Министерство образования Российской Федерации
Уральский государственный университет им. А. М. Горького

Сборник задач по общей алгебре и дискретной математике

Под редакцией Л. Н. Шеврина

Рекомендовано Научно-методическим советом
по математике и механике УМО классических университетов РФ
в качестве учебного пособия
для математических специальностей и направлений

Екатеринбург
2003

УДК 512.64
З000
ББК 22.143

Составители:
В.А. Баранский, Ю.М. Важенин, М.В. Волков, А.Г. Гейн, А.П. Замятин, А.Я. Овсянников, А.Н. Петров, Н.Ф. Сесекин, Л.Н. Шеврин

Рецензенты:
кафедра алгебры и теории чисел Уральского государственного педагогического университета (заведующий кафедрой доктор физико-математических наук, профессор А.П. Ильиных);
доктор физико-математических наук, профессор В.Б. Репницкий (Уральский государственный технический университет–УПИ)

З000 Сборник задач по общей алгебре и дискретной математике: Учеб. пособие. / Под ред. Л.Н. Шеврина – Екатеринбург: Изд-во Урал. ун-та, 2003 г. — 129 с.
ISBN 5-7996-000-0

Пособие содержит задачи для решения на практических занятиях по курсу “Алгебра и дискретная математика", изучаемого студентами математико-механического факультета.

Предназначено студентам, обучающимся по специальностям “Математика" и “Компьютерная безопасность".

УДК 512.64
ББК 22.143

ISBN 5-7996-000-0

Оглавление

От составителей

Настоящий сборник предназначен для использования на практических занятиях по курсу “Алгебра и дискретная математика", изучаемого в Уральском университете студентами специальностей “Математика" и “Компьютерная безопасность" в третьем семестре. Он может быть полезен также студентам математических специальностей других университетов.

Содержание указанного курса в основных чертах отражается оглавлением сборника. Первые четыре главы посвящены основным типам алгебраических структур — полугруппам, группам, кольцам, полям, и в параграфах этих глав задачи подобраны по единому плану: примеры, некоторые простейшие свойства, порождающие множества и подалгебры, гомоморфизмы, конгруэнции и факторалгебры. В гл. 7 по тому же плану рассматриваются решетки и булевы алгебры; предварительно в гл. 6 обсуждаются частично упорядоченные множества, линейно упорядоченные множества и ординальные числа. Гл. 8 включает как задачи о произвольных универсальных алгебрах, так и задачи, связанные с производными структурами, в которых используются различные типы алгебр. Главы 5, 9 и 10 содержат задачи, связанные с приложениями общей алгебры к теориям соответственно двоичных кодов, булевых функций, автоматов и формальных языков.

Предполагается, что читатель знаком — по лекциям или соответствующей учебной литературе, в частности, по пособию [2], отражающему большинство тем курса, — с основными понятиями курса. Это прежде всего понятия, фигурирующие в заголовках глав и параграфов, а также следующие понятия: бинарное отношение, отношение эквивалентности, разбиение множества, конечно порожденная алгебра[1], симметрическая полугруппа, симметрическая группа, свободная полугруппа, свободная группа, кольцо многочленов над (коммутативным ассоциативным) кольцом, кольцо матриц над кольцом, поле

[1] Под алгеброй всюду понимается произвольная универсальная алгебра.

рациональных функций над полем, максимальный и минимальный элементы частично упорядоченного множества, наибольший и наименьший элементы частично упорядоченного множества, цепь и антицепь в частично упорядоченном множестве, кардинальное число, ординальное число. Напомним лишь определения нескольких понятий, примыкающих к основным. Порождающее множество алгебры называется *минимальным* (*неприводимым*), если никакое его собственное подмножество не будет порождающим для этой алгебры. Минимальное порождающее множество называют также *базисом*; мы будем пользоваться именно этим термином. Алгебра называется *n-порожденной*, если для нее существует порождающее множество, содержащее n элементов. Полугруппа (группа) называется *циклической*, если она 1-порождена. Подалгебра называется *собственной*, если она не совпадает со всей алгеброй. Собственная подалгебра называется *нетривиальной*, если она не совпадает с подалгеброй, порожденной пустым множеством. Решетка называется *полной*, если существуют точная нижняя и точная верхняя грани для любого подмножества ее элементов.

Целый ряд определений дается в формулировках соответствующих заданий; нередко такие определения используются в некоторых последующих задачах. Узнать, в каком задании дается в задачнике то или иное определение, можно по предметному указателю. Аналогичной цели служит список обозначений; в него включены, как правило, обозначения, используемые в нескольких главах. Ряд других обозначений (используемых в более или менее ограниченном круге заданий) вводятся по ходу изложения.

При выполнении некоторых заданий не обязательно делать те или иные записи; вполне достаточно (в условиях аудиторного практического занятия) провести решение устно, приводя необходимые объяснения. Такие задания помечены символом **(У)** . Некоторые задания предлагают исследовать тот или иной вопрос и найти критерий; такие задания помечены символом **(И)** . Задания повышенной трудности помечены звездочкой. Для некоторых заданий мы в конце задачника даем советы или указания по решению; в конце формулировки такого задания стоит символ **(С)**.

В предметном указателе для каждого термина указан номер задания или параграфа, в котором этот термин определен (если термин определяется в задании или во вводном абзаце параграфа), и через запятую страница.

Часть задач сборника заимствована из книг, указанных в приводимом ниже списке литературы.

Список литературы

1. *Атья М., Макдональд И.* Введение в коммутативную алгебру. М.: Мир, 1972.

2. *Баранский В. А.* Введение в общую алгебру и ее приложения: Учеб. пособие / Урал. гос. ун-т. Екатеринбург, 1998.

3. *Биркгоф Г.* Теория решеток. М.: Наука, 1984.

4. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. М.: Мир, 1976.

5. *Важенин Ю. М.* Множества, логика, алгоритмы. / Урал. гос. ун-т. Екатеринбург, 1999.

6. *Важенин Ю. М., Попов В. Ю.* Множества, логика, алгоритмы в задачах. / Урал. гос. ун-т. Екатеринбург, 1997.

7. *Гаврилов Г. П., Сапоженко А. А.* Сборник задач по дискретной математике. М.: Наука, 1977.

8. *Гиндикин С. Г.* Алгебра логики в задачах. М.: Наука, 1972.

9. *Горбатов В.А.* Основы дискретной математики. М.: Высш. шк., 1986.

10. *Замятин А. П., Сесекин Н. Ф.* Задачи по алгебре: Метод. разраб. для студ. 2 курса мат.-мех. фак. / Урал. гос. ун-т. Екатеринбург, 1985.

11. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1982.

12. *Клиффорд А., Престон Г.* Алгебраическая теория полугрупп. М.: Мир, 1972.

13. *Ламбек И.* Кольца и модули. М.: Мир, 1971.

14. *Лидл Р., Пильц Г.* Прикладная абстрактная алгебра. Екатеринбург: Изд-во Урал. ун-та, 1996.

15. *Пирс Р.* Ассоциативные алгебры. М.: Мир, 1986.

16. Сборник задач по алгебре / Под ред. *А. И. Кострикина.* М.: Физматлит, 2001.

17. *Grimaldi R. P.* Discrete and Combinatorial Mathematics. An Applied Introduction. 3-rd Ed., 1994.

18. *Sierpiński W.* Cardinal and Ordinal Numbers. 2-nd Edition Revised, W–wa, 1965.

Список обозначений

$\mathbb{N}$ — множество всех натуральных чисел ($0 \notin \mathbb{N}$).

$\mathbb{Z}$ — множество всех целых чисел.

$\mathbb{Q}$ — множество всех рациональных чисел.

$\mathbb{R}$ — множество всех вещественных чисел.

$\mathbb{C}$ — множество всех комплексных чисел.

$\mathbb{Q}^+$ — множество всех положительных рациональных чисел.

$\mathbb{R}^+$ — множество всех положительных вещественных чисел.

$\mathbb{C}_n$ — множество всех комплексных корней из единицы степени n.

$\mathbb{C}_{p^\infty}$ — множество всех комплексных корней из единицы степеней вида p^n, где $n \in \mathbb{N}$ и p — фиксированное простое число.

nA — множество всех чисел вида na, $a \in A$, где n — натуральное число, $A = \mathbb{N}$ или $A = \mathbb{Z}$.

$\mathbb{Z}_n$ — множество всех классов вычетов по модулю n.

K^* — множество всех обратимых элементов ассоциативного кольца K с единицей.

$\mathbb{Q}_p$ — множество всех рациональных чисел, знаменатели которых являются степенями фиксированного простого числа p.

$\mathbf{M}_n(K)$ — множество всех $n \times n$-матриц над кольцом K.

$\mathbf{GL}_n(K)$ — множество всех обратимых $n \times n$-матриц над ассоциативным кольцом K с единицей.

$\mathbf{SL}_n(K)$ — множество всех $n \times n$-матриц над ассоциативным коммутативным кольцом K с единицей, определитель которых равен единице.

$\mathbf{T}_n(K)$ — множество всех обратимых верхнетреугольных (т. е. имеющих лишь нулевые элементы ниже главной диагонали) $n \times n$-матриц над ассоциативным кольцом K с единицей.

$\mathbf{UT}_n(K)$ — множество всех матриц из $\mathbf{T}_n(K)$, имеющих единицы на главной диагонали.

$\mathbf{D}_n(K)$ — множество всех обратимых диагональных $n \times n$-матриц над ассоциативным кольцом K с единицей.

$K[x]$ — множество всех многочленов от переменной x с коэффициентами из кольца K.

A^+ — свободная полугруппа над алфавитом A.

S_n — симметрическая группа на множестве $\{1, 2, \ldots, n\}$.

$\mathcal{T}_n$ — симметрическая полугруппа на множестве $\{1, 2, \ldots, n\}$.

$\mathcal{T}(X)$ — симметрическая полугруппа на множестве X.

$\mathcal{PT}(X)$ — полугруппа всех частичных преобразований на множестве X.

$\mathcal{B}(X)$ — множество всех бинарных отношений на множестве X.

$X_1 \times X_2 \times \ldots \times X_n$ — декартово произведение множеств $X_1, X_2, \ldots X_n$, т.е. множество всех кортежей $(x_1, x_2, \ldots, x_n)$, где $x_k \in X_k$ для $k = 1, 2, \ldots, n$.

$\mathcal{P}(X)$ — множество всех подмножеств множества X.

$\mathcal{P}'(X)$ — множество всех непустых подмножеств множества X.

$|X|$ — число элементов конечного множества X.

$(A, \circ)$ — множество A с бинарной операцией $\circ$ на нем.

(M, ρ) — множество M с бинарным отношением ρ на нем; в качестве ρ могут фигурировать такие отношения, как $\leq$, $\subseteq$ и т.п.

$\cong$ — символ изоморфизма.

$\rightleftharpoons$ — “есть по определению".

Глава 1

Полугруппы

1.1 Примеры и простейшие свойства. Изоморфизм

1.1.1. Выяснить, какие из перечисленных ниже множеств относительно указанной операции являются полугруппами и какие из выявленных полугрупп оказываются группами:

а) $(\mathbb{N}, \circ)$, где $a \circ b \rightleftharpoons a^b$;

б) $(\mathbb{N}, \circ)$, где $a \circ b \rightleftharpoons b$;

в) $(Z, -)$;

г) $\mathbb{Q}^+$ относительно операции взятия частного;

д) **(У)** $(A, +)$, где A — одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

е) **(У)** $(A, \cdot)$, где A — одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

ж) **(У)** $(A\backslash\{0\}, \cdot)$, где A — одно из множеств $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

з) **(У)** $(n\mathbb{Z}, +)$, где n — произвольное натуральное число;

и) **(У)** $(\{-1, 1\}, \cdot)$;

к) множество $\cup_{n=1}^{\infty} \mathbb{C}_n$ относительно умножения;

л) множество всех комплексных чисел с фиксированным модулем r относительно умножения;

м) множество всех степеней данного вещественного числа $a \neq 0$ с целыми показателями относительно умножения.

1.1.2. Выяснить, какие из перечисленных ниже множеств вещественных $n \times n$-матриц относительно указанной операции образуют

полугруппу и какие из выявленных полугрупп оказываются группами:

а) множество всех симметрических матриц относительно сложения;

б) множество всех кососимметрических матриц относительно сложения;

в) множество всех симметрических матриц относительно умножения;

г) множество всех кососимметрических матриц относительно умножения;

д) множество всех невырожденных матриц относительно сложения;

е) **(У)** множество всех невырожденных матриц относительно умножения;

ж) **(У)** множество всех матриц с фиксированным определителем d относительно умножения **(С)**;

з) **(У)** множество всех матриц с положительным определителем относительно умножения;

и) **(У)** множество всех матриц с отрицательным определителем относительно умножения;

к) **(У)** множество всех диагональных матриц относительно сложения;

л) **(У)** множество всех диагональных матриц относительно умножения;

м) **(У)** множество всех невырожденных диагональных матриц относительно умножения;

н) множество всех ортогональных матриц относительно умножения;

о) множество всех ненулевых матриц вида $\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}$, где $x, y \in \mathbb{Q}$, λ — фиксированное рациональное число, относительно умножения **(С)**;

п) множество всех ненулевых матриц вида $\begin{pmatrix} x & y \\ -\overline{y} & x \end{pmatrix}$, где $x, y \in \mathbb{C}$, относительно умножения;

р) множество из восьми матриц

$$\left\{\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\right\}$$

относительно умножения.

1.1.3. Убедиться, что множество $S = \{a, b, c, d\}$, на котором бинарная операция задана одной из следующих таблиц Кэли, является полугруппой:

а)

	a	b	c	d
a	c	c	d	d
b	c	c	d	d
c	d	d	d	d
d	d	d	d	d

б)

	a	b	c	d
a	b	b	a	a
b	b	b	b	b
c	a	b	d	c
d	a	b	c	d

в)

	a	b	c	d
a	a	b	a	b
b	a	b	a	b
c	a	b	c	d
d	a	b	c	d

1.1.4. Обозначим через B_2 множество, состоящее из нулевой 2×2-матрицы $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ и четырех "матричных единиц"

$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

а) Проверить, что B_2 является полугруппой относительно умножения.

б) Составить таблицу Кэли полугруппы B_2.

1.1.5. Доказать, что для любого группоида G множества

$$G_1 = \{a \in G \mid a(xy) = (ax)y \text{ для всех } x, y \in G\},$$
$$G_2 = \{a \in G \mid x(ay) = (xa)y \text{ для всех } x, y \in G\},$$
$$G_3 = \{a \in G \mid (xy)a = x(ya) \text{ для всех } x, y \in G\},$$

если они не пусты, замкнуты относительно умножения и являются полугруппами относительно этой операции.

1.1.6. Пусть G — группоид. Зафиксируем элемент $a \in G$. Рассмотрим две бинарные операции на множестве G:

$$x *_a y \rightleftharpoons x(ay), \quad x \circ_a y \rightleftharpoons (xa)y.$$

а) **(У)** Убедиться, что операции $*_a$ и $\circ_a$ совпадают для каждого элемента a из G тогда и только тогда, когда G является полугруппой.

б) **(И)** Разработать алгоритм проверки ассоциативности бинарной операции на конечном множестве по таблице Кэли, используя таблицы Кэли для операций $*_a$ и $\circ_a$. **(С)**

1.1.7. (У) Пусть на множестве M определена операция по правилу $x \circ y \rightleftharpoons x$.

а) Убедиться, что $(M, \circ)$ — полугруппа. Она называется *полугруппой левых нулей*.

б) В каком случае полугруппа левых нулей имеет нейтральный элемент?

в) Указать критерий изоморфности двух полугрупп левых нулей.

1.1.8. (У) Пусть X, Y — два множества. На множестве $A = X \times Y$ определим операцию $\circ$, полагая $(x, y) \circ (z, t) \rightleftharpoons (x, t)$.

а) Убедиться, что $(A, \circ)$ будет полугруппой. В каком случае она имеет нейтральный элемент?

б) Найти критерий перестановочности элементов из $(A, \circ)$.

1.1.9. Пусть M — непустое множество вещественных чисел. Определим на M операции $\wedge$ и $\vee$, полагая

$$x \wedge y \rightleftharpoons \min\{x, y\}, \quad x \vee y \rightleftharpoons \max\{x, y\}.$$

а) Убедиться, что $(M, \wedge)$ и $(M, \vee)$ являются полугруппами.

б) **(У)** При каком условии на множество M полугруппа $(M, \wedge)$ имеет нейтральный элемент? Ответить на аналогичный вопрос для полугруппы $(M, \vee)$.

в) Доказать, что если множество M конечно, то полугруппы $(M, \wedge)$ и $(M, \vee)$ изоморфны.

г) **(У)** Изоморфны ли полугруппы $(\mathbb{N}, \wedge)$ и $(\mathbb{N}, \vee)$?

д) **(У)** Изоморфны ли полугруппы $(\mathbb{Z}, \wedge)$ и $(\mathbb{Z}, \vee)$?

е) **(У)** Изоморфны ли полугруппы $(\mathbb{Z}, \wedge)$ и $(\mathbb{Q}, \wedge)$?

1.1.10. На множестве $\mathbb{N}$ рассмотрим операции $\circ$ и $*$, заданные следующими условиями:

$$x \circ y \rightleftharpoons \text{НОД}(x, y), \quad x * y \rightleftharpoons \text{НОК}(x, y).$$

а) Убедиться, что $(\mathbb{N}, \circ)$ и $(\mathbb{N}, *)$ являются полугруппами.

б) **(У)** Изоморфны ли полугруппы $(\mathbb{N}, \circ)$ и $(\mathbb{N}, *)$?

1.1.11. Операции $\circ$ и $*$, введенные в задании 1.1.10, определяются и на множестве $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

а) Убедиться, что $(\mathbb{N}_0, \circ)$ и $(\mathbb{N}_0, *)$ являются полугруппами.

б)* Выяснить, изоморфны ли полугруппы $(\mathbb{N}_0, \circ)$ и $(\mathbb{N}_0, *)$.

1.1.12. Пусть M — произвольное множество вещественных чисел, $a, b \in M$ и $a \leq b$. *Отрезком* $[a, b]$ в M называется множество

$$\{x \in M \mid a \leq x \leq b\};$$

отрезок назовем *нетривиальным*, если $a < b$. Через S_M обозначим множество всех нетривиальных отрезков из M, дополненное пустым

множеством. Зададим на S_M операцию $\circ$, полагая

$$[a,b]\circ[c,d]=\begin{cases}[a,d], & \text{если } b=c,\\ \emptyset, & \text{если } b\neq c,\end{cases}$$
$$[a,b]\circ\emptyset=\emptyset\circ[a,b]=\emptyset\circ\emptyset=\emptyset.$$

а) Убедиться, что $(S_M,\circ)$ является полугруппой.

б) Выяснить, изоморфны ли полугруппы $(S_{\mathbb{N}},\circ)$ и $(S_{\mathbb{Z}},\circ)$.

в)* Выяснить, изоморфны ли полугруппы $(S_{\mathbb{Z}},\circ)$ и $(S_{\mathbb{Q}},\circ)$.

г) Найти критерий изоморфности полугрупп $(S_{M_1},\circ)$ и $(S_{M_2},\circ)$ для конечных множеств M_1 и M_2.

д) **(И)** Найти критерий изоморфности полугрупп $(S_{M_1},\circ)$ и $(S_{M_2},\circ)$, если множества M_1 и M_2 не обязательно конечны.

1.1.13. Пусть M — произвольное множество вещественных чисел. Через S'_M обозначим множество всех отрезков множества M (включая тривиальные, т.е. одноэлементные, см. задание 1.1.12) и рассмотрим операцию $\circ$ на этом множестве, определенную точно так же, как в указанном задании.

а) Убедиться, что $(S'_M,\circ)$ является полугруппой.

б) Выяснить, изоморфны ли полугруппы $(S'_{\mathbb{N}},\circ)$ и $(S'_{\mathbb{Z}},\circ)$.

в)* Выяснить, изоморфны ли полугруппы $(S'_{\mathbb{Z}},\circ)$ и $(S'_{\mathbb{Q}},\circ)$.

г) Найти критерий изоморфности полугрупп $(S'_{M_1},\circ)$ и $(S'_{M_2},\circ)$ для конечных множеств M_1 и M_2.

д) **(И)** Найти критерий изоморфности полугрупп $(S'_{M_1},\circ)$ и $(S'_{M_2},\circ)$, если множества M_1 и M_2 не обязательно конечны.

1.1.14. Пусть M — произвольное множество вещественных чисел. На множестве S_M, определенном в задании 1.1.12, зададим операцию $*$, полагая

$$[a,b]*[c,d]=\begin{cases}[\min\{a,c\},\max\{b,d\}], & \text{если } b\geq c,\\ \emptyset, & \text{если } b<c,\end{cases}$$
$$[a,b]*\emptyset=\emptyset*[a,b]=\emptyset*\emptyset=\emptyset.$$

а) **(У)** Убедиться, что $(S_M,*)$ является полугруппой.

б) Выяснить, изоморфны ли полугруппы $(S_{\mathbb{N}},*)$ и $(S_{\mathbb{Z}},*)$.

в)* Выяснить, изоморфны ли полугруппы $(S_{\mathbb{Z}},*)$ и $(S_{\mathbb{Q}},*)$.

г) Найти критерий изоморфности полугрупп $(S_{M_1},*)$ и $(S_{M_2},*)$ для конечных множеств M_1 и M_2.

д) **(И)** Найти критерий изоморфности полугрупп $(S_{M_1}, *)$ и $(S_{M_2}, *)$, если множества M_1 и M_2 не обязательно конечны.

1.1.15. Пусть S — полугруппа. На множестве $\mathcal{P}'(S)$ введем умножение, полагая

$$XY = \{xy \mid x \in X,\ y \in Y\}.$$

а) Убедиться, что относительно введенного умножения $\mathcal{P}'(S)$ является полугруппой.

б) Доказать, что если $|S| > 1$, то полугруппа $\mathcal{P}'(S)$ не может быть группой.

1.1.16. Пусть X — произвольное непустое множество. Выяснить, изоморфны ли полугруппы $(\mathcal{P}(X), \cap)$ и $(\mathcal{P}(X), \cup)$.

1.1.17. а) **(У)** Изоморфны ли мультипликативные полугруппы всех натуральных чисел и всех нечетных натуральных чисел?

б)* Выяснить, изоморфны ли полугруппы $(2\mathbb{N}, \cdot)$ и $(3\mathbb{N}, \cdot)$.

в) **(И)** Найти критерий изоморфности полугрупп $(m\mathbb{N}, \cdot)$ и $(n\mathbb{N}, \cdot)$.

1.1.18. Пусть P — фиксированное множество простых чисел. Через $\mathbb{Q}_P$ обозначим множество всех положительных рациональных чисел, в записи которых несократимой дробью знаменатель больше 1 и все его простые делители принадлежат P.

а) **(У)** Убедиться, что $(\mathbb{Q}_P, \cdot)$ является полугруппой.

б) Выяснить, изоморфны ли полугруппы $(\mathbb{Q}_{P_1}, \cdot)$ и $(\mathbb{Q}_{P_2}, \cdot)$, где $P_1 = \{2, 3\}$, $P_2 = \{3, 5\}$; $P_1 = \{2, 3, 5\}$, $P_2 = \{3, 5, 7\}$.

в)* Выяснить, изоморфны ли полугруппы $(\mathbb{Q}_{P_1}, \cdot)$ и $(\mathbb{Q}_{P_2}, \cdot)$, где $P_1 = \{2, 3\}$, $P_2 = \{2, 3, 5\}$.

г) **(И)** Найти — в терминах произвольных множеств простых чисел P_1 и P_2 — критерий изоморфности полугрупп $(\mathbb{Q}_{P_1}, \cdot)$ и $(\mathbb{Q}_{P_2}, \cdot)$.

1.1.19. Выяснить, изоморфны ли полугруппа $(\mathbb{N}, \cdot)$ и полугруппа всех конечных подмножеств счетного множества относительно объединения.

1.1.20. Пусть S — полугруппа, $a \in S$. Положим $S_a = (S, \circ)$, где новая операция $\circ$ на S определяется через исходную следующим образом: $x \circ y \rightleftharpoons xay$. Согласно утверждению п. а) задания 1.1.6 группоид S_a является полугруппой.

а) Выяснить, изоморфны ли полугруппы $\mathbb{N}_2$ и $\mathbb{N}_3$; $\mathbb{N}_3$ и $\mathbb{N}_4$, где $\mathbb{N}$ — аддитивная полугруппа натуральных чисел. **(С)**

б) Выяснить, изоморфны ли полугруппы $\mathbb{N}_2$ и $\mathbb{N}_3$; $\mathbb{N}_3$ и $\mathbb{N}_4$, где $\mathbb{N}$ — мультипликативная полугруппа натуральных чисел. **(С)**

1.1.21. Выяснить, какие из перечисленных ниже совокупностей преобразований множества $M = \{1, 2, \ldots, n\}$ образуют полугруппу относительно суперпозиции, какие из выявленных полугрупп оказываются группами:

а) **(У)** множество всех преобразований;

б) множество всех инъективных преобразований;

в) множество всех сюръективных преобразований;

г) множество всех четных подстановок;

д) множество всех нечетных подстановок;

е) множество всех транспозиций;

ж) множество всех подстановок, оставляющих неподвижными элементы некоторого подмножества $X \subseteq M$;

з) множество всех подстановок, при которых образы всех элементов некоторого подмножества $S \subseteq M$ принадлежат этому подмножеству.

1.1.22. *Произведением* двух бинарных отношений ρ и σ на множестве X называется бинарное отношение
$\rho \circ \sigma \rightleftharpoons \{(x, y) |\ (x, z) \in \rho \ \text{ и } \ (z, y) \in \sigma \ \text{ для некоторого } \ z \in X\}$. Убедиться, что множество $\mathcal{B}(X)$ всех бинарных отношений на множестве X является полугруппой относительно этой операции.

1.1.23. Если Y — произвольное (непустое) подмножество множества X, то отображение $\varphi : Y \to X$ называется *частичным преобразованием* множества X. Всякое частичное преобразование φ множества X можно отождествить с бинарным отношением на X, состоящим из всех пар $(x, \varphi(x))$, где x пробегает область определения φ. Будем рассматривать также *пустое* частичное преобразование, соответствующее пустому бинарному отношению. Совокупность всех частичных преобразований множества X (включая пустое) обозначается через $\mathcal{PT}(X)$. Тогда $\mathcal{PT}(X)$ оказывается подмножеством полугруппы $\mathcal{B}(X)$.

а) Проверить, что это подмножество замкнуто относительно умножения, т.е. является полугруппой.

б) Убедиться, что применительно к преобразованиям операция умножения бинарных отношений есть не что иное, как суперпозиция.

1.1.24. а) **(У)** Сколько элементов содержит полугруппа $\mathcal{T}_n$?

б) Подсчитать, сколько элементов содержит полугруппа $\mathcal{PT}(X)$, если $|X| = n$.

в) **(У)** Сколько элементов содержит полугруппа $\mathcal{B}(X)$, если $|X|=n$?

1.1.25. Пусть I — множество индексов, а ρ, ρ_i $(i \in I)$, σ, τ — произвольные элементы полугруппы $\mathcal{B}(X)$. Доказать, что в $\mathcal{B}(X)$ выполняются следующие соотношения:

а) из $\rho \subseteq \sigma$ следует $\rho \circ \tau \subseteq \sigma \circ \tau$ и $\tau \circ \rho \subseteq \tau \circ \sigma$;

б) $\sigma \circ (\cup_{i\in I}\rho_i) = \cup_{i\in I}\sigma \circ \rho_i$;

в) $\sigma \circ (\cap_{i\in I}\rho_i) \subseteq \cap_{i\in I}\sigma \circ \rho_i$.

1.1.26. Доказать, что в соотношении в) задания 1.1.25 равенство, вообще говоря, не имеет места. **(С)**

1.1.27. Доказать, что если ρ и σ — такие симметричные отношения, что $\rho \circ \sigma \subseteq \sigma \circ \rho$, то $\rho \circ \sigma = \sigma \circ \rho$.

1.1.28. Доказать, что произведение $\rho \circ \sigma$ двух отношений эквивалентности ρ и σ будет отношением эквивалентности тогда и только тогда, когда $\rho \circ \sigma = \sigma \circ \rho$.

1.1.29. Пусть S_1, S_2, …, S_n — полугруппы.

а) Проверить, что декартово произведение $S_1 \times S_2 \times \cdots \times S_n$ является полугруппой относительно покомпонентно определенной операции: для всех $s_i, t_i \in S_i$, $i = 1, 2, \ldots, n$, положим

$$(s_1, s_2, \ldots, s_n) \cdot (t_1, t_2, \ldots, t_n) \rightleftharpoons (s_1t_1, s_2t_2, \ldots, s_nt_n).$$

Указанная полугруппа называется *прямым произведением* полугрупп S_1, S_2, …, S_n.

б) **(У)** Убедиться, что если все полугруппы S_1, S_2, …, S_n коммутативны, то их прямое произведение есть коммутативная полугруппа.

в) Убедиться, что если все полугруппы S_1, S_2, …, S_n являются группами, то и полугруппа $S_1 \times S_2 \times \cdots \times S_n$ является группой.

1.1.30. Пусть S_1 — мультипликативная полугруппа всех нечетных чисел, а S_2 — мультипликативная полугруппа всех степеней числа 2 с целыми неотрицательными показателями. Доказать, что мультипликативная полугруппа всех натуральных чисел изоморфна прямому произведению полугрупп S_1 и S_2.

1.1.31. Для каждой из приведенных ниже полугрупп установить, изоморфна ли она прямому произведению каких-либо неодноэлементных полугрупп:

а) аддитивная полугруппа $\mathbb{C}$; **(С)**

б) мультипликативная полугруппа $\mathbb{C}$. **(С)**

1.1.32. Пусть $|A| = n$.

а) **(У)** Сколько в A^+ слов длины m?

б) Подсчитать, сколько в A^+ слов длины, не превосходящей m.

1.1.33.* Пусть $u, v \in A^+$.

а) Доказать, что $uv = vu$ тогда и только тогда, когда существуют такие $w \in A^+$ и $m, n \in \mathbb{N}$, что $u = w^m$, $v = w^n$.

б) Доказать, что $u^k = v^l$ для некоторых $k, l \in \mathbb{N}$ тогда и только тогда, когда существуют такие $w \in A^+$ и $m, n \in \mathbb{N}$, что $u = w^m$, $v = w^n$.

1.1.34. (У) Доказать, что свободная полугруппа неразложима в прямое произведение неодноэлементных полугрупп. **(С)**

1.1.35. Говорят, что полугруппа S есть *полугруппа с сокращениями* (или *удовлетворяет закону сокращения*), если для любых $a, b, c \in S$ из $ab = ac$ следует $b = c$ и из $ba = ca$ следует $b = c$.

а) Убедиться, что свободная полугруппа удовлетворяет закону сокращения.

б) **(У)** Убедиться, что всякая группа удовлетворяет закону сокращения, и привести пример — отличный от примера из задания а) — полугруппы с сокращениями, не являющейся группой.

в) Выяснить, для каких множеств X симметрическая полугруппа $\mathcal{T}(X)$ удовлетворяет закону сокращения.

г) **(У)** Убедиться, что если все полугруппы $S_1, S_2, \ldots, S_n$ удовлетворяют закону сокращения, то их прямое произведение удовлетворяет закону сокращения.

1.1.36.* Выяснить, может ли при $|S| > 1$ полугруппа $\mathcal{P}'(S)$ относительно умножения, введенного в задании 1.1.15, быть полугруппой с сокращениями.

1.1.37. Пусть M — произвольное множество вещественных чисел, $(S_M, \circ)$ — полугруппа, определенная в задании 1.1.12. Выяснить, обладает ли полугруппа $(S_M, \circ)$ следующими свойствами:

а) удовлетворяет следующему ослабленному закону сокращения:

$$xy = xz \neq 0 \Rightarrow y = z,$$
$$yx = zx \neq 0 \Rightarrow y = z.$$

б) удовлетворяет даже закону сокращения.

1.1.38.* Доказать, что конечная полугруппа с сокращениями является группой. (В задании 1.2.22 в) предлагается доказать более общее утверждение.)

1.1.39. Полугруппа S называется *регулярной*, если для любого $a \in S$ существует $b \in S$ такой, что $aba = a$.

а) **(У)** Убедиться, что любая группа является регулярной полугруппой, и привести пример регулярной полугруппы, не являющейся группой.

б) Доказать, что регулярная полугруппа с сокращениями является группой.

в) **(У)** Доказать, что если все полугруппы S_1, S_2, ..., S_n регулярны, то и полугруппа $S_1 \times S_2 \times \cdots \times S_n$ регулярна.

1.1.40. Элемент b полугруппы S называется *инверсным* к элементу $a \in S$, если $aba = a$ и $bab = b$.

а) Доказать, что если полугруппа S регулярна, то для любого элемента $a \in S$ существует инверсный к нему элемент.

б) **(У)** Убедиться, что в группе элемент, инверсный к данному элементу, — это обратный к нему элемент, и, следовательно, он единствен. Привести пример полугруппы, в которой каждый элемент имеет более одного инверсного элемента.

в) Убедиться, что в полугруппе B_2, определенной в задании 1.1.4, каждый элемент имеет единственный инверсный элемент. **(С)**

1.1.41. Доказать, что для любого множества X полугруппа $\mathcal{T}(X)$ регулярна.

1.1.42. Доказать, что для любого множества X полугруппа $\mathcal{PT}(X)$ регулярна.

1.1.43. Доказать, что полугруппа $\mathbf{M}_n(\mathbb{C})$ регулярна. **(С)**

1.1.44.* Определить, является ли регулярной полугруппа всех $n \times n$-матриц

а) над произвольным полем, б) над кольцом целых чисел.

1.1.45. Введем на множестве $\mathcal{F}(\mathbb{R})$ всех действительнозначных функций действительной переменной поточечное умножение: $(fg)(x) \rightleftharpoons f(x)g(x)$. Доказать, что $\mathcal{F}(\mathbb{R})$ является регулярной полугруппой относительно этой операции.

1.1.46.* Выяснить, является ли регулярной полугруппа $\mathcal{B}(X)$.

1.1.47. Выписать таблицы Кэли всех попарно неизоморфных полугрупп из двух элементов.

1.1.48. Среди найденных в задании 1.1.47 полугрупп выделить: а) коммутативные полугруппы, б) полугруппы с сокращениями, в) регулярные полугруппы, г) группы.

1.2 Порождающие множества, подполугруппы, порядки элементов

1.2.1. а) Доказать, что преобразования

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix}$$

составляют порождающее множество полугруппы $\mathcal{T}_3$.

б) Выяснить, существует ли двухэлементное порождающее множество полугруппы $\mathcal{T}_3$.

1.2.2. а) Найти все базисы полугруппы $\mathcal{T}_2$.

б) Доказать, что любая подполугруппа свободной полугруппы имеет единственный базис.

в)* Привести пример полугруппы, не имеющей базиса.

1.2.3.* Доказать, что каждая подполугруппа полугруппы $(\mathbb{N}, +)$ конечно порождена.

