МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Нижегородский государственный университет им. Н.И. Лобачевского

М.М. Шульц

АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

ЗАДАЧИ И РЕШЕНИЯ

Учебно-методическое пособие

Рекомендовано методической комиссией факультета ВМК
для студентов ННГУ, обучающихся по направлениям подготовки
010400 «Прикладная математика и информатика»

010300 «Фундаментальная информатика и информационные технологии»

230700 «Прикладная информатика»

Нижний Новгород

2012

УДК 512.64
ББК В22.143
Ш 95

Ш 95 Шульц М.М. АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ. ЗАДАЧИ И РЕШЕНИЯ: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2012. – 101 с.

Рецензент: к.ф.-м.н., доцент **Н.Г. Чебочко**

В учебно-методическом пособии рассматриваются основные алгебраические структуры: группа, кольцо, поле. В каждой главе имеется справочная информация по теории, даются примеры решения нескольких типовых задач, приведено большое количество задач для самостоятельного решения и контрольные работы по некоторым темам.

Пособие предназначено для студентов 2-го курса факультета ВМК.

Ответственный за выпуск:

заместитель председателя методической комиссии факультета ВМК ННГУ,
к.т.н., доцент **В.М. Сморкалова**

УДК 512.64

ББК В22.143

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

В курсе «Геометрия и алгебра», входящем в учебный план факультета ВМК ННГУ, имеется раздел, в котором студенты знакомятся с основными алгебраическими структурами: группа, кольцо, поле. Изучение этого раздела встречает определенные трудности, частично связанные с тем, что в отличие от более традиционных разделов (геометрия, системы уравнений, многочлены и т.д.) здесь возникает проблема недостаточно формализованного *языка*, на котором формулируются задачи и описываются их решения. Настоящее пособие представляет собой скромную попытку автора предложить свое понимание данного вопроса.

Преподаватели кафедры математической логики и высшей алгебры факультета ВМК ННГУ в течение ряда лет накопили значительный методический материал по этой теме, которым автор с благодарностью воспользовался.

Особую благодарность автор выражает Н.Ю. Золотых, чьи советы позволили значительно улучшить первоначальный текст. В разделах «Циклические группы» и «Вычисления в полях вычетов» были использованы материалы из его (совместно с С.В. Сидоровым) сборника задач «Группы, кольца, поля».

Доцент кафедры геометрии и алгебры механико-математического факультета ННГУ Н.Г. Чебочко очень помогла при подготовке некоторых разделов. Она внимательно прочитала весь текст, исправила много опечаток и содержательных ошибок.

Первый раздел пособия «Бинарные операции» носит предварительный характер. Его целью является формирование у студента «общеалгебраической» точки зрения, в соответствии с которой разница между, скажем, сложением чисел, матриц и многочленов заключается не столько в природе операндов и в способе выполнения операции, сколько в *свойствах* этой операции. Второй

раздел – «Группы», третий – «Кольца и поля», четвертый – «Вычисления в полях вычетов».

В каждом разделе приведены краткие сведения из теории, разобрано несколько задач. Подробное описание их решения является, собственно говоря, главной целью пособия. Кроме того, даны задачи для самостоятельного решения.

Пятый раздел пособия включает контрольные работы по темам: «Факторизация групп», «Факторизация колец», «Линейная алгебра над полем вычетов» и «Многочлены над полем вычетов». В контрольных работах использованы материалы, предоставленные доцентом Л.Г. Киселевой.

Автор

ОБОЗНАЧЕНИЯ

Числовые множества

$\mathbf{N}$ – множество натуральных чисел.

$\mathbf{Z}$ – множество целых чисел.

$2\mathbf{Z}$ – множество четных чисел.

$2\mathbf{Z}+1$ – множество нечетных чисел.

$n\mathbf{Z}+k$ – множество целых чисел, которые при делении на n дают в остатке k .

$\mathbf{Z}_0 = \{0,1,2, \ldots\}$ – множество целых неотрицательных чисел.

$\mathbf{Q}$ – множество рациональных чисел.

$\mathbf{R}$ – множество вещественных чисел.

$[a, b] = \{x \in \mathbf{R} \mid a \le x \le b\}$ – замкнутый интервал (отрезок, сегмент) числовой оси.

$]a, b[= \{x \in \mathbf{R} \mid a < x < b\}$ – открытый интервал числовой оси

(другое обозначение (a, b)).

$[a, b[= \{x \in \mathbf{R} \mid a \le x < b\}$ – полуоткрытый интервал числовой оси

(другое обозначение $[a, b)$).

$]a, b] = \{x \in \mathbf{R} \mid a < x \le b\}$ – полуоткрытый интервал числовой оси

(другое обозначение $(a, b]$).

$\mathbf{C}$ – множество комплексных чисел.

$\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ – множества рациональных, вещественных, комплексных чисел, отличных от 0.

$\mathbf{Q}_+$, $\mathbf{R}_+$ – множества рациональных, вещественных положительных чисел.

Множества вычетов

$\mathbf{Z}_2 = \{0,1\}$ – множество вычетов по модулю 2.

$\mathbf{Z}_n = \{0,1, \dots , n-1\}$ – множество вычетов по модулю n.

$\mathbf{Z}_p^* = \{1, \dots, p\}$ – множество ненулевых вычетов по простому модулю p.

Множества многочленов

$\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$, $\mathbf{C}[x]$ – множества многочленов от переменной x с целыми, рациональными, вещественными, комплексными коэффициентами.

Множества матриц

$\mathbf{Z}^{m\times n}$, $\mathbf{Q}^{m\times n}$, $\mathbf{R}^{m\times n}$, $\mathbf{C}^{m\times n}$ – множества матриц из m строк и n столбцов с целыми, рациональными, вещественными, комплексными элементами.

GL(F,n) – полная линейная группа, квадратные невырожденные матрицы порядка n над числовым полем F.

Uni(F,n) – группа унимодулярных матриц порядка n (определители равны ±1).

SL(F,n) – специальная линейная группа, квадратные матрицы, определители которых равны 1.

GO(n) – полная ортогональная группа, ортогональные матрицы порядка n.

Tri(F,n) – группа невырожденных верхних треугольных матриц порядка n.

Sym(F,n) – множество симметричных матриц порядка n.

1. БИНАРНЫЕ ОПЕРАЦИИ

Основы теории

Общая алгебра изучает *алгебраические системы*. Любая такая система определяется:

- базовым множеством *элементов* произвольной природы; это могут быть числа, векторы, матрицы, функции (например, многочлены) и т.д.;
- набором алгебраических *операций* с этими элементами; результатом выполнения операции с какими-то элементами-участниками является новый элемент базового множества; элементы-участники называются *операндами*.

Примеры: (**N**, +) – множество натуральных чисел с операцией сложения, (**N**, ·) – множество натуральных чисел с операцией умножения, (**Z**, +, ·) – множество целых чисел с операциями сложения и умножения.

Заметим, что в соответствии с принятым определением из рассмотрения исключаются многие системы, реально изучаемые в курсе алгебры, например – линейное векторное пространство. Даже умножение числа на матрицу фактически оказывается «вне закона». Таким образом, тот вариант «общей алгебры», который рассматривается в настоящем пособии, является лишь упрощенной моделью «большой алгебры».

Каждая операция характеризуется количеством операндов, участвующих в ней. Для большинства операций это количество равно двум, такие операции называются *бинарными* или *двухместными*, однако встречаются *унарные* или *одноместные* операции, а также *тернарные* или *трехместные*. Операции с количеством операндов больше трех встречаются редко.

Операция должна быть определена (выполнима) при любых значениях операндов, другими словами, множество должно быть *замкнуто* относительно этой операции. В противном случае алгебраическая система считается заданной некорректно (фактически она не существует). При рассмотрении конкретных примеров алгебраических систем свойство замкнутости должно проверяться в первую очередь, до таких свойств, как коммутативность и т.п.

Проблема замкнутости возникает, в частности, когда базовое множество как-то ограничено: не все целые числа, а только четные, не все вещественные числа, а только положительные и т.п.

При «абстрактном» рассмотрении, не привязанном к конкретным примерам, операции часто обозначаются традиционными символами + и · (хотя их смысл может отличаться от традиционного), либо какими-то иными символами (чтобы подчеркнуть, что сам по себе символ *ничего конкретного не обозначает*). Часто для этих целей будет использоваться жирная точка •.

Любую бинарную операцию на конечном множестве можно задать с помощью квадратной таблицы, которую называют *таблицей Кэли* (Cayley table). Каждая строка этой таблицы соответствует конкретному значению первого операнда, это значение указано в *боковике* (дополнительном столбце-заголовке), а каждый столбец – конкретному значению второго операнда, это значение указано в *шапке* (дополнительной строке-заголовке). Так, операции алгебры логики задаются следующими таблицами Кэли:

Таблица 1.1

Таблицы Кэли для логических операций

конъюнкция

$\wedge$	0	1
0	0	0
1	0	1

дизъюнкция

$\vee$	0	1
0	0	1
1	1	1

«разделительное или»

$\oplus$	0	1
0	0	1
1	1	0

импликация

$\rightarrow$	0	1
0	1	1
1	0	1

Таблица 1.2

Формальная операция

•	*e*	*a*	*b*
e	*e*	*a*	*b*
a	*a*	*b*	*e*
b	*b*	*e*	*a*

С помощью таблицы Кэли можно задавать и чисто формальные операции на некотором конечном множестве, не имеющие (по крайней мере, на первый взгляд) никакого конкретного смысла. Пусть, например, базовое множество $M=\{e,a,b\}$, о природе его элементов ничего не известно. Формальную операцию • зададим таблицей Кэли (таблица 1.2).

Коммутативность

Операция • называется *коммутативной*, если для любых x, y из базового множества M выполняется равенство $x \bullet y = y \bullet x$.

Таковы операции сложения чисел, сложения векторов, сложения матриц, умножения чисел и многочленов. Коммутативны логические операции конъюнкция, дизъюнкция и «разделительное или», импликация некоммутативна (таблица 1.1). Из таблицы 1.2 видно, что заданная ею формальная операция • коммутативна. Напротив, умножение матриц некоммутативно (хотя имеются примеры перестановочных матриц, для которых $A \cdot B = B \cdot A$). Также некоммутативно (*антикоммутативно*) векторное умножение геометрических векторов – для него $\boldsymbol{x} \times \boldsymbol{y} = -\boldsymbol{y} \times \boldsymbol{x}$. Некоммутативно произведение подстановок, композиция многочленов (и вообще функций), задаваемая равенством $(f \circ g)(x) = f(g(x))$.

Нейтральный элемент

Элемент $e \in M$ называется *нейтральным* относительно операции •, если для любого $x \in M$ выполняются равенства $x \bullet e = x$ и $e \bullet x = x$.

Относительно сложения чисел нейтральным является число 0, относительно сложения векторов – нуль-вектор $\mathbf{0}$, относительно сложения матриц – нулевая матрица надлежащего размера (т.е. матрица, заполненная нулями), относительно умножения чисел и многочленов – число 1 (многочлен нулевой

степени), относительно умножения квадратных матриц – единичная матрица E надлежащего порядка, относительно умножения подстановок – тождественная подстановка. Для конъюнкции нейтральным элементом является 1, для дизъюнкции и «разделительного или» 0, для импликации нейтрального элемента нет (таблица 1.1), но есть *левый нейтральный* – это 1 (поскольку $1\to0=0$ и $1\to1=1$). Для формальной операции, заданной таблицей 1.2, нейтральным элементом является e (не потому, что он так обозначен, а по свойствам таблицы).

Симметричный элемент

Для произвольного элемента $x\in M$ *симметричным элементом* относительно операции $\bullet$ называется такой $\bar{x}\in M$, что $x\bullet\bar{x}=e$ и $\bar{x}\bullet x=e$ (существование нейтрального элемента e предполагается).

Относительно сложения чисел $e=0$, симметричным к числу x является число $-x$.

Относительно сложения векторов $e=\mathbf{0}$ (нуль-вектор), симметричным к вектору $\boldsymbol{x}$ является вектор $-\boldsymbol{x}$.

Относительно умножения чисел $e=1$, симметричным к числу x является число x^{-1}. Поскольку x^{-1} существует только для $x\neq0$, необходимо аккуратно определить базовое множество. Например, можно взять множество рациональных чисел, отличных от нуля $\mathbf{Q}^*$. Если $x\neq0$ и $y\neq0$, то и $z=x\cdot y\neq0$, так что операция $x\cdot y$ на этом множестве определена корректно (множество замкнуто относительно операции) и симметричный элемент x^{-1} существует для всякого $x\in\mathbf{Q}^*$.

Относительно умножения матриц нейтральным элементом является единичная матрица E, симметричным элементом к матрице A является обратная матрица A^{-1}, которая существует, если матрица A невырождена, т.е. $\det(A)\neq0$. Чтобы получить алгебраическую систему с хорошими свойствами,

необходимо ограничить базовое множество именно такими матрицами. Это множество замкнуто относительно умножения, так как $\det(A \cdot B)=\det(A)\cdot\det(B)$.

Относительно умножения подстановок нейтральным элементом является тождественная подстановка (например, $e=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$) симметричным элементом к подстановке a является *обратная подстановка* a^{-1}, полученная из a обменом первой и второй строк. Например, для подстановки $a=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ обратная подстановка $a^{-1}=\begin{pmatrix}2 & 3 & 1\\ 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$.

Относительно конъюнкции нейтральным элементом является 1, относительно дизъюнкции и относительно «разделительного или» нейтральный элемент 0. Симметричных элементов относительно этих операций нет, относительно «разделительного или» любой элемент симметричен самому себе.

Относительно формальной операции, заданной таблицей 1.2, симметричные элементы таковы: $\overline{e} = e$, $\overline{a} = b$, $\overline{b} = a$.

Ассоциативность

Операция $\bullet$ называется *ассоциативной*, если для любых $x,y,z \in M$ выполняется равенство $(x\bullet y)\bullet z=x\bullet(y\bullet z)$. Только в этом случае мы можем писать без скобок просто $x\bullet y\bullet z$ и рассматривать не только трехчленные, но и многочленные комбинации типа $x_1\bullet x_2\bullet\ldots\bullet x_n$.

Откуда известно, что сложение и умножение чисел ассоциативны? Ответим на вопрос вопросом: а откуда известно, что они коммутативны? На интуитивном уровне эти (и многие другие) факты, относящиеся к числам, воспринимаются, как «впитанные с молоком матери», а на теоретическом – доказываются в математической дисциплине, которая называется «Теоретическая арифметика», и далеко выходит за рамки университетского курса математики. Заметим, что для подобных доказательств надо сначала дать определение, что значит *сложить* или *перемножить* два числа (хотя бы натуральных).

Сложение векторов ассоциативно, в курсе векторной алгебры это доказывается простым геометрическим построением.

Сложение матриц ассоциативно, это следует из ассоциативности сложения чисел.

Ассоциативность умножения матриц доказывается в теории матриц исходя из определения этой операции.

В алгебре многочленов сложение и умножение ассоциативны – эти операции сводятся к сложению и умножению их коэффициентов. Композиция функций ассоциативна, поскольку для любых заданных функций f,g,h обе композиции $(f\circ g)\circ h$ и $f\circ(g\circ h)$ задаются одним и тем же выражением $f(g(h(x)))$. Умножение подстановок ассоциативно, потому что подстановки это функции, отображающих конечное множество на себя, умножение подстановок – композиция этих функций.

Конъюнкция, дизъюнкция и «разделительное или» ассоциативны, импликация неассоциативна.

Ассоциативна ли формальная операция, заданная таблицей 1.2? Если действовать на основании определения, надо подставлять вместо переменных x,y и z в уравнение $(x\bullet y)\bullet z=x\bullet(y\bullet z)$ константы e,a,b в различных комбинациях. Всего таких комбинаций $3^3=27$. За счет симметрии таблицы это количество можно уменьшить примерно вдвое, но все равно получается слишком много. На самом деле эта операция ассоциативна, мы это докажем позже косвенным способом.

Дистрибутивность

Если алгебраическая система содержит две бинарные операции, которые в этом случае обычно называются сложением (+) и умножением (·), важным является еще одно свойство, описывающее взаимодействие этих операций. Это *дистрибутивность умножения относительно сложения* (правила раскрытия скобок): $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$ (левая дистрибутивность) и $(y+z)\cdot x=(y\cdot x)+(z\cdot x)$

(правая дистрибутивность). В случае коммутативного умножения эти свойства сливаются в одно, но в общем случае они независимы друг от друга.

Дистрибутивно относительно сложения умножение чисел, умножение многочленов, умножение матриц, векторное умножение векторов (последнее доказывается не очень просто).

В алгебре логики дистрибутивность свойственна многим (но не всем) парам операций (см. ниже **С 1.7**).

Интересный пример дистрибутивности, где роль умножения играет сложение вещественных чисел, а роль сложения – взятие минимума или максимума: $x+\min(y,z)=\min(x+y,x+z)$, $x+\max(y,z)=\max(x+y,\ x+z)$ (см. ниже **С 1.13**).

Решение задач

Р 1.1. Выяснить свойства алгебраических систем (замкнутость множества относительно операции, коммутативность, наличие нейтрального элемента, симметричных элементов, ассоциативность).

1) (**N**, НОД), 2) (**N**, НОК).

Решение. Замкнутость множества по обеим операциям очевидна, коммутативность и ассоциативность следует из определений (НОД и НОК трех чисел).

1) Очевидно, что если НОД(x,y) = x, то y делится на x. Для нейтрального элемента e операции НОД должно быть НОД(e,x) = x при любом x. Поэтому число e должно делиться на любое натуральное число x. Ясно, что такого числа e не существует. Поэтому и симметричных элементов относительно операции НОД не существует.

2) Нейтральный элемент e для операции НОК должен удовлетворять равенству НОК(e,x) = x для любого x. Такое число есть – это 1. Симметричный элемент $\bar{x}$ должен удовлетворять условию НОК($x,\bar{x}$) = e = 1. Однако для любых x и y выполняются неравенства НОК(x,y) ≥ x и НОК(x,y) ≥ y, т.е. в данном случае $1 \geq x$ и $1 \geq \bar{x}$, что невозможно ввиду произвольности натурального

числа x. Таким образом, симметричных элементов относительно операции НОК не существует.

Р 1.2. Выяснить свойства алгебраической системы $(\mathbf{V}, \times)$, где

$\mathbf{V}$ – множество геометрических векторов трехмерного пространства,

$\times$ – векторное умножение векторов.

Решение. Замкнутость множества очевидна, коммутативности нет, вместо нее имеет место антикоммутативность: $\boldsymbol{x}\times\boldsymbol{y} = -\boldsymbol{y}\times\boldsymbol{x}$.

Для нейтрального вектора $\boldsymbol{e}$ должно выполняться условие $\boldsymbol{x}\times\boldsymbol{e}=\boldsymbol{e}\times\boldsymbol{x}=\boldsymbol{x}$. Ясно, что такого вектора $\boldsymbol{e}$ не существует, поскольку $\boldsymbol{x}\times\boldsymbol{y}$ ортогонально к векторам $\boldsymbol{x}$ и $\boldsymbol{y}$ и поэтому не может быть равно одному из них. Кроме того, из антикоммутативности следует, что векторы $\boldsymbol{x}\times\boldsymbol{e}$ и $\boldsymbol{e}\times\boldsymbol{x}$ противоположны, их равенство возможно, только если они оба равны $\mathbf{0}$. Поэтому и симметричных элементов относительно операции $\times$ не существует.

Векторное умножение *неассоциативно*. Для доказательства приведем контрпример. Рассмотрим векторные произведения ортов декартовых осей $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, $\boldsymbol{e}_3$. Возьмем, например, $(\boldsymbol{e}_1\times\boldsymbol{e}_2)\times\boldsymbol{e}_2=\boldsymbol{e}_3\times\boldsymbol{e}_2=-\boldsymbol{e}_1$. Расставим скобки по-другому и получим $\boldsymbol{e}_1\times(\boldsymbol{e}_2\times\boldsymbol{e}_2)=\boldsymbol{e}_1\times\mathbf{0}=\mathbf{0}$.

Р 1.3. На некотором, пока не определенном, числовом множестве введем *нестандартное умножение* $x\otimes y=x+y-x\cdot y$. Выяснить свойства операции $\otimes$.

Решение. Если множество замкнуто относительно стандартных операций $+$ и $\cdot$, оно замкнуто и относительно $\otimes$. Коммутативность операции очевидна. Проверим ассоциативность. Для произвольных x,y,z запишем гипотетическое равенство (которое надо проверить): $(x\otimes y)\otimes z = x\otimes(y\otimes z)$ и в два шага развернем его левую и правую часть в соответствии с определением операции.

$(x\otimes y)\otimes z=(x+y-x\cdot y)\otimes z=(x+y-x\cdot y)+z-(x+y-x\cdot y)\cdot z=x+y+z-(x\cdot y+x\cdot z+y\cdot z)+x\cdot y\cdot z$.

$x\otimes(y\otimes z)=x\otimes(y+z-y\cdot z)=x+(y+z-y\cdot z)-x\cdot(y+z-y\cdot z)=x+y+z-(x\cdot y+x\cdot z+y\cdot z)+x\cdot y\cdot z$.

Видим, что операция $\otimes$ ассоциативна.

Для нейтрального элемента e должно при любом x быть $x\otimes e=x+e-x\cdot e=x$, откуда $e\cdot(1-x)=0$. Так как x – любое число, $e=0$.

Для симметричного элемента $\bar{x}$ должно при любом x выполняться условие $x\otimes\bar{x}=x+\bar{x}-x\cdot\bar{x}=e=0$, откуда $\bar{x}\cdot(1-x)+x=0$, следовательно, $\bar{x}=\frac{x}{x-1}$. Заключаем, что для существования симметричных элементов в базовом множестве должно быть выполнимо деление (т.е. это, как минимум, множество рациональных чисел $\mathbf{Q}$), причем из этого множества надо исключить число 1 (а не 0, как в обычной арифметике). Важно, что множество $\mathbf{Q}\backslash\{1\}$ замкнуто относительно операции $\otimes$ (см. ниже **С 1.6**).

Р 1.4. ($\mathbf{R}\cup\mathbf{V}$, $\bullet$). Базовое множество содержит все вещественные числа и все векторы трехмерного пространства. Операция $\bullet$ определяется так:

– если оба операнда суть числа, это произведение чисел;

– если один операнд число, а другой вектор, это произведение числа на вектор;

– если оба операнда векторы, это скалярное произведение векторов.

Выяснить свойства операции $\bullet$.

Решение. Замкнутость базового множества и коммутативность операции очевидна, на роль нейтрального элемента e годится число 1. Проверим, ассоциативна ли операция, т.е. выполняется ли равенство $(x\bullet y)\bullet z=x\bullet(y\bullet z)$ при любых x, y, z.

Если все три операнда суть числа, равенство выполняется, поскольку умножение чисел ассоциативно.

Если два операнда суть числа, а третий – вектор, равенство также выполняется по свойствам умножения числа на вектор.

Если два операнда суть векторы, а третий – число, равенство выполняется по свойствам скалярного умножения векторов.

Пусть все три операнда суть векторы. Заменим в равенстве символ операции $\bullet$ в соответствии с ее определением и получим $(\boldsymbol{x},\boldsymbol{y})\cdot\boldsymbol{z}=\boldsymbol{x}\cdot(\boldsymbol{y},\boldsymbol{z})$ (векторы обозначены жирными буквами). Поскольку скалярные произведения $(\boldsymbol{x},\boldsymbol{y})$ и $(\boldsymbol{y},\boldsymbol{z})$

суть числа, слева имеем вектор, коллинеарный $\boldsymbol{z}$, а справа – коллинеарный $\boldsymbol{x}$. Равенство в общем случае неверно, операция $\bullet$ не ассоциативна.

Р 1.5. (Sym(F,n), $\cdot$). Базовое множество – симметричные матрицы заданного порядка n над некоторым числовым полем. Выяснить свойства этой алгебраической системы.

Решение. В первую очередь необходимо выяснить – замкнуто ли множество симметричных матриц относительно умножения, т.е. будет ли произведение матриц $A{\cdot}B$ симметрично, если симметричны сомножители A и B. Для симметричных матриц имеем $A^{\mathrm{T}} = A$ и $B^{\mathrm{T}} = B$. По свойствам транспонирования имеем $(A{\cdot}B)^{\mathrm{T}} = B^{\mathrm{T}}{\cdot}A^{\mathrm{T}} = B{\cdot}A$. Мы почти доказали (надо только аккуратно все записать) *теорему Шика*: произведение симметричных матриц симметрично тогда и только тогда, когда эти матрицы *перестановочны*. В общем случае произведение симметричных матриц несимметрично, например $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}\cdot\begin{bmatrix}1 & 2\\ 2 & 3\end{bmatrix}=\begin{bmatrix}3 & 5\\ 3 & 5\end{bmatrix}$.

Таким образом, алгебраическая система (Sym(F,n), $\cdot$) фактически *не существует* (а система (Sym(F,n), +) существует).

Р 1.6. Пусть L – множество линейных функций вида $f(x) = ax+b$ (коэффициенты a и b могут принадлежать любому числовому полю), операция «$\circ$« – композиция функций $(f_1\circ f_2)(x)=f_1\big(f_2(x)\big)$. Выяснить свойства алгебраических систем (L, $\circ$) и (L, +, $\circ$) («+» – обычное сложение функций).

Решение. Операция «$\circ$«, как сказано выше, ассоциативна. Проверим замкнутость относительно нее множества L и выясним другие ее свойства. Пусть $f_1(x) = a_1x+b_1$, $f_2(x) = a_2x+b_2$, найдем $f_1\circ f_2$ и $f_2\circ f_1$. В соответствии с определением

$$(f_1\circ f_2)(x)=f_1\big(f_2(x)\big) = a_1(a_2x+b_2)+b_1 = a_1a_2x + (a_1b_2+b_1), \qquad (*)$$

$$(f_2\circ f_1)(x)=f_2\big(f_1(x)\big) = a_2(a_1x+b_1)+b_2 = a_2a_1x + (a_2b_1+b_2). \qquad (**)$$

В обоих случаях получилась линейная функция, т.е. множество L замкнуто относительно операции.

Заметим, что если бы множество состояло из *квадратных трехчленов*, композиция дала бы многочлен 4-й степени, т.е. замкнутости *не было бы*. Заметим также, что множество линейных функций *незамкнуто* относительно обычного арифметического умножения: произведение двух линейных функций дает квадратный трехчлен.

Коэффициенты при переменной x в формулах (*) и (**) совпадают (умножение чисел коммутативно), но свободные члены, вообще говоря, различны. Таким образом, операция «$\circ$« некоммутативна.

Нейтральным элементом в алгебраической системе $(L, \circ)$ является, очевидно, тождественная функция $e(x) = x$, которая получается при $a=1$, $b=0$.

Выясним, при каких условиях существуют симметричные элементы. Пусть $f(x)=y=ax+b$, найдем обратную функцию, т.е. выразим x через y. Имеем $x = \frac{1}{a} \cdot y - \frac{b}{a}$. Чтобы получить функцию $\bar{f}(x)$, симметричную линейной функции $f(x)$ относительно композиции, переобозначим переменные x и y, получим $\bar{f}(x) = \frac{1}{a} \cdot x - \frac{b}{a}$. Ясно, что симметричная функция существует только при $a \neq 0$. Линейные функции с коэффициентом $a \neq 0$ будем называть *невырожденными* (а с $a=0$ – вырожденными). Из формул (*) и (**) видим, что множество невырожденных линейных функций замкнуто относительно композиции.

Ситуация аналогична той, которая имеет место для матриц – их умножение ассоциативно и некоммутативно, имеется нейтральный элемент (единичная матрица), симметричные элементы (обратные матрицы) существуют только для невырожденных матриц, множество которых замкнуто относительно умножения.

Проверим, выполняются ли в системе $(L, +, \circ)$ законы дистрибутивности: $f_1 \circ (f_2+f_3) = (f_1 \circ f_2)+(f_1 \circ f_3)$ и $(f_2+f_3) \circ f_1 = (f_2 \circ f_1)+(f_3 \circ f_1)$, где $f_i(x) = a_i \cdot x + b_i$ для $i = 1,2,3$?

Левая дистрибутивность: обозначим сумму линейных функций $p=f_2+f_3$, имеем $p(x)=(a_2+a_3)\cdot x+(b_2+b_3)$. В левой части проверяемого равенства получаем

$$(f_1 \circ p)(x) = (f_1(p(x)) = a_1 \cdot ((a_2+a_3)\cdot x+(b_2+b_3)) + b_1 = (a_1 \cdot a_2 + a_1 \cdot a_3)\cdot x + (a_1 \cdot b_2 + a_1 \cdot b_3 + b_1).$$

В правой части первое слагаемое $(f_1 \circ f_2)(x)=a_1 \cdot a_2 \cdot x+(a_1 \cdot b_2+b_1)$ (см. (∗)), второе слагаемое $(f_1 \circ f_3)(x)=(f_1(f_3(x))=a_1 \cdot (a_3 \cdot x+b_3)+b_1=a_1 \cdot a_3 \cdot x+(a_1 \cdot b_3+b_1)$. Сумма равна $(a_1 \cdot a_2+a_1 \cdot a_3) \cdot x+(a_1 \cdot b_2+a_1 \cdot b_3+2 \cdot b_1)$.

Коэффициенты при переменной x совпадают, но свободные члены линейных функций различны, левая дистрибутивность нарушена.

Замечание. Правая дистрибутивность выполняется – см. ниже **С 1.8**.

Р 1.7. Рассмотрим алгебраическую систему, элементами которой являются квадратные матрицы, а операцией *коммутатор матриц* $[A,B]=A \cdot B-B \cdot A$. Выяснить свойства этой алгебраической системы.

Решение. Очевидно, что множество замкнуто относительно этой операции и что операция антикоммутативна, т.е. $[A,B]=-[B,A]$ (наподобие векторного произведения, еще с векторным произведением ее роднит свойство $[A,A]=O$). Почти очевидно, что коммутатор дистрибутивен относительно сложения матриц (см. ниже **С 1.11**).

Проверим ассоциативность, т.е. равенство $[[A,B],C]=[A,[B,C]]$. Имеем

$[[A,B],C]=[A \cdot B-B \cdot A,C]=(A \cdot B-B \cdot A) \cdot C-C \cdot (A \cdot B-B \cdot A)=A \cdot B \cdot C-B \cdot A \cdot C-C \cdot A \cdot B+C \cdot B \cdot A$,

$[A,[B,C]]=[A,(B \cdot C-C \cdot B)]=A \cdot (B \cdot C-C \cdot B)-(B \cdot C-C \cdot B) \cdot A=A \cdot B \cdot C-A \cdot C \cdot B-B \cdot C \cdot A+C \cdot B \cdot A$.

Надо проверить, всегда ли равны эти выражения. Возьмем их разность $D=A \cdot C \cdot B+B \cdot C \cdot A-B \cdot A \cdot C-C \cdot A \cdot B$. Например, для $A=\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}, B=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}, C=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$ получим $D=\begin{bmatrix}1 & 2\\ 0 & -1\end{bmatrix}$. Вывод: операция коммутатор матриц не ассоциативна (как и векторное произведение).

Р 1.8. Рассмотрим алгебраическую систему, элементами которой являются квадратные матрицы, а операцией – *произведение Йордана* $\{A,B\}=\frac{1}{2}(A \cdot B+B \cdot A)$. Выяснить свойства этой алгебраической системы.

Решение. Очевидно, что множество замкнуто относительно этой операции и что операция коммутативна, т.е. $\{A,B\}=\{B,A\}$. Также очевидно, что от

обычного произведения эта операция унаследовала нейтральный элемент и симметричные элементы, т.е. $\{A,E\}=A$ и $\{A,\ A^{-1}\}=E$. Очевидна и дистрибутивность относительно сложения матриц. Произведение Йордана не ассоциативно (см. **С 1.12**). Некоторым сюрпризом является незамкнутость относительно произведения Йордана множества *невырожденных матриц*. Возьмем две невырожденные матрицы $A=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ и $B=\begin{bmatrix}1 & 2\\ 2 & 3\end{bmatrix}$. Их произведение Йордана $\{A,B\}=\begin{bmatrix}2 & 2\\ 2 & 2\end{bmatrix}$ – вырожденная матрица. Напомним, что относительно обычного произведения множество невырожденных матриц замкнуто – см. выше.

Р 1.9. Введем понятие одностороннего нейтрального элемента: *левый нейтральный элемент* e_{L} такой, что $e_{\mathrm{L}}\bullet x=x$ для любого x, *правый нейтральный элемент* e_{R} такой, что $x\bullet e_{\mathrm{R}}=x$ для любого x. Так, на с. 8 говорится о левом нейтральном элементе для логической операции импликации, другие примеры см. в разделе 3 «Кольца и поля» (задачи **Р 3.1.13** и **С 3.1.17)**.

Доказать, что если в алгебраической системе существуют оба нейтральных элемента e_{L} и e_{R}, то они совпадают.

Решение. Рассмотрим комбинацию $e_{\mathrm{L}}\bullet e_{\mathrm{R}}$. С одной стороны, поскольку e_{L} – левый нейтральный, имеем $e_{\mathrm{L}}\bullet e_{\mathrm{R}}=e_{\mathrm{R}}$. С другой стороны, поскольку e_{R} – правый нейтральный, имеем $e_{\mathrm{L}}\bullet e_{\mathrm{R}}=e_{\mathrm{L}}$. Получаем $e_{\mathrm{L}}=e_{\mathrm{R}}$.

Задачи для самостоятельного решения

С 1.1. Охарактеризуйте свойства следующих алгебраических систем (замкнутость множества относительно операций, коммутативность, наличие нейтрального элемента, симметричных элементов, ассоциативность).

1) $(\mathbf{N}, +, \cdot)$, 2) $(\mathbf{Z}, +, \cdot)$, 3) $(\mathbf{Q}, +, \cdot)$, 4) $(\mathbf{R}, +, \cdot)$, 5) $(\mathbf{C}, +, \cdot)$.

С 1.2. Символом $2\mathbf{Z}$ обозначается множество четных целых чисел, символом $2\mathbf{Z}+1$ – множество нечетных целых чисел. По той же схеме, как в **С 1.1**, охарактеризуйте свойства алгебраических систем $(2\mathbf{Z}, +, \cdot)$ и $(2\mathbf{Z}+1, +, \cdot)$.

С 1.3. Символом $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$ обозначается *множество вычетов* по модулю n (остатков от деления на n). Операции на множестве вычетов: *сложение и умножение по модулю* n. Их определение: $x +_n y$ – остаток от деления $x + y$ на n, $x \cdot_n y$ – остаток от деления $x \cdot y$ на n.

Коммутативность этих операций очевидна, ассоциативность и дистрибутивность доказываются в теоретическом курсе.

Постройте таблицы сложения и умножения по модулям 2, 3, 4, 5, 6.

Найдите нейтральные и симметричные элементы относительно этих операций (в случае умножения необходимо исключить из множества вычетов 0).

С 1.4. *Нестандартное сложение* чисел задается формулой $x \oplus y = x + y - 1$. Выясните свойства операции $\oplus$ (с «разделительным или» в алгебре логики здесь совпадает только символ).

Указание. Используйте подход задачи **Р 1.3.**

С 1.5. Докажите дистрибутивность нестандартного умножения $\otimes$ чисел (см. выше **Р 1.3**) относительно нестандартного сложения $\oplus$ (см. выше **С 1.4**).

С 1.6. Докажите замкнутость множества $\mathbf{Q}\backslash\{1\}$ относительно операции $\otimes$ (см. выше **Р 1.3**).

Указание. Покажите, что если $x \otimes y = 1$, то $x = 1$ или $y = 1$.

С 1.7. Для различных пар бинарных операций алгебры логики (конъюнкция $\wedge$, дизъюнкция $\vee$, «разделительное или» $\oplus$, импликация $\rightarrow$) выясните их дистрибутивность (конъюнкция относительно дизъюнкции, дизъюнкция относительно конъюнкции и т.д.).

С 1.8. Докажите правую дистрибутивность в системе $(L, +, \circ)$

Левая дистрибутивность в этой системе отсутствует, см. выше **Р 1.6**.

С 1.9. Выясните свойства алгебраической системы GO(n), где базовое множество – ортогональные матрицы заданного порядка n, операция – умножение матриц.

Указание. Используйте подход задачи **Р 1.5.**

С 1.10. Выясните свойства алгебраической системы (Tri(F,n), + , ·) где базовое множество – верхние треугольные матрицы заданного порядка n, операция – умножение матриц.

Указание. Можно ограничиться конкретными небольшими значениями n = 2 и 3**.**

С 1.11. Докажите, что операция коммутатор матриц $[A,B]=A\cdot B-B\cdot A$ дистрибутивна относительно сложения.

С 1.12. Докажите, что произведение Йордана $\{A,B\}=\frac{1}{2}(A\cdot B+B\cdot A)$ не ассоциативно.

Указание. Используйте подход задачи **Р 1.7.**

С 1.13. Докажите, что $x+\min(y,z)=\min(x+y,x+z)$, $x+\max(y,z)=\max(x+y, x+z)$.

Указание. Рассмотрите отдельно случаи $y>z$ и $y<z$, используйте свойства неравенств $y>z \Rightarrow x+y>x+z$ и $y<z \Rightarrow x+y<x+z$**.**

С 1.14. Охарактеризуйте свойства следующих алгебраических систем, состоящих из матриц 2-го порядка с обычными операциями сложения и умножения матриц (замкнутость множества относительно каждой из операций, коммутативность, наличие нейтрального элемента, симметричных элементов).

1) $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a,b \in \mathbf{R}\right\}$;

2) $\left\{\begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \middle| \, a,b \in \mathbf{R}\right\}$;

3) $\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| \, a,b \in \mathbf{R}\right\}$;

4) $\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| \, a,b \in \mathbf{Q}\right\}$;

5) $\left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \middle| \alpha \in \mathbf{R} \right\}$.

С 1.15. Докажите, что двусторонний нейтральный элемент e (для него $e \bullet x = x$ и $x \bullet e = x$ при любом x) является единственным.

2. ГРУППЫ

2.1. Определения и примеры

Основы теории

Непустое множество M с заданной на нем бинарной операцией $\bullet$ называется *группой* (group), символически записывают $G=(M, \bullet)$, если

Group1. Операция $\bullet$ ассоциативна, т.е. для любых $x,y,z \in M$ верно равенство $(x \bullet y) \bullet z = x \bullet (y \bullet z)$;

Group2. В множестве M имеется *нейтральный элемент* e такой, что для любого $x \in M$ верны равенства $x \bullet e = x$ и $e \bullet x = x$;

Group3. Для всякого $x \in M$ существует *симметричный элемент* $\bar{x} \in M$ такой, что $x \bullet \bar{x} = e$ и $\bar{x} \bullet x = e$.

