УДК 512 (075.8)
ББК 22.143
З 15

Авторский коллектив:

В. А. Артамонов, Ю. А. Бахтурин, Э. Б. Винберг, Е. С. Голод, В. А. Исковских, А. И. Кострикин, В. Н. Латышев, А. В. Михалев, А. П. Мишина, А. Ю. Ольшанский, А. А. Панчишкин, И. В. Проскуряков, А. Н. Рудаков, Л. А. Скорняков, А. Л. Шмелькин

Сборник задач по алгебре / Под ред. А.И. Кострикина: Учеб. пособ.: Для вузов. В 2 т. Т. 2. / Ч. III. Основные алгебраические структуры. — М.: ФИЗМАТЛИТ, 2007. — 168 с. — ISBN 978-5-9221-0726-6.

Задачник составлен применительно к учебнику А.И. Кострикина «Введение в алгебру» (Т. 1. «Основы алгебры». Т. 2. «Линейная алгебра». Т. 3. «Основные структуры алгебры»).

Цель книги — обеспечить семинарские занятия сразу по двум обязательным курсам: «Высшая алгебра» и «Линейная алгебра и геометрия», а также предоставить студентам материал для самостоятельной работы.

Настоящее издание выходит в 2-х томах. В 1 том вошли «Основы алгебры» и «Линейная алгебра и геометрия». Второй том составляет часть III «Основные алгебраические структуры».

Для студентов первых двух курсов математических факультетов университетов и педагогических институтов.

Библиогр. 20 назв.

Учебное издание

СБОРНИК ЗАДАЧ ПО АЛГЕБРЕ

Том 2

Редактор *И.Л. Легостаева*
Оригинал-макет: *И.В. Шутов*
Оформление переплета: *А.Ю. Алехина*

Подписано в печать 30.05.06. Формат 60×90/16. Бумага офсетная. Печать офсетная. Усл. печ. л. 10,5. Уч.-изд. л. 12,5. Тираж 2000 экз. Заказ №

Издательская фирма «Физико-математическая литература»
МАИК «Наука/Интерпериодика»
117997, Москва, ул. Профсоюзная, 90
E-mail: fizmat@maik.ru, fmlsale@maik.ru;
http://www.fml.ru

Отпечатано с готовых диапозитивов
в ОАО «Ивановская областная типография»
153008, г. Иваново, ул. Типографская, 6
E-mail: 091-018@adminet.ivanovo.ru

ISBN 978-5-9221-0726-6

9 785922 107266

ISBN 978-5-9221-0726-6

ОГЛАВЛЕНИЕ

III. Основные алгебраические структуры

Часть III

ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Глава 13

ГРУППЫ

§ 54. Алгебраические операции. Полугруппы

54.1. Ассоциативна ли операция $*$ на множестве M, если

а) $M = \mathbb{N}$, $x * y = x^y$; б) $M = \mathbb{N}$, $x * y = \text{НОД}\,(x, y)$;
в) $M = \mathbb{N}$, $x * y = 2xy$; г) $M = \mathbb{Z}$, $x * y = x - y$;
д) $M = \mathbb{Z}$, $x * y = x^2 + y^2$; е) $M = \mathbb{R}$, $x * y = \sin x \cdot \sin y$;
ж) $M = \mathbb{R}^*$, $x * y = x \cdot y^{x/|x|}$?

54.2. Пусть S — полугруппа матриц $\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)$, где $x, y \in \mathbb{R}$, с операцией умножения. Найти в этой полугруппе левые и правые нейтральные элементы, а также элементы, обратимые слева или справа относительно этих нейтральных.

54.3. На множестве M определена операция $\circ$ по правилу $x \circ y = x$. Доказать, что $(M, \circ)$ — полугруппа. Что можно сказать о нейтральных и обратимых элементах этой полугруппы? В каких случаях она является группой?

54.4. На множестве M^2, где M — некоторое множество, определена операция $\circ$ по правилу $(x, y) \circ (z, t) = (x, t)$. Является ли M^2 полугруппой относительно этой операции? Существует ли в M^2 нейтральный элемент?

54.5. Сколько элементов содержит полугруппа, состоящая из всех степеней матрицы

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}?$$

Является ли эта полугруппа группой?

54.6. Доказать, что полугруппы $(2^M, \cup)$ и $(2^M, \cap)$ изоморфны.

54.7. Сколько существует неизоморфных между собой полугрупп порядка 2?

54.8. Доказать, что во всякой конечной полугруппе найдется идемпотент.

54.9. Полугруппа называется *моногенной*, если она состоит из положительных степеней одного из своих элементов (такой элемент является *порождающим*).

Доказать, что:

а) моногенная полугруппа конечна тогда и только тогда, когда содержит идемпотент;

б) конечная моногенная полугруппа либо является группой, либо имеет только один порождающий элемент;

в) любые две бесконечные моногенные полугруппы изоморфны;

г) всякая конечная моногенная полугруппа изоморфна полугруппе вида $S(n,k)$, определенной на множестве $\{a_1,\ldots,a_n\}$ следующим образом:

$$a_i + a_j = \begin{cases} a_{i+j}, & \text{если} \quad i+j \leqslant n, \\ a_{k+l+1}, & \text{если} \quad i+j > n, \end{cases}$$

где l — остаток от деления числа $i+j-n-1$ на $n-k$.

§ 55. Понятие группы. Изоморфизм групп

55.1. Какие из указанных числовых множеств с операциями являются группами:

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

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

в) $(A_0,\cdot)$, где A — одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, а $A_0 = A\setminus\{0\}$;

г) $(n\mathbb{Z},+)$, где n — натуральное число;

д) $(\{-1,1\},\cdot)$;

е) множество степеней данного вещественного числа $a\neq 0$ с целыми показателями относительно умножения;

ж) множество всех комплексных корней фиксированной степени n из 1 относительно умножения;

з) множество комплексных корней всех степеней из 1 относительно умножения;

и) множество комплексных чисел с фиксированным модулем r относительно умножения;

к) множество ненулевых комплексных чисел с модулем, не превосходящим фиксированное число r, относительно умножения;

л) множество ненулевых комплексных чисел, расположенных на лучах, выходящих из начала координат и образующих с лучом Ox углы φ_1, $\varphi_2,\ldots,\varphi_n$, относительно умножения;

м) множество всех непрерывных отображений $\varphi : [0,1] \to [0,1]$, для которых $\varphi(0)=0, \varphi(1)=1$, и $x<y \Rightarrow \varphi(x)<\varphi(y)$, относительно суперпозиции?

55.2. Доказать, что полуинтервал $[0,1)$ с операцией $\oplus$, где $\alpha \oplus \beta$ — дробная часть числа $\alpha+\beta$, является группой. Какой из групп из задачи 55.1 изоморфна эта группа? Доказать, что всякая ее конечная подгруппа является циклической.

55.3. Доказать, что множество 2^M всех подмножеств в непустом множестве M является группой относительно операции симметрической разности

$$A\Delta B = [A \cap (M \setminus B)] \cup [B \cap (M \setminus A)].$$

55.4. Пусть G — группа относительно умножения. Зафиксируем в G элемент a и зададим в G операцию $x \circ y = x \cdot a \cdot y$. Доказать, что G относительно новой операции $\circ$ является группой, изоморфной $(G, \cdot)$.

55.5. Какие из указанных ниже совокупностей отображений множества $M=\{1,2,\ldots,n\}$ в себя образуют группу относительно умножения:

а) множество всех отображений;
б) множество всех инъективных отображений;
в) множество всех сюръективных отображений;
г) множество всех биективных отображений;
д) множество всех четных перестановок;
е) множество всех нечетных перестановок;
ж) множество всех транспозиций;
з) множество всех перестановок, оставляющих неподвижными элементы некоторого подмножества $S \subseteq M$;
и) множество всех перестановок, при которых образы всех элементов некоторого подмножества $S \subseteq M$ принадлежат этому подмножеству;
к) множество $\{E, (12)(34), (13)(24), (14)(23)\}$;
л) множество

$$\{E, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}?$$

55.6. Какие из указанных множеств квадратных вещественных матриц фиксированного порядка образуют группу:

а) множество симметрических (кососимметрических) матриц относительно сложения;
б) множество симметрических (кососимметрических) матриц относительно умножения;
в) множество невырожденных матриц относительно сложения;
г) множество невырожденных матриц относительно умножения;

д) множество матриц с фиксированным определителем d относительно умножения;

е) множество диагональных матриц относительно сложения;

ж) множество диагональных матриц относительно умножения;

з) множество диагональных матриц, все элементы диагоналей которых отличны от 0, относительно умножения;

и) множество верхних треугольных матриц относительно умножения;

к) множество верхних нильтреугольных матриц относительно умножения;

л) множество верхних нильтреугольных матриц относительно сложения;

м) множество верхних унитреугольных матриц относительно умножения;

н) множество всех ортогональных матриц относительно умножения;

о) множество матриц вида $f(A)$, где A — фиксированная нильпотентная матрица, $f(t)$ — произвольный многочлен со свободным членом, отличным от 0, относительно умножения;

п) множество верхних нильтреугольных матриц относительно операции $X \circ Y = X + Y - XY$;

р) множество ненулевых матриц вида $\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$ $(x, y \in \mathbb{R})$ относительно умножения;

с) множество ненулевых матриц вида $\left(\begin{smallmatrix} x & y \\ \lambda y & x \end{smallmatrix}\right)$ $(x, y \in \mathbb{R})$, где λ — фиксированное вещественное число, относительно умножения;

т) множество матриц

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

относительно умножения?

55.7. Показать, что множество $\mathbf{O}_n(\mathbb{Z})$ всех целочисленных ортогональных матриц размера n образует группу относительно умножения. Найти порядок этой группы.

55.8. Доказать, что множество верхних нильтреугольных матриц порядка 3 является группой относительно операции

$$X \circ Y = X + Y + \frac{1}{2}[X, Y].$$

55.9. Пусть X — множество точек кривой $y = x^3$, l — прямая, проходящая через точки $a, b \in X$ (касательная к X при $a = b$), c — ее третья точка пересечения с X и m — прямая, проходящая через начало координат O и точку c (касательная к X при $c = 0$).

Положим $a \oplus b = d$, где d — третья точка пересечения m и X или O, если m касается X в точке O. Доказать, что $(X, \oplus)$ — коммутативная группа.

55.10. Доказать, что множество функций вида

$$y = \frac{ax+b}{cx+d},$$

где a, b, c, $d \in \mathbb{R}$ и $ad - bc \neq 0$, является группой относительно операции композиции функций.

55.11. Доказать, что коммутатор

$$[x, y] = xyx^{-1}y^{-1}$$

элементов x, y группы G обладает свойствами:
а) $[x, y]^{-1} = [y, x]$;
б) $[xy, z] = x[y, z]x^{-1}[x, z]$;
в) $[z, xy] = [z, x]x[z, y]x^{-1}$.

55.12. Пусть задано разложение подстановки σ в произведение независимых циклов

$$\sigma = (i_1, \ldots, i_k)(j_1, \ldots, j_m)\ldots.$$

Найти разложение подстановки σ^{-1} в произведение независимых циклов.

55.13. Какие из следующих равенств тождественно выполняются в группе $\mathbf{S}_3$:
а) $x^6 = 1$;
б) $[[x, y], z] = 1$;
в) $[x^2, y^2] = 1$?

55.14. Доказать, что в группе верхних унитреугольных матриц порядка 3 выполняется тождество

$$(xy)^n = x^n y^n [x, y]^{-n(n-1)/2}, \qquad n \in \mathbb{N}.$$

55.15. Доказать, что если в группе G выполняется тождество $[[x, y], z] = 1$, то в G выполняются тождества

$$[x, yz] = [x, y][x, z], \qquad [xy, z] = [x, z][y, z].$$

55.16. Доказать, что если в группе G выполняется тождество $x^2 = 1$, то G коммутативна.

55.17. Какие из отображений групп $f : \mathbb{C}^* \mapsto \mathbb{R}^*$ являются гомоморфизмами:

а) $f(z) = |z|$; б) $f(z) = 2|z|$; в) $f(z) = \dfrac{1}{|z|}$;

г) $f(z) = 1 + |z|$; д) $f(z) = |z|^2$; е) $f(z) = 1$;

ж) $f(z) = 2$?

55.18. Для каких групп G отображение $f : G \mapsto G$, определенное правилом:
а) $f(x) = x^2$, б) $f(x) = x^{-1}$,
является гомоморфизмом?

При каком условии эти отображения являются изоморфизмами?

55.19. Сопоставим каждой матрице $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{GL}(2, \mathbb{C})$ функцию $y = \dfrac{ax+b}{cx+d}$ (см. задачу 55.10). Будет ли это отображение гомоморфизмом?

55.20. Разбить на классы попарно изоморфных групп следующий набор групп:

$$\mathbb{Z}, \quad n\mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{Q}^*, \quad \mathbb{R}^*, \quad \mathbb{C}^*, \quad \mathbf{UT}_2(A),$$

где A — одно из колец $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

55.21. Найти все изоморфизмы между группами $(\mathbf{Z}_4, +)$ и $(\mathbf{Z}_5^*, \cdot)$.

55.22. Доказать, что группа порядка 6 либо коммутативна, либо изоморфна группе $\mathbf{S}_3$.

55.23. Доказать, что если рациональное число a не равно нулю, то отображение $\varphi : x \mapsto ax$ является автоморфизмом группы $\mathbb{Q}$. Найти все автоморфизмы группы $\mathbb{Q}$.

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

55.25. Привести примеры плоских геометрических фигур, группы движения которых изоморфны:
а) $\mathbf{Z}_2$; б) $\mathbf{Z}_3$; в) $\mathbf{S}_3$; г) $\mathbf{V}_4$.

55.26. Какие из следующих групп изоморфны между собой:
группа $\mathbf{D}_4$ движений квадрата;
группа кватернионов $\mathbf{Q}_8$;
группа из задачи 55.5, л);
группа из задачи 55.6, т)?

55.27. Доказать, что группы собственных движений тетраэдра, куба и октаэдра изоморфны соответственно группам $\mathbf{A}_4$, $\mathbf{S}_4$, $\mathbf{S}_4$.

55.28. Доказать, что группы $\mathbf{U}$ и $\mathbf{SO}_2(\mathbb{R})$ изоморфны.

55.29. Пусть G — множество всех пар элементов (a, b), $a \neq 0$, из поля k относительно операции $(a, c) \circ (c, d) = (ac, ad + b)$. Доказать, что G является группой, изоморфной группе всех линейных функций $x \mapsto ax + b$ относительно суперпозиции.

55.30. Пусть G — множество всех вещественных чисел, отличных от -1. Доказать, что G является группой относительно умножения

$$x \cdot y = x + y + xy.$$

55.31. Доказать, что:

а) множество всех автоморфизмов произвольной группы является группой относительно композиции;

б) отображение
$$\sigma : x \mapsto axa^{-1},$$
где a — фиксированный элемент группы G, является автоморфизмом группы G (внутренним автоморфизмом);

в) множество всех внутренних автоморфизмов произвольной группы является группой относительно композиции.

55.32. Найти группы автоморфизмов групп:

а) $\mathbb{Z}$; б) $\mathbf{Z}_p$; в) $\mathbf{S}_3$;
г) $\mathbf{V}_4$; д) $\mathbf{D}_4$; е) $\mathbf{Q}_8$.

55.33. Доказать, что отображение $a \mapsto \sigma$, сопоставляющее каждому элементу a группы G перестановку $\sigma : x \mapsto ax$ множества G, является инъективным гомоморфизмом группы G в группу S_G.

55.34. Найти в соответствующих группах $\mathbf{S}_n$ подгруппы, изоморфные группам:

а) $\mathbf{Z}_3$; б) $\mathbf{D}_4$; в) $\mathbf{Q}_8$.

55.35. Пусть σ — перестановка степени n и $A_\sigma = (\delta_{i\sigma(j)})$ — квадратная матрица порядка n. Доказать, что если G — некоторая группа перестановок степени n, то множество матриц A_σ, где $\sigma \in G$, образует группу, изоморфную группе G.

55.36. Найти в соответствующих группах матриц $\mathbf{GL}_n(\mathbb{C})$ подгруппы, изоморфные группам:

а) $\mathbf{Z}_3$; б) $\mathbf{D}_4$; в) $\mathbf{Q}_8$.

55.37. Найти в группе вещественных матриц порядка 4 подгруппу, изоморфную группе $\mathbf{Q}_8$.

55.38. Доказать, что группу $\mathbf{U}_{p^\infty}$ нельзя отобразить гомоморфно на конечную группу, отличную от единичной.

55.39. Будут ли изоморфны группы
а) $\mathbf{SL}_2(3)$; б) $\mathbf{S}_4$; в) $\mathbf{A}_5$?

§ 56. Подгруппы, порядок элемента группы. Смежные классы

56.1. Доказать, что во всякой группе:
а) пересечение любого набора подгрупп является подгруппой;
б) объединение двух подгрупп является подгруппой тогда и только тогда, когда одна из подгрупп содержится в другой;
в) если подгруппа C содержится в объединении подгрупп A и B, то либо $C \subseteq A$, либо $C \subseteq B$.

56.2. Доказать, что конечная подполугруппа любой группы является подгруппой. Верно ли это утверждение, если подполугруппа бесконечна?

56.3. Найти порядок элемента группы:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in \mathbf{S}_5$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} \in \mathbf{S}_6$;

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

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

и) $\begin{pmatrix} \lambda_1 & * & \ldots & * \\ 0 & \lambda_2 & * & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \lambda_n \end{pmatrix} \in \mathbf{GL}_n(\mathbb{C})$,

где $\lambda_1, \ldots, \lambda_n$ — различные корни k-й степени из 1.

56.4. Пусть p — простое нечетное число, X — целочисленная квадратная матрица размера n, причем матрица $E + pX$ лежит в $\mathbf{SL}_n(\mathbb{Z})$ и имеет конечный порядок. Доказать, что $X = 0$.

56.5. Доказать, что:

а) элемент $\dfrac{3}{5} + \dfrac{4}{5}i$ группы $\mathbb{C}^*$ имеет бесконечный порядок;

б) число $\dfrac{1}{\pi}\operatorname{arctg}\dfrac{4}{3}$ иррационально.

56.6. Сколько элементов порядка 6 содержится в группе:
а) $\mathbb{C}^*$; б) $\mathbf{D}_2(\mathbb{C})$; в) $\mathbf{S}_5$; г) $\mathbf{A}_5$?

56.7. Доказать, что во всякой группе:
а) элементы x и yxy^{-1} имеют одинаковый порядок;
б) элементы ab и ba имеют одинаковый порядок;
в) элементы xyz и zyx могут иметь разные порядки.

56.8. Пусть элементы x и y группы G имеют конечный порядок и $xy = yx$.

а) Доказать, что если порядки элементов x и y взаимно просты, то порядок произведения xy равен произведению их порядков.

б) Доказать, что существуют показатели k и l такие, что порядок произведения $x^k y^l$ равен наименьшему общему кратному порядков x и y.

в) Верны ли эти утверждения для некоммутирующих элементов x и y?

56.9. Доказать, что:

а) если элемент x группы G имеет бесконечный порядок, то $x^k = x^l$ тогда и только тогда, когда $k = l$;

б) если элемент x группы G имеет порядок n, то $x^k = x^l$ тогда и только тогда, когда $n|(k-l)$;

в) если элемент x группы G имеет порядок n, то $x^k = e$ тогда и только тогда, когда $n|k$.

56.10. Доказать, что в группе $\mathbf{S}_n$:
а) порядок нечетной перестановки является четным числом;
б) порядок любой перестановки является наименьшим общим кратным длин независимых циклов, входящих в ее разложение.

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

56.12. Пусть G — конечная группа, $a \in G$. Доказать, что $G = \langle a \rangle$ тогда и только тогда, когда порядок a равен $|G|$.

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

56.14. 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 НОД $(k, n) =$ НОД (l, n);

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

в) всякая подгруппа $H \subseteq G$ порождается элементом вида a^d, где $d|n$;

г) для всякого делителя d числа n существует единственная подгруппа $H \subseteq G$ порядка d.

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

а) $n = 24$, $k = 6$; б) $n = 24$, $k = 4$;
в) $n = 100$, $k = 20$; г) $n = 100$, $k = 5$;
д) $n = 360$, $k = 30$; е) $n = 360$, $k = 12$;
ж) $n = 360$, $k = 7$.

56.16. Найти все подгруппы в циклической группе порядка:

а) 24; б) 100; в) 360; г) 125;
д) p^n (p — простое число)

56.17. Предположим, что в некоторой неединичной группе все неединичные элементы имеют одинаковый порядок p. Доказать, что p является простым числом.

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

Доказать, что:

а) период $d(G)$ делит $|G|$ и равен наименьшему общему кратному порядков элементов группы G;

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

в) конечная коммутативная группа является циклической тогда и только тогда, когда $d(G) = |G|$.

Верны ли утверждения б) и в) для некоммутативной группы?

56.19. Существует ли бесконечная группа, все элементы которой имеют конечный порядок?

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

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

б) Верно ли утверждение а) для некоммутативной группы?

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

г) Доказать, что если в коммутативной группе G есть элементы бесконечного порядка и все они содержатся в подгруппе H, то H совпадает с G.

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

56.22. Найти все конечные группы, в которых существует наибольшая собственная подгруппа.

56.23. Является ли циклической группа $(\mathbb{Z}/15\mathbb{Z})^*$ обратимых элементов кольца $\mathbb{Z}/15\mathbb{Z}$?

56.24. Множество всех подгрупп группы G *образует цепь*, если для любых двух ее подгрупп одна содержится в другой.

а) Доказать, что подгруппы циклической группы порядка p^n, где p — простое число, образуют цепь.

б) Найти все конечные группы, в которых подгруппы образуют цепь.

в) Найти все группы, у которых подгруппы образуют цепь.

56.25. Представить группу $\mathbb{Q}$ в виде объединения возрастающей цепочки циклических подгрупп.

56.26. Установить изоморфизм между группами $\mathbf{U}_n$ комплексных корней степени n из 1 и группой $\mathbf{Z}_n$ вычетов по модулю n.

56.27. Какие из групп $\langle g\rangle$, порожденных элементом $g \in G$, изоморфны:

а) $G = \mathbb{C}^*, \quad g = -\dfrac{1}{\sqrt{2}} + \dfrac{1}{\sqrt{2}}i;$

б) $G = \mathbf{GL}_2(\mathbb{C}), \quad g = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix};$

в) $G = \mathbf{S}_6, \quad g = (3\,2\,6\,5\,1);$

г) $G = \mathbb{C}^*, \quad g = 2 - i;$

д) $G = \mathbb{R}^*, \quad g = 10;$

е) $G = \mathbb{C}^*, \quad g = \cos\dfrac{6\pi}{5} + i\sin\dfrac{6\pi}{5};$

ж) $G = \mathbb{Z}, \quad g = 3$?

56.28. Доказать, что во всякой группе четного порядка имеется элемент порядка 2.

56.29. Будет ли группа обратимых элементов кольца вычетов $\mathbf{Z}_{16}$ циклической?

56.30. Доказать, что всякая собственная подгруппа группы $\mathbf{U}_{p^\infty}$ является циклической конечного порядка.

56.31. Доказать, что:

а) в мультипликативной группе поля для любого натурального числа n существует не более одной подгруппы порядка n;

б) всякая конечная подгруппа мультипликативной группы поля является циклической;

в) мультипликативная группа конечного поля является циклической.

56.32. Найти все подгруппы в группах:

а) $\mathbf{S}_3$; б) $\mathbf{D}_4$; в) $\mathbf{Q}_8$; г) $\mathbf{A}_4$.

56.33. Доказать, что каждая конечная подгруппа в $\mathbf{SO}_2(\mathbb{R})$ является циклической.

56.34. Доказать, что если подгруппа H группы $\mathbf{S}_n$ содержит одно из множеств

$$\{(1\,2), (1\,3), \ldots, (1\,n)\} \quad \{(1\,2), (1\,2\,3\ldots n)\},$$

то $H = \mathbf{S}_n$.

56.35. Найти все элементы группы G, коммутирующие с данным элементом $g \in G$ (централизатор элемента g), если:

а) $G = \mathbf{S}_4, \quad g = (1\,2)(3\,4)$;

б) $G = \mathbf{SL}_2(\mathbb{R}), \quad g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$;

в) $G = \mathbf{S}_n, \quad g = (1\,2\,3\,\ldots\,n)$.

56.36. Для многочлена f от переменных x_1, x_2, x_3, x_4 положим

$$G_f = \{\sigma \in \mathbf{S}_4 \mid f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}) = f(x_1, x_2, x_3, x_4)\}.$$

Доказать, что G_f — подгруппа в $\mathbf{S}_4$, и найти эту подгруппу для многочлена:

а) $f = x_1x_2 + x_3x_4$; б) $f = x_1x_2x_3$;

в) $f = x_1 + x_2$; г) $f = x_1x_2x_3x_4$;

д) $f = \prod\limits_{1 \leqslant j < i \leqslant 4} (x_i - x_j)$.

56.37. Найти смежные классы:

а) аддитивной группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$, n — натуральное число;

б) аддитивной группы $\mathbb{C}$ по подгруппе $\mathbb{Z}[i]$ целых гауссовых чисел, т. е. чисел $a + bi$ с целыми a, b;

в) аддитивной группы $\mathbb{R}$ по подгруппе $\mathbb{Z}$;

г) аддитивной группы $\mathbb{C}$ по подгруппе $\mathbb{R}$;

д) мультипликативной группы $\mathbb{C}^*$ по подгруппе $\mathbf{U}$ чисел с модулем 1;

е) мультипликативной группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}^*$;

ж) мультипликативной группы $\mathbb{C}^*$ по подгруппе положительных вещественных чисел;

з) группы подстановок $\mathbf{S}_n$ по стационарной подгруппе элемента n;

и) аддитивной группы вещественных (3×2)-матриц по подгруппе всех матриц (a_{ij}) с условием $a_{31} = a_{32} = a_{22} = 0$;

к) аддитивной группы всех многочленов степени не выше 5 с комплексными коэффициентами по подгруппе многочленов степени не выше 3;

л) циклической группы $\langle a \rangle_6$ по подгруппе $\langle a^4 \rangle$.

56.38. Пусть g — невырожденная матрица из $\mathbf{GL}_n(\mathbb{C})$ и $H = \mathbf{SL}_n(\mathbb{C})$. Доказать, что смежный класс gH состоит из всех матриц $a \in \mathbf{GL}_n(\mathbb{C})$, определитель которых равен определителю матрицы g.

56.39. Пусть H — подгруппа в группе G. Доказать, что отображение $xH \mapsto Hx^{-1}$ задает биекцию между множеством левых и множеством правых смежных классов G по H.

56.40. Пусть g_1, g_2 — элементы группы G и H_1, H_2 — подгруппы в G. Доказать, что следующие свойства эквивалентны:

а) $g_1H_1 \subseteq g_2H_2$; б) $H_1 \subseteq H_2$ и $g_2^{-1}g_1 \in H_2$.

56.41. Пусть g_1, g_2 — элементы группы G и H_1, H_2 — подгруппы в G. Доказать, что непустое множество $g_1H_1 \cap g_2H_2$ является левым смежным классом G по подгруппе $H_1 \cap H_2$.

56.42. Пусть K — правый смежный класс группы G по подгруппе H. Доказать, что если $x, y, z \in K$, то $xy^{-1}z \in K$.

56.43. Пусть K — непустое подмножество в группе G, причем если $x, y, z \in K$, то $xy^{-1}z \in K$. Доказать, что K является правым смежным классом группы G по некоторой подгруппе H.

56.44. Пусть H_1, H_2 — подгруппы в группе G, причем $H_1 \subseteq H_2$. Если индекс H_1 в H_2 равен n, а индекс H_2 в G равен m, то индекс H_1 в G равен mn.

56.45. Доказать, что в группе диэдра все осевые симметрии образуют смежный класс по подгруппе вращений.

§ 57. Действие группы на множестве. Отношение сопряженности

57.1. Найти все орбиты группы G невырожденных линейных операторов, действующих на n-мерном пространстве V, если:

а) G — группа всех невырожденных линейных операторов;

б) G — группа ортогональных операторов;

в) G — группа операторов, матрицы которых в базисе $(e_1, \ldots, e_n)$ диагональны;

г) G — группа операторов, матрицы которых в базисе $(e_1, \ldots, e_n)$ верхние треугольные.

57.2. Найти стационарную подгруппу G_a вектора $a = e_1 + e_2 + \ldots + e_n$, если:

а) G — группа из 57.1, в); б) G — группа из 57.1, г).

57.3. Найти стационарную подгруппу G_x и орбиту вектора x, если:

а) G — группа всех ортогональных операторов в трехмерном евклидовом пространстве;

б) G — группа всех собственных ортогональных операторов в двумерном евклидовом пространстве.

57.4. Пусть G — группа всех невырожденных линейных операторов в n-мерном векторном пространстве V и X — множество всех подпространств размерности k в X.

а) Найти орбиты группы G в X.

б) Пусть $e_1, \ldots, e_n$ — такой базис в V, что $e_1, \ldots, e_k$ — базис некоторого подпространства U. Найти в базисе $e_1, \ldots, e_n$ матрицы операторов из стационарной подгруппы G_U.

57.5. Пусть G — группа всех невырожденных линейных операторов в n-мерном векторном пространстве V и F — множество флагов в V, т. е. наборов $f = (V_0, V_1, \ldots, V_n)$ подпространств в V, причем $0 = V_0 < V_1 < \ldots < V_n = V$.

а) Найти орбиты G в F.

б) Пусть $e_i \in V_i \setminus V_{i-1}$, $i = 1, \ldots, n$. Доказать, что $e_1, \ldots, e_n$ — базис V.

в) В базисе $e_1, \ldots, e_n$ найти матрицы операторов из стационарной подгруппы G_f.

57.6. Пусть G — группа всех невырожденных линейных операторов в n-мерном векторном пространстве V и X (соответственно Y) — множество всех ненулевых разложимых q-векторов из $\Lambda^q V$ (из $S^q(V)$).

а) Найти орбиты действия G в X и Y.

б) Найти стационарную подгруппу G_a разложимого q-вектора a (вектора из $S^q(V)$).

57.7. Пусть G — группа всех невырожденных линейных операторов в n-мерном вещественном (комплексном) пространстве V и B — множество всех симметричных (эрмитовых) билинейных функций в V. Если $g \in G$ и $b \in B$, то положим $g(b)(x, y) = b(g^{-1}x, g^{-1}y)$.

а) Доказать, что задано действие G в B.

б) Описать орбиты G в B. Найти их число.

в) Описать стационарную подгруппу G_b положительно определенной функции b.

57.8. Пусть G — группа всех невырожденных линейных операторов в n-мерном комплексном пространстве V и $L(V)$ — множество всех линейных операторов в V. Если $g \in G$ и $f \in L(V)$, то положим $g(f) = gfg^{-1}$.

а) Доказать, что задано действие G в $L(V)$.

б) Описать орбиты G в $L(V)$.

57.9. Найти во множестве $\{1, 2, \ldots, 10\}$ все орбиты и все стационарные подгруппы для группы G, порожденной подстановкой:

а) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 9 & 4 & 10 & 6 & 2 & 1 & 7 \end{pmatrix} \in \mathbf{S}_{10}$;

б) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 4 & 6 & 1 & 8 & 3 & 2 & 9 & 5 & 10 \end{pmatrix} \in \mathbf{S}_{10}$;

в) $g = (1\,6\,9)(2\,10)(3\,4\,5\,7\,8) \in \mathbf{S}_{10}$.

57.10. В прямоугольной системе координат задан ромб с вершинами

$$A = (0, 1), \quad B = (2, 0), \quad C = (0, -1), \quad D = (-2, 0).$$

а) Найти матрицы ортогональных преобразований плоскости, переводящих ромб в себя.

б) Доказать, что эти матрицы образуют относительно умножения группу G, изоморфную группе $\mathbf{V}_4$.

в) Найти орбиты действия группы G на множестве вершин ромба и их стационарные подгруппы.

57.11. Найти порядок группы диэдра $\mathbf{D}_n$.

57.12. Найти порядок:

а) группы вращений куба;

б) группы вращений тетраэдра;

в) группы вращений додекаэдра.

57.13. Доказать, что:

а) группа вращений икосаэдра изоморфна группе $\mathbf{A}_5$;

б) группа движений тетраэдра изоморфна $\mathbf{S}_4$.

57.14. Найти порядок стационарной подгруппы вершины для группы вращений:

а) октаэдра; б) икосаэдра; в) тетраэдра;

г) куба; д) диэдра.

57.15. Пусть G — группа аффинных преобразований в n-мерном аффинном пространстве X. Предположим, что Y — множество всех наборов из $n+1$ точки $(A_0, \ldots, A_n)$, находящихся в общем положении.

а) Найти орбиты G в Y.

б) Найти стационарную подгруппу G_a набора $a \in Y$.

57.16. Пусть G — группа аффинных преобразований в n-мерном аффинном вещественном (комплексном) пространстве X. Обозначим через Q — множество всех квадратичных функций в X. Если $g \in G$, $h \in Q$ и $x \in X$, то положим $g(h) = h(g^{-1}x)$.

а) Доказать, что задано действие G в Q.

б) Описать орбиты G в Q.

в) Описать стационарную подгруппу G_h невырожденной функции $h \in Q$.

57.17. Пусть G — группа дробно-линейных преобразований $z \to \to a\dfrac{z-b}{1-z\bar{b}}$, $|a| = 1$, $|b| < 1$, единичного круга с центром O из задачи 24.25. Найти:

а) стационарную подгруппу точки O;

б) орбиту точки O;

в) пересечение стационарных подгрупп двух различных точек единичного круга.

57.18. Пусть группа G действует на множестве X и x, y — элементы одной орбиты G в X. Доказать, что все такие $g \in G$, что $g(x) = y$, составляют левый смежный класс G по стационарной подгруппе G_x и правый смежный класс по стационарной подгруппе G_y.

57.19. Пусть коммутативная группа G действует на некотором множестве M. Доказать, что если для некоторых $g \in G$ и $m_0 \in M$ справедливо равенство $gm_0 = m_0$, то $gm = m$ для любой точки m, лежащей в одной орбите с точкой m_0.

57.20. Пусть H — подгруппа группы G, $a \in G$. Доказать, что:

а) отображение $\sigma_a\colon\ gH \mapsto agH$ есть перестановка на множестве M всех левых смежных классов группы G по подгруппе H;

б) отображение $f\colon\ a \mapsto \sigma_a$ определяет действие группы G на M;

в) σ_a является тождественной перестановкой тогда и только тогда, когда a принадлежит пересечению всех подгрупп, сопряженных с H в группе G.

57.21. Перенумеровав левые смежные классы группы G по подгруппе H, найти все перестановки σ_a (задача 57.20), если:

а) $G = \mathbf{Z}_4$, H — единичная подгруппа;

б) $G = \mathbf{D}_4$, H — подгруппа, состоящая из тождественного преобразования и некоторой осевой симметрии квадрата.

57.22. Доказать, что для любой группы G:

а) сопряжение определяет действие

$$m \mapsto g \cdot m = gmg^{-1}, \qquad g, m \in G,$$

группы G на множестве G;

б) стационарная подгруппа точки m (централизатор элемента m) совпадает со множеством элементов группы G, перестановочных с m.

57.23. Найти централизатор:
а) перестановки $(1\,2)(3\,4)$ в группе $\mathbf{S}_4$;
б) перестановки $(1\,2\,3\ldots n)$ в группе $\mathbf{S}_n$.

57.24. В группе $\mathbf{GL}_2(\mathbb{R})$ найти централизатор матрицы:
а) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; б) $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$; в) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$; г) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

57.25. В группе $\mathbf{GL}_n(\mathbb{R})$ найти централизатор матрицы $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, если:
а) все элементы диагонали различны;
б) $\lambda_1 = \ldots = \lambda_k = a$, $\lambda_{k+1} = \ldots = \lambda_n = b$ и $a \neq b$.

57.26. Какие из трех матриц сопряжены между собой в группе $\mathbf{GL}_2(\mathbb{C})$:
$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}?$$

57.27. Пусть F — поле. В группе $\mathbf{SL}_n(F)$ найти:
а) централизатор C_{ij} элементарной матрицы $E + E_{ij}$ при $1 \leqslant i \neq j \leqslant n$;
б) пересечение C_{ij} при всех i, j, где $1 \leqslant i \neq j \leqslant n$;
в) класс сопряженных элементов, содержащих $E + E_{ij}$.
Доказать, что любые две элементарные матрицы $E + \alpha E_{ij}$ и $E + \beta E_{pq}$, где $1 \leqslant i \neq j$, $p \neq q \leqslant n$ и α, $\beta \in F^*$, сопряжены.

57.28. В группе $\mathbf{O}_2(\mathbb{R})$ ортогональных операторов найти:
а) централизатор оператора поворота на угол $q \neq k\pi$;
б) централизатор симметрии относительно оси OX.

57.29. Доказать, что в группе $\mathbf{O}_2(\mathbb{R})$ любые две симметрии сопряжены.

57.30. Найти классы сопряженных элементов групп:
а) $\mathbf{S}_3$; б) $\mathbf{A}_4$; в) $\mathbf{D}_4$.

57.31. Найти все конечные группы, число классов сопряженности которых равно: а) 1; б) 2; в) 3.

57.32. В группе $\mathbf{S}_4$ найти класс сопряженности:
а) перестановки $(1\,2)(3\,4)$; б) перестановки $(1\,2\,4)$.

57.33. Есть ли в группах $\mathbf{S}_5$, $\mathbf{S}_6$ несопряженные элементы одинаковых порядков?

57.34. Доказать, что две перестановки сопряжены в группе $\mathbf{S}_n$ тогда и только тогда, когда они имеют одинаковую цикловую структуру, т. е. их разложения в произведения независимых циклов для любого k содержат одинаковое число циклов длины k.

57.35. Найти число классов сопряженности в группах:
а) $\mathbf{S}_4$; б) $\mathbf{S}_5$; в) $\mathbf{S}_6$; г) $\mathbf{D}_n$.

57.36. *Канонической формой* матрицы $A \in \mathbf{SO}_3(\mathbb{R})$ называется сопряженная с A матрица вида

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}.$$

Доказать, что матрицы A_1 и A_2 сопряжены в $\mathbf{SO}_3(\mathbb{R})$ тогда и только тогда, когда их канонические формы связаны соотношением $\varphi_1 + \varphi_2 = 2\pi k$ или $\varphi_1 - \varphi_2 = 2\pi k$ для некоторого целого k.

57.37. Доказать, что:
а) если H и K — сопряженные подгруппы конечной группы и $K \subseteq H$, то $K = H$;
б) подгруппы

$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad (n \in \mathbb{Z}) \right\}, \quad K = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \quad (n \in \mathbb{Z}) \right\}$$

сопряжены в группе $\mathbf{GL}_2(\mathbb{R})$, и $K \subset H$.

57.38. Найти нормализатор $N(H)$ подгруппы H в группе G, если:
а) $G = \mathbf{GL}_2(\mathbb{R})$, H — подгруппа диагональных матриц;
б) $G = \mathbf{GL}_2(\mathbb{R})$, H — подгруппа матриц вида

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \qquad a \in \mathbb{R};$$

в) $G = \mathbf{S}_4$, $H = \langle (1234) \rangle$.

57.39. Найти группу автоморфизмов:
а) группы $\mathbf{Z}_5$; б) группы $\mathbf{Z}_6$.

57.40. Доказать, что:
а) $\mathrm{Aut}\, \mathbf{S}_3 \simeq \mathbf{S}_3$, причем все автоморфизмы группы $\mathbf{S}_3$ внутренние;
б) $\mathrm{Aut}\, \mathbf{V}_4 \simeq \mathbf{S}_3$, причем внутренним для $\mathbf{V}_4$ является лишь тождественный автоморфизм.

57.41. Является ли циклической группа автоморфизмов:
а) группы $\mathbf{Z}_9$; б) группы $\mathbf{Z}_8$?

57.42. Найти порядок группы $\mathrm{Aut}\,\mathrm{Aut}\,\mathrm{Aut}\, \mathbf{Z}_9$.

57.43. В группе $\mathbf{S}_6$ построить внешний автоморфизм.

57.44. Доказать, что в группе $\mathbf{S}_n$ $(n \neq 6)$ все автоморфизмы внутренние.

57.45. Доказать, что группа автоморфизмов $\mathbf{D}_4$ изоморфна $\mathbf{D}_4$. Найти подгруппу внутренних автоморфизмов группы $\mathbf{D}_4$.

57.46. Найти группу автоморфизмов группы $\mathbf{D}_n$ и подгруппу ее внутренних автоморфизмов.

§ 58. Гомоморфизмы и нормальные подгруппы. Факторгруппы, центр

58.1. Доказать, что подгруппа H группы G нормальна, если:
а) G — коммутативная группа, H — любая ее подгруппа;
б) $G = \mathbf{GL}_n(\mathbb{R})$, H — подгруппа матриц с определителем, равным 1;
в) $G = \mathbf{S}_n$, $H = \mathbf{A}_n$;
г) $G = \mathbf{S}_4$, $H = \mathbf{V}_4$;
д) G — группа невырожденных комплексных верхнетреугольных матриц, H — группа матриц вида

$$E + \sum_{\substack{1 \leqslant i < j \leqslant n \\ j-i \geqslant k}} \alpha_{ij} E_{ij}, \qquad \alpha_{ij} \in \mathbb{C}.$$

58.2. Будет ли нормальной подгруппой в группе $\mathbf{GL}_n(\mathbb{Z})$ множество всех матриц вида

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

где числа a, d нечетны, а числа b, c четны?

58.3. Доказать, что любая подгруппа индекса 2 является нормальной.

58.4. Найти все нормальные подгруппы, отличные от единичной и от всей группы в группах:
а) $\mathbf{S}_3$; б) $\mathbf{A}_4$; в) $\mathbf{S}_4$.

58.5. На примере группы $\mathbf{A}_4$ показать, что нормальная подгруппа K нормальной подгруппы H группы G не обязательно является нормальной в G.

58.6. Пусть A и B — нормальные подгруппы группы G и $A \cap B$ — единичная подгруппа. Доказать, что $xy = yx$ для любых $x \in A$, $y \in B$.

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

58.8. Доказать, что факторгруппа $\mathbb{R}^*/\mathbb{Q}^*$ не является циклической.

58.9. Найти число классов сопряженности в группе $\mathbf{A}_5$ и число элементов в каждом из классов.

58.10. Доказать, что группа $\mathbf{A}_5$ является простой.

58.11. а) Доказать, что в группе кватернионов $\mathbf{Q}_8$ любая подгруппа является нормальной.

б) Найти центр и все классы сопряженности в группе $\mathbf{Q}_8$.

в) Доказать, что комплексные матрицы

$$\pm E = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \pm I = \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$\pm J = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \pm K = \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

относительно умножения матриц образуют группу, изоморфную $\mathbf{Q}_8$.

58.12. Найти все нормальные подгруппы в группе диэдра $\mathbf{D}_n$.

58.13. Доказать, что каждая конечная подгруппа в $\mathbf{O}_2(\mathbb{R})$, не лежащая в $\mathbf{O}_2(\mathbb{R})$, является группой диэдра $\mathbf{D}_n$, $n \geqslant 2$.

58.14. Пусть F — поле и G — подгруппа в $\mathbf{GL}_n(F)$, содержащая $\mathbf{SL}_n(F)$. Доказать, что G нормальна в $\mathbf{GL}_n(F)$.

58.15. Сопоставим каждой матрице $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{C})$ дробно-линейное преобразование

$$f(z) = \frac{az+b}{cz+d}.$$

Доказать, что это сопоставление является гомоморфизмом и найти ядро этого гомоморфизма.

58.16. Доказать, что ядро любого гомоморфизма группы $\mathbb{C}^*$ в аддитивную группу $\mathbb{R}$ является бесконечной группой.

58.17. Пусть n, $m \geqslant 2$ — натуральные числа и $\mathbf{SL}_n(\mathbb{Z}; m\mathbb{Z})$ — подмножество в $\mathbf{SL}_n(\mathbb{Z})$, состоящее из матриц вида $E + Xm$, где X — целочисленная квадратная матрица размера n. Доказать, что:

а) $\mathbf{SL}_n(\mathbb{Z}; m\mathbb{Z})$ — нормальная подгруппа в $\mathbf{SL}_n(\mathbb{Z})$;

б) если $m = p$ — простое число, то

$$\mathbf{SL}_n(\mathbb{Z})/\mathbf{SL}_n(\mathbb{Z}; p\mathbb{Z}) \simeq \mathbf{SL}_n(\mathbb{Z}_p);$$

в) группа $\mathbf{SL}_n(\mathbb{Z}; m\mathbb{Z})$ не содержит элементов конечного порядка при $m \geqslant 3$;

г) если G — конечная подгруппа в $\mathbf{SL}_n(\mathbb{Z})$, то порядок G делит

$$\frac{1}{2}(3^n - 1)(3^n - 3) \times \ldots \times (3^n - 3^{n-1}).$$

58.18. Доказать, что для любой группы G множество всех внутренних автоморфизмов является нормальной подгруппой в группе $\operatorname{Aut} G$ всех автоморфизмов группы G.

58.19. Доказать, что любая подгруппа, содержащая коммутант группы, нормальна.

58.20. Найти центр группы: а) $\mathbf{S}_n$; б) $\mathbf{A}_n$; в) $\mathbf{D}_n$.

58.21. Пусть группа G порождена элементами a, b, причем

$$a^2 = b^2 = (ab)^4 = 1.$$

Доказать, что элемент $(ab)^2$ лежит в центре группы G.

58.22. Доказать, что центр группы порядка p^n, где p — простое число ($n \in \mathbb{N}$), содержит более одного элемента.

58.23. Пусть G — множество верхних унитреугольных матриц порядка 3 с элементами из поля $\mathbf{Z}_p$.

а) Доказать, что G — некоммутативная группа порядка p^3 относительно умножения.

б) Найти центр группы G.

в) Найти все классы сопряженных элементов группы G.

58.24. Найти центр группы:
а) $\mathbf{GL}_n(\mathbb{R})$; б) $\mathbf{O}_2(\mathbb{R})$; в) $\mathbf{SO}_2(\mathbb{R})$; г) $\mathbf{SO}_3(\mathbb{R})$;
д) $\mathbf{SU}_2(\mathbb{C})$; е) $\mathbf{SU}_n(\mathbb{C})$; ж) верхнетреугольных матриц.

58.25. Найти центр:

а) группы всех дробно-линейных преобразований комплексной плоскости;

б) группы всех преобразований единичного круга из задачи 57.17.

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

58.27. Доказать, если группа G гомоморфно отображена на группу H, причем $a \mapsto a'$, то:

а) порядок a делится на порядок a';

б) порядок G делится на порядок H.

58.28. Найти все гомоморфные отображения:
а) $\mathbf{Z}_6 \to \mathbf{Z}_6$; б) $\mathbf{Z}_6 \to \mathbf{Z}_{18}$; в) $\mathbf{Z}_{18} \to \mathbf{Z}_6$;
г) $\mathbf{Z}_{12} \to \mathbf{Z}_{15}$; д) $\mathbf{Z}_6 \to \mathbf{Z}_{25}$.

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

58.30. Найти факторгруппы:
а) $\mathbb{Z}/n\mathbb{Z}$; б) $\mathbf{U}_{12}/\mathbf{U}_3$; в) $4\mathbb{Z}/12\mathbb{Z}$; г) $\mathbb{R}^*/\mathbb{R}_+$.

58.31. Пусть F^n — аддитивная группа n-мерного линейного пространства над полем F и H — подгруппа векторов k-мерного подпространства. Доказать, что факторгруппа F^n/H изоморфна F^{n-k}.

58.32. Пусть H_n — множество чисел с аргументами вида $2\pi k/n$ ($k \in \mathbb{Z}$). Доказать, что:
а) $\mathbb{R}/\mathbb{Z} \simeq \mathbf{U}$; б) $\mathbb{C}^*/\mathbb{R}^* \simeq \mathbf{U}$; в) $\mathbb{C}^*/\mathbf{U} \simeq \mathbb{R}_+$;
г) $\mathbf{U}/\mathbf{U}_n \simeq \mathbf{U}$; д) $\mathbb{C}^*/\mathbf{U}_n \simeq \mathbb{C}^*$; е) $\mathbb{C}^*/H_n \simeq \mathbf{U}$;
ж) $H_n/\mathbb{R}_+ \simeq \mathbf{U}_n$; з) $H_n/\mathbf{U}_n \simeq \mathbb{R}_+$.

58.33. Пусть

$$G = \mathbf{GL}_n(\mathbb{R}), \qquad H = \mathbf{GL}_n(\mathbb{C}), \qquad P = \mathbf{SL}_n(\mathbb{R}), \qquad Q = \mathbf{SL}_n(\mathbb{C})$$

$$A = \{X \in G \mid |\det X| = 1\}, \qquad B = \{X \in H|\ |\det X| = 1\},$$
$$B = \{X \in G \mid \det X > 1\}, \qquad N = \{X \in H|\ \det X > 0\}.$$

Доказать, что:
а) $G/P \simeq \mathbb{R}^*$; б) $H/Q \simeq \mathbb{C}^*$; в) $G/(N \cap G) \simeq \mathbf{Z}_2$;
г) $H/N \simeq \mathbf{U}$; д) $G/A \simeq \mathbb{R}_+$; е) $H/B \simeq \mathbb{R}_+$.

58.34. Пусть G — группа аффинных преобразований n-мерного пространства, H — подгруппа параллельных переносов, K — подгруппа преобразований, оставляющих неподвижной данную точку O. Доказать, что:
а) H является нормальной подгруппой в G;
б) $G/H \simeq K$.

58.35. Доказать, что факторгруппа группы $\mathbf{S}_4$ по нормальной подгруппе $\{e, (12)(34), (13)(24), (14)(23)\}$ изоморфна группе $\mathbf{S}_3$.

58.36. Доказать, что если H — подгруппа индекса k в группе G, то H содержит некоторую нормальную в G подгруппу, индекс которой в G делит $k!$.

58.37. Доказать, что подгруппа, индекс которой является наименьшим простым делителем порядка группы, нормальна.

58.38. Доказать, что факторгруппа группы $\mathbf{GL}_2(\mathbf{Z}_3)$ по ее центру изоморфна группе $\mathbf{S}_4$.

58.39. Доказать, что в группе $\mathbb{Q}/\mathbb{Z}$:
а) каждый элемент имеет конечный порядок;
б) для каждого натурального n имеется в точности одна подгруппа порядка n.

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

58.41. Доказать, что факторгруппа некоммутативной группы по ее центру не может быть циклической.

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

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

* * *

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

58.45. Подгруппа H называется *максимальной* в группе G, если $H \neq G$ и любая подгруппа, содержащая H, совпадает с H или G. Доказать, что:
а) пересечение любых двух различных максимальных коммутативных подгрупп содержится в центре группы;
б) во всякой конечной простой некоммутативной группе найдутся две различные максимальные подгруппы, пересечение которых содержит более одного элемента;
в) во всякой конечной простой некоммутативной группе существует собственная некоммутативная подгруппа.

58.46. Доказать, что факторгруппа $\mathbf{SL}_2(\mathbf{Z}_5)$ по ее центру изоморфна $\mathbf{A}_5$.

58.47. Пусть F — поле, $n \geqslant 3$ и G — нормальная подгруппа в $\mathbf{GL}_n(F)$. Доказать, что либо $G \supseteq \mathbf{SL}_n(F)$, либо G состоит из скалярных матриц.

58.48. Пусть F — поле, содержащее не менее четырех элементов и G — нормальная подгруппа в $\mathbf{GL}_2(F)$. Доказать, что либо $G \supseteq \mathbf{SL}_2(F)$, либо G состоит из скалярных матриц.

58.49. Доказать, что $\mathbf{SL}_2(2) \simeq \mathbf{S}_3$.

58.50. Найти все нормальные подгруппы в $\mathbf{SL}_2(3)$.

58.51. Пусть G — нормальная подгруппа конечного индекса в $\mathbf{SL}_n(\mathbb{Z})$, $n \geqslant 3$. Тогда существует такое натуральное число m, что $G \subseteq \mathbf{SL}_n(\mathbb{Z}, m\mathbb{Z})$.

58.52. Пусть F — поле, $n \geqslant 3$ и φ — автоморфизм группы $\mathbf{GL}_n(F)$. Доказать, что существует такой гомоморфизм групп $\eta : \mathbf{GL}_n(F) \to F^*$ и автоморфизм η поля F, индуцирующий автоморфизм $\mathbf{GL}_n(F)$ такой, что либо
$$\varphi(x) = \eta(x)\, g\, \tau(x)\, g^{-1},$$
либо
$$\varphi(x) = \eta(x)\, g^t\, \tau(x)^{-1}\, g^{-1},$$
для всех $x, y \in \mathbf{GL}_n(F)$ $g \in \mathbf{GL}_n(F)$.

§ 59. Силовские подгруппы. Группы малых порядков

59.1. Найти порядок групп:
а) $\mathbf{GL}_n(\mathbb{F}_q)$; б) $\mathbf{SL}_n(\mathbb{F}_q)$;
в) невырожденных верхнетреугольных матриц размера n над конечным полем из q элементов.

59.2. Изоморфны ли: а) группа $\mathbf{Q}_8$ и группа $\mathbf{D}_4$;
б) группа $\mathbf{S}_4$ и группа $\mathbf{SL}_2(3)$?