1.2.4. (У) а) Указать базис полугруппы $(\mathbb{N}, \cdot)$.

б) Показать, что полугруппа $(\mathbb{Z}, \cdot)$ имеет бесконечно много базисов.

1.2.5. Определить, имеет ли базис:

а) полугруппа $(\mathbb{N}, \circ)$ из задания 1.1.10,

б) полугруппа $(\mathbb{N}, *)$ из задания 1.1.10,

в) полугруппа $(\mathbb{N}, \circ)$ из задания 1.1.11,

г) полугруппа $(\mathbb{N}, *)$ из задания 1.1.11.

1.2.6. Найти критерий того, что полугруппа $(S_M, \circ)$ из задания 1.1.12:

а) **(У)** является конечно порожденной,

б) **(И)** имеет базис.

1.2.7. Пусть a — элемент полугруппы S и $\langle a \rangle$ — циклическая подполугруппа полугруппы S, порожденная элементом a. *Порядком* конечной полугруппы называется число ее элементов. Если $\langle a \rangle$ конечна, то ее порядок называют *порядком* элемента a. Если $\langle a \rangle$ бесконечна, то говорят, что a имеет *бесконечный порядок*.

а) Доказать, что если $\langle a \rangle$ бесконечна, то все степени элемента a различны и $\langle a \rangle \cong (\mathbb{N}, +)$.

б) Доказать, что если $\langle a \rangle$ конечна, то существуют два натуральных числа, *индекс* r и *период* m элемента a, для которых $a^{m+r} = a^r$, $|\langle a \rangle| = m + r - 1$ и $\langle a \rangle = \{a, a^2, \ldots, a^{m+r-1}\}$.

в) Доказать, что в ситуации, описанной в п. б), множество $G = \{a^r, a^{r+1}, \ldots, a^{m+r-1}\}$ является циклической подгруппой порядка m в $\langle a\rangle$ и эта группа содержит каждую подгруппу полугруппы $\langle a\rangle$.

1.2.8. а) **(У)** Привести пример нециклической подполугруппы в бесконечной циклической полугруппе.

б) Привести пример конечной циклической полугруппы, имеющей нециклические подполугруппы.

1.2.9. Доказать, что подполугруппа полугруппы преобразований $\mathcal{T}_n$, где $n = r + m - 1$, порожденная преобразованием

$$\begin{pmatrix} 1 & 2 & \ldots & r-1 & r & \ldots & r+m-2 & r+m-1 \\ 2 & 3 & \ldots & r & r+1 & \ldots & r+m-1 & r \end{pmatrix},$$

является циклической полугруппой, индекс которой равен r, а период m.

1.2.10. Найти индекс и период следующих элементов полугруппы $\mathcal{T}_9$:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 1 & 2 & 4 & 5 & 3 & 2 \end{pmatrix}$;

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 1 & 6 & 6 & 4 & 5 & 6 & 6 \end{pmatrix}$.

1.2.11. Найти порядок, индекс и период циклической подполугруппы, порожденной матрицей $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ в мультипликативной полугруппе $\mathbf{M}_3(\mathbb{Z})$.

1.2.12. Найти порядки, а в случае конечного порядка — индекс и период следующих элементов мультипликативной полугруппы целочисленных матриц:

а) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; б) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$; в) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$; г) $\begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}$.

1.2.13. Указать все элементы конечного порядка в мультипликативной полугруппе: а)* $\mathbf{M}_2(\mathbb{Z})$; б) **(И)** $\mathbf{M}_n(\mathbb{Z})$.

1.2.14. (У) Используя утверждение задания 1.1.33, доказать, что любая коммутативная подполугруппа свободной полугруппы содержится в некоторой ее циклической подполугруппе.

1.2.15. Найти все подполугруппы полугруппы, определенной:

а) в п. а) задания 1.1.3,

б) в п. б) того же задания,

в) в п. в) того же задания.

1.2.16. Элемент e полугруппы S называется *идемпотентом*, если $e^2 = e$.

Доказать, что любая конечная полугруппа содержит хотя бы один идемпотент.

1.2.17. Описать все идемпотенты:

а) полугруппы $\mathcal{T}(X)$,

б) полугруппы $\mathcal{PT}(X)$,

в) полугруппы $\mathcal{B}(X)$,

г) **(У)** полугруппы отрезков $(S_M, \circ)$, определенной в задании 1.1.12, для произвольного множества вещественных чисел M,

д) **(У)** полугруппы отрезков $(S'_M, \circ)$, определенной в задании 1.1.13, для произвольного множества вещественных чисел M,

е) полугруппы отрезков $(S_M, *)$, определенной в задании 1.1.14, для произвольного множества вещественных чисел M.

1.2.18. Найти число идемпотентов полугруппы $\mathcal{T}_n$.

1.2.19. Доказать, что полугруппа с сокращениями может содержать не более одного идемпотента, который, если он существует, является единицей.

1.2.20. а) **(У)** Убедиться, что в любой регулярной полугруппе есть идемпотент.

б) Доказать, что регулярная полугруппа, имеющая единственный идемпотент, является группой.

1.2.21. а) Подполугруппа свободной полугруппы может быть не изоморфна никакой свободной полугруппе; убедиться в этом приведя соответствующий пример.

б) В полугруппе $\{a, b\}^+$ найти подполугруппу, изоморфную свободной полугруппе A^+, где A — счетное множество.

1.2.22. Полугруппа называется *периодической*, если каждая ее циклическая подполугруппа конечна.

а) Доказать, что полугруппа S будет периодической тогда и только тогда, когда для любого $x \in S$ существует $n \in \mathbb{N}$ такое, что x^n есть идемпотент.

б) Из определения периодической полугруппы следует, что всякая конечная полугруппа является периодической. Привести примеры бесконечных периодических полугрупп, коммутативных и некоммутативных.

в) Доказать, что периодическая полугруппа с сокращениями является группой.

1.2.23.* а) Доказать, что в полугруппе, содержащей идемпотенты, существуют максимальные подгруппы, т.е. подполугруппы, являющиеся группами и не содержащиеся в отличных от них подполугрупп, являющихся группами.

б) Доказать, что две произвольные различные максимальные подгруппы в полугруппе имеют пустое пересечение.

1.2.24. Непустое подмножество L полугруппы S называется ее *левым идеалом*, если $LS \subseteq L$. Симметрично определяется *правый идеал*. *Идеалом (двусторонним идеалом)* полугруппы называется подмножество, являющееся одновременно левым и правым идеалом.

а) **(У)** Убедиться, что объединение любого семейства левых (соответственно правых) идеалов данной полугруппы будет ее левым (соответственно правым) идеалом.

б) **(У)** Убедиться, что пересечение любого семейства левых (соответственно правых) идеалов данной полугруппы, если оно не пусто, будет ее левым (соответственно правым) идеалом.

в) Доказать, что пересечение любых двух идеалов полугруппы не пусто. Привести пример, когда пересечение двух левых идеалов полугруппы пусто.

г) Доказать, что полугруппа S является группой тогда и только тогда, когда каждый ее левый и каждый правый идеал совпадает с S.

д) Описать все левые и все правые идеалы полугруппы левых нулей.

1.2.25. а) **(У)** Описать все идеалы бесконечной циклической полугруппы.

б) Доказать, что каждый идеал полугруппы $(A, \circ)$, определенной в задании 1.1.8, совпадает с A.

1.2.26. а) Пусть $\mathcal{S}(X)$ — симметрическая группа на множестве X. Доказать, что множество $\mathcal{T}(X)\backslash\mathcal{S}(X)$ является идеалом полугруппы $\mathcal{T}(X)$, который содержит все ее идеалы, отличные от $\mathcal{T}(X)$.

б) **(И)** Описать все идеалы полугруппы $\mathcal{T}_n$.

1.3 Гомоморфизмы и конгруэнции

1.3.1. Пусть полугруппа T есть гомоморфный образ полугруппы S. Выяснить,

а) будет ли T полугруппой с сокращениями, если S такова,

б) будет ли T группой, если S такова,

в) будет ли S полугруппой с сокращениями, если T такова,

г) будет ли S группой, если T такова.

1.3.2. Пусть полугруппа T есть гомоморфный образ полугруппы S.

а) Доказать, что если полугруппа S регулярна, то и полугруппа T регулярна.

б) Выяснить, верно ли обратное.

1.3.3. Определить, существует ли гомоморфизм полугруппы $\mathcal{T}(\mathbb{N})$:

а) в полугруппу $(\mathbb{N}, +)$,

б) в полугруппу $(\{0, 1\}, \cdot)$.

1.3.4. (У) Указать все гомоморфизмы:

а) полугруппы $(\mathbb{N}, +)$ в себя,

б) полугруппы $(\mathbb{N}, +)$ в группу $(\mathbb{Z}, +)$,

в) группы $(\mathbb{Z}, +)$ в полугруппу $(\mathbb{N} \cup \{0\}, +)$.

1.3.5. Пусть $M_2 = \{1, 2\}$, $M_3 = \{1, 2, 3\}$, $M_n = \{1, 2, \ldots, n\}$, $\wedge$ — операция, определенная в задании 1.1.9. Указать все гомоморфизмы:

а) полугруппы $(M_2, \wedge)$ в полугруппу $(M_3, \wedge)$,

б) полугруппы $(M_3, \wedge)$ в полугруппу $(M_2, \wedge)$,

в)* полугруппы $(M_n, \wedge)$ в полугруппу $(M_m, \wedge)$.

1.3.6. Указать все гомоморфизмы полугруппы $(\mathbb{N}, +)$:

а) в группу $(\mathbb{Z}_3, +)$,

б) в группу $(\mathbb{Z}_8, +)$,

в) в группу $(\mathbb{Z}_n, +)$.

1.3.7. Найти все конгруэнции полугруппы, определенной:

а) в п. а) задания 1.1.3,

б) в п. б) того же задания,

в) в п. в) того же задания.

1.3.8. Пусть A — непустой алфавит.

а) Доказать, что отношение λ на полугруппе A^+, определяемое правилом

$$u \,\lambda\, v \iff u \text{ и } v \text{ имеют одинаковую длину,}$$

является конгруэнцией на полугруппе A^+ и что факторполугруппа A^+/λ изоморфна полугруппе $(\mathbb{N}, +)$.

б) *Содержанием* слова $u \in A^+$ называется множество входящих в u букв. Доказать, что отношение γ, определяемое правилом

$$u \,\gamma\, v \iff u \text{ и } v \text{ имеют одинаковое содержание,}$$

является конгруэнцией на полугруппе A^+ и что факторполугруппа A^+/γ изоморфна полугруппе $(\mathcal{P}'(A), \cup)$.

1.3.9. (И) Найти все конгруэнции полугруппы $(\mathbb{N}, +)$.

1.3.10. Найти все конгруэнции полугруппы B_2, определенной в задании 1.1.4.

1.3.11. Пусть S — полугруппа. Эквивалентность ρ на множестве S называется *правой конгруэнцией*, если для любых $a, b, c \in S$ из того, что $a \ \rho \ b$, следует, что $ac \ \rho \ bc$. Определение *левой конгруэнции* симметрично определению правой конгруэнции.

а) Доказать, что если ρ — правая конгруэнция, то существует гомоморфизм полугруппы S в полугруппу всех преобразований фактормножества S/ρ.

б)* Доказать, что если правая конгруэнция ρ имеет n классов, то существует такая конгруэнция σ, что $\sigma \subseteq \rho$ и σ имеет не более чем n^n классов (*теорема Пуанкаре*).

1.3.12. Пусть M — непустое подмножество полугруппы S. Определим на S отношение ρ_M, полагая

$$x \rho y \ \Leftrightarrow \ x = y \text{ или } x, y \in M.$$

а) **(У)** Убедиться, что если M — левый (соответственно правый) идеал полугруппы S, то ρ_M есть левая (соответственно правая) конгруэнция на S. Тем самым, если M — идеал полугруппы S, то ρ_M есть конгруэнция на S.

б) Для идеалов M и N данной полугруппы найти соотношения, связывающие $\rho_{M\cap N}$ и $\rho_{M\cup N}$ с ρ_M и ρ_N.

1.3.13. Рассмотрим на произвольной полугруппе S *правое отношение Грина* $\mathscr{R}$:

$a \mathscr{R} b \iff a = b$ или $a = bx$ и $b = ay$ для некоторых $x, y \in S$.

Левое отношение Грина $\mathscr{L}$ определяется симметрично правому.

а) Проверить, что $\mathscr{R}[\mathscr{L}]$ — левая [правая] конгруэнция на S.

б) Доказать, что отношения $\mathscr{R}$ и $\mathscr{L}$ перестановочны, т.е. $\mathscr{R} \circ \mathscr{L} = \mathscr{L} \circ \mathscr{R}$.

в) Описать отношения $\mathscr{R}$ и $\mathscr{L}$ на полугруппе левых нулей.

г) Описать отношения $\mathscr{R}$ и $\mathscr{L}$ на полугруппе из задания 1.1.8.

д) Описать отношения $\mathscr{R}$ и $\mathscr{L}$ на полугруппе B_2 из задания 1.1.4.

1.3.14. Для каждого преобразования $\varphi \in \mathcal{T}(X)$ через $\mathsf{Ker}\,\varphi$ обозначим эквивалентность на X, состоящую из всех пар (x, y), для которых $\varphi(x) = \varphi(y)$. Доказать, что для произвольных преобразований $\varphi, \psi \in \mathcal{T}(X)$:

а) $\varphi \mathscr{R} \psi$ означает, что $\mathsf{Ker}\,\varphi = \mathsf{Ker}\,\psi$,
б) $\varphi \mathscr{L} \psi$ означает, что $\mathsf{Im}\,\varphi = \mathsf{Im}\,\psi$.

1.3.15. Описать отношения Грина $\mathscr{R}$ и $\mathscr{L}$ на мультипликативной полугруппе всех линейных операторов на произвольном векторном пространстве. **(C)**

Глава 2

Группы

2.1 Примеры и простейшие свойства. Изоморфизм

2.1.1. Продолжая список групп, выявленных при выполнении заданий 1.1.1, 1.1.2 и 1.1.21, убедиться, что следующие множества являются группами:

а) **(У)** $(\mathbb{Q}_p, +)$;

б) **(У)** $(\mathbb{C}_{p^\infty}, \cdot)$;

в) промежуток $[0, 1)$ с операцией $\oplus$, где $\alpha \oplus \beta$ есть дробная часть $\alpha + \beta$;

г) множество всех функций из $\mathbb{R}$ в $\mathbb{R}$ вида $y = \frac{ax+b}{cx+d}$, где $a, b, c, d \in \mathbb{R}$ и $ad - bc \neq 0$, относительно операции суперпозиции.

2.1.2. (У) Пусть R — ассоциативное кольцо коммутативное с единицей. Убедиться, что следующие множества матриц являются группами относительно умножения матриц:

а) множество $\mathbf{GL}_n(R)$ всех обратимых $n \times n$-матриц над R;

б) множество $\mathbf{T}_n(R)$ всех обратимых верхнетреугольных $n \times n$-матриц над R;

в) множество $\mathbf{UT}_n(R)$ всех верхнетреугольных $n \times n$-матриц, у которых на главной диагонали стоят единицы, над R;

г) множество $\mathbf{D}_n(R)$ всех обратимых диагональных $n \times n$-матриц над R.

2.1.3. (У) Убедиться, что множество $\mathbf{SL}_n(K)$ всех $n \times n$-матриц над ассоциативным коммутативным кольцом K с единицей, определитель которых равен единице, является группой относительно умножения матриц.

2.1.4. Пусть G — группа, $a \in G$.

а) Доказать, что полугруппа G_a, определенная в задании 1.1.20, является группой.

б) Выяснить, изоморфны ли группы $\mathbb{Q}_2^+$ и $\mathbb{Q}_3^+$, $\mathbb{Q}_3^+$ и $\mathbb{Q}_4^+$.

в) Определить, при каких условиях G будет группой относительно операции $x * y = xya$.

2.1.5. (У) Показать, что $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. Изоморфны ли группы $(\mathbb{R}^+, \cdot)$ и $(\mathbb{R}^*, \cdot)$?

2.1.6. (У) а) Доказать, что группы $(Q, +)$ и $(\mathbb{Q}^*, \cdot)$ не изоморфны.

б) Изоморфны ли группы $(\mathbb{Q}, +)$ и $(\mathbb{Z}, +)$?

2.1.7. Доказать, что группа $(\mathbb{C}^*, \cdot)$ изоморфна подгруппе матриц из $\mathbf{GL}_2(\mathbb{R})$ вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

2.1.8. (И) Выделить в следующем списке групп классы изоморфных групп:

$(\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$,

$\mathbf{UT}_2(A)$, где A — одно из колец $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$,

$E(A)$ — мультипликативная группа вещественных чисел $\{\pi^a \mid a \in A\}$, где A — одно из колец $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

2.1.9. Доказать, что если в группе выполнено тождество $x^2 = 1$, то эта группа абелева.

2.1.10.* Пусть G — ненулевая аддитивная группа вещественных чисел такая, что в каждом ограниченном промежутке содержится лишь конечное число ее элементов. Доказать, что $G \cong \mathbb{Z}$.

2.1.11. Пусть $\delta_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$. Для каждой подстановки σ степени n определим матрицу $A_\sigma = (\delta_{i\sigma(j)})$. Доказать, что для каждой подгруппы G группы S_n множество матриц $\{A_\sigma \mid \sigma \in G\}$ образует подгруппу группы $\mathbf{GL}_n(\mathbb{Z})$, изоморфную группе G.

2.1.12. Доказать, что $\mathbf{D}_n(F) \cong F^* \times F^* \ldots \times F^*$ (n раз).

2.1.13. Каждую из указанных ниже мультипликативных групп разложить в прямое произведение неединичных групп:

а) $\mathbb{C}_6$, б) $\mathbb{C}^*$, в) $\mathbf{GL}_n(\mathbb{R})$, где n — нечетное натуральное число.

2.1.14. Доказать, что группы $(\mathbb{Q}_p, +)$ и $(\mathbb{Q}_q, +)$ не изоморфны для различных простых чисел p, q.

2.1.15. (У) Изоморфны ли группы $(\mathbb{C}_{p^\infty}, \cdot)$ и $(\mathbb{C}_{q^\infty}, \cdot)$ для различных простых чисел p и q?

2.1.16. Доказать, что подгруппа группы $\mathbf{GL}_2(\mathbb{Q})$, состоящая из матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, изоморфна мультипликативной группе чисел $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Q},\ a^2 + b^2 \neq 0\}, \cdot)$.

2.1.17. а) Доказать, что все группы порядка < 6 абелевы.

б) Доказать, что неабелева группа порядка 6 изоморфна симметрической группе S_3.

2.1.18. Элемент $[x, y] \rightleftharpoons xyx^{-1}y^{-1}$ называется *коммутатором* элементов x, y данной группы. Доказать, что в любой группе выполняются следующие тождества:

а) **(У)** $[x, y]^{-1} = [y, x]$; б) $[xy, z] = x[y, z]x^{-1}[x, z]$;

в) $[z, xy] = [z, x]x[z, y]x^{-1}$.

2.1.19. Любую группу можно рассматривать как группоид относительно операции взятия коммутатора $[,]$.

а) **(У)** Убедиться, что если группа G абелева, то группоид $(G, [,])$ есть коммутативная полугруппа.

б) Выяснить, верно ли обратное утверждение. **(С)**

в) Определить, является ли группоид $(S_3, [,])$ коммутативным и является ли он полугруппой.

2.1.20. а) Доказать, что в группе выполняется правый дистрибутивный закон $[xy, z] = [x, z][y, z]$ тогда и только тогда, когда в ней выполняется левый дистрибутивный закон $[z, xy] = [z, x][z, y]$. **(С)**

б) Доказать, что если в группе G выполняется тождество $[[x, y], z] = 1$, то в G выполняются дистрибутивные законы, указанные в п. а).

в) Привести пример группы, в которой не выполняется тождество $[[x, y], z] = 1$.

г)* Привести пример неабелевой группы, в которой выполняется тождество $[[x, y], z] = 1$.

2.2 Порождающие множества, подгруппы, порядки элементов

2.2.1. а) Найти все базисы группы $(\mathbb{Z}, +)$, состоящие из двух элементов;

б) Найти какой-нибудь базис группы $(\mathbb{Z}, +)$, состоящий из n элементов, где $n \in \mathbb{N}$, $n > 2$.

2.2.2. (У) Доказать, что группа $(\mathbb{C}_{p^\infty}, \cdot)$ не является конечно порожденной.

2.2.3. а) Доказать, что группа $(\mathbb{Q}, +)$ порождается множеством $\{\frac{1}{n} \mid n \in \mathbb{N}\}$.

б) **(У)** Является ли группа $(\mathbb{Q}, +)$ конечно порожденной?

в)* Выяснить, существует ли базис группы $(\mathbb{Q}, +)$.

2.2.4. Выяснить, существует ли базис группы $(\mathbb{Q}^*, \cdot)$.

2.2.5.* Выяснить, существует ли в группе $(\mathbb{Q}_p, \cdot)$: а) конечное порождающее множество, б) базис.

2.2.6. Пусть m, n — натуральные числа, $m \leq n$, и $\alpha_1, \ldots, \alpha_m$ — различные числа из множества $\{1, \ldots, n\}$. Рассмотрим элемент из S_n, который переводит α_1 в α_2, α_2 в α_3 и так далее, α_{m-1} — в α_m и α_m — в α_1. Такой элемент называется *циклом* длины m и обозначается через $(\alpha_1 \alpha_2 \ldots \alpha_m)$.

Доказать, что любой элемент группы S_n представим в виде произведения *независимых* циклов, т.е. циклов, каждая пара которых не имеет общих перемещаемых элементов.

2.2.7. Доказать, что каждое из следующих множеств является базисом группы S_6:

а) $\{(12), (34), (56), (23)(45)\}$;

б) $\{(12), (34), (123)(456)\}$;

в) $\{(12), (23), (24)(156)\}$.

2.2.8. Доказать, что группа S_n порождается:

а) множеством всех транспозиций на множестве $\{1, \ldots, n\}$,

б) множеством $\{(12), (13), \ldots, (1n)\}$,

в) множеством $\{(12), (123), \ldots, (12 \cdots n)\}$,

г) множеством $\{(12), (12 \cdots n)\}$.

2.2.9. Доказать, что любое множество, состоящее менее чем из $n-1$ транспозиций, не является порождающим множеством группы S_n.

2.2.10. Пользуясь результатом п, г) задания 2.2.8, найти для $n \geq 3$:

а) какой-нибудь базис полугруппы $\mathcal{T}_n$;

б) наименьшее число преобразований в базисе полугруппы $\mathcal{T}_n$.

2.2.11.* Пусть T — произвольное множество, состоящее из $n-1$ транспозиций на множестве $\{1, \ldots, n\}$. Через $G(T)$ обозначим граф на множестве вершин $\{1, \ldots, n\}$, в котором две вершины i и j смежны тогда и только тогда, когда $(ij) \in T$. Доказать, что множество T

порождает группу S_n в том и только в том случае, когда граф $G(T)$ является деревом, т.е. связным графом без замкнутых путей.

2.2.12. Пусть F — поле. Через e_n обозначим единичную $n \times n$-матрицу, а через e_{ij} — матричные единицы порядка n. Рассмотрим в группе $\mathbf{GL}_n(F)$ матрицы вида $t_{ij}(\alpha) = e_n + \alpha e_{ij}$, $d(\beta) = e_n + (\beta - 1)e_{nn}$, где $\alpha, \beta \in F$, $\beta \neq 0$, $i \neq j$. Матрицы t_{ij} называются *трансвекциями*. Доказать, что $\mathbf{GL}_n(F)$ порождается трансвекциями и матрицами $d(\beta)$. **(С)**

2.2.13. Доказать, что группа $\mathbf{T}_n(F)$ порождается трансвекциями $t_{ij}(\alpha)$ при $1 \leq i < j \leq n$, $\alpha \in F$ и диагональными матрицами с ненулевыми элементами на главной диагонали.

2.2.14. Доказать, что группа $\mathbf{UT}_n(F)$ порождается всеми трансвекциями $t_{ij}(\alpha)$ при $1 \leq i < j \leq n$, $\alpha \in F$.

2.2.15. Доказать, что группа $\mathbf{SL}_n(\mathbb{Z})$ порождается всеми матрицами $e_n + e_{ij}$ при $1 \leq i \leq n$, $1 \leq j \leq n$, $i \neq j$.

2.2.16. Доказать, что группа $\mathbf{SL}_n(\mathbb{Z})$ порождается двумя матрицами $e_n + e_{12}$ и $e_{12} + e_{23} + \ldots e_{n-1,n} + (-1)^{n-1} e_{n1}$.

2.2.17. (У) Доказать, что непустое подмножество H группы G будет подгруппой тогда и только тогда, когда $xy^{-1} \in H$ для любых $x, y \in H$.

2.2.18. Пусть A, B — произвольные подгруппы группы G. Доказать, что

а) **(У)** $A \cap B$ есть подгруппа в G,

б) $A \cup B$ является подгруппой тогда и только тогда, когда $A \subseteq B$ или $B \subseteq A$,

в) AB является подгруппой тогда и только тогда, когда $AB = BA$,

г)* если A, B — конечные подгруппы, то $|AB| \cdot |A \cap B| = |A| \cdot |B|$.

2.2.19. (У) Доказать, что нециклическая группа четвертого порядка есть прямое произведение двух циклических групп второго порядка. **(С)**

2.2.20. (У) а) Доказать, что пересечение любых двух ненулевых подгрупп группы $(\mathbb{Q}, +)$ есть ненулевая подгруппа.

б) Справедливо ли такое же утверждение для группы $(\mathbb{R}, +)$?

2.2.21. Указать все элементы подгрупп:

а) группы $(\mathbb{Z}, +)$, порожденных множествами $\{2\}$, $\{3, 4\}$, $\{15, 9\}$,

б) группы $\mathbb{C}^*$, порожденных множествами $\{i\}$, $\{-\frac{1}{2} + \frac{\sqrt{3}}{2} i\}$, $\{2, i\}$.

2.2.22. Через e обозначим единицу группы S_4. Определить, будут ли следующие множества подстановок подгруппами группы S_4:

а) $\{e, (12)(34), (13)(24), (14)(23)\}$;

б) $\{e,\ (13),\ (24),\ (12)(34),\ (13)(24),\ (14)(23),\ (1234),\ (1432)\}$.

2.2.23. Доказать, что любая подгруппа циклической группы является циклической (ср. с ситуацией для полугрупп, см. задание 1.2.8).

2.2.24. Пусть $G = \langle a \rangle$ — циклическая группа порядка n. Найти все ее подгруппы при

а) $n = 24$, б) $n = 100$, в) $n = 360$,

г) $n = 125$, д) $n = p^m$, где p — простое число.

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

а) элементы a^k и a^l имеют одинаковые порядки тогда и только тогда, когда $\text{НОД}(k, n) = \text{НОД}(l, n)$,

б) элемент a^k является порождающим элементом группы G тогда и только тогда, когда k и n взаимно просты,

в) всякая подгруппа H группы G порождается элементом вида a^d, где d делит n,

г) для всякого делителя d числа n существует единственная подгруппа H группы G порядка d.

2.2.26. а) Доказать, что всякая собственная подгруппа группы $\mathbb{C}_{p^\infty}$ является циклической.

б) **(У)** Из утверждений предыдущего задания и задания 2.2.2 вывести, что каждое конечное подмножество из $\mathbb{C}_{p^\infty}$ порождает циклическую подгруппу.

2.2.27. а) Доказать, что любая подгруппа порядка n группы $\mathbb{C}^*$ совпадает с $\mathbb{C}_n$.

б)* Доказать, что любая конечная подгруппа мультипликативной группы произвольного поля является циклической.

2.2.28. а) **(У)** Сформулировать критерий изоморфности двух конечных циклических групп.

б) Воспользовавшись этим критерием, найти критерий изоморфности двух циклических полугрупп. **(С)**

2.2.29. Пусть элемент $g \in S_n$ представлен в виде произведения независимых циклов:

$$g = (\alpha_{11} \dots \alpha_{1k_1})(\alpha_{21} \dots \alpha_{2k_2}) \dots (\alpha_{m1} \dots \alpha_{mk_m}),$$

где $\{\alpha_{11}, \dots, \alpha_{1k_1}, \alpha_{21}, \dots, \alpha_{2k_2}, \alpha_{m1}, \dots, \alpha_{mk_m}\} = \{1, 2, \dots, n\}$ и $k_1, \dots, k_m \geq 1$, и пусть

$$h = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1k_1} & \alpha_{21} & \dots & \alpha_{2k_2} & \dots & \alpha_{m1} & \dots & \alpha_{mk_m} \\ \beta_{11} & \dots & \beta_{1k_1} & \beta_{21} & \dots & \beta_{2k_2} & \dots & \beta_{m1} & \dots & \beta_{mk_m} \end{pmatrix}$$

— элемент из S_n. Доказать, что тогда в S_n выполняется равенство

$$hgh^{-1} = (\beta_{11} \dots \beta_{1k_1})(\beta_{21} \dots \beta_{2k_2}) \dots (\beta_{m1} \dots \beta_{mk_m}).$$

2.2.30. Элемент a группы G называется *сопряженным* с элементом b этой группы, если существует $x \in G$ такой, что $a = xbx^{-1}$.

а) Убедиться, что отношение "быть сопряженным" является отношением эквивалентности на любой группе.

б) Убедиться, что сопряженные элементы группы имеют одинаковые порядки.

в) Проверить, что два элемента из S_n сопряжены тогда и только тогда, когда они имеют одинаковое число циклов каждой длины в своих разложениях в произведения независимых циклов.

2.2.31. Доказать, что если φ — изоморфизм группы G на группу H, то для любого $g \in G$ элементы g и $\varphi(g)$ имеют одинаковые порядки.

2.2.32. Найти порядки следующих элементов мультипликативной группы целочисленных матриц:

а) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, б) $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, в) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, г) $\begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}$.

2.2.33. Найти порядки следующих элементов различных групп:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} \in S_6$;

в) $\frac{-\sqrt{3}}{2} + \frac{1}{2}i \in \mathbb{C}^*$; г) $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i \in \mathbb{C}^*$;

д) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathbf{GL}_4(\mathbb{R})$; е) $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{C})$;

ж) $\begin{pmatrix} -1 & a \\ 1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{C})$.

2.2.34. Найти порядки следующих элементов группы S_8:
а) (12345678), б) (2345)(1678), в) (12345)(678), г) (123)(45)(78).

2.2.35. Определить наибольший порядок элементов в группе S_8.

2.2.36. Определить, элементы каких порядков могут содержаться в группах: а) $\mathbb{Z}_4$, б) $\mathbb{Z}_5$, в) $\mathbb{Z}_8$, г) S_3, д) S_4.

2.2.37. Пусть A_5 — подгруппа всех четных подстановок группы S_5. Доказать, что A_5 не содержит элементов порядка 6, хотя 6 делит порядок A_5.

2.2.38. Определить, какие из следующих тождеств выполняются в симметрической группе S_3: а) $x^6 = 1$, б) $[[x, y], z] = 1$, в) $[x^2, y^2] = 1$.

2.2.39. а) Найти порядок класса вычетов числа 2 в мультипликативной группе поля $\mathbb{Z}_p$ для $p = 3, 5, 7, 11$.

б) Определить, в каких из групп, указанных в п. а), класс вычетов числа 2 является порождающим элементом.

2.2.40. а) **(У)** Объяснить, что в группе $\mathbb{C}^*$ каждый элемент конечного порядка имеет модуль, равный 1.

б) То, что утверждение, обратное к утверждению из п. а), неверно, демонстрирует, например, число $\frac{3}{5} + \frac{4}{5}i$; убедиться, что это число есть элемент бесконечного порядка в группе $\mathbb{C}^*$.

в) **(У)** То, что утверждение, обратное к утверждению из п. а), неверно, можно объяснить и не приводя контрпримера; привести соответствующие рассуждения.

2.2.41. а) Показать, что если в группе с единицей e элементы a и b имеют конечные порядки и $ab = ba$, $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$, то ab имеет порядок, равный наименьшему общему кратному порядков a и b.

б) **(У)** Используя доказанное в п. а) утверждение, убедиться, что порядок подстановки, представленной в виде произведения независимых циклов, равен наименьшему общему кратному длин этих циклов.

в) Доказать, что если числа m и n взаимно просты, то циклическая группа порядка mn изоморфна прямому произведению циклической группы порядка m и циклической группы порядка n.

2.2.42. Пусть порядок элемента x группы равен n, где $n \in \mathbb{N}$. Найти порядок элемента x^k для любого $k \in \mathbb{N}$.

2.2.43. В циклической группе $\langle a\rangle$ порядка n найти все элементы g, удовлетворяющие условию $g^k = 1$, и все элементы порядка k при

а) $n = 24$, $k = 6$, б) $n = 24$, $k = 4$, в) $n = 100$, $k = 20$,

г) $n = 100$, $k = 5$, д) $n = 100$, $k = 6$, е) $n = 100$, $k = 7$.

2.2.44. Найти число элементов порядка p^m в циклической группе порядка p^n, где p — простое число, $0 < m \leq n$.

2.2.45. Доказать, что если в конечной группе имеется инволюция (элемент второго порядка), то число инволюций в этой группе нечетно.

2.2.46. Пусть G — конечная группа и $d(G)$ — наименьшее среди натуральных чисел s таких, что $g^s = 1$ для всякого $g \in G$ (*период группы* G). Доказать, что

а) период группы G делит ее порядок и равен наименьшему общему кратному порядков элементов группы G,

б) если группа G абелева, то существует элемент $g \in G$ порядка $d(G)$,

в) конечная абелева группа является циклической тогда и только тогда, когда ее период и порядок совпадают.

2.2.47.* Выяснить, верно ли для неабелевых групп утверждение, аналогичное утверждению п. б) задания 2.2.46.

2.2.48. Группа называется *периодической*, если каждая ее циклическая подгруппа конечна.

а) Привести примеры абелевой и неабелевой бесконечных периодических групп.

б) Доказать, что всякая подполугруппа периодической группы является ее подгруппой.

2.2.49. *Периодической частью* группы называется множество всех ее элементов конечного порядка.

а) Доказать, что периодическая часть абелевой группы является подгруппой.

б) Найти периодическую часть групп $\mathbb{C}^*$ и $\mathbf{D}_n(\mathbb{C})$.

2.2.50. Доказать, что если абелева группа G имеет элементы бесконечного порядка и все они принадлежат подгруппе H, то $H = G$.

2.2.51. Пусть H — подгруппа группы G, $g \in G$. Найти смежный класс gH в следующих случаях:

а) $G = (\mathbb{R}^*, \cdot)$, $H = \mathbb{R}^+$, $g = -3$;

б) $G = (\mathbb{R}^*, \cdot)$, $H = \{-1, 1\}$, $g = -3$;

в) $G = (\mathbb{C}^*, \cdot)$, $H = \mathbb{R}^+$, $g = 1 - i$;

г) $G = (\mathbb{C}^*, \cdot)$, $H = \{z \in \mathbb{C}^* \mid |z| = 1\}$, $g = 1 + i$.

2.2.52. Найти левый и правый смежные классы группы $G = S_3$:

а) по подгруппе H, порожденной циклом (12), для элемента $g =$ (13),

б) по подгруппе H, порожденной циклом (13), для элемента $g =$ (123).

2.2.53. Найти все смежные классы группы $(\mathbb{Z}, +)$:

а) по подгруппе $3\mathbb{Z}$, б) по подгруппе $n\mathbb{Z}$.

2.2.54. Найти все смежные классы группы $\mathbb{C}^*$:

а) по подгруппе $\mathbb{R}^+$, б) по подгруппе $\{z \in \mathbb{C}^* \mid |z| = 1\}$.

Охарактеризовать эти результаты в геометрических терминах (относящихся к комплексной плоскости).

2.2.55. Пусть G — произвольная группа. Доказать, что каждая левая конгруэнция на группе G (определение см. в задании 1.3.13)

определяет разложение G на левые смежные классы по некоторой ее подгруппе H, и обратно — любое разложение G на левые смежные классы по некоторой ее подгруппе определяет левую конгруэнцию на группе G.

2.3 Гомоморфизмы и факторгруппы

2.3.1. (У) Определить, какие из следующих отображений φ группы $(\mathbb{Z}, +)$ в себя являются эндоморфизмами:
а) $\varphi(x) \rightleftharpoons 3x$; б) $\varphi(x) \rightleftharpoons 3x + 2$;
в) $\varphi(x) \rightleftharpoons x^3$; г) $\varphi(x) \rightleftharpoons 0$.

2.3.2. Определить, какие из следующих отображений $\varphi : (\mathbb{C}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$ являются гомоморфизмами:
а) $\varphi(z) \rightleftharpoons |z|$; б) $\varphi(z) \rightleftharpoons 2|z|$; в) $\varphi(z) \rightleftharpoons \frac{1}{|z|}$;
г) $\varphi(z) \rightleftharpoons 1 + |z|$; д) $\varphi(z) \rightleftharpoons |z|^2$; е) $\varphi(z) \rightleftharpoons 1$;
ж) $\varphi(z) \rightleftharpoons 2$.

2.3.3. (У) Убедиться, что отображение φ группы G в себя, определенное правилом $\varphi(x) \rightleftharpoons x^{-1}$, является автоморфизмом тогда и только тогда, когда G абелева.

2.3.4. Найти необходимые и достаточные условия для группы G, чтобы отображение $\varphi : G \longrightarrow G$, определенное правилом $\varphi(x) \rightleftharpoons x^2$, было а) эндоморфизмом, б) автоморфизмом.

2.3.5. Найти все гомоморфизмы
а) из группы $(\mathbb{Z}, +)$ в группу $(\mathbb{Z}_n, +)$,
б) из группы $(\mathbb{Z}_{15}, +)$ в группу $(\mathbb{Z}_3, +)$,
в) из группы $(\mathbb{Z}_7, +)$ в группу $(\mathbb{Z}_3, +)$.

2.3.6. Доказать, что следующие отображения являются гомоморфизмами и найти их ядра:
а) $\varphi : \mathbb{Q}^* \longrightarrow \mathbb{Q}^+$, $\varphi(x) \rightleftharpoons |x|$;
б) $\varphi : \mathbb{C}^* \longrightarrow \mathbb{R}^*$, $\varphi(x) \rightleftharpoons |x|$;
в) $\varphi : \mathbf{GL}_n(F) \longrightarrow F^*$, $\varphi(X) \rightleftharpoons \det(X)$;
г) $\varphi : \mathbb{R} \longrightarrow \{z \in \mathbb{C}^* \mid |z| = 1\}$, $\varphi(x) \rightleftharpoons \cos x + i \sin x$;
д) $\varphi : \mathbb{C}^* \longrightarrow \mathbb{C}^*$, $\varphi(z) \rightleftharpoons z^n$.

2.3.7. Доказать, что отображение $\mathbf{T}_n(K) \longrightarrow \mathbf{D}_n(K)$, сопоставляющее каждой треугольной матрице диагональную матрицу, на главной диагонали которой расположены соответствующие элементы исходной матрицы, является гомоморфизмом, и найти его ядро.

2.3.8. Для группы G множество

$$Z(G) = \{z \in G \mid az = za \text{ для любого } a \in G\}$$

называется ее *центром*.

а) **(У)** Доказать, что центр группы является ее нормальной подгруппой.

б) Привести пример неабелевой группы с неединичным центром.

в) Доказать, что факторгруппа группы по ее центру не может быть неединичной циклической группой.

г) Убедиться, что факторгруппа группы $\mathbf{UT}_3(\mathbb{Z})$ по ее центру является неединичной абелевой группой.

2.3.9. а) **(У)** Убедиться, что в абелевой группе любая подгруппа нормальна.

б)* Выяснить, верно ли обратное утверждение. **(С)**

2.3.10. Доказать, что множество всех четных подстановок образует нормальную подгруппу симметрической группы S_n.

2.3.11. Доказать, что группа $\mathbf{SL}_n(F)$ является нормальной подгруппой в группе $\mathbf{GL}_n(F)$ над полем F.

2.3.12. Доказать, что

а) факторгруппа $\mathbb{Q}_p/\mathbb{Z}$ изоморфна группе $\mathbb{C}_{p^\infty}$,

б) факторгруппа $\mathbb{C}_{p^\infty}/\mathbb{C}_p$ изоморфна группе $\mathbb{C}_{p^\infty}$.

2.3.13. Охарактеризовать факторгруппы (указав изоморфные им аддитивные или мультипликативные группы чисел)

а) $(\mathbb{R}^*, \cdot)$ по $(\mathbb{R}^+, \cdot)$, б) $(\mathbb{C}^*, \cdot)$ по $(\{z \in \mathbb{C}^* \mid |z| = 1\}, \cdot)$,

в) $(\mathbb{C}^*, \cdot)$ по $(\mathbb{C}_n, \cdot)$, г) $(\mathbb{R}^*, \cdot)$ по $(\{-1, 1\}, \cdot)$,

д) $(\mathbb{C}, +)$ по $(\mathbb{R}, +)$, е) $(\mathbb{R}, +)$ по $(\mathbb{Z}, +)$,

ж) $(\mathbb{Q}, +)$ по $(\mathbb{Z}, +)$.

2.3.14. Пусть $G = \mathbf{UT}_3(F)$, где F — поле, H — подмножество G, состоящее из всех матриц вида $\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Доказать, что H — нормальная подгруппа в G и что факторгруппа G/H абелева.

2.3.15. Доказать, что $\mathbf{UT}_n(K)$ — нормальная подгруппа группы $\mathbf{T}_n(K)$ и найти факторгруппу $\mathbf{T}_n(K)/\mathbf{UT}_n(K)$.

2.3.16. Через e обозначим единицу группы S_4 и рассмотрим множество подстановок $H = \{e, (12)(34), (13)(24), (14)(23)\}$. Доказать, что H — нормальная подгруппа в S_4 и $S_4/H \cong S_3$.

Глава 3

Кольца

3.1 Примеры и простейшие свойства. Изоморфизм

3.1.1. Выяснить, какие из перечисленных ниже числовых множеств являются кольцами относительно обычного сложения и умножения чисел (при ответах воспользоваться подходящими заданиями из §§1.1, 2.1) и какие из выявленных колец оказываются полями:

а) $\mathbb{Z}$; б) $\mathbb{Q}$; в) $\mathbb{R}$; г) $\mathbb{C}$;

д) множество чисто мнимых комплексных чисел;

е) $\{x = a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$; ж) $\{x = a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$;

з) множество рациональных чисел, в записи которых несократимой дробью знаменатели делят фиксированное число $n \in \mathbb{N}$;

и) множество рациональных чисел, в записи которых несократимой дробью знаменатели не делятся на фиксированное простое число p;

к) $\mathbb{Q}_p$;

л) $\{x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b \in \mathbb{Q}\}$;

м) $\{x = a + bi \mid a, b \in \mathbb{Z}\}$;

н) $\{x = a + bi \mid a, b \in \mathbb{Q}\}$.

3.1.2. Выяснить, какие из указанных множеств матриц образуют кольцо относительно матричного сложения и умножения и какие из выявленных колец оказываются полями:

а) множество вещественных симметрических $n \times n$-матриц;

б) множество вещественных ортогональных $n \times n$-матриц;

в) множество вещественных верхнетреугольных $n \times n$-матриц;

г) множество вещественных $n \times n$-матриц ($n \geq 2$), у которых две последние строки — нулевые;

д) множество матриц вида $\begin{pmatrix} x & y \\ dy & x \end{pmatrix}$, где d — фиксированное целое число, $x, y \in \mathbb{Z}$;

е) множество матриц вида $\begin{pmatrix} x & y \\ dy & x \end{pmatrix}$, где d — фиксированное рациональное число, $x, y \in \mathbb{Q}$; **(С)**

ж) множество матриц вида $\begin{pmatrix} x & y \\ dy & x \end{pmatrix}$, где d — фиксированное вещественное число, $x, y \in \mathbb{R}$;

з) множество комплексных матриц вида $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$;

и) множество вещественных матриц вида
$$\begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix}.$$

3.1.3. *Симметрической разностью* множеств A и B называется множество $A \dot{-} B = (A \backslash B) \cup (B \backslash A)$.

Доказать, что для любого множества X множество $\mathcal{P}(X)$ является кольцом относительно операций взятия симметрической разности и пересечения.

3.1.4. (У) Объяснить, почему множество всех векторов вещественного трехмерного пространства является кольцом относительно операций сложения и векторного умножения.

3.1.5. Пусть K — ассоциативное кольцо.

а) Доказать, что множество K является кольцом относительно исходной операции сложения и новой операции умножения, заданной правилом $x \circ y = xy - yx$.

б) Привести пример кольца K, для которого операция $\circ$ неассоциативна.

в) Привести пример некоммутативного кольца K, для которого операция $\circ$ ассоциативна.

3.1.6. Выполнить задания, аналогичные заданиям 3.1.5, для операции $*$, заданной правилом $x * y = xy + yx$.

3.1.7. (И) Описать все 3-элементные ассоциативные кольца.

3.1.8. а) *Следом* квадратной матрицы называется сумма элементов ее главной диагонали. Проверить, что множество вещественных $n \times n$-матриц с нулевым следом является кольцом относительно операции $\circ$, описанной в задании 3.1.5 а).

б) Проверить, что множество вещественных кососимметрических $n \times n$-матриц является кольцом относительно операции $\circ$, описанной в задании 3.1.5 а).

в) Проверить, что множество вещественных симметрических $n \times n$-матриц является кольцом относительно операции $*$, описанной в задании 3.1.6 а).

3.1.9. Пусть X — произвольное множество, K — произвольное кольцо. Через $\mathcal{F}(X, K)$ обозначим множество всех функций из X в K. Определим операции сложения и умножения на функциях из $\mathcal{F}(X, K)$ поточечно: для любых $f, g \in \mathcal{F}(X, K)$ положим $(f + g)(x) \rightleftharpoons f(x) + g(x)$, $(fg)(x) \rightleftharpoons f(x)g(x)$ для любых $x \in X$. Проверить, что относительно этих операций множество $\mathcal{F}(X, K)$ является кольцом.

3.1.10. Определить, какие из указанных множеств функций из $\mathbb{R}$ в $\mathbb{R}$ образуют кольцо относительно операций сложения и умножения функций, определенных в задании 3.1.9:

а) множество всех функций вещественного переменного, непрерывных на отрезке $[a, b]$;

б) множество всех функций вещественного переменного, имеющих на промежутке (a, b) вторую производную;

в) множество всех функций вещественного переменного, обращающихся в нуль на некотором подмножестве $D \subseteq \mathbb{R}$.

3.1.11. (И) Любую аддитивную абелеву группу A можно превратить в ассоциативное кольцо введением подходящего умножения, например полагая $xy = 0$ для любых $x, y \in A$. Выяснить, любую ли

полугруппу с нулем можно превратить в ассоциативное кольцо введением подходящего сложения.

3.1.12. (У) Доказать, что поле $\mathbb{Q}$ не изоморфно ни полю $\mathbb{R}$, ни полю $\mathbb{C}$.

3.1.13. а) Доказать, что при каждом неотрицательном целом d кольцо из задания 3.1.2 д) изоморфно кольцу

$$\mathbb{Z}(\sqrt{d}) \rightleftharpoons \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

б) Доказать, что при каждом отрицательном целом d кольцо из задания 3.1.2 д) изоморфно кольцу

$$\mathbb{Z}(\sqrt{d}) \rightleftharpoons \{a + b\sqrt{-di} \mid a, b \in \mathbb{Z}\},$$

состоящему из комплексных чисел.

в) Разбить на классы изоморфных колец кольца из задания 3.1.2 е) при всевозможных рациональных значениях d.

3.1.14. Найти все делители нуля в следующих кольцах:

а) $\mathbb{Z}_9$; б) $\mathbb{Z}_{12}$; в) $\mathbb{Z}_8$; г) $\mathbb{Z}$.

3.1.15. Выяснить, при каких значениях d кольцо, определенное в п. д) задания 3.1.2, не имеет делителей нуля.

3.1.16. Доказать, что в кольце всех матриц данного порядка над произвольным полем ненулевые вырожденные матрицы и только они являются делителями нуля.

3.1.17. Доказать, что если конечное ассоциативное кольцо не имеет делителей нуля, то оно имеет единицу и все его ненулевые элементы обратимы. **(С)**

3.1.18. Пусть K — ассоциативное кольцо с единицей e, a — элемент из K. Элемент a из K называется *нильпотентным*, если $a^n = 0$ для некоторого натурального n.

Доказать, что если a — нильпотентный элемент, то элемент $e + a$ обратим.

3.1.19. Найти все обратимые элементы, все делители нуля и все нильпотентные элементы в следующих кольцах:

а) $\mathbb{Z}_n$;

б) $\mathbb{Z}_{p^n}$, где p — простое число;

в) $\mathbf{M}_2(\mathbb{R})$.

3.1.20. Пусть K — ассоциативное коммутативное кольцо с единицей и пусть $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$. Доказать следующие утверждения:

а) $f(x)$ является обратимым элементом тогда и только тогда, когда a_0 — обратимый элемент, а $a_1, \ldots, a_n$ — нильпотентные элементы;

б) $f(x)$ является нильпотентным элементом тогда и только тогда, когда $a_0, a_1, \ldots, a_n$ — нильпотентные элементы;

в) $f(x)$ является делителем нуля тогда и только тогда, когда существует ненулевой элемент a кольца K такой, что $af(x) = 0$.

3.1.21. Пусть K_1, K_2, …, K_n — кольца. Проверить, что декартово произведение $K_1 \times K_2 \times \cdots \times K_n$ является кольцом относительно покомпонентно определенных операций:

$$(r_1, g_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) \rightleftharpoons (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n),$$
$$(r_1, r_2, \ldots, r_n) \cdot (s_1, s_2, \ldots, s_n) \rightleftharpoons (r_1 s_1, r_2 s_2, \ldots, r_n s_n)$$
$$\text{для всех } r_i, s_i \in K_i,\ i = 1, 2, \ldots, n.$$

Кольцо $K_1 \times K_2 \times \cdots \times K_n$ называется *прямым произведением* колец K_1, K_2, …, K_n.

3.1.22. (У) Пусть $K = K_1 \times K_2 \times \ldots \times K_n$. Определить, при каких условиях на кольца K_1, K_2, …, K_n кольцо K:

а) коммутативно, б) ассоциативно,

в) имеет единицу, г) будет полем.

3.1.23. Показать, что если натуральное число n имеет каноническое разложение на простые множители $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, то кольцо вычетов $\mathbb{Z}_n$ изоморфно кольцу

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_2^{k_m}}.$$

3.1.24. Пусть X — произвольное конечное множество, $|X| = n$, K — произвольное кольцо. Доказать, что кольцо $\mathcal{F}(X, K)$, определенное в задании 3.1.9, изоморфно кольцу $\underbrace{K \times K \times \ldots \times K}_{n \text{ раз}}$.

3.1.25. (У) Охарактеризовать в терминах соответствующих элементов колец K_i

а) все обратимые элементы прямого произведения
$K_1 \times K_2 \times \ldots \times K_n$,

б) все делители нуля в $K_1 \times K_2 \times \ldots \times K_n$,

в) все нильпотентные элементы в $K_1 \times K_2 \times \ldots \times K_n$.

3.2 Порождающие множества, подкольца

3.2.1. Убедиться, что каждое из следующих колец имеет базис и найти один из базисов этого кольца: а) $\mathbb{Z}$, б) $\mathbb{Z}\times\mathbb{Z}$, в) $\mathbb{Z}[x]$, г) $\mathbf{M}_2(\mathbb{Z})$, д) $\mathbf{M}_n(\mathbb{Z})$, е) $\mathbf{M}_2(\mathbb{Z}[x])$.

3.2.2. Доказать, что для любого натурального числа n кольцо $\mathbb{Z}$ имеет базис, состоящий из n элементов.

3.2.3. а) Доказать, что кольцо $\mathbb{Q}$ не является конечно порожденным.

б) Доказать, что множество $\{\frac{1}{p} \mid p\text{–простое число}\}$ является базисом кольца $\mathbb{Q}$.

3.2.4. (У) Найти все подкольца следующих колец: а) $\mathbb{Z}$, б) $\mathbb{Z}_3$, в) $\mathbb{Z}_9$, г) $\mathbb{Z}_{12}$.

3.2.5. Найти все подкольца кольца $\mathbb{Z}_3 \times \mathbb{Z}_3$.

3.2.6. а) Выяснить, может ли кольцо быть теоретико-множественным объединением двух своих собственных подколец.

б) **(У)** Проверить, что кольцо $\mathbb{Z}_2\times\mathbb{Z}_2$ является теоретико-множественным объединением трех своих собственных подколец.

3.2.7. а) Доказать, что в коммутативном ассоциативном кольце подкольцо, порожденное двумя конечными подкольцами, само конечно.

б)* Выяснить, верно ли утверждение п. а) для произвольных ассоциативных колец.

3.2.8. Найти подкольца кольца $\mathbf{M}_2(\mathbb{Z})$, порожденные следующими матрицами:

$$\text{а) } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \text{ б) } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \text{ в) } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

3.2.9. (У) Через K обозначим подкольцо кольца $\mathbb{R}$, порожденное числами $1, \pi$. Убедиться, что $K \cong \mathbb{Z}[x]$. **(С)**

3.2.10. Найти в кольце $\mathbb{Z}[x]$ подкольца, порожденные следующими многочленами: а) x; б) x^2, x^3; в) x, x^2+2; г) x^2, x^5.

3.2.11. Найти подкольца кольца $\mathbb{R}$, порожденные следующими множествами: а) $\{2,3\}$; б) $\{1,\sqrt{2}\}$; в) $\{1,\sqrt{2},\sqrt{3}\}$.

3.2.12. Пусть K — конечно порожденное коммутативное кольцо. Выяснить, будут ли конечно порожденными следующие кольца: а) $K\times K$; б) $K[x]$; в)* $\mathbf{M}_n(K)$. **(С)**

3.2.13. (У) Доказать, что кольца $\mathbb{R}$ и $\mathbb{C}$ не являются конечно порожденными.

3.2.14. Доказать, что кольцо функций $\mathcal{F}(X, K)$, введенное в задании 3.1.9, конечно порождено тогда и только тогда, когда X конечно и K конечно порождено. **(С)**

3.2.15. Элемент a кольца K называется *центральным*, если $ax = xa$ для любого $x \in K$. Множество всех центральных элементов кольца называется его *центром* и обозначается $Z(K)$.

а) **(У)** Доказать, что центр любого ассоциативного кольца является его подкольцом.

б) Найти центр кольца $\mathbf{M}_n(\mathbb{R})$.

в) Доказать, что $Z(K_1 \times K_2) = Z(K_1) \times Z(K_2)$.

3.2.16. (У) а) Вспоминив результат п. а) задания 3.2.4, убедиться, что в кольце $\mathbb{Z}$ любое подкольцо является идеалом.

б) Указать идеал полугруппы $(\mathbb{Z}, \cdot)$, не являющийся идеалом кольца $\mathbb{Z}$.

3.2.17.* Найти все идеалы кольца матриц $\mathbf{M}_n(\mathbb{Z})$ для $n = = 2, 3, \ldots$. **(С)**

3.2.18. а) Доказать, что в кольце многочленов $F[x]$ над полем F каждый ненулевой идеал представим в виде $f(x)F[x]$, где $f(x)$ — некоторый многочлен со старшим коэффициентом 1.

б) Выяснить, будет ли многочлен $f(x)$ определяться исходным идеалом однозначно.

3.2.19. Доказать, что если идеал I кольца R содержит обратимый элемент, то $I = R$.

3.2.20. Выяснить, образуют ли идеал необратимые элементы следующих колец: а) $\mathbb{Z}_9$; б) $\mathbb{Z}_{12}$; в) $\mathbb{Z}_{16}$.

3.2.21. а) **(У)** Доказать, что в любом кольце K множество $\{a \in K \mid ax = xa = 0$ для любого $x \in K\}$ является идеалом. Этот идеал называется *аннулятором* кольца K.

б) Привести пример кольца K, аннулятор которого отличен от $\{0\}$ и K.

3.2.22. Пусть K — коммутативное ассоциативное кольцо.

а) Доказать, что множество всех нильпотентных элементов кольца K образует идеал. Этот идеал называется *нильрадикалом* кольца K.

б) Привести пример кольца K, нильрадикал которого совпадает с аннулятором и отличен от $\{0\}$ и K.

в) Привести пример кольца K, нильрадикал которого отличен от аннулятора K.

г) Пусть пересечение всех ненулевых идеалов кольца K отлично от $\{0\}$. Доказать, что множество, состоящее из нуля и всех делителей нуля кольца K, образует идеал.

3.2.23. Кольцо называется *простым*, если оно не имеет нетривиальных идеалов. Доказать, что ассоциативное коммутативное кольцо с единицей является простым тогда и только тогда, когда оно есть поле. **(С)**

3.2.24.* а) Доказать, что кольцо $\mathbf{M}_n(F)$ над полем F является простым. **(С)**

б) Доказать, что кольцо всех векторов обычного трехмерного пространства (с операцией векторного произведения) является простым.

3.2.25. Идеал I кольца R называется *максимальным*, если $I \subset R$ и не существует такого идеала J, что $I \subset J \subset R$. Найти все максимальные идеалы:

а) **(У)** кольца $\mathbb{Z}$;

б) кольца $\mathbb{Z}\times\mathbb{Z}$;

в) кольца вещественных верхнетреугольных 2×2-матриц с обычными операциями матричного сложения и умножения;

г)* кольца вещественных верхнетреугольных 2×2-матриц с операциями сложения и $\circ$ (см. задание 3.1.5);

д)* кольца вещественных верхнетреугольных 2×2-матриц с операциями сложения и $*$ (см. задание 3.1.6).

3.3 Гомоморфизмы и факторкольца

3.3.1. Пусть отображение $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ ставит в соответствие целому числу (неотрицательный) остаток от деления его на n. Доказать, что φ является гомоморфизмом колец.

3.3.2. Пусть $K = \mathbb{R}[x]$ и отображение $\varphi : K \longrightarrow \mathbb{C}$ ставит в соответствие многочлену $f(x)$ комплексное число $f(i)$. Доказать, что φ — гомоморфизм колец, и найти его ядро.

3.3.3. Пусть $K = \mathbb{Q}[x]$ и отображение $\varphi : K \longrightarrow \mathbb{C}$ ставит в соответствие многочлену $f(x)$ комплексное число $f(-1/2 + i\sqrt{3}/2)$. Доказать, что φ — гомоморфизм колец, и найти его ядро.

3.3.4. Пусть $K = \mathbb{Q}[x]$ и отображение $\varphi : K \longrightarrow \mathbb{R}$ ставит в соответствие многочлену $f(x)$ действительное число $f(\sqrt{2})$. Доказать,

что φ — гомоморфизм колец, и найти его ядро.

3.3.5. Доказать, что кольцо $K = \mathbb{Q}[x_1, x_2, \ldots]$ многочленов от счетного множества переменных изоморфно своему факторкольцу по ненулевому идеалу $I = x_1 K$.

3.3.6. Пусть $K = \{a + bi \mid a, b \in \mathbb{Z}\}$ — кольцо целых гауссовых чисел, $J = \{2z \mid z \in K\}$. Доказать, что J — идеал в K и найти делители нуля в K/J.

3.3.7. Пусть F — поле. Доказать, что если многочлены f, g из $F[x]$ взаимно просты, то

$$F[x]/fgF[x] \cong F[x]/fF[x] \times F[x]/gF[x].$$

3.3.8. Пусть F — поле и f пробегает множество всех многочленов степени 2 из $F[x]$. Разбить на классы попарно изоморфных колец совокупность колец $F[x]/fF[x]$ для случаев, когда: а) $F = \mathbb{C}$, б) $F = \mathbb{R}$, в) $F = \mathbb{Q}$, г) F — конечное поле.

3.3.9. Найти все обратимые элементы, все делители нуля и все нильпотентные элементы в кольце $F[x]/f(x)F[x]$, где F — поле, $f(x)$ — фиксированный многочлен.

3.3.10. (*Китайская теорема об остатках*). Пусть K — кольцо с единицей, I_1 и I_2 — такие его идеалы, что $K = I_1 + I_2$. Доказать, что отображение $\varphi : x \mapsto (x+I_1, x+I_2)$ является сюръективным гомоморфизмом кольца K на прямое произведение колец $K/I_1 \times K/I_2$. **(C)**

3.3.11. Пусть K — коммутативное ассоциативное кольцо. Доказать, что факторкольцо кольца K по его нильрадикалу (см. задание 3.2.22) не содержит ненулевых нильпотентных элементов.

3.3.12. Доказать, что идеал I кольца R является максимальным тогда и только тогда, когда факторкольцо R/I простое.

3.4 Модули и алгебры над ассоциативным кольцом

3.4.1. Пусть K — ассоциативное кольцо с единицей 1, S — подкольцо кольца K, содержащее 1. Показать, что K является модулем над S.

3.4.2. Доказать, что всякую аддитивную абелеву группу можно превратить в модуль над кольцом целых чисел.

3.4.3. Пусть K — ассоциативное кольцо с единицей, J — идеал K. Доказать, что идеал J и факторкольцо K/J можно превратить в K-модули сохраняя операции сложения в J и K/J соответственно.

3.4.4. Пусть L — линейное пространство над полем F, $\mathcal{A}$ — линейный оператор пространства L, $K = F[x]$ — кольцо многочленов от одной переменной над F. Доказать, что L является K-модулем относительно своей операции сложения и операции умножения на многочлены из K, определенной так: $f(x)\mathbf{a} = f(\mathcal{A})(\mathbf{a})$ для всех $f(x) \in F[x]$, $\mathbf{a} \in L$.

3.4.5. Пусть X — произвольное непустое множество, M — модуль над кольцом K. Доказать, что множество $\mathcal{F}(X, M)$ всех отображений из X в M является модулем над K относительно операций, определенных следующим образом:

$$(f + g)(x) \rightleftharpoons f(x) + g(x),$$
$$(\alpha f)(x) \rightleftharpoons \alpha f(x),$$

где $f, g \in \mathcal{F}(X, M)$, $x \in X$, $\alpha \in K$.

3.4.6. Определить, будут ли следующие кольца, рассматриваемые как $\mathbb{Z}$-модули, конечно порождены:

а) кольцо, состоящее из действительных чисел вида $a + b\sqrt{2}$, где $a, b \in \mathbb{Z}$;

б) кольцо, состоящее из действительных чисел вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Z}$;

в) подкольцо из $\mathbb{R}$, порожденное множеством $\{1, \pi\}$.

3.4.7. Будем рассматривать кольцо $\mathbf{M}_2(F)$ над полем F как модуль над самим собой. Описать все подмодули данного модуля. **(С)**

3.4.8. (У) *Алгеброй* над ассоциативно-коммутативным кольцом K с 1 называется кольцо M, являющееся одновременно модулем над K таким, что условие $\alpha(xy) = (\alpha x)y = x(\alpha y)$ выполнено для любых элементов x, y кольца M и любого $\alpha \in K$.

Проверить, что перечисленные ниже кольца являются алгебрами над соответствующими кольцами:

а) кольцо $\mathbb{C}$ над кольцом $\mathbb{R}$,

б) кольцо $K[x]$ над кольцом K,

в) кольцо $\mathbf{M}_n(K)$ над кольцом K.

3.4.9. Алгебра над полем называется *конечномерной*, если она является конечномерным линейным пространством над этим полем. Доказать, что в конечномерной алгебре всякий ненулевой элемент либо обратим, либо является делителем нуля. **(С)**

3.4.10. Обозначим через A векторное пространство над полем $\mathbb{R}$ с базисом e, i, j, k. Определим умножение в A, считая e единицей, полагая $i^2 = -e$, $j^2 = -e$, $ij = -ji = k$, и продолжая его на все пространство A по дистрибутивности и билинейности, так что $k^2 = -e$, $ik = -ki = j$, $jk = -kj = -i$. Отождествим каждый элемент x поля $\mathbb{R}$ с элементом xe пространства A.

а) **(У)** Проверить, что A является алгеброй над полем $\mathbb{R}$.

б) Доказать, что A не имеет нетривиальных идеалов и его центр совпадает с $\mathbb{R}$.

Эта алгебра называется *алгеброй кватернионов*.

3.4.11. Как обычно, символом $\oplus$ обозначается операция взятия прямой суммы подпространств.

а) Убедиться, что $A = \mathbb{R} \oplus A_+$, где $A_+ = \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$.

б) Для $z = c + u$, где $c \in \mathbb{R}$, $u \in A_+$, положим $z^\star = c - u$. Доказать, что для любых $z_1, z_2, z \in A$, $c \in \mathbb{R}$ имеют место равенства $(z_1 + z_2)^\star = z_1^\star + z_2^\star$, $(z_1 z_2)^\star = z_2^\star z_1^\star$, $z^{\star\star} = z$, $c^\star = c$.

3.4.12. Пусть A — алгебра кватернионов. Для любого элемента $z \in A$ определим его *норму* $\nu(z)$, полагая

$$\nu(z) = zz^\star.$$

Доказать, что для любых $z_1, z_2 \in A$, $c \in \mathbb{R}$ имеют место следующие условия:

а) $\nu(z_1) \in \mathbb{R}$, б)$\nu(z_1 z_2) = \nu(z_1)\nu(z_2)$,

в) $\nu(c) = c^2$, г) $\nu(z_a^\star) = \nu(z_a)$.

3.4.13. Доказать, что для любого элемента z алгебры кватернионов следующие условия эквивалентны:

(1) z обратим;

(2) $\nu(z) \neq 0$.

3.4.14. Доказать, что алгебра кватернионов изоморфна алгебре матриц из п. з) задания 3.1.2.

Глава 4

Поля

4.1 Примеры и простейшие свойства. Изоморфизм

4.1.1. Доказать, что кольцо вычетов $\mathbb{Z}_n$ будет полем тогда и только тогда, когда n — простое число.

4.1.2. а) Доказать, что поле $\mathbb{C}$ изоморфно кольцу матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $a, b \in \mathbb{R}$, относительно обычных операций с матрицами (ср. с заданием 2.1.7).

б) Доказать, что множество чисел $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ является полем, изоморфным кольцу матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, где $a, b \in \mathbb{Q}$, относительно обычных операций с матрицами.

4.1.3. Пусть F — некоторое поле и q — элемент поля F, не являющийся квадратом (т.е. $q \neq x^2$ для любого $x \in F$). На множестве $M = F \times F$ введем операции

$$(x, y) + (z, t) \rightleftharpoons (x + z, y + t);$$
$$(x, y) \cdot (z, t) \rightleftharpoons (xz + qyt, xt + yz).$$

Доказать, что M является полем относительно этих операций. Оно называется *квадратичным расширением* поля F.

4.1.4. (У) Доказать, что любое подполе поля $\mathbb{C}$ содержит поле $\mathbb{Q}$.

4.1.5. Указать в поле $\mathbb{R}$ все элементы подполя, порожденного множеством: а) $\{2, 3\}$, б) $\{1, \sqrt{2}\}$, в) $\{\sqrt[3]{2}\}$.

4.1.6. Указать в поле $\mathbb{C}$ все элементы подполя, порожденного множеством: а) $\{i\}$, б) $\{z \in \mathbb{C} \mid |z| = 1\}$.

4.1.7. Для любого $n \in \mathbb{N}$ положим

$$\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}.$$

а) Выяснить, изоморфны ли поля $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$.

б) **(И)** Пусть $m, n \in \mathbb{N}$. Найти критерий изоморфности полей $\mathbb{Q}(\sqrt{m})$ и $\mathbb{Q}(\sqrt{n})$.

4.1.8. а) **(У)** Доказать, что поле $\mathbb{Q}$ не имеет автоморфизмов, отличных от тождественного.

б) Доказать, что поле $\mathbb{R}$ не имеет автоморфизмов, отличных от тождественного.

4.1.9. Найти все автоморфизмы поля $\mathbb{C}$, при которых каждое вещественное число переходит в себя.

4.1.10. Доказать, что в поле характеристики p для любого $m \in \mathbb{N}$ справедливо тождество $(x + y)^{p^m} = x^{p^m} + y^{p^m}$.

4.1.11. Доказать, что для любого автоморфизма φ произвольного поля множество элементов, неподвижных относительно φ, образует подполе.

4.1.12. (У) Доказать, что всякое алгебраически замкнутое поле бесконечно.

4.1.13.* Доказать, что поле рациональных функций от одной переменной x над произвольным полем не является алгебраически замкнутым.

4.1.14. (У) Существует ли поле, строго содержащее поле комплексных чисел? **(С)**

4.1.15. Решить в поле $\mathbb{Q}(\sqrt{2})$ следующие уравнения:

а) $x^2 + (4 - 2\sqrt{2})x + 3 - 2\sqrt{2} = 0$;

б) $x^2 - (1 + 2\sqrt{2})x - 8 + 7\sqrt{2} = 0$;

в) $x^2 + x - 7 + 6\sqrt{2} = 0$;

г) $x^2 - 2x + 1 - \sqrt{2} = 0$.

4.1.16. В поле рациональных функций над полем $\mathbb{R}$ решить следующие уравнения: а) $f^4 = 1$; б) $f^2 - f = x$.

4.1.17. а) Пусть F — поле, $g(x)$ — неприводимый многочлен над F. Доказать, что факторкольцо $F[x]/g(x)F[x]$ есть поле, содержащее корень многочлена $g(x)$.

б) Пусть $f(x)$ — многочлен над полем F. Расширение L поля F называется *полем разложения* для многочлена $f(x)$, если над полем L он разлагается на линейные множители и поле L порождается всеми элементами поля F и всеми корнями многочлена $f(x)$.

Опираясь на утверждение п. а), доказать существование поля разложения для любого многочлена.

4.2 Конечные поля

4.2.1. Доказать, что любое подполе конечного поля содержит поле $\mathbb{Z}_p$ для некоторого простого числа p.

4.2.2. Доказать, что поле из p^2 элементов, где p — простое число, имеет единственное собственное подполе.

4.2.3. а) Доказать, что в конечном поле характеристики p отображение $x \mapsto x^p$ является автоморфизмом.

б)* Привести пример поля характеристики p, для которого указанное в п. а) отображение не является автоморфизмом.

4.2.4. Решить систему линейных уравнений $\begin{cases} x + 2z = 1, \\ y + 2z = 2, \\ 2x + z = 1 \end{cases}$ а) в поле $\mathbb{Z}_3$, б) в поле $\mathbb{Z}_5$. в) в поле $\mathbb{Z}_7$.

4.2.5. Определить, какие из следующих уравнений имеют решения в поле $\mathbb{Z}_{11}$: а) $x^2 = 5$; б) $x^7 = 7$; в) $x^3 = a$.

4.2.6. В линейном пространстве $\mathbb{Z}_p^n$ над полем $\mathbb{Z}_p$ (p — простое число) найти число одномерных подпространств.

4.2.7. Рассматривая многочлены над полем $\mathbb{Z}_p$ для простого числа p, доказать *критерий Вильсона*: число p просто тогда и только тогда, когда p делит $(p-1)! + 1$. **(C)**

4.2.8. а) Разложить многочлен $x^{15} - 1$ на неприводимые множители над полем $\mathbb{Z}_2$.

б) Решить аналогичную задачу для многочлена $x^8 - 1$ над полем $\mathbb{Z}_3$.

В заданиях 4.2.9–4.2.14 через $\mathbf{GF}(n)$ обозначается (единственное с точностью до изоморфизма) поле из n элементов.

4.2.9. а) Убедиться, что многочлен $x^3 + x + 1$ неприводим над полем $\mathbb{Z}_2$ и доказать, что поле разложения этого многочлена над $\mathbb{Z}_2$ изоморфно полю $\mathbf{GF}(8)$.

б) Отправляясь от представления $\mathbf{GF}(8)$ как поля разложения неприводимого над $\mathbb{Z}_2$ многочлена x^3+x+1 (см. п. а)), найти все примитивные элементы этого поля.

4.2.10. а) Убедиться, что многочлен x^4+x+1 неприводим над полем $\mathbb{Z}_2$ и доказать, что поле разложения этого многочлена над $\mathbb{Z}_2$ изоморфно полю $\mathbf{GF}(16)$.

б) Отправляясь от представления $\mathbf{GF}(16)$ как поля разложения неприводимого над $\mathbb{Z}_2$ многочлена x^4+x+1 (см. п. а)), найти все примитивные элементы этого поля.

4.2.11. а) Найти минимальные многочлены для каждого ненулевого элемента поля $\mathbf{GF}(16)$.

б) Выполнить аналогичное задание для поля $\mathbf{GF}(32)$.

4.2.12. Пусть α — примитивный элемент поля $\mathbf{GF}(16)$. Найти многочлен наименьшей степени (над $\mathbb{Z}_2$), среди корней которого встречаются:

а) α и α^3;

б) α, α^3 и α^5;

в) α, α^3, α^5 и α^7.

4.2.13. Пусть β — примитивный элемент поля $\mathbf{GF}(32)$. Найти многочлен наименьшей степени (над $\mathbb{Z}_2$), среди корней которого встречаются:

а) β и β^3;

б) β, β^3 и β^5;

в) β, β^3, β^5 и β^7;

г) β, β^3, β^5, β^7 и β^9.

4.2.14.* Пусть α — примитивный элемент поля $\mathbf{GF}(2^n)$, где n — некоторое натуральное число.

а) Убедиться, что для каждого $j=1,\ldots,2^{n-2}$ сумма $1+\alpha^j$ равна некоторой степени $\alpha^{Z(j)}$ элемента α и при этом получается биекция $j\mapsto Z(j)$ на множестве $\{1,\ldots,2^{n-2}\}$ (это так называемый *логарифм Зеха*).

б) Составить таблицу значений логарифма Зеха при $n=3$, взяв в качестве α корень многочлена x^3+x+1.

в) Выполнить аналогичное задание для $n=4$, взяв в качестве α корень многочлена x^4+x+1.

Глава 5

Двоичные коды

5.1 Блочные коды

Всюду далее в этой главе $\mathbb{F} = \{0, 1\}$ — двухэлементное поле. Через $S(x, k)$ обозначается множество всех $y \in \mathbb{F}^n$, для которых расстояние Хэмминга от данного $x \in \mathbb{F}^n$ не превосходит k.

5.1.1. Перечислить все элементы множества:
а) $S(101010, 1)$, б) $S(111111, 1)$.

5.1.2. а) Для $x \in \mathbb{F}^{10}$ определить $|S(x, 1)|$, $|S(x, 2)|$, $|S(x, 3)|$.

б) Пусть n, k — натуральные числа, $1 \leq k \leq n$. Для $x \in \mathbb{F}^n$ определить $|S(x, k)|$.

5.1.3. Рассмотрим кодирующую функцию $E : \mathbb{F}^2 \to \mathbb{F}^6$, определенную следующим образом: $E(00) = 000000$, $E(01) = 010101$, $E(10) = 101010$, $E(11) = 111111$. Декодировать слова 110101, 101011, 001111, 110000.

5.1.4. (У) Пусть $E : \mathbb{F}^5 \to \mathbb{F}^{25}$ — кодирующая функция двоичного кода с минимальным расстоянием 9 между кодовыми словами.

а) Каково наибольшее значение k такое, что при декодировании можно исправить ошибки веса, не превосходящего k?

б) Каково наибольшее значение k такое, что при декодировании можно обнаружить ошибки веса, не превосходящего k?

5.1.5. (У) Показать, что код исправляет t ошибок тогда и только тогда, когда расстояние между любыми двумя кодовыми словами больше $2t$.

5.1.6. (У) Определить, верно ли, что код, исправляющий t ошибок, обнаруживает:

а) не менее $2t+1$ ошибок;

б) не менее $2t$ ошибок;

в) не более $2t$ ошибок.

5.1.7. (У) Показать, что из всякого подмножества $C \subseteq \mathbb{F}^n$ можно получить код, обнаруживающий одну ошибку, удалив из C не более половины элементов.

5.1.8. Для каждой из следующих кодирующих функций найти наименьшее расстояние между кодовыми словами. Определить, сколько ошибок соответствующий код обнаруживает и сколько ошибок может исправить:

а) $E : \mathbb{F}^2 \to \mathbb{F}^5$, $00 \mapsto 00001$, $01 \mapsto 01010$, $10 \mapsto 10100$, $11 \mapsto 11111$;

б) $E : \mathbb{F}^2 \to \mathbb{F}^{10}$, $00 \mapsto 0000000000$, $01 \mapsto 0000011111$, $10 \mapsto 1111100000$, $11 \mapsto 1111111111$;

в) $E : \mathbb{F}^3 \to \mathbb{F}^6$, $000 \mapsto 000111$, $001 \mapsto 001001$, $010 \mapsto 010010$, $011 \mapsto 011100$, $100 \mapsto 100100$, $101 \mapsto 101010$, $110 \mapsto 110001$, $111 \mapsto 111000$;

г) $E : \mathbb{F}^3 \to \mathbb{F}^8$, $000 \mapsto 00011111$, $001 \mapsto 00111010$, $010 \mapsto 01010101$, $011 \mapsto 01110000$, $100 \mapsto 10001101$, $101 \mapsto 10101000$, $110 \mapsto 11000100$, $111 \mapsto 11100011$.

5.2 Линейные коды. Циклические коды.

5.2.1. Доказать, что в любом линейном коде $C \subseteq \mathbb{F}^n$ либо все слова имеют четный вес, либо половина имеет четный вес, а половина — нечетный.

5.2.2. Порождающая матрица *систематического* линейного (n,k)-кода $C \subseteq \mathbb{F}^n$ имеет вид $G = (E_k \mid A)$, где E_k — единичная $k \times k$-матрица, а A — некоторая $k \times (n-k)$-матрица. Убедиться, что в качестве проверочной матрицы кода C может быть взята матрица $H = (A^T \mid E_{n-k})$.

5.2.3. Порождающие матрицы (5,2)-кодов имеют вид

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}; \quad G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

а) Записать проверочную матрицу и найти минимальное расстояние каждого кода.

б) Составить таблицу синдромов одиночных ошибок и убедиться, что каждый код позволяет исправлять все одиночные ошибки.

в) Декодировать с помощью каждого кода слова 10010, 11011, 10101, 11010, 00111, 11101, 00110.

5.2.4. Порождающие матрицы (6,3)-кодов имеют вид

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}; \quad G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

а) Записать проверочную матрицу и найти минимальное расстояние каждого кода.

б) Составить таблицу синдромов одиночных ошибок и убедиться, что каждый код позволяет исправлять все одиночные ошибки.

в) Декодировать с помощью каждого из кодов слова 111101, 110101, 001111, 100100, 110001, 111111, 111100, 010100.

5.2.5. Пусть кодирование осуществляется с помощью (9,8)-кода, заданного функцией

$E : \mathbb{F}^8 \longrightarrow \mathbb{F}^9$, $(w_1, \ldots, w_8) \mapsto (w_1, \ldots, w_8, w_9)$,

$w_9 = (w_1 + \ldots + w_8) \bmod 2$.

а) Найти порождающую и проверочную матрицы этого кода.

б) Найти минимальное расстояние данного кода. Определить, сколько ошибок он обнаруживает и сколько ошибок может исправить.

5.2.6. Зафиксируем число $r \in \mathbb{N}$. *Кодом Хэмминга* называется $(2^r - 1, 2^r - 1 - r)$-код, проверочная матрица которого составлена из стобцов, содержащих двоичные представления чисел $1, 2, \ldots, 2^r - 1$.

а) Пусть кодирование осуществляется с помощью (7,4)-кода Хэмминга, столбцы проверочной матрицы которого расположены в естественном порядке. Декодировать принятые слова 1001010 и 1101011.

б) Пусть кодирование осуществляется с помощью (15,11)-кода Хэмминга, столбцы проверочной матрицы которого расположены в естественном порядке. Декодировать принятое слово 111100101100010.

в) *Стиранием* называется потеря передаваемого символа в некоторой позиции. Оно отличается от ошибки тем, что известно, в какой именно позиции это произошло. Найти алгоритм исправления двух стираний при использовании (7,4)-кода Хэмминга.

5.2.7. *Расширенный код Хэмминга* — это $(2^r, 2^r - r - 1)$-код, проверочная матрица которого получается из проверочной матрицы $(2^r - 1, 2^r - r - 1)$-кода Хэмминга дописыванием сначала нулевого столбца (обычно слева), а затем единичной строки (обычно сверху).

а) **(У)** Как получаются слова расширенного кода Хэмминга из слов кода Хэмминга?

б) Найти порождающую матрицу расширенного (8,4)-кода Хэмминга.

в) Доказать, что вес любого слова из расширенного кода Хэмминга четен. Пользуясь этим, показать, что минимальное расстояние расширенного кода Хэмминга равно 4.

г) Пусть кодирование осуществляется с помощью расширенного кода Хэмминга. Найти способ декодирования, который позволяет одновременно исправлять все одиночные ошибки и распознавать все двойные ошибки.

д) Выяснить, возможно ли при кодировании с помощью расширенного кода Хэмминга одновременно исправлять все одиночные ошибки и распознавать все двойные и тройные ошибки.

е) Пусть кодирование осуществляется с помощью расширенного (8,4)-кода Хэмминга. Декодировать слово 11001101.

5.2.8. Доказать, что если минимальное расстояние кода не меньше $d+t+1$ ($d \geq t$), то код можно использовать для исправления s ошибок ($s \leq t$) и одновременного обнаружения c ошибок ($c \leq d$).

5.2.9. На линейном пространстве $\mathbb{F}^n$ может быть определено "скалярное произведение": для слов $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ полагают

$$xy \rightleftharpoons \sum_{k=1}^{n} x_k y_k.$$

Перенося на пространство $\mathbb{F}^n$ с этим произведением терминологию евклидовых пространств, можно говорить об ортогональности слов $x, y \in \mathbb{F}^n$ ($x \perp y$ если $xy = 0$) и об ортогональном дополнении к подпространству: если $U \subseteq F^n$ — подпространство $\mathbb{F}^n$, то его ортогональное дополнение

$$U^{\perp} \rightleftharpoons \{x \in \mathbb{F}^n \mid x \perp u \text{ для любого } u \in U\}.$$

а) Доказать, что если код $C \subseteq \mathbb{F}^n$ циклический, то и $C^{\perp}$ будет циклическим кодом.

б) Объяснить, как связаны порождающие многочлены кодов C и $C^{\perp}$.

5.2.10. а) Проверить, что многочлен $x^8 + x^7 + x^6 + x^4 + 1$ делит многочлен $x^{15} - 1$ в кольце $\mathbb{F}[x]$. Найти проверочную матрицу соот-

ветствующего циклического кода. Сколько ошибок может исправлять этот код?

б) Выполнить аналогичные задания для многочлена $x^6 + x^5 + x^4 + x^3 + 1$.

В заданиях 5.2.11–5.2.12 сообщения рассматриваются как коэффициенты многочленов из $\mathbb{Z}_2[x]$, записанных слева направо по убыванию степеней начиная с высшей и заканчивая нулевой. Для решения этих заданий рекомендуется воспользоваться таблицей, полученной при решении п. в) задания 4.2.14. Поле $\mathbf{GF}(16)$ строится как поле разложения неприводимого многочлена $x^4 + x + 1$. Через α обозначается корень этого многочлена.

5.2.11. Пусть кодирование осуществляется с помощью (15,7)-кода БЧХ с порождающим многочленом

$$x^8 + x^7 + x^6 + x^4 + 1.$$

а) Допустим, что по некоторому принятому слову вычислены синдромы $S_1 = \alpha^{14}$ и $S_3 = \alpha^6$. Найти число ошибок, многочлен локаторов ошибок и многочлен ошибок.

б) Декодировать следующие сообщения:

100111000000000; 100100110000100.

5.2.12. Пусть кодирование осуществляется с помощью (15,5)-кода БЧХ с порождающим многочленом

$$x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Допустим, что по некоторому принятому слову вычислены синдромы S_1, S_3, S_5. В каждом из следующих трех случаев найти число ошибок, многочлен локаторов ошибок и многочлен ошибок:

а) $S_1 = \alpha^5$, $S_3 = \alpha^3$, $S_5 = 1$;

б) $S_1 = \alpha^{14}$, $S_3 = 1$, $S_5 = \alpha^5$;

в) $S_1 = \alpha^{12}$, $S_3 = \alpha^7$, $S_5 = \alpha^{10}$.

Декодировать следующие сообщения:

000010110110011; 000111101101100; 110001001101000.

5.2.13. Доказать, что для любого натурального m и любого $t \leq 2^{m-1} - 1$ существует код БЧХ длины $n = 2^m - 1$, который исправляет t ошибок и имеет размерность $\geq n - mt$.

Глава 6

Частично упорядоченные множества

6.1 Примеры и простейшие свойства. Изоморфизм

Для краткости вместо “частично упорядоченное множество" будем писать “ч.у. множество". Напомним, что линейно упорядоченное множество называют также *цепью*.

6.1.1. а) **(У)** Сколько существует 2-элементных попарно неизоморфных ч.у. множеств?

б) Нарисовать диаграммы всех 3-элементных попарно неизоморфных ч.у. множеств.

в) Нарисовать диаграммы всех 4-элементных попарно неизоморфных ч.у. множеств.

6.1.2. Перечислить все отношения частичного порядка:

а) **(У)** на 2-элементном множестве $\{a, b\}$,

б) на 3-элементном множестве $\{a, b, c\}$. **(С)**

6.1.3. Нарисовать диаграммы ч.у. множеств:

а) $(\mathcal{P}(\emptyset); \subseteq)$, б) $(\mathcal{P}(\{1\}; \subseteq)$,

в) $(\mathcal{P}(\{1, 2\}); \subseteq)$, г) $(\mathcal{P}(\{1, 2, 3\}); \subseteq)$.

6.1.4. Любое подмножество множества $\mathbb{N}$ будем рассматривать как ч.у. множество относительно делимости (в $\mathbb{N}$).

а) Нарисовать диаграмму ч.у. множества

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

б) **(У)** Не рисуя диаграммы, определить, будут ли изоморфны ч.у. множества:

$\{3, 4, 5, 6, 7\}$ и $\{4, 5, 6, 7, 8\}$; $\{3, 4, 5, 6, 7\}$ и $\{5, 6, 7, 8, 9\}$.

в) Выяснить, изоморфны ли ч.у. множества $2\mathbb{N}$ и $3\mathbb{N}$.

6.1.5. Нарисовать диаграмму ч.у. множества $(\mathcal{B}(X); \subseteq)$ для случая, когда $|X| = 2$.

6.1.6. Через $\mathcal{E}(X)$ и $\mathcal{O}(X)$ обозначим соответственно множество всех отношений эквивалентности и множество всех отношений частичного порядка на множестве X.

а) На диаграмме ч.у. множества, нарисованной при выполнении задания 6.1.5, отметить одним способом элементы из $\mathcal{E}(X)$, а другим способом — элементы из $\mathcal{O}(X)$.

б) Нарисовать диаграммы ч.у. множеств $\mathcal{E}(X)$ и $\mathcal{O}(X)$ для случая, когда $|X| = 3$.

в) Нарисовать диаграмму ч.у. множества $\mathcal{E}(X)$ для случая, когда $|X| = 4$.

6.1.7. а) Сопоставляя результаты выполнения п. б) задания 6.1.2 и п. б) задания 6.1.6, убедиться, что все максимальные элементы в рассмотренном там ч.у. множестве $\mathcal{O}(X)$ являются линейными порядками.

б) **(У)** Объяснить, почему для любого множества X все максимальные элементы в ч.у. множестве $\mathcal{O}(X)$ являются линейными порядками.

6.1.8. Пусть τ_1, τ_2 — частичные порядки на данном множестве. Говорят, что τ_2 *продолжает* τ_1, если $\tau_1 \subseteq \tau_2$.

а) **(У)** Доказать, что любой частичный порядок на конечном множестве может быть продолжен до линейного порядка.

б) Перерисовав диаграммы ч.у. множеств, полученных при выполнении задания 6.1.1 б), и обозначив элементы этих множеств буквами a, b, c, продолжить каждый из полученных тем самым частичных порядков на множестве $\{a, b, c\}$ до линейного порядка всеми возможными способами.

в) Найти все линейные порядки на множестве $\{a, b, c, d\}$, продолжающие частичный порядок, представленный диаграммой на рис. 1. Убедиться, что исходный порядок равен пересечению найденных линейных порядков.

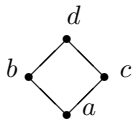


Рис. 1

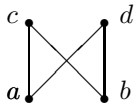


Рис. 2

г) Выполнить аналогичное задание применительно к частичному порядку, представленному диаграммой на рис. 2.

6.1.9.* Доказать, что любой частичный порядок на конечном множестве может быть представлен в виде пересечения линейных порядков.

6.1.10. а) Привести пример ч.у. множества, имеющего точно один максимальный элемент и не имеющего наибольшего элемента.

б) **(У)** Может ли конечное ч.у. множество обладать свойством, указанным в п. а)?

6.1.11. Доказать, что для ч.у. множества A следующие условия эквивалентны:

(1) A удовлетворяет условию минимальности и не содержит бесконечных антицепей;

(2) любое бесконечное подмножество из A не удовлетворяет условию максимальности.

6.1.12.* а) Доказать, что если в ч.у. множестве A все цепи и все антицепи конечны, то A конечно.

б) Указать максимум числа элементов ч.у. множества, в котором каждая цепь содержит не более h элементов, а каждая антицепь — не более l элементов.

6.1.13. Найти все автоморфизмы ч.у. множества, представленного диаграммой: а) на рис. 3, б) на рис. 4, в) на рис. 5.

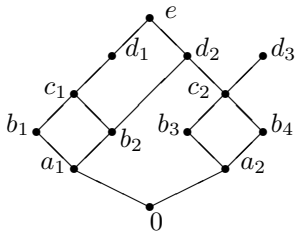


Рис. 3

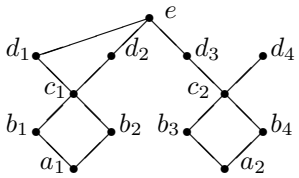


Рис. 4

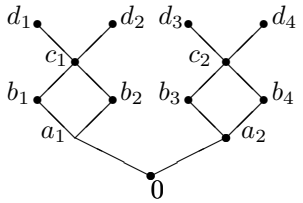


Рис. 5

6.1.14. Определить строение группы автоморфизмов ч.у. множества, представленного диаграммой: а) **(У)** на рис. 3, б) на рис. 4, в) на рис. 5.

6.1.15. (У) Для любого натурального n указать ч.у. множество, группа автоморфизмов которого изоморфна симметрической группе S_n.

6.1.16. Через A_n $(n \geq 2)$ обозначим ч.у. множество, представленное диаграммой на рис. 6. Найти все автоморфизмы A_n и охарактеризовать его группу автоморфизмов

а) **(У)** при $n = 2$; б) при $n = 3$;

в)* при $n = 4$; г) **(И)** при любом $n > 3$.

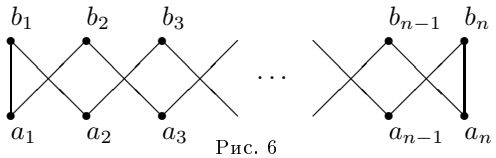


Рис. 6

6.1.17. (У) Ч.у. множеством, *двойственным* к ч.у. множеству $(A, \leq)$, называется ч.у. множество $(A, \geq)$.

Объяснить, почему группа автоморфизмов произвольного ч.у. множества совпадает с группой автоморфизмов двойственного к нему множества.

6.1.18. Ч.у. множество называется *антиизоморфным* данному ч.у. множеству, если оно изоморфно двойственному к нему ч.у. множеству. Ч.у. множество называется *самодвойственным*, если оно антиизоморфно себе.

а) Рассматривая диаграммы ч.у. множеств, нарисованных при выполнении п. б), в) задания 6.1.1 и задания 6.1.3, выявить среди упомянутых ч.у. множеств пары взаимно антиизоморфных и отметить самодвойственные.

б) Нарисовать диаграммы ч.у. множеств, антиизоморфных ч.у. множествам из п. а) задания 6.1.4 и задания 6.1.13.

в) Для каждого из ч.у. множеств, фигурирующих в п. б) задания 6.1.4 и в задании 6.1.6, определить, будет ли оно самодвойственным.

6.1.19. Пусть $A_1, A_2 \ldots, A_n$ — произвольные ч.у. множества с отношениями частичного порядка $\leq_1$, $\leq_2, \ldots, \leq_n$ соответственно. На декартовом произведении $A_1 \times A_2 \times \ldots A_n$ рассмотрим отношение $\leq$, заданное следующим условием:

$$(a_1, a_2, \ldots, a_n) \leq (b_1, b_2, \ldots, b_n) \;\Leftrightarrow\; a_i \leq_i b_i \text{ для всех } i = 1, 2, \ldots, n.$$

Убедиться, что $\leq$ есть отношение частичного порядка. Ч.у. множество $(A_1 \times A_2 \times \ldots A_n, \leq)$ называется *прямым произведением* ч.у. множеств $A_1, A_2 \ldots, A_n$.

6.1.20. (У) а) Убедиться, что для любых ч.у. множеств A_1 и A_2 имеет место $A_1 \times A_2 \cong A_2 \times A_1$.

б) Как обобщить утверждение п. а) на случай любого числа прямых множителей?

В заданиях 6.1.–6.1.25 через C_n обозначается цепь из n элементов.

6.1.21. Нарисовать диаграммы ч.у. множеств: а) $C_2 \times C_2$, б) $C_2 \times C_3$, в) $C_3 \times C_3$.

6.1.22.* а) Выяснить, изоморфны ли ч.у. множества $C_2 \times C_6$ и $C_3 \times C_4$.

б) Для произвольных натуральных чисел k, l, m, n указать критерий изоморфизма ч.у. множеств $C_k \times C_l$ и $C_m \times C_n$.

6.1.23. Нарисовать диаграмму ч.у. множества $C_2 \times B$, где $B = (\mathcal{P}(\{1, 2\}); \subseteq)$.

6.1.24. а) **(У)** Рассматривая диаграммы ч.у. множеств, нарисованных при выполнении задания 6.1., убедиться, что все упомянутые ч.у. множества самодвойственны.

б)* Выяснить, верно ли, что для любых m и n ч.у. множество $C_m \times C_n$ самодвойственно.

6.1.25. Пусть $(A, \leq)$ и $(B, \leq_1)$ — ч.у. множества. Отображение $\varphi : A \to B$ называется *изотонным*, если для любых $x, y \in A$ из $x \leq y$ следует $\varphi(x) \leq_1 \varphi(y)$.

а) **(У)** Подсчитать, сколько существует изотонных отображений C_2 в себя; C_2 в C_3; C_3 в C_2.

б) Найти все изотонные отображения $C_2 \times C_2$ в ч.у. множество A, представленное диаграммой на рис. 7.

Рис. 7

в) Найти все изотонные отображения ч.у. множества A из п. б) в $C_2 \times C_2$.

г) Пусть φ — изотонная биекция ч.у. множества A на B. Убедиться, что если A — цепь, то φ является изоморфизмом, и привести пример таких ч.у. множеств A и B, что φ^{-1} не является изоморфизмом.

6.1.26. Пусть $A_1, A_2 \ldots, A_n$ — произвольные попарно непересекающиеся ч.у. множества. На объединении $A_1 \cup A_2 \cup \ldots \cup A_n$ определим отношение $\leq$ следующим условием: на каждом A_i отношение $\leq$ совпадает с исходным частичным порядком, а для любых $i, j \in \{1, 2, \ldots, n\}$ таких, что $i < j$, и любых $x \in A_i$, $y \in A_j$ полагаем $x \leq y$. Убедиться, что $\leq$ есть отношение частичного порядка. Ч.у. множество $(A_1 \cup A_2 \cup \ldots \cup A_n, \leq)$ называется *ординальной суммой* ч.у. множеств $A_1, A_2 \ldots, A_n$ и обозначается через $A_1 + A_2 + \ldots + A_n$.

6.1.27. а) Пусть A — двухэлементная антицепь, B — ч.у. множество, представленное диаграммой на рис. 8. Нарисовать диаграммы ч.у. множеств $A + B$ и $B + A$.

Рис. 8

б) Пример из п. а) показывает, что ч.у. множества $A + B$ и $B + A$ могут быть неизоморфными. Привести пример неизоморфных ч.у. множеств A и B, для которых $A + B \cong B + A$.

в) Доказать, что если выполняется ситуация, указанная в п. б), то для любого изоморфизма $\varphi : A + B \longrightarrow B + A$ либо $B \subset \varphi(A)$, либо $\varphi(A) \subset B$. Убедиться, что в первом случае A, а во втором случае B разложимо в ординальную сумму.

6.1.28. Ч.у. множество, которое нельзя разложить в ординальную сумму, называется *ординально неразложимым*.

а) Доказать, что любое конечное ч.у. множество либо само является ординально неразложимым, либо разложимо в ординальную сумму ординально неразложимых ч.у. множеств.

б) **(У)** Рассматривая диаграммы ч.у. множеств, нарисованные при выполнении п. в) задания 6.1.1, выделить из упомянутых ч.у. множеств ординально неразложимые, а для остальных указать компоненты разложения в ординальную сумму ординально неразложимых ч.у. множеств.

6.1.29. (И) Распространить определение ординальной суммы на общий случай произвольного линейно упорядоченного множества слагаемых. Доказать общую версию утверждения п. а) задания 6.1.28 (т.е. не для конечных, а для произвольных ч.у. множеств).

6.1.30. Через A^* обозначим ч.у. множество, двойственное к ч.у. множеству A (определение см. в задании 6.1.17). Доказать, что для любых ч.у. множеств $A_1, A_2, \ldots, A_n$

а) $(A_1 \times A_2 \times \ldots \times A_n)^* \cong A_1^* \times A_2^* \times \ldots \times A_n^*$,

б) $(A_1 + A_2 + \ldots + A_n)^* \cong A_n^* + A_{n-1}^* + \ldots + A_1^*$.

6.1.31. Объяснить, что результат п. б) задания 6.1.24 есть непосредственное следствие результата п. а) задания 6.1.30.

6.1.32.* Пусть $(A; \leq)$ — ч.у. множество, $a, b \in A$ и $a \leq b$. *Отрезком* $[a, b]$ называется подмножество $\{x \in A | a \leq x \leq b\}$. Через $\mathsf{Seg}(A)$ обозначим множество всех отрезков A. Доказать, что ч.у. множество $(\mathsf{Seg}(A); \subseteq)$ изоморфно вложимо в прямое произведение $A \times A^*$.

6.1.33. Пусть $(A_1, \leq_1)$ и $(A_2, \leq_2)$ — ч.у. множества. На множестве $A_1 \times A_2$ определим отношение $\leq$, полагая $(x_1, y_1) \leq (x_2, y_2)$ тогда и только тогда, когда либо $x_1 <_1 x_2$, либо $x_1 = x_2$ и $y_1 \leq_2 y_2$. Убедиться, что $(A_1 \times A_2, \leq)$ является ч.у. множеством.

Оно называется *ординальным произведением* ч.у. множеств A_1 и A_2 и обозначается через $A_1 \circ A_2$.

6.1.34. Как и выше, пусть C_k — k-элементная цепь, где $k = 2, 3$.

а) Нарисовать диаграмму ч.у. множества $C_2 \circ C_3$.

б) Убедиться, что $C_2 \circ C_3 \cong C_3 \circ C_2$.

в) Объяснить, почему $C_2 \circ C_3$ не изоморфно $C_2 \times C_3$.

г) **(У)** Может ли для каких-либо цепей C и D выполняться условие $C \circ D \cong C \times D$ и если да, то в каких случаях?

6.1.35. Пусть C_2 — двухэлементная цепь, B — ч.у. множество, представленное диаграммой на рис. 8.

а) Нарисовать диаграмму ч.у. множества $C_2 \circ B$.

б) Нарисовать диаграмму ч.у. множества $B \circ C_2$.

в) Будут ли ч.у. множества $C_2 \circ B$ и $B \circ C_2$ изоморфны?

6.1.36. Доказать, что для любых ч.у. множеств A, B, C справедливы равенства:

а) $(A+B)\circ C = A\circ C + B\circ C$; б) $(A\circ B)^* = A^*\circ B^*$.

При решении заданий 6.1.37–6.1.43 надо воспользоваться леммой Цорна.

6.1.37. Доказать, что в любом линейном пространстве существует базис.

6.1.38. а) Доказать, что если группоид имеет подполугруппу (в частности если он содержит идемпотент), то этот группоид обладает максимальной подполугруппой.

б) Привести пример неассоциативного группоида, который имеет единственную максимальную подполугруппу.

6.1.39. а) Доказать, что любая полугруппа обладает максимальной коммутативной подполугруппой.

б) **(У)** Убедиться, что любая некоммутативная полугруппа имеет более одной максимальной коммутативной подполугруппы.

6.1.40. Выполнить задание, аналогичное заданию 6.1.39, применительно к группам и их коммутативным подгруппам.

6.1.41. Выполнить задание, аналогичное заданию 6.1.39, применительно к ассоциативным кольцам и их коммутативным подкольцам.

6.1.42. а) Доказать, что любое кольцо с единицей обладает максимальным собственным идеалом.

б) Привести пример ассоциативного кольца с единицей, имеющего единственный максимальный собственный идеал.

в) **(У)** Верно ли утверждение, аналогичное сформулированному в п. а), для полугрупп с единицей?

6.1.43.* Перенося утверждения п. а) задания 6.1.8 и задания 6.1.9 на общий случай, доказать следующие утверждения:

а) любой частичный порядок на произвольном множестве может быть продолжен до линейного порядка;

б) любой частичный порядок на произвольном множестве может быть представлен в виде пересечения линейных порядков.

6.2 Линейно упорядоченные множества

Порядковым типом цепи C называется класс всех цепей, изоморфных C. Порядковые типы вполне упорядоченных множеств называются *ординалами*. Через ω, κ, ρ обозначим порядковые типы

соответственно цепей $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ относительно естественного порядка. Для любого натурального числа n буква n используется и для обозначения порядкового типа n-элементной цепи. Если α и β — порядковые типы цепей A и B, то через $\alpha + \beta$ обозначим порядковый тип ординальной суммы $A + B$, через $\alpha \circ \beta$ — порядковый тип ординального произведения $A \circ B$, а через α^* — порядковый тип цепи A^* (определение см. в задании 6.1.30).

6.2.1. Построить какой-либо линейный порядок на множестве: а) $\mathbb{N}^2$, б) $\bigcup_{i=1}^{\infty} \mathbb{N}^i$, в) $\mathbb{C}$.

6.2.2. (У) а) Сформулировать критерий изоморфности двух конечных цепей.

б) Доказать, что цепь конечна тогда и только тогда, когда она и двойственная к ней цепь вполне упорядочены.

6.2.3. (У) Охарактеризовать группу автоморфизмов

а) конечной цепи, б) цепи $\mathbb{N}$, в) цепи $\mathbb{Z}$.

6.2.4. (У) а) Привести пример двух счетных неизоморфных цепей.

б) Привести пример двух несчетных равномощных неизоморфных цепей.

6.2.5. Доказать, что цепь C изоморфна цепи $\mathbb{N}$ тогда и только тогда, когда выполняются следующие условия:

(1) C обладает наименьшим элементом c_0;

(2) для любого $c \in C$ в множестве $\{x \in C | c < x\}$ существует наименьший элемент, который обозначается через c';

(3) для любого подмножества M из C из того, что $c_0 \in M$ и для любого $c \in M$ также и $c' \in M$, следует $M = C$.

6.2.6. Пусть C — цепь, $a, b \in C$ и $a < b$. *Интервалом* (a, b) в C называется множество $\{x \in C \mid a < x < b\}$.

а) Убедиться, что функция $f(x) = \dfrac{x}{1 - |x|}$ является изоморфизмом интервала $(-1, 1)$ из $\mathbb{Q}$ на всю цепь $\mathbb{Q}$.

б) Найти другой изоморфизм $(-1, 1)$ на $\mathbb{Q}$.

в) Найти изоморфизм произвольного интервала (a, b) на всю цепь $\mathbb{Q}$.

6.2.7. а) Очевидно, что если цепь C изоморфно вложима в цепь $\mathbb{Z}$, то в C все интервалы конечны. Доказать, что справедливо и обратное.

б)* Доказать, что любая счетная цепь изоморфно вложима в цепь $\mathbb{Q}$.

в)* Очевидно, что если цепь C изоморфно вложима в цепь $\mathbb{Q}$, то в C она не имеет наименьшего и наибольшего элементов и все интервалы в C непусты. Доказать, что справедливо и обратное.

6.2.8. Подмножество A цепи C называется *плотным в* C, если для любых $x, y \in C$, таких что $x < y$, существует $a \in A$ такой, что $x \leq a \leq y$.

а) **(У)** Указать счетное плотное подмножество в цепи $\mathbb{R}$.

б)* Доказать, что если цепь содержит счетное плотное в ней подмножество, то она изоморфно вложима в цепь $\mathbb{R}$.

6.2.9. Пусть $(A; \leq)$ — цепь, содержащая более одного элемента, и $B = \cup^{\infty}{}_{k=1} A^k$. На B введем отношение $\leq_1$:

$$(x_1, \ldots, x_m) \leq_1 (y_1, \ldots, y_n)$$

тогда и только тогда, когда либо $m \leq n$ и $x_1 = y_1, \ldots, x_m = y_m$, либо найдется $i \leq \min\{m, n\}$ такое, что $x_1 = y_1, \ldots, x_{i-1} = y_{i-1}$ и $x_i < y_i$.

а) **(У)** Доказать, что $\leq_1$ — линейный порядок. Порядок $\leq_1$ называется *лексикографическим*.

б) Доказать, что любая счетная цепь изоморфно вложима в $(B; \leq_1)$.

6.2.10. На множестве B из предыдущего задания определим отношение $\leq_2$: $(x_1, \ldots, x_m) \leq_2 (y_1, \ldots, y_n)$ тогда и только тогда, когда либо $m < n$, либо $m = n$ и выполняется одно из двух условий: либо существует $i \leq m$ такое, что $x_1 = y_1, \ldots, x_{i-1} = y_{i-1}$ и $x_i < y_i$, либо $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$.

а) Убедиться, что $\leq_2$ — отношение линейного порядка.

б) Выяснить, верно ли, что цепь $(B; \leq_2)$ изоморфна цепи $(B; \leq_1)$, определенной в задании 6.2.9.

6.2.11. (У) Объяснить, почему:

а) цепь $\mathbb{Z}$ имеет порядковый тип $\omega^* + \omega$,

б) $n + \omega = \omega$ для любого конечного ординала n,

в) $\omega + \omega \neq \omega$.

6.2.12. (У) Привести пример порядковых типов α, β, для которых: а) $\alpha + \beta \neq \beta + \alpha$, б) $\alpha \neq \beta$ и $\alpha + \beta = \beta + \alpha$.

6.2.13. Доказать, что:

а) $\kappa + \kappa \neq \kappa$, б) $\rho + \rho \neq \rho$,

в) $\kappa + 1 + \kappa = \kappa$, г) $\rho + 1 + \rho = \rho$.

6.2.14. Пусть α, β, γ — ординалы. Результат п. б) задания 6.2.11 показывает, что из равенства $\alpha + \gamma = \beta + \gamma$, вообще говоря, не следует $\alpha = \beta$. Выяснить, следует ли всегда $\alpha = \beta$ из равенства $\gamma + \alpha = \gamma + \beta$.

6.2.15. Определить, сколько различных ординалов можно получить складывая в произвольном порядке взятые по одному разу следующие ординалы:

а) **(У)** 1, 2, ω;

б) 1, 2, 3, ω;

в) 1, 2, ..., n, ω для любого $n \geq 2$.

6.2.16. а) **(У)** Убедиться, что ординальное произведение двух цепей является цепью.

б) Доказать, что ординальное произведение двух вполне упорядоченных множеств является вполне упорядоченным (и тем самым для любых ординалов α, β порядковый тип $\alpha \circ \beta$ является ординалом).

6.2.17. Привести пример таких ординалов α и β, что:

а) **(У)** $\alpha \neq \beta$ и $\alpha \circ \beta = \beta \circ \alpha$, б) $\alpha \circ \beta \neq \beta \circ \alpha$.

6.2.18. Убедиться, что для любого порядкового типа α и для любого n, трактуемого и как натуральное число, и как конечный ординал, выполняется равенство

$$\alpha \circ n = \underbrace{\alpha + \alpha + \ldots + \alpha}_{n \text{ раз}}.$$

6.2.19. **(У)** Объяснить, почему:

а) для любого конечного ординала n имеет место $n \circ \omega = \omega$,

б) для любых различных m и n имеет место $\omega \circ m \neq \omega \circ n$,

в) $\omega \circ \omega \neq \omega$.

6.2.20. Доказать, что для любых ординалов α, β и γ справедливо равенство $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.

Глава 7

Решетки

7.1 Примеры и простейшие свойства. Изоморфизм

7.1.1. Выяснить, какие из перечисленных ниже ч.у. множеств являются решетками и какие из выявленных решеток оказываются полными:

а) **(У)** $(\mathcal{P}(X), \subseteq)$;

б) **(У)** $(\mathbb{N}, \leq)$;

в) **(У)** $(\mathbb{N}, |)$, где $x \mid y$ означает, что y делится на x;

г) $(M, \subseteq)$, где M — множество всех линейных подпространств данного линейного пространства;

д) $(M \cup \{\emptyset\}, \subseteq)$, где M — множество всех открытых прямоугольников на координатной плоскости, стороны которых параллельны осям координат;

е) $(M \cup \{\emptyset\}, \subseteq)$, где M — множество всех открытых кругов на координатной плоскости;

ж) множество всех функций $\mathcal{F}(X, \mathbb{R})$ с отношением $\leq$: $f \leq g \Leftrightarrow f(x) \leq g(x)$ для любого $x \in \mathbb{R}$;

з) $(M, \subseteq)$, где M — множество всех идеалов данного кольца;

и) $(M, \subseteq)$, где M — множество всех рефлексивных отношений на данном множестве M;

к) $(M, \subseteq)$, где M — множество всех симметричных отношений на данном множестве M;

л) $(M, \subseteq)$, где M — множество всех антисимметричных отношений на данном множестве M;

м) $(M, \subseteq)$, где M — множество всех транзитивных отношений на данном множестве M;

н) множество $\mathcal{E}(X)$ (см. задание 6.1.6) для произвольного множества X.

7.1.2. (У) Будет ли решеткой ч.у. множество со следующей диаграммой:

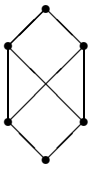
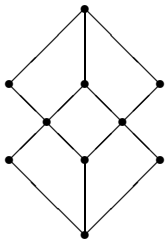
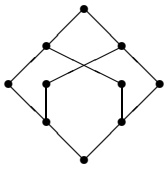
а)  б)  в) 

Рис. 9

7.1.3. В задании 6.1.4 отмечено, что любое подмножество множества натуральных чисел является ч.у. множеством относительно делимости. Доказать, что для любого натурального числа n множество всех его делителей образует решетку относительно указанного отношения. Эту решетку будем называть *решеткой делителей числа* n.

7.1.4. Нарисовать диаграмму решетки делителей следующих чисел: а) 12; б) 60; в) 120; г) 32; д) 243.

7.1.5. Доказать, что решетка идеалов кольца $\mathbb{Z}$ антиизоморфна решетке из п. в) задания 7.1.1.

7.1.6. Выяснить, изоморфны ли решетка из п. в) задания 7.1.1 и решетка всех конечных подмножеств счетного множества.

7.1.7. а) Нарисовать диаграмму решетки подпространств двумерного линейного пространства над полем из двух элементов; над полем из трех элементов.

б) Подсчитать, сколько элементов имеет решетка подпространств двумерного линейного пространства над конечным полем из q элементов.

7.1.8. а) Нарисовать диаграмму решетки подпространств трехмерного линейного пространства над полем из двух элементов; над полем из трех элементов.

б)* Подсчитать, сколько элементов имеет решетка подпространств трехмерного линейного пространства над конечным полем из q элементов.

7.1.9. Доказать, что две решетки изоморфны как алгебры тогда и только тогда, когда они изоморфны как ч.у. множества.

7.1.10. а) Доказать, что для любых элементов x, y, u, v решетки из $x \leq y$ и $u \leq v$ следует $x \wedge u \leq y \wedge v$ и $x \vee u \leq y \vee v$.

б) **(У)** Убедиться, что для любых элементов x, y решетки следующие условия эквивалентны:

(1) $x \leq y$, (2) $x \leq x \wedge y$, (3) $x \vee y \leq y$.

в) **(У)** Убедиться, что если в решетке для элементов x, y, z выполняется равенство $x \wedge y \wedge z = x \vee y \vee z$, то $x = y = z$.

7.1.11. Привести пример решетки L, обладающей таким подмножеством H, что H является решеткой относительно частичного порядка, индуцированного L в H, но не является подрешеткой L (т.е. не замкнуто относительно хотя бы одной решеточной операции).

7.1.12. Нарисовать диаграммы всех

а) 4-элементных решеток,

б) 5-элементных решеток,

в) 6-элементных решеток.

Выявить среди них дистрибутивные и модулярные решетки.

7.1.13. Нарисовать диаграммы всех 7-элементных дистрибутивных решеток.

7.1.14. Доказать дистрибутивность следующих решеток:

а) любая цепь;

б) решетка из п. в) задания 7.1.1;

в) решетка из п. и) того же задания;

г) решетка из п. к) того же задания.

7.1.15. Доказать, что конечно порожденная дистрибутивная решетка конечна.

7.1.16. а) **(У)** Выделить среди решеток, фигурирующих в задании 7.1.12, пары взаимно антиизоморфных (и неизоморфных) решеток и отметить самодвойственные решетки.

б) Выполнить задание, аналогичное приведенному в п. а), применительно к решеткам, фигурирующим в п. а) заданий 7.1.7 и 7.1.8.

в) Выяснить, является ли самодвойственной решетка $\mathcal{P}(X)$ для любого множества X.

7.1.17. (У) Рассматривая диаграммы решеток, нарисованные при выполнении задания 7.1.12, найти все автоморфизмы каждой этих решеток, и охарактеризовать соответствующую группу автоморфизмов.

7.1.18. а) Найти все автоморфизмы решетки, представленной диаграммой на рис. 10 и охарактеризовать группу автоморфизмов этой решетки.

б) Выполнить аналогичное задание применительно к решетке, представленной диаграммой на рис. 11.

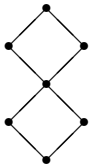


Рис. 10

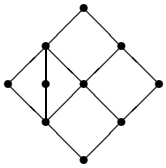


Рис. 11

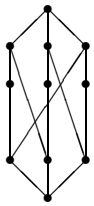


Рис. 12

7.1.19. а) Привести пример бесконечной решетки, имеющей в точности два автоморфизма.

б) Убедиться, что решетка, представленная диаграммой на рис. 12, имеет в точности три автоморфизма.

в) **(И)** Распространяя на общий случай идею построения решетки, фигурирующей в п. б), построить для любого $n > 2$ решетку, имеющую в точности n автоморфизмов. Что можно сказать о группе автоморфизмов построенной решетки?

7.1.20. (У) Для любого натурального n указать решетку, группа автоморфизмов которой изоморфна симметрической группе S_n.

7.1.21. а) Доказать, что прямое произведение конечного числа решеток (рассматриваемое как ч.у. множество, см. задание 6.1.19) будет решеткой. Убедиться при этом, что решеточные операции в прямом произведении определяются покомпонентно.

б) Доказать, что прямое произведение решеток
$L_1 \times L_2 \times \ldots \times L_n$ будет дистрибутивной решеткой тогда и только тогда, когда все решетки $L_1, L_2, \ldots, L_n$ дистрибутивны.

в) Доказать утверждение аналогичное утверждению п. б) для свойства модулярности.

7.1.22. Как и выше, через C_m обозначим n-элементную цепь. Пусть $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ — каноническое разложение натурального числа n на простые множители.

а) Доказать, что решетка делителей числа n изоморфна прямому произведению $C_{r_1+1} \times C_{r_2+1} \times \ldots \times C_{r_k+1}$ (при $k = 1$ получается вырожденный случай цепи C_{r_1+1}).

б) Решетка делителей любого натурального числа дистрибутивна. Указать те утверждения из предыдущих заданий, применением которых можно получить только что высказанное утверждение.

в) **(И)** Найти условия для двух натуральных чисел, необходимые и достаточные для того, чтобы решетки их делителей были изоморфны.

7.1.23. а) Доказать, что ординальная сумма конечного числа решеток (см. определение в задании 6.1.26) будет решеткой.

б) Доказать, что ординальная сумма решеток $L_1 + L_2 + \ldots + L_n$ будет дистрибутивной решеткой тогда и только тогда, когда все решетки $L_1, L_2, \ldots, L_n$ дистрибутивны.

в) Доказать утверждение, аналогичное утверждению п. б), для свойства модулярности.

7.2 Гомоморфизмы и конгруэнции

7.2.1. а) Убедиться, что всякий гомоморфизм решетки является изотонным отображением и что для цепей справедливо обратное — всякое изотонное отображение есть гомоморфизм.

б) Привести пример решеток L_1 и L_2, для которых существует изотонное отображение L_1 в L_2, не являющееся гомоморфизмом.

7.2.2. Для решетки, представленной диаграммой на рис. 10, найти все ее гомоморфизмы:

а) в 2-элементную цепь,

б) в 3-элементную цепь,

в) в 4-элементную решетку, не являющуюся цепью,

г) в себя.

7.2.3. (У) а) Описать все гомоморфизмы цепи $\mathbb{N}$ на двухэлементную цепь.

б) Выполнить такое же задание для цепи $\mathbb{Z}$.

в) Выполнить такое же задание для цепи $\mathbb{Q}$.

г) Выполнить такое же задание для цепи $\mathbb{R}$.

7.2.4. Пусть L — решетка, $a \in L$. Определим отображения $\varphi_a, \psi_a : L \longrightarrow L$, полагая $\varphi_a(x) = a \wedge x$, $\psi_a(x) = a \vee x$ для любого $x \in L$.

а) **(У)** Какому свойству решетки L эквивалентно условие, что при всех $a \in L$ отображения φ_a являются эндоморфизмами?

б) Привести пример решетки L и таких ее элементов a, b, что φ_a — эндоморфизм, а φ_b не является эндоморфизмом.

в) **(У)** Объяснить, что решетка L удовлетворяет условию п. а) тогда и только тогда, когда при всех $a \in L$ отображения ψ_a являются эндоморфизмами.

г) Выполнить задание аналогичное приведенному в п. б) применительно к отображениям ψ_a и ψ_b.

д) Через D обозначим множество всех элементов $a \in L$, для которых φ_a и ψ_a являются эндоморфизмами. Доказать, что D является дистрибутивной подрешеткой L.

е)* Привести пример решетки L, в которой существует элемент a такой, что φ_a — эндоморфизм, а ψ_a не является эндоморфизмом.

7.2.5. Пусть $L_1, L_2, \ldots, L_n$ — произвольные решетки, $n > 1$.

а) Доказать, если каждая решетка L_k имеет нуль и единицу, то существует гомоморфизм решетки $L_1 + L_2 + \ldots + L_n$ на L_k при $k = 1, 2, \ldots, n$.

б) Привести пример решеток L_1 и L_2 таких, что решетка $L_1 + L_2$ не обладает гомоморфизмом ни на решетку L_1, ни на решетку L_2.

7.2.6. Пусть L_1 и L_2 — произвольные решетки, L_3 и L_4 — гомоморфные образы соответственно L_1 и L_2. Убедиться, что решетка $L_3 + L_4$ является гомоморфным образом $L_1 + L_2$.

7.2.7. Пусть ρ — конгруэнция решетки L. Доказать, что для любого $a \in L$ ρ-класс $a^\rho = \{x \in L \mid x \rho a\}$ является подрешеткой решетки L и для любых $x, y \in a^\rho$, из $x < y$ следует, что все элементы отрезка $[x, y]$ принадлежат a^ρ.

7.2.8. а) Найти все конгруэнции четырехэлементной цепи и для каждой из них определить соответствующую фактор-решетку.

б) Выполнить аналогичное задание применительно к пятиэлементной немодулярной решетке ("пентагону").

в) Выполнить аналогичное задание применительно к решетке делителей числа 12 (диаграмма этой решетки была нарисована при выполнении п. а) задания 7.1.4).

7.2.9. Пусть L — решетка, определенная в п. в) задания 7.1.1. Рассмотрим на L следующие отношения ρ и σ: $m \rho n$ означает, что в каноническом разложении чисел m и n участвуют одни и те же простые числа; $m \sigma n$ означает, что показатели числа 2 в канонических разложениях чисел m и n совпадают. Доказать, что эти отношения являются конгруэнциями на решетке L, причем фактор-решетка L/ρ изоморфна решетке всех подмножеств множества $\mathbb{N}$, а L/σ изоморфна решетке из п. б) задания 7.1.1.

7.2.10. а) Привести пример решетки, имеющей в точности четыре конгруэнции.

б) Решетка, фигурирующая в п. б) задания 7.2.8, имеет в точности три конгруэнции. Убедиться, что никакая цепь не может иметь в точности три конгруэнции.

7.2.11. Решетка называется *простой*, если она не имеет конгруэнций, отличных от отношения равенства и от универсального отношения.

а) Выделить среди решеток, имеющих не более шести элементов, простые решетки. (Диаграммы всех четырехэлементных, пятиэлементных и шестиэлементных решеток были нарисованы при выполнении задания 7.1.12.)

б) Убедиться, что решетка, представленная диаграммой на рис. 13, не является простой.

Рис. 13

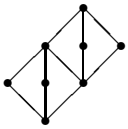


Рис. 14

в) Убедиться, что решетка, представленная диаграммой на рис. 14, является простой.

г)* Среди решеток, выделенных при выполнении п. а), есть одна пятиэлементная — модулярная недистрибутивная решетка ("бриллиант"). Распространяя особенности ее строения на общий случай, доказать, что для любой мощности $\mathfrak{m} > 4$ существует простая решетка мощности $\mathfrak{m}$.

д)* Доказать, что любая дистрибутивная решетка, содержащая более двух элементов, не является простой.

7.3 Булевы алгебры

Через B_n будем обозначать булеву алгебру всех подмножеств n-элементного множества.

7.3.1. Нарисовать диаграмму булевой алгебры B_n

а) при $n = 2$ и $n = 3$,

б) при $n = 4$.

7.3.2. (У) а) Сравнивая диаграммы, нарисованные при выполнении задания 6.1.5 и п. б) задания 7.3.1, убедиться, что фигурирующие в них решетки изоморфны.

б) Объяснить, как утверждение об изоморфности решеток, упомянутых в п. а), получается без сравнения диаграмм этих решеток.

7.3.3. Пусть B — произвольная булева алгебра.

а) Доказать, что для любых элементов $a, b \in B$ следующие условия равносильны:

(1) $a \wedge b = a$; (2) $a \wedge b' = 0$; (3) $a' \vee b = 1$.

б) Доказать, что если φ — гомоморфизм B на решетку L, то L есть булева алгебра, а φ сохраняет и дополнения, т.е. для любого $x \in B$ имеет место $\varphi(x') = \varphi(x)'$.

в) Доказать, что любой отрезок $[a, b]$ в B является булевой алгеброй, причем если $[a, b] \neq B$, то $[a, b]$ не будет подалгеброй алгебры B.

7.3.4. Убедиться, что конечно порожденная булева алгебра конечна.

7.3.5. Охарактеризовать все натуральные числа n, для которых решетка делителей является булевой алгеброй.

7.3.6. Пусть X — счетное множество.

а) Пусть B — совокупность всех конечных подмножеств множества X и их дополнений. Доказать, что B является подалгеброй булевой алгебры $\mathcal{P}(X)$.

б) Убедиться, что булева алгебра B из п. а) не изоморфна булевой алгебре $\mathcal{P}(Y)$ ни для какого множества Y.

в) Булева алгебра B из п. а) в силу результата задания 7.3.4 не является конечно порожденной. Выяснить, имеет ли она базис.

7.3.7. Пусть L — дистрибутивная решетка с нулем и единицей.

а) Доказать, что множество всех элементов из L, обладающих дополнениями, образует подрешетку, являющуюся булевой алгеброй.

б) Доказать, что если все цепи в L конечны и единица является объединением атомов, то L есть конечная булева алгебра.

7.3.8. Пусть $L_1, L_2, \ldots, L_n$ — произвольные булевы алгебры.

а) Доказать, что прямое произведение $L_1 \times L_2 \times \ldots \times L_n$ будет булевой алгеброй.

б) **(У)** Выяснить, может ли ординальная сумма $L_1 + L_2 + \ldots + L_n$ быть булевой алгеброй, и если да, то в каких случаях.

7.3.9. Рассматривая диаграмму алгебры B_3,

а) **(У)** указать все ее подалгебры,

б) **(У)** указать все ее 4-элементные подрешетки, не являющиеся подалгебрами,

в) найти все ее базисы,

г) найти все ее конгруэнции,

д) найти все ее автоморфизмы.

7.3.10. Для алгебры B_4

а) найти все ее подалгебры, б) найти все ее базисы.

7.3.11. (И) Учитывая известную связь между булевыми алгебрами и булевыми кольцами, а также описание конгруэнций колец в терминах идеалов, описать в аналогичных терминах конгруэнции на произвольной булевой алгебре.

Глава 8

Универсальные алгебры

8.1 Порождающие множества, подалгебры

Для краткости будем использовать сокращение “к.п. алгебра" вместо “конечно порожденная алгебра".

8.1.1. (У) Пусть $(K, +, \cdot)$ — кольцо, X — порождающее множество группы $(K, +)$, X — порождающее множество группоида $(K, \cdot)$. Очевидно, что X и Y будут порождающими множествами кольца $(K, +, \cdot)$. Привести пример ситуации, когда:

а) множество X есть базис группы $(K, +)$, но не является базисом кольца $(K, +, \cdot)$,

б) множество Y есть базис группоида $(K, \cdot)$, но не является базисом кольца $(K, +, \cdot)$.

8.1.2. (У) а) Привести пример кольца $(K, +, \cdot)$, имеющего базис, не являющийся порождающим множеством ни группы $(K, +)$, ни группоида $(K, \cdot)$.

б) Привести пример к.п. кольца $(K, +, \cdot)$, у которого ни группа $(K, +)$, ни группоид $(K, \cdot)$ не являются конечно порожденными. Не получилось ли, что пример, приведенный при выполнении п.а), обладает указанным свойством?

8.1.3. Пусть A — к.п. алгебра. Доказать, что

а) **(У)** A обладает базисом,

б) в любом порождающем A множестве имеется конечное подмножество, также порождающее A,

в) **(У)** все базисы алгебры A конечны.

8.1.4. а) Доказать, что прямое произведение двух к.п. групп является к.п. группой.

б) Выполнить аналогичное задание для колец.

в) Выполнить аналогичное задание для решеток.

г) Привести пример двух к.п. полугрупп, прямое произведение которых не является к.п. полугруппой.

8.1.5. Пусть $S_1 = (\mathbb{N}, \vee)$, $S_2 = (\mathbb{N}, \wedge)$ — полугруппы с операциями, заданными соответственно формулами

$$x \vee y = \max\{x, y\},\ x \wedge y = \min\{x, y\}.$$

а) **(У)** Объяснить, что каждая из этих полугрупп имеет (единственный) базис: он совпадает со всей полугруппой.

б) **(У)** Убедиться, что прямое произведение $S_1 \times S_1$ имеет базис и притом единственный.

в)* Доказать, что прямое произведение $S_2 \times S_2$ не имеет базиса.

8.1.6. а) Доказать, что если к.п. алгебра не является 1-порожденной, то она обладает максимальной собственной подалгеброй.

б) Доказать, что любая неодноэлементная циклическая группа обладает максимальной собственной подгруппой. Выделить среди циклических групп те, которые имеют единственную максимальную собственную подгруппу.

в) Учитывая факты, приведенные в задании 1.2.7, и результаты, полученные при выполнении п. б), доказать, что любая неодноэлементная циклическая полугруппа обладает максимальной собственной подполугруппой. Выделить среди циклических полугрупп те, которые имеют единственную максимальную собственную подполугруппу.

г) **(У)** Найти все максимальные собственные подкольца кольца $\mathbb{Z}$.

д) **(И)** Описать ассоциативные кольца, в которых $\{0\}$ является максимальным (и, следовательно, единственным) собственным подкольцом.

е) **(У)** Объяснить, почему никакая решетка не может иметь единственную максимальную собственную подрешетку. Убедиться, что булева алгебра B_2 имеет единственную собственную (и тем самым максимальную) подалгебру.

ж) **(И)** Для любого $n \geq 3$ определить, сколько максимальных собственных подалгебр имеет булева алгебра B_n.

8.1.7. (У) а) Объяснить, почему непусто пересечение любого семейства подгрупп группы и пересечение любого семейства подколец кольца. Привести пример полугруппы, имеющей две непересекающиеся подполугруппы, и доказать, что в любой неодноэлементной решетке есть две непересекающиеся подрешетки.

б) Привести пример полугруппы, в которой любые две подполугруппы имеют непустое пересечение, но существует (автоматически бесконечное) семейство подполугрупп, пересечение которых пусто.

8.1.8. Пусть A — универсальная алгебра. Через $\mathsf{Sub}(A)$ обозначим ч.у. множество (по включению) всех подалгебр A; если в A есть семейство подалгебр с пустым пересечением, то пустое множество также считается подалгеброй. Доказать, что при указанном соглашении $\mathsf{Sub}(A)$ является решеткой и притом полной. Это *решетка подалгебр* алгебры A.

8.1.9. а) **(У)** Ясно, что $\mathsf{Sub}(A) \subseteq \mathcal{P}(A)$. Но решетка $\mathsf{Sub}(A)$ не обязана быть подрешеткой решетки $\mathcal{P}(A)$; проиллюстрировать это утверждение соответствующими примерами полугруппы, группы, кольца и решетки.

б) Пусть G — конечная группа. Доказать, что $\mathsf{Sub}(G)$ является подрешеткой решетки $\mathcal{P}(G)$ тогда и только тогда, когда G — примарная циклическая группа.

в) **(У)** Охарактеризовать решетки L с тем свойством, что $\mathsf{Sub}(L)$ есть подрешетка в $\mathcal{P}(L)$, и убедиться, что для таких решеток попросту имеет место равенство $\mathsf{Sub}(L) = \mathcal{P}(L)$.

г) **(У)** Пусть A — универсальная алгебра, имеющая лишь унарные операции. Убедиться, что $\mathsf{Sub}(A) \subseteq \mathcal{P}(A)$ и привести примеры, когда $\mathsf{Sub}(A) = \mathcal{P}(A)$ и когда $\mathsf{Sub}(A) \neq \mathcal{P}(A)$.

8.1.10. Убедиться, что решетка подполугрупп $\mathsf{Sub}(\mathcal{T}_2)$ немодулярна.

8.1.11. Убедиться, что

а) решетка подгрупп $\mathsf{Sub}(S_3)$ модулярна, но недистрибутивна,

б) решетка подгрупп $\mathsf{Sub}(S_3 \times \mathbb{C}_2)$ немодулярна.

8.1.12. а) Доказать, что решетка подгрупп любой абелевой группы модулярна.

б) Убедиться, что решетка $\mathsf{Sub}(\mathbb{C}_2 \times \mathbb{C}_2)$ недистрибутивна.

в) Доказать, что решетка подгрупп конечной циклической группы порядка n изоморфна решетке делителей числа n.

г)* Из утверждения п. в) и утверждения п. б) задания 7.1.22 следует, что решетка подгрупп конечной циклической группы дистри-

бутивна. Доказать обратное: если для конечной группы G решетка $\mathsf{Sub}(G)$ дистрибутивна, то группа G циклическая.

8.1.13. а) **(У)** Объяснить, почему из утверждения п. а) задания 8.1.12 следует, что решетка подпространств любого линейного пространства является модулярной.

б) Выяснить, при каком условии для линейного пространства решетка его подпространств дистрибутивна.

8.1.14. Пусть L — решетка. Доказать, что следующие условия равносильны:

(1) решетка $\mathsf{Sub}(L)$ модулярна;

(2) решетка $\mathsf{Sub}(L)$ дистрибутивна;

(3) L есть цепь.

8.1.15. Доказать, что решетка подалгебр произвольной универсальной алгебры удовлетворяет условию максимальности тогда и только тогда, когда каждая подалгебра данной алгебры является к.п. алгеброй.

8.1.16. Привести пример к.п. алгебры, имеющей не к.п. подалгебры: а) в случае полугрупп, б) в случае групп, в) в случае колец.

8.1.17. Пусть A — универсальная алгебра. Элемент $x \in A$ называется *непорождающим*, если для любого порождающего множества X алгебры A, содержащего x, множество $X \backslash \{x\}$ также порождающее.

а) Доказать, что множество всех непорождающих элементов алгебры A является подалгеброй (быть может, пустой). Эта подалгебра называется *подалгеброй Фраттини* алгебры A. **(С)**

б) **(У)** Привести пример двух конечных решеток, у одной из которых подрешетка Фраттини непустая, а у другой — пустая.

в) Доказать, что если алгебра A обладает максимальными собственными подалгебрами, то ее подалгебра Фраттини (неважно, пустая или непустая) совпадает с пересечением всех ее максимальных собственных подалгебр.

8.1.18. Найти подгруппу Фраттини у следующих аддитивных групп: а) $\mathbb{Z}_n$; б) $\mathbb{Z}$; в)* $\mathbb{Q}$. **(С)**

8.1.19.* Найти подкольцо Фраттини кольца $\mathbb{Q}$. **(С)**

8.1.20. а) Доказать, что для любой группы ее подгруппа Фраттини является нормальной подгруппой.

б)* Привести пример кольца, у которого подкольцо Фраттини не является идеалом.

8.1.21. (У) Найти все подгруппоиды группоида с операцией, заданной на множестве $\{a, b, c\}$ следующей таблицей Кэли:

	a	b	c
a	a	a	a
b	a	a	a
c	a	a	c

8.1.22. Выполнить задание, аналогичное заданию 8.1.21, для группоидов, заданных на множестве $\{a, b, c, d\}$ следующими таблицами Кэли:

а)

	a	b	c	d
a	a	a	a	a
b	a	c	c	c
c	a	c	c	c
d	a	c	c	c

б)

	a	b	c	d
a	c	c	c	b
b	c	c	c	b
c	c	c	c	d
d	c	c	c	b

в)

$\cdot$	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	b	a	c	d
d	b	a	c	d

8.1.23. Найти все подалгебры алгебры с одной унарной операцией f, заданной на множестве $\{a, b, c, d\}$ следующим образом: а) $f = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$; б) $f = \begin{pmatrix} a & b & c & d \\ c & c & d & c \end{pmatrix}$.

8.1.24. Найти все подалгебры алгебры с двумя унарными операциями f и g, заданными на множестве $\{a, b, c, d, e\}$ следующим образом:

а) $f = \begin{pmatrix} a & b & c & d & e \\ a & a & c & b & b \end{pmatrix}$, $g = \begin{pmatrix} a & b & c & d & e \\ b & a & c & a & b \end{pmatrix}$;

б) $f = \begin{pmatrix} a & b & c & d & e \\ b & c & a & e & d \end{pmatrix}$, $g = \begin{pmatrix} a & b & c & d & e \\ a & a & a & e & e \end{pmatrix}$.

8.1.25. (У) Определим на множестве A тернарную операцию t, заданную следующим образом:

$$t(x, y, z) = \begin{cases} x, \text{если } y = z; \\ z, \text{если } x = y; \\ y, \text{если } x \neq y, y \neq z. \end{cases}$$

Описать все подалгебры (A, t).

8.1.26. (У) Доказать конечность алгебры, имеющей лишь конечное число подалгебр,

а) в случае полугрупп,

б) в случае групп,

в) в случае ассоциативных колец.

8.1.27. а) Из описания циклических полугрупп вытекает, что полугруппа без собственных подполугрупп одноэлементна. Привести пример неодноэлементного группоида, не имеющего собственных подгруппоидов.

б) Выяснить, для любого ли $n \geq 2$ существует n-элементный группоид без собственных подгруппоидов.

в) Привести пример бесконечного группоида без собственных подгруппоидов.

г) Привести пример неодноэлементной алгебры с одной унарной операцией, не имеющей собственных подалгебр, и выяснить, для любого ли $n \geq 2$ существует n-элементная алгебра с указанными свойствами.

д) **(У)** Объяснить, почему никакая алгебра со свойствами, указанными в п. г), не может быть бесконечной.

е)* **(У)** Привести пример бесконечной алгебры с двумя унарными операциями, не имеющей собственных подалгебр.

8.1.28.* Привести пример двух однотипных неизоморфных универсальных алгебр, изоморфно вложимых друг в друга.

8.2 Гомоморфизмы и конгруэнции

8.2.1. Пусть A, B — однотипные универсальные алгебры, причем B — гомоморфный образ A. Выяснить, верны ли следующие утверждения:

а) если A — к.п. алгебра, то и B — к.п. алгебра;

б) утверждение, обратное к утверждению п. а);

в) если A имеет базис, то и B имеет базис;

г) **(У)** утверждение, обратное к утверждению п. в).

8.2.2. Пусть в ситуации задания 8.2.1 φ — гомоморфизм A на B. Убедиться, что справедливы следующие утверждения:

а) если F — подалгебра алгебры A, то

$$\varphi(F) = \{\varphi(f) \mid f \in F\}$$

есть подалгебра алгебры B;

б) если H — подалгебра алгебры B, то

$$\varphi^{-1}(H) = \{a \in A \mid \varphi(a) \in H\}$$

есть подалгебра алгебры A;

в) если ψ — гомоморфизм A на B, отличный от φ, то множество $C = \{a \in A \mid \varphi(a) = \psi(a)\}$ есть собственная (быть может, пустая) подалгебра алгебры A.

8.2.3. а) В ситуации, описанной в п. а) задания 8.2.2, гомоморфизм φ индуцирует гомоморфизм подалгебры F на подалгебру $\varphi(F)$.

Привести пример алгебры A и такой ее подалгебры F, что существует гомоморфизм подалгебры F, который не индуцируется никаким гомоморфизмом алгебры A.

б) Привести пример ситуации, когда подалгебра C, указанная в п. в) задания 8.2.2, непуста.

в) **(У)** Привести пример ситуации, когда подалгебра C, указанная в п. в) задания 8.2.2, пуста.

8.2.4. Пусть $A_1, A_2, \ldots, A_n$ — произвольные однотипные универсальные алгебры. *Прямое произведение* этих алгебр определяется на декартовом произведении $A_1 \times A_2 \times \ldots \times A_n$ покомпонентным осуществлением всех операций на алгебрах A_k. (См. конкретные случаи данного определения, представленные в заданиях 1.1.29, 3.1.21, 7.1.21.)

Убедиться, что каждая алгебра A_k является гомоморфным образом прямого произведения $A_1 \times A_2 \times \ldots \times A_n$.

8.2.5.* Привести пример двух однотипных неизоморфных универсальных алгебр A, B таких, что B есть гомоморфный образ A, а A есть гомоморфный образ B.

8.2.6. Пусть A — произвольная универсальная алгебра.

а) Убедиться, что произведение двух эндоморфизмов алгебры A есть эндоморфизм, так что множество $\mathsf{End}(A)$ всех эндоморфизмов A является подполугруппой полугруппы $\mathcal{T}(A)$; это *полугруппа эндоморфизмов* алгебры A.

б) Доказать, что полугруппа эндоморфизмов полугруппы $(\mathbb{N}, +)$ изоморфна полугруппе $(\mathbb{N}, \cdot)$.

в) Написать таблицу Кэли для полугруппы эндоморфизмов двухэлементной цепи.

г) Выяснить, будет ли коммутативна полугруппа эндоморфизмов кольца $\mathbb{Z}_3 \times \mathbb{Z}_3$.

8.2.7. а) Доказать, что множество всех сюръективных эндоморфизмов универсальной алгебры A есть подполугруппа полугруппы $\mathsf{End}(A)$; убедиться, что она удовлетворяет левому закону сокращения: $xy = xz \Rightarrow y = z$.

б) Привести пример алгебры, для которой полугруппа эндоморфизмов не удовлетворяет левому закону сокращения.

8.2.8. а) Привести пример неодноэлементной алгебры A с одной унарной операцией, для которой всякий эндоморфизм является автоморфизмом.

б) **(У)** Объяснить, почему ситуация, указанная в п. а), невозможна для групп, колец и решеток.

в) Доказать, что любой ненулевой эндоморфизм группы $(\mathbb{Q}, +)$ является автоморфизмом.

8.2.9. а) Пусть A — аддитивная абелева группа. Доказать, что полугруппа $\mathsf{End}(A)$ превращается в кольцо, если на ней дополнительно определить операцию сложения, полагая для любых $\varphi, \psi \in \mathsf{End}(A)$ и любого $a \in A$

$$(\varphi + \psi)(a) \rightleftharpoons \varphi(a) + \psi(a).$$

б) Доказать, что кольцо эндоморфизмов группы $(\mathbb{Z}, +)$ изоморфно кольцу $(\mathbb{Z}, +, \cdot)$.

в) Выяснить, имеет ли кольцо $\mathsf{End}(\mathbb{Z}_{12})$ делители нуля.

г) Найти все натуральные n такие, что кольцо $\mathsf{End}(\mathbb{Z}_n)$ имеет делители нуля.

8.2.10. Найти все конгруэнции группоида, фигурирующего

а) в задании 8.1.21, б) в п. а) задания 8.1.22,

в) в п. б) задания 8.1.22, г) в п. в) задания 8.1.22.

8.2.11. Найти все конгруэнции алгебры, фигурирующей

а) в п. а) задания 8.1.23, б) в п. б) задания 8.1.23,

в) в п. а) задания 8.1.24, г) в п. б) задания 8.1.24.

8.2.12. Всякая конгруэнция на кольце $(K, +, \cdot)$ является одновременно конгруэнцией группы $(K, +)$ и группоида $(K, \cdot)$. Привести пример кольца $(K, +, \cdot)$ и такого отношения τ на нем, что

а) τ есть конгруэнция на $(K, +)$, но не является конгруэнцией на $(K, \cdot)$;

б) τ есть конгруэнция на $(K, \cdot)$, но не является конгруэнцией на $(K, +)$.

8.2.13. Всякая конгруэнция на решетке $(L, \vee, \wedge)$ является одновременно конгруэнцией на каждой из полугрупп $(L, \vee)$ и $(L, \wedge)$. Привести пример решетки $(L, \vee, \wedge)$ и такого отношения τ на ней, что τ является конгруэнцией только на одной из полугрупп $(L, \vee)$, $(L, \wedge)$.

8.2.14. Обозначим через $\mathsf{Con}(A)$ множество всех конгруэнций на универсальной алгебре A, частично упорядоченное отношением включения.

а) Доказать, что $\mathsf{Con}(A)$ является решеткой и притом полной.

б)* Выяснить, будет ли для любой алгебры A решетка $\mathsf{Con}(A)$ подрешеткой решетки $\mathcal{E}(A)$ всех отношений эквивалентности на A.

8.2.15. а) Убедиться, что если конгруэнции ρ и σ на данной алгебре перестановочны, то их произведение $\rho \circ \sigma$ также является конгруэнцией.

б) Доказать, что на группе любые две конгруэнции перестановочны.

в) Привести пример решетки, имеющей неперестановочные конгруэнции.

8.2.16. а) Доказать, что если отношения эквивалентности ρ и σ на множестве X перестановочны, то их произведение $\rho \circ \sigma$ совпадает с объединением $\rho \vee \sigma$ в решетке $\mathcal{E}(X)$.

б) Применяя результат, приведенный в п. а), доказать, что если любые две конгруэнции на универсальной алгебре A перестановочны, то решетка $\mathsf{Con}(A)$ модулярна.

8.2.17. Пусть A — универсальная алгебра, ρ — конгруэнция на ней, $\overline{A} = A/\rho$ — соответствующая факторалгебра.

а) Доказать, что для любой конгруэнции $\overline{\sigma}$ на $\overline{A}$ существует такая конгруэнция σ на A, что $\sigma \supseteq \rho$ и $\overline{A}/\overline{\sigma} \cong A/\sigma$.

б) Доказать, что для любой конгруэнции σ на A такой, что $\sigma \supseteq \rho$ существует такая конгруэнция $\overline{\sigma}$ на $\overline{A}$, что $A/\sigma \cong \overline{A}/\overline{\sigma}$.

8.2.18. Универсальная алгебра A называется *простой*, если у нее нет конгруэнций, кроме отношения равенства и универсального отношения.

а) **(У)** Применяя результат, приведенный в п. а) задания 8.2.17, доказать, что у любой конечной неодноэлементной алгебры есть неодноэлементный гомоморфный образ, являющийся простой алгеброй.

б) Убедиться, что алгебра, фигурирующая в задании 8.1.25, является простой.

в) **(И)** Описать все простые конечные алгебры с одной унарной операцией.

Глава 9

Булевы функции

Приведем таблицы, задающие функции, которые встречаются в формулировках заданий этой главы.

x	y	0	1	$\overline{x}$	$x \cdot y$	$x \vee y$	$x \to y$	$x \sim y$	$x + y$	$x \mid y$	$x \downarrow y$
0	0	0	1	1	0	0	1	1	0	1	1
0	1	0	1	1	0	1	1	0	1	1	0
1	0	0	1	0	0	1	0	0	1	1	0
1	1	0	1	0	1	1	1	1	0	0	0

Приоритет бинарных операций в записи формул не устанавливается, за тем исключением, что обычно предполагается, что умножение имеет более высокий приоритет (т.е. выполняется раньше), нежели остальные операции.

9.1 Простейшие свойства. Нормальные формы

9.1.1. Построить таблицы для функций, реализуемых следующими формулами:

а) $(x \to y) \oplus [(y \to z) \oplus (z \to x)]$; б) $\overline{(x \vee y)} \vee [(x \cdot \overline{z}) \downarrow (x \sim y)]$;

в) $\overline{x} \to [\overline{z} \sim (y \oplus x \cdot z)]$; г) $[((x \mid y) \downarrow z) \mid y] \downarrow z$.

9.1.2. Выяснить, какие из следующих формул являются тождественно истинными и какие — тождественно ложными:

а) $(x \to y) \to [(x \vee z) \to (y \vee z)]$;

б) $[(x \oplus y) \sim z] \cdot (x \to yz)$;
в) $[(x \vee \overline{y}) \downarrow (x \oplus \overline{y})] \oplus [\overline{(x \to \overline{y})} \to (\overline{x} \vee y]$;
г) $\{[(x \vee \overline{y}) \cdot z] \to [(x \sim z) \oplus y]\} \cdot x \cdot y \cdot z$.

9.1.3. Доказать, что формула, содержащая только связку $\sim$, тождественно истинна тогда и только тогда, когда каждая ее переменная входит в эту формулу четное число раз.

9.1.4. Привести к дизъюнктивной нормальной форме формулы:
а) $(x_1 \vee x_2\overline{x}_3) \cdot (x_1 \vee x_3)$;
б) $\{(x_1 \vee x_2\overline{x}_3x_4) \cdot [(\overline{x}_2 \vee x_4) \to x_1\overline{x}_3\overline{x}_4]\} \vee x_2x_3 \vee (\overline{x}_1 \vee x_4)$;
в) $\{(x_1 \to x_2x_3) \cdot [(x_3 \oplus x_4) \to x_1\overline{x}_4]\} \vee \overline{x}_1$.

9.1.5. Привести к совершенной дизъюнктивной нормальной форме формулы:
а) $x_1 \vee x_2x_3$;
б) $x_1\overline{x}_2 \vee \overline{x}_1x_3$;
в) $x_1 \vee \overline{x}_1x_2 \vee \overline{x}_2x_3$.

9.1.6. Привести к конъюнктивной нормальной форме формулы из задания 9.1.5.

9.1.7. Построить совершенную конъюнктивную нормальную форму для каждой формулы из задания 9.1.5.

9.1.8. Построить многочлены Жегалкина для следующих функций:
а) $(x_1 \mid x_2) \downarrow x_3$;
б) $(x_1 \to x_2)(x_2 \downarrow x_3)$;
в) $((x_1 \to x_2) \vee \overline{x}_3) \mid x_1$.

9.1.9. Выяснить, будут ли следующие функции самодвойственными:
а) $\overline{x}$; б) $x \cdot y$;
в) $x \to y$; г) $x \oplus y$;
д) $x \oplus y \oplus z$; е) $(x \cdot y) \vee (x \cdot z) \vee (y \cdot z)$;
ж) $(x \vee y) \cdot (x \vee z) \cdot (y \vee z)$.

9.1.10. Доказать, что не существует самодвойственной функции от двух переменных, существенно зависящей от каждой переменной.

9.1.11. Выяснить, будут ли следующие функции монотонными:
а) $x \cdot y \oplus y$; б) $x \cdot y \oplus x \oplus y$;
в) $x \sim y$; г) $x \to (y \to x)$;
д) $x \to (x \to y)$; е) $(x \cdot y) \vee (x \cdot z) \vee (y \cdot z)$.

9.1.12. Доказать, что функция, двойственная монотонной, сама монотонна.

9.1.13. Выяснить, будут ли следующие функции линейными:

а) $x \vee y$; б) $x \to y$; в) $x \sim y$;
г) $\overline{x \sim \overline{y}}$; д) $(x \sim y) \sim z$; е) $x \to (y \to x)$.

9.1.14. Привести пример самодвойственной линейной функции.

9.1.15.* Пусть функции f и g самодвойственны. Выяснить, при каких условиях будет самодвойственной функция:
а) $f \vee g$; б) $f \cdot g$; в) $f \to g$; г) $f \sim g$.

9.1.16.* Пусть функции f и g монотонны. Выяснить, при каких условиях будет монотонной функция:
а) $\overline{f}$; б) $f \to g$; в) $f \sim g$.

9.1.17. Пусть функции f и g линейны. Выяснить, при каких условиях будет линейной функция:
а) $f_1 \vee f_2$, б) $f \cdot g$, в) $f_1 \to f_2$.

9.1.18. а) **(У)** Объяснить, почему множество всех булевых функций от n переменных образует конечную булеву алгебру относительно операций дизъюнкции, конъюнкции и отрицания. Обозначим ее через BF_n.
б) **(У)** Найти $|BF_n|$.
в) Указать какой-нибудь базис булевой алгебры BF_n.
г) Найти все базисы алгебры BF_2.

9.1.19.* Доказать, что функцию f нельзя реализовать формулой над множеством S, когда
а) $f = x \oplus y$, $S = \{\cdot\}$;
б) $f = x \cdot y$, $S = \{\to\}$;
в) $f = x \vee y$, $S = \{\sim\}$.

9.1.20. Пусть Φ — некоторое множество функциональных символов (замещаемых булевыми функциями). *Глубина формулы* F над множеством Φ обозначается через $\mathsf{dep}_\Phi(F)$ и определяется по индукции:
1) Если F — символ переменной или 0-арный функциональный символ, то $\mathsf{dep}_\Phi(F) = 0$;
2) Если $F = f^{(n)}(F_1, \ldots, F_n)$, где $f^{(n)} \in \Phi$, то

$$\mathsf{dep}_\Phi(F) = \max_{1 \le i \le n} \mathsf{dep}_\Phi(F_i) + 1.$$

Найти формулу F минимальной глубины над множеством $\{\downarrow\}$, реализующую функцию
а) $f = x \vee y$; б) $f = x \oplus y$; в) $f = x \cdot y$.

9.1.21.* Выяснить, можно ли реализовать функцию f формулой F глубины k над множеством S, когда:

а) $f = xy$, $k = 2$, $S = \{|\}$;
б) $f = x \to y$, $k = 3$, $S = \{\vee, \sim\}$;
в) $f = x \oplus y \oplus z$, $k = 2$, $S = \{\vee, \cdot\}$.

9.2 Замкнутые и полные классы

9.2.1. Сведением к известной полной системе функций $\{x \wedge y, x \vee y, \overline{x}\}$ доказать полноту следующих систем функций:
а) $x \wedge y$, $\overline{x}$; б) $x \vee y$, $\overline{x}$; в) $\overline{(x \vee y)}$; г) $\overline{(x \wedge y)}$; д) $x \to y$, $\overline{x}$.

9.2.2. Используя теорему Поста, доказать полноту следующих классов функций:
а) $\{x \vee y, \overline{x}\}$; б) $\{0, 1, (x \cdot y) \vee z\}$;
в) $\{x \cdot y \oplus x, x \oplus y, 1\}$; г) $\{x \oplus y, x \sim (y \cdot z)\}$;
д) $\{x \cdot y, x \oplus y, x \sim (x \cdot y)\}$; е) $\{0, x \sim y, x \vee y\}$.

9.2.3. Доказать, что множество функций, двойственных функциям из замкнутого класса, образует замкнутый класс.

9.2.4. Выяснить, является ли объединение замкнутых классов замкнутым классом.

9.2.5. (У) Замкнутый класс, отличный от пустого класса и от класса всех функций алгебры логики, называется *собственным замкнутым классом*.

Доказать, что дополнение собственного замкнутого класса в классе всех функций алгебры логики не может быть замкнутым классом.

9.2.6. *Базисом* класса всех булевых функций называется минимальная полная система функций (т.е. такая полная система функций, после удаления из которой любой функции получается неполная система). Доказать, что все системы функций, приведенные в задании 9.2.1, являются базисами.

9.2.7. Доказать, что для полноты системы функций необходимо и достаточно, чтобы для всякого замкнутого класса, не совпадающего с множеством всех функций, в данной системе нашлась функция, не принадлежащая этому классу. **(С)**

9.2.8. Найти все базисы из n функций, содержащихся в классе $\{0, 1, \overline{x}, x \cdot y, x \to y, x \sim y, x \oplus y, x \mid y, x \downarrow y\}$ при
а) $n = 1$; б) $n = 2$; в) $n = 3$.

9.2.9.* а) Доказать, что из всякого базиса с помощью отождествления аргументов у входящих в него функций можно получить базис, в котором все функции зависят не более чем от трех переменных.

б) Доказать, что дальнейшее уменьшение числа переменных в утверждении п. а), вообще говоря, невозможно.

9.2.10. Базис называется *минимальным*, если при всяком отождествлении переменных у любой функции базиса получается неполная система.

Доказать, что имеется лишь конечное число различных минимальных базисов. **(С)**

9.2.11.* *Обобщенной функцией Шеффера* называется функция алгебры логики, составляющая одноэлементный базис.

Подсчитать, сколько имеется обобщенных функций Шеффера от n переменных.

9.2.12. Пусть $P_k = \{0, 1, \ldots, k-1\}$, $k \geq 2$. Всюду определенная функция, заданная на P_k, называется *функцией k-значной логики.* Класс всех таких функций обозначим через $\mathcal{F}_k$. Ясно, что класс всех булевых функций — это класс $\mathcal{F}_2$. При $k > 2$ для класса $\mathcal{F}_k$ понятия замкнутости и полноты вводятся так же, как для класса $\mathcal{F}_2$. Пусть ρ — некоторое l-местное отношение на P_k. Говорят, что функция $f(x_1, \ldots, x_m)$ из $\mathcal{F}_k$ *сохраняет* отношение ρ, если из того, что $(x_{i1}, x_{i2}, \ldots, x_{il}) \in \rho$ при $i = 1, 2, \ldots, m$ следует, что $(f(x_{11}, x_{21}, \ldots, x_{m1}), f(x_{12}, x_{22}, \ldots, x_{m2}), f(x_{1l}, x_{2l}, \ldots, x_{ml})) \in \rho$ для любых $x_{11}, x_{12}, \ldots, x_{ml} \in P_k$. Класс всех функций, сохраняющих ρ, обозначим через K_ρ.

Класс K_ρ называется *предполным*, если он является максимальным среди всех замкнутых собственных классов функций k-значной логики.

а) Доказать, что для любого непустого отношения ρ класс K_ρ является замкнутым.

б) При $k = 2$ для каждого из классов всех булевых функций, сохраняющих нуль, сохраняющих единицу, самодвойственных, монотонных, линейных найти отношение ρ, заданное на $\{0, 1\}$, для которого данный класс совпадает с K_ρ.

в) **(И)** Определить, для каких отношений эквивалентности ρ класс K_ρ будет предполным.

г) Пусть ρ — отношение частичного порядка на P_k и соответствующее ч.у. множество имеет наибольший и наименьший элементы. Доказать, что K_ρ — предполный класс.

Глава 10

Языки и автоматы

10.1 Формальные языки

Пустое слово обозначается через λ.

10.1.1. (У) Для данного множества слов над алфавитом $\{a, b\}$ определить, будет ли оно кодом, и в случае положительного ответа указать, будет ли данный код суффиксным, префиксным или бипрефиксным:

а) $\{a, aba\}$; б) $\{ab, aba\}$; в) $\{ab, ba, aba\}$;
г) $\{ab, ba, a\}$; д) $\{a^2, ba^2, ba\}$; е) $\{a^5, ba^2, ab, b\}$.

10.1.2. Рассмотрим множество слов

$$M = \{a^2, ab, c^2, c^2a, bc^2a\}$$

над алфавитом $\{a, b, c\}$.

а) Доказать, что M не является кодом.

б) Для слова $(c^2ab)^3c^2$, принадлежащего подполугруппе $\langle M\rangle$, выяснить, однозначно ли выражается это слово через элементы множества M.

в) Выполнить задание, аналогичное заданию п. б), для слова $a^2bc^2ac^2abc^2a^2bab$.

10.1.3. Выполнить задание, аналогичное заданию 10.1.1, для данного множества над алфавитом $\{a, b, c, d\}$:

а) $\{a, ab, ca, dc, bcad^2\}$;
б) $\{a, b, d^2, cd^3, d^2ac, cd^2ab\}$;

в) $\{a, ab, ab^2, acb^2, b^2ac^2\}$;

г) $\{abc, b^2c, bcb, ca^2, acb^2, (cb)^2, bc^2ab^2, abcacb^3\}$;

д) $\{abc, ab^2, bc^2, c^2a^2, bcab^3c^2, b^2c^2a^3bca, abcab^2ab^3c^2a\}$;

е) $\{ab, b^2, ca, ab^2, bac, cba, a^2bc, cab^2a\}$.

10.1.4. Выполнить задание, аналогичное заданию 10.1.1, для каждого из следующих множеств над алфавитом A:

а) $\{x_1x_2\dots x_n \mid x_j \in A,\ j = 1, \dots, n\}$ для данного $n \in \mathbb{N}$;

б) $\{a^nb \mid n \in \mathbb{N}\}$ для различных фиксированных $a, b \in A$;

в) $\{ab^n \mid n \in \mathbb{N}\}$ для различных фиксированных $a, b \in A$;

г) $\{a^nb^n \mid n \in \mathbb{N}\}$ для различных фиксированных $a, b \in A$.

10.1.5. Выяснить, справедливы ли для любых языков L_1, L_2, L_3 над алфавитом A равенства:

а) $L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3$;

б) $L_1(L_2 \cap L_3) = L_1L_2 \cap L_1L_3$.

10.1.6. Для конечных языков L_1 и L_2 над данным алфавитом убедиться, что $|L_1 \cdot L_2| \le |L_1| \cdot |L_2|$ и привести примеры, когда $|L_1 \cdot L_2| = |L_1| \cdot |L_2|$ и когда $|L_1 \cdot L_2| < |L_1| \cdot |L_2|$.

10.1.7. а) Доказать, что если L_1 и L_2 — конечные языки над данным алфавитом, то из $L_1^2 = L_2^2$ следует $L_1 = L_2$.

б) Выяснить, верна ли импликация, указанная в п. а), для любых языков.

10.1.8. Пусть L, L_1, L_2 — произвольные языки, u, v — произвольные слова над данным алфавитом A, $a \in A$. Через $u^{-1}L$ обозначим множество $\{v \in A^* \mid uv \in L\}$.

Доказать формулы:

а) $u^{-1}(L_1 \cup L_2) = u^{-1}L_1 \cup u^{-1}L_2$;

б) $u^{-1}(L_1 \cap L_2) = u^{-1}L_1 \cap u^{-1}L_2$;

в) $u^{-1}(L_1 \setminus L_2) = u^{-1}L_1 \setminus u^{-1}L_2$;

г) $v^{-1}(u^{-1}L) = (uv)^{-1}L$;

д) $a^{-1}L^* = (a^{-1}L)L^*$;

е) $a^{-1}(L_1L_2) = \begin{cases} (a^{-1}L_1)L_2, & \text{если } \lambda \notin L_1, \\ (a^{-1}L_1)L_2 \cup a^{-1}L_2, & \text{если } \lambda \in L_1. \end{cases}$

10.1.9. Через v^* обозначается язык, состоящий из всех степеней слова v и пустого слова. Выписать все слова длины $\le m$, принадлежащие языку над алфавитом $\{a, b\}$, заданному следующим регулярным выражением:

а) a^*bb^*, $m = 4$; б) $(a^* + b^*)(ab^2 + a^2b)$, $m = 5$;

в) $(ab)^* + (ba)^*$, $m = 6$; г) $b^*a^*b + a^*(ba)^*$, $m = 6$.

10.1.10. Определить, будет ли регулярным язык над алфавитом $\{a, b\}$, состоящий из слов, указанных ниже, и в случае положительного ответа записать соответствующее регулярное выражение:

а) содержащих ровно один раз букву a,

б) начинающихся с a,

в) не содержащих подслово aba,

г) не содержащих в качестве подслова фиксированное слово v.

10.1.11. Найти праволинейные грамматики, порождающие следующие языки:

а) множество всех непустых слов над алфавитом $\{a, b, 0, 1\}$, начинающихся с a или с b;

б) множество всех непустых слов длины не более 3, составленных из латинских букв $a, b, c, \ldots, z$, цифр $0, 1, \ldots, 9$ и начинающихся с некоторой буквы;

в) множество всех непустых слов над алфавитом $\{0, 1\}$, имеющих четную длину.

10.1.12. Задать регулярными выражениями языки, указанные в задании 10.1.11.

10.1.13. а) Доказать, что грамматика с множеством нетерминальных символов $\{A, S\}$, где S — начальный символ, множеством терминальных символов $\{0, 1\}$ и множеством продукций $\{S \to 0A1,\ 0A \to 00A1,\ A \to \lambda\}$ порождает язык $\{0^n 1^n \mid n \in \mathbb{N}\}$.

б) Найти контекстно-свободную грамматику, порождающую язык, указанный в п. а)

10.1.14. Доказать, что формальная грамматика с множеством нетерминальных символов $\{B, C, S\}$, где S — начальный символ, множеством терминальных символов $\{a, b, c\}$ и множеством продукций $\{S \to aSBC,\ S \to abc,\ CB \to BC,\ bB \to bb,\ cB \to Bc,\ bC \to bc,\ cC \to cc\}$ порождает язык $\{a^n b^n c^n \mid n \in \mathbb{N}\}$.

10.1.15. Пусть формальная грамматика G_k $(k = 1, 2, 3, 4)$ имеет множество нетерминальных символов $\{D, S\}$, причем S — начальный символ, множество терминальных символов $\{a, b, c\}$ и множество продукций P_k. В каждом из указанных случаев найти язык, порождаемый соответствующей грамматикой: а) $P_1 = \{S \to aSa,\ S \to bSb,\ S \to c\}$; б) $P_2 = = \{S \to Sab,\ Sa \to aD,\ Db \to b\}$; в) $P_3 = \{S \to aSS,\ S \to a\}$;
г) $P_4 = \{S \to SS,\ S \to aDb,\ D \to aDb,\ D \to \lambda$.

10.2 Конечные автоматы

Автоматы в заданиях этого параграфа определяются либо помеченными графами, либо таблицами переходов, строки которых помечены состояниями, а столбцы — символами входного алфавита. Начальное состояние помечено входящей стрелкой $\rightarrow$, а заключительные состояния помечены исходящей стрелкой $\leftarrow$. Если начальное состояние является и заключительным, то оно помечается двусторонней стрелкой $\leftrightarrow$. При решении заданий, в которых используется задание автомата с помощью таблицы, целесообразно представлять автомат в виде помеченного графа.

10.2.1. Дан автомат $\mathscr{A}$.

$\mathscr{A}$	a	b
$\rightarrow 1$	4	1
2	1	3
3	1	6
4	2	3
$\leftarrow 5$	2	3
$\leftarrow 6$	5	1

а) Найти самое короткое слово, принимаемое автоматом $\mathscr{A}$.

б) Найти четыре других слова, принимаемых $\mathscr{A}$.

в) Найти четыре слова, отвергаемых $\mathscr{A}$.

г) Построить граф автомата $\mathscr{A}$.

10.2.2. Даны два автомата $\mathscr{A}_1$ и $\mathscr{A}_2$:

$\mathscr{A}_1$	a	b
$\leftrightarrow 1$	1	2
2	3	4
$\leftarrow 3$	2	1
4	1	2

$\mathscr{A}_2$	a	b
$\leftrightarrow 1$	1	4
2	1	4
$\leftarrow 3$	2	1
4	3	2

Существует ли слово, которое их различает (т.е. отвергается одним автоматом, но принимается другим)?

10.2.3. Построить конечный автомат, распознающий язык над алфавитом $\{a, b\}$, состоящий из всех таких слов u, что

а) буква a входит в u четное число раз, а буква b — нечетное число раз,

б) между любыми двумя вхождениями буквы a в u четное число вхождений буквы b,

в) подслово aa входит в u четное число раз (перекрывающиеся вхождения допускаются, т.е., скажем, в слово aaa подслово aa входит 2 раза),

г) за каждым вхождением подслова bb в u следует буква a,

д) каждый третий символ в u — буква a.

10.2.4. По данной таблице построить граф автомата и охарактеризовать язык, распознаваемый этим автоматом.

а)

$\mathscr{A}$	a	b
$\to 1$	2	1
2	2	3
$\leftarrow 3$	3	3

б)

$\mathscr{B}$	a	b
$\to 1$	2	3
$\leftarrow 2$	3	2
3	3	3

в)

$\mathscr{C}$	a	b
$\to 1$	2	3
$\leftarrow 2$	4	2
$\leftarrow 3$	3	4
4	4	4

г)

$\mathscr{D}$	a	b
$\to 1$	2	1
2	4	3
$\leftarrow 3$	3	4
4	4	4

10.2.5. Для каждого из автоматов, представленных графами на рис. 15, описать язык, распознаваемый этим автоматом.

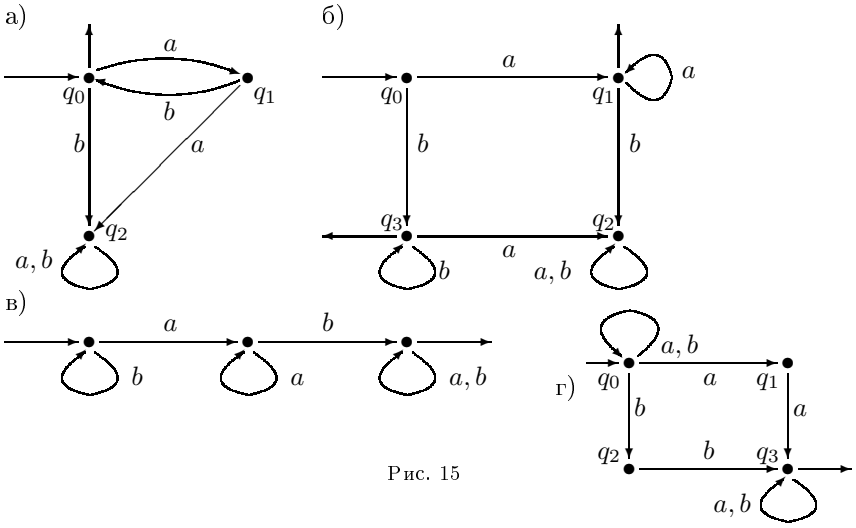


Рис. 15

10.2.6. Определить, будет ли распознаваемым язык над конечным алфавитом, состоящий из всех слов: а) четной длины, б) нечетной длины.

10.2.7.* Доказать, что язык $\{a^p \mid p$ — простое число$\}$ над алфавитом $\{a\}$ нераспознаваем.

10.2.8.* Построить конечный автомат, распознающий числа $\leq$ 10000, записанные римскими цифрами, как слова в алфавите {I, V, X, L, C, D, M}.

10.2.9. Рассмотрим автоматы, полученные с помощью графа на рис. 16 указанием начального и заключительного состояния.

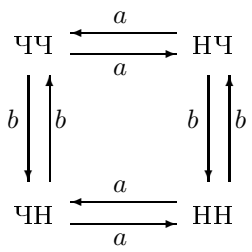


Рис. 16

а) Убедиться, что каждый полученный таким образом автомат, в зависимости от того, какое состояние считается начальным, а какое — заключительным, принимает слова с четным или нечетным числом букв a или b.

б) Построить моноид переходов каждого такого автомата.

10.2.10. Если автомат $\mathscr{A}=(Q, A, \delta)$ *неполный*, т.е. функция δ определена не на всем множестве $Q \times A$, а лишь на некотором его подмножестве, то моноид переходов $M(\mathscr{A})$ строится по тому же алгоритму, что и для полных автоматов, с той лишь разницей, что элементами $M(\mathscr{A})$ будут не полные, а частичные преобразования множества Q. Для каждого $m = 1, 2, 3, \ldots$ рассмотрим следующий автомат $\mathscr{A}_m$:

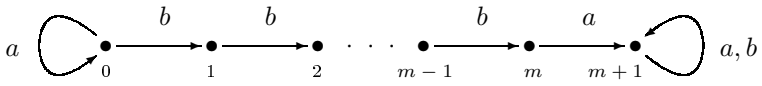


Рис. 17

а) Построить моноид $M(\mathscr{A}_1)$.

б) Построить моноид $M(\mathscr{A}_2)$.

в) Сколько элементов содержит моноид $M(\mathscr{A}_m)$?

10.2.11. Построить моноид переходов неполного автомата, представленного графом на рис. 18.

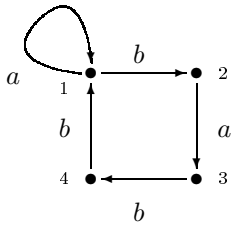


Рис. 18

10.2.12. Построить автомат с тремя состояниями, моноидом переходов которого была бы симметрическая полугруппа на трехэлементном множестве.

10.2.13. Пусть $A = \{a\}$ — одноэлементный алфавит. Зафиксируем произвольный корень $\varepsilon \in \mathbb{C}_n$ и определим отображение моноидов $\varphi_\varepsilon : A^* \longrightarrow \mathbb{C}_n$, которое в каждом слове из A^* заменяет букву a на ε. Доказать, что φ_ε — гомоморфизм, который будет сюръективным тогда и только тогда, когда корень ε — первообразный.

10.2.14. В каждом из следующих случаев нарисовать граф автомата, отвечающего гомоморфизму $\varphi_\varepsilon A^* \longrightarrow \mathbb{C}_n$, определенному в задании 10.2.13:

а) $n = 3$, $\varepsilon = \frac{1}{2} + i\frac{\sqrt{3}}{2}$; б) $n = 6$, $\varepsilon = \frac{1}{2} + i\frac{\sqrt{3}}{2}$;

в) $n = 7$, $\varepsilon = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$; г) $n = 8$, $\varepsilon = i$.

10.2.15. Нарисовать граф минимального автомата для каждого из следующих языков:

а) $L = \{a^m b^n |\ m, n > 0\}$;

б) $L = (a^2 + aba + ba)^*$;

в) $L = a^*b + bb^*a$;

г) $L = a^*(a^2b + bb^*a + b^2)^*$.

10.2.16. Нарисовать граф минимального автомата, распознающий тот же язык, что и следующие автоматы:

а)

$\mathscr{A}$	a	b
$\to 0$	1	2
1	1	3
$\leftarrow 2$	2	4
3	1	5
$\leftarrow 4$	6	2
5	5	3
$\leftarrow 6$	6	6

б)

$\mathscr{A}$	a	b
$\leftrightarrow 1$	4	1
$\leftarrow 2$	5	1
3	4	5
4	2	6
5	1	7
$\leftarrow 6$	1	4
$\leftarrow 7$	2	5

10.2.17. Автомат $\mathscr{A}$ называется *синхронизируемым*, если существует слово w (над входным алфавитом автомата), которое переводит $\mathscr{A}$ из произвольного состояния q в некоторое фиксированное состояние q^*, не зависящее от q. Слово w с таким свойством называется *синхронизирующим*.

а) Проверить, что слово ab^3ab^3a является синхронизирующим для автомата $\mathscr{A}$, представленного графом на рис. 19.

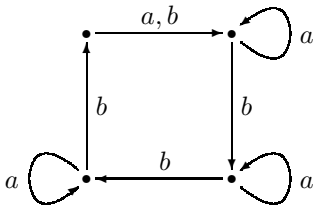


Рис. 19

б) Проверить, что никакое слово длины < 9 не является синхронизирующим для $\mathscr{A}$.

в) **(И)** Для каждого из автоматов, представленных графами на рис. 15 а),б), в) и на рис. 16, определить, какие из них являются синхронизируемыми. Для каждого синхронизируемого автомата определить, какова наименьшая длина синхронизирующих слов.

г) **(И)** Выяснить, какова наименьшая длина синхронизирующих слов для синхронизируемых автоматов с тремя состояниями.

д)* Для каждого натурального $n > 4$ привести пример синхронизируемого автомата с n состояниями, для которого никакое слово длины $< (n-1)^2$ не является синхронизирующим.

е)* Доказать, что для любого синхронизируемого автомата язык, состоящий из всех его синхронизирующих слов, является регулярным.

Советы и указания

1.1.2 ж), о). Обратить внимание, что ответ зависит от значений d и λ соответственно.
1.1.6 б). Такой алгоритм описан в книге [12], т.1, §1.2.
1.1.20 а), б). Рассмотреть неразложимые (т.е. не представимые в виде произведения двух каких-либо элементов) элементы соответствующих полугрупп.
1.1.26. Достаточно взять двухэлементное множество I.
1.1.31 а). Вспомнить представление комплексных чисел в алгебраической форме.
1.1.31 б). Доказать, что если полугруппа с нулем изоморфна прямому произведению полугрупп S_1 и S_2, то эти полугруппы также имеют нуль. Вывести отсюда, что тогда в $S_1 \times S_2$ должны быть ненулевые элементы, произведение которых равно нулю.
1.1.34. Показать, что в прямом произведении двух неодноэлементных полугрупп не выполняется утверждение п. а) задания 1.1.33.
1.1.40 в). Можно воспользоваться таблицей Кэли для полугруппы B_2, составленной при выполнении задания 1.1.4.
1.1.43. Использовать изоморфизм полугруппы матриц $\mathbf{M}_n(\mathbb{C})$ и полугруппы линейных операторов на n-мерном унитарном пространстве.
1.3.15. Сравнить с заданием 1.3.14.
2.1.19 б). Рассмотреть группу $\mathbf{UT}_3(\mathbb{Z}_2)$.
2.1.20 а). Воспользоваться первым из тождеств, указанным в задании 2.1.18.
2.2.12. Показать, что каждая матрица из $\mathbf{GL}_n(F)$ представима в виде $t_1 \cdots t_r d(\beta) t_{r+1} \cdots t_s$, где t_k — трансвекции.
2.2.19. Воспользоваться результатом задания 2.1.17.
2.2.28 б). Нетривиален здесь случай, когда данные циклические по-

лугруппы S_1 и S_2 конечны, и искомые условия в этом случае должны быть сформулированы в терминах индекса и периода полугрупп S_1 и S_2.

2.3.9 б). Рассмотреть в группе S_8 подгруппу $G = \langle a, b\rangle$, где $a = (1234)(5678)$, $b = (1537)(2846)$. Показать, что $|G| = 8$ и группа G неабелева, хотя все ее подгруппы нормальны.

3.1.17. Воспользоваться утверждением задания 1.1.38.

3.2.9. Считать известным, что π является трансцендентным числом, т.е. не является корнем никакого многочлена с целыми коэффициентами.

3.2.12. Рассмотреть матрицы, аналогичные матричным единицам, имеющие на соответствующих местах элементы порождающего множества кольца K.

3.2.14. Рассмотреть функции $\delta_{x,k}$ $(x \in X,\ k \in K)$, определенные следующим образом: $\delta_{x,k}(z) = \begin{cases} k, \text{ если } z = x, \\ 0, \text{ если } z \neq x. \end{cases}$

3.2.17. Использовать умножение с каждой стороны на матричные единицы.

3.2.23. Рассмотреть идеалы вида xR для $x \in R$.

3.2.24 а). См. указание к заданию 3.2.17.

3.3.10. Доказать, что для любых x_1, x_2 из K найдется $x \in K$ такой, что $x - x_1 \in I_1$ и $x - x_2 \in I_2$.

3.4.7. Принять во внимание, что подмодули кольца, рассматриваемого как правый модуль над собой, суть в точности его правые идеалы.

3.4.9. Заменить элементы алгебры линейными операторами, индуцируемыми при умножении справа (элементу $a \in A$ сопоставляется линейный оператор $\mathcal{A}_a : V \longrightarrow V$, определяемый следующим образом: $\mathcal{A}_a x = xa$ для любого $x \in A$).

4.1.14. Рассмотреть поле рациональных функций над полем $\mathbb{C}$.

4.2.7. Для доказательства необходимости разложить многочлен $x^{p-1} - 1$ на линейные множители над полем $\mathbb{Z}_p$.

6.1.2 б). Воспользоваться результатом п. б) задания 6.1.1.

8.1.17 а). Рассмотреть отдельно случаи, когда U обладает максимальными собственными подалгебрами и когда не обладает. Доказать, что в первом случае ее подалгебра Фраттини совпадает с пересечением всех максимальных собственных подалгебр.

8.1.18 в). Убедиться, что в аддитивной группе $\mathbb{Q}$ любой элемент является непорождающим.

8.1.19. Убедиться, что в кольце $\mathbb{Q}$ максимальные подкольца исчер-

пываются множествами $\{\frac{m}{n} \mid m \in \mathbb{Z},\ n \in \mathbb{N},\ p$ не делит $n\}$, где p — фиксированное простое число, по всем простым p.

9.2.7. Воспользоваться теоремой Поста и тем фактом, что каждый замкнутый класс содержится в одном из классов функций, сохраняющих нуль, функций, сохраняющих единицу, самодвойственных функций, монотонных функций, линейных функций.

9.2.10. Воспользоваться утверждением а) из задания 9.2.9.

Ответы

1.1.1. В п. а), в), г) — не полугруппы; в п. б), д) $(\mathbb{N}, +)$, е), ж) $(\mathbb{Z}\backslash\{0\}, \cdot)$ — полугруппы, но не группы; все группоиды из пп. д) и ж), за исключением упомянутых выше, и из пп. з), и), к), м) — группы; в п. л) при $r = 0$ или $r = 1$ группа, при положительных $r \neq 1$ множество не замкнуто относительно умножения; при $r < 0$ пустое множество.
1.1.2. В пп. а), б), е), з), к) ,м), н), п), р) — группа; в пп. в), г), д), и) — множество не замкнуто относительно умножения; в п. ж) при $d = 0$ — полугруппа, но не группа; при $d = 1$ — группа; при остальных значениях d множество не замкнуто относительно умножения; в п. л) — полугруппа, но не группа; в п. о) — если λ является квадратом рационального числа, то полугруппа, но не группа; в противном случае — группа.
1.1.4. б)

	O	e_{11}	e_{12}	e_{21}	e_{22}
O	O	O	O	O	O
e_{11}	O	e_{11}	e_{12}	O	O
e_{12}	O	O	O	e_{11}	e_{12}
e_{21}	O	e_{21}	e_{22}	O	O
e_{22}	O	O	O	e_{21}	e_{22}

1.1.7. б) В случае, когда она одноэлементна; в) тогда и только тогда, когда они равномощны. **1.1.8.** а) В случае, когда она одноэлементна; б) тогда и только тогда, когда они равны. **1.1.9.** б) Множество M имеет наибольший элемент; наименьший элемент; г) не изоморфны; д) изоморфны; е) не изоморфны. **1.1.10.** б) Не изоморфны. **1.1.11.** б) Не изоморфны. **1.1.12.** б), в) Не изоморфны; г) тогда и только тогда, когда M_1 и M_2 равномощны. **1.1.13.** б), в) Не изоморфны; г) тогда и только тогда, когда M_1 и M_2 равномощны. **1.1.14.** б), в) Не изоморфны; г) тогда и только тогда, когда M_1 и M_2 равномощны. **1.1.16.** Изоморфны. **1.1.17.** а), б) Изоморфны. **1.1.18.** б) Изоморфны; в) Не изоморфны. **1.1.19.** Не изоморфны. **1.1.20.** а), б) Не изоморфны. **1.1.21.** В п. а), б), в), г), ж), з) — полугруппы; в пп. г), ж) — группы, в пп. д), е) — множество не замкнуто относительно операции. **1.1.24.** а) n^n; б) $(1+n)^n$ в) 2^{n^2}. **1.1.31.** а) Изоморфна прямому произведению аддитивной полугруппы действительных чисел на себя; б) не изоморфна прямому произведению никаких неодноэлементных полугрупп. **1.1.32.** а) n^m; б) $\frac{n^{m+1}-1}{n-1}$ при $n \neq 1$ и 1 при $n = 1$. **1.1.35.** в) При $|X| = 1$. **1.1.36.** Нет. **1.1.37.** а) Да; б) нет. **1.1.40.** б) Например, любая неодноэлементная прямоугольная полугруппа.

1.1.44. а) Да; б) нет. **1.1.46.** Нет. **1.1.47.** 1) $\begin{array}{|c|c|c|}\hline & a & b \\ \hline a & a & a \\ \hline b & a & a \\ \hline \end{array}$; 2) $\begin{array}{|c|c|c|}\hline & a & b \\ \hline a & a & b \\ \hline b & b & a \\ \hline \end{array}$; 3) $\begin{array}{|c|c|c|}\hline & a & b \\ \hline a & a & a \\ \hline b & a & b \\ \hline \end{array}$; 4) $\begin{array}{|c|c|c|}\hline & a & b \\ \hline a & a & b \\ \hline b & a & b \\ \hline \end{array}$; 5) $\begin{array}{|c|c|c|}\hline & a & b \\ \hline a & a & a \\ \hline b & b & b \\ \hline \end{array}$. **1.1.48.** В обозначениях ответа к заданию 1.1.47: а) коммутативные полугруппы — 1), 2), 3); б) полугруппы с сокращениями — 2); в) регулярные полугруппы — 2)–5); г) группы — 2). **1.2.1.** б) Нет. **1.2.2.** а) $\left\{\begin{pmatrix}1&2\\2&1\end{pmatrix}, \begin{pmatrix}1&2\\1&1\end{pmatrix}\right\}$; $\left\{\begin{pmatrix}1&2\\2&1\end{pmatrix}, \begin{pmatrix}1&2\\2&2\end{pmatrix}\right\}$; в) $(\mathbb{Q},+)$. **1.2.5.** а)–г) Нет. **1.2.6.** а) M конечно; б) существует система попарно непересекающихся интервалов, каждый из которых содержит ровно одну точку множества M. **1.2.8.** а) Подполугруппа $\{a^k \mid k \geq 2\}$ бесконечной циклической полугруппы $\langle a\rangle$; б) полугруппа индекса 6 и периода 1. **1.2.10.** а) Индекс 2, период 3; б) индекс 3, период 2. **1.2.11.** Порядок 2, индекс 2, период 1. **1.2.12.** В пп. а),г) порядок 2, индекс 1, период 2; б) порядок 4, индекс 1, период 4; в) бесконечный порядок. **1.2.13.** а) Все матрицы, аннулируемые многочленами x, $x+1$, $x-1$, x^2, x^2+1, x^2-1, x^2-x+1, x^2+x+1. б) Все матрицы, аннулируемые многочленами с целочисленными коэффициентами степени не выше n, имеющие вид $x^m f(x)$, где $f(x)$ — делитель x^k-1 для некоторого натурального числа k. **1.2.15.** а) $\{d\}$, $\{c,d\}$, $\{b,c,d\}$, $\{a,c,d\}$, $\{a,b,c,d\}$; б) $\{b\}$, $\{a,b\}$, $\{d\}$, $\{c,d\}$, $\{a,b,d\}$, $\{a,b,c,d\}$; в) каждое подмножество является подполугруппой. **1.2.17.** а), б) Отображения, тождественные на своем образе; в) транзитивное отношение α, удовлетворяющее условию $\forall (a,b)\in\alpha\ \exists c\in X\colon (a,c),\ (b,c)\in\alpha$; г) $\emptyset$; д) $\emptyset$ и все одноэлементные отрезки; е) все элементы полугруппы. **1.2.18.** $\sum_{k=0}^{n} k^n C_n^k$. **1.2.21.** а) Подполугруппа $\langle a^2, a^3\rangle$ свободной полугруппы $\{a\}^+$ не изоморфна никакой свободной полугруппе; б) подполугруппа $\langle a, ab, ab^2, \ldots\rangle$. **1.2.22.** б) Мультипликативная полугруппа всех корней из единицы всевозможных степеней (коммутативная); полугруппа всех преобразований множества $\mathbb{N}$, имеющих конечные образы, (некоммутативная). **1.2.24.** д) Левые идеалы — всевозможные непустые подмножества, правый идеал единствен (сама полугруппа). **1.2.25.** а) Множества $\{n\in\mathbb{N} \mid n\geq m\}$, где $m\in\mathbb{N}$. **1.2.26.** б) $\{\alpha\in\mathcal{T}_n \mid |\alpha(X)|\leq k\}$, $1\leq k\leq n$. **1.3.1.** а), в), г) Нет, б) да. **1.3.2.** б) Нет. **1.3.3.** а) Нет, б) да. **1.3.4.** а) $n\mapsto na$, где $a\in\mathbb{N}$; б) $n\mapsto na$, где $a\in\mathbb{Z}$; в) $m\mapsto 0$ для любого $m\in\mathbb{Z}$. **1.3.5.** а) $\begin{pmatrix}1&2\\1&2\end{pmatrix}$, $\begin{pmatrix}1&2\\1&3\end{pmatrix}$, $\begin{pmatrix}1&2\\2&3\end{pmatrix}$, $\begin{pmatrix}1&2\\1&1\end{pmatrix}$, $\begin{pmatrix}1&2\\2&2\end{pmatrix}$, $\begin{pmatrix}1&2\\3&3\end{pmatrix}$; б) $\begin{pmatrix}1&2&3\\1&1&1\end{pmatrix}$, $\begin{pmatrix}1&2&3\\2&2&2\end{pmatrix}$, $\begin{pmatrix}1&2&3\\1&1&2\end{pmatrix}$, $\begin{pmatrix}1&2&3\\1&2&2\end{pmatrix}$; в) $\begin{pmatrix}1&2&\ldots&n\\ \alpha_1&\alpha_2&\ldots&\alpha_n\end{pmatrix}$, где $\alpha_1,\alpha_2,\ldots,\alpha_n\in\{1,2,\ldots,m\}$ и $\alpha_1\leq\alpha_2\leq\ldots\leq\alpha_n$. **1.3.6.** $n\mapsto n[a]$, где $[a]$ — класс вычетов из $\mathbb{Z}_m$, $m=3,8,n$. **1.3.7.** а) $\{\{a,b,c\},\{d\}\}$, $\{\{a,b\},\{c,d\}\}$, $\{\{a\},\{b\},\{c,d\}\}$, Δ, ∇; б) $\{\{a,b\},\{c,d\}\}$, Δ, ∇; в) $\{\{a,b\},\{c,d\}\}$, Δ, ∇. **1.3.9.** $\{(s,t)\mid s,t\in\mathbb{N}, s\geq t\geq m,\ k \text{ делит } s-t\}$ для всех $m,k\in\mathbb{N}$. **1.3.10.** Δ, ∇. **1.3.12.** б) $\rho_{M\cap N}=\rho_M\cap\rho_N$, $\rho_{M\cup N}=\rho_M\cup\rho_N\cup(M\cup N)$. **1.3.13.** в) $\mathscr{R}=\Delta$, $\mathscr{L}=\nabla$; г) $(x,y)\mathscr{L}(u,v)\Leftrightarrow y=v$, $(x,y)\mathscr{R}(u,v)\Leftrightarrow x=u$; д) $x\mathscr{L}y\Leftrightarrow x=e_{km}$, $y=e_{lm}$, где $k,l,m\in\{1,2\}$ или $x=y$, $x\mathscr{R}y\Leftrightarrow x=e_{km}$, $y=e_{kl}$, где $k,l,m\in\{1,2\}$ или $x=y$. **1.3.14.** $\mathcal{A}\,\mathscr{R}\,\mathcal{B}\Leftrightarrow \mathsf{Ker}\mathcal{A}=$

$\mathsf{Ker}\mathcal{B}$, $\mathcal{A}\mathscr{L}\mathcal{B} \Leftrightarrow \mathsf{Im}\mathcal{A} = \mathsf{Im}\mathcal{B}$. **2.1.4.** б) Нет. в) Не всегда, тогда и только тогда, когда $ax = xa$ для всех $x \in G$. **2.1.5.** Нет. **2.1.6.** б) Нет. **2.1.8.** $\{(\mathbb{Z},+)$, $(n\mathbb{Z},+)$, $\mathbf{UT}_2(\mathbb{Z})$, $E(\mathbb{Z})\}$, $\{(\mathbb{Q},+)$, $\mathbf{UT}_2(\mathbb{Q})$, $E(\mathbb{Q})\}$, $\{(\mathbb{R},+)$, $\mathbf{UT}_2(\mathbb{R})$, $E(\mathbb{R})\}$, $\{(\mathbb{C},+)$, $\mathbf{UT}_2(\mathbb{C})\}$, $\{(\mathbb{Q}^*,\cdot)\}$, $\{(\mathbb{R}^*,\cdot)\}$, $\{(\mathbb{C}^*,\cdot)\}$. **2.1.13.** а) $\mathbb{C}_6 \cong \mathbb{C}_2 \times \mathbb{C}_3$. б) $\mathbb{C}^* \cong \mathbb{R}^+ \times \{z \in \mathbb{C} \mid |z| = 1\}$. в) $\mathbf{GL}_n(\mathbb{R}) \cong \mathbb{R}^* \times \mathbf{SL}_n(\mathbb{R})$. **2.1.15.** Нет. **2.1.19.** б) Нет. **2.1.20.** в) S_3, г) $\mathbf{UT}_3(\mathbb{Z}_2)$. **2.2.1.** а) $\{m, n\}$, где $(m, n) = 1$ и $1 \notin \{m, n\}$, б) $\{q_1, \ldots, q_n\}$, где $q_k = \prod_{m \neq k} p_m$, $k = 1, \ldots, n$, $p_1, \ldots, p_n$ — различные простые числа. **2.2.3.** б), в) Нет. **2.2.4.** Да. **2.2.5.** а) Да, б) нет. **2.2.10.** а) Например, $\{(12), (12\ldots n), \begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 2 & \ldots & n \end{pmatrix}\}$, б) 3. **2.2.20.** б) Нет. **2.2.21.** а) $2\mathbb{Z}$, $\mathbb{Z}$, $3\mathbb{Z}$; б) $\mathbb{C}_4$, $\mathbb{C}_3$, $\mathbb{C}_4$, $\{2^m, 2^m i, -2^m i \mid m \in \mathbb{Z}\}$. **2.2.22.** а), б) Да. **2.2.24.** а) G, $\langle a^2\rangle$,$\langle a^3\rangle$, $\langle a^4\rangle$, $\langle a^6\rangle$, $\langle a^8\rangle$, $\langle a^{12}\rangle$, $E = \langle a^{24}\rangle$; б) G, $\langle a^2\rangle$, $\langle a^5\rangle$, $\langle a^{10}\rangle$, $\langle a^{20}\rangle$, $\langle a^{25}\rangle$, $\langle a^{50}\rangle$, $E = \langle a^{100}\rangle$; в) G, $\langle a^2\rangle$, $\langle a^3\rangle$, $\langle a^4\rangle$, $\langle a^5\rangle$, $\langle a^6\rangle$, $\langle a^8\rangle$, $\langle a^9\rangle$, $\langle a^{10}\rangle$, $\langle a^{12}\rangle$, $\langle a^{15}\rangle$, $\langle a^{18}\rangle$, $\langle a^{20}\rangle$, $\langle a^{24}\rangle$, $\langle a^{30}\rangle$, $\langle a^{36}\rangle$, $\langle a^{40}\rangle$, $\langle a^{45}\rangle$, $\langle a^{45}\rangle$, $\langle a^{60}\rangle$,$\langle a^{72}\rangle$, $\langle a^{90}\rangle$, $\langle a^{120}\rangle$, , $\langle a^{240}\rangle$, $E = \langle a^{360}\rangle$; г) G, $\langle a^5\rangle$, $\langle a^2 5\rangle$, $E = \langle a^{125}\rangle$; д) G, $\langle a^{p^m}\rangle$, где $m = 1, 2, \ldots, n-1$, $E = \langle a^{p^n}\rangle$. **2.2.28.** а) Две конечные циклические группы изоморфны тогда и только тогда, когда они имеют одинаковые порядки; б) две конечные циклические полугруппы изоморфны тогда и только тогда, когда они имеют одинаковые индексы и периоды. **2.2.32.** а) 2, б) 2, в) бесконечный порядок, г) 4. **2.2.33.** а) 6, б) 5, в) 12, г) 8, д) 4, е) 8, ж) 2. **2.2.34.** а) 8, б) 4, в) 15, г) 6. **2.2.35.** Наибольший порядок 15. **2.2.36.** а) $1, 2, 4$; б) $1, 5$; в) $1, 2, 4, 8$; г) $1, 2, 3$; д) $1, 2, 3, 4$. **2.2.38.** Тождества а) и б) выполняются. **2.2.39.** а) $3, 5, 4, 11$; б) в $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_{11}$. **2.2.42.** $n/(k, n)$. **2.2.43.** а) a^{4k}, $k = 1, 2, 3, 4, 5$; a^4 и a^{20} имеют порядок 5. б) a^{6k}, $k = 1, 2, 3, 4$; a^6 и a^{18} имеют порядок 4. в) a^{5k}, $k = 1, 2, \ldots, 20$; a^{5m} при $m = 1, 3, 7, 9, 11, 13, 17, 19$ имеют порядок 20. г) a^{20k}, $k = 1, 2, 3, 4, 5$; все эти элементы имеют порядок 5. д) a^{50}, элементов порядка 6 нет. е) 1, элементов порядка 7 нет. **2.2.44.** $p^m - p^{m-1}$. **2.2.47.** Неверно. **2.2.48.** а) $\mathbb{C}_{p^\infty}$ — бесконечная периодическая абелева группа; множество всех биекций α множества $\mathbb{N}$ на себя, обладающих тем свойством, что множество $\{n \in \mathbb{N} \mid \alpha(n) \neq n\}$ конечно, является бесконечной периодической неабелевой группой. **2.2.49.** Периодическая часть группы $\mathbb{C}^*$ — группа $G = \cup_{k=1}^{\infty} \mathbb{C}_k$, периодическая часть группы $\mathbf{D}_n(\mathbb{C})$ — группа $\mathbf{D}_n(G)$ диагональных матриц с элементами из группы G на главной диагонали. **2.2.51.** а) $\{x \in \mathbb{R} \mid x < 0\}$. б) $\{-3, 3\}$. в) $\{a - ai \mid a \in \mathbb{R},\ a > 0\}$. г) $\{\sqrt{2}(\cos\varphi + i\sin\varphi) \mid 0 \leq \varphi < 2\pi\}$. **2.2.52.** а) $gH = \{(123), (13)\}$, $Hg = \{(132), (13)\}$. б) $gH = Hg = \{(23), (12), (13)\}$. **2.2.53.** а) $3\mathbb{Z}$, $\{3k+1 \mid k \in \mathbb{Z}\}$, $\{3k+2 \mid k \in \mathbb{Z}\}$. б) $\{nk+r \mid k \in \mathbb{Z}\}$, $r = 0, 1, \ldots, n-1$. **2.2.54.** а) $\{x(a + bi) \mid x \in \mathbb{R}^+,\ a^2 + b^2 > 0\}$, лучи, исходящие из начала координат. б) $\{a(\cos\varphi + i\sin\varphi) \mid 0 \leq \varphi < 2\pi,\ a > 0\}$, концентрические окружности с центром в начале координат. **2.3.1.** а), г). **2.3.2.** а), в), д), е). **2.3.4.** а) G — абелева группа. б) G — абелева группа, не содержащая инволюций. **2.3.5.** а), б) Отображения, получаемые продолжением до гомоморфизма из отображений $1 \mapsto a$ $(a \in \mathbb{Z}_n)$ в случае а) и отображений $[1] \mapsto a$ $(a \in \mathbb{Z}_3)$ в случае б). в) Нулевой гомоморфизм. **2.3.6.** а) $\{-1, 1\}$. б) $\{z \in \mathbb{C} \mid |z| = 1\}$. в) $\mathbf{SL}_n(F)$. г) $2\pi\mathbb{Z}$. д) $\mathbb{C}_n$. **2.3.7.** $\mathbf{UT}_n(K)$. **2.3.8.** б) $\mathbf{GL}_2(\mathbb{Q})$. г) Да. **2.3.9.** б) Нет. **2.3.13.** а) $(\{-1, 1\}, \cdot)$. б), г) $(\mathbb{R}^+, \cdot)$. в) $(\mathbb{C}^*, \cdot)$. д) $(\mathbb{R}, +)$. е) $\{z \in \mathbb{C} \mid |z| = 1\}$. ж) $\cup_{k=1}^{\infty} \mathbb{C}_k$. **2.3.15.** $\mathbf{D}_n(K)$. **3.1.1.** В пп.

а) – г), е) – н) — кольца; б)–г), л), н) — поля. **3.1.2.** В пп. в), д), е), ж), з), и) — кольца; е) поле; ж) поле, при условии, что d не является квадратом в соответствующем поле. **3.1.5. 3.1.7.** 3-элементное поле и 3-элементное кольцо, в котором произведение двух любых элементов равно нулю. **3.1.10.** В пп. а), б), в) — кольца. **3.1.7.** б) Нет. **3.1.14.** В $\mathbb{Z}_9$ — классы вычетов [3], [6]; в $\mathbb{Z}_{12}$ — [2], [3], [4], [6], [8], [9], [10]; $\mathbb{Z}_8$ — [2], [4], [6]; в $\mathbb{Z}$ нет делителей нуля. **3.1.15.** Если d не является полным квадратом. **3.1.19.** Если $[a] \in \mathbb{Z}_n$, то $[a]$ обратим $\Leftrightarrow (a,n)=1$; $[a]$ — делитель нуля $\Leftrightarrow (a,n)>1$; $[a]$ — делитель нуля $\Leftrightarrow (a,n)>1$ $[a]$ — нильпотентный элемент $\Leftrightarrow a$ и n имеют совпадающие множества простых делителей. Если $[a] \in \mathbb{Z}_{p^n}$, то $[a]$ обратим $\Leftrightarrow p$ не делит a; $[a]$ — делитель нуля $\Leftrightarrow [a]$ — нильпотентный элемент $\Leftrightarrow p$ делит a. Если $A \in \mathbf{M}_2(\mathbb{R})$, то A обратим $\Leftrightarrow \mathsf{det}(A) \neq 0$; A — делитель нуля $\Leftrightarrow \mathsf{det}(A)=0$; A — нильпотентный элемент $\Leftrightarrow A^2=0$, откуда легко получаются условия для элементов матрицы A. **3.1.22.** Тогда и только тогда, когда каждое из колец R_k обладает соответствующим свойством. **3.1.25.** $x=(x_1,x_2,\ldots,x_n)\in R$ является обратимым элементом $\Leftrightarrow$ все элементы x_k обратимы; x является делителем нуля $\Leftrightarrow x_k=0$ для некоторого k или все элементы $x_1,x_2,\ldots,x_n$ являются делителями нуля; x является нильпотентным элементом $\Leftrightarrow$ элементы $x_1,x_2,\ldots,x_n$ являются нильпотентными элементами или равны нулю. **3.2.1.** а) $\{1\}$. б) $\{(1,0),(0,1)\}$. в) $\{1,x\}$. г) $\{e_{11},e_{12},e_{21},e_{22}\}$. д) $\{e_{ij} \mid i,j=1,2,\ldots,n\}$. е) $\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}x&0\\0&0\end{pmatrix},\begin{pmatrix}0&x\\0&0\end{pmatrix},\begin{pmatrix}0&0\\x&0\end{pmatrix},\begin{pmatrix}0&0\\0&x\end{pmatrix}\right\}$. **3.2.4.** Подкольца в $\mathbb{Z}$: $n\mathbb{Z}$, где $n\in\mathbb{Z}$. Подкольца в $\mathbb{Z}_3$: $\{[0]\}$, $\mathbb{Z}_3$. Подкольца в $\mathbb{Z}_9$: $\{[0]\}$, $3\mathbb{Z}_9$, $\mathbb{Z}_9$. Подкольца в $\mathbb{Z}_{12}$: $\{[0]\}$, $2\mathbb{Z}_{12}$, $3\mathbb{Z}_{12}$, $4\mathbb{Z}_{12}$, $6\mathbb{Z}_{12}$, $\mathbb{Z}_{12}$. **3.2.5.** $\{([0],[0])\}$; $\{([0],[0]),([0],[1]),([0],[2])\}$; $\{([0],[0]),([1],[0]),([2],[0])\}$; $\{([1],[1]),([2],[2]),([3],[3])\}$.

3.2.6. а), б) Нет (если объединяемые кольца не совпадают). **3.2.8.** а) $\left\{\begin{pmatrix}a&0\\0&b\end{pmatrix} \;\middle|\; \begin{array}{l}a,b\in\mathbb{Z}\\ a+b\in 2\mathbb{Z}\end{array}\right\}$. б), в) $\left\{\begin{pmatrix}a&b\\0&a\end{pmatrix} \mid a,b\in\mathbb{Z}\right\}$. **3.2.10.** а) $x\mathbb{Z}[x]$. б) $x^2\mathbb{Z}[x]$. в) $x\mathbb{Z}[x]+2\mathbb{Z}$. г) Множество всех многочленов из $\mathbb{Z}[x]$, не содержащих свободного члена, первой и третьей степени x. **3.2.11.** а) $\mathbb{Z}$. б) $\mathbb{Z}+\sqrt{2}\mathbb{Z}$. в) $\mathbb{Z}+\sqrt{2}\mathbb{Z}+\sqrt{3}\mathbb{Z}+\sqrt{6}\mathbb{Z}$. **3.2.12.** а), б), в) Да. **3.2.15.** б) Множество всех скалярных матриц (т.е. матриц вида aE, где E — единичная матрица). **3.2.18.** Да. **3.2.20.** В $\mathbb{Z}_9$ и $\mathbb{Z}_{16}$ необратимые элементы образуют идеал, а в $\mathbb{Z}_{12}$ нет. **3.2.17.** $\mathbf{M}_n(m\mathbb{Z})$ при всех $m\in\mathbb{Z}$. **3.2.25.** а) $p\mathbb{Z}$, где p — простое число. б) $p\mathbb{Z}\times\mathbb{Z}$, $\mathbb{Z}\times p\mathbb{Z}$, где p — простое число. в), г), д) $\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix} \mid a,b\in\mathbb{R}\right\}$, $\left\{\begin{pmatrix}0&a\\0&b\end{pmatrix} \mid a,b\in\mathbb{R}\right\}$ **3.3.2.** $\mathsf{Ker}\varphi=(x^2+1)\mathbb{R}[x]$. **3.3.3.** $\mathsf{Ker}\varphi=(x^2+x+1)\mathbb{Q}[x]$. **3.3.4.** $\mathsf{Ker}\varphi=(x^2-2)\mathbb{Q}[x]$. **3.3.6.** $(1+i)+J$ — нильпотентный элемент. **3.3.8.** Для $\mathbb{C}$ один класс — кольца, изоморфные $\mathbb{C}\times\mathbb{C}$. Для $\mathbb{R}$ два класса — кольца, изоморфные $\mathbb{C}$ или $\mathbb{R}\times\mathbb{R}$. Для $\mathbb{Q}$ счетное множество классов — кольца, изоморфные $\mathbb{Q}\times\mathbb{Q}$ или $\mathbb{Q}+\sqrt{k}\mathbb{Q}$ или $\mathbb{Q}+\sqrt{k}i\mathbb{Q}$, где k — натуральное число, являющееся произведением различных простых чисел. Для конечного поля $\mathbb{F}$ — кольца, изоморфные $\mathbb{F}\times\mathbb{F}$ или расширению $\mathbb{F}$ с помощью одного элемента. **3.3.9.** Обратимые элементы $[g]$, где $(f,g)=1$. Делители

нуля $[g]$, где $(f,g)\neq 1$. Нильпотентные элементы $[g]$, где множества неприводимых делителей многочленов f и g совпадают. **3.3.5.** а), б) Да. **3.4.6.** а), б) Да. в) Нет. **3.4.7.** Подмодули — односторонние идеалы. Ненулевые собственные правые идеалы кольца $\mathbf{M}_2(F)$ исчерпываются множествами $\left\{\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}\,\middle|\, a,b\in F\right\}$, $\left\{\begin{pmatrix} 0 & 0\\ a & b\end{pmatrix}\,\middle|\, a,b\in F\right\}$ **4.1.5.** а) Все рациональные числа; б) все числа вида $\alpha+\beta\sqrt{2},\quad \alpha,\beta\in\mathbb{Q}$; в) все числа вида $\alpha+\beta\sqrt[3]{2}+\gamma\sqrt[3]{4},\quad \alpha,\beta,\gamma\in\mathbb{Q}$. **4.1.6.** а) все числа вида $\alpha+\beta i,\quad \alpha,\beta\in\mathbb{Q}$; б) все комплексные числа. **4.1.7.** а) Нет; б) тогда и только тогда, когда $\frac{m}{n}$ — квадрат рационального числа. **4.1.9.** Тождественный автоморфизм и $z\mapsto\overline{z}$. **4.1.14.** Да, существует. **4.1.15.** а) $x_1=-1$, $x_2=-3+2\sqrt{2}$; б) $x_1=2-2\sqrt{2}$, $x_2=-1+3\sqrt{2}$; в) $\emptyset$ (нет действительных корней); г) $\emptyset$ ($\sqrt[4]{2}\notin\mathbb{Q}(\sqrt{2})$). **4.1.16.** а) $f_1=1$, $f_2=-1$; б) $\emptyset$, так как $1+4x$ не является квадратом в поле $\mathbb{R}(x)$. **4.2.4.** а) Система несовместна; б) $(2,3,2)$ в) $(5,6,5)$. **4.2.5.** а) 4, 7; б) 2; в) при $a=0$ $x=0$; при $a=1$ $x_{1,2}=1,8$; при $a=2$ $x=7$; при $a=3$ $x=9$; при $a=4$ $x=5$; при $a=5$ $x=3$; при $a=6$ нет решений; при $a=7$ $x=6$; при $a=8$ $x=2$; при $a=9$ $x=4$; при $a=10$ $x=10$. **4.2.6.** $\frac{p^n-1}{p-1}$. **4.2.8.** а) $(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$; б) $(x-1)(x+1)(x^2+1)(x^4+1)$. **4.2.9** б) Все элементы, кроме 0 и 1, являются примитивными. **4.2.10.** б) Если α — какой-то примитивный элемент $\mathbf{GF}(16)$, то примитивными будут элементы α, α_2, α_4, α_7, α_8, α_{11}, α_{13}, α_{14}. При условии, что в качестве α выбран один из корней многочлена x^4+x+1, представление этих элементов в виде многочленов от α будет следующим: α, α_2, $1+\alpha$, $1+\alpha+\alpha^3$, $1+\alpha^2$, $\alpha+\alpha^2+\alpha^3$, $1+\alpha^2+\alpha^3$, $1+\alpha^3$.**4.2.11.** а) Возьмем в качестве примитивного элемента поля корень α многочлена x^4+x+1. Тогда ответ можно записать в виде следующей таблицы:

элементы	минимальный многочлен
1	$x+1$
α, α^2, α^4, α^8	x^4+x+1
α^3, α^6, α^9, α^{12}	$x^4+x^3+x^2+x+1$
α^5, α^{10}	x^2+x+1
α^7, α^{11}, α^{13}, α^{14}	

б) Возьмем в качестве примитивного элемента поля корень β многочлена x^5+x^2+1. Тогда ответ можно записать в виде следующей таблицы:

элементы	минимальный многочлен
1	$x+1$
β, β^2, β^4, β^8, β^{16}	x^5+x^2+1
β^3, β^6, β^{12}, β^{17}, β^{24}	$x^5+x^4+x^3+x^2+1$
β^5, β^9, β^{10}, β^{18}, β^{20}	$x^5+x^4+x^2+x+1$
β^7, β^{14}, β^{19}, β^{25}, β^{28}	$x^5+x^3+x^2+x+1$
β^{11}, β^{13}, β^{21}, β^{22}, β^{26}	$x^5+x^4+x^3+x+1$
β^{15}, β^{23}, β^{27}, β^{29}, β^{30}	x^5+x^3+1

4.2.12. а) $x^8+x^7+x^6+x^3+1$; б) $x^{10}+x^8+x^5+x^4+x^2+x+1$;
в) $x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$. **4.2.13.**
а) $x^{10}+x^9+x^8+x^6+x^5+x^3+1$;
б) $x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1$;
в,г) $x^{20}+x^{18}+x^{17}+x^{13}+x^{10}+x^9+x^7+x^6+x^4+x^2+1$.
4.2.14. в) Для β из первой строки под ним дано значение $1+\beta$:

α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
α^4	α^8	α^{14}	α	α^{10}	α^{13}	α^9	α^2	α^7	α^5	α^{12}	α^{11}	α^6	α^3

5.1.2. б) $\sum_{r=0}^{k} C_n^r$. **5.1.3.** 01, 10, 11, 00. **5.1.8.** а), г) Обнаруживает 2 ошибки, исправляет одну ошибку; б) обнаруживает 4 ошибки, исправляет одну ошибку; в) обнаруживает одну ошибку, не исправляет ни одной (для слова 110000 однозначное декодирование невозможно).

5.2.3. а) $H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$, $H_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$,
минимальное расстояние каждого кода равно 3;

б) Ошибка	Синдром для H_1	Синдром для H_2
10000	111	110
01000	101	011
00100	100	100
00010	010	010
00001	001	001

в) Слово	Результат декодирования с помощью первого кода	Результат декодирования с помощью второго кода
10010	11	10
11011	11	01
10101	10	11
11010	11	не декодируется
00111	10	не декодируется
11101	01	11
00110	00	10

5.2.4. а) $H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$, б) $H_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$,
минимальное расстояние каждого кода равно 3;

б) Ошибка	Синдром для H_1	Синдром для H_2
100000	110	100
010000	011	010
001000	101	001
000100	100	101
000010	010	110
000001	001	011

в) Слово	Результат декодирования с помощью первого кода	Результат декодирования с помощью второго кода
111101	110	101
110101	110	111
001111	001	не декодируется
100100	100	100
110001	110	не декодируется
111111	не декодируется	не декодируется
111100	111	100
010100	не декодируется	не декодируется

5.2.5. а) Порождающая матрица $\begin{pmatrix} 1&0&0&0&0&0&0&0&1\\ 0&1&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&0&0&1\\ 0&0&0&1&0&0&0&0&1\\ 0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&0&1&1 \end{pmatrix}$, проверочная матрица (111111111);

б) минимальное расстояние равно 2. Код обнаруживает одну ошибку; исправлять ошибки он не может.

5.2.6. а) Исходные слова 1011 и 1101, а передавались слова 1011010 и 1101001; б) Исходное слово 11110010110, передавалось слово 111100101100000.

в) Пусть стирания произошли в позициях i и j, $1 \leq i < j \leq 7$. Полагаем i-й и j-й разряды равными 0 и вычисляем синдром. Если синдром равен 0, то i-й и j-й разряды передаваемого слова равнялись нулю. Если синдром равен i (соотв. j), то в i-м (соотв. в j-м) разряде передаваемого слова стояла единица, а в j-м (соотв. в i-м) — нуль. Наконец, если синдром не равен ни 0, ни i, ни j, то i-й и j-й разряды передаваемого слова равнялись нулю.

5.2.7. д) Нет, не всегда удастся отличить тройную ошибку от одиночной. е) Ошибочен 8-й символ. Если считать, что кодирование осуществлялось систематическим образом, то исходное слово 1100.

5.2.9. б) Если порождающий многочлен $g(x)$ кода C выбрать так, чтобы он делил $x^n - 1$, то порождающий многочлен кода $C^\perp$ будет частным $\frac{x^n-1}{g(x)}$.

5.2.10. а) Проверочная матрица

$$\begin{pmatrix} 1&0&0&0&1&0&1&1&0&0&0&0&0&0&0\\ 0&1&0&0&0&1&0&1&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&1&0&1&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&1&0&1&1&0&0&0&0\\ 0&0&0&0&1&0&0&0&1&0&1&1&0&0&0\\ 0&0&0&0&0&1&0&0&0&1&0&1&1&0&0\\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&0\\ 0&0&0&0&0&0&0&1&0&0&0&1&0&1&1 \end{pmatrix},$$

минимальное расстояние равно 5, код может исправлять две ошибки.

б) Проверочная матрица

$$\begin{pmatrix} 1&0&0&1&1&1&0&0&1&1&0&0&0&0&0\\ 0&1&0&0&1&1&1&0&0&1&1&0&0&0&0\\ 0&0&1&0&0&1&1&1&0&0&1&1&0&0&0\\ 0&0&0&1&0&0&1&1&1&0&0&1&1&0&0\\ 0&0&0&0&1&0&0&1&1&1&0&0&1&1&0\\ 0&0&0&0&0&1&0&0&1&1&1&0&0&1&1 \end{pmatrix},$$

минимальное расстояние равно 3, код может исправлять одну ошибку.

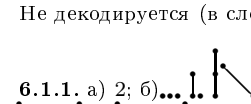
5.2.11. а) Допущено две ошибки. Многочлен локаторов ошибок $\alpha^6 x^2 + \alpha^{14} x + 1$, многочлен ошибок $x^{11} + x^{10}$.

б) Многочлен ошибок $x^6 + x^5$, передававшееся слово 100111001100000, исходное слово 0110000.

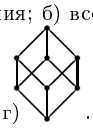
Многочлен ошибок $x^7 + x^5$, передававшееся слово 100100100100100, исходное слово 1100100.

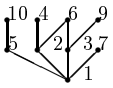
5.2.12. а) Допущено три ошибки. Многочлен локаторов ошибок $\alpha^5 x^3 + \alpha^7 x^2 +$

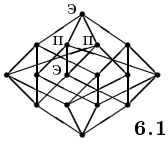
$\alpha^5 x + 1$, многочлен ошибок $x^{12} + x^7 + x$.
б) Допущено три ошибки. Многочлен локаторов ошибок $\alpha^{14}x^3 + \alpha^{11}x^2 + \alpha^{14}x + 1$, многочлен ошибок $x^7 + x^5 + ^2 x$.
в) Допущено две ошибки. Многочлен локаторов ошибок $\alpha^{13}x^2 + \alpha^{12}x + 1$, многочлен ошибок $x^{10} + x^3$.
Многочлен ошибок $x^{10} + x^3$, передававшееся слово 000010100110001, исходное слово 00001.
Многочлен ошибок $x^{10} + x^3 + x$, передававшееся слово 000101101100110, исходное слово 00010.
Не декодируется (в слове допущено больше трех ошибок).

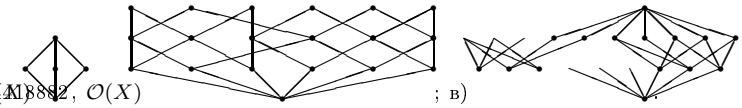
6.1.1. а) 2; б)  ; в).

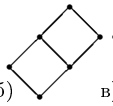
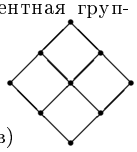
6.1.2. а) всего 3 отношения; б) всего 19 отношений.

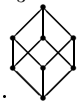
6.1.3. а) ; б) ; в)  ; г)  .

6.1.4. а) 

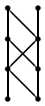
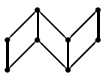
; б) нет; да; в) да. **6.1.5.**, **6.1.6.** а) 

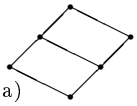
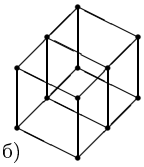
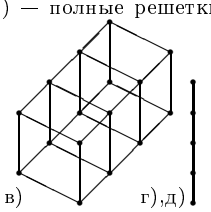
6.1.6. б) 
$Z(X)$, $\mathcal{O}(X)$; в) .

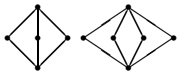
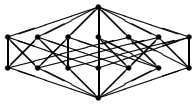
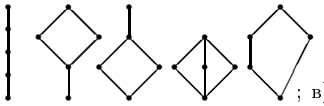
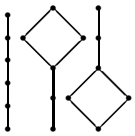
6.1.8. в) $a < b < c < d$, $a < c < b < d$; г) $a < b < c < d$, $a < c < b < d$, $b < a < c < d$. **6.1.10.** а) Ч.у. множество, являющееся объединением бесконечной возрастающей цепи и 1-элементного множества, элемент которого несравним ни с одним элементом цепи; б) нет. **6.1.12.** б) hl. **6.1.13.** а) Тождественное отображение ε и цикл (b_3, b_4); б) ε, (b_1, b_2), (b_3, b_4), $(b_1, b_2)(b_3, b_4)$; в) ε, (b_1, b_2), (b_3, b_4), (d_1, d_2), (d_3, d_4) и всевозможные произведения этих элементов по 2, по 3 и по 4 (всего 12), (b_1, b_3, b_2, b_4), (b_1, b_4, b_2, b_3), (d_1, d_3, d_2, d_4), (d_1, d_4, d_2, d_3) и попарные произведения этих элементов (всего 12), итого 32 автоморфизма. **6.1.14.** Группа автоморфизмов изоморфна а) $\mathbb{Z}_2$; б) $\mathbb{Z}_2^2$; в) $\mathbb{Z}_2^5$. **6.1.16.** а) 1-элементная группа; б) изоморфна симметрической группе S_3. **6.1..** а)  б)  в) 

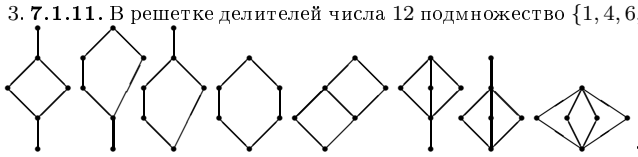
6.1.aea7a. а) Нет; б) $\{k, l\} = \{m, n\}$. **6.1.23.**  **6.1.24.** б) Да, верно. **6.1.25.** а) 3;

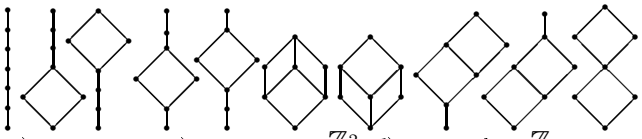
6; 4; г) A — 2-элементная антицепь, B — 2-элементная цепь. **6.1.27.** а) $A{+}B$  $B{+}A$  б) A — 1-элементное множество, B — 2-элементная цепь. **6.1.34.** а) 6-элементная цепь; г) может, если одна из цепей 1-элементна.

6.1.35. а)  б)  **6.1.38.** б) Группоид $\{a, b\}$, в котором $ab = b$, а все остальные произведения равны a. **6.1.42.** б) $\mathbb{Z}_4$. **6.2.2.** а) Две конечные цепи изоморфны тогда и только тогда, когда они имеют одинаковое число элементов. **6.2.3.** а), б) 1-элементная группа; в) группа, изоморфная $(\mathrm{Z}, +)$. **6.2.4.**а) $\mathbb{Z}$, $\mathbb{Q}$; б) множества действительных чисел $[0, 1]$, $(0, 1)$. **6.2.6.** б) $f(x) = \frac{2x}{1-|x|}$; в) $f(x) = \frac{2x-a-b}{b-a-|x|}$. **6.2.8.** а) $\mathbb{Q}$. **6.2.15.** а) 4; б) 7; в) $\frac{n^2+n+3}{2}$. **6.2.17.** а) Любые конечные ординалы; б) $\alpha = \omega$, $\beta = 2$.

7.1.1. Все, кроме д), е) — решетки; а), г), з)–н) — полные решетки. **7.1.2.** а), в) Нет; б) да. **7.1.4.** а)  б)  в)  г),д)

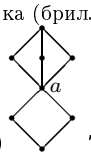
7.1.6. Нет. **7.1.7.** а)  б) $q{+}3$. **7.1.8.** а)  б) $q^2{+}q{+}3$. **7.1.11.** В решетке делителей числа 12 подмножество $\{1, 4, 6, 12\}$. **7.1.12.** а)  ; б)  ; в) 



7.1.13. 

7.1.16. в) Да. **7.1.18.** а) Изоморфна $\mathbb{Z}_2^2$; б) изоморфна $\mathbb{Z}_2$. **7.1.19.** а) Например, ординальная сумма 4-элементной решетки, не являющейся цепью, и цепи натуральных чисел. **7.2.1.** б) Например, L_1 — 4-элементная решетка, не являющаяся цепью, L_2 — 4-элементная цепь, φ — биекция L_1 на L_2, переводящая нуль в нуль, единицу в единицу. **7.2.3.** а)–г) Цепь разбивается в объединение

двух подмножеств, все элементы первого из которых переводятся в 0, а второго — в единицу; если оба подмножества непусты, то цепь является ординальной суммой первого и второго подмножества. **7.2.4.** а) L — дистрибутивная решетка; б) L — 5-элементная модулярная недистрибутивная решетка (бриллиант), a — ее

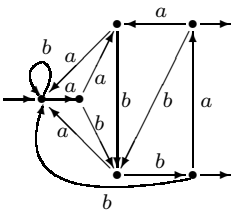


нуль, b — произвольный элемент, отличный от 0 и от 1; е) **7.2.8.** а) Цепь $a < b < c < d$, конгруэнции: отношение равенства Δ, универсальное отношение ∇, отношения, определяемые разбиениями $\{a\}$, $\{b,c,d\}$; $\{a,b\}$, $\{c,d\}$; $\{a\}$, $\{b\}$, $\{c,d\}$; $\{a,b\}$, $\{c\}$, $\{d\}$; $\{a,b,c\}$, $\{d\}$. б) Пусть a, b — сравнимые элементы пентагона, отличные от 0 и от 1, c — оставшийся элемент, конгруэнции: Δ, ∇, $\{a,b\}$, $\{c\}$, $\{1\}$, $\{0\}$; $\{1,c\}$, $\{0,a,b\}$; $\{0,c\}$, $\{1,a,b\}$. **7.2.10.** а) Например, 3-элементная цепь. **7.3.1.** а), б) См. ответы к заданиям 6.1.3 в), г). **7.3.5.** n — произведение различных простых чисел. **7.3.6.** в) Да. **7.3.8.** б) При $n \geq 2$, только если $n = 2$ и L_1, L_2 — одноэлементные булевы алгебры. **8.1.1.** а) $K = \mathbb{Z}[x]$, $X = \{1, x, x^2, \ldots\}$; б) $K = \mathbb{Z}$, $Y = \{0, -1, 2, 3, 5, 7, \ldots\}$. **8.1.2.** а) $K = \mathbb{Z}[x]$, базис $\{1, x\}$. **8.1.4.** г) Например, обе полугруппы — $(\mathbb{N}, +)$. **8.1.7.** а) Например, полугруппа левых нулей; б) $(\mathbb{N}, +)$. **8.1.13.** б) При условии, что размерность пространства не превосходит 1. **8.1.16.** а) Свободная 2-порожденная полугруппа; б) свободная 2-порожденная группа; в) $\mathbb{Z}[x_1, x_2]$. **8.1.17.** б) Неодноэлементная решетка и одноэлементная решетка. **8.1.18.** а) $\{0\}$, если n делится на два различных простых числа, и $p^{k-1}\mathbb{Z}_n$, если $n = p^k$; б) $\{0\}$; в) $\mathbb{Q}$. **8.1.19.** $\{0\}$. **8.1.21.** $\{a\}$, $\{c\}$, $\{a,b\}$, $\{a,c\}$, $\{a,b,c\}$. **8.1.22.** а) $\{a\}$, $\{c\}$, $\{b,c\}$, $\{a,c\}$, $\{c,d\}$, $\{a,b,c\}$, $\{a,c,d\}$, $\{b,c,d\}$, $\{a,b,c,d\}$; б) $\{a,c\}$, $\{b,c\}$, $\{c,d\}$, $\{a,b,c\}$, $\{b,c,d\}$, $\{a,b,d\}$, $\{a,b,c,d\}$. **8.1.23.** а) $\{a,b\}$, $\{c,d\}$, $\{a,b,c,d\}$; б) $\{c,d\}$, $\{a,c,d\}$, $\{b,c,d\}$, $\{a,b,c,d\}$, **8.1.24.** а) $\{c\}$, $\{a,b\}$, $\{a,b,d\}$, $\{a,b,e\}$ $\{a,b,c,d,e\}$; б) $\{a,b,c\}$, $\{a,b,c,d\}$, $\{a,b,c,e\}$, $\{a,b,c,d,e\}$. **8.1.25.** Все непустые подмножества. **8.1.27.** а)

	a	b
a	b	a
b	a	a

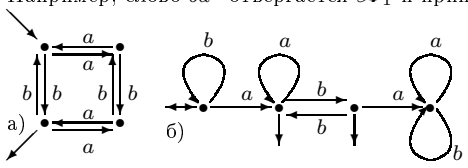
; б) да; в) $G = \{a_1, a_2, \ldots\}$, $a_i \circ a_j = a_{i+1}$, $i = 1, 2, \ldots$; г) $G = \{a_1, a_2, \ldots, a_n\}$, $f(a_i) = a_{i+1}$, $i = 1, 2, \ldots, n-1$, $f(a_n) = a_1$; е) $G = \{a_1, a_2, \ldots\}$, $f(a_i) = a_{i+1}$, $i = 1, 2, \ldots$, $g(a_1) = a_1$, $g(a_i) = a_{i-1}$, $i = 2, 3 \ldots$, **8.1.28.** Например, 2-порожденная и 3-порожденная свободные полугруппы. **8.2.1.** а) да; б)–г) нет. **8.2.3.** а) $A = S_3$, $F = \langle(12)\rangle$, тождественный автоморфизм F; б) если $\psi(A) \cap \varphi(A) \neq \emptyset$, например, для любых гомоморфизмов групп или колец; в) если $\psi(A) \cap \varphi(A) = \emptyset$, например, для подходящих гомоморфизмов 3-элементной цепи в 2-элементную, когда все элементы переходят в 0 или все элементы переходят в 1. **8.2.5.** Например, полугруппы $(\mathbb{N}, \cdot)$ и $(\mathbb{Z}\backslash\{0\}, \cdot)$. **8.2.6.** г) Нет. **8.2.7.** б) Например, полугруппа левых нулей. **8.2.8.** а) $A = (\{a,b\}, f)$, $f(a) = b$, $f(b) = a$. **8.2.9.** в) Да; г) $n > 1$ и n не является простым числом. **8.2.10.** а) Δ, ∇, $\{a,b\} \cup \{c\}$, $\{a,c\} \cup \{b\}$; б) Δ, ∇, $\{a,c\} \cup \{b,d\}$, $\{a,,b\} \cup \{d\}$, $\{a,,d\} \cup \{b\}$; в) Δ, ∇, $\{a\} \cup \{b,c,d\}$; г) Δ, ∇, $\{a,b\} \cup \{c,d\}$. **8.2.11.** а) Δ, ∇, $\{a,b\} \cup \{c,d\}$; б) Δ, ∇, $\{a,b\} \cup \{c,d\}$, $\{a\} \cup \{b,c,d\}$; в) Δ, ∇, $\{a,b,c\} \cup \{d,e\}$, $\{c\} \cup \{a,b,e,d\}$, $\{d\} \cup \{a,b,c,e\}$, $\{e\} \cup \{a,b,c,d\}$; г) Δ, ∇, $\{a,b,c\} \cup \{d,e\}$. **8.2.12.** а) $\mathbb{Q}$, $x \tau y \Leftrightarrow x - y \in \mathbb{Z}$; б) $\mathbb{Q}$, $x \tau y \Leftrightarrow xy = 1$ или $x = y = 0$. **8.2.13.** L — 4-элементная решетка, не являющаяся цепью, τ — отношение экви-

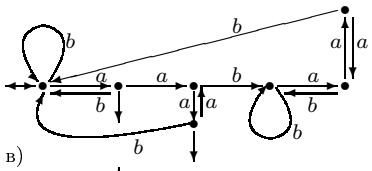
валентности, определяемое разбиением $\{1\}\cup L\backslash\{1\}$. **8.2.14.** б) Нет. **8.2.15.** в) Например, 4-элементная цепь. **9.1.2.**а) Тождественно истинная, г) тождественно ложная. **9.1.4.** а) x_1; б) $x_1x_2\overline{x}_4\vee x_1\overline{x}_3\overline{x}_4\vee x_2x_3\vee\overline{x}_1\vee x_4$; в) $x_1x_2x_3\overline{x}_4\vee x_2x_3x_4\vee\overline{x}_1$. Напомним, что результат приведения к дизъюнктивной нормальной форме определен не однозначно. **9.1.5.** а) $x_1x_2x_3\vee x_1x_2\overline{x}_3\vee x_1\overline{x}_2x_3\vee x_1\overline{x}_2\overline{x}_3\vee\overline{x}_1x_2x_3$; б) $x_1\overline{x}_2x_3\vee x_1\overline{x}_2\overline{x}_3\vee\overline{x}_1x_2x_3\vee\overline{x}_1\overline{x}_2x_3$; в) $x_1x_2x_3\vee x_1x_2\overline{x}_3\vee x_1\overline{x}_2x_3\vee x_1\overline{x}_2\overline{x}_3\vee\overline{x}_1x_2x_3\vee\overline{x}_1\overline{x}_2x_3\vee\overline{x}_1x_2\overline{x}_3\vee\overline{x}_1\overline{x}_2x_3$. **9.1.6.** а) $(x_1\vee x_2)(x_1\vee x_3)$; б) $(x_1\vee x_3)(\overline{x}_1\vee\overline{x}_2)(\overline{x}_2\vee x_3)$; в) $x_1\vee x_2\vee x_3$. Напомним, что результат приведения к конъюнктивной нормальной форме определен не однозначно. **9.1.7.** а) $(x_1\vee x_2\vee x_3)(x_1\vee x_2\vee\overline{x}_3)(x_1\vee\overline{x}_2\vee x_3)$; б) $(x_1\vee x_2\vee x_3)(x_1\vee\overline{x}_2\vee x_3)(\overline{x}_1\vee\overline{x}_2\vee x_3)(\overline{x}_1\vee\overline{x}_2\vee\overline{x}_3)$; в) $x_1\vee x_2\vee x_3$. **9.1.8.** а) $x_1x_2x_3\oplus x_1x_2$; б) $x_1x_2x_3\oplus x_1x_2\oplus x_1x_3\oplus x_2x_2\oplus x_1\oplus x_2\oplus x_3\oplus 1$; в) $x_1x_2x_3\oplus x_1x_3\oplus x_1\oplus 1$. **9.1.9.** а), д), е), ж) Самодвойственные, остальные не являются самодвойственными. **9.1.11.** б), г), е) Монотонные, остальные не являются монотонными. **9.1.13.** в), г), д), е) Линейные, остальные не являются линейными. **9.1.20.** а) $x\vee y=(x\downarrow y)\downarrow(x\downarrow y)$; б) $x\oplus y=(x\downarrow y)\downarrow[(x\downarrow x)\downarrow(y\downarrow y)]$; в) $x\cdot y=(x\downarrow x)\downarrow(y\downarrow y)$. **9.1.21.** а) да, $x\cdot y=(x\mid y)\mid(x\mid y)$; б) нет; в) нет. **9.2.4.** Нет, не является. **9.2.8.** а) $\{x\mid y\}$, $\{x\downarrow y\}$; б) $\{x\cdot y,\overline{x}\}$, $\{x\vee y,\overline{x}\}$ $\{x\to y,\overline{x}\}$, $\{x\to y,0\}$; в) $\{0,x\cdot y,x\sim y\}$, $\{0,x\vee y,x\sim y\}$, $\{1,x\cdot y,x\oplus y\}$, $\{1,x\vee y,x\oplus y\}$, $\{x\cdot y,x\to y,x\oplus y\}$, $\{x\vee y,x\to y,x\oplus y\}$. **10.1.1.** а) Да, б) да, суффиксный код; в),г) нет. **10.1.2.** б), в) да. **10.1.3.** Да во всех случаях. **10.1.5.** Да. **10.1.7.** б) Нет. **10.1.9.** а) b, ab, b^2, b^3, b^4, ab^2, ab^3, a^2b, a^3b, a^2b^2; б) ab^2, a^2b, a^2b^2, a^3b, bab^2, ba^2b, a^4b, b^2a^2b. **10.1.10.** а) b^*ab^*; б) $a(a+b)^*$. **10.1.11.** а) $\{S\to aA,\ S\to bA,\ A\to aA,\ A\to bA,\ A\to 0A,\ A\to 1A,\ A\to\lambda\}$; б) $\{S\to aA,\dots,S\to zA,\ A\to aB,\ A\to zB,\ A\to 0B,\dots,A\to 9B,\ A\to\lambda,\ B\to a,\dots,B\to z,\ B\to 0,\dots,B\to 9,\ B\to\lambda\}$; в) $\{S\to\lambda,\ S\to 0A,\ S\to 1A,\ A\to 0S,\ A\to 1S\}$. **10.1.12.** а) $\{a+b\}\{a+b+0+1\}^*$; б) $\{a+\ldots+z\}\cdot(\{a+\ldots+z+0+\ldots+1\}\cup\{\lambda\})\cdot(\{a+\ldots+z+0+\ldots+1\}\cup\{\lambda\})$; в) $(\{0+1\}\cdot\{0+1\})^*$. **10.1.15.** а) $\{wcw'\mid w\in\{a,b\}^*\}$, где w' — слово, полученное из w записыванием букв в обратном порядке; б) $\{(ab)^n\mid n\in\mathbb{N}\}$; в) $\{a^{2n-1}\mid n\in\mathbb{N}\}$; г) $\{a^{\alpha_1}b^{\alpha_1}a^{\alpha_2}b^{\alpha_2}\dots a^{\alpha_k}b^{\alpha_k}\mid k,\alpha_1,\dots,\alpha_k\in\mathbb{N}\}$. **10.2.1.** а) ab^2; б) например, a^2b^2, ab^2a, a^4b^2, aba^2b^2; в) например, a, b, ab, ba. г)



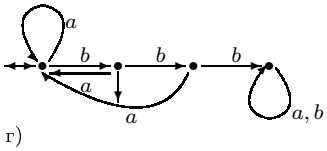
10.2.2. Например, слово ba^4 отвергается $\mathscr{A}_1$ и принимается $\mathscr{A}_2$.

10.2.3.

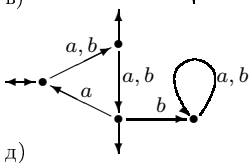




в)

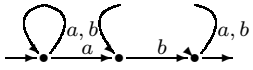


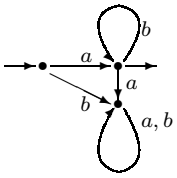
г)



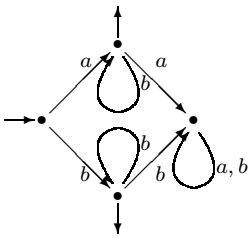
д)

10.2.4. а) $L = (a+b)^*ab(a+b)^*$, автомат

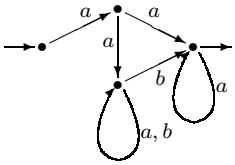




б) $L = ab^*$, автомат



в) $L = ab^* + ba^*$, автомат



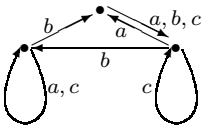
г) $L = b^*aba^*$, автомат

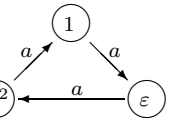
10.2.5. а) $(ab)^*$; б) $a^* + b^*$; в) $(a+b)^*ab(a+b)^*$; г) $(a+b)^*(a^2+b^2)(a+b)^*$.
10.2.6. а,б) Да, будет. **10.2.9.** б) Группа порядка 4, являющаяся прямым произведением двух циклических групп порядка 2.
10.2.10. а) Моноид состоит из 8 частичных преобразований на множестве $\{0,1,2\}$: тождественного и $a = \begin{pmatrix} 0 & 2 \\ 0 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix}$, $ab = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$, $ba = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$, $b^2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 2 & 2 \end{pmatrix}$, $aba = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$, $ab^2 = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}$; б) моноид состоит из 11 частичных преобразований на множестве $\{0,1,2,3\}$: тождественного и $a = \begin{pmatrix} 0 & 3 \\ 0 & 3 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 3 \end{pmatrix}$, $ab = \begin{pmatrix} 1 & 3 \\ 1 & 3 \end{pmatrix}$, $ba = \begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix}$, $b^2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 3 & 3 \end{pmatrix}$, $aba = \begin{pmatrix} 3 \\ 3 \end{pmatrix}$, $ab^2 = \begin{pmatrix} 0 & 3 \\ 2 & 3 \end{pmatrix}$, $b^2a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}$,

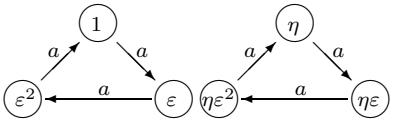
$b^3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 3 & 3 & 3 \end{pmatrix}$, $ab^3 = \begin{pmatrix} 0 & 3 \\ 0 & 3 \end{pmatrix}$; в) $3m + 5$ элементов.

10.2.11. Моноид состоит из 26 частичных преобразований на множестве $\{0, 1, 2, 3\}$. Кроме тождественного и пустого преобразования, он содержит все преобразования с одноэлементным образом (таковых 16), а также следующие 8 преобразований: $a = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 2 & 3 \\ 1 & 3 & 1 \end{pmatrix}$, $a = \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix}$, $ba = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}$, $b^2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 3 & 3 \end{pmatrix}$, $bab = \begin{pmatrix} 0 & 3 \\ 3 & 1 \end{pmatrix}$, $b^2a = \begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix}$, $b^2ab = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$.

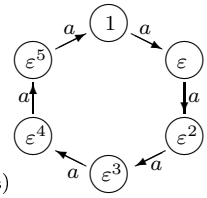
10.2.12. Например,

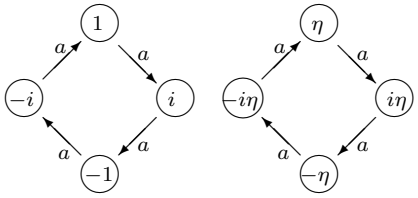


10.2.14. а) 

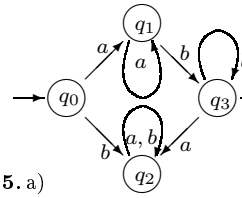
б) 

где $\eta = \frac{\sqrt{3}}{2} + \frac{i}{2}$;

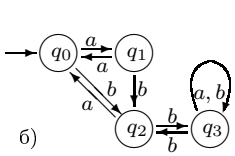
в) 

г) 

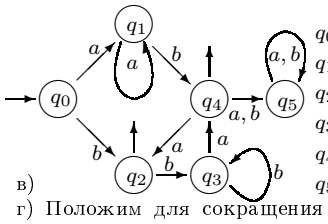
где $\eta = \frac{1+i}{\sqrt{2}}$.

10.2.15. а) 

$q_0 = L$,
$q_1 = a^*b^*$,
$q_2 = \emptyset$,
$q_3 = b^*$;

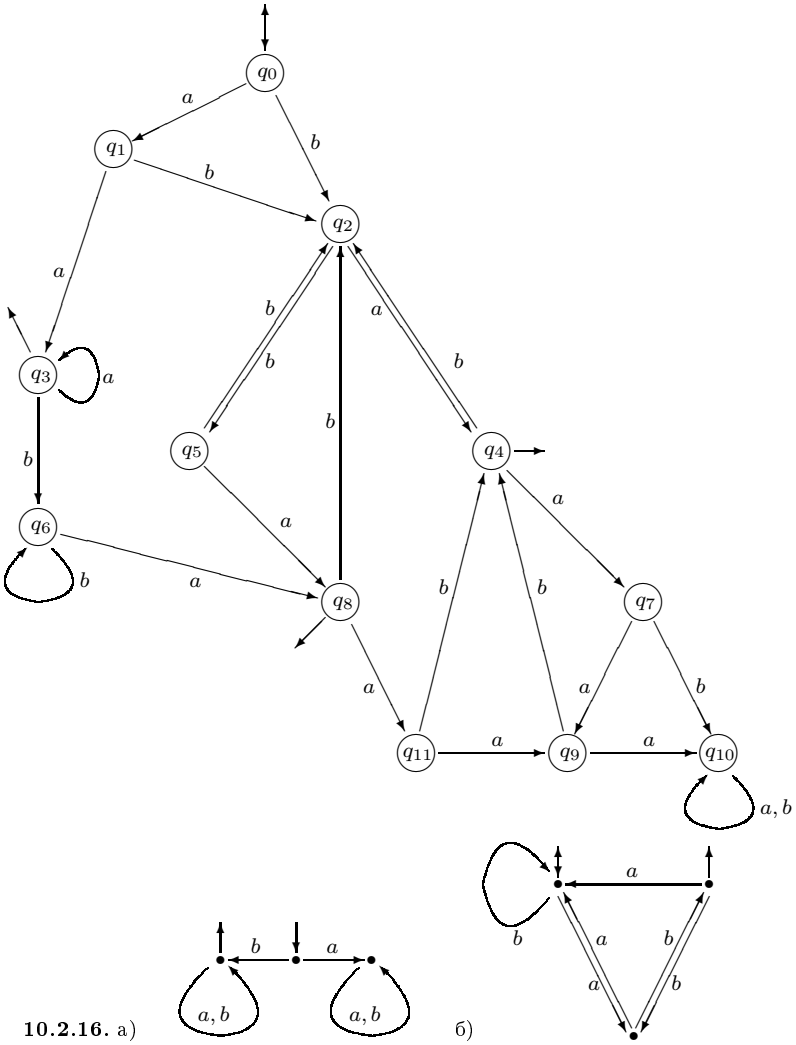
б) 

$q_0 = L$,
$q_1 = (a + ba)L$,
$q_2 = aL$,
$q_3 = \emptyset$;

в) 

$q_0 = L$,
$q_1 = a^*b$,
$q_2 = a^*b + \lambda$,
$q_3 = b^*a$;
$q_4 = \lambda$;
$q_5 = \emptyset$;

г) Положим для сокращения записей $L_1 = (a^2b + bb^*a + b^2)^*$. Пусть $q_0 = L$, $q_1 = (a^* + ab)L_1$, $q_2 = (b^*a + b)L_1$, $q_3 = (a^* + b + ab)L_1$, $q_4 = L_1$, $q_5 = (b^*a + \lambda)L_1$, $q_6 = (b^*a + b + \lambda)L_1$, $q_7 = abL_1$, $q_8 = (ab + \lambda)L_1$, $q_9 = bL_1$, $q_{10} = \emptyset$, $q_{11} = (ab + b)L_1$. Тогда граф автомата выглядит следующим образом:



10.2.16. а) б)

Предметный указатель

Учебное издание

Сборник задач по общей алгебре и дискретной математике

под редакцией Л. Н. Шеврина

Составители:
Баранский Виталий Анатольевич
Важенин Юрий Михайлович
Волков Михаил Владимирович
Гейн Александр Георгиевич
Замятин Алексей Петрович
Овсянников Александр Яковлевич
Петров Алексей Николаевич
Сесекин Николай Федорович
Шеврин Лев Наумович

Учебное пособие

Ответственные за выпуск
А. Г. Гейн, А. Я. Овсянников
Редактор и корректор
М. А. Овечкина
Оригинал-макет
А. Я. Овсянников

Лицензия ИД № 05974 от 03.10.2001.
Темплан 2003 г., поз. 11.
Подписано в печать 22.12.2003.
Гарнитура NT-Times. Формат 60×84 1/16. Бумага офсетная.
Усл.-печ. л. 8,1. Уч. изд. л. 7,2. Тираж 500 экз. Заказ .

Издательство Уральского университета.
620219 Екатеринбург, ГСП-830, пр. Ленина 13-б.

Отпечатано в Тип. Упр. изд., полиграфии и кн. торговли.
В. Пышма, Кривоусова, 11.