Замечание. Переход от произвольного элемента x к симметричному элементу $\bar{x}$ можно рассматривать как *унарную* (одноместную) операцию, порожденную основной групповой операцией $\bullet$.

Если групповая операция $\bullet$ коммутативна, группа $G=(M, \bullet)$ называется *коммутативной* (используется также исторический термин «*абелева группа*»).

Допуская некоторую вольность речи и обозначений, иногда будем говорить, что элемент *принадлежит группе* (а не базовому множеству) и писать $x \in G$ вместо $x \in M$.

Количество элементов группы называется *порядком* этой группы.

Три теоремы о группах

Теорема 1. Нейтральный элемент e является единственным.

Теорема 2. Для всякого x симметричный элемент $\bar{x}$ является единственным.

Теорема 3. Каждое из уравнений $a \bullet x = b$ и $y \bullet a = b$ однозначно разрешимо. Здесь a и b – *параметры*, их значения суть произвольные элементы базового множества.

Доказательству этих теорем посвящена задача **С 2.1.1**.

Из теоремы 3 следует, что если конечная группа задана таблицей Кэли, то

Cay1. Все элементы любой строки таблицы различны.

Cay2. В каждой строке присутствуют ровно по одному разу все элементы.

Аналогичное утверждение верно и для столбцов таблицы.

Аксиомы (свойства), входящие в определение группы, более или менее независимы. Так, если сохранить только аксиому ассоциативности, отказавшись от аксиом существования нейтрального и симметричного элементов, получится определение *полугруппы* (semigroup). Если взять формулировку теоремы 3 в виде аксиомы, отказавшись от обязательной ассоциативности, а также от аксиом **Group2** и **Group3**, получится определение *квазигруппы* (quasigroup). Заметим, что свойства **Cay**1 и **Cay**2 таблицы Кэли определяют именно квазигруппу. Очевидно, что каждая группа является также полугруппой и квазигруппой.

Примеры групп

G 1. (**Z**, +) – *аддитивная группа целых чисел*. Термин «аддитивная» здесь и дальше говорит не о каких-то свойствах этой группы, а лишь о способе обозначения групповой операции (additio по-латыни означает прибавление, сложение). Также можно говорить об аддитивной группе рациональных чисел (**Q**, +), аддитивной группе вещественных чисел (**R**, +) и аддитивной группе комплексных чисел (**C**, +). Во всех этих группах нейтральный элемент – число 0, для произвольного числа x симметричным элементом является число $-x$. Заметим, что все эти группы коммутативны. Вообще обозначение операции «крестиком» (+) и термин «аддитивная» обычно относят только к коммутативным группам, для некоммутативных используют другие символы. Впрочем, это всего лишь общепринятое соглашение.

Напротив, система ($\mathbf{Z}$, $\cdot$) не является группой, это коммутативная полугруппа, обладающая нейтральным элементом («*полугруппа с единицей*»), симметричные элементы имеются только у чисел 1 и –1 (это они сами).

G 2. ($\mathbf{Q}^*$, $\cdot$) – *мультипликативная группа рациональных чисел, отличных от нуля*. Термин «мультипликативная» говорит не о каких-то свойствах этой группы, а лишь о способе обозначения групповой операции (multiplicatio по-латыни означает умножение). Также можно говорить о мультипликативной группе вещественных чисел, отличных от нуля ($\mathbf{R}^*$, $\cdot$) и мультипликативной группе комплексных чисел, отличных от нуля ($\mathbf{C}^*$, $\cdot$). Во всех мультипликативных группах нейтральный элемент – число 1, для произвольного числа x симметричным элементом является число x^{-1}. Число 0 пришлось исключить из базовых множеств этих групп по понятным причинам: не существует 0^{-1}.

Напротив, системы ($\mathbf{Q}$, $\cdot$), ($\mathbf{R}$, $\cdot$) и ($\mathbf{C}$, $\cdot$) не являются группами, это коммутативные полугруппы с единицей, поскольку для числа 0 нет симметричного элемента.

G 3. ($\mathbf{Q}_+$, $\cdot$) – *мультипликативная группа положительных рациональных чисел*. Также можно говорить о мультипликативной группе положительных вещественных чисел ($\mathbf{R}_+$, $\cdot$). В этих мультипликативных группах нейтральный элемент также число 1, для произвольного числа x симметричным элементом является число x^{-1}.

G 4. ($F^{m\times n}$, +) – *аддитивная группа матриц* из m строк и n столбцов с элементами из числового поля F. Нейтральный элемент – матрица 0, заполненная нулями, для произвольной матрицы X симметричный элемент группы – матрица $-X$ (все элементы заменены на противоположные по знаку).

Говоря неформально, ($F^{m\times n}$, +) – векторное пространство, из которого удалили операцию умножения вектора на число, сохранили только сложение векторов.

При $m = 1$ матрицы являются *арифметическими векторами-строками*, при $n = 1$ – *арифметическими векторами-столбцами*.

G 5. GL(F, n) – *полная линейная группа*. Это мультипликативная группа квадратных невырожденных матриц заданного порядка n над числовым полем F. Нейтральный элемент – единичная матрица E, для произвольной невырожденной матрицы X симметричный элемент группы – обратная матрица X^{-1}.

Система, состоящая из *всех* матриц, в том числе вырожденных, не является группой относительно операции умножения, это некоммутативная полугруппа с единицей, поскольку для вырожденных матриц нет симметричных элементов.

G 6. GO(n) – *полная ортогональная группа*. Это мультипликативная группа ортогональных матриц порядка n над полем вещественных чисел $\mathbf{R}$ (доказательство замкнутости и прочие групповые свойства см. выше **С 1.9**). Нейтральный и симметричные элементы как в примере **G 5**.

G 7. ($\mathbf{Z}[x]$, +), ($\mathbf{Q}[x]$, +), $\mathbf{R}[x]$, +), ($\mathbf{C}[x]$, +) – *аддитивные группы многочленов*. Нейтральный элемент – нулевой многочлен, для произвольного многочлена $f(x)$ симметричный элемент группы – многочлен $-f(x)$.

G 8. *Симметрическая группа* S_n. Ее элементами являются все подстановки множества $\{1, 2, \ldots, n\}$, порядок группы равен $n!$. Операция в этой группе – умножение подстановок.

G 9. (L, $\circ$) – *группа линейных невырожденных функций* вида $f(x) = ax + b$ при $a \neq 0$, групповая операция – композиция функций. Коэффициенты a и b могут принадлежать любому из числовых полей $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$.

G 10. ($\mathbf{V}$, +) – *аддитивная группа геометрических векторов* (*направленных отрезков*) на плоскости или в трехмерном геометрическом пространстве. Нейтральный элемент – нуль-вектор $\mathbf{0}$, для произвольного вектора $\boldsymbol{x}$ симметричный элемент группы – противоположный вектор $-\boldsymbol{x}$.

G 11. ($\mathbf{Z}_n$, $+_n$) – *аддитивная группа вычетов* по модулю n (см. выше **C 1.3**). Нейтральный элемент 0, для любого вычета $x \neq 0$ симметричный вычет есть $n-x$.

G 12. Попробуем построить мультипликативную группу вычетов (операция $\cdot_n$ ассоциативна, но доказывать это мы не станем). Вычет 0 необходимо исключить – произведение $x \cdot_n 0$ равно 0 при любом x, уравнение $x \cdot_n 0 = 1$ неразрешимо. Ограничимся ненулевыми вычетами: $\mathbf{Z}_n^* = \{1, \ldots, n-1\}$. Рассмотрим пример. Пусть $n = 6$, $\mathbf{Z}_6^* = \{1, 2, 3, 4, 5\}$. Найдем произведение $2 \cdot_6 3 = 0$ – видим, что $\mathbf{Z}_6^*$ *незамкнуто* относительно операции $\cdot_6$. Причина неудачи очевидна – обычное произведение $2 \cdot 3$ равно 6, т.е. основанию нашей модулярной арифметики $n=6$. Чтобы этого не происходило, число n должно быть *простым*, т.е. не раскладываться на множители («разложение» $n = n \cdot 1$, разумеется, не в счет). Условие простоты модуля сравнения p необходимо для получения мультипликативной группы ($\mathbf{Z}_p^*$, $\cdot_p$).

На самом деле это условие также и достаточно (доказывательство см. ниже в задаче **P 3.1.3**), пока ограничимся примером. Построим таблицу умножения вычетов по простому модулю $p=5$. В соответствии с этой таблицей для вычета 2 симметричным элементом группы является вычет 3, именно их произведение равно нейтральному элементу 1. Пренебрегая разницей в обозначениях с обычным умножением, найдем по таблице $2^{-1}=3$. Аналогично $3^{-1}=2$, $4^{-1}=4$.

Таблица 2.1

Умножение по модулю 5

$\cdot_5$	1	2	3	4
1	1	2	3	4

G 13. ($\mathbf{Z}$, $\oplus$) – группа с нестандартной операцией $\oplus$, задаваемой равенством $x \oplus y = x + y - 1$. При решении задачи **C 1.4** была доказана ассоциативность этой операции (ее коммутативность очевидна), существование нейтрального элемента $e=1$ и существование элемента, симметричного для произвольного x,

это $\bar{x}=2-x$. С той же операцией можно построить группы (**Q**, $\oplus$), (**R**, $\oplus$), (**C**, $\oplus$), все эти группы коммутативны.

G 14. (**Q**\{1}, $\otimes$) – группа с нестандартной операцией $\otimes$, задаваемой равенством $x\otimes y=x+y-x\cdot y$. При решении задачи **P 1.3** была доказана ассоциативность этой операции (ее коммутативность очевидна), существование нейтрального элемента $e=0$ и существование элемента, симметричного для произвольного x, это $\bar{x}=\dfrac{x}{x-1}$. Замкнутость множества **Q**\{1} относительно операции $\otimes$, доказана в задаче **C 1.6**. С той же операцией можно построить группы (**R**\{1}, $\otimes$), (**C**\{1}, $\otimes$), все эти группы коммутативны.

G 15. *Группа симметрий* фигуры – это множество всех движений, переводящих фигуру в себя, операция в группе – композиция, т.е. последовательное выполнение движений. Для прямоугольника, отличного от квадрата, группа симметрий состоит из вращений a и b вокруг осей симметрии (с выходом из плоскости) и вращения c вокруг центра симметрии (без выхода из плоскости), все вращения на 180° (рис. 2.1). Нейтральный элемент группы e – «никакое движение» (прямоугольник неподвижен).

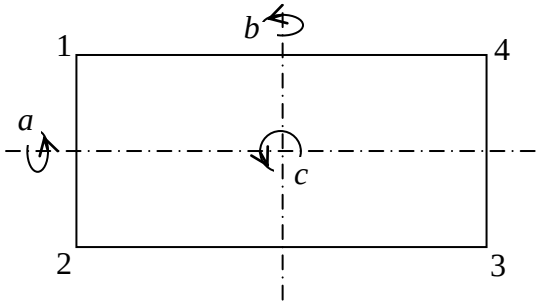

Рис. 2.1. Группа симметрий

Каждое движение описывается соответствующей подстановкой на множестве номеров вершин прямоугольника:

$$e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ a=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$

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

Эта группа имеет индивидуальное название *четверная группа Клейна*.

Важное понятие теории групп – *подгруппа* (subgroup). Пусть $G=(M, \bullet)$ – некоторая группа. Тогда группа $G'=(M', \bullet)$, где множество $M'\subseteq M$, называется *подгруппой* группы G, символически $G'\subseteq G$. Операция в группе и в подгруппе

одна и та же, нейтральный элемент в группе и в подгруппе – один и тот же, способ построения симметричного элемента также одинаковый. У каждой группы есть, по меньшей мере, две подгруппы: она сама и *единичная* подгруппа, базовое множество которой состоит из одного элемента e. Эти подгруппы называются *несобственными*, остальные (если они имеются) – *собственными*.

Для конечных групп и их подгрупп важную роль играет *теорема Лагранжа*: порядок любой подгруппы является делителем порядка самой группы.

Очевидное следствие из теоремы Лагранжа: у группы, порядок которой простое число, нет собственных подгрупп.

Примеры подгрупп

SG 1. Аддитивная группа целых чисел $(\mathbf{Z}, +)$ является подгруппой аддитивной группы рациональных чисел $(\mathbf{Q}, +)$, которая сама является подгруппой аддитивной группы вещественных чисел $(\mathbf{R}, +)$, а та – подгруппой аддитивной группы комплексных чисел $(\mathbf{C}, +)$. Нейтральный элемент во всех этих группах – число 0, симметричный элемент для любого числа x – противоположное по знаку число $-x$.

Символически отношения между этими группами можно записать так: $(\mathbf{Z}, +)\subset(\mathbf{Q}, +)\subset(\mathbf{R}, +)\subset(\mathbf{C}, +)$. Здесь все включения – строгие, все подгруппы – собственные.

SG 2. Мультипликативная группа рациональных чисел, отличных от нуля $(\mathbf{Q}^*, \cdot)$ является подгруппой мультипликативной группы вещественных чисел комплексных чисел $(\mathbf{R}^*, \cdot)$, а та – подгруппой мультипликативной группы комплексных чисел, отличных от нуля $(\mathbf{C}^*, \cdot)$.

Символически отношения между этими группами можно записать так: $(\mathbf{Q}^*, \cdot)\subset(\mathbf{R}^*, \cdot)\subset(\mathbf{C}^*, \cdot)$. Здесь все включения – строгие, все подгруппы – собственные.

SG 3. Мультипликативная группа положительных рациональных чисел $(\mathbf{Q}_+, \cdot)$ является собственной подгруппой мультипликативной группы $(\mathbf{Q}^*, \cdot)$ рациональных чисел, отличных от нуля: $(\mathbf{Q}_+, \cdot) \subset (\mathbf{Q}^*, \cdot)$.

SG 4. Мультипликативная группа положительных вещественных чисел $(\mathbf{R}_+, \cdot)$ является собственной подгруппой мультипликативной группы $(\mathbf{R}^*, \cdot)$ вещественных чисел, отличных от нуля: $(\mathbf{R}_+, \cdot) \subset (\mathbf{R}^*, \cdot)$.

SG 5. Мультипликативные группы невырожденных матриц порядка n над числовым полем F:

специальная линейная группа $\mathrm{SL}(F,n)$ (определители ее матриц равны 1).

группа *унимодулярных матриц* $\mathrm{Uni}(F,n)$ (определители равны ± 1).

Эти группы являются подгруппами полной линейной группы $\mathrm{GL}(F,n)$ (см. пример **G 5**): $\mathrm{SL}(F,n) \subset \mathrm{Uni}(F,n) \subset \mathrm{GL}(F,n)$.

SG 6. Полная ортогональная группа $\mathrm{GO}(n)$ является собственной подгруппой полной линейной группы над полем вещественных чисел $\mathrm{GL}(\mathbf{R},n)$.

SG 7. Аддитивная группа четных чисел $(2\mathbf{Z}, +)$ является собственной подгруппой аддитивной группы целых чисел: $(2\mathbf{Z}, +) \subset (\mathbf{Z}, +)$.

Очевидно, что пересечение двух подгрупп одной группы также является подгруппой. Так, пересечение $\mathrm{SL}(\mathbf{R},n) \cap \mathrm{GO}(n) = \mathrm{SO}(n)$ – *специальная ортогональная группа* состоит из ортогональных матриц, определители которых равны 1 (в общей ортогональной группе $\mathrm{GO}(n)$ определители равны ± 1).

Очень важно, что операция $\bullet$ в группе и в подгруппе *одна и та же*. Т.е. если для некоторой группы $G=(M, \bullet)$ взять какое-то подмножество $M' \subseteq M$, какую-то *новую операцию* $\lozenge$ и построить (если удастся) группу $G'=(M', \lozenge)$, то эта группа *не будет* подгруппой в группе G, хотя $M' \subseteq M$.

Так, если взять аддитивную группу квадратных матриц некоторого порядка n с операцией $+$, а потом взять подмножество невырожденных матриц по-

рядка n и построить на нем мультипликативную группу с операцией $\cdot$, эта группа *не будет* подгруппой исходной аддитивной группы.

Какие свойства подмножества M' надо проверять, чтобы выяснить, является ли алгебраическая система $(M', \bullet)$ подгруппой группы $(M, \bullet)$?

Самое главное – подмножество должно быть замкнуто относительно операции $\bullet$. Кроме того, подмножеству должен принадлежать нейтральный элемент группы, наконец, если некоторый элемент $x \in M'$, то и симметричный элемент $\bar{x}$ также должен принадлежать M'.

Ассоциативность операции $\bullet$ на подмножестве проверять *не надо*, поскольку уже известно, что $(M, \bullet)$ – группа и ассоциативность имеет место для всех элементов множества M, а стало быть, и для всех элементов подмножества M'.

Примеры и контрпримеры подгрупп

1. В множестве целых чисел $\mathbf{Z}$ рассмотрим два подмножества – четных чисел $2\mathbf{Z}$ и нечетных чисел $2\mathbf{Z}+1$. Подмножество $2\mathbf{Z}$ замкнуто относительно сложения, нейтральный элемент группы $(\mathbf{Z}, +)$ – это число 0 – является четным; если $x \in 2\mathbf{Z}$, то и симметричный элемент группы, т.е. противоположное по знаку число $-x \in 2\mathbf{Z}$. Таким образом, мы установили, что $(2\mathbf{Z}, +)$ – группа (об этом говорилось выше). А вот подмножество нечетных чисел $2\mathbf{Z}+1$ незамкнуто относительно сложения, поэтому $(2\mathbf{Z}+1, +)$ не является группой и вообще такая система *не существует*.
2. В множестве целых чисел $\mathbf{Z}$ возьмем подмножество натуральных чисел $\mathbf{N}$. Это подмножество замкнуто относительно сложения, однако система $(\mathbf{N}, +)$ не является подгруппой в группе $(\mathbf{Z}, +)$, так как нейтральный элемент группы 0 не является натуральным числом. Система $(\mathbf{N}, +)$ – полугруппа.
3. Расширим множество натуральных чисел до множества целых неотрицательных $\mathbf{Z}_0=\{0,1,2,\ldots\}$. Это множество замкнуто относительно сложения и с нейтральным элементом все в порядке: $0 \in \mathbf{Z}_0$, Однако система $(\mathbf{Z}_0, +)$ также не является подгруппой в группе $(\mathbf{Z}, +)$, так как для произвольного $x \in \mathbf{Z}_0$ симметричный элемент группы $-x \notin \mathbf{Z}_0$. Система $(\mathbf{Z}_0, +)$ – полугруппа.

Важное теоретическое понятие – *изоморфизм* (isomorphism) *групп*. Пусть $G_1=(M_1, \bullet)$ и $G_2=(M_2, \lozenge)$ – две группы на разных множествах и с разными (вообще говоря) операциями. Группы G_1 и G_2 изоморфны, если

- существует биекция (взаимно однозначное отображение) $\varphi: M_1 \to M_2$,
- для любых $x,y \in M_1$ имеем $\varphi(x \bullet y) = \varphi(x) \lozenge \varphi(y)$
  (словесная формулировка: «биекция, сохраняющая операцию»).

Символически изоморфизм групп записывается так: $G_1 \cong G_2$.

Примеры изоморфизма групп

IsoG 1. Пусть $G_1=(\mathbf{R}_+, \cdot)$ – мультипликативная группа положительных вещественных чисел, $G_2=(\mathbf{R}, +)$ – аддитивная группа вещественных чисел. Определим отображение $\varphi: \mathbf{R}_+ \to \mathbf{R}$ с помощью логарифмической функции по любому основанию, можно взять натуральные логарифмы, т.е. положить $\varphi(x)=\ln x$. Это отображение взаимно однозначное, обратное отображение задается формулой e^x. Известно, что $\ln(x \cdot y) = \ln(x) + \ln(y)$. Таким образом, эти две группы изоморфны, т.е. $(\mathbf{R}_+, \cdot) \cong (\mathbf{R}, +)$.

IsoG 2. Группа $(\mathbf{Z}, \oplus)$ с нестандартной операцией $\oplus$, задаваемой равенством $x \oplus y = x+y-1$, (пример **G 13**) изоморфна «обычной» группе $(\mathbf{Z}, +)$ (см. выше задачу **P 2.1.5**).

IsoG 3. Группа может быть изоморфна своей собственной подгруппе, например $(\mathbf{Z}, +) \cong (n\mathbf{Z}, +)$. Отображение $\varphi: \mathbf{Z} \to n\mathbf{Z}$ задается формулой $\varphi(x)=nx$.

Изоморфизм – сильный инструмент для изучения групп. Вспомним формальную операцию $\bullet$ на множестве $M=\{e,a,b\}$, заданную таблицей 1.2. на с. 7. Кое-какие свойства этой операции (коммутативность, наличие нейтрального элемента, наличие симметричных элементов) мы установили «методом глядения» (на таблицу). Однако свойство ассоциативности оказалось слишком трудоемким для «переборного» доказательства.

Докажем ассоциативность этой операции косвенным способом. Для этого установим изоморфизм алгебраической системы $(M, \bullet)$ с аддитивной группой

вычетов по модулю 3, т.е. с ($\mathbf{Z}_3$, $+_3$), где $\mathbf{Z}_3 = \{0,1,2\}$. Введем отображение φ: $M \to \mathbf{Z}_3$, положив $\varphi(e)=0$, $\varphi(a)=1$, $\varphi(b)=2$. Проверим, что $\varphi(a \bullet b)=\varphi(a) +_3 \varphi(b)$. Слева имеем, в соответствии с таблицей 1.2, $a \bullet b = e$ и $\varphi(e) = 0$. Справа $1 +_3 2 = 0$. Так можно просмотреть всю таблицу 1.2. и убедиться, что эти системы в самом деле изоморфны. Вывод: алгебраическая система (M, $\bullet$) является группой, поэтому операция $\bullet$ ассоциативна.

IsoG 4. Построим изоморфизм той же группы (M, $\bullet$) *с собой*: положим $\varphi(e)=e$, $\varphi(a)=b$, $\varphi(b)=a$. Проверим, что $\varphi(a \bullet b)=\varphi(a) \bullet \varphi(b)$. Слева $\varphi(a \bullet b)=\varphi(e)=e$, справа $b \bullet a = e$. Другие проверки с использованием таблицы 1.2 также дают положительный результат.

Изоморфизм группы с собой называется *автоморфизмом*. Всегда существует *тривиальный автоморфизм*, когда $\varphi(x)=x$ для любого x. Автоморфизм в нашем примере – нетривиальный.

IsoG 5. Еще пример нетривиального автоморфизма: для аддитивной группы ($\mathbf{Z}$, $+$) возьмем отображение $\varphi(x)= -x$. Имеем $-(x+y)=(-x)+(-y)$. То же самое отображение задает автоморфизмы групп ($\mathbf{Q}$, $+$), ($\mathbf{R}$, $+$), ($\mathbf{C}$, $+$).

IsoG 6. Любая конечная группа изоморфна некоторой группе подстановок своих элементов (теорема Кэли). Эта группа подстановок называется *представлением* исходной группы. Так, группа, заданная таблицей 1.2 на с. 7, изоморфна группе подстановок на множестве $M=\{e,a,b\}$:

$\varphi(e)=\begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$ (соответствует 1-й строке таблицы),

$\varphi(a)=\begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$ (соответствует 2-й строке таблицы),

$\varphi(b)=\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$ (соответствует 3-й строке таблицы).

Замечание. Если порядок конечной группы равен n, то изоморфная ей группа из n подстановок *не есть* S_n. Так, в примере порядок группы n=3, тогда как группа S_3 состоит из 6 подстановок.

IsoG 7. Обычно считается, что в мультипликативной матричной группе матрицы обязательно должны быть невырожденными. Это не совсем так. Рассмотрим пример. Пусть имеем группу невырожденных матриц, каждую матрицу *окаймим*, добавив одну или несколько строк и такое же количество столбцов, заполненных нулями. Например, $\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix} \rightarrow \begin{bmatrix}1 & 1 & 0\\ 1 & 2 & 0\\ 0 & 0 & 0\end{bmatrix}$. По правилам действий с блочными матрицами при умножении «больших матриц» (т.е. окаймленных вырожденных) их невырожденные «родительницы» также будут перемножаться. По тем же правилам множество окаймленных вырожденных матриц замкнуто относительно умножения. Констатируем, что полученные таким способом матрицы образуют мультипликативную группу, изоморфную «родительской» группе. Нейтральным элементом в новой группе является матрица, полученная путем окаймлений из единичной «родительницы», симметричные элементы таким же образом получаются из обратных «родительских» матриц.

Возникает вопрос: могут ли в одной мультипликативной группе присутствовать как вырожденные, так и невырожденные матрицы? Отрицательный ответ получается при решении задачи **C 2.1.11** (см. ниже).

Близкое к изоморфизму понятие – *гомоморфизм* (homomorphism) *групп* $G_1=(M_1, \bullet)$ и $G_2=(M_2, \lozenge)$. Гомоморфизм получается, если в определении изоморфизма отказаться от требования взаимной однозначности отображения $\varphi: M_1 \rightarrow M_2$, но сохранить условие $\varphi(x \bullet y)=\varphi(x) \lozenge \varphi(y)$. Группа G_2 в этом случае называется *гомоморфным образом* группы G_1.

Ядро гомоморфизма $\ker(\varphi)$ – множество элементов группы G_1, переходящих в нейтральный элемент группы G_2. Ядро гомоморфизма является подгруппой в группе G_1 (см. ниже **Р 2.1.6)**.

Примеры гомоморфизма групп

HomG 1. $G_1=(\mathbf{R}^*, \cdot)$, $G_2=(\mathbf{R}_+, \cdot)$, $\varphi(x) = |x|$, $\ker(\varphi) = \{1, -1\}$. Сохранение операции обеспечивается тем, что $|x\cdot y| = |x|\cdot|y|$. Здесь G_2 – подгруппа в G_1, операция в группах одна и та же (умножение вещественных чисел).

Гомоморфизм группы внутрь самой себя называется *эндоморфизм*.

HomG 2. $G_1=(\mathbf{C}^*, \cdot)$, $G_2=(\mathbf{R}_+, \cdot)$, $\varphi(x) = |x|$, $\ker(\varphi) = \mathbf{U}$ – множество комплексных чисел, по модулю равных 1: $\mathbf{U} = \{z \mid z \in \mathbf{R}, |z|=1\} = \{\cos\alpha + i\cdot\sin\alpha \mid \alpha \in [0,2\pi[\}$.

HomG 3. Для любой группы G можно построить эндоморфизм, положив $\forall x \in G \;\; \varphi(x)=e$.

HomG 4. $G_1=\mathrm{GL}(F,n)$, $G_2=(F^*, \cdot)$ – мультипликативная группа ненулевых элементов числового поля F. Гомоморфизм задается формулой $\varphi(X) = \det(X)$, ядро гомоморфизма $\ker(\varphi) = \mathrm{SL}(F,n)$ (Базовое множество группы SL – матрицы, определители которых равны 1). Определитель произведения равен произведению определителей, т.е. $\det(X\cdot Y) = \det(X)\cdot\det(Y)$, так что операция сохраняется. Здесь базовые множества групп состоят из элементов *разной природы* и, хотя операция в обеих группах обозначена одним и тем же символом, но это *разные* операции: в G_1 – умножение матриц, в G_2 – умножение чисел.

Изоморфизм – частный случай гомоморфизма. Ядро изоморфизма тривиально – оно содержит только нейтральный элемент группы G_1.

Решение задач

Р 2.1.1. Будем использовать мультипликативную запись и не будем предполагать умножение коммутативным. Доказать, что $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$.

Решение. Найдем произведение $(a\cdot b)\cdot(b^{-1}\cdot a^{-1})=a\cdot b\cdot b^{-1}\cdot a^{-1}=a\cdot e\cdot a^{-1}=a\cdot a^{-1}=e$. Также и $(b^{-1}\cdot a^{-1})\cdot(a\cdot b)=e$. Таким образом, произведение $b^{-1}\cdot a^{-1}$ есть симметричный элемент к $a\cdot b$, т.е. $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$.

Р 2.1.2. Доказать, что если в группе $a^2=e$, $b^2=e$ и $(a\cdot b)^2=e$, то $a\cdot b=b\cdot a$.

Решение. Возьмем $(a\cdot b)^2 =a\cdot b\cdot a\cdot b=e$ и умножим слева на a: $a\cdot a\cdot b\cdot a\cdot b=a\cdot e$. В левой части заменим $a\cdot a$ на e и получим $b\cdot a\cdot b$, в правой части имеем a, т.е. $b\cdot a\cdot b=a$. Умножим это равенство слева на b, заменим $b\cdot b$ на e, получим $a\cdot b=b\cdot a$.

Если равенство $a^2=e$ верно для всех элементов группы, она коммутативная.

Р 2.1.3. Является ли группой алгебраическая система (**Q**, $\otimes$), где операция $x\otimes y=x+y-x\cdot y$?

Решение. В задаче **Р 1.3** было установлено, что операция $\otimes$ ассоциативна, нейтральный элемент $e=0$ и симметричный элемент к любому числу x задается формулой $\bar{x}=\frac{x}{x-1}$. Чтобы получилась группа, из числового поля надо исключить 1, причем множество **Q**\{1} замкнуто относительно $\otimes$ (см. выше задачу **С 1.6**).

Р 2.1.4. В базовом множестве полной линейной группы GL(F,n) квадратных невырожденных матриц порядка n над числовым полем F выделим подмножество Tri(F,n) верхних треугольных матриц, также невырожденных. (Напомним, что у верхних треугольных матриц все элементы, лежащие ниже главной диагонали равны 0.) Это множество замкнуто относительно умножения матриц.

Проверим это на примере матриц 2-го порядка. Пусть $A_1=\begin{pmatrix} p_1 & q_1 \\ 0 & r_1 \end{pmatrix}$, $A_2=\begin{pmatrix} p_2 & q_2 \\ 0 & r_2 \end{pmatrix}$, произведение: $A_1\cdot A_2=\begin{pmatrix} p_1p_2 & p_1q_2+q_1r_2 \\ 0 & r_1r_2 \end{pmatrix}$ – треугольная матрица. Из этого же примера видно, что умножение треугольных матриц некоммутативно: если поменять местами матрицы-сомножители, то в элементах матрицы-

произведения поменяются местами индексы 1 и 2, элементы на диагонали не изменятся, но внедиагональный элемент станет равен $p_2q_1+q_2r_1 \neq p_1q_2+q_1r_2$.

Нейтральный элемент группы, т.е. единичную матрицу можно считать треугольной, наконец, если матрица $A \in T_n$, то и симметричный элемент группы, т.е. обратная матрица $A^{-1} \in T_n$.

Покажем это также на примере матриц 2-го порядка. Пусть верхняя треугольная матрица $A = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix}$, где $p \neq 0$ и $r \neq 0$. Тогда обратная матрица также верхняя треугольная: $A^{-1} = \frac{1}{p \cdot r} \cdot \begin{pmatrix} r & -q \\ 0 & p \end{pmatrix} = \begin{pmatrix} \frac{1}{p} & -\frac{q}{p \cdot r} \\ 0 & \frac{1}{r} \end{pmatrix}$.

Таким образом, мы доказали, что Tri(F,n) является подгруппой в группе GL(F,n) при n=2. На самом деле это верно при всех n.

Р 2.1.5. Доказать, что группа (**Z**, $\oplus$) с нестандартной операцией $\oplus$, задаваемой равенством $x \oplus y = x+y-1$ (см. пример **G 13**), изоморфна «обычной» группе (**Z**, +).

Решение. Отображение φ: **Z**$\to$**Z** зададим формулой $\varphi(x)=1-x$. Проверим, что $\varphi(x \oplus y)=\varphi(x)+\varphi(y)$. Слева $\varphi(x \oplus y)=1-(x \oplus y)=1-(x+y-1)=2-(x+y)$, справа $\varphi(x)+\varphi(y)=(1-x)+(1-y)=2-(x+y)$.

Р 2.1.6. Доказать, что ядро гомоморфизма является группой.

Решение. Будем считать обе группы мультипликативными, соответствующим образом обозначим бинарную операцию и унарную операцию перехода к симметричному элементу. Нейтральные элементы групп обозначим e_1 и e_2 соответственно. Коммутативность операции не предполагаем.

Пусть $x \in \ker(\varphi)$ и $y \in \ker(\varphi)$, т.е. $\varphi(x) = \varphi(y) = e_2$. Тогда

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = e_2 \cdot e_2 = e_2, \text{ т.е. } x \cdot y \in \ker(\varphi)$$

– ядро замкнуто относительно операции.

Для произвольного $x \in G_1$ имеем $x \cdot e_1 = e_1 \cdot x = x$, поэтому

$$\varphi(x\cdot e_1)=\varphi(x)\cdot\varphi(e_1)=\varphi(e_1\cdot x)=\varphi(e_1)\cdot\varphi(x)=\varphi(x)\Rightarrow \varphi(e_1)=e_2\Rightarrow e_1\in\ker(\varphi).$$

Для произвольного $x\in G_1$ имеем $x\cdot x^{-1}=x^{-1}\cdot x=e_1\Rightarrow \varphi(x\cdot x^{-1})=\varphi(x^{-1}\cdot x)=\varphi(e_1)$. Но $\varphi(x\cdot x^{-1})=\varphi(x)\cdot\varphi(x^{-1})$, $\varphi(x^{-1}\cdot x)=\varphi(x^{-1})\cdot\varphi(x)$, $\varphi(e_1)=e_2$. Если $x\in\ker(\varphi)$, то $\varphi(x)=e_2$, получаем $e_2\cdot\varphi(x^{-1})=\varphi(x^{-1})\cdot e_2=e_2$.

Следовательно, $\varphi(x^{-1}) = e_2\Rightarrow \varphi(x^{-1})\in\ker(\varphi)$.

Мы доказали, что ядро гомоморфизма замкнуто относительно групповой операции, что ядру принадлежит нейтральный элемент, и что для любого элемента ядра оно содержит симметричный элемент. Заключаем, что ядро является группой.

Р 2.1.7. Построить все неизоморфные группы 4-го порядка.

Решение задачи основывается на свойствах **Cay**1 и **Cay**2 таблицы Кэли, задающей группу (см. с. 17). На самом деле эти свойства определяют квазигруппу, поэтому важнейшее свойство группы – ассоциативность операции – придется устанавливать косвенным способом.

Пусть базовое множество состоит из букв $\{e, a, b, c\}$, причем e – нейтральный элемент. Сделаем заготовку таблицы Кэли, строки и столбцы пронумеруем для удобства обсуждения, бинарную операцию обозначим •. Первая строка и первый столбец таблицы заполняются «на автомате».

Таблица 2.2

	1	2	3	4
•	*e*	*a*	*b*	*c*
1	*e*	*e*	*a*	*b*	*c*

Что можно поместить в клетку (2,2)? Букву *a* нельзя (она уже есть и в строке и в столбце), попробуем *e*. Чтобы показать произвольность этого выбора, подчеркнем букву. Поскольку в строке 2 уже имеются буквы *a* и *e*, в оставшихся двух клетках должны стоять *b* и *c*. Ограничения на заполнения столбцов (по одному разу все буквы) приводят к однозначному выбору: в клетку (2,3) – букву *c*, в клетку (2,4) – букву *b*. Аналогично заполняются клетки столбца 2.

В клетку (3,3) можно поместить e или a (но не b и не c !), попробуем e, причем ввиду произвольности этого выбора опять подчеркнем букву. Оставшиеся клетки (3,4), (4,3) и (4,4) заполняются однозначно.

Таким образом, мы получили одну из таблиц Кэли (таблица 2.2). Некоторые свойства этой алгебраической системы очевидны, но ассоциативность надо как-то доказывать. Если основываться только на определении, потребовалось бы перебрать 4^3=256 вариантов (или раза в два меньше за счет коммутативности, которой мы, кстати, не добивались, «она сама пришла»).

Вместо этого построим группу подстановок, изоморфную данной алгебраической системе. Подстановки обозначим теми же буквами. Положим

$$e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ a=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ b=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\ c=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

Перемножая эти подстановки по обычным правилам, мы воспроизведем нашу таблицу Кэли. Умножение подстановок ассоциативно, тем самым доказана ассоциативность операции •. Все остальные свойства (замкнутость и т.п.) были очевидны с самого начала.

Замечание 1. Как были построены подстановки, моделирующие таблицу? Использован прием из доказательства теоремы Кэли (всякая конечная группа порядка n изоморфна некоторой группе подстановок степени n). Цифры 1, 2, 3, 4 в подстановках являются «псевдонимами» букв e, a, b, c.

Замечание 2. Эта *четверная группа Клейна* уже встречалась как группа симметрий (вращений) прямоугольника, отличного от квадрата (пример **G 15**). Она замечательна тем, что квадраты всех ее элементов равны нейтральному элементу e, т.е. $e^2=a^2=b^2=c^2=e$.

Итак, мы построили одну группу 4-го порядка. Чтобы получить другие, применим метод «перебора с возвратом» (по-английски *backtracking*).

Последний произвольный выбор был сделан для клетки (3,3), изменим его и поместим в

Таблица 2.3

	1	2	3	4
	•	e	a	b	c
1	e	e	a	b	c
2	a	a	e	c	b
3	b	b	c	a	e

эту клетку вместо буквы *e* букву *a*, клетки (3,4), (4,3) и (4,4) заполним по-новому (также однозначно). Мы получили новую таблицу (таблица 2.3). Чтобы ее «легитимизировать» (т.е. доказать ассоциативность операции), построим другую группу подстановок

$$e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ a=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ b=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\ c=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}.$$

Вспомним условие задачи: группы должны быть неизоморфными. Рассмотрим квадраты элементов новой группы. Имеем $e^2=e$ и $a^2=e$, но $b^2\neq e$ и $c^2\neq e$.

В группе Клейна, построенной раньше, квадраты всех элементов были равны *e*. Ясно, что группы неизоморфны.

Вернемся (backtracking!) к клетке (2,2). Вместо буквы *e* в нее можно поместить букву *b*. Этот выбор опять произволен, букву подчеркнем. Заполнение остальных клеток строки 2 и столбца 2 однозначно.

В клетку (3,3) можно поместить только букву *e*, так как если туда поместить *a*, то в клетку (3,4) придется поместить *e*, что недопустимо.

Мы получили еще одну таблицу Кэли (таблица 2.4). На самом деле группы, представленные таблицами 2.3 и 2.4. изоморфны. Отображение множества $\{e, a, b, c\}$ на себя, задающее изоморфизм этих групп, предлагается построить в качестве самостоятельного упражнения (см. ниже задачу **С 2.1.13**). **З**аодно будет доказана ассоциативность операции, представленной последней таблицей.

Таблица 2.4

	1	2	3	4
•	*e*	*a*	*b*	*c*
1	*e*	*e*	*a*	*b*	*c*

Строго говоря, следовало бы создать еще варианты таблицы Кэли, поместив *на первом шаге* произвольного выбора в клетку (2,2) вместо *a* букву *b* или *c*. Но здравый смысл подсказывает, что никакой разницы между этими тремя буквами нет (другое дело – нейтральный элемент *e*, который играет в группе осо-

бую роль). Поэтому делаем вывод: поставленная задача решена, неизоморфных групп 4-го порядка существует всего две: одна группа Клейна, другая – циклическая.

Задачи для самостоятельного решения

С 2.1.1. Докажите теоремы 1,2,3 (формулировки см. на с. 17).

Указание. Теоремы 1 и 2 можно доказать «от противного», для теоремы 3 легко написать решения обоих уравнений**.**

С 2.1.2. Постройте все неизоморфные группы 3-го порядка.

Указание. Используйте подход задачи **Р 2.1.7.** На самом деле, существует *всего одна* группа – в этом и надо убедиться.

С 2.1.3. Рассмотрите $\mathrm{Uni}(F,n)$ – множество унимодулярных квадратных матриц порядка n над числовым полем F (их определители равны ± 1). Докажите, что $\mathrm{Uni}(F,n)$ – группа.

С 2.1.4. Постройте таблицу умножения для группы симметрий прямоугольника (пример **G 15**).

С 2.1.5. В примере **IsoG 6** было построено представление подстановками группы, заданной таблицей 1.2. Измените обозначения элементов множества, на котором заданы перестановки, на более традиционные: $e\to 1$, $a\to 2$, $b\to 3$. В результате получатся подстановки $e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $b=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$. Постройте таблицу умножения этих подстановок и убедитесь, что она совпадает с таблицей 1.2.

С 2.1.6. Постройте таблицы умножения для групп симметрий квадрата и правильного треугольника.

Указание. К вращениям, входящим в группу симметрий прямоугольника, в группу симметрий квадрата надо добавить еще вращения вокруг двух диагоналей квадрата, порядок этой группы равен 6. Порядок группы симметрий правильного треугольника также равен 6 (три вращения без выхода из плоскости, три – с выходом).

С 2.1.7. Пусть D_n – множество диагональных матриц порядка n. Являются ли группами алгебраические системы $(D_n, +)$ и $(D_n, \cdot)$? Какие дополнительные ограничения нужны для положительного ответа?

С 2.1.8. Какие из множеств матриц 2-го порядка являются группами относительно умножения матриц? Какие из них являются подгруппами других?

1) $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a,b \in \mathbf{R},\ a^2+b^2>0 \right\}$;

2) $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a,b \in \mathbf{R},\ a^2+b^2=1 \right\}$;

3) $\left\{ \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \middle| \, a,b \in \mathbf{R},\ a^2+b^2>0 \right\}$;

4) $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| \, a,b \in \mathbf{R},\ a^2+b^2>0 \right\}$;

5) $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| \, a,b \in \mathbf{Q},\ a^2+b^2>0 \right\}$;

6) $\left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \middle| \, \alpha \in \mathbf{R} \right\}$.

С 2.1.9. При каких значениях параметра λ множество *ненулевых* матриц вида $\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}$ является мультипликативной группой? Значение λ одно и то же для всех матриц предполагаемой группы, x, y произвольные, не равные неулю одновременно. Рассмотрите варианты: a) $x, y, \lambda \in \mathbf{Q}$; b) $x, y, \lambda \in \mathbf{R}$; c) $x, y, \lambda \in \mathbf{C}$.

С 2.1.10. Рассмотрите $(L, \circ)$ – группу линейных невырожденных функций вида $f(x)=ax+b$ при $a \neq 0$, групповая операция – композиция функций (см. пример **G 9**). Докажите, что следующие подмножества функций являются коммутативными подгруппами

a) $a=1$, b любое; b) $a \neq 0$ любое, $b=0$.

Каким числовым группам изоморфны эти подгруппы?

Рассмотрите также подмножество функций при $a=\pm 1$, b любое. Является ли оно подгруппой? Является ли эта подгруппа коммутативной?

С 2.1.11. Докажите, что мультипликативная матричная группа может состоять либо только из невырожденных матриц, либо только из вырожденных (пример группы вырожденных матриц см. пример **IsoG 6**).

Указание. Учтите, что в любой группе нейтральный элемент – единственный. Чему должно равняться произведение произвольной матрицы на симметричный элемент группы?

С 2.1.12. Убедитесь, что предлагаемая таблица Кэли (таблица 2.5) задает квазигруппу. Для этого проверьте, что выполняются свойства **Cay**1 и **Cay**2, благодаря чему каждое из уравнений $a\cdot x=b$ и $y\cdot a=b$ однозначно разрешимо при любых a и b. (Здесь a и b – *параметры*, их значениями могут быть произвольные элементы базового множества $\{p,q,r,s\}$). Кроме того, покажите, что это *не группа*: в этой казигруппе нет нейтрального элемента e, для которого $e\cdot x=x$ и $x\cdot e=x$ при любом x (хотя имеется левый нейтральный элемент – это p). Ассоциативности тоже нет (приведите контрпример).

Таблица 2.5

Квазигруппа

$\cdot$	p	q	r	s
p	p	q	r	s

В группе, где существует нейтральный элемент и симметричные элементы, решения уравнений $a\cdot x=b$ и $y\cdot a=b$ можно записать в виде $x=a^{-1}\cdot b$ и $y=b\cdot a^{-1}$. Здесь удобно использовать обозначения из пакета MatLab® $x=a^{-1}\cdot b=a\backslash b$ (\ – «левое деление») и $y=b\cdot a^{-1}=b/a$ (/ – «правое деление»). Хотя нейтрального элемента и симметричных элементов в квазигруппе нет, на основании таблицы операции «умножения» ($\cdot$) можно построить две таблицы новых операций: «левого деления» (\) и «правого деления» (/).

Найдем, например, $q\backslash s$. Это решение уравнения $q\cdot x=s$. В строчке таблицы, соответствующей элементу q, найдем элемент s, он стоит в столбце, соответствующем элементу p. Таким образом, имеем $q\backslash s=p$. Остальные элементы таб-

лицы операции (\) найдем тем же способом. Элементы таблицы операции (/) ищутся так же, только роль строк и столбцов меняется.

Задание: постройте таблицы Кэли для левого и правого деления в данной квазигруппе.

С 2.1.13. Докажите изоморфизм групп, представленных таблицами 2.3 и 2.4 на с. 29 и 30.

С 2.1.14. Пусть U – непустое множество, $B = 2^U$ его *булеан* (множество всех подмножеств). Элементами булеана являются подмножества в U.

Введем симметрическую разность множеств

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y).$$

Какие из алгебраических систем $(B, \cap)$, $(B, \cup)$, (B, Δ) являются группами?

2.2. Циклические группы

Группа называется *циклической*, если все ее элементы являются (в мультипликативной терминологии) *степенями* какого-то ее элемента. Например, возьмем группу комплексных чисел, отличных от нуля ($\mathbf{C}^*$, ·), выберем в ней мнимую единицу i и рассмотрим ее степени: $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$. Дальше числа будут повторяться, процесс *зациклится* (отсюда и название). У нас получилась группа ($\{i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1\}$, ·). Говорят, что эта группа *порождена* элементом i и обозначают ее $\langle i \rangle$ (объемлющая группа должна подразумеваться).

Если вместо мнимой единицы i взять число 2, получится бесконечная последовательность $2^1 = 2$, $2^2 = 2 \cdot 2$, $2^3 = 2^2 \cdot 2$, … . Чтобы превратить ее в мультипликативную группу, надо добавить $2^0 = 1$ и все отрицательные степени двойки: $2^{-1} = \frac{1}{2}$, $2^{-2} = \frac{1}{4}$, $2^{-3} = \frac{1}{8}$, … Получится бесконечная циклическая группа

$$(\{\dots, 2^{-3} = \tfrac{1}{8}, 2^{-2} = \tfrac{1}{4}, 2^{-1} = \tfrac{1}{2}, 2^0 = 1, 2^1 = 2, 2^2 = 2, 2^3 = 2, \dots\}, \cdot) = \langle 2 \rangle$$

(объемлющая группа та же ($\mathbf{C}^*$, ·) или, если угодно, ($\mathbf{R}^*$, ·) или даже ($\mathbf{Q}^*$, ·)).

Очевидно, что группа $\langle 2 \rangle$ изоморфна аддитивной группе ($\mathbf{Z}$, +): любому ее элементу 2^k соответствует $k \in \mathbf{Z}$, при перемножении степеней с равным основанием показатели складываются, нейтральному элементу $2^0 = 1$ соответствует нейтральный элемент 0, симметричному элементу 2^{-k} соответствует симметричный элемент $-k$.

Как построить циклическую группу ($\mathbf{Z}$, +), следуя определению о «степенях»? Образующий элемент 1, далее 1+1=2, 2+1=3 и т.д. Но это не степени! В случае, когда объемлющая группа аддитивная, вместо степеней говорят о *кратностях* и пишут так: (2)1=1+1=2, (3)1=2+1 и т.д.

Конечно, писать (2)1 вместо 2·1 немного смешно, однако элементами объемлющей группы могут быть, например, матрицы: ($\mathbf{Z}^{n \times n}$, +), а умножение числа на матрицу в этой алгебраической системе *не определено* и тогда запись (2)A как сокращение для $A+A$ вполне уместна.

В разделе 2.1 было доказано, что алгебраическая система $(\{e,a,b\}, \bullet)$, заданная таблицей 1.2 на с. 7, является группой, изоморфной $(\mathbf{Z}_3, +_3)$. Сейчас мы (независимо от прежнего доказательства) покажем, что эта алгебраическая система является циклической группой. Используя обозначения степеней для «произведений» с операцией $\bullet$, найдем $a^2=a\bullet a=b$, $a^3=b\bullet a=e$. Действительно, воспроизвелись все элементы базового множества.

Три теоремы о циклических группах

Теорема 1. Любая циклическая группа коммутативна.

Теорема 2. Все подгруппы циклической группы циклические.

В конечной циклической группе порядка n существует и притом единственная подгруппа порядка k для любого k, являющегося делителем n.

Теорема 3. Все циклические группы одного порядка изоморфны.

Например, группа $<i>$ изоморфна группе вычетов $(\mathbf{Z}_4, +_4)$ – любой k-ой степени числа i соответствует остаток от деления k на 4.

Согласно теореме Кэли, любая конечная группа изоморфна некоторой группе подстановок ее элементов. Для циклической группы порядка n таким изоморфным представлением является циклическая группа C_n, состоящая из степеней подстановки-цикла $c_n=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ 2 & 3 & \cdots & n & 1\end{pmatrix}$: $C_n=\left\{c_n^1, c_n^2, \cdots, c_n^{n-1}, c_n^n\right\}$, причем c_n^n – тождественная подстановка: $c_n^n=\begin{pmatrix}1,2,\cdots,n\\ 1,2,\cdots,n\end{pmatrix}$, т.е. нейтральный элемент группы. (Циклическая группа подстановок C_6 строится при решении задачи **С 2.2.6**.)

Порядком любого *элемента* x объемлющей группы (в примере это $(\mathbf{C}^*, \cdot)$) называется порядок порожденной им циклической группы $<x>$, т.е. число ее элементов. Порядок элемента x можно обозначать $|x|$ (если это не вызывает недоразумений). В группе $(\mathbf{C}^*, \cdot)$ порядок мнимой единицы i равен 4, порядок

числа –1 равен 2, порядок числа 1 равен 1, число 2 имеет бесконечный порядок.

Примеры циклических групп

1. $(\mathbf{Z}_n, +_n)$ – аддитивная группа вычетов по модулю n, порядок группы равен n.
2. $(\mathbf{Z}_p^*, \cdot_p)$ – мультипликативная группа ненулевых вычетов по простому модулю p. В теории доказывается, что эта группа циклическая. Порядок группы $\mathbf{Z}_p^*$ равен p–1 (см. ниже **Р 2.2.1**).
3. Комплексные корни из единицы: $\left(U_n = \left\{\varepsilon_k = \cos\frac{2\pi k}{n} + i\cdot\sin\cdots, k = 0,1,\cdots,n-1\right\}, \cdot\right)$. Порядок группы равен n, образующим элементом является, например, ε_1.
4. $(n\mathbf{Z}, +)$ – аддитивная группа целых чисел, кратных заданному натуральному числу n, образующим элементом является число n. Порядок группы бесконечен.

Решение задач

Р 2.2.1. Убедиться, что группа $(\mathbf{Z}_5^*, \cdot_5)$ является циклической. Выяснить, какими из ее элементов она порождается.

Решение. На с. 20 представлена таблица 2.1, задающая умножение в группе $(\mathbf{Z}_5^*, \cdot_5)$. В соответствии с этой таблицей найдем степени одного из элементов группы, например 2 (для простоты записи «умножение по модулю» $\cdot_5$ заменим обычным знаком умножения, степени также будем изображать «без затей»):

$$2^1 = 2,\ 2^2 = 2\cdot2 = 4,\ 2^3 = 4\cdot2 = 3,\ 2^4 = 3\cdot2 = 1.$$

Видим, что за 4 шага получились все элементы группы, следовательно, она циклическая, порядок элемента 2 равен 4. Таков же порядок элемента 3, порядок элемента 4 равен 2, так как $4^2 = 4\cdot4 = 1$, порядок элемента 1 равен 1. Таким образом, циклическая группа $(\mathbf{Z}_5^*, \cdot_5)$ порождается любым из ее элементов 2 и 3.

Р 2.2.2. Доказать, что в любой группе произведения ab и ba имеют одинаковый порядок.

Решение. Пусть $|ab| = p$. Это значит, что $(ab)^p = e$ (нейтральный элемент группы) и $(ab)^q \neq e$ для любого $0 < q < p$. Развернем выражение $(ab)^p$, получится $\underbrace{(ab)\cdot(ab)\cdot\ldots\cdot(ab)}_{p \text{ пар}} = e$. Умножим обе части равенства слева на a^{-1}, справа на a: $a^{-1}\cdot\underbrace{(ab)\cdot(ab)\cdot\ldots\cdot(ab)}_{p \text{ пар}}\cdot a = a^{-1}\cdot e\cdot a$. В правой части снова получится e, а в левой, пользуясь ассоциативностью, расставим скобки по-другому и получим $\underbrace{(ba)\cdot(ba)\cdot\ldots\cdot(ba)}_{p \text{ пар}} = e$. Это означает, что порядок произведения ba не превосходит p. Допустим, что $|ba| = q < p$, т.е. $\underbrace{(ba)\cdot(ba)\cdot\ldots\cdot(ba)}_{q \text{ пар}} = e$. Умножим обе части равенства слева на b^{-1}, справа на b и такими же преобразованиями придем к равенству $\underbrace{(ab)\cdot(ab)\cdot\ldots\cdot(ab)}_{q \text{ пар}} = e$, что противоречит условию $(ab)^q \neq e$ для любого $q < p$.

Р 2.2.3. Пусть G – группа порядка n, не обязательно циклическая. Доказать, что для любого элемента $g \in G$ верно соотношение $g^n = e$ (нейтральный элемент группы).

Решение. Рассмотрим циклическую подгруппу $<g>$, пусть ее порядок равен k, т.е. $g^k=e$. По теореме Лагранжа порядок группы n делится на k, обозначим $n/k=p$, тогда $n=k\cdot p$, $g^n=g^{k\cdot p}=(g^k)^p=e^p=e$.

Р 2.2.4. Найти порядок элемента группы $a = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,4\,5\,2\,1 \end{pmatrix} \in S_5$.

Решение. Порядок объемлющей группы 5!=120 слишком велик, чтобы перебирать a, a^2 и т.д. Построим цикловое представление данной подстановки $a = (1, 3, 5)(2, 4)$. В подстановке a^2 цикл (2, 4) распадется и превратится в (2)(4), то же самое будет и в подстановках a^{2k} при любом k. В подстановке a^2 цикл (1, 3, 5) не распадется, а превратится в (1, 5, 3). В подстановке a^3 цикл (1, 3, 5) распадется и превратится в (1)(3)(5), то же самое будет и в подстановках a^{3k} при любом k. Напротив, цикл (2, 4) в подстановке a^3 не распадется, он

перейдет в себя. Делаем вывод: чтобы распались оба цикла и подстановка превратилась в тождественную e = (1)(2)(3)(4)(5), показатель степени должен делиться на 2 и на 3. Наименьшее такое число равно 6. В общем случае порядок подстановки равен НОК длин всех ее циклов.

Р 2.2.5. Найти наибольший порядок элемента группы S_{12}.

Решение. Порядок группы S_{12} равен 12!=479001600. Ясно, что перебор элемента за элементом неприемлем, хотя совсем без перебора не обойтись. Цивилизованный подход таков: представим 12 в виде суммы нескольких чисел, у которых НОК имеет максимально возможное значение (в комбинаторике такие представления называются *неупорядоченными разбиениями*, переставлять слагаемые не имеет смысла). Разбиения 2+10, 3+9, 4+8 совсем плохие, 5+7 немного получше, НОК=35; 6+6 никуда не годится. Попробуем три слагаемых, не беря совсем бесперспективные варианты. Разбиение 1+3+8 дает НОК=24<35, 1+5+6 дает НОК=30 – тоже хуже прежнего рекорда. Разбиение 3+4+5 дает НОК=60 и это максимум. Пример подстановки, имеющей такой порядок:

(1, 2, 3)(4, 5, 6, 7)(8, 9, 10, 11, 12).

Р 2.2.6. Построить одну из подгрупп циклической группы порядка 12.

Решение. Число 12 имеет много делителей, это 1,2,3,4,6,12. Пусть заданная группа порядка 12 имеет вид $\{a, a^2, a^3, a^4, \dots, a^{11}, a^{12}=e\}$. Построим, например, подгруппу порядка 4. Найдем *сопряженный делитель* для 4, это 12/4=3, возьмем в данной группе элемент $b=a^3$ и построим группу $\langle b\rangle$. Получим $b^1=a^3$, $b^2=a^6$, $b^3=a^9$, $b^4=a^{12}=e$ – циклическая группа порядка 4.

Р 2.2.7. Найти порядок элемента группы.

1) $\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}$ в группе GL($\mathbf{C}$, 2) ($a\in \mathbf{C}$, любое).

Решение. $\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}\cdot\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ – порядок элемента равен 2.

2) $-\frac{\sqrt{3}}{2}-\frac{1}{2}i$ в группе $\mathbf{C}^*$.

Решение. $-\frac{\sqrt{3}}{2}-\frac{1}{2}i=\cos\frac{7\pi}{6}+\sin\frac{7\pi}{6}$, модуль равен 1. Заметим, что при любом другом модуле порядок элемента был бы бесконечным (почему?).

Умножение комплексных чисел соответствует сложению их аргументов. Рассмотрим последовательность аргументов $\frac{7\pi}{6}$, $\frac{2\cdot 7\pi}{6}$, $\frac{3\cdot 7\pi}{6}$ и т.д. Чтобы получить нейтральный элемент группы, т.е. $1=\cos 2k\pi+i\sin 2k\pi$, надо, во-первых, «подавить» знаменатель, а во-вторых, сделать числитель четным. В первый раз это произойдет, когда множитель при $\frac{7\pi}{6}$ станет равен 12: $\frac{12\cdot 7\pi}{6}=14\pi=7\cdot(2\pi)$. Видим, что порядок элемента равен 12.

Задачи для самостоятельного решения

С 2.2.1. Докажите, что множество $\left\{E=\begin{pmatrix}1&0\\0&1\end{pmatrix}, I=\begin{pmatrix}0&1\\-1&0\end{pmatrix}, -E, -I\right\}$ с операцией матричного умножения является циклической группой.

С 2.2.2. Найдите порядок элемента группы $a=\begin{pmatrix}1\,2\,3\,4\,5\,6\,7\,8\;9\,10\\2\,1\,4\,5\,3\,7\,8\,9\,10\;6\end{pmatrix}\in S_{10}$.

Указание. Воспользуйтесь подходом задачи **Р 2.2.4.**

С 2.2.3. Найдите порядок элемента группы:

1) $\begin{pmatrix}0&1\\i&0\end{pmatrix}$ в группе GL(**C**, 2);

2) $\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$ в группе SL(**R**, 2);

3) $\begin{pmatrix}2&a\\0&½\end{pmatrix}$ в группе SL(**R**, 2), $a\in$**R**;

4) $\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$ в группе GL(**R**, 3).

5) $-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$ в группе $\mathbf{C}^*$;

С 2.2.4. Докажите, что если порядок группы – нечетное число, то каждый элемент является квадратом какого-то элемента группы.

Указание. Воспользуйтесь результатом решения задачи **Р 2.2.3**.

С 2.2.5. Докажите, что в любой группе элементы a и $b=p\cdot a\cdot p^{-1}$ имеют одинаковый порядок. (Здесь p – произвольный элемент группы.)

Указание. Воспользуйтесь подходом задачи **Р 2.2.2**.

С 2.2.6. Выпишите все подстановки циклической группы C_6, для каждой подстановки укажите ее порядок в этой группе.

С 2.2.7. Какими из элементов группы $(\mathbf{Z}_7^*, \cdot_7)$ она порождается? Тот же вопрос для групп $(\mathbf{Z}_{11}^*, \cdot_{11})$ и $(\mathbf{Z}_{13}^*, \cdot_{13})$.

Указание. Воспользуйтесь подходом задачи **Р 2.2.1.**

2.3. Факторизация групп

Основы теории

Пусть задана группа G с мультипликативной записью операции и подгруппа $H\subset G$. Возьмем произвольный элемент $a\in G$ и построим множество элементов группы $L_a=a\cdot H=\{a\cdot h|h\in H\}$. Это множество называется *левый смежный класс* элемента a по подгруппе H. Левые смежные классы попарно не пересекаются, их объединение равно базовому множеству группы G, одним из классов является сама подгруппа H. Таким образом, смежные классы задают *разбиение* базового множества группы G (см. ниже **С 2.3.1**). Критерием (необходимым и достаточным условием) принадлежности двух элементов x и y одному и тому же левому смежному классу является $x^{-1}\cdot y=x\backslash y\in H$ (см. ниже **Р 2.3.12**). Этот критерий легко запомнить: элементы группы принадлежат одному *левому классу* если их *левое частное* принадлежит подгруппе.

Определение левого (и правого) деления см. выше **С 2.1.12.**

Аналогично построим правый смежный класс $R_a=H\cdot a=\{h\cdot a|h\in H\}$. Все, что сказано о левых смежных классах, справедливо и для правых. Критерием принадлежности двух элементов x и y одному и тому же правому смежному классу является $x\cdot y^{-1}=x/y\in H$ (см. ниже **С 2.3.15**). Элементы группы

принадлежат одному *правому классу* если их *правое частное* принадлежит подгруппе.

Между подгруппой и любым смежным классом (как левым, так и правым) имеет место биекция.

В случае конечной группы G количество смежных классов называется *индексом* подгруппы H в группе G, индекс равен частному от деления порядка группы G на порядок подгруппы H, обозначение индекса $I(G/H)$ (в некоторых книгах $[G:H]$).

Если каждый левый класс совпадает с соответствующим правым классом, подгруппа H называется *нормальной* (*инвариантной*) *подгруппой*, чаще ее называют *нормальный делитель* группы G (конечно, термин «делитель» хорошо смотрится только для мультипликативных групп). На практике это свойство трудно проверить, если индекс подгруппы велик (тем более, если он бесконечен). Поэтому используются эквивалентные формулировки:

$$\forall g\in G \quad g^{-1}\cdot H\cdot g=H \text{ или } \forall g\in G\ \forall h\in H \quad h'=g^{-1}\cdot h\cdot g\in H.$$

Очевидно, что в коммутативной (абелевой) группе все подгруппы являются нормальными.

Достаточное (не необходимое!) условие нормальности подгруппы – ее индекс равен 2 (см. ниже **С 2.3.2**).

Принадлежность двух элементов x и y одному и тому же смежному классу по нормальному делителю H теперь можно описать двояко: $x^{-1}\cdot y=x\backslash y\in H$ и $x\cdot y^{-1}=x/y\in H$, причем любое из этих условий является следствием другого.

Имея группу G и нормальную подгруппу H, можно построить новую группу. Это *факторгруппа* группы G по подгруппе H, она обозначается G/H.

Элементами факторгруппы являются смежные классы, операцию в факторгруппе G/H обозначают и называют так же, как операцию в группе G. При изложении мы будем придерживаться мультипликативной терминологии и обозначений (впрочем, см. ниже задачи **Р 2.3.1** и **Р 2.3.2**). Операция в

факторгруппе выполняется *по представителям*: чтобы получить произведение двух классов $K_1 \cdot K_2$ в G/H, надо взять по одному элементу-представителю в этих классах $x_1 \in K_1$, $x_2 \in K_2$ и перемножить их в группе G. Пусть произведение элементов принадлежит некоторому классу K: $x_1 \cdot x_2 = x \in K$. Тогда этот класс объявляется *произведением классов*: $K = K_1 \cdot K_2$.

Это определение может вызвать недоумение: а если мы возьмем в тех же классах других представителей $y_1 \in K_1$, $y_2 \in K_2$ и перемножим их, какому классу будет принадлежать произведение? В теории доказывается, что *если подгруппа является нормальным делителем, результат не зависит от выбора представителей*: $y_1 \cdot y_2 = y \in K$ (тому же самому), хотя, возможно, $y \neq x$.

В задаче **Р 2.3.9** (см. ниже) делается неудачная попытка построить «одностороннюю факторгруппу» по подгруппе, *не являющейся* нормальным делителем. Неудача проявляется в том, что при выборе разных пар представителей в перемножаемых классах, произведения разных пар представителей попадают в разные классы.

В любой группе G несобственные подгруппы $\{e\}$ и G являются нормальными делителями (см. ниже **С 2.3.3**).

Понятия нормального делителя, смежных классов и факторгруппы тесно связаны с понятием гомоморфизма. Если G – группа, H – нормальный делитель, $F = G / H$ – факторгруппа, то существует гомоморфизм $\varphi: G \to F$ и ядром этого гомоморфизма является нормальный делитель H. Если факторгруппа F изоморфна некоторой другой группе F', то существует гомоморфизм $\varphi': G \to F'$ и ядром этого гомоморфизма также является нормальный делитель H.

Построение группы $F' \cong G/H$ является интересной задачей. Дело в том, что факторгруппа – весьма громоздкая конструкция (ее *элементами* являются *множества*, зачастую бесконечные) и хочется получить для нее какое-то более простое описание. Эта «интересная задача» формально некорректна: мало ли какие группы изоморфны данной… Можно, однако, предложить некий (неформальный) прием, во многих случаях позволяющий все же получить

искомую изоморфную группу. Прием заключается в том, что в каждом смежном классе факторгруппы G/H надо выбрать *простейшего представителя*. Если окажется, что совокупность этих простейших представителей является группой относительно той же самой (или похожей) операции, на которой построена исходная группа G, то это и будет искомая группа F'.

Решение задач

Р 2.3.1. Построить факторгруппу аддитивной группы целых чисел ($\mathbf{Z}$, +) по подгруппе $3\mathbf{Z}$.

Замечание. Полное обозначение этой подгруппы ($3\mathbf{Z}$, +), но операция + автоматически переносится в подгруппу из группы, поэтому можно писать просто $3\mathbf{Z}$. В дальнейшем упрощенные обозначения подгрупп будем использовать без оговорок.

Решение. Имеем три смежных класса: $3\mathbf{Z}$, $3\mathbf{Z}+1$, $3\mathbf{Z}+2$ (используем операцию «+», а не «·«, как в теории, потому что объемлющая группа аддитивная):

$3\mathbf{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$,

$3\mathbf{Z}+1 = \{\dots, -5, -2, 1, 4, 7, \dots\}$,

$3\mathbf{Z}+2 = \{\dots, -4, -1, 2, 5, 8, \dots\}$.

Попробуем применить критерий принадлежности двух элементов к одному классу. Его надо слегка видоизменить, поскольку операция в группе не умножение, а сложение. Теперь критерий выглядит так: два целых числа принадлежат одному и тому же смежному классу, если их разность кратна 3. Легко видеть, что это условие выполняется для любого из трех классов.

Таблица 2.5

Таблица сложения классов

в факторгруппе $\mathbf{Z} / 3\mathbf{Z}$

+	$3\mathbf{Z}$	$3\mathbf{Z}+1$	$3\mathbf{Z}+2$

Смежные классы образуют базовое множество факторгруппы, операцию в факторгруппе обозначим тем же символом «+», но *это совсем другая операция*, чем обычное сложение целых чисел в группе ($\mathbf{Z}$, +). Вычисление результатов «сложения» смежных классов делается с помощью представителей

этих классов. Найдем, например, сумму классов (3**Z**+1)+(3**Z**+2). Возьмем любого представителя в классе 3**Z**+1, скажем, –2, и любого представителя в классе 3**Z**+2, скажем, 5. Сумма этих двух чисел –2+5=3 принадлежит классу 3**Z**. Если взять в классах-слагаемых других представителей, конкретная сумма чисел может получиться другой, но в любом случае она будет принадлежать классу 3**Z**. Таким же способом заполняются все клетки таблицы 2.5.

Выберем в смежных классах простейших представителей: 0 в 3**Z**, 1 в 3**Z**+1, 2 в 3**Z**+2. Если рассматривать 0,1,2 не как числа, а как вычеты по модулю 3, то окажется, что факторгруппа (**Z**, +) / 3**Z** ≅ ($\mathbf{Z}_3$, $+_3$). Соответствие элементов изоморфных групп: 3**Z** ↔ 0, 3**Z**+1 ↔ 1, 3**Z**+2 ↔ 2.

Имеет место гомоморфизм группы (**Z**, +) и группы вычетов $\varphi : \mathbf{Z} \to \mathbf{Z}_3$, где $\varphi(x)$ – остаток от деления x на 3. Используя обозначения MatLab®, можно записать $\varphi(x) = \mathrm{mod}(x,3)$. Подгруппа-делитель является ядром этого гомоморфизма: 3**Z** = ker(φ).

Р 2.3.2. Построить факторгруппу аддитивной группы вещественных чисел (**R**, +) по подгруппе **Z**.

Решение. В этом примере множество смежных классов бесконечно и даже несчетно. Возьмем $x \in \mathbf{R}$, ему соответствует смежный класс $K_x = \mathbf{Z}+x$. Представим x в виде суммы целой и дробной части: $x=[x]+\{x\}$, имеем $K_x = K_{\{x\}}$ (слагаемое $[x]$ «утонет» в бесконечном **Z**). Критерий теперь выглядит так: два числа принадлежат одному и тому же смежному классу, если их разность *является целым числом*.

Сумма классов $K_{\{x\}}+K_{\{y\}}=K_{\{x\}+\{y\}}$, а точнее, $K_{\{\{x\}+\{y\}\}}$, поскольку сумма $\{x\}+\{y\}$ может оказаться больше 1. Вместо корявого обозначения $\{\{x\}+\{y\}\}$ можно использовать «сумму вещественных чисел по модулю 1» или, по аналогии с операцией в аддитивной группе вычетов, $\{x\} +_1 \{y\}$. Итак, сложение классов в факторгруппе (**R**, +) / **Z** опишем формулой $K_{\{x\}}+K_{\{y\}}= K_{\{x\}+_1\{y\}}$.

В качестве простейшего представителя любого смежного класса $K_{\{x\}}$ выберем $\{x\}$. Множество простейших представителей является группой ([0, 1[, $+_1$), которая изоморфна факторгруппе (**R**, +) / **Z**.

Этим группам изоморфна еще одна: мультипликативная группа комплексных чисел, модуль которых равен 1: (**U**, ·), где **U** = $\{z \in \mathbf{C}, |z| = 1\}$. Соответствие задается формулой $z = \cos(2\pi\cdot\alpha) + i\cdot\sin(2\pi\cdot\alpha)$, где $\alpha \in [0, 1[$ (другое обозначение полуоткрытого интервала – [0, 1)).

Гомоморфизм (**R**, +) на ([0,1[, $+_1$) задается формулой $\varphi(x) = \{x\}$ (дробная часть), ядро гомоморфизма – числа с нулевой дробной частью, т.е. целые.

Р 2.3.3. Построить факторгруппу мультипликативной группы ($\mathbf{C}^*$, ·) комплексных чисел, не равных нулю, по подгруппе положительных вещественных чисел $\mathbf{R}_+$.

Решение. Рассмотрим геометрическую модель. Множество $\mathbf{C}^*$ представляет комплексную плоскость с выколотым началом координат. Возьмем произвольную точку $z \in \mathbf{C}^*$. Соответствующий ей смежный класс $K_z = z \cdot \mathbf{R}_+$ геометрически представляет собой луч, выходящий из начала координат и проходящий через точку z (начало луча «отрезано»). Множество всех таких лучей – это и есть базовое множество факторгруппы.

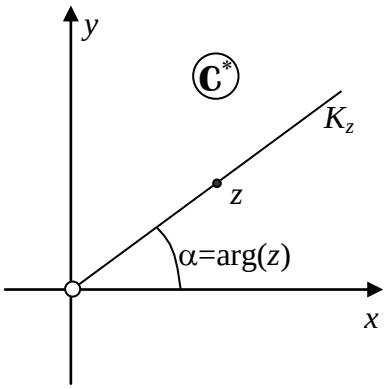

Рис. 2.2. Комплексная плоскость

По критерию два комплексных числа принадлежат одному классу (точки лежат на одном луче), если их отношение является вещественным положительным числом. При делении комплексных чисел их модули делятся, а аргументы вычитаются, при этом разность должна быть равна 0 – это и есть алгебраическая формулировка утверждения «точки лежат на одном луче».

Умножение классов-лучей делается по формуле $K_{z_1} \cdot K_{z_2} = K_{z_1 \cdot z_2}$. Комплексное число z «состоит» из модуля $|z|$ и аргумента $\arg(z)$, причем модуль

не влияет на построение смежного класса. Поэтому введем $\alpha=\arg(z)$ и будем обозначать класс не K_z, а K_α.

Тогда $K_{\alpha_1} \cdot K_{\alpha_2} = K_{\alpha_1+\alpha_2}$ (аргументы складываются «по модулю 2π«).

В качестве простейшего представителя любого смежнлго класса K_α выберем комплексное число с аргументом α и модулем 1. Множество простейших представителей является упоминавшейся ранее группой ($\mathbf{U}$, $\cdot$), которая изоморфна факторгруппе ($\mathbf{C}^*$, $\cdot$) / $\mathbf{R}_+$.

Гомоморфизм ($\mathbf{C}^*$, $\cdot$) на $\mathbf{U}$ задается формулой

$$\varphi(z) = \cos(\arg(z)) + i\cdot\sin(\arg(z)) = \frac{z}{|z|},$$

ядро гомоморфизма $\ker(\varphi)=\mathbf{R}_+$.

Р 2.3.4. Построить факторгруппу мультипликативной группы комплексных чисел, отличных от нуля ($\mathbf{C}^*$, $\cdot$), по подгруппе U_n корней n-й степени из единицы. Показать, что факторгруппа изоморфна мультипликативной группе комплексных чисел, отличных от нуля.

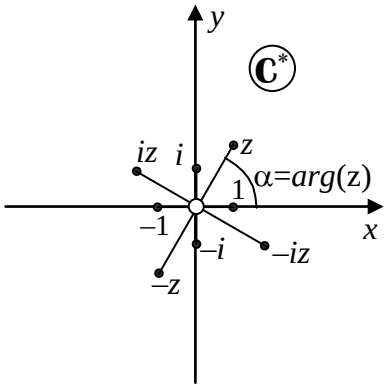

Рис. 2.3. Комплексная плоскость,

Решение. Пусть, для определенности, n=4. Рассмотрим геометрическую модель (рис. 2.3). Подгруппа U_4={1, i, –1, –i}, геометрически четыре конца креста на комплексной плоскости. Возьмем произвольную точку $z\in\mathbf{C}^*$. Соответствующий ей смежный класс $K_z = z \cdot U_4$ геометрически представляет собой также концы креста, повернутого на угол $\alpha=arg(z)$ и растянутого/сжатого с коэффициентом $|z|$ (на рисунке $\alpha\approx60°$, $|z|\approx2$). Чтобы $|z|$ и угол $\alpha=arg(z)$ однозначно характеризовали смежный класс K_z, примем соглашение: точка z лежит в *первой четверти*, иначе разным значениям z будет соответствовать концы одного и того же креста на комплексной плоскости.

Два комплексных числа принадлежат одному смежному классу, коль скоро их отношение принадлежит подгруппе. Это значит, что отношение их модулей равно 1 (т.е. их модули равны), а разность аргументов равна одному из четырех чисел 0, $\frac{\pi}{4}$, $\frac{2\pi}{4}=\frac{\pi}{2}$, $\frac{3\pi}{4}$ (в общем случае при произвольном n – одному из чисел $\frac{2k\pi}{n}$, k=0, 1, … , n–1).

Умножение смежных классов происходит по обычным правилам умножения комплексных чисел: модули перемножаются, аргументы складываются, но сложение происходит не по модулю 2π, как в группе $(\mathbf{C}^*, \cdot)$, а по модулю $\frac{\pi}{2}$, в общем случае при произвольном n – по модулю $\frac{2\pi}{n}$.

Таким образом, изоморфизм $(\mathbf{C}^*, \cdot) / U_n \cong (\mathbf{C}^*, \cdot)$ доказан.

Р 2.3.5. Построить факторгруппу аддитивной группы целочисленных матриц 2-го порядка $(\mathbf{Z}^{2\times2}, +)$ по подгруппе матриц с четными элементами $(2\mathbf{Z})^{2\times2}$.

Решение. Возьмем произвольную матрицу $m \in \mathbf{Z}^{2\times2}$. Соответствующий ей смежный класс $K_m = m + (2\mathbf{Z})^{2\times2}$ состоит из матриц, у которых на всех четырех местах стоят числа той же четности, что и в матрице m. Всего имеем $2^4 = 16$ смежных классов, простейшие представители которых суть матрицы $\begin{pmatrix}0&0\\0&0\end{pmatrix}$ (нейтральный элемент факторгруппы), $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $\begin{pmatrix}0&1\\0&0\end{pmatrix}$, … , $\begin{pmatrix}0&0\\1&1\end{pmatrix}$, … , $\begin{pmatrix}1&1\\1&1\end{pmatrix}$.

Две матрицы принадлежат одному смежному классу, если все элементы матрицы-разности четны. Складываются представители смежных классов поэлементно, как обычно складываются матрицы, причем сумма элементов берется по модулю 2. т.е. используется операция $+_2$.

Факторгруппа изоморфна группе матриц второго полядка, элементы которых суть вычеты по модулю 2: $(\mathbf{Z}^{2\times2}, +) / (2\mathbf{Z})^{2\times2} \cong (\mathbf{Z}_2)^{2\times2}$.

Замечание. Факторгруппа конечная, но не циклическая, все ее элементы (кроме нейтрального) имеют порядок 2.

Р 2.3.6. Построить факторгруппу полной линейной группы G = GL(F,n) по специальной линейной группе H = SL(F,n) (ее элементы – матрицы, определители которых равны 1).

Решение. Возьмем произвольную невырожденную матрицу $g \in G$. Соответствующий ей левый смежный класс $L_g = g \cdot H$ состоит из матриц, определители которых равны det(g). Покажем, что он включает все такие матрицы. Пусть для некоторой матрицы m определитель det(m) = det(g). Тогда $m \in L_g$, т.е. $\exists h \in H$ такой, что $m = g \cdot h$. Нужный элемент h однозначно вычисляется, это $h = g^{-1} \cdot m$. В самом деле, det(h) = det($g^{-1} \cdot m$) = det(g^{-1})·det(m). Но det(m) = det(g), поэтому det(g^{-1})·det(m) = 1, так что, в самом деле, $h \in H$. Итак, левый смежный класс включает все матрицы с фиксированным значением определителя.

Если построить правый смежный класс $R_g = H \cdot g$, он также будет включать все матрицы, определители которых равны det(g) (доказательство аналогично), т.е. левый класс равен правому. Факторизация возможна, описание смежных классов (элементов факторгруппы) дано выше. Любой смежный класс характеризуется не матрицей $g \in G$, а ее определителем d=det(g), поэтому его следует обозначать K_d.

Рассмотрим построение смежных классов с точки зрения критерия. Две матрицы m_1 и m_2 принадлежат одному классу, если $m_1^{-1} \cdot m_2 \in H$. Это означает, что $\det(m_1^{-1} \cdot m_2) = 1$ т.е. det(m_1)=det(m_2). Получили тот же результат: любой смежный класс состоит из матриц с одинаковым определителем.

Умножение классов соответствует умножению их индексов (значений определителей). (См. также замечание к задаче **Р 2.3.7** и задачу **С 2.3.7**).

Этот пример интересен тем, что здесь не срабатывает прием с «простейшими представителями». В самом деле, какую матрицу взять в качестве представителя класса, в котором все матрицы имеют фиксированное значение определителя, равное d? Можно, конечно, взять матрицу, полученную

из единичной заменой первой диагональной единицы числом d, множество таких матриц будет группой, однако это будет *нечисловая* группа (хотя и изоморфная числовой). Впрочем, здесь и без «простейших представителей» ясно, что факторгруппа изоморфна мультипликативной группе чисел того поля, над которым строились матрицы группы G.

Р 2.3.7. Построить факторгруппу полной линейной группы над полем вещественных чисел $G = \mathrm{GL}(\mathbf{R},n)$ по полной ортогональной группе $H = \mathrm{GO}(n)$.

Решение. Возьмем произвольную невырожденную матрицу $g \in G$. Из равенства смежных классов $g \cdot H = H \cdot g$, которое должно выполняться для нормального делителя H, не следует, вообще говоря, равенство произвольных элементов этих классов $g \cdot h$ и $h \cdot g$. Вместо этого должно выполняться более деликатное условие: $\forall g \ \forall h \ \exists h'$ такой, что $g \cdot h' = h \cdot g$, откуда $h' = g^{-1} \cdot h \cdot g$ (это условие было сформулировано на с. 38). Рецепт проверки нормальности делителя H таков: берем произвольный элемент $g \in G$ и произвольный элемент $h \in H$, находим $h' = g^{-1} \cdot h \cdot g$ и проверяем $h' \in H$?

Известно, что признаком ортогональности матрицы h является равенство $h^{-1} = h^{\mathrm{T}}$ или, что то же самое, $h^{\mathrm{T}} \cdot h = e$ (единичная матрица). У нас это условие должно выполняться для матрицы h', т.е.

$$(h')^{\mathrm{T}} \cdot h' = (g^{-1} \cdot h \cdot g)^{\mathrm{T}} \cdot (g^{-1} \cdot h \cdot g) = g^{\mathrm{T}} \cdot h^{\mathrm{T}} \cdot (g^{-1})^{\mathrm{T}} \cdot g^{-1} \cdot h \cdot g = e.$$

Неясно, почему такое громоздкое произведение должно равняться единичной матрице, скорее всего это не так и H *не является нормальным делителем*, факторизация невозможна.

Построим контрпример: $g = \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}, g^{-1} = \begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix}, h = \frac{1}{5} \cdot \begin{bmatrix} 3 & -4 \\ 4 & 3 \end{bmatrix}$. Возьмем произведение $h' = g^{-1} \cdot h \cdot g = \begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix} \cdot \frac{1}{5} \cdot \begin{bmatrix} 3 & -4 \\ 4 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix} = \cdots = \frac{1}{5} \cdot \begin{bmatrix} -25 & -40 \\ 20 & 31 \end{bmatrix} \notin H.$

Замечание. В задаче **Р 2.3.6** мы доказали нормальность подгруппы другим способом, без вычисления h' и проверки $h' \in H$. Попробуем сделать это сейчас. В той задаче подгруппа H состояла из матриц, определители которых равны 1. Возьмем h

$=g^{-1}\cdot h\cdot g$ и найдем $\det(h')=\det(g^{-1}\cdot h\cdot g)=\det(g^{-1})\cdot\det(h)\cdot\det(g)=1$, т.е. $h'\in H$. Делаем вывод: подгруппа H в задаче **Р 2.3.6** является нормальным делителем.

Р 2.3.8. Построить факторгруппу полной линейной группы $G = \mathrm{GL}(F,n)$ по группе скалярных матриц $H = \{\alpha\cdot E \mid \alpha\in F^*\}$ (F^* – мультипликатиная группа ненулевых элементов числового поля F).

Решение. Возьмем произвольную невырожденную матрицу $g\in G$. Соответствующий ей смежный класс (левый, он же и правый) $K_g = g\cdot H = H\cdot g$ состоит из матриц, получающихся из матрицы g умножением на всевозможные ненулевые числа: $K_g = \{m=\alpha\cdot g \mid \alpha\in F^*\}$.

По критерию две матрицы m_1 и m_2 принадлежат одному классу, если $m_1^{-1}\cdot m_2 \in H$. Это означает, что $\forall\alpha_1,\alpha_2\in F^*\ \exists\alpha\in F^*$: $(\alpha_1\cdot g_1)^{-1}\cdot(\alpha_2\cdot g_2)=\alpha\cdot E$, откуда после несложных преобразований получается $g_2=\beta\cdot g_1$ (для некоторого $\beta\in F^*$). Иными словами, матрицы g_1 и g_2, классам которых K_{g_1} и K_{g_2} принадлежат матрицы m_1 и m_2, могут отличаться лишь числовым множителем, т.е. эти классы совпадают.

Умножение классов происходит по очевидной формуле $K_{g_1}\cdot K_{g_2} = K_{g_1\cdot g_2}$.

Гомоморфизм $\varphi: G\to G/H$: $\varphi(g)=K_g$.

Попробуем “придумать” какую-нибудь группу, изоморфную факторгруппе G/H. В качестве простейшего представителя смежного класса K_g возьмем матрицу $\alpha\cdot g$, определитель которой равен 1 или –1. Вспомним формулу изменения определителя при умножении матрицы на число: $\det(\alpha\cdot g)=\alpha^n\cdot\det(g)$, где n – порядок матрицы g. Мы хотим, чтобы $\det(\alpha\cdot g)=\pm1$, т.е. $\alpha^n\cdot\det(g)=\pm1$, отсюда коэффициент $\alpha=\dfrac{1}{\sqrt[n]{\pm\det(g)}}$, простейший представитель смежного класса K_g – матрица $\dfrac{g}{\sqrt[n]{\pm\det(g)}}$. Если поле $F=\mathbf{C}$, этот результат неконкретен – в комплексной области $\sqrt[n]{\ }$ имеет n различных

значений, «±« под корнем торже не добавляет определенности. Непонятно, какую из этих $2n$ матриц взять в качестве простейшего представителя? Поэтому сузим числовое поле, над которым происходят все события, пусть $F=\mathbf{R}$.

Если порядок матриц группы GL($\mathbf{R}$,n) четный, то $\alpha^n>0$ при любом $\alpha\neq 0$, из формулы $\det(\alpha\cdot g)=\alpha^n\cdot\det(g)$ следует, что у всех матриц класса K_g знак определителя один и тот же, он совпадает со знаком определителя матрицы g. Таким образом, имеются классы «положительные» и «отрицательные». Естественно считать представителем “положительного” класса матрицу с определителем, равным 1, а “отрицательного” – матрицу с определителем, равным –1. Матрицы, определители которых равны ±1, это унимодулярные матрицы, мультипликативная группа таких матриц порядка n над полем вещественных чисел – это Uni($\mathbf{R}$,n).

Изоморфизм $\psi: G/H\to$Uni($\mathbf{R}$,n) определяется формулой $\psi(K_g)=\dfrac{g}{\sqrt[n]{|\det(g)|}}$.

При нечетном n ситуация меняется: любой класс K_g включает матрицы как с положительными, так и с отрицательными определителями. В этом случае “простейшим представителем” любого класса факторгруппы надо считать матрицу с определителем, равным 1, мультипликативная группа таких матриц порядка n над полем вещественных чисел – это специальная линейная группа SL($\mathbf{R}$,n).

Изоморфизм $\psi: G/H\to$ SL($\mathbf{R}$,n) определяется формулой $\psi(K_g)=\dfrac{g}{\sqrt[n]{\det(g)}}$.

Замечание. В формулах, определяющих изоморфизм, $\sqrt[n]{\ }$ в знаменателе следует понимать как *арифметическое значение* корня. Например, $\sqrt[4]{16}=2$, $\sqrt[3]{8}=2$, $\sqrt[3]{-8}=-2$.

Р 2.3.9. Изучить симметрическую группу S_3. Какие из ее подгрупп являются нормальными делителями?

Решение. Порядок этой группы $|S_3|=3!=6$. Перечислим ее подстановки.

$$e=\begin{pmatrix}1\,2\,3\\1\,2\,3\end{pmatrix},\ a=\begin{pmatrix}1\,2\,3\\2\,3\,1\end{pmatrix},\ b=\begin{pmatrix}1\,2\,3\\3\,1\,2\end{pmatrix},\ p=\begin{pmatrix}1\,2\,3\\2\,1\,3\end{pmatrix},\ q=\begin{pmatrix}1\,2\,3\\3\,2\,1\end{pmatrix},\ r=\begin{pmatrix}1\,2\,3\\1\,3\,2\end{pmatrix}.$$

Таблица 2.6

Симметрическая группа S_3

·	e	a	b	p	q	r
e	e	a	b	p	q	r

Для удобства дальнейших рассмотрений построим таблицу Кэли (таблица 2.6).

Имеются две несобственные подгруппы и четыре собственные (постарайтесь увидеть их в таблице):

$$T=\{e,a,b\},\ P=\{e,p\},\ Q=\{e,q\},\ R=\{e,r\}$$

Порядок $|T|=3$ равен половине порядка $|S_3|=6$, поэтому индекс подгруппы равен 2, она является нормальным делителем (см. ниже задачу **С 2.3.2**). В качестве самостоятельного упражнения постройте факторгруппу S_3 / T и связанные с ней гомоморфизм и изоморфизм (см. ниже задачу **С 2.3.5**).

Подгруппы P,Q,R, очевидно, изоморфны, поэтому рассмотрим только одну из них, $P=\{e,p\}$. Построим левые и правые смежные классы по этой подгруппе (произведения элементов S_3 берем из таблицы 2.6), смежные классы для e и для p совпадают с подгруппой P.

Видим, что соответствующие левые и правые смежные классы *не совпадают*, подгруппа не является нормальным делителем.

$$L_a=a\cdot\{e,p\}=\{a,q\},\quad R_a=\{e,p\}\cdot a=\{a,r\},$$

$$L_b=b\cdot\{e,p\}=\{b,r\},\quad R_b=\{e,p\}\cdot b=\{b,q\},$$

Зададимся, однако, вопросом, а так ли необходимо это совпадение? Построим две «односторонние факторгруппы», левую с элементами $\{e,p\}$, $\{a,q\}$ и $\{b,r\}$, правую с элементами $\{e,p\}$, $\{a,r\}$ и $\{b,q\}$. Вычислим в «левой факторгруппе» произведение $\{a,q\}\cdot\{b,r\}$ с помощью представителей этих классов. Возьмем $a\cdot b=e\in\{e,p\}$ – произведением классов должна быть сама подгруппа. Возьмем других представителей тех же классов: $q\cdot r=b\in\{b,r\}$ – получился совсем другой класс. Приходится признать, что красивая идея о «левой и правой

факторгруппах» потерпела неудачу: базовые множества мы построили, а операцию определить не смогли.

Кто-то из великих физиков сказал: «Нет ничего практичнее хорошей теории»…

Р 2.3.10. Доказать, что подгруппа функций вида $f(x) = x + b$ в группе всех невырожденных линейных функций $f(x) = ax + b$ (пример **G 9**) является нормальным делителем и построить факторгруппу.

Решение. Будем придерживаться «общегрупповых» обозначений. Пусть функция из объемлющей группы $g(x) = ax + b$, тогда обратный элемент группы $g^{-1}(x)=\frac{1}{a}\cdot x-\frac{b}{a}$ (см. выше **Р 1.6**). Возьмем функцию из подгруппы $h(x) = x + p$ (обозначение свободного члена надо сделать *самостоятельным*!) и найдем произведение $h' = g^{-1}hg$ (у нас произведение – это композиция).

Композиция $h\circ g=(ax+b)+p=ax+b+p$, затем $h'=g^{-1}\circ(h\circ g)=\frac{1}{a}\cdot(ax+b+p)-\frac{b}{a}=x+\frac{p}{a}$.

Получилась функция такого же вида (только свободный член другой). Вывод: h' принадлежит подгруппе функций вида $x+p$, эта подгруппа является нормальным делителем группы всех невырожденных линейных функций вида $ax+b$.

При факторизации смежный класс $gH=Hg$ состоит из функций вида $(ax+b)+p=ax+(b+p)$, где a и b – фиксированные, а p принимает любые значения. Видим, что у функций, входящих в смежный класс, коэффициент a один и тот же, а свободный член может быть любым за счет произвольного p. По критерию для $f_1(x)=a_1x+b_1$ и $f_2(x)=a_2x+b_2$, принадлежащих одному смежному классу, должно выполняться условие $a_1^{-1}\cdot a_2=1$, т.е. $a_1= a_2$, Смежный класс имеет смысл обозначить K_a, умножение в факторгруппе происходит по формуле

$K_a \cdot K_c = K_{a\cdot c}$ – факторгруппа изоморфна мультипликативной числовой группе. В качестве простейшего представителя класса K_a удобно взять функцию с нулевым свободным членом $f(x)=ax$.

Гомоморфизм очевиден: функция $ax+b$ отображается в число a, ядро гомоморфизма – функции, отображающиеся в число 1, т.е. имеющие вид $x+b$.

Р 2.3.11. Доказать, что ядро гомоморфизма является нормальным делителем.

Решение. Пусть имеем гомоморфизм $\varphi: G_1 \to G_2$, его ядро $H=\ker(\varphi) \subseteq G_1$. В задаче **Р 2.1.6** было доказано, что ядро является подгруппой. Будем считать обе группы мультипликативными, соответствующим образом обозначим бинарную операцию и унарную операцию перехода к симметричному элементу. Нейтральные элементы групп обозначим e_1 и e_2 соответственно. Коммутативность операции не предполагаем.

В основу доказательства положим требование, чтобы элемент $h'=g^{-1}hg$, где $g \in G_1$, $h \in H$, также принадлежал подгруппе H. Возьмем образ этого элемента

$$\varphi(h')=\varphi(g^{-1}hg) = \varphi(g^{-1})\cdot\varphi(h)\cdot\varphi(g) =$$

$$=\varphi(g^{-1})\cdot e_2\cdot\varphi(g)=\varphi(g^{-1})\cdot\varphi(g)=\varphi(g^{-1}\cdot g)=\varphi(e_1)=e_2,$$

т.е. $h' \in H=\ker(\varphi)$.

Таким образом, ядро гомоморфизма является нормальным делителем.

Р 2.3.12. Обосновать критерий принадлежности двух элементов x и y одному и тому же левому смежному классу по подгруппе H: $x^{-1}\cdot y=x\backslash y \in H$.

Решение. Пусть два элемента группы x и y принадлежат одному и тому же левому смежному классу $L_a=a\cdot H$. Это означает, что $\exists h_1 \in H$, для которого $x=a\cdot h_1$ и $\exists h_2 \in H$, для которого $y=a\cdot h_2$. Произведение $x^{-1}\cdot y={h_1}^{-1}\cdot a^{-1}\cdot a\cdot h_2={h_1}^{-1}\cdot h_2 \in H$.

Пусть, напротив, $x^{-1}\cdot y=h \in H$ и элемент x принадлежат некоторому левому смежному классу $L_a=a\cdot H$, т.е. $\exists h_1 \in H$, для которого $x=a\cdot h_1$. Надо показать, что элемент y принадлежит тому же смежному классу.

Произведение $x^{-1}\cdot y={h_1}^{-1}\cdot a^{-1}\cdot y=h$. Умножив это равенство слева на h_1, получим $a^{-1}\cdot y=h_1\cdot h$. Обозначив h_2 этот элемент подгруппы H, получим $a^{-1}\cdot y=h_2$. Умножим последнее равенство слева на a, получится $y=a\cdot h_2$, что и означает принадлежность элемента y тому же смежному классу $L_a=a\cdot H$.

Задачи для самостоятельного решения

С 2.3.1. Докажите, что смежные классы (как левые, так и правые) задают разбиение базового множества группы, т.е. пересечение любых двух различных классов пусто, а объединение всех классов равно базовому множеству.

С 2.3.2. Докажите, что подгруппа индекса 2 является нормальным делителем.

Указание. Существует всего один смежный класс, отличный от подгруппы.

С 2.3.3. Докажите, что в любой группе G несобственные подгруппы $\{e\}$ и G являются нормальными делителями, постройте соответствующие факторгруппы, гомоморфизмы и изоморфизмы.

С 2.3.4. Постройте факторгруппу циклической группы порядка 12 $G = \{a, a^2, a^3, a^4, \dots, a^{11}, a^{12}=e\}$ по подгруппе $H = \{a^3, a^6, a^9, a^{12}=e\}$.

С 2.3.5. Постройте факторгруппу симметрической группы S_3 по подгруппе T (см. выше **Р 2.3.9**).

С 2.3.6. Постройте факторгруппу мультипликативной группы комплексных чисел, не равных нулю $(\mathbf{C}^*, \cdot)$, по подгруппе комплексных чисел, модуль которых равен 1: $\mathbf{U} = \{z \in \mathbf{C}, |z|=1\}$.

С 2.3.7. В задаче **Р 2.3.6** была построена факторгруппа GL(F,n) / SL(F,n), где матрицы, входящие в группу SL(F,n)) имеют определитель, равный 1. Постройте факторгруппу GL(F,n) / Uni(F,n), где унимодулярные матрицы, входящие в группу Uni(F,n), имеют определитель, равный ± 1.

С 2.3.8. Постройте факторгруппу полной линейной группы GL($\mathbf{R}$,n) по подгруппе матриц с положительными определителями.

С 2.3.9. Рассмотрите полную линейную группу G = GL(F,n) и подгруппу треугольных матриц $H = Tri_n$. Является ли она нормальным делителем?

Указание. Можно ограничиться значением n=2.

С 2.3.10. Постройте факторгруппу аддитивной группы векторов вида (x,y) ($x,y \in \mathbf{Z}$) по подгруппе векторов вида (5x,6y).

Указание. Воспользуйтесь подходом задачи **Р 2.3.5.**

С 2.3.11. Постройте факторгруппу полной линейной группы G = GL($\mathbf{R}$,n) по подгруппе положительных скалярных матриц $H = \{\alpha \cdot E \mid \alpha \in \mathbf{R}_+\}$.

Указание. Воспользуйтесь задачей **Р 2.3.8.**

С 2.3.12. Пусть $G = (\mathbf{R}^2, +)$ – аддитивная группа вещественных двухкомпонентных векторов $H = \{(x_1, x_2) \mid x_1, x_2 \in \mathbf{R},\ x_1 + x_2 = 0\}$. Докажите, что H – нормальный делитель в G и постройте факторгруппу G / H.

С 2.3.13. Пусть G – множество невырожденных матриц вида $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$, где a, b, c – числа из некоторого поля, операция – умножение матриц. Докажите, что G является группой. Пусть H – множество матриц из G, у которых $a \cdot c = 1$. Докажите, что H – нормальный делитель в G и постройте факторгруппу G / H.

С 2.3.14. Докажите, что множество функций вида $f(x)=ax$ является подгруппой в группе всех невырожденных линейных функций (пример **G 9**). Является ли эта подгруппа нормальным делителем?

С 2.3.15. Обоснуйте критерий принадлежности двух элементов x и y одному и тому же правому смежному классу по подгруппе H: $x \cdot y^{-1} = x/y \in H$.

Указание. Воспользуйтесь задачей **Р 2.3.12.**

С 2.3.16. Докажите, используя критерии (см. выше задачи **Р 2.3.12** и **С 2.3.15**), что для отношения принадлежности двух элементов одному классу выполняются все свойства, присущие отношениям эквивалентности (*рефлексивность, симметрия, транзитивность*).

3. КОЛЬЦА И ПОЛЯ

3.1. Определения и примеры

Основы теории

Непустое множество M с заданными на нем двумя бинарными операциями *сложение* (+) и *умножение* (·), называется *кольцом* (ring), если

Ring1. Подсистема $(M, +)$ является коммутативной группой, она называется *аддитивной группой кольца*. Нейтральный элемент этой группы обозначается 0, элемент, симметричный x, обозначается $-x$.

В кольце можно ввести операцию *вычитание* (–), положив $x-y=x+(-y)$.

Ring2. Сложение и умножение связаны законами *дистрибутивности*:

левая $\forall x,y,z \quad x\cdot(y+z)=(x\cdot y)+(x\cdot z)$,

правая $\forall x,y,z \quad (y+z)\cdot x=(y\cdot x)+(z\cdot x)$.

Символически записывают $R=(M, +, \cdot)$, это общее обозначение не следует путать с общепринятым обозначением множества вещественных чисел **R**.

К мультипликативной подсистеме $(M, \cdot)$ в кольце предъявляются минимальные требования: умножение не обязательно коммутативно и ассоциативно, не обязательно имеется нейтральный элемент и симметричные элементы. Если умножение все же коммутативно, кольцо также называется коммутативным, если умножение ассоциативно, кольцо называется ассоциативным. (Впрочем, иногда ассоциативность умножения включают в число аксиом кольца – терминология в этой области несколько зыбка…)

Общие свойства колец (доказательства свойств в задаче **С 3.1.1**).

Мультипликативные свойства нуля: для всякого элемента кольца a выполняются равенства $a\cdot 0=0$ и $0\cdot a=0$.

«*Правило знаков*»: для всяких элементов кольца a и b выполняются равенства $a\cdot(-b)=-(a\cdot b)$, $(-a)\cdot b=-(a\cdot b)$, $(-a)\cdot(-b)=a\cdot b$.

Используя определение разности и правило знаков, можно доказать *дистрибутивность при вычитании*: $x\cdot(y-z)=(x\cdot y)-(x\cdot z)$, $(y-z)\cdot x=(y\cdot x)-(z\cdot x)$

Многие кольца обладают следующим замечательным свойством: система $(M\backslash\{0\}, \cdot)$ является *коммутативной группой* (нуль необходимо исключить ввиду его мультипликативных свойств – см. выше). Такое кольцо называется *полем* (field), группа $(M\backslash\{0\}, \cdot)$ называется *мультипликативной группой* этого поля (система $(M, +)$, напомним, называется его аддитивной группой). Произвольное поле будем обозначать F.

Примеры колец (обозначения традиционных операций опущены).

R 1. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ – числовые кольца с обычными операциями сложения и умножения. Числовые кольца коммутативны и ассоциативны. Кольца $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ являются полями.

R 2. $n\mathbf{Z}$ – кольцо целых чисел, кратных натуральному числу n.

R 3. $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$, $\mathbf{C}[x]$ – кольца многочленов. с обычными операциями сложения и умножения. Кольца многочленов коммутативны и ассоциативны.

R 4. $\mathbf{Z}^{n\times n}$, $\mathbf{Q}^{n\times n}$, $\mathbf{R}^{n\times n}$, $\mathbf{C}^{n\times n}$ – кольца квадратных матриц порядка n (не только невырожденных) с обычными матричными операциями. Матричные кольца ассоциативны, но не коммутативны.

Вообще, если имеется некоторое кольцо R, можно построить кольцо многочленов $R[x]$ и кольцо квадратных матриц $R^{n\times n}$. Эти два механизма могут комбинироваться. Так $R^{n\times n}[x]$ – кольцо многочленов с матричными коэффициентами. Пример такого многочлена $f(x)=\begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}x^2+\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}x+\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$. Другой вариант – $(R[x])^{n\times n}$ – кольцо матриц, элементы которых суть многочлены, например $g(x)=\begin{bmatrix}2x^2+x+1 & x^2+x\\ x^2+x & x^2+1\end{bmatrix}$.

Если представить матрицу $g(x)$ как сумму трех матриц, элементы которых содержат x в некоторой (одной и той же) степени, то окажется, что $f(x)=g(x)$.

R 5. $\mathrm{Tri}(R,n)$ – кольцо треугольных матриц порядка n (не только невырожденных) над произвольным числовым кольцом K с обычными матричными операциями. Это кольцо также ассоциативно и некоммутативно.

R 6. ($\mathbf{Z}_n$, $+_n$, $\cdot_n$) – кольцо вычетов по модулю n. Кольцо вычетов коммутативно и ассоциативно.

R 7. ($\mathbf{V}$, $+$, $\times$) – кольцо геометрических векторов с операциями сложения и векторного умножения. Это кольцо не ассоциативно и не коммутативно.

R 8. Кольцо подмножеств. Возьмем произвольный универс U и его булеан (множество всех подмножеств) $B=2^U$. В качестве сложения возьмем симметрическую разность множеств Δ, в качестве произведения – пересечение $\cap$. Алгебраическая система (2^U, Δ, $\cap$) является кольцом, притом ассоциативным и коммутативным. Роль нуля в этом кольце играет пустое множество $\varnothing$, имеется единица (нейтральный элемент по умножению), это универс U.

R 9. ($\mathbf{Z}$, $\oplus$, $\otimes$) – кольцо целых чисел с нестандартными операциями: $x \oplus y = x+y-1$ в качестве сложения и $x \otimes y = x+y-x \cdot y$ в качестве умножения. Также кольцами являются алгебраические системы ($\mathbf{Q}$, $\oplus$, $\otimes$), ($\mathbf{R}$, $\oplus$, $\otimes$), ($\mathbf{C}$, $\oplus$, $\otimes$). Все эти кольца ассоциативны и коммутативны. В последних трех кольцах мультипликативные подсистемы ($\mathbf{Q}\backslash\{1\}$, $\otimes$), ($\mathbf{R}\backslash\{1\}$, $\otimes$), ($\mathbf{C}\backslash\{1\}$, $\otimes$) являются коммутативными группами (см. пример **G 14** в разделе 2 «Группы»), так что сами эти кольца являются числовыми полями с нестандартными операциями.

R 10. F^n – кольцо арифметических векторов с покомпонентными операциями. Например $\begin{bmatrix} 2 \\ -1 \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$, $\begin{bmatrix} 2 \\ -1 \end{bmatrix} \cdot \begin{bmatrix} -1 \\ 0 \end{bmatrix} = \begin{bmatrix} -2 \\ 0 \end{bmatrix}$.

Контрпример. Алгебраическая система (L, $+$, $\circ$), где L – множество линейных функций вида $f(x)=ax+b$ с произвольными числовыми коэффициентами a и b, сложение выполняется путем приведения подобных членов, а операция ($\circ$) есть композиция. Эта система обсуждалась в задаче **P 1.6**, там было выяснено, что *левой дистрибутивности* в этой системе нет, в задаче **C 1.8** доказывается, что *правая дистрибутивность* имеет место. Таким образом, система (L, $+$, $\circ$) *не является* кольцом. По той же причине не является кольцом и более широкая

система, элементами которой являются многочлены любой, а не только первой степени, а в роли умножения выступает композиция.

Если к базовому множеству кольца добавить один или несколько элементов, которых в нем не было, то для сохранения свойств кольца понадобится добавить к нему и другие элементы, получающиеся путем сложения и умножения. Такой процесс называется *замыканием* (чтобы расширенное базовое множество было замкнутым). Полученное кольцо называется *расширением* старого.

Опишем более подробно этот способ порождения новых колец. Пусть имеется некоторое поле F (например, числовое), построим векторное пространство V над этим полем. Векторами пространства будут линейные комбинации базисных векторов $e_1, e_2, \ldots, e_n$, т.е. суммы вида $x_1 \cdot e_1 + x_2 \cdot e_2 + \ldots + x_n \cdot e_n$, причем по определению считаем, что $x_i \cdot e_i = e_i \cdot x_i$, это просто два варианта записи. Базисные векторы имеют произвольную природу, это могут быть геометрические отрезки, многочлены, матрицы, абстрактные символы – все, что угодно. Количество n базисных векторов называется *размерностью* пространства V.

Определим на множестве базисных векторов операцию умножения. Произведение $e_i \cdot e_j$ является элементом пространства V и раскладывается по базису $e_1, e_2, \ldots, e_n$, т.е. $e_i \cdot e_j = \sum_{k=1}^{n} \varepsilon_{ij}^k \cdot e_k$. Конкретно операция умножения определяется набором коэффициентов ε_{ij}^k, количество которых равно n^3. К операции умножения в общем случае не предъявляется никаких требований, т.е. она может быть некоммутативной, может быть неассоциативной и т.д.

Естественным образом (по дистрибутивности) распространим умножение на все векторы пространства V, например

$$(x_1 \cdot e_1 + x_2 \cdot e_2) \cdot (y_1 \cdot e_1 + y_2 \cdot e_2) = x_1 \cdot e_1 \cdot y_1 \cdot e_1 + x_1 \cdot e_1 \cdot y_2 \cdot e_2 + x_2 \cdot e_2 \cdot y_1 \cdot e_1 + x_2 \cdot e_2 \cdot y_2 \cdot e_2 =$$

$$= x_1 \cdot y_1 \cdot e_1 \cdot e_1 + x_1 \cdot y_2 \cdot e_1 \cdot e_2 + x_2 \cdot y_1 \cdot e_2 \cdot e_1 + x_2 \cdot y_2 \cdot e_2 \cdot e_2.$$

Далее произведения базисных векторов $e_1 \cdot e_1$, $e_1 \cdot e_2$ и т.д. надо заменить их значениями в соответствии с таблицей умножения.

Такая алгебраическая система называется *алгеброй над полем* и обозначается $F[e_1, e_2,\ldots,e_n]$. Пространство V называется *аддитивным пространством* алгебры, размерность пространства называется размерностью алгебры. Алгебра над полем *является кольцом* (а иногда и полем).

Термин «алгебра» в этом контексте нельзя признать удачным – слово «алгебра» и так перегружено смыслами и значениями, но с традицией не поспоришь.

Алгебра может строиться не только над полем, но и над коммутативным и ассоциативным кольцом с единицей, например, над кольцом целых чисел. В этом случае вместо термина «пространство» используется термин «*модуль*». Алгебра над кольцом также является кольцом.

Многие ранее рассмотренные примеры на самом деле строятся по этой схеме.

Так, кольцо геометрических векторов с операциями сложения и векторного умножения ($\mathbf{V}$, +, ×) (пример **R 7**) можно представить как трехмерную алгебру над полем вещественных чисел $\mathbf{R}[\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3]$, где $\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$ – орты прямоугольных осей координат, умножение ортов задается известными формулами ($\boldsymbol{e}_1\times\boldsymbol{e}_2=\boldsymbol{e}_3$ и т.д.).

Поле комплексных чисел можно представить как двумерную алгебру над полем вещественных чисел, один базисный вектор – число $1\in\mathbf{R}$, другой – мнимая единица i, умножение этих «векторов» делается по известным правилам. Символически можно записать $\mathbf{C}=\mathbf{R}[1, i]$. Впрочем, базисные векторы, являющиеся элементами «материнского» поля, как здесь 1, в квадратных скобках обычно не указываются, т.е. пишут $\mathbf{C}=\mathbf{R}[i]$.

Кольцо многочленов $R[x]$ над кольцом R строится по той же схеме: базисными векторами является $1\in R$ и «вектор» (фактически просто символ) x. Степени x^k получаются при повторном умножении x самого на себя, многочлены вида $\sum_k a_k \cdot x_k$ – путем линейной комбинации степеней.

Кольцо матриц $R^{n\times n}$ также можно построить как алгебру $R[E_{ij} \mid i,j=\overline{1,n}]$, где *матричные единицы* E_{ij} – матрицы, в каждой из которых все элементы, кроме одного, равны нулю, элемент в i-ой строке, j-ом столбце равен 1.

Следующие примеры колец являются алгебрами над тем или иным кольцом (полем).

R 11. $\mathbf{Z}[\frac{1}{10}]=\{a+(\frac{1}{10})^p\cdot b \mid a,b\in\mathbf{Z},\ p\in\mathbf{Z}_0\}$ – двухмерная алгебра конечных десятичных дробей над кольцом целых чисел (другое название *десятично-рациональные* числа). Это кольцо является основой всей школьной арифметики.

R 12. $\mathbf{Q}[\sqrt{2}]=\{a+\sqrt{2}\,b \mid a,b\in\mathbf{Q}\}$ – двухмерная алгебра над кольцом рациональных чисел. Вместо $\sqrt{2}$ можно взять любое другое иррациональное число или несколько таких чисел:

$\mathbf{Q}[\sqrt{2},\sqrt{3}]=\{a+\sqrt{2}\,b+\sqrt{3}\,c+\sqrt{6}\,d \mid a,b,c,d\in\mathbf{Q}\}$ – четырехмерная алгебра

($\sqrt{6}$ включен, чтобы обеспечить замкнутость по умножению),

$\mathbf{Q}[\sqrt[3]{2}]=\{a+\sqrt[3]{2}\,b+\sqrt[3]{4}\,c \mid a,b,c\in\mathbf{Q}\}$ – трехмерная алгебра, …

R 13. $\mathbf{Z}[i]=\{a+ib \mid a,b\in\mathbf{Z}\}$ – кольцо *целых комплексных* (*гауссовых*) *чисел*, двухмерная алгебра над кольцом целых чисел.

R 14. Следующие два кольца представляют собой своеобразные вариации на тему комплексных чисел, общий вид которых $z=x+i\cdot y$. Что если квадрат мнимой единицы i равен не –1, а чему-то другому? Обычно рассматриваются две двухмерные алгебры над полем вещественных чисел:

1) *Двойные* числа $\mathbf{R}[\omega]=\{x+\omega\cdot y \mid x,y\in\mathbf{R},\ \omega^2=1\}$.
2) *Дуальные* числа $\mathbf{R}[\sigma]=x+\sigma\cdot y \mid x,y\in\mathbf{R},\ \sigma^2=0\}$.

Пусть $R=(M,\ +,\ \cdot)$ – некоторое кольцо. Тогда кольцо $R'=(M',\ +,\ \cdot)$, где $M'\subseteq M$, называется *подкольцом* в K (subring), символически $R'\subseteq R$. Операции в подкольце те же самые, нейтральный элемент относительно сложения в кольце и в подкольце (т.е. 0) – один и тот же, способ построения симметричного элемента также одинаковый. У каждого кольца есть, по меньшей мере, два под-

кольца: оно само и подкольцо, базовое множество которого состоит из одного элемента 0. Эти подкольца называются *несобственными*, остальные (если они имеются) – *собственными*.

Если кольцо и его подкольцо являются полями, то говорят о *подполе*.

Примеры подколец и подполей

SR 1. Кольцо целых чисел $\mathbf{Z}$ является подкольцом в кольце (поле) рациональных чисел $\mathbf{Q}$, которое само является подполем в поле вещественных чисел $\mathbf{R}$, а последнее – подполем в поле комплексных чисел $\mathbf{C}$. Нейтральный элемент во всех этих кольцах – число 0, симметричный элемент относительно сложения для любого числа x – противоположное по знаку число $-x$. Символически: $\mathbf{Z}\subset\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$. Все подкольца (подполя) в этой цепочке – собственные.

Включения числовых колец (полей) индуцируют аналогичные включения порожденных ими колец многочленов и матричных колец.

SR 2. $n\mathbf{Z}$ – кольцо целых чисел, кратных натуральному числу n, является собственным (при $n>1$) подкольцом в кольце $\mathbf{Z}$.

SR 3. $\mathbf{Z}[\frac{1}{10}]\subset\mathbf{Q}$ – кольцо конечных десятичных дробей является собственным подкольцом в кольце рациональных чисел $\mathbf{Q}$ с любыми знаменателями.

SR 4. $\mathbf{Q}\subset\mathbf{Q}[\sqrt{2}]\subset\mathbf{Q}[\sqrt{2},\sqrt{3}]$, $\mathbf{Q}\subset\mathbf{Q}[\sqrt[3]{2}]$, …

SR 5. $\mathbf{Z}\subset\mathbf{Z}[i]$,

SR 6. Кольцо верхних треугольных матриц в кольце квадратных матриц $R^{n\times n}$.

Важным свойством колец является наличие или отсутствие *делителей нуля*. Делителями нуля называются элементы базового множества $x\neq0$ и $y\neq0$, произведение которых $x\cdot y=0$. Делители нуля есть во многих кольцах.

Так, $2\cdot3=6$, поэтому в кольце $(\mathbf{Z}_6, +_6, \cdot_6)$ вычеты 2 и 3 являются делителями нуля: $2\cdot_6 3=0$.

В кольце арифметических векторов с покомпонентными операциями делителями нуля являются ненулевые векторы, у которых есть нулевые компоненты: $\begin{bmatrix}0\\5\end{bmatrix}\cdot\begin{bmatrix}-2\\0\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix}$.

В кольце геометрических векторов с операциями сложения и векторного умножения *любой вектор* $\boldsymbol{a}$ является делителем нуля, поскольку $\boldsymbol{a}\times\boldsymbol{a}=\boldsymbol{0}$.

В кольце матриц с обычным умножением делителями нуля являются любые вырожденные матрицы (см. ниже задачу **C 3.1.4**)

Например, $\begin{bmatrix}2&4\\3&6\end{bmatrix}\cdot\begin{bmatrix}6&-4\\-3&2\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$.