59.3. Найти все силовские 2-подгруппы и 3-подгруппы в группах:
а) $\mathbf{S}_3$; б) $\mathbf{A}_4$.

59.4. Указать сопрягающие элементы для силовских 2-подгрупп и силовских 3-подгрупп в группах:
а) $\mathbf{S}_3$; б) $\mathbf{A}_4$.

59.5. Доказать, что любая силовская 2-подгруппа группы $\mathbf{S}_4$ изоморфна группе диэдра $\mathbf{D}_4$.

59.6. В каких силовских 2-подгруппах группы $\mathbf{S}_4$ содержатся перестановки:
а) $(1\,3\,2\,4)$; б) $(1\,3)$; в) $(1\,2)(3\,4)$?

59.7. Доказать, что существуют в точности две некоммутативные неизоморфные группы порядка 8 — группа кватернионов $\mathbf{Q}_8$ и группа диэдра $\mathbf{D}_4$.

59.8. Доказать, что силовская 2-подгруппа группы $\mathbf{SL}_2(\mathbb{Z}_3)$:
а) изоморфна группе кватернионов;
б) нормальна в $\mathbf{SL}_2(\mathbb{Z}_3)$.

59.9. Сколько различных силовских p-подгрупп в группе $\mathbf{A}_5$, где:
а) $p = 2$; б) $p = 3$; в) $p = 5$?

59.10. Найти порядок силовской p-подгруппы в группе $\mathbf{S}_n$.

59.11. Сколько различных силовских p-подгрупп в группе $\mathbf{S}_p$, где p — простое число?

59.12. Доказать, что силовская p-подгруппа в группе G единственна тогда и только тогда, когда она нормальна в G.

59.13. Пусть

$$P = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbf{Z}_p, \quad p \text{ — простое число} \right\}.$$

а) Доказать, что P — силовская p-подгруппа в группе $\mathbf{SL}_2(\mathbf{Z}_p)$.
б) Найти нормализатор подгруппы P в $\mathbf{SL}_2(\mathbf{Z}_p)$.
в) Найти число различных силовских p-подгрупп в $\mathbf{SL}_2(\mathbf{Z}_p)$.
г) Доказать, что P — силовская p-подгруппа в группе $\mathbf{GL}_2(\mathbf{Z}_p)$.
д) Найти нормализатор подгруппы P в $\mathbf{GL}_2(\mathbf{Z}_p)$.
е) Найти число различных силовских p-подгрупп в $\mathbf{GL}_2(\mathbf{Z}_p)$.

59.14. Доказать, что подгруппа верхних унитреугольных матриц является силовской p-подгруппой в $\mathbf{GL}_n(\mathbf{Z}_p)$.

59.15. В группе диэдра $\mathbf{D}_n$ для каждого простого делителя p числа $2n$:
а) найти все силовские p-подгруппы;
б) указать сопрягающие элементы для силовских p-подгрупп.

59.16. Доказать, что образ силовской p-подгруппы конечной группы G при гомоморфизме группы G на группу H является силовской подгруппой в H.

59.17. Доказать, что любая силовская p-подгруппа прямого произведения конечных групп A и B является произведением силовских p-подгрупп сомножителей A и B.

59.18. Пусть P — силовская p-подгруппа конечной группы G, H — нормальная в G подгруппа.
а) Доказать, что пересечение $P \cap H$ является силовской p-подгруппой в H.
б) Привести пример, показывающий, что без предположения о нормальности подгруппы H утверждение пункта а) неверно.

59.19. Доказать, что все силовские подгруппы группы порядка 100 коммутативны.

59.20. Доказать, что любая группа порядка:
а) 15; б) 35; в) 185; г) 255;
коммутативна.

59.21. Сколько различных силовских 2-подгрупп и силовских 5-подгрупп в некоммутативной группе порядка 20?

59.22. Доказать, что не существует простых групп порядка:
а) 36; б) 80; в) 56; г) 196; д) 200.

59.23. Пусть p и q — простые числа, $p < q$. Доказать, что:
а) если $q - 1$ не делится на p, то любая группа порядка pq коммутативна;
б) если $q - 1$ делится на p, то в группе невырожденных матриц вида $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ $(a, b \in \mathbf{Z}_q)$ имеется некоммутативная подгруппа порядка pq.

59.24. Сколько элементов порядка 7 в простой группе порядка 168?

* * *

59.25. Пусть K — нормальная подгруппа в p-группе G. Доказать, что $K \cap Z(G) \neq 1$.

59.26. Пусть V — конечномерное векторное пространство над полем F характеристики p и G — p-группа линейных невырожден ных операторов в V. Доказать, что существует такой ненулевой вектор $x \in V$, что $gx = x$ для всех $g \in G$.

59.27. Пусть P — силовская p-подгруппа в конечной группе G и H — подгруппа в G, содержащая нормализатор $N_G(P)$. Доказать, что $N_G(H) = H$.

59.28. Пусть G — конечная группа, N — нормальная подгруппа в G и P — силовская подгруппа в N. Доказать, что $G = N \cdot N_G(P)$ (лемма Фиттинга).

59.29. Предположим, что в конечной группе G имеется такой элемент a, что $\dfrac{|G|}{|K(a)|} = p$ — простое число, где $K(a)$ — класс сопряженных с a элементов из G. Доказать, что:
а) p^2 не делит порядок группы G;
б) если $p = 2$, то в группе G имеется такая абелева подгруппа H нечетного порядка и индекса 2, что $aha^{-1} = h^{-1}$ для любого $h \in H$.

§ 60. Прямые произведения и прямые суммы. Абелевы группы

60.1. Доказать, что группы $\mathbb{Z}$ и $\mathbb{Q}$ не разлагаются в прямую сумму ненулевых подгрупп.

60.2. Разлагаются ли в прямое произведение неединичных подгрупп группы:
а) $\mathbf{S}_3$; б) $\mathbf{A}_4$; в) $\mathbf{S}_4$; г) $\mathbf{Q}_8$?

60.3. Доказать, что конечная циклическая группа является прямой суммой примарных циклических подгрупп.

60.4. Доказать, что прямая сумма циклических групп $\mathbf{Z}_m \oplus \mathbf{Z}_n$ является циклической группой тогда и только тогда, когда наибольший общий делитель m и n равен 1.

60.5. Разложить в прямую сумму группы:
а) $\mathbf{Z}_6$; б) $\mathbf{Z}_{12}$; в) $\mathbf{Z}_{60}$.

60.6. Доказать, что мультипликативная группа комплексных чисел является прямым произведением группы положительных вещественных чисел и группы всех комплексных чисел, по модулю равных 1.

60.7. Доказать, что при $n \geqslant 3$ мультипликативная группа кольца вычетов $\mathbf{Z}_{2^n}$ является прямым произведением подгруппы $\{\pm 1\}$ и циклической группы порядка 2^{n-2}.

60.8. Чему равен порядок:
а) прямого произведения конечных групп;
б) элемента прямого произведения конечных групп?

60.9. Доказать, что если в абелевой группе подгруппы $A_1, A_2, \ldots \ldots, A_k$ имеют конечные попарно взаимно простые порядки, то их сумма является прямой.

60.10. Пусть D — подгруппа прямого произведения $A \times B$ групп Aи B взаимно простых порядков. Доказать, что

$$D \simeq (D \cap A) \times (D \cap B).$$

60.11. Пусть k — наибольший порядок элементов конечной абелевой группы G. Доказать, что порядок любого элемента группы G делит k. Верно ли это утверждение без предположения об абелевости группы?

60.12. Найти все прямые разложения группы, состоящей из чисел вида $\pm 2^n$.

60.13. Пусть A — конечная абелева группа. Найти все прямые разложения группы $\mathbb{Z} \oplus A$, в которых одно из слагаемых является бесконечной циклической группой.

60.14. Найти классы сопряженности группы $A \times B$, если известны классы сопряженности групп A и B.

60.15. а) Доказать, что центр прямого произведения $A \times B$ равен прямому произведению центров A и B.

б) Пусть N — нормальная подгруппа в $A \times B$, причем

$$N \cap A = N \cap B = 1.$$

Доказать, что N лежит в центре $A \times B$.

60.16. Доказать, что если факторгруппа A/B абелевой группы A по подгруппе B является свободной абелевой группой, то $A = B \oplus C$, где C — свободная абелева группа.

60.17. Доказать, что подгруппа A абелевой группы G выделяется в G прямым слагаемым тогда и только тогда, когда существует сюръективный гомоморфизм $\pi\colon\ G \to A$ такой, что $\pi^2 = \pi$.

60.18. Пусть φ_1, φ_2 — гомоморфизмы групп A_1, A_2 в абелеву группу B. Доказать, что существует единственный гомоморфизм $\varphi : A_1 \times A_2 \to B$, ограничения которого на A_1 и A_2 совпадают соответственно с φ_1 и φ_2. Существенна ли здесь абелевость группы B?

60.19. На множестве гомоморфизмов абелевой группы A в абелеву группу B определим операцию сложения по правилу

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x).$$

Доказать, что гомоморфизмы $A \to B$ образуют абелеву группу $\mathrm{Hom}\,(A, B)$.

60.20. Найти группы гомоморфизмов:

а) $\mathrm{Hom}\,(\mathbf{Z}_{12}, \mathbf{Z}_6)$; б) $\mathrm{Hom}\,(\mathbf{Z}_{12}, \mathbf{Z}_{18})$;
в) $\mathrm{Hom}\,(\mathbf{Z}_6, \mathbf{Z}_{12})$; г) $\mathrm{Hom}\,(A_1 \oplus A_2, B)$;
д) $\mathrm{Hom}\,(A, B_1 \oplus B_2)$; е) $\mathrm{Hom}\,(\mathbf{Z}_n, \mathbf{Z}_k)$;
ж) $\mathrm{Hom}\,(\mathbb{Z}, \mathbf{Z}_n)$; з) $\mathrm{Hom}\,(\mathbf{Z}_n, \mathbb{Z})$;
и) $\mathrm{Hom}\,(\mathbb{Z}, \mathbb{Z})$; к) $\mathrm{Hom}\,(\mathbf{Z}_2 \oplus \mathbf{Z}_2, \mathbf{Z}_8)$;
л) $\mathrm{Hom}\,(\mathbf{Z}_2 \oplus \mathbf{Z}_3, \mathbf{Z}_{30})$.

60.21. Доказать, что $\mathrm{Hom}\,(\mathbb{Z}, A) \simeq A$.

60.22. Пусть A — абелева группа. Доказать, что все ее эндоморфизмы образуют кольцо $\mathrm{End}\,A$ с единицей относительно сложения и обычного умножения отображений.

60.23. Доказать, что группа автоморфизмов абелевой группы совпадает с группой обратимых элементов ее кольца эндоморфизмов.

60.24. Найти кольца эндоморфизмов групп:
а) $\mathbb{Z}$; б) $\mathbf{Z}_n$; в) $\mathbb{Q}$.

60.25. Доказать, что в абелевой группе отображение $x \to nx$ ($n \in \in \mathbb{Z}$) является эндоморфизмом. Для каких групп оно будет:
а) инъективным; б) сюръективным?

60.26. Доказать, что кольцо эндоморфизмов свободной абелевой группы ранга n изоморфно кольцу $\mathbf{M}_n(\mathbb{Z})$.

60.27. Найти группы автоморфизмов групп:
а) $\mathbb{Z}$; б) $\mathbb{Q}$; в) $\mathbf{Z}_{2^n}$; г) свободной абелевой ранга n.

60.28. Доказать, что:
а) $\mathrm{Aut}\,\mathbf{Z}_{30} \simeq \mathrm{Aut}\,\mathbf{Z}_{15}$; б) $\mathrm{Aut}\,(\mathbb{Z} \oplus \mathbf{Z}_2) = \mathbf{Z}_2 \oplus \mathbf{Z}_2$.

60.29. Доказать, что кольцо $\mathrm{End}\,(\mathbb{Z} \oplus \mathbf{Z}_2)$ бесконечно и некоммутативно.

60.30. Доказать, что кольцо эндоморфизмов конечной абелевой группы является прямой суммой колец эндоморфизмов ее примарных компонент.

60.31. Доказать, что подгруппа конечно порожденной абелевой группы также конечно порождена.

60.32. Доказать, что всякий гомоморфизм конечно порожденной абелевой группы на себя является автоморфизмом.

Верно ли аналогичное утверждение для аддитивной группы кольца многочленов?

60.33. Доказать, что свободные абелевы группы рангов m и n изоморфны тогда и только тогда, когда $m = n$.

60.34. Пусть A, B, C — конечнопорожденные абелевы группы, причем $A \oplus C \simeq B \oplus C$. Доказать, что $A \simeq B$.

60.35. Пусть порядок конечной абелевой группы G делится на натуральное число m. Доказать, что в G есть подгруппа порядка m.

60.36. Пусть A и B — конечные абелевы группы, причем для любого натурального числа m в A и B число элементов порядка m одинаково. Доказать, что $A \simeq B$.

60.37. Пусть A и B — конечнопорожденные абелевы группы, причем каждая из них изоморфна подгруппе другой. Доказать, что $A \simeq B$.

60.38. Доказать, что подгруппа B свободной абелевой группы A является свободной, причем ранг B не превосходит ранга A.

60.39. Пользуясь основной теоремой о конечно порожденных абелевых группах, найти с точностью до изоморфизма все абелевы группы порядка:
а) 2; б) 6; в) 8; г) 12;
д) 16; е) 24; ж) 36; з) 48.

60.40. Говорят, что абелева группа *имеет тип* $(n_1, n_2, \ldots, n_k)$, если она является прямой суммой циклических групп порядков $n_1, n_2, \ldots$ $\ldots, n_k$.

Есть ли в абелевой группе типа (2,16) подгруппы типа:
а) (2,8); б) (4,4); в) (2,2,2)?

60.41. Найти тип группы $(\langle a\rangle_9 \oplus \langle b\rangle_{27})/\langle 3a + 9b\rangle$.

60.42. Изоморфны ли группы:

а) $(\langle a\rangle_2 \oplus \langle b\rangle_4)/\langle 2b\rangle$ и $(\langle a\rangle_2 \oplus \langle b\rangle_4)/\langle a+2b\rangle$;
б) $\mathbf{Z}_6 \oplus \mathbf{Z}_{36}$ и $\mathbf{Z}_{12} \oplus \mathbf{Z}_{18}$;
в) $\mathbf{Z}_6 \oplus \mathbf{Z}_{36}$ и $\mathbf{Z}_9 \oplus \mathbf{Z}_{24}$;
г) $\mathbf{Z}_6 \oplus \mathbf{Z}_{10} \oplus \mathbf{Z}_{10}$ и $\mathbf{Z}_{60} \oplus \mathbf{Z}_{10}$?

60.43. Сколько подгрупп:
а) порядков 2 и 6 в нециклической абелевой группе порядка 12;
б) порядков 3 и 6 в нециклической абелевой группе порядка 18;
в) порядков 5 и 15 в нециклической абелевой группе порядка 75?

60.44. Найти все прямые разложения групп:
а) $\langle a\rangle_2 \oplus \langle b\rangle_2$;
б) $\langle a\rangle_p \oplus \langle b\rangle_p$;
в) $\langle a\rangle_2 \oplus \langle b\rangle_4$.

60.45. Сколько элементов:
а) порядка 2, 4 и 6 в группе $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3$;
б) порядка 2, 4 и 5 в группе $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_5$?

60.46. Пользуясь основной теоремой о конечных абелевых группах, доказать, что конечная подгруппа мультипликативной группы поля является циклической.

60.47. Пусть F — поле, у которого мультипликативная группа F^* конечно порождена. Доказать, что поле F конечно.

60.48. Доказать, что конечно порожденная подгруппа мультипликативной группы комплексных чисел разлагается в прямое произведение свободной абелевой группы и конечной циклической.

60.49. Пусть A — свободная абелева группа с базисом $e_1, \ldots, e_n$ и $x = m_1e_1 + \ldots + m_ne_n \in A \setminus 0$, где $m_i \in \mathbb{Z}$. Доказать, что циклическая группа $\langle x\rangle$ является прямым слагаемым в A тогда и только тогда, когда наибольший общий делитель чисел $m_1, \ldots, m_n$ равен 1.

60.50. Пусть A — свободная абелева группа с базисом $x_1, \ldots, x_n$. Доказать, что элементы

$$y_j = \sum_{i=1}^{n} a_{ij}x_i, \qquad j = 1, \ldots, n, \quad a_{ij} \in \mathbb{Z},$$

составляют базис группы A тогда и только тогда, когда $\det(a_{ij}) = \pm 1$.

60.51. Пусть A — свободная абелева группа с базисом $x_1, \ldots, x_n$, B — ее подгруппа с порождающими элементами

$$y_j = \sum_{i=1}^{n} a_{ij}x_i, \qquad j = 1, \ldots, n, \quad a_{ij} \in \mathbb{Z}.$$

Доказать, что факторгруппа A/B конечна тогда и только тогда, когда $\det(a_{ij}) \neq 0$, и при этом $|A/B| = |\det(a_{ij})|$.

60.52. Разложить в прямую сумму циклических групп факторгруппу A/B, где A — свободная абелева группа с базисом x_1, x_2, x_3, B — ее подгруппа, порожденная y_1, y_2, y_3:

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

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

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

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

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

л) $\begin{cases} y_1 = 4x_1 + 5x_2 + 3x_3, \\ y_2 = 5x_1 + 6x_2 + 5x_3, \\ y_3 = 8x_1 + 7x_2 + 9x_3; \end{cases}$ м) $\begin{cases} y_1 = 3x_1 + 3x_2, \\ y_2 = 9x_1 + 3x_2 - 6x_3, \\ y_3 = -3x_1 + 3x_2 + 6x_3. \end{cases}$

60.53. В факторгруппе свободной абелевой группы A с базисом x_1, x_2, x_3 по подгруппе B, порожденной $x_1 + x_2 + 4x_3$ и $2x_1 - x_2 + 2x_3$, найти порядок смежного класса $(x_1 + 2x_3) + B$.

60.54. В факторгруппе свободной абелевой группы A с базисом x_1, x_2, x_3 по подгруппе B, порожденной $2x_1 + x_2 - 50x_3$ и $4x_1 + 5x_2 + 60x_3$, найти порядок элемента $32x_1 + 31x_2 + B$.

60.55. Доказать, что кольцо эндоморфизмов конечной абелевой группы коммутативно тогда и только тогда, когда каждая ее примарная компонента является циклической.

* * *

60.56. Аддитивная подгруппа H в n-мерном вещественном пространстве $\mathbb{R}^n$ дискретна, если существует такая окрестность нуля U, что $U \cap H = 0$. Доказать, что дискретная подгруппа в $\mathbb{R}^n$ является свободной абелевой группой и ее ранг не превосходит n.

60.57. Найти все элементы конечного порядка в $\mathbb{R}^n/\mathbb{Z}^n$.

60.58. Пусть $H = \mathbb{Z}[i]$ — подгруппа целых гауссовых чисел в аддитивной группе поля комплексных чисел $\mathbb{C}$. Предположим, что $z = x + iy \in \mathbb{C} \setminus H$, где $x, y \in \mathbb{R}^*$, причем xy^{-1} иррационально. Доказать, что $\langle z \rangle + H$ всюду плотно в $\mathbb{C}$.

60.59. Пусть H — аддитивная замкнутая подгруппа в $\mathbb{R}^n$. Доказать, что $H = L \oplus H_1$, где L — подпространство в $\mathbb{R}^n$ и H_1 — дискретная подгруппа в $\mathbb{R}^n$.

60.60. Доказать, что если порядок элемента a абелевой группы A взаимно прост с n, то уравнение $nx = a$ имеет в A решение.

60.61. Абелева группа A называется *делимой*, если уравнение $nx = a$ имеет в ней решение при любом $a \in A$ и целом $n \neq 0$.

Доказать, что группа делима тогда и только тогда, когда при любом a и любом простом p уравнение $px = a$ имеет решение.

60.62. Доказать, что прямая сумма делима тогда и только тогда, когда делимы все прямые слагаемые.

60.63. Доказать, что группы $\mathbb{Q}$ и $\mathbf{U}_{p^\infty}$ (p — простое число) делимы.

60.64. Доказать, что в группе без кручения можно ввести структуру линейного пространства над полем $\mathbb{Q}$ тогда и только тогда, когда она является делимой.

60.65. Пусть A — делимая подгруппа группы G, B — максимальная подгруппа группы G такая, что $A \cap B = \{0\}$ (такая всегда существует). Доказать, что $G = A \oplus B$.

60.66. Доказать, что в любой абелевой группе существует делимая подгруппа, факторгруппа по которой не имеет делимых подгрупп.

60.67. Пусть A — конечно порожденная абелева группа и B — подгруппа в A. Предположим, что A/B — группа без кручения. Тогда $A = B \oplus C$, где C — свободная абелева группа.

60.68. Пусть A, B — свободные абелевы группы и $\varphi : A \to B$ — гомоморфизм групп. Доказать, что $\operatorname{Ker} \varphi$ — прямое слагаемое в A.

60.69. Пусть A — свободная абелева группа с базой $e_1, \ldots, e_n$, C — целочисленная квадратная матрица размера n. Обозначим через B множество всех таких векторов $x_1e_1 + \ldots + x_ne_n \in A$, что

$$C\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Доказать, что B — подгруппа в A, являющаяся прямым слагаемым в A. Обратно, любое прямое слагаемое в A задается системой линейных однородных целочисленных уравнений.

§ 61. Порождающие элементы и определяющие соотношения

61.1. Доказать, что:
а) группа $\mathbf{S}_n$ порождается транспозицией (12) и циклом $(12\ldots n)$;
б) группа $\mathbf{A}_n$ порождается тройными циклами.

61.2. Доказать, что:
а) группа $\mathbf{GL}_n(K)$ над полем K порождается матрицами вида $E + aE_{ij}$, где $a \in K$, $1 \leqslant i \neq j \leqslant n$, и матрицами $E + bE_{11}$, где $b \in K$, $b \neq -1$;
б) группа $\mathbf{UT}_n(K)$ порождается матрицами $E + aE_{ij}$, где $a \in K$, $1 \leqslant i < j \leqslant n$.

61.3. Доказать, что специальная линейная группа $\mathbf{SL}_n(K)$ над полем K порождается *трансвекциями*, т. е. элементарными матрицами вида $E + \alpha E_{ij}$ $(i \neq j)$.

61.4. Доказать, что:
а) любую целочисленную матрицу с единичным определителем можно привести к единичному виду только элементарными преобразованиями, заключающимися в том, что к одной строке прибавляется другая строка, умноженная на ± 1;
б) группа $\mathbf{SL}_n(\mathbb{Z})$ конечно порождена.

* * *

61.5. Пусть $\mathbb{F}_q$ — поле из $q \neq 9$ элементов и a — образующий циклической группы $\mathbb{F}_q^*$. Доказать, что $\mathbf{SL}_2(\mathbb{F}_q)$ порождается двумя матрицами

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

61.6. Доказать, что
а) $\mathbf{A}_5$ порождается двумя подстановками, (2 5 4) и (1 2 3 4 5).
б) Доказать, что $\mathbf{A}_n$ при четном $n \geqslant 4$ порождается двумя элементами: $a = (12)(n-1, n)$, $b = (1, 2, \ldots, n-1)$.
в) Доказать, что $\mathbf{A}_n$ при нечетном $n \geqslant 5$ порождается двумя элементами: $a = (1, n)(2, n-1)$, $b = (1, 2, \ldots, n-2)$.

61.7. Найти все двухэлементные множества, порождающие группы:
а) $\mathbf{Z}_6$; б) $\mathbf{S}_3$; в) $\mathbf{Q}_8$; г) $\mathbf{D}_4$; д) $\langle a \rangle_2 \oplus \langle b \rangle_2$.

61.8. Доказать, что если d — минимальное число порождающих конечной абелевой группы A, то для группы $A \oplus A$ аналогичное число равно $2d$.

61.9. Доказать, что группа $\mathbf{S}_2 \times \mathbf{S}_3$ порождается двумя элементами.

61.10. Доказать, что если группа имеет конечную систему порождающих, то из любой системы порождающих можно выбрать конечную подсистему, порождающую всю группу.

61.11. Будет ли конечно порожденным нормальное замыкание матрицы $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ в группе G, порожденной матрицами A и $B = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$?

61.12. Доказать, что:
а) каждое слово в свободной группе эквивалентно единственному несократимому слову;
б) «свободная группа» действительно является группой.

61.13. Пусть F — свободная группа со свободными порождающими $x_1, \ldots, x_n$, G — произвольная группа. Доказать, что для любых элементов $g_1, \ldots, g_n \in G$ существует единственный гомоморфизм $\varphi : F \to G$ такой, что $\varphi(x_1) = g_1, \ldots, \varphi(x_n) = g_n$. Вывести отсюда, что любая конечно порожденная группа изоморфна факторгруппе подходящей свободной группы конечного ранга.

61.14. Доказать, что в свободной группе нет элементов конечного порядка, отличных от единицы.

61.15. Доказать, что два коммутирующих элемента свободной группы лежат в одной циклической подгруппе.

61.16. Доказать, что слово w лежит в коммутанте свободной группы с системой свободный порождающих $x_1, \ldots, x_n$ тогда и только тогда, когда для каждого $i = 1, \ldots, n$ сумма показателей у всех вхождений x_i в w равна 0.

61.17. В свободной группе описать все слова, сопряженные слову w.

61.18. Доказать, что факторгруппа свободной группы по ее коммутанту — свободная абелева группа.

61.19. Доказать, что свободные группы рангов m и n изоморфны тогда и только тогда, когда $m = n$.

61.20. Сколько подгрупп индекса 2 в свободной группе ранга 2?

61.21. а) Доказать, что в свободной группе F ранга k все слова, в которых сумма показателей при каждой переменной делится на n, образуют нормальную подгруппу N.

б) Доказать, что $F/N = \overbrace{\mathbf{Z}_n \oplus \ldots \oplus \mathbf{Z}_n}^{k \text{ раз}}$

61.22. Доказать, что все сюръективные гомоморфизмы свободной группы ранга 2 на группу $\mathbf{Z}_n \oplus \mathbf{Z}_n$ имеют одно и то же ядро.

61.23. Сколько существует гомоморфизмов свободной группы ранга 2 в группу:
а) $\mathbf{Z}_2 \oplus \mathbf{Z}_2$; б) $\mathbf{S}_3$?

61.24. Доказать, что в $\mathbf{SL}_2(\mathbb{Z})$ множество матриц $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, где $a \equiv \equiv d \equiv 1 \pmod 4$, $b \equiv c \equiv 0 \pmod 2$, образует группу с двумя порождающими

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

61.25. Доказать, что если группа G с порождающими элементами $x_1, \ldots, x_n$ задана определяющими соотношениями $R_i(x_1, \ldots, x_n) = 1$ $(i \in I)$ и в какой-либо группе H для элементов $h_1, \ldots, h_n \in H$

$$R_i(h_1, \ldots, h_n) = 1,$$

то существует единственный гомоморфизм $\varphi : G \to H$ такой, что $\varphi(x_1) = h_1, \ldots, \varphi(x_n) = h_n$.

61.26. Доказать, что если между элементами a и b группы выполнены соотношения

$$a^5 = b^3 = 1, \qquad b^{-1}ab = a^2,$$

то $a = 1$.

61.27. Показать, что группа, порожденная элементами a, b с соотношениями $a^2 = b^7 = 1$, $a^{-1}ba = b^{-1}$, конечна.

61.28. Доказать, что группа, заданная порождающими элементами x_1, x_2 с соотношениями:
а) $x_1^2 = x_2^3 = (x_1x_2)^2 = 1$;
б) $x_1^2 = x_2^3 = 1$, $\quad x_1^{-1}x_2x_1 = x_2^2$;
изоморфна $\mathbf{S}_3$.

61.29. Доказать, что группа, заданная порождающими элементами x_1, x_2 и определяющими соотношениями

$$x_1^2 = x_2^n = 1, \qquad x_1^{-1}x_2x_1 = x_2^{-1},$$

изоморфна группе диэдра $\mathbf{D}_n$.

61.30. Доказать, что группа, заданная порождающими элементами x_1, x_2 и определяющими соотношениями

$$x_1^4 = 1, \qquad x_1^2 = x_2^2, \qquad x_2^{-1}x_1x_2 = x_1^3,$$

изоморфна группе кватернионов $\mathbf{Q}_8$.

61.31. Доказать, что группа, заданная порождающими элементами x_1, x_2 и определяющими соотношениями $x_1^2 = x_2^2 = 1$, изоморфна группе матриц

$$\left\{ \begin{pmatrix} \pm 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}.$$

61.32. Доказать, что группа, заданная порождающими элементами x_1, x_2 и определяющими соотношениями $x_1^2 = x_2^2 = (x_1x_2)^n = 1$, изоморфна группе матриц

$$\left\{ \begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix} \;\middle|\; k \in \mathbf{Z}_n \right\}.$$

61.33. Найти порядок группы, заданной образующими a, b и определяющими соотношениями:

а) $a^3 = b^2 = (ab)^3 = 1$;

б) $a^4 = b^2 = 1, \quad ab^2 = b^3a, \quad ba^3 = a^2b$.

61.34. Пусть G — группа, порожденная элементами x_{ij}, $1 \leqslant i < j \leqslant n$, с определяющими соотношениями

$$x_{ij}x_{kl} = x_{kl}x_{ij}, \qquad 1 \leqslant i < j \neq k < l \neq i \leqslant n;$$
$$x_{ij}x_{jl}x_{ij}^{-1}x_{jl}^{-1} = x_{il}, \qquad 1 \leqslant i < j < l \leqslant n.$$

Доказать, что:

а) каждый элемент группы G представляется в виде

$$x_{12}^{m_{12}}x_{13}^{m_{12}} \ldots x_{1n}^{m_{1n}}x_{23}^{m_{23}} \ldots x_{2n}^{m_{2n}} \ldots x_{n-1,n}^{m_{n-1,n}},$$

где $m_{ij} \in \mathbb{Z}$;

б) $G \simeq \mathbf{UT}_n(\mathbb{Z})$.

61.35. Доказать, что если $G/H = \langle gH \rangle$ — бесконечная циклическая группа, то $G = \langle g \rangle H$, $\langle g \rangle \cap H = \{e\}$.

61.36. Описать в терминах порождающих элементов и определяющих соотношений группы, у которых имеется бесконечная циклическая нормальная подгруппа с бесконечной циклической факторгруппой.

61.37. Пусть группа G задана порождающими элементами x_1, x_2 и определяющим соотношением $x_1 x_2 x_1^{-1} = x_2^2$. Найти наименьшую подгруппу, порожденную в G элементом x_2. Является ли эта подгруппа нормальной?

61.38. Пусть группа G порождена элементами a, b, c с определяющими соотношениями $a^2 = b^3 = c^5 = abc$. Доказать, что abc — центральный элемент порядка 2.

§ 62. Разрешимые группы

62.1. Найти коммутатор:

а) невырожденных матриц $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$;

б) $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ и $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$;

в) двух транспозиций в симметрической группе $\mathbf{S}_n$;

г) $\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}$ и $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.

62.2. Доказать следующие свойства коммутанта G' групп:
а) G' — нормальная подгруппа в G;
б) факторгруппа G/G' коммутативна;
в) если N нормальна в G и G/N коммутативна, то $G' \subseteq N$.

62.3. Доказать, что при сюръективном гомоморфизме $\varphi : G' \to H$ выполнено равенство $\varphi(G)' = H'$.

62.4. Установить биективное соответствие между гомоморфизмами группы в коммутативные группы и гомоморфизмами ее факторгруппы по коммутанту.

62.5. Доказать, что коммутант группы $\mathbf{GL}_n(K)$ содержится в $\mathbf{SL}_n(K)$.

62.6. Доказать, что коммутант прямого произведения есть прямое произведение коммутантов сомножителей.

62.7. Найти коммутанты и порядки факторгрупп по коммутантам для групп:

а) $\mathbf{S}_3$; б) $\mathbf{A}_4$; в) $\mathbf{S}_4$; г) $\mathbf{Q}_8$.

62.8. Найти коммутанты групп: а) $\mathbf{S}_n$; б) $\mathbf{D}_n$.

62.9. Доказать, что коммутант нормальной подгруппы нормален во всей группе.

62.10. *Рядом коммутантов* (или *производным рядом*) группы G называется ряд подгрупп

$$G = G^0 \supseteq G' \supseteq G'' \supseteq \ldots,$$

где $G^{i+1} = (G^i)'$.

Доказать, что:

а) все члены ряда коммутантов нормальны в G;

б) для всякого гомоморфизма φ группы G на группу H

$$\varphi(G^i) = H^i.$$

62.11. Доказать, что:

а) всякая подгруппа разрешимой группы разрешима;

б) всякая факторгруппа разрешимой группы разрешима;

в) если A и B — разрешимые группы, то группа $A \times B$ разрешима;

г) если $G/A \simeq B$ и A, B — разрешимые группы, то G разрешима.

62.12. Доказать разрешимость групп:

а) $\mathbf{S}_3$; б) $\mathbf{A}_4$; в) $\mathbf{S}_4$; г) $\mathbf{Q}_8$; д) $\mathbf{D}_n$.

62.13. Пусть $\mathbf{UT}_n(K)$ — группа верхних унитреугольных матриц. Доказать, что:

а) $\mathbf{UT}_n^m(K)$ (множество матриц из $\mathbf{UT}_n(K)$ с $m-1$ нулевыми диагоналями выше главной) — подгруппа в $\mathbf{UT}_n(K)$;

б) если $A \in \mathbf{UT}_n^i(K)$, $B \in \mathbf{UT}_n^j(K)$, то $[A, B] \in \mathbf{UT}_n^{(i+j)}(K)$;

в) группа $\mathbf{UT}_n(K)$ разрешима.

62.14. Доказать, что группа невырожденных верхних треугольных матриц разрешима.

62.15. Доказать, что конечная группа G разрешима тогда и только тогда, когда в ней имеется ряд подгрупп

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_k = \{e\}$$

такой, что H_{i+1} нормальна в H_i и H_i/H_{i+1} — (циклическая) группа простого порядка.

62.16. Доказать, что конечная p-группа разрешима.

62.17. Доказать разрешимость группы порядка pq, где p, q — различные простые числа.

62.18. Доказать разрешимость группы порядка:
а) 20; б) 12;
в) p^2q, где p, q — различные простые числа;
г) 42; д) 100; е) $n < 60$.

62.19. Доказать для трансвекций $t_{ij}(\alpha) = E + \alpha E_{ij}$ формулу

$$[t_{ik}(\alpha), t_{kj}(\beta)] = t_{ij}(\alpha\beta)$$

при различных i, j, k.

62.20. Пусть F — поле и $n \geqslant 3$. Доказать, что:
а) $\mathbf{SL}_n'(F) = \mathbf{GL}_n'(F) = \mathbf{SL}_n(F)$;
б) группы $\mathbf{SL}_n(F)$ и $\mathbf{GL}_n(F)$ не являются разрешимыми.

62.21. Пусть F — поле, содержащее не менее четырех элементов. Доказать, что:
а) $\mathbf{SL}_2'(F) = \mathbf{GL}_2'(F) = \mathbf{SL}_2(F)$;
б) группы $\mathbf{SL}_2(F)$ и $\mathbf{GL}_2(F)$ не являются разрешимыми.

* * *

62.22. Пусть p, q, r — различные простые числа. Доказать, что любая группа порядка pqr разрешима.

62.23. Пусть p, q, r — различные простые числа. Доказать, что неразрешимая группа порядка p^2qr изоморфна $\mathbf{A}_5$.

62.24. Если порядок конечной группы является произведением различных простых чисел, то G — разрешимая группа, обладающая такой циклической нормальной подгруппой N, что G/N — циклическая группа.

62.25. Пусть G — конечная группа, причем $G = G'$, центр G имеет порядок 2 и факторгруппа по центру изоморфна $\mathbf{A}_5$. Доказать, что $G \simeq \mathbf{SL}_2(\mathbf{Z}_5)$.

62.26. Пусть F — поле, V — n-мерное векторное пространство над F и G — группа невырожденных линейных операторов в V, причем, если $g \in G$, то $g = 1 + h$, где $h^n = 0$. Доказать, что:
а) в V существует такой вектор $x \neq 0$, что $gx = x$ для всех $g \in G$;
б) в V существует такой базис $e_1, \ldots, e_n$, что матрицы всех операторов g, $g \in G$ в этом базисе верхнетреугольные;
в) группа G разрешима.

62.27. Пусть p, q — простые числа, причем p делит $q-1$. Доказать, что:

а) существует целое $r \not\equiv 1 \pmod{q}$ такое, что $r^p \equiv 1 \pmod{q}$;

б) существует (с точностью до изоморфизма) ровно одна некоммутативная группа порядка pq.

62.28. Доказать, что:

а) если в коммутативной группе элементы a, b связаны соотношениями $a^3 = b^5 = (ab)^7 = e$, то $a = b = e$;

б) подгруппа, порожденная в $\mathbf{S}_7$ перестановками $(1\,2\,3)$ и $(1\,4\,5\,6\,7)$, не является разрешимой;

в) группа с порождающими элементами x_1, x_2 и определяющими соотношениями $x_1^3 = x_2^5 = (x_1 x_2)^7 = e$ не является разрешимой.

62.29. Разрешима ли свободная группа?

Глава 14

КОЛЬЦА

§ 63. Кольца и алгебры

63.1. Какие из следующих числовых множеств образуют кольцо относительно обычных операций сложения и умножения:

а) множество $\mathbb{Z}$;

б) множество $n\mathbb{Z}$ $(n > 1)$;

в) множество неотрицательных целых чисел;

г) множество $\mathbb{Q}$;

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

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

ж) множество рациональных чисел, в несократимой записи которых знаменатели являются степенями фиксированного простого числа p;

з) множество вещественных чисел вида $x + y\sqrt{2}$, где $x, y \in \mathbb{Q}$;

и) множество вещественных чисел вида $x + y\sqrt[3]{2}$, где $x, y \in \mathbb{Q}$;

к) множество вещественных чисел вида $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, где $x, y, z \in \mathbb{Q}$;

л) множество комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Z}$;

м) множество комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Q}$;

н) множество всевозможных сумм вида $a_1z_1 + a_2z_2 + \ldots + a_nz_n$, где $a_1, a_2, \ldots, a_n$ — рациональные числа, $z_1, z_2, \ldots, z_n$ — комплексные корни степени n из 1;

о) множество комплексных чисел вида $\dfrac{x + y\sqrt{D}}{2}$, где D — фиксированное целое число, *свободное от квадратов* (не делящееся на квадрат простого числа), x, y — целые числа одинаковой четности?

63.2. Какие из указанных множеств матриц образуют кольцо относительно матричного сложения и умножения:

а) множество вещественных симметрических матриц порядка n;

б) множество вещественных ортогональных матриц порядка n;

в) множество верхних треугольных матриц порядка $n \geqslant 2$;

г) множество матриц порядка $n \geqslant 2$, 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 — фиксированный элемент некоторого кольца K, $x, y \in K$;

ж) множество матриц вида $\dfrac{1}{2}\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}$, где D — фиксированное целое число, свободное от квадратов, x и y — целые числа одинаковой четности;

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

и) множество вещественных матриц вида

$$\begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix}?$$

63.3. Какие из следующих множеств функций образуют кольцо относительно обычных операций сложения и умножения функций:

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

б) множество функций, имеющих вторую производную на интервале (a, b);

в) множество целых рациональных функций вещественного переменного;

г) множество рациональных функций вещественного переменного;

д) множество функций вещественного переменного, обращающихся в 0 на некотором подмножестве $D \subseteq \mathbb{R}$;

е) множество тригонометрических многочленов

$$a_0 + \sum_{k=1}^{n} (a_k \cos kx + b_k \sin kx)$$

с вещественными коэффициентами, где n — произвольное натуральное число;

ж) множество тригонометрических многочленов вида

$$a_0 + \sum_{k=1}^{n} \cos kx$$

с вещественными коэффициентами, где n — произвольное натуральное число;

з) множество тригонометрических многочленов вида

$$a_0 + \sum_{k=1}^{n} a_k \sin kx$$

с вещественными коэффициентами, где n — произвольное натуральное число;

и) множество функций, определенных на некотором множестве D и принимающих значение в некотором кольце R;

к) все степенные ряды от одной или нескольких переменных;

л) все лорановские степенные ряды от одной переменной?

63.4. Во множестве многочленов от переменного t с обычным сложением рассматривается операция умножения, заданная правилом

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

Является ли это множество кольцом относительно заданного умножения и обычного сложения?

63.5. Образует ли кольцо множество всех подмножеств некоторого множества относительно симметрической разности и пересечения, рассматриваемых как сложение и умножение соответственно?

63.6. Доказать изоморфизм колец из задач:

а) 63.1, о) и 63.2, ж);

б) 63.2, з) и 63.2, и).

63.7. Какие из колец, указанных в задачах 63.1–63.5, содержат делители нуля?

63.8. Найти обратимые элементы в кольцах с единицей из задач 63.1–63.5.

63.9. Доказать, что одно из колец задач 63.3, д) и 63.3, е) изоморфно, а другое не изоморфно кольцу многочленов $\mathbb{R}[x]$.

63.10. Доказать, что все обратимые элементы кольца с единицей образуют группу относительно умножения.

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

а) $\mathbf{Z}_n$;

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

в) $K[x]/(fK[x])$, где K — поле;

г) верхних треугольных матриц над полем;

д) $\mathbf{M}_2(\mathbb{R})$;

е) всех функций, определенных на некотором множестве S и принимающих значения в поле K;

ж) всех степенных рядов от одной переменной;

з) $\mathbb{Z}$;

и) $\mathbb{Z}[i]$.

63.12. Доказать, что группа обратимых элементов $\mathbb{Z}[\sqrt{3}\,]^*$ бесконечна.

63.13. Пусть R — конечное кольцо. Доказать, что:

а) если R не содержит делителей нуля, то оно имеет единицу и все его ненулевые элементы обратимы;

б) если R имеет единицу, то каждый его элемент, имеющий односторонний обратный, обратим;

в) если R имеет единицу, то всякий левый делитель нуля является правым делителем нуля.

63.14. Доказать, что в кольце с единицей и без делителей нуля каждый элемент, имеющий односторонний обратный, является обратимым.

63.15. Пусть R — кольцо с единицей, $x, y \in R$. Доказать, что:

а) если произведения xy и yx обратимы, то элементы x и y также обратимы;

б) если R без делителей нуля и произведение xy обратимо, то x и y обратимы;

в) без дополнительных предположений о кольце R из обратимости произведения xy не следует обратимость элементов x и y;

г) если обратим элемент $1 + ab$, то обратим и элемент $1 + ba$.

63.16. Пусть R — прямая сумма колец $R_1, \ldots, R_k$.

а) При каких условиях R коммутативно; имеет единицу; не имеет делителей нуля?

б) Найти в R все обратимые элементы; все делители нуля; все нильпотентные элементы.

63.17. Доказать, что:

а) если числа k и l взаимно просты, то $\mathbf{Z}_{kl} = \mathbf{Z}_k \oplus \mathbf{Z}_l$;

б) если $n = p_1^{k_1} \ldots p_s^{k_s}$, где $p_1, \ldots, p_s$ — различные простые числа, то
$$\mathbf{Z}_n = \mathbf{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbf{Z}_{p_s^{k_s}};$$

в) если числа k и l взаимно просты, то $\varphi(kl) = \varphi(k)\varphi(l)$, где φ — функция Эйлера.

63.18. Найти все делители нуля в $\mathbb{C} \oplus \mathbb{C}$.

63.19. Доказать, что:

а) делитель нуля в произвольной (ассоциативной) алгебре не является обратимым;

б) в конечномерной алгебре с единицей всякий элемент, не являющийся делителем нуля, обратим;

в) конечномерная алгебра без делителей нуля является *телом* (алгеброй с делением).

63.20. Доказать, что:

а) конечномерная алгебра с единицей и без делителей нуля над полем $\mathbb{C}$ изоморфна $\mathbb{C}$;

б) над полем $\mathbb{C}$ не существует конечномерных алгебр с делением, отличных от $\mathbb{C}$.

63.21. Перечислить с точностью до изоморфизма все коммутативные двумерные алгебры над $\mathbb{C}$:

а) с единицей;

б) не обязательно с единицей.

63.22. Перечислить с точностью до изоморфизма все коммутативные двумерные алгебры над $\mathbb{R}$:

а) с единицей;

б) не обязательно с единицей.

63.23. Пусть $\mathbb{H}$ — тело кватернионов.

а) Является ли $\mathbb{H}$ алгеброй над полем $\mathbb{C}$, если умножение на скаляр $\alpha \in \mathbb{C}$ понимать как левое умножение на $\alpha \in \mathbb{H}$?

б) Доказать, что отображения

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

являются изоморфизмами $\mathbb{H}$ как алгебры над полем $\mathbb{R}$ на некоторую подалгебру в алгебре матриц $\mathbf{M}_2(\mathbb{C})$ над $\mathbb{R}$.

в) Доказать, что отображение $z \mapsto \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$ является изоморфным вложением поля $\mathbb{C}$ в алгебру $\mathbb{H}$, реализованную в виде подалгебры алгебры $\mathbf{M}_2(\mathbb{C})$ над $\mathbb{R}$ (см. б)).

г) Решить в $\mathbb{H}$ уравнение $x^2 = -1$.

63.24. *Тензорной алгеброй* $\mathbb{T}(V)$ векторного пространства V над полем K называется (бесконечномерное) векторное пространство

$$\mathbb{T}(V) = \bigoplus_{k=0}^{\infty} \mathbb{T}_k(V),$$

где $\mathbb{T}_0(V) = K$, $\mathbb{T}_k(V) = \underbrace{V \otimes \ldots \otimes V}_{k \text{ раз}}$ для любых $k, m > 0$, с умножением

$$f \cdot g = f \otimes g, \quad \text{где} \quad f \in T_k(V), \quad g \in T_m(V).$$

Доказать, что:

а) $\mathbb{T}(V)$ — ассоциативная алгебра с единицей над полем K;
б) в $\mathbb{T}(V)$ нет делителей нуля.

63.25. *Алгеброй Грассмана* $\Lambda(V)$ векторного пространства V над полем K называется векторное пространство

$$\Lambda(V) = \bigoplus_{k=0}^{\infty} \Lambda^k(V),$$

где $\Lambda^0(V) = K$, с умножением

$$f \cdot g = f \wedge g,$$

где $f \in \Lambda^k(V), \quad g \in \Lambda^m(V)$ для любых $k, m > 0$.

Доказать, что:
а) $\Lambda(V)$ является ассоциативной алгеброй с единицей над полем K;
б) каждый элемент из $I = \bigoplus\limits_{k \geqslant 1} \Lambda^k(V)$ является нильпотентным;
в) каждый элемент из $\Lambda(V)$, не лежащий в I, обратим.

63.26. *Симметрической алгеброй* $S(V)$ векторного пространства V над полем K называется векторное пространство

$$S(V) = \bigoplus_{k=0}^{\infty} S^k(V),$$

где $S^0(V) = k$, с умножением

$$f \cdot g = \mathrm{Sym}\,(f \otimes g),$$

где $\quad f \in S^k(V), \quad g \in S^m(V)$ для любых $k, m > 0$.

Доказать, что:
а) $S(V)$ является ассоциативной, коммутативной алгеброй над K;
б) если $x_1, \ldots, x_n$ — базис пространства V, то $S(V)$ изоморфно алгебре многочленов от $x_1, \ldots, x_n$.

63.27. Пусть A и B — алгебры над полем K. *Тензорное произведение* алгебр $C = A \otimes_K B$ определяется как тензорное произведение векторных пространств A и B над K с умножением

$$(a' \otimes b') \cdot (a'' \otimes b'') = a'a'' \otimes b'b''.$$

Доказать изоморфизм алгебр над полем K:
а) $\mathbb{C} \otimes_K \mathbb{C} \simeq \mathbb{C} \oplus \mathbb{C} \quad (K = \mathbb{R})$;
б) $\mathbf{M}_n(K) \otimes_K \mathbf{M}_m(K) \simeq \mathbf{M}_{mn}(K)$;
в) $\mathbf{M}_n(K) \otimes_K A \simeq \mathbf{M}_n(A)$, где A — произвольная ассоциативная алгебра над K;

г) $K[X_1, \ldots, X_n] \otimes_K K[Y_1, \ldots, Y_m] \simeq K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$;
д) $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbf{M}_2(\mathbb{C})$;
е) $\mathbf{S}(V) \otimes_K \Lambda(V) \simeq \mathbb{T}(V)$ при $\dim V = 2$;
ж) $\mathbb{Q}(\sqrt{p}\,) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q}\,) \simeq \mathbb{Q}(\sqrt{p} + \sqrt{q}\,)$, где p и q — различные простые числа.

63.28. Пусть K — поле характеристики нуль, $R = K[x_1, \ldots, x_n]$ — кольцо многочленов и p_i, q_i — линейные операторы на R как векторном пространстве над K, причем для $f \in R$

$$p_i(f) = x_i f, \qquad q_i(f) = \frac{\partial}{\partial x_i} f.$$

Обозначим через $A_n(K)$ подалгебру в алгебре линейных операторов в R, порожденную $p_1, \ldots, p_n, q_1, \ldots, q_n$. Она называется *алгеброй Вейля* или алгеброй дифференциальных операторов.

Доказать, что:
а) $q_j p_i - p_i q_j = \delta_{ij}, \quad p_i p_j = p_j p_i, \quad q_i q_j = q_j q_i$;
б) базис $A_n(K)$ как векторного пространства образуют одночлены

$$p_1^{l_1} \ldots p_n^{l_n} q_1^{t_1} \ldots q_n^{t_n}, \qquad l_i, t_j \geqslant 0.$$

63.29. Пусть $f = f(p_1, \ldots, p_n, q_1, \ldots, q_n)$ — элемент алгебры Вейля $A_n(K)$ (см. задачу 63.28.) Доказать, что

$$p_i f = f p_i + \frac{\partial f}{\partial q_i}, \qquad q_i f = f q_i - \frac{\partial f}{\partial p_i}.$$

63.30. Доказать, что алгебра верхних нильтреугольных матриц порядка n является нильпотентной алгеброй индекса n.

63.31. Доказать, что:
а) в кольце всех функций на отрезке $[0, 1]$ делителями нуля являются функции, принимающие нулевое значение, и только они;
б) в кольце непрерывных функций на отрезке $[0, 1]$ делителями нуля являются ненулевые функции, принимающие нулевое значение на некотором отрезке $[a, b]$, где $0 \leqslant a < b \leqslant 1$.

§ 64. Идеалы, гомоморфизмы, факторкольца

64.1. Найти все идеалы кольца:
а) $\mathbb{Z}$;
б) $K[x]$, где K — поле.

64.2. Доказать, что кольца:
а) $\mathbb{Z}[x]$;

б) $K[x, y]$, где K — поле;
не являются кольцами главных идеалов.

64.3. Доказать, что в кольце матриц над полем всякий двусторонний идеал либо нулевой, либо совпадает со всем кольцом.

64.4. Доказать, что в кольце матриц $\mathbf{M}_n(R)$ с элементами из произвольного кольца R идеалами являются в точности множества матриц, элементы которых принадлежат фиксированному идеалу кольца R.

64.5. Найти все идеалы кольца верхних треугольных матриц порядка 2 с целыми элементами.

64.6. Пусть I и J — множества матриц вида

$$\begin{pmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & l & 2m \\ 0 & 0 & 2n \\ 0 & 0 & 0 \end{pmatrix}$$

с целыми коэффициентами g, h, $k, \ldots$. Доказать, что I является идеалом в кольце R верхних треугольных матриц над $\mathbb{Z}$, J есть идеал кольца I, но J не является идеалом кольца R.

64.7. Найти все левые идеалы алгебры $\mathbf{M}_2(\mathbf{Z}_2)$.

64.8. Найти все идеалы двумерной алгебры L над полем $\mathbb{R}$ с базисом $(1, e)$, где 1 — единица в L, и:

а) $e^2 = 0$; б) $e^2 = 1$.

64.9. Доказать, что если идеал кольца содержит обратимый элемент, то он совпадает со всем кольцом.

64.10. Образуют ли идеал необратимые элементы колец:
а) $\mathbb{Z}$; б) $\mathbb{C}[x]$; в) $\mathbb{R}[x]$; г) $\mathbf{Z}_n$.

64.11. Доказать, что кольцо целых чисел не содержит минимальных идеалов.

64.12. Найти максимальные идеалы в кольцах:
а) $\mathbb{Z}$; б) $\mathbb{C}[x]$; в) $\mathbb{R}[x]$; г) $\mathbf{Z}_n$.

64.13. Доказать, что множество I_S непрерывных функций, обращающихся в 0 на фиксированном подмножестве $S \subseteq [a, b]$, является идеалом в кольце функций, непрерывных на $[a, b]$.

Верно ли, что всякий идеал этого кольца имеет вид I_S для некоторого $S \subseteq [a, b]$?

64.14. Пусть R — кольцо непрерывных функций на отрезке $[0, 1]$, $I_c = \{f(x) \in R \mid f(c) = 0\}$ $(0 \leqslant c \leqslant 1)$. Доказать, что:
а) I_c — максимальный идеал R;
б) всякий максимальный идеал R совпадает с I_c для некоторого c.

