии к левой и правой частям равенства (3.10). Получим равенство

$$\prod_n \frac{1}{(1-t^n)^{d_n}} = \frac{1}{1-pt}\,, \tag{3.11}$$

которое и означает, в сущности, искомое рекуррентное соотношение. Чтобы это увидеть, прологарифмируем его, потом продифференцируем по t, после чего снова воспользуемся суммой геометрической прогрессии. Более подробно:

$$\begin{gathered}
\sum_n d_n \ln(1-t^n) = \ln(1-pt), \\
\sum_n d_n \frac{nt^{n-1}}{1-t^n} = \frac{p}{1-pt}\,, \\
\sum_{n,k} d_n n t^{n-1} t^{nk} = \sum_s p^{s+1} t^s, \\
\sum_{n,k} n d_n t^{n(k+1)} = \sum_s p^s t^s.
\end{gathered} \tag{3.12}$$

Равенство коэффициентов при одинаковых степенях t в левой и правой части (3.12) и есть утверждение леммы. $\square$

Замечание 3.49. Единственное, что нужно от поля коэффициентов в этом доказательстве — это число элементов. Так что утверждение леммы справедливо и при p, равном степени простого.

Второе доказательство теоремы 3.16. Заметим, что из леммы 3.48 следует неравенство $nd_n \leqslant p^n$. Теперь осталось сделать простую оценку:

$$nd_n = p^n - \sum_{k|n,k<n} kd_k \geqslant p^n - \sum_{k=0}^{n-1} p^k = p^n - \frac{p^n-1}{p-1} > 0.$$

Мы доказали, что $d_n > 0$. Но это означает, что существует хотя бы один неприводимый многочлен степени n. □

Замечание 3.50. Из леммы 3.48 вытекает, что при $n \to \infty$ величина d_n эквивалентна p^n/n. Таким образом, примерно, $1/n$ часть всех многочленов степени n над полем из p элементов неприводима.

3.8. Единственность поля из p^n элементов

В этом разделе мы докажем вторую часть теоремы 3.15: любые два поля с одинаковым числом элементов изоморфны. Доказательство будет использовать теорему 3.38, утверждающую, что все неприводимые многочлены степени n над полем $GF(p)$ являются делителями многочлена $x^{p^n} - x$ и следствие 3.36, которое утверждает по сути, что над полем из p^n элементов многочлен $x^{p^n} - x$ разлагается на линейные множители.

Из первого доказательства теоремы 3.16, приведенного в предыдущем разделе, можно понять, что любое конечное поле является кольцом вычетов кольца многочленов $GF(p)[x]$ по модулю некоторого неприводимого многочлена. Сформулируем это утверждение явно.

Теорема 3.51. *Пусть m — минимальная функция элемента $\alpha \in GF(p^n)$ и d — ее степень. Тогда поле $GF(p)[x]/(m)$ изоморфно подполю $GF(p^d)$, порожденному степенями α.*

Доказательство. Степени α принадлежат d-мерному пространству с базисом $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, которое является подполем поля $GF(p^n)$, поскольку замкнуто относительно сложения и умножения и содержит 0 и 1.

Искомый изоморфизм φ отображает вычет $\{x^k\}$ в α^k:

$$\varphi\colon \{x^k\} \mapsto \alpha^k, \tag{3.13}$$

на остальных элементах $GF(p)[x]/(m)$ его можно доопределить по линейности:

$$\varphi\colon \left(\sum_{k=0}^{d-1} a_k\{x^k\}\right) \mapsto \sum_{k=0}^{d-1} a_k\alpha^k. \tag{3.14}$$

Из (3.14) ясно, что отображение φ взаимно однозначно и является гомоморфизмом аддитивных групп рассматриваемых полей. Осталось проверить, что $\varphi(\{f\}\{g\}) = \varphi(\{f\})\varphi(\{g\})$. Разделим fg на m с остатком: $fg = qm + r$. Тогда

$$\varphi(\{f\})\varphi(\{g\}) = f(\alpha)g(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = r(\alpha) = \varphi(\{r\}),$$

а в $GF(p)[x]/(m)$ мы имеем равенство $\{f\}\{g\} = \{r\}$. Итак, построенное отображение — изоморфизм полей. □

Рассмотрим теперь два поля с одинаковым количеством элементов $F = GF(p)/(f)$ и $G = GF(p)/(g)$, которые по предыдущей теореме можно считать кольцами вычетов по модулю неприводимых многочленов f и g соответственно. Степень этих многочленов одинакова, обозначим ее n.

Поскольку в поле G многочлен $x^{p^n} - x$ разлагается на линейные множители, его множитель f имеет в этом поле корень α. Из неприводимости f следует, что он является минимальной функцией α. По теореме 3.51 убеждаемся, что наши два поля изоморфны.

3.9. Циклические подпространства

В приложениях к теории кодирования мы будем использовать кольцо многочленов над $GF(p)$ по модулю главного идеала, порожденного некоторым (не обязательно неприводимым) многочленом f. Приведем некоторые свойства этого кольца.

Сначала докажем две теоремы о том, как устроены идеалы в кольце классов вычетов кольца многочленов над $GF(p)$ по модулю главного идеала, порожденного некоторым многочленом f. Если f неприводим, то кольцо вычетов является полем, этот случай мы уже рассмотрели в предыдущем разделе.

Заметим, что, как и раньше, вычеты образуют векторное пространство над $GF(p)$ многочленов степени не выше $\deg f$.

Теорема 3.52. *Пусть φ — неприводимый нормированный многочлен, который делит f. Тогда совокупность всех вычетов, кратных φ, образует идеал в кольце классов вычетов по модулю f и φ — единственный нормированный многочлен минимальной степени в этом идеале.*

Доказательство. Проверим, что это идеал:

$$\{v\}\cdot\{\varphi\}+\{u\}\cdot\{\varphi\}=\{v+u\}\cdot\{\varphi\},$$
$$\{u\}\cdot\{v\}\cdot\{\varphi\}=\{uv\}\cdot\{\varphi\}.$$

Поскольку разность элементов идеала принадлежит идеалу, а старшие коэффициенты нормированных многочленов равны 1, осталось доказать, что в этом идеале нет многочленов степени меньше $\deg\varphi$. Докажем, что любой ненулевой многочлен степени меньше $\deg\varphi$ не сравним по модулю f ни с каким кратным φ. Поскольку $f=w\varphi$, то многочлен, сравнимый с кратным φ по модулю f имеет вид $u\varphi-vf=(u-vw)\varphi$, степень такого многочлена не меньше, чем степень φ. □

Теорема 3.53. *Рассмотрим идеал (φ), порожденный φ — неприводимым нормированным делителем f. Пусть степень f равна n, а степень φ равна k. Тогда идеал (φ) — векторное пространство размерности $n-k$.*

Доказательство. Утверждение теоремы будет следовать из того, что любой элемент идеала (φ) можно представить в виде

$$\{(a_0+a_1x+\cdots+a_{n-k-1}x^{n-k-1})\varphi\}, \tag{3.15}$$

где $a_0,\ldots,a_{n-k-1}$ — произвольные элементы $GF(p)$.

Степень многочлена $(a_0+a_1x+\cdots+a_{n-k-1}x^{n-k-1})\varphi$ не больше $n-1$, поэтому все вычеты в (3.15) различны. Пусть $\{u\}=\{v\}\{\varphi\}$, а $v\varphi$ делится на f с остатком r. Тогда

$$v\varphi=uf+r=uw\varphi+r,$$

т. е. $r = (v - uw)\varphi$. Поэтому $\{u\} = \{r\}$ и мы доказали, что (3.15) описывает все элементы идеала (φ). □

Теперь изучим кольцо вычетов по модулю многочлена $x^n - 1$.

Введем понятие циклического подпространства. Пусть в n-мерном векторном пространстве над полем F фиксирован некоторый базис. Тогда это пространство можно отождествить с координатным пространством F^n, точки которого — упорядоченные наборы $(a_0, \ldots, a_{n-1})$ элементов F длины n. Подпространство координатного пространства F^n называется *циклическим*, если вместе с набором $(a_0, \ldots, a_{n-1})$ оно содержит циклический сдвиг этого набора, т. е. $(a_{n-1}, a_0, \ldots, a_{n-2})$.

В кольце классов вычетов по модулю многочлена $x^n - 1$, рассматриваемом как векторное пространство над полем $GF(p)$, есть базис $\{1\}$, $\{x\}$, $\ldots$, $\{x^{n-1}\}$. Циклический сдвиг координат в этом базисе равносилен умножению на x. Действительно,

$$\{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}\} \cdot \{x\} = \{a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n\} = \\ = \{a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1}\}.$$

Теорема 3.54. *В кольце классов вычетов по модулю многочлена $x^n - 1$ подпространство является циклическим тогда и только тогда, когда оно идеал.*

Доказательство. Если подпространство — идеал, то оно замкнуто относительно умножения на $\{x\}$, а умножение на $\{x\}$ и есть циклический сдвиг.

В другую сторону, пусть элемент v принадлежит циклическому подпространству I. Тогда $v \cdot \{x\}$, $v \cdot \{x^2\}$, $\ldots$ — циклические сдвиги, т. е. также принадлежат I. Значит, $v \cdot \{u\} \in I$ для любого многочлена u. Поэтому I — идеал. □

Разложим многочлен $x^n - 1$ на неприводимые над $GF(p)$ множители:

$$x^n - 1 = f_1^{a_1}(x) f_2^{a_2}(x) \ldots f_s^{a_s}(x).$$

По китайской теореме об остатках кольцо классов вычетов по модулю многочлена $x^n - 1$ изоморфно прямой сумме колец

классов вычетов по модулю многочленов $f_i^{a_i}(x)$. Иногда такое разложение оказывается полезным. Поэтому рассмотрим задачу разложения $x^n - 1$ на неприводимые множители.

Мы показали в разделе 3.7, что любой многочлен с коэффициентами из $GF(p)$ разлагается в некотором конечном поле характеристики p на линейные множители. Пусть $GF(q)$ — поле характеристики p, в котором многочлен $x^n - 1$ разлагается на линейные множители. Поскольку в поле характеристики p выполняется равенство $x^{kp} - 1 = (x^k - 1)^p$, интересен случай, когда n взаимно просто с p. В этом случае у многочлена $x^n - 1$ кратных корней нет, так как он взаимно прост со своей производной nx^{n-1}.

Равенство $x^n = 1$ означает, что порядок элемента x в мультипликативной группе поля $GF(q)$ делит n. Мультипликативная группа конечного поля циклична (теорема 3.44). Корни уравнения $x^n - 1 = 0$ образуют подгруппу этой группы (группа корней из единицы степени n), и эта подгруппа также циклическая. Ее порождающие элементы называются *примитивными корнями степени* n.

Подгруппа порядка n в циклической группе существует тогда и только тогда, когда n делит порядок циклической группы. Таким образом, мы получаем необходимое и достаточное условие того, что поле $GF(q)$ содержит группу корней из единицы степени n: n должно быть делителем $q - 1$.

Чтобы вернуться от разложения $x^n - 1$ на линейные множители в поле $GF(q)$ к разложению на неприводимые множители в поле $GF(p)$, нужно понять, какие корни из единицы будут входить в неприводимый делитель $f(x)$. Как мы уже установили (теорема 3.41), если уравнение $f(x) = 0$ имеет корень β, то и β^p, β^{p^2} и т. д. также будут корнями $f(x)$. Таким образом, количество и степени неприводимых делителей $x^n - 1$ можно найти, разбив вычеты по модулю n на орбиты отображения $t \mapsto pt \bmod n$.

Пример 3.55. Рассмотрим еще раз разложение многочлена $x^{15} - 1$ над полем $GF(2)$. Относительно умножения на 2 вычеты по модулю 15 разбиваются на такие орбиты:

$$\{0\},\ \{1, 2, 4, 8\}, \{3, 6, 12, 9\},\ \{5, 10\},\ \{7, 14, 13, 11\}.$$

Поэтому $x^{15}-1$ разлагается в произведение одного неприводимого многочлена степени 1, одного неприводимого многочлена степени 2 и трех неприводимых многочленов степени 4 (см. разложение на с. 148).

Пример 3.56. Рассмотрим разложение многочлена $x^{23}-1$ над полем $GF(2)$. Относительно умножения на 2 вычеты по модулю 23 разбиваются на три орбиты:

$$\{0\},\ \{1,2,4,8,16,9,18,13,3,6,12\},$$
$$\{5,10,20,17,11,22,21,19,15,7,14\}.$$

Поэтому $x^{23}-1$ разлагается в произведение одного неприводимого многочлена степени 1 и двух неприводимых многочленов степени 11.

3.10. Задачи

3.1. Доказать, что минимальное подполе любого поля характеристики 0 изоморфно полю рациональных чисел.

3.2. Доказать, что минимальное подполе любого поля характеристики p изоморфно полю $GF(p)$.

3.3. Решить уравнение $4x=1$ в поле $\mathbb{Z}/(101)$.

3.4. Найти 73^{-1} в поле $\mathbb{Z}/(103)$.

3.5. Решить систему уравнений

$$\begin{cases} x+2z=1, \\ y+2z=2, \\ 2x+z=1 \end{cases}$$

в поле вычетов по модулю 3 и по модулю 5.

3.6. Решить систему уравнений

$$\begin{cases} 3x+y+2z=1, \\ x+2y+3z=1, \\ 4x+3y+2z=1 \end{cases}$$

в поле вычетов по модулю 5 и по модулю 7.

3.7. Ненулевой вычет a называется квадратичным вычетом по модулю p, если уравнение $x^2=a$ имеет решение в поле $\mathbb{Z}/(p)$. В противном случае вычет называется квадратичным

невычетом. Чего больше: квадратичных вычетов или квадратичных невычетов?

3.8. Доказать, что a является квадратичным вычетом по нечетному простому модулю p тогда и только тогда, когда $a^{(p-1)/2} = 1 \pmod p$.

3.9. Найти произведение всех квадратичных вычетов по модулю 71.

3.10. Найти сумму всех квадратичных вычетов по модулю 67.

3.11. (Теорема Вильсона.) Доказать, что

$$(p-1)! \equiv -1 \pmod p$$

для простого p.

3.12. Доказать, что в поле $GF(p)$ выполняются равенства:

$$\text{а)}\ \sum_{k=1}^{p-1} \frac{1}{k} = 0\ (p > 2); \qquad \text{б)}\ \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} = 0\ (p > 3).$$

3.13. Найти $1^{2006} + 2^{2006} + 3^{2006} + \cdots + 16^{2006}$ по модулю 17.

3.14. Сколько решений имеет уравнение $x^2 = a$ в поле $GF(2^n)$?

3.15. Для каких из чисел $n = 2, 3, 4, 5, 6, 7$ существует поле из n элементов?

3.16. В поле F выполнено равенство $5 = 21$. Верно ли, что в поле F выполнено равенство $7 = 15$?

3.17. Можно ли в поле из 64 элементов найти подполе из 16 элементов?

3.18. Доказать, что поле из p^2 элементов, где p — простое число, имеет единственное собственное подполе.

3.19*. а) Доказать, что если многочлены $f(x)$ и $g(x)$ с целыми коэффициентами взаимно просты над полем вычетов по простому модулю p, причем хотя бы один из старших коэффициентов не делится на p, то эти многочлены взаимно просты над полем рациональных чисел.

б) Показать на примере, что для любого простого числа p обратное утверждение не верно.

3.20. Доказать, что многочлены $f(x)$ и $g(x)$ с целыми коэффициентами тогда и только тогда взаимно просты над полем рациональных чисел, когда они взаимно просты над полем

вычетов по модулю p, где p — любое простое число, исключая, быть может, конечное множество таких чисел.

3.21*. Доказать, что если многочлен $f(x)$ с целыми коэффициентами приводим над полем рациональных чисел, то он приводим над полем вычетов по любому простому модулю p, не делящему старший коэффициент. Привести пример многочлена, приводимого над полем рациональных чисел, но неприводимого над полем вычетов по модулю p, где p делит старший коэффициент.

3.22*. Существуют многочлены с целыми коэффициентами, неприводимые над полем рациональных чисел, но приводимые над полем вычетов по любому простому модулю p. Доказать, что таким будет, например, многочлен $f(x) = x^4 - 10x^2 + 1$. Это многочлен наименьшей степени с целыми коэффициентами, имеющий корень $\alpha = \sqrt{2} + \sqrt{3}$.

3.23. Многочлен $f(x) = x^2 + ax + b$, $a, b \in GF(5)$, неприводим над $GF(5)$. Верно ли, что $f(x)$ неприводим над $GF(125)$?

3.24. Доказать, что $n!$ делит

$$(p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}).$$

3.25. Решить уравнение $x^p - x = 0$ в поле $GF(p^n)$.

3.26. Решить уравнение $5x - 7 = 0$ в поле из 169 элементов.

3.27. Решить уравнение $x^2 + x + 4 = 0$ в поле $GF(121)$.

3.28. Сколько решений имеет уравнение $x^{23} - x^7 - 1 = 0$ в поле $GF(2^4)$?

3.29. Производная многочлена $f \neq 0$ над полем характеристики p тождественно равна 0. Доказать, что этот многочлен приводимый.

3.30. Доказать, что многочлен f над полем F характеристики p, который взаимно прост со своей производной f', неприводим тогда и только тогда, когда уравнение $x^p = x$ имеет в кольце $F[x]/(f)$ ровно p решений.

3.31. Пусть $(f, f') = 1$ и $v^p = v$ в кольце $F[x]/(f)$, $v \notin \{0, 1, \dots, p-1\}$. (Здесь p — характеристика поля коэффициентов F.) Доказать, что тогда для некоторого $a \in F$ многочлены $v - a$ и f имеют нетривиальный общий делитель.

3.32. Доказать, что любая функция $f\colon GF(p^n) \to GF(p^n)$ может быть представлена многочленом.

3.33. Является ли x^4+1 неприводимым многочленом над полем $GF(3)$?

3.34. Многочлен $x^5+x^3+x^2+1$ разложить на неприводимые множители над полем вычетов по модулю 2.

3.35. Многочлен x^3+2x^2+4x+1 разложить на неприводимые множители над полем вычетов по модулю 5.

3.36. Многочлен x^4+x^3+x+2 разложить на неприводимые множители над полем вычетов по модулю 3.

3.37. Многочлен $x^4+3x^3+2x^2+x+4$ разложить на неприводимые множители над полем вычетов по модулю 5.

3.38. Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены второй степени от x.

3.39. Разложить на неприводимые множители над полем вычетов до модулю 2 все нормированные многочлены третьей степени от x.

3.40. Найти все нормированные многочлены второй степени от x, неприводимые над полем вычетов по модулю 3.

3.41. Найти все нормированные многочлены третьей степени от x, неприводимые над полем вычетов по модулю 3.

3.42. а) Проверить, что $F=GF(7)[x]/(x^2+x-1)$ является полем. б) Выразите обратный к $1-x$ в F в базисе $1, x$.

3.43. Найти порядок элемента $x+x^2$ в мультипликативной группе

а) поля $GF(2)[x]/(x^4+x+1)$;

б) поля $GF(2)[x]/(x^4+x^3+1)$.

3.44. Найти количество неприводимых многочленов

а) степени 7 над полем $GF(2)$;

б) степени 6 над полем $GF(5)$;

в) степени 24 над полем $GF(3)$.

3.45. Чему равно произведение всех ненулевых элементов поля $GF(2^6)$?

3.46. Чему равна сумма всех элементов поля $GF(3^7)$?

3.47. Многочлен $f\in GF(13)[x]$ седьмой степени разлагается над $GF(13)$ на неприводимые множители степени 3 и 4. В каких полях $GF(13^n)$ многочлен f разлагается на линейные множители?

3.48. Найти наименьшее поле характеристики 2, в котором многочлен $x^{19}-1$ разлагается на линейные множители.

3.49. Построить изоморфизм между полями

$$GF(7)[x]/(x^2+x-1) \text{ и } GF(7)[x]/(x^2+1).$$

3.50. Доказать, что группа автоморфизмов поля $GF(p^n)$ — циклическая, а ее порождающим является автоморфизм Фробениуса.

3.51. Конечная проективная плоскость порядка n — это такое семейство подмножеств $L_1, \ldots, L_m$ («прямых») конечного множества «точек» P, что выполняются следующие свойства:

- через каждую точку проходит $n+1$ прямая;
- каждая прямая содержит $n+1$ точку;
- через любые две различные точки проходит ровно одна прямая;
- любые две различные прямые пересекаются ровно по одной точке.

Построить конечную проективную плоскость порядка q, где q — степень простого числа.

3.52. Пусть p — простое нечетное число. Определим для элемента a поля вычетов $GF(p^m)$ *символ Лежандра* $\chi(a)$ как 0, если $a=0$, как $+1$, если уравнение $x^2=a$ имеет решение в поле $GF(p^m)$, и как -1 в противном случае. Доказать

а) $\chi(a)\chi(b)=\chi(ab)$;

б) если $p^m \equiv 1 \pmod 4$, то $\chi(-1)=1$; если $p^m \equiv -1 \pmod 4$, то $\chi(-1)=-1$;

в) $\sum_{a\in GF(p^m)} \chi(a)=0$;

г) для любого $b\neq 0$ выполнено $\sum_{a\in GF(p^m)} \chi(a)\chi(a+b) = -1$.

3.53*. Матрица Адамара H порядка n состоит из элементов ± 1 и удовлетворяет условию

$$HH^T = nI, \qquad \text{где } I \text{ — единичная матрица.}$$

Построить матрицу Адамара порядка $n=p^m+1$, где p — простое, а n делится на 4.

Глава 4

Коды, исправляющие ошибки

4.1. Основная задача теории кодирования

Пусть есть набор сообщений S_i, $1 \leqslant i \leqslant n$, которые нужно передавать по каналу связи. Сообщения будем кодировать нулями и единицами, т. е. каждому сообщению будем сопоставлять его код — слово из нулей и единиц (бинарный набор), который обычно называется *кодовым словом*. Мы ограничимся только случаем, когда все сообщения кодируются словами одинаковой длины. Будем считать, что *ошибки при передаче* могут только изменять значения некоторых битов. Вообще говоря, это не единственный вид ошибок. Возможны, например, выпадения и вставки — какой-то из битов может не дойти до приемника или, наоборот, из-за помех может произойти ложное срабатывание приемника и получится бит, которого никто не посылал. Мы такие ситуации рассматривать не будем.

Задача состоит в том, чтобы построить код минимальной длины, при передаче с помощью которого сообщение может быть однозначно восстановлено при условии, что произошло не более r ошибок.

Более удобно рассматривать другую задачу: даны n — длина кода, r — максимально допустимое число ошибок. Требуется найти максимальное число сообщений k, которое можно передать. Решив задачу про максимальное число сообщений, нетрудно получить решение и решение предыдущей задачи про код минимальной длины.

Мы приближенно решим эту задачу для произвольных n и r. Точное решение будет дано лишь для случая $n = 2^m - 1$ и $r = 1$, а также для $n = 23$, $r = 3$ (см. раздел 4.5). Введем *расстояние* между бинарными наборами

$$\rho(\tilde{\alpha}, \tilde{\beta}) = \sum_{i=1}^{n} |\alpha_i - \beta_i|,$$

где $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, $\alpha_i, \beta_i \in \{0, 1\}$. (Это расстояние часто называется *метрикой Хэмминга*.)

Говоря попросту, $\rho(\tilde{\alpha}, \tilde{\beta})$ — это число координат, по которым различаются наборы $\tilde{\alpha}$ и $\tilde{\beta}$.

Введем еще одно определение: *норма* $\|\tilde{\gamma}\|$ — это число единичных координат в $\tilde{\gamma}$.

Читателю предлагается самостоятельно проверить справедливость следующего простого утверждения.

Утверждение 4.1. $\rho(\tilde{\alpha}, \tilde{\beta}) = \|\tilde{\alpha} \oplus \tilde{\beta}\|$, *где*

$$\tilde{\alpha} \oplus \tilde{\beta} = \big((\alpha_1 + \beta_1) \bmod 2, \ldots, (\alpha_n + \beta_n) \bmod 2\big).$$

Пример 4.2. $\tilde{\alpha} = (101011)$, $\tilde{\beta} = (000110)$, $\rho(\tilde{\alpha}, \tilde{\beta}) = 4$, $\tilde{\alpha} \oplus \tilde{\beta} = (101101)$, $\|\tilde{\alpha} \oplus \tilde{\beta}\| = 4$.

Бóльшая часть теории кодирования построена на так называемых групповых кодах, т. е. кодах, образующих группу (их также называют *линейными кодами*). Другими словами, множество кодовых слов $\{\tilde{\alpha}^1, \ldots, \tilde{\alpha}^q\}$ образует группу относительно операции $\oplus$: для любых кодовых слов $\tilde{\alpha}^i$, $\tilde{\alpha}^j$ выполняется $\tilde{\alpha}^i \oplus \tilde{\alpha}^j = \tilde{\alpha}^t$, $1 \leqslant t \leqslant q$ (достаточно проверить это утверждение, так как наличие обратного здесь очевидно — это сам элемент).

Теорема 4.3. *Предположим, что мы имеем групповой код* $\{\tilde{\alpha}^1, \ldots, \tilde{\alpha}^q\}$ *относительно операции* $\oplus$ (*здесь и далее рассматриваются группы только относительно операции* $\oplus$). *Для минимального расстояния между различными кодовыми словами выполняется соотношение*:

$$\min_{i \neq j} \rho(\tilde{\alpha}^i, \tilde{\alpha}^j) = \min_{\tilde{\alpha}^t \neq \tilde{0}} \|\alpha^t\|.$$

Доказательство. $\rho(\tilde{\alpha}^i, \tilde{\alpha}^j) = \|\tilde{\alpha}^i \oplus \tilde{\alpha}^j\| = \|\tilde{\alpha}^u\|$, причем $\tilde{\alpha}^u \neq (0, \ldots, 0)$ при $\tilde{\alpha}^i \neq \tilde{\alpha}^j$. Отсюда получаем оценку

$$\min_{i \neq j} \rho(\tilde{\alpha}^i, \tilde{\alpha}^j) \geqslant \min_{\tilde{\alpha}^t \neq \tilde{0}} \|\alpha^t\|.$$

Ясно, что эта оценка достигается: набор $(0, \ldots, 0)$ обязательно принадлежит групповому коду, а $\|\tilde{\alpha}^u\| = \|\tilde{\alpha}^u \oplus \tilde{0}\| = \rho(\tilde{\alpha}^u, \tilde{0})$.

Пусть передавалось сообщение

$$\tilde{\alpha}^i = (\alpha_{1i}, \ldots, \alpha_{ni}),$$

а получено сообщение

$$\tilde{\beta}^i = (\beta_{1i}, \ldots, \beta_{ni}).$$

Мы предположили, что число ошибок не больше r. Поэтому $\rho(\tilde{\alpha}^i, \tilde{\beta}^i) \leqslant r$. □

Определение 4.4. Минимальное расстояние между кодовыми словами кода C называется *кодовым расстоянием* C.

Совокупность таких $\tilde{\beta}^i$, что $\rho(\tilde{\alpha}^i, \tilde{\beta}^i) \leqslant r$ назовем *шаром Хэмминга* $S_r(\tilde{\alpha}^i)$ с центром в $\tilde{\alpha}^i$ и радиусом r.

Утверждение 4.5. *Множество* $\{\tilde{\alpha}^1, \ldots, \tilde{\alpha}^q\}$ *образует код с исправлением ошибок, если* $S_r(\tilde{\alpha}^i) \cap S_r(\tilde{\alpha}^j) = \varnothing$ *при* $i \neq j$.

Доказательство. Если при передаче сообщения $\tilde{\alpha}^i$ сделано не более r ошибок, то набор останется в шаре $S_r(\tilde{\alpha}^i)$. Если шары не пересекаются, то мы можем однозначно восстановить центр шара по любой точке из этого шара. □

Отсюда следует, что у кода, исправляющего r ошибок, кодовое расстояние не меньше $2r + 1$.

Итак, чтобы построить код максимального размера, исправляющий r ошибок, нужно вложить в множество всех бинарных наборов E^n (*булев куб*) максимальное число непересекающихся шаров Хэмминга радиуса r. В случае $n = 2^m - 1$, $r = 1$ можно так расположить шары, чтобы они покрывали куб E^n и не пересекались. Ясно, что такой код имеет самый большой размер. Интересен вопрос, при каких других n и r можно разбиение E^n на шары радиуса r. Оказывается, такое возможно лишь еще при одной паре n и r: $n = 23$, $r = 3$ (см. раздел 4.5).

Теорема 4.6 (теорема Хэмминга). *При $2r < n$ максимальное число сообщений k находится в следующих пределах*

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}} \leqslant k \leqslant \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}} .$$

Доказательство. Подсчитаем, сколько точек попадает в шар радиуса r — это сам центр, все точки с одной измененной координатой (которую можно выбрать $\binom{n}{1}$ способами), все точки с двумя измененными координатами (которые можно выбрать $\binom{n}{2}$ способами), ..., все точки с r измененными координатами (их можно выбрать $\binom{n}{r}$ способами). Так как шары не пересекаются, получаем верхнюю оценку.

Для оценки снизу построим пример кода (негруппового). Берем произвольную точку $\tilde{\alpha}^1$ и строим вокруг нее шар радиуса $2r$. В качестве следующей точки берем произвольную точку вне этого шара $\tilde{\alpha}^2$ и строим снова около нее шар радиуса $2r$. Третью точку выберем вне этих двух шаров. Далее аналогично. Заметьте, что каждый новый шар занимает не более, чем

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}$$

точек. Значит, число таких шаров будет не меньше

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}} .$$

Очевидно, что шары радиуса r с центрами в построенных точках не пересекаются, так как в построении использовались шары радиуса $2r$. □

Теперь разберем случай $n = 2^m - 1$, $r = 1$.

Покажем, что

$$k = \frac{2^n}{n+1} ,$$

т. е. при таких значениях параметров верхняя оценка в теореме Хэмминга достигается.

Вначале построим код, а потом определим его кодовое расстояние.

Рассмотрим такую таблицу:

$100\ldots$	$\ldots$	$\ldots 000$	$1100\ldots 000$
$010\ldots$	$\ldots$	$\ldots 000$	$1010\ldots 000$
$001\ldots$	$\ldots$	$\ldots 000$	$1001\ldots 000$
		$\ldots$	
$000\ldots$	$\ldots$	$\ldots 100$	$1111\ldots 101$
$000\ldots$	$\ldots$	$\ldots 010$	$1111\ldots 110$
$000\ldots$	$\ldots$	$\ldots 001$	$1111\ldots 111$

Справа выписываются все бинарные наборы длины m, содержащие более одной единичной координаты. Слева — единичная матрица размера $(2^m-(m+1))\times(2^m-(m+1))$. Рассмотрим множество наборов (оно называется *кодом Хэмминга*), которые получаются при суммировании строчек этой таблицы всеми возможными способами. В этом множестве $2^{2^m-(m+1)}$ наборов (результаты сложения различны для любого множества строчек). Заметим, что

$$2^{2^m-(m+1)} = \frac{2^{2^m-1}}{2^m} = \frac{2^n}{n+1}\ .$$

Найдем минимальное $\rho(\tilde\alpha^i, \tilde\alpha^j)$. Легко видеть, что $\rho \geqslant 3$, так как норма любого ненулевого набора, получаемого суммированием строчек таблицы, не меньше трех: если суммируем не менее трех строчек, то в левой части будет не менее трех единиц; если суммируем две строчки, то в левой части будет две единицы, а в правой (наборы разные) — хотя бы одна; в любой строчке таблицы также содержится не менее трех единиц.

Раз расстояния между кодовыми наборами не меньше трех, шары радиуса 1 с центрами в этих наборах не пересекаются.

Пример 4.7. Составим таблицу для кода Хэмминга длины 7:

1	0	0	0	1	0	1
0	1	0	0	1	1	0
0	0	1	0	0	1	1
0	0	0	1	1	1	1

Складываем строчки произвольным образом и получаем 16 возможных комбинаций. Ими можно закодировать 16 сообщений, например, все 10 цифр и знаки операций. При передаче с

помощью кода Хэмминга можно исправить одну ошибку, возникающую при передаче.

4.2. Циклические коды

Одной из самых важных конструкций кодов являются циклические коды.

Определение 4.8. Код C называется *циклическим*, если он инвариантен относительно циклических сдвигов: из того, что набор $(\alpha_0, \ldots, \alpha_{n-1})$ принадлежит C, следует, что и всякий набор $(\alpha_s, \alpha_{s+1}, \ldots, \alpha_{n-1}, \alpha_0, \ldots, \alpha_{s-1})$ принадлежит C.

По теореме 3.54 циклические линейные коды совпадают с идеалами в кольце $\mathbb{F}_2[x]/(x^n - 1)$. Поэтому построить циклический код можно так: возьмем многочлен $x^n - 1$, выберем некоторый делитель $\varphi(x)$ этого многочлена и в кольце вычетов по модулю $x^n - 1$ рассмотрим идеал, порожденный $\varphi(x)$. Оказывается, что при удачном выборе $\varphi(x)$ коэффициенты многочленов, принадлежащих этому идеалу, будут давать хороший код.

Давайте рассмотрим простой пример.

Пример 4.9. Пусть $n = 7$. Запишем разложение на неприводимые множители:

$$x^7 - 1 = (1 + x)(1 + x^2 + x^3)(1 + x + x^3).$$

В качестве φ возьмем последний множитель. Умножая его на степени x получим базис в подпространстве, которое является кодом:

(1101000)	φ
(0110100)	$\varphi \cdot x$
(0011010)	$\varphi \cdot x^2$
(0001101)	$\varphi \cdot x^3$

Можно проверить, что кодовое расстояние для этого кода равно 3.

В самом деле, умножение на x в кольце вычетов по модулю $x^7 - 1$ приводит к циклическому сдвигу коэффициентов. Если

есть набор коэффициентов с двумя единицами, то расстояние между единицами в наборе не больше 2 (либо в одну сторону, либо в другую). Но тогда есть такой циклический сдвиг этого набора, у которого единицы помещаются в младшей (левой половине). Значит, это либо многочлен степени не выше 2, чего не может быть по теореме 3.52, либо многочлен $1 + x^3$. Но $1 + x^3 \equiv x \bmod (1 + x + x^3)$, поэтому в последнем случае мы бы получили все кольцо вычетов. Таким образом, минимальное число единиц (равное кодовому расстоянию) для этого кода равно 3.

Вопрос о кодовом расстоянии произвольного циклического кода безнадежно труден. Но есть несколько важных конструкций циклических кодов с хорошими параметрами. Далее мы приводим несколько примеров.

4.3. Коды БЧХ

В этом разделе будем рассматривать коды, имеющие длину $n = 2^k - 1$. Описываемый ниже способ способ построения «хорошего» кода, исправляющего «много» ошибок, придуман Боузом, Чоудхури и Хоквингемом. Поэтому коды, которые мы получим, называются БЧХ-кодами.

Рассмотрим такое уточнение описанной выше схемы. Возьмем какой-нибудь неприводимый многочлен и построим по нему поле. Ненулевые элементы поля, как было показано выше, образуют циклическую группу по умножению. Выберем порождающий элемент этой группы α и рассмотрим степени α, α^2, $\ldots$, α^{2r}, где r — число ошибок, которые нужно уметь исправлять. И теперь в разложении соответствующего многочлена $x^n - 1$ выберем такие неприводимые множители, чтобы каждая из указанных степеней была корнем одного из них. Оказывается, что это гарантирует исправление r ошибок.

Пример 4.10. Возьмем $x^{15} - 1$. Предположим, что нужен код, исправляющий три ошибки. Значит, нужно найти многочлены, корнями которых являются первые шесть степеней порождающего элемента α. Если многочлен имеет корень α, то по теореме 3.41 можно указать все его корни: α, α^2, α^4, α^8.

Аналогично, если у многочлена есть корень α^3, то у него будут корни α^3, α^6, α^{12}, α^9. Наконец, если у многочлена есть корень α^5, то у него также есть корень α^{10}.

Перемножив три многочлена, подобранных по указанным множествам корней, получим многочлен 10-й степени. Значит, идеал по модулю этого многочлена дает пять степеней свободы. Построенный код будет 5-мерным пространством.

Теперь проведем эти рассуждения в более общем виде.

Начнем с простой части — построения кода, а затем уже будем доказывать, что он действительно исправляет ошибки.

Итак, полагаем $n = 2^k - 1$. Из разложения на множители многочлена $x^n - 1$

$$x^n - 1 = \varphi_1(x) \cdot \ldots \cdot \varphi_k(x) \cdot \ldots \cdot \varphi_p(x) \tag{4.1}$$

выберем те сомножители, корни которых содержат степени

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2r}. \tag{4.2}$$

Перемножая выбранные сомножители, получаем искомый многочлен φ, порождающий идеал, который и даст нам хороший код. Какова степень φ?

Если какой-то многочлен имеет корень α, значит, он также имеет корень α^2. И вообще, если многочлен имеет корень α^s, то он имеет также и корень α^{2s}. Таким образом, нам потребуется не более r штук многочленов, потому что каждый из выбираемых многочленов имеет по крайней мере два корня. А степень неприводимого делителя $x^n - 1$ не больше k (напомним, что было выбрано $n = 2^k - 1$). Поэтому общая степень произведения всех выбранных многочленов не больше rk, где $k = \log_2(n+1)$, $rk = r\log_2(n+1)$.

Итак, идеал, порожденный φ, будет иметь размерность n минус степень порождающего полинома, значит точек в этом идеале будет не меньше, чем

$$2^{n - r\log_2(n+1)} = \frac{2^n}{(n+1)^r}\,.$$

На самом деле эта оценка неточная: в ней учитываются только по два корня из каждого многочлена, а их может быть больше.

Докажем, что расстояние между точками кода не меньше, чем $2r+1$. Заметим, что все многочлены, входящие в наш код,

кратны φ. Поэтому каждый кодовый многочлен имеет корни α, α^2, $\ldots$, α^{2r}. Значит, нам достаточно доказать следующее утверждение.

Лемма 4.11. *Если $\psi(\alpha^s) = 0$ при $1 \leqslant s \leqslant 2r$, то у ψ не менее $2r+1$ ненулевого коэффициента.*

Доказательство. Рассмотрим многочлен $\psi(x) = a_0 + a_1 x + {} + \cdots + a_{n-1}x^{n-1}$, удовлетворяющий этому условию. Его коэффициенты дают решение следующей системы линейных уравнений:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & (\alpha^2) & (\alpha^2)^2 & \ldots & (\alpha^2)^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{2r} & (\alpha^{2r})^2 & \ldots & (\alpha^{2r})^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \ldots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \ldots \\ 0 \end{pmatrix}. \quad (4.3)$$

Если набор $a = (a_0, \ldots, a_{n-1})$ — решение этой системы, то, как нетрудно видеть, между $\|a\|$ столбцами матрицы системы (4.3) есть линейная зависимость. Поэтому для доказательства леммы 4.11 достаточно показать, что любые $2r$ столбцов этой матрицы линейно независимы.

Теория решения линейных уравнений над конечным полем ничем не отличается от привычной теории решения линейных уравнений над полем действительных чисел $\mathbb{R}$. (На самом деле, она вовсе не зависит от того, над каким полем мы решаем систему линейных уравнений.) В частности, линейная зависимость между столбцами квадратной матрицы равносильна обращению в нуль определителя этой матрицы.

Давайте выберем из матрицы системы (4.3) столбцы j_1, j_2, $\ldots$, j_{2r}. Получим квадратную матрицу

$$\begin{pmatrix} \alpha^{j_1} & \alpha^{j_2} & \ldots & \alpha^{j_{2r}} \\ (\alpha^2)^{j_1} & (\alpha^2)^{j_2} & \ldots & (\alpha^2)^{j_{2r}} \\ \ldots & \ldots & \ldots & \ldots \\ (\alpha^{2r})^{j_1} & (\alpha^{2r})^{j_2} & \ldots & (\alpha^{2r})^{j_{2r}} \end{pmatrix}.$$

Вынесем из всех элементов столбца t общий множитель α^{j_t}. Получим, что определитель нашей матрицы с точностью до

ненулевого множителя $\alpha^{j_1+j_2+\cdots+j_{2r}}$ равен

$$V = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \dots & \alpha^{j_{2r}} \\ (\alpha^{j_1})^2 & (\alpha^{j_2})^2 & \dots & (\alpha^{j_{2r}})^2 \\ \dots & \dots & \dots & \dots \\ (\alpha^{j_1})^{2r-1} & (\alpha^{j_2})^{2r-1} & \dots & (\alpha^{j_{2r}})^{2r-1} \end{vmatrix}. \qquad (4.4)$$

Это хорошо известный определитель Вандермонда. Вычисляется он над конечным полем точно так же, как и над привычным $\mathbb{R}$:

$$V = \prod_{t_1<t_2} (\alpha^{j_{t_2}} - \alpha^{j_{t_1}}).$$

В нашем случае определитель отличен от нуля: напомним, что мы взяли в качестве α порождающий элемент мультипликативной группы поля, поэтому все степени α вплоть до $(n-1)$-й различны. □

Итак, мы доказали лемму 4.11. Значит, построенный нами код действительно исправляет r ошибок (расстояние между кодовыми словами не меньше $2r+1$).

4.4. Квадратично-вычетные коды

Квадратично-вычетные коды дают еще один пример хороших циклических кодов.

В этом разделе предполагаем, что длина кода простое число, которое дает остаток ± 1 от деления на 8. Длину кода в этом разделе будем обозначать через $p = 8m \pm 1$. Напомним (см. с. 164), что ненулевой вычет a называется квадратичным вычетом по модулю p, если уравнение $x^2 = a$ имеет решение в поле $\mathbb{Z}/(p)$. Множество квадратичных вычетов по модулю n обозначим через Q_p, а множество квадратичных невычетов — через N_p.

Если $x^2 = a$, $y^2 = b$ в поле $\mathbb{Z}/(p)$, то $(xy^{-1})^2 = ab^{-1}$. Поэтому квадратичные вычеты по модулю p образуют подгруппу мультипликативной группы поля $\mathbb{Z}/(p)$.

Утверждение 4.12. *Пусть q — нечетное простое число. Тогда $2 \in Q_q$ тогда и только тогда, когда $q \equiv \pm 1 \pmod 8$.*

Доказательство (по [21]). Используем результат задачи 3.8: 2 является квадратичным вычетом по нечетному простому модулю q тогда и только тогда, когда $2^{(q-1)/2} = 1 \pmod q$. Любое поле характеристики q содержит подполе $GF(q)$, поэтому условие можно проверять в любом таком поле.

Рассмотрим расширение F поля $GF(q)$, которое содержит группу корней 8-й степени из единицы (см. раздел 3.9). Обозначим через α примитивный корень 8-й степени из единицы. В поле F у 2 есть квадратный корень. А именно, $\beta^2 = 2$, где $\beta = \alpha + \alpha^{-1}$. В самом деле,

$$(\alpha + \alpha^{-1})^2 = 2 + \alpha^2 + \alpha^{-2} = 2 + \alpha^{-2}(\alpha^4 + 1) = 2$$

($\alpha^4 = -1$ так как α — примитивный корень восьмой степени).

Теперь нам нужно вычислить $\beta^{q-1} = 2^{(q-1)/2}$. Пусть $q = 8m \pm 1$. Тогда

$$\beta^q = \alpha^q + \alpha^{-q} = \alpha^{\pm 1} + \alpha^{\mp 1} = \beta,$$

поэтому $\beta^{q-1} = 1$.

Пусть $q = 8m \pm 5$. Тогда

$$\beta^q = \alpha^q + \alpha^{-q} = \alpha^{\pm 5} + \alpha^{\mp 5} = -\beta,$$

поэтому $\beta^{q-1} = -1$. □

Возьмем поле F характеристики 2, которое содержит группу корней степени p. Примитивный корень степени p обозначим через ω. Рассмотрим многочлены

$$f(x) = \prod_{i \in Q_p} (x - \omega^i), \quad g(x) = \prod_{i \in N_p} (x - \omega^i)$$

В силу утверждения 4.12 если $p = 8m \pm 1$, то 2 является квадратичным вычетом по модулю p. Умножение на квадратичный вычет переводит множество квадратичных вычетов в себя и множество квадратичных невычетов в себя. Вспоминая структуру разложения $x^n - 1$ на неприводимые множители, описанную в разделе 3.9, получаем, что $f(x)$ и $g(x)$ являются многочленами над полем $GF(2)$. Таким образом, над $GF(2)$ имеем разложение

$$x^n - 1 = (x - 1) f(x) g(x). \tag{4.5}$$

Определение 4.13. *Квадратично-вычетными кодами* называются идеалы кольца $GF(2)/(x^n-1)$, порожденные $f(x)$, $g(x)$, $(x-1)f(x)$, $(x-1)g(x)$.

Код, порожденный $f(x)$, будем обозначать Q, а код, порожденный $g(x)$, будем обозначать N.

Теорема 4.14. *Кодовое расстояние d кодов Q и N удовлетворяет неравенству $d^2 \geqslant p$. Если $p = 8m-1$, то выполняется более сильное неравенство $d^2 - d + 1 \geqslant p$.*

Доказательство. Прежде всего убедимся, что кодовые расстояния кодов Q и N одинаковы. Пусть $c(x) \in Q$, а a — квадратичный невычет по модулю p. Тогда $\bar{c}(x) = c(x^a)$ будет принадлежать N. Верно и обратное. Чтобы проверить эти утверждения, достаточно проверить, что возведение в степень a меняет местами корни уравнений $f(x) = 0$ и $g(x) = 0$. Действительно, квадратичные вычеты образуют группу по умножению. Поэтому произведение квадратичного невычета на квадратичный вычет является квадратичным невычетом, а произведение квадратичного невычета на квадратичный невычет является квадратичным вычетом.

Рассмотрим произведение $c(x)\bar{c}(x)$. Оно делится на взаимно простые многочлены $f(x)$ и $g(x)$, а значит, и на их произведение

$$f(x)g(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{p-1}.$$

Если многочлен $c(x)$ содержит d ненулевых коэффициентов, то столько же ненулевых коэффициентов содержит $\bar{c}(x)$, а их произведение содержит не более d^2 ненулевых коэффициентов. Значит, $p \leqslant d^2$.

В случае $p = 8m-1$ оценку можно усилить, если выбрать $a = -1$. Это действительно невычет, так как $(-1)^{(8m-1-1)/2} = -1$ (см. задачу 3.8). При таком выборе $\bar{c}(x) = c(x^{-1})$. Тогда из d^2 произведений, в сумме дающих $c(x)\bar{c}(x)$, d штук дают вклад в свободный член. Поэтому количество возможных ненулевых коэффициентов в $c(x)\bar{c}(x)$ не больше $d^2 - d + 1$. $\square$

4.5. Совершенный код Голея

В этом разделе мы построим совершенный код Голея, т. е. код, содержащий 2^{12} слов длины 23, который исправляет 3 ошибки (кодовое расстояние равно 7). Вычислением можно найти объем 23-мерного шара радиуса 3 в E^{23}:

$$1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}=2^{11}.$$

Поэтому в булев куб E^{23} можно вложить не более 2^{12} шаров радиуса 3. Так что построенный код будет разбивать булев куб E^{23} на шары радиуса 3. (Поэтому он и называется совершенным.)

Фактически мы уже построили такой код. Обозначим через G_{23} квадратично-вычетный код при $p=23$, который в обозначениях предыдущего раздела порожден многочленом $f(x)$.

Теорема 4.15. *Количество кодовых слов в G_{23} равно 2^{12}, а кодовое расстояние равно 7.*

Доказательство. Квадратичных вычетов, которые образуют подгруппу индекса 2 мультипликативной группы поля вычетов $GF(23)$ столько же, сколько и квадратичных невычетов (смежный класс по этой подгруппе), степень многочлена $f(x)$ при $p=23$ равна 11. Значит, размерность идеала $(f(x))$ равна 12 и он содержит 2^{12} элементов.

Из теоремы 4.14 следует, что $d\geqslant 6$, так как $23=8\cdot 3-1$.

Теперь докажем, что если вес многочлена из кода Голея четен, то он делится на 4. Это означает, в частности, что в коде Голея нет слов веса 6. Поэтому $d\geqslant 7$. Но из границы Хэмминга следует, что $d\leqslant 7$. Таким образом $d=7$.

Пусть $c(x)$ — многочлен четного веса w. Тогда $c(1)=0$, т. е. $(x-1)\mid c(x)$, откуда следует, что $c(x)\bar{c}(x)=0$ в $GF(2)/(x^{23}-1)$, где $\bar{c}(x)=c(x^{-1})$.

Из равенства $c(x)\bar{c}(x)=0$ получаем равенства для коэффициентов c_i многочлена $c(x)$, рассматриваемых как целые числа: для $r=0,\ldots,22$ имеем

$$\sum_{i-j\equiv r \bmod 23} c_ic_j=2a_r,\quad a_i \text{ — целые числа.}$$

Меняя местами i и j, получаем равенства $a_r = a_{23-r}$ при $r \neq 0$. Поэтому

$$w(w-1) = \sum_{i=0}^{22} \sum_{j \neq i} c_i c_j = 2 \sum_{r=1}^{22} a_r = 4 \sum_{r=1}^{11} a_r,$$

т. е. из четности w следует, что w делится на 4. □

Мы доказали существование кода Голея, но не предъявили его явно. Напомним, что конструкция квадратично-вычетного кода включает в себя произведение мономов вида $x - \omega^i$ по всем квадратичным невычетам, где ω — примитивный корень степени 23. Вычисление коэффициентов многочлена $f(x)$ непосредственно из этого определения весьма мучительно. Но проверить полученный ответ довольно легко. Оказывается, что над полем $GF(2)$

$$x^{23} - 1 = (x-1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \times \\ \times (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1). \quad (4.6)$$

Проверить это равенство можно прямым вычислением. В приводимой ниже таблице мы перемножаем два последних множителя, указывая только показатели мономов многочленов и их коэффициенты и опуская обозначение переменной

22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	0	0	0	1	1
0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	0	0	0	1	1	0	0
0	0	0	0	0	0	0	1	0	1	0	1	1	1	0	0	0	1	1	0	0	0	0
0	0	0	0	0	0	1	0	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0
0	0	0	0	0	1	0	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0	0
0	1	0	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
1	0	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Из равенства (4.6) и примера 3.56 следует, что множители 11-й степени, которые входят в (4.6), и есть многочлены $f(x)$ и $g(x)$ из предыдущего раздела. Как было показано выше в теореме 4.14, идеалы $(f(x))$ и $(q(x))$ имеют одинаковое кодовое расстояние. Поэтому любой из них можно выбрать для построения совершенного кода размерности 12 длины 23, исправляющего 3 ошибки.

Итак, код Голея образуют линейные комбинации строк, которые получаются циклическими сдвигами из строки

$$0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,.$$

4.6. Коды Рида – Соломона

До сих пор мы рассматривали двоичные коды: сообщения кодировались последовательностями 0 и 1. Этот случай наиболее интересен в практических приложениях, так как двоичная система широко применяется в компьютерах. Но в принципе ничто не мешает рассматривать коды, которые используют для кодирования большее количество символов. Если используется q символов, то говорят о q-ичном коде.

На множестве q-ичных слов длины n можно ввести метрику Хэмминга: расстояние между двумя q-ичными словами равно количеству позиций, в которых слова содержат разные символы. Основная задача теории кодирования переформулируется для q-ичных кодов дословно.

Если q — степень простого числа, то понятие линейного кода и все с ним связанные определения можно переформулировать и для q-ичных кодов, если считать, что символы принадлежат полю из q элементов. Общие результаты, которые приведены выше для двоичных кодов, сохраняются и в случае q-ичных кодов, иногда с небольшими изменениями.

Например, теорема Хэмминга имеет естественный аналог для q-ичных кодов. Нужно только правильно сосчитать объем n-мерного шара радиуса r.

Теорема 4.16 (q-ичная теорема Хэмминга). *При $2r < n$ максимальное число сообщений k для q-ичных кодов длины n находится в следующих пределах*

$$\frac{q^n}{\sum_{i=0}^{2r}(q-1)^i\binom{n}{i}} \leqslant k \leqslant \frac{q^n}{\sum_{i=0}^{r}(q-1)^i\binom{n}{i}}\ .$$

Доказательство аналогично доказательству теоремы 4.6. Нужно только заметить, что количество точек на расстоянии i от данной равно $(q-1)^i\binom{n}{i}$ (выбираем i позиций из n, в которых

символы различаются, для каждой такой позиции есть $q-1$ вариант выбора символа).

Мы уже упоминали, что значения несовпадающих многочленов небольшой степени должны различаться во многих точках. Но это и есть условие исправления ошибок! Коды Рида – Соломона строятся следующим образом. Пусть q — степень простого числа, $F = GF(q)$ — поле из q элементов. неотрицательное число. Кодом Рида – Соломона $R_q(X, r)$ назовем q-ичный код длины n, который состоит из наборов значений многочленов степени не выше g в точках множества

$$X = \{x_1, \ldots, x_n\} \subseteq F.$$

Другими словами, каждому многочлену $f \in F[x]$, $\deg f \leqslant g$, сопоставлено кодовое слово

$$(f(x_1), \ldots, f(x_n)).$$

Во всех дальнейших рассмотрениях мы предполагаем, что $n > g$.

Многочлены степени не выше g образуют векторное пространство над полем F размерности $g+1$. Поэтому в коде Рида – Соломона q^{g+1} точек.

Теорема 4.17. *Кодовое расстояние для кода Рида – Соломона равно*

$$d = n - g. \tag{4.7}$$

Доказательство. Поскольку многочлены степени не выше g, совпадающие в $g+1$ точке, задают одну и ту же функцию, получаем оценку $d \geqslant n - g$. Построим многочлен степени g, имеющий g корней:

$$(x - x_1) \cdot \ldots \cdot (x - x_2) \cdot \ldots \cdot (x - x_g).$$

Значит, кодовое расстояние не превосходит $n - g$. □

Для линейных кодов справедлива следующая простая оценка кодового расстояния.

Теорема 4.18 (граница Синглтона). *Пусть q — степень простого числа, а C — линейный q-ичный код длины n с кодовым расстоянием d, содержащий q^k слов. Тогда*

$$n - k \geqslant d - 1.$$

Доказательство. C является векторным пространством размерности k над полем F из q элементов. Пространство размерности k имеет базис $(b_1, \ldots, b_k)$ из k элементов, поэтому можно задать F-линейное отображение пространства $\varphi\colon F^k \to F^n$, образом которого будет C:

$$\varphi\colon \underbrace{(0, \ldots, 0, 1, 0 \ldots, 0)}_{i-1 \text{ нулей слева от } 1} \mapsto b_i.$$

Матрица отображения φ имеет размер $n \times k$ и полный ранг. Покажем, что можно найти такое ненулевое кодовое слово, у которого $k-1$ нулей. Выберем для этого невырожденную подматрицу размера $k \times k$, пусть ее строки соответствуют позициям в слове с номерами i_1, i_2, …, i_k. Будем искать такой $u \in F^k$, что $\varphi(u)_{i_1} = 1$, $\varphi(u)_{i_2} = 0$, …, $\varphi(u)_{i_k} = 0$. Получаем систему линейных уравнений, матрица которой невырождена. Значит, решение u этой системы существует. Тогда $\varphi(u)$ и есть искомое кодовое слово с $k-1$ нулями.

Мы доказали, что $d \leqslant n - (k-1) = n - k + 1$. □

Как следует из теоремы 4.17, на кодах Рида – Соломона граница Синглтона достигается, т. е. неравенство в ней обращается в равенство. В этом смысле коды Рида – Соломона оптимальны. Однако с точки зрения оценки в теореме Хэмминга дело обстоит иначе.

Пример 4.19. Пусть $n = 4$ (т. е. мы берем значения многочленов в четырех точках поля), $g = 1$. Код образуют значения линейных многочленов, кодовое расстояние 3, т. е. код исправляет одну ошибку. Напишем границу Хэмминга для таких параметров:

$$\frac{q^4}{1 + 4(q-1)n + 6(q-1)^2} \leqslant q^2 \leqslant \frac{q^4}{1 + 4(q-1)}\,.$$

При больших q число кодовых слов в коде Рида – Соломона ближе к нижней границе, чем к верхней.

Пример 4.20. Пусть $n = q$ (т. е. мы берем значения многочленов во всех точках поля), $g = 1$. Код образуют значения линейных многочленов, кодовое расстояние $q-1$. Так как

$$2(q-3)/2 + 1 \leqslant q - 1 < 2(q-1)/2 + 1,$$

такой код исправляет $(q-3)/2$ ошибок. Напишем оценки из теоремы Хэмминга для этих значений параметров:

$$\frac{q^n}{\sum_{i=0}^{q-3}(q-1)^i\binom{n}{i}} \leqslant q^2 \leqslant \frac{q^n}{\sum_{i=0}^{(q-3)/2}(q-1)^i\binom{n}{i}}\,.$$

При больших q нижняя оценка близка к константе

$$(1-2.5e^{-1})^{-1} \approx 12.5,$$

мощность кода намного больше. Но мощность кода намного меньше верхней оценки из теоремы Хэмминга. Покажем, что отношение q^2 к верхней оценке в теореме Хэмминга стремится к 0 при $q \to \infty$. Имеем

$$q^{2-q}\sum_{i=0}^{(q-3)/2}(q-1)^i\binom{q}{i} < q^{2-q}q(q-1)^{(q-3)/2}\binom{q}{(q-3)/2} <$$

$$< q^{3-q+(q-3)/2}\left(1-\frac{1}{q}\right)^{(q-3)/2}2^q < 8q^{-(q-3)/2}4^{(q-3)/2} =$$

$$= 8\left(\frac{4}{q}\right)^{(q-3)/2} \to 0.$$

4.7. Коды Рида – Маллера

Приведем еще одну оценку для кодового расстояния.

Теорема 4.21 (граница Плоткина). *Кодовое расстояние d любого q-ичного кода длины n, содержащего q^k кодовых слов, удовлетворяет неравенству*

$$d \leqslant \frac{nq^k(q-1)}{(q^k-1)q}\,. \tag{4.8}$$

Доказательство. Минимальное расстояние между кодовыми словами не превосходит среднего расстояния:

$$d \leqslant \frac{1}{q^k(q^k-1)}\sum_{x\neq y\in C}\rho(x,y).$$

Оценим, какой вклад в сумму вносит каждая позиция в кодовом слове. Для этого нужно оценить количество пар слов, различающихся в позиции i. Обозначим через F множество

символов кода, а для каждого i через $f_{a,i}$ — количество кодовых слов, у которых в позиции i стоит $a \in F$. Тогда ясно, что $\sum_{a\in F} f_{a,i} = q^k$, а количество пар слов, различающихся в i-й позиции, равно

$$\sum_{a\neq b\in F} f_{a,i}f_{b,i} = \left(\sum_{a\in F} f_{a,i}\right)^2 - \sum_{a\in F} f_{a,i}^2 = q^{2k} - \sum_{a\in F} f_{a,i}^2.$$

При заданной сумме чисел сумма квадратов этих чисел достигает минимума, когда все числа равны. Поэтому вклад каждой позиции не превосходит

$$q^{2k} - q\cdot\left(\frac{q^k}{q}\right)^2 = q^{2k} - \frac{q^{2k}}{q} = q^{2k}\frac{q-1}{q} = q^{2k-1}(q-1).$$

Отсюда получаем искомую оценку

$$d \leqslant \frac{1}{q^k(q^k-1)}\cdot nq^{2k-1}(q-1) = \frac{nq^{k-1}(q-1)}{q^k-1} = \frac{nq^k(q-1)}{(q^k-1)q}\,.$$

□

Если q является степенью простого числа, граница Плоткина достигается на кодах Рида – Маллера первого порядка. Возьмем $n = q^m - 1$. Тогда слову длины n можно однозначно сопоставить функцию $F^m \setminus \{0\} \to F$. *Код Рида – Маллера первого порядка* образуют такие слова, которым соответствуют линейные однородные функции и 0. Количество кодовых слов также равно q^m (линейная однородная функция задается m коэффициентами). Поскольку любая отличная от 0 линейная однородная функция принимает нулевое значение ровно в q^{m-1} точках, кодовое расстояние для кода Рида – Маллера первого порядка равно $d = q^m - q^{m-1}$. Граница Плоткина в этом случае имеет вид

$$\frac{(q^m-1)q^m(q-1)}{(q^m-1)q} = q^m - q^{m-1}.$$

Ответы, указания, решения

1.1. Ответ: да. Указание: результат операции $*$ — это обратное к сумме обратных

$$\frac{1}{x*y} = \frac{1}{x} + \frac{1}{y}.$$

1.2. Ответ: операция $x*y = (1+2xy)(x+y)$ на множестве целых чисел $\mathbb{Z}$.

1.4. Докажем, что всякий правый обратный является левым обратным: возьмем равенство $x^{-1}\cdot x\cdot x^{-1} = x^{-1}$, умножим его справа на $(x^{-1})^{-1}$, получаем $x^{-1}\cdot x = e$.

Докажем, что всякая правая единица является левой единицей: $ex = xx^{-1}x = xe = x$.

Теперь легко проверяется единственность единицы и обратного.

Пусть e, e' — две единицы. Тогда $e = e\cdot e' = e'$.

Пусть $xy = xz = e$. Поскольку y, z являются также левыми обратными, имеем: $y = ye = yxz = ez = z$.

1.5. 1) да; 2) да; 3) да; 4) да; 5) нет; 6) нет; 7) нет; 8) да; 9) нет; 10) да; 11) да; 12) нет; 13) да; 14) да; 15) да; 16) да; 17) нет; 18) да; 19) нет; 20) да; 21) да; 22) да; 23) да; 24) да; 25) нет 26) да; 27) да; 28) да; 29) да; 30) да; 31) да; 32) нет; 33) нет; 34) да; 35) нет; 36) да; 37) нет; 38) да.

1.9. Прямое вычисление:

$$ab = aeb = a(ab)^2b = a(abab)b = a^2bab^2 = ba.$$

1.10. Указание. Первый способ: показать, что $|a| = 1$ для любого a из данной группы G порядка n. При $n > 1$ взять в G элемент $b = \cos(\psi) + i\sin(\psi)$ с наименьшим положительным аргументом ψ и проверить, что $G = \{1, b, b^2, \ldots, b^{n-1}\}$.

Второй способ: пользуясь теоремой Лагранжа, показать, что $a^n = 1$ для любого $a \in G$.

1.11. а) Одна группа — циклическая группа третьего порядка с элементами $\{e, a, a^2\}$ и таблицей

$$\begin{array}{|ccc|}\hline e & a & a^2 \\ a & a^2 & e \\ a^2 & e & a \\ \hline\end{array}.$$

В представлении перестановками можно положить:

$$e = (1)(2)(3),\ a = (123),\ a^2 = (132)$$

(e — единица).

Доказательство единственности см. на с. 15.

б) Существуют две группы порядка 4. По теореме Лагранжа порядки элементов должны делить 4.

Первая возможность: существует элемент порядка 4. Это циклическая группа четвертого порядка с элементами $\{e,\ a,\ a^2,\ a^3\}$ и таблицей

$$\begin{array}{|cccc|}\hline e & a & a^2 & a^3 \\ a & a^2 & a^3 & e \\ a^2 & a^3 & e & a \\ a^3 & e & a & a^2 \\ \hline\end{array}.$$

В представлении перестановками можно положить:

$$e = (1)(2)(3)(4),\ a = (1234),\ a^2 = (13)(24),\ a^3 = (1432)$$

(e — единица.)

Вторая возможность: все неединичные элементы имеют порядок 2. Поэтому группа коммутативна (задача 1.9). Если взять любые два неединичных элемента a, b, то четвертый элемент будет их произведением: $c = ab$. По этим данным таблица умножения восстанавливается однозначно:

$$\begin{array}{|cccc|}\hline e & a & b & ab \\ a & e & ab & b \\ b & ab & e & a \\ ab & b & a & e \\ \hline\end{array}.$$

В представлении перестановками можно положить:

$$e = (1)(2)(3)(4),\ a = (12)(34),\ b = (13)(24),\ c = (14)(23).$$

(e — единица).

Эта группа называется четвернóй группой Клейна V.

в) Существуют две группы порядка 6: циклическая группа C_6 и группа перестановок трех элементов S_3.

1.13. а) Указание. Проверить равенство $(1i) \circ (1j) \circ (1i) = (ij)$.

б) Указание. Проверить, что произведение двух транспозиций следующим образом выражается через тройные циклы:

$$(ik) \circ (ij) = (ijk), \quad (ij) \circ (kl) = (ilk) \circ (ijk).$$

в) Решение. Пусть G — подгруппа знакопеременной группы A_n, порожденная множеством указанных тройных циклов, и i, j, k — различные числа, большие двух (при $n = 3$ утверждение очевидно, а при $n = 4$ данное ниже доказательство упрощается). Вместе с циклом $(12i)$ группа G содержит обратный элемент $(i21)$, поэтому G содержит

$$(j21) \circ (12i) \circ (12j) = (1ij), \quad (12j) \circ (i21) \circ (j21) = (2ij).$$

При $n = 4$ группа G уже содержит все тройные циклы. При $n > 4$ она содержит

$$(k21) \circ (1ij) \circ (12k) = (ijk).$$

Значит, G содержит все тройные циклы и по пункту б) совпадает с A_n.

1.14. Ответ: 2.

При $\geqslant 3$ группа S_n не коммутативна и потому не является циклической. Осталось указать два элемента, порождающих S_n. Докажем, что $a = (01)$ и $b = (012\ldots(n-1))$ порождают всю группу перестановок (здесь удобно занумеровать элементы множества числами от 0 до $n-1$). Поскольку S_n порождается транспозициями (см. пример 1.39 на с. 39), для доказательства достаточно выразить любую транспозицию через a и b.

Сначала рассмотрим транспозиции соседних элементов $(i\,(i+1))$. Так как перестановка b^k переводит i в $(i+k) \bmod n$,

для перестановки $b^i a b^{-i}$ получаем:

$$i \overset{b^{-i}}{\longmapsto} 0 \overset{a}{\mapsto} 1 \overset{b^i}{\mapsto} i+1,$$

$$i+1 \overset{b^{-i}}{\longmapsto} 1 \overset{a}{\mapsto} 0 \overset{b^i}{\mapsto} i,$$

$$\text{если } k \neq i,\ i+1,\ \text{то} \quad k \overset{b^{-i}}{\longmapsto} k-i \overset{a}{\mapsto} k-i \overset{b^i}{\mapsto} k.$$

Значит, $(i\,(i+1)) = b^i a b^{-i}$.

Чтобы выразить любую транспозицию через транспозиции соседних, нужно индуктивно применять равенство

$$(ik) = (jk) \circ (ij) \circ (jk).$$

Предположим, что все транспозиции вида $(i\,(i+j))$ выражаются через транспозиции соседних при $j < k$. Тогда имеем выражение

$$(i\,(i+k) = ((k-1)\,k) \circ (i\,(k-1)) \circ ((k-1)\,k)$$

для транспозиции $(i\,(i+k)$, откуда по индукции заключаем, что всякая транспозиция выражается через транспозиции соседних.

1.19. а) Рассмотрим подгруппу H порядка $d = n/k$, порожденную элементом a^k. Она содержит e, a^k, a^{2k}, $\ldots$, $a^{(d-1)k}$. Если $(a^s)^d = e$, то sd кратно n, а s кратно k. Поэтому порядки подгрупп, порожденных элементами $G \setminus H$, отличаются от d. Но всякая подгруппа циклической группы — циклическая (теорема 1.27 на с. 30). Значит, H — единственная подгруппа порядка d.

б) Следует из а): любой элемент порядка d группы G порождает подгруппу порядка d, которая совпадает с H.

1.23. Указание а) Рассмотреть $(ab)^{pr}$ и $(ab)^{ps}$, где p — порядок ab. б) Рассмотреть $(ab)^p$, где p — порядок ab, и показать, что $a^p = b^{-p} = e$.

Пример 1. Для элементов $a \neq e$, $b = a^{-1}$ условие (1°) выполнено, а (2°) — нет. Утверждение б) не выполнено, так как порядки a и b равны между собой и не равны единице, а порядок $ab = e$ равен единице.

Пример 2. Элементы $a = (12)(3)$, $b = (123)$ симметрической группы S_3 имеют взаимно простые порядки 2 и 3. Условие (1°) не выполнено, так как $ab = (23)$, $ba = (13)$, а условие

(2°) выполнено. Утверждение б) не выполнено: a порядка 2, b порядка 3, ab порядка 2.

в) Обе части равенства $a^k = b^n$ возвести в степень s, равную порядку b.

г) Пример 3. В циклической группе C_8 с порождающим a элементы a, a^3, a^5 имеют порядок 8, но $aa^3 = a^4$ порядка 2, $aa^5 = a^6$ порядка 4.

1.26. Обозначим через $\varphi(n)$ количество порождающих элементов циклической группы C_n. (Это число совпадает с функцией Эйлера — количеством натуральных чисел, меньших n и взаимно простых с n. Впрочем, этот факт в решении никак не используется.)

Каждый элемент $a \in C_n$ порождает подгруппу $\langle a \rangle$ порядка $d(a)$. В циклической группе есть ровно одна подгруппа порядка d (задача 1.19), поэтому

$$n = \sum_{d|n} \varphi(d) \qquad (*)$$

(слева — все элементы группы, а справа — они же, но разбитые на множества порождающих элементов подгрупп).

Рассмотрим элемент порядка d. Он порождает подгруппу порядка d, элементы которой дают d решений уравнения $x^d = e$. Других решений по условию быть не может (по теореме Лагранжа d делит порядок группы). Значит, для любого делителя d порядка группы n либо вообще нет элементов порядка d, либо есть ровно $\varphi(d)$ элементов порядка d. Первый случай невозможен, так как иначе нарушилось бы равенство $(*)$. Поэтому в группе есть элементы порядка d для любого делителя n, в том числе и для самого n. Но это и означает, что группа — циклическая.

1.27. Порядок любого элемента группы делит порядок группы n, а порядок порождающего элемента циклической группы строго равен n. Поэтому показатель циклической группы совпадает с порядком.

В общем случае показатель r не превосходит порядка группы n. Рассмотрим делитель числа r вида p^a, где p — простое. Это означает, что в группе есть элемент порядка $p^a k$, т. е. p^a делит порядок группы. Но тогда и r делит порядок группы (здесь использована основная теорема арифметики).

Если $r < n$, то количество решений уравнения $x^r = e$ совпадает с порядком группы и больше, чем r. Такая группа не является циклической.

1.28. 2) и 3) для 1); 4) и 11) для 10); 1), 2), 3), 13), 14) для 8); 15) для 16); 20) и 21) для 18); 20) для 21); 24) для 23); 29) и 30) для 31); 34) для 36).

1.30. Бесконечная циклическая группа, все циклические группы простых порядков и единичная группа.

1.31. а) $C_6 = \langle a\rangle$, $\langle a^2\rangle$, $\langle a^3\rangle$, $\langle e\rangle$;

б) $C_{24} = \langle a\rangle$, $\langle a^2\rangle$, $\langle a^3\rangle$, $\langle a^4\rangle$, $\langle a^6\rangle$, $\langle a^8\rangle$, $\langle a^{12}\rangle$, $\langle e\rangle$;

в) $V = \{e, a, b, c = ab\}$, $\langle a\rangle$, $\langle b\rangle$, $\langle c\rangle$, $\langle e\rangle$;

г) применяя запись перестановок в циклах, получим подгруппы:

S_3, $\langle(123)\rangle$, $\langle(12)(3)\rangle$, $\langle(13)(2)\rangle$, $\langle(1)(23)\rangle$;

д) нормальными делителями будут S_3, $\langle(123)\rangle$, $\langle e\rangle$.

е) Указание. Разложение на циклы перестановки из A_4 может содержать лишь циклы длины 1 (тождественная перестановка), два цикла длины 2 (порядок 2) или один цикл длины 3 (порядок 3). Поэтому A_4 не имеет циклической подгруппы шестого порядка, а все ее элементы второго порядка перестановочны. Значит, A_4 не имеет подгруппы, изоморфной S_3. Но любая группа шестого порядка либо является циклической, либо изоморфна S_3 (задача 1.11 в)).

1.32. Выберем в G элемент $a \neq e$, затем $b \notin \{a, e\}$, затем $c \notin \{e, a, b, ab\}$. Тогда остальными элементами группы G будут ab, ac, bc, abc. Группа G абелева (задача 1.9). Она имеет следующие 16 подгрупп: $\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, $\{e, ab\}$, $\{e, ac\}$, $\{e, bc\}$, $\{e, abc\}$, $\{e, a, b, ab\}$, $\{e, a, c, ac\}$, $\{e, b, c, bc\}$, $\{e, a, bc, abc\}$, $\{e, b, ac, abc\}$, $\{e, c, ab, abc\}$, $\{e, ab, ac, bc\}$, $\{e,\ a,\ b,\ c,\ ab,\ ac,\ bc,\ abc\} = G$.

1.33. В аддитивной записи все подгруппы имеют вид $G_0 = \langle a\rangle$, $G_1 = \langle pa\rangle$, $G_2 = \langle p^2a\rangle$, $\ldots$, $G_{k-1} = \langle p^{k-1}a\rangle$, $G_k = \langle p^k a\rangle = \langle 0\rangle$. Они образуют убывающую цепочку подгрупп соответственно порядков p^k, p^{k-1}, p^{k-2}, $\ldots$, p, 1.

Указание. Использовать задачу 1.19 б) или показать, что подгруппа $\langle na\rangle$, где $0 < n < p^k$, совпадает с подгруппой $\langle p^m a\rangle$, где $n = p^m t$, $0 \leqslant m < k$ и t не делится на p.

1.41. Указание. Пусть K — множество всех элементов группы G, не принадлежащих H, и $a \in K$. Показать, что,

умножая a на все элементы из H, получим все элементы K. Вывести отсюда, что, умножая a на все элементы из K, получим все элементы из H. В частности, a^2 принадлежит H.

1.42. Примером может служить четверная группа V с элементами $e, a, b, c = ab$ (см. ответ задачи 1.11). Она имеет три циклические подгруппы второго порядка: $\langle a\rangle$, $\langle b\rangle$ и $\langle c\rangle$.

Указание. Доказать, что при возведении в квадрат всех тройных циклов мы получим снова все тройные циклы, и использовать задачи 1.13 и 1.41.

1.48. Гомоморфизм однозначно определяется образом порождающего элемента a. Ниже указаны возможные образы этого элемента: а) любой элемент группы; число гомоморфизмов равно n; б) e, b^3, b^6, b^9, b^{12}, b^{15}; в) e, b, b^2, b^3, b^4, b^5; г) e, b^5, b^{10}; д) e.

1.49. Рассмотрим гомоморфизм $\varphi\colon \mathbb{Q}^+ \to \mathbb{Z}^+$. Предположим, что $0 \neq x \in \operatorname{Ker}\varphi$, а $y \notin \operatorname{Ker}\varphi$. Некоторые ненулевые кратные любых двух рациональных чисел, отличных от 0, совпадают: если $x = p/q$, $y = r/s$, то $qrx = pr = spy$. Поэтому $\varphi(spy) = 0$ и приходим к противоречию (в $\mathbb{Z}^+$ нет элементов конечного порядка). Значит, либо ядро φ нулевое, либо совпадает с $\mathbb{Q}^+$. В последнем случае гомоморфизм переводит все рациональные числа в 0. Первый случай невозможен, так как гомоморфизм с нулевым ядром задает изоморфизм $\mathbb{Q}^+$ с некоторой подгруппой бесконечной циклической группы, а все такие группы — циклические. (Группа $\mathbb{Q}^+$ не является циклической — число $1/(2q)$ не принадлежит подгруппе, порожденной p/q.)

1.53. а) Указание. Каждому вращению тетраэдра $ABCD$ соответствует перестановка его вершин. Композиции двух вращений соответствует композиция соответствующих перестановок. Двум различным вращениям a и b соответствуют две различные перестановки, так как иначе нетождественному вращению ab^{-1} соответствовала бы тождественная перестановка, сохраняющая все вершины на месте. В группе тетраэдра 12 элементов (пример 1.28) и она изоморфна подгруппе (двенадцатого порядка) симметрической группы S_4. Далее, можно либо проверить, что все перестановки, соответствующие вращениям тетраэдра, четные, либо использовать задачу 1.42.

б) Решение. Группы куба и октаэдра изоморфны (см. пример 1.34). Каждому вращению куба соответствует перестановка его четырех диагоналей. Композиции вращений соответствует композиция соответствующих перестановок. Всего вращений куба 24 (пример 1.28). Это тождественное вращение, восемь вращений вокруг диагоналей на углы $2\pi/3$ и $4\pi/3$, шесть вращений вокруг осей, проходящих через середину противоположных ребер, на угол π, и девять вращений вокруг осей, проходящих через центры противоположных граней, на углы $\pi/4$, $2\pi/4$, $3\pi/4$. Непосредственной проверкой убеждаемся, что только при тождественном вращении все четыре диагонали остаются на месте. Отсюда заключаем, как в пункте а), что группа куба изоморфна группе перестановок четырех элементов, имеющей порядок 24, т. е. симметрической группе S_4.

в) Решение. Группы додекаэдра и икосаэдра изоморфны (пример 1.34). Для каждого ребра икосаэдра имеется одно противоположное параллельное ему ребро и две пары перпендикулярных ему ребер: рёбра одной пары начинаются в вершинах граней, примыкающих к данному ребру, а рёбра другой пары принадлежат граням, имеющим вершинами концы данного ребра. Ребра одной из этих пар параллельны, а разных пар — перпендикулярны между собой. Таким образом, все 30 ребер делятся на пять систем по шесть в каждой системе. Ребра одной системы либо параллельны, либо перпендикулярны, а рёбра разных систем не параллельны и не перпендикулярны. С каждой системой ребер связан октаэдр, вершинами которого служат середины ребер данной системы. Этим определены пять октаэдров, вписанных в икосаэдр. Каждому вращению икосаэдра соответствует перестановка пяти указанных систем ребер (или соответствующих им октаэдров). Композиции двух вращений соответствует композиция соответствующих перестановок. Вращений икосаэдра 60 (пример 1.28). Это тождественное вращение; 24 вращения вокруг каждой из шести осей, проходящих через противоположные вершины, на углы $2\pi/5$, $4\pi/5$, $6\pi/5$ и $8\pi/5$; 20 вращений вокруг каждой из десяти осей, проходящих через центры противоположных граней, на углы $2\pi/3$ и $4\pi/3$; 15 вращений вокруг каждой из пятнадцати осей, проходящих через

середины противоположных ребер, на угол π. Непосредственной проверкой убеждаемся, что для каждого нетождественного вращения найдется ребро, переводящееся данным вращением в другое ребро, не параллельное и не перпендикулярное данному ребру. Поэтому только тождественному вращению соответствует тождественная подстановка систем ребер. Отсюда, как в пункте а), заключаем, что группа икосаэдра изоморфна подгруппе порядка 60 симметрической группы S_5. По задаче 1.42 эта подгруппа совпадает со знакопеременной группой A_5.

1.60. Поскольку сопряженный с произведением является произведением сопряженных с множителями:

$$g(a_1a_2\dots a_n)g^{-1} = (ga_1g^{-1})(ga_2g^{-1})\dots(ga_ng^{-1}),$$

то сопряженный с коммутатору a, b посредством элемента g является коммутатором сопряженных gag^{-1} и gbg^{-1}. По тем же причинам сопряженный с произведением коммутаторов является произведением коммутаторов.

1.61. Докажем, что любая четная перестановка является композицией двух сопряженных инволюций (перестановок порядка 2). Отсюда будет следовать утверждение задачи, так как обратная к инволюции совпадает с ней.

Используем равенства

$$(1\,3\,5\,\dots\,(1+2k)\,2k\,(2k-2)\,\dots\,2) =$$
$$= \Big[(2\,3)(4\,5)\dots(2k\,(1+2k))\Big] \circ \Big[(1\,2)(3\,4)\dots((2k-1)\,2k)\Big], \qquad (*)$$

$$(1\,3\,5\,\dots\,(2k-1)\,2k\,(2k-2)\,\dots\,2) =$$
$$= \Big[(2\,3)(4\,5)\dots((2k-2)\,(2k-1))\Big] \circ \Big[(1\,2)(3\,4)\dots((2k-1)\,2k)\Big], \qquad (**)$$

$$(1\,2\,4\,\dots\,2k\,(2k-1)\,(2k-3)\,\dots\,3) =$$
$$= \Big[(1\,2)(3\,4)\dots((2k-1)\,2k)\Big] \circ \Big[(2\,3)(4\,5)\dots((2k-2)\,(2k-1))\Big]. \qquad (***)$$

Равенство $(*)$ выражает цикл нечетной длины в виде произведения инволюций одного циклового типа (следовательно,

сопряженных). Равенства $(**)$ и $(***)$ выражают цикл четной длины в виде произведения инволюций, в которых число циклов длины 2 различается на 1. Поэтому пару циклов четной длины можно представить в виде произведения сопряженных инволюций.

1.62. Указание. Наиболее естественный пример предоставляют свободные группы ранга $\geqslant 2$. (Определение и свойства свободных групп см. в [15, 17].)

1.64. В группе S_3 подгруппа $\{e, (12)(3)\}$ имеет индекс 3, но не содержит элемента $(13)(2)$ порядка 2.

1.69. Указания. а) Применить критерий сопряженности, описанный в примере 1.46. б) Показать, что каждый смежный класс содержит точно одну подстановку, оставляющую на месте число 4.

1.70. Если в разложении данной перестановки σ на независимые циклы встречается k_i циклов длины n_i, $i = 1, 2, \ldots, m$, причем учтены все циклы, включая и циклы длины 1, то число перестановок, коммутирующих с перестановкой σ, равно $\prod_{i=1}^{m}(k_i)!n_i^{k_i}$. Считая $0! = 1$, можно искомое число записать иначе. Пусть j_i — число циклов длины i, входящих в разложение перестановки σ, где $i = 1, 2, \ldots, n$, и если циклов длины i в разложении нет, то положим $j_i = 0$. Тогда искомое число равно $\prod_{i=1}^{n}(j_i)!i^{j_i}$.

Указание. Циклы одной и той же длины r, входящие в разложение σ, при сопряжении перестановкой x, коммутирующей с σ, могут лишь переставляться между собой, причем первое число какого-либо цикла может перейти в любое число любого цикла той же длины, входящего в разложение перестановки σ.

1.71. Указание. Рассмотреть коммутатор $h_1h_2h_1^{-1}h_2^{-1}$ этих элементов.

1.75. а) Прямо следует из определения нормализатора.

б) Группа G действует сопряжениями на множестве своих подгрупп

$$g\colon H \mapsto gHg^{-1}.$$

Нормализатор $N(H)$ является стабилизатором H относительно этого действия, а количество подгрупп, сопряженных с H, равно мощности орбиты H при этом действии, которая равна

индексу $(G : N(H))$ (см. следствие 1.53 на с. 49).

1.76. Указание. Использовать задачи: 1.74 в случае а), 1.75 в случае б).

1.79. Если в разложении данной перестановки σ на независимые циклы встречается k_i циклов длины n_i, $i = 1, 2, \ldots, m$, причем учтены все циклы, включая и циклы длины 1, то искомое число равно

$$\frac{n!}{\prod_{i=1}^{m}(k_i)!n_i^{k_i}}.$$

Это число можно записать иначе, пользуясь другим выражением знаменателя, указанным в ответе задачи 1.70.

1.80. Указание. Обозначить через n_k число классов сопряженных элементов с p^k элементами и, пользуясь задачей 1.76, показать, что $n_0 + n_1 p + n_2 p^2 + \cdots = p^n$.

1.81. Указание. Если нормальный делитель H содержит цикл (α, β, γ), то H содержит и любой другой 3-цикл $(\alpha', \beta', \gamma')$. Покажите это, рассмотрев сопряжение цикла (α, β, γ) посредством перестановки

$$x = \begin{pmatrix} \alpha & \beta & \gamma & \delta & \varepsilon & \ldots \\ \alpha' & \beta' & \gamma' & \delta' & \varepsilon' & \ldots \end{pmatrix},$$

где δ' и ε' выбраны так, что перестановка x четна. Далее используйте задачу 1.13 в).

1.82. Решение. а) Все 60 вращений, составляющие группу икосаэдра, указаны в ответе задачи 1.53 в). Тождественное вращение является единицей группы и составляет один класс. Сопряженные элементы имеют одинаковый порядок. Элементами пятого порядка являются 24 вращения на углы $2k\pi/5$, $k = 1, 2, 3, 4$, вокруг каждой из шести осей, проходящих через противоположные вершины. Под вращением вокруг вершины A на угол α будем понимать вращение вокруг оси, проходящей через A и противоположную вершину, на угол α против часовой стрелки, если смотреть вдоль оси от A к противоположной вершине. У каждой вершины отметим один из плоских углов с данной вершиной. Каждое вращение икосаэдра вполне характеризуется указанием вершины B, в которую переходит данная вершина A (B может совпадать с A), и плоского угла при B, в который переходит отмеченный угол при A.

Поэтому каждое вращение x, переводящее A в B, представляется в виде композиции $x = yz$, где y переводит отмеченный угол при A в отмеченный угол при B, а z есть вращение вокруг вершины B на угол α. Обратный элемент $x^{-1} = z^{-1}y^{-1}$ есть композиция вращения z^{-1} вокруг B на угол $(-\alpha)$ и вращения y^{-1}, переводящего отмеченный угол при B в отмеченный угол при A. Пусть теперь g — вращение вокруг вершины A на угол α, а x — любой элемент группы, переводящий A в B. Представляя x в виде композиции $x = yz$, как указано выше, найдем, что сопряженный элемент $x^{-1}gx = z^{-1}y^{-1}gyz$ является поворотом снова на угол α, но уже вокруг вершины B. В частности, если A и B — противоположные вершины, то поворот вокруг B на угол α совпадает с поворотом вокруг A на угол $2\pi - \alpha$. Таким образом, все вращения вокруг вершин на углы $2\pi/5$ и $8\pi/5$ принадлежат одному классу сопряженных элементов, так же как и все вращения на углы $4\pi/5$ и $6\pi/5$. Покажем, что вращения g_1 и g_2 вокруг вершины A на углы $2\pi/5$ и $4\pi/5$ принадлежат различным классам. Если x переводит A в другую вершину B, то $x^{-1}g_1x$ есть вращение вокруг B и либо не будет вращением вокруг A, либо (если B противоположна A) будет вращением вокруг A на угол $8\pi/5$, т. е. $x^{-1}g_1x \neq g_2$. Если же x — вращение вокруг A, то g_1 и x — элементы циклической (и, значит, коммутативной) подгруппы вращений вокруг A и снова $x^{-1}g_1x = g_1 \neq$ $\neq g_2$. Итак, все элементы пятого порядка разбиваются на два класса по 12 элементов. Аналогично, отмечая по плоскому углу каждой грани и по вершине каждого ребра, убедимся, что 20 элементов третьего порядка (вращения на углы $2\pi/3$ и $4\pi/3$ вокруг осей, проходящих через центры противоположных граней) составляют один класс и 15 элементов второго порядка (вращения на угол π вокруг осей, проходящих через середины противоположных ребер) также составляют один класс.

б) Нормальный делитель должен состоять из объединения классов сопряженных элементов, он должен содержать единицу, и его порядок должен делить порядок 60 группы икосаэдра. По пункту а) классы сопряженных элементов содержат соответственно 1, 12, 12, 20, 15 элементов. Из этих чисел можно составить лишь две суммы, содержащие слагаемое 1 и

делящие число 60, именно 1 и 60. Это дает лишь два нормальных делителя — единичную подгруппу и всю группу.

1.83. Указание. Применить задачи 1.53 в) и 1.82 б).

1.85. Ответы. а) Циклическая группа порядка d; б) циклическая группа порядка 5; в) циклическая группа порядка 6; г) циклическая группа порядка 2; д) $U \times U$ (см. задачу 1.88); е) аддитивная группа действительных чисел.

1.88. Указания. В случаях г), д) и з) рассмотреть отображении $f(z) = z^n$, а в случае е) — отображение $f(z) = z^n/|z|^n$.

1.92. Пусть $\varphi\colon G \to G$ — некоторый автоморфизм группы G, а $\psi\colon G \to G$ — внутренний автоморфизм, что по определению означает $\psi\colon x \mapsto gxg^{-1}$. Проверим, что сопряжение ψ посредством φ дает внутренний автоморфизм:

$$\varphi \circ \psi \circ \varphi^{-1}(x) = \varphi \circ \psi(y) = \varphi(gyg^{-1}) = \\ = \varphi(g)\varphi(y)\varphi(g^{-1}) = \varphi(g)x\varphi(g)^{-1}.$$

1.93. Указание: заполните пробелы в следующем кратком решении. Группа $GL(2, GF(5))$ линейных преобразований двумерного пространства над полем из 5 элементов действует на множестве одномерных подпространств этого пространства. Таких подпространств 6 штук, поэтому это действие является гомоморфизмом $GL(2, GF(5))$ в S_6. Обозначим образ при этом гомоморфизме через H. Можно проверить, что $(S_6 : H) = 6$. Группа S_6 действует на классах смежности по подгруппе H, что задает автоморфизм S_6. Этот автоморфизм не может быть внутренним: транспозиция переходит при этом автоморфизме в произведение трех транспозиций непересекающихся пар смежных классов.

1.96. Указание. Предположив, что G/Z — циклическая группа, выбрать в классе, служащем для нее порождающим элементом, элемент a и показать, что a и Z порождают всю группу G.

1.97. Решение. Применим индукцию по порядку n группы G. При $n = 2$ группа G — циклическая второго порядка, и теорема для нее верна. Пусть теорема верна для всех групп, порядок которых меньше n, и G — группа порядка n.

Пусть сначала G коммутативна. Возьмем любой элемент a, отличный от единицы e группы G. Его порядок $k > 1$. Если k

делится на p, $k = pq$, то элемент a^q имеет порядок p. Если k не делится на p, то порядок n' факторгруппы $G' = G/\langle a\rangle$ группы G по циклической подгруппе $\langle a\rangle$ равен $n/k < n$ и делится на p. По предположению индукции G' содержит элемент b' порядка p. Пусть b — элемент группы G, входящий в смежный класс b'. Из $(b')^p = e'$, где e' — единица группы G', следует, что b^p содержится в подгруппе $\langle a\rangle$, т. е. $b^p = a^l$, откуда $b^{pk} = a^{lk} = e$. Если $b^k = e$, то $(b')^k = e'$ и k делится на порядок p элемента b', что невозможно. Значит, $b^{kp} = e$, но $b \neq e$, т. е. элемент b^k имеет порядок p.

Пусть теперь группа G некоммутативна. Если существует подгруппа H, отличная от G, индекс которой не делится на p, то порядок H меньше n и делится на p. По предположению индукции H содержит элемент порядка p. Если же индексы всех подгрупп группы G, отличных от G, делятся на p, то число элементов, сопряженных с любым элементом группы G, не входящим в ее центр $C(G)$ (задача 1.59), делится на p (задача 1.74). Так как порядок n группы G также делится на p, то и порядок центра $C(G)$ делится на p и меньше n, так как G некоммутативна. По предположению индукции $C(G)$ содержит элемент порядка p.

1.98. Указание. Воспользоваться предыдущей задачей.

1.106. а) $\langle a\rangle = \langle 3a\rangle + \langle 2a\rangle$; б) $\langle a\rangle = \langle 4a\rangle + \langle 3a\rangle$; в) $\langle a\rangle = \langle 3a\rangle + \langle 4a\rangle + \langle 5a\rangle$; г) $\langle a\rangle = \langle 9a\rangle + \langle 100a\rangle$;

1.107. Указание. В случае в) использовать задачу 1.105 б).

1.108. Указания. а) Принять соответственно за A и B множества всех элементов a и b из G, для которых $pa = 0$ и $qb = 0$;

б) рассмотреть разложения $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ порядка n группы G на простые множители и применить а).

1.109. Обозначим через $G(n_1, n_2, \dots, n_s)$ прямую сумму циклических групп порядков соответственно $n_1, n_2, \dots, n_s$. Любая конечная абелева группа изоморфна $G(n_1, n_2, \dots, n_s)$, где числа n_k равны степеням простых чисел (не обязательно различных). В этих обозначениях приведем ответы:

а) $G(3)$; б) $G(4)$, $G(2,2)$; в) $G(2,3)$; г) $G(8)$, $G(2,4)$, $G(2,2,2)$;
д) $G(9)$, $G(3,3)$; е) $G(4,3)$, $G(2,2,3)$;
ж) $G(16)$, $G(2,8)$, $G(4,4)$, $G(2,2,4)$, $G(2,2,2,2)$;
з) $G(8,3)$, $G(2,4,3)$, $G(2,2,2,3)$;
и) $G(2,3,5)$; к) $G(4,9)$, $G(2,2,9)$, $G(4,3,3)$, $G(2,2,3,3)$;

л) $G(16,3)$, $G(2,8,3)$, $G(4,4,3)$, $G(2,2,4,3)$, $G(2,2,2,2,3)$;
м) $G(4,3,5)$, $G(2,2,3,5)$; н) $G(9,7)$, $G(3,3,7)$;
о) $G(8,9)$, $G(2,4,9)$, $G(2,2,2,9)$, $G(8,3,3)$, $G(2,4,3,3)$, $G(2,2,2,3,3)$;
п) $G(4,25)$, $G(2,2,25)$, $G(4,5,5)$, $G(2,2,5,5)$.

1.110. Если C_k — циклическая группа порядка k и Z — бесконечная циклическая группа, то искомое прямое разложение факторгруппы $\mathbb{Z}^3/H$ имеет вид: а) $C_2+C_2+C_3$; б) C_3+C_4; в) $C_2+C_3+C_3$; г) C_2+C_4; д) C_4+Z; е) $C_2+C_2+C_8$; ж) C_5; з) $Z+Z$; и) Z; к) $\mathbb{Z}^3/H$ — нулевая группа. Искомого разложения не существует.

1.111. в) Группа G единственным образом разлагается в прямую сумму подгрупп: $G=A_1+A_2+\cdots+A_s$, где A_i — циклическая подгруппа порядка p_i. Любая подгруппа H группы G, отличная от нулевой, является прямой суммой некоторых из подгрупп A_i. Число всех подгрупп равно 2^s.

Указание. Использовать пункт б) и показать, что если h — порождающий элемент подгруппы H, то H является прямой суммой тех подгрупп A_i, которые содержат ненулевые компоненты элемента h.

1.112. Указание. в) Для доказательства разложения $G=H+K$ взять любой элемент a_1 вне H, затем любой элемент a_2 вне $\{H,a_1\}$ и т. д., и положить $K=\{a_1,a_2,\dots\}$.

г) Любая подгруппа H порядка p^s разлагается в прямую сумму s циклических подгрупп порядка p. Пусть это разложение имеет вид

$$H=\langle a_1\rangle+\langle a_2\rangle+\cdots+\langle a_s\rangle.$$

Находим число всех систем $(a_1,a_2,\dots,a_s)$, определенных указанным образом для всех подгрупп H порядка p^s. Так как $a_1\neq 0$, то для a_1 имеем p^k-1 возможностей. Так как a_2 лежит вне циклической подгруппы $\langle a_1\rangle$, то для a_2 имеем p^k-p возможностей и т. д. Аналогично находим число всех систем $(a_1,a_2,\dots,a_s)$, дающих одну группу H порядка p^s. Число всех подгрупп порядка p^s равно частному двух найденных чисел.

1.113. Указание. Сначала рассмотреть случай примарной группы, затем взять разложение группы на примарные компоненты и применить задачу 1.105 б).

2.1. а) Кольцо. б) Кольцо. в) Кольцо. При $n = 0$ получаем нулевое кольцо, состоящее из одного числа 0, который будет единицей кольца и сам для себя противоположным. Нулевое кольцо не будет полем, так как поле должно содержать более одного элемента. г) Поле. д) Поле. е) Поле. ж) Кольцо. з) Поле. и) Кольцо. к) Поле. л) Кольцо. м) Кольцо. н) Кольцо. о) Кольцо. п) Кольцо. р) Матрицы с рациональными a, b образуют поле, а с действительными a, b — кольцо, но не поле. с) Полиномы от синусов и косинусов и полиномы от одних косинусов образуют кольцо, а от одних синусов не образуют. (Указание. В последнем случае использовать то, что произведение двух нечетных функций является функцией четной.)

2.2. г) Не образуют. Указание. Используя неприводимость многочлена $x^3 - 2$ над полем рациональных чисел, доказать, что $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ не принадлежит рассматриваемому множеству.

2.13. Делители нуля имеют вид $(a, 0)$, где $a \neq 0$ и $(0, b)$, где $b \neq 0$.

2.17. Матрицы, в которых элемент в левом верхнем углу отличен от нуля, не будут левыми (но будут правыми) делителями нуля.

2.24. Указание. Двумя разными способами раскрыть скобки в произведении $(a + b)(e + e)$.

2.26. Матрицы порядка $n \geqslant 2$ с элементами из данного поля при условии, что все строки, начиная со второй, состоят из нулей, образуют кольцо с несколькими левыми единицами, а при аналогичном условии для столбцов — с несколькими правыми единицами.

2.27. Указание. Показать, что если $a = ae$, то e — единица.

2.28. а) $a = p$ в кольце вычетов по модулю p^2; б) $a = p$ в кольце вычетов по модулю p^n. Здесь p — любое целое число, большее 1.

2.30. Указание. Для числа $a + b\sqrt{-3}$ ввести норму $N(z) = z \cdot \bar{z} = a^2 + 3b^2$. Доказать, что $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$; для данного $M > 0$ существует лишь конечное множество чисел z с $N(z) < M$, делителями единицы являются лишь ± 1, делитель с наименьшей нормой, большей 1, является простым.

2.31. Указание. Рассмотреть разложения

$$2 = 2^{1/2} \cdot 2^{1/2} = 2^{1/2} \cdot 2^{1/4} \cdot 2^{1/4} = \dots$$

2.35. а) Раскроем скобки в произведении

$$(a_0 + a_1 i + a_2 j + a_3 k)(a_0 - a_1 i - a_2 j - a_3 k)$$

и приведем подобные. Получится выражение $a_0^2 + a_1^2 + a_2^2 + a_3^2$, так как $i^2 = j^2 = k^2 = -1$, а остальные слагаемые сокращаются, так как $ij = -ji$, $ik = -ki$, $jk = -jk$.

б) Аксиомы кольца проверяются непосредственной подстановкой в определения. Легко также проверить справедливость следующей формулы для обратного к h кватерниона:

$$h^{-1} = \bar{h}/(h\bar{h}).$$

в) Будем записывать кватернион в виде суммы «действительной» и «мнимой» части: $h = h_0 + \boldsymbol{h}_1$, где $h_0 \in \mathbb{R}$, а $\boldsymbol{h}_1 = a_1 i + a_2 j + a_3 k$ рассматривается как вектор в трехмерном пространстве с ортонормированным базисом i, j, k. Из определения умножения кватернионов следует, что

$$hq = (h_0 q_0 - \boldsymbol{h}_1 \cdot \boldsymbol{h}_2) + h_0 \boldsymbol{q}_1 + q_0 \boldsymbol{h}_1 + \boldsymbol{h}_1 \times \boldsymbol{h}_2\,, \qquad (*)$$

здесь $\boldsymbol{a} \cdot \boldsymbol{b}$ — скалярное, а $\boldsymbol{a} \times \boldsymbol{b}$ — векторное произведение векторов.

Проверим, что поворот на угол θ вокруг оси, задаваемой единичным вектором v, в пространстве «чистых» кватернионов (с нулевой действительной частью) задается формулой

$$\boldsymbol{h} \mapsto (\cos(\theta/2) + \sin(\theta/2)\boldsymbol{v})\boldsymbol{h}(\cos(\theta/2) - \sin(\theta/2)\boldsymbol{v}). \qquad (**)$$

Проверку достаточно сделать в двух случаях: $\boldsymbol{h} = \boldsymbol{v}$ и $\boldsymbol{h} = \boldsymbol{u}$, где $\boldsymbol{u}$ — единичный вектор, перпендикулярный $\boldsymbol{v}$. На остальные векторы формула продолжится по линейности.

В первом случае действие $(**)$ не меняет вектора $\boldsymbol{v}$: используя $(*)$, можно проверить, что

$$(\cos(\theta/2) + \sin(\theta/2)\boldsymbol{v})\boldsymbol{v}(\cos(\theta/2) - \sin(\theta/2)\boldsymbol{v}) = \boldsymbol{v}.$$

Во втором случае вычисления приводят к следующему результату

$$(\cos(\theta/2) + \sin(\theta/2)\boldsymbol{v})\boldsymbol{u}(\cos(\theta/2) - \sin(\theta/2)\boldsymbol{v}) = \\ = \cos\theta\boldsymbol{u} + \sin\theta(\boldsymbol{v} \times \boldsymbol{u}),$$

т. е. $\boldsymbol{u}$ переходит в $\cos\theta\boldsymbol{u} + \sin\theta(\boldsymbol{v} \times \boldsymbol{u})$, что совпадает с поворотом на угол θ.

На формулу $(**)$ можно посмотреть иначе: $\boldsymbol{h} \mapsto q\boldsymbol{h}q^{-1}$, где q — кватернион нормы 1. Но композиция сопряжений посредством двух кватернионов совпадает с сопряжением посредством произведения этих кватернионов. Отсюда и получается требуемый гомоморфизм.

2.36. Указание. Найти матрицы E, I, J, K, соответствующие единицам 1, i, j, k и проверить таблицу умножения для них: $I^2 = J^2 = K^2 = -E$, $IJ = -JI = K$, $JK = -KJ = I$, $KI = -IK = J$.

2.44. Если $ne \neq 0$ для любого $n \neq 0$ из $\mathbb{Z}$, то φ — изоморфизм, и $\varphi(\mathbb{Z})$ изоморфно $\mathbb{Z}$. Если $ne = 0$ для некоторого $n \neq 0$ из $\mathbb{Z}$ и d — наименьшее положительное число, для которого $de = 0$, то $\varphi(\mathbb{Z})$ изоморфно кольцу вычетов по модулю d.

2.45. а) Идеал; б) подкольцо; в) идеал; г) не является подгруппой аддитивной группы; д) подкольцо; е) подгруппа аддитивной группы; ж) идеал; з) подкольцо; и) идеал; к) идеал; л) не является подгруппой аддитивной группы.

2.62. Указание. Пусть a — элемент кольца, отличный от нуля. Показать, что соответствие $x \mapsto ax$, где x — любой элемент, является взаимно однозначным отображением данного кольца на себя.

2.65. $\frac{1}{43}(5 + 9\sqrt[3]{2} - \sqrt[3]{4})$. Указание. Для доказательства однозначности использовать неприводимость многочлена $x^3 - 2$ над полем рациональных чисел. Для отыскания обратного элемента применить метод неопределенных коэффициентов.

2.66. $x^{-1} = \frac{1}{123}(34 + 14\sqrt[3]{5} + 13\sqrt[3]{25})$.

2.67. Указание. Использовать, что неприводимый многочлен взаимно прост с любым многочленом меньшей степени.

2.68. $\beta^{-1} = \frac{1}{405}(101 + 37\alpha + 4\alpha^2)$. Указание. Пусть $\varphi(x) = x^2 - x + 3$. Методом неопределенных коэффициентов найти многочлены $f_1(x)$ первой степени и $\varphi_1(x)$ второй степени, удовлетворяющие равенству $f(x)f_1(x) + \varphi(x)\varphi_1(x) = 1$, и положить в этом равенстве $x = \alpha$.

2.71. Указание. Рассмотреть образы единицы, целых и дробных чисел.

2.72. Указание. Показать, что положительное число, как квадрат действительного числа, переходит в положительное.

Затем доказать, что любое действительное число переходит в себя, используя то, что любое рациональное число переходит в себя, и то, что между двумя различными действительными числами лежит рациональное число.

2.73. Возможны лишь два таких автоморфизма: тождественный и переводящий каждое число в сопряженное.

2.78. Ответ: $a^{(n,m)} - 1$. Указание: см. доказательство теоремы 3.37.

2.79. а) $x + 2$; б) 1.

2.80. а) 1; б) $5x + 1$.

2.81. а) $x^2 + x - 1$; б) 1.

2.84. Обозначим через G группу обратимых элементов кольца $\mathbb{Z}/(p^n)$. Так как $|G| = (p-1)p^{n-1}$, из теоремы о конечных абелевых группах заключаем, что $G \cong A \times B$, где A состоит из элементов G, порядки которых делят $p-1$, а B — из элементов G, порядки которых делят p^{n-1}, причем $|A| = p-1$, $|B| = p^{n-1}$.

Теперь рассмотрим последовательность

$$H_0 \supset H_1 \supset \dots H_{n-1} = \{1\}$$

подгрупп в G, где

$$H_k = \{1 + p^{k+1}x\}.$$

Из формулы бинома и неравенств $3k \geqslant k+2$, $2k+2 \geqslant k+2$, справедливых при $k \geqslant 1$, получаем

$$(1+p^k x)^p \equiv 1 + p^{k+1}x + \binom{p}{2} p^{2k}x^2 \equiv 1 + p^{k+1}x \pmod{p^{k+2}} \quad (*)$$

($\binom{p}{2}$ делится на p^2 при $p \geqslant 3$).

Равенство $(*)$ означает, что образ H_{k-1} при возведении в степень p лежит в H_k, но не лежит в H_{k+1}. Поэтому в H_0 есть элемент порядка p^{n-1}. Значит, $B = H_0$ и B — циклическая.

Группа A изоморфна $G/B = G/H_0$. Но последняя группа совпадает с группой группой обратимых элементов $\mathbb{Z}/(p)$, которая является мультипликативной группой поля и потому циклическая порядка $p-1$.

Теперь цикличность G следует из того, что G является прямым произведением циклических групп взаимно простых порядков.

2.86. б) Четыре смежных класса, состоящие из чисел $a+bi$ со свойствами: 1) a и b четны; 2) a четно, а b нечетно; 3) a нечетно, а b четно; 4) a и b нечетны; в) класс B, содержащий $1+i$, является делителем нуля, причем $B^2=0$.

3.4. Решим уравнение $103x+73y=1$ в целых числах расширенным алгоритмом Евклида (см. с. 108).

Вычисления удобно свести в таблицу

a_i	a_{i+1}	q_{i+1}	x	y
103	73	1	-90	$37-1\cdot(-90)=127$
73	30	2	37	$-16-2\cdot 37=-90$
30	13	2	-16	$5-2\cdot(-16)=37$
13	4	3	5	$-1-3\cdot 5=-16$
4	1	4	-1	5

Получаем ответ $y=127=24 \pmod{103}$.

3.5. По модулю 3 система несовместна, а по модулю 5 она имеет единственное решение $x=2$, $y=3$, $z=2$.

3.6. По модулю 5 система несовместна, а по модулю 7 она имеет единственное решение $x=2$, $y=6$, $z=5$.

3.7. При $p=2$ квадратичных вычетов больше $(1>0)$. При $p>2$ количество квадратичных вычетов и квадратичных невычетов одинаково.

Поскольку $(-a)^2=a^2$, возведение в квадрат спаривает ненулевые элементы. В поле у уравнения $x^2=a$ не больше двух корней. Поэтому квадратов среди ненулевых вычетов ровно половина.

3.8. Все ненулевые элементы поля $GF(p)$ являются корнями многочлена

$$x^{p-1}-1=(x^{(p-1)/2}-1)(x^{(p-1)/2}+1).$$

Но для любого вычета a имеем $a=x^2$, значит $a^{(p-1)/2}=x^{p-1}=1$. Поэтому квадратичные вычеты — это в точности корни многочлена $x^{(p-1)/2}-1$, а квадратичные невычеты — корни многочлена $x^{(p-1)/2}+1$.

3.9. -1.

3.10. 0.

3.11. Для $p=2$ утверждение тривиально. Рассмотрим случай простого $p>2$. Ненулевые вычеты по модулю p являются

корнями уравнения $x^{p-1}-1=0$ в поле $GF(p)$. Других корней у этого уравнения нет (многочлен степени $p-1$ имеет не больше $p-1$ корня). По теореме Виета произведение всех ненулевых вычетов равно свободному члену (так как $p-1$ четно).

3.13. 2006-е степени ненулевых вычетов образуют подгруппу мультипликативной группы поля $GF(17)$. Так как 2006 не делится на $17-1=16$, эта группа собственная. Поэтому сумма из условия задачи по модулю 17 равна некоторому кратному суммы по элементам подгруппы мультипликативной группы индекса $k>1$. Эти элементы, и в точности они, являются корнями уравнения $x^k-1=0$. По теореме Виета их сумма равна 0.

3.19. а) Решение. Предположим, что $f(x)$ и $g(x)$ имеют над полем $\mathbb{Q}$ общий делитель $d(x)$ положительной степени. Тогда $f(x)=a(x)d(x)$, $g(x)=b(x)d(x)$, где $a(x)$, $b(x)$, $d(x)$ — многочлены над $\mathbb{Q}$. Вынося общие знаменатели и общие наибольшие делители числителей коэффициентов и применяя лемму Гаусса о произведении примитивных многочленов, получим: $f(x)=a_1(x)d_1(x)$, $g(x)=b_1(x)d_1(x)$, где все многочлены имеют целые коэффициенты, степень $d_1(x)$ равна степени $d(x)$ и старший коэффициент $d_1(x)$ не делится на p. Переходя к полю вычетов по модулю p, получим общий делитель положительной степени для $f(x)$ и $g(x)$ над этим полем, что невозможно.

б) Многочлены $f(x)=x$, $g(x)=x+p$ взаимно просты над полем рациональных чисел и равны x, т. е. не взаимно просты, над полем вычетов по модулю p.

3.20. Указание. Если $f(x)$ и $g(x)$ взаимно просты, то, получив равенство $f(x)u(x)+g(x)v(x)=c$, где $u(x)$, $v(x)$ — многочлены с целыми коэффициентами и c — целое число, доказать, что $f(x)$ и $g(x)$ взаимно просты над полем вычетов по любому простому p, не делящему c. При доказательстве обратного утверждения использовать задачу 3.19.

3.21. Указание. Применяя лемму Гаусса, из разложения $f(x)$ на два множителя с рациональными коэффициентами получить разложение на два множителя с целыми коэффициентами. Многочлен $f(x)=px^2+(p+1)x+1=(px+1)(x+1)$ приводим над полем рациональных чисел, но по модулю p равен $x+1$ и, значит, неприводим.

3.22. Решение. Сначала докажем лемму из теории групп. Если два элемента a и b циклической группы G не являются квадратами, то их произведение является квадратом. Множество H элементов из G, являющихся квадратами, есть подгруппа. Факторгруппа G/H — циклическая. Если $D = dH$ — ее порождающий, то из $d^2 \in H$ следует $D^2 = d^2H = H$. Значит, или $H = G$, или G/H — группа второго порядка и $ab \in aH \cdot bH = H$, т. е. ab есть квадрат.

Отсюда следует, что по любому простому модулю p одно из чисел 2, 3, 6 сравнимо с квадратом. В самом деле, при $p = 2$ имеем $2 \equiv 0^2$, при $p = 3$ также $3 \equiv 0^2$. Если $p > 3$, то 2 и 3 можно рассматривать как элементы мультипликативной группы G поля вычетов по модулю p. Согласно теореме 3.44 группа G — циклическая и по лемме, доказанной выше, если 2 и 3 — не квадраты, то $2 \cdot 3 = 6$ — квадрат. Многочлен

$$(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) = \\ = x^4 - 10x^2 + 1$$

неприводим над полем рациональных чисел, так как линейные множители и их произведения по два не являются многочленами с рациональными коэффициентами. Пусть $GF(p)$ — поле вычетов по простому модулю p. По доказанному существует элемент $a \in GF(p)$, для которого $a^2 = 2$, или $a^2 = 3$, или $a^2 = 6$.

Если $a^2 = 2$, то $x^4 - 10x^2 + 1 = (x^2 + 2ax - 1)(x^2 - 2ax - 1)$;
если $a^2 = 3$, то $x^4 - 10x^2 + 1 = (x^2 + 2ax + 1)(x^2 - 2ax + 1)$;
если $a^2 = 6$, то $x^4 - 10x^2 + 1 = (x^2 + 2a - 5)(x^2 - 2a - 5)$.

3.28. Два. Уравнение $x^{23} - x^7 - 1 = 0$ имеет в поле $GF(2^4)$ столько же решений, сколько и уравнение $x^{46} - x^{14} - 1 = 0$ (автоморфизм Фробениуса). Используя равенства $x^{15} = 1$ и $+1 = -1$, упростим уравнение

$$x^{46} - x^{14} - 1 = x - x^{-1} - 1 = \frac{x^2 + x + 1}{x}\,.$$

Поле $GF(2^4)$ содержит подполе $GF(2^2)$, в котором у многочлена $x^2 + x + 1$ два корня.

3.29. Производная монома $(x^n)' = nx^{n-1}$ тождественно равна 0 только если $p \mid n$. Поэтому показатели степеней всех мономов многочлена f делят p, значит $f(x) = g(x^p) = g^p(x)$.

3.30. Если многочлен f взаимно прост со своей производной, то (утверждение 3.47) он является произведением неприводимых многочленов f_i в первой степени

$$f = f_1 \cdot f_2 \cdot \ldots \cdot f_k \,.$$

По китайской теореме об остатках $F[x]/(f) \cong F[x]/(f_1) \oplus \oplus F[x]/(f_2) \ldots \oplus F[x]/(f_k)$. Каждый сомножитель в этой сумме является полем (так как f_i — неприводимые). Уравнение $x^p = x$ имеет p корней в любом поле характеристики p (в точности элементы подполя $GF(p)$, которое есть в любом поле характеристики p). Поэтому число решений уравнения $x^p = x$ в кольце $F[x]/(f)$ равно p^k.

3.31. Используем обозначения предыдущей задачи. Корень v можно задать последовательностью $v_1, \ldots, v_k$ остатков от деления v на f_i (китайская теорема). Так как $v^p = v$, то $v_i \in \{0, 1, \ldots, p-1\}$. Если все v_i одинаковы, то $v \in \{0, 1, \ldots, p-1\}$. Без ограничения общности считаем, что $v_1 \neq v_2$. Тогда $v - v_1$ делится на f_1 и не делится на f_2. Поэтому $(v - v_1, f) \neq 1$.

3.32. Можно, например, использовать интерполяционный многочлен Лагранжа (3.7):

$$f(x) = \sum_{a \in GF(p^n)} f(a) \frac{\prod_{b \in GF(p^n) \setminus \{a\}} (x - b)}{\prod_{b \in GF(p^n) \setminus \{a\}} (a - b)} \,.$$

3.34. $(x+1)^3(x^2+x+1)$.

3.35. $(x+3)(x^2+4x+2)$.

3.36. $(x^2+1)(x^2+x+2)$.

3.37. $(x^2+x+1)(x^2+2x+4)$.

3.38. $f_1 = x^2$, $f_2 = x^2+1 = (x+1)^2$, $f_3 = x^2+x = x(x+1)$, $f_4 = x^2+x+1$ неприводим.

3.39. $f_1 = x^3$, $f_2 = x^3+1 = (x+1)(x^2+x+1)$, $f_3 = x^3+x = = x(x+1)^2$, $f_4 = x^3+x^2 = x^2(x+1)$, $f_5 = x^3+x+1$ неприводим, $f_6 = x^3+x^2+1$ неприводим, $f_7 = x^3+x^2+x = x(x^2+x+1)$, $f_8 = x^3+x^2+x+1 = (x+1)^3$.

3.40. $f_1 = x^2+1$, $f_2 = x^2+x+2$, $f_3 = x^2+2x+2$.

3.41. $f_1 = x^3+2x+1$, $f_2 = x^3+2x+2$, $f_3 = x^3+x^2+2$, $f_4 = x^3+2x^2+1$, $f_5 = x^3+x^2+x+2$, $f_6 = x^3+x^2+2x+1$, $f_7 = x^3+2x^2+x+1$, $f_8 = x^3+2x^2+2x+2$.

3.48. Нужно найти наименьшее k такое, что $19 \mid 2^k - 1$ или, что то же самое $2^k \equiv 1 \pmod{19}$. Такое k нужно искать среди делителей $19-1 = 18$. Так как $2^9 = 2 \cdot 16^2 = 2 \cdot 9 = -1 \pmod{19}$, а $2^6 = 4 \cdot 2^4 = -12 \pmod{19}$, то ни один собственный делитель 18 не подходит.

Ответ: искомое поле имеет 2^{18} элементов.

3.50. Рассмотрим поле $F = GF(p)/(f)$, $\deg f = n$. Класс вычетов $\alpha = \{x\}$ является корнем уравнения $f(x) = 0$ в этом поле. По теореме 3.41 остальными корнями этого уравнения будут α^{p^i}. Множество корней этого уравнения сохраняется при действии любого автоморфизма.

Любой автоморфизм $\varphi\colon F \to F$ переводит элементы подполя $GF(p) \subset F$ в себя (так $\varphi(1) = 1$). Если $\varphi(\alpha) = \alpha$, то тогда φ — тождественный, так как все элементы поля выражаются через 1, α. Значит, есть не более одного автоморфизма, переводящего α в α^{p^i}. Но один такой автоморфизм точно есть — это i-я степень автоморфизма Фробениуса.

Итак, мы доказали, что никаких автоморфизмов поля F, кроме степеней автоморфизма Фробениуса, у поля F нет.

3.51. Рассмотрим трехмерное векторное пространство F^3 над полем F из q элементов. «Точками» проективной плоскости порядка q будут одномерные подпространства F^3, а «прямыми» — двумерные подпространства. Отношение инцидентности «прямая проходит через точку» зададим очевидным образом: если одномерное подпространство V содержится в двумерном подпространстве W, то W проходит через V.

Проверим выполнение свойств конечной проективной плоскости.

Любые два несовпадающих одномерных подпространства V_1, V_2 содержатся в двумерном подпространстве $V_1 + V_2$, состоящем из линейных комбинаций их векторов. Любое другое подпространство, содержащее V_1 и V_2, должно содержать и $V_1 + V_2$. Отсюда следует, что через любые две различные «точки» проходит ровно одна «прямая».

Два различных двумерных подпространства $W_1 \neq W_2$ обязаны пересекаться по ненулевому вектору (иначе в F^3 нашлось бы четыре линейно независимых вектора). Отсюда следует, что любые две различные «прямые» проходят через одну «точку».

Выберем некоторое одномерное подпространство $V \subset F^3$. На факторгруппе F^3/V естественно вводится структура векторного пространства над полем F, это пространство двумерно. Канонический гомоморфизм $F^3 \to F^3/V$ устанавливает взаимно однозначное соответствие между одномерными подпространствами в F^2 и двумерными подпространствами в F^3, содержащими V. Отсюда уже следует, что на каждой «прямой» лежит столько же «точек», сколько «прямых» проходит через данную «точку». Чтобы найти это число, заметим, что одномерное подпространство в F^2 однозначно задается любым своим ненулевым вектором, и каждому такому пространству принадлежит ровно $q-1$ ненулевой вектор. Всего ненулевых векторов в F^2 имеется q^2-1 штук. Поэтому, количество одномерных подпространств в F^2 равно

$$\frac{q^2-1}{q-1} = q+1.$$

3.52. а) Если $a=0$ или $b=0$, то равенство очевидно. Для ненулевых a, b оно следует из того, что множество квадратов ненулевых элементов поля образует подгруппу (индекса 2) мультипликативной группы поля.

б) Так как мультипликативная группа поля циклическая, квадраты ненулевых элементов поля и только они удовлетворяют равенству

$$a^{(q-1)/2} = 1.$$

Если $p^m = 4k \pm 1$, то $(-1)^{(p^m-1)/2} = \pm 1$, что и требовалось.

в) Это равенство говорит, что в подгруппе и ее (единственном) смежном классе одинаковое количество элементов.

г) Вклад $a=0$ в сумму нулевой. Если $a \neq 0$, то запишем $a+b=ac$ и

$$\sum_{a\neq 0} \chi(a)\chi(a+b) = \sum_{a\neq 0} \chi(a)\chi(ac) =$$

$$= \sum_{a\neq 0} \chi(a)\chi(a)\chi(c) = \sum_{a\neq 0} \chi\left(1+\frac{b}{a}\right).$$

При $a \neq 0$ выражение b/a принимает все возможные значения, кроме 0. Поэтому последняя сумма отличается от суммы из пункта в) на $-\chi(1) = -1$.

3.53. Приводимая ниже конструкция матриц Адамара называется конструкцией Пейли (см. [18]). Она использует свойства квадратичных вычетов в произвольном конечном поле, сформулированные в предыдущей задаче.

Вначале построим матрицу Q порядка p^m, строки и столбцы которой индексированы элементами поля F из p^m элементов. Полагаем $Q_{ab} = \chi(a-b)$.

Так как $p^m + 1 \equiv 0 \pmod 4$, то $\chi(a-b) = \chi(-1)\chi(b-a) = -\chi(b-a)$, т. е. матрица Q является кососимметрической. Кроме того, выполняются матричные равенства $QJ = JQ = 0$, где J — матрица из одних единиц. Эти равенства в точности означают, что в каждой строке и каждом столбце количество $+1$ равно количеству -1 (пункт в) предыдущей задачи).

Теперь проверим, что $QQ^T = p^m I - J$. Для диагональных элементов получаем

$$(QQ^T)_{aa} = \sum_b Q_{ab}^2 = p^m - 1,$$

а для внедиагональных применяем равенство из пункта г) предыдущей задачи:

$$(QQ^T)_{ab} = \sum_c Q_{ac}Q_{bc} = \sum_c \chi(a-c)\chi(b-c) = \sum_x \chi(x)\chi(x+b-a) = -1.$$

Искомая матрица Адамара имеет вид

$$H = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & Q - I \end{pmatrix},$$

где $\mathbf{1}$ — строка из одних единиц длины p^m. Элементы этой матрицы равны ± 1 по построению. Для HH^T имеем

$$HH^T = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & Q - I \end{pmatrix} \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & Q^T - I \end{pmatrix} = \begin{pmatrix} p^m + 1 & 0 \\ 0 & J + (Q-I)(Q^T - I) \end{pmatrix}$$

Но $J + (Q-I)(Q^T - I) = J + p^m I - J - Q - Q^T + I = (p^m + 1)I$. Поэтому выполняется искомое равенство $HH^T = (p^m + 1)I$.

Список литературы

[1] *Алексеев В. Б.* Теорема Абеля в задачах и решениях. М.: МЦНМО, 2001.

[2] *Беклемишев Д. В.* Курс аналитической геометрии и линейной алгебры. М.: Наука, 1988.

[3] *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.

[4] *Ван дер Варден Б.:Л.* Алгебра. М.: Наука, 1976.

[5] *Винберг Э. Б.* Курс алгебры. М.: Факториал, 1999.

[6] *Виноградов И. М.* Основы теории чисел. М.: Наука, 1972.

[7] *Влэдуц С. Г.*, *Ногин Д. Ю.*, *Цфасман М. А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003.

[8] *Гельфанд И. М.* Лекции по линейной алгебре. М.: Наука, 1971.

[9] *Горенстейн Д.* Конечные простые группы. Введение в их классификацию. М.: Мир, 1985.

[10] *Каргаполов М. И.*, *Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1977.

[11] *Кострикин А. И.* Введение в алгебру. М.: Наука, 1977.

[12] Кострикин А. И. (ред.) Сборник задач по алгебре. М.: Факториал, 1995.

[13] *Кострикин А. И.*, *Манин Ю. И.* Линейная алгебра и геометрия. М.: Наука, 1986.

[14] *Курош А. Г.* Курс высшей алгебры. М.: Наука, 1975.

[15] *Ленг С.* Алгебра. М.: Мир, 1968.

[16] *Лидл Р.*, *Нидерейтер Х.* Конечные поля. М.: Мир, 1989.

[17] *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. М.: Наука, 1974.

[18] *Мак-Вильямс Ф. Дж., Слоан Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.

[19] *Прасолов В. В.* Многочлены. М.: МЦНМО, 1999.

[20] *Прасолов В. В.* Задачи и теоремы линейной алгебры. М.: Наука. Физматлит, 1996.

[21] *Серр Ж.-П.* Курс арифметики. М.: Мир, 1972.

[22] *Холл М.* Теория групп. М.: ИЛ, 1962.

Предметный указатель

About authors of the book

Yurii I. Zhuravlev — Academician of the Russian Academy of Sciences, Deputy Director of Dorodnicyn Computing Centre of the Russian Academy of Science, Head of Scientific Council "Cybernetics" of Russian Academy of Sciences, Head of the Chair of Moscow state University, Professor of Moscow Institute of Physics and Technology. Editor-in-Chief of International Journal "Pattern Recognition and Image Processing".

Research interests: mathematical logic, theory of controlling systems, pattern recognition and image analysis, operations research, artificial intelligence.

Yurii A. Flerov — Corresponding Member of the Russian Academy of Sciences, Deputy Director of Dorodnicyn Computing Centre of the Russian Academy of Science, Professor of Moscow Institute of Physics and Technology.

Research interests: mathematical modelling, computer-aided design.

Mikhail N. Vyalyi — PhD (Physics, Mathematics), research scientist of the department "Mathematical Pattern Recognition and Methods of Combinatorial Analysis" of Dorodnicyn Computing Centre of the Russian Academy of Science, Assistant Professor at Moscow Institute of Physics and Technology.

Research interests: complexity theory, quantum computations.

This book is based on lectures of Yu. I. Zhuravlev that were read in Moscow Institute of Physics and Technology. The second part of the course "Discrete Analysis" is devoted to an introduction to basic algebraic structures: groups, rings and fields.

The central topic is finite fields. They are the very important tool in applications to combinatorics and computer science. As an example of application of finite fields, a brief introduction to error-correcting codes is given.

The book is supplied with large number of problems. Some of them are mere exercises to check the understanding of basic material in the book, some provide extra information on the objects in study.

Level: undergraduates.

Книга основана на курсе лекций, прочитанных Ю. И. Журавлёвым в Московском физико-техническом институте. Это вторая часть курса «Дискретный анализ», она посвящена введению в высшую алгебру, в ней рассматриваются основные свойства групп, колец и полей.

Центральную роль играет теория конечных полей. Конечные поля являются одним из важнейших инструментов в комбинаторике и теоретической информатике. Как пример приложения конечных полей приводится теория кодов, исправляющих ошибки.

Книга содержит много задач. Часть из них — упражнения на понимание материала основной части книги, часть дает представление о дальнейших результатах в теории групп, колец и полей.

Книга предназначена для изучения основ высшей алгебры студентами младших курсов. Наиболее полезной она окажется для студентов, специализирующихся на прикладной математике.

Ю. И. Журавлёв,
Ю. А. Флёров,
М. Н. Вялый

В издательстве «МЗ Пресс» при участии Московского физико-технического института в серии «Естественные науки. Математика. Информатика» выпущены следующие книги:

1. **Лабораторный практикум по курсу «Основы вычислительной математики».** Иванов В.Д., Косарев В.И., Лобанов А.И., Петров И.Б. и др. 1-е изд. (2001), 2-е изд. (2003), 194 с.

2. **Теория и реализация языков программирования.** Учебное пособие. Серебряков В. А., Галочкин М. П., Гончар Д. Р., Фуругян М. Г., 1-е изд., 2003, 296 с.

3. **Основы теории случайных процессов.** Учебное пособие. Натан А. А., Горбачев О. Г., Гуз С. А., 2003, 168 с.

4. **Оптимизация. Элементы теории. Численные методы.** Учебное пособие. Бирюков С. И., 2003, 248 с.

5. **Введение в нелинейную физику плазмы.** Учебное пособие. Кингсеп А. С., 2004, 264 с.

6. **Ряды Фурье. Интегралы, зависящие от параметра, и обобщенные функции.** Курс лекций. Черняев А. П., 2004, 149 с.

7. **Математическая статистика.** Натан А. А., Горбачев О. Г., Гуз С. А., 2005, 160 с.

8. **Современные проблемы прикладной математики.** Сборник научно-популярных статей. Под ред. Петрова А. А., 2005, 232 стр.

9. **Опыт имитационного моделирования при анализе социально-экономических явлений.** Павловский Ю. Н., Белотелов Н. В., Бродский Ю. И., Оленев Н. Н., 2005, 136 с.

10. **Структурная согласованность данных и знаний.** Учебное пособие. Дулин С. К., 2005, 144 с.

11. **Теория и реализация языков программирования.** Учебное пособие. Серебряков В. А., Галочкин М. П., Гончар Д. Р., Фуругян М. Г., 2-е изд., допол. и испр., 2006, 352 с.

12. **Дискретный анализ. Основы общей алгебры.** Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н., 1-е изд., 2006, 208 с.

13. **Симметрии уравнений Гамильтона и Лагранжа.** Яковенко Г. Н., 2006, 120 с.

14. **Математическое моделирование газодинамических процессов с источниками.** Волосевич П. П., Ермолин Е. В., Леванов Е. И., 2006, 216 с.

15. **Лекции по теории игр и экономическому моделированию.** Меньшиков И. С., 2007, 208 с.

16. **Механика космического полета. Орбитальное движение.** Учебное пособие. Мирер С. А., 2007, 270 с.

Издательство **«МЗ Пресс»**
тел. 8-916-916-12-09
e-mail: mzpress@mail.ru

Учебное издание

Журавлёв Юрий Иванович, *Флёров Юрий Арсеньевич*,
Вялый Михаил Николаевич

Дискретный анализ. Основы высшей алгебры

Издание второе, исправленное и дополненное

Издатель *З. А. Отарашвили*
Компьютерная верстка: *М. Н. Вялый*

Подписано в печать 06.04.2007 г. Формат 60×84/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 14,0.
Тираж 1000 экз. Заказ №

Отпечатано в ОАО «Калужская типография стандартов»
248021, г. Калуга, ул. Московская, 256