В кольце матриц, где роль умножения играет коммутатор $[A,B]=A\cdot B-B\cdot A$ (см. задачу **P 1.7**), делителем нуля является любая матрица, так как $[A, A]=0$.

В кольце матриц, где роль умножения играет произведение Йордана $\{A,B\}=\frac{1}{2}(A\cdot B+B\cdot A)$ (см. задачу **P 1.8**), делителями нуля являются все вырожденные матрицы (почему?), а также матрицы, у которых равен нулю *след* (сумма диагональных элементов) (см. ниже задачу **P 3.1.6**).

Делители нуля имеются в кольце двойных чисел и в кольце дуальных чисел, определение этих чисел см. **R 14**, о делителях нуля – задачи **P 3.1.5** и **C 3.1.5**.

Если в кольце нет делителей нуля, а базовое множество конечно, мультипликативная подсистема кольца является квазигруппой (см. ниже задачу **P 3.1.11**), а если умножение ассоциативно, то группой. Поэтому *всякое конечное ассоциативное и коммутативное кольцо без делителей нуля является полем*. Условие конечности здесь существенно: бесконечное ассоциативное кольцо целых чисел $\boldsymbol{Z}$ не имеет делителей нуля, однако его мультипликативная подсистема не является группой, это коммутативная полугруппа с единицей.

Ассоциативное и коммутативное кольцо без делителей нуля называется *областью целостности* или *целостным кольцом*. Таковы все числовые кольца и кольца многочленов над произвольным числовым кольцом.

Очень важное свойство любого поля – в нем нет *делителей нуля*. Это означает, что если $x \cdot y = 0$, то, по крайней мере, один из элементов x и y равен 0. В самом деле, пусть, скажем $x \neq 0$, тогда существует x^{-1}. Умножив на него обе части равенства $x \cdot y = 0$, получим слева $x^{-1} \cdot x \cdot y = y$, а справа $x^{-1} \cdot 0 = 0$ (используем мультипликативное свойство нуля). Окончательно получили $y = 0$.

По-другому отсутствие делителей нуля можно описать так: множество ненулевых элементов замкнуто относительно умножения.

Примеры полей

F 1. $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

F 2. $\mathbf{Q} \subset \mathbf{Q}[\sqrt{2}\,] \subset \mathbf{Q}[\sqrt{2}, \sqrt{3}\,]$, $\mathbf{Q} \subset \mathbf{Q}[\sqrt[3]{2}\,]$, …

Доказательство того, что $\mathbf{Q}[\sqrt{2}\,]$ является полем, см. ниже в задаче **P 3.1.1.**

F 3. $(\mathbf{Z}_p, +_p, \cdot_p)$ – поле вычетов по простому модулю p.

Кроме полей $\mathbf{Z}_p$ имеются и другие конечные поля (см. раздел 3.3 «Факторизация колец»).

Обобщением полей $\mathbf{Q}[\sqrt{2}\,]$, $\mathbf{Q}[\sqrt{2}, \sqrt{3}\,]$, $\mathbf{Q}[\sqrt[3]{2}\,]$ и т.п. является поле *алгебраических чисел* $\mathbf{A}$, которое, кроме рациональных чисел, содержит *корни всех многочленов* из кольца $\mathbf{Z}[x]$, как вещественные, так и комплексные. Поэтому, например, корень многочлена x^2+1 (мнимая единица i) – тоже алгебраическое число. Поле алгебраических чисел весьма сложно, даже его замкнутость относительно арифметических операций является серьезной проблемой. Так, число $\sqrt{2}$ – корень многочлена x^2-2, $\sqrt{3}$ – корень многочлена x^2-3, их произведение $\sqrt{6}$ – корень многочлена x^2-6. А корнем какого многочлена с целыми коэффициентами является $\sqrt{2}+\sqrt{3}$? Многочлен наименьшей степени –

это $x^4 - 10x^2 + 1$, подставить в него $\sqrt{2}+\sqrt{3}$ нетрудно (см. ниже задачу **C 3.1.8**), но как до этого многочлена додуматься?

Поле алгебраических чисел замкнуто не только относительно арифметических операций, но и в следующем более сильном смысле (*алгебраическая замкнутость*): если построить многочлен, коэффициенты которого являются алгебраическими числами, то его корни будут не какими-то мифическими гипералгебраическими числами, а снова алгебраическими. Например, четыре корня любого многочлена (вроде $(\sqrt{2}+\sqrt{3})x^4 - \sqrt[3]{2}\,x^3 + i\,x^2$ и т.п.) – тоже алгебраические числа, т.е. существует какой-то *другой* многочлен, уже *с целыми коэффициентами*, корнями которого являются все эти четыре числа (а кроме них, скорее всего, и какие-то другие).

Аналогичная ситуация имеет место с полем комплексных чисел **C**, которое также алгебраически замкнуто: корнями многочлена с комплексными коэффициентами являются не какие-то гиперкомплексные числа, а снова комплексные. Это фундаментальное (и неочевидное) утверждение – *основная теорема алгебры многочленов*. А вот поля вещественных чисел **R** и рациональных чисел **Q** алгебраически незамкнуты: корни многочлена с вещественными коэффициентами не обязательно вещественные, корни многочлена с рациональными коэффициентами не обязательно рациональные.

Как видим, существует бесконечно много числовых полей, на их множестве определено отношение частичного порядка – включение. Минимальное числовое поле – рациональные числа. В самом деле, если в поле имеются нуль и единица, то имеется и сумма любого количества единиц, получаем множество натуральных чисел **N**. Вместе с симметричными по сложению (противоположными) получаются все целые

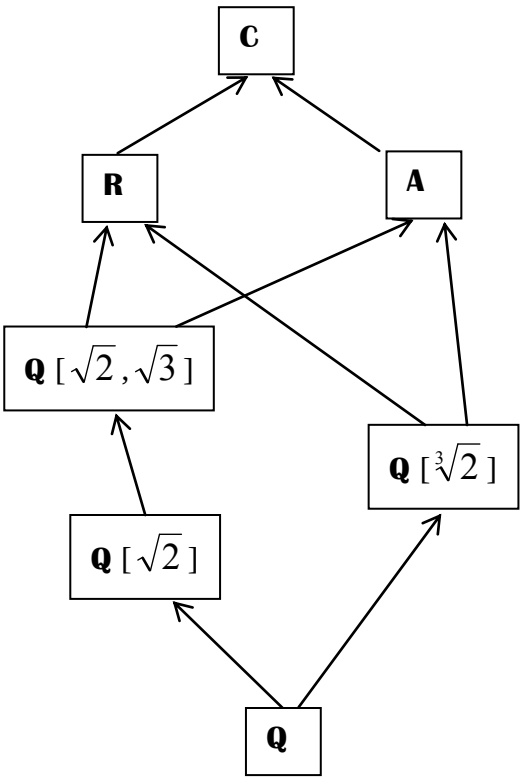

Рис. 3.1. Иерархия

числа **Z**. В поле возможно деление – получаются все рациональные числа **Q**. Это поле является подполем в любом числовом поле.

С другой стороны, поле комплексных чисел **C** максимальное, все числовые поля являются его подполями. Поле вещественных чисел **R** и поле алгебраических чисел **A** занимают промежуточное положение. Поля **Q**[$\sqrt{2}$], **Q**[$\sqrt{2}$, $\sqrt{3}$], **Q**[$\sqrt[3]{2}$] и т.п. лежат между **Q** и **A**, причем они включены еще и в **R**. Получающуюся сложную картину можно изобразить в виде ориентированного графа, вершины которого представляют различные числовые поля, а дуги – их включение (рис. 3.1).

Пусть $R_1=(M_1, +, \cdot)$ и $R_2=(M_2, +, \cdot)$ два кольца (поля) на разных множествах и с разными (вообще говоря) операциями, хотя и одинаково обозначенными. Кольца (поля) R_1 и R_2 *изоморфны*, если:

- существует биекция (взаимно однозначное отображение) $\varphi : M_1 \to M_2$;
- для любых $x,y \in M_1$ имеем $\varphi(x + y) = \varphi(x) + \varphi(y)$ и $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

(словесная формулировка: «биекция, сохраняющая обе операции»).

Символически изоморфизм колец (полей) записывается так: $R_1 \cong R_2$. Интересный пример изоморфных колец: кольцо многочленов с матричными коэффициентами $R^{n\times n}[x]$ и кольцо матриц, элементы которых суть многочлены $(R[x])^{n\times n}$ (см. выше пример **R 4**).

Для многих числовых колец и полей существуют изоморфные им матричные кольца и поля (см. 3.2. «Матричные представления колец и полей»).

Изоморфизм кольца (поля) на себя называется *автоморфизмом*. Здесь ограничимся одним примером нетривиального автоморфизма поля комплексных чисел: $\varphi(z) = \bar{z}$ (комплексно сопряженное число). Сохранение операций при комплексном сопряжении – хорошо известный факт. Замечательно, что поля вещественных и рациональных чисел *не имеют нетривиальных автоморфизмов* (лемма Дарбу).

Поле вещественных чисел $\mathbf{R}$ (и все его подполя) *упорядочено*, т.е. для его элементов определено отношение «меньше» (<) и производные от него отношения «больше» (>), «меньше или равно» (≤), «больше или равно» (≥). Очень важно, что эти отношения *согласованы* с операциями поля.

Поле комплексных чисел $\mathbf{C}$ *не является* упорядоченным в этом смысле. Можно ввести на этом множестве лексикографический порядок: $z_1<z_2$, если $\mathrm{Re}(z_1)<\mathrm{Re}(z_2)$ или $\mathrm{Re}(z_1)=\mathrm{Re}(z_2)$ и $\mathrm{Im}(z_1)<\mathrm{Im}(z_2)$. Однако это будет упорядочение только *множества* комплексных чисел, но не поля $\mathbf{C}$. В задаче **Р 3.1.4** приводятся аксиомы упорядоченного числового поля и доказывается невозможность упорядочения поля комплексных чисел.

Кольцо целых чисел $\mathbf{Z}$ и кольцо многочленов над произвольным числовым полем $F[x]$ во многом аналогичны (хотя, конечно, не изоморфны). Оба кольца – целостные, в обоих кольцах можно определить деление с остатком, имеет смысл понятие общего делителя. Над кольцом $\mathbf{Z}$ надстраивается (с помощью операции деления) поле рациональных чисел $\mathbf{Q}$. Его элементы – числовые дроби вида $\frac{a}{b}$, где $a,b\in\mathbf{Z}$ ($b\neq0$). При этом дроби $\frac{a}{b}$ и $\frac{a\cdot c}{b\cdot c}$, где $c\in\mathbf{Z}$ ($c\neq0$) считаются равными (представляют одно и то же рациональное число). За счет этого в множестве дробей можно определить сложение путем приведения к общему знаменателю.

Точно так же над кольцом $F[x]$ надстраивается *поле рациональных дробей* вида $\frac{a(x)}{b(x)}$, где многочлены $a(x),b(x)\in F[x]$ ($b(x)\neq0$). Точно так же дроби $\frac{a(x)}{b(x)}$ и $\frac{a(x)\cdot c(x)}{b(x)\cdot c(x)}$, где $c(x)\in F[x]$ ($c(x)\neq0$) считаются равными, в множестве рациональных дробей можно определить сложение путем приведения к общему знаменателю.

Коммутативность мультипликативной группы поля независима от остальных аксиом, т.е. от нее можно отказаться. В результате получается другой тип алгебраических систем, который в математической литературе на

русском языке называется *тело*. В англоязычной литературе используется термин skew-field (*косое поле*). Поле является частным случаем тела (коммутативное тело), однако в реальной математической практике положение дел скорее обратное: поля – важный класс алгебраических систем, имеется масса конкретных примеров полей, поля широко изучаются и применяются. Напротив, тела – довольно экзотические системы, находящиеся где-то на периферии алгебры.

Таблица 3.1

Умножение в теле кватернионов

·	1	*i*	*j*	*k*

Мы ограничимся одним примером – телом *кватернионов* (quaternion). Кватернионы представляют собой кольцо выражений вида $q=x+y\cdot i+z\cdot j+u\cdot k$, где $x,y,z,u\in\mathbf{R}$, а i,j,k – *кватернионные единицы*. Сложение в теле кватернионов происходит путем приведения подобных членов, умножение задается таблицей 3.1, при перемножении произвольных элементов тела используется дистрибутивность.

Можно сказать, что кватернионы – это комплексные числа с тремя разными мнимыми единицами, которые при умножении друг на друга ведут себя как орты прямоугольной системы координат при векторном умножении. Кольцо кватернионов является четырехмерной алгеброй над полем вещественных чисел. Формулы для умножения произвольных кватернионов будут выведены при решении задачи **Р 3.1.7**.

Ассоциативность умножения кватернионов является трудным вопросом, мы ее докажем позже. Не сразу ясно и существование симметричных по умножению кватернионов, хотя для кватернионных единиц оно очевидно: $i^{-1}=-i$, $j^{-1}=-j$, $k^{-1}=-k$. С нахождением q^{-1} для произвольного ненулевого кватернионов можно справиться так же, как в случае комплексных чисел. Для кватерниона $q=x+y\cdot i+z\cdot j+u\cdot k$ введем *сопряженный* кватернион $\overline{q}=x-y\cdot i-z\cdot j-u\cdot k$. Сопряженные кватернионы обладают свойствами, аналогичными свойствам сопряженных комплексных чисел:

$\overline{p+q}=\overline{p}+\overline{q}$, $\overline{p\cdot q}=\overline{q}\cdot\overline{p}$ (именно так!), $q+\overline{q}=2x$ – вещественное число,

$q\cdot\bar{q}=\bar{q}\cdot q=x^2+y^2+z^2+u^2$ – вещественное неотрицательное число, *норма* кватерниона, ее обозначают $N(q)$.

Свойства нормы: $N(q)=0$ только при $q=0$, $N(q_1\cdot q_2)=N(q_1)\cdot N(q_2)$ (**С 3.1.10**).

Чтобы найти q^{-1}, умножим равенство $q\cdot q^{-1}=1$ слева на сопряженный кватернион $\bar{q}$ и получим $N(q)\cdot q^{-1}=\bar{q}$, откуда $q^{-1}=\frac{1}{N(q)}\cdot\bar{q}$. Решение уравнения $a\cdot x=b$ можно записать в виде $x=a^{-1}\cdot b$, символически $x=a\backslash b$ (левое деление), решение уравнения $y\cdot a=b$ – в виде $y=b\cdot a^{-1}$, символически $x=b/a$ (правое деление).

Отсутствие коммутативности умножения приводит ко многим неожиданным и неприятным последствиям. Так, многочлен степени n в теле кватернионов не обязательно имеет n корней! Например, для многочлена x^2+1 можно сразу указать 6 корней: $\pm i$, $\pm j$, $\pm k$. На самом деле этот многочлен имеет *бесконечно много* (несчетное множество) корней! Их все можно описать простой формулой $x=b\cdot i+c\cdot j+d\cdot k$, где $b,c,d\in\mathbf{R}$, $b^2+c^2+d^2=1$ (см. ниже задачу **С 3.1.11**).

Совсем катастрофическая ситуация с линейной алгеброй: невырожденная матрица после транспонирования может стать вырожденной (см. ниже задачи **Р 3.1.9** и **С 3.1.12**), что делать с определителями – вообще непонятно!

Выражения вида $v=y\cdot i+z\cdot j+u\cdot k$ называются *чистыми* кватернионами, их можно поставить во взаимно однозначное соответствие с векторами трехмерного геометрического пространства, где i, j, k – орты декартовых осей координат. Тогда уравнение $y^2+z^2+u^2=1$ (см. выше) описывает единичную сферу.

Если взять два кватерниона-вектора $v_1=y_1\cdot i+z_1\cdot j+u_1\cdot k$, и $v_2=y_2\cdot i+z_2\cdot j+u_2\cdot k$ то вещественное число, равное $-\frac{1}{2}\cdot(v_1\cdot v_2+v_2\cdot v_1)$, есть скалярное произведение векторов, а чистый кватернион $\frac{1}{2}\cdot(v_1\cdot v_2-v_2\cdot v_1)$ – их векторное произведение (см. ниже задачи **Р 3.1.8** и **С 3.1.13**).

Почти все кольца, встречавшиеся в примерах до сих пор, были ассоциативными, единственное исключение – кольцо геометрических векторов с операциями сложения и векторного умножения (пример **R 7**). А бывают ли другие неассоциативные кольца? Целое семейство таких колец можно построить следующим образом. Возьмем какую-нибудь квазигруппу с заведомо неассоциативным умножением. Пусть ее элементы, например, *p, q, r* (порядок квазигруппы может быть любым, но меньше трех просто не получится).

Возьмем некоторое кольцо (в частности, поле) *R* и построим над ним новое кольцо (алгебру *R*[*p,q,r*]) элементами которого являются выражения вида $a+b\cdot p+c\cdot q+d\cdot r$, где $a,b,c,d\in R$. Сложение в новом кольце происходит путем приведения подобных членов, умножение «базисных элементов» *p,q,r* задается таблицей квазигруппы, при перемножении произвольных элементов кольца используется дистрибутивность. Произведения типа $b\cdot p$ и $p\cdot b$, которые могут возникнуть при раскрытии скобок, считаются равными (это не «теорема», которую надо доказывать, а определение). Любое такое кольцо, построенное на основе квазигруппы, будет заведомо неассоциативным. Конкретный пример такого кольца см. ниже в задаче **Р 3.1.10**.

Решение задач

Р 3.1.1. Доказать, что $\mathbf{Q}[\sqrt{2}]$ (кольцо чисел вида $a+\sqrt{2}\,b$, где $a,b\in\mathbf{Q}$) является полем.

Решение. Центральным моментом является построение для произвольного ненулевого $x = a + b\cdot\sqrt{2}$ элемента x^{-1}.

Имеем $x^{-1}=\frac{1}{x}=\frac{1}{a+b\cdot\sqrt{2}}=\frac{a-b\cdot\sqrt{2}}{(a+b\cdot\sqrt{2})\cdot(a-b\cdot\sqrt{2})}=\frac{a-b\cdot\sqrt{2}}{a^2-b^2\cdot 2}$. Знаменатель последней дроби обращается в нуль при $a^2-b^2\cdot 2=0$, т.е. при $\frac{a^2}{b^2}=2$. Но тогда

$\frac{a}{b} = \sqrt{2}$, что невозможно при рациональных a, b. Таким образом, x^{-1} существует и принадлежит данному полю.

Р 3.1.2. Доказать, что поле $\mathbf{Q}[\sqrt{2}]$ не изоморфно аналогичному полю $\mathbf{Q}[\sqrt{3}]$.

Решение. Доказательство «от противного». Допустим, что существует изоморфизм φ: $\mathbf{Q}[\sqrt{3}] \to \mathbf{Q}[\sqrt{2}]$. Это изоморфизм полей, поэтому изоморфны их аддитивные и мультипликативные группы. Отсюда имеем $\varphi(0)=0$, $\varphi(1)=1$, из сохранения операции сложения следует, что $\varphi(n)=n$ для любого целого n, а из сохранения операций умножения и деления следует, что $\varphi(r)=r$ для любого рационального r. Возьмем $\varphi(\sqrt{3})$, мы предполагаем, что это элемент поля $\mathbf{Q}[\sqrt{2}]$, т.е. $\varphi(\sqrt{3})=a+b\cdot\sqrt{2}$, где $a,b \in \mathbf{Q}$, причем $b \neq 0$. При гомоморфизме (в частности – при изоморфизме) полей $\varphi(3)=\varphi(\sqrt{3})\cdot\varphi(\sqrt{3})=(a+b\cdot\sqrt{2})^2=a^2+2b^2+2ab\sqrt{2}$. Слева имеем $\varphi(3)=3$, справа иррациональное число – противоречие.

Р 3.1.3. Доказать, что кольцо вычетов по простому модулю $\mathbf{Z}_p$ является полем.

Решение. Фактически надо доказать, что для любого ненулевого вычета существует обратный. Возьмем произвольный вычет $a \neq 0$ и подбором найдем a^{-1}. Рассмотрим произведения a по модулю p на все элементы кольца $\mathbf{Z}_p$, т.е. на 0, на 1, на 2, … , на $(p-1)$. Получим последовательность $0, a, 2\cdot a, \ldots, (p-1)\cdot a$. Все эти вычеты различны. В самом деле, пусть $k\cdot a = l\cdot a$, где $(0 \le k < l \le p-1)$, тогда $l\cdot a - k\cdot a = 0$. По дистрибутивности отсюда следует $(l-k)\cdot a = 0$ (по модулю p), т.е. обычное произведение $(l-k)\cdot a$ делится на p. Для этого хотя бы в одном из разложений на простые сомножители чисел $l-k$ и a должно присутствовать простое число p, что невозможно – оба эти числа $< p$.

Все элементы последовательности вычетов $0, a, 2\cdot a, \ldots, (p-1)\cdot a$ различны, а их количество равно p, значит, в этой последовательности присутствуют все

вычеты, в том числе и 1, т.е. существует вычет b такой, что $b\cdot a=1$. Мы нашли обратный элемент к вычету a, т.е. $a^{-1}=b$.

Р 3.1.4. Доказать, что поле комплексных чисел **C** не является упорядоченным, как упорядочено поле вещественных чисел **R** и любое его подполе.

Решение. Допустим, что на **C** задано отношение порядка >, обладающее следующими свойствами (кванторы $\forall$ по всем переменным подразумеваются).

1. Неверно, что $x>x$.
2. $x>y$ и $y>z \Rightarrow x>z$.
3. $x\neq y \Rightarrow x>y\ y>x$.
4. $x>y \Rightarrow x+z>y+z$.
5. $x>y$ и $z>0 \Rightarrow x\cdot z>y\cdot z$.

Сделаем выводы из этих аксиом. Мнимая единица $i\neq 0 \Rightarrow i>0$ или $0>i$, пусть $i>0$. По свойству 5 имеем $i\cdot i>0\cdot i$, т.е. $-1>0$. Применим свойство 4 и получим $-1+1>0+1$, т.е. $0>1$. Это, конечно, странно (как и $-1>0$), но здесь еще нет *логического* противоречия – наше гипотетическое отношение порядка > на множестве **C** не обязано на подмножестве **R** совпадать с добрым старым «больше».

Снова применим к $-1>0$ свойство 5 и получим $(-1)\cdot(-1)>0\cdot(-1)$, т.е. $1>0$. Теперь применив свойство 2 к неравенствам $0>1$ и $1>0$, получим $0>0$ – противоречие со свойством 1.

Если взять вариант $0>i$, получится такой же результат. Вывод: свойства отношения порядка > противоречат арифметическим свойствам поля **C**.

Р 3.1.5. Найти делители нуля в кольце двойных чисел

R$[\omega]=\{x+\omega\cdot y \mid x,y\in$ **R**, $\omega^2=1\}$ (см. выше пример **R 14**).

Решение. Возьмем два таких числа $c=a+\omega\cdot b$, $u=x+\omega\cdot y$, перемножим их и приравняем к нулю их произведение:

$$c\cdot u=(a+\omega\cdot b)\cdot(x+\omega\cdot y)=a\cdot x+\omega\cdot(b\cdot x+a\cdot y)+\omega^2\cdot b\cdot y=(a\cdot x+b\cdot y)+\omega\cdot(b\cdot x+a\cdot y)=0.$$

Получили систему уравнений $\{a\cdot x+b\cdot y=0,\ b\cdot x+a\cdot y=0\}$, она имеет ненулевые решения при $a=\pm b$. Если взять $a=b$, то $y=-x$, если $a=-b$, то $y=x$.

Вывод: в этом кольце делителями нуля являются числа вида $a\cdot(1\pm\omega)$.

Р 3.1.6. Рассмотрим кольцо матриц 2-го порядка, где роль умножения играет произведение Йордана $\{A,B\}=\frac{1}{2}(A\cdot B+B\cdot A)$ (см. задачу **Р 1.8**). Доказать, что матрицы, у которых равен нулю *след* (сумма диагональных элементов), являются делителями нуля.

Решение. Возьмем такую матрицу $A=\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$ и найдем ее произведение Йордана на произвольную матрицу $B=\begin{bmatrix} x & y \\ z & u \end{bmatrix}$

Имеем $A\cdot B=\begin{bmatrix} ax+bz & ay+bu \\ cx-az & cy-au \end{bmatrix}$, $B\cdot A=\begin{bmatrix} xa+yc & xb-ya \\ za+uc & zb-ua \end{bmatrix}$.

Приравняем нулю сумму $A\cdot B+B\cdot A=\begin{bmatrix} 2ax+cy+bz & b(x+u) \\ c(x+u) & cy+bz-2au \end{bmatrix}$. Считая a, b, c известными, получим однородную систему из трех (почему?) линейных уравнений с четырьмя неизвестными x, y, z, u. Ясно, что она имеет ненулевое решение, т.е. для нашей матрицы A найдется такая матрица $B\neq 0$, что произведение Йордана $\{A,B\}=0$.

Конкретный пример. Пусть $a=1$, $b=c=0$, тогда $A=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, от системы останутся два уравнения $2ax=0$, $2au=0$, откуда $B=\begin{bmatrix} 0 & y \\ z & 0 \end{bmatrix}$ (y, z произвольны).

Произведение Йордана этих матриц $\{A,B\}=\frac{1}{2}(A\cdot B+B\cdot A)=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Р 3.1.7. Вывести формулы умножения кватернионов.

Решение. Возьмем кватернионы $q_1=x_1+y_1\cdot i+z_1\cdot j+u_1\cdot k$, $q_2=x_2+y_2\cdot i+z_2\cdot j+u_2\cdot k$ и найдем их произведение $q_1\cdot q_2=q=x+y\cdot i+z\cdot j+u\cdot k$. Раскроем скобки по дистрибутивности:

$x+y\cdot i+z\cdot j+u\cdot k=(x_1+y_1\cdot i+z_1\cdot j+u_1\cdot k)\cdot(x_2+y_2\cdot i+z_2\cdot j+u_2\cdot k)=$

$=(x_1\cdot x_2+x_1\cdot y_2\cdot i+x_1\cdot z_2\cdot j+x_1\cdot u_2\cdot k)+(y_1\cdot i\cdot x_2+y_1\cdot i\cdot y_2\cdot i+y_1\cdot i\cdot z_2\cdot j+y_1\cdot i\cdot u_2\cdot k)+$

$+(z_1\cdot j\cdot x_2+z_1\cdot j\cdot y_2\cdot i+z_1\cdot j\cdot z_2\cdot j+z_1\cdot j\cdot u_2\cdot k)+(u_1\cdot k\cdot x_2+u_1\cdot k\cdot y_2\cdot i+u_1\cdot k\cdot z_2\cdot j+u_1\cdot k\cdot u_2\cdot k)$.

Вещественные множители вынесем вперед, произведения кватернионных единиц заменим согласно таблице 3.1 и приведем подобные члены:

$x+y\cdot i+z\cdot j+u\cdot k=(x_1\cdot x_2-y_1\cdot y_2-z_1\cdot z_2-u_1\cdot u_2)+(x_1\cdot y_2+y_1\cdot x_2+z_1\cdot u_2-u_1\cdot z_2)\cdot i+$

$+(x_1\cdot z_2-y_1\cdot u_2+z_1\cdot x_2+u_1\cdot y_2)\cdot j+(x_1\cdot u_2+ y_1\cdot z_2-z_1\cdot y_2+u_1\cdot x_2)\cdot k.$

Окончательно получаем формулы умножения

$x=x_1\cdot x_2-y_1\cdot y_2-z_1\cdot z_2-u_1\cdot u_2,\quad y=x_1\cdot y_2+y_1\cdot x_2+z_1\cdot u_2-u_1\cdot z_2,$

$z=x_1\cdot z_2-y_1\cdot u_2+z_1\cdot x_2+u_1\cdot y_2,\quad u=x_1\cdot u_2+ y_1\cdot z_2-z_1\cdot y_2+u_1\cdot x_2.$

Р 3.1.8. Доказать, что для двух чистых кватернионов $v_1=y_1\cdot i+z_1\cdot j+u_1\cdot k$, и $v_2=y_2\cdot i+z_2\cdot j+u_2\cdot k$ выражение $\frac{1}{2}\cdot(v_1\cdot v_2-v_2\cdot v_1)$ является чистым кватернионом и представляет векторное произведение соответствующих им векторов.

Решение. Если v_1 и v_2 чистые кватернионы, то $x_1=x_2=0$. По формулам умножения кватернионов для произведения $v_1\cdot v_2= v_{12}$ имеем

$x_{12}= -y_1\cdot y_2-z_1\cdot z_2-u_1\cdot u_2,\ y_{12}=z_1\cdot u_2-u_1\cdot z_2,\ z_{12}= -y_1\cdot u_2+u_1\cdot y_2,\ u_{12}=y_1\cdot z_2-z_1\cdot u_2.$

Для произведения $v_2\cdot v_1= v_{21}$ (механически меняем индексы $1\leftrightarrow2$):

$x_{21}= -y_2\cdot y_1-z_2\cdot z_1-u_2\cdot u_1,\ y_{21}=z_2\cdot u_1-u_2\cdot z_1,\ z_{21}= -y_2\cdot u_1+u_2\cdot y_1,\ u_{21}=y_2\cdot z_1-z_2\cdot u_1.$

Полуразность произведений – чистый кватернион

$(z_1\cdot u_2-u_1\cdot z_2)\cdot i-(y_1\cdot u_2-u_1\cdot y_2)\cdot j+(y_1\cdot z_2-z_1\cdot y_2)\cdot k.$

Рассматривая $i,\ j,\ k$ как орты осей, найдем векторное произведение векторов $v_1=y_1\cdot i+z_1\cdot j+u_1\cdot k$ и $v_2=y_2\cdot i+z_2\cdot j+u_2\cdot k$ (например, с помощью символического определителя): $[v_1,\ v_2]=(z_1\cdot u_2-u_1\cdot z_2)\cdot i-(y_1\cdot u_2-u_1\cdot y_2)\cdot j+(y_1\cdot z_2-z_1\cdot y_2)\cdot k$ – тот же результат.

Р 3.1.9. Решить в теле кватернионов систему уравнений (коэффициенты слева от неизвестных): $\begin{cases} i\cdot x_1+j\cdot x_2=1,\\ k\cdot x_1-1\cdot x_2=i. \end{cases}$

Решение. Применим метод Гаусса в матричной форме, умножение строк на те или иные множители-кватернионы будем делать *слева*.

$$\left[\begin{array}{cc|c} i & j & 1\\ k & -1 & i \end{array}\right]\xrightarrow[i\cdot(1)]{}\left[\begin{array}{cc|c} -1 & k & i\\ k & -1 & i \end{array}\right]\xrightarrow[(2)-(1)]{}\left[\begin{array}{cc|c} -1 & k & i\\ 1+k & -1-k & 0 \end{array}\right]\xrightarrow[(1+k)^{-1}\cdot(2)]{}\left[\begin{array}{cc|c} -1 & k & i\\ 1 & -1 & 0 \end{array}\right]\xrightarrow[(1)+(2)]{}\left[\begin{array}{cc|c} 0 & k-1 & i\\ 1 & -1 & 0 \end{array}\right]\xrightarrow[(-1-k)\cdot(1)]{}\left[\begin{array}{cc|c} 0 & 2 & -j-i\\ 1 & -1 & 0 \end{array}\right].$$

Далее проще решать «в алгебраической форме»: $x_1 = x_2 = -\frac{1}{2}\cdot(i+j)$.

Самостоятельно подставьте найденное решение в данную систему.

Замечание. Аналогичная система с транспонированной матрицей *не имеет решений* (см. ниже задачу **С 3.1.13**).

Р 3.1.10. Попробуем построить некоммутативное тело, аналогичное телу кватернионов, но конечное. Используем механизм алгебры над конечным полем, т.е. элементами тела будут выражения вида $q = x + y\cdot i + z\cdot j + u\cdot k$, где $x, y, z, u \in \mathbf{Z}_p$, а i, j, k – кватернионные единицы.

1) Поправить таблицу умножения кватернионных единиц (таблица 3.1), учитывая свойства поля вычетов $\mathbf{Z}_p$.

Таблица 3.1'

Умножение кватернионных единиц над полем вычетов $\mathbf{Z}_3$

·	1	i	j	k

Решение. Если взять p=2, то –1=1, умножение получится коммутативным. Пусть p=3, тогда –1=2, из таблицы 3.1 получаем некоммутативную таблицу 3.1'.

2) Проверить обратимость умножения – для всякого ли элемента $q=x+y\cdot i+z\cdot j+u\cdot k$ существует такой q^{-1}, что $q\cdot q^{-1}=q^{-1}\cdot q=1$.

Решение. Когда коэффициенты x,y,z,u были вещественными числами, нам помогло использование сопряженного кватерниона $\overline{q} = x-y\cdot i-z\cdot j-u\cdot k$. В этом случае $q\cdot\overline{q}=\overline{q}\cdot q=x^2+y^2+z^2+u^2=N(q)$ – вещественное неотрицательное число, норма кватерниона, обратный кватернион $q^{-1}=\frac{1}{N(q)}\cdot\overline{q}$.

Теперь у нас $x,y,z,u \in \mathbf{Z}_p$ (конкретно мы взяли $\mathbf{Z}_3$) и вопрос сводится к такому: всегда ли в поле вычетов $x^2+y^2+z^2+u^2\neq 0 \pmod 3$? Ответ отрицательный: возьмем, например $x=y=z=1$, $u=0$, $x^2+y^2+z^2+u^2=1+1+1+0=0 \pmod 3$. Т.е. в построенном нами кольце обнаружились делители нуля: $(1+i+j)\cdot(1+2i+2j)=0$ (убедитесь в этом самостоятельно, раскрыв скобки в соответствии с таблицей 3.1' и свойствами поля $\mathbf{Z}_3$).

Замечание. Может быть, мы неудачно выбрали поле вычетов и при каком-нибудь другом p (5,7 или еще большем) все могло получиться? Увы, в теории чисел есть теорема Лагранжа: *любое простое число* p (и даже любое натуральное) можно представить как *сумму квадратов четырех целых чисел*, среди которых могут быть и нули, как в нашем примере. Эти числа, естественно, можно заменить вычетами по модулю p и получится ненулевой «кватернион» с нулевой нормой.

И даже совсем другая конструкция не привела бы к успеху, потому что есть теорема Веддерберна: *вся кое конечное тело коммутативно*, т.е. является полем.

Р 3.1.11. Пусть a,b,c,d принадлежат некоторому кольцу (в частности, полю) R, а p,q,r – элементы неассоциативной квазигруппы. Построить алгебру $R[1,p,q,r]$ т.е. новое кольцо, элементами которого являются выражения вида $a+b\cdot p+c\cdot q+d\cdot r$.

Таблица 3.2

Квазигруппа

·	p	q	r

1) Убедиться, что умножение, задаваемое таблицей 3.2, неассоциативно.

Решение. Достаточно привести один пример, за которым далеко ходить не надо: $(p\cdot p)\cdot p=r\cdot p=q$, $p\cdot(p\cdot p)=p\cdot r=p$.

2) Вывести формулы умножения элементов кольца $a+b\cdot p+c\cdot q+d\cdot r$.

Решение. Возьмем два таких элемента и перемножим их, используя дистрибутивность:

$(a_1+b_1\cdot p+c_1\cdot q+d_1\cdot r)\cdot(a_2+b_2\cdot p+c_2\cdot q+d_2\cdot r)=(a_1\cdot a_2+a_1\cdot b_2\cdot p+a_1\cdot c_2\cdot q+a_1\cdot d_2\cdot r)+$

$+(b_1\cdot p\cdot b_2\cdot p+b_1\cdot p\cdot c_2\cdot q+b_1\cdot p\cdot d_2\cdot r)+(c_1\cdot q\cdot b_2\cdot p+c_1\cdot q\cdot c_2\cdot q+c_1\cdot q\cdot d_2\cdot r)+(d_1\cdot r\cdot b_2\cdot p+d_1\cdot r\cdot c_2\cdot q+d_1\cdot r\cdot d_2\cdot r)$.

Заменим $b_1\cdot p\cdot b_2\cdot p$ на $b_1\cdot b_2\cdot p\cdot p$, а $p\cdot p$ на r (в соответствии с таблицей квазигруппы), аналогично преобразуем и остальные слагаемые формулы. После приведения подобных членов получим

$$a_1\cdot a_2+(a_1\cdot b_2+b_1\cdot a_2+b_1\cdot d_2+c_1\cdot b_2+d_1\cdot c_2)\cdot p+(a_1\cdot c_2+b_1\cdot c_2+c_1\cdot a_2+c_1\cdot d_2+d_1\cdot b_2)\cdot q+$$
$$+(a_1\cdot d_2+b_1\cdot b_2+c_1\cdot c_2+d_1\cdot a_2+d_1\cdot d_2)\cdot r.$$

Здесь коэффициенты $a_{1,2}$, $b_{1,2}$, $c_{1,2}$, $d_{1,2}$ могут быть, например, числами – целыми, рациональными, вещественными, даже комплексными. Тогда неассоциативное кольцо будет бесконечным.

Если коэффициенты принадлежат полю вычетов $\mathbf{Z}_p$ по простому модулю p (не путать с элементом квазигруппы!), то неассоциативное кольцо будет конечным. Количество элементов такого кольца равно p^4 (почему?), так что минимальное их количество (при p=2) будет 16.

В построенном нами неассоциативном кольце имеются делители нуля (см. ниже задачу **С 3.1.15**).

Р 3.1.12. Доказать, что если в кольце нет делителей нуля, а базовое множество конечно, мультипликативная подсистема кольца является квазигруппой.

Решение. В таблице умножения такого кольца возьмем строку, соответствующую некоторому элементу a. Допустим, что два элемента этой строки совпадают, они стоят в столбцах, соответствующих элементам t_1 и t_2, т.е. равны произведения $a{\cdot}t_1$ и $a{\cdot}t_2$. Возьмем разность этих произведений, она равна нулю: $a{\cdot}t_1{-}a{\cdot}t_2{=}0$. По дистрибутивности имеем $a{\cdot}(t_1{-}t_2){=}0$, получились делители нуля – противоречие. Значит, все элементы строки различны, поэтому в ней представлены все элементы базового множества. Также доказываются аналогичные свойства для столбцов. В этом кольце однозначно разрешимы уравнения $a{\cdot}x{=}b$ и $y{\cdot}a{=}b$ при любых a и b, т.е. это кольцо является квазигруппой.

Р 3.1.13. В аксиомах кольца не предъявляется почти никаких требований к умножению (кроме дистрибутивности). В частности, ничего не говорится о нейтральном элементе по умножению, который естественно назвать единицей. Построить пример кольца, в котором существуют *односторонние единицы*.

Решение. Рассмотрим матрицы вида $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, где a,b принадлежат некоторому кольцу с мультипликативной единицей (то, что это множество матриц является кольцом, докажите самостоятельно**)**.

Возьмем матрицу $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$. Произведение $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$. Таким образом, *все* матрицы вида $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$ являются в этом кольце *левыми единицами*. Правых единиц в этом кольце нет (см. ниже задачу **Р 3.1.14)**. В задаче **Р 1.9** доказано, что если существуют как левые, так и правые единицы, то они совпадают. Такая двухсторонняя единица единственна (см. задачу **С 1.15**).

Р 3.1.14. Доказать, что в кольце, о котором идет речь в задаче **Р 3.1.13**, нет правых единиц.

Решение. Допустим, что правая единица имеется, найдем ее. Пусть это матрица $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$. Тогда $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, т.е. $a\cdot x=a$, $a\cdot y=b$, откуда $x=1$, $y=b/a$. Но правая единица должна быть универсальной, т.е. *не должна зависеть* от a и b. Делаем вывод: правых единиц в этом кольце не существует.

Задачи для самостоятельного решения

С 3.1.1. Докажите мультипликативные свойства нуля в произвольном кольце, правило знаков и дистрибутивность при вычитании.

С 3.1.2. Докажите, что в кольце целых чисел $\mathbf{Z}$ любое подкольцо имеет вид $n\mathbf{Z}$, т.е. состоит из чисел, кратных некоторому натуральному n.

Указание. Воспользуйтесь тем, что аддитивная группа кольца $\mathbf{Z}$ – циклическая.

С 3.1.3. Докажите, что кольцо целых чисел $\mathbf{Z}$ не изоморфно его подкольцу $n\mathbf{Z}$ при $n\neq 1$.

Указание. Аддитивные группы этих колец изоморфны, причем биекция $\varphi:\mathbf{Z}\to n\mathbf{Z}$ определяется однозначно. Проблемы возникают с умножением …

С 3.1.4. Докажите, что вырожденные матрицы (и только они) являются делителями нуля в кольце матриц $F^{n\times n}$.

Указание. Вспомните, что такое *присоединенная* матрица и чему равно ее произведение на данную матрицу.

С 3.1.5. Найдите делители нуля в кольце дуальных чисел

$[\sigma]=x+\sigma\cdot y \mid x,y\in\mathbf{R}, \sigma^2=0\}$.

С 3.1.6. В поле $\mathbf{Q}[\sqrt{2},\sqrt{3}]=\{a+\sqrt{2}\,b+\sqrt{3}\,c+\sqrt{6}\,d \mid a,b,c,d\in\mathbf{Q}\}$ найдите x^{-1} для числа $x=\sqrt{2}+\sqrt{3}$.

С 3.1.7. В поле $\mathbf{Q}[\sqrt[3]{2}]=\{a+\sqrt[3]{2}\,b+\sqrt[3]{4}\,c \mid a,b,c\in\mathbf{Q}\}$ найдите x^{-1} для числа $x=1+\sqrt[3]{2}$.

С 3.1.8. Проверьте, что $\sqrt{2}+\sqrt{3}$ является корнем многочлена $x^4 - 10x^2 + 1$. Какие еще корни имеет этот многочлен?

С 3.1.9. Докажите свойства сопряженных кватернионов.

С 3.1.10. Докажите свойства нормы кватернионов.

С 3.1.11. Докажите, что при любых $b,c,d\in\mathbf{R}$, для которых $b^2+c^2+d^2=1$, чистый кватернион $x=b\cdot i+c\cdot j+d\cdot k$ является корнем многочлена x^2+1.

С 3.1.12. Докажите, что для двух чистых кватернионов $v_1=y_1\cdot i+z_1\cdot j+u_1\cdot k$, и $v_2=y_2\cdot i+z_2\cdot j+u_2\cdot k$ выражение $-\frac{1}{2}\cdot(v_1\cdot v_2+v_2\cdot v_1)$ является вещественным числом и представляет скалярное произведение соответствующих им векторов.

Указание. Используйте выражения для $v_1\cdot v_2$ и $v_2\cdot v_1$ из задачи **Р 3.1.8**.

С 3.1.13. Покажите, что система уравнений $\begin{cases} i\cdot x_1 + k\cdot x_2 = 1, \\ j\cdot x_1 - 1\cdot x_2 = i \end{cases}$ в теле кватернионов не имеет решений.

Указание. Повторите с необходимыми изменениями вычисления из задачи **Р 3.1.9** и получите систему, в которой одно из уравнений имеет вид $0\cdot x_1 + 0\cdot x_2 = q \neq 0$.

С 3.1.14. В задаче **С 1.13** было доказано, что сложение вещественных чисел дистрибутивно относительно операций min и max. Являются ли системы (**R**, min, +) и (**R**, max, +) кольцами?

Указание. Выясните, являются ли подсистемы ($\mathbf{R}$, min) и ($\mathbf{R}$, max) группами.

С 3.1.15. Неассоциативное кольцо, построенное в **Р 3.1.10**, обладает делителями нуля. Если коэффициенты суть числа, примером делителей нуля являются $(p+q+r)\cdot(1-p+q-r)$.

1) Проверьте с помощью таблицы умножения квазигруппы (таблица 3.2), что данное произведение действительно равно нулю.

2) Найдите по этому образцу делители нуля в случаях, когда коэффициенты являются вычетами по модулю 2 и по модулю 3.

С 3.1.16. Является ли полем кольцо конечных десятичных дробей $\mathbf{Z}[\frac{1}{10}]$ (пример **R 11**)?

С 3.1.17. Постройте матричное кольцо с множеством *правых единиц*.

Указание. Воспользуйтесь задачей **Р 3.1.13** и тем, что при умножении матриц $(A\cdot B)^{\mathrm{T}}=B^{\mathrm{T}}\cdot A^{\mathrm{T}}$.

3.2. Матричные представления колец и полей

Для многих колец и полей можно построить изоморфную систему, элементами которой являются матрицы определенного вида. Операции в этой системе – обычное сложение и умножение матриц. Такой подход позволяет взглянуть на те же кольца или поля с другой стороны. Этим способом автоматически обосновывается ассоциативность умножения, которая заранее может быть неочевидной, например, для кватернионов, умножение которых находится в опасном родстве с неассоциативным векторным умножением.

Решение задач

Р 3.2.1. Построить изоморфное отображение поля комплексных чисел **Cё** в кольцо матриц $\mathbf{R}^{2\times 2}$.

Решение. Пусть комплексному числу $z=x+i\cdot y$ соответствует некоторая матрица $\varphi(z)=Z\in\mathbf{R}^{2\times 2}$, ее элементы должны выражаться через x и y, сложение и умножение таких матриц должно соответствовать сложению и умножению комплексных чисел. Матрицу Z построим постепенно. Сначала положим, что ее первая строка состоит из чисел x и y, т.е. $Z=\begin{bmatrix} x & y \\ * & * \end{bmatrix}$, т.е. $Z_{11}=x=\mathrm{Re}(z)$, $Z_{12}=y=\mathrm{Im}(z)$. Заполнение второй строки пока не определено.

Возьмем два комплексных числа $z_1=x_1+i\cdot y_1$ и $z_2=x_2+i\cdot y_2$, им соответствуют матрицы $\varphi(z_1)=\mathrm{Z}^{(1)}=\begin{bmatrix} x_1 & y_1 \\ * & * \end{bmatrix}$ и $\varphi(z_2)=Z^{(2)}=\begin{bmatrix} x_2 & y_2 \\ * & * \end{bmatrix}$. Для произведения этих чисел $z=z_1\cdot z_2$ вещественная и мнимая часть $x=x_1\cdot x_2-y_1\cdot y_2$, $y=x_1\cdot y_2+y_1\cdot x_2$.

Начнем заполнять матрицу $Z=Z^{(1)}\cdot Z^{(2)}$. Ее элемент $Z_{11}=x=x_1\cdot x_2-y_1\cdot y_2$, откуда следует, что элемент $Z_{21}^{(2)}$ должен равняться $-y_2$. Элемент $Z_{12}=y=x_1\cdot y_2+y_1\cdot y_2$, откуда следует, что элемент $Z_{22}^{(2)}$ должен равняться x_2. Таким образом, у нас определился вид матрицы $Z^{(2)}=\begin{bmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{bmatrix}$, матрица $\mathrm{Z}^{(1)}$ должна быть устроена

аналогично, матрица, представляющая произвольное число $z\in\mathbf{C}$, имеет вид $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$.

Операция умножения при таком соответствии сохраняется – на этом и был построен изоморфизм. Сохранение операции сложения очевидно.

Замечание 1. $\det(Z)=x^2+y^2$, поэтому любая ненулевая матрица данного вида невырождена, для нее существует обратная матрица. Эти матрицы образуют поле, хотя *произвольные* матрицы поля не образуют (имеются делители нуля, умножение не коммутативно).

Замечание 2. Знак «минус» перед y в выражении элемента Z_{21} – не что иное, как $i^2=-1$. Это замечание поможет решить задачи **С 3.2.1-3**.

Замечание 3. Другой (по форме) способ матричного представления поля комплексных чисел – начать с двух матриц $E=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ и $I=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, убедиться в том, что $I^2=-E$. Затем рассмотреть алгебру $\mathbf{R}[E, I]$ (т.е. кольцо матриц вида $x\cdot E+y\cdot I$).

Р 3.2.2. Построить изоморфное отображение в кольцо матриц $\mathbf{Q}^{3\times3}$ поля $\mathbf{Q}[\sqrt[3]{2}]=\{a+\sqrt[3]{2}\,b+\sqrt[3]{4}\,c \mid a,b,c\in\mathbf{Q}\}$.

Решение. Выведем формулы умножения чисел этого поля. Пусть

$a+\sqrt[3]{2}\,b+\sqrt[3]{4}\,c=(a_1+\sqrt[3]{2}\,b_1+\sqrt[3]{4}\,c_1)\cdot(a_2+\sqrt[3]{2}\,b_2+\sqrt[3]{4}\,c_2)=$

$(a_1a_2+2b_1c_2+2c_1b_2)+(a_1b_2+b_1a_2+2c_1c_2)\sqrt[3]{2}+(a_1c_2+b_1b_2+c_1a_2)\sqrt[3]{4}$.

Приравнивая коэффициенты при соответствующих степенях $\sqrt[3]{2}$, получим

$$a=a_1a_2+2b_1c_2+2c_1b_2,\ b=a_1b_2+b_1a_2+2c_1c_2,\ c=a_1c_2+b_1b_2+c_1a_2.$$

Как при решении задачи **Р 3.2.1**, матричное представление будем строить постепенно. Пусть числам из этого поля соответствуют матрицы $T^{(1)}=\begin{bmatrix} a_1 & b_1 & c_1 \\ * & * & * \\ * & * & * \end{bmatrix}$

и $T^{(2)}=\begin{bmatrix} a_2 & b_2 & c_2 \\ * & * & * \\ * & * & * \end{bmatrix}$, их произведение $T=\begin{bmatrix} a & b & c \\ * & * & * \\ * & * & * \end{bmatrix}$ (пока определены только элементы первой строки). По формулам умножения чисел из данного поля

$$T=\begin{bmatrix} a_1a_2+2b_1c_2+2c_1b_2 & a_1b_2+b_1a_2+2c_1c_2 & a_1c_2+b_1b_2+c_1a_2 \\ * & * & * \\ * & * & * \end{bmatrix}.$$

Чтобы в первой строке получились такие выражения, матрица $T^{(2)}$ должна быть заполнена совершенно определенным образом, а именно $T^{(2)}=\begin{bmatrix} a_2 & b_2 & c_2 \\ 2c_2 & a_2 & b_2 \\ 2b_2 & 2c_2 & a_2 \end{bmatrix}$, матрица $T^{(1)}$ должна быть устроена аналогично, матрица представляющая произвольное число данного поля $a+\sqrt[3]{2}\,b+\sqrt[3]{4}\,c$, имеет вид $T=\begin{bmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{bmatrix}$.

Замечание 1. Чтобы кольцо матриц данного вида было полем, любая ненулевая матрица должна быть невырожденной, т.е. $\det(T)=a^2+2b^2+4c^2-6abc=0$ должно быть *только* при $a=b=c=0$. Проверить это *в общем виде* при любых рациональных (на самом деле достаточно при любых целых) a,b,c весьма трудно, по правде сказать, непонятно как. Цивилизованный способ заключается в исследовании многочленов $a+bx+cx^2$ и x^3-2. Над полем рациональных чисел $\mathbf{Q}$ многочлен x^3-2 неприводим, поэтому он взаимно прост с $a+bx+cx^2$ при любых a,b,c, т.е. НОД$(x^3-2,\ a+bx+cx^2)=1$. Следовательно, существуют многочлены (коэффициенты Безу) $u(x)$ и $v(x)$ такие, что $(x^3-2)\cdot u(x)+(a+bx+cx^2)\cdot v(x)=1$ ($u(x)$ и $v(x)$ ищутся с помощью алгоритма Евклида).

Если в это тождество подставить $x=\sqrt[3]{2}$, получится $(a+b\sqrt[3]{2}+c\sqrt[3]{4})\cdot v(\sqrt[3]{2})=1$, откуда $(a+b\sqrt[3]{2}+c\sqrt[3]{4})^{-1}=v(\sqrt[3]{2})$. Правда, построить многочлен $v(x)$ при *произвольных* (*буквенных*) a,b,c не легче, чем найти матрицу T^{-1} (тоже при произвольных a,b,c), однако при любых *конкретных численных* значениях коэффициентов задача вполне разрешима…

Замечание 2. Другой способ матричного представления числового поля $\mathbf{Q}[\sqrt[3]{2}]$ – взять матрицы

$E=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$, $S=\begin{bmatrix}0&1&0\\0&0&1\\2&0&0\end{bmatrix}$, $S^2=\begin{bmatrix}0&0&1\\2&0&0\\0&2&0\end{bmatrix}$, проверить, что $S^3=\begin{bmatrix}2&0&0\\0&2&0\\0&0&2\end{bmatrix}=2E$.

Затем рассмотреть алгебру $\mathbf{Q}[E, S]$ (т.е. кольцо матриц вида $a\cdot E+b\cdot S+c\cdot S^2$).

Р 3.2.3. Построить отображение тела кватернионов $q=x+i\cdot y+j\cdot z+k\cdot u$ в кольцо матриц $\mathbf{R}^{4\times4}$.

Решение. Двум кватернионам $q_1=x_1+i\cdot y_1+j\cdot z_1+k\cdot u_1$, $q_2=x_2+i\cdot y_2+j\cdot z_2+k\cdot u_2$, соответствуют матрицы $Q^{(1)}=\begin{bmatrix}x_1&y_1&z_1&u_1\\*&*&*&*\\*&*&*&*\\*&*&*&*\end{bmatrix}$ и $Q^{(2)}=\begin{bmatrix}x_2&y_2&z_2&u_2\\*&*&*&*\\*&*&*&*\\*&*&*&*\end{bmatrix}$, их произведение Q согласно формулам умножения кватернионов (см. ниже задачу **Р 3.1.7**)

$$Q=\begin{bmatrix}x_1x_2-y_1y_2-z_1z_2-u_1u_2 & x_1y_2+y_1x_2+z_1u_2-u_1z_2 & x_1z_2-y_1u_2+z_1x_2+z_1x_2+u_1y_2 & x_1u_2+y_1z_2-z_1y+u_1x_2\\ * & * & * & *\\ * & * & * & *\\ * & * & * & *\end{bmatrix}$$

Заполнение первой строки матрицы Q фактически задает столбцы матрицы $Q^{(2)}=\begin{bmatrix}x_2&y_2&z_2&u_2\\-y_2&x_2&-u_2&z_2\\-z_2&u_2&x_2&-y_2\\-u_2&-z_2&y_2&x_2\end{bmatrix}$, матрица $Q^{(1)}$ должна быть устроена аналогично, матрица, представляющая произвольный кватернион $q=x+i\cdot y+j\cdot z+k\cdot u$, имеет вид

$$Q=\begin{bmatrix}x&y&z&u\\-y&x&-u&z\\-z&u&x&-y\\-u&-z&y&x\end{bmatrix}.$$

Теперь проблема ассоциативности умножения кватернионов решена.

Замечание. Другой способ матричного представления тела кватернионов – взять матрицы $E=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$, $I=\begin{bmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&-1\\0&0&1&0\end{bmatrix}$, $J=\begin{bmatrix}0&0&1&0\\0&0&0&1\\-1&0&0&0\\0&-1&0&0\end{bmatrix}$, $K=\begin{bmatrix}0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0\end{bmatrix}$,

проверить, что при умножении они ведут себя как кватернионные единицы (таблица 3.1). Затем рассмотреть $\mathbf{R}[E, I, J, K]$ (т.е.кольцо матриц вида $x\cdot E+y\cdot I+z\cdot J+u\cdot K$).

Задачи для самостоятельного решения

Указание к задачам **С 3.2.1-3**. Воспользуйтесь подходом задачи **Р 3.2.1**.

С 3.2.1. Постройте изоморфное отображение в кольцо матриц $\mathbf{Q}^{2\times 2}$ поля $\mathbf{Q}[\sqrt{2}]=\{x+\sqrt{2}\,y \mid x,y\in\mathbf{Q}\}$.

С 3.2.2. Постройте изоморфное отображение в кольцо матриц $\mathbf{R}^{2\times 2}$ кольца двойных чисел $\mathbf{R}[\omega]=\{x+\omega\cdot y \mid x,y\in\mathbf{R},\ \omega^2=1\}$.

С 3.2.3. Постройте изоморфное отображение в кольцо матриц $\mathbf{R}^{2\times 2}$ кольца дуальных чисел $\mathbf{R}[\sigma]=\{x+\sigma\cdot y \mid x,y\in\mathbf{R},\ \sigma^2=0\}$.

С 3.2.4. Существует представление тела кватернионов матрицами из $\mathbf{C}^{2\times 2}$ вида $\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}$, $\alpha,\beta\in\mathbf{C}$. Сопоставьте умножение таких матриц с умножением кватернионов. Опишите отображение (изоморфизм): какая комплексная матрица соответствует кватерниону $q=x+i\cdot y+j\cdot z+k\cdot u$?

С 3.2.5. Какие из множеств матриц 2-го порядка являются кольцами относительно сложения и умножения матриц? Какие из них являются подкольцами других? Какие из них являются полями?

7) $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a,b\in\mathbf{R},\ a^2+b^2>0\right\}$;

8) $\left\{\begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \middle| a,b\in\mathbf{R},\ a^2+b^2>0\right\}$;

9) $\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a,b\in\mathbf{R},\ a^2+b^2>0\right\}$;

10) $\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a,b\in\mathbf{Q},\ a^2+b^2>0\right\}$.

3.3. Факторизация колец

Основы теории

Пусть задано кольцо R и его подкольцо I. При определенных условиях можно построить новое кольцо, которое называется *факторкольцом R по I* и обозначается R/I. Главной операцией в кольце является сложение и смежные классы, являющиеся элементами факторкольца, мы будем строить именно с помощью операции сложения. Поскольку сложение заведомо коммутативно, у нас не возникнет (как в некоммутативных группах) проблема корректности определения операции сложения классов. Однако, желая построить не просто аддитивную факторгруппу, но факторкольцо, где кроме сложения, есть умножение, мы должны побеспокоиться о мультипликативных свойствах подкольца I.

Конкретно речь идет о следующих свойствах. Подкольцо I называется

– *левым идеалом*, если $I \cdot R \subseteq I$ (т.е. $\forall i \in I,\ \forall a \in R\ \ i \cdot a \in I$),

– *правым идеалом*, если $R \cdot I \subseteq I$ (т.е. $\forall i \in I,\ \forall a \in R\ a \cdot i \in I$).

Если подкольцо удовлетворяет обоим условиям, оно называется *двусторонним идеалом* или просто *идеалом*.

Пример 1. В кольце $\mathbf{Z}$ подкольцо $n\mathbf{Z}$ ($n \in \mathbf{N}$) является идеалом.

Пример 2. В кольце многочленов $R[x]$ подкольцо $f(x) \cdot R[x]$ (где $f(x)$ – некоторый конкретный многочлен из $R[x]$) является идеалом.

Идеалы такого вида называются *главными идеалами*, их можно обозначать более просто: (n) вместо $n\mathbf{Z}$, $(f(x))$ вместо $f(x) \cdot R[x]$ и т.п.

Эта формулировка относится к коммутативным и ассоциативным кольцам с единицей (нейтральным элементом относительно операции умножения). Для произвольных колец также можно ввести (другим способом) понятие главного идеала.

Если кольцо R является телом (в частности, полем), его идеалами являются только несобственные подкольца, т.е. $\{0\}$ и R (см. задачу **Р 3.3.1**).

Факторкольцо строится на основе аддитивной группы кольца. Рассматривается ее факторгруппа, каждый смежный класс которой имеет вид

$K_a=a+I$ ($a\in R$). Сложение классов происходит с помощью их представителей (см. 2.3 ″Факторизация групп″, в частности, задачу **Р 2.3.1**), кратко его можно описать формулой $K_a+K_b=(a+I)+(b+I)=(a+b)+I$.

Умножение классов происходит также с помощью их представителей: $K_a\cdot K_b=(a+I)\cdot(b+I)=a\cdot b+I$. Корректность этого определения, т.е. независимость результата умножения классов от выбора представителей в этих классах, обосновывается ″идеальными″ свойствами подкольца I (см. ниже задачу **Р 3.3.2**).

Роль нуля в факторкольце играет класс $K_0=0+I=I$, т.е. сам идеал.

Как и факторизация групп, факторизация колец тесно связана с гомоморфизмом, т.е. отображением (не обязательно взаимно однозначным), сохраняющим обе операции. Пусть R – кольцо, I – идеал, $F=R/I$ – факторкольцо. Определим отображение φ: $R\to F$, задаваемое формулой $\varphi(x)=x+I$ (образ элемента x – класс факторкольца, которому принадлежит x). Это отображение является гомоморфизмом (см. ниже задачу **С 3.3.1**), идеал I является ядром этого гомоморфизма: $\ker(\varphi)=I$ (см. ниже задачу **С 3.3.2**).

Если факторкольцо F изоморфно некоторому другому кольцу F', то существует другой гомоморфизм φ': $R\to F'$, ядром этого гомоморфизма также является идеал I.

Построение кольца $F'\cong R/I$ – формально некорректная задача (как и аналогичная задача о построении группы $F'\cong G/H$ – см. раздел 2.3. «Факторизация групп»). Для ее решения можно использовать тот же неформальный прием, который был предложен для групп: в каждом смежном классе факторкольца R/I надо выбрать *простейшего представителя*. Если окажется, что совокупность этих простейших представителей является кольцом относительно тех же самых (или похожих) операций, на которых построено исходное кольцо R, то это и будет искомое кольцо F'.

При переходе к факторкольцу не теряются «хорошие» свойства кольца: коммутативность и ассоциативность, сохраняется также дистрибутивность, так

что факторкольцо и в самом деле является кольцом. Сохранение следует из того, что операции в факторкольце определяются через операции в исходном кольце. Дополнительный аргумент в пользу этого утверждения – факторкольцо является гомоморфным образом исходного кольца.

Некоторые свойства, которых не было у исходного кольца, могут возникнуть при переходе к факторкольцу. Так, при факторизации кольца целых чисел $\mathbf{Z}$ по идеалу $p\mathbf{Z}$, где p – простое число, получается факторкольцо, изоморфное *полю* вычетов $\mathbf{Z}_p$, т.е. операция умножения приобретает свойство *обратимости*. Это следует из решения задачи **Р 3.1.11**, где доказано, что если в конечном кольце нет делителей нуля, мультипликативная подсистема кольца является квазигруппой, а в случае ассоциативного умножения – группой (пример в задаче **Р 3.3.3**).

Такое свойство, как отсутствие делителей нуля при факторизации может «потеряться». Например, они есть в факторкольце $\mathbf{Z}/n\mathbf{Z}$, где n – составное число.

При факторизации кольца многочленов $F[x]$ над полем F по идеалу $f(x)\cdot F[x]$, где $f(x)$ – многочлен из $F[x]$, *неприводимый* (т.е. неразложимый на многочлены меньшей степени) над этим кольцом, получается поле, элементами которого являются многочлены (задача **Р 3.3.6**).

Заметим, что кольцо целых чисел и кольцо многочленов над полем коммутативны, ассоциативны и не имеют делителей нуля.

Решение задач

Р 3.3.1. Доказать, что если кольцо R является телом (в частности, полем) его идеалами являются только несобственные подкольца, т.е. {0} и R.

Решение. То, что {0} является идеалом, следует из мультипликативных свойств нуля. Пусть теперь $I\neq\{0\}$. Возьмем некоторый элемент $a\in I$, $a\neq 0$. Для него в теле существует a^{-1}. В произведении $a\cdot a^{-1}=1$ первый множитель принадлежит идеалу, поэтому произведение также принадлежит идеалу, т.е. $1\in I$. Возьмем произвольный элемент $b\in R$. Произведение $b\cdot 1=b\in I$, поскольку второй сомножитель $1\in I$. Вывод: $I=R$.

Р 3.3.2. Доказать корректность определения умножения классов с помощью их представителей согласно формуле $(a+I)\cdot(b+I)=a\cdot b+I$.

Решение. Нужно доказать, что если взять произвольные элементы $a'\in a+I$, $b'\in b+I$ (возможно, отличные от a и b), то их произведение $a'\cdot b'$ принадлежит тому же классу, что и произведение $a\cdot b$, т.е. $a'\cdot b'\in a\cdot b+I$.

Поскольку $a'\in a+I$, имеем $a'=a+i$ (где $i\in I$). Аналогично $b'=b+j$ (где $j\in I$). Возьмем произведение $a'\cdot b'$ и воспользуемся дистрибутивностью:

$$a'\cdot b'=(a+i)\cdot(b+j)=a\cdot b+i\cdot b+a\cdot j+i\cdot j.$$

Слагаемое $i\cdot b\in I$ (поскольку $i\in I$), слагаемое $a\cdot j\in I$ (поскольку $j\in I$). Тем более $i\cdot j\in I$. Таким образом, произведение $a'\cdot b'$ отличается от произведения $a\cdot b$ слагаемыми, принадлежащими идеалу I, поэтому $a'\cdot b'\in a\cdot b+I$, что и требовалось доказать.

Р 3.3.3. Построить факторкольцо кольца целых чисел $\mathbf{Z}$ по идеалу $3\mathbf{Z}$. Кратко это факторкольцо можно обозначить $\mathbf{Z}/(3)$.

Решение. При решении задачи **Р 2.3.1** строилась факторгруппа аддитивной группы целых чисел $(\mathbf{Z}, +)$ по подгруппе $3\mathbf{Z}$.

$3\mathbf{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$,

$3\mathbf{Z}+1 = \{\dots, -5, -2, 1, 4, 7, \dots\}$,

$3\mathbf{Z}+2 = \{\dots, -4, -1, 2, 5{,}8, \dots\}$.

Получилось три смежных класса: $3\mathbf{Z}$, $3\mathbf{Z}+1$, $3\mathbf{Z}+2$ и таблица их сложения.

Таблица 3.3

Таблицы сложения и умножения классов в факторкольце $\mathbf{Z}/(3)$

+	$3\mathbf{Z}$	$3\mathbf{Z}+1$	$3\mathbf{Z}+2$

·	$3\mathbf{Z}$	$3\mathbf{Z}+1$	$3\mathbf{Z}+2$

Построим (используя представителей классов) таблицу умножения. Найдем, например, произведение классов $(3\mathbf{Z}+1)\cdot(3\mathbf{Z}+2)$. Возьмем любого представителя в классе $3\mathbf{Z}+1$, скажем, -2, и любого представителя в классе $3\mathbf{Z}+2$, скажем, 2. Произведение этих двух чисел $(-2)\cdot 2 = -4$ принадлежит классу $3\mathbf{Z}+2$. Если взять в классах-слагаемых других представителей, конкретное произведение чисел может получиться другим, но в любом случае она будет принадлежать классу $3\mathbf{Z}+2$. Таким же способом заполняются все клетки таблицы умножения.

Из таблицы умножения видно, что для ненулевых классов существуют обратные (они сами): $(3\mathbf{Z}+1)^{-1}=3\mathbf{Z}+1$, $(3\mathbf{Z}+2)^{-1}=3\mathbf{Z}+2$.

Легко видеть, что построенное факторкольцо изоморфно кольцу (на самом деле – полю) вычетов по модулю 3: $(\mathbf{Z}, +)/(3) \cong (\mathbf{Z}_3, +_3)$. «Простейшими представителями» классов факторкольца являются: 0 для $3\mathbf{Z}$, 1 для $3\mathbf{Z}+1$, 2 для $3\mathbf{Z}+2$.

Имеет место гомоморфизм кольца $\mathbf{Z}$ на кольцо вычетов $\varphi : \mathbf{Z} \to \mathbf{Z}_3$. Значение $\varphi(x)$ – остаток от деления x на 3. В обозначениях MatLab® $\varphi(x)=\mathrm{mod}(x,3)$. Идеал является ядром этого гомоморфизма: $3\mathbf{Z} = \ker(\varphi)$.

Р 3.3.4. Построить факторкольцо кольца целых комплексных чисел $\mathbf{Z}[i]$ (пример **R 13**) по идеалу $(2-i)\cdot\mathbf{Z}[i]$ (кратко: $\mathbf{Z}[i]/(2-i)$).

Решение. Идеал состоит из произведений $(2-i)\cdot(x+iy)=x\cdot(2-i)+y\cdot(1+2i)$. Представим это множество точек комплексной плоскости геометрически (рис.

3.2). Все кольцо $\mathbf{Z}[i]$ – это целочисленная решетка, идеал – решетка, построенная на векторах, соответствующих комплексным числам $(2–i)$ и $(2–i)\cdot i=1+2i$. На рисунке выделен один из квадратов этой решетки.

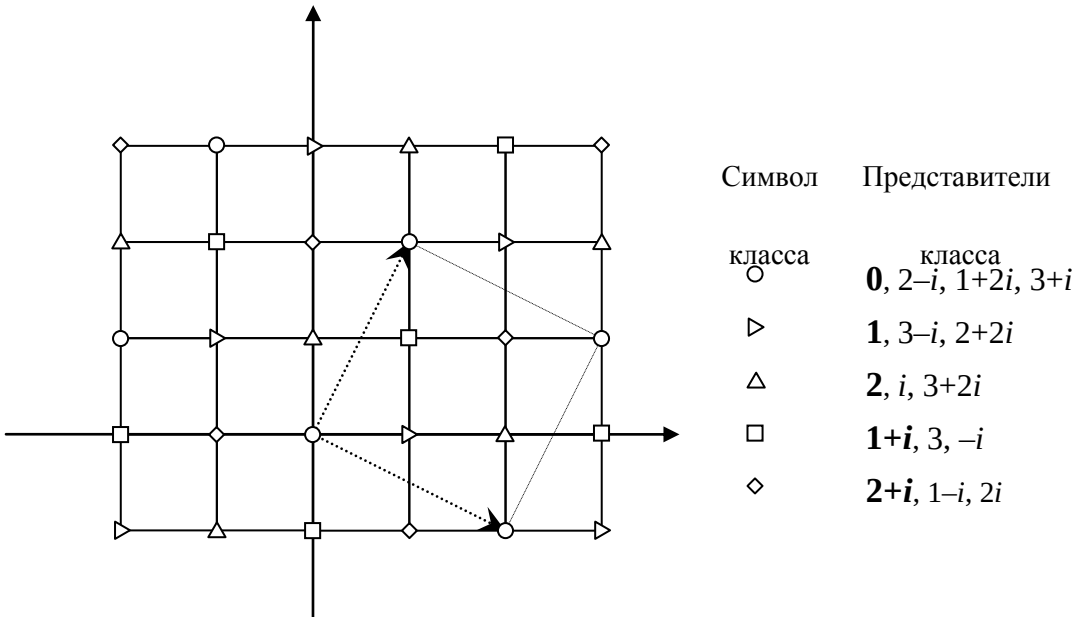

Рис. 3.2. Факторкольцо $\mathbf{Z}[i]/(2–i)$

Имеется 5 классов, представители которых обозначены различными символами, для некоторых представителей указаны их арифметические значения. В каждом списке первый (простейший) представитель выделен жирным шрифтом и несколько увеличенным размером, это обозначение в дальнейшем используется как идентификатор класса (т.е. 0 вместо $(2–i)\cdot\mathbf{Z}[i]$, 1 вместо $1+(2–i)\cdot\mathbf{Z}[i]$ и т.д.). Выбор простейшего представителя произволен: вместо 2 можно было взять i и т.п., для определенности были выбраны элементы внутри выделенного на рисунке «наклоненного» квадрата.

Покажем на нескольких примерах способ вычисления сумм и произведений в факторкольце.

$(1+i)+(2+i)=3+2i$. Вычтем из этого промежуточного результата входящее в идеал число $1+2i$ – получится 2, этот результат можно занести в таблицу сложения. Кратко это вычисление запишем так: $(1+i)+(2+i)=3+2i\Rightarrow(3+2i)–(1+2i)=2$.

$(2+i)+(2+i)=4+2i \Rightarrow (4+2i)-(1+2i)=3 \Rightarrow 3-(2-i)=1+i$ (вычитаемое $2-i$ входит в идеал)

$(1+i)\cdot(2+i)=1+3i \Rightarrow (1+3i)-(1+2i)=i \Rightarrow i+(2-i)=2$.

$(2+i)\cdot(2+i)=3+4i \Rightarrow (3+4i)-(1+2i)=2+2i \Rightarrow (2+2i)+(1+2i)=1$.

Чтобы сообразить, какой из элементов идеала надо прибавить или вычесть из промежуточного результата, проще всего ориентироваться на рисунок.

Окончательно получатся таблицы сложения и умножения в нашем факторкольце.

Таблица 3.4

Таблицы сложения и умножения классов в факторкольце $\mathbf{Z}[i]/(2-i)$

+	0	1	2	$1+i$	$2+i$
0	0	1	2	$1+i$	$2+i$

·	0	1	2	$1+i$	$2+i$
0	0	0	0	0	0

Из этих таблиц видно, что в нашем факторкольце отсутствуют делители нуля и более того – это факторкольцо является полем. Любое конечное поле изоморфно некоторому *полю Галуа* $\mathrm{GF}(p^n)$ (см. ниже замечания к задаче **Р 3.3.6**). В данном случае это $\mathrm{GF}(5^1) \cong \mathbf{Z}_5$ – поле вычетов по модулю 5 (см. задачу **С 3.3.4**).

Р 3.3.5. Построить факторкольцо кольца многочленов $\mathbf{R}[x]$ по идеалу $(x^2+1)\cdot\mathbf{R}[x]$ (кратко $\mathbf{R}[x]/(x^2+1)$).

Решение. Возьмем любой многочлен $f(x)\in\mathbf{R}[x]$ и разделим его с остатком на x^2+1: $f(x)=(x^2+1)\cdot p(x)+r(x)$. Ясно, что классы $f(x)+(x^2+1)\cdot\mathbf{R}[x]$ и $r(x)+(x^2+1)\cdot\mathbf{R}[x]$ совпадают (слагаемое $(x^2+1)\cdot p(x)$ «утонет» в $(x^2+1)\cdot\mathbf{R}[x]$, частью которого оно является). Таким образом, классы разбиения соответствуют остаткам $r(x)$. Степень этих многочленов не превосходит степени многочлена-делителя x^2+1, т.е. двух. В общем виде любой такой многочлен можно записать как $ax+b$, содержащий его класс $K_{a,b}=(ax+b)+(x^2+1)\cdot\mathbf{R}[x]$. Операции с классами определяются через соответствующие операции с многочленами-остатками.

Сложение многочленов-остатков выполняется путем приведения свободных членов: $(a_1x+b_1)+(a_2x+b_2)=(a_1+a_2)x+(b_1+b_2)$.

Произведение $(a_1x+b_1)\cdot(a_2x+b_2)=a_1a_2x^2+(a_1b_2+b_1a_2)x+b_1b_2$ надо заменить остатком от его деления на x^2+1. Остаток равен $(a_1b_2+b_1a_2)x+(b_1b_2-a_1a_2)$, он найден его с помощью деления «уголком»:

$$\begin{array}{lll} a_1a_2x^2+(a_1b_2+b_1a_2)x+b_1b_2 & & x^2+1 \\ \hline a_1a_2x^2+ & a_1a_2 & a_1a_2 \\ \hline (a_1b_2+b_1a_2)x+(b_1b_2-a_1a_2) & & \end{array}$$

Сопоставим умножение классов в нашем факторкольце с умножением комплексных чисел $(b_1+ia_1)\cdot(b_2+ia_2)=(b_1b_2-a_1a_2)+i\cdot(b_1a_2+b_1a_2)$. Видим, что факторкольцо изоморфно полю комплексных чисел.

Замечание. Это более «интеллектуальный» изоморфизм, чем $(\mathbf{Z}, +, \cdot)/(3)\cong(\mathbf{Z}_3, +_3, \cdot_3)$ в **Р 3.3.3**: здесь для получения результата надо «включить воображение».

Гомоморфизм кольца $\mathbf{R}[x]$ в факторкольцо определяется так. Для произвольного многочлена $f(x)\in\mathbf{R}[x]$ найдем остаток $r(x)=\mathrm{mod}(f(x), x^2+1)$ (здесь обозначение из MatLab® распространено на многочлены). Пусть $r(x)=ax+b$, тогда $\varphi(f(x))=K_{a,b}$. Идеал является ядром этого гомоморфизма: $(x^2+1)\cdot\mathbf{R}[x]=\ker(\varphi)=K_{0,0}$.

Р 3.3.6. Построить факторкольцо кольца многочленов $\mathbf{Z}_2[x]$ по идеалу $f(x)\cdot\mathbf{Z}_2[x]$, где многочлен второй степени $f(x)$ неприводим над полем вычетов $\mathbf{Z}_2$.

Решение. Над полем $\mathbf{Z}_2$ не так много многочленов второй степени, их всего четыре: x^2, x^2+1, x^2+x, x^2+x+1. Первые три приводимы ($x^2=x\cdot x$, $x^2+1=(x+1)\cdot(x+1)$ – такова арифметика поля вычетов, $x^2+x=x\cdot(x+1)$). Неприводим только многочлен x^2+x+1, поскольку у него нет корней в этом поле.

Классы факторкольца соответствуют многочленам не выше первой степени, их всего четыре: 0, 1, x, $x+1$, мы эти классы так и обозначим.

Сложение классов производится путем приведения подобных членов (с учетом особенностей арифметики поля вычетов).

При умножении классов надо каждое произведение заменить остатком от деления на x^2+x+1. В результате получаем таблицы сложения и умножения в

Таблица 3.5

Таблицы сложения и умножения классов в факторкольце $\mathbf{Z}_2[x]/(x^2+x+1)$

+	0	1	x	$x+1$
0	0	1	x	$x+1$

·	0	1	x	$x+1$
0	0	0	0	0

факторкольце.

Покажем, например, как вычислено произведение $(x+1)\cdot(x+1)$. Обычное произведение в кольце $\mathbf{Z}_2[x]$ равно x^2+1 (см. выше). Его надо разделить с остатком на многочлен x^2+x+1, фактически – вычесть x^2+x+1 из x^2+1, а с учетом специфики поля вычетов $\mathbf{Z}_2$, сложить эти многочлены. Получится x, что и зафиксировано в таблице умножения.

Полученное факторкольцо является полем ($x^{-1}=x+1$ и т.д.). Оно называется полем Галуа и обозначатся $GF(2^2)$ (GF – аббревиатура от французско-английского словосочетания Galois field). Вообще существуют поля Галуа $GF(p^n)$ для любого простого p и любого натурального n, где $\mathbf{Z}_p$ – лежащее в основе поле вычетов, а n – степень неприводимого многочлена. Если p и/или n больше двух, неприводимых многочленов будет несколько и таблицы умножения могут получиться разными, но *все полученные поля будут изоморфными*. Любое конечное поле изоморфно некоторому полю Галуа.

Р 3.3.7. Рассмотрим кольцо треугольных матриц третьего порядка вида $m=\begin{bmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{bmatrix}$ над произвольным числовым кольцом. Доказать, что матрицы из этого кольца при $a=0$ образуют идеал и построить соответствующее факторкольцо.

Решение. Доказательство того, что матрицы данного вида образуют кольцо, см. ниже задачу **С 3.3.7**. Возьмем произвольную матрицу из идеала $i=$

$\begin{bmatrix} 0 & p & q \\ 0 & 0 & p \\ 0 & 0 & 0 \end{bmatrix}$ (обозначения элементов, естественно, другие) и найдем произведения $i \cdot m$ и $m \cdot i$. Они равны между собой (это несущественно для доказательства) $i \cdot m = m \cdot i = \begin{bmatrix} 0 & pa & pa+qb \\ 0 & 0 & pa \\ 0 & 0 & 0 \end{bmatrix}$ и, что важно, имеют «идеальную» структуру.

Класс, которому принадлежит матрица m, состоит из матриц вида $i+m = \begin{bmatrix} a & b+p & c+q \\ 0 & a & b+p \\ 0 & 0 & a \end{bmatrix}$. Здесь a,b,c – фиксированные числа, элементы *конкретной* матрицы m, слагаемые p и q – любые, поскольку i – не конкретная, а *произвольная* матрица из идеала. Таким образом, класс, которому принадлежит матрица m, определяется одним единственным числом a и этот класс уместно обозначить K_a. «Простейшим представителем» этого класса является, очевидно, скалярная матрица $a \cdot E$. Скалярные матрицы образуют кольцо (см. ниже задачу **С 3.3.8**), изоморфное факторкольцу. Немного подумав, можно заметить, что эти кольца изоморфны числовому кольцу, над которым построено данное кольцо треугольных матриц.

Р 3.3.8. Рассмотрим кольцо матриц и в нем подмножество вырожденных матриц. Является ли это подмножество идеалом и как выглядит факторкольцо?

Решение. На первый взгляд – да. В самом деле, произведение любой матрицы на вырожденную – снова вырожденная матрица (поскольку определитель произведения равен произведению определителей), т.е. ″идеальные″ свойства соблюдаются. Попробуем сформировать классы разбиения. Сам предполагаемый идеал это, очевидно, нулевой класс, он состоит из вырожденных матриц. Возьмем какую-нибудь невырожденную матрицу, например, единичную, в один класс с ней попадают матрицы вида $E+D$, где D – вырожденная. Например, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ – невырожденная, все в порядке. Другой пример:

$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}+\begin{bmatrix}-1 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}$ – вырожденная, т.е. *из нулевого класса*. Получились пересекающиеся «классы», что никуда не годится. Причина в том, что в определении идеала еще до ″идеальных″ мультипликативных свойств требовалось, чтобы это было *подкольцо*, т.е. множество должно быть замкнуто относительно операций (еще в нем должен присутствовать кольцевой нуль и противоположные по сложению элементы). С умножением все в порядке (замкнутость по умножению следует из «идеальных″ свойств), но относительно сложения множество вырожденных матриц *незамкнуто*. Например, $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}+\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$.

Задачи для самостоятельного решения

С 3.3.1. Докажите, что отображение кольца в факторкольцо φ: $R\to R\,/\,I$, задаваемое формулой $\varphi(x)=x+I$, является гомоморфизмом, т.е. $\varphi(x+y)=\varphi(x)+\varphi(y)$ и $\varphi(x\cdot y)=\varphi(x)\cdot\varphi(y)$.

С 3.3.2. Докажите, что идеал I является ядром этого гомоморфизма: $\ker(\varphi)=I$, т.е. $\forall i\in I$ его образ $\varphi(i)=0$.

С 3.3.3. Постройте факторкольцо $\mathbf{Z}[i]\,/\,(1+i)$.

Указание. Используйте подход задачи **Р 3.3.4.**

С 3.3.4. Докажите, что факторкольцо $\mathbf{Z}[i])\,/\,(2-i)$ (задача **Р 3.3.4)** изоморфно полю вычетов $\mathbf{Z}_5$.

С 3.3.5. Постройте факторкольцо $\mathbf{R}[x]\,/\,(x^2-1)$.

Указание. Используйте подход задачи **Р 3.3.5**.

С 3.3.6. Опишите гомоморфизмы, связанные с факторизацией в задачах **Р 3.3.5–7**.

С 3.3.7. Докажите, что треугольные матрицы, о которых идет речь в задаче **Р 3.3.7**, образуют кольцо. Является ли это кольцо коммутативным?

С 3.3.8. Докажите, что скалярные матрицы вида $a \cdot E$, о которых также идет речь в задаче **Р 3.3.7**, образуют подкольцо в кольце треугольных матриц. Является ли это подкольцо идеалом?

С 3.3.9. Докажите, что множество матриц вида $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ является кольцом, а матрицы, у которых $a=b$, образуют идеал. Постройте факторкольцо.

Замечание. Это кольцо изоморфно кольцу двойных чисел (пример **R 14**), а идеал состоит из делителей нуля в этом кольце (см. выше задачу **Р 3.1.5**).

С 3.3.10. Рассмотрите кольцо ($\mathbf{V}$, +, ×) из примера **R 7**. Его элементы – трехмерные геометрические векторы, сложение векторов происходит как обычно, по правилу параллелограмма (треугольника), а умножение есть векторное умножение векторов. Это кольцо не ассоциативно и не коммутативно. Могут ли у этого кольца быть собственные идеалы (т.е. отличные от нулевого и всего кольца)?

Указание. Подумайте, что представляют собой с *геометрической* точки зрения подгруппы аддитивной группы этого кольца. И учтите, что векторное произведение перпендикулярно к обоим сомножителем.

С 3.3.11. Постройте фактор-кольцо $\mathbf{Z}[i]$ / (2). Сколько в нем элементов? Является ли оно полем?

С 3.3.12. Постройте фактор-кольцо $\mathbf{Q}[x]$ / (x^2-2). Докажите, что оно является полем. Какому из ранее рассмотренных полей оно изоморфно?

С 3.3.13. Рассмотрите множество R комплексных чисел вида $2a+bi$, где $a,b \in \mathbf{Z}$. Докажите, что R является кольцом. Докажите, что множество $I = 2 \cdot R$ является идеалом в R и постройте факторкольцо R / I

С 3.3.14. Рассмотрите множество R функций $y=f(x)$, $x,y \in \mathbf{R}$. Докажите, что R является кольцом. Докажите, что подмножество $I = \{y=h(x) \mid h(-1)=h(1)=0\}$ является идеалом в R и постройте факторкольцо R / I.

С 3.3.15. В кольце целочисленных многочленов $\mathbf{Z}[x]$ рассмотрите подмножество многочленов с четными свободными членами. Докажите, что это подмножество является идеалом и постройте факторкольцо.

С 3.3.16. В кольце целочисленных многочленов $\mathbf{Z}[x]$ рассмотрите подмножество многочленов с четными коэффициентами. Докажите, что это подмножество является идеалом и постройте факторкольцо.

С 3.3.17. Рассмотрите отображение кольца многочленов $F[x]$ в кольцо F, задаваемое формулой $\varphi(f(x))=f(0)$. Докажите, что φ является гомоморфизмом, опишите его ядро, докажите, что это множество является идеалом и постройте факторкольцо.

4. ВЫЧИСЛЕНИЯ В ПОЛЯХ ВЫЧЕТОВ

4.1. Арифметика вычетов

Основы теории

Вычетами по модулю m называются остатки от деления целых чисел на натуральное число m, множество вычетов $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$. Операции на множестве вычетов – *сложение и умножение по модулю* m, их определение: $x +_m y$ – остаток от деления $x + y$ на n, $x \cdot_m y$ – остаток от деления $x \cdot y$ на n. Разность $x -_n y$ вычисляется как $x +_n (-y)$, где симметричный по сложению вычет $(-y)=m - y$ (для $y \neq 0$). Относительно операций $+_m$ и $\cdot_m$ множество вычетов $\mathbf{Z}_m$ является кольцом, оно изоморфно факторкольцу $\mathbf{Z}/m\mathbf{Z}$. Гомоморфизм $\varphi : \mathbf{Z} \to \mathbf{Z}_m$ задается формулой $\varphi(x)=\mathrm{mod}(x,m)$ (в MatLab® так обозначается функция, вычисляющая остаток от деления x на m).

Если модуль – простое число (его обычно обозначают p), кольцо вычетов $\mathbf{Z}_p$ и факторкольцо $\mathbf{Z}/p\mathbf{Z}$ являются *полями*.

Еще один способ представления отношения между целыми числами, имеющими одинаковый остаток при делении на заданный модуль: $x \equiv y \pmod{m}$ (словами: «*x сравнимо с y по модулю m*»). Это отношение называется *сравнением по модулю m*). Оно означает равенство остатков: $\mathrm{mod}(x,m)=\mathrm{mod}(y,m)$. Данное отношение является рефлексивным, симметричным и транзитивным, оно определяет разбиение множества $\mathbf{Z}$ на классы, являющиеся элементами факторкольца $\mathbf{Z}/m\mathbf{Z}$.

Существует довольно обширная теория сравнений. Сравнения можно умножать на любое целое число и возводить в любую натуральную степень. Два сравнения по одному и тому же модулю можно складывать и перемножать, а сокращать, т.е. делить, не всегда. Так, сравнение $8 \equiv 20 \pmod 6$ можно сократить на 2, получится $4 \equiv 10 \pmod 6$, но нельзя сократить на 4, получится $2 \equiv 5 \pmod 6$, что *неверно*. Возможность сложения и умножения сравнений является выраже-

нием (в этой символике) независимости результата операций с классами фактор-кольца от выбора представителей в этих классах.

Сравнения, содержащие неизвестные, можно *решать*, т.е. находить значения неизвестных, при которых сравнение выполняется.

Приведем без доказательства две теоремы о сравнениях.

Малая теорема Ферма: для любого простого p и любого $a \geq 1$, не делящегося на p, справедливо сравнение $a^{p-1} \equiv 1 \pmod{p}$.

Теорема Эйлера (одна из почти бесконечного множества теорем и формул, носящих его имя): для любого модуля m и любого $a \geq 1$, взаимно простого с m, справедливо сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$. Здесь $\varphi(m)$ – функция Эйлера, ее значение равно количеству натуральных чисел, меньших m и взаимно простых с m. Для простого числа значение функции Эйлера $\varphi(p)=p-1$, так что малая теорема Ферма является частным случаем теоремы Эйлера.

В поле вычетов $\mathbf{Z}_p$ у каждого вычета $x \neq 0$ имеется обратный (симметричный по умножению) вычет x^{-1}. К сожалению, не существует такой же простой формулы для вычисления x^{-1}, как для $(-x)=p-x$ (при $x \neq 0$).

Если p совсем мало (<10, т.е. 2,3,5,7), можно просто построить таблицу умножения – в ней все и будет видно. Если p не очень велико (<20), можно умножить x на вычеты $\{2, \ldots, p-1\}$ – когда-то произведение окажется равным 1. Найдем этим способом 11^{-1} в поле $\mathbf{Z}_{19}$.

Имеем $11 \cdot 2 = 22 = 19+3 \equiv 3 \neq 1$, $11 \cdot 3 = 33 = 19+14 \equiv 14 \neq 1$, $11 \cdot 4 = 44 = 19 \cdot 2 + 6 \equiv 6 \neq 1$, постепенно дойдем до $11 \cdot 7 = 77 = 19 \cdot 4 + 1 \equiv 1$, так что $11^{-1}=7$.

Вычет x^{-1} можно найти с помощью *расширенного алгоритма Евклида*, когда ищется не только наибольший общий делитель, но и так называемые *коэффициенты Безу*, задающие линейное представление наибольшего общего делителя через заданные числа: НОД$(x,y) = x \cdot u + y \cdot v$, где $|u| \leq y$, $|v| \leq x$. Если взять $y=p$, получится $x \cdot u + p \cdot v = 1$ или $x \cdot u \equiv 1 \pmod{p}$ (поскольку второе слагаемое $p \cdot v$ по модулю p обращается в нуль). Таким образом, $x^{-1} = u$ (см. ниже задачу **Р 4.1.5**).

Решение задач

Р 4.1.1. Вычислить в кольце вычетов $\mathbf{Z}_{275}$ значение выражения $200^2–100^2$.

Решение. Сначала найдем $200^2 = 200 \cdot_{275} 200$. Это остаток от деления $200 \cdot 200 = 40000$ на 275. Имея под рукой компьютер, можно применить MatLab®: mod(40000,275)=125, аналогично mod(10000,275)=100, результат 25.

Можно воспользоваться калькулятором: 40000/275=145,45..., целая часть равна 145, остаток от деления 40000–275·145=125.

Аналогично 10000/275=36,36..., целая часть равна 36, остаток от деления 10000–275·36=100 и т.д.

Р 4.1.2. Найти остаток при делении

1) 15^{231} на 14. 2) 15^{231} на 16. 3) 18^{2815} на 14.

Решение.

1) В кольце вычетов по модулю 14 числу 15 соответствует вычет, равный 1, используя гомоморфизм $\varphi : \mathbf{Z} \to \mathbf{Z}_{14}$, найдем $\varphi(15^{231})=1^{231}=1$.

2) В кольце вычетов $\mathbf{Z}_{16}$ числу 15 соответствует вычет, равный 15, так что на этом пути получить хороший результат не удастся. Рассмотрим изоморфное кольцу вычетов факторкольцо $\mathbf{Z}/16\mathbf{Z}$. В нем число 15 находится в одном классе с числом –1. Возведение в степень это просто многократное умножение, а результат умножения в факторкольце не зависит от выбора представителей в перемножаемых классах. Вместо 15 возьмем –1 и найдем $(–1)^{231}= –1$, остаток mod(–1,16)=15.

Более компактное решение получается с использованием символики сравнений: $15 \equiv –1$, откуда $15^{231} \equiv (–1)^{231} = –1 \equiv 15$ (все сравнения по модулю 16).

3) Сразу можно уменьшить основание степени: у нас $18 \equiv 4 \pmod{14}$, поэтому $18^{2815} \equiv 4^{2815} \pmod{14}$. Однако число 4^{2815} слишком велико, оно далеко выходит за границы, доступные программной системе MatLab®. В ней максимальное вещественное число realmax=1.7977e+308, а максимальное число,

которое может быть представлено, как целое, содержит всего 9 десятичных цифр.

Поэтому необходима «разборка» показателя степени на составные части. Ее можно выполнить разными способами. Разложим показатель степени на простые множители: $2815=5\cdot563$, тогда $4^{2815}=(4^5)^{563}$. Без труда найдем (даже вручную), что $4^5=2^{10}=1024\equiv2 \pmod{14}$. Далее рассмотрим 2^{563}. Это число все еще слишком велико для целочисленного представления (2^563=3.0192e+169), а «в плавающей форме» об остатках от деления говорить нельзя. Продолжим «разборку» показателя степени, представим его в виде $563=3+10\cdot56$, степень $2^{563}=2^3\cdot(2^{10})^{56}$. Было установлено, что $2^{10}\equiv2 \pmod{14}$, поэтому можно упростить выражение: $2^3\cdot2^{56}=2^{59}=2^9\cdot(2^{10})^5$. Опять заменим 2^{10} на 2 и получим $2^9\cdot2^5=2^{10}\cdot2^4$. Еще раз заменим 2^{10} на 2 и получим $2\cdot2^4=32=14\cdot2+4$. Ответ: 4.

Р 4.1.3. Найти остаток при делении 10^{101} на 7.

Решение. 7 – простое число, поэтому можно применить малую теорему Ферма. Разделим с остатком показатель степени $N=101$ на $p-1=6$: $101=6\cdot16+5$, поэтому $10^{101}=10^{6\cdot16+5}=(10^6)^{16}\cdot10^5$. Далее все сравнения берутся по mod 7. Согласно теореме Ферма имеем $10^6\equiv1$, поэтому $10^{101}\equiv10^5$. Поскольку $10\equiv3$, $10^5\equiv3^5=243$. Остаток от деления 243 на 7 найдем вручную или с помощью пакета MatLab®: mod(243,7)=5.

Р 4.1.4. Найти две последние цифры числа

1) 11^{203}. 2) 803^{1254}.

Решение. Речь идет о сравнениях по mod 100, будем писать просто ≡.

1) $11^{203}=11^3\cdot(11^2)^{100}$, $11^3=1331\equiv31$, $11^2=121\equiv21$. Далее имеем $(21)^{100}=(21^4)^{5\cdot5}$, $21^4=194481\equiv81$. $(21)^{100}\equiv(81^5)^5$. Вычислить 81^5 в целом виде MatLab® не может (81^5=3.4868e+009), поэтому представим его как произведение $81^5=81^3\cdot81^2$. Имеем $81^3=531441\equiv41$, $81^2=6561\equiv61$, их произведение $41\cdot61=2501\equiv1$, значит $(21)^{100}\equiv1^5=1$. Учтем множитель $11^3\equiv31$ и получим ответ: 31.

2) $803 \equiv 3$, поэтому $803^{1254} \equiv 3^{1254}$. Имеем $1254 = 6 \cdot 209$ (более «глубокого» разложения делать не станем), $3^{1254} = (3^6)^{209} = (729)^{209} \equiv (29)^{209} = 29^9 \cdot (29^2)^{100}$. Представим первый сомножитель в виде $29^9 = (29^3)^3$. В скобках имеем $29^3 = 24389 \equiv 89$, $29^9 \equiv 89^3 = 704969 \equiv 69$. Второй сомножитель $(29^2)^{100} = 841^{100} \equiv 41^{100}$. Представим показатель степени как произведение $100 = 4 \cdot 5 \cdot 5$, тогда $41^{100} = (41^4)^{5 \cdot 5}$. Степень в скобках $41^4 = 2825761 \equiv 61$, $(41^4)^{5 \cdot 5} \equiv (61^5)^5 = (844596301)^5 \equiv 1^5 = 1$. Учтем первый сомножитель и получим ответ: 69.

Р 4.1.5. Найти 11^{-1} в поле $\mathbf{Z}_{19}$.

Решение. Выполним расширенный алгоритм Евклида для чисел 19 и 11. Результаты промежуточных вычислений будем записывать в «полубуквенном

$p = x \cdot 1 + r_1, \quad r_1 = 8$	$r_1 = p - x$
$x = r_1 \cdot 1 + r_2, \quad r_2 = 3$	$r_2 = x - r_1$

виде» – числовая конкретика может запутать дело. Промежуточные частные, которые не играют важной роли, будем писать прямо в виде чисел.

Итак, разделим с остатком $p = 19$ на $x = 11$, затем x на первый остаток r_1 и т.д.:

$d = r_2 - r_3 = r_2 - (r_1 - 2 \cdot r_2) = 3 \cdot r_2 - r_1 = 3 \cdot (x - r_1) - r_1 = 3 \cdot x - 4 \cdot r_1 = 3 \cdot x - 4 \cdot (p - x) = 7 \cdot x - 4 \cdot p = 1$.

Перейдя в поле вычетов по модулю $p = 19$, получим $7 \cdot x \equiv 1$, т.е. $x^{-1} = 7$.

Расширенный алгоритм Евклида можно выполнить в матричной форме:

$$\begin{array}{c|c|c} 19 & \begin{bmatrix} 19 & 11 \\ 1 & 0 \end{bmatrix} \xrightarrow[[1]-[2]]{} \begin{bmatrix} 8 & 11 \\ 1 & 0 \end{bmatrix} \xrightarrow[[2]-[1]]{} \begin{bmatrix} 8 & 3 \\ 1 & -1 \end{bmatrix} \xrightarrow[[1]-2\cdot[2]]{} \begin{bmatrix} 2 & 3 \\ 3 & -1 \end{bmatrix} \xrightarrow[[2]-[1]]{} \begin{bmatrix} 2 & 1 \\ 3 & -4 \end{bmatrix} \xrightarrow[[1]-2\cdot[2]]{} \begin{bmatrix} 0 & 1 \\ 11 & -4 \end{bmatrix} & 19 \\ 11 & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} -1 & 1 \end{bmatrix} \quad \begin{bmatrix} -1 & 2 \end{bmatrix} \quad \begin{bmatrix} -5 & 2 \end{bmatrix} \quad \begin{bmatrix} -5 & 7 \end{bmatrix} \quad \begin{bmatrix} -19 & 7 \end{bmatrix} & 11 \end{array}$$

Интерпретация *столбцов*: начальная матрица: $19 = 19 \cdot 1 + 11 \cdot 0$, $11 = 19 \cdot 0 + 19 \cdot 1$, конечная матрица: $0 = 19 \cdot 11 + 11 \cdot (-19)$, $1 = 19 \cdot (-4) + 11 \cdot 7$.

Тот же результат можно получить с помощью MatLab®, вызвав функцию gcd (greatest common divisor – наибольший общий делитель):

[g,c,d] = gcd(19,11), получится g = 1, c = –4, d = 7

(интерпретация результата: наибольший общий делитель 1 = (–4)·19+7·11).

Р 4.1.5. Решить сравнения

1) $2x+1\equiv 0 \pmod{13}$. 2) $x^2+1\equiv 0 \pmod{13}$.

Решение. Будем писать просто ≡, без указания модуля.

1) $2x+1\equiv 0 \Rightarrow 2x\equiv -1 \Rightarrow 2x\equiv -1+13=12 \Rightarrow x\equiv 6$.
2) $x^2+1\equiv 0 \Rightarrow x^2\equiv -1 \Rightarrow x^2\equiv -1+13=12 \Rightarrow x^2\equiv 12+13=25 \Rightarrow x\equiv \pm 5$.

Задачи для самостоятельного решения

С 4.1.1. Найдите остаток при делении

1) $12^{1231} + 14^{4324}$ на 13. 2) 208^{208} на 23. 3) 10^{2732} на 22.

4) $10^{1054}-23\cdot 16^{285}+22^{17}$ на 15. Ответы: 1) 0. 2) 1. 3) 12. 4) 3.

С 4.1.2. Найдите две последние цифры числа

1) 2^{341}. 2) 6^{30}. Ответы: 1) 52. 2) 76.

С 4.1.3. Найдите 15^{-1} в поле $\mathbf{Z}_{37}$. Ответ: 5.

4.2. Линейная алгебра над полем вычетов

Основы теории

Большая часть теоретических положений и алгоритмов линейной алгебры над числовыми полями переносится с небольшими изменениями на случай полей вычетов. Остаются в силе метод Гаусса, теория определителей, правило Крамера. Сохраняется теория линейной зависимости, ранга матрицы, алгебра матриц, общая теория систем линейных уравнений.

Очевидное отличие от случая числового поля: линейное пространство или многообразие ненулевой размерности является *конечным множеством*.

Кроме полей вычетов, можно рассматривать поля Галуа $GF(2^2)$ (**Р 3.3.6**). В таблице 3.5 элементы этого поля обозначены 0, 1, *x*, *x*+1. Для удобства мани-

Таблица 3.5'

Таблицы сложения и умножения в $GF(2^2)$

+	0	1	α	β
0	0	1	α	β

·	0	1	α	β
0	0	0	0	0

пулирования заменим x на α, $x+1$ на β и получим таблицу 3.5'.

Теперь можно, например, решать системы уравнений над этим полем (см. ниже задачу **Р 4.2.8**).

Решение задач

Р 4.2.1. Вычислить в поле вычетов $\mathbf{Z}_3$ определитель $d = \begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix}$.

Решение. «По науке» надо действовать так:

$$d = (1 \cdot_3 1) -_3 (2 \cdot_3 2),$$

где $x -_3 y = x +_3 (-y)$, а $(-y)=3-y$ (для $y \neq 0$). Вычисляя шаг за шагом, получим

$$1 \cdot_3 1 = 1, \quad 2 \cdot_3 2 = 1, \quad 1 -_3 1 = 1 +_3 2 = 0.$$

Можно, однако, поступить проще. Будем считать элементы определителя целыми числами из кольца $\mathbf{Z}$, тогда $d=1\cdot1-2\cdot2=-3$. Далее воспользуемся гомоморфизмом $\varphi:\mathbf{Z}\to\mathbf{Z}_p$, задаваемом формулой $\varphi(x)=\mathrm{mod}(x,p)$. При малых x и p достаточно к числу x прибавить (или отнять от него) величину, кратную p, чтобы «загнать» результат в множество вычетов $\mathbf{Z}_p$. В данном случае прибавим 3 и получим $-3+3=0$ – тот же результат. При больших x и/или p придется в самом деле делить x на p с остатком.

Замечание. В этой задаче несущественно – имеем мы дело с полем или кольцом.

Р 4.2.2. Решить над полями вычетов $\mathbf{Z}_3$ и $\mathbf{Z}_5$ систему линейных уравнений $\{x+2z=1, y+2z=2, 2x+z=1\}$ (Проскуряков, 1756).

Решение. Воспользуемся правилом Крамера. Сначала решим систему над полем рациональных чисел $\mathbf{Q}$. Определители

$$\Delta = \begin{vmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{vmatrix} = -3, \quad \Delta_x = \begin{vmatrix} 1 & 0 & 2 \\ 2 & 1 & 2 \\ 1 & 0 & 1 \end{vmatrix} = -1, \quad \Delta_y = \begin{vmatrix} 1 & 1 & 2 \\ 0 & 2 & 2 \\ 2 & 1 & 1 \end{vmatrix} = -4, \quad \Delta_z = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{vmatrix} = -1.$$

Значения неизвестных $x=\frac{1}{3}$, $y=\frac{4}{3}$, $z=\frac{1}{3}$.

Приведем значения определителей в поле вычетов $\mathbf{Z}_3$: $\Delta=0$, $\Delta_x=2$, $\Delta_y=2$, $\Delta_z=2$. Над этим полем система несовместна.

Приведем значения определителей в поле вычетов $\mathbf{Z}_5$: $\Delta=2$, $\Delta_x=4$, $\Delta_y=1$, $\Delta_z=4$. Значения неизвестных найдем по формулам Крамера: $x=\frac{4}{2}=2$, $y=\frac{1}{2}$, $z=\frac{4}{2}=2$. Как понимать найденное значение неизвестной y? Дробь $\frac{1}{2}$ *не является* элементом поля $\mathbf{Z}_5$, поэтому будем ее рассматривать как *выражение*, которое необходимо вычислить согласно правилам действий в этом поле: $\frac{1}{2}=1\cdot 2^{-1}=3$, поскольку произведение $2\cdot 3=6$, а $6\equiv 1 \pmod 5$. Итак, решение системы уравнений над полем $\mathbf{Z}_5$: $x=2$, $y=3$, $z=2$.

Проверка. Первое уравнение: $1\cdot 2+2\cdot 2=6\equiv 1$, второе уравнение: $1\cdot 3+2\cdot 2=7\equiv 2$, третье уравнение: $2\cdot 2+1\cdot 2=6\equiv 1$. Найденные значения удовлетворяют системе уравнений над полем $\mathbf{Z}_5$.

Замечание. Фактически это системы сравнений по соответствующим модулям.

Р 4.2.3. Решить ту же систему линейных уравнений над полями $\mathbf{Z}_3$ и $\mathbf{Z}_5$ методом Гаусса.

Решение. Составим расширенную матрицу: $\left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 2 & 0 & 1 & 1 \end{array}\right)$. Если бы мы решали систему над полем рациональных чисел $\mathbf{Q}$, то первым шагом выполнили бы операцию (3)–2·(1). В поле $\mathbf{Z}_3$ коэффициенту –2 соответствует вычет 1, поэтому выполним операцию (3)+1·(1). В 1-ом столбце имеем $2+1\cdot 1=3\equiv 0$, во 2-ом столбце сохранится 0, в третьем столбце $1+1\cdot 2=3\equiv 0$, в столбце свободных членов $1+1\cdot 1=2$, так что $\left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 2 & 0 & 1 & 1 \end{array}\right) \underset{(3)+1\cdot(1)}{\Rightarrow} \left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 2 \end{array}\right)$. В алгебраической форме 3-е уравнение этой системы имеет вид $0\cdot x+0\cdot y+0\cdot z=2$. Очевидно, что оно не имеет решения, поэтому система над полем $\mathbf{Z}_3$ несовместна.

Найдем решение той же системы над полем $\mathbf{Z}_5$ методом Гаусса. Вместо операции (3)–2·(1), с которой начинается решение этой системы над полем рациональных чисел $\mathbf{Q}$, выполним операцию (3)+3·(1), поскольку в поле $\mathbf{Z}_5$ ко-

эффициенту –2 соответствует вычет 3. В 1-ом столбце получим 2+3·1=5≡0, во 2-ом столбце сохранится 0, в 3-ем столбце имеем 1+3·2=7≡2, в столбце свободных членов 1+3·1=4. Таким образом $\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\2&0&1&1\end{array}\right)\underset{(3)+3\cdot(1)}{\Rightarrow}\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\0&0&2&4\end{array}\right)$. 3-ю строку этой матрицы можно сократить (разделить) на 2: $\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\0&0&2&4\end{array}\right)\underset{(3)/2}{\Rightarrow}\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\0&0&1&2\end{array}\right)$.

Выполним операции (1)+3·(3) и (2)+3·(3) – в 1-й и во 2-й строках 3-го столбца получится 2+3·1=5≡0, остальные элементы этих строк сохраняться: $\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\0&0&1&2\end{array}\right)\underset{(2)+3\cdot(3)}{\overset{(1)+3\cdot(3)}{\Rightarrow}}\left(\begin{array}{ccc|c}1&0&0&2\\0&1&0&3\\0&0&1&2\end{array}\right)$.

Видим, что получилось решение, ранее найденное по правилу Крамера: x=2, y=3, z=2.

Р 4.2.4. Решить систему линейных уравнений {x+2z=1, y+2z=2, 2x+z=2} над полем $\mathbf{Z}_3$ методом Гаусса.

Решение. При решении задачи **Р 4.2.2** (см. выше) было обнаружено, что определитель матрицы $\Delta=\begin{vmatrix}1&0&2\\0&1&2\\2&0&1\end{vmatrix}$ = –3 ≡ 0 (mod 3), а определители Δ_x=2, Δ_y=2, Δ_z=2. Система над этим полем оказалась несовместной. Однако по сравнению с той задачей у нас изменились свободные члены.

Применим метод Гаусса. Составим расширенную матрицу: $\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\2&0&1&2\end{array}\right)$.

Проделаем (с необходимыми изменениями) те же преобразования, которые делались в задаче **Р 4.2.3**: $\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\2&0&1&2\end{array}\right)\underset{(3)+1\cdot(1)}{\Rightarrow}\left(\begin{array}{ccc|c}1&0&2&1\\0&1&2&2\\0&0&0&0\end{array}\right)$. Последнее уравнение мож-

но отбросить, для оставшихся запишем общее решение: x=1–2z, y=2–2z. В поле $\mathbf{Z}_3$ коэффициент –2 заменим на 1 и получим x=1+z, y=2+z, где z=0,1,2.

Окончательно имеем многообразие из трех решений: (1,2,0), (2,0,1), (0,1,2),

Р 4.2.5. Для системы линейных уравнений $\{2x_1+2x_2=0,\ x_1+2x_2+2x_3=2\}$ над полем $\mathbf{Z}_3$ найдем многообразие решений другим способом.

Решение. Расширенная матрица $\left(\begin{array}{ccc|c} 2 & 2 & 0 & 0 \\ 1 & 2 & 2 & 2 \end{array}\right)$. Для матрицы $A=\begin{pmatrix} 2 & 2 & 0 \\ 1 & 2 & 2 \end{pmatrix}$ возьмем какой-нибудь набор базисных столбцов (над полем $\mathbf{Z}_3$!). Например, определитель $\begin{vmatrix} 2 & 2 \\ 1 & 2 \end{vmatrix} = 4-2=2\neq 0 \pmod 3$, набор столбцов (1,2) – базисный. Матрица, содержащая выбранные базисные столбцы $B=\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$, обратная матрица (считая элементы матрицы B целыми числами) $B^{-1}=\frac{1}{2}\cdot\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}$. Приведем B^{-1} в поле вычетов $\mathbf{Z}_3$. Выражение $\frac{1}{2}=2^{-1}\underset{\text{mod}3}{=}2,\quad -2\underset{\text{mod}3}{=}1,\quad -1\underset{\text{mod}3}{=}2$. Получим $B^{-1}\underset{\text{mod}3}{=}2\cdot\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}=\begin{pmatrix} 4 & 2 \\ 4 & 4 \end{pmatrix}\underset{\text{mod}3}{=}\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. Проверка: $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\cdot\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}=\begin{pmatrix} 4 & 6 \\ 3 & 4 \end{pmatrix}\underset{\text{mod}3}{=}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Умножим слева расширенную матрицу на B^{-1}:

$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\cdot\left(\begin{array}{ccc|c} 2 & 2 & 0 & 0 \\ 1 & 2 & 2 & 2 \end{array}\right)=\left(\begin{array}{ccc|c} 4 & 6 & 4 & 4 \\ 3 & 4 & 2 & 2 \end{array}\right)\underset{\text{mod}3}{=}\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \end{array}\right)$. В алгебраической форме система уравнений, разрешенная относительно базисных неизвестных x_1,x_2

$$\begin{cases} x_1+\ x_3=1, \\ x_2+2x_3=2, \end{cases} \quad \text{т.е.} \quad \begin{cases} x_1=1-x_3\underset{\text{mod}3}{=}1+2x_3, \\ x_2=2-2x_3\underset{\text{mod}3}{=}2+x_3. \end{cases}$$

Таблица 4.1

Многообразие решений неоднородной системы в $\mathbf{Z}_3$

x_1	1	0	2
x_2	2	1	0
x_3	0	1	2

Придадим свободной переменной x_3 все возможные значения в поле вычетов $\mathbf{Z}_3$ и получим многообразие из трех решений неоднородной системы (столбцы таблицы 4.1).

Приведем некоторые подробности вычислений, результаты которых зафиксированы в этой таблице: для x_3=1 значения x_1=1+2·1=3≡0, x_2=2+1=3≡0; для x_3=2 значения x_1=1+2·2=5≡2, x_2=2+2=4≡1 (все сравнения по mod 3).

Сформируем матрицу M, столбцы которой суть найденные решения: $M=\begin{pmatrix}1&0&2\\2&0&1\\0&1&2\end{pmatrix}$. Произведение $A\cdot M=\begin{pmatrix}2&2&0\\1&2&2\end{pmatrix}\cdot\begin{pmatrix}1&0&2\\2&0&1\\0&1&2\end{pmatrix}=\begin{pmatrix}6&0&6\\5&2&8\end{pmatrix}\underset{\text{mod }3}{\equiv}\begin{pmatrix}0&0&0\\2&2&2\end{pmatrix}$ – повторенный 3 раза столбец свободных членов заданной системы уравнений.

Р 4.2.6. Построить систему линейных уравнений над полем $\mathbf{Z}_3$, многообразие решений которой задается таблицей 4.1.

Решение. Обозначим M_0, M_1, M_2 столбцы матрицы M из задачи **Р 4.2.5**, соответствующие значениям свободной переменной x_3=0,1,2 и найдем разности

$$M_1-M_0=\begin{pmatrix}0\\0\\1\end{pmatrix}-\begin{pmatrix}1\\2\\0\end{pmatrix}=\begin{pmatrix}-1\\-2\\1\end{pmatrix}\underset{\text{mod }3}{\equiv}\begin{pmatrix}2\\1\\1\end{pmatrix}\text{ и }M_2-M_0=\begin{pmatrix}2\\1\\2\end{pmatrix}-\begin{pmatrix}1\\2\\0\end{pmatrix}=\begin{pmatrix}1\\-1\\2\end{pmatrix}\underset{\text{mod }3}{\equiv}\begin{pmatrix}1\\2\\2\end{pmatrix}.$$

Легко видеть, что 2·(M_1– M_0)≡(M_2– M_0) (mod 3), т.е. столбцы матрицы M линейно зависимы над полем вычетов $\mathbf{Z}_3$. К этому выводу можно придти также, вычислив определитель det(M)=3≡0 (mod 3) или непосредственно заметить, что M_0+M_1+M_2≡0 (mod 3).

Построим систему однородных уравнений, определяющую линейную оболочку $L(M_1–M_0)$: {x_1–2x_3=0, x_2–x_3=0}. Перейдем в поле вычетов $\mathbf{Z}_3$, получим {x_1+x_3=0, x_2+2x_3=0}. Эта система задает одномерное *направляющее пространство* нашего многообразия. Чтобы получить свободные члены неоднородной системы, задающей многообразие, подставим в левые части уравнений компоненты любого из векторов многообразия, например M_1. Получится 0+1=1, 0+2·1=2. Окончательно система уравнений {x_1+x_3=1, x_2+2x_3=2}.

Замечание. Построенная система отличается от предложенной в задаче **Р 4.2.5**, решением которой было наше многообразие. Однако эти системы эквивалентны (см. ниже задачу **С 4.2.6**).

Р 4.2.7. Построить многочлен f над полем вычетов $\mathbf{Z}_5$, принимающий заданные значения: $f(0)=4$, $f(1)=3$, $f(2)=2$, $f(4)=1$.

Решение 1. Применим метод неопределенных коэффициентов. Задано 4 значения многочлена, его степень не превосходит 3, $f(x)=ax^3+bx^2+cx+d$. Подставив заданные значения, получим систему уравнений (*) с целыми коэффициентами. Переведя коэффициенты в поле вычетов $\mathbf{Z}_5$, получим систему (**).

$$\begin{cases} f(0) = d = 4, \\ f(1) = a + b + c + d = 3, \\ f(2) = 8a + 4b + 2c + d = 2, \\ f(4) = 64a + 16b + 4c + d = 1. \end{cases} \quad (*) \qquad \begin{cases} f(0) = d = 4, \\ f(1) = a + b + c + d = 3, \\ f(2) = 3a + 4b + 2c + d = 2, \\ f(4) = 4a + b + 4c + d = 1. \end{cases}$$

Решив эту систему любым способом, найдем $a=4$, $b=3$, $c=2$, $d=4$. Искомый многочлен равен $f(x)=4x^3+3x^2+2x+4$.

Решение 2. Применим интерполяционную формулу Лагранжа, пока над полем рациональных чисел $\mathbf{Q}$:

$$4\cdot\frac{(x-1)\cdot(x-2)\cdot(x-4)}{(0-1)\cdot(0-2)\cdot(0-4)}+3\cdot\frac{(x-0)\cdot(x-2)\cdot(x-4)}{(1-0)\cdot(1-2)\cdot(1-4)}+2\cdot\frac{(x-0)\cdot(x-1)\cdot(x-4)}{(2-0)\cdot(2-1)\cdot(2-4)}+1\cdot\frac{(x-0)\cdot(x-1)\cdot(x-2)}{(4-0)\cdot(4-1)\cdot(4-2)}.$$

Раскрыв скобки и приведя подобные члены, получим многочлен с рациональными коэффициентами $\frac{1}{24}\cdot(x^3-3x^2-22x+96)$. Легко видеть, что $24^{-1}=4$ в поле $\mathbf{Z}_5$, так как $24\cdot4=96\equiv1$. Дальнейшие вычисления в этом поле приведут к тому же многочлену.

Р 4.2.8. Над полем GF(2^2) (таблица 3.5' на стр.85) решить систему линейных уравнений $\{x+\alpha y=\beta,\ \alpha x+\beta y=1\}$.

Решение. Сначала попробуем правило Крамера, определители будем вычислять с помощью таблиц сложения и умножения в поле Галуа и правил арифметики вычетов в $\mathbf{Z}_2$.

$$\Delta=\begin{vmatrix}1 & \alpha\\ \alpha & \beta\end{vmatrix}=\beta-\alpha^2=\beta-\beta=0,\ \Delta_x=\begin{vmatrix}\beta & \alpha\\ 1 & \beta\end{vmatrix}=\beta^2-\alpha=\alpha-\alpha=0,\Delta_y=\begin{vmatrix}1 & \beta\\ \alpha & 1\end{vmatrix}=1-\beta\alpha=1-1=0.$$

Вывод: система имеет многообразие решений, но таким путем его не найти.

Преобразуем систему методом Гаусса:

$$\left[\begin{array}{cc|c} 1 & \alpha & \beta \\ \alpha & \beta & 1 \end{array}\right] \underset{(2)+\alpha\cdot(1)}{\rightarrow} \left[\begin{array}{cc|c} 1 & \alpha & \beta \\ 0 & 0 & 0 \end{array}\right] \rightarrow \left[\begin{array}{cc|c} 1 & \alpha & \beta \end{array}\right]$$

– осталось одно уравнение $x+\alpha y=\beta$, запишем его в виде $x=\beta-\alpha y=\beta+\alpha y$. Придадим переменной y все четыре возможных значения, найдем соответствующие значения x и получим многообразие решений, представленное столбцами таблицы 4.2.

Таблица 4.2

Многообразие решений неоднородной системы в $GF(2^2)$

Задачи для самостоятельного решения

С 4.2.1. Решите над полями вычетов $\mathbf{Z}_5$ и $\mathbf{Z}_7$ систему линейных уравнений

$\{3x+y+2z=1,\ x+2y+3z=1,\ 4x+3y+2z=1\}$ (Проскуряков. 1757).

Ответ: над $\mathbf{Z}_5$ система несовместна; над $\mathbf{Z}_7$ решение (2,6,5).

С 4.2.2. Решите над полями вычетов $\mathbf{Z}_3$ и $\mathbf{Z}_5$ систему линейных уравнений

$\{x+2y+2z=1,\ 2x+y+2z=2,\ 2x+2y+z=2\}$

Ответ: над $\mathbf{Z}_3$ (и над $\mathbf{Q}$) решение (1,0,0);

над $\mathbf{Z}_5$ многообразие решений $x=1+z$, $y=z$.

С 4.2.3. Решите над полями вычетов $\mathbf{Z}_5$ и $\mathbf{Z}_7$ систему линейных уравнений

$\{3x+2y=1,\ 3x+2y+z=2,\ x+3y+4z=3\}$

Ответ: над $\mathbf{Z}_5$ решение (0,3,1), над $\mathbf{Z}_7$ система несовместна.

С 4.2.4. Постройте многочлены над полем вычетов $\mathbf{Z}_5$, принимающие заданные значения.

1) $f(x)=ax^2+bx+c$, $f(0)=1$, $f(2)=1$, $f(4)=0$.

2) $g(x)=ax^3+bx^2+cx+d$, $g(0)=0$, $g(1)=1$, $g(2)=2$, $g(3)=4$.

Ответ: 1) $f(x)=2x^2+x+1$; 2) $g(x)=x^3+2x^2+3x$.

С 4.2.5. Приведите к каноническому виду квадратичную форму $x_1 \cdot x_2$ над полем вычетов $\mathbf{Z}_3$.

Ответ (не единственный): $(x_1')^2+2(x_2')^2$, где $\{x_1=x_1'+x_2',\ x_2=x_1'+2x_2'\}$.

С 4.2.6. Докажите эквивалентность над полем $\mathbf{Z}_3$ систем линейных уравнений $\{2x_1+2x_2=0,\ x_1+2x_2+2x_3=2\}$ (из задачи **Р 4.2.5**) и $\{x_1+x_3=1,\ x_2+2x_3=2\}$ (из задачи **Р 4.2.6**).

С 4.2.7. Решите над полем $GF(2^2)$ систему линейных уравнений

$$\{\alpha x+y=\alpha,\ \beta x+y=\beta\}.$$

Ответ: единственное решение (1,0).

4.3. Многочлены над полем вычетов

Основы теории

Многочлены в алгебре рассматриваются в двух аспектах.

Во-первых – как функции вещественного или комплексного переменного вида $y=f(x)=a_0\cdot x^n+a_1\cdot x^{n-1}+\ldots+a_{n-1}\cdot x+a_n$. В этом случае главная задача – нахождение *корней*, т.е. значений переменной x, при которых значение $y=f(x)=0$.

Во-вторых – как формальные выражения вида $a_0\cdot x^n+a_1\cdot x^{n-1}+\ldots+a_{n-1}\cdot x+a_n$, которые образуют кольцо относительно обычных операций. Кроме этих операций представляет интерес деление с остатком и разложение на множители. При этом обычно не возникает вопрос о том, какие значения принимают соответствующие функции.

В числовом поле или кольце между этими двумя точками зрения нет противоречия, поскольку любой функции-многочлену соответствует единственный многочлен-выражение (с точностью до перестановки слагаемых и других невинных преобразований).

Для многочленов над полями вычетов $\mathbf{Z}_p$, ситуация принципиально иная. Так, в поле $\mathbf{Z}_2$ выражение x^n *при любом* $n\geq 1$ задает одну и ту же функцию, значения которой $f(0)=0$, $f(1)=1$. А кроме 0 и 1 в этом поле ничего и нет… В этом поле выражение x^2+x задает функцию, которая тождественно (в этом поле) равна нулю. Выражения x^3+x^2+x+1 и x^3+1 задают одну и ту же функцию, значения которой $f(0)=1$, $f(1)=0$. Такие же «чудеса» происходят и в других полях вычетов, естественно, с другими многочленами (см. ниже задачу **С 4.3.4**).

Несмотря на такую сложную ситуацию с многочленами-функциями, можно ставить (и решать) задачи о корнях многочленов и о разложении многочлена на неприводимые множители в полях вычетов $\mathbf{Z}_p$ (см. ниже задачи **Р 4.3.1-3** и **С 4.3.1-10**). В принципе задачи о корнях решаются перебором, поскольку в поле $\mathbf{Z}_p$ имеется лишь p различных элементов. Простейший вид задач о корнях – *двучленные сравнения*, имеющие вид $x^n \equiv a \pmod p$. Для $p=2$ и для $a=0$ задача тривиальна, для $p>2$ существует достаточно развитая теория. Мы ограничимся случаем $n=2$. При $a\neq 0$ возможны два случая: сравнение имеет два решения и сравнение не имеет решений. В первом случае a называется *квадратичным вычетом*, во втором – *квадратичным невычетом*. Конечное поле $\mathbf{Z}_p$ имеет $p-1$ ненулевых элементов, из них половина являются квадратичными вычетами, половина – невычетами. Известен довольно простой критерий: если $a\neq 0$ и простое число $p>2$ не является делителем числа a, то $a\in\mathbf{Z}_p$ является квадратичным вычетом тогда и только тогда, когда верно сравнение $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Основными задачами о многочленах (при формальной точке зрения), являются нахождение наибольшего общего делителя и коэффициентов Безу, а также разложение на неприводимые множители.

Наибольший общий делитель многочленов над полем $\mathbf{Z}_p$ ищется так же, как над числовым полем (например, $\mathbf{Q}$) с помощью алгоритма Евклида (см. ниже задачи **Р 4.3.4** и **С 4.3.11**). Никаких принципиальных сложностей здесь не возникает, хотя результаты могут зависеть от рассматриваемого поля. Возьмем, например, два многочлена над некоторым полем $\mathbf{Z}_p$, пусть они взаимно просты. Рассмотрим их как многочлены с целыми коэффициентами – они также будут взаимно просты над полем $\mathbf{Q}$ (Проскуряков, 1761). Обратное утверждение неверно, т.е. многочлены, взаимно простые над полем $\mathbf{Q}$, *не обязательно* взаимно просты над $\mathbf{Z}_p$ (см. см. ниже задачу **Р 4.3.4**).

Возьмем многочлен с целыми коэффициентами, приводимый над полем рациональных чисел $\mathbf{Q}$. Заменив его коэффициенты соответствующими вычетами

по модулю p, получим многочлен над полем $\mathbf{Z}_p$, который также приводим (Проскуряков, 1771). Впрочем, это утверждение может оказаться неверным, если старший коэффициент многочлена делится на модуль сравнения p – в этом случае при переходе в $\mathbf{Z}_p$ степень многочлена уменьшается (см. см. ниже задачу **Р 4.3.5**).

Напротив, существуют многочлены, неприводимые над полем $\mathbf{Q}$, но приводимые *над любым полем* $\mathbf{Z}_p$ (в задаче **Р 4.3.3** рассмотрены случаи p=2 и p=3).

Решение задач

Р 4.3.1. Решить сравнение $x^2 \equiv 3 \pmod{11}$.

Решение. 1) Применим критерий: $3^5=243\equiv 1 \pmod{11}$, число 3 является квадратичным вычетом. Значения x найдем перебором: $1^2=1$, $2^2=4$, $3^2=9$, $4^2=16\equiv 5$, $5^2=25\equiv 3$, $6^2=36\equiv 3$, найдено два решения $x_1=5$ и $x_2=6$, перебор можно прекратить.

Р 4.3.2. Решить квадратичное сравнение $x^2+3x+2\equiv 0 \pmod{5}$.

Решение. Выделим полный квадрат. Поскольку коэффициент при x нечетный, предварительно прибавим к нему 5: $x^2+8x+2\equiv 0 \Rightarrow (x+4)^2\equiv 16-2=14\equiv 4$. Обозначим $y=x+4$ и получим $y^2\equiv 4$, откуда $y\equiv\pm 2$. Получили два решения: $y_1=2$, $y_2=-2$, соответственно $x_1=2-4=-2\equiv 3$, $x_2=-2-4=-6\equiv 4$.

Проверка: $x_1=3$, $3^2+3\cdot 3+2=20\equiv 0$; $x_2=4$, $4^2+3\cdot 4+2=30\equiv 0$.

Р 4.3.3. Разложить на неприводимые множители над полями $\mathbf{Z}_2$ и $\mathbf{Z}_3$ многочлен x^4+1.

Решение. Над полем $\mathbf{Z}_2$ ответ очевиден: $x^4+1\equiv(x+1)^4$.

В случае поля $\mathbf{Z}_3$ множителей степени 1 нет, поскольку в этом поле у нашего многочлена нет корней (проверьте). Для отыскания множителей степени 2 применим метод неопределенных коэффициентов. Без ограничения общности можно считать, что многочлены-сомножители являются приведенными, т.е. имеют старшие коэффициенты, равные 1.

Тогда $x^4+1=(x^2+a_1\cdot x+b_1)\cdot(x^2+a_2\cdot x+b_2)$.

Отсюда $b_1\cdot b_2=1$. В $\mathbf{Z}_3$ возможны два варианта: $b_1=b_2=1$ и $b_1=b_2=2$.

В первом случае

$$x^4+1=(x^2+a_1\cdot x+1)\cdot(x^2+a_2\cdot x+1)=x^4+(a_1+a_2)\cdot x^3+(a_1\cdot a_2+2)\cdot x^2+(a_1+a_2)\cdot x+1.$$

Для неопределенных коэффициентов получились два уравнения: $a_1+a_2=0$ и $a_1\cdot a_2+2=0$. Из первого имеем $a_2=-a_1\equiv 2\cdot a_1$, из второго $a_1\cdot 2\cdot a_1+2=0$, $a_1^2+1=0$, $a_1^2=-1\equiv 2$. Даже без применения критерия квадратичного вычета видим, что ни одно из возможных значений коэффициента a_1 не удовлетворяет этому уравнению, первый случай невозможен.

Во втором случае

$$x^4+1=(x^2+a_1\cdot x+2)\cdot(x^2+a_2\cdot x+2)=x^4+(a_1+a_2)\cdot x^3+(a_1\cdot a_2+4)\cdot x^2+(2\cdot a_1+2\cdot a_2)\cdot x+4\equiv$$
$$\equiv x^4+(a_1+a_2)\cdot x^3+(a_1\cdot a_2+1)\cdot x^2+2\cdot(a_1+a_2)\cdot x+1.$$

Как в первом случае, $a_1+a_2=0$ и $a_1\cdot a_2+2=0$. Далее $a_2=-a_1\equiv 2\cdot a_1$, $a_1\cdot 2\cdot a_1+1=0$, $2\cdot a_1^2+1=0$, $2\cdot a_1^2=-1\equiv 2$, $a_1^2=1$, откуда получаем два решения: $a_1=1$ и $a_1=-1\equiv 2$. Соответствующие значения $a_2=2$ и $a_2=1$.

Разложение многочлена над полем $\mathbf{Z}_3$: $x^4+1=(x^2+x+2)\cdot(x^2+2\cdot x+2)$.

Р 4.3.4. Найти наибольший общий делитель и коэффициенты Безу для многочленов $f=x^3+x^2+2x+2$ и $g=x^2+x+1$ (Проскуряков, 1758)

1) над полем рациональных чисел $\mathbf{Q}$,

2) над полем вычетов $\mathbf{Z}_3$.

$$\begin{array}{lll} f=x^3+x^2+2x+2 & x^2+x+1=g & f=g\cdot q_1+r_1 \\ \hline x^3+x^2+x & x=q_1 & r_1=f-g\cdot q_1 \\ \hline x+2=r_1 & & \end{array}$$

$$\begin{array}{lll} g=x^2+x+1 & x+2=r_1 & g=r_1\cdot q_1+r_2 \end{array}$$

Решение. 1) Выполним алгоритм Евклида:

Соберем полученные результаты:

$$3=d=g-r_1\cdot q_2=g-(f-g\cdot q_1)\cdot q_2=g\cdot(1+q_1\cdot q_2)-f\cdot q_2=g\cdot(1+x\cdot(x-1))-f\cdot(x-1)=g\cdot(x^2-x+1)-f\cdot(x-1).$$

Замечание. Многочлены f и g взаимно просты, их наибольший общий делитель равен 1. Чтобы коэффициенты Безу оставались целочисленными, мы взяли d=3. При необходимости сделать d=1, его линейное выражение через f и g надо разделить на 3.

Решение. 2) Выполним алгоритм Евклида, учитывая особенности

$f=x^3+x^2+2x+2$ $\quad x^2+x+1=g$ $\quad f=g\cdot q_1+r_1$

x^3+x^2+x $\quad x=q_1$ $\quad r_1=f-g\cdot q_1\equiv f+2\cdot g\cdot q_1$

$x+2=r_1$

$g=x^2+x+1$ $\quad x+2=r_1$ $\quad g=r_1\cdot q_1+r_2$

арифметических операций в поле $\mathbf{Z}_3$ (–1≡2, 4≡1):

Соберем полученные результаты: $x+2=d=r_1\equiv f+2\cdot g\cdot q_1=1\cdot f+2x\cdot g$.

Наибольший общий делитель равен x+2, коэффициенты Безу 1 и 2·x.

Сделаем проверку: $1\cdot f+2x\cdot g=(x^3+x^2+2x+2)+2x\cdot(x^2+x+1)=3x^3+3x^2+4x+2\equiv x+2$.

Р 4.3.5. Показать, что многочлен $p\cdot x^2+(p+1)\cdot x+1$ приводим над полем рациональных чисел $\mathbf{Q}$, но неприводим над полем вычетов $\mathbf{Z}_p$.

Решение. Выполним преобразования над полем $\mathbf{Q}$ (фактически над кольцом $\mathbf{Z}$): $p\cdot x^2+(p+1)\cdot x+1=p\cdot x^2+p\cdot x+x+1=p\cdot x\cdot(x+1)+(x+1)=(p\cdot x+1)\cdot(x+1)$ – многочлен приводим.

Перейдем в поле вычетов $\mathbf{Z}_p$: $p\cdot x^2+(p+1)\cdot x+1\equiv(p+1)\cdot x+1\equiv x+1 \pmod p$. Этот многочлен неприводим (его степень равна 1, некуда дальше приводить…).

Задачи для самостоятельного решения

С 4.3.1. Решите сравнение (или докажите, что решение не существует).

1) $x^2+1\equiv 0 \pmod{13}$. 2) $x^2+1\equiv 0 \pmod{11}$.

Указание. Примените условие квадратичного вычета.

С 4.3.2. Решите сравнение $2x^2+3x+1\equiv 0 \pmod 5$.

Указание. До выделения полного квадрата умножьте сравнение на $2^{-1}\equiv 3$.

С 4.3.3. Какие ненулевые элементы полей $\mathbf{Z}_5$ и $\mathbf{Z}_7$ являются квадратичными вычетами по соответствующему модулю, а какие – невычетами? Укажите значения квадратных корней из квадратичных вычетов (два значения для каждого квадратичного вычета).

С 4.3.4. Найдите (подберите, сконструируйте) многочлен $f(x)$ над полем $\mathbf{Z}_3$, не все коэффициенты которого нули, но обращающийся в нуль при всех $x \in \mathbf{Z}_3$.

Указание. Степень этого многочлена не может быть меньше трех.

С 4.3.5. Разложите на неприводимые множители над полем $\mathbf{Z}_2$ многочлен $x^5+x^3+x^2+1$ (Проскуряков, 1763).

С 4.3.6. Разложите на неприводимые множители над полем $\mathbf{Z}_5$ многочлен $x^3+2\cdot x^2+4\cdot x+1$ (Проскуряков, 1764).

Указание. Подбором найдите корень многочлена в этом поле.

С 4.3.7. Разложите на неприводимые множители над полем $\mathbf{Z}_5$ многочлен $x^4+3x^3+2x^2+x+4$ (Проскуряков, 1766).

С 4.3.8. Найдите все многочлены третьей степени со старшим коэффициентом 1, неприводимые множители над полем $\mathbf{Z}_3$. (Проскуряков, 1770).

Указание. Не очень творческий, но надежный способ: перебрать все 9 многочленов вида $x^2+a\cdot x+b$, где $a,b=0,1,2$.

С 4.3.9. Найдите наибольший общий делитель и коэффициенты Безу для многочленов $f=x^4+1$ и $g=x^3+x+1$ (Проскуряков, 1760).

1) над полем рациональных чисел $\mathbf{Q}$,

2) над полем вычетов $\mathbf{Z}_3$,

3) над полем вычетов $\mathbf{Z}_5$.

5. КОНТРОЛЬНЫЕ РАБОТЫ

5.1. Факторизация групп

1. Докажите, что множество G с указанной операцией является группой.
2. Докажите, что подмножество $H \subset G$ является подгруппой.
3. Докажите, что подмножество H является нормальным делителем в G.
4. Опишите классы факторгруппы $\boldsymbol{G/H}$ и операцию в ней.
5. Опишите гомоморфизм группы $\boldsymbol{G}$ на факторгруппу G/H.
6. Какой группе изоморфна факторгруппа G/H?

   (Последний вопрос не всегда имеет конкретный ответ)

Ниже приводится 30 вариантов контрольной работы.

1. G – комплексные числа, не равные нулю, операция – умножение.

   H – комплексные числа с модулем, равным 1.

2. G – комплексные числа, не равные нулю, операция – умножение.

   H – вещественные числа, не равные нулю.

3. G – комплексные числа, не равные нулю, операция – умножение.

   H – комплексные числа с аргументами вида $2\pi k/6$.

4. G – комплексные числа с аргументами вида $2\pi k/6$, операция – умножение.

   H – корни степени 6 из единицы.

5. $G = \boldsymbol{Z}^{2\times 2}$ – целочисленные матрицы порядка 2, операция – сложение.

   H – матрицы вида $\begin{bmatrix} a & 0 \\ 2c & d \end{bmatrix}$, где

   $a, b, c, d \in \boldsymbol{Z}$.

6. $G = \boldsymbol{Z}^{2\times 2}$ – целочисленные матрицы порядка 2, операция – сложение.

   H – матрицы вида $\begin{bmatrix} a & 3b \\ 2c & 2d \end{bmatrix}$, где

   $a, b, c, d \in \boldsymbol{Z}$.

7. $G = \boldsymbol{Z}^{2\times 2}$ – целочисленные матрицы порядка 2, операция – сложение.

   H – матрицы вида $\begin{bmatrix} 3a & b \\ 2c & d \end{bmatrix}$, где

   $a, b, c, d \in \boldsymbol{Z}$.

8. $G = \boldsymbol{Z}^{2\times 2}$ – целочисленные матрицы порядка 2, операция – сложение.

   H – матрицы вида $\begin{bmatrix} a & 2b \\ 2c & 2d \end{bmatrix}$, где

   $a, b, c, d \in \boldsymbol{Z}$.

9. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

10. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} a & 2b \\ 2c & d \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

11. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} 4a & 2b \\ c & 0 \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

12. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} a & b \\ c & 2d \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

13. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} a & b \\ 2c & 4d \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

14. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} 3a & b \\ c & d \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

15. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} 3a & 2b \\ c & 0 \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

16. $G = \mathbf{Z}^{2\times2}$ – целочисленные матрицы порядка 2, операция – сложение.

H – матрицы вида $\begin{bmatrix} a & 2b \\ 3c & d \end{bmatrix}$, где

$a, b, c, d \in \mathbf{Z}$.

17. G – комплексные невырожденные матрицы, операция – умножение.

H – унимодулярные матрицы (их определители равны ±1).

18. G – вещественные невырожденные матрицы, операция – умножение.

H – унимодулярные матрицы (их определители равны ±1).

19. G – вещественные невырожденные матрицы, операция – умножение.

H – матрицы с положительным определителем.

20. G – комплексные невырожденные матрицы, операция – умножение.

H – матрицы с положительным определителем.

21. G – вещественные матрицы с

22. G – комплексные невырожденные

положительным определителем, операция – умножение.

H – матрицы с определителем, равным 1.

матрицы, операция – умножение.

H – матрицы, у которых модуль определителя равен 1.

23. *G* – невырожденные треугольные матрицы вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, операция – умножение.

H – матрицы, у которых $a \cdot c = 1$.

24. *G* – невырожденные треугольные матрицы вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, операция – умножение.

H – матрицы, у которых $a = c = 1$.

---

25. *G* – невырожденные треугольные матрицы вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, операция – умножение.

H – матрицы, у которых $a \cdot c = \pm 1$.

26. *G* – невырожденные треугольные матрицы вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, операция – умножение.

H – матрицы, у которых $a \cdot c > 0$.

27. *G* – трехкомпонентные арифметические векторы, операция – сложение.

H – векторы, у которых сумма компонент равна 0.

28. *G* – комплексные числа, операция – сложение.

H – вещественные числа.

---

29. *G* – целочисленные векторы вида (x, y), операция – сложение.

H – векторы вида $(3x, 4y)$.

30. *G* – комплексные числа с модулем равным 1, операция – умножение

H – корни степени 6 из единицы.

5.2. Факторизация колец

1. Докажите, что множество *R* является кольцом (операции подразумеваются).
2. Докажите, что подмножество $I \subset R$ является подкольцом.
3. Докажите, что подмножество *I* является идеалом в *R*.
4. Опишите классы факторкольца ***R/I*** и операции в нем.
5. Опишите гомоморфизм кольца ***R*** на факторкольцо *R/I*.
6. Имеются ли в кольце *R* и в факторкольце *R/I* делители нуля?
7. Является ли факторкольцо *R/I* полем?

8. Какому кольцу изоморфно факторкольцо R/I?
(Последний вопрос не всегда имеет конкретный ответ)

Ниже приводится 30 вариантов контрольной работы.

1. $R = \mathbf{Z}[i]$ – целые комплексные числа.
$I = 2\cdot\mathbf{Z}[i]$.

2. $R = \mathbf{Z}[i]$ – целые комплексные числа.
$I = (1+i)\cdot\mathbf{Z}[i]$.

3. $R = \mathbf{Z}[i]$ – целые комплексные числа.
$I = 2i\cdot\mathbf{Z}[i]$.

4. R – функции вида $y=f(x)$, $x,y\in\mathbf{R}$.
$I = \{y=h(x) \mid h(0)=0\}$.

5. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^3+1)\cdot\mathbf{Z}[x]$.

6. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^3+x^2+x+1)\cdot\mathbf{Z}[x]$.

7. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^2+2)\cdot\mathbf{Z}[x]$.

8. $R = \mathbf{Q}[x]$ – многочлены с рациональными коэффициентами.
$I = (x^2-4)\cdot\mathbf{Q}[x]$.

9. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^2+x-1)\cdot\mathbf{Z}[x]$.

10. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^2-2x+2)\cdot\mathbf{Z}[x]$.

11. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^2-2x+1)\cdot\mathbf{Z}[x]$.

12. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^2-x-1)\cdot\mathbf{Z}[x]$.

13. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^3+2x+2)\cdot\mathbf{Z}[x]$.

14. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^3+2x^2+2x+2)\cdot\mathbf{Z}[x]$.

15. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^3+2x^2+2x)\cdot\mathbf{Z}[x]$.

16. $R = \mathbf{Z}[x]$ – многочлены с целыми коэффициентами.
$I = (x^3+2x^2)\cdot\mathbf{Z}[x]$.

17. $R = \mathbf{Z}_2[x]$ – многочлены с коэффициентами из поля вычетов $\mathbf{Z}_2$.

18. $R = \mathbf{Z}_2[x]$ – многочлены с коэффициентами из поля вычетов $\mathbf{Z}_2$.

$I = (x^2+1)\cdot\mathbf{Z}_2[x]$.

19. $R = \mathbf{Z}_2[x]$ – многочлены с коэффициентами из поля вычетов $\mathbf{Z}_2$.

$I = (x^2+x+1)\cdot\mathbf{Z}_2[x]$.

20. $R \subset \mathbf{Z}[i]$ – целые комплексные числа вида $2a+bi$, где $a,b\in\mathbf{Z}$.

$I = 2\cdot R$.

$I = (x^2+x)\cdot\mathbf{Z}_2[x]$.

21. R – матрицы вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$.

I – матрицы при $a=0$.

22. R – матрицы вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$.

I – матрицы при $c=0$.

23. R – числа вида $a+b\sqrt{2}$, где $a,b\in\mathbf{Z}$.

$I = 2\cdot R$.

24. R – числа вида $a+b\sqrt{3}$, где $a,b\in\mathbf{Z}$.

$I = 2\cdot R$.

25. R – числа вида $2a+b\sqrt{2}$, где $a,b\in\mathbf{Z}$.

$I = 2\cdot R$.

26. R – числа вида $3a+b\sqrt{3}$, где $a,b\in\mathbf{Z}$.

$I = 2\cdot R$.

27. $R = \mathbf{Z}^2$. Операции – покомпонентное сложение и умножение.

$I = 2\cdot\mathbf{Z}^2$.

28. $R = \mathbf{Z}[i]$ – целые комплексные числа.

$I = 3\cdot\mathbf{Z}[i]$.

29. R – матрицы вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, где $a,b\in\mathbf{Z}$.

$I = 2\cdot R$.

30. R – матрицы вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $a,b\in\mathbf{Z}$.

$I = 2\cdot R$.

5.3. Многочлены над полем вычетов

Для многочленов $f(x)$ и $g(x)$ над каждым из полей вычетов $\mathbf{Z}_3$, $\mathbf{Z}_5$ найдите наибольший общий делитель $d(x)$ и коэффициенты Безу $u(x)$ и $v(x)$. Старший коэффициент многочлена $d(x)$ должен быть равен 1. Если в задании присутствует коэффициент –1, предварительно приведите его в поле вычетов, используя сравнения $-1\equiv 2 \pmod 3$ и $-1\equiv 4 \pmod 5$.

Ниже приводится 30 вариантов контрольной работы.

1. $f=x^5+x^4+1$, $g=x^4+x^2+1$
2. $f=x^5+x^3+x+1$, $g=x^4+1$
3. $f=x^5+x+1$, $g=x^4+x^3+1$
4. $f=x^5+x^3+x$, $g=x^4+x+1$
5. $f=x^5+x^4+1$, $g=x^3+x^2+1$
6. $f=x^4+1$, $g= x^5+x^4+x^2+1$
7. $f=x^5-x^4+1$, $g= x^3+x^2+1$
8. $f=x^5+x^4+1$, $g=x^3-x^2+1$
9. $f=x^5-x^4+1$, $g= x^3+x^2-1$
10. $f=x^5-x^4+1$, $g=x^3-x^2+1$
11. $f=x^5-x+1$, $g= x^4+x^3+1$
12. $f=x^5+x+1$, $g=x^4+x^3-1$
13. $f=x^5-x-1$, $g= x^4+x^3+1$
14. $f=x^5+x+1$, $g= -x^4+x^3-1$
15. $f=x^5+x-1$, $g= x^4+x^3-1$
16. $f=x^5-x-1$, $g=x^4+x^3-1$
17. $f=x^5+x^4+1$, $g= x^4+x^2+1$
18. $f=x^5+x^3+x+1$, $g=x^4+2$
19. $f=x^5+x+1$, $g= x^4+x^3+1$
20. $f=x^5+x^3+x$, $g=x^4+x+1$
21. $f=x^5+x^4+1$, $g= x^3+x^2+1$
22. $f=x^4-1$, $g=x^5+x^4+x^2+1$
23. $f=x^5-x^4+1$, $g= x^3+x^2+1$
24. $f=x^5+x^4+1$, $g=x^3-x^2+1$
25. $f=x^5-x+1$, $g= x^4+x^3+1$
26. $f=x^5+x^3+x$, $g=x^3-x^2+1$
27. $f=x^5+x^4+1$, $g= x^3+x^2-1$
28. $f=x^4+1$, $g= x^5+x^4+x^2-1$
29. $f=x^5-x^4+1$, $g= x^3+x^2+1$
30. $f=x^5+x^4+1$, $g= x^4-x^2+1$

5.4. Линейная алгебра над полем вычетов

Найдите пространство решений системы $\boldsymbol{Ax=0}$ и многообразие решений системы $\boldsymbol{Ax=b}$ над полями вычетов $\boldsymbol{Z}_3$ и $\boldsymbol{Z}_5$.

Ниже приводится 30 вариантов контрольной работы.

1. $A=\begin{bmatrix}1&2&2\\2&2&2\end{bmatrix}$ $b=\begin{bmatrix}1\\1\end{bmatrix}$
2. $A=\begin{bmatrix}2&2&1\\2&1&2\end{bmatrix}$ $b=\begin{bmatrix}1\\2\end{bmatrix}$
3. $A=\begin{bmatrix}2&2&2\\2&1&0\end{bmatrix}$ $b=\begin{bmatrix}1\\0\end{bmatrix}$
4. $A=\begin{bmatrix}1&1&1\\1&0&1\end{bmatrix}$ $b=\begin{bmatrix}0\\2\end{bmatrix}$
5. $A=\begin{bmatrix}0&1&1\\1&1&0\end{bmatrix}$ $b=\begin{bmatrix}2\\2\end{bmatrix}$
6. $A=\begin{bmatrix}1&2&1\\2&2&0\end{bmatrix}$ $b=\begin{bmatrix}1\\1\end{bmatrix}$
7. $A=\begin{bmatrix}2&2&2\\2&1&2\end{bmatrix}$ $b=\begin{bmatrix}2\\0\end{bmatrix}$
8. $A=\begin{bmatrix}0&1&2\\1&1&1\end{bmatrix}$ $b=\begin{bmatrix}2\\2\end{bmatrix}$

9. $A=\begin{bmatrix}2&1&1\\2&0&1\end{bmatrix}$ $b=\begin{bmatrix}1\\2\end{bmatrix}$

10. $A=\begin{bmatrix}0&2&1\\2&1&2\end{bmatrix}$ $b=\begin{bmatrix}2\\0\end{bmatrix}$

11. $A=\begin{bmatrix}2&2&1\\2&1&0\end{bmatrix}$ $b=\begin{bmatrix}1\\0\end{bmatrix}$

12. $A=\begin{bmatrix}2&0&2\\2&2&1\end{bmatrix}$ $b=\begin{bmatrix}2\\1\end{bmatrix}$

13. $A=\begin{bmatrix}1&2&0\\0&2&1\end{bmatrix}$ $b=\begin{bmatrix}1\\1\end{bmatrix}$

14. $A=\begin{bmatrix}2&0&1\\0&1&1\end{bmatrix}$ $b=\begin{bmatrix}0\\1\end{bmatrix}$

15. $A=\begin{bmatrix}0&1&1\\1&1&1\end{bmatrix}$ $b=\begin{bmatrix}1\\2\end{bmatrix}$

16. $A=\begin{bmatrix}0&2&1\\1&1&1\end{bmatrix}$ $b=\begin{bmatrix}1\\0\end{bmatrix}$

17. $A=\begin{bmatrix}0&1&1\\2&2&2\end{bmatrix}$ $b=\begin{bmatrix}0\\2\end{bmatrix}$

18. $A=\begin{bmatrix}0&1&2\\2&1&0\end{bmatrix}$ $b=\begin{bmatrix}1\\1\end{bmatrix}$

19. $A=\begin{bmatrix}1&0&1\\1&1&2\end{bmatrix}$ $b=\begin{bmatrix}1\\2\end{bmatrix}$

20. $A=\begin{bmatrix}0&2&2\\2&1&2\end{bmatrix}$ $b=\begin{bmatrix}2\\0\end{bmatrix}$

21. $A=\begin{bmatrix}1&0&1\\2&1&1\end{bmatrix}$ $b=\begin{bmatrix}0\\2\end{bmatrix}$

22. $A=\begin{bmatrix}1&0&2\\1&1&0\end{bmatrix}$ $b=\begin{bmatrix}1\\1\end{bmatrix}$

23. $A=\begin{bmatrix}1&0&2\\1&2&1\end{bmatrix}$ $b=\begin{bmatrix}1\\2\end{bmatrix}$

24. $A=\begin{bmatrix}1&0&2\\1&1&1\end{bmatrix}$ $b=\begin{bmatrix}2\\2\end{bmatrix}$

25. $A=\begin{bmatrix}1&2&2\\2&2&1\end{bmatrix}$ $b=\begin{bmatrix}2\\1\end{bmatrix}$

26. $A=\begin{bmatrix}2&0&1\\2&2&2\end{bmatrix}$ $b=\begin{bmatrix}0\\1\end{bmatrix}$

27. $A=\begin{bmatrix}2&1&1\\0&2&1\end{bmatrix}$ $b=\begin{bmatrix}1\\2\end{bmatrix}$

28. $A=\begin{bmatrix}2&0&2\\1&2&2\end{bmatrix}$ $b=\begin{bmatrix}1\\0\end{bmatrix}$

29. $A=\begin{bmatrix}2&2&2\\2&2&1\end{bmatrix}$ $b=\begin{bmatrix}0\\2\end{bmatrix}$

30. $A=\begin{bmatrix}2&1&2\\1&2&0\end{bmatrix}$ $b=\begin{bmatrix}1\\1\end{bmatrix}$

ЛИТЕРАТУРА

1. Бурдун А.А. и др. Сборник задач по алгебре и аналитической геометрии, – 2-е изд., – Минск, 1999. – 302 с.
2. Винберг Э.Б. Курс алгебры, 2-е изд., – М.: Изд-во «Факториал Пресс», 2001. – 544 с.
3. Золотых Н.Ю., Сидоров С.В. Группы, кольца, поля». Электронное учебно-методическое пособие, – Н. Новгород, ННГУ, 2012. – 52 с. www.unn.ru/books/met_files/groupsringsfields.pdf
4. Курош А.Г. Курс высшей алгебры, – Изд. 18-е стер. – Спб.; М.; Краснодар: Лань, 2011. – 432 с.
5. Курош А.Г. Теория групп, – Изд. 4-е стер. – Спб.: Лань, 2005. – 648 с.
6. Курош А.Г. Лекции по общей алгебре, – Спб.; М.; Краснодар: Лань, 2005. – 560 с.
7. Ляпин Е.С.и др. Упражнения по теории групп, – М.: Изд-во «Наука», 1967. – 264 с.
8. Мальцев А.И. Основы линейной алгебры, – Изд. 4-е стер. – М.: «Наука», 1978. – 400 с.
9. Проскуряков И.В. Сборник задач по линейной алгебре, – Изд. 8-е. – М.: Лаборатория базовых знаний, 2003. – 382 с.
10. Сборник задач по алгебре, ред. Кострикин А.И., – Изд. 3-е. – ФИЗМАТЛИТ, 2001. – 464 с.
11. Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре, – Изд. 13-е стер. – Спб.: Лань, 2001. – 288 с.

Михаил Михайлович Шульц

АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

ЗАДАЧИ И РЕШЕНИЯ

Учебно-методическое пособие

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Нижегородский государственный университет им. Н.И. Лобачевского»
603950, Нижний Новгород, пр. Гагарина, 23

Подписано в печать Формат 60 × 84 1/16.
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл. печ. л. Уч.-изд. л.
Заказ № Тираж 300 экз.

Отпечатано в типографии Нижегородского госуниверситета
им. Н.И. Лобачевского
603600, Н. Новгород, ул. Большая Покровская, 37
Лицензия ПД № 18-0099 от 14.05.01