64.15. Доказать, что коммутативное кольцо с единицей (отличной от нуля), не имеющее идеалов, отличных от нуля и всего кольца, является полем. Существенно ли для этого утверждения наличие единицы?

64.16. Доказать, что кольцо с ненулевым умножением и без собственных односторонних идеалов является телом.

64.17. Доказать, что кольцо с единицей и без делителей нуля, в котором всякая убывающая цепочка левых идеалов конечна, является телом.

64.18. Пусть K — коммутативное кольцо без делителей нуля и отображение $\delta\colon\ K\setminus\{0\}\to\mathbb{N}$ удовлетворяет условию: для любых элементов a, $b\in K$, где $b\neq 0$, существуют элементы $q,r\in K$ такие, что $a=bq+r$ и $\delta(r)<\delta(b)$ или $r=0$.

Доказать, что существует отображение $\delta_1\colon\ K\setminus\{0\}\to\mathbb{N}$, удовлетворяющее как этому условию, так и условию: для любых $a,b\in K$, где $ab\neq 0$, $\delta_1(ab)\geqslant\delta(b)$.

64.19. Доказать, что:

а) кольцо целых гауссовых чисел вида $x+iy$ $(x,y\in\mathbb{Z})$ евклидово;

б) кольцо комплексных чисел вида $x+iy\sqrt{3}$ $(x,y\in\mathbb{Z})$ не является евклидовым;

в) кольцо комплексных чисел вида $\dfrac{x+iy\sqrt{3}}{2}$, где x и y — целые числа одинаковой четности, евклидово.

64.20. В кольце $\mathbb{Z}[i]$ разделить $a=40+i$ на $b=3-i$ с остатком относительно функции $\delta(x+iy)=x^2+y^2$ из задачи 64.18.

64.21. В кольце $\mathbb{Z}[i]$ найти наибольший общий делитель чисел $20+9i$ и $11+2i$.

64.22. Доказать, что всякую прямоугольную матрицу с элементами из евклидова кольца с помощью элементарных преобразований ее строк и столбцов можно привести к виду

$$\begin{pmatrix} e_1 & 0 & \ldots & 0 & 0 & \ldots & 0\\ 0 & e_2 & \ldots & 0 & 0 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & e_r & 0 & \ldots & 0\\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix},$$

где $e_1|e_2|\ldots|e_r$, $e_i\neq 0$ $(i=1,2\ldots,r)$.

64.23. Доказать, что в задаче 64.22 для $i = 1, \ldots, r$ произведение $e_1 \ldots e_i$ совпадает с наибольшим общим делителем всех миноров размера i исходной матрицы.

64.24. Доказать, что любое кольцо, заключенное между кольцом главных идеалов R и его полем частных Q, само является кольцом главных идеалов.

64.25. Доказать, что кольцо многочленов $R[x]$ над коммутативным кольцом R с единицей и без делителей нуля является кольцом главных идеалов тогда и только тогда, когда R — поле.

64.26. Найти все идеалы в алгебре рядов $\mathbb{C}[[x]]$ от одной переменной x.

64.27. Доказать, что алгебра Вейля $A_n(K)$ (см. задачу 63.28) проста, если K — поле нулевой характеристики.

64.28. (*Китайская теорема об остатках.*) Пусть A — коммутативное кольцо с единицей. Доказать, что:

а) если I_1 и I_2 — идеалы в A и $I_1 + I_2 = A$, то для любых элементов $x_1, x_2 \in A$ существует такой элемент $x \in A$, что $x - x_1 \in I_1$, $x - x_2 \in I_2$;

б) если $I_1, \ldots, I_n$ — идеалы в A и $I_i + I_j = A$ для всех $i \neq j$, то для любых элементов $x_1, \ldots, x_n \in A$ существует такой элемент $x \in A$, что $x - x_k \in I_k$ $(k = 1, \ldots, n)$.

64.29. Пусть R и S — кольца с единицей и $\varphi\colon\ R \to S$ — гомоморфизм.

а) Верно ли, что образ единицы кольца R является единицей кольца S?

б) Верно ли утверждение а), если гомоморфизм φ сюръективен?

64.30. Пусть K — поле и $K[x_1, \ldots, x_n]$ — алгебра многочленов. Предположим, что $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$.

Доказать, что:

а) отображение φ, при котором

$$\varphi(g(x_1, \ldots, x_n)) = g(f_1, \ldots, f_n),$$

является эндоморфизмом K-алгебры $K[x_1, \ldots, x_n]$;

б) если φ — автоморфизм $K[x_1, \ldots, x_n]$, то якобиан

$$J = \det\left(\frac{\partial f_i}{\partial x_j}\right)$$

является ненулевой константой;

в) если $h = h(x_2, \ldots, x_n)$, то отображение Ψ, при котором

$$\Psi(g(x_1, \ldots, x_n)) = g(x_1 + h, x_2, \ldots, x_n),$$

является автоморфизмом $K[x_1, \ldots, x_n]$.

64.31. Пусть K — поле и $K[[x_1 \ldots x_n]]$ — алгебра степенных рядов от $x_1, \ldots, x_n$. Предположим, что $f_1, \ldots, f_n \in K[[x_1 \ldots x_n]]$ имеют нулевые свободные члены.

Доказать, что:

а) отображение φ, при котором

$$\varphi(g(x_1, \ldots, x_n)) = g(f_1, \ldots, f_n),$$

является эндоморфизмом $K[[x_1, \ldots, x_n]]$;

б) отображение φ является автоморфизмом тогда и только тогда, когда якобиан

$$J = \det\left(\frac{\partial f_i}{\partial x_j}\right)$$

имеет ненулевой свободный член.

64.32. Пусть K — поле нулевой характеристики и $h = h(q_1) \in A_n(K)$. Доказать, что отображение φ, при котором

$$\varphi(f(p_1, \ldots, p_n, q_1, \ldots, q_n)) = f(p_1 + h, p_2, \ldots, p_n, q_1, \ldots, q_n),$$

является автоморфизмом K-алгебры $A_n(K)$.

64.33. Пусть φ — автоморфизм $\mathbb{C}$-алгебры $\mathbf{M}_n(\mathbb{C})$. Доказать, что:

а) левый аннулятор матрицы $\varphi(E_{nn})$ имеет размерность $n(n-1)$;

б) жорданова форма матрицы $\varphi(E_{nn})$ равна E_{11};

в) существует такая обратимая матрица Y, что

$$Y^{-1}\varphi(E_{nn})Y = E_{nn};$$

г) отображение $A \to Y^{-1}\varphi(A)Y$ является автоморфизмом $\mathbf{M}_n(\mathbb{C})$, переводящим $\mathbf{M}_{n-1}(\mathbb{C})$ в себя;

д) существует такая обратимая матрица X, что $\varphi(A) = XAX^{-1}$ для любой матрицы $A \in \mathbf{M}_n(\mathbb{C})$.

64.34. Пусть K — поле.

а) Доказать, что линейное отображение

$$\varphi\colon\ \mathbf{M}_n(K) \otimes_K \mathbf{M}_m(K) \to \mathbf{M}_{nm}(K),$$

где $1 \leqslant i, j \leqslant n$, $1 \leqslant r, s \leqslant m$ и

$$\varphi(E_{ij} \otimes E_{rs}) = E_{i+n(r-1),j+n(s-1)},$$

является изоморфизмом K-алгебр.

б) Доказать, что линейное отображение

$$\Psi\colon \mathbf{M}_n(K) \to \mathbf{M}_n(K) \otimes_K \mathbf{M}_n(K),$$

где

$$\Psi(E_{ij}) = E_{ij} \otimes E_{ij},$$

является гомоморфизмом K-алгебр. Найти $\operatorname{Ker}\Psi$.

64.35. Доказать, что образ коммутативного кольца при гомоморфизме является коммутативным кольцом.

64.36. Доказать, что отображение $\varphi\colon\ f(x) \to f(c)$ $(c \in \mathbb{R})$ является гомоморфизмом кольца вещественных функций, определенных на $\mathbb{R}$, на поле $\mathbb{R}$.

64.37. Найти все гомоморфизмы колец:

а) $\mathbb{Z} \to 2\mathbb{Z}$; б) $2\mathbb{Z} \to 2\mathbb{Z}$; в) $2\mathbb{Z} \to 3\mathbb{Z}$; г) $\mathbb{Z} \to \mathbf{M}_2(\mathbf{Z}_2)$.

64.38. Найти все гомоморфизмы:

а) группы $\mathbb{Z}$ в группу $\mathbb{Q}$;

б) кольца $\mathbb{Z}$ в поле $\mathbb{Q}$.

64.39. Доказать, что любой гомоморфизм поля в кольцо является или нулевым, или изоморфным отображением на некоторое подполе.

64.40. Пусть K — поле и $R = K[x_1, \ldots, x_n]$ — алгебра многочленов от $x_1, \ldots, x_n$ над полем K. Построить биекцию между пространством строк K^n и множеством всех гомоморфизмов K-алгебр $R \to K$.

64.41. Доказать, что:

а) $F[x]/\langle x - \alpha\rangle \simeq F$ (F — поле);

б) $\mathbb{R}[x]/\langle x^2 + 1\rangle \simeq \mathbb{C}$;

в) $\mathbb{R}[x]/\langle x^2 + x + 1\rangle \simeq \mathbb{C}$.

64.42. При каких a и b факторкольца $\mathbf{Z}_2[x]/\langle x^2 + ax + b\rangle$

а) изоморфны между собой;

б) являются полями?

64.43. Изоморфны ли факторкольца

$$\mathbb{Z}[x]/\langle x^3 + 1\rangle, \qquad \mathbb{Z}[x]/\langle x^3 + 2x^2 + x + 1\rangle?$$

64.44. Изоморфны ли факторкольца
$$\mathbb{Z}[x]/\langle x^2-2\rangle, \qquad \mathbb{Z}[x]/\langle x^2-3\rangle?$$

64.45. Пусть a и b — различные элементы поля F. Доказать, что $F[x]$-модули
$$F[x]/\langle x-a\rangle, \qquad F[x]/\langle x-b\rangle \simeq F$$
не изоморфны, но соответствующие факторкольца изоморфны.

64.46. Доказать, что если $a\neq b$ и $c\neq d$ — элементы поля F, то факторкольца
$$F[x]/\langle (x-a)(x-b)\rangle F, \qquad F[x]/\langle (x-c)(x-d)\rangle$$
изоморфны.

64.47. Какие из следующих алгебр изоморфны над $\mathbb{C}$:
$$A_1=\mathbb{C}[x,y]/\langle x-y, xy-1\rangle, \qquad A_2=\mathbb{C}[x]/\langle (x-1)^2\rangle,$$
$$A_3=\mathbb{C}\oplus\mathbb{C}, \qquad A_4=\mathbb{C}[x,y], \qquad A_5=\mathbb{C}[x]/\langle x^2\rangle?$$

64.48. Изоморфны ли алгебры A и B над полем $\mathbb{C}$:
а) $A=\mathbb{C}[x,y]/\langle x^n-y\rangle, \quad B=\mathbb{C}[x,y]/\langle x-y^m\rangle$;
б) $A=\mathbb{C}[x,y]/\langle x^2-y^2\rangle, \quad B=\mathbb{C}[x,y]/\langle (x-y)^2\rangle$?

64.49. Изоморфны ли следующие алгебры над полем $\mathbb{R}$:
а) $A=\mathbb{R}[x]/\langle x^2+x+1\rangle, \quad B=\mathbb{R}[x]/\langle 2x^2-3x+3\rangle$;
б) $A=\mathbb{R}[x]/\langle x^2+2x+1\rangle, \quad B=\mathbb{R}[x]/\langle (x^2-3x+2\rangle$?

64.50. Доказать, что элемент f алгебры $K[x]/\langle x^{n+1}\rangle$ (K — поле) обратим тогда и только тогда, когда $f(0)\neq 0$.

64.51. Пусть K — поле и $f\in K[x]$ имеет степень n. Доказать, что размерность K-алгебры $K[x]/fK[x]$ равна n.

64.52. Пусть K — поле. Доказать, что:
а) если многочлены $f,g\in K[x]$ взаимно просты, то
$$K[x]/fgK[x]\simeq K[x]/fK[x]\oplus K[x]/gK[x];$$
б) если $f=p_1^{k_1}\ldots p_s^{k_s}$, где $p_1,\ldots,p_s$ — взаимно простые неприводимые многочлены, то
$$K[x]/fK[x]\simeq K[x]/p_1^{k_1}K[x]\oplus\ldots\oplus K[x]/p_s^{k_s}K[x].$$

64.53. Доказать, что факторкольцо R/I коммутативного кольца с единицей является полем тогда и только тогда, когда I — максимальный идеал в R.

64.54. Доказать, что идеал I коммутативного кольца R является простым тогда и только тогда, когда I — ядро гомоморфизма R в некоторое поле.

64.55. Доказать, что:

а) факторкольцо $\mathbb{Z}[i]/\langle 2\rangle$ не является полем;

б) факторкольцо $\mathbb{Z}[i]/\langle 3\rangle$ является полем из девяти элементов;

в) $\mathbb{Z}[i]/\langle n\rangle$ является полем тогда и только тогда, когда n — простое число, не равное сумме квадратов двух целых чисел.

64.56. При каких $a \in \mathbb{F}_7$ факторкольцо $\mathbb{F}_7[x]/\langle x^2 + a\rangle$ является полем?

64.57. Доказать, что при любом целом $n > 1$ факторкольцо $\mathbb{Z}[x]/\langle n\rangle$ изоморфно $\mathbf{Z}_n[x]$.

64.58. Пусть $f(x)$ — неприводимый многочлен степени n из кольца $\mathbf{Z}_p[x]$. Доказать, что факторкольцо $\mathbf{Z}_p[x]/\langle f(x)\rangle$ является конечным полем, и найти число его элементов.

64.59. Доказать, что:

а) всякое кольцо изоморфно подкольцу некоторого кольца с единицей;

б) n-мерная алгебра с единицей над полем F изоморфна подалгебре алгебры с единицей размерности $n+1$;

в) n-мерная алгебра с единицей над полем K изоморфна некоторой подалгебре алгебры $\mathbf{M}_n(K)$;

г) n-мерная алгебра над K изоморфна подалгебре алгебры $\mathbf{M}_{n+1}(K)$.

64.60. Пусть $I_1, \ldots, I_s$ — идеалы в алгебре с единицейA, $I_i + I_j = A$ при $i \neq j$. Доказать, что отображение

$$f\colon\ A\Big/\bigcap_{k=1}^{s} I_k \mapsto A/I_1 \oplus \ldots \oplus A/I_s,$$

задаваемое формулой

$$f\Big(a + \bigcap_{k=1}^{s} I_k\Big) = (a + I_1, \ldots, a + I_s),$$

является изоморфизмом алгебр.

64.61. Установить изоморфизм $\mathbb{Q}[x]/\langle x^2-1\rangle \simeq \mathbb{Q}\oplus\mathbb{Q}$.

64.62. Доказать, что

$$\mathbb{Q}[x]/\langle x^2-2\rangle \simeq \mathbb{Q}[\sqrt{2}\,].$$

64.63. Пусть I — максимальный идеал в $\mathbb{Z}[x]$. Доказать, что $\mathbb{Z}[x]/I$ — конечное поле.

64.64. Пусть V — векторное пространство над полем K нулевой характеристики. Доказать, что

$$S(V) \simeq \mathbb{T}(V)/I,$$

где I — идеал в $T(V)$, порожденный всеми элементами

$$x\otimes y - y\otimes x, \quad \text{где} \quad x, y \in V.$$

64.65. Пусть V — векторное пространство над полем K нулевой характеристики. Доказать, что

$$\Lambda(V) \simeq \mathbb{T}(V)/I,$$

где I — идеал в $\mathbb{T}(V)$, порожденный всеми элементами

$$x\otimes y + y\otimes x, \quad \text{где} \quad x, y \in V.$$

64.66. Пусть V — векторное пространство размерности $2n$ с базисом $p_1\ldots p_n, q_1\ldots q_n$ над полем K нулевой характеристики. Доказать, что

$$A_n(K) \simeq T(V)/I,$$

где I — идеал в $T(V)$, порожденный всеми элементами

$$p_i\otimes q_j - q_j\otimes p_i - \delta_{ij}, \quad p_i\otimes p_j - p_j\otimes p_i, \quad q_i\otimes q_j - q_j\otimes q_i.$$

64.67. Пусть $(e_1,\ldots,e_n)$ — базис векторного пространства V над полем K характеристики, отличной от 2, и $\Lambda(V)$ — внешняя (или грассманова алгебра) над векторным пространством V.

Доказать, что:

а) $\dim\Lambda(V) = 2^n$;

б) если $x_1,\ldots,x_{n+1}\in\Lambda^1(V)\oplus\ldots\oplus\Lambda^n(V)$, то $x_1\times\ldots\times x_{n+1} = 0$;

в) формула

$$\varphi(e_i) = \sum_{j=1}^{n} a_{ij} e_j + \omega_i, \qquad i = 1, \ldots, n,$$

где $\omega_i \in \Lambda^1(V) \oplus \ldots \oplus \Lambda^n(V)$, задает автоморфизм тогда и только тогда, когда $\det(a_{ij}) \neq 0$.

64.68. Пусть R — кольцо с единицей. *Левым аннулятором* подмножества $M \subseteq R$ называется множество

$$\{x \in R \mid xm = 0 \quad \text{для всякого} \quad m \in M\}.$$

Доказать, что:

а) левый аннулятор любого подмножества является в R левым идеалом;

б) левый аннулятор правого идеала кольца R, порожденного идемпотентом, также порождается (как левый идеал) некоторым идемпотентом.

64.69. Доказать, что сумма левых идеалов, порожденных попарно ортогональными идемпотентами, также порождается идемпотентом.

64.70. Пусть I_k $(k = 1, \ldots, n)$ — множество матриц порядка n над полем K, состоящее из матриц, у которых вне k-го столбца все элементы равны 0.

Доказать, что:

а) I_k — левый идеал $\mathbf{M}_n(K)$;

б) I_k — минимальный подмодуль в $\mathbf{M}_n(K)$, рассматриваемый как левый модуль над собой;

в) $\mathbf{M}_n(K) = I_1 \oplus \ldots \oplus I_n$;

г) модуль $\mathbf{M}_2(K)$ обладает разложением в прямую сумму минимальных подмодулей, отличным от разложения в);

д) между двумя этими разложениями модуля $\mathbf{M}_2(K)$ существует модульный изоморфизм.

64.71. Пусть R — алгебра всех линейных операторов в конечномерном векторном пространстве V и J_L — множество всех операторов из R, образ которых лежит в подпространстве L. Доказать, что J_L является правым идеалом в R.

Обратно, пусть J — левый идеал в R. Доказать, что существует, и притом единственное, такое подпространство L в V, что $J = J_L$.

64.72. Пусть R — алгебра всех линейных операторов в конечномерном векторном пространстве V и I_L — множество всех операторов из R, ядро которых содержит подпространство L. Доказать, что I_L является левым идеалом в R.

Обратно, пусть I — левый идеал в R. Доказать, что существует, и притом единственное, такое подпространство L в V, что $I = I_L$.

64.73. Доказать, что множества матриц:

а) $I = \left\{ \begin{pmatrix} x & 2x \\ y & 2y \end{pmatrix} \quad (x, y \in K) \right\}, \quad J = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \quad (x, y \in K) \right\};$

б) $I = \left\{ \begin{pmatrix} -x & 3x \\ -y & 3y \end{pmatrix} \quad (x, y \in K) \right\}, \quad J = \left\{ \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \quad (x, y \in K) \right\};$

являются подмодулями кольца $\mathbf{M}_2(K)$ как левого модуля над собой и $\mathbf{M}_2(K)/I \simeq J$.

64.74. Пусть $R = I_1 \oplus I_2$ — разложение кольца с единицей e в прямую сумму двусторонних идеалов I_1, I_2 и $e = e_1 + e_2$, где $e_1 \in I_1$, $e_2 \in I_2$. Доказать, что e_1 и e_2 — единицы колец I_1 и I_2.

64.75. Доказать, что кольца $\mathbf{Z}_{mn}$ и $\mathbf{Z}_m \oplus \mathbf{Z}_n$ изоморфны тогда и только тогда, когда m и n взаимно просты.

64.76. Кольцо называется *вполне приводимым справа*, если оно является прямой суммой правых идеалов, являющихся простыми модулями над этим кольцом. При каких n кольцо вычетов $\mathbf{Z}_n$ вполне приводимо?

64.77. Доказать, что алгебра всех верхних треугольных матриц порядка $n \geqslant 2$ над полем не является вполне приводимой.

64.78. Доказать, что в коммутативном вполне приводимом кольце с единицей число идемпотентов и число идеалов конечны.

64.79. Доказать, что во всякой вполне приводимой алгебре пересечение всех максимальных идеалов равно нулю.

64.80. Доказать, что всякое коммутативное вполне приводимое кольцо с единицей изоморфно прямой сумме полей.

64.81. Модуль называется *вполне приводимым*, если его можно разложить в прямую сумму минимальных подмодулей. Какие циклические группы вполне приводимы как модули над кольцом $\mathbb{Z}$?

64.82. Кольцо называется *вполне приводимым слева*, если оно вполне приводимо как левый модуль над собой. Доказать, что если кольцо R вполне приводимо слева и I — его левый идеал, то $R = I \oplus J$ для некоторого левого идеала J кольца R.

64.83. Доказать, что всякий левый идеал вполне приводимого слева кольца R:

а) вполне приводим как левый модуль над R;

б) порождается идемпотентом.

64.84. Пусть R — вполне приводимое слева кольцо с единицей.

Доказать, что:

а) если R не содержит идемпотентов, отличных от 0 и 1, то R — тело;

б) если R не содержит делителей нуля, то R — тело.

Верны ли эти утверждения для колец, в которых существование единицы заранее не предположено?

64.85. Доказать, что если $xy = 0$ для любых двух элементов x, y левого идеала I вполне приводимого слева кольца R с единицей, то $I = \{0\}$.

64.86. Доказать, что если I — идеал кольца R с единицей, то факторкольцо R/I тоже имеет единицу.

64.87. Доказать, что факторкольцо коммутативного нётерова кольца также нётерово.

64.88. Доказать, что кольцо вычетов $\mathbf{Z}_{p_1 \ldots p_m}$, где $p_1, \ldots, p_m$ — различные простые числа, является прямой суммой полей.

64.89. Найти все подмодули в векторном пространстве с базисом $(e_1, \ldots, e_n)$ как модули над кольцом всех диагональных матриц, если

$$\operatorname{diag}(\lambda_1, \ldots, \lambda_n) \circ (\alpha_1 e_1 + \ldots + \alpha_n e_n) = \lambda_1 \alpha_1 e_1 + \ldots + \lambda_n \alpha_n e_n.$$

64.90. Пусть R — коммутативное кольцо с единицей и без делителей нуля, рассматриваемое как модуль над собой. Доказать, что R изоморфно любому своему ненулевому подмодулю тогда и только тогда, когда R — кольцо главных идеалов.

64.91. Доказать, что правило

$$h(x) \circ f = h(x^r) f,$$

где $h(x)$ — фиксированный многочлен, превращает кольцо многочленов $F[x]$ над полем F в свободный модуль ранга r над $F[x]$.

64.92. Пусть в кольце R нет делителей нуля и M — свободный R-модуль. Доказать, что если $r \in R \setminus 0$ и $m \in M \setminus 0$, то $rm \neq 0$.

64.93. Пусть R — кольцо с единицей, причем все R-модули свободны. Доказать, что R является телом.

* * *

64.94. Пусть K — поле нулевой характеристики. Доказать, что алгебра полиномов $K[x_1, \ldots, x_n]$ является простым модулем над алгеброй Вейля $A_n(K)$ (см. задачу 63.28).

64.95. Пусть K — поле нулевой характеристики. Доказать, что каждый ненулевой модуль над алгеброй Вейля $A_n(K)$ имеет бесконечную размерность над K.

64.96. Пусть K — алгебра вещественных функций на отрезке $[-\pi, \pi]$, представимых многочленами от $\cos x$, $\sin x$ с вещественными коэффициентами.

Доказать, что:

а) K является областью;

б) $K \simeq \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$;

в) поле частных для K изоморфно полю рациональных функций $\mathbb{R}(T)$.

§ 65. Специальные классы алгебр

65.1. Доказать, что кольцо многочленов от одного переменного над коммутативным нётеровым кольцом с единицей является нётеровым.

65.2. Доказать, что алгебра многочленов от конечного числа переменных над полем нётерова.

65.3. *Алгебра $A(\alpha, \beta)$ обобщенных кватернионов* над полем F характеристики, отличной от 2, где $\alpha, \beta \in F^*$, определяется как векторное пространство над F с базисом $(1, i, j, k)$ и таблицей умножения

$$1 \cdot 1 = 1, \qquad 1 \cdot i = i \cdot 1 = i$$
$$1 \cdot j = j \cdot 1 = j, \qquad 1 \cdot k = k \cdot 1 = k,$$
$$i^2 = -\alpha, \qquad j^2 = -\beta, \qquad ij = -ji = k.$$

Доказать, что:

а) $A(\alpha, \beta)$ — (ассоциативная) центральная простая алгебра над полем F;

б) отображение

$$x = x_0 + x_1 i + x_2 j + x_3 k \mapsto x_0 - x_1 i - x_2 j - x_3 k = \overline{x}$$

является *инволюцией* (т. е. для любых $x, y \in A(\alpha, \beta)$ выполняются равенства $\overline{x + y} = \overline{x} + \overline{y}$, $\overline{xy} = \overline{y}\,\overline{x}$, $\overline{\overline{x}} = x$);

в) для любого $x \in A(\alpha, \beta)$

$$x^2 - (\operatorname{tr} x)x + N(x) = 0,$$

где $\operatorname{tr} x = x + \overline{x}$ и $N(x) = x\overline{x}$ — элементы поля F;

г) алгебра $A(\alpha, \beta)$ является телом тогда и только тогда, когда норменное уравнение $N(x) = 0$ имеет в ней только нулевое решение;

д) алгебра $A(\alpha, \beta)$ является либо телом, либо изоморфна алгебре матриц $\mathbf{M}_2(F)$ — в соответствии с существованием или отсутствием в ней делителей нуля;

е) если норменное уравнение имеет в алгебре $A(\alpha, \beta)$ ненулевое решение, то оно имеет решение и во множестве ненулевых чистых кватернионов;

ж) подалгебра $F(a)$, порожденная элементом a алгебры $A(\alpha, \beta)$, является коммутативной алгеброй размерности $\leqslant 2$ над F, и если a не является делителем нуля, то $F(a)$ — поле, изоморфное полю разложения многочлена $x^2 - (\operatorname{tr} a)x + N(a)$;

з) (*теорема Витта*) норма $N(x)$ является квадратичной формой ранга 3 на пространстве чистых кватернионов, и, обратно, каждой квадратичной форме ранга 3 на трехмерном векторном пространстве W над полем F соответствует алгебра обобщенных кватернионов, определяемая как векторное пространство $F \oplus W$ с правилами умножения

$$1 \cdot w = w \cdot 1,$$
$$w_1 \cdot w_2 = -Q(w_1, w_2) \cdot 1 + [w_1, w_2],$$

где Q — билинейная форма на W, ассоциированная с данной квадратичной формой, $[w_1, w_2]$ — векторное произведение элементов пространства W;

и) приведенная конструкция устанавливает биективное соответствие между кватернионными алгебрами над полем F (с точностью до изоморфизма) и классами эквивалентности квадратичных форм ранга 3 на трехмерном векторном пространстве над F. (Формы $Q\colon\ W \times W \to F$ и $Q'\colon\ W' \times W' \to F$ называются *эквивалентными*, если существуют изоморфизм $\alpha\colon\ W \to W'$ и элемент $\lambda \in F^*$ такие, что $Q'(\alpha(x), \alpha(y)) = \lambda Q(x, y)$ для любых $x, y \in W$.)

65.4. Конечномерная алгебра называется *полупростой*, если она не содержит ненулевых нильпотентных идеалов.

Доказать, что:

а) факторалгебра $\mathbb{C}[x]/\langle f(x) \rangle$ полупроста тогда и только тогда, когда многочлен $f(x)$ не имеет кратных корней;

б) алгебра, порожденная полем $\mathbb{C}$ и матрицей A в алгебре $\mathbf{M}_n(\mathbb{C})$, полупроста тогда и только тогда, когда минимальный многочлен матрицы A не имеет кратных корней;

в) конечномерная алгебра над полем полупроста тогда и только тогда, когда она вполне приводима слева;

г) коммутативная полупростая алгебра с единицей изоморфна прямой сумму полей;

д) если все идемпотенты полупростой алгебры лежат в центре, то алгебра является прямой суммой нескольких тел.

65.5. Пусть $H = (h_{ij})$ — симметрическая $(n \times n)$-матрица над полем F. *Алгеброй Клиффорда* называется 2^n-мерное пространство $\mathbb{C}(F, H)$ над F с базисом, составленным из символов

$$e_{i_1 \ldots i_k} \quad (1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n) \quad \text{и} \quad e_0 = 1,$$

и с умножением, определяемым правилами

$$e_i e_i = h_{ii}, \qquad e_0 e_i = e_i e_0 = e_i, \qquad e_i e_j + e_j e_i = h_{ij},$$
$$e_{i_1 \ldots i_k} = e_{i_1} \ldots e_{i_k} \qquad (1 \leqslant i_1 < \ldots < i_k \leqslant n).$$

Если V — n-мерное векторное пространство с базисом $(e_1, \ldots, e_n)$ и квадратичной формой Q, то алгебра Клиффорда $\mathbb{C}_Q(F)$ квадратичной формы Q определяется как алгебра $\mathbb{C}(F, H)$, где $h_{ij} = Q(e_i, e_j)$.

а) Доказать, что если $H = 0$, то $\mathbb{C}(F, H) \simeq \Lambda(V)$.

б) *Четной алгеброй Клиффорда* $\mathbb{C}^+(F, H)$ (или $\mathbb{C}^+{}_Q(F)$) называется подалгебра алгебры Клиффорда, порожденная элементами $e_{i_1} \ldots e_{i_{2m}}$ $(m = 0, 1, \ldots, [n/2])$. Доказать, что четная алгебра Клиффорда квадратичной формы

$$Q(x_1, x_2, x_3) = h_{11} x_1^2 + h_{12} x_1 x_2 + h_{22} x_2^2,$$

не распадающаяся в F на линейные множители, является квадратичным расширением поля F, изоморфным полю разложения

$$F(\sqrt{h_{12}^2 - 4 h_{11} h_{22}}\,)$$

формы Q.

в) Доказать, что при $\operatorname{char} F \neq 2$ четная алгебра Клиффорда квадратичной формы Q на трехмерном векторном пространстве V изоморфна алгебре обобщенных кватернионов формы $Q^{(2)}$ на трехмерном векторном пространстве $W = \Lambda^2 V$ (см. задачу 65.3).

г) В условиях задачи в) доказать, что квадратичная форма

$$N(x) = x\overline{x}$$

на пространстве чистых кватернионов эквивалентна форме λQ $(\lambda \in F^*)$.

65.6. Пусть $A = A_0 \oplus A_1$ — 2-градуированная ассоциативная алгебра над полем K, т. е. $A_i A_j \subset A_{i+j}$ (сложение индексов по модулю 2).

Определим в A новую операцию, полагая

$$[x, y] = xy - (-1)^{ij} yx,$$

где $x \in A_i$, $y \in A_j$.

а) Доказать, что для любых однородных элементов $x \in A_i$, $y \in A_j$, $z \in A$ имеем

$$[x, y] = (-1)^{ij}[y, x],$$
$$[x, [y, z]] + [y, [z, x]] + (-1)^{ij+1}[z, [x, y]] = 0.$$

Алгебра с 2-градуировкой, для которой однородные элементы удовлетворяют данным соотношениям, называется *супералгеброй Ли*.

б) Пусть V — n-мерное векторное пространство с базисом $(e_1, \ldots \ldots, e_n)$ над полем K характеристики, не равной 2, и $\Lambda(V)$ — внешняя алгебра на V, I — тождественный оператор на V, $L_0 = = K \cdot I$ и L_1 — линейная оболочка операторов φ_i и ψ_i, где

$$\varphi_i(w) = w \wedge e_i,$$
$$\psi_i(e_{i_1} \wedge \ldots \wedge e_{i_p}) = \begin{cases} (-1)^{p-k} e_{i_1} \wedge \ldots \wedge \widehat{e}_{i_k} \wedge \ldots \wedge e_{i_p}, & \text{если } i_k = i, \\ 0, \quad \text{если } i_k \neq i \text{ для всех } k = 1, \ldots, p. \end{cases}$$

Доказать, что $L = L_0 \oplus L_1$ является супералгеброй Ли относительно операции, введенной в а).

65.7. Пусть K — расширение поля $\mathbb{Q}$ степени n.

Доказать, что:

а) для любого многочлена $f(x) \in \mathbb{Q}[x]$ степени n найдется матрица A порядка n, для которой $f(A) = 0$;

б) алгебра $\mathbf{M}_n(\mathbb{Q})$ содержит подалгебру, изоморфную K;

в) если L — подалгебра в $\mathbf{M}_n(\mathbb{Q})$, являющаяся полем, то

$$[L : Q] \leqslant n.$$

65.8. Имеет ли делители нуля $\mathbb{C}$-алгебра аналитических функций, определенных в области $U \subseteq \mathbb{C}$?

65.9. Функция комплексного переменного называется *целой*, если она аналитична на всей комплексной плоскости. Доказать, что всякий конечно порожденный идеал алгебры целых функций является главным.

65.10. *Дифференцированием* кольца R называется отображение $D : R \to R$, удовлетворяющее условиям

$$D(x + y) = D(x) + D(y),$$

$$D(xy) = D(x)y + xD(y), \quad x, y \in R.$$

Найти все дифференцирования колец:
а) $\mathbb{Z}$; б) $\mathbb{Z}[x]$; в) $\mathbb{Z}[x_1, x_2, \ldots, x_n]$.

65.11. Множество L с операцией сложения, относительно которой L является коммутативной группой, и операцией умножения $\circ$, связанной со сложением законами дистрибутивности, называется *кольцом Ли*, если для любых $x, y, z \in L$ выполняются равенства

$$x \circ x = 0,$$
$$(x \circ y) \circ z + (y \circ z) \circ x + (z \circ x) \circ y = 0 \quad (\textit{тождество Якоби}).$$

Доказать, что:
а) в кольце Ли выполняется тождество $x \circ y = -y \circ x$;
б) векторы трехмерного пространства образуют кольцо Ли относительно сложения и векторного умножения;
в) всякое кольцо R является кольцом Ли относительно сложения и операции $x \circ y = xy - yx$;
г) множество всех дифференцирований кольца R является кольцом Ли относительно сложения и операции $D_1 \circ D_2 = D_1D_2 - D_2D_1$.

65.12. Пусть K — поле и D — дифференцирование K-алгебры матриц $\mathbf{M}_n(K)$. Доказать, что существует такая матрица $A \in \mathbf{M}_n(K)$, что $D(X) = AX - XA$ для всех X.

65.13. Пусть K — поле нулевой характеристики и D — дифференцирование алгебры Вейля $A_n(K)$. Доказать, что существует такой элемент $f \in A_n(K)$, что $D(g) = fg - gf$ для любого $g \in A_n(K)$.

65.14. Доказать, что полугрупповое кольцо $R[S]$ упорядоченной полугруппы S не имеет делителей нуля тогда и только тогда, когда кольцо R не имеет делителей нуля.

65.15. Пусть p — простое число и $\mathbb{Z}_p$ — кольцо целых p-адических чисел, т. е. множество всех формальных рядов $\sum_{i\geqslant 0} a_ip^i$, где $a_i \in \mathbb{Z}$ и $0 \leqslant a_i < p$. При этом

$$\sum_{i\geqslant 0} a_ip^i + \sum_{i\geqslant 0} b_ip^i = \sum_{i\geqslant 0} c_ip^i,$$
$$\Big(\sum_{i\geqslant 0} a_ip^i\Big)\Big(\sum_{i\geqslant 0} b_ip^i\Big) = \sum_{i\geqslant 0} d_ip^i,$$

если для любого $n \geqslant 0$ в $\mathbf{Z}_{p^n}$

$$\sum_{i=0}^{n-1} a_i p^i + \sum_{i=0}^{n-1} b_i p^i = \sum_{i=0}^{n-1} c_i p^i,$$

$$\Big(\sum_{i=0}^{n-1} a_i p^i\Big)\Big(\sum_{i=0}^{n-1} b_i p^i\Big) = \sum_{i=0}^{n-1} d_i p^i.$$

Доказать, что:

а) $\mathbb{Z}_p$ — кольцо без делителей нуля, содержащее $\mathbb{Z}$;

б) элемент $\sum_{i\geqslant 0} a_i p^i$ обратим в $\mathbb{Z}_p$ тогда и только тогда, когда $a_0 = 1, 2, \ldots, p-1$;

в) естественный гомоморфизм групп обратимых элементов $\mathbb{Z}_p^* \to \mathbf{Z}_{p^n}^*$ сюръективен при любом n;

г) каждый идеал в $\mathbb{Z}_p$ главный и имеет вид (p^n), $n \geqslant 0$;

д) найти все простые элементы в $\mathbb{Z}_p$.

65.16.

а) Доказать, что поле p-адических чисел $\mathbb{Q}_p$, т. е. поле частных $\mathbb{Z}_p$, состоит из элементов вида $p^m h$, где $m \in \mathbb{Z}$, $h \in \mathbb{Z}_p$.

б) Показать, что $\mathbb{Q}$ содержится в $\mathbb{Q}_p$ в качестве подполя.

в) Доказать, что элемент $p^m\Big(\sum_{i\geqslant 0} a_i p^i\Big)$ из $\mathbb{Q}_p$, где $0 \leqslant a_i \leqslant p-1$, для некоторого $m \geqslant 1$ лежит в $\mathbb{Q}$ тогда и только тогда, когда, начиная с некоторого N, элементы a_i, $i \geqslant N$, образуют периодическую последовательность.

г) Найти в $\mathbb{Q}_5$ образы элементов $2/7$ и $1/3$.

65.17. Пусть K — поле, p — неприводимый многочлен от одной переменной X с коэффициентами в K. Построить по аналогии с задачей 65.15 кольцо $K[X]_p$ и его поле частных $K(X)_p$. Показать, что если p имеет степень 1, то $K[X]_p \simeq K[[X]]$.

65.18. Найти все подкольца поля рациональных чисел $\mathbb{Q}$, содержащие единицу.

§ 66. Поля

66.1. Какие из колец в задачах 63.1–63.3 являются полями?

66.2. Какие из следующих множеств матриц образуют поле относительно обычных матричных операций:

а) $\left\{\begin{pmatrix} x & y \\ ny & x \end{pmatrix};\quad x, y \in \mathbb{Q}\right\}$, где n — фиксированное целое число;

б) $\left\{\begin{pmatrix} x & y \\ ny & x \end{pmatrix};\quad x, y \in \mathbb{R}\right\}$, где n — фиксированное целое число;

в) $\left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix}; \quad x, y \in \mathbf{Z}_p \right\}$, где $p = 2, 3, 5, 7$?

66.3. Пусть K — поле и F — поле дробей алгебры формальных степенных рядов $K[[x]]$. Доказать, что каждый элемент из F представляется в виде $x^{-s}h$, где $s \geqslant 0$ и $h \in K[[x]]$.

66.4. Доказать, что порядок единицы поля в его аддитивной группе либо бесконечен, либо является простым числом.

66.5. Для каких чисел $n = 2, 3, 4, 5, 6, 7$ существует поле из n элементов?

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

66.7. Доказать, что поля $\mathbb{Q}$ и $\mathbb{R}$ не имеют автоморфизмов, отличных от тождественного.

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

66.9. Имеет ли поле $\mathbb{Q}(\sqrt{2})$ автоморфизмы, отличные от тождественного?

66.10. Доказать, что в поле F характеристики p:

а) справедливо тождество

$$(x+y)^{p^m} = x^{p^m} + y^{p^m} \quad (m \text{ — натуральное число});$$

б) если F конечно, то отображение $x \mapsto x^p$ является автоморфизмом.

66.11. Доказать, что если комплексное число z не является вещественным, то кольцо $\mathbb{R}[z]$ совпадает с полем $\mathbb{C}$.

66.12. При каких $m, n \in \mathbb{Z} \setminus \{0\}$ поля $\mathbb{Q}(\sqrt{m})$ и $\mathbb{Q}(\sqrt{n})$ изоморфны?

66.13. Доказать, что для любого автоморфизма φ поля K множество элементов, неподвижных относительно φ, является подполем.

66.14. Доказать, что любые два поля из четырех элементов изоморфны.

66.15. Существует ли поле, строго содержащее поле комплексных чисел?

66.16. Доказать, что любое конечное поле имеет положительную характеристику.

66.17. Существует ли бесконечное поле положительной характеристики?

66.18. Решить в поле $\mathbb{Q}(\sqrt{2})$ уравнения:
а) $x^2 + (4 - 2\sqrt{2})x + 3 - 2\sqrt{2} = 0$;
б) $x^2 - x - 3 = 0$;
в) $x^2 + x - 7 + 6\sqrt{2} = 0$;
г) $x^2 - 2x + 1 - \sqrt{2} = 0$.

66.19. Решить систему уравнений

$$x + 2z = 1, \qquad y + 2z = 2, \qquad 2x + z = 1:$$

а) в поле $\mathbf{Z}_3$; б) в поле $\mathbf{Z}_5$.

66.20. Решить систему уравнений

$$3x + y + 2z = 1, \qquad x + 2y + 3z = 1, \qquad 4x + 3y + 2z = 1$$

в поле вычетов по модулю 5 и по модулю 7.

66.21. Найти такой многочлен $f(x)$ степени не выше 3 с коэффициентами из $\mathbf{Z}_5$, что

$$f(0) = 3, \qquad f(1) = 3, \qquad f(2) = 5, \qquad f(4) = 4.$$

66.22. Найти все многочлены $f(x)$ с коэффициентами из $\mathbf{Z}_5$, что

$$f(0) = f(1) = f(4) = 1, \qquad f(2) = f(3) = 3.$$

66.23. Какие из уравнений:
а) $x^2 = 5$, б) $x^7 = 7$, в) $x^3 = a$,
имеют решения в поле $\mathbf{Z}_{11}$?

66.24. В поле вычетов по модулю 11 решить уравнения:
а) $x^2 + 3x + 7 = 0$;
б) $x^2 + 5x + 1 = 0$;
в) $x^2 + 2x + 3 = 0$;
г) $x^2 + 3x + 5 = 0$.

66.25. Доказать, что в поле из n элементов выполняется тождество $x^n = x$.

66.26. В поле $\mathbf{Z}_p$ решить уравнение $x^p = a$.

66.27. Доказать, что если $x^n = x$ для всех элементов x поля K, то K конечно и его характеристика делит n.

66.28. Найти все порождающие элементы в мультипликативной группе поля:
а) $\mathbf{Z}_7$; б) $\mathbf{Z}_{11}$; в) $\mathbf{Z}_{17}$.

66.29. Пусть a, b элементы поля порядка 2^n, где n нечетно. Доказать, что если $a^2+ab+b^2=0$, то $a=b=0$.

66.30. Пусть F — поле, причем группа F^* циклическая. Доказать, что F конечно.

66.31. В поле рациональных функций с вещественными коэффициентами решить уравнения:

а) $f^4=1$; б) $f^2-f-x=0$.

66.32. Доказать, что в поле $\mathbf{Z}_p$ выполняются равенства:

а) $\sum\limits_{k=1}^{p-1} k^{-1}=0 \quad (p>2)$; б) $\sum\limits_{k=1}^{(p-1)/2} k^{-2}=0 \quad (p>3)$.

66.33. Пусть $n \geqslant 2$ и $\zeta_1,\ldots,\zeta_m$ — все корни n-й степени из 1 в поле K. Доказать, что:

а) $\{\zeta_1,\ldots,\zeta_m\}$ — группа по умножению;

б) $\{\zeta_1,\ldots,\zeta_m\}$ — корни степени m из 1;

в) m делит n;

г) если $k \in \mathbb{Z}$, то

$$\zeta_1^k+\ldots+\zeta_m^k=\begin{cases} 0, & \text{если } m \text{ не делит } k,\\ m, & \text{если } m \text{ делит } k. \end{cases}$$

66.34. Пусть $m_k m_{k-1}\ldots m_0$ и $n_k n_{k-1}\ldots n_0$ — записи натуральных чисел m и n в системе счисления с основанием s, где s — простое число.

Доказать, что:

а) числа $\binom{m}{n}$ и $\binom{m_0}{n_0}\binom{m_1}{n_1}\ldots\binom{m_n}{n_n}$ при делении на s дают одинаковые остатки;

б) $\binom{m}{n}$ делится на s тогда и только тогда, когда при некотором i выполняется неравенство $m_i<n_i$.

66.35. *Нормированием поля* K называется функция $\|x\|$, $x \in K$, принимающая вещественные неотрицательные значения, причем:

$\|x\|=0$ тогда и только тогда, когда $x=0$;

$\|xy\|=\|x\|\|y\|$;

$\|x+y\| \leqslant \|x\|+\|y\|$.

Доказать, что следующие функции в $\mathbb{Q}$ являются нормированиями:

а) $\|x\|=\begin{cases} 1, & x \neq 0,\\ 0, & x=0; \end{cases}$

б) $\|x\|=|x|^s$, где s — фиксированное число, $0<s\leqslant 1$;

в) $\|x\| = |x|_p^s$, p — простое число, s — фиксированное положительное число, меньшее 1, причем если $x = p^r mn^{-1}$, где m, n — целые числа, не делящиеся на p, то $|x|_p = p^{-r}$.

* * *

66.36. Пусть $\|x\|$ — нормирование $\mathbb{Q}$, причем существует такое y, что $\|y\| \neq 0, 1$. Тогда $\|x\|$ имеет либо вид б), либо вид в) из задачи 66.35.

66.37. Пусть K — поле и $K(x)$ — поле рациональных функций от одной переменной x. Доказать, что следующие функции в $K(x)$ являются нормированиями:

а) $\|f\| = \begin{cases} 1, & \text{если} \quad f \neq 0, \\ 0, & \text{если} \quad f = 0; \end{cases}$

б) $\|hg^{-1}\| = c^{\deg h - \deg g}$, где $h, g \in K[x]$ и $0 < c < 1$;

в) если $p(x)$ — неприводимый многочлен, $h = p^r(x)u(x)v^{-1}(x)$, где $u(x)$, $v(x)$ — многочлены, не делящиеся на $p(x)$, то $|h| = c^r$, где $0 < c < 1$.

66.38. Доказать, что:

а) пополнение $\mathbb{Q}$ относительно нормирования из задачи 66.37, б) равно $\mathbb{R}$;

б) пополнение $\mathbb{Q}$ относительно нормирования из задачи 66.37, в) равно $\mathbb{Q}_p$;

в) пополнение $\mathbb{Z}$ относительно нормирования из задачи 66.37, б) равно $\mathbb{Z}_p$;

г) пополнение $\mathbb{C}[x]$ относительно нормирования из задачи 66.37, в) с $p = x$ равно алгебре степенных рядов $\mathbb{C}[[x]]$.

66.39. Последовательность x_n, $n \geqslant 1$, элементов из $\mathbb{Q}_p$ сходится относительно метрики $\|f\|$ из задачи 66.37, в) тогда и только тогда, когда

$$\lim_{n\to\infty} \|x_n - x_{n+1}\|_p = 0.$$

66.40. При каких $t \in \mathbb{Q}_p$ сходятся ряды:

а) $e^t = \sum \dfrac{t^n}{n!}$; б) $\ln(1+x) = \sum\limits_{n\geqslant 1} \dfrac{1}{n}(-1)^n t^n$; в) $\sum\limits_{n\geqslant 0} x^n$?

66.41. Пусть $a \in \mathbb{Q}_p$ и $x_n = a^{p^n}$. Существует ли $\lim\limits_{n\to\infty} x_n$?

66.42. Пусть $f(x) \in \mathbb{Z}_p[x]$, $a_0 \in \mathbb{Z}_p$, причем $\|f(a_0)/f'(a_0)^2\|_p < 1$. Положим

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

Доказать, что существует $a = \lim a_n$, причем $f(a) = 0$ и $\|a - a_0\|_p < 1$.

66.43. Доказать, что любой автоморфизм в $\mathbb{Q}_p$ тождествен.

66.44. Пусть $f(x) \in \mathbb{Z}_p[x]$ имеет степень n и старший коэффициент $f(x)$ равен 1. Пусть образ $\overline{f(x)}$ многочлена $f(x)$ в $\mathbb{Z}/p\mathbb{Z}[x]$ разложим, $\overline{f}(x) = g(x)h(x)$, где $g(x)$, $h(x)$ взаимно просты, имеют старший коэффициент 1, причем

$$\deg g(x) = r, \qquad \deg h(x) = n - r.$$

Тогда $f(x) = u(x)v(x)$, где $\deg u(x) = r$, $\deg h(x) = n - r$, старшие коэффициенты $u(x)$, $v(x)$ равны 1, причем образы $u(x)$, $v(x)$ в $\mathbb{Z}/p\mathbb{Z}[x]$ равны соответственно $g(x)$ и $h(x)$.

66.45. Пусть $f(x) \in \mathbb{Z}_p[x]$ и $a \in \mathbf{Z}_p$, причем в $\mathbf{Z}_p$

$$f(a) = 0, \qquad f'(a) \neq 0.$$

Тогда существует такой элемент $b \in \mathbb{Z}_p$, что $f(b) = 0$ и образ b в $\mathbf{Z}_p$ равен a.

66.46. Пусть m — натуральное число, не делящееся на p и $a \in 1 + p\mathbf{Z}_p$. Тогда существует такое $b \in \mathbb{Z}_p$, что $b^m = a$.

66.47. Пусть поля $\mathbb{Q}_p$ и $\mathbb{Q}_{p'}$ изоморфны. Доказать, что $p = p'$.

66.48. Кольцо $\mathbb{Z}_p$ компактно в $\mathbb{Q}_p$ относительно p-адической топологии.

§ 67. Расширения полей. Теория Галуа

В этом параграфе все кольца и алгебры предполагаются коммутативными и обладающими единицей.

67.1. Пусть A — алгебра над полем K и

$$K = K_0 \subset K_1 \subset K_1 \subset \ldots \subset K_s$$

— башня подполей в A.

Доказать, что

$$(A : K) = (A : K_s)(K_s : K_{s-1}) \times \ldots \times (K_1 : K_0).$$

67.2. Пусть A — алгебра над полем K и $a \in A$.
Доказать, что:
а) если элемент a не является алгебраическим над K, то подалгебра $K[a]$ изоморфна кольцу многочленов $K[x]$;
б) если a — алгебраический элемент над K, то
$$K[a] \simeq K[x]/\langle \mu_a(x) \rangle,$$
где $\mu_a(x)$ — некоторый однозначно определенный унитарный многочлен (минимальный многочлен элемента a) над K;
в) если A — поле, то для всякого алгебраического над K элемента $a \in A$ многочлен $\mu_a(x)$ неприводим в $K[x]$;
г) если все элементы из A алгебраичны над K и для всякого $a \in A$ многочлен $\mu_a(x)$ неприводим, то A — поле.

67.3. Найти минимальные многочлены для элементов:
а) $\sqrt{2}$ над $\mathbb{Q}$; б) $\sqrt[7]{5}$ над $\mathbb{Q}$; в) $\sqrt[105]{9}$ над $\mathbb{Q}$;
г) $2 - 3i$ над $\mathbb{R}$; д) $2 - 3i$ над $\mathbb{C}$; е) $\sqrt{2} + \sqrt{3}$ над $\mathbb{Q}$;
ж) $1 + \sqrt{2}$ над $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

67.4. Доказать, что:
а) если A — конечномерная алгебра над K, то всякий элемент из A алгебраичен над K;
б) если $a_1, \ldots, a_s \in A$ — алгебраические элементы над K, то подалгебра $K[a_1, \ldots, a_s]$ конечномерна над K.

67.5. Доказать, что если A — поле и $a_1, \ldots, a_s \in A$ — алгебраические элементы над K, то расширение $K(a_1, \ldots, a_s)$ совпадает с алгеброй $K[a_1, \ldots, a_s]$.

67.6. Доказать, что множество всех элементов K-алгебры A, алгебраических над K, является подалгеброй в A, а если A — поле, то подполем.

67.7. Доказать, что если в башне полей
$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_s = L$$
каждый этаж $K_{i-1} \subset K_i$ $(i = 1, \ldots, s)$ является алгебраическим расширением, то L/K — алгебраическое расширение.

67.8. Доказать, что всякий многочлен с коэффициентами из поля K имеет корень в некотором расширении L/K.

* * *

67.9. Пусть K — поле. Доказать, что:

а) для произвольного многочлена из $K[x]$ существует поле разложения этого многочлена над K;

б) для любого конечного множества многочленов из $K[x]$ существует поле разложения над K.

67.10. Пусть K — поле, $g(x) \in K[x]$, $h(x) \in K[x]$, $f(x) = g(h(x))$, и α — корень многочлена $g(x)$ в некотором расширении L/K. Доказать, что многочлен f неприводим над K тогда и только тогда, когда $g(x)$ неприводим над K и $h(x) - \alpha$ неприводим над $K[\alpha]$.

67.11. Пусть K — поле, $a \in K$. Доказать, что:

а) если p — простое число, то многочлен $x^p - a$ либо неприводим, либо имеет корень в K;

б) если многочлен $x^n - 1$ разлагается в $K[x]$ на линейные множители, то многочлен $x^n - a \in K[x]$ либо неприводим, либо для некоторого делителя $d \neq 1$ числа n многочлен $x^d - a$ имеет корень в K;

в) предположение о разложимости $x^n - 1$ на линейные множители существенно для справедливости утверждения б).

67.12. Доказать, что над полем K характеристики $p \neq 0$ многочлен $f(x) = x^p - x - a$ либо неприводим, либо разлагается в произведение линейных множителей, и указать это разложение, если $f(x)$ имеет корень x_0.

67.13. Найти степень поля разложения над $\mathbb{Q}$ для многочленов:

а) $ax + b \quad (a, b \in \mathbb{Q}, \quad a \neq 0)$;

б) $x^2 - 2$; в) $x^3 - 1$; г) $x^3 - 2$; д) $x^4 - 2$;

е) $x^p - 1 \quad$ (p — простое число);

ж) $x^n - 1 \quad (n \in \mathbb{N})$;

з) $x^p - a \quad$ ($a \in \mathbb{Q}$ и не является p-й степенью в $\mathbb{Q}$, p — простое число);

и) $(x^2 - a_1) \times \ldots \times (x^2 - a_n) \quad$ ($a_1, \ldots, a_n$ принадлежит $\mathbb{Q}^*$ и все различны).

67.14. Доказать, что конечное расширение L/K является простым тогда и только тогда, когда множество промежуточных полей между K и L конечно, и привести пример конечного расширения, не являющегося простым.

67.15. Пусть L/K — алгебраическое расширение. Доказать, что расширение $L(x)/K(x)$ также алгебраическое и

$$(L(x) : K(x)) = (L : K).$$

67.16. Пусть L/K — расширение. Элементы $a_1, \ldots, a_s \in L$ называются *алгебраически независимыми над* K, если $f(a_1, \ldots, a_s) \neq 0$ для всякого ненулевого многочлена $f(x_1, \ldots, x_s) \in K[x_1, \ldots, x_s]$.

Доказать, что элементы $a_1, \ldots, a_s \in L$ алгебраически независимы над K тогда и только тогда, когда расширение $K(a_1, \ldots, a_s)$ K-изоморфно полю рациональных функций $K(x_1, \ldots, x_s)$.

67.17. Пусть L/K — расширение и $a_1, \ldots, a_s$; $b_1, \ldots, b_n$ — две максимальные алгебраически независимые над K системы элементов из L. Доказать, что $m = n$ (*степень трансцендентности* L над K).

67.18. Доказать, что:

а) в конечномерной коммутативной K-алгебре A имеется лишь конечное число максимальных идеалов и их пересечение совпадает с множеством $N(A)$ всех нильпотентных элементов алгебры A (*нильрадикал* алгебры A);

б) $A^{\mathrm{red}} = A/N(A)$ — *редуцированная* алгебра (не содержит отличных от 0 нильпотентных элементов);

в) алгебра $A/N(A)$ изоморфна прямому произведению полей $K_1, \ldots$ $\ldots, K_s$, являющихся расширениями поля K;

г) $s \leqslant (A : K)$;

д) набор расширений K_i определен для алгебры A однозначно с точностью до изоморфизма [1]);

е) если B — подалгебра в A, то всякая компонента B является расширением в одной или нескольких компонентах A;

ж) если I — идеал в A, то компоненты алгебры A/I содержатся среди компонент алгебры A.

67.19. Пусть K — поле, $f(x) \in K[x]$, $p_1(x)^{k_1} \times \ldots \times p_s(x)^{k_s}$ — разложение $f(x)$ в произведение степеней различных неприводимых многочленов над K, $A = K[x]/\langle f(x)\rangle$. Доказать, что

$$A^{\mathrm{red}} = A/N(A) \simeq \prod_{i=1}^{s} k[x]/\langle p_l(x)\rangle.$$

67.20. Пусть A — K-алгебра и L — расширение поля K.
Доказать, что:

а) если $f_1, \ldots f_n$ — различные K-гомоморфизмы $A \to L$, то $f_1, \ldots, f_n$ линейно независимы как элементы векторного пространства над L всех K-линейных отображений $A \to L$;

б) число различных K-гомоморфизмов $A \to L$ не превосходит $(A : L)$.

Найти все автоморфизмы полей $\mathbb{Q}(\sqrt{2}\,)$, $\mathbb{Q}(\sqrt{2} + \sqrt{3}\,)$, $\mathbb{Q}(\sqrt[3]{2})$.

67.21. Пусть A — конечномерная K-алгебра и L — расширение поля K. Положим $A_L = L \otimes_K A$. Пусть $(e_1, \ldots, e_n)$ — базис A над K.
Доказать, что:

а) $(1 \otimes e_1, \ldots, 1 \otimes e_n)$ — базис A_L над L;

б) при естественном вложении A в A_L образ A является K-подалгеброй в A_L.

67.22. Пусть A — конечномерная K-алгебра, L — расширение поля K. Доказать, что:

а) если B — подалгебра в A, то B_L — подалгебра в A_L;

б) если I — идеал алгебры A и I_L — соответствующий идеал в A_L, то $(A/I)_L \simeq A_L/I_L$;

в) если $A = \prod_{i=1}^{s} A_i$, то $A_L \simeq \prod_{i=1}^{s} (A_i)_L$;

г) если $K_1, \ldots, K_s$ — множество компонент алгебры A, то множество компонент алгебр A_L совпадает с объединением множеств компонент алгебр $(K_1)_L, \ldots, (K_s)_L$;

д) если F — расширение поля L, то $(A_L)_F \cong A_F$.

67.23. Пусть A — конечномерная K-алгебра, L — расширение поля K, B — некоторая L-алгебра. Доказать, что:

а) каждый K-гомоморфизм $A \to B$ однозначно продолжается до L-гомоморфизма $A_L \to B_L$;

б) множество K-гомоморфизмов $A \to L$ находится в биективном соответствии со множеством компонент алгебры A_L, изоморфных L;

в) число различных K-гомоморфизмов $A \to L$ не превосходит $(A : K)$ (ср. с задачей 67.20, б)).

67.24. Пусть F и L — расширения поля K, причем F/K конечное. Доказать, что существует расширение E/K, для которого имеются вложения F в E и L в E, оставляющие на месте все элементы из K.

67.25. Пусть A — конечномерная K-алгебра и $A = K[a_1, \ldots, a_s]$. Доказать, что следующие свойства расширения L/K равносильны:

а) все компоненты A_L изоморфны L;

б) L — *поле расщепления* для минимального многочлена любого элемента $a \in A$ (расщепляющее поле K-алгебры A).

67.26. Доказать, что если L — расщепляющее поле K-алгебры A и B — подалгебра в A, то любой K-гомоморфизм $B \to L$ продолжается до K-гомоморфизма $A \to L$.

67.27. Расщепляющее поле L для конечномерной K-алгебры A называется *полем разложения* для A, если никакое его собственное подполе, содержащее K, не является расщепляющим для A.

Доказать, что:

а) если $A = K[a_1, \ldots, a_s]$, то L — поле разложения для A тогда и только тогда, когда L — поле разложения для минимальных многочленов элементов $a_1, \ldots, a_s$;

б) любые два поля разложения K-алгебры A изоморфны над K;

в) для поля разложения K-алгебры A существует K-вложение в любое расщепляющее поле для A.

67.28. Пусть A — конечномерная K-алгебра, L — поле расщепления для A. Доказать, что число компонент L-алгебры A_L одно и то же для всех расщепляющих полей алгебры A (*сепарабельная степень* $(A:K)_s$ алгебры A).

67.29. Пусть A — K-алгебра и L — расширение поля K. Доказать, что:

а) число компонент алгебры A_L не превосходит $(A:K)_s$;

б) число различных K-гомоморфизмов $A \to L$ не превосходит $(A:K)_s$ и равенство имеет место тогда и только тогда, когда L — расщепляющее поле для A.

67.30. Доказать, что следующие свойства конечного расширения L/K равносильны:

а) все компоненты алгебры L_L изоморфны L;

б) L имеет $(L:K)$ различных K-автоморфизмов;

в) для любых K-вложений $\varphi_i\colon\ L \to L'$ $(i = 1, 2)$ поля L в любое расширение L'/K имеем $\varphi_1(L) = \varphi_2(L)$;

г) всякий неприводимый многочлен из $K[x]$, имеющий корень в L, разлагается над L в произведение линейных множителей;

д) L есть поле разложения некоторого многочлена из $K[x]$. (Расширение L/K, удовлетворяющее этим условиям, называется *нормальным*.)

67.31. Пусть $K \subset L \subset F$ — башня конечных расширений поля K. Доказать, что:

а) если расширение F/K нормальное, то расширение F/L также нормальное;

б) если расширения L/K и F/L нормальные, то расширение F/K не обязательно нормальное;

в) всякое расширение степени 2 нормально.

67.32. Пусть A — конечномерная K-алгебра и $a \in A$. Характеристический многочлен, определитель и след линейного оператора $t \mapsto at$ на A обозначаются соответственно через

$$\chi_{A/K}(a, x), \qquad N_{A/K}(a), \qquad \operatorname{tr}_{A/K}(a)$$

и называются соответственно *характеристическим многочленом*, *нормой* и *следом* элемента a алгебры A над K.

Доказать, что если $K \subset L \subset F$ — башня конечных расширений полей и $a \in F$, то:

а) $\chi_{F/K}(a, x) = N_{L(x)/K(x)}(\chi_{F/L}(a, x))$, где $\chi_{F/L}(a, x)$ рассматривается как элемент поля рациональных функций $K(x)$;

б) $N_{F/K}(a) = N_{L/K}(N_{F/L}(a))$;
в) $\operatorname{tr}_{F/K}(a) = \operatorname{tr}_{L/K}(\operatorname{tr}_{F/L}(a))$.

67.33. Пусть L/K — конечное расширение и $a \in L$.
Доказать, что:
а) минимальный многочлен элемента a равен $\pm\chi_{K(a)/K}(a, x)$;
б) $\chi_{L/K}(a, x)$ является (с точностью до знака) степенью минимального многочлена элемента a.

67.34. Пусть L/K — конечное расширение. Доказать, что K-билинейная форма на L
$$(x, y) \mapsto \operatorname{tr}_{L/K}(xy)$$
либо невырожденная, либо $\operatorname{tr}_{L/K}(x) = 0$ для всех $x \in L$.

67.35. Доказать, что следующие свойства конечномерной K-алгебры A равносильны:
а) для всякого расширения L/K алгебра A_L редуцированная (задача 67.18);
б) $(A : K)_s = (A : K)$ (задача 67.28);
в) для некоторого расширения L/K существует $(A : K)$ гомоморфизмов K-алгебр $A \to L$;
г) билинейная форма $(x, y) \mapsto \operatorname{tr}_{A/K}(xy)$ на A невырождена. (Алгебра A, удовлетворяющая этим условиям, называется *сепарабельной*.)

67.36. Пусть L — расширение поля K. Доказать, что конечномерная K-алгебра A сепарабельна тогда и только тогда, когда сепарабельна L-алгебра A_L.

67.37. Доказать, что всякая подалгебра и всякая факторалгебра сепарабельной K-алгебры являются сепарабельными K-алгебрами.

67.38. Пусть A — сепарабельная K-алгебра, $(A : K) = n$ и $\varphi_1, \ldots, \varphi_n$ — различные K-гомоморфизмы алгебры A в некоторое ее расщепляющее поле L. Доказать, что для всякого элемента $a \in A$
$$\operatorname{tr}_{A/K}(a) = \sum_{i=1}^{n} \varphi_i(a), \qquad N_{A/K}(a) = \prod_{i=1}^{n} \varphi_i(a),$$
$$\chi_{A/K}(a, x) = \prod_{i=1}^{n} (\varphi_i(a) - x).$$

67.39. Конечное расширение L/K называется *сепарабельным*, если L — сепарабельная K-алгебра.
а) Доказать, что сепарабельное расширение полей является простым.

б) Являются ли числа

$$a = -\frac{1}{2} + i\frac{\sqrt{2}}{2}, \qquad b = \sqrt{2} + i$$

примитивными элементами расширения $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$?

67.40. Доказать, что конечномерная K-алгебра сепарабельна тогда и только тогда, когда она является прямым произведением сепарабельных расширений поля K.

67.41. Пусть $K = K_0 \subset K_1 \subset \ldots \subset K_s = L$ — башня конечных расширений полей. Доказать, что расширение L/K сепарабельно тогда и только тогда, когда каждое расширение K_i/K_{i-1} $(i = 1, \ldots, s)$ сепарабельно.

67.42. Пусть K — поле. Многочлен $f(x) \in K[x]$ называется *сепарабельным*, если ни в каком расширении поля K он не имеет кратных корней.

Доказать, что:

а) если K имеет характеристику 0, то всякий неприводимый многочлен из $K[x]$ сепарабелен;

б) если K имеет характеристику $p \neq 0$, то всякий неприводимый многочлен $f(x) \in K[x]$ сепарабелен тогда и только тогда, когда его нельзя представить в виде $g(x^p)$, где $g(x) \in K[x]$.

Привести пример несепарабельного неприводимого многочлена над каким-либо полем.

67.43. Пусть A — конечномерная K-алгебра. Элемент $a \in A$ называется *сепарабельным* над полем K, если $K[a]$ — сепарабельная K-алгебра. Доказать, что элемент сепарабелен тогда и только тогда, когда сепарабелен его минимальный многочлен.

67.44. Пусть $K \subset L \subset F$ — башня конечных расширений полей.

Доказать, что:

а) если элемент $a \in F$ сепарабелен над K, то a сепарабелен над L;

б) утверждение, обратное к а), верно, если расширение L/K сепарабельно.

67.45. Пусть A — сепарабельная K-алгебра, $f(x) \in K[x]$ — сепарабельный многочлен.

Доказать, что алгебра $B = A[x]/\langle f(x)\rangle$ сепарабельна.

67.46. Пусть $A = K[a_1, \ldots, a_s]$ — конечномерная K-алгебра. Доказать, что следующие условия утверждения равносильны:

а) A — сепарабельная K-алгебра;

б) всякий элемент $a \in A$ сепарабелен;

в) элементы $a_1, \ldots, a_s$ сепарабельны.

67.47. Доказать, что:

а) конечное расширение K/F поля F сепарабельно тогда и только тогда, когда либо K имеет характеристику 0, либо характеристика K равна $p > 0$ и $K^p = K$;

б) всякое конечное расширение конечного поля сепарабельно.

67.48. Конечное расширение полей L/K характеристики $p > 0$ называется *чисто несепарабельным*, если в $L \setminus K$ нет сепарабельных элементов над K. Доказать, что L/K является чисто несепарабельным расширение тогда и только тогда, когда $L^{p^k} \subseteq K$ для некоторого $k \geqslant 1$.

67.49. Пусть $K \subset K_0 \subset K_1 \ldots \subset K_s = L$ — башня конечных расширений полей. Доказать, что расширение L/K чисто несепарабельно тогда и только тогда, когда каждое расширение K_i/K_{i-1} $(i = 1, \ldots, s)$ чисто несепарабельно.

67.50. Доказать, что степень чисто несепарабельного расширения поля характеристики $p > 0$ является степенью числа p, а его сепарабельная степень равна 1.

67.51. Пусть L/K — конечное расширение полей.

Доказать, что:

а) множество K_s всех сепарабельных над K элементов из L является полем, сепарабельным над K;

б) L/K_s — чисто несепарабельное расширение;

в) $(K_s : K) = (L : K)_s$;

г) $(L : K) = (L : K)_s \cdot (L : K)_i$, где $(L : K)_i = (L : K_s)$ несепарабельная степень расширения L/K.

67.52. Пусть $K \subset L \subset F$ — башня конечных расширений полей. Доказать, что:

а) $(F : K)_s = (F : L)_s \cdot (L : K)_s$;

б) $(F : K)_i = (F : L)_i \cdot (L : K)_i$.

67.53. Пусть L/K — конечное расширение полей, $n = (L : K)_s$ и $\varphi_1, \ldots, \varphi_n$ — множество всех K-вложений поля L в какое-либо расщепляющее поле расширения L/K.

Доказать, что при любом $a \in L$:

а) $\operatorname{tr}_{L/K}(a) = (L : K)_i \sum\limits_{j=1}^{n} \varphi_j(a)$;

б) $N_{L/K}(a) = \Big(\prod\limits_{j=1}^{n} \varphi_j(a)\Big)^{(L:K)_i}$;

в) $\chi_{L/K}(a, x) = \Big(\prod\limits_{j=1}^{n} (\varphi_j(a) - x)\Big)^{(L:K)_i}$.

67.54. Нормальное конечное сепарабельное расширение полей L/K называется *расширением Галуа*, а группа K-автоморфизмов такого расширения называется его *группой Галуа* и обозначается через $G(L/K)$.

Доказать, что:

а) $G(L/K)$ транзитивно действует на множестве корней из поля L минимального многочлена любого элемента поля L;

б) порядок группы $G(L/K)$ равен степени расширения L/K.

67.55. Найти группу Галуа расширения:

а) $\mathbb{C}/\mathbb{R}$; б) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$;

в) L/K, где $(L:K)=2$; г) $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$.

67.56. *Группой Галуа* над полем K сепарабельного многочлена $f(x)\in K[x]$ называется группа Галуа поля разложения этого многочлена над K (как некоторая группа перестановок на множестве корней $f(x)$). Найти группы Галуа над полем $\mathbb{Q}$ многочленов из задачи 67.13.

67.57. Пусть G — конечная группа автоморфизмов поля L и $K=L^G$ — поле неподвижных элементов. Доказать, что L/K — расширение Галуа и $G(L/K)=G$.

67.58. Доказать, что если элементы $a_1,\ldots,a_n$ алгебраически независимы над полем K, то группа Галуа многочлена

$$x^n+a_1x^{n-1}+\ldots+a_n$$

над полем рациональных функций $K(a_1,\ldots,a_n)$ есть $\mathbf{S}_n$.

67.59. Доказать, что всякая конечная группа является группой Галуа некоторого расширения полей.

67.60. (*Основная теорема теории Галуа.*) Пусть L/K — расширение Галуа и G — его группа Галуа. Доказать, что сопоставление всякой подгруппе $H\subset G$ подполя L^H неподвижных элементов определяет биективное соответствие между всеми подгруппами группы G и всеми промежуточными подполями расширения L/K, при котором промежуточное подполе F соответствует подгруппе $H=G(L/F)$; при этом расширение F/K нормально тогда и только тогда, когда подгруппа H нормальна в G, и в этом случае каноническое отображение $G\to G(F/K)$ определяет изоморфизм $G(F/K)\simeq G/H$.

67.61. Используя основную теорему теории Галуа и существование вещественного корня у всякого многочлена нечетной степени с вещественными коэффициентами, доказать алгебраическую замкнутость поля комплексных чисел.

67.62. Доказать, что группа Галуа всякого конечного расширения $L/\mathbb{F}_p$ циклическая и порождается автоморфизмом $x\mapsto x^p$ $(x\in L)$.

67.63. Доказать, что группа Галуа над полем K сепарабельного многочлена $f(x) \in K[x]$, рассматриваемая как подгруппа в $\mathbf{S}_n$, содержится в группе четных перестановок тогда и только тогда, когда дискриминант

$$D = \prod_{i>j}(x_i - x_j)^2$$

многочлена $f(x)$, где $x_1, \ldots, x_n$ — корни $f(x)$ в его поле разложения, является квадратом в поле K.

67.64. Пусть L/K — расширение Галуа с циклической группой Галуа $\langle\varphi\rangle_n$. Доказать, что существует такой элемент $a \in L$, что элементы $a, \varphi(a), \ldots, \varphi^{n-1}(a)$ образуют базис L над K.

67.65. Пусть L/K — сепарабельное расширение степени n и $\varphi_1, \ldots$ $\ldots, \varphi_n$ — различные K-вложения L в некоторое расщепляющее для L поле. Доказать, что элемент $a \in L$ является примитивным элементом в L/K тогда и только тогда, когда образы $\varphi_1(a), \ldots, \varphi_n(a)$ различны.

67.66. Найти группу автоморфизмов K-алгебры, являющейся прямым произведением n полей, изоморфных K.

67.67. Пусть L/K — расширение Галуа с группой Галуа G, $L = \prod L_\sigma$, где L_σ — компонента алгебры L_L, проекция на которую индуцирует на L автоморфизм σ, и e_σ — единица компоненты L_σ. Доказать, что для продолжений автоморфизмов из G до L-автоморфизмов алгебры L_L справедливы равенства

$$\tau(e_\sigma) = e_{\sigma\tau^{-1}}, \qquad \sigma, \tau \in G.$$

67.68. Пусть L — расщепляющее поле для сепарабельной K-алгебры A и $\varphi_1, \ldots, \varphi_n$ — множество всех K-гомоморфизмов $A \to L$. Доказать, что элементы $y_1, \ldots, y_n \in A$ образуют базис A над K тогда и только тогда, когда $\det(\varphi_i(y_j)) \neq 0$.

67.69. (*Теорема о нормальном базисе.*) Доказать, что в расширении Галуа L/K с группой Галуа G существует такой элемент $a \in L$, что множество $\{\sigma(a) \mid \sigma \in G\}$ является базисом поля L над K.

67.70. Найти поле инвариантов $K(x_1, \ldots, x_n)^{A_n}$ для группы $\mathbf{A}_n$, действующей на поле рациональных функций посредством перестановок переменных.

67.71. Пусть ε — первообразный комплексный корень степени n из 1 и группа $G = \langle\sigma\rangle_n$ действует на поле $\mathbb{C}(x_1, \ldots, x_n)$ по правилу

$$\sigma(x_1) = \varepsilon^i x_i \quad (i = 1, \ldots, n).$$

Найти поле инвариантов $\mathbb{C}(x_1, \ldots, x_n)^G$.

67.72. Найти поле инвариантов для группы G, действующей на поле $\mathbb{C}(x_1, \ldots, x_n)$ посредством циклической перестановки переменных.

67.73. Пусть поле K содержит все корни степени n из 1 и элемент $a \in K$ не является степенью с показателем $d > 1$ ни для какого делителя d числа n. Найти группу Галуа над K многочлена $x^n - a$.

67.74. Пусть поле K содержит все корни степени n из 1 и L/K — расширение Галуа с циклической группой Галуа порядка n. Доказать, что $L = K(\sqrt[n]{a})$ для некоторого элемента $a \in K$.

67.75. Пусть поле K содержит все корни степени n из 1. Доказать, что конечное расширение L/K является расширением Галуа с абелевой группой Галуа периода n тогда и только тогда, когда

$$L = K(\theta_1, \ldots, \theta_s),$$

где

$$\theta_i^n = a_i \in K \quad (i = 1, \ldots, s)$$

(т. е. L является полем разложения над K многочлена $\prod_{i=1}^{s}(x_i^n - a_i)^s$).

67.76. Пусть поле K содержит все корни степени n из 1 и $L = K(\vartheta_1, \ldots, \theta_s)$, где

$$\theta_i^n = a_i \in K^* \quad (i = 1, \ldots, s).$$

Доказать, что

$$G(L/K) \simeq \langle (K^*)^n, a_1, \ldots, a_s \rangle / (K^*)^n.$$

67.77. Пусть поле K содержит все корни степени n из 1. Установить биективное соответствие между множеством всех (с точностью до K-изоморфизма) расширений Галуа с абелевой группой Галуа периода n и множеством всех конечных подгрупп группы $K^*/(K^*)^n$.

67.78. Доказать, что всякое расширение Галуа L/K степени p поля K характеристики $p > 0$ имеет вид $L = K(\theta)$, где θ — корень многочлена $x^p - x - a$ $(a \in K)$, и, обратно, всякое такое расширение является расширением Галуа степени 1 или p.

67.79. Пусть K — поле характеристики $p > 0$. Доказать, что конечное расширение L/K является расширением Галуа периода p тогда и только тогда, когда $L = K(\theta_1, \ldots, \theta_s)$, где θ_i — корень многочлена $x^p - x - a_i$ $(a_i \in K;\ i = 1, \ldots, s)$.

67.80. Пусть K — поле характеристики $p > 0$ и $L = K(\theta_1, \ldots, \theta_s)$, где θ_i — корень многочлена $x^p - x - a_i$ $(a_i \in K,\ i = 1, \ldots, s)$.Доказать,

что
$$G(L/K) \simeq \langle \rho(K), a_1, \ldots, a_s \rangle / K,$$

где $\rho : K \to K$ — аддитивный гомоморфизм $x \mapsto x^p - x$.

67.81. Пусть K — поле характеристики $p > 0$. Установить биективное соответствие между множеством всех (с точностью до K-изоморфизма) расширений Галуа L/K с абелевой группой Галуа периода p и множеством всех конечных подгрупп группы $K/\rho(K)$.

§ 68. Конечные поля

68.1. Доказать, что всякое конечное расширение конечного поля является простым.

68.2. Доказать, что:
а) конечное расширение конечного поля нормально;
б) любые два конечных расширения конечного поля F одной степени F-изоморфны.

68.3. Доказать, что:
а) для любого числа q, являющегося степенью простого числа, существует единственное (с точностью до изоморфизма) поле из q элементов;
б) вложение поля $\mathbb{F}_q$ в поле $\mathbb{F}_{q'}$ существует тогда и только тогда, когда q' есть степень q;
в) если K и L — конечные расширения конечного поля F, то F-вложение поля K в L существует тогда и только тогда, когда $(K : L) | (L : F)$;
г) если многочлен $f(x)$ над конечным полем F разлагается в произведение неприводимых множителей степеней $n_1, \ldots, n_s$, то степень поля разложения многочлена $f(x)$ над F равна наименьшему общему кратному чисел $n_1, \ldots, n_s$.

68.4. Пусть F — конечное поле из нечетного числа q элементов. Элемент $a \in F^*$ называется *квадратичным вычетом* в F, если двучлен $x^2 - a$ имеет корень в F.

Доказать, что:
а) число квадратичных вычетов равно $(q - 1)/2$;
б) a является квадратичным вычетом тогда и только тогда, когда $a^{(q-1)/2} = 1$, и не является квадратичным вычетом при $a^{(q-1)/2} = -1$.

68.5. Разложить на неприводимые множители:
а) $x^5 + x^3 + x^2 + 1$ в $\mathbb{F}_2[x]$;
б) $x^3 + 2x^2 + 4x + 1$ в $\mathbb{F}_5[x]$;
в) $x^4 + x^3 + x + 2$ в $\mathbb{F}_3[x]$;
г) $x^5 + 3x^3 + 2x^2 + x + 4$ в $\mathbb{F}_5[x]$;

* * *

68.6. Для элемента $a \in F^*$ положим $\left(\dfrac{a}{F}\right)$ равным 1, если a — квадратичный вычет в F, и -1 — в противном случае.

Доказать, что:

а) отображение $F^* \to \{-1, 1\}$, при котором $a \mapsto \left(\dfrac{a}{F}\right)$, является гомоморфизмом групп;

б) $\left(\dfrac{a}{F}\right) = \operatorname{sgn}\sigma_a$, где $\sigma_a\colon\ x \mapsto ax$ — перестановка на множестве элементов поля F.

68.7. Пусть a и b — взаимно простые числа и $\sigma\colon\ x \to ax$ — перестановка на множестве классов вычетов по модулю b.

Доказать, что:

а) если b четно, то

$$\operatorname{sgn}\sigma = \begin{cases} 1 \quad \text{при } b \equiv 2 \pmod 4, \\ (-1)^{(a-1)/2} \quad \text{при } b \equiv 0 \pmod 4; \end{cases}$$

б) если b нечетно, $b = \prod_{i=1}^{s} p_i$ ($p_1, \ldots, p_s$ — простые числа), то

$$\operatorname{sgn}\sigma = \prod_{i=1}^{s} \left(\frac{n}{p_i}\right),$$

где $\left(\dfrac{a}{p_i}\right) = \left(\dfrac{a}{\mathbf{Z}_{p_i}}\right)$ (*символ Лежандра*) (в этом случае $\operatorname{sgn}\sigma$ обозначается через $\left(\dfrac{a}{b}\right)$ и называется *символом Якоби*);

в) $\left(\dfrac{a}{b_1 b_2}\right) = \left(\dfrac{a}{b_1}\right)\left(\dfrac{a}{b_2}\right)$, $\left(\dfrac{a_1 a_2}{b}\right) = \left(\dfrac{a_1}{b}\right)\left(\dfrac{a_2}{b}\right)$;

г) $\left(\dfrac{-1}{b}\right) = (-1)^{(b-1)/2}$.

68.8. Пусть G — аддитивно записанная конечная абелева группа нечетного порядка, σ — автоморфизм группы G, $\left(\dfrac{\sigma}{G}\right) = \operatorname{sgn}\sigma$, где σ

рассматривается как перестановка на множестве G. Доказать, что если G представляется в виде объединения $\{0\} \cup S \cup \{-S\}$ непересекающихся подмножеств, то

$$\left(\frac{\sigma}{G}\right) = (-1)^{|\sigma(S)\cap(-S)|}.$$

68.9. Пусть σ — автоморфизм группы G нечетного порядка, G_1 — подгруппа в G, инвариантная относительно σ, $G_2 = G/G_1$ и σ_1, σ_2 — автоморфизмы G_1 и G_2, индуцированные σ. Доказать, что

$$\left(\frac{\sigma}{G}\right) = \left(\frac{\sigma_1}{G_1}\right)\left(\frac{\sigma_2}{G_2}\right),$$

и получить отсюда утверждение задачи 68.7, б).

68.10. (*Лемма Гаусса.*) Доказать, что если N — количество чисел x из промежутка $1 \leqslant x \leqslant (b-1)/2$, для которых $ax \equiv r \pmod b$, $-(b-1)/2 \leqslant r \leqslant 1$, то

$$\left(\frac{a}{b}\right) = (-1)^N.$$

68.11. Доказать, что $\left(\dfrac{2}{b}\right) = (-1)^{(b^2-1)/8}$.

68.12. (*Квадратичный закон взаимности.*) Доказать, что для любых взаимно простых нечетных чисел a и b

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)/2\cdot(b-1)/2}.$$

68.13. Пусть V — конечномерное пространство над конечным полем F нечетного порядка, $\mathcal{A}$ — невырожденный линейный оператор на V. Доказать, что

$$\left(\frac{\mathcal{A}}{V}\right) = \left(\frac{\det\mathcal{A}}{F}\right).$$

68.14. Пусть F — конечное расширение поля $\mathbb{F}_q$ степени n. Доказать, что в F как векторном пространстве над $\mathbb{F}_q$ существует базис вида $x, x^q, \ldots, x^{q^{m-1}}$ для некоторого $x \in F$.

68.15. Доказать, что элементы $x_1, \ldots, x_n \in \mathbb{F}_{q^n}$ образуют базис над $\mathbb{F}_q$ тогда и только тогда, когда

$$\det \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_1^q & x_2^q & \ldots & x_n^q \\ \multicolumn{4}{c}{\dotfill} \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \ldots & x_n^{q^{n-1}} \end{pmatrix} \neq 0.$$

68.16. Пусть $a \in \mathbb{F}_{q^n}$. Элементы $a, a^q, \ldots, a^{q^{n-1}}$ образуют базис $\mathbb{F}_{q^n}$ как векторного пространства над $\mathbb{F}_q$ тогда и только тогда, когда в $\mathbb{F}_{q^n}[x]$ многочлены $x^n - 1$ и

$$ax^{n-1} + a^q x^{n-2} + \ldots + a^{q^{n-2}} x + a^{q^{n-1}}$$

взаимно просты.

Глава 15

ЭЛЕМЕНТЫ ТЕОРИИ ПРЕДСТАВЛЕНИЙ

§ 69. Представления групп. Основные понятия

69.1. Доказать, что отображение $\rho\colon\ \mathbb{Z} \to \mathbf{GL}_2(\mathbb{C})$, при котором

$$\rho(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \qquad n \in \mathbb{Z},$$

является приводимым двумерным комплексным представлением группы $\mathbb{Z}$ и не эквивалентно прямой сумме двух одномерных представлений.

69.2. Доказать, что отображение $\rho\colon\ \langle a\rangle_p \to \mathbf{GL}_2(\mathbb{F}_p)$ (p — простое число), при котором

$$\rho(a^k) = \begin{pmatrix} 1 & k\cdot 1 \\ 0 & 1 \end{pmatrix}$$

является приводимым двумерным представлением циклической группы $\langle a\rangle_p$ и не эквивалентно прямой сумме двух одномерных представлений.

69.3. Пусть $A \in \mathbf{GL}_n(\mathbb{C})$. Доказать, что отображение $\rho_A\colon\ \mathbb{Z} \to \mathbf{GL}_n(\mathbb{C})$, при котором $\rho_A(n) = A^n$, является представлением группы $\mathbb{Z}$ и представления ρ_A и ρ_B эквивалентны тогда и только тогда, когда жордановы нормальные формы матриц A и B совпадают (с точностью до порядка клеток).

69.4. Будет ли линейным представлением группы $\mathbb{R}$ в пространстве $C(\mathbb{R})$ непрерывных функций на вещественной прямой отображение L, определяемое по формулам:

а) $(L(t)f)(x) = f(x - t)$;

б) $(L(t)f)(x) = f(tx)$;

в) $(L(t)f)(x) = f(e^t x)$;

г) $(L(t)f)(x) = e^t f(x)$;

д) $(L(t)f)(x) = f(x) + t$;

е) $(L(t)f)(x) = e^t f(x + t)$?

69.5. Какие из подпространств в $C(\mathbb{R})$ инвариантны относительно линейного представления L из задачи 69.4, а):

а) подпространство бесконечно дифференцируемых функций;

б) подпространство многочленов;

в) подпространство многочленов степени $\leqslant n$;

г) подпространство четных функций;

д) подпространство нечетных функций;

е) линейная оболочка функций $\sin x$ и $\cos x$;

ж) подпространство многочленов от $\cos x$ и $\sin x$;

з) линейная оболочка функций $\cos x, \cos 2x, \ldots, \cos nx$;

и) линейная оболочка функций $e^{c_1 t}, e^{c_2 t}, \ldots, e^{c_n t}$, где $c_1, c_2, \ldots, c_n$ — различные фиксированные вещественные числа?

69.6. Найти подпространства пространства многочленов, инвариантные относительно представления L из задачи 69.4, а.

69.7. Записать матрицами (в каком-либо базисе) ограничение линейного представления L из задачи 69.5 на подпространство многочленов степени $\leqslant 2$.

69.8. Записать матрицами (в каком-либо базисе) ограничение линейного представления L из задачи 69.5 на линейную оболочку функций $\sin x$ и $\cos x$.

69.9. Доказать, что каждая из следующих формул определяет линейное представление группы $\mathbf{GL}_n(F)$ в пространстве $\mathbf{M}_n(F)$:

а) $\Lambda(A) \cdot X = AX$;

б) $\mathrm{Ad}\,(A) \cdot X = AXA^{-1}$;

в) $\Phi(A) \cdot X = AX\,{}^tA$.

69.10. Доказать, что линейное представление Λ (см. задачу 69.9, а)) вполне приводимо и его инвариантные подпространства совпадают с левыми идеалами алгебры $\mathbf{M}_n(K)$.

69.11. Доказать, что если $\mathrm{char}\, F$ не делит n, то линейное представление Ad (см. задачу 69.9, б)) вполне приводимо и его нетривиальные инвариантные подпространства — пространство матриц с нулевым следом и пространство скалярных матриц.

69.12. Доказать, что если $\mathrm{char}\, F \neq 2$, то линейное представление Φ (см. задачу 69.9, в)) вполне приводимо и его нетривиальные инвариантные подпространства — пространства симметрических и кососимметрических матриц.

69.13. Пусть V — двумерное пространство над полем F. Показать, что существуют представления ρ_1 и ρ_2 группы $\mathbf{S}_3$ на V, для которых в некотором базисе пространства V будут выполнены соотношения

$$\rho_1((1\ 2)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \rho_1((1\ 2\ 3)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

$$\rho_2((1\ 2)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \rho_2((1\ 2\ 3)) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Доказать, что эти представления изоморфны тогда и только тогда, когда $\operatorname{char} F \neq 3$.

69.14. Пусть V — двумерное векторное пространство над полем F. Показать, что существуют два представления ρ_1, ρ_2 группы

$$\mathbf{D}_4 = \langle a, b \mid a^4 = b^2 = (ab)^2 = 1 \rangle$$

на V, для которых в некотором базисе пространства V будут выполнены соотношения

$$\rho_1(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \rho_1(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\rho_2(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \rho_2(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Будут ли эти представления эквивалентны?

69.15. Пусть ρ_1 и ρ_2 — представления групп $\mathbf{S}_3$ и $\mathbf{D}_4$ из задач 69.13 и 69.14. Будут ли эти представления неприводимы?

69.16. Пусть V — векторное пространство над полем F с базисом $(e_1, \ldots, e_n)$. Зададим отображение $\psi\colon\ \mathbf{S}_n \to \mathbf{GL}(V)$, полагая

$$\psi_\sigma(e_i) = e_{\sigma(i)},$$

где $\sigma \in \mathbf{S}_n,\ i = 1, \ldots, n$.

Доказать, что:

а) ψ — представление группы $\mathbf{S}_n$;

б) подпространство W векторов, сумма координат которых относительно базиса $(e_1, \ldots, e_n)$ равна нулю, и подпространство U векторов с равными координатами инвариантны относительно представления ψ;

в) если $\operatorname{char} F$ не делит n, то ограничение представления ψ на W — неприводимое $(n-1)$-мерное представление группы $\mathbf{S}_n$.

69.17. Пусть $P_{n,m}$ — подпространство однородных многочленов степени m в алгебре $F[x_1, \ldots, x_n]$ и $\operatorname{char} F = 0$. Определим отображение Θ: $\mathbf{GL}_n(F) \to \mathbf{GL}(P_{n,m})$, полагая для $f \in P_{n,m}$ и $A = (a_{ij}) \in$ $\in \mathbf{GL}_n(F)$:

$$(\Theta_A f)(x_1, \ldots, x_n) = f\left(\sum_{i=1}^{n} x_i a_{i1}, \ldots, \sum_{i=1}^{n} x_i a_{in}\right).$$

Доказать, что Θ — неприводимое представление группы $\mathbf{GL}_n(F)$ на пространстве $P_{n,m}$.

69.18. Пусть задано n-мерное пространство V над полем F нулевой характеристики. Определим отображение $\Theta : \mathbf{GL}(V) \to \mathbf{GL}(\Lambda^m V)$, полагая

$$\Theta(f)(x_1 \wedge \ldots \wedge x_m) = (fx_1) \wedge \ldots \wedge (fx_m),$$

где $x_1, \ldots, x_m \in V$ и $f \in \mathbf{GL}(V)$. Доказать, что Θ — неприводимое представление группы $\mathbf{GL}(V)$.

69.19. Доказать, что:

а) для любого представления ρ группы G существует представление $\rho^{\otimes m}$ группы G на пространстве

$$V^{\otimes m} = \underbrace{V \otimes \ldots \otimes V}_{m}$$

m раз контравариантных тензоров на пространстве V такое, что

$$\rho^{\otimes m}(g)(v_1 \otimes \ldots \otimes v_m) = (\rho(g)v_1) \otimes \ldots \otimes (\rho(g)v_m)$$

при любых $v_1, \ldots, v_m \in V$, $g \in G$;

б) подпространства симметрических и кососимметрических тензоров являются инвариантными подпространствами для представления $\rho^{\otimes m}$. Найти размерности этих подпространств, если $\dim V = n$.

69.20. Пусть задано представление $\Phi : G \to \mathbf{GL}(V)$ над полем F и гомоморфизм $\xi : G \to F^*$. Рассмотрим отображение $\Phi_\xi : G \to \mathbf{GL}(V)$, заданное по правилу $\Phi_\xi(g) = \xi(g)\Phi(g)$, $g \in G$. Доказать, что Φ_ξ — представление группы G. Оно неприводимо тогда и только тогда, когда неприводимо представление Φ.

69.21. Пусть Φ — комплексное представление конечной группы G. Доказать, что каждый оператор Φ_g, $g \in G$, диагонализируем.

69.22. Пусть $\rho{:}G \to \mathbf{GL}(V)$ — конечномерное представление группы G над полем F. Доказать, что в V существует базис, в котором для любого $g \in G$ матрица $\rho(g)$ имеет клеточно-верхнетреугольный вид

$$\rho(g) = \begin{pmatrix} \rho_1(g) & & * \\ & \ddots & \\ 0 & & \rho_m(g) \end{pmatrix},$$

где ρ_i — неприводимые представления группы G.

69.23. Пусть $\rho\colon\ G \to \mathbf{GL}(V)$ — конечномерное представление группы G и в V существует базис $(e_1, \ldots, e_n)$, в котором для любого $g \in G$ матрица $\rho(g)$ имеет клеточно-верхнетреугольный вид из задачи 69.22, где размер d_i квадратной матрицы $\rho_i(g)$ не зависит от g. Доказать, что:

а) линейная оболочка V_i векторов $e_{d_1+\ldots+d_{i-1}+1}, \ldots, e_{d_1+\ldots+d_i}$ является G-инвариантным подпространством $(1 \leqslant i \leqslant m)$;

б) отображение $g \mapsto \rho_i(g)$ является матричным представлением группы G;

в) линейное представление группы G, соответствующее этому матричному представлению, изоморфно представлению, возникающему на факторпространстве V_i/V_{i-1} (по определению $V_0 = 0$).

69.24. Пусть $\rho : G \to \mathbf{GL}(V)$ — представление группы G.
Доказать, что:

а) для любого $v \in V$ линейная оболочка $\langle \rho(g)v \mid\ g \in G\rangle$ является инвариантным подпространством для представления ρ;

б) любой вектор из V лежит в некотором инвариантном подпространстве размерности $\leqslant |G|$.

в) минимальное инвариантное подпространство, содержащее вектор $v \in V$, совпадает с $\langle \rho(g)v \mid\ g \in G\rangle$.

69.25. Пусть $\rho\colon\ G \to \mathbf{GL}(V)$ — представление группы G и H — подгруппа в G, $[G : H] = k < \infty$. Доказать, что если подпространство U инвариантно относительно ограничения представления ρ на подгруппу H, то размерность минимального подпространства, содержащего U, инвариантного относительно представления ρ, не превосходит $k \cdot \dim U$.

69.26. Пусть V — векторное пространство над полем $\mathbb{C}$ с базисом $(e_1, \ldots, e_n)$. Определим в V представление Φ циклической группы $\langle a\rangle_n$, полагая $\Phi(a)(e_i) = e_{i+1}$ при $i < n$ и $\Phi(a)(e_n) = e_1$. При $n = 2m$ найти размерность минимального инвариантного подпространства, содержащего векторы:

а) $e_1 + e_{m+1}$;

б) $e_1 + e_3 + \ldots + e_{2m-1}$;

в) $e_1 - e_2 + e_3 - \ldots - e_{2m}$;

г) $e_1 + e_2 + \ldots + e_m$.

69.27. Доказать, что у любого множества попарно коммутирующих операторов на конечномерном комплексном векторном пространстве V есть общий собственный вектор.

69.28. Доказать, что всякое неприводимое представление абелевой группы на конечномерном векторном пространстве над полем $\mathbb{C}$ одномерно.

69.29. Пусть $G = \langle a\rangle_p \times \langle b\rangle_p$, где p — простое число и K — поле характеристики p. Предположим, что V — векторное пространство над K с базисом $x_0, x_1, \ldots, x_n, y_1, \ldots, y_n$. Зададим отображение $\rho\colon G \to \mathbf{GL}(V)$, полагая

$\rho(a)x_i = \rho(b)x_i = x_i, \quad 0 \leqslant i \leqslant n;$

$\rho(a)y_i = x_i + y_i, \quad 1 \leqslant i \leqslant n;$

$\rho(b)y_i = y_i + x_{i-1}, \quad 1 \leqslant i \leqslant n.$

Доказать, что ρ продолжается до представления группы G. Проверить, что это представление неразложимо.

69.30. Доказать, что неприводимые комплексные представления группы $\mathbf{U}_{p^\infty}$ взаимно однозначно соответствуют последовательностям (a_n) натуральных чисел таким, что

$$0 \leqslant a_n \leqslant p^n - 1, \qquad a_n \equiv a_{n+1} \pmod{p^n}$$

при всех n.

69.31. Доказать, что неприводимые комплексные представления группы $\mathbb{Q}/\mathbb{Z}$ взаимно однозначно соответствуют последовательностям натуральных чисел (a_n) таким, что

$$0 \leqslant a_n \leqslant n - 1, \qquad a_n \equiv a_m \pmod{n},$$

если n делит m.

§ 70. Представления конечных групп

70.1. Пусть $\mathcal{A}$ и $\mathcal{B}$ — два перестановочных оператора на конечномерном векторном пространстве V над $\mathbb{C}$ и $\mathcal{A}^m = \mathcal{B}^n = \mathcal{E}$ для некоторых натуральных чисел m и n. Доказать, что пространство V распадается в прямую сумму одномерных инвариантных относительно $\mathcal{A}$ и $\mathcal{B}$ подпространств.

70.2. Перечислить все неприводимые комплексные представления групп:

а) $\langle a\rangle_2$;	б) $\langle a\rangle_4$;	в) $\langle a\rangle_2 \times \langle b\rangle_2$;
г) $\langle a\rangle_6$;	д) $\langle a\rangle_8$;	е) $\langle a\rangle_4 \times \langle b\rangle_2$;
ж) $\langle a\rangle_2 \times \langle b\rangle_2 \times \langle c\rangle_2$;	з) $\langle a\rangle_6 \times \langle b\rangle_3$;	и) $\langle a\rangle_9 \times \langle b\rangle_{27}$.

70.3. Пусть V — векторное пространство над полем F, $\mathcal{A} \in \mathbf{GL}(V)$ и $\mathcal{A}^n = \mathcal{E}$.

а) Доказать, что соответствие $a^k \mapsto \mathcal{A}^k$ определяет представление циклической группы $\langle a \rangle_n$ на пространстве V.

б) Найти все инвариантные подпространства этого представления при указанных порядках n, если оператор $\mathcal{A}$ задается в некотором базисе матрицей A:

$$n = 4, \quad A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \qquad n = 6, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

в) Пусть $F = \mathbb{C}$ и в V имеется такой базис $e_0, e_1, \ldots, e_{n-1}$, что

$$\mathcal{A}(e_i) = \begin{cases} e_{i+1}, & \text{если} \quad i < n-1, \\ e_0, & \text{если} \quad i = n-1. \end{cases}$$

Разложить это представление в прямую сумму неприводимых.

г) Доказать, что представление из в) изоморфно регулярному представлению группы $\langle a \rangle_n$.

70.4. Разложить в прямую сумму одномерных представлений регулярное представление группы:

а) $\langle a \rangle_2 \times \langle b \rangle_2$; б) $\langle a \rangle_2 \times \langle b \rangle_3$; в) $\langle a \rangle_2 \times \langle b \rangle_4$.

70.5. Пусть $H = \langle a \rangle_3$ — циклическая подгруппа группы G, Φ — регулярное представление группы G и Ψ — его ограничение на H. Найти кратность каждого неприводимого представления группы H в разложении представления Ψ в сумму неприводимых:

а) $G = \langle b \rangle_6$, $a = b^2$; б) $G = \mathbf{S}_3$, $a = (1, 2, 3)$.

70.6. Найти все неизоморфные одномерные вещественные представления группы $\langle a \rangle_n$.

70.7. Доказать, что неприводимое вещественное представление конечной циклической группы имеет размерность не более двух.

70.8. Пусть $\rho_k \colon \langle a \rangle_n \to \mathbf{GL}_2(\mathbb{R})$ — представление, для которого

$$\rho_k(a) = \begin{pmatrix} \cos \dfrac{2\pi k}{n} & -\sin \dfrac{2\pi k}{n} \\ \sin \dfrac{2\pi k}{n} & \cos \dfrac{2\pi k}{n} \end{pmatrix}, \qquad 0 < k < n.$$

Доказать, что:

а) представление ρ_k неприводимо, если $k \neq n/2$;

б) представления ρ_k и $\rho_{k'}$ эквивалентны тогда и только тогда, когда $k = k'$ или $k + k' = n$;

в) любое двумерное вещественное неприводимое представление группы $\langle a \rangle_n$ эквивалентно представлению ρ_k для некоторого k.

70.9. Найти число неэквивалентных неприводимых вещественных представлений:

а) группы $\mathbf{Z}_n$;

б) всех абелевых групп порядка 8.

70.10. Найти число неэквивалентных двумерных комплексных представлений групп:

а) $\mathbf{Z}_2$, б) $\mathbf{Z}_4$, в) $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

70.11. Пусть G — абелева группа порядка n. Доказать, что число неэквивалентных k-мерных комплексных представлений группы G равно коэффициенту при t^k ряда $(1-t)^{-n}$. Найти этот коэффициент.

70.12. Доказать, что ядро одномерного представления группы G содержит коммутант этой группы.

70.13. Пусть ρ — представление группы G в пространстве V и в V существует базис, в котором все операторы $\rho(g)$ $(g \in G)$ диагональны. Доказать, что $\operatorname{Ker} \rho \supseteq G'$.

70.14. Доказать, что все неприводимые комплексные представления конечной группы одномерны тогда и только тогда, когда она коммутативна.

70.15. Найти все неизоморфные одномерные комплексные представления групп $\mathbf{S}_3$ и $\mathbf{A}_4$.

70.16. Найти все одномерные комплексные представления групп $\mathbf{S}_n$ и $\mathbf{D}_n$.

70.17. Построить неприводимое двумерное комплексное представление группы $\mathbf{S}_3$.

70.18. Используя гомоморфизм группы $\mathbf{S}_4$ на группу $\mathbf{S}_3$, построить неприводимое двумерное комплексное представление группы $\mathbf{S}_4$.

70.19. Используя изоморфизм групп перестановок и соответствующих групп движений куба и тетраэдра (см. 57.13), построить:

а) два неприводимых трехмерных матричных комплексных представления группы $\mathbf{S}_4$;

б) неприводимое трехмерное представление группы $\mathbf{A}_4$.

70.20. Доказать, что если ε — корень степени n из 1, то отображение

$$a \mapsto \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

продолжается до представления ρ_ε группы $\mathbf{D}_n$. Является ли оно неприводимым при $\varepsilon \neq \pm 1$?

70.21. Пусть ρ_ε и $\rho_{\varepsilon'}$ — неприводимые двумерные комплексные группы представления $\mathbf{D}_n$ из задачи 70.20. Доказать, что ρ_ε и $\rho_{\varepsilon'}$ изоморфны тогда и только тогда, когда $\varepsilon' = \varepsilon^{\pm 1}$.

70.22. Пусть ρ — неприводимое комплексное представление группы $\mathbf{D}_n$. Доказать, что ρ изоморфно ρ_ε для некоторого ε.

70.23. Пусть ρ — естественное двумерное вещественное представление $\mathbf{D}_n$ в виде преобразований, составляющих правильный n-угольник. Найти такое ε, что ρ изоморфно ρ_ε.

70.24. Используя реализацию кватернионов в виде комплексных матриц порядка 2 (см. задачу 58.11, в)), построить двумерное комплексное представление группы $\mathbf{Q}_8$.

70.25. Пусть группа G имеет точное приводимое двумерное представление.

Доказать, что:

а) коммутант группы G' — абелева группа;

б) если G конечна и основное поле имеет характеристику 0, то G коммутативна.

70.26. Доказать, что точное двумерное комплексное представление конечной некоммутативной группы неприводимо.

70.27. Пусть G — конечная группа, ρ — ее конечномерное комплексное представление и в некотором базисе матрицы всех операторов $\rho(g)$ $(g \in G)$ верхнетреугольные. Доказать, что $\operatorname{Ker}(\rho) \supseteq G'$.

70.28. Доказать, что если в задачах 69.22, 69.23 основное поле является полем комплексных чисел и группа G конечна, то представление ρ эквивалентно прямой сумме представлений $\rho_1, \ldots, \rho_m$.

70.29. Доказать, что если в задаче 69.22 основное поле является полем комплексных чисел и группа G конечна, то существует такая невырожденная матрица C, что для всех $g \in G$

$$C^{-1}\rho(g)C = \begin{pmatrix} \rho_1(g) & & 0 \\ & \ddots & \\ 0 & & \rho_m(g) \end{pmatrix}.$$

70.30. Пусть G — конечная группа порядка n, ρ — ее регулярное представление. Доказать, что

$$\operatorname{tr}\rho(g) = \begin{cases} 0, & g \neq 1, \\ n, & g = 1. \end{cases}$$

70.31. Доказать, что для любого неединичного элемента конечной группы существует неприводимое комплексное представление, переводящее его в неединичный оператор.

70.32. Пусть $\mathcal{A}$, $\mathcal{B}$ — линейные операторы в конечномерном векторном пространстве V над полем F характеристики 0 и $\mathcal{A}^3 = \mathcal{B}^2 = \mathcal{E}$, $\mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{A}^2$.

Доказать, что для всякого подпространства U, инвариантного относительно $\mathcal{A}$ и $\mathcal{B}$, существует подпространство W, инвариантное относительно $\mathcal{A}$, $\mathcal{B}$ и такое, что $V = U \oplus W$.

70.33. Найти все неэквивалентные двумерные комплексные представления групп:

а) $\mathbf{A}_4$; б) $\mathbf{S}_3$.

70.34. Найти число и размерности неприводимых комплексных представлений групп:

а) $\mathbf{S}_3$; б) $\mathbf{A}_4$; в) $\mathbf{S}_4$; г) $\mathbf{Q}_8$; д) $\mathbf{D}_n$; е) $\mathbf{A}_5$.

70.35. Сколько прямых слагаемых в разложении на неприводимые компоненты регулярного представления следующих групп:

а) $\mathbf{Z}_3$; б) $\mathbf{S}_3$; в) $\mathbf{Q}_8$; г) $\mathbf{A}_4$?

70.36. С помощью теории представлений доказать, что группа порядка 24 не может совпадать со своим коммутантом.

70.37. Могут ли неприводимые комплексные представления конечной группы исчерпываться:

а) тремя одномерными и четырьмя двумерными;

б) двумя одномерными и двумя пятимерными;

в) пятью одномерными и одним пятимерным?

70.38. Доказать, что в группе $\mathbf{GL}_2(\mathbb{C})$ нет подгруппы, изоморфной $\mathbf{S}_4$.

70.39. Доказать существование двумерного инвариантного подпространства в любом восьмимерном комплексном представлении группы $\mathbf{S}_4$.

70.40. Доказать существование одномерного инвариантного подпространства в любом пятимерном представлении группы $\mathbf{A}_4$.

70.41. Доказать, что число неприводимых представлений группы G строго больше числа неприводимых представлений любой ее факторгруппы по нетривиальной нормальной подгруппе.

70.42. Для каких конечных групп регулярное представление над полем $\mathbb{C}$ содержит лишь конечное число подпредставлений?

70.43. Доказать, что любое неприводимое представление конечной p-группы над полем характеристики p единично.

70.44. Пусть G — конечная p-группа и ρ — ее представление в конечномерном пространстве V над полем характеристики p. Доказать, что в V существует такой базис, что для любого $g \in G$ матрица оператора $\rho(g)$ — верхняя унитреугольная.

70.45. Пусть H — нормальная подгруппа в конечной группе G. Доказать, что размерность любого неприводимого представления группы G над полем F не превосходит $[G : H]m$, где m — наибольшая размерность неприводимого представления группы H над полем F.

70.46. Доказать, что в $\mathbf{GL}_n(\mathbb{C})$ существует лишь конечное число попарно несопряженных подгрупп фиксированного конечного порядка.

70.47. Пусть $\rho : G \to \mathbf{GL}_3(\mathbb{R})$ — неприводимое трехмерное вещественное представление конечной группы G и представление $\widetilde{\rho} : G \to \mathbf{GL}_3(\mathbb{C})$ получается как композиция отображения ρ со стандартным вложением $\mathbf{GL}_3(\mathbb{R}) \to \mathbf{GL}_3(\mathbb{C})$. Доказать, что представление $\widetilde{\rho}$ неприводимо.

70.48. Доказать, что всякое неприводимое неодномерное комплексное представление группы порядка p^3, где p — простое число, является точным.

70.49. Найти число неприводимых комплексных представлений некоммутативной группы порядка p^3 и их размерности.

70.50. Вещественное представление Φ циклической группы $\langle a \rangle$ порядка 4, при котором

$$\Phi(a) = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

разложить в прямую сумму неприводимых.

70.51. Рассмотрим вещественное трехмерное представление группы $G = \langle a \rangle_2 \times \langle b \rangle_2$, где

$$\Phi(a) = \begin{pmatrix} 5 & -4 & 0 \\ 6 & -5 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \Phi(b) = -E.$$

Разложить Φ в прямую сумму неприводимых представлений.

70.52. Рассмотрим двумерное комплексное представление Φ группы $G = \langle a\rangle_2 \times \langle b\rangle_2$, где

$$\Phi(a) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \Phi(b) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Разложить Φ в прямую сумму неприводимых представлений.

70.53. Доказать, что любая конечная подгруппа в группе $\mathbf{GL}(2, \mathbb{C})$ (соответственно в $\mathbf{GL}(2, \mathbb{C})$) сопряжена с подгруппой в группе унитарных (соответственно ортогональных матриц) размера 2.

70.54. Доказать, что всякая конечная подгруппа в $\mathbf{SL}_2(\mathbb{Q})$ является подгруппой одной из следующих групп: $\mathbf{D}_3$, $\mathbf{D}_4$, $\mathbf{D}_6$.

70.55. Доказать, что каждая конечная подгруппа в $\mathbf{SL}_2(\mathbb{R})$ сопряжена с подгруппой в $\mathbf{SO}_2(\mathbb{R})$ и потому является циклической.

70.56. Доказать, что каждая конечная подгруппа в $\mathbf{SL}_2(\mathbb{R})$ сопряжена с подгруппой в $\mathbf{SO}_2(\mathbb{R})$ и потому является циклической.

70.57. Доказать, что каждая конечная подгруппа в $\mathbf{GL}_2(\mathbb{R})$ сопряжена с подгруппой в $\mathbf{O}_2(\mathbb{R})$ и потому является либо циклической, либо группой диэдра $\mathbf{D}_n$, $n \geqslant 2$.

70.58. Пусть G — конечная неабелева простая группа. Доказать, что размерность любого неприводимого нетривиального комплексного или вещественного представления больше 2.

§ 71. Групповые алгебры и модули над ними

71.1. Является ли алгебра кватернионов вещественной групповой алгеброй:

а) группы кватернионов;

б) какой-либо группы?

71.2. Пусть V — векторное пространство над полем F с базисом (e_1, e_2, e_3), $\varphi : F[\mathbf{S}_3] \to \operatorname{End} V$ — гомоморфизм, где $\varphi(\sigma)(e_i) = e_{\sigma(i)}$ для всех $\sigma \in \mathbf{S}_3$ $(i = 1, 2, 3)$. Найти размерность ядра и размерность образа гомоморфизма φ.

71.3. Найти базис ядра гомоморфизма φ: $\mathbb{C}(\langle a\rangle_n) \to \mathbb{C}$, при котором $\varphi(a) = \varepsilon$, где ε — корень степени n из 1.

71.4. Пусть группа H изоморфна факторгруппе группы G. Доказать, что $F[H]$ изоморфна факторалгебре алгебры $F[G]$.

71.5. Пусть $G = G_1 \times G_2$. Доказать, что

$$F[G] \simeq F[G_1] \otimes F[G_2].$$

71.6. Пусть G — конечная группа, R — множество отображений из G в поле F. Определим на R операции, полагая для $f_1, f_2 \in R$

$$(\alpha f_1 + \beta f_2)(g) = \alpha f_1(g) + \beta f_2(g),$$
$$(f_1 f_2)(g) = \sum_{h \in G} f_1(h) f_2(h^{-1}g).$$

Доказать, что R — алгебра над полем F и отображение

$$f \mapsto \sum_{g \in G} f(g)g$$

из R в $F[G]$ — изоморфизм алгебр.

71.7. Доказать, что если группа G содержит элементы конечного порядка, то групповая алгебра $F[G]$ имеет делители нуля.

71.8. Доказать, что всякий неприводимый $F[G]$-модуль изоморфен фактормодулю регулярного $F[G]$-модуля.

71.9. Найти все коммутативные двусторонние идеалы групповой алгебры $\mathbb{C}[G]$ для:
а) $G = \mathbf{S}_3$; б) $G = \mathbf{Q}_8$; в) $G = \mathbf{D}_5$.

71.10. Найти все элементы x групповой алгебры $F[G]$, удовлетворяющие условию $xg = x$ при любом $g \in G$.

71.11. Найти базис центра групповой алгебры групп:
а) $\mathbf{S}_3$; б) $\mathbf{Q}_8$; в) $\mathbf{A}_4$.

71.12. Доказать, что в групповой алгебре A свободной абелевой группы ранга r нет делителей нуля. Поле частных для A изоморфно полю рациональных дробей от r переменных.

71.13. Пусть A — кольцо, V — A-модуль и $V = U \oplus W$, причем U — неприводимый модуль и в W нет подмодулей, изоморфных U. Доказать, что если α — автоморфизм модуля V, то $\alpha(U) = U$.

71.14. Пусть A — кольцо, A-модуль V разложен в прямую сумму подмодулей $V = U \oplus W$, $\varphi\colon U \to W$ — гомоморфизм A-модулей. Доказать, что $U_1 = \{x + \varphi(x) \mid x \in U\}$ есть A-подмодуль в V, изоморфный U, и $V = U_1 \oplus W$.

71.15. Пусть A — полупростая конечномерная алгебра над $\mathbb{C}$ и A-модуль V разлагается в прямую сумму попарно неизоморфных неприводимых A-модулей: $V = V_1 \oplus \ldots \oplus V_k$. Найти группу автоморфизмов модуля V.

71.16. Пусть A — полупростая конечномерная алгебра над $\mathbb{C}$ и A-модуль V есть прямая сумма двух изоморфных неприводимых A-

модулей. Доказать, что группа автоморфизмов A-модуля V изоморфна $\mathbf{GL}_2(\mathbb{C})$.

71.17. Пусть A — полупростая конечномерная алгебра над $\mathbb{C}$ и V — A-модуль, конечномерный над $\mathbb{C}$. Доказать, что V имеет конечное число A-подмодулей тогда и только тогда, когда он является прямой суммой попарно неизоморфных неприводимых A-модулей.

71.18. Пусть G — конечная группа, F — поле характеристики 0 и групповая алгебра $A = F[G]$ рассматривается как левый модуль над собой. Доказать, что для любого его подмодуля U и гомоморфизма A-модулей $\varphi : U \to A$ существует такой элемент $a \in A$, что $\varphi(u) = ua$ для всех $u \in U$.

71.19. Для каких конечных групп комплексная групповая алгебра является простой?

71.20. Пусть $A = F[G]$ (F — поле), G — конечная группа порядка $n > 1$, и для $n \cdot 1 \neq 0$ положим

$$e_1 = (n \cdot 1)^{-1} \sum_{g \in G} g, \quad e_2 = 1 - e_1.$$

Доказать, что Ae_1 и Ae_2 — собственные двусторонние идеалы и $A = Ae_1 \oplus Ae_2$.

71.21. Доказать, что равенство

$$xy = f(x,y) \cdot 1 + \sum_{g \in G \setminus \{1\}} \alpha_g \cdot g, \qquad \alpha_g \in F,$$

в групповой алгебре $F[G]$ задает на пространстве $F[G]$ симметрическую билинейную функцию и ядро этой функции f — двусторонний идеал в $F[G]$.

71.22. Пусть G — конечная группа, f — билинейная функция на $\mathbb{R}[G]$, определенная в задаче 71.21. Доказать, что f невырождена, и найти сигнатуру функции f для групп:

а) $\mathbf{Z}_2$; б) $\mathbf{Z}_3$; в) $\mathbf{Z}_4$; г) $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

71.23. Пусть H — подгруппа группы G и $\omega(H)$ — левый идеал в $F[G]$, минимальный среди левых идеалов, содержащих $\{h - 1 \mid h \in H\}$. Доказать, что если H — нормальная подгруппа, то идеал $\omega(H)$ двусторонний.

71.24. Разложить в прямую сумму полей групповые алгебры группы $\langle a \rangle_3$ над полями вещественных и комплексных чисел.

71.25. Доказать, что $\mathbb{Q}[\langle a\rangle_p]$ (p — простое число) есть прямая сумма двух двусторонних идеалов, один из которых изоморфен $\mathbb{Q}$, а другой $\mathbb{Q}(\varepsilon)$, где ε — первообразный корень степени p из 1.

71.26. Пусть G — конечная группа, $\operatorname{char} F$ не делит $|G|$, I — идеал в $F[G]$. Доказать, что $I^2 = I$.

71.27. Найти идемпотенты и минимальные идеалы в кольцах:
а) $\mathbb{F}_3[\langle a\rangle_2]$; б) $\mathbb{F}_2[\langle a\rangle_2]$; в) $\mathbb{C}[\langle a\rangle_2]$; г) $\mathbb{R}[\langle a\rangle_3]$.

71.28. Пусть G — конечная группа. Доказать, что при любом $a \in \mathbb{C}[G]$ уравнение $a = axa$ разрешимо в $\mathbb{C}[G]$.

71.29. Сколько различных двусторонних идеалов в алгебре:
а) $\mathbb{C}[\mathbf{S}_3]$; б) $\mathbb{C}[\mathbf{Q}_8]$?

71.30. Для каких конечных групп G групповая алгебра $\mathbb{C}[G]$ является прямой суммой $n = 1, 2, 3$ матричных алгебр?

71.31. Пусть G — группа, A — алгебра над полем F с единицей, φ — гомоморфизм $G \to A^*$. Доказать, что существует единственный гомоморфизм $F[G] \to A$, ограничение которого на G совпадает с φ.

71.32. Доказать, что если $\operatorname{char} F$ не делит порядка конечной группы G, то любой двусторонний идеал групповой алгебры $F[G]$ является кольцом с единицей. Верно ли это утверждение для произвольных алгебр с единицей?

71.33. Пусть F — поле характеристики $p > 0$, p делит порядок конечной группы G и
$$u = \sum_{g\in G} g \in F[G].$$
Доказать, что $F[G]u$ — подмодуль левого регулярного модуля, не выделяющийся прямым слагаемым.

71.34. Пусть $G = \langle a\rangle_p$, F — поле характеристики p, $\Phi\colon\ G \to \mathbf{GL}_2(F)$, где
$$\Phi(a^s) = \begin{pmatrix} 1 & s\cdot 1 \\ 0 & 1 \end{pmatrix}$$
— представление группы G. Указать такой $F[G]$ подмодуль U регулярного представления $V = F[G]$, что представление G на V/U изоморфно Φ. При каких p представление Φ изоморфно регулярному представлению?

71.35. Доказать, что алгебра $\mathbb{F}_2[\langle a\rangle_2]$ не является прямой суммой минимальных левых идеалов.

71.36. Пусть H — p-группа, являющаяся нормальной подгруппой в конечной группе G, F — поле характеристики p.

а) Доказать, что идеал $\omega(H)$ из задачи 71.23 нильпотентен.

б) Найти индекс нильпотентности идеала $\omega(H)$ при $G = \langle a\rangle_2$, $H = \langle a\rangle_2$, $F = \mathbb{F}_2$.

71.37. Доказать, что все идеалы групповой алгебры бесконечной циклической группы главные.

71.38. Доказать, что циклический модуль над алгеброй $F[\langle a\rangle_\infty]$ либо конечномерен над F, либо изоморфен левому регулярному $F[\langle a\rangle_\infty]$-модулю.

71.39. Пусть $A = \mathbb{C}[\langle g\rangle_\infty]$, $P = Ax_1 \oplus Ax_2$ — свободный A-модуль с базисом (x_1, x_2), H — подмодуль, порожденный в P элементами h_1, h_2. Разложить P/H в прямую сумму циклических A-модулей и найти их размерности, если:

а) $h_1 = gx_1 + x_2, \quad h_2 = x_1 - (g+1)x_2$;

б) $h_1 = g^2x_1 + g^{-2}x_2, \quad h_2 = g^4x_1 + (1-g)x_2$;

в) $h_1 = gx_1 + 2g^{-1}x_2, \quad h_2 = (1+g)x_1 + 2(g^{-2} + g^{-1})x_2$.

71.40. Пусть $\mathcal{A}, \mathcal{B}$ — линейные операторы на $V = F[x]$, $\mathcal{A}(f(x)) = f'(x)$, $\mathcal{B}(f(x)) = xf(x)$. Доказать, что отображение $\varphi : g \mapsto \mathcal{AB}$ продолжается до гомоморфизма $F[\langle g\rangle_\infty] \to \operatorname{End} V$, и найти $\operatorname{Ker}\varphi$.

71.41. Пусть M — максимальный идеал алгебры $A = F[\langle a\rangle_\infty]$ и $r = \dim_F(A/M)$.

Доказать, что:

а) если $F = \mathbb{C}$, то $r = 1$;

б) если $F = \mathbb{R}$, то $r = 1$ или $r = 2$;

в) если $F = \mathbb{F}_2$, то r может быть неограниченно велико.

71.42. Доказать, что групповая алгебра свободной абелевой группы конечного ранга является нетеровой.

71.43. Доказать, что в групповой алгебре свободной абелевой группы конечного ранга справедлива теорема о существовании и единственности разложения на простые множители.

71.44. Разложить в произведение простых множителей элемент групповой алгебры $A = \mathbb{C}[G]$ свободной абелевой группы G с базисом (g_1, g_2):

а) $g_1g_2 + g_1^{-1}g_2^{-1}$;

б) $1 + g_1^{-1}g_2 - g_1g_2^{-1} - g_1^{-2}g_2^2$.

71.45. Пусть G — свободная абелева группа с базисом (g_1, g_2). Найти факторалгебру групповой алгебры $A = F[G]$ по идеалу I, порожденному элементами:

а) $g_1g_2^{-1}$; б) $g_1 - g_2$; в) $g_1 - 1$ и $g_2 - 2$.

71.46. Доказать, что если группа G конечна и алгебра $\mathbb{C}[G]$ не имеет нильпотентных элементов, то G коммутативна.

71.47. Пусть H — нормальная подгруппа в группе G, V — некоторый $F[G]$-модуль и $(H-1)V$ — линейная оболочка элементов вида $(h-1)v$, где $h \in H$, $v \in V$.

Доказать, что:

а) $(H-1)V$ является $F[G]$-подмодулем в V;

б) если H — силовская (нормальная) p-подгруппа в G, $\operatorname{char} F = p$ и $(H-1)V = V$, то $V = 0$.

71.48. Доказать, что комплексные групповые алгебры групп $\mathbf{D}_4$ и $\mathbf{Q}_8$ изоморфны.

71.49. Найти число попарно неизоморфных комплексных групповых алгебр размерности 12.

71.50. Доказать, что число слагаемых в разложении групповой алгебры симметрической группы $\mathbf{S}_n$ над полем $\mathbb{C}$ в прямую сумму матричных алгебр равно числу представлений числа n в виде

$$n = n_1 + n_2 + \ldots + n_k,$$

где $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_k > 0$.

§ 72. Характеры представлений

72.1. Пусть элемент g группы G имеет порядок k и χ — n-мерный характер группы G. Доказать, что $\chi(g)$ есть сумма n (не обязательно различных) корней степени k из 1.

72.2. Пусть Φ — трехмерное комплексное представление группы $\langle a\rangle_3$ и $\chi_\Phi(g) = 0$ для некоторого $g \in \mathbf{Z}_3$. Доказать, что Φ эквивалентно регулярному представлению.

72.3. Пусть χ — двумерный комплексный характер группы $G = \langle a\rangle_3 \times \langle b\rangle_3$. Доказать, что $\chi(g) \neq 0$ для всякого $g \in G$.

72.4. Пусть χ — двумерный комплексный характер группы нечетного порядка. Доказать, что $\chi(g) \neq 0$ для любого $g \in G$.

72.5. Пусть Φ — n-мерное комплексное представление конечной группы G. Доказать, что $\chi_\Phi(g) = n$ тогда и только тогда, когда g принадлежит ядру представления Φ.

72.6. Пусть A — аддитивная группа n-мерного векторного пространства V над полем $\mathbb{F}_p$ и χ — неприводимый нетривиальный комплексный характер группы A. Доказать, что подмножество

$$\{a \in A \mid \chi(\alpha) = 1\}$$

есть $(n-1)$-мерное подпространство в V.

72.7. Пусть χ — комплексный характер конечной группы G и $m = \max\{|\chi(g)| \mid g \in G\}$. Доказать, что

$$H = \{g \in G \mid \chi(g) = m\}, \qquad K = \{g \in G \mid |\chi(g)| = m\}$$

— нормальные подгруппы в G.

72.8. Доказать, что двумерный комплексный характер χ группы $\mathbf{S}_3$ неприводим тогда и только тогда, когда $\chi((123)) = -1$.

72.9. Пусть χ — двумерный комплексный характер конечной группы G и $g \in G'$. Доказать, что если $\chi(g) \neq 2$, то χ неприводим.

72.10. Чему равно «среднее значение»

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)$$

неприводимого характера неединичной конечной группы G?

72.11. Доказать, что для любого элемента g неединичной конечной группы G существует такой нетривиальный неприводимый комплексный характер χ группы G, что $\chi(g) \neq 0$.

72.12. Доказать, что отображение группы G в $\mathbb{C}$ является одномерным характером группы G тогда и только тогда, когда это отображение является гомоморфизмом группы G в группу $\mathbb{C}^*$.

72.13. Доказать, что центральная функция, равная произведению двух одномерных характеров группы G, является одномерным характером группы G.

72.14. Доказать, что операция умножения функций определяет во множестве одномерных характеров группы G структуру абелевой группы $\widehat{G}$, двойственной к группе G.

72.15. Доказать, что для конечной циклической группы A группа $\widehat{A}$ — конечная циклическая группа того же порядка.

72.16. Пусть конечная абелева группа A разлагается в прямое произведение $A = A_1 \times A_2$, $\alpha_1 \in \widehat{A}_1$, $\alpha_2 \in \widehat{A}_2$. Доказать, что отображение $A \to \mathbb{C}^*$, переводящее элемент (a_1, a_2) в $\alpha_1(a_1) \cdot \alpha_2(a_2)$, является одномерным характером группы A и $\widehat{A} \simeq \widehat{A}_1 \times \widehat{A}_2$.

72.17. Пусть B — подгруппа конечной абелевой группы A и

$$B^0 = \{\alpha \in \widehat{A} \mid \ \alpha(b) = 1 \text{ для всякого } b \in B\}.$$

Доказать, что:

а) B^0 — подгруппа в $\widehat{A}$ и всякая подгруппа в $\widehat{A}$ совпадает с B^0 для некоторой подгруппы B;

б) $\widehat{B} \simeq \widehat{A}/B^0$;

в) $B_1 \subset B_2$ тогда и только тогда, когда $B_1^0 \supset B_2^0$;

г) $(B_1 \cap B_2)^0 = B_1^0 \cdot B_2^0$;

д) $(B_1 B_2)^0 = B_1^0 \cap B_2^0$.

72.18. Пусть Φ — гомоморфизм группы G в $\mathbf{GL}_n(\mathbb{C})$.

Доказать, что:

а) отображение $\Phi^*\colon\ g \mapsto (\Phi(g^{-1}))^t$ также является представлением группы G;

б) $\chi_\Phi(g) = \overline{\chi}_{\Phi^*}(g)$ для всякого $g \in G$;

в) представления Φ и Φ^* эквивалентны тогда и только тогда, когда значения характера χ вещественны.

72.19. Пусть Φ — неприводимое комплексное представление группы $\mathbf{S}_n$ и $\Phi'(\sigma) = \Phi(\sigma)\operatorname{sgn}\sigma$ $(\sigma \in \mathbf{S}_n)$.

Доказать, что Φ' — представление группы $\mathbf{S}_n$ и следующие утверждения эквивалентны:

а) $\Phi \sim \Phi'$;

б) ограничение представления Φ на $\mathbf{A}_n$ приводимо;

в) $\chi_\Phi(\sigma) = 0$ для любой нечетной подстановки $\sigma \in \mathbf{S}_n$.

72.20. В задаче 58.11 задана группа матриц из $\mathbf{M}_2(\mathbb{C})$, изоморфная группе кватернионов $\mathbf{Q}_8$. Доказать неприводимость этого двумерного представления группы $\mathbf{Q}_8$ и найти его характер.

72.21. Найти характер представления группы $\mathbf{S}_n$ в пространстве с базисом $(e_1, \ldots, e_n)$, задаваемого формулой

$$\Phi(\sigma)e_i = e_{\sigma(i)} \quad \text{для} \quad \sigma \in \mathbf{S}_n.$$

72.22. Найти характер двумерного представления группы $\mathbf{D}_n$, определяющегося изоморфизмом группы $\mathbf{D}_n$ с группой симметрий фиксированного правильного n-угольника.

72.23. Найти характер трехмерного представления группы $\mathbf{S}_4$, определяющегося изоморфизмом группы $\mathbf{S}_4$ с группой симметрий фиксированного правильного тетраэдра.

72.24. Найти характер представления группы $\mathbf{S}_4$, определяющегося изоморфизмом группы $\mathbf{S}_4$ с группой вращений куба.

72.25. Составить таблицу неприводимых характеров групп:

а) $\langle a\rangle_2$; б) $\langle a\rangle_3$; в) $\langle a\rangle_4$;
г) $\langle a\rangle_2 \times \langle b\rangle_2$; д) $\langle a\rangle_2 \times \langle b\rangle_2 \times \langle c\rangle_2$.

72.26. Составить таблицу характеров одномерных представлений и вычислить группу одномерных характеров (задача 72.14) для групп:
а) $\mathbf{S}_3$; б) $\mathbf{A}_4$; в) $\mathbf{Q}_8$; г) $\mathbf{S}_n$; д) $\mathbf{D}_n$.

72.27. Найти модуль определителя матрицы, строки которой совпадают со строками таблицы неприводимых характеров абелевой группы порядка n.

72.28. Составить таблицу неприводимых характеров групп:
а) $\mathbf{S}_3$; б) $\mathbf{S}_4$; в) $\mathbf{Q}_8$; г) $\mathbf{D}_4$; д) $\mathbf{D}_5$; е) $\mathbf{A}_4$.

72.29. Может ли характер представления некоторой группы порядка 8 принимать значения $(1, -1, 2, 0, 0, -2, 0, 0)$?

72.30. Разложить центральную функцию

$$(1, -1, i, -i, j, -j, k, -k) \mapsto (5, -3, 0, 0, -1, -1, 0, 0)$$

на $\mathbf{Q}_8$ по базису неприводимых характеров. Является ли она характером какого-либо представления?

72.31. Определить, какая из центральных функций на $\mathbf{S}_3$

$$f_1\colon\ (e, (12), (13), (23), (123), (132)) \mapsto (6, -4, -4, -4, 0, 0),$$
$$f_2\colon\ (e, (12), (13), (23), (123), (132)) \mapsto (6, -4, -4, -4, 3, 3)$$

является характером, и указать это представление.

72.32. Пусть A — аддитивная группа конечномерного векторного пространства V над полем $\mathbb{F}_p$ и Ψ — нетривиальный неприводимый (комплексный) характер аддитивной группы поля $\mathbb{F}_p$.

а) Доказать, что всякий неприводимый характер χ группы A имеет вид
$$\chi(a) = \Psi(l(a))$$
для некоторой линейной функции $l \in V^*$.

б) Установить изоморфизм двойственной группы $\widehat{A}$ (см. задачу 72.14) и аддитивной группы пространства V^*.

в) Построить изоморфизм A и $\widehat{\widehat{A}}$.

72.33. Пусть в условиях предыдущей задачи f — комплекснозначная функция на A. Определим функцию $\widehat{f}$ на $\widehat{A}$, полагая для $\chi \in \widehat{A}$
$$\widehat{f}(\chi) = \frac{1}{|A|} \sum_{a \in A} f(a)\chi(a) = (f, \chi)_A.$$

а) Доказать, что
$$f = \sum_{\chi \in \widehat{A}} \widehat{f}(\chi) \cdot \chi.$$

б) Доказать, что
$$\widehat{fg}(\chi) = \sum_{\varphi \in \widehat{A}} \widehat{f}(\varphi)\widehat{g}(\varphi^{-1} \cdot \chi).$$

в) Сравнить функции f на A и $\widehat{\widehat{f}}$ на $\widehat{\widehat{A}}$, используя изоморфизм из задачи 72.32, в).

72.34. Пусть A — аддитивная группа поля $\mathbb{F}_p$. Рассмотрим функцию f на A, полагая
$$f(a) = \begin{cases} 0, & \text{если} \quad a = 0, \\ 1, & \text{если} \quad a = x^2 \text{ для некоторого } x \in \mathbb{F}_p^*, \\ -1, & \text{в остальных случаях.} \end{cases}$$

Доказать, что если χ — неприводимый комплексный характер группы A, то $|(f, \chi)_A| = p^{-1/2}$.

72.35. Пусть G — конечная группа, H — ее подгруппа. Доказать, что центральная функция на H, получающаяся ограничением на H характера группы G, является характером группы H.

72.36. Пусть Φ — матричное n-мерное представление группы G. Построим представление Ψ группы G на пространстве квадратных матриц порядка n, полагая для $\mathcal{A} \in \mathbf{M}_n(K)$

$$\Psi_g(A) = \Phi_g A^t \Phi_g.$$

Выразить χ_Ψ через χ_Φ.

72.37. Найти неприводимые слагаемые представления Ψ задачи 72.36 и их кратности, если:

а) Φ — двумерное неприводимое представление группы $\mathbf{S}_3$;

б) Φ — представление из задачи 72.23;

в) Φ — двумерное представление группы $\mathbf{Q}_8$ из задачи 72.20.

72.38. Пусть Φ — матричное n-мерное представление группы G. Построим представление Ψ группы G на пространстве квадратных матриц $\mathbf{M}_n(K)$, полагая

$$\Psi_g(A) = \Phi_g \cdot A.$$

Выразить χ_Ψ через χ_Φ.

72.39. Пусть $\rho : G \to \mathbf{GL}(V)$ — регулярное комплексное представление группы $\langle a \rangle_n$. Найти кратность единичного представления группы $\mathbf{Z}_n$ в разложении представления $\rho^{\otimes m}$ (см. задачу 69.19) на неприводимые представления.

72.40. Пусть ρ — двумерное неприводимое комплексное представление группы $\mathbf{S}_3$. Разложить на неприводимые представления $\rho^{\otimes 2}$ и $\rho^{\otimes 3}$.

72.41. Пусть $\rho : \langle a \rangle_n \mapsto \mathbf{GL}(V)$ — комплексное регулярное представление группы $\langle a \rangle_n$. Найти кратность единичного представления группы в разложении на неприводимые компоненты представления, возникающего на пространстве кососимметрических m-контравариантных тензоров на V (см. задачу 69.19).

* * *

72.42. Пусть χ — характер группы G, f — центральная функция на G,

$$f(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$

Доказать, что f — характер группы G.

72.43. Пусть Φ — представление группы $G = \mathbf{S}_3$ в пространстве $\mathbb{C}(G)$ всех комплекснозначных функций на G:

$$(\Phi_\sigma f)(x) = f(\sigma^{-1}x), \qquad f \in \mathbb{C}(G), \quad x \in G, \quad \sigma \in G,$$

$f_0 \in \mathbb{C}(G)$ и V_0 — линейная оболочка множества элементов вида $\Phi_\sigma f_0$, где $\sigma \in G$.

Найти характер ограничения Φ на V_0 для:

а) $f_0(\sigma) = \operatorname{sgn}\sigma$;

б) $f_0(\sigma) = \begin{cases} 1, & \text{если} \quad \sigma \in \{e, (12)\}, \\ 0 & \text{в противном случае;} \end{cases}$

в) $f_0(\sigma) = \begin{cases} 1, & \text{если} \quad \sigma \in \{e, (123), (132)\}, \\ 0 & \text{в противном случае;} \end{cases}$

г) $f_0(\sigma) = \begin{cases} 1, & \text{если} \quad \sigma \in \{e, (13), (23)\}, \\ -1, & \text{если} \quad \sigma \in \{(12), (123), (132)\}. \end{cases}$

72.44. Пусть Φ — комплексное представление конечной группы G на пространстве V, Ψ — представление группы G на пространстве W. Обозначим через $T(\Phi, \Psi)$ пространство таких линейных отображений S из V в W, что $S \circ \Phi_g = \Psi_g \circ S$ для всех $g \in G$.

Доказать, что

$$\dim T(\Phi, \Psi) = (\chi_\Phi, \chi_\Psi)_G.$$

§ 73. Первоначальные сведения о представлениях непрерывных групп

Если не указывается противное, то все рассматриваемые в этом параграфе представления предполагаются конечномерными.

* * *

73.1. Пусть F есть поле $\mathbb{R}$ или $\mathbb{C}$.

Доказать, что:

а) для любой матрицы $A \in \mathbf{M}_n(F)$ отображение $P_A\colon\ t \mapsto e^{tA}$ $(t \in \in F)$ является дифференцируемым матричным представлением аддитивной группы поля F;

б) всякое дифференцируемое матричное представление P аддитивной группы поля F имеет вид P_A, где $A = P'(0)$;

в) представления P_A и P_B эквивалентны тогда и только тогда, когда матрицы A и B подобны.

73.2. Доказать, что P является матричным представлением аддитивной группы поля $\mathbb{R}$, и найти такую матрицу A, что $P = P_A$, если:

а) $P(t) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$; б) $P(t) = \begin{pmatrix} \operatorname{ch} t & \operatorname{sh} t \\ \operatorname{sh} t & \operatorname{ch} t \end{pmatrix}$;

в) $P(t) = \begin{pmatrix} e^t & 0 \\ 0 & 1 \end{pmatrix}$; г) $P(t) = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}$;

д) $P(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$; е) $P(t) = \begin{pmatrix} 1 & e^t - 1 \\ 0 & e^t \end{pmatrix}$.

73.3. Какие из матричных представлений группы $\mathbb{R}$ из задачи 73.2 эквивалентны?

73.4. В каком случае представления P_A и P_{-A} эквивалентны для $F = \mathbb{C}$?

73.5. Найти все дифференцируемые комплексные матричные представления групп:

а) $\mathbb{R}_+^*$; б) $\mathbb{R}^*$; в) $\mathbb{C}^*$;

г) $\mathbf{U}$ (предполагается дифференцируемость представления по аргументу комплексного числа z).

73.6. Всякое ли комплексное линейное представление группы $\mathbb{Z}$ получается ограничением на $\mathbb{Z}$ некоторого представления группы $\mathbb{C}$?

73.7. Найти в пространстве $\mathbb{C}^n$ все подпространства, инвариантные относительно матричного представления P_A (см. задачу 73.1) в случае, когда характеристический многочлен матрицы A не имеет кратных корней.

73.8. Доказать, что матричное представление P_A (см. задачу 73.1) вполне приводимо тогда и только тогда, когда матрица A диагонализируема.

73.9. Пусть R_n — пространство однородных многочленов степени n от x, y с комплексными коэффициентами. Для

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{C})$$

и $f \in R_n$ положим

$$(\Phi_n(A)f)(x, y) = f(ax + cy, bx + dy).$$

Доказать, что ограничение представления Φ_n на подгруппу $\mathbf{SU}_2(\mathbb{C})$ неприводимо.

73.10. Пусть $G = \mathbf{GL}_2(\mathbb{C})$. Комплексную функцию на G назовем *полиномиальной*, если она есть многочлен от матричных элементов.

а) Пусть $t(A) = \operatorname{tr} A$, $d(A) = \det A$. Доказать, что t и d — центральные полиномиальные функции на G.

б) Доказать, что любая центральная полиномиальная функция на G является многочленом от t и d.

в) Пусть $A = (a_{ij}) \in G$ и $R = \mathbb{C}[x, y]$. Обозначим через $\Psi(A)$ гомоморфизм $R \to R$, для которого

$$\Psi(A)\colon\ x \mapsto a_{11}x + a_{12}y,$$
$$\Psi(A)\colon\ y \mapsto a_{21}x + a_{22}y.$$

Доказать, что Ψ — представление группы G в пространстве R и подпространства однородных многочленов степени n инвариантны относительно представления Ψ.

г) Доказать, что для $A \in \mathbf{SL}_2(\mathbb{C})$ ограничение $\Psi(A)$ на под пространство R_n совпадает с оператором $\Phi_n(A)$ из задачи 73.9.

д) Пусть χ_n — характер ограничения $\Psi|_{R_n}$. Доказать, что

$$\chi_n = t\chi_{n-1} - d\chi_{n-2}.$$

73.11. Пусть $\mathbb{H}$ — пространство комплексных матриц вида

$$X = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$$

со структурой четырехмерного евклидова пространства $(X, X) = \det X$ и $\mathbb{H}_0 = \{X \in \mathbb{H} \mid \operatorname{tr} X = 0\}$.

Доказать, что:

а) отображение $P\colon\ \mathbf{SU}_2 \to \mathbf{GL}(\mathbb{H}_0)$, определенное формулой

$$P(A)\colon\ X \mapsto AXA^{-1},$$

является (вещественным) линейным представлением группы $\mathbf{SU}_2$, $\operatorname{Ker} P = \pm E$, а $\operatorname{Im} P$ состоит из всех собственных ортогональных преобразований пространства H_0;

б) отображение $R : \mathbf{SU}_2 \times \mathbf{SU}_2 \to \mathbf{GL}(\mathbb{H})$, определенное формулой $R(A, B) :\quad X \mapsto AXB^{-1}$, является (вещественным) линейным представлением группы $\mathbf{SU}_2 \times \mathbf{SU}_2$, $\operatorname{Ker} R = \{(E, E), (-E, -E)\}$, а $\operatorname{Im} R$ состоит из всех собственных ортогональных преобразований пространства $\mathbb{H}_0$;

в) комплексификация линейного представления P изоморфна ограничению представления Φ_2 группы $\mathbf{SL}_2$ из задачи 73.9 на подгруппу $\mathbf{SU}_2$.

73.12. Пусть G — топологическая связная разрешимая группа и ρ — непрерывный гомоморфизм G в группу невырожденных линейных операторов в конечномерном комплексном пространстве V.

Доказать, что:

а) в V существует ненулевой вектор, являющийся собственным для всех операторов $\rho(g)$, $g \in G$;

б) в V существует такой базис $e_1, \ldots, e_n$, что все матрицы $\rho(g)$, $g \in G$, в этом базисе верхнетреугольные.

73.13. Пусть F — алгебраически замкнутое поле и G — разрешимая группа невырожденных линейных операторов в конечномерном векторном пространстве V над F. Доказать, что существуют такие базис $e_1, \ldots, e_n$ в V и нормальная подгруппа N в G конечного индекса (зависящего только от n), что N состоит из верхнетреугольных матриц.

ОТВЕТЫ И УКАЗАНИЯ

54.1. а) Нет. б) Да. в) Нет. г) Нет. д) Да. е) Нет. ж) Да.

54.2. Все элементы вида $e_a = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix}$ нейтральны слева; нейтральных справа и двусторонних нейтральных нет. Относительно e_a обратимы справа все элементы $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ при $x \neq 0$; обратимы слева лишь элементы вида $\begin{pmatrix} x & ax \\ 0 & 0 \end{pmatrix}$ при $x \neq 0$.

54.3. Любой элемент нейтрален справа; относительно любого нейтрального x каждый элемент обратим слева и лишь сам x обратим справа при $|M| = 1$.

54.4. Да; не существует, если $|M| > 1$.

54.5. а) 3. б) Нет.

54.6. Рассмотреть отображение $A \to \overline{A}$.

55.1. Все множества в а), кроме $\mathbb{N}$, все множества в в), кроме $\mathbb{N}_0$ и $\mathbb{Z}_0$, г), д), е), ж), з), и) при $r = 1$ и при $r = 0$, л) при $\varphi_k = 2k\pi/n$ (считая, что $\varphi_1 < \varphi_2 < \ldots < \varphi_n$).

55.2. Группе и) при $r = 1$.

55.5. б), в), г), д), з), и), к), л).

55.6. а), г), д) при $d = 1$, е), з), л), м), н), о), п), р), с) при $\lambda < 0$, т).

55.13. а) и в).

55.16. Рассмотреть элемент $(xy)^2$.

55.17. а), в), д), е).

55.18. Для коммутативных групп.

55.19. Будет.

55.20. $\{\mathbb{Z}, n\mathbb{Z}, \mathbf{UT}_2(\mathbb{Z})\}$, $\{\mathbb{Q}, \mathbf{UT}_2(\mathbb{Q})\}$, $\{\mathbb{R}, \mathbf{UT}_2(\mathbb{R}), \mathbb{C}, \mathbf{UT}_2(\mathbb{C})\}$, $\{\mathbb{Q}^*\}$, $\{\mathbb{R}^*\}$, $\{\mathbb{C}^*\}$.

55.21. $[k] \to [2^k]$ и $[k] \to [3^k]$.

55.22. Если в группе тождественно $x^2 = e$, то см. задачу 55.16; в противном случае найти некоммутирующие элементы x и y, для которых $x^2 = y^3 = 1$.

55.23. Других автоморфизмов нет.

55.25. а) Равнобедренный, но не равносторонний треугольник или пара точек.

б) $[KB] \cap [LC] \cap [MA]$, где K, L, M — середины сторон правильного треугольника ABC.

в) Правильный треугольник.

г) Параллелограмм или прямоугольник.

55.26. $\mathbf{D}_4$ изоморфна группе из задачи 55.5, л); $\mathbf{Q}_8$ изоморфна группе из задачи 55.6, г).

55.32. а) $\mathbf{Z}_2$. б) $\mathbf{Z}_{p-1}$. в) $\mathbf{S}_3$. г) $\mathbf{S}_3$.
д) $\mathbf{D}_4$. е) $\mathbf{S}_4$.

55.34. а) $\{e, (123), (132)\}$. б), в) см. задачу 55.26.

55.36. Использовать задачу 55.26.

55.37. Использовать задачи 55.26 и 55.35.

55.39. Эти группы попарно не изоморфны. Рассмотреть центры групп.

56.1. б) Если $A \cup B$ — подгруппа, $x \in A \setminus B$, $y \in B \setminus A$, рассмотреть xy.
в) Рассмотреть $x \in (C \setminus A) \cap (C \setminus B)$.

56.2. Для любого элемента a подполугруппы найдутся различные k и l такие, что $a^k = a^l$, откуда $a \cdot a^{k-l-1} = a^{k-l} = e$, так что элемент a обратим в подполугруппе; утверждение неверно для $\mathbb{N} \subset \mathbb{Z}$.

56.3. а) 6. б) 5. в) 12. г) 8. д) 4. е) 8. ж) 2.

56.4. Рассмотреть случай, когда порядок $E + pX$ является простым числом.

56.5. а) Доказать по индукции, что для любого натурального числа n найдутся такие целые числа m, k, что $(3 + 4i)^n = (3 + 5m) + (4 + 5k)i$.
б) вытекает из а).

56.6. а) 2. б) 4. в) 20. г) 0.

56.7. б) Использовать а).
в) Рассмотреть перестановки (123), (12) и (13).

56.8. а) Для взаимно простых чисел p и q существуют u и v такие, что $pu + qv = 1$.
б) Следует из а).
в) Рассмотреть (12) и (123).

56.9. Воспользоваться тем, что порядок цикла равен его длине.

56.11. $n/\text{НОД}(n, k)$.

56.13. $p^m - p^{m-1}$.

56.14. а) См. задачу 56.11. б) См. указание к задаче 56.8.
в) Рассмотреть наименьшее из натуральных чисел s, для которых $a^s \in H$.
г) Использовать в). Если d_1 и d_2 — различные делители n, то соответствующие подгруппы имеют различные порядки.

56.15. Если $x^k = e$ и $x = a^l$, то $a^{kl} = e$, откуда $kl \vdots n$ и $l \vdots \text{НОД}(n, k)$; элемент a^k имеет порядок $n/\text{НОД}(n, k)$, (см. задачу 56.10) и поэтому удовлетворяет условию при $\text{НОД}(n, l) = n/k$.

56.18. Пусть $n = |G|$, $d = d(G)$, m — наименьшее общее кратное порядков элементов G.

а) По теореме Лагранжа $d|n$, откуда $x^d = 1$, так что d делится на порядок любого элемента группы, т. е. $m|d$.

б) Пусть $d = p_1^{k_1} \ldots p_s^{k_s}$ — разложение на простые множители; в силу а) в G существует элемент x, порядок которого равен $p_1^{k_1} l$, где l и p_1 взаимно просты;

тогда x^l имеет порядок $p_1^{k_1}$; аналогично получаются элементы $x_2, \ldots, x_s$, и произведение $x_1, \ldots, x_s$ (см. задачу 56.8, а)) имеет порядок d.

Утверждения б) и в) неверны для $\mathbf{S}_3$.

56.19. $\mathbf{U}_{p^\infty}$.

56.20. б) Неверно: в группе G биекций плоскости на себя композиция симметрий относительно двух параллельных прямых является параллельным переносом.

в) Множество корней всех степеней из 1; множество диагональных матриц с корнями из 1 на главной диагонали.

56.21. Неверно: в $\mathbf{GL}_2(\mathbb{R})$ элементы порядка 2 не составляют подгруппу (см. ответ к задаче 56.20, б)).

56.22. $\mathbf{Z}_{p^k}$ (p — простое число).

56.24. а) Выписать явно все подгруппы (см. задачу 56.14, г)).

б) $\mathbf{Z}_{p^k}$ (p — простое число); заметить, что группа является объединением своих циклических подгрупп, и если они образуют цепь, то группа циклическая, далее использовать задачу 56.14, г).

в) $\mathbf{Z}_{p^n}$ $\mathbf{U}_{p^\infty}$; пусть p — наименьший из порядков элементов группы; p — простое число, так как из $p = kl$ следует, что в подгруппе $\langle x\rangle$ имеется элемент порядка k; $\langle x\rangle_p$ — наименьшая нееединичная подгруппа, содержащаяся во всех других подгруппах, так что порядки всех элементов делятся на p и на самом деле являются степенями p.

56.25. $\bigcup\limits_{n\in N} \left\langle \dfrac{1}{n!}\right\rangle$.

56.26. $\cos\dfrac{2k\pi}{n} + i\sin\dfrac{2k\pi}{n} \to [k]$.

56.27. а) $\cong$ б). в) $\cong$ е). г) $\cong$ д) $\cong$ ж).

56.28. Если в группе G нет элементов порядка 2, то

$$G = \{(x, x^{-1})(x \neq e)\} \cup \{e\}$$

и $|G|$ нечетен.

56.29. Эта группа не является циклической, так как она имеет порядок 8, но порядок каждого элемента не превосходит 4.

56.30. См. задачу 56.24, в).

56.31. б) Показать, что если конечная абелева группа содержит не более одной подгруппы любого заданного порядка, то она циклическая, и воспользоваться а).

56.32. а) E, $\mathbf{S}_3$, $\langle (ij)\rangle$, $\langle (123)\rangle$.

б) E, $\mathbf{D}_4$, $\langle(13)\rangle$, $\langle(24)\rangle$, $\langle(12)(34)\rangle$, $\langle(13)(24)\rangle$, $\langle(14)(23)\rangle$, $\langle(1234)\rangle$, $\mathbf{V}_4$.

в) E, $\mathbf{Q}_8$, $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$.

г) E, $\mathbf{A}_4$, $\langle(12)(34)\rangle$, $\langle(13)(24)\rangle$, $\langle(14)(24)\rangle$, $\mathbf{V}_4$, $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, $\langle(234)\rangle$.

56.34. а) $(ij) = (1i)(1j)(1i)$.

56.35. а) $\mathbf{D}_4$. б) $\mathbf{D}_2(\mathbb{R})$ при $a \neq b$; $\mathbf{SL}_2(\mathbb{R})$ при $a = b$. в) $\langle g\rangle$.

56.36. а) $\mathbf{D}_4$.

б) $\mathbf{S}_3$ как подгруппа $\mathbf{S}_4$, состоящая из перестановок с неподвижным элементом 4.

в) $\{e,(12),(34),(12)(34)\}$.

г) $\mathbf{S}_4$. д) $\mathbf{A}_4$.

56.41. Использовать задачу 56.40.

57.1. а) Две орбиты; одна состоит только из одного нулевого вектора, другая — из всех ненулевых векторов.

б) Каждая орбита состоит из всех векторов одинаковой длины.

в) Каждому подмножеству $I \subseteq \{1,2,\ldots,n\}$ отвечает орбита O_I, состоящая из тех векторов x, у которых координата x_i равна 0 тогда и только тогда, когда $i \in I$. Всего 2^n различных орбит.

г) Всего $n+1$ различных орбит O, $O_1,\ldots,O_n$, где O состоит только из нулевого вектора, а O_i, $i \geqslant 1$, — из всех таких векторов $x = \sum_{t=1}^n x_t e_t$, для которых $x_i \neq 0$ и $x_j = 0$ для всех $j > i$.

57.2. а) G_a содержит только тождественный оператор.

б) G_a состоит из операторов с матрицами $A = (a_{ij})$ такими, что $\sum_{j=1}^n a_{ij} = 1$ для любого $i = 1,2,\ldots,n$.

57.3. а) Группа ортогональных операторов в плоскости $\langle x\rangle^{\perp}$.

б) Группа поворотов в плоскости $\langle x\rangle^{\perp}$.

57.4. а) Орбита G равна X.

б) G_U состоит из всех матриц вида

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix},$$

где A — обратимая матрица размера k, C — обратимая матрица размера $n-k$ и B — матрица размера $k \times (n-k)$.

57.5. в) G_f состоит из всех верхнетреугольных матриц в базисе $e_1,\ldots,e_n$.

57.9. Орбиты: а) $\{1,5,4,9\}$, $\{2,8\}$, $\{3\}$, $\{6,10,7\}$;

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

57.10. а) $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$.

б) Рассмотреть, например, отображение

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto e, \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto (12)(34),$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto (13)(24), \qquad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto (14)(23)$$

или установить изоморфизм, занумеровав стороны ромба.

в) Две орбиты: $\{A,C\}$ и $\{B,D\}$,

$$G_A = G_C = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\};$$

$$G_B = G_D = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

57.11. В группу входят n различных поворотов n-угольника вокруг центра и n осевых симметрий; $|\mathbf{D}_n| = 2n$.

57.12. а) 24. б) 12.

в) 60. Все вершины правильного многогранника образуют одну орбиту относительно действия группы вращения многогранника. При этом порядок стационарной подгруппы равен числу ребер, выходящих из вершины.

57.13. а) Каждому вращению куба сопоставить перестановку на множестве диагоналей куба.

б) Каждому движению тетраэдра сопоставить перестановку на множестве его вершин; полученное отображение в $\mathbf{S}_4$ инъективно, ибо каждое аффинное преобразование определяется однозначно образами четырех точек общего положения; сюръективность вывести из того факта, что в образе, кроме подгруппы $\mathbf{A}_4$, есть нечетная подстановка.

57.14. а) 4. б) 5.

57.15. а) Орбита G равна Y. б) $G_a = 1$.

57.17. а) $\{az \mid |a| = 1\}$. б) Орбита нуля — весь круг. в) 1.

57.19. По условию задачи $m = hm_0$ для некоторого $h \in G$. Отсюда

$$gm = g(hm_0) = (gh)m_0 = (hg)m_0 = h(gm_0) = hm_0 = m.$$

57.20. а) Заметить, что $ag_1H = ag_2H \to g_1H = g_2H$; и для каждого $x \in G$ $xH = a(a^{-1}xH)$.

б) Проверить, что $\sigma_{ab} = \sigma_a\sigma_b$.

в) Доказать, что условия $gH = agH$ и $a \in gHg^{-1}$ равносильны.

57.21. а) Каждый смежный класс $\{e\}$, $\{x\}$, $\{x^2\}$, $\{x^3\}$ состоит из одного элемента, присвоим им соответственно номера 1, 2, 3, 4, тогда $\sigma_x = (1234)$, $\sigma_{x^2} = (13)(24)$, $\sigma_{x^3} = (1432)$, σ_e — тождественная перестановка.

б) Пусть x — данная симметрия, а y — поворот квадрата на 90°. Тогда $G = H \cup yH \cup y^2H \cup y^3H$, и, занумеровав смежные классы в указанном порядке, имеем: σ_e — тождественная перестановка, $\sigma_y = (1234)$, $\sigma_{y^2} = (13)(24)$, $\sigma_{y^3} = (14)(23)$, $\sigma_x = (24)$, $\sigma_{xy} = (12)(34)$, $\sigma_{y^2x} = (13)$, $\sigma_{y^3x} = (14)(23)$. (Для вычисления воспользоваться соотношением $xy = y^{-1}x$.)

57.23. а) Подгруппа, порожденная группой Клейна и циклом (12).

б) Множество всех степеней данной перестановки.

57.24. а) Подгруппа диагональных матриц. б) Вся группа.

в) Множества матриц вида $\begin{pmatrix} a+b & 2a \\ 3a & 4a+b \end{pmatrix}$, где $a, b \in \mathbb{R}$ и $b^2+5ab-2a^2 \neq 0$.

г) Множество матриц вида $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, где $a, b \in \mathbb{R}$, $a \neq 0$.

57.25. а) Подгруппа всех диагональных матриц.

б) Подгруппа всех матриц вида $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, где A и B — невырожденные матрицы порядка k и $n-k$ соответственно.

57.26. A_1 и A_3 сопряжены, так как имеют одинаковую жорданову форму, а A_1 и A_2 не сопряжены, так как имеют разные жордановы нормальные формы.

57.27. а) C_{ij} как группа порождается матрицами $E + \lambda E_{pq}$, где $j \neq p \neq$ $\neq q \neq i$.

б) λE, $\lambda^n = 1$.

в) $E + {}^t ab$, где a, b — строки, причем $b^t a = 0$. Последнее утверждение вытекает из в).

57.28. а) $\mathbf{SO}_2(\mathbb{R})$. б) $\pm E$, симметрии относительно OX и OY.

57.30. а) $\mathbf{S}_3 = \{e\} \cup \{(12), (13), (23)\} \cup \{(123), (132)\}$.

б) $\mathbf{A}_4 = \{e\} \cup \{(12)(34), (13)(24), (14)(23)\} \cup$
$\cup \{(123), (134), (142), (243)\} \cup \{(132)(143), (124), (234)\}$.

в) Симметрия относительно средних линий квадрата, повороты квадрата на углы $\pm\pi/2$, центральная симметрия квадрата, тождественное отображение.

57.31. а) Единичная группа.

б) Группа порядка 2; поскольку все неединичные элементы группы сопряжены, порядок группы n должен делится на $n-1$.

в) Группа изоморфна группе подстановок $\mathbf{S}_3$ или имеет порядок 3. В любой группе есть класс, состоящий только из единицы. Пусть n — порядок группы G, а k, l — числа сопряженных элементов в каждом из классов, $k \leqslant l$. Тогда n делится на k и l и $1 + k + l = n$. Возможные решения: 1) $n = 3$, $k = l = 1$; 2) $n = 4$, $k = 1$, $l = 2$, это решение нужно отбросить, поскольку группы порядка 4 абелевы (т. е. имеют 4 класса); 3) $n = 6$, $k = 2$, $l = 3$; чтобы установить изоморфизм $G \cong \mathbf{S}_3$, использовать действие группы G сопряжениями (см. задачу 57.22 на классе, состоящем из трех элементов).

57.32. а) $\{(12)(34), (13)(24), (14)(23)\}$.

б) $\{(123), (132), (124), (142), (134), (143), (234), (243)\}$.

57.34. Пусть $a = (i_1 \dots i_k)(i_{k+1} \dots i_l)\dots$ — разложение перестановки a на независимые циклы. Для вычисления перестановки $c = bab^{-1}$ записать b в виде

$$\begin{pmatrix} i_1 & \dots & i_k & i_{k+1} & \dots & i_l & \dots \\ j_1 & \dots & j_k & j_{k+1} & \dots & j_l & \dots \end{pmatrix}.$$

Тогда $c = (j_1 \dots j_k)(j_{k+1} \dots j_l)\dots$

57.35. а) 5. б) 7. в) 11.

г) $\dfrac{n+6}{2}$, если n четно, и $\dfrac{n+3}{2}$, если n нечетно; для нахождения числа элементов, сопряженных с данным, достаточно найти порядок его централизатора; обратить внимание на то, что поворот вокруг центра на угол π совмещает n-угольник с собой, если n четно.

57.36. Необходимость следует из равенства следов сопряженных матриц. Для доказательства достаточности равенства $\varphi_1 + \varphi_2 = 2\pi k$ в качестве сопрягающей матрицы для канонических форм рассмотреть матрицу $\mathrm{diag}\,(-1, -1, 1)$.

57.37. а) Сопряженные подгруппы имеют одинаковый порядок.

б) $K = gHg^{-1}$, где $g = \mathrm{diag}\,(2, 1)$.

57.38. а) $N(H) = \langle H, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\rangle$.

б) $N(H)$ состоит из всех невырожденных матриц второго порядка, в которых $a_{21} = 0$.

в) $N(H)$ состоит из 8 перестановок, выписанных в ответе к задаче 57.21, б).

57.39. а) $\mathrm{Aut}\, G$ — циклическая группа порядка 4, состоящая из автоморфизмов возведения в степень $k = 1, 2, 3, 4$.

б) $\mathrm{Aut}\, G$ — группа второго порядка, в которую кроме тождественного автоморфизма входит автоморфизм возведения в пятую степень.

57.40. а) Каждый автоморфизм группы $\mathbf{S}_3$ определяется своим действием на трех элементах второго порядка.

б) Любая перестановка неединичных элементов группы $\mathbf{V}_4$ определяет ее автоморфизм.

57.41. а) Да, $\operatorname{Aut}\mathbf{Z}_9$ — циклическая группа порядка 6, порождаемая автоморфизмом возведения в квадрат.

б) Нет, $|\operatorname{Aut}\mathbf{Z}_8| = 4$, но квадрат каждого автоморфизма — тождественное отображение.

57.42. $|\operatorname{Aut}\operatorname{Aut}\operatorname{Aut}\mathbf{Z}_9| = 1$. Использовать задачи 57.41 и 57.39.

57.43, 57.44. *Каргаполов М.И.*, *Мерзляков Ю.И.* Основы теории групп. — М.: Наука, 1982. — Гл. 2, § 5.3.

57.45. Пусть $\mathbf{D}_4 = \langle a, b \mid a^4 = b^2 = (ab)^2 = 1\}$. Тогда $\operatorname{Aut}\mathbf{D}_4 = \langle \varphi, \psi\rangle$, где $\varphi(a) = a$, $\varphi(b) = ba$, $\psi(a) = a^{-1}$, $\varphi(b) = b$. При этом $\varphi^4 = \psi^2 = (\varphi\psi) = 1$, т. е. $\operatorname{Aut}\mathbf{D}_4 \simeq \mathbf{D}_4$, $\operatorname{Int}\mathbf{D}_4 = \langle \varphi^2, \psi\rangle$.

57.46. Пусть $\mathbf{D}_n = \langle a, b \mid a^n = b^2 = (ab)^2 = 1\}$. Тогда $\operatorname{Aut}\mathbf{D}_n = \langle \varphi, \psi_k,\ (k, n) = 1\rangle$, где $\varphi(a) = a$, $\varphi(b) = ba$, $\varphi(a) = a^k$, $\psi(b) = b$, где $(k, n) = 1$, $1 \leqslant k \leqslant n - 1$.

58.1. б) Использовать теорему об определителе произведения матриц.

в) Использовать теорему о четности произведения перестановок.

58.4. а) $\mathbf{A}_3$. б) $\mathbf{V}_4$.

в) $\mathbf{V}_4$ и $\mathbf{A}_4$. Воспользоваться тем, что порядок подгруппы делит порядок группы, что нормальная подгруппа вместе с любым элементом содержит все сопряженные, а также задачами 57.27 и 57.30.

58.5. Например, $K = \{(12)(34)\}$, $H = \mathbf{V}_4$.

58.6. $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in A \cap B$.

58.7. Пусть $c \in C$ и $G = H \cup Hx$ разложение группы G на два смежных класса. Тогда любой элемент из C может быть записан в виде hch^{-1} или в виде $hxcx^{-1}h^{-1}$, где $h \in H$.

58.9. Пять классов сопряженности, состоящих из 1, 15, 20, 12 и 12 элементов. Воспользоваться задачами 57.34 и 58.7. Группа $\mathbf{A}_5$ состоит из четырех классов элементов, сопряженных в $\mathbf{S}_5$, представителями которых являются e, (12)(34), (124) и (12345). Первый и второй состоят из нечетного числа элементов (1 и 15), поэтому являются классами сопряженности и в $\mathbf{A}_5$. Третий также не распадается в $\mathbf{A}_5$ на два класса, ибо в качестве x (см. указание к задаче 58.7) можно выбрать перестановку (45), но тогда $(45)(123)(45)^{-1} = (123)$. Наконец, четвертый распадается в $\mathbf{A}_5$ на два класса, ибо число его элементов 24 не делит порядок группы $\mathbf{A}_5$.

58.10. В соответствии с задачей 58.9 порядок нормальной подгруппы, делящей число 60, можно составить из слагаемых 1, 15, 20, 12, 12, причем в качестве одного из слагаемых непременно нужно взять 1, ибо e входит в любую подгруппу.

58.11. Сначала доказать в). Центр состоит из $\pm E$. Других подгрупп порядка 2 нет, поэтому все они нормальны (см. задачу 58.3). Классы сопряженности $\{E\}$, $\{-E\}$, $\{\pm I\}$, $\{\pm J\}$, $\{\pm K\}$.

58.12. Подгруппы $\mathbf{D}_k$ в $\mathbf{D}_n$, где k делит n, и подгруппа вращений в $\mathbf{D}_n$.

58.15. λE.

58.17. в) Вытекает из задачи 56.4.

г) По в) при естественном гомоморфизме $\mathbf{SL}_n(\mathbb{Z})$ в $\mathbf{SL}_n(\mathbf{Z}_3)$ группа G отображается инъективно.

58.18. Если α_g — автоморфизм $x \to gxg^{-1}$, то α_e — тождественный автоморфизм, $(\alpha_g)^{-1} = \alpha_{g^{-1}}$, $\alpha_g\alpha_h = \alpha_{gh}$ и

$$(\varphi\alpha_g\varphi^{-1})(x) = \varphi(g\varphi^{-1}(x)g^{-1}) = \varphi(g)x\varphi(g^{-1}) = \alpha_{\varphi(g)}(x)$$

для любого $\varphi \in \operatorname{Aut} G$.

58.20. а) $\mathbf{S}_2$ при $n = 2$ и $\{e\}$ при $n \neq 2$.

б) $\mathbf{A}_3$ при $n = 3$ и $\{e\}$ при $n \neq 3$.

в) Центр является единичным при нечетных n, а при четных включает еще поворот на угол π.

58.22. Элемент лежит в центре тогда и только тогда, когда он совпадает со всеми сопряженными ему элементами. Поэтому, если в центре лежит лишь одна единица, то $p^n = 1 + p^{k_1} + \ldots + p^{k_i}$ $(k_i \geqslant 1)$ (число элементов любого класса сопряженности делит порядок группы). Но тогда 1 делится на p.

58.23. б) Центр состоит из матриц вида $E + bE_{13}$.

в) Класс сопряженности нецентрального элемента $E + aE_{12} + bE_{13} + cE_{23}$ состоит из матриц вида $E + aE_{12} + xE_{13} + cE_{23}$ $(x \in \mathbf{Z}_p)$.

58.24. а) $\{\lambda E\}$. б) $\{\pm E\}$. в) Вся группа. г) $\{E\}$.

д) $\{\pm E\}$. е) $\{\alpha E \mid \alpha^n = 1\}$. ж) $\{E + \lambda E_{1n}\}$.

58.27. Группа H изоморфна факторгруппе группы G.

58.28. Гомоморфизм определяется образом порождающего элемента a. Ниже указаны возможные образы этого элемента.

а) Любой элемент группы; число гомоморфизмов равно n.

б) $e, b^3, b^6, b^9, b^{12}, b^{15}$.

в) e, b, b^2, b^3, b^4, b^5.

г) e, b^5, b^{10}.

д) e.

58.29. Найти образ $a/2$, если $a \mapsto 1$.

58.30. а) $\mathbf{Z}_n$. б) $\mathbf{Z}_4$. в) $\mathbf{Z}_3$. г) $\mathbf{Z}_2$.

58.31. Построить линейное отображение F^n на F^{n-k} с ядром H.

58.32. Рассмотреть отображения:

а) $x \to \cos 2\pi x + i \sin 2\pi x$; б) $z \to \dfrac{z}{|z|}$;

в) $z \to |z|$; г) $z \to z^n$; д) $z \to z^n$.

е) $z \to \left(\dfrac{z}{|z|}\right)^n$; ж) $z \to \dfrac{z}{|z|}$; з) $z \to |z|$.

58.33. Для доказательства изоморфизма вида $X/Y \cong \mathbb{Z}$ найти гомоморфизм X на $\mathbb{Z}$ с ядром Y.

58.34. Воспользоваться тем, что каждый элемент $g \in G$ однозначно представим в виде kh, где $k \in K$, $h \in H$. Доказать, что отображение $g \to k$ является при этом гомоморфизмом $G \to K$.

58.35. В силу задачи 57.13 группа $\mathbf{S}_4$ действует на кубе. Отсюда, если занумеровать три пары противоположных граней куба числами 1, 2, 3, мы получим действие группы на множестве $\{1, 2, 3\}$. Проверить, что ядром этого действия является подгруппа $\mathbf{V}_4$.

58.36. Проверить, что пересечение N всех подгрупп группы G, сопряженных в G с H, является нормальной в G подгруппой. С помощью задачи 57.20 установить, что факторгруппа G/N изоморфна некоторой подгруппе группы $\mathbf{S}_k$.

58.37. Пусть N — нормальная в G подгруппа, построенная в решении задачи 58.36. Тогда $p!$ делится на $|G/N|$ и $|G/N| \geqslant p$, ибо $N \subseteq H$. Но по условию p — минимальный простой делитель числа $|G|$, а значит, и у числа $|G/N|$ не может быть простых делителей, меньших, чем p, так как $|G|$ делится на $|G/N|$. С другой стороны, в разложении числа $p!$ простые делители, кроме одного, меньше p. Поэтому $|G/N| = p$, т. е. индексы, а следовательно, и порядки подгрупп N и H совпадают. Из включения $N \subseteq H$ следует тогда равенство $N = H$ (и нормальность подгруппы H).

58.38. Любой линейный оператор действует на одномерных подпространствах, переставляя их. Проверить, что в двумерном пространстве над $\mathbf{Z}_3$ имеется четыре одномерных подпространства, которые можно произвольным образом переставить с помощью подходящего линейного оператора. Проверить, наконец, что ядром действия является центр группы $\mathbf{GL}_2(\mathbf{Z}_3)$.

58.39. В собственную подгруппу порядка n попадают все смежные классы вида $k/n + \mathbb{Z}$, где k — любое целое число.

58.40. Рассмотреть отображение, сопоставляющее каждому $g \in G$ автоморфизм $x \to gxg^{-1}$.

58.41. Если $G/\mathbb{Z} = \langle a\mathbb{Z} \rangle$, то любые элементы $x, y \in G$ имеют вид $x = a^k z_1$, $y = a^l z_2$, а тогда $xy = yx$.

58.42. Использовать задачи 58.22 и 58.41.

58.43. Использовать задачи 58.40 и 58.41.

58.44. $p^2 + p - 1$, причем p классов состоят из одного элемента, а остальные — из p элементов. Вывести из задач 58.22 и 58.41, что центр $\mathbb{Z}$ имеет порядок p. Централизатор любого элемента $a \notin \mathbb{Z}$ имеет порядок p^2, так как он содержит $\mathbb{Z} \cup \{a\}$ и не совпадает со всей группой. Число сопряженных с a элементов равно $p^3 : p^2 = p$.

58.45. а) Проверить, что произведения $a_0 b_1 \ldots a_{n-1} b_{n-1} a_n$ элементов максимальных подгрупп A и B составляют подгруппу C, строго содержащую A и B (а значит, совпадающую с G). Элементы из $A \cap B$ перестановочны с элементами из C, так как A и B коммутативны.

б) Пусть H — некоторая максимальная подгруппа в G: $H \neq \{e\}$, так как G не является циклической группой. Обозначим $|H| = m$ и $|G| = n = lm$. Из максимальности подгруппы H и простоты группы G следует, что нормализатор N подгруппы H в группе G совпадает с H, т. е. существует l различных сопряженных с H максимальных подгрупп. Если допустить, что их попарные пересечения содержат только e, то в их объединение входит $1 + l(m-1)$ элементов из G. Поскольку $lm - l + 1 < n$, то найдется элемент, не лежащий ни в одной из них, а значит, найдется содержащая этот элемент максимальная подгруппа K, не сопряженная с H. Пусть опять $|K| = m_1$ и $n = l_1 m_1$. Тогда, допустив, как и выше, что $l + l_1$ максимальных подгрупп попарно пересекаются по $\{e\}$, получим

$$1 + l(m-1) + l_1(m_2-1) \geqslant 1 + \frac{n}{2} + \frac{n}{2} > n$$

элементов в G.

в) Одна из максимальных подгрупп некоммутативна, иначе, как видно из пп. а), б), в группе G был бы нетривиальный центр вопреки ее простоте.

58.46. См.: *Gorenstein D.* Finite groups. — Harper and Row, 1968. — Гл. 2, § 8.

58.47, 58.51. См.: *Супруненко Д.А.* Группы матриц. — М.: Наука, 1972. — Гл. III.

58.52. См.: Изоморфизмы классических групп над целостными кольцами. — М.: Мир, 1980. — С. 252–258.

59.1. а) $(q^n-1)(q^n-q)\times\ldots\times(q^n-q^{n-1})$. При подсчете числа невырожденных матриц заметить, что если уже выбраны i первых строк, то для выбора $(i+1)$-й строки имеется $q^n - q^i$ возможностей: действительно, всего существует q^n различных строк длины n над полем из q элементов, но в качестве $(i+1)$-й подходят лишь те из них, которые не являются линейными комбинациями i строк, выбранных раньше. Число таких линейных комбинаций — это число упорядоченных наборов, составленных из i коэффициентов, т. е. q^i.

б) $\dfrac{1}{1-q}(q^n-1)(q^n-q)\times\ldots\times(q^n-q^{n-1})$; подгруппа $\mathbf{SL}_n(\mathbb{F}_q)$ есть ядро гомоморфизма $A \to \det A$ группы $\mathbf{GL}_n(\mathbb{F}_q)$ на мультипликативную группу поля $\mathbf{Z}_q$ (состоящую из $q-1$ элементов). Отсюда по теореме о гомоморфизме $|\mathbf{GL}_n(\mathbb{F}_q)/\mathbf{SL}(\mathbb{F}_q)| = q-1$; остается применить а) и теорему Лагранжа.

59.2. а) Нет; найти число э лементов второго порядка в этих группах.

б) Нет; заметить, что матрица $2E$ лежит в центре группы $\mathbf{SL}_2(\mathbf{Z}_3)$ и воспользоваться задачей 58.14, а).

59.3. а) 2-подгруппы $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$; 3-подгруппа $\langle(123)\rangle$.

б) 2-подгруппа $\mathbf{V}_4$; 3-подгруппы $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, $\langle(234)\rangle$.

59.4. а) Первая и вторая (см. ответ к задаче 59.3, а)) из силовских 2-подгрупп сопряжены с помощью перестановки (23), первая и третья — с помощью (13).

б) Первая и вторая из силовских 3-подгрупп сопряжены с помощью перестановки (12)(34), первая и третья — с помощью (13)(24), первая и четвертая — с помощью (23)(14).

59.5. Занумеровав вершины квадрата, получить изоморфное представление группы $\mathbf{D}_4$ перестановками: $\mathbf{D}_4 \simeq P \subset \mathbf{S}_4$. Поскольку $|\mathbf{D}_4| = 8$ и $|\mathbf{S}_4| = 24 = 8\cdot 3$, P — силовская 2-подгруппа в $\mathbf{S}_4$. Другие силовские 2-подгруппы группы $\mathbf{S}_4$ изоморфны P в силу сопряженности.

59.6. а) В подгруппе $\{e, (1324), (1423), (12)(34), (13)(24), (14)(23), (12), (34)\}$.

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

в) В каждой из трех силовских 2-подгрупп.

59.7. Эти группы неизоморфны по задаче 59.2. Если в некоторой неабелевой группе G порядка 8 есть подгруппа второго порядка, не лежащая в центре, то $G \cong \mathbf{D}_4$; это следует из задач 57.20 и 59.5. В противном случае обозначаем e и $-e$ — элементы центра группы G (по задачам 58.22 и 58.23 центр группы G состоит из двух элементов). Пусть $i, j \in G$ и $ij \neq ji$. Обозначим $k = ij$, $i^{-1} = -i$, $j^{-1} = -j$, $k^{-1} = -k$. Проверить, что естественное отображение группы G на группу кватернионов является изоморфизмом.

59.8. Решая в группе $\mathbf{SL}_2(\mathbf{Z}_3)$ уравнение $X^2 = E$, получаем лишь два решения: $X = \pm E$. Аналогично находим шесть элементов порядка 4, решая уравнение $X^2 = -E$. Из них уже не извлекаются квадратные корни, т. е. в $\mathbf{SL}_2(\mathbf{Z}_3)$ нет элементов порядка 8. Поскольку получилось восемь элементов, порядки которых — степени двойки, в $\mathbf{SL}_2(\mathbf{Z}_3)$ есть лишь одна силовская 2-подгруппа, так как $|\mathbf{SL}_2(\mathbf{Z}_3)| = 24 = 8 \cdot 3$ по задаче 59.2. Следовательно, это подгруппа нормальна. Она неабелева, так как, например, элементы $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ и $\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$ имеют порядок 4 и не коммутируют. Далее использовать задачу 59.7.

59.9. а) 5. б) 10. в) 6.

59.10. p^m, где $m = \left[\dfrac{n}{p}\right] + \left[\dfrac{n}{p^2}\right] + \left[\dfrac{n}{p^3}\right] + \ldots$

59.11. $(p-2)!$. Число $p!$ делится на p, но не делится на p^2. Значит, каждая силовская p-подгруппа состоит из степеней одного цикла $(i_1 i_2 \ldots i_p)$. Число таких циклов равно $(p-1)!$, а число различных порождающих в циклической подгруппе порядка p равно $p-1$.

59.12. Воспользоваться теоремой о сопряженности силовских подгрупп.

59.13. а) $|\mathbf{SL}_2(\mathbf{Z}_p)| = p(p-1)(p+1)$ (см. задачу 59.1). Значит, силовская p-подгруппа имеет порядок p.

б) Нормализатор состоит из всех матриц вида $\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}$, где $x \neq 0$.

в) Поскольку порядок нормализатора равен $p(p-1)$, его индекс, а значит, и число различных силовских p-подгрупп, равно $p+1$.

г) Использовать задачу 59.1.

д) Множество всех матриц вида $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$, где $x, z \neq 0$.

е) $p+1$.

59.14. Доказать, что порядок подгруппы и максимальная степень числа p, делящая $|\mathbf{GL}_n(\mathbb{Z}_p)|$, равны $p^{n(n-1)/2}$ (см. задачу 59.1).

59.15. а) Если p нечетно, то силовская p-подгруппа единственна и состоит из поворотов правильного n-угольника на углы $2\pi k/p^l$, $0 \leqslant k < p^l$, где p^l — наибольшая степень числа d, делящая n. Пусть $n = 2^l \cdot m$, где m нечетно. Тогда в $\mathbf{D}_n$ содержится m различных силовских 2-подгрупп. Каждую такую подгруппу можно получить, если выбрать правильный 2^l-угольник, вершины которого содержатся среди вершин данного n-угольника (а центр тот же), и рассмотреть все движения, совмещающие его с собой.

б) При $p = 2$ в качестве сопрягающих элементов можно взять повороты на углы $2\pi k/m$, $0 \leqslant k < m-1$.

59.16. Пусть $|G| = p^l \cdot m$, где m не делится на p, и $|\mathrm{Ker}\,\varphi| = p^s \cdot t$, где t не делится на p. Тогда $H \simeq G/\mathrm{Ker}\,\varphi$, и по теореме Лагранжа порядок силовской p-подгруппы P в H равен p^{l-s}. С другой стороны, $|P \cap \mathrm{Ker}\,\varphi| \leqslant p^s$, ибо $|\mathrm{Ker}\,\varphi|$ делится на $|P \cap \mathrm{Ker}\,\varphi|$. Значит, $|\varphi(P)| = |P/P \cap \mathrm{Ker}\,\varphi| \geqslant p^{l-s}$, что и требовалось.

59.17. Очевидно, что $P \subseteq \varphi_A(P) \times \varphi_B(P)$, где φ_A и φ_B — гомоморфизмы проецирования на A и B соответственно. Это включение на самом деле является равенством, как видно из сравнения порядков $|P|$, $|\varphi_A(P)|$ и $|\varphi_B(P)|$.

59.18. а) Пусть $|G| = p^l \cdot m$ и $|H| = p^s \cdot t$, где m, t не делятся на p. Тогда порядок p-подгруппы PH/H в G/H не больше p^{t-s}. Значит, порядок ядра $P \cap H$ естественного гомоморфизма $P \to PH/H$ не меньше p^s, что и требуется доказать.

б) В качестве P и H взять, например, различные силовские 2-подгруппы в $\mathbf{S}_3$ (см. задачу 59.3).

59.19. См. задачу 58.36.

59.20. Использовать теорему о том, что число различных силовских p-подгрупп делит порядок группы и сравнимо с 1 по модулю p, а также 59.12 и 58.6.

59.21. Пять силовских 2-подгрупп и одна силовская 5-подгруппа (см. указание к задаче 59.20).

59.22. а) К силовской 3-подгруппе H применить задачу 58.36.

б) Если силовская 5-подгруппа не является нормальной, то, как следует из теоремы о числе силовских подгрупп, в группе должно быть 16 различных 5-подгрупп. Поскольку их попарные пересечения тривиальны, в группе не больше, чем $80 - 16 \cdot 4 = 16$ элементов, порядки которых суть степени двойки, они могут образовывать лишь одну силовскую 2-подгруппу, которая, следовательно, нормальна.

в) Решение аналогично б).

59.23. а) См. указание к задаче 59.20.

б) Рассмотреть все матрицы вида $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, где $b \in \mathbf{Z}_q$ и a принадлежат подгруппе порядка p в мультипликативной группе поля $\mathbf{Z}_q$ (эта подгруппа существует, так как $|q-1|$ делится на p).

59.24. 48.

59.25. Индукция по порядку группы.

59.26. Индукция по порядку группы. Выбрать в G нормальную подгруппу индекса p.

60.1. Если $\mathbb{Z} = A \oplus B$, где $A \neq 0$, $B \neq 0$, и $m \in A$, $n \in B$, то $mn \in A \cap \cap B = \{0\}$. Аналогичное соображение применимо и к группе $\mathbb{Q}$.

60.2. В группах $\mathbf{S}_3$, $\mathbf{A}_4$, $\mathbf{S}_4$ нет нормальных подгрупп, пересекающихся по единице, а в $\mathbf{Q}_8$ любая нетривиальная подгруппа содержит -1; поэтому перечисленные группы неразложимы в прямое произведение.

60.3. Если $\langle a \rangle$ — аддитивная циклическая группа порядка $n = n_1 \cdot n_2$, где $(n_1, n_2) = 1$, то $\langle a \rangle = \langle a^{n_1} \rangle + \langle a^{n_2} \rangle$ (указанные слагаемые имеют соответственно порядки n_2 и n_1, и поэтому их пересечение тривиально).

60.5. а) $\langle a \rangle_6 = \langle a^3 \rangle \times \langle a^2 \rangle$.

б) $\mathbf{Z}_{12} \simeq \mathbf{Z}_3 \oplus \mathbf{Z}_4$.

в) $\mathbf{Z}_{60} \simeq \mathbf{Z}_3 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_5$ (укажите порождающие элементы слагаемых).

60.6. Следует из представления комплексных чисел в тригонометрической форме.

60.7. Элемент из $\mathbf{Z}_{2^n}$ обратим тогда и только тогда, когда его класс содержит нечетное число, поэтому порядок мультипликативной группы кольца $\mathbf{Z}_{2^n}$ равен 2^{n-1}. Элемент $3 = 1 + 2 \pmod{2^n}$ имеет порядок 2^{n-2} и его циклическая подгруппа тривиально пересекается с подгруппой $\{\pm 1\}$; поэтому их произведение имеет порядок 2^{n-1}, т. е. совпадает с группой $\mathbf{Z}^*_{2^n}$.

60.8. а) Произведению порядков сомножителей.

б) Наименьшему общему кратному порядков компонент.

60.9. Используя предыдущую задачу, показать, что $(A_1 + A_2 + \ldots + A_{i-1}) \cap A_i = \{0\}$ при любом i.

60.11. Если $m = p_1^{k_1} \ldots p_r^{k_r}$, то в группе существуют элементы порядков $p_1^{k_1}, \ldots, p_r^{k_r}$ (см., например, задачу 60.3). Пользуясь задачами 60.8, 60.7, показать, что их сумма имеет порядок m. В группе $\mathbf{S}_3$ есть элементы порядка 2 и 3, но нет элемента порядка 6. Использовать 56.8, б).

60.12. $\{\pm 1\} \times \langle 2 \rangle = \{\pm 1\} \times \langle -2 \rangle$.

60.13. Одно из слагаемых совпадает с A, другое порождается суммой порождающего элемента группы $\mathbb{Z}$ с любым элементом группы A. Таким образом, будет $|A|$ прямых разложений.

60.14. Каждый класс группы $A \times B$ является произведением класса из A на класс из B.

60.16. В качестве C взять подгруппу, порожденную прообразами базисных элементов A/B.

60.17. $G = A \oplus \operatorname{Ker} \pi$.

60.18. Абелевость группы B существенна, так как образы групп A_1 и A_2 коммутируют при любом гомоморфизме $\varphi : A_1 \times A_2 \to B$.

60.20. а), б), в) $\mathbf{Z}_6$.

г) $\operatorname{Hom}(A_1, B) \oplus \operatorname{Hom}(A_2, B)$.

д) $\operatorname{Hom}(A, B_1) \oplus \operatorname{Hom}(A, B_2)$.

е) $\mathbf{Z}_d$, где $d = (m, n)$.

ж) $\mathbf{Z}_n$. з) $\{0\}$. и) $\mathbb{Z}$.

60.21. Гомоморфизму $\varphi : \mathbb{Z} \to A$ сопоставить $\varphi(1)$.

60.24. а) $\mathbb{Z}$. б) $\mathbf{Z}_n$.

в) $\mathbb{Q}$; показать, что если $\varphi : \mathbb{Q} \to \mathbb{Q}$ эндоморфизм, то $\varphi(r) = r\varphi(1)$.

60.25. а) Отображение $x \to nx$ имеет тривиальное ядро тогда и только тогда, когда в группе нет элементов, порядок которых делит n, и если $n = p_1^{k_1} \ldots p_r^{k_r}$ — каноническое разложение на простые множители, это означает, что примарные компоненты групп относительно простых чисел $p_1, \ldots, p_r$ равны 0.

б) Сюръективность отображения означает, что в группе уравнение $nx = g$ разрешимо для любого g.

60.26. Эндоморфизму φ поставить в соответствие матрицу так же, как это делается для линейных операторов.

60.27. а) $\mathbf{Z}_2$. б) $\mathbb{Q}^*$.

в) Единичная при $n = 1$, циклическая порядка 2 при $n = 2$, $\mathbf{Z}_2 \times \mathbf{Z}_{2^{n-2}}$ при $n > 2$.

г) Группа целочисленных матриц с определителем ± 1. Во всех случаях использовать задачи 60.23 и 60.24.

60.28. а) $\langle a \rangle_{30} = \langle a_1 \rangle_2 \oplus \langle a_2 \rangle_{15}$, где $a_1 = 15a$, $a_2 = 2a$. При любом автоморфизме $\varphi(\langle a_1 \rangle) = \langle a_1 \rangle$, $\varphi(\langle a_2 \rangle) = \langle a_2 \rangle$, так как a_1 и a_2 имеют взаимно простые порядки. Остается заметить, что у $\langle a_1 \rangle$ имеется лишь тождественный автоморфизм.

б) Пусть $\mathbb{Z} = \langle a \rangle$, $\mathbf{Z}_2 = \langle b \rangle$; при любом автоморфизме $\varphi(\mathbf{Z}_2) = \mathbf{Z}_2$ и $\varphi(b) = b$. Кроме того, $\varphi(a)$ может быть равен $a, -a, a + b, -a + b$. Нетрудно проверить, что каждый из этих автоморфизмов в квадрате дает тождественный автоморфизм.

60.29. В обозначениях ответа к предыдущей задаче $\varphi(a) = na + \varepsilon b$, $\varphi(b) = \delta b$, где $n \in \mathbb{Z}$, $\varepsilon, \delta = 0, 1$. Не коммутируют эндоморфизмы φ_1, φ_2, где $\varphi_1(a) = a$, $\varphi_1(b) = 0$, $\varphi_2(b) = 0$, $\varphi_2(a) = b$.

60.30. Всякая примарная компонента инвариантна относительно любого эндоморфизма данной группы; воспользоваться задачей 60.20.

60.31. Индукция по числу порождающих элементов группы. Если группа циклическая и равна $\langle a \rangle$ (операция — сложение), U — ее ненулевая подгруппа, k — наименьшее положительное число такое, что $ka \in U$, то U порождается элементом ka. Действительно, если $ma \in U$, разделим m с остатком на k: $m = qk + r$. Тогда $ra = ma - q(ka) \in U$, следовательно, $r = 0$ и $ma = q(ka)$. Предположим, что утверждение доказано для группы с $n - 1$ порождающим, $G = \langle a_1, \ldots, a_{n-1} \rangle$ и $U \subseteq G$ — подгруппа. Рассмотрим элементы $u = m_1 a_1 + \ldots + m_n a_n \in U$. Если $m_n = 0$ для всех $u \in U$, то $U \subseteq \langle a_1, \ldots, a_{n-1} \rangle$, и можно воспользоваться индуктивным предположением. В противном случае пусть m_n^0 — наименьшее положительное число для всех элементов $u \in U$, т. е. существует $u^0 \in U$ такой, что $u^0 = m_1^0 a_1 + \ldots + m_n^0 a_n$. Очевидно, любое число m_n, входящее в разложение любого $u \in U$, делится на m_n^0 нацело, скажем, $m_n = q m_n^0$. Тогда $u - qu^0 \in U \cap \langle a_1, \ldots, a_{n-1} \rangle$. Эта подгруппа, по предположению индукции порождается $n - 1$ элементом. Тогда U порождается теми же элементами и u^0.

60.32. а) Если φ — гомоморфизм группы G на себя, не являющийся автоморфизмом, то $\operatorname{Ker} \varphi \subset \operatorname{Ker} \varphi^2 \subset \ldots$ — строго возрастающая цепочка подгрупп, и ее объединение не может порождаться конечным множеством элементов: каждый из них лежал бы в члене цепочки с конечным номером. Остается воспользоваться предыдущей задачей.

б) Рассмотреть дифференцирование.

60.33. Если бы свободные абелевы группы рангов m и n $(m \neq m)$ были изоморфны, то ранг не был бы инвариантом свободной абелевой группы, однако его инвариантность может быть доказана так же, как основная лемма о линейной зависимости. Можно использовать и такое соображение: если G — свободная абелева группа ранга n, то $|G/2G| = 2^n$.

60.34. Воспользоваться единственностью разложения конечнопорожденных абелевых групп.

60.35. Индукция по порядку группы и числу m.

60.36. Использовать доказательство теоремы единственности конечных абелевых групп.

60.37. Использовать теорему единственности для разложений.

60.40. а) Есть. б) Нет. в) Нет.

60.41. (3,27); показать, что $\langle a\rangle_9 \oplus \langle b\rangle_{27} = \langle a \oplus 3b\rangle \oplus \langle b\rangle$.

60.42. а) Нет: вторая группа циклическая, а первая нет.
б) Изоморфны. в) Не изоморфны.

60.43. а) 3. б) 4.

60.46. Доказать, что если конечная абелева группа не является циклической, то в ней найдется подгруппа типа (p, p) (см. задачу 60.40). Учесть, что уравнение $x^p = 1$ имеет в поле не более p решений.

60.47. Пусть $a_1, \ldots, a_n$ — максимальная независимая система элементов. Рассмотреть элемент $1 + a_1 \cdots a_n$ и вывести отсюда, что группа F^* конечна.

60.48. Использовать задачу 60.46.

60.50. Если y_i $(j = 1, \ldots, n)$ составляют базис, то через них можно выразить x_i $(i = 1, \ldots, n)$ с целочисленной матрицей B коэффициентов. Тогда $AB = E$ и $\det A = \pm 1$, где $A = (a_{ij})$.

60.51. Использовать доказательство основной теоремы о конечно порожденных абелевых группах, основанное на приведении матрицы к диагональному виду элементарными преобразованиями строк и столбцов.

60.52. а) $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$. б) $\mathbf{Z}_{31}$. в) $\mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$. г) $\mathbf{Z}_2 \oplus \mathbf{Z}_4$.
д) $\mathbf{Z}_4 \oplus \mathbb{Z}$. е) $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$. ж) $\mathbf{Z}_3$. з) $\mathbb{Z} \oplus \mathbb{Z}$. и) $\mathbb{Z}$. к) $\{0\}$.
л) $\mathbf{Z}_3 \oplus \mathbf{Z}_4$. м) $\mathbf{Z}_3 \oplus \mathbf{Z}_6 \oplus \mathbb{Z}$.

60.53. 3.

60.55. Учитывая задачи 60.30 и 60.24, остается показать, что кольцо эндоморфизмов конечной примарной нециклической группы некоммутативно. Не уменьшая общности, можно рассмотреть группу $\langle a\rangle_{p^k} \oplus \langle b\rangle_{p^l}$, $k \geqslant l$. В силу задачи 60.20 любой эндоморфизм такой группы имеет вид

$$\varphi(a) = s_1 a + t_1 b, \qquad \varphi(b) = s_2 a + t_2 b,$$

где s_2 делится на p^{k-l}. Не коммутируют, например, автоморфизмы φ, ψ такие, что $\varphi(a) = a$, $\varphi(b) = 0$, $\psi(a) = b$, $\psi(b) = 0$.

60.56. Доказать конечную порожденность H. Для этого выбрать максимальную независимую над $\mathbb{R}$ систему элементов $e_1, \ldots, e_k$ в H. Доказать, что H порождается $e_1, \ldots, e_k$ и конечным множеством $H \cap D$, где $D = \{\sum x_i e_i \mid 0 \leqslant x_i \leqslant 1\}$.

60.59. Использовать задачу 60.56.

60.60. Отображение $x - nx$ есть автоморфизм циклической группы $\langle a\rangle$ (имеет тривиальное ядро), поэтому при подходящем x будет $nx = a$.

60.63. Делимость группы $\mathbb{Q}$ очевидна. Если $\varepsilon^{p^k} = 1$, то существует δ такое, что $\delta^p = \varepsilon$. Если $q \neq p$ — простое число, то $(q, p^k) = 1$, и можно воспользоваться задачами 60.60 и 60.61.

60.65. То, что сумма подгрупп A и B прямая, следует из условия; надо показать, что она равна G. Пусть существует элемент $g \notin A \oplus B$. Подгруппа $\langle g\rangle$ имеет ненулевое пересечение с $A \oplus B$ — иначе сумма $A \oplus B \oplus \langle g\rangle$ прямая и вместо B можно было бы взять $B \oplus \langle g\rangle$, что невозможно в силу максимальности B. Пусть $ng \in A \oplus B$. Можно считать n простым числом (если бы было не так, вместо g мы взяли бы $\dfrac{n}{p}g$ при некотором $p|n$). Итак, $ng = a + b$, $a \in A$, $b \in B$. Ввиду делимости A в ней есть элемент a_1 такой, что $na_1 = a$. Получаем, что $ng_1 = b$, где $g_1 = g - a$ также не лежит в $A \oplus B$. По выбору подгруппы B будет $A \cap \langle g_1, B\rangle \neq 0$. Значит, некоторый элемент $a' \in A$ можно выразить в виде $a' = kg_1 + b'$, $b' \in B$, $0 < k < n$. Так как $(k, n) = 1$, существуют u, v такие, что $ku + nv = 1$, значит, $g_1 = kug_1 + nvg_1$. Так как $ng_1 \in A \oplus B$, $kg_1 = a' - b' \in A \oplus B$, то $g_1 \in A \oplus B$. Получили противоречие.

60.66. Пусть D — сумма всех делимых подгрупп. Нетрудно проверить, что D делима. Пусть $a \in D$, тогда $a = a_1 + \ldots + a_k$, где a_i принадлежит A_i $(i = 1, \ldots, k)$ — делимому слагаемому группы D. Если $na_i' = a_i$, $i = 1, \ldots, k$, то $n\left(\sum_{i=1}^k a_i'\right) = a$. Согласно предыдущей задаче вся группа разлагается в прямую сумму $D \oplus B$. Если бы в B нашлась делимая подгруппа, то она содержалась бы в D, что невозможно. Итак, в B нет делимых подгрупп. Факторгруппа всей группы по D изоморфна B.

60.67. Использовать задачу 60.16.

60.68. Использовать задачу 60.67.

60.69. Воспользоваться задачей 60.67.

61.1. а) Рассмотреть элементы, сопряженные с транспозицией (12) при помощи степеней данного цикла.

б) Элементы из $\mathbf{A}_n$ — произведения четного числа транспозиций, и $(ij)(jk) = (ijk)$, $(ij)(kl) = (ikj)(ikl)$.

61.2. Использовать приведение матриц элементарными преобразованиями строк к ступенчатому виду.

61.3. Невырожденная матрица приводится к диагональному виду элементарными преобразованиями над строками, т. е. умножением слева на соответствующую элементарную матрицу.

61.5. См.: *Gorenstein D.* Finite groups. — Harper and Row, 1968. — P. 44.

61.7. а) $\{1, a\}$, $\{5, a\}$, $\{2, 3\}$, $\{4, 3\}$, где a — любой элемент из $\mathbf{Z}_6$.

б) Две различные транспозиции или транспозиция и тройной цикл.

в) Любые два не взаимно обратные элементы порядка 4.

г) Поворот σ квадрата на угол $\pm\pi/2$ и любая осевая симметрия τ, а также τ и $\tau\sigma$.

д) $\{a, b\}$, $\{a, a + b\}$, $\{b, a + b\}$.

61.10. Если $g_1, \ldots, g_n$ — конечная система порождающих, $f_1, f_2, \ldots, f_k, \ldots$ — другая система порождающих, то элементы $g_1, \ldots, g_n$ выражаются через вторую систему. В каждом таком выражении участвует лишь конечное число элементов второй системы, скажем, $f_1, \ldots, f_m$. Тогда $f_1, \ldots, f_m$ порождают всю группу.

61.11. Нормальное замыкание элемента A порождается как подгруппа элементами $B^iAB^{-i} = \begin{pmatrix} 1 & 2^i \\ 0 & 1 \end{pmatrix}$ $(i \in \mathbb{Z})$, и поэтому изоморфно группе рациональных чисел вида $m/2^k$ относительно сложения. Эта подгруппа не конечно порождена.

61.12. а) Использовать индукцию по числу возможных сокращений.

б) Операция определена корректно в силу а). Ассоциативность очевидна. Единицей служит пустое слово. Словом, обратным к $u = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$, служит $x_{i_n}^{-\varepsilon_n} \dots x_{i_1}^{-\varepsilon_1}$.

61.13. Гомоморфизм φ определяется так: если $u = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$, то $\varphi(u) = g_{i_1}^{\varepsilon_1} \dots g_{i_n}^{\varepsilon_n}$. Это единственно возможное определение.

61.14. Всякое несократимое слово можно записать в виде $u = vwu^{-1}$, где w имеет в начале и в конце не взаимно простые буквы. Тогда $u^n = vw^nv^{-1}$, где длина w^n в n раз больше длины w и вообще $d(u^n) = d(u) + +(n-1)d(w)$, поэтому $u^n \neq 1$ (пустому слову).

61.15. Будем считать, что коммутирующие элементы u, v несократимы. Пусть $d(u) \leqslant d(v)$.

1) Если в uv сокращается больше половины слова u, то переходим к словам u, uv (второе более короткое, чем v, и эти слова коммутируют, как и u с v).

2) Если в vu сокращаются больше половины слова u, то, аналогично, переходим к рассмотрению u^{-1}, vu.

3) Если в слове vu^{-1} сокращается больше половины второго сомножителя, переходим к рассмотрению u^{-1}, $u^{-1}v$.

4) Если в vu^{-1} сокращается больше половины первого сомножителя, переходим к uvu^{-1}.

5) В оставшемся случае будет $u = u_1u_2$, где $d(u_1) = d(u_2)$, $v = u_2^{-1}v'$, где между сомножителями нет сокращений. Из равенства $uv = vu$ получаем $u, v' = u_2^{-1}v'u_1u_2$. Так как в $v'u_1u_2$ сокращается не более, чем u_1, получаем $u_1 = u_2^{-1}$ и $u = 1$.

6) Делая каждый раз замены типа (1)–(4), мы в конце концов придем к случаю (5). Рассматривая предыдущий шаг, найдем порождающий элемент, через который выражаются u и v.

61.16. В любом коммутаторе и в произведении коммутаторов сумма показателей по каждому вхождению x_i равна 0 при любом i. Пусть в слове u сумма показателей при некотором x_i равна $k \neq 0$. Согласно задаче 61.13 построим гомоморфизм свободной группы в $\mathbb{Z}$ такой, что $x_i \to 1$, $x_j \to 0$ $(j \neq i)$. Тогда u перейдет в $k \neq 0$, и следовательно, не лежит в коммутанте.

61.17. Слова, имеющие несократимую запись uw_1u^{-1}, где w_1 — циклическая перестановка w.

61.18. Пусть F — свободная группа со свободными порождающими $x_1, \dots \dots, x_n$, A — свободная абелева с базисом $a_1, \dots, a_n$. Если гомоморфизм $F \to A$ продолжает отображения $x_i \to a_1, \dots, x_n \to a_n$ (см. задачу 61.13), то его ядром является коммутант.

61.19. Воспользоваться задачей 61.16.

61.20. Подгруппа индекса 2 нормальна в любой группе. Задача сводится к описанию различных сюръективных гомоморфизмов свободной группы на группу $\langle a \rangle_2$. Если x_1, x_2 — свободные порождающие свободной группы, то согласно 61.13 нужно по-разному выбрать образы x_1, x_2. Ответ: $\varphi_1(x_1) = a$, $\varphi_1(x_2) = 1$, $\varphi_2(x_1) = a$, $\varphi_2(x_2) = a$, $\varphi_3(x_1) = 1$, $\varphi_3(x_2) = a$, т. е. имеются три подгруппы индекса 2.

61.22. Очевидно, при любом гомоморфизме группы $F = (x_1, x_2)$ в $\mathbf{Z}_n \times \mathbf{Z}_n$ коммутант, а также элементы x_1^n, x_2^n переходят в единицу. Факторгруппа по подгруппе N, порожденной коммутантом и элементами x_1^n, x_2^n, изоморфна $\mathbf{Z}_n \times \mathbf{Z}_n$. Поэтому N будет ядром любого сюръективного гомоморфизма $F \to \to \mathbf{Z}_n \times \mathbf{Z}_n$.

61.23. а) 16. б) 36; воспользоваться задачей 61.13.

61.25. Согласно задаче 61.13 построим гомоморфизм φ свободной группы F со свободными порождающими $x_1, \ldots, x_n$ в H такой, что $\varphi(x_i) = h_i$, $i = = 1, 2, \ldots, n$. При этом гомоморфизме наименьшая нормальная подгруппа R, содержащая слова $R_i(x_1, \ldots, x_n)$, $i \in I$, перейдет в единицу. Если $N = \operatorname{Ker}\varphi$, то $\operatorname{Im}\varphi \simeq F/N \simeq (F/R)/(N/R)$.

61.27. Доказать, что каждый элемент выражается в виде $a^i b^j$, $0 \leqslant i < 2$, $0 \leqslant j < 7$.

61.28. Вывести из определяющих соотношений, что порядок группы $\leqslant 8$, затем воспользоваться задачей 61.25.

61.29. Вывести из определяющих соотношений, что порядок группы $\leqslant 2n$, затем воспользоваться задачей 61.25.

61.30. Вывести из определяющих соотношений, что порядок группы $\leqslant 8$, затем воспользоваться задачей 61.25.

61.31. Согласно задаче 61.25 рассмотреть гомоморфизм этой группы на группу указанных матриц, при котором

$$x_1 \to \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad x_2 \to \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

(квадрат второй матрицы равен E); воспользоваться тем, что подгруппа, порожденная x_1x_2, нормальна.

61.32. См. указание к задаче 61.31.

61.34. См.: *Милнор Дж.* Введение в алгебраическую K-теорию. — М.: Мир, 1974. — § 5.

61.35. Каждый смежный класс по H имеет вид $g^i H$, $i \in \mathbb{Z}$, поэтому любой элемент группы имеет вид $g^i h$, $h \in H$.

61.36. Пусть $\langle h \rangle$ — бесконечная циклическая подгруппа, порожденная h; факторгруппа G/H бесконечная циклическая, порожденная gH. По предыдущей задаче $G = \langle g \rangle \langle h \rangle$. Так как H нормальна, $ghg^{-1} \in H$ и отображение $x \to gxg^{-1}$ $(x \in H)$ — автоморфизм группы H. Поэтому ghg^{-1}, как и h, — порождающий элемент группы H. Значит, ghg^{-1} равен h или h^{-1}. Поэтому в группе выполнено одно из двух соотношений: $ghg^{-1} = h$, $ghg^{-1} = h^{-1}$. В первом случае группа свободная абелева, так как она порождается элементами x_1, x_2 и задается определяющим соотношением $x_1x_2x_1^{-1} = x_2$. Рассмотрим группу с порождающими x_1, x_2 и определяющим соотношением $x_1x_2x_1 = x_2^{-1}$. В этой группе циклическая подгруппа, порождённая x_2, нормальна (видно из определяющего соотношения), факторгруппа по ней бесконечная циклическая (рассмотреть гомоморфизм в $\mathbb{Z}$ такой, что $x_1 \to 1$, $x_2 \to 0$). Элемент x_2 также имеет бесконечный порядок, для этого рассмотрим гомоморфизм нашей группы в группу матриц вида $\begin{pmatrix} \pm 1 & n \\ 0 & 1 \end{pmatrix}$, $x_2 \to \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (см. задачу 61.25).

61.37. Наименьшая нормальная подгруппа, порожденная x, изоморфна аддитивной группе чисел вида $m/2^k$, $m, k \in \mathbb{Z}$. Рассмотреть гомоморфизм в группу матриц второго порядка, при котором $x_1 \to \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$, $x_2 \to \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (сравнить с задачей 61.11).

62.1. а) $\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & a \end{pmatrix}$. б) $\begin{pmatrix} 1 & \frac{b}{c} + \frac{ay - bx}{cz} - \frac{y}{z} \\ 0 & 1 \end{pmatrix}$. в) $\begin{pmatrix} 1 & \lambda(\beta^2 - 1) \\ 0 & 1 \end{pmatrix}$.

62.2. а) $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$. б) $[aG', bG'] = [a, b]G' = G'$.
в) Если $[aN, bN] = N$, то $[a, b]N = N$ и $[a, b] \in N$.

62.3. $\varphi([a, b]) = [\varphi(a), \varphi(b)]$.

62.4. Если $\varepsilon : G \to G/G'$ — естественный гомоморфизм, $\varphi : G/G' \to A$ — гомоморфизм в абелеву группу A, то $\varphi\varepsilon : G \to A$ — также гомоморфизм. Биективность этого соответствия следствия следует из задачи 62.2, в) и того, что ε сюръективен.

62.5. По теореме об определителе произведения $ABA^{-1}B^{-1} = 1$.

62.6. Вытекает из того, что $[(a_1, b_1), (a_2, b_2)] = ([a_1, a_2], [b_1, b_2])$.

62.7. а) $\mathbf{A}_3$, 2. б) $\{e, (12)(34), (13)(24), (14)(23)\}$, 3.
в) $\mathbf{A}_4$, 2. г) $\{\pm 1\}$, 4.

62.8. а) $\mathbf{A}_n$; коммутатор — четная перестановка и согласно задаче 62.1, в), коммутант содержит все тройные циклы; $\mathbf{A}_n$ порождается тройными циклами (см. задачу 61.1).

б) Если элемент $a \in \mathbf{D}_n$ есть поворот на угол $2\pi/n$, то $\mathbf{D}_n' = \langle a \rangle$, если n нечетно, и $\mathbf{D}_n' = \langle a^2 \rangle$, если n четно.

62.10. а) Индукция с применением предыдущей задачи.
б) Индукция с применением задачи 62.2.

62.11. а) Следует из того, что коммутант подгруппы содержится в коммутанте группы.
б) Следует из задачи 62.3.
в) Индукция с применением задачи 62.6.
г) Так как $B^{(k)} = \langle e \rangle$, то $G^{(k)} \subseteq A$ и $G^{(k+l)} = \langle e \rangle$, где $A^{(l)} = \langle e \rangle$.

62.12. См. задачи 62.7 и 62.8.

62.14. Следует из задачи 62.13, в), так как коммутант этой группы содержится в $\mathbf{UT}_n(K)$.

62.15. Если ряд, указанный в задаче, имеется, то $G^{(l)} = \langle e \rangle$ в силу задачи 62.2, в). Если группа разрешима, то факторы ее ряда коммутантов $G^{(i)}/G^{(i+1)}$ абелевы, поэтому между $G^{(i)}$ и $G^{(i+1)}$ можно вставить несколько подгрупп так, что получается ряд с нужными свойствами.

62.16. Согласно задаче 58.22 центр конечной p-группы G нетривиален. Пусть A — подгруппа порядка p, лежащая в центре. Тогда A нормальна в G. Завершается доказательство индукцией с переходом к G/A (тоже p-группа) и использованием задачи 62.12.

62.17. Если $q > p$, то силовская q-подгруппа нормальна в группе (см. указание к задаче 59.20).

62.18. а) Силовская 5-подгруппа нормальна, так как индекс ее нормализатора — делитель числа 4 и сравним с 1 по модулю 5.

б) Если в группе порядка 12 силовская 3-подгруппа не нормальна, то таких подгрупп по крайней мере 8. Но по теореме Силова существует подгруппа порядка 4, и тогда она в силу сказанного единственна.

в) Если $p > q$, то число m подгрупп порядка p^2 сравнимо с 1 по модулю p только при $m = 1$. Если $p < q$, то число q-подгрупп сравнимо с 1 по модулю q и делит p или p^2. Так как p оно делить не может, оно равно p^2. Значит, элементов порядка q будет $p^2(q-1)$. Однако подгруппа p^2 существует, поэтому она единственна $(p^2q = p^2(q-1) + p^2)$.

г) Силовская 7-подгруппа нормальна.

д) Силовская 5-подгруппа нормальна.

е) Комбинируются соображения задач 62.16, 62.18, в), а также то, что если некоторая силовская подгруппа имеет индекс нормализатора k, то группа представляется подстановками на множестве силовских подгрупп, т. е. на k символах.

62.20. Использовать задачу 62.19.

62.21. Использовать задачу 62.1, в).

62.26. См.: *Хамфри Дж.* Линейные алгебраические группы. — М.: Мир, 1980. — С. 184–186.

62.27. а) Так как порядок $q-1$ мультипликативной группы $\mathbf{Z}_q$ делится на p, то таких чисел r существует $p-1$ (см. задачу 60.46).

б) Группа, состоящая из матриц $\begin{pmatrix} r^i & x \\ 0 & 1 \end{pmatrix}$, где r — число из а), рассматриваемое по подмодулю q, $\quad x \in \mathbf{Z}_q$ $(0 \leqslant i < p)$, некоммутативна — достаточно рассмотреть матрицы $\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Эта группа имеет порядок pq. Пусть G — неабелева группа порядка pq, $A = \langle a \rangle$ — ее силовская подгруппа порядка q, $B = \langle b \rangle$ — силовская подгруппа порядка p. Тогда по теореме Силова (см. также задачу 62.17) A нормальна в G. Поэтому $bab^{-1} = a^{s^i}$, в частности, $b^p a b^{-p} = a = a^{s^p}$; поэтому $s^p \equiv 1 \pmod q$, так как G неабелева. Меняя, если нужно, элемент b на его k-ю степень $(1 < k < p)$, мы можем s заменить на любое число, обладающее аналогичными свойствами. Поэтому если G_1 и G_2 — две неабелевы группы порядка pq, в них можно выбрать элементы a_i, b_i $(i = 1, 2)$, аналогичные a и b, обладающие свойствами: $a_i^q = e$, $b_i^q = e$, $b_i a_i b_i^{-1} = a_i^r$, где $r^p \equiv 1 \pmod q$. Изоморфизм между такими группами устанавливается соответствием $\varphi(a_1^s b_1^t) = a_2^s b_2^t$, где $0 \leqslant s < q$, $0 \leqslant t < p$.

62.28. б) Произведение этих перестановок в указанном порядке есть цикл длины 7. Согласно а) факторгруппа этой группы по коммутанту тривиальна, поэтому группа совпадает со своим коммутантом.

в) Данная группа гомоморфно отображается на группу из б) согласно задаче 61.25 и поэтому неразрешима.

62.29. Неразрешима, если система свободных порождающих состоит более, чем из одного элемента, так как в этом случае нет нетривиальных абелевых нормальных подгрупп. См. также задачу 62.11, б).

63.1. а), б), г), е), ж), з), к), л), м), н), о) при $D \equiv 1 \pmod 4$.

63.2. в), г), д), е), ж) при $D \equiv 1 \pmod 4$.

з), и) Использовать, что $\sqrt[3]{2}$ не является корнем квадратного трехчлена над $\mathbb{Q}$.

63.3. Все, кроме з).

63.4. Нет.

63.5. См. задачу 1.2.

63.7. 63.2, в); 63.4, г) при $n > 2$; 63.2, д) при $D = c^2$ $(c \in \mathbb{Z})$; 63.2, е) при $D = c^2$ $(c \in K)$; 63.3, а); 63.3, б); 63.3, д) при $|R \setminus D| > 1$; 63.3, и); 63.5.

63.10. Заметить, что $(xy)^{-1} = y^{-1}x^{-1}$.

63.11. а) $\mathbf{Z}_n^*$ состоит из всех таких классов $[k]$, что числа k и n взаимно просты; делителями нуля являются все такие классы $[k]$, что k и n имеют нетривиальный общий делитель; нильпотентными элементами являются все такие классы $[k]$, что k делится на все простые делители n.

б) $\mathbf{Z}_{p^n}^*$ состоит из всех таких классов $[k]$, что k не делится на p; делителями нуля являются все классы вида $[pm]$; каждый делитель нуля нильпотентен.

в) Аналогично а), где вместо n берется многочлен f.

г) Множества матриц (α_{ij}), у которых соответственно $\alpha_{ii} \neq 0$ $(i = 1, \ldots, n)$; $\alpha_{ii} = 0$ хотя бы при одном i; все $\alpha_{ii} = 0$.

д) Множества матриц A соответственно с $\det A \neq 0$, $\det A = \operatorname{tr} A = 0$.

е) Множество функций, не принимающих значение 0; множество функций, принимающих значение 0; нулевая функция.

ж) Обратимыми элементами являются ряды с ненулевым свободным членом; делителей нуля и нетривиальных нильпотентных элементов нет.

63.13. а) Отображение $x \to ax$ $(a \in R,\ a \neq 0)$ — биекция, поэтому $ax = a$ при некотором $x \in R$; любой $b \in R$ представим в виде $b = ya$, и тогда $bx = b$, т. е. x — левая единица.

б) Элемент, обратимый справа, не является правым делителем нуля, и поэтому $x \to xa$ — биекция.

в) Если $ab = 0$ и a не является правым делителем 0, то элементы $x_1a, \ldots, x_na$ попарно различны и один из них равен 1. Утверждение в) неверно в алгебре над $\mathbf{Z}_2$ с базисом (x, y) и таблицей умножения $xy = y^2 = 0$, $yx = y$, $x^2 = x$.

б) Неверно в бесконечномерной алгебре над $\mathbb{Z}$ с базисом $(y^kx^l \mid k, l \in \mathbb{N})$ (элементы x и y не коммутируют) и умножением

$$y^kx^l \cdot y^rx^s = \begin{cases} y^kx^{l-r+s} & \text{при} \quad l > r, \\ y^kx^s & \text{при} \quad l = r, \\ y^{k+r-l}x^s & \text{при} \quad l < r. \end{cases}$$

63.14. Если $ab = 1$, то $(ba - 1)b = 0$.

63.15. б) См. ответ к задаче 63.14.

в) См. ответ к задаче 63.13.

63.16. а) R коммутативно (имеет единицу) тогда и только тогда, когда каждое прямое слагаемое R_i коммутативно (имеет единицу); в R нет делителей нуля тогда и только тогда, когда $k = 1$.

б) Элемент $a \in R$, $a = (a_1, \dots, a_k)$, $a_i \in R_i$, обратим (нильпотентен) тогда и только тогда, когда каждое a_i обратимо (нильпотентно) в R_i, $i = 1, \dots, k$.

63.17. а) Отображение $[x]_k \to ([x]_k, [x]_l)$ — изоморфизм.

в) Пара $([x], [y])$ обратима в $\mathbf{Z}_k \times \mathbf{Z}_l$ тогда и только тогда, когда $[x]$ обратим в $\mathbf{Z}_k$, $[y]$ обратим в $\mathbf{Z}_l$; $\varphi(n)$ — число порождающих элементов $\mathbf{Z}_n$.

63.19. б), в) Рассмотреть линейное отображение $\varphi_a : A \to A$, задаваемое формулой $\varphi_a(x) = ax$.

63.20. Использовать существование аннулирующего многочлена у каждого элемента алгебры.

63.21. а) $\mathbb{C} \oplus \mathbb{C}$, $\mathbb{C}[x]/\langle x^2 \rangle$.

б) Кроме алгебр в а), еще три алгебры: $\mathbb{C}e \oplus \mathbb{C}e$, где $e^2 = 0$; $\mathbb{C}e \oplus \mathbb{C}f$, где $e^2 = ef = fe = 0$, $f^2 = e$; $\mathbb{C}e \oplus \mathbb{C}f$, где $e^2 = 0$, $f^2 = f$.

63.22. а) $\mathbb{R} \oplus \mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[x]/\langle x^2 \rangle$.

б) Кроме алгебр в а), $\mathbb{R}e \oplus \mathbb{R}e$, где $e^2 = 0$; $\mathbb{R}e \oplus \mathbb{R}f$, где $e^2 = 0$, $f^2 = f$, и векторное пространство $\mathbb{R}e \oplus \mathbb{R}f$, где $e^2 = ef = fe = 0$, $f^2 = e$.

63.23. а) Нет.

г) Все кватернионы $x_1 i + x_2 j + x_3 k$ с условием $x_1^2 + x_2^2 + x_3^2 = 1$.

63.24. Использовать базис $T(V)$, построенный с помощью базиса V.

63.25. б) Использовать базис $\Lambda^k(V)$, построенный по базису V.

в) Если x — нильпотентный элемент кольца, то $\alpha + x$ обратим при $\alpha \neq 0$.

63.28. Применить операторы $p_1^{l_1} \times \ldots \times p_n^{l_n} q_1^{t_1} \times \ldots \times q_n^{t_n}$ к одночленам $x_1^{m_1} \times \ldots \times x_n^{m_n}$.

63.31. б) Нули непрерывной функции образуют замкнутое подмножество. Если $fg = 0$, то нули f и g в объединении дают $[0, 1]$.

64.1. Использовать деление с остатком. а) $n\mathbb{Z}$. б) $f(x)K[x]$.

64.2. а) Рассмотреть идеал $(2, x)$. б) Рассмотреть идеал (x, y).

64.3. Если ненулевая матрица X принадлежит идеалу I, то матрица AXB вида $E_{11} + \ldots + E_{rr} \in I$, откуда $AXBE_{11} = E_{11} \in I$; поэтому $E = E_{11} + \ldots + E_{nn} \in I$.

64.5. Каждый идеал состоит из всех матриц вида $\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}$, где элементы a_k составляют в $\mathbb{Z}$ идеал I_k $(k = 1, 2, 3)$, причем $I_1 \subseteq I_2$ и $I_3 \subseteq I_2$.

64.7. 0; вся алгебра; все матрицы с нулевым первым (вторым) столбцом; все матрицы с одинаковыми столбцами.

64.8. а) 0, L и подалгебра $\langle e \rangle$.

б) 0, L, $\langle 1 + e \rangle$ и $\langle 1 - e \rangle$. Всякий идеал, отличный от 0 и L, является одномерным подпространством в L.

64.12. а) $\langle p \rangle$, где p — простое число.

б) $\langle p(x) \rangle$, где $p(x)$ — многочлен первой степени.

в) $\langle p(x) \rangle$, где $p(x)$ — многочлен первой степени или многочлен второй степени, не имеющий действительных корней.

64.13. Неверно.

64.14. б) Если нет точки, где все функции обращаются в 0, то для каждой точки $a \in [0, 1]$ найдется такая функция f_a, что $f_a(a) \neq 0$. В силу непрерывности функция $f_a^2(x)$ строго положительна в некоторой окрестности $(a-\varepsilon_a, a+\varepsilon_a)$ точки a (и неотрицательна в остальных точках). Поскольку из каждого покрытия отрезка интервалами можно выбрать конечное покрытие, найдется конечное число функций $f_1, \ldots, f_k$ из идеала таких, что $f_1^2(x) + \ldots + f_k^2(x) > 0$ для любого x.

64.15. Рассмотреть идеал, порожденный элементом $a \neq 0$. Кольцо с нулевым умножением, аддитивная группа которого циклическая простого порядка, не имеет нетривиальных идеалов, но полем не является.

64.16. Доказать, что полные правые делители нуля (т. е. элементы $a \in R$, для которых $Ra = 0$) образуют левый идеал и поэтому не могут быть отличными от нуля. Если же $ba \neq 0$, то $Ra = R$. Вывести отсюда, что в R вообще нет делителей нуля и что отличные от нуля элементы кольца образуют группу по умножению.

64.17. Пусть $R \ni a \neq 0$. Имеем $Ra \supseteq Ra^2 \supseteq \ldots$, откуда $Ra^k = Ra^{k+1}$ при некотором k. Отсюда $a^k = ba^{k+1}$, $1 = ba$.

64.18. Положить $\delta_1(a) = \min\limits_{x \in K \setminus \{0\}} \delta_1(ax)$.

64.19. а) Рассмотреть норму $\delta(x+iy) = x^2 + y^2$.

б) В этом кольце элементы 2 и $1 \pm \sqrt{3}$ простые, и $4 = 2 \cdot 2 = (1 + i\sqrt{3}) \times (1 - i\sqrt{3})$ — два неассоциированных разложения на простые множители.

в) Рассмотреть норму $\delta(x+iy) = x^2 + y^2$.

64.24. Пусть $R \subseteq A \subseteq Q$ и I — идеал в A. Доказать, что $I = \langle r_0 \rangle$, где r_0 порождает идеал кольца, состоящий из числителей всех элементов из I.

64.25. Пусть $R[x]$ — кольцо главных идеалов. Для $0 \neq a \in R$ рассматриваем идеал $I = \langle x, a \rangle$ кольца $R[x]$. Так как $a \in R$, то $I = \langle f_0 \rangle$, где f_0 — константа, т. е. $I = R[x]$. Отсюда $1 = u(x)x + v(x)a$, а $v(0) = 1$, так что R — поле; заметить, что $F[x,y] \cong F[x][y]$.

64.26. (x^n), $n \geqslant 0$.

64.28. а) Представить единицу в виде $1 = a_1 + a_2$, где $a_1 \in I_1$, $a_2 \in I_2$.

б) По индукции свести к случаю $n = 2$. Для каждого $i \geqslant 2$ можно найти элементы $a_i \in I_i$ и $b_i \in I_i$ такие, что $1 = a_i + b_i$. Тогда

$$1 = \prod_{i=1}^{n} (a_i + b_i) \in I_1 + \prod_{i=2}^{n} I_k.$$

Следовательно, $I_1 + \prod_{i=2}^{n} I_i = A$ и согласно задаче а) можно найти $y_1 \equiv 1 \pmod{I_1}$ и $y_1 \equiv 0 \pmod{\prod_{i=2}^{n} I_i}$. Аналогично найдутся $y_2, \ldots, y_n \in A$ такие, что $y_j \equiv 1 \pmod{I_j}$ и $y_j \equiv 0 \pmod{I_i}$ при $i \neq j$. Тогда элемент $x = x_1y_1 + \ldots + x_ny_n$ удовлетворяет требованиям задачи.

64.29. а) Нет. б) Да.

64.31. а) Использовать задачу 63.11, в).

64.37. а) $n \to 0$. б) $n \to n$; $n \to 0$. в) $n \to 0$.

г) Любой гомоморфизм имеет вид $n \to ne_i$, где e_i — идемпотент кольца матриц; всего восемь гомоморфизмов, соответствующих идемпотентам O, E, E_{11}, E_{22}, $E_{11} + E_{12}$, $E_{21} + E_{22}$, $E_{11} + E_{21}$, $E_{12} + E_{22}$.

64.38. а) $n \to na$, где a — произвольный фиксированный элемент из $\mathbb{Q}$.

б) $n \to 0$, $n \to n$.

64.39. Доказать, что ядро гомоморфизма или равно нулю или совпадает с полем.

64.41. Рассмотреть гомоморфизмы:

а) $f(x) \to f(\alpha)$; б) $f(x) \to f(i)$; в) $f(x) \to f\left(\dfrac{-1+i\sqrt{3}}{2}\right)$.

64.42. Поле получается при $f_1(x) = x^2 + x + 1$, изоморфные факторкольца — при $f_1(x) = x^2$ и $f_2(x) = x^2 + 1$. Рассмотреть таблицы умножения для указанных факторколец.

64.43. Нет: в первом факторкольце есть ненулевой элемент, куб которого равен нулю, а во втором факторкольце элемента с таким свойством нет.

64.44. Нет.

64.45. При умножении на элемент $x - a \in F[x]$ любой элемент первого модуля обращается в 0, а во втором модуле это не так; оба факторкольца изоморфны F.

64.46. Пусть $\langle(x-a)(x-b)\rangle = I_1$, $\langle(x-c)(x-d)\rangle = I_2$. Записать произвольный элемент из $F[x]/I_1$ в виде $\alpha(x-a) + \beta(x-b) + I_1$ и поставить ему в соответствие элемент $k\alpha(x-c) + k\beta(x-d) + I_2 \in F[x]/I_2$, где $k = \dfrac{a-b}{c-d}$.

64.47. $\mathbf{A}_1$ и $\mathbf{A}_3$, $\mathbf{A}_2$ и $\mathbf{A}_5$.

64.48. а) Да. б) Нет.

64.49. а) Да. б) Нет.

64.50. Искать обратный элемент к f методом неопределенных коэффициентов.

64.52. Аналогично задаче 63.17.

64.53. См. задачу 64.15.

64.54. Использовать вложение колец без делителей нуля в поле.

64.55. а) Найти делители нуля.

б) Доказать, что каждый ненулевой элемент имеет обратный.

в) Доказать, что данное кольцо не содержит делителей нуля, если n — простое число, не равное сумме двух квадратов, и что конечное ненулевое коммутативное кольцо без делителей нуля является полем.

64.57. Рассмотреть отображение $a_0x^k + \ldots + a_k \to \overline{a}_0x^k + \ldots + \overline{a}_k$, где $\overline{a}_i = a_i + \langle n\rangle$ $(i = 0, \ldots, k)$.

64.58. p^n.

64.59. а) Ввести структуру кольца на прямой сумме $S = R \oplus \mathbb{Z}$.

б) Если R — алгебра над полем K, то превратить в алгебру над K прямую сумму $S = R \oplus K$.

в) Сопоставить каждому элементу a в данной алгебры A линейный оператор φ_a на векторном пространстве A над K, при котором $\varphi_a(x) = ax$.

г) Использовать б).

64.60. Доказать, что $I_k + \cap_{i\neq k} I_i = A$ для всякого $k = 1, \ldots, s$; вывести отсюда сюръективность отображения f.

64.61. Использовать гомоморфизм $f(x) \to (f(1), f(-1))$.

64.63. Показать, что $I \cap \mathbb{Z} \neq 0$ и I содержит нетривиальный по модулю $I \cap \mathbb{Z}$ многочлен.

64.64–64.66. Воспользоваться теоремой о гомоморфизмах.

64.67. в) Условие $\det(a_{ij}) \neq 0$ вытекает из сюръективности композиции $\Lambda(V) \xrightarrow{\varphi} \Lambda(V) \longrightarrow \Lambda(V)/I_2$, где I_2 — идеал, порожденный $\Lambda^2(V)$. Для доказательства того, что φ — автоморфизм, необходимо показать, что $\varphi(e_i) \wedge \varphi(e_j) + \varphi(e_j) \wedge \varphi(e_i) = 0$ для всех i, j, а также сюръективность φ. Последнее достаточно показать для отображения φ с единичной матрицей (a_{ij}). Доказательство проводится убывающей индукцией по k, начиная с включения $\Lambda^n V \subset \operatorname{Im} \varphi$.

64.68. б) Аннулятор порождается идемпотентом $1 - e$, где e — порождающий элемент данного идеала.

64.69. Если идеалы $I_1, \ldots, I_n$ порождаются попарно ортогональными идемпотентами $e_1, \ldots, e_n$, то $I_1 + \ldots + I_n$ порождается идемпотентом $e_1 + \ldots + e_n$.

64.70. г) Например, $L_2 = \left\{\begin{pmatrix} a & a \\ b & b \end{pmatrix}\right\} \oplus \left\{\begin{pmatrix} a & 2a \\ b & 2b \end{pmatrix}\right\}$, где a, b — любые элементы поля.

д) $\varphi\left(\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}\right) = \begin{pmatrix} a & a \\ c & c \end{pmatrix}$, $\varphi\left(\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}\right) = \begin{pmatrix} b & 2b \\ d & 2d \end{pmatrix}$.

64.73. $\mathbf{M}_2(K) = I \oplus J$.

64.75. Рассмотреть ядро гомоморфизма $\mathbf{Z}_{mn} \to \mathbf{Z}_m \oplus \mathbf{Z}_n$, при котором $l + mn\mathbb{Z} \to (l + m\mathbb{Z}, l + n\mathbb{Z})$.

64.76. При n, не делящихся на квадрат простого числа; использовать задачу 64.75.

64.77. Доказать, что идеал, состоящий из всех матриц вида aE_{1n}, лежит в ненулевом идеале этой алгебры.

64.78. Если $R = I_1 \oplus \ldots \oplus I_n$ — разложение кольца R в прямую сумму простых колец и e — идемпотент в R, то $e = e_1 + \ldots + e_n$, где $e_i \in I_i$ — идемпотенты. Доказать, что в I_i число идемпотентов конечно (использовать задачу 64.16). Затем использовать задачу 64.15.

64.79. Если $A = I_1 \oplus \ldots \oplus I_n$ — вполне приводимая алгебра (I_k — простые алгебры), то $I_1 \oplus \ldots \oplus I_{k-1} \oplus I_{k+1} \oplus \ldots \oplus I_n$ — ее максимальный идеал ($k = 1, 2, \ldots, n$).

64.80. Использовать задачу 64.15.

64.81. Конечные циклические группы, порядки которых не делятся на квадрат. Циклическая группа не содержит собственных подгрупп тогда и только тогда, когда ее порядок — простое число; использовать разложение циклической группы в прямую сумму примарных циклических групп.

64.82. Пусть $R = I_1 \oplus \ldots \oplus I_n$ — разложение кольца R в прямую сумму минимальных левых идеалов. Если $I \subset R$, то существует $I_{k_1} \not\subseteq I$, и тогда $I_{k_1} \cap I = 0$. Если $I_{k_1} \oplus I \neq R$, то существует $I_{k_2} \not\subseteq I_{k_1} \oplus I$, и $I_{k_2} \cap (I_{k_1} \oplus I) = 0$. В конце концов получаем $I_{k_1} \oplus \ldots \oplus I_{k_s} \oplus I = R$ (при некотором $s < n$).

64.83. а) Если $R = I_1 \oplus \ldots \oplus I_n$ — разложение кольца в прямую сумму минимальных левых идеалов и I — левый идеал в R, то $R = I_1 \oplus \ldots \oplus I_k \oplus I$

при соответствующей нумерации слагаемых (см. указание к задаче 64.82) и $I \simeq R/(I_1 \oplus \ldots \oplus) \simeq I_{k+1} \oplus \ldots \oplus I_n$.

б) $R = I \oplus J$ (см. задачу 64.82), $1 = e_1 + e_2$, где $e_1 \in I$, $e_2 \in J$; доказать, что e_1, e_2 — идемпотенты и что $I = Re_1$.

64.84. Рассмотреть циклическую группу простого порядка с нулевым умножением. См. указание к задачам 64.82, б) и 64.16.

64.85. См. задачу 64.82.

64.88. См. задачу 64.75.

64.89. Линейные оболочки наборов векторов $e_{i_1}, \ldots, e_{i_s}$, где $1 \leqslant i_1 < \ldots \ldots < i_s \leqslant n$. Доказать, что если подмодуль A содержит вектор $\alpha_{i_1} e_{i_1} + \ldots + \alpha_{i_s} e_{i_s}$, где $\alpha_{i_1}, \ldots, \alpha_{i_s} \neq 0$, то $e_{i_1}, \ldots, e_{i_s} \in A$.

64.90. $k \to kk_0$, где k_0 — фиксированный, k — произвольный элемент из R, дает изоморфизм R-модуля R с левым идеалом $I = Rk_0$. Обратно: наличие изоморфизма R-модуля R с левым идеалом $I \subseteq R$ означает, что $I = Rk_0$, где k_0 — образ 1 при этом изоморфизме.

64.91. $F[x] = F[x] \circ 1 \oplus F[x] \circ x \oplus \ldots \oplus F[x] \circ x^{k_1}$, причем $F[x] \circ x^i \simeq F[x]$ (изоморфизм $F[x]$-модулей).

65.1. Пусть I — идеал в $A[x]$. Легко видеть, что множество коэффициентов a_i многочленов $a_0 + a_1 x + \ldots + a_i x^i$ из J является идеалом I в A. Последовательность идеалов $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ стабилизируется, скажем, на I_r; пусть a_{ij} $(i = 0, \ldots, r,\ j = 1, \ldots, n)$ — образующие для I_i, и пусть для каждого из указанных i, j выбран многочлен f_{ij} из J степени i со старшим коэффициентом a_{ij}. Тогда $\{f_{ij}\}$ — множество образующих J. Для каждого $f \in J$ индукцией по степени можно показать, что f лежит в идеале, порожденном f_{ij}.

65.2. Воспользоваться предыдущей задачей.

65.3. г) Написать формулу для обратного элемента.

д) Рассмотрим три случая.

Случай 1. Среди элементов $-\alpha, -\beta, -\alpha\beta$ есть элемент, равный γ^2 для некоторого $\gamma \in F$. Пусть для определенности $-\alpha = \gamma^2$, $\gamma \in K$. Тогда в A есть, очевидно, делители нуля, и изоморфизм $A \cong \mathbf{M}_2(F)$ можно задать явными формулами, например,

$$1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \to \begin{pmatrix} \gamma & 0 \\ 0 & -\gamma \end{pmatrix}, \quad j \to \begin{pmatrix} 0 & \beta \\ -1 & 0 \end{pmatrix}, \quad k \to \begin{pmatrix} 0 & \gamma\beta \\ \gamma & 0 \end{pmatrix}.$$

Случай 2. В A есть делитель нуля вида $u + p$, где $u = \gamma \cdot 1$, $\gamma \in K$, $\gamma \neq 0$, $p = x_1 i + x_2 j + x_3 k$ — чистый кватернион. Тогда (см. г)) $N(u + p) = \gamma^2 - p^2 = 0$. Положим $i' = p$ и дополним i' до базиса i', j', k' пространства чистых кватернионов так, чтобы выполнялись соотношения $i'^2 = \gamma^2$, $j'^2 = -\beta$, $i'j' = -j'i' = k'$. Это сводит случай 2 к случаю 1.

Случай 3. В A есть чисто мнимый делитель нуля $p = x_1 i + x_2 j + x_3 k$. Если $x_1 \neq 0$, то, рассматривая кватернион

$$u + x_1 \left(1 + \frac{u^2}{4\alpha x_1^2}\right) i + x_2 \left(1 - \frac{u^2}{4\alpha x_1^2}\right) j + x_3 \left(1 + \frac{u^2}{4\alpha x_1^2}\right) k,$$

мы сводим случай 3 к случаю 2. Если $x_1 = 0$, то имеет место случай 1.

е) В матричном представлении д) чистые кватернионы выделяются условием $\operatorname{tr} P = 0$. Таким образом, все нильпотентные матрицы (и только они) представляют чисто мнимые делители нуля в A.

ж) Воспользоваться г), е).

з) Умножением на ненулевой элемент $\lambda \in F$ можно добиться того, что определитель матрицы Q станет квадратом поля F; тогда Q в некоторой системе координат имеет вид $\alpha x_1^2 + \beta x_2^2 + \alpha\beta x_3^2$. Следует обратить внимание на то, что векторное произведение зависит от выбора ориентации. Проверить, что замена ориентации W приводит к замене алгебры A на двойственную алгебру A°, умножение $*$ в которой связано с умножением $\cdot$ в A по правилу $a \cdot b = b * a$ (как векторные пространства A и $A^{\cdot}$ совпадают). Далее, если A — алгебра кватернионов, то $A \simeq A^\circ$.

65.4. в) Рассмотреть F-линейное отображение $x \to ax$.

д) Свести утверждение к случаю простой алгебры с единицей. Минимальные идеалы имеют вид Ae, где $e^2 = e$.

65.5. в) Подпространство A_0 чистых кватернионов алгебры $A = C^+{}_Q(F)$ выделяется условием $x = -\overline{x}$, где черта обозначает естественную инволюцию алгебры Клиффорда: $\overline{1} = 1$, $\overline{e_i} = e_i$, $\overline{e_i e_j} = e_j e_i$. В качестве базиса A_0 можно выбрать элементы $e_1e_2 - \dfrac{1}{2}Q(e_1, e_2)$, $e_2e_3 - \dfrac{1}{2}Q(e_2, e_3)$, $e_1e_3 - \dfrac{1}{2}Q(e_1, e_3)$.

65.7. а) Достаточно рассмотреть случай неприводимого многочлена f над $\mathbb{Q}$. Тогда $K = \mathbb{Q}[X]/(f(X))$ — конечное расширение степени n над $\mathbb{Q}$; пусть x — класс $X \pmod{f(X)}$. Тогда отображение $K \to K$, определенное формулой $a \to xa$, является линейным отображением n-мерного векторного пространства K над $\mathbb{Q}$ в себя, причем его минимальный многочлен совпадает с минимальным многочленом элемента x.

65.8. Нет.

65.9. Пусть $I = \langle f_1, \ldots, f_n \rangle$. Для любой точки $z \in \mathbb{C}$ определим неотрицательное целое число $n(z) = \min\limits_i \gamma_z(f_i)$, где $\gamma_z(f_i)$ обозначает порядок нуля функции f_i в точке z (если $f_i(z) \neq 0$, то $\gamma_z(f_i) = 0$). Пусть (z_k) — с последовательность всех точек в $\mathbb{C}$, для которых $n(z_k) \neq 0$. Построить целую функцию f, имеющую последовательность (z_k), последовательностью нулей с кратностями $n(z_k)$ и показать, что $I = \langle f \rangle$.

65.10. а) $D = 0$; рассмотреть $x = y = 1$.

б) $f(x)D$, где $f(x) \in \mathbb{Z}[x]$, D — обычное дифференцирование.

в) $\sum f_i D_i$, где $f_i \in \mathbb{Z}[x_1, \ldots, x_n]$, D_i — частные дифференцирования по переменным.

65.12. См.: *Херстейн.* Некоммутативные кольца. — М.: Мир, 1972. — С. 99.

65.13. См.: *Диксмье.* Универсальные обертывающие алгебры. — М.: Мир, 1978. — С. 170, 171.

65.15, 65.16. См.: *Боревич З.И.*, *Шафаревич И.Р.* Теория чисел. — М.: Наука, 1985.

66.2. а) Если $\sqrt{n} \notin \mathbb{Q}$. б) Если $n < 0$.

в) $n = 2$ при $p = 3$; $n = 2, 3$ при $p = 5$; $n = 3, 5, 6$ при $p = 7$.

66.5. Мультипликативная группа поля из четырех элементов имеет порядок 3, и для построения такого поля достаточно иметь матрицу порядка 2 над полем $\mathbf{Z}_2$, для чего достаточно, чтобы она удовлетворяла уравнению $A^2 + A + E = 0$, т. е. $\operatorname{tr} A = \det A = 1$. Такая матрица есть $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, и поле состоит из элементов $O, E, A, A + E$; при $n = 6$ рассмотреть порядки элементов в аддитивной группе.

66.6. $\{ke \mid k \in \mathbb{Z}\}$; аддитивная группа собственного подполя имеет порядок p и содержит указанное подполе.

66.7. Для поля $\mathbb{Q}$ доказать сначала неподвижность целых чисел при любом автоморфизме; для поля $\mathbb{R}$ заметить, что неотрицательные числа являются квадратами, и поэтому их образы неотрицательны; из $x > y$ следует, что $\varphi(x) = \varphi(x - y) + \varphi(y) > \varphi(y)$; далее воспользоваться рациональными приближениями.

66.8. $z \to z$ и $z \to \overline{z}$; рассмотреть образ i.

66.9. $x + y\sqrt{2} \to x - y\sqrt{2}$ — единственный такой автоморфизм; рассмотреть образ $\sqrt{2}$.

66.10. При $m = 1$ заметить, что биномиальные коэффициенты $\binom{p}{n}$ делятся на p; далее применить индукцию.

б) Ненулевой гомоморфизм поля в себя является автоморфизмом.

66.12. При $m/n = r^2$ $(r \in \mathbb{Q} \setminus \{0\})$.

66.14. Аддитивная группа поля K из четырех элементов не может быть циклической, и поэтому все ее отличные от 0 элементы имеют порядок 2, $K = \{0, 1, a, a + 1\}$; при этом умножение определяется однозначно, в частности, $a(a + 1) = 1$.

66.15. Например, поле рациональных функций, с комплексными коэффициентами.

66.17. Существует, например, $F_p(X)$.

66.18. а) $\{-1, -3 + 2\sqrt{2}\}$.

б) $\varnothing$; 13 не является квадратом в $\mathbb{Q}(\sqrt{2})$.

в) $\varnothing$. г) $\varnothing$.

66.19. а) $\varnothing$. б) (2, 3, 2).

66.21. $t + 3t^2 + t^3$

66.23. Все.

66.25. Мультипликативная группа поля из n элементов имеет порядок $n - 1$.

66.26. $x = a$.

66.28. а) 3 и 5. б) 2, 3, 8 и 9.

66.29. Показать , что если $a \neq 0$, то $(ba^{-1})^3 = 1$ и 3 делит $2^n - 1$, что неверно.

66.30. Пусть $F^* = \langle x \rangle$. Доказать, что x алгебраично над простым подполем. Простое подполе отлично от $\mathbb{Q}$, так как $\mathbb{Q}^*$ не является циклической группой.

66.31. а) $\{\pm 1\}$. б) $\varnothing$.

66.32. а) Так как при $p > 2$ в $\mathbf{Z}_p$ нет элементов порядка 2, то $k \to k^{-1}$ — биекция и $\sum_{k=1}^{p-1} k^{-1} = \sum_{k=1}^{p-1} k$.

б) Аналогично а); $8|(p^2-1)$.

66.35, 66.36. См.: *Платонов В. П.*, *Рапинчук А. С.* Алгебраические группы и теория чисел. — М: Наука, 1991. — Гл. I, § 1.1.

66.37, 66.38. Решение аналогично решениям задач 66.35 и 66.36.

66.42–66.45. См.: *Боревич З. И.*, *Шафаревич И. Р.* Теория чисел — М.: Мир, 1985.

66.46. Использовать задачу 66.45.

66.47. Использовать нормирование полей p-адических чисел.

67.1. Индукцией по s свести к случаю $s = 1$; в этом случае построить базис A над K, исходя из базисов A над K_1 и K_1 над K.

67.6. Применить задачу 67.4.

67.7. Индукцией по s свести к случаю $s = 2$; в этом случае применить задачи 67.1, 67.4, 67.5.

67.8. Если многочлен $p(x)$ неприводим, то он имеет корень в $K[x]/\langle p(x)\rangle$.

67.9. а) Применить индукцию по степени $f(x)$, используя задачу 67.8.

б) Применить а) к многочлену $f_1(x) \times \ldots \times f_l(x)$.

67.10. Рассмотреть степени расширений в башне полей $K \subset K(\alpha) \subset \subset K(\theta, \eta)$, где η — корень многочлена $h(x) - \alpha$ в некотором расширении поля L, и воспользоваться задачами 67.1, 67.2.

67.11. а), б) Сравнить разложение многочлена $x^n - a$ на линейные множители в его поле разложения с возможным разложением этого многочлена над полем K.

в) Например, многочлен $x^4 + 1$ над полем вещественных чисел.

67.12. $f(x) = \prod_{i \in \mathbb{F}_p} (x - x_0 - i)$, где $\mathbb{F}_p$ — поле из p элементов, содержащиеся в K. Доказать, что если в некотором расширении L поля K многочлен $f(x)$ имеет корень, то $f(x)$ разлагается над L в произведение линейных множителей, и вывести отсюда, что над K все неприводимые множители многочлена $f(x)$ имеют одинаковую степень.

67.13. а) 1. б) 2. в) 2. г) 6. д) 8.

е) $p - 1$. ж) $\varphi(n)$. з) $p(p-1)$.

и) 2^r, где r — ранг матрицы (k_{ij}), $i = 1, \ldots, s$, $j = 0, \ldots, t$, над полем вычетов по модулю 2 и $\overline{k}_{ij}$ — класс вычетов по модулю 2 показателя k_{ij} в разложении $a_i = (-1)^{k_{i0}} \cdot \prod_{j=1}^{t} p_j^{k_{ij}}$ числа a_i в произведение степеней различных простых чисел $p_1, \ldots, p_t$ (допускается, что некоторые $k_{ij} = 0$).

ж) Показать, что если ζ — первообразный корень n-й степени из 1 и $\mu_\zeta(x)$ — его минимальный многочлен над $\mathbb{Q}$, то для всякого простого $p|n$, ζ_p также является корнем $\mu_\zeta(x)$; в противном случае, если $x^n - 1 = \mu_\zeta(x)h(x)$, ζ является корнем многочлена $h(x^p)$; привести последнее в противоречие с тем, что $x^n - 1$ не имеет кратных множителей над полем вычетов по модулю p.

з) Воспользоваться задачей 67.11.

и) Если K — искомое поле, рассмотреть $(K^*)^2 \cap \mathbb{Q}^*$ и применить индукцию по n.

67.14. $F(X,Y)/F(X^p,Y^p)$, где F — поле характеристики p. Если поле K конечно, воспользоваться задачей 56.36. Пусть K бесконечно и $L = K(a_1,\ldots,a_s)$. Индукцией по s вопрос о существовании примитивного элемента сводится к случаю $s = 2$; в этом случае показать, что при некотором $\lambda \in K$ элемент $a_1 + \lambda a_2$ не содержится в собственном промежуточном поле. Обратно: если $L = K(a)$, то показать, что всякое промежуточное поле порождается над K коэффициентами некоторого делителя из $L[x]$ минимального многочлена $\mu_a(x)$ элемента a над K.

67.15. Выбрать базис $L(x)$ над $K(x)$, состоящий из элементов L.

67.17. Индукцией по i $(0 \leqslant i \leqslant m)$ доказать, что при надлежащей нумерации элементов $b_1,\ldots,b_n$ система $a_1,\ldots,a_i,b_{i+1},\ldots,b_n$ является максимальной системой алгебраически независимых над K элементов в L.

67.18. а) Показать, что число максимальных идеалов не превосходит $(A : K)$. Далее показать, что если элемент $a \in A$ не является нильпотентным, то идеал, максимальный во множестве идеалов, не пересекающихся с $\{a, a^2,\ldots,\}$, является максимальным идеалом в A.

б) Использовать а). Для получения единственности в д) показать, что во всяком представлении $A = \prod_{j=1}^{t} L_j$ поля L_j изоморфны факторалгебрам по всевозможным максимальным идеалам в A.

67.20. Применить индукцию по n. Записав соотношение линейной зависимости для f_i, получить противоречие, исходя из того, что f_i — гомоморфизм алгебры.

67.23. а) Всякий K-гомоморфизм $A \to B$ единственным образом продолжается до L-гомоморфизма $A_L \to B$.

б) Использовать а).

67.24. Взять в качестве E любую компоненту алгебры F_L.

67.25. Для доказательства б)$\to$ а) заметить, что если L_i — любая компонента A_L и $\overline{a}_1,\ldots,\overline{a}_s$ — образы $a_1,\ldots,a_s$ в L_i, то $L_i = L(\overline{a}_1,\ldots,\overline{a}_s)$; для получения импликации а)$\to$ в) применить к подалгебре $K[a]$ задачи 67.22, а), 67.19 и 67.18, е).

67.26. Применить задачу 67.25.

67.27. б) Заметить, что каждое из полей L_1, L_2 является расщепляющим для другого; получить отсюда K-вложения $L_1 \to L_2$ и $L_2 \to L_1$.

67.28. Использовать задачи 67.27, в) и 67.22.

67.29. а) Выбрать расщепляющее поле для A, содержащее поле L, и применить задачу 67.22.

б) Применить а) и задачу 67.23, б).

67.30. Воспользоваться задачами 67.25 и 67.29, б).

67.31. б) Необязательно: например, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}\,) \subset \mathbb{Q}(\sqrt[4]{2}\,)$.

67.32. Для получения двух последних соотношений общий случай свести к двум частным, когда $a \in K$ и $L = K(a)$. В первом случае использовать любой базис в L/F, связанный с башней полей, а во втором в L/K использовать базис из степеней a. Для получения первого соотношения заметить, что $\chi_{L/K}(a,x) = \mathbf{N}_{L(x)/K(x)}(a - x)$.

67.33. Использовать задачу 67.32.

67.34. Если $\mathrm{Tr}_{L/K}(a) \neq 0$ для некоторого $a \in L$, то

$$(x, ax^{-1}) \to \mathrm{Tr}_{L/K}(a) \neq 0$$

для всякого $x \neq 0$ из L.

67.35. Каждое из условий а)–в) равносильно тому, что $A_L \simeq \prod L$ для расщепляющего поля L. Невырожденность формы следа на A и A_L означает одно и то же. Нильпотентные элементы всегда содержатся в ядре формы следа.

67.37. Использовать задачи 67.22 и 67.12.

67.38. Воспользоваться тем, что $\mathrm{Tr}_{A/K}(a) = \mathrm{Tr}_{A_L/L}(a)$, и аналогично в других случаях.

67.39. а) Воспользоваться задачами 67.14, 67.22.

б) b — примитивный элемент, a примитивным элементом не является.

67.40. Использовать задачу 67.22, в).

67.41. Воспользоваться задачами 67.34 и 67.35, г).

67.42. Многочлен $x^p - t$ над полем рациональных функций $K(t)$, где K — произвольное поле характеристики $p \neq 0$.

67.43. Использовать задачу 67.19.

67.44. Для доказательства обратного утверждения воспользоваться задачей 67.41.

67.45. Пусть L — расщепляющее поле для многочлена $f(x)$. Показать, что $B_L \simeq \prod_{i=1}^{n} A_i$, где $A_i \simeq A_L$, $n = \deg f$.

67.46. Для доказательства импликации в) $\to$ а) представить A как факторалгебру алгебры $K[x_1, \ldots, x_s]/\left(\mu_{a_1}(x_1), \ldots, \mu_{a_s}(x_s)\right)$ и воспользоваться задачей 67.45.

67.47. а) Использовать задачи 67.46, 67.45, 67.42, 67.11.

67.48. Рассмотреть $\mu_a(x)$ для всякого элемента $a \in L$.

67.50. Воспользоваться задачами 67.48 и 67.49.

67.51. б) Используя задачу 67.26, доказать, что для всякого расщепляющего поля E расширения L/K число различных K-вложений $L \to L$ равно $(K_s : K)$.

67.52. а) Подсчитать число различных K-вложений поля F в какое-либо расщепляющее поле расширения F/K.

67.53. Рассмотреть башню полей $K \subset K_s \subset L$ и применить задачи 67.31, 67.38.

67.54. а) Применить задачи 67.30 и 67.35.

б) Применить задачу 67.27.

67.55. а) Группа $G(\mathbb{C}/\mathbb{R})$ состоит из тождественного автоморфизма и комплексного сопряжения.

б), в) $\mathbf{Z}_2$. г) $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

67.56. а) $\{e\}$. б) $\mathbf{S}_2$. в) $\mathbf{S}_2$. г) $\mathbf{S}_3$.

д) $\mathbf{D}_4$. е) $\mathbf{Z}_{p-1}$. ж) $\mathbf{Z}_n^*$.

з) *Полупрямое* произведение группы $\mathbf{Z}_p$ и ее группы автоморфизмов.

и) Прямое произведение r экземпляров группы $\mathbf{Z}_2$ (см. ответ к задаче 67.13).

67.57. Всякий элемент $a \in L$ является корнем сепарабельного многочлена над K степени $\leqslant |G|$, а именно $f(x) = \prod_{\sigma \in G}(x - \sigma(a))$. Используя существование примитивного элемента у всякого (конечного) сепарабельного расширения, доказать, что $(L:K) = |G|$.

67.58. Рассмотреть действие $\mathbf{S}_n$ на поле рациональных функций $K(a_1, \ldots$ $\ldots, a_n)$ и применить задачу 67.57.

67.59. Вложить группу G в симметрическую группу и применить задачу 67.57.

67.60. Применить задачу 67.57.

67.61. Сначала доказать, что всякое отличное от $\mathbb{R}$ расширение Галуа $L/\mathbb{R}$ имеет степень, равную степени числа 2. Затем, используя разрешимость конечной 2-группы и несуществование расширений $L'/\mathbb{R}$ степени $\geqslant 2$, показать, что $L = \mathbb{C}$.

67.63. Рассмотреть действие элементов группы G на $\sqrt{D}$.

67.64. Используя линейную независимость автоморфизмов (задача 67.21), доказать, что L является циклическим модулем над $K[\varphi]$.

67.66. Группа $\mathbf{S}_n$, действующая посредством перестановок на компонентах алгебры $A = \prod K_i$ $(K_i \simeq K)$. Использовать, что K_i являются единственными минимальными идеалами в A.

67.67. Принять во внимание, что $\tau(x) = \sum_\sigma \sigma(\tau x)e_\sigma = \sum_\sigma \sigma(x)\tau(e_\sigma)$ для $x \in L$.

67.68. Использовать задачу 67.20 или интерпретировать $(\varphi_i(y_j))$ как матрицу перехода к новому базису, вложив A в A_L.

67.69. Если поле K конечно, см. задачу 67.64. Пусть K бесконечно, $\omega_1, \ldots, \omega_n$ — некоторый базис L над K и $\omega = a_1\omega_1 + \ldots + a_n\omega_n$ — произвольный элемент из L (если $a_i \in K$) или из L_L (если $a_i \in L$). Условие из задачи 67.68, обеспечивающее, что элементы $\{\sigma(\omega), \sigma \in G\}$ образуют базис в L (соответственно в L_L), означает, что для некоторого многочлена $f(x_1, \ldots, x_n) \in L[x_1, \ldots, x_n]$ его значение $f(a_1, \ldots, a_n) \neq 0$. Далее использовать существование нормального базиса в L_L (задача 67.67).

67.70. Если характеристика поля $K \neq 2$, то

$$K(x_1, \ldots, x_n)^{A_n} = K(\sigma_1, \ldots, \sigma_n, \Delta),$$

где $\sigma_1, \ldots, \sigma_n$ — элементарные симметрические многочлены от $x_1, \ldots, x_n$, $\Delta = \prod_{j>i}(x_j - x_i)$. В случае произвольной характеристики имеет место равенство

$$K(x_1, \ldots, x_n)^{A_n} = K(\sigma_1, \ldots, \sigma_n, y),$$

где $y = \sum_{\sigma \in A_n} \sigma\left(\prod_{i=1}^n x_i^{i-1}\right)$.

67.71. $\mathbb{C}(x_1^n, x_1^{n-2}x_2, \ldots, x_1x_{n-1}, x_n)$. Использовать задачу 67.60.

67.72. $\mathbb{C}(y_1^n, y_1^{n-2}y_2, \ldots, y_1y_{n-1}, y_n)$, где $y_i = \sum_{k=1}^n \varepsilon^{-ik}x_k$, ε — первообразный корень степени n из единицы. В пространстве линейных форм от $x_1, \ldots, x_n$ выбрать базис, состоящий из собственных векторов оператора σ; затем использовать задачу 67.71.

67.73. Группа $\mathbf{Z}_n$. Поле разложения L многочлена $x^n - a$ над K имеет вид $L = K(\theta)$, где θ — некоторый корень многочлена $x^n - a$ в L. Группа $G(L/K)$ порождается автоморфизмом σ, при котором $\sigma(\theta) = \varepsilon\theta$, где ε —

некоторый порождающий элемент (циклической) группы корней степени n из 1. Использовать задачу 67.11.

67.74. Пусть ε — порождающий элемент группы корней степени n из 1 в K; $y \in L$ — такой элемент из L, что $\sum_{i=1}^{n} \varepsilon^{-i}\sigma^{i}y \neq 0$ (почему такой элемент существует?); тогда $a = \left(\sum_{i=1}^{n} \varepsilon^{-i}\sigma^{i}y\right)^{n}$. Рассмотреть собственные векторы оператора σ на L.

67.75. Если $L = K(\theta_1, \ldots, \theta_s)$, то для всякого $\sigma \in G(L/K)$ $\sigma(\theta_i) = \varepsilon_i(\sigma)\theta_i$, где $\varepsilon_i(\sigma)^n = 1$. Обратно, если группа $G(L/K)$ абелева периода n, то использовать следующий факт: если во множестве попарно коммутирующих линейных операторов, каждый из которых диагонализируем, то существует базис из векторов, собственных для всех этих операторов. (Этот факт следует из задачи 40.7.)

67.76. Рассмотреть билинейное отображение $G(L/K) \times A \to \mathbf{U}_n$ для $\sigma \in G(L/K), \overline{a} \in A$ $(a \in \langle K^{*n}, a_1, \ldots, a_s\rangle)$, $(\sigma, \overline{a}) \to (\sigma\theta) \cdot \theta^{-1}$, где $\theta \in L$ и $\theta^n = a$.

67.77. $L \to (L^{*n} \cap K^*)/K^{*n}$; если $A = B/K^{*n}$, $B = \langle K^{*n}, a_1, \ldots, a_s\rangle$ — подгруппа в K^*, то $A \to L = K(\theta, \ldots, \theta_s)$, где $\theta_i^n = a_i$. Воспользоваться задачей 67.76.

67.78. Если $G(L/K) = \langle\sigma\rangle$, то для отыскания θ использовать корневой вектор высоты 2 линейного оператора σ. Для доказательства обратного утверждения воспользоваться задачей 67.12.

67.79. Если $L = K(\theta_1, \ldots, \theta_s)$, то для всякого $\sigma \in G(L/K)$ $\sigma(\theta_i) = \theta_i + \gamma_i$, $\gamma_i \in \mathbb{F}_p$ (см. задачу 67.12). Обратно: если $G = G(L/K)$ есть прямое произведение s циклических групп порядка p, то выберем в G подгруппы H_i $(i = 1, \ldots, s)$ индекса p, для которых $\cap_{i=1}^{s} H_i = \{e\}$; тогда $L^{H_i} = K(\theta_i)$ (см. задачу 67.78) и $L = K(\theta_1, \ldots, \theta_s)$.

67.80. Рассмотреть билинейное отображение $G(L/K) \times A \to \mathbb{F}_p$, где для $\sigma \in G(L/K)$, $\overline{u} \in A$ $(a \in \langle\rho(k), a_1, \ldots, a_s\rangle)$, $(\sigma, a) \to \sigma(\theta) - \theta$, где $\theta \in L$ и $\rho(\theta) = a$.

67.81. $L \to (\rho(L) \cap K)/\rho(K)$; если $A = B/\rho(K)$, $B = \langle\rho(K), a_1, \ldots, a_s\rangle$, то $A \to K(\theta_1, \ldots, \theta_s)$, где $\rho(\theta_i) = a_i$. Воспользоваться задачами 67.79 и 67.80.

68.1. Воспользоваться задачей 56.36.

68.2. а) Если $|L| = q$, то L является полем разложения многочлена $x^q - x$. б) Использовать указание к а) и задачу 67.27, б).

68.3. В пункте а) использовать, что многочлен $x^q - x$ не имеет кратных корней.

68.4. Использовать задачу 56.36.

68.5. г) $(x^2 + x + 1)(x^2 + 2x + 4)$.

68.6. б) Разложить σ в произведение независимых циклов.

68.7. Если $b = \prod_{j=1}^{k} p_j^{n_j}$, где p_j — различные простые числа, то разложить кольцо $\mathbf{Z}_8$ в прямое произведение колец вычетов по модулю $p_j^{n_j}$. Если $b = p^n$, p простое, то представить множество классов вычетов в виде объединения подмножеств, каждое из которых содержит все элементы, имеющие одинаковый порядок в аддитивной группе кольца вычетов. Далее использовать строение группы обратимых элементов кольца вычетов по модулю p^n.

68.8. Подсчитать число инверсий перестановки σ, упорядочив элементы из G следующим образом: $0, x_1, \ldots, x_n, -x_n, \ldots, -x_1$, где $\{x_1, \ldots, x_n\} = S$.

68.9. а) Использовать задачу 68.8, взяв произвольным образом множества S_1 и S_2 в G_1 и G_2 и положив $S = S_1 \cup \varphi^{-1}(S_2)$, где $\varphi\colon\ G \to G_2$ — канонический гомоморфизм.

68.10. Использовать задачу 68.8.

68.11. Использовать задачу 68.10.

68.12. Множество R пар чисел (x, y), где $1 \leqslant x \leqslant (a-1)/2$, $1 \leqslant y \leqslant$ $\leqslant (b-1)/2$, разбивается в объединение четырех подмножеств:

$$\begin{aligned}
R_1 &= \{(x, y) \in R \mid ay - bx < -b/2\},\\
R_2 &= \{(x, y) \in R \mid\ -b/2 < ay - bx < 0\},\\
R_3 &= \{(x, y) \in R \mid 0 < ay - bx < a/2\},\\
R_4 &= \{(x, y) \in R \mid a/2 < ay - bx\}.
\end{aligned}$$

Используя биекцию

$$(x, y) \to \left(\frac{a+1}{2} - x, \frac{b+1}{2} - y\right),$$

показать, что $|R_1| = |R_4|$. Используя задачу 68.10, показать, что

$$\left(\frac{a}{b}\right) = (-1)^{|R_2|}, \quad \left(\frac{b}{a}\right) = (-1)^{|R_3|}.$$

68.13. Представить матрицу оператора $\mathcal{A}$ в виде произведения элементарных.

68.14 – 68.16. См.: *Лидл З., Нидеррайтер Г.* Конечные поля. Т. 1 — М.: Мир, 1988. — Гл. 2, § 3.

69.4. а) Да. б) Нет. в) Да. г) Да. д) Нет. е) Да.

69.5. Все указанные подпространства, за исключением г), д) и з).

69.7. $\begin{pmatrix} 1 & -t & t^2 \\ 0 & 1 & -2t \\ 0 & 0 & 1 \end{pmatrix}$ (в базисе $1, x, x^2$).

69.8. $\begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$ (в базисе $\sin x, \cos x$).

69.10. Представить пространство $\mathbf{M}_n(K)$ в виде суммы подпространств, состоящих из матриц, все столбцы которых, кроме одного, нулевые.

69.11. Доказать предварительно, что подпространства в $\mathbf{M}_n(K)$ инвариантное относительно всех операторов $\mathrm{Ad}\,(A)$, где матрица A диагональна, является линейной оболочкой некоторого множества матричных единиц E_{ij} $(i \neq j)$ и некоторого подпространства диагональных матриц.

69.12. Доказать предварительно, что всякое подпространство в $\mathbf{M}_n(K)$, инвариантное относительно всех операторов вида $\Phi(A)$, где матрица A диагональна, является линейной оболочкой некоторого множества матриц вида $aE_{ij} + bE_{ji}$ $(i \neq j)$ и некоторого подпространства диагональных матриц.

69.13. Найти общий вид матриц X таких, что

$$X\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}X,$$

$$X\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}X,$$

и показать, что всегда $\det X = 0$.

69.16. в) Пусть $H \subseteq W$ — инвариантное подпространство и $x \in H$. Рассмотреть вектор $\pi x - x$ для $\pi = \{ij\}$.

69.17. Определить сначала подпространства, инвариантные относительно ограничения представления Θ на подгруппу диагональных матриц.

69.25. Использовать задачу 69.24, в) и разложение группы G на левые смежные классы по H.

69.26. а) m. б) 2. в) 1. г) $m+1$.

69.27. Если A и B — коммутирующие операторы, то каждое собственное подпространство оператора A инвариантно относительно B.

70.2. Использовать задачу 69.28.

70.5. В обоих случаях каждое неприводимое представление группы H встречается с кратностью 2.

70.6. Только тривиальное для группы нечетного порядка; для группы четного порядка — еще гомоморфизм на подгруппу $\{-1, 1\}$ в $\mathbf{GL}_1(\mathbb{R}) \simeq \mathbb{R}^*$.

70.7. Воспользоваться теоремой о существовании у вещественного оператора двумерного инвариантного подпространства.

70.9. а) $[n/2]+1$. Использовать задачу 70.8.

70.15. Для $\mathbf{S}_3$: тривиальное и сопоставляющее подстановке ее знак; использовать теорему о коммутанте и задачу 62.7, а). Для $\mathbf{A}_4$: использовать теорему о коммутанте и задачу 62.7, б).

70.16. Использовать теорему о коммутанте и задачу 62.8.

70.17. Можно взять представление задачи 69.13.

70.31. Рассмотреть разложение регулярного представления в сумму неприводимых подпредставлений.

70.32. Доказать, что подгруппа, порожденная $\mathcal{A}$ и $\mathcal{B}$ в $\mathbf{GL}(V)$, изоморфна $\mathbf{S}_3$.

70.34. а) 1, 1, 2. б) 1, 1, 1, 3.

в) 1, 1, 2, 3, 3. г) 1, 1, 1, 1, 2.

д) если $n = 2k$, то четыре одномерных и $k-1$ двумерных, если $n = 2k+1$, то два одномерных и k двумерных.

е) 1, 3, 3, 4, 5. Использовать основные теоремы и задачу 69.16.

70.37. а), б), в) Нет.

70.38. Существование подгруппы приводит к существованию двумерного представления группы $\mathbf{S}_4$.

70.42. Только для абелевых.

70.43. Провести индукцию по порядку группы.

70.45. Использовать задачу 69.25.

70.46. Воспользоваться конечностью числа неизоморфных групп фиксированного порядка и конечностью числа неизоморфных представлений данной размерности фиксированной конечной группы.

70.48. Заметить, что группы порядков p и p^2 абелевы.

70.49. p^2 одномерных представлений и $p-1$ p-мерных. Заметить, что центр данной группы имеет порядок p и число классов сопряженных элементов равно p^2+p-1. Так как факторгруппа по центру коммутативна, то коммутант данной группы имеет порядок p. Этим определяется число одномерных представлений. Заметить еще, что в данной группе есть нормальная подгруппа индекса p и доказать, что размерность неприводимого представления не может быть больше p.

70.54. Пусть G — конечная подгруппа в $\mathbf{SL}_2(\mathbb{Q})$. Ввести в пространстве $\mathbb{R}^2$ новое скалярное произведение

$$(x, y)_G = \sum_{g \in G} (gx, gy),$$

где $(x, y) = x_1y_1 + x_2y_2$ для строк $x = (x_1, x_2)$ и $y = (y_1, y_2)$. Показать, что относительно этого скалярного произведения каждый оператор g становится ортогональным. Поэтому G состоит из поворотов и отражений. Вывести, что $G \subseteq \mathbf{D}_n$ для некоторого n. Так как $\operatorname{tr} g \in \mathbb{Q}$, то, используя задачу 4.13, показать, что n равно $3, 4$ или 6.

70.55. Воспользоваться задачами 70.54, 56.33.

70.57. Воспользоваться задачами 56.33, 58.13.

70.58. Простая неабелева группа G совпадает со своим коммутантом G'. Поэтому при любом неприводимом комплексном представлении $\varphi : G \to \mathbf{GL}_2(\mathbb{C})$ определитель каждой матрицы $\varphi(g)$, $g \in G$, равен единице. Более того, это представление точно, т. е. ядро представления состоит только из единичного элемента. Размерность неприводимого представления делит порядок группы G. Следовательно, если φ — двумерное неприводимое комплексное представление группы G, то в силу первой теоремы Силова в G имеется элемент g порядка 2. При этом собственные значения матрицы $\varphi(g)$ равны ± 1. Если у этой матрицы оба собственных значения равны, то матрица $\varphi(g)$ лежит в центре группы $\mathbf{GL}_2(\mathbb{C})$, и поэтому сам элемент g лежит в центре G, что невозможно в силу простоты неабелевой группы G. Поэтому матрица $\varphi(g)$ имеет два разных собственных значения: $1, -1$. В частности, $\det(\varphi(g)) = -1$, что невозможно, как показано выше.

71.2. Базис состоит из одного вектора

$$\sum_{\sigma \in S_3} (\operatorname{sgn} \sigma)\sigma.$$

Размерность равна 5.

71.3. $\{\varepsilon - a, \varepsilon^2 - a^2, \ldots, \varepsilon^{n-1} - a^{n-1}\}$.

71.9. а) Пусть

$$e_1 = \frac{1}{6}\sum_{\sigma\in\mathbf{S}_3}\sigma, \qquad e_2 = \frac{1}{6}\sum_{\sigma\in\mathbf{S}_3}(\operatorname{sgn}\sigma)\sigma.$$

Коммутативные идеалы: 0, $\mathbb{C}e_1$, $\mathbb{C}e_2$, $\mathbb{C}e_1\oplus\mathbb{C}e_2$.

б) Пусть $Q_8 = \{E,\overline{E},I,\overline{I},J,\overline{J},K,\overline{K}\}$,

$$e_1 = (E+\overline{E})(E+I+J+K), \quad e_2 = (E+\overline{E})(E+I-J-K),$$
$$e_3 = (E+\overline{E})(E-I-J-K), \quad e_4 = (E+\overline{E})(E+I-J+K).$$

Коммутативные идеалы — линейные оболочки любого подмножества векторов множества $\{e_1,e_2,e_3,e_4\}$.

в) Пусть

$$e_1 = \frac{1}{10}\sum_{A\in\mathbf{D}_5}A, \qquad e_2 = \frac{1}{10}\sum_{A\in\mathbf{D}_5}(\det A)A.$$

Коммутативные идеалы: 0, $\mathbb{C}e_1$, $\mathbb{C}e_2$, $\mathbb{C}e_1\oplus\mathbb{C}e_2$.

71.10. Если G бесконечна, то $x=0$, если конечна, то

$$x = \alpha\sum_{g\in G}g, \qquad \alpha\in F.$$

71.11. Базис центра $F[G]$ образуют элементы вида $\sum_{g\in C}g$, если в качестве C взять последовательно все классы сопряжённых элементов в G.

71.16. Использовать лемму Шура.

71.19. Только для $G=\{e\}$.

71.22. а) 2. б) 1. в) 2. г) 4.

71.24. Пусть ε — первообразный корень степени 3 из единицы в $\mathbb{C}$,

$$r_0 = \frac{1}{3}(e+a+a^2)\in\mathbb{R}[\langle a\rangle_3]\subset\mathbb{C}[\langle a\rangle_3],$$
$$r_1 = \frac{1}{3}(e+\varepsilon a+\varepsilon^2a^2)\in\mathbb{C}[\langle a\rangle_3],$$
$$r_2 = \frac{1}{3}(e+\varepsilon^2a+\varepsilon a^2)\in\mathbb{C}[\langle a\rangle_3].$$

$\mathbb{R}[\langle a\rangle_3] = F_0\oplus F_1$, где поле $F_0=\mathbb{R}r_0\simeq\mathbb{R}$ и

$$F_1 = \left\{\alpha_0e+\alpha_1a+\alpha_2a^2 \;\middle|\; \sum_{i=0}^{2}\alpha_i=0,\ \alpha_i\in\mathbb{R}\right\}\simeq\mathbb{C}.$$

При изоморфизме $\mathbb{C}\to F_1$ имеем $1\to e-r_0$, $\varepsilon\to a(e-r_0)$. $\mathbb{C}[\langle a\rangle_3] = F_0'\oplus F_1'\oplus F_2'$. Поля $F_i'=\mathbb{C}r_i$ изоморфны $\mathbb{C}$.

71.25. Использовать неприводимость многочлена $x^{p-1} + x^{p-2} + \ldots + x + {}$ $+ 1$ над полем $\mathbb{Q}$.

71.27. а) Идемпотенты $e_1 = 2 + 2a$, $e_2 = 2 + a$; идеалы $\mathbb{F}_3 e_1, \mathbb{F}_3 e_2$.
б) Идемпотент — единица групповой алгебры; идеал $\mathbb{F}_2(1 + a)$.
в) Идемпотенты $\dfrac{1}{2}(1 + a)$, $\dfrac{1}{2}(1 - a)$; идеалы $\mathbb{C}e_1$, $\mathbb{C}e_2$.
г) Идемпотенты $\dfrac{1}{3}(1 + a + a^2)$, $\dfrac{1}{3}(2 - a - a^2)$; идеалы $\mathbb{R}e_1$, $\mathbb{R}[\langle a\rangle_3]e_2$.

71.28. Проверить аналогичное утверждение для групповой алгебры $\mathbf{M}_n(\mathbb{C})$ и использовать теорему о структуре групповой алгебры конечной группы.

71.29. а) 8. б) 32.

71.30. а) $\{e\}$. б) $G \simeq \mathbf{Z}_2$.
в) $G \simeq \mathbf{Z}_3$ или $\mathbf{S}_3$. Воспользоваться тем, что n равно числу классов сопряженных элементов в G.

71.34. При $p = 2$
$$U = F[G](a - e)^2.$$

71.36. а) Рассмотреть случай $G = H$. Провести индукцию по порядку группы H.
б) $n = 2$.

71.39. а) $P/H \simeq a/(g - ge)A \oplus A/(g - \varepsilon^2 e)A$, где ε — первообразный корень степени три из единицы в $\mathbb{C}$.
б) $P/H = 0$. в) $P/H \simeq A$.

71.40. $\operatorname{Ker} \varphi = 0$.

71.41. Рассмотреть аналогичный вопрос для $A = F[t]$ — кольца многочленов.

71.44. а) Элемент прост. б) $(g_1 - g_2)^2(-g_1^{-1}g_2^{-1} - g_1^{-2})$.

71.45. а) 0. б) $F[\langle g_1\rangle]$. в) F.

72.1. Использовать задачу 69.21.

72.2. Используя задачу 69.11, найти возможный диагональный вид матрицы оператора $\Phi(g)$.

72.3, 72.4. Использовать задачу 72.1.

72.5. Заметить, что сумма n корней из 1 равна n только когда все слагаемые равны 1.

72.6. Использовать задачу 72.5 и доказать, что любая подгруппа индекса p в A есть подгруппа элементов некоторого $(n - 1)$-мерного подпространства.

72.7. Пусть χ — характер представления Φ. Используя задачу 72.5, доказать, что $\Phi(g) = E$ для $g \in H$. Аналогично, показать, что $g \in K$ тогда и только тогда, когда матрица $\Phi(g)$ скалярная.

72.8. Использовать теорему Машке и свойства коммутанта.

72.9. Использовать теорему Машке и свойства коммутанта.

72.20.

	1	-1	i	j	k
χ	2	-2	0	0	0

. Использовать задачу 70.24.

72.21. $\chi_\Phi(\sigma)$ есть число элементов множества $\{1, 2, 3, \ldots, n\}$, неподвижных относительно σ.

72.22. Пусть $\mathbf{D}_n = \langle a, b \mid a^2 = b^n = e, \ \ aba = b^{-1}\rangle$. Тогда $\chi(b^k) = 2\cos\dfrac{2\pi k}{n}$, $\quad \chi(ab^k) = 0$.

72.23.

	e	(12)	(123)	(12)(34)	(1234)
χ	3	1	1	-1	-1

. Использовать задачу 70.19.

72.24.

	e	(12)	(123)	(12)(34)	(1234)
χ	3	-1	0	-1	1

. Использовать задачу 70.19.

72.25. Использовать задачу 72.4.

72.26. а) Два характера: тривиальный и $\sigma \to \operatorname{sgn}\sigma$.

б)

	e	(123)	(132)	(12)(34)
φ_0	1	1	1	1
φ_1	1	ε	ε^2	1
φ_2	1	ε^2	ε	1

, где ε — первообразный корень степени 3 из 1 в $\mathbb{C}$.

в)

	e	-1	i	j	k
φ_0	1	1	1	1	1
φ_1	1	1	-1	-1	1
φ_2	1	1	-1	1	-1
φ_3	1	1	1	-1	-1

г) См. а).

д) Пусть $\mathbf{D}_n = \langle a, b \mid a^2 = b^n = e, \ aba = b^{-1}\rangle$. Если n нечетно, то одномерных характеров два: тривиальный и $a^i b^j \to (-1)^i$. Если n четно, то четыре: тривиальный и $a^i b^j \to (-1)^i$, $a^i b^j \to (-1)^j$, $a^i b^j \to (-1)^{i+j}$.

72.27. $n^{n/2}$. Использовать соотношения ортогональности для характеров для вычисления произведения матрицы на ее сопряженную.

72.28. а)

	e	(12)	(123)
φ_0	1	1	1
φ_1	1	-1	1
φ_0	2	0	-1

. Использовать задачи 72.26 и 70.19.

б)

	e	(12)	(123)	(12)(34)	(1234)
φ_0	1	1	1	1	1
φ_1	-1	1	1	1	-1
φ_2	3	1	0	-1	-1
φ_3	3	-1	0	-1	1
φ_4	2	0	-1	2	0

. Использовать задачи 72.26, 72.23, 72.24, 72.20.

в)

	1	-1	i	j	k
φ_0	1	1	1	1	1
φ_1	1	1	1	-1	-1
φ_2	1	1	-1	1	-1
φ_3	1	1	-1	-1	1
φ_4	2	-2	0	0	0

. Использовать задачи 72.26 и 72.20.

г)

	e	b	b^2	a	ab
φ_0	1	1	1	1	1
φ_1	1	-1	1	-1	1
φ_2	1	-1	1	1	-1
φ_3	1	1	1	-1	-1
φ_4	2	0	-2	0	0

. Использовать задачи 72.26 и 72.22.

д)

	e	b	b^2	a
φ_0	1	1	1	1
φ_1	2	$2\cos\dfrac{2\pi}{5}$	$2\cos\dfrac{4\pi}{5}$	0
φ_2	2	$2\cos\dfrac{4\pi}{5}$	$2\cos\dfrac{2\pi}{5}$	0

. Использовать задачи 72.26 и 72.22.

е)

	e	(12)(34)	(123)	(132)
φ_0	1	1	1	1
φ_1	1	1	ε	ε^2
φ_2	1	1	ε^2	ε
φ_3	3	-1	0	0

, где ε — корень третьей степени из 1 в $\mathbb{C}$. Использовать задачу 72.26.

72.29. Нет, так как скалярный квадрат указанной функции не является целым числом.

72.30. В обозначениях к задаче 72.28, а) $F = 2\varphi_4 + 0,5\varphi_1 + 0,5\varphi_3$.

72.31. В обозначениях ответа к задаче 72.28, а) запишем $f_1 = -\varphi_0 + 3\varphi_1 + 2\varphi_2$, $f_2 = 4\varphi_1 + \varphi_2$. Отсюда следует, что f_1 не является характером представления. f_2 — характер прямой суммы неприводимого двумерного представления группы $\mathbf{S}_3$ и четырех экземпляров нетривиального одномерного представления этой группы.

72.32. а) Доказать, что отображение A в $\mathbb{C}$, переводящее χ в $\chi(a)$, при некотором $a \in A$ есть характер группы A и доказать, что возникающее таким образом отображение $A \to \widehat{A}$ есть изоморфизм.

72.33. в) Вывести с помощью а) равенство

$$f(a) = \sum_{\chi \in \widehat{A}} f(\chi) \cdot \chi(a)$$

и доказать, что $\widehat{\widehat{f}}$ переходит в $(|A|)^{-1} f$ при изоморфизме задачи 72.32, в).

72.34. Использовать равенство $(f,f)_A = \sum_{\chi\in\widehat{A}}(f,\chi)_A^2$.

72.37. Приведем разложение характера представления Ψ на неприводимые характеры.

а) $\chi_\Psi = \Psi_0 + \Psi_1 + \Psi_2$.
б) $\chi_\Psi = \Psi_0 + \Psi_1 + \Psi_2 + \Psi_4$.
в) $\chi_\Phi = \Psi_0 + \Psi_1 + \Psi_2 + \Psi_3$.

72.38. $\chi_\Psi = n\cdot\chi_\Phi$.

72.39. n^{m-1}. Доказать, что все неприводимые представления группы G входят в $\rho^{\otimes m}$ с одинаковой кратностью.

72.40. а) $\chi_{\rho^2} = \Psi_0 + \Psi_1 + \Psi_2$.
б) $\chi_{\rho^3} = \Psi_0 + \Psi_1 + 3\Psi_2$.

72.41. Если

$$\overline{n} = \left[\frac{n+1}{2}\right], \qquad \overline{m} = \left[\frac{m}{2}\right],$$

то кратность равна $\binom{\overline{n}-1}{\overline{m}}$.

72.42. Рассмотреть представление на пространстве кососимметрических дважды контравариантных тензоров.

72.43. В обозначениях ответа к задаче 72.28, а):
а) φ_1; б) $\varphi_0+\varphi_2$; в) $\varphi_0+\varphi_1$; г) $\varphi_1+\varphi_2$.

73.2. а) $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$. б) $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

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

д) $\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$. е) $\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}$.

73.3. б) и г). в) и е).

73.4. В том случае, когда для любых k, λ в жордановой форме матрицы A число жордановых клеток порядка k с собственным значением λ равно числу жордановых клеток порядка k с собственным значением $-\lambda$.

73.5. а) Всякое представление имеет вид $R_A(t) = e^{(\ln t)A}$, $\mathbf{A}\in\mathbf{M}_n(\mathbb{C})$.
б) Всякое представление эквивалентно представлению вида

$$R_{A,B}(t) = \begin{pmatrix} e^{\ln|t|\cdot|A|} & 0\\ 0 & (\operatorname{sgn} t)e^{\ln|t|\cdot B}\end{pmatrix}, \quad A\in\mathbf{M}_p(\mathbb{C}), \quad B\in\mathbf{M}_q(\mathbb{C}).$$

Рассмотреть образ элемента $-1\in\mathbb{R}^*$ при данном представлении, доказать, что его собственные подпространства инвариантны, и воспользоваться а).

в) Всякое представление эквивалентно представлению вида

$$z\to\begin{pmatrix} z^{k_1} & & & 0\\ & z^{k_2} & & \\ & & \ddots & \\ 0 & & & z^{k_n}\end{pmatrix}, \quad k_1,\dots,k_n\in\mathbb{Z}.$$

Доказать, что представление аддитивной группы $\mathbb{C}$, получаемое как композиция гомоморфизма $\mathbb{C} \to \mathbb{C}^*$ $(t \to e^t)$ и представления группы $\mathbb{C}^*$, имеет вид P_A (см. задачу 73.1) и $e^{2\pi i A} = E$. Затем доказать, что матрица A подобна целочисленной диагональной матрице.

г) Всякое представление эквивалентно представлению вида

$$z \to \begin{pmatrix} z^{k_1} & & & 0 \\ & z^{k_2} & & \\ & & \ddots & \\ 0 & & & z^{k_n} \end{pmatrix}, \quad k_1, \ldots, k_n \in \mathbb{Z}.$$

Рассмотреть представление аддитивной группы поля $\mathbb{R}$, получаемое как композиция гомоморфизма $\mathbb{R} \to \mathbf{U}$ $(t \to e^{it})$, и представления группы $\mathbf{U}$, затем воспользоваться задачей 73.1.

73.6. Да; доказать, что всякую невырожденную комплексную квадратную матрицу можно представить в виде e^A, и воспользоваться задачей 73.1.

73.7. Линейные оболочки наборов собственных векторов для A.

73.9. Рассмотреть ограничение представления Φ_n на подгруппу диагональных матриц.

73.10. д) Доказать, что равенство имеет место на подмножестве диагонализируемых матриц.

73.11. Заметить, что

$$\mathbf{SU}_2(\mathbb{C}) = \{A \in \mathbb{H} \mid (A, A) = 1\}.$$

Доказать, что если $A \in \mathbf{SU}_2(\mathbb{C})$ имеет собственные значения $e^{\pm i\varphi}$, то оператор $P(A)$ есть поворот пространства $\mathbb{H}_0$ на угол 2φ вокруг оси, проходящей через $A - \dfrac{1}{2}(\operatorname{tr} A)E \in \mathbb{H}_0$.

б) Доказать, что группа $R(\mathbf{SU}_2(\mathbb{C}) \times \mathbf{SU}_2(\mathbb{C}))$ транзитивно действует на единичной сфере в $\mathbb{H}$, и воспользоваться а).

в) Комплексификация пространства $\mathbb{H}_0$ есть подпространство матриц вида $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ в $\mathbf{M}_2(\mathbb{C})$. Искомый изоморфизм осуществляется отображением, сопоставляющим такой матрице многочлен $f(x, y) = -bx^2 + 2axy + cy^2$.

73.12, 73.13. См.: *Супруненко Д.А.* Группы матриц. — М.: Наука, 1972. — Гл. V.

Приложение

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

§ V. Элементы теории представлений

Для изложения основных определений и первоначальных результатов в теории представлений групп традиционно используется несколько разных способов. При дальнейшем развитии теории выясняются связи между различными вариантами определений и вырабатываются способы "перевода с одного языка на другой". Мы не имеем в виду определенного способа первоначального изложения, считая целесообразным ознакомить изучающих с основными способами, принятыми в литературе, и дать возможность преподавателю найти задачи, использующие удобные ему варианты изложения.

Напомним в основных чертах эти основные подходы к построению теории представлений или варианты терминологии.

А. Терминология линейных представлений *Линейным представлением* группы G на пространстве V называется гомоморфизм $\Phi\colon G \to \mathbf{GL}(V)$ группы G в группу невырожденных линейных операторов на V. Размерность пространства V называется *размерностью* или *степенью представления*. *Гомоморфизмом представления* Φ группы G на пространстве V в представление Ψ группы G на пространстве W называется линейное отображение $\alpha : V \to W$, для которого $\alpha(\Phi(g)v) = \Psi(\alpha(v))$ при всех $g \in G$, $v \in V$. Если гомоморфизм α является изоморфизмом пространств, то представления Φ и Ψ называют *изоморфными*.

Подпространство U в пространстве V представления Φ группы G называют *инвариантным*, если $\Phi(g)U = U$ при всех $g \in G$. Представление ненулевой степени, не имеющее инвариантных подпространств, отличных от нуля и всего пространства, называют *неприводимым*.

Б. Терминология матричных представлений *Матричным представлением* группы G степени n над полем F называется гомоморфизм $\rho : G \to \mathbf{GL}_n(F)$ группы G в группу обратимых матриц порядка n над полем F. Два матричных представления ρ и σ группы G одного и того же порядка n над F называют *эквивалентными* (*изоморфными*), если существует такая невырожденная матрица $C \in \mathbf{M}_n(F)$, что $\rho(g) = C^{-1}\sigma(g)C$ для всех $g \in G$.

Матричное представление называется *приводимым*, если оно эквивалентно представлению, в котором все матрицы имеют один и тот же “угол нулей”, т. е. имеют вид $\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$, где A и B — матрицы порядков r и s, одинаковых для всех $g \in G$.

В. Терминология линейных G-пространств Пусть G — группа, V — линейное пространство. Говорят, что на V задана структура линейного G-пространства, если на $G \times V$ определена операция со значениями в V, причем отображение $v \to g * v$ является линейным отображением пространства V в себя и $g_1 * (g_2 * v) = (g_1 g_2) * v$ при всех $g_1, g_2 \in G$, $v \in V$. Два G-пространства V и W называют изоморфными, если существует такой изоморфизмом пространств $\alpha : V \to W$, что $\alpha(g * v) = g * \alpha(v)$ для всех $g \in G$, $v \in V$.

Подпространство U в G-пространстве V называют *инвариантным*, если $g * u \in U$ при всех $g \in G$, $u \in U$. Ненулевое G-пространство V называют *неприводимым*, если оно не имеет нетривиальных инвариантных подпространств.

Г. Терминология модулей над групповой алгеброй Пространство V называют *модулем* над групповой алгеброй $F[G]$ или $F[G]$-модулем, если на $F[G] \times V$ определена операция $(a, v) \to a \cdot v$ со значениями в V, для которой $a_1(a_2 v) = (a_1 a_2) \cdot v$. Два $F[G]$-модуля V и W изоморфны, если существует линейное отображение $\alpha\colon V \to W$, для которого $\alpha(a \cdot v) = a \cdot \alpha(v)$ при всех $a \in F[G]$, $v \in V$.

Подпространство U в $F[G]$-модуле V называют *подмодулем*, если $a \cdot u \in U$ при всех $a \in F[G]$, $u \in U$, и ненулевой модуль V называют *простым* или *неприводимым*, если он не имеет нетривиальных подмодулей.

Отметим, что, имея структуру $F[G]$-модуля на V и рассматривая группу G как подмножество в $F[G]$ (суммы с одним ненулевым коэффициентом, равным 1), при ограничении операции на $G \times V$ мы получаем на V структуру G-пространства $(g, v) \to g \cdot v$.

Наоборот, имея на V структуру G-пространства, мы можем положить

$$\Big(\Big(\sum \alpha_g \cdot g\Big), v\Big) \to \sum \alpha_g (g * v),$$

и это превращает V в $F[G]$-модуль.

Если Φ — линейное представление группы G на V, то операция

$$(g, v) \to \Phi(g) v$$

задает на V структуру G-пространства.

Если V — G-пространство и $\Phi(g)\colon v \to g * v$, то $\Phi(g)$ — линейный оператор на V, и легко показать, что $g \to \Phi(g)$ — линейное представление группы G на пространстве V.

Если имеется линейное представление группы G на n-мерном пространстве V, то, выбирая в V базис и сопоставляя каждому элементу $g \in G$ матрицу оператора $\Phi(g)$ в этом базисе, мы получаем отображение G в $\mathbf{GL}_n(F)$, которое оказывается матричным представлением группы G. Другой выбор базиса приводит к эквивалентному матричному представлению.

Если задано n-мерное матричное представление ρ группы G, то, сопоставляя каждому элементу $g \in G$ оператор умножения на матрицу $\rho(g)$ в пространстве F^n, мы получаем линейное представление группы G на пространстве F^n.

Нетрудно проверить, что указанные способы перехода от $F[G]$-модулей к G-пространствам, линейным и матричным представлениям и обратно переводят неприводимые объекты в неприводимые и изоморфные — в изоморфные.

Операция умножения в $F[G]$ задает на пространстве $V = F[G]$ структуру $F[G]$-модуля; соответствующее линейное представление группы G на V называют *регулярным представлением*. Мы можем также задавать регулярное представление, рассматривая пространство V с базисом (e_g), $g \in G$, и определяя отображение $R : G \to \mathbf{GL}(V)$ правилом $R(h)e_g = e_{hg}$ при всех $g, h \in G$. Базис (e_g) называется *каноническим базисом* пространства регулярного представления.

Приведем основные теоремы о представлениях групп.

Теорема 1. *Пусть G' — коммутант группы G и $\varphi : G \to G/G'$ — канонический гомоморфизм. Тогда формула $\psi \to \psi \circ \varphi$ устанавливает взаимно однозначное соответствие между множествами одномерных представлений групп G и G/G'.*

Теорема 2 (Машке). *Пусть группа G конечна и* $\operatorname{char} F$ *не делит $|G|$. Тогда всякое конечномерное представление группы G над полем F изоморфно прямой сумме неприводимых представлений.*

Теорема 3. *Пусть группа G конечна, поле F алгебраически замкнуто и* $\operatorname{char} F$ *не делит $|G|$. Тогда число различных неприводимых представлений группы G над полем F равно числу классов сопряженных элементов группы G, а сумма квадратов размерностей этих представлений равна порядку группы G.*

§ VI. Список определений

Приведем список основных понятий, использованных в задачнике.

Алгебра банахова — полная нормированная алгебра.

Алгебра Грассмана векторного пространства — внешняя алгебра пространства.

Алгебра групповая (группы G над полем F) — множество конечных формальных линейных комбинаций вида $\sum_g \alpha_g g$ ($g \in G$, $a_g \in F$) с естественным сложением и умножением на элементы поля F и операцией умножения

$$\alpha_g g \cdot \alpha_h h = \alpha_g \alpha_h gh,$$

распространяющейся на линейные комбинации по закону дистрибутивности.

Алгебра дифференциальных операторов — алгебра Вейля.

Алгебра нетерова (коммутативная) — коммутативная алгебра, в которой всякая строго возрастающая последовательность идеалов конечна.

Алгебра нормированная (над нормированном полем K) — алгебра с функцией $\|x\|$, $x \in A$, принимающей неотрицательные вещественные значения, причем:

а) $\|x\| \geqslant 0$ и $\|x\| = 0$ тогда и только тогда, когда $x = 0$;

б) $\|x+y\| \leqslant \|x\| + \|y\|$;

в) $\|\lambda x\| = |\lambda| \cdot \|x\|$, где $\lambda \in K$, $x \in A$;

г) $\|xy\| \leqslant \|x\| \cdot \|y\|$.

Алгебра полупростая — алгебра, не имеющая ненулевых двусторонних идеалов, состоящих из нильпотентных элементов; в коммутативном случае алгебра без нильпотентных элементов, отличных от 0.

Алгебра простая — алгебра, не имеющая двусторонних идеалов, отличных от 0 и всей алгебры.

Алгебра формальных степенных рядов (от переменного x над полем K) — множество формальных выражений вида $\sum_{k=0}^{\infty} a_k x^k$ $(a_k \in K)$ с естественнымсложением и умножением на элементы поля K и операцией умножения

$$\sum_{k=0}^{\infty} a_k x^k \cdot \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} c_k x^k, \quad \text{где} \quad c_k = \sum_{\substack{i+j=k \\ i \geqslant 0,\ j \geqslant 0}} a_i b_j.$$

Алгебра центральная — алгебра, центр которой совпадает с$1 \cdot K$, где 1 — единица алгебры, K — ее основное поле.

Векторное пространство нормированное (над нормированном полем K) — векторное пространство с функцией $\|x\|$, принимающей неотрицательные вещественные значения, причем:

а) $\|x\| \geqslant 0$ и $\|x\| = 0$ тогда и только тогда, когда $x = 0$;

б) $\|x+y\| \leqslant \|x\| + \|y\|$;

в) $\|\lambda x\| = |\lambda| \cdot \|x\|$, где $\lambda \in K$, $x \in V$.

Вращение — движение, сохраняющее ориентацию пространства и имеющее неподвижную точку.

K-вложение — инъективный K-гомоморфизм.

Гомоморфизм унитарный — гомоморфизм колец (алгебр), при котором единица переходит в единицу.

K-гомоморфизм — гомоморфизм алгебр над полем K; термин употребляется в случае, когда алгебры рассматриваются одновременно над некоторым расширением поля K.

Группа делимая — абелева группа, в которой для любого элемента a и любого целого числа n уравнение $nx = a$ имеет решение.

Группа диэдра $\mathbf{D}_n$ — группа движений плоскости, отображающих правильный n-угольник на себя.

Группа кватернионов $\mathbf{Q}_8$ — множество элементов ± 1, $\pm i$, $\pm j$, $\pm k$ с умножением элементов, как в теле кватернионов.

Группа Клейна $\mathbf{V}_4$ — группа перестановок

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

и всякая изоморфная ей группа.

Группа периодическая — группа, все элементы которой имеют конечный порядок.

Движение — отображение евклидова пространства в себя, сохраняющее расстояния между точками.

Действие группы на множестве — группа G действует на множестве M, если каждому элементу $g \in G$ поставлена в соответствие биекция $M \to M$ и $g_1 g_2(m)) = (g_1 g_2)(m)$ для любых $g_1, g_2 \in G$, $m \in M$.

Декремент перестановки — разность между степенью перестановки и числом циклов в ее разложении на независимые циклы (с учетом циклов длины 1).

Делитель нуля в кольце — элемент a, для которого существует элемент $b \neq 0$ такой, что $ab = 0$ (левый делитель нуля).

Единицы матричные — квадратные матрицы E_{ij} $(i, j = 1, \ldots, n)$, у которых на пересечении i-й строки и j-го столбца стоит 1, а остальные элементы равны 0.

Идеал максимальный — идеал кольца (алгебры), не содержащийся строго ни в каком идеале, отличном от всего кольца (всей алгебры).

Идеал простой (коммутативного кольца) — идеал, факторкольцо (фактороалгебра) по которому не содержит делителей нуля.

Идемпотент — элемент кольца, совпадающий со своим квадратом.

Идемпотенты ортогональные — идемпотенты, произведение которых равно нулю.

Кватернион — элемент тела кватернионов.

Кватернион чистый — кватернион, действительная часть которого равна 0.

Кольцо без делителей нуля — кольцо, не содержащее делителей нуля, отличных от 0.

Кольцо многочленов от некоммутирующих переменных $x_1, \ldots, x_n$ (над кольцом A) — множество формальных выражений вида

$$\sum_{k_1, \ldots, k_m} a_{k_1, \ldots, k_m} x_{k_1} \times \ldots \times x_{k_m} \quad (a_{k_1, \ldots, k_m} \in A)$$

с естественными операциями сложения и умножения одночленов

$$a_{k_1, \ldots, k_m} x_{k_1} \times \ldots \times x_{k_m} \cdot b_{i_1, \ldots, i_s} x_{i_1} \times \ldots \times x_{i_s} = \\ = a_{k_1, \ldots, k_m} b_{i_1, \ldots, i_s} x_{k_1} \times \ldots \times x_{k_m} x_{i_1} \times \ldots \times x_{i_s},$$

распространяемыми на суммы по закону дистрибутивности.

Кольцо нетерово (коммутативное) — коммутативное кольцо, в котором всякая строго возрастающая последовательность идеалов конечна.

Кольцо простое — кольцо с ненулевым умножением, не имеющее двусторонних идеалов, отличных от нулевого и самого кольца.

Кольцо целых гауссовых чисел — кольцо, состоящее из комплексных чисел $x + yi$ $(x, y \in \mathbb{Z})$.

Коммутант группы — подгруппа, порожденная всеми коммутаторами элементов группы.

Коммутатор элементов группы x и y — элемент группы $xyx^{-1}y^{-1}$.

Коммутатор кольца x и y — элемент кольца $xy - yx$.

Координаты барицентрические — координаты $\lambda_0, \lambda_1, \ldots, \lambda_n$ точки x аффинного пространства относительно системы точек $x_0, x_1, \ldots, x_n$, находящихся в общем положении, определяющиеся равенством

$$x = \sum_{i=0}^{n} \lambda_i x_i, \qquad \text{где} \quad \sum_{i=0}^{n} \lambda_i = 1.$$

Коразмерность подпространства — разность между размерностью пространства и размерностью подпространства.

Корень (*комплексный*) *из* 1 — комплексное число, некоторая степень которого с ненулевым показателем равна 1.

Корень (*комплексный*) *из* 1 *первообразный степени* n — корень из 1, не являющийся корнем из 1 степени, меньшей n.

Матрица верхняя (*нижняя*) *треугольная* — матрица, у которой элементы, стоящие ниже (выше) главной диагонали, равны 0.

Матрица Грама (системы векторов $e_1, \ldots, e_n$ евклидова пространства) — матрица $((e_i, e_j))$ порядка n.

Матрица кососимметрическая — матрица A, для которой ${}^tA = -A$.

Матрица косоэрмитова — комплексная матрица, для которой ${}^tA = -\overline{A}$, где $\overline{A}$ — матрица, полученная из A заменой ее элементов на комплексно сопряженные.

Матрица нильпотентная — матрица, некоторая степень которой равна нулевой матрице (нильпотентный элемент кольца матриц).

Матрица нильтреугольная — верхняя (или нижняя) треугольная матрица с нулями на главной диагонали.

Матрица ортогональная — матрица A, для которой ${}^tA = A^{-1}$.

Матрица перестановки — матрица, у которой в каждой строке и в каждом столбце стоит ровно один элемент, равный 1, а остальные элементы равны 0.

Матрица периодическая — матрица, некоторая степень которой равна единичной матрице.

Матрица присоединенная — матрица, транспонированная к матрице, составленной из алгебраических дополнений элементов данной матрицы.

Матрица симметрическая — матрица A, для которой ${}^tA = A$.

Матрица треугольная — верхняя или нижняя треугольная матрица.

Матрица унимодулярная — матрица с определителем 1.

Матрица унитарная — комплексная матрица A, для которой ${}^t\overline{A} = A^{-1}$, где ${}^t\overline{A}$ — матрица, полученная из ${}^tA$ заменой ее элементов на комплексно сопряженные.

Матрица унитреугольная — треугольная матрица с единицами на главной диагонали.

Матрица элементарная — матрица вида $E + (\gamma - 1)E_{ij}$, $\gamma \neq 0$ (матрица I типа), $E + \alpha E_{ij}$, $\alpha \neq 0$ (II типа); иногда элементарными называют также матрицы-перестановки.

Матрица эрмитова — комплексная матрица A, для которой ${}^tA = \overline{A}$, где $\overline{A}$ — матрица, полученная из A заменой ее элементов на комплексно сопряженные.

Многочлен круговой (деления круга) $\Phi_n(x)$ — многочлен

$$\prod_{k=1}^{\varphi(n)} (x - \varepsilon_k),$$

где $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ — первообразные корни степени n из 1.

Многочлен минимальный линейного оператора — многочлен наименьшей степени, аннулирующий данный оператор; минимальный многочлен матрицы оператора.

Многочлен минимальный матрицы — многочлен наименьшей степени, аннулирующий данную матрицу.

Модуль неприводимый — ненулевой модуль, не имеющий подмодулей, отличных от нулевого и самого модуля.

Модуль приводимый — ненулевой модуль, не являющийся неприводимым.

Модуль унитарный — модуль, в котором единица кольца действует тождественно.

Модуль циклический — модуль, в котором существует такой элемент m_0, что для любого элемента m модуля M существует элемент кольца a такой, что $am_0 = m$.

Нильрадикал кольца — наибольший (в смысле теоретико-множественного включения) двусторонний идеал кольца, состоящий из нильпотентных элементов.

Нормализатор подгруппы — наибольшая подгруппа, в которой данная подгруппа является нормальной.

Нормальное замыкание элемента группы — наименьшая нормальная подгруппа, содержащая данный элемент.

Оператор кососимметрический — линейный оператор $\mathcal{A}$, для которого $(\mathcal{A}x, y) = -(y, \mathcal{A}x)$ при любых векторах x и y (т. е. $\mathcal{A}^* = -\mathcal{A}$).

Оператор косоэрмитов — линейный оператор A в эрмитовом пространстве, для которого $(\mathcal{A}x, y) = -(x, A^*y)$ при любых векторах x и y (т. е. $\mathcal{A}^* = -\mathcal{A}$).

Оператор нормальный — линейный оператор в евклидовом или метрическом пространстве, перестановочный со своим сопряженным оператором.

Оператор ортогональный — линейный оператор $\mathcal{A}$, сохраняющий скалярное произведение векторов $((\mathcal{A}x,\ \mathcal{A}y) = (x, y)$ для любых векторов x и $y)$ (т. е. $\mathcal{A}^* = \mathcal{A}^{-1}$).

Оператор полупростой — линейный оператор, у которого всякое инвариантное подпространство обладает инвариантным дополнительным подпространством.

Оператор самосопряженный — линейный оператор в евклидовом или эрмитовом пространстве, для которого $(\mathcal{A}x, y) = (x, \mathcal{A}y)$ при любых векторах x и y (т. е. $\mathcal{A}^* = \mathcal{A}$).

Оператор симметрический — линейный оператор в евклидовом или эрмитовом пространстве, для которого $(\mathcal{A}x, y) = (x, \mathcal{A}y)$ при любых векторах x и y (т. е. $\mathcal{A}^* = \mathcal{A}$).

Оператор сопряженный (к оператору $\mathcal{A}$) — линейный оператор $\mathcal{A}^*$, для которого $(\mathcal{A}x, y) = (x, \mathcal{A}^*y)$.

Оператор унитарный — линейный оператор $\mathcal{A}$ в эрмитовом пространстве, сохраняющий скалярное произведение векторов $(\mathcal{A}x, \mathcal{A}y) = (x, y)$ для любых векторов x, y) (т. е. $\mathcal{A}^* = \mathcal{A}^{-1}$).

Оператор эрмитов — линейный оператор $\mathcal{A}$ в эрмитовом пространстве, для которого $(\mathcal{A}x, y) = (x, \mathcal{A}y)$ при любых векторах x и y (т. е. $\mathcal{A}^* = \mathcal{A}$).

Определитель Грама — определитель матрицы Грама.

Орбита элемента — множество образов элемента при действии всех элементов группы.

Отражение (в пространстве U параллельно дополнительному подпространству V) — линейный оператор, ставящий каждому вектору $x = u + v$ $(u \in U,\ v \in V)$ в соответствие вектор $u - v$.

Параллелепипед (со сторонами $a_1, \ldots, a_k$) — множество линейных комбинаций $\sum_{i=1}^{k} \lambda_i a_i$ $(0 \leqslant \lambda_i \leqslant 1,\ i = 1, \ldots, k)$.

Перестановка — взаимно однозначное отображение конечного множества на себя; подстановка.

Период группы — наименьшее натуральное число n, для которого $x^n = e$ для любого элемента группы x.

Периодическая часть группы — множество элементов группы, имеющих конечный порядок.

Подгруппа максимальная — подгруппа, не содержащаяся строго ни в какой подгруппе, отличной от всей группы.

Подпространство дополнительное (к подпространству U) — подпространство V, для которого все пространство равно $U \oplus V$.

Подпространство вполне изотропное (относительно симметрической или полуторалинейной функции $f(x, y)$) — подпространство, на котором $f(x, y)$ принимает нулевое значение.

Поле разложения многочлена — наименьшее расщепляющее поле многочлена. *Поле расщепляющее многочлена* — расширение поля коэффициентов многочлена, над которым он раскладывается в произведение линейных множителей.

Поле расщепляющее многочленов — расширение поля коэффициентов многочленов, над которым все данные многочлены раскладываются в произведение линейных множителей.

Пополнение метрического пространства — пополнение относительно последовательности Коши.

Проектирование (на подпространство U параллельно дополнительному подпространству V) — линейный оператор, ставящий каждому вектору $x = u + v$ ($u \in U$, $v \in V$) в соответствие вектор u.

Произведение полупрямое групп G и H — множество $G \times H$ с операцией

$$(x, y)(z, t) = (x \cdot \varphi(y)(z), yt),$$

где $\varphi : H \to \operatorname{Aut} G$ — некоторый гомоморфизм.

Символ Кронекера — $\delta_{ij} = 1$, $\delta_{ij} = 0$ при $i \neq j$ ($i, j = 1, \ldots, n$).

След матрицы — сумма элементов матрицы, стоящих на главной диагонали.

След оператора — след матрицы данного оператора.

Тело кватернионов — векторное пространство над полем $\mathbb{R}$ с базисом $1, i, j, k$, где 1 — единица умножения, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$; алгебра обобщенных кватернионов при $\alpha = \beta = 1$.

Функция Мёбиуса — функция натурального числа n, определяемая равенством

$$\mu(n) = \begin{cases} 1 & \text{при } n = 1, \\ (-1)^r, & \text{если } n \text{ — произведение } r \text{ различных простых чисел,} \\ 0 & \text{в остальных случаях.} \end{cases}$$

Функция Эйлера — при $n = 1$ равна 1, при $n > 1$ равна числу натуральных чисел, меньших n и взаимно простых с n.

Центр группы (кольца) — множество элементов, перестановочных со всеми элементами группы (кольца).

Централизатор элемента группы — множество элементов группы, перестановочных с данным элементом.

Элемент нильпотентный кольца — элемент, некоторая степень которого равна 0.

Элементарные преобразования строк матрицы над кольцом — умножение строки на обратный элемент кольца (I тип), прибавление к строке другой строки, умноженной на элемент кольца (II тип).

p-группа — группа, все элементы которой имеют порядок вида p^n $(n \in \mathbb{N})$.

p-подгруппа силовская — максимальная подгруппа, являющаяся p-подгруппой.

§ VII. Список обозначений

${}^tA$ — транспонированная матрица для матрицы A.

$\widehat{A}$ — присоединенная матрица для матрицы A.

$\mathcal{A}^*$ — сопряженный оператор для линейного оператора $\mathcal{A}$.

$\mathbf{A}_n$ — знакопеременная группа степени n (группа четных перестановок на множестве $\{1, 2, \ldots, n\}$).

$|A|$ — число элементов множества A.

$[A, B]$ — коммутатор $AB - BA$ матриц A и B.

$\operatorname{Aut} G$ — группа автоморфизмов группы G.

Alt — оператор альтернирования в пространстве $\mathbb{T}_0^q(V)$.

(a) — идеал кольца, порожденный элементом a.

$\langle a \rangle$ — подгруппа (подкольцо, подалгебра, подпространство), порожденная элементом a.

$\langle a \rangle_n$ — циклическая группа порядка n с образующим элементом a.

$\arg z$ — аргумент комплексного числа z; считается, что $0 \leqslant \arg z < 2\pi$.

$\mathbb{C}$ — множество (поле, аддитивная группа) комплексных чисел.

$\mathbf{D}_n$ — группа диэдра (группа движений правильного n-угольника).

$\mathbf{D}_n(A)$ — множество диагональных матриц порядка n над кольцом A.

$\mathcal{D}$ — оператор дифференцирования в функциональных пространствах.

$\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ — диагональная матрица с элементами $\lambda_1, \ldots, \lambda_n$ на главной диагонали.

$\operatorname{End} A$ — кольцо эндоморфизмов абелевой группы A (кольца A).

e^A — сумма ряда Тейлора функции e^x при $x = A$ (A — матрица).

E_{ij} (матричная единица) — матрица, у которой элемент на пересечении i-й строки с j-м столбцом равен 1, а остальные элементы равны 0.

$\mathbb{F}_q$ — поле из q элементов.

G_a — стационарная подгруппа элемента $a \in M$ при действии группы G на множестве M.

G' — коммутант группы G.

$\mathbf{GL}(V)$ — группа невырожденных линейных операторов в векторном пространстве V.

$\mathbf{GL}_n(F)$ — группа невырожденных линейных операторов в n-мерном векторном пространстве над полем F, группа невырожденных матриц порядка n над полем F.

$\mathbf{GL}_n(q)$ — то же самое, что и $\mathbf{GL}_n(\mathbb{F}_q)$.

$\mathbb{H}$ — тело кватернионов.

$\operatorname{Hom}(A, B)$ — группа гомоморфизмов группы A в абелеву группу B.

K^* — группа обратимых элементов кольца K.

$K(a)$ — расширение поля K, полученное присоединением элемента a.

$F[G]$ — групповая алгебра группы G над полем K.

$K[x]$ — кольцо многочленов от переменного x с коэффициентами из кольца K.

$K[x]_n$ — множество многочленов из кольца $K[x]$ степени, не большей n.

$K(x)$ — поле рациональных функций от переменного x с коэффициентами из поля K.

$K[[x]]$ — кольцо формальных степенных рядов от переменного x с коэффициентами из кольца K.

$K[x_1, \ldots, x_n]$ — кольцо многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами из кольца K.

$K\{x_1, \ldots, x_n\}$ — кольцо многочленов от некоммутирующих переменных $x_1, \ldots, x_n$ с коэффициентами из кольца K.

$L(V)$ — множество линейных операторов в векторном пространстве V.

$\ln A$ — сумма ряда Тейлора функции $\ln(1-x)$ при $x = E - A$ (A — матрица).

$\mathbf{M}_n(K)$ — кольцо (алгебра) матриц порядка n над кольцом K.

$\mathbb{N}$ — множество натуральных чисел.

$N(A)$ — нильрадикал алгебры A.

$N(H)$ — нормализатор подгруппы H.

$\mathbf{N}_{A/K}(a)$ — норма элемента a алгебры A над полем K.

$n\mathbb{Z}$ — множество целых чисел, кратных числу n.

$\mathbf{O}_n(K)$ — группа ортогональных матриц порядка n над полем K.

$\mathbb{Q}$ — множество (поле, аддитивная группа) рациональных чисел.

$\mathbb{Q}_p$ — поле p-адических чисел.

$\mathbb{R}_+$ — множество (мультипликативная группа) положительных вещественных чисел.

$\operatorname{rk} A$ — ранг матрицы.

$\operatorname{rk} \mathcal{A}$ — ранг линейного оператора $\mathcal{A}$.

$\langle S \rangle$ — подгруппа (подкольцо, подалгебра, подпространство) с множеством порождающих S; аффинная оболочка множества S.

$\mathbf{S}_n$ — симметрическая группа степени n (группа перестановок множества $\{1, \ldots, n\}$).

$\mathbf{S}_X$ — группа взаимно однозначных отображений множества X на себя.

$\mathbf{SL}_n(K)$ — группа матриц с определителем 1 над полем K.

$\mathbf{SL}_n(q)$ — то же самое, что $\mathbf{SL}_n(\mathbb{F}_q)$.

$\mathbf{SO}_n(\mathbb{C})$ — группа ортогональных матриц с определителем 1 над полем K.

$\mathbf{SU}_n(\mathbb{C})$ — группа унитарных комплексных матриц с определителем 1.

$\mathbf{SU}_n$ — то же самое, что и $\mathbf{SU}_n(\mathbb{C})$.

$\mathbf{S}(V)$ — симметрическая алгебра векторного пространства V.

$\mathbf{S}^q(V)$ — q-я симметрическая степень векторного пространства V.

Sym — оператор суммирования в пространстве $\mathbb{T}_0^q(V)$.

$\mathbb{T}(V)$ — тензорная алгебра векторного пространства V.

$\mathbb{T}_p^q(V)$ — векторное пространство тензоров типа (p, q) на векторном пространстве V.

$\operatorname{tr} A$ — след матрицы A.

$\operatorname{tr} \mathcal{A}$ — след линейного оператора $\mathcal{A}$.

$\operatorname{tr}_{A|K}(a)$ — след элемента a алгебры A над полем K.

$\mathbf{U}$ — группа комплексных чисел с модулем 1.

$\mathbf{U}_n$ — группа комплексных корней степени n из 1.

$\mathbf{U}_{p^\infty}$ — группа комплексных корней степени p^n из 1 ($n \in \mathbb{N}$) (p — простое число).

U° — ортогональное дополнение к подмножеству U векторного пространства в сопряженном пространстве.

$U^\perp$ — ортогональное дополнение к подмножеству U векторного пространства относительно заданной билинейной функции.

$\mathbf{UT}_n(K)$ — группа унитреугольных матриц порядка n над полем K.

$\mathbf{V}_4$ — группа Клейна.

V^* — векторное пространство, сопряженное (двойственное) к пространству V.

$V(a_1, \ldots, a_k)$ — объем параллелепипеда со сторонами $a_1, \ldots, a_k$.

$x \wedge y$ — произведение элементов x, y в алгебре Грассмана векторного пространства.

$\mathbb{Z}$ — множество (кольцо, аддитивная группа) целых чисел; бесконечная циклическая группа.

$\mathbf{Z}_n$ — циклическая группа порядка n; кольцо вычетов по модулю n.

$\mathbb{Z}_p$ — кольцо целых p-адических чисел.

$\mathbb{Z}[i]$ — кольцо целых гауссовых чисел.

$\sqrt[n]{z}$ — множество комплексных корней степени n из числа $z \in \mathbb{C}$.

$\mu(n)$ — функция Мебиуса.

$\mu(a)$ — минимальный многочлен алгебраического элемента a.

$\Lambda(V)$ — внешняя алгебра (алгебра Грассмана) векторного пространства V.

$\Phi_n(x)$ — многочлен деления круга (круговой многочлен) $\prod_{k=1}^{\varphi(n)}(x - \varepsilon_k)$, где ε_k — первообразный корень степени n из 1 ($k = 1, \ldots \ldots, \varphi(n)$).

$\varphi(n)$ — функция Эйлера.

$\chi_{A|K}(a, x)$ — характеристический многочлен элемента a алгебры A над полем K.

1_X — тождественное отображение множества X.

2^X — множество всех подмножеств множества X.