Нижегородский государственный университет им. Н.И. Лобачевского

Национальный исследовательский университет

Учебно-научный и инновационный комплекс
«Модели, методы и программные средства»

Основная образовательная программа
010300.62 «Фундаментальная информатика и информационные технологии»,
общий профиль, квалификация (степень) бакалавр

Учебно-методический комплекс по дисциплине
«Геометрия и алгебра»

Основная образовательная программа
010400.62 «Прикладная математика и информатика»,
общий профиль, квалификация (степень) бакалавр

Учебно-методический комплекс по дисциплине
«Геометрия и алгебра»

Золотых Н.Ю., Сидоров С.В.

ГРУППЫ, КОЛЬЦА, ПОЛЯ

Электронное учебно-методическое пособие

Мероприятие 1.2. Совершенствование образовательных технологий, укрепление
материально-технической базы учебного процесса

Нижний Новгород
2012

ГРУППЫ, КОЛЬЦА, ПОЛЯ. Н. Ю. Золотых, С. В. Сидоров. Электронное учебно-методическое пособие. — Нижний Новгород: Нижегородский госуниверситет, 2012. — 52 с.

В сборнике содержится 316 задач по теории групп, колец и полей. Задачи снабжены ответами, задачи повышенной трудности — указаниями, а в некоторых случаях — решениями.

Электронное учебно-методическое пособие предназначено для студентов ННГУ, обучающихся по направлениям подготовки 010300.62 «Фундаментальная информатика и информационные технологии» и 010400.62 «Прикладная математика и информатика», изучающих курс «Геометрия и алгебра».

Предлагается 316 задач по теме «Группы, кольца, поля». Многие задачи снабжены ответами. Для сложных задач, как правило, даются указания или решения. Многие задачи естественным образом объединяются в группы; ключ к решению может находиться в предыдущих задачах.

При составлении задачника были использованы различные источники (см. список литературы). Многие задачи предложены составителями.

1 Числовые кольца и поля

1. Какие из следующих множеств образуют кольцо, а какие поле:
1) множество $\{0\}$;
2) множество $\mathbb{N}$ натуральных чисел;
3) множество целых неотрицательных чисел;
4) множество целых неположительных чисел;
5) множество $\mathbb{Z}$ целых чисел;
6) множество $2\mathbb{Z}$ четных чисел;
7) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n \neq 0$;
8) множество $\mathbb{Q}$ рациональных чисел;
9) множество иррациональных чисел;
10) множество $\mathbb{R}$ вещественных чисел;
11) множество $\mathbb{C}$ комплексных чисел;
12) множество $\mathbb{Z}[i]$ *целых гауссовы чисел*, т. е. комплексных чисел с целыми действительной и мнимой частями;
13) множество комплексных чисел с рациональными действительной и мнимой частями?

2. Какие из колец предыдущей задачи не содержат 1?

3. Доказать, что любое числовое поле содержит $\mathbb{Q}$.

4. Доказать, что кольца $\mathbb{Z}$ и $n\mathbb{Z}$ при $n \geq 2$ не изоморфны.

5. Доказать, что
1) поля $\mathbb{Q}$ и $\mathbb{R}$ не изоморфны;
2) поля $\mathbb{R}$ и $\mathbb{C}$ не изоморфны.

6. Доказать, что
1) при любом изоморфизме числовых полей подполе $\mathbb{Q}$ отображается тождественно, следовательно, поле $\mathbb{Q}$ обладает только тождественным автоморфизмом;
2) поле $\mathbb{R}$ обладает только тождественным автоморфизмом.

7. Найти все автоморфизмы поля $\mathbb{C}$, переводящие действительные числа снова в действительные.

8. Какие из следующих множеств образуют кольцо, а какие поле:
1) множество чисел вида $a + b\sqrt{2}$, где a, b — целые;
2) множество чисел $a + b\sqrt{2}$, где a, b — рациональные;
3) множество чисел $a + b\sqrt[3]{2}$, где a, b — целые;
4) множество чисел $a + b\sqrt[3]{2}$, где a, b — рациональные;
5) множество чисел $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c — целые;
6) множество чисел $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c — рациональные?

9. Изоморфны ли поля $\left\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\right\}$ и $\left\{a + b\sqrt{3} : \ a, b \in \mathbb{Q}\right\}$?

10. Найти элемент, обратный к заданному:
1) $2 + 3\sqrt{3}$ в поле $\left\{a + b\sqrt{3} : \ a, b \in \mathbb{Q}\right\}$;
2) $1 - \sqrt{5}$ в поле $\left\{a + b\sqrt{5} : \ a, b \in \mathbb{Q}\right\}$;

3) $3+\sqrt[3]{2}-3\sqrt[3]{4}$ в поле $\left\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:\ a,b,c\in\mathbb{Q}\right\}$;
4) $1-2\sqrt[3]{3}+\sqrt[3]{9}$ в поле $\left\{a+b\sqrt[3]{3}+c\sqrt[3]{9}:\ a,b,c\in\mathbb{Q}\right\}$.

11. Пусть α — корень неприводимого над полем $\mathbb{Q}$ многочлена $f(x)\in\mathbb{Q}[x]$ степени $n\geq 2$. Доказать, что числа вида $a_0+a_1\alpha+a_2\alpha^2+\ldots+a_{n-1}\alpha^{n-1}$ с рациональными $a_0,a_1,\ldots,a_{n-1}$ образуют поле, причем каждый элемент этого поля однозначно записывается в таком виде. Говорят, что это поле, обозначаемое $\mathbb{Q}(\alpha)$, получено *присоединением* числа α к полю рациональных чисел.

12. В поле, полученном присоединением к $\mathbb{Q}$ корня многочлена $\alpha^4-\alpha^3+2\alpha+1$, найти число, обратное $3\alpha^3+\alpha^2-2\alpha-1$.

13. Описать поле $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Найти в этом поле элемент, обратный к указанным элементам:
1) $\sqrt{2}+\sqrt{3}$; 2) $1+\sqrt{2}+\sqrt{3}$; 3) $2+\sqrt{2}-2\sqrt{3}$.

2 Группы

2.1 Определения и примеры полугрупп и групп

14. Какие из следующих множеств чисел относительно сложения образуют полугруппу, а какие группу:
1) множество $\mathbb{N}$ натуральных чисел;
2) множество целых неотрицательных чисел;
3) множество целых неположительных чисел;
4) множество $\mathbb{Z}$ целых чисел;
5) множество $2\mathbb{Z}$ четных чисел;
6) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n\neq 0$;
7) множество $\mathbb{Q}$ рациональных чисел;
8) множество иррациональных чисел;
9) множество $\mathbb{R}$ вещественных чисел;
10) множество $\mathbb{C}$ комплексных чисел?

15. Какие из следующих множеств чисел относительно умножения образуют полугруппу, а какие группу:
1) множество $\mathbb{N}$ натуральных чисел;
2) множество целых неотрицательных чисел;
3) множество целых неположительных чисел;
4) множество $\mathbb{Z}$ целых чисел;
5) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n\neq 0$;
6) множество $\mathbb{Q}$ рациональных чисел;
7) множество $\mathbb{Q}^*$ ненулевых рациональных чисел;
8) множество $\mathbb{Q}_+$ положительных рациональных чисел;
9) множество иррациональных чисел;
10) множество $\mathbb{R}$ вещественных чисел;
11) множество $\mathbb{R}^*$ ненулевых вещественных чисел;
12) множество $\mathbb{R}_+$ положительных вещественных чисел;
13) множество $\mathbb{C}$ комплексных чисел;
14) множество $\mathbb{C}^*$ ненулевых комплексных чисел;
15) множество U_n всех значений корня n-й степени из 1;
16) множество U всех комплексных чисел, по модулю равных 1;

17) множество H_n чисел вида

$$\rho\left(\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}\right),$$

где $\rho>0$, $k=0,1,\ldots,n-1$?

16. Доказать, что мультипликативная группа всех значений корня n-й степени из 1 является единственной конечной группой с числовыми элементами порядка n, за исключением случая $n=1$.

17. Образуют ли полугруппу/группу

1) вещественные числа относительно вычитания;
2) вещественные числа относительно операции $-a-b$;
3) ненулевые вещественные числа относительно деления;
4) натуральные числа относительно операции НОД $\{a,b\}$?

18. Образует ли полугруппу/группу множество положительных вещественных чисел относительно указанной операции:

1) $a\circ b=a^b$;
2) $a\circ b=a^2b^2$?

19. Пусть X — некоторое непустое множество. Образует ли множество 2^X полугруппу/группу относительно указанной операции? Указать нейтральный элемент, если он существует:

1) объединение множеств;
2) пересечение множеств;
3) симметрическая разность множеств?

20. Какие из следующих множеств с указанными операциями образуют полугруппу, а какие группу:

1) множество векторов плоскости относительно сложения;
2) множество векторов пространства относительно сложения;
3) множество векторов пространства относительно скалярного произведения;
4) множество векторов пространства относительно векторного произведения?

21. Пусть K — кольцо, а F — поле. Какие из следующих множеств являются полугруппами, а какие группами:

1) множество $K[x]$ многочленов с коэффициентами из K относительно сложения;
2) $K[x]$ относительно умножения;
3) $K[x]$ относительно суперпозиции: $fg=f(g(x))$;
4) $F[x]$ относительно умножения?

22. Доказать, что

1) множество всех отображений множества $\{1,2,\ldots,n\}$ в себя относительно операции композиции (произведения) образует полугруппу, но (при $n>1$) не группу;
2) множество всех подстановок (биективных отображений) множества $\{1,2,\ldots,n\}$ на себя образует группу относительно произведения. Эта группа называется *симметрической группой степени* n и обозначается S_n. Найти ее порядок;
3) множество всех четных подстановок образует подгруппу в S_n. Эта подгруппа называется *знакопеременной группой степени* n и обозначается A_n. Найти ее порядок;
4) множество нечетных подстановок подгруппы не образуют.

23. Пусть X — некоторое непустое множество (возможно, бесконечное). Доказать, что

1) множество всех отображений $X\to X$ относительно операции произведения образует полугруппу, но (при $|Z|\neq 1$) не группу;

2) множество всех биективных отображений $X \to X$ относительно операции произведения образует группу.

24. Доказать *теорему Кэли*:

1) любая конечная группа изоморфна некоторой подгруппе симметрической группы;
2) любая бесконечная группа изоморфна некоторой подгруппе группы биекций некоторого множества на себя.

25. Доказать, что множество $K^{m\times n}$ всех матриц размера $m \times n$ с элементами из кольца K относительно операции сложения образуют абелеву группу.

26. Пусть V — линейное пространство над полем F. Доказать, что относительно сложения множество V — абелева группа.

27. Пусть F — некоторое поле. Доказать, что

1) множество $F^{n\times n}$ всех матриц порядка n относительно умножения образуют полугруппу, но не группу;
2) множество всех невырожденных матриц порядка n относительно умножения образуют группу. Эта группа называется *полной линейной группой* и обозначается $\mathrm{GL}(F, n)$;
3) множество всех матриц порядка n с определителем, равным 1, относительно умножения образуют группу. Эта группа называется *специальной линейной группой* и обозначается $\mathrm{SL}(F, n)$.

28. Доказать, что

1) множество всех ортогональных вещественных матриц порядка n относительно операции умножения образуют группу. Эта группа называется *полной ортогональной группой* и обозначается $\mathrm{GO}(n)$;
2) множество всех ортогональных матриц порядка n с определителем, равным 1, относительно операции умножения образуют группу. Эта группа называется *специальной ортогональной группой* и обозначается $\mathrm{SO}(n)$;
3) $\mathrm{GO}(n)$ является подгруппой группы вещественных матриц порядка n с определителем ± 1;
4) множество всех унитарных комплексных матриц порядка n относительно умножения образуют группу. Эта группа называется *полной унитарной группой* и обозначается $\mathrm{GU}(n)$;
5) множество всех унитарных матриц порядка n с определителем, равным 1, относительно умножения образуют группу. Эта группа называется *специальной унитарной группой* и обозначается $\mathrm{SU}(n)$;
6) $\mathrm{GU}(n)$ является подгруппой группы комплексных матриц порядка n с определителем, по модулю равным 1.

29. Доказать, что

1) множество квадратных матриц порядка n, в каждой строке и каждом столбце которых не более одной единицы, а остальные нули, относительно умножения образуют полугруппу, но не группу. Каков ее порядок?
2) множество квадратных матриц порядка n, в каждой строке и каждом столбце которых ровно одна единица, а остальные нули, относительно умножения образуют группу. Каков ее порядок? Доказать, что эта группа изоморфна S_n;
3) множество квадратных матриц порядка n, в каждой строке и каждом столбце которых ровно один ненулевой элемент, равный ± 1, относительно умножения образуют группу. Каков ее порядок?

30. Доказать, что

1) множество $\mathbb{Z}^{n\times n}$ квадратных целочисленных матриц порядка n относительно умножения образует полугруппу, но не группу;
2) множество квадратных целочисленных унимодулярных (т. е. с определителем ± 1) матриц порядка n относительно умножения образуют группу;
3) множество квадратных целочисленных матриц порядка n с определителем 1 относительно умножения образуют группу.

31. Пусть V — линейное пространство над полем F размерности n. Доказать, что
1) множество всех преобразований пространства V относительно умножения образует полугруппу, но не группу;
2) при этом множество всех невырожденных преобразований образует группу, изоморфную $\mathrm{GL}(F, n)$.

32. Доказать, что
1) множество всех ортогональных преобразований вещественного пространства размерности n образует группу, изоморфную $\mathrm{GO}(n)$;
2) множество всех унитарных преобразований комплексного пространства размерности n образует группу, изоморфную $\mathrm{GU}(n)$.

33. Пусть V — евклидово или унитарное пространство. Какие из следующих множеств преобразований пространства V образуют полугруппу, а какие группу:
1) множество всех самосопряженных преобразований относительно сложения;
2) множество всех самосопряженных преобразований относительно умножения?

34. Доказать, что каждое из следующих множеств преобразований плоскости или пространства образует группу относительно операции произведения отображений:
1) движения плоскости/пространства включая отражения;
2) движения плоскости/пространства без отражений;
3) движения плоскости/пространства включая отражения, переводящие заданную фигуру в себя;
4) движения плоскости/пространства без отражений, переводящие заданную фигуру в себя. Если фигура ограниченная, то достаточно рассматривать только вращения вокруг некоторой точки, поэтому эта группа называется также *группой вращения* (заданной фигуры).

35. Группа движений плоскости без отражений, переводящих правильный n-угольник в себя, называется *группой вращения* (заданного n-угольника). Группа движений плоскости (включая отражения), переводящих правильный n-угольник в себя, называется *группой диэдра*.
1) Найти порядок группы вращений n-угольника.
2) Найти порядок группы диэдра.
3) Проверить, что при $n = 3$ группа диэдра изоморфна S_3.
4) Доказать, что при $n = 4$ группа диэдра изоморфна группе подстановок ε, $(1\,3)$, $(2\,4)$, $(1\,2)(3\,4)$, $(1\,4)(2\,3)$, $(1\,3)(3\,4)$, $(1\,2\,3\,4)$, $(1\,4\,3\,2)$.

36. Доказать, что
1) группа вращений правильной n-угольной пирамиды (при $n = 3$ пирамида не должна быть правильным тетраэдром) изоморфна группе вращений правильного n-угольника;
2) группа вращений правильной n-бипирамиды (при $n = 3$ пирамида не должна быть правильным октаэдром) изоморфна группе диэдра. Другое название бипирамиды — диэдр, отсюда название группы.

37. Доказать, что группа движений прямоугольника, т. е. движений плоскости (включая отражения), переводящих прямоугольник, не являющийся квадратом, в себя, изоморфна

1) *четверной группе Клейна*

$$V_4 = \{\varepsilon, (1\,2)(3\,4), (1\,4)(2\,3), (1\,3)(3\,4)\};$$

2) мультипликативной группе матриц, состоящей из

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

38. Найти порядок группы вращений каждого из пяти правильных многогранников. Доказать, что
1) группа вращений тетраэдра изоморфна A_4;
2) группы вращений куба и октаэдра изоморфны S_4;
3) группы вращений икосаэдра и додекаэдра изоморфны A_5.

39. Пусть $G = \langle V, E\rangle$ — простой без петель и кратных ребер граф. Здесь V — конечное множество *вершин*, а E — множество *ребер*, т. е. неупорядоченных пар (i, j), где $i \neq j$, $i \in V$, $j \in V$. *Автоморфизмом* графа G называется такое отображение $\varphi : V \to V$, при котором $(\varphi i, \varphi j) \in E$ тогда и только тогда, когда $(i, j) \in E$. Доказать, что множество $\operatorname{Aut} G$ автоморфизмов графа G является группой, если в качестве произведения автоморфизмов рассматривается их последовательное выполнение.

40. Пусть G — группа. Доказать, что множество $\operatorname{Aut} G$ автоморфизмов группы G также является группой, если в качестве произведения автоморфизмов рассматривается их последовательное выполнение.

41. Доказать, что
1) множество всех аффинных преобразований линейного пространства относительно умножения образует группу;
2) множество всех изометрий (движений, включая отражения) вещественного пространства относительно операции умножения образует группу.

42. На множестве $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, где $n > 1$, введены операция *сложения по модулю* n: $a \oplus_n b$ есть остаток от деления $a + b$ на n, и операция *умножения по модулю* n: $a \otimes_n b$ есть остаток от деления ab на n. Записать таблицы модулярного сложения и модулярного умножения в $\mathbb{Z}_n$ $(n = 2, 3, \ldots, 6)$. Доказать, что
1) $\mathbb{Z}_n$ с операцией сложения по модулю n образует циклическую группу;
2) $\mathbb{Z}_n$ с операцией умножения по модулю n образует полугруппу, но (при $n \geq 2$) не группу;
3) $\{1, 2, \ldots, n-1\}$ с операцией умножения по модулю n образует группу тогда и только тогда, когда n простое.
4) Обозначим $\mathbb{Z}_n^*$ множество ненулевых элементов множества $\mathbb{Z}_n$, взаимно простых с n. Число таких элементов равно $\varphi(n)$ — *функции Эйлера*. В частности, $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$, если p — простое. Доказать, что $\mathbb{Z}_n^*$ с операцией умножения по модулю n — группа.

43. Доказать, что 4-элементное множество матриц

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

относительно операции матричного умножения образует группу, изоморфную группе U_4 корней 4-й степени из 1.

44. Доказать, что 8-элементное множество матриц

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

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

относительно операции матричного умножения образует неабелеву группу (*группу кватернионных единиц* Q_8). Найти все подгруппы группы Q_8.

45. Доказать, что множество дробно-рациональных функций вида

$$f(x) = \frac{ax + b}{cx + d},$$

где a, b, c, d — вещественные и $ad - bc \neq 0$, является группой относительно операции суперпозиции.

46. Доказать, что множество функций

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = 1 - x, \quad f_4(x) = \frac{x}{x - 1},$$

$$f_5(x) = \frac{x - 1}{x}, \quad f_6(x) = \frac{1}{1 - x}$$

относительно операции суперпозиции образует группу, изоморфную S_3.

47. Пусть M — множество точек кривой $y = x^3$. Определим на M операцию сложения. Пусть $P, Q \in X$. Проведем через P и Q прямую (если P и Q совпадают, то проведем касательную к M в точке P). Пусть R — третья точка пересечения этой прямой с M. Обозначим через S точку, симметричную R, относительно начала координат. Точку S назовем суммой точек P и Q. Доказать, что M относительно введенной операции сложения образует абелеву группу.

48. Пусть E — множество точек *эллиптической* кривой $y^2 = x^3 + ax + b$, где $4a^3 + 27b^2 \neq 0$, дополненное «бесконечно удаленной» точкой N:

$$E = \left\{(x, y) \in \mathbb{R}^2 : \; y^2 = x^3 + ax + b\right\} \cup \{N\}.$$

Определим на E операцию сложения. Положим

$$N + (x, y) = (x, y) + N = (x, y), \qquad (x, y) + (x, -y) = N.$$

Пусть теперь $P = (x_1, y_1)$, $Q = (x_2, y_2)$, где $x_1 \neq x_2$. Для определения суммы $P+Q$ проведем через эти точки прямую. Пусть $R = (x_3, y_3)$ — третья точка пересечения этой прямой с E. Положим $P + Q = (x_3, -y_3)$. Для определения $P + P$ проведем через P касательную; далее аналогично. Доказать, что E относительно введенной операции сложения образует абелеву группу. Данная конструкция работает над произвольным полем характеристики, отличной от 2 и 3.

49. Доказать, что если квадрат любого элемента группы равен единице, то группа абелева.

50. Найти все с точностью до изоморфизма группы 1) третьего 2) четвертого 3) шестого порядков. Выписать их таблицы умножения. Для каждой группы найти в S_n изоморфную подгруппу.

51. На множестве $G = \{e, a, b, c, d\}$ введена операция умножения согласно таблице

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

Является ли G группой?

52. Доказать, что изоморфны аддитивная группа $\mathbb{Z}$ всех целых чисел и аддитивная группа $n\mathbb{Z}$ всех целых, кратных заданному $n \neq 0$.

53. Доказать, что

1) мультипликативная группа положительных вещественных чисел изоморфна аддитивной группе всех вещественных чисел;
2) мультипликативная группа положительных рациональных чисел не изоморфна аддитивной группе всех рациональных чисел.

54. Найти все автоморфизмы аддитивной группы рациональных чисел.

55. Доказать, что в группе G

1) единица единственна;
2) для любого a из G обратный элемент a^{-1} единственен.

56. Доказать, что

1) если G — группа, то для любых a, b из G каждое из уравнений $ax = b$ и $xa = b$ имеет в G единственное решение;
2) если для любых a, b из полугруппы G каждое из уравнений $ax = b$ и $xa = b$ имеет в G по крайней мере одно решение, то G — группа;
3) если G — конечная полугруппа и для любых a, b из G каждое из уравнений $ax = b$ и $xa = b$ имеет в G не более одного решения, то G — группа.

57. Пусть G — группа, а H — непустое подмножество в G. Доказать, что

1) H — подгруппа тогда и только тогда, когда $ab \in H$ и $a^{-1} \in H$ для любых a, b из H;
2) H — подгруппа тогда и только тогда, когда $ab^{-1} \in H$ для любых a, b из H;
3) если H конечно, то для того, чтобы H была подгруппой необходимо и достаточно, чтобы $ab \in H$ для любых a, b из H.

58. Доказать, что любая бесконечная группа содержит бесконечное число подгрупп.

59. Доказать, что конечная полугруппа содержит *идемпотент*, т. е. такой элемент a, что $a^2 = a$.

60. Доказать, что множество обратимых элементов кольца K, содержащего единицу, образует группу (обозначается K^*).

61. Найти группу обратимых элементов следующих колец:

1) F — поле;
2) $F^{n\times n}$, где F — поле;
3) $K[x]$, где K — коммутативное кольцо с единицей.

62. Вычислить порядок группы $\mathrm{GL}(\mathbb{Z}_p, n)$, где p — простое число.

63. Вычислить порядок группы $\mathrm{GL}(\mathbb{Z}_m, n)$, где $m \geq 2$.

64. Приведите пример неабелевой группы нечетного порядка. Какое минимальное число элементов содержит такая группа?

65. Определим произведение двух подмножеств A и B группы G следующим образом: $AB = \{ab : \ a \in A, \ b \in B\}$. Верно ли, что произведение двух подгрупп является подгруппой?

66. Доказать, что произведение HK двух подгрупп H и K группы G является подгруппой тогда и только тогда, когда $HK = KH$.

67. Докажите, что если объединение двух подгрупп H и K группы G является подгруппой, то либо H подгруппа в K, либо K подгруппа в H.

68. Пусть H и K — две подгруппы в группе G. Доказать, что

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

69. Аддитивная группа целых чисел $\mathbb{Z}$ изоморфна любой своей собственной подгруппе. Существуют ли другие группы с таким свойством?

2.2 Порядок элемента в группе. Циклические группы

70. Пусть a, b, c — некоторые элементы группы G. Доказать, что

1) элементы ab и ba имеют одинаковый порядок;
2) элементы aba^{-1} и b имеют одинаковый порядок;
3) элементы abc, bca, cab имеют одинаковый порядок.
4) Привести пример, показывающий, что элементы abc, acb могут иметь разный порядок.

71. Доказать, что порядок любой подстановки в S_n равен наименьшему общему кратному длин независимых циклов, входящих в ее разложение.

72. Найти порядок элемента группы:

1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ в S_5;

2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 5 & 3 & 7 & 8 & 9 & 10 & 6 \end{pmatrix}$ в S_{10};

3) $-\frac{\sqrt{3}}{2} - \frac{1}{2}i$ в $\mathbb{C}^*$; 4) $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ в $\mathbb{C}^*$;

5) $\begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$ в $\mathrm{GL}(\mathbb{C}, 2)$; 6) $\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}$ в $\mathrm{GL}(\mathbb{C}, 2)$;

7) $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ в $\mathrm{GL}(\mathbb{R}, 3)$.

73. Доказать, что элемент $z = \dfrac{2+i}{2-i}$ в $\mathbb{C}^*$ имеет бесконечный порядок.

74. Найти все элементы порядка 6 в группе

1) C^*; 2) S_5; 3) A_5.

75. Доказать, что во всякой группе четного порядка есть элемент порядка 2.

76. Пусть a — элемент группы G, причем $|a| = n$. Доказать, что для того, чтобы $a^m = e$ необходимо и достаточно, чтобы $m \vdots n$.

77. Доказать, что циклическая группа является абелевой. Вывести отсюда, что группа S_n при $n \geq 3$ не абелева.

78. Доказать, что

1) любая конечная циклическая группа изоморфна мультипликативной группе U_n всех значений корня n-й степени из 1;

2) любая бесконечная циклическая группа изоморфна аддитивной группе целых чисел $\mathbb{Z}$.

79. Найти все образующие аддитивной группы целых чисел.

80. Доказать, что любая подгруппа циклической группы (конечной или бесконечной) циклическая.

81. Построить все подгруппы аддитивной группы целых чисел.

82. Пусть $G = (a)$ — конечная циклическая группа порядка n. Доказать, что

$$|a^k| = \frac{n}{\text{НОД}\,\{n, k\}}$$

(в частности, элемент a^k тогда и только тогда является образующим группы G, когда n и k взаимно просты). Вывести отсюда, что для любого делителя m числа n существует единственная подгруппа порядка m и других подгрупп в циклической группе нет.

83. Найти все подгруппы циклической группы $G = (a)$ порядка n, где

1) $n = 6$; 2) $n = 24$.

84. Пусть $G = (a)$ — конечная циклическая группа порядка n. Доказать, что

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

2) если n четно, то все элементы в G являются квадратами.

85. Порождающие элементы мультипликативной группы всех значений корня n-й степени из 1 называются *первообразными* или *примитивными* корнями n-й степени. Докажите, что следующее определение эквивалентно: корень n-й степени из 1 называется первообразным, если он не является корнем m-й степени из 1 ни для какого $m < n$.

86. Выпишите все первообразные корни из 1 степени n для значений $n = 1, 2, 3, 4, 5, 6, 12$.

87. При каких n группа $\mathbb{Z}_n$ с операцией сложения по модулю n (см. № 42) является циклической? Указать все порождающие элементы.

88. Известно, что группа $\mathbb{Z}_p^*$ с операцией умножения по модулю p, где p — простое, является циклической (см. № 311). Найти все порождающие элементы этой группы для $p = 2, 3, 5, 7, 11$.

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

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

2) Верно ли утверждение 1) для неабелевой группы?

3) Найти периодическую часть группы $\mathbb{C}^*$.

90. Описать элементы конечного порядка в группах:

1) $\text{GL}(\mathbb{Z}, 2)$; 2) $\text{GL}(\mathbb{R}, 2)$; 3) $\text{GL}(\mathbb{C}, 2)$.

91. Пусть a и b некоторые элементы группы G, порядки которых взаимно просты, причем $ab = ba$. Доказать, что порядок элемента ab равен произведению порядков a и b.

92. Пусть a и b некоторые элементы группы G, причем $ab = ba$. Доказать, что

1) $\text{НОК}\,\{|a|, |b|\}$ делится на $|ab|$. Привести пример коммутирующих элементов a и b, для которых $\text{НОК}\,\{|a|, |b|\} \neq |ab|$.

2) в G существует элемент c такой, что $|c| = \text{НОК}\,\{|a|, |b|\}$.

93. Пусть G — конечная группа и $m = \max\limits_{g \in G} |g|$. Доказать, что m делится на порядок любого элемента из G.

94. Доказать, что множество G всех пар (a, b), где $a \in \mathbb{R}\backslash\{0\}$, $b \in \mathbb{R}$ является группой относительно операции

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2,\ a_1 b_2 + b_1).$$

Найти в G две подгруппы, одна из которых изоморфна аддитивной группе действительных чисел, а другая — мультипликативной группе ненулевых действительных чисел. Указать в G все инволюции. Содержит ли G элементы конечного порядка, большего двух?

95. Пусть G конечная группа и $G_k = \{x \in G :\ x^k = e\}$, $k \in \mathbb{N}$. Доказать, что G циклическая тогда и только тогда, когда $|G_k| \leq k$ для всех $k \in \mathbb{N}$.

96. Доказать, что абелева группа порядка pq, где p и q — различные простые числа, является циклической.

2.3 Симметрическая группа

97. Найти все подгруппы

1) четверной группы Клейна V_4;
2) группы S_3;
3) группы A_4.

98. Доказать, что симметрическая группа S_n является циклической только в случае $n = 1, 2$.

99. Доказать:

1) симметрическая группа S_n при $n \geq 2$ порождается множеством всех транспозиций $(i\,j)$;
2) симметрическая группа S_n при $n \geq 2$ порождается множеством транспозиций $(1\,2), (1\,3), \ldots, (1\,n$
3) симметрическая группа S_n при $n \geq 3$ порождается множеством из двух циклов: $(1\,2)$, $(1\,2\,\ldots\,n)$;
4) знакопеременная группа A_n при $n \geq 3$ порождается множеством всех тройных циклов $(i\,j\,k)$;
5) знакопеременная группа A_n при $n \geq 3$ порождается множеством тройных циклов $(1\,2\,3), (1\,2\,4), .$

100. Найти порядок элемента

$$(1\,2)(3\,4\,5)(6\,7\,8\,9)(10\,11\,12\,13\,14)(15\,16\,17\,18\,19\,20)$$

группы S_{20}.

101. Чему равен наибольший порядок элемента в группе S_{12}?

2.4 Смежные классы, нормальные делители, фактор-группы

102. Какие из отображений $\varphi :\ \mathbb{R}^* \to \mathbb{C}^*$ являются гомоморфизмами:

1) $\varphi a = |a|$; 2) $\varphi a = 2|a|$; 3) $\varphi a = |a|^2$;
4) $\varphi a = \dfrac{1}{|a|}$; 5) $\varphi a = 1 + |a|$; 6) $\varphi a = 1$; 7) $\varphi a = 2$?

103. Какие из отображений являются гомоморфизмами групп:

1) отображение φ из аддитивной группы $\mathbb{R}$ вещественных чисел в мультипликативную группу $\mathbb{R}^*$ ненулевых вещественных чисел, если $\varphi x = e^x$;
2) отображение φ из аддитивной группы $\mathbb{R}^{n\times n}$ квадратных матриц в аддитивную группу $\mathbb{R}$ вещественных чисел, если $\varphi A = a_{11}$;
3) $\varphi :\ \mathrm{GL}(\mathbb{R}, n) \to \mathbb{R}^*$, где $\varphi A = \det A$.

104. Указать ядро и образ гомоморфизмов из №№ 102, 103.

105. Описать левые и правые смежные классы при разложении группы G по подгруппе H:
1) $G = (a)$ — циклическая группа 6-го порядка, H — ее подгруппа 3-го порядка;
2) $G = (a)$ — циклическая группа 6-го порядка, H — ее подгруппа 2-го порядка;
3) $G = S_3$, $H = \{e, (1\,2\,3), (1\,3\,2)\}$;
4) (р) $G = S_3$, $H = \{e, (1\,2)\}$;
5) G — группа вращений тетраэдра, H — подгруппа вращений, оставляющих на месте заданную вершину.
6) (р) $G = \mathrm{GL}(\mathbb{R}, n)$ — мультипликативная группа невырожденных вещественных матриц порядка n, $H = \mathrm{SL}(\mathbb{R}, n)$ — подгруппа матриц с определителем, равным 1.

106. Найти все нормальные делители группы:
1) V_4; 2) S_3; 3) A_4; 4) S_4.

107. Пусть H — нормальный делитель группы G, а G — подгруппа группы G'. Будет ли H — нормальным делителем группы G'?

108. Доказать, что пересечение нормальных делителей группы G является нормальным делителем этой группы.

109. Доказать, что ядро гомоморфизма группы G в группу G' является нормальным делителем в G.

110. Доказать, что подгруппа индекса 2 является нормальным делителем.

111. Элемент $aba^{-1}b^{-1}$ называется *коммутатором* элементов a и b. *Коммутантом* группы G называется подгруппа, порожденная всеми коммутаторами этой группы. Доказать, что
1) коммутатор группы является ее нормальным делителем;
2) фактор-группа по коммутанту абелева.

112. *Центром* $C(G)$ группы G называется множество ее элементов, каждый из которых коммутирует со всеми элементами группы G, т. е.

$$C(G) = \{x \in G : \forall y \in G\ xy = yx\}.$$

Доказать, что
1) центр является подгруппой группы G;
2) центр является нормальным делителем группы G.

113. Пусть H — некоторая подгруппа группы G. Пусть φ_b — преобразование множества левых смежных классов по подгруппе H, заданное формулой $\varphi_b(aH) = (ba)H$, где a, b — элементы группы G. Доказать, что
1) множество $G' = \{\varphi_b : b \in G\}$ всех таких преобразований образует группу относительно операции суперпозиции;
2) отображение $\psi : G \to G'$, заданное формулой $\psi b = \varphi_b$, является гомоморфизмом;
3) ядро гомоморфизма ψ содержится в H.

114. Пусть G — группа, а H — ее подгруппа индекса k. Доказать, что H содержит нормальный делитель группы G индекса, делящего $k!$.

115. Доказать, что подгруппа, индекс которой есть наименьший простой делитель порядка группы, является нормальным делителем.

116. Из теоремы Лагранжа вывести, что
1) порядок подгруппы конечной группы является делителем порядка группы;
2) порядок любого элемента конечной группы является делителем порядка группы;
3) группа простого порядка — циклическая.

117. Пусть G — группа порядка n. Доказать, что для любого элемента $g \in G$ имеет место соотношение $g^n = e$, где e — единица группы.

118. *«Малая» теорема Ферма*. Доказать, что для любого целого a и любого простого p справедливо сравнение $a^p \equiv a \pmod p$.

119. *Теорема Эйлера*. Доказать, что для любого целого a и любого натурального n справедливо сравнение $a^{\varphi(n)} \equiv 1 \pmod p$, где $\varphi(n)$ — функция Эйлера.

120. *Теорема Вильсона*. Доказать, что для того, чтобы натуральное p было простым, необходимо и достаточно, чтобы $(p-1)! \equiv -1 \pmod p$.

121. *Криптографическая система с открытым ключом RSA*. Пусть p, q — различные простые числа,

$$N = pq, \qquad n = |\mathbb{Z}_N^*| = \varphi(N) = (p-1)(q-1).$$

Предположим, что также заданы целые a и b, такие, что

$$ab \equiv 1 \pmod n, \quad \text{НОД}(a,n) = 1, \quad \text{НОД}(b,n) = 1.$$

Определим функции

$$f(x) = x^a \bmod N, \qquad g(y) = y^b \bmod N.$$

Боб публикует числа N и a, а числа p, q, b держит в тайне. Алиса желает передать Бобу сообщение $x \in \mathbb{Z}_N$. Для этого она зашифровывает его:

$$y = f(x),$$

пользуясь публичной информацией, предоставленной Бобом, и передает y по открытому каналу. Для расшифровки сообщения Боб использует функцию $g(y)$:

$$x = g(y).$$

Владимир перехватил y, но, несмотря на знание N и a, ему весьма сложно определить x (задача нахождения разложения $N = pq$ чрезвычайно трудна). Доказать, что

1) $f(x)$ задает биекцию из $\mathbb{Z}_N^*$ в $\mathbb{Z}_N^*$, причем $g(y)$ — обратное отображение;
2) $f(x)$ задает биекцию из $\mathbb{Z}_N$ в $\mathbb{Z}_N$, причем $g(y)$ — обратное отображение.

122. Пусть группа G имеет нечетный порядок. Доказать, что любой элемент этой группы является квадратом.

123. Привести пример, показывающий, что группа G порядка n для некоторого k, делящего n, может не иметь подгруппы порядка k.

124. Доказать, что $S_n/A_n \cong U_2$.

125. Пусть V — n-мерное линейное пространство, W — его некоторое k-мерное подпространство. Доказать, что $V/W \cong U$, где U — $(n-k)$-мерное пространство.

126. Пусть n — натуральное число. Построить фактор-группу $\mathbb{Z}/n\mathbb{Z}$ аддитивной группы целых чисел $\mathbb{Z}$. Доказать, что отображение φ, заданное формулой $\varphi a = a + n\mathbb{Z}$, есть изоморфизм $\varphi : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$, где $\mathbb{Z}_n$ — группа, определенная в № 42, с операцией сложения по модулю n. Изоморфизм φ позволяет нам в дальнейшем не различать эти две изоморфные группы. Фактор-группа $\mathbb{Z}/n\mathbb{Z}$ называется *аддитивной группой вычетов по модулю* n.

127. Пусть n, m — натуральные числа, причем m кратно n. Построить фактор-группу $n\mathbb{Z}/m\mathbb{Z}$ и доказать, что $n\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{m/n}$.

128. Построить соответствующие фактор-группы и доказать изоморфизм (обозначения см. в №№ 14, 15)

1) $\mathbb{R}/\mathbb{Z} \cong U$; 2) $\mathbb{C}^*/\mathbb{R}_+ \cong U$; 3) $\mathbb{C}^*/U \cong \mathbb{R}_+$;
4) $U/U_n \cong U$; 5) $\mathbb{C}^*/U_n \cong \mathbb{C}^*$; 6) $H_n/\mathbb{C}^* \cong U$;

7) $H_n/\mathbb{R}_+ \cong U_n$; 8) $H_n/U_n \cong \mathbb{R}_+$.

129. Доказать, что H — нормальный делитель в G. Построить фактор-группу G/H и доказать изоморфизм $G/H \cong G'$:

1) $G = \mathrm{GL}(\mathbb{R}, n)$, $H = \mathrm{SL}(\mathbb{R}, n)$, $G' = \mathbb{R}^*$;
2) $G = \mathrm{GL}(\mathbb{R}, n)$, $H = \{A \in \mathrm{GL}(\mathbb{R}, n) : \ |\det A| = 1\}$, $G' = \mathbb{R}_+$;
3) $G = \mathrm{GL}(\mathbb{R}, n)$, $H = \{A \in \mathrm{GL}(\mathbb{R}, n) : \ \det A > 0\}$, $G' = U_2$;
4) $G = \mathrm{GL}(\mathbb{C}, n)$, $H = \{A \in \mathrm{GL}(\mathbb{C}, n) : \ |\det A| = 1\}$, $G' = \mathbb{R}_+$;
5) $G = \mathrm{GL}(\mathbb{C}, n)$, $H = \{A \in \mathrm{GL}(\mathbb{C}, n) : \ \det A > 0\}$, $G' = U$.

130. Доказать, что в фактор-группе $\mathbb{Q}/\mathbb{Z}$

1) каждый элемент имеет конечный порядок;
2) для каждого натурального n существует единственная подгруппа порядка n.

131. Пусть G, G' — группы, а φ — гомоморфизм из G на G'. Доказать, что

1) порядок G делится на порядок G';
2) порядок элемента a группы G делится на порядок φa.

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

133. Пусть $G = (a)$ — циклическая группа порядка n, а $G' = (b)$ — циклическая группа порядка m. Найти все гомоморфизмы:

1) группы G в себя;
2) группы G на себя;
3) группы G в группу G';
4) группы G на группу G'.

134. Найти порядок группы автоморфизмов группы

1) $\mathbb{Z}$; 2) $\mathbb{Z}_n$.

135. Найти группу автоморфизмов группы

1) $\mathbb{Z}_p$, где p — простое; 2) $\mathbb{Z}_6$; 3) $\mathbb{Z}_8$;
4) $\mathbb{Z}_9$; 5) S_3; 6) V_4; 7) D_4 (группа диэдра);
8) Q_8 (группа кватернионных единиц; см. № 44).

136. Найти порядок группы $\mathrm{Aut}(\mathrm{Aut}(\mathrm{Aut}\,\mathbb{Z}_9))$.

137. Пусть a и b — два элемента циклической группы G, не являющиеся квадратами. Доказать, что квадратом будет тогда ab.

138. Доказать, что если H — нормальный делитель, а K — подгруппа в G, то $HK = KH$ — подгруппа в G.

139. Пусть H и K — нормальные делители в группе G, причем $H \cap K = \{e\}$. Доказать, что $hk = kh$ для всех $h \in H$, $k \in K$.

140. В симметрической группе S_5 выяснить, какие из следующих множеств являются смежными классами и по каким подгруппам:

1) $K_1 = \{(2\,3\,4),\ (1\,2\,3\,4)\}$;
2) $K_2 = \{(1\,2),\ (1\,2\,3),\ (1\,2\,3\,4)\}$;
3) $K_3 = \{\varepsilon,\ (1\,2\,3\,4),\ (1\,3)\,(2\,4),\ (1\,4\,3\,2)\}$;
4) $K_4 = \{(1\,2),\ (1\,3),\ (1\,4),\ (1\,5)\}$;
5) $K_5 = \{(1\,2),\ (1\,5\,2)\,(3\,4)\}$.

141. Доказать, что любая подгруппа центра группы является нормальным делителем.

142. Доказать, что фактор-группа неабелевой группы G по ее центру $Z(G)$ не может быть циклической.

143. Доказать, что если фактор-группа $G/Z(G)$ циклическая, то $G = Z(G)$.

144. Пусть $G = (a)$ — циклическая группа порядка n, а G' — бесконечная циклическая группа. Найти все гомоморфизмы:
1) группы G в G';
2) группы G' в G;

145. Описать левые смежные классы группы $\mathrm{GL}(\mathbb{Q}, 2)$ по подгруппе невырожденных верхнетреугольных матриц.

146. Приведите пример неабелевой группы, все подгруппы которой являются нормальными делителями.

147. Пусть H — нормальный делитель в группе G. Доказать, что фактор-группа G/H абелева тогда и только тогда, когда H содержит коммутант группы.

148. Пусть p — простое число, $p > 2$. Доказать, что отображение $\varphi : \mathrm{GL}(\mathbb{Z}, n) \to \mathrm{GL}(\mathbb{Z}_p, n)$, определенное по правилу $\varphi(A) = B = (b_{ij})$, где b_{ij} — остаток от деления a_{ij} на p, является гомоморфизмом группы $\mathrm{GL}(\mathbb{Z}, n)$ на $\mathrm{GL}(\mathbb{Z}_p, n)$. Доказать, что любая конечная подгруппа группы $\mathrm{GL}(\mathbb{Z}, n)$ отображается при этом изоморфно на некоторую подгруппу группы $\mathrm{GL}(\mathbb{Z}_p, n)$, и, следовательно, порядок любой конечной подгруппы в $\mathrm{GL}(\mathbb{Z}, n)$ не превосходит $|\mathrm{GL}(\mathbb{Z}_p, n)|$.

2.5 Коммутанты, централизаторы, нормализаторы

149. Найти коммутант симметрической группы S_n.

150. Найти коммутант группы $\mathrm{GL}(\mathbb{R}, 2)$.

151. *Централизатором* элемента g из группы G называется множество $C(g) = \{x \in G \mid gx = xg\}$. Доказать, что $C(g)$ является подгруппой в G. Является ли $C(g)$ нормальным делителем в G?

152. Найти централизаторы матриц:

1) $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ в группе $\mathrm{GL}(\mathbb{C}, 2)$.

2) $C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ в группе $\mathrm{GL}(\mathbb{C}, 3)$.

153. *Нормализатором* подгруппы H группы G называется множество $N(H) = \{x \in G \mid xH = Hx\}$. Доказать, что $N(H)$ является подгруппой в G. Является ли $N(H)$ нормальным делителем в G?

2.6 Автоморфизмы групп

154. Доказать, что циклическая группа третьего порядка не может быть группой автоморфизмов никакой группы.

155. Пусть g — некоторый элемент группы G. Доказать, что отображение $\varphi_g(x) = gxg^{-1}$, $x \in G$, является автоморфизмом группы G. Такой автоморфизм называется *внутренним* . Доказать, что множество внутренних автоморфизмов $\mathrm{Inn}\, G$ является нормальным делителем в группе всех автоморфизмов $\mathrm{Aut}\, G$ и фактор-группа $G/Z(G)$ изоморфна $\mathrm{Inn}\, G$.

156. Доказать, что симметрическая группа S_n при $n \geq 3$ изоморфна группе ее внутренних автоморфизмов.

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

158. Доказать, что группа автоморфизмов конечной циклической группы, порядок которой больше 2, является абелевой группой четного порядка.

159. Найти группу автоморфизмов аддитивной группы целых гауссовых чисел $\mathbb{Z}[i]$. Доказать, что она изоморфна группе целочисленных унимодулярных матриц второго порядка.

2.7 Действие группы на множестве

Пусть G — группа, X — множество. Отображение $G \times X \to X$, сопоставляющее каждой упорядоченной паре $(g, x) \in G \times X$ элемент $g * x \in X$, называется *левым действием* группы G на множестве X, если оно удовлетворяет следующим аксиомам:

1) $e * x = x$ для всех $x \in X$;

2) $g_1 * (g_2 * x) = (g_1 g_2)x$ для всех $x \in X, g_1, g_2 \in G$.

При этом элементы множества X часто называют *точками*. Множество

$$Gx = \{g * x \mid g \in G\}$$

называется *орбитой* точки x, а число элементов орбиты — ее *длиной*. *Стабилизатором* точки $x \in X$ называется множество

$$\mathrm{St}_G(x) = \{g \in G \mid g * x = x\}\,.$$

160. Доказать, что орбиты любых двух точек либо совпадают, либо не пересекаются.

161. Доказать следующие утверждения:

1) $\mathrm{St}_G(x)$ является подгруппой в G;

2) длина орбиты Gx равна индексу $\mathrm{St}_G(x)$ в группе G для любого $x \in X$.

3) $|X| = \sum\limits_{i=1}^{r} \dfrac{|G|}{\mathrm{St}_G(x_i)} = \sum\limits_{i=1}^{r} I(G/\mathrm{St}_G(x_i))$, где x_i — представители различных орбит ($i = 1, 2, \ldots, r$).

162. Доказать, что правило $g * a = gag^{-1}$ задает левое действие группы G на множестве элементов группы G. Это действие называется *сопряжением*, а элементы a и gag^{-1} называются *сопряженными* в группе G. Орбиты элементов при этом называются *классами сопряженных элементов*, а стабилизатор элемента $a \in G$ называется *централизатором* и обозначается $C_G(a)$.

163. Доказать, что правило $g * x = gx$ задает действие группы $\mathrm{GL}(\mathbb{R}, n)$ на множестве $\mathbb{R}^n$, где gx означает обычное умножение матрицы $g \in \mathrm{GL}(\mathbb{R}, n)$ на столбец $x \in \mathbb{R}^n$. Описать орбиты всех элементов из $\mathbb{R}^n$.

164. Опишите орбиты и стабилизаторы следующих действий:

1) действие G на себе левыми сдвигами: $(g, x) \mapsto gx$;

2) действие G на себе правыми сдвигами: $(g, x) \mapsto xg^{-1}$;

3) действие подгруппы H группы G на группе G левыми (соответственно правыми) сдвигами.

165. Говорят, что подгруппа A *сопряжена* подгруппе B в G посредством элемента $g \in G$, если $A = gBg^{-1} = \{gbg^{-1} : b \in B\}$. Доказать:

1) отношение сопряженности на множестве всех подгрупп группы G является отношением эквивалентности;

2) стабилизаторы элементов из одной орбиты являются сопряженными подгруппами.

166. *Лемма Бернсайда.* Множество $\mathrm{Fix}(g) = \{x \in X \mid g * x = x\}$ называется *множеством неподвижных точек* элемента g из группы G. Доказать, что число различных орбит, получающихся при действии конечной группы G на множестве X, равно

$$r_G(X) = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|.$$

167. *Формула классов.* Доказать, что

$$|G| = |Z(G)| + \sum_{i=q+1}^{r} I(G/C_G(g_i)),$$

где G — конечная группа, $q = |Z(G)|$, r — число различных орбит относительно действия сопряжения.

168. *Теорема Коши.* Доказать, что если порядок конечной группы G делится на простое число p, то G содержит элемент порядка p.

169. Доказать, что если порядок группы G есть степень простого числа, то центр этой группы неединичен.

170. Доказать, что группа порядка p^2, где p — простое число, абелева и изоморфна либо $\mathbb{Z}_{p^2}$, либо $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

171. Доказать, что если группа G неабелева и $|G| = p^3$, где p — простое число, то $|Z(G)| = p$.

172. Доказать, что подгруппа, индекс которой есть наименьший простой делитель порядка группы, является нормальным делителем. Задача повторяет № 115. Здесь привести доказательство, использующее действие групп.

173. *Первая теорема Силова.* Пусть G — конечная группа, $|G| = p^n m$, где p — простое число, НОД $\{p, m\} = 1$. *Силовской p-подгруппой* группы G называется любая ее подгруппа порядка p^n. Доказать, что силовская p-подгруппа существует.

174. *Вторая теорема Силова.* Доказать, что всякая p-подгруппа группы G содержится в некоторой силовской p-подгруппе и все силовские p-подгруппы сопряжены.

175. *Третья теорема Силова.* Доказать, что число силовских p-подгрупп группы G

1) делит индекс любой силовской p-подгруппы S;
2) сравнимо с 1 по модулю p;
3) равно индексу $N(S)$ в G.

176. Доказать, что если силовская p-подгруппа единственна, то она является нормальным делителем.

177. Пусть G — группа порядка pq, где p, q — простые числа, $p < q$ и $q - 1$ не делится на p. Доказать, что группа G циклическая.

178. Доказать, что любая группа порядка 45 абелева.

3 Кольца и поля

3.1 Определения и примеры колец и полей

См. также задачи из раздела 1. Если не оговорено противное, под кольцом понимается ассоциативное (но не обязательно коммутативное) кольцо.

179. Какие из следующих множеств являются ассоциативными/неассоциативными коммутативными/некоммутативными кольцами:

1) множество векторов геометрического пространства относительно операции сложения и векторного умножения;
2) множество $K[x]$ многочленов над кольцом K, если в качестве операций выбраны обычное сложение и умножение многочленов;
3) множество $K[x]$ многочленов над кольцом K, если в качестве операции сложения выбрано обычное сложение многочленов, а в качестве операции умножения — суперпозиция;
4) множество K^n столбцов высоты n с элементами из кольца K, если в качестве операций выбраны покомпонентные сложение и умножение;
5) множество $K^{n\times n}$ квадратных матриц порядка n с элементами из кольца K относительно обычных операций сложения и умножения матриц;
6) множество $K^{n\times n}$, если в качестве операции сложения выбрано обычное сложение матриц, а в качестве операции умножения — *коммутатор* $[A, B] = AB - BA$;
7) множество $K^{n\times n}$, если в качестве операции сложения выбрано обычное сложение матриц, а в качестве операции умножения — *произведение Йордана* $A*B = \frac{1}{2}(AB+BA)$.

180. Рассмотрим четырехмерную (некоммутативную) линейную алгебру над полем вещественных чисел, в которой умножение задано таблицей

	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	$-j$
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

,

где e, i, j, k — базисные векторы. Элементы данной алгебры называются *кватернионами*. Пусть a, b, c, d — вещественные числа. Кватернион $ae + 0i + 0j + 0k$ отождествляется с вещественным числом a. Кватернион $ae + bi + 0j + 0k$ отождествляется с комплексным числом $a + bi$. Доказать, что алгебра кватернионов есть некоммутативное тело. В частности, указать элемент, обратный к $a + bi + cj + dk$.

181. Рассмотрим двумерную коммутативную линейную алгебру $\mathbb{R}[d]$ над полем вещественных чисел, в которой $e \cdot e = e$, $e \cdot d = d$, $d \cdot d = 0$, где e, d — базисные векторы. Элементы алгебры $\mathbb{R}[d]$ называются *дуальными числами*. Пусть x, y — вещественные. Дуальное число $xe+0d$ отождествляется с вещественным числом x. Число $0e+yd$ называется *актуальным бесконечно малым первого порядка*. Вместо $xe + yd$ будем писать $x + dy$. Конструкция дуальных чисел предложена П.Ферма в 1638 г. и использовалась им для отыскания наибольших и наименьших значений.

1) Является ли алгебра дуальных чисел $\mathbb{R}[d]$ полем?
2) Найти все делители нуля в $\mathbb{R}[d]$.
3) Вещественную функцию $f(x)$ назовем *дифференцируемой*, если существует ее продолжение на алгебру $\mathbb{R}[d]$, такое, что отношение

$$f'(x) = \frac{f(x + dy) - f(x)}{dy}$$

существует и не зависит от y. Данное отношение называется *производной* функции $f(x)$ в точке x. Доказать, что функция x^n, где n — натуральное, дифференцируема, и найти ее производную.

182. Рассмотрим двумерную коммутативную линейную алгебру $\mathbb{R}[j]$ над полем вещественных чисел, в которой $e \cdot e = e$, $e \cdot j = j$, $j \cdot j = e$, где e, j — базисные векторы. Элементы алгебры $\mathbb{R}[j]$ называются *двойными числами*. Пусть x, y — вещественные. Двойное число $xe + 0j$ отождествляется с вещественным числом x.

1) Является ли алгебра двойных чисел $\mathbb{R}[j]$ полем?
2) Найти все делители нуля в $\mathbb{R}[j]$.
3) Проверить, что в базисе

$$\alpha = \frac{1+j}{2}, \quad \beta = \frac{1-j}{2},$$

сложение и умножение производится покоординатно, следовательно, алгебра двойных чисел есть прямое произведение двух полей вещественных чисел.

183. Доказать, что

1) множество матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, где a, b — рациональные, образует линейную алгебру над полем $\mathbb{Q}$, изоморфную полю чисел вида $a + b\sqrt{2}$;
2) множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a, b — вещественные, образует линейную алгебру над полем $\mathbb{R}$, изоморфную полю комплексных чисел;
3) множество матриц вида

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

где a, b, c, d — вещественные, образует линейную алгебру над полем $\mathbb{R}$, изоморфную телу кватернионов;
4) множество матриц вида $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, где a, b — вещественные, образуют алгебру, изоморфную алгебре дуальных чисел;
5) множество матриц вида $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, где a, b — вещественные, образуют алгебру, изоморфную алгебре двойных чисел;
6) множество матриц вида $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$, где a, b, c, d — вещественные, образуют кольцо, изоморфное телу кватернионов. Является ли множество таких матриц линейной алгеброй над полем $\mathbb{C}$?

184. *Булева алгебра*. На множестве $B = \{0, 1\}$ определим бинарные операции: *дизъюнкцию* $\vee$, *конъюнкцию* (или *умножение по модулю* 2) $\&$, *сложение по модулю* 2 $\oplus$ по следующим правилам:

$$0 \vee 0 = 0, \qquad 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1,$$
$$0 \,\&\, 0 = 0 \,\&\, 1 = 1 \,\&\, 0 = 0, \qquad 1 \,\&\, 1 = 1,$$
$$0 \oplus 0 = 1 \oplus 1 = 0, \qquad 0 \oplus 1 = 1 \oplus 0 = 1.$$

Является ли кольцом/полем

1) алгебраическая система $\langle B, \vee, \& \rangle$;

2) алгебраическая система $\langle B, \oplus, \& \rangle$?

185. Проверить, что

1) $\mathbb{Z}_n$ является кольцом относительно сложения и умножения по модулю n (см. № 42); это кольцо называется *кольцом вычетов* по модулю n;

2) $\mathbb{Z}_n$ образует поле (*поле вычетов*) тогда и только тогда, когда n простое.

186. Пусть F — поле и m не является квадратом никакого элемента из F. Рассмотрим множество пар (a, b), где a, b — произвольные элементы из F. Определим операции над элементами этого множества следующим образом: $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \cdot (c, d) = (ac + mbd, ad + bc)$.

1) Доказать, что множество пар с такими операциями образует поле. Это поле называется *квадратичным расширением поля* F.

2) Доказать, что множество пар вида $(a, 0)$ образует подполе этого поля, изоморфное полю F. Естественно не различать элементы $(a, 0)$ и a, и поэтому пару (a, b) можно записывать как $a + bj$, где $j^2 = m$.

187. Доказать, что все квадратичные расширения поля $\mathbb{R}$ изоморфны полю $\mathbb{C}$.

188. Доказать, что поле $\mathbb{Q}$ обладает бесконечным множеством попарно неизоморфных квадратичных расширений.

189. Существует ли квадратичное расширение поля $\mathbb{Z}_2$?

190. Доказать, что в поле $\mathbb{Z}_p$, $p \geq 3$, найдется элемент не являющийся квадратом.

191. Сколько элементов содержит квадратичное расширение поля $\mathbb{Z}_p$ при $p \geq 3$?

192. Пусть X — непустое множество. Является ли кольцом/полем множество 2^X, если

1) сложение — это объединение, а умножение — пересечение множеств;

2) сложение — это симметрическая разность множеств, а умножение — пересечение множеств?

193. Алгебраическая система $\langle X, +, \cdot \rangle$ с двумя бинарными операциями $+$ и $\cdot$ (сложением и умножением соответственно) называется *полукольцом*, если $\langle X, + \rangle$ — коммутативная полугруппа, $\langle X, \cdot \rangle$ — полугруппа и выполнен закон дистрибутивности: для любых a, b, c из X справедливо $(a + b) \cdot c = a \cdot c + b \cdot c$ и $a \cdot (b + c) = a \cdot b + a \cdot c$. Доказать, что полукольцом является:

1) любое кольцо;

2) алгебраическая система $\langle B, \vee, \& \rangle$ из № 184(1);

3) алгебраическая система $\langle 2^X, \cup, \cap \rangle$ из № 192(1).

194. Пусть X — некоторое непустое подмножество множества действительных чисел. В качестве операций сложения и умножения на множестве X рассмотрим операции $\downarrow$ и $\uparrow$ соответственно, определяемые следующим образом: $a \downarrow b = \min\{a, b\}$, $a \uparrow b = \max\{a, b\}$. Доказать, что операции коммутативны, ассоциативны и удовлетворяют двум свойствам дистрибутивности: $(a \downarrow b) \uparrow c = (a \uparrow c) \downarrow (b \uparrow c)$, $(a \uparrow b) \downarrow c = (a \downarrow c) \uparrow (b \downarrow c)$. Является ли X относительно этих операций полукольцом/кольцом?

195. На множестве $X = \mathbb{R} \cup \{\infty\}$ «сложением» назовем операцию $\downarrow$ из № 194, а «умножением» — обычное сложение (предполагается, что ∞ больше любого вещественного числа и $\infty + x = x + \infty = \infty$). Доказать, что данная алгебраическая система является полукольцом, но не кольцом. Она называется *тропическим полукольцом*.

196. Доказать, что если в кольце нашлись левая и правая единицы, то они совпадают и других единиц нет.

197. Привести пример кольца матриц специального вида, обладающих несколькими левыми или несколькими правыми единицами.

198. Доказать, что в кольце с единицей коммутативность сложения вытекает из остальных аксиом.

199. Пусть $\langle K, +, \cdot\rangle$ — кольцо с единицей 1. На множестве элементов кольца K введем новые операции сложения $\oplus$ и умножения $\circ$ следующим образом: $x \oplus y = x+y-1$, $x \circ y = x+y-xy$. Доказать, что $\langle K, \oplus, \circ\rangle$ является кольцом, изоморфным исходному.

200. В кольце $\mathbb{C}^{2\times 2}$ укажите бесконечное подмножество, состоящее только из вырожденных матриц и являющееся группой относительно матричного умножения. Существует ли в $\mathbb{C}^{2\times 2}$ подмножество, являющееся группой относительно матричного умножения и содержащее как вырожденные, так и невырожденные матрицы?

201. *Центром* $C(K)$ кольца K называется множество его элементов, коммутирующих с любым элементом из K:

$$C(K) = \{x \in K : \ \forall y \in K \ xy = yx\}.$$

Доказать, что $C(K)$ является подкольцом в K.

202. Найти центр тела кватернионов $\mathbf{H}$. Проверить, что $\mathbb{C}$ не содержится в центре тела кватернионов.

203. Рассмотрим кольцо $\mathbb{Z}[\sqrt{D}] = \left\{a + b\sqrt{D} : \ a, b \in \mathbb{Z}\right\}$, где D — целое число, не являющееся квадратом целого числа.

1) Определим отображение, называемое *нормой*, $N : \ \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$ по правилу:

$$N(a + b\sqrt{D}) = a^2 - Db^2.$$

Доказать, что $N(xy) = N(x)N(y)$ для всех $x, y \in \mathbb{Z}[\sqrt{D}]$.

2) Доказать, что элемент $u \in \mathbb{Z}[\sqrt{D}]$ обратим в $\mathbb{Z}[\sqrt{D}]$ тогда и только тогда, когда $N(u) = \pm 1$.

3) Найти группу обратимых элементов кольца $\mathbb{Z}[\sqrt{2}]$.

204. Пусть K — коммутативное кольцо, а S — подмножество в K, не содержащее нуля, делителей нуля и замкнутое относительно умножения. На множестве пар (a, b), где $a \in K$, $b \in S$ введем отношение $\sim$. А именно, $(a, b) \sim (c, d)$, если $ad = bc$. Ясно, что это отношение эквивалентности. Доказать, что множество классов эквивалентности образует коммутативное кольцо с единицей относительно операций: $(a, b)+(c, d) = (ad+bc,\ bd)$, $(a, b)\cdot(c, d) = (ac,\ bd)$ и содержит подкольцо, изоморфное K. Данное кольцо обозначается $S^{-1}K$ и называется *кольцом частных* кольца K по S. Доказать, что каждый элемент из S является обратимым в $S^{-1}K$. Если $S = K\backslash\{0\}$, то $S^{-1}K$ является полем (*поле частных* кольца K).

205. Доказать, что поле частных кольца $\mathbb{Z}$ изоморфно полю $\mathbb{Q}$.

206. Описать поле частных над $\mathbb{R}[x]$ (поле *дробно-рациональных функций* над $\mathbb{R}$).

207. Пусть $K = \mathbb{Z}_n$ и S — множество обратимых элементов в K. Построить кольцо частных K по S.

208. Существует ли поле, строго содержащее поле комплексных чисел?

209. *Дифференцированием* кольца K называется отображение $D : K \to K$, удовлетворяющее условиям

$$D(x + y) = D(x) + D(y), \quad D(xy) = D(x)y + xD(y), \quad x, y \in K.$$

Найти все дифференцирования колец:

1) $\mathbb{Z}$; 2) $\mathbb{Z}[x]$; 3) $\mathbb{Z}[x_1, x_2, \ldots, x_n]$.

210. Доказать, что если элемент кольца имеет хотя бы два правых обратных, то он имеет бесконечно много правых обратных.

211. Доказать, что если у элемента x есть единственный правый обратный, то x обратим.

212. Приведите пример кольца, в котором из равенства $xy = 1$ для некоторых элементов x и y не следует равенство $yx = 1$.

213. Доказать, что делитель нуля является необратимым элементом кольца.

214. Доказать, что элемент в конечном кольце необратим тогда и только тогда, когда он является делителем нуля или нулем.

215. Пусть K — конечное кольцо. Доказать, что:

1) если K не содержит делителей нуля, то оно содержит единицу и все его ненулевые элементы обратимы;
2) если K имеет единицу, то каждый его элемент, имеющий односторонний обратный, обратим;
3) если K имеет единицу, то всякий левый делитель нуля является правым делителем нуля.

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

217. Пусть K — кольцо с единицей, $x, y \in K$. Доказать, что:

1) если произведения xy и yx обратимы, то элементы x и y также обратимы;
2) если K без делителей нуля и произведение xy обратимо, то x и y обратимы;
3) без дополнительных предположений о кольце K из обратимости произведения xy не следует обратимость элементов x и y;
4) если обратим элемент $1 + yx$, то обратим также элемент $1 + xy$.

218. Пусть K — коммутативное кольцо с единицей. Доказать, что множество $\mathrm{GL}(K, n)$ обратимых элементов кольца матриц $K^{n\times n}$ совпадает с множеством матриц, определители которых обратимы в K.

219. В кольце $\mathbf{H}^{2\times 2}$ найти матрицу X, у которой $\det X \neq 0$, но X необратима. Таким образом, в случае некоммутативного кольца K утверждение № 218 неверно.

220. Элемент x кольца K называется *нильпотентным*, если $x^m = 0$ для некоторого $m \in \mathbb{N}$. Пусть x – нильпотентный элемент коммутативного кольца K. Доказать, что:

1) x является либо нулем, либо делителем нуля;
2) ax нильпотентный для любого $a \in K$;
3) $1 + x$ обратим в K;
4) $u + x$ обратим для любого обратимого элемента u.

221. Доказать, что множество нильпотентных элементов коммутативного кольца образует идеал.

222. Пусть K – коммутативное кольцо и $f(x) = f_0x^n + f_1x^{n-1} + \ldots + f_n \in K[x]$. Доказать, что:

1) $f(x)$ обратим в кольце $K[x]$ тогда и только тогда, когда f_0 обратим в K, а коэффициенты $f_1, \ldots, f_n$ являются нильпотентными в K;
2) $f(x)$ нильпотентен в кольце $K[x]$ тогда и только тогда, когда коэффициенты $f_0, f_1, \ldots, f_n$ являются нильпотентными в K.

223. Пусть K — коммутативное кольцо с единицей и $K[[x]]$ — множество всех формальных степенных рядов $a(x) = \sum\limits_{n=0}^{\infty} a_nx^n$, $a_n \in K$. Введем обычные операции сложения и умножения рядов: $\sum\limits_{n=0}^{\infty} a_nx^n + \sum\limits_{n=0}^{\infty} b_nx^n = \sum\limits_{n=0}^{\infty}(a_n + b_n)x^n$, $\left(\sum\limits_{n=0}^{\infty} a_nx^n\right) \cdot \left(\sum\limits_{n=0}^{\infty} b_nx^n\right) = \sum\limits_{n=0}^{\infty} c_nx^n$, где $c_n = \sum\limits_{i+j=n} a_ib_j$. Доказать, что

1) $K[[x]]$ — коммутативное кольцо с единицей;

2) $K[[x]]$ содержит подкольцо, изоморфное K;
3) если K не имеет делителей нуля, то это верно и для $K[[x]]$;
4) ряд $a(x) = \sum\limits_{n=0}^{\infty} a_n x^n$ обратим тогда и только тогда, когда a_0 обратим в K.

3.2 Линейная алгебра и алгебра многочленов над $\mathbb{Z}_p$

224. Решить систему линейных уравнений:

$$\begin{cases} x + 2y + 2z = 1; \\ 2x + y + 2z = 2; \\ 2x + 2y + z = 2. \end{cases}$$

1) в поле $\mathbb{Z}_3$,2) в поле $\mathbb{Z}_5$.

225. Решить систему линейных уравнений:

$$\begin{cases} 3x + 2y = 1; \\ 3x + 2y + z = 2; \\ x + 3y + 4z = 3. \end{cases}$$

1) в поле $\mathbb{Z}_5$,2) в поле $\mathbb{Z}_7$.

226. Найти НОД многочленов $x^5 + x^3 + x^2 + 2x + 1$, $x^5 + 2x^4 + x^3 + 1$
1) над полем $\mathbb{Z}_3$;
2) над полем $\mathbb{Q}$.

227. Найти НОД многочленов $x^5 + 4x^4 + 3x^3 + x^2 + 4$ и $x^4 + 4x^3 + 4x^2 + 4$
1) над полем $\mathbb{Z}_3$ (все коэффициенты нужно заменить на наименьшие вычеты по модулю 3);
2) над полем $\mathbb{Z}_5$;
3) над полем $\mathbb{Q}$.

228. Найти НОД многочленов $x^5 - x^4 - 2x^3 + 2x^2 + 9x - 9$ и $x^5 + x^4 + 4x^3 - x^2 + x - 6$
1) над полем $\mathbb{Z}_3$;
2) над полем $\mathbb{Z}_5$;
3) над полем $\mathbb{Z}_7$;
4) над полем $\mathbb{Q}$.

229. Сколько существует многочленов степени m с коэффициентами из кольца $\mathbb{Z}_n$?

230. Разложить на неприводимые множители над полем $\mathbb{Z}_2$ все многочлены1) 2-й степени;2) 3-й степени.

231. Найти все неприводимые многочлены со старшим коэффициентом 1 над полем $\mathbb{Z}_3$ 1) 2-й степени;2) 3-й степени.

232. Разложить на неприводимые множители:
1) $x^5 + x^3 + x^2 + 1$ над полем $\mathbb{Z}_2$;
2) $x^5 + 2x^4 + x^2 + 2x + 2$ над полем $\mathbb{Z}_3$;
3) $x^5 + 2x^4 + 4x^2 + 3x + 3$ над полем $\mathbb{Z}_5$.

233. Разложить на неприводимые множители $x^5 + x^4 - 2x^3 - 2x^2 + 9x + 9$
1) над $\mathbb{Z}_3$;2) над $\mathbb{Z}_5$;3) над $\mathbb{Z}_7$;4) над $\mathbb{Q}$.

234. Разложение многочлена $x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ на неприводимые над полем $\mathbb{Z}_2$ имеет вид

$$(x^6 + x^5 + x^4 + x + 1)(x^2 + x + 1),$$

а над полем $\mathbb{Z}_{13}$ —

$$(x^4 + 2x^3 + 3x^2 + 4x + 6)(x^3 + 8x^2 + 4x + 12)(x + 3).$$

Найти его разложение над полем $\mathbb{Q}$ (Д. Кнут).

235. Здесь устанавливается связь между взаимной простотой многочленов над полем вычетов и полем $\mathbb{Q}$.

1) Доказать, что если многочлены $f(x)$ и $g(x)$ с целыми коэффициентами взаимно просты над полем $\mathbb{Z}_p$ для некоторого простого p, причем хотя бы один из старших коэффициентов не делится на p, то $f(x)$ и $g(x)$ взаимно просты над полем $\mathbb{Q}$.
2) Привести пример, показывающий, что обратное неверно ни для какого простого p.

236. Здесь устанавливается связь между неприводимостью многочлена над полем вычетов и полем $\mathbb{Q}$.

1) Доказать, что если многочлен $f(x)$ с целыми коэффициентами приводим над полем рациональных чисел, то он приводим над полем $\mathbb{Z}_p$ для любого простого p, не делящего старший коэффициент.
2) Привести пример многочлена, приводимого над $\mathbb{Q}$, но неприводимого над $\mathbb{Z}_p$, где p делит старший коэффициент.
3) Существуют многочлены с целыми коэффициентами, неприводимые над $\mathbb{Q}$, но приводимые над $\mathbb{Z}_p$ при любом простом p. Доказать, что таковым является, например, многочлен $x^4 + 1$.

237. В $\mathbb{Z}_7[x]$ найти многочлен $f(x)$ 4-й степени, такой, что $f(0) = 1$, $f(1) = 4$, $f(2) = 6$, $f(3) = 0$, $f(4) = 3$.

238. В поле $\mathbb{Z}_{11}$ найти все решения уравнения:

1) $x^2 = 5$;
2) $x^2 = 6$;
3) $x^2 + 4x + 1 = 0$;
4) $x^2 + 2x + 1 = 0$;
5) $x^2 + 2x + 4 = 0$;
6) $x^7 = 7$;
7) $x^{10} = 1$;
8) $x^3 = a$.

239. В поле $\mathbb{Z}_p$ найти все решения уравнения:

1) $x^p = x$; 2) $x^p = a$.

3.3 Идеалы и фактор-кольца

240. Какие из следующих множеств являются подгруппами аддитивной группы, подкольцами или идеалами указанных ниже колец:

1) $\mathbb{N}$ в кольце $\mathbb{Z}$;
2) $n\mathbb{Z}$ в кольце $\mathbb{Z}$, где n — целое;
3) $\mathbb{Z}[i]$ в поле $\mathbb{C}$;
4) $\mathbb{Z}$ в кольце $\mathbb{Z}[i]$;
5) множество чисел вида $a + ai$, где $a \in \mathbb{Z}$, в кольце $\mathbb{Z}[i]$;

6) $(1+i)\mathbb{Z}$ в кольце $\mathbb{Z}[i]$;
7) $\mathbb{Z}[x]$ в кольце $\mathbb{R}[x]$;
8) $n\mathbb{Z}[x]$ в кольце $\mathbb{Z}[x]$, где n — целое;
9) $f(x)F[x]$ в кольце $F[x]$, где F — поле, $f(x) \in F[x]$?

241. Доказать, что пересечение идеалов является идеалом.

242. Пусть K — коммутативное кольцо, а M — некоторое непустое подмножество в K. *Идеалом* (M)*, порожденным множеством* M, называется минимальный (по включению) идеал, содержащий M. Если $M = \{a_1, a_2, \ldots, a_m\}$, то идеал (M) обозначается $(a_1, \ldots, a_m)$. Идеал (a), порожденный одним элементом a, называется *главным*. Доказать, что
1) если K содержит 1, то (M) состоит из всех конечных сумм вида $\sum r_i a_i$, где $r_i \in K$, $a_i \in M$; в частности, $(a) = \{ra : r \in K\}$;
2) если K не имеет единицы, то (M) состоит из всех конечных сумм вида $\sum r_i a_i + \sum n_i a_i$, где $r_i \in K$, $a_i \in M$, $n_i \in ZZ$; в частности, $(a) = \{ra + na : r \in K,\ n \in \mathbb{Z}\}$.

243. Доказать, что кольцо матриц $F^{n\times n}$ над полем F является *простым* кольцом, т. е. всякий двусторонний идеал в нем либо нулевой, либо совпадает со всем кольцом.

244. Доказать, что в кольце матриц $K^{n\times n}$ над произвольным кольцом K идеалами являются в точности множества матриц, элементы которых принадлежат фиксированному идеалу кольца K. Таким образом, если K — простое кольцо, то $K^{n\times n}$ также является простым кольцом.

245. Найти все идеалы кольца верхнетреугольных целочисленных матриц второго порядка.

246. Найти все левые идеалы кольца $\mathbb{Z}_2^{2\times 2}$.

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

248. 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?

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

250. Пусть n — натуральное число. Построить фактор-кольцо $\mathbb{Z}/n\mathbb{Z}$. Доказать, что отображение φ, заданное формулой $\varphi a = a + n\mathbb{Z}$, есть изоморфизм $\varphi : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$, где $\mathbb{Z}_n$ — кольцо, определенное в № 185, с операциями сложения и умножения по модулю n. Изоморфизм φ позволяет нам в дальнейшем не различать эти два изоморфных кольца. Фактор-кольцо $\mathbb{Z}/n\mathbb{Z}$ называется *кольцом вычетов по модулю* n (ср. № 126).

251. Построить фактор-кольцо и доказать, что оно изоморфно полю комплексных чисел:
1) $\mathbb{R}[x]/(x^2+1)$;
2) $\mathbb{R}[x]/(x^2+x+1)$;
3) $\mathbb{R}[x]/(x^2+px+q)$, если многочлен x^2+px+q неприводим над $\mathbb{R}$.

252. Построить фактор-кольцо $\mathbb{Q}[x]/(x^2-1)$. Является ли оно полем?

253. Построить фактор-кольцо и указать числовое поле, которому оно изоморфно:
1) $\mathbb{Q}[x]/(x^2-2)$; 2) $\mathbb{Q}[x]/(x^4-10x^2+1)$.

254. Построить фактор-кольцо; определить, является ли оно полем:
1) $\mathbb{Z}[i]/(2)$; 2) $\mathbb{Z}[i]/(3)$.

255. Пусть $f(x)$ — неприводимый многочлен степени n над полем $\mathbb{Z}_p$, где p — простое (известно, что такой многочлен существует для произвольного n и произвольного простого p). Построить фактор-кольцо $\mathbb{Z}_p[x]/(f(x))$. Сколько элементов оно содержит? Является ли оно полем?

256. Пусть m — натуральное число, $f(x) \in \mathbb{Z}[x]$ — многочлен со старшим коэффициентом 1.

Доказать изоморфизм фактор-колец:

$$\mathbb{Z}[x]/(f(x), m) \cong \mathbb{Z}_m[x]/(f(x)).$$

257. Построить фактор-кольцо $\mathbb{Z}[x]/(2x^2)$.

258. Построить фактор-кольца и описать группы их обратимых элементов:
1) $\mathbb{Z}_4[x]/(x^2+1)$; 2) $\mathbb{Z}_6[x]/(x^2+1)$;
3) $\mathbb{Z}_6[x]/(x^2+2)$; 4) $\mathbb{Z}_4[x]/(2x)$.

259. Найти все гомоморфизмы колец:
1) $\mathbb{Z} \to 2\mathbb{Z}$; 2) $2\mathbb{Z} \to 2\mathbb{Z}$; 3) $2\mathbb{Z} \to 3\mathbb{Z}$; 4) $\mathbb{Z} \to \mathbb{Z}_2^{2\times 2}$.

260. Найти число гомоморфизмов из кольца вычетов $\mathbb{Z}_m$ в $\mathbb{Z}_n$.

261. *Китайская теорема об остатках.* Пусть $m_1, m_2, \ldots, m_s$ — попарно взаимно простые положительные целые числа, а $r_1, r_2, \ldots, r_s$ — целые числа, удовлетворяющие неравенствам

$$0 \le r_i \le m_i - 1 \quad (i = 1, 2, \ldots, s).$$

Доказать, что найдется, причем единственное, число x, такое, что r_i есть остаток от деления x на m_i $(i = 1, 2, \ldots, s)$ и $0 \le x \le m - 1$, где $m = m_1 \cdot m_2 \cdot \ldots \cdot m_s$.

3.4 Целостные, евклидовы и факториальные кольца

262. Коммутативное кольцо с единицей и без делителей нуля называется *целостным кольцом*, или *областью целостности*. Какие из следующих колец являются целостными:
1) поле F;
2) кольцо целых чисел $\mathbb{Z}$;
3) кольцо $n\mathbb{Z}$;
4) кольцо многочленов $K[x]$ над любым целостным кольцом K;
5) кольцо многочленов от многих переменных $K[x_1, \ldots, x_n]$, если K — целостное кольцо;
6) кольцо вычетов $\mathbb{Z}_n$;
7) кольцо многочленов над полем F, не содержащих линейных членов?

263. Пусть K — целостное кольцо. Говорят, что элемент a из K *делится* на элемент b из K (обозначение: $a \vdots b$), если существует q из K, такой, что $a = qb$. Элементы a и b называются *ассоциированными* (обозначение: $a \sim b$), если $a \vdots b$, $b \vdots a$. Доказать, что
1) $a \sim b$ тогда и только тогда, когда в K существует обратимый элемент q (делитель единицы), такой, что $a = qb$;
2) $a \sim b$ тогда и только тогда, когда $(a) = (b)K$.

264. Целостное кольцо K, не являющееся полем, называется *евклидовым*, если существует функция $N : K \setminus \{0\} \to \mathbb{Z}_+$, такая, что для любых a, b из K, где $b \ne 0$, выполнено два условия: $N(ab) \ge N(a)$ и существуют (не обязательно единственные) q, r из K, такие, что $a = qb + r$, где $r = 0$ или $N(r) < N(b)$. Второе условие означает возможность «деления с остатком». Доказать, что следующие кольца являются евклидовыми:
1) кольцо целых чисел $\mathbb{Z}$;
2) кольцо многочленов $F[x]$ над полем F;
3) кольцо целых гауссовых чисел $\mathbb{Z}[i]$.

265. Доказать, что в евклидовом кольце, если $N(ab) = N(a)$, то b обратим.

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

диагональной форме Смита:

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

(все неуказанные элементы — нули), где $d_1 \mid d_2$, $d_2 \mid d_3$, $\ldots$, $d_{r-1} \mid d_r$.

267. *Наибольшим общим делителем* НОД $\{a, b\}$ элементов a и b целостного цольца K называется их общий делитель, делящийся на все их общие делители. Наибольший общий делитель, если он существует, определен однозначно с точностью до ассоциированности. Доказать, что в евклидовом кольце для любых элементов a и b существует $d = \text{НОД}\{a, b\}$ и он может быть представлен в виде $d = ua + vb$, где u, v — некоторые элементы из K.

268. Элементы a и b целостного кольца называются *взаимно простыми*, если НОД $\{a, b\} = 1$. Доказать, что в евклидовом кольце для того, чтобы НОД $\{a, b\} = 1$ необходимо и достаточно, чтобы существовали u и v, такие, что $ua + vb = 1$

269. Необратимый ненулевой элемент p целостного кольца называется *простым*, если он не может быть представлен в виде $p = ab$, где a, b — необратимые, иначе говоря, элемент p — простой, если любой его делитель ассоциирован с 1 или p.

270. Пусть a, b, c — элементы евклидова кольца, а p — простой элемент этого кольца. Доказать, что

1) если $ab \vdots p$, то $a \vdots p$ или $b \vdots p$;
2) если $a \vdots b$, $a \vdots c$ и НОД $\{b, c\} = 1$, то $a \vdots bc$;
3) если $ab \vdots c$ и НОД $\{b, c\} = 1$, то $a \vdots c$.

271. Целостное кольцо называется *факториальным*, если любой его необратимый элемент может быть разложен в произведение простых элементов этого кольца, причем это разложение единственно с точностью до перестановки множителей и умножения их на обратимые элементы. Доказать, что евклидово кольцо — факториально.

272. В кольце $\mathbb{Z}[i]$ разложить на простые множители числа 2, 3, 4, 5.

273. В кольце $\mathbb{Z}[\sqrt{-5}] = \left\{a + ib\sqrt{5} : \ a, b \in \mathbb{Z}\right\}$ найти два разных (с точностью до перестановок и умножения на обратимые элементы) разложения 6 на простые множители и тем самым показать, что $\mathbb{Z}[\sqrt{-5}]$ не является факториальным кольцом. Это классический пример, возникший в результате анализа Дирихле доказательства большой теоремы Ферма, предложенного Куммером.

274. Привести примеры, показывающие, что следующие кольца не факториальны:
1) $\mathbb{Z}[\sqrt{-3}]$; 2) $\mathbb{Z}[\sqrt{10}]$.

275. Пусть K — факториальное кольцо и a — некоторый его необратимый элемент. Доказать, что если $a = cp_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, где c — обратимый элемент, а p_i — простой ($i = 1, 2, \ldots, s$), причем p_i и p_j не ассоциированы при $i \neq j$, тогда любой делитель d элемента a имеет вид $c'p_1^{l_1}p_2^{l_2}\ldots p_s^{l_s}$, где $0 \leq l_i \leq k_i$, а c' — обратимый элемент.

276. Целостное кольцо, в котором каждый идеал — главный, называется *кольцом главных идеалов*. Доказать, что евклидово кольцо является кольцом главных идеалов.

277. Является ли $\mathbb{Z}[x]$
1) факториальным кольцом;
2) кольцом главных идеалов;
3) евклидовым кольцом?

278. Доказать, что кольцо многочленов $K[x]$ над областью целостности K является кольцом главных идеалов тогда и только тогда, когда K — поле.

279. Пусть F — поле. Является ли $F[x, y]$
1) факториальным кольцом;
2) кольцом главных идеалов;
3) евклидовым кольцом?

280. Доказать, что в кольце главных идеалов для любых элементов a и b существует $d = \text{НОД}\,\{a, b\}$ и он может быть представлен в виде $d = ua + vb$, где u, v — некоторые элементы из кольца (ср. № 267).

281. Пусть a — ненулевой необратимый элемент кольца главных идеалов K. Доказать, что факторкольцо $K/(a)$ является полем тогда и только тогда, когда a — простой.

3.5 Расширения полей

282. Пусть F — подполе поля L. Поле L называется *расширением* поля F. Доказать, что L является линейным пространством (линейной алгеброй) над F. Размерность этого пространства называется *степенью* L над F и обозначается $[L : F]$ или $\dim_F L$. Расширение называется *конечным*, если это пространство конечномерное.

283. Найти степень расширения:
1) $[\mathbb{R} : \mathbb{Q}]$; 2) $[\mathbb{C} : \mathbb{R}]$.

284. Пусть $f(x)$ — многочлен, неприводимый над полем F. Отождествляя элементы из F с соответствующими смежными классами в фактор-кольце $F[x]/(f(x))$, можно считать, что $F \subseteq F[x]/(f(x))$. Найти степень $[F[x]/(f(x)) : F]$.

285. Доказать, что если K — конечное расширение поля L, а L — конечное расширение поля F, то $[K : F] = [K : L] \cdot [L : F]$.

286. Пусть $f(x)$ — некоторый многочлен положительной степени над полем F. Доказать, что
1) существует расширение поля F, содержащее по крайней мере один корень многочлена $f(x)$.
2) существует расширение поля F, в котором $f(x)$ раскладывается на линейные множители; это расширение называется *полем разложения* многочлена $f(x)$.

287. Пусть L — расширение поля F. Элемент $\alpha \in L$ называется *алгебраическим* над F, если он является корнем некоторого ненулевого многочлена (*аннулирующего*) с коэффициентами из F. В противном случае α называется *трансцендентным* над F. Доказать, что:
1) множество всех многочленов, аннулирующих α, есть идеал;
2) существует единственный многочлен $m_\alpha(x) \in F[x]$ минимальной степени со старшим коэффициентом 1, корнем которого является α; многочлен $m_\alpha(x)$ называется *минимальным многочленом элемента* α;
3) если $f(x) \in F[x]$ и $f(\alpha) = 0$, то $f(x)$ делится на $m_\alpha(x)$;
4) $m_\alpha(x)$ неприводим над полем F.

288. Пусть L — конечное расширение поля F. Доказать, что любой элемент $\alpha \in L$ является алгебраическим над F.

289. Пусть L — расширение поля F. Обозначим $F(\alpha) \subseteq L$ — минимальное расширение поля F, содержащее $\alpha \in L$. Доказать, что

1) если α — алгебраический над F, то $F(\alpha) \cong F[x]/(m_\alpha(x))$ (*простое* расширение поля);
2) если α — трансцендентен над F, то $F(\alpha)$ изоморфно полю частных над $F[x]$ (см. № 204).

290. Пусть L_1 и L_2 — расширения поля F. Доказать, что $F(\alpha_1) \cong F(\alpha_2)$, если $\alpha_1 \in L_1$, $\alpha_2 \in L_2$, $m_{\alpha_1}(x) = m_{\alpha_2}(x)$.

291. Пусть L_1 и L_2 — два минимальных поля разложения для многочлена $f(x) \in F[x]$. Доказать, что $L_1 \cong L_2$.

292. Найти минимальный многочлен над полем $\mathbb{Q}$ для следующих чисел:
1) $\sqrt{2}+\sqrt{5}$; 2) $1+\sqrt[3]{2}+\sqrt[3]{4}$; 3) $\sqrt{3}+\sqrt[3]{2}$.

293. Найти минимальный многочлен над полем $\mathbb{R}$ для $3-2i$.

294. Доказать, что множество всех алгебраических над F элементов поля L образует подполе в L, содержащее F.

295. Доказать, что множество алгебраических над $\mathbb{Q}$ комплексных чисел является алгебраически замкнутым полем.

296. Доказать, что $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p}+\sqrt{q})$, где p и q — натуральные числа.

297. Доказать, что $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

3.6 Характеристика поля и конечные поля

298. Рассмотрим аддитивную подгруппу поля F, порожденную единицей поля. *Характеристикой* поля F называется порядок этой подгруппы, если она конечна, и 0 в противном случае. Доказать, что
1) характеристика поля (если она не 0) есть простое число;
2) характеристика конечного поля есть делитель порядка этого поля;
3) аддитивная группа, порожденная единицей поля F, есть минимальное подполе в F.

299. Найти характеристику поля:
1) $\mathbb{R}$;
2) $\mathbb{Z}_p$, где p — простое;
3) $\mathbb{Z}_p[x]/(f(x))$, где $f(x)$ — многочлен степени n, неприводимый над $\mathbb{Z}_p$.

300. Существует ли бесконечное поле ненулевой характеристики?

301. Доказать, что поле из p^2 элементов содержит единственное собственное подполе.

302. Пусть F — поле характеристики p. Доказать, что
1) для любых a, b из F и любого натурального k выполнено равенство $(a+b)^{p^k} = a^{p^k} + b^{p^k}$;
2) для любых $a_1, a_2, \ldots, a_n$ из F и любого натурального k выполнено равенство

$$(a_1 + a_2 + \ldots + a_n)^{p^k} = a_1^{p^k} + a_2^{p^k} + \ldots + a_n^{p^k};$$

3) отображение $x \mapsto x^p$ является автоморфизмом (*автоморфизм Фробениуса*);
4) множество всех автоморфизмов поля F образует циклическую группу порядка n, порождающим элементом которой является автоморфизм Фробениуса.

303. Из тождества задачи № 302(2) вывести малую теорему Ферма (см. № 118).

304. Пусть F — конечное поле порядка q. Доказать, что для любого $a \in F$ верно равенство $a^q = a$.

305. Доказать, что
1) поле F характеристики $p \neq 0$ содержит подполе, изоморфное $\mathbb{Z}_p$ (далее для простоты это подполе обозначается просто $\mathbb{Z}_p$); это подполе является минимальным подполем в F;

2) поле F нулевой характеристики содержит подполе, изоморфное $\mathbb{Q}$; это подполе является минимальным подполем в F (ср. с № 3).

306. Пусть F — конечное поле характеристики p. Доказать, что $|F| = p^n$ для некоторого натурального n.

307. Пусть $f(x)$ — многочлен над полем F степени n. Доказать, что $f(x)$ имеет не более n корней в F.

308. Пусть $|F| = q$. Доказать, что F есть поле разложения многочлена $f(x) = x^q - x \in \mathbb{Z}_p[x]$.

309. Доказать, что для любого простого p и любого натурального n существует поле порядка $q = p^n$.

310. Доказать, что конечные поля одного порядка изоморфны между собой.

311. Доказать, что любая конечная подгруппа G мультипликативной группы F^* поля F — циклическая. В частности, циклической является группа $\mathbb{Z}_p^*$.

312. Доказать, что если мультипликативная группа поля является циклической, то поле конечно.

313. При каких простых p число 2 является порождающим элементом мультипликативной группы поля вычетов $\mathbb{Z}_p$?

314. Доказать, что для любого простого нечетного p и любого натурального m группа обратимых элементов кольца вычетов $\mathbb{Z}_{p^m}$ циклическая.

315. Пусть $f(x)$ — неприводимый многочлен степени n над полем вычетов $\mathbb{Z}_p$ и A — сопровождающая матрица многочлена $f(x)$. Доказать, что множество матриц вида $\alpha_0 E + \alpha_1 A + \ldots + \alpha_{n-1} A^{n-1}$, где $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{Z}_p$, образует конечное поле из p^n элементов.

316. Доказать, что для любого автоморфизма φ поля F множество элементов, неподвижных относительно φ, является подполем в F.

Ответы, указания, решения

1. 1) Кольцо, но не поле.
2) Не является кольцом.
3) Не является кольцом.
4) Не является кольцом.
5) Кольцо, но не поле.
6) Кольцо, но не поле.
7) Кольцо, но не поле.
8) Поле.
9) Не является кольцом.
10) Поле.
11) Поле.
12) Кольцо, но не поле.
13) Поле.

6. 1) Пусть φ — автоморфизм $\mathbb{Q} \to \mathbb{Q}$. Имеем $\varphi 0 = 0$, $\varphi 1 = 1$, поэтому $\varphi 2 = \varphi(1+1) = \varphi 1 + \varphi 1 = 1 + 1 = 2$, $\varphi 3 = \varphi(2+1) = \varphi 2 + \varphi 1 = 2 + 1 = 3$, ... Следовательно, все целые неотрицательные числа отображаются тождественно. Далее, если a — целое неотрицательное, то $\varphi(-a) = -\varphi a$. Следовательно, все целые числа отображаются тождественно. Если p, q — целые и $q \neq 0$, то $\varphi\left(\dfrac{p}{q}\right) = \dfrac{\varphi p}{\varphi q} = \dfrac{p}{q}$. Таким оразом, $\mathbb{Q}$ отображается тождественно.

2) Пусть φ — автоморфизм $\mathbb{R} \to \mathbb{R}$. Сперва докажем, что положительные числа переводятся в положительные. Действительно, пусть $a > 0$. Тогда найдется такое b, что $a = b^2$. Имеем $\varphi a = \varphi b^2 = (\varphi b)^2 > 0$. Теперь выводим, что если $a < b$, то $\varphi a < \varphi b$, так как $\varphi b - \varphi a = \varphi(b-a) > 0$. Теперь докажем от противного, что все вещественные числа отображаются тождественно. Пусть $a \in \mathbb{R}$, $\varphi a = b \neq a$. Рассмотрим случай $\varphi a < b$. Найдется рациональное c, такое, что $a < c < b$. Тогда $c < b = \varphi a < \varphi c = c$. Противоречие. Аналогичные рассуждения, если $\varphi a > b$.

7. Два автоморфизма: тождественный и переводящий каждое число в сопряженное. *Решение:* Легко проверить, что указанные отображения — автоморфизмы. Пусть φ — автоморфизм $\mathbb{C} \to \mathbb{C}$. Так как $i^2 = -1$, то $\varphi(i^2) = (\varphi i)^2 = \varphi(-1) = -1$. Следовательно, $\varphi i = i$ или $\varphi i = -i$ и других автоморфизмов, кроме указанных выше нет.

8. 1) Кольцо, но не поле.
2) Поле.
3) Не является кольцом.
4) Не является кольцом.
5) Кольцо, но не поле.
6) Поле. *Указание.* Если $\sqrt[3]{4} = a + b\sqrt[3]{2}$, то, домножая обе части на $\sqrt[3]{2}$, получаем $2 = a\sqrt[3]{2} + b(a + b\sqrt[3]{2})$. Из полученного равенства выразить $\sqrt[3]{2}$.

9. Не изоморфны.

10. 1) $-\dfrac{2}{23} + \dfrac{3}{23}\sqrt{3}$; 2) $-\dfrac{1}{4} - \dfrac{1}{4}\sqrt{5}$; 3) $-\dfrac{3}{5} - \dfrac{3}{5}\sqrt[3]{2} - \dfrac{2}{5}\sqrt[3]{4}$; 4) $\dfrac{7}{4} + \dfrac{5}{4}\sqrt[3]{3} + \dfrac{3}{4}\sqrt[3]{9}$.

13. $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : \ a, b, c, d \in \mathbb{Q}\right\}$.
1) $\sqrt{3} - \sqrt{2}$; 2) $\dfrac{1}{2} + \dfrac{1}{4}\sqrt{2} - \dfrac{1}{4}\sqrt{6}$; 3) $-5 - \dfrac{7}{2}\sqrt{2} - 3\sqrt{3} - 2\sqrt{6}$.

14. 1) полугруппа, но не группа; 2) полугруппа, но не группа;
3) полугруппа, но не группа; 4) группа;

5) группа;
6) группа; 7) группа;
8) не является полугруппой; 9) группа; 10) группа.

15. 1) полугруппа, но не группа;
2) полугруппа, но не группа;
3) не является полугруппой;
4) полугруппа, но не группа;
5) полугруппа, но не группа;
6) полугруппа, но не группа;
7) группа;
8) группа;
9) не является полугруппой;
10) полугруппа, но не группа;
11) группа;
12) группа;
13) полугруппа, но не группа;
14) группа;
15) группа;
16) группа;
17) группа.

17. 1) полугруппой не является; 2) полугруппой не является; 3) полугруппой не является; 4) полугруппа с единицей, но не группа.

18. 1) полугруппой не является, 2) полугруппой не является.

19. 1) Полугруппа, но (при $X \neq \emptyset$) не группа. Нейтральный элемент $\emptyset$.
2) Полугруппа, но (при $X \neq \emptyset$) не группа. Нейтральный элемент X.
3) Группа. Нейтральный элемент $\emptyset$.

20. 1) группа; 2) группа; 3) операция не алгебраическая; 4) не является полугруппой.

21. 1) группа; 2) полугруппа, но (если $K \neq \{0\}$) не группа; 3) полугруппа, но (если $K \neq \{0\}$) не группа; 4) полугруппа, но не группа.

22. 2) $n!$; 3) $n!/2$, если $n \geq 2$.

29. 1) $\sum\limits_{i=0}^{n} n(n-1)\dots(n-i+1)$; 2) $n!$; 3) $2^n n!$.

33. 1) Группа; 2) не является полугруппой (нет замкнутости).

35. 1) n. 2) $2n$. 4) *Указание.* Пронумеровать вершины квадрата.

37. 1) *Указание.* Пронумеровать вершины прямоугольника. 2) *Указание.* Это матрицы ортогональных преобразований, совмещающих прямоугольник с самим собой.

38. Группа вращений тетраэдра имеет порядок 12, куба и октаэдра — 24, икосаэдра и додекаэдра — 60. *Указание.* Рассмотреть движение, переводящее заданную вершину $\mathcal{A}$ в некоторую вершину $\mathcal{B}$ (не обязательно отличную от $\mathcal{A}$) и доказать, что порядок группы вращений правильного многогранника равен nk, где n — число вершин, а k — число ребер, выходящих из каждой вершины.

47. *Указание.* Доказать, что операция выполняется по правилу: $(x_1, x_1^3)+(x_2, x_2^3) = (x_1+x_2, (x_1+x_2)^3)$.

48. Явные формулы для сложения точек эллиптической кривой следующие: при $x_1 \neq x_2$

$$(x_1, y_1) + (x_2, y_2) = \left(-x_1 - x_2 + \lambda^2,\ -y_1 - \lambda(-2x_1 - x_2 + \lambda^2)\right),\ \text{где } \lambda = \frac{y_2 - y_1}{x_2 - x_1};$$

$$(x_0, y_0) + (x_0, y_0) = \left(-2x_0 + \lambda^2,\ -y_0 - \lambda(-3x_0 + \lambda^2)\right), \quad \text{где} \quad \lambda = \frac{3x_0^2 + a}{2y_0}.$$

49. Так как $(ab)^2 = e$, то $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

50. 1) Одна группа — циклическая. Задается таблицей

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Представляется подстановками: $e = \varepsilon$, $a = (1\,2\,3)$, $b = (1\,3\,2)$.

2) Две группы: циклическая и четверная группа Клейна V_4, которые задаются таблицами умножения соответственно:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Представление подстановками для циклической: $e = \varepsilon$, $a = (1\,2\,3\,4)$, $b = (1\,3)(2\,4)$, $c = (1\,4\,3\,2)$; для V_4: $e = \varepsilon$, $a = (1\,2)(3\,4)$, $b = (1\,3)(2\,4)$, $c = (1\,4)(2\,3)$.

3) Две группы: циклическая и группа, изоморфная S_3, которые задаются таблицами умножения соответственно:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Представление подстановками для циклической: $e = \varepsilon$, $a = (1\,2\,3\,4\,5\,6)$, $b = (1\,3\,5)(2\,4\,6)$, $c = (1\,4)(2\,5)(3\,6)$, $d = (1\,5\,3)(2\,6\,4)$, $f = (1\,6\,5\,4\,3\,2)$; для S_3: $e = \varepsilon$, $a = (1\,2\,3)$, $b = (1\,3\,2)$, $c = (1\,2)$, $d = (1\,3)$, $f = (2\,3)$.

51. Не является группой, так как операция неассоциативна. Например, $(aa)b = eb = b$, но $a(ab) = ad = c$. Множество с одной алгебраической операцией называется *квазигруппой*, если уравнения $ax = b$, $ya = b$ в нем всегда разрешимы, причем однозначно. Квазигруппа с нейтральным элементом называется *лупой*. Таким образом, G является примером неассоциативной *лупы*.

54. $\varphi x = \alpha x$, где $\alpha \in \mathbb{Q}$, $\alpha \neq 0$.

56. 3) *Указание*. Воспользовавшись конечностью G, доказать, что из того, что уравнение $ax = b$ имеет не более одного решения, следует, что решение существует.

57. 3) *Указание.* Воспользоваться № 56(3).

59. Пусть a — произвольный элемент конечной полугруппы. Рассмотрим множество элементов вида a^{2^k}, $k \in \mathbb{N}$. Поскольку полугруппа конечная, то существуют такие различные натуральные числа s и t, $s > t$, что $a^{2^t} = a^{2^s}$. Если $s = t+1$, то элемент $b = a^{2^t}$ является идемпотентом. В противном случае умножив равенство $a^{2^t} = a^{2^s}$ на a^x, получим $a^{2^t+x} = a^{2^s+x}$. Найдем такое натуральное x, что $a^{2^t+x} = (a^{2^s+x})^2$. Тогда искомым идемпотентом будет $b = a^{2^s+x}$. Имеем $a^{2^t+x} = (a^{2^s+x})^2 = a^{2^{t+1}+2x} = a^{2^s+x}$. Если $2^{t+1} + 2x = 2^s + x$, то $x = 2^s - 2^{t+1} \in \mathbb{N}$.

61. 1) $F \setminus \{0\}$;

2) множество матриц, определители которых отличны от нуля, т. е. $\mathrm{GL}(F, n)$;

3) обратимые элементы кольца K.

62. $|\mathrm{GL}(\mathbb{Z}_p, n)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$.

63. $|\mathrm{GL}(\mathbb{Z}_m, n)| = m^{n^2} \prod\limits_{i=1}^{s} \prod\limits_{j=1}^{n} \left(1 - \frac{1}{p_i^j}\right) = \left(\frac{m}{p_1 \dots p_s}\right)^{n^2} \prod\limits_{i=1}^{s} \prod\limits_{j=0}^{n-1} (p_i^n - p_i^j)$, где $p_1, ..., p_s$ — простые сомножители в разложении числа m.

65. Вообще говоря, неверно.

67. Если $H \subseteq K$, то всё доказано. Предположим, что $H \nsubseteq K$. Тогда найдется элемент $a \in H \backslash K$. Докажем, что $K \subseteq H$. Действительно, рассмотрим произвольный элемент $b \in K$. Тогда $ab \in H \cup K$. Если $ab \in K$, то $a = (ab)b^{-1} \in K$, поскольку $ab \in K$ и $b^{-1} \in K$. Пришли к противоречию. Значит, $ab \in H \backslash K$ и, следовательно, $b = a^{-1}(ab) \in H$. Тем самым доказано, что $K \subseteq H$.

68. Рассмотрим декартово произведение $H \times K = \{(h, k) : h \in H, k \in K\}$. Назовем две пары (h, k) и (h', k') эквивалентными, если $hk = h'k'$. Ясно, что таким образом мы определили отношение эквивалентности $\sim$ на $H \times K$ и число классов эквивалентности равно $|HK|$. Тогда $(h, k) \sim (h', k')$ только в том случае, если $h^{-1}h' = kk'^{-1} \in H \cap K$. Другими словами, $(h, k) \sim (h', k')$ тогда и только тогда, когда существует такой элемент $g \in H \cap K$, что $h' = hg$, $k' = g^{-1}k$. Поскольку $|H \times K| = |H| \cdot |K|$ и каждый класс эквивалентности содержит ровно $|H \cap K|$ элементов, то число классов равно $|H| \cdot |K|/|H \cap K|$.

69. Все такие группы изоморфны $\mathbb{Z}$.

72. 1) 6; 2) 30; 3) 12; 4) 8; 5) 8; 6) 2; 7) 3.

73. $z = \dfrac{3+4i}{5}$ имеет конечный порядок только в том случае, если $(3+4i)^n = 5^n$ для некоторого натурального n. Если $g = 3 + 4i$, то $g^2 = -7 + 24i \equiv 3 + 4i \equiv g \pmod 5$. Поэтому для любого натурального n число g^n не может быть вещественным.

74. 1) $\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$ и $\dfrac{1}{2} - \dfrac{\sqrt{3}}{2}i$;

2) Каждый элемент порядка 6 в S_5 есть произведение двух независимых циклов: длины 2 и длины 3. Всего 10 элементов.

3) Элементов порядка 6 в A_5 нет.

79. ± 1.

81. Подгруппами являются $n\mathbb{Z}$, где n — целое неотрицательное.

82. Пусть $d = \text{НОД}\{n, k\}$, причем $n = n'd$, $k = k'd$ и $nu + kv = d$ для некоторых целых u, v. Сначала докажем, что $(a^k) = (a^d)$. Включение $(a^k) \subseteq (a^d)$ следует из $a^k = (a^d)^{k'} \in (a^d)$. Включение $(a^d) \subseteq (a^k)$ следует из $a^d = a^{nu+kv} = (a^n)^u + (a^k)^v = (a^k)^v \in (a^k)$. Теперь легко видеть, что $(a^d) = \left\{e, a^d, a^{2d}, \dots, a^{(n'-1)d}\right\}$, т. е. $|a^k| = |a^d| = n'$.

83. 1) 4 подгруппы: $\{e\}$, $\{e, a^3\}$, $\{e, a^2, a^4\}$, G.

2) 7 подгрупп: $\{e\}$, $\{e, a^{12}\}$, $\{e, a^8, a^{16}\}$, $\{e, a^6, a^{12}, a^{18}\}$, $\{e, a^4, a^8, a^{12}, a^{16}, a^{20}\}$, $\{e, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, $
G.

86. Для $n = 1$ первообразный корень 1.
Для $n = 2$ первообразный корень -1.
Для $n = 3$ первообразные корни $-\dfrac{1}{2} \pm \dfrac{\sqrt{3}}{2}i$.
Для $n = 4$ первообразные корни $\pm i$.
Для $n = 5$ первообразные корни $\cos\dfrac{2\pi}{5} \pm i\sin\dfrac{2\pi}{5}$.
Для $n = 6$ первообразные корни $\dfrac{1}{2} \pm \dfrac{\sqrt{3}}{2}i$.
Для $n = 12$ первообразными корнями являются $\pm\dfrac{\sqrt{3}}{2} \pm \dfrac{1}{2}i$ (4 элемента).

Указание. Согласно № 82, первообразными корнями n-й степени из 1 являются числа $\cos\dfrac{2\pi k}{n} + i\sin\dfrac{2\pi k}{n}$ для всех k, не превосходящих n и взаимно простых с ним.

87. $\mathbb{Z}_n$ является циклической при любом натуральном n. Для того, чтобы $k \in \mathbb{Z}_n$ был производящим группы $\mathbb{Z}_n$ необходимо и достаточно, чтобы НОД $\{n, k\} = 1$.

88. Для $p = 2$ порождающий элемент 1.
Для $p = 3$ порождающий элемент 2.
Для $p = 5$ порождающие элементы 2, 3.
Для $p = 7$ порождающие элементы 3, 5.
Для $p = 11$ порождающие элементы $2, 6, 7, 8$.
Указание. Достаточно найти один порождающий элемент. Остальные можно отыскать на основании № 82.

89. 2) В общем случае неверно. Например, элементы

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

группы $\mathrm{GL}(\mathbb{R}, 2)$ имеют конечный порядок, но элемент AB имеет бесконечный порядок.
3) Множество всех значений корня произвольной натуральной степени из 1.

90. 3) Матрицы вида $P^{-1}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}P$, где P — невырожденная матрица, а a и b — произвольные корни из 1.

91. Пусть $|a| = k$, $|b| = s$, НОД $\{k, s\} = 1$. Поскольку $ab = ba$, то $(ab)^{ks} = (a^k)^s(b^s)^k = e$. Если $(ab)^m = e$, то $e = (ab)^{mk} = b^{mk}$ и $e = (ab)^{ms} = a^{ms}$. Следовательно, ms делится на k, а mk делится на s, поэтому в силу взаимной простоты k и s имеем делимость m на k, m на s и m на ks. Таким образом, $|ab| = ks = |a||b|$.

92.
1) Пусть $|a| = k$, $|b| = s$, НОК $\{k, s\} = l$. Тогда $(ab)^l = (a^k)^{\frac{l}{k}}(b^s)^{\frac{l}{s}} = e$. Следовательно, l делится на $|ab|$. Если в качестве b взять a^{-1}, то $|a| = |a^{-1}| = k$, но $|ab| = |e| = 1 \neq k =$ НОК $\{k, k\}$.
2) Пусть $|a| = k$, $|b| = s$. Если НОД $\{k, s\} = 1$, то согласно № 91 имеем $|ab| = ks$. Поэтому НОК $\{|a|, |b|\} = ks$ делится на $|ab|$. Пусть теперь НОД $\{k, s\} > 1$ и $p_1, \ldots, p_r$ — простые числа, входящие в каноническое разложение k и s на множители. Пусть $k = p_1^{u_1} \cdots p_r^{u_r}$, $s = p_1^{v_1} \cdots p_r^{v_r}$. Можно считать, что $k = k_0k_1$, $s = s_0s_1$, $k_0 = p_1^{u_1} \cdots p_t^{u_t}$, $k_1 = p_{t+1}^{u_{t+1}} \cdots p_r^{u_r}$,

$s_0 = p_1^{v_1} \cdots p_t^{v_t}$, $s_1 = p_{t+1}^{v_{t+1}} \cdots p_r^{v_r}$ и $u_i \geq v_i$ для $i = 1, \ldots, t$, и $u_i < v_i$ для $i = t+1, \ldots, r$. Тогда $\text{НОК}\{k, s\} = k_0 s_1$. Далее, $|a^{k_1}| = k_0$, $|b^{s_0}| = s_1$. Поскольку $\text{НОД}\{k_0, s_1\} = 1$, то согласно № 91 имеем $|a^{k_1} b^{s_0}| = k_0 s_1 = \text{НОК}\{k, s\}$. Искомый элемент $c = a^{k_1} b^{s_0}$.

93. Пусть $G = \{g_1, g_2, \ldots, g_s\}$, $m = \max\limits_{1 \leq i \leq s} |g_i| = |g_k|$. Докажем, что m делится на $m_i = |g_i|$ для любого $i = 1, \ldots, s$. Предположим, что m не делится на m_i. Тогда $\text{НОК}\{m, m_i\} > m$. Согласно № 92 в G существует элемент, порядок которого равен $\text{НОК}\{m, m_i\} > m$, что противоречит выбору m.

94. Подгруппа $H_1 = \{(1, b) : \ b \in \mathbb{R}\}$ изоморфна аддитивной группе действительных чисел, подгруппа $H_2 = \{(a, 0) : \ a \in \mathbb{R} \setminus \{0\}\}$ изоморфна мультипликативной группе ненулевых действительных чисел. Инволюциями являются элементы вида $(-1, b)$ и единица группы $(1, 0)$. Группа не содержит элементов конечного порядка, большего двух.

95. Ясно, что достаточно рассматривать $1 \leq k \leq n = |G|$. Пусть G циклическая, порождаемая элементом a. Выясним, как устроены решения уравнения $x^k = e$. Пусть $x = a^t$, тогда $x^k = a^{kt} = e = a^n$. Поэтому kt делится на n. Последнее условие равносильно тому, что t делится на $\dfrac{n}{\text{НОД}\{n, k\}}$. Таким образом, t принимает значения из множества

$$\left\{ \frac{n}{\text{НОД}\{n, k\}} \cdot i : \ i = 0, 1, \ldots, \text{НОД}\{n, k\} - 1 \right\}$$

и $|G_k| = \text{НОД}\{n, k\} \leq k$. Докажем обратное утверждение. Пусть $|G_k| \leq k$ для всех $k \in \mathbb{N}$. Положим

$$m = \max_{1 \leq i \leq n} |g_i|.$$

Согласно № 93 m делится на $|g_i|$ для любого $1 \leq i \leq n$. Поэтому $g_i^m = e$ для любого $1 \leq i \leq n$. Если G нециклическая, то $m < n$ и $|G_m| = n > m$, что противоречит условию.

96. Предположим, что абелева группа G порядка pq нециклическая. Тогда в ней существует либо элемент порядка p, либо элемент порядка q. Не уменьшая общности, пусть a — элемент порядка p, $H = (a)$. Фактор-группа G/H состоит тогда из q смежных классов и является циклической. Пусть смежный класс bH является ее порождающим элементом. Тогда смежные классы $eH, bH, \ldots, b^{q-1}H$ различны. Таким образом, $(bH)^q = eH = b^q H$, поэтому $b^q \in H$ и $b^q = a^t$ для некоторого $0 \leq t < p$. Докажем, что $t = 0$. Тогда a и b — два коммутирующих элемента порядков p и q соответственно. Следовательно, согласно № 91 элемент ab имеет порядок pq, то есть группа G циклическая. Пусть $t \neq 0$. Тогда порядок элемента b равен p, то есть $b^p = e$. Если $p < q$, то имеем равенство смежных классов $b^p H$ и eH, что невозможно. Если $q < p$, то разделим p на q с остатком: $p = ql + r$, $0 < r < q$. Тогда $b^p = b^{ql+r} = b^{ql} b^r = a^{tl} b^r = e$. Следовательно, $b^r = a^{-tl} \in H$, что противоречит различности смежных классов $b^r H$ и eH.

97. 1) $\{e\}$, $\{e, (1\,2)(3\,4)\}$, $\{e, (1\,3)(2\,4)\}$, $\{e, (1\,4)(2\,3)\}$, V_4.
2) $\{e\}$, $\{e, (1\,2)\}$, $\{e, (1\,3)\}$, $\{e, (2\,3)\}$, $\{e, (1\,2\,3), (1\,3\,2)\}$, S_3.
3) V_4 и все ее подгруппы, $\{e, (1\,2\,3), (1\,3\,2)\}$, $\{e, (1\,2\,4), (1\,4\,2)\}$, $\{e, (1\,3\,4), (1\,4\,3)\}$, $\{e, (2\,3\,4), (2\,4\,3)\}$, A_4.

100. Порядок элемента равен наименьшему общему кратному длин циклов в разложении подстановки на независимые циклы. Для элемента, указанного в формулировке задачи, порядок равен 60.

101. Наибольший порядок, 60, имеет элемент, равный произведению трех независимых циклов длины 3, 4, 5 соответственно.

102. 1) гомоморфизм;

2) гомоморфизм;
3) не является гомоморфизмом;
4) гомоморфизм;
5) не является гомоморфизмом;
6) гомоморфизм;
7) не является гомоморфизмом.

103. 1) изоморфизм; 2) гомоморфизм; 3) гомоморфизм.

105. 1) 2 смежных класса: $\{e, a^2, a^4\}$ и $\{a, a^3, a^5\}$.

2) 3 смежных класса: $\{e, a^3\}$, $\{a, a^4\}$, $\{a^2, a^5\}$.

3) Разбиение на левые смежные классы совпадает с разбиением на правые смежные классы. Всего 2 смежных класса: $\{e, (1\,2\,3), (1\,3\,2)\}$ и $\{(1\,2), (1\,3), (2\,3)\}$.

4) *Решение:* Умножая $H = \{e, (1\,2)\}$ слева на каждый из элементов группы $G = \{e,\ (1\,2),\ (1\,3),\ (2\,3),$ получаем:

$$\begin{aligned} eH &= H, \\ (1\,2)H &= \{(1\,2),\ e\} = H, \\ (1\,3)H &= \{(1\,3),\ (1\,2\,3)\}, \\ (2\,3)H &= \{(2\,3),\ (1\,3\,2)\}, \\ (1\,2\,3)H &= \{(1\,2\,3),\ (1\,3)\} = (1\,3)H, \\ (1\,3\,2)H &= \{(1\,3\,2),\ (2\,3)\} = (2\,3)H. \end{aligned}$$

Таким образом, получили 3 левых смежных класса: $H = (1\,2)H = \{e, (1\,2)\}$, $(1\,3)H = (1\,2\,3)H = \{(1\,3), (1\,2\,3)\}$, $(2\,3)H = (1\,3\,2)H = \{(2\,3), (1\,3\,2)\}$.

Умножая H справа на каждый из элементов группы G, получаем:

$$\begin{aligned} He &= H, \\ H(1\,2) &= \{(1\,2),\ e\} = H, \\ H(1\,3) &= \{(1\,3),\ (1\,3\,2)\}, \\ H(2\,3) &= \{(2\,3),\ (1\,2\,3)\}, \\ H(1\,2\,3) &= \{(1\,2\,3),\ (2\,3)\} = H(2\,3), \\ H(1\,3\,2) &= \{(1\,3\,2),\ (1\,3)\} = H(1\,3). \end{aligned}$$

Таким образом, получили 3 правых смежных класса: $H = H(1\,2) = \{e, (1\,2)\}$, $H(1\,3) = H(1\,3\,2) = \{(1\,3), (1\,3\,2)\}$, $H(2\,3) = H(1\,2\,3) = \{(2\,3), (1\,2\,3)\}$.

5) Элементы, составляющие один левый смежный класс, — все вращения, переводящие заданную вершину в какую-либо другую. Элементы, составляющие один правый смежный класс, — все вращения, переводящие какую-либо вершину в заданную. Всего 4 левых и 4 правых смежных класса.

6) *Решение:* Матрицы A и B из $\mathrm{GL}(\mathbb{R}, n)$ принадлежат одному и тому же *левому* смежному классу тогда и только тогда, когда $A^{-1}B \in \mathrm{SL}(\mathbb{R}, n)$, что эквивалентно $\det(A^{-1}B) = 1$. Преобразуя левую часть последнего равенства, получаем

$$(\det A)^{-1} \det B = 1,$$

т. е. $\det A = \det B$.

Матрицы A и B принадлежат одному и тому же *правому* смежному классу тогда и только

тогда, когда $AB^{-1} \in \mathrm{SL}(\mathbb{R}, n)$, т. е. $\det(AB^{-1}) = 1$, откуда снова легко получить равносильное условие $\det A = \det B$.

Ответ: Разбиение на левые смежные классы совпадает с разбиением на правые смежные классы. Смежные классы — множества матриц с фиксированным определителем.

106. 1) Все подгруппы четверной группы Клейна V_4 (они перечислены в ответе к № 97 (1)) являются нормальными делителями.

2) $\{e\}$, $\{e, (1\,2\,3), (1\,3\,2)\}$, S_3.

3) $\{e\}$, V_4, A_4.

4) $\{e\}$, V_4, A_4, S_4.

107. Не всегда. Например, $G' = A_4$, $G = V_4$, $H = \{e, (1\,2)(3\,4)\}$.

114. *Указание.* Воспользоваться № 113.

115. Пусть H — подгруппа, индекс p которой есть наименьший простой делитель порядка группы G. Согласно № 114 построим нормальный делитель N группы G, такой, что $p! \vdots |G/N|$ и $N \subseteq H$, следовательно, $|G/N| \geq p$. Докажем, что $N = H$. Так как $|G| \vdots |G/N|$ и p — минимальный простой делитель числа $|G|$, то $|G/N|$ также не может иметь простых делителей, меньших p. Однако все простые делители, кроме одного, числа $p!$ меньше p, поэтому, в силу $p! \vdots |G/N|$, получаем $|G/N| = p$, откуда $|G/N| = |G/H|$, следовательно, $|N| = |H|$. Так как $N \subseteq H$, то $N = H$, поэтому H — нормальный делитель. Возможно доказательство, использующее действие групп. См. решение к № 172.

117. Пусть H — циклическая подгруппа, порожденная элементом g. По теореме Лагранжа порядок k подгруппы H делит n. Тогда $g^n = (g^k)^{n/k} = e^{n/k} = e$. Для абелевой группы можно дать доказательство, не использующее теорему Лагранжа. Пусть $G = \{a_1, a_2, \ldots, a_n\}$. Тогда $aG = G$ и, рассмотрев произведение всех элементов группы, получаем

$$a^n \prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_i,$$

откуда $a^n = e$.

118. Если $a \equiv 0 \pmod p$, то утверждение очевидно. Иначе исходное сравнение эквивалентно $a^{p-1} \equiv 1 \pmod p$, что выражает тот факт, что степень элемента a в мультипликативной группе $\mathbb{Z}_p^*$ является делителем порядка этой группы.

121. 1) Если $x \in \mathbb{Z}_N^*$, то

$$g(f(x)) = (x^a \bmod)^b \bmod N = x^{ab} \bmod N = x^{1+kn} \bmod N = x \bmod N = x$$

для некоторого целого k.

2) Достаточно доказать, что если $c \equiv 1 \pmod n$, то $x^c \equiv x \pmod N$. Так как n делит $c - 1$, то $q - 1$ делит $c - 1$, поэтому

$$p^{c-1} \equiv 1 \pmod q \Rightarrow p^c \equiv p \pmod q \Rightarrow p^c \equiv p \pmod{pq}.$$

Аналогично,

$$q^c \equiv q \pmod{pq}.$$

Так как p и q взаимно простые, то произвольный целый x можно представить в виде $x = kq + mp$ для некоторых целых k и m, откуда $x^c \equiv x \pmod{pq}$.

122. *Указание.* Воспользуйтесь № 117.

123. Например, A_4 не имеет подгруппы 6-го порядка (см. № № 97 (3)).

133. Гомоморфизм однозначно определяется образом порождающего элемента.

1) φa может быть равен любому элементу группы. Число гомоморфизмов равно n.
2) $\varphi a = a^k$ для любого k, не превосходящего n и взаимно простого с ним.
3) Пусть $d = \text{НОД}\,\{n, m\}$, тогда $\varphi a = b^{mk/d}$ $(k = 0, 1, \ldots, d-1)$. Число гомоморфизмов равно d.
4) Если n не кратно m, то сюръективного гомоморфизма нет. Иначе $\varphi a = b^k$ для любого k, не превосходящего m и взаимно простого с ним.

134. 1) 2; 2) $\varphi(n)$ (функция Эйлера).

135. 1) $\mathbb{Z}_{p-1}$; 2) $\mathbb{Z}_2$; 3) V_4; 4) $\mathbb{Z}_6$; 5) S_3; 6) S_3; 7) D_4; 8) S_4.

136. 1.

137. Множество H всех квадратов группы G является подгруппой. Фактор-группа G/H — циклическая, порядка не менее 2. Пусть cH — ее порождающий элемент. Так как, по определению H, $c^2 \in H$, то $(cH)^2 = c^2H = H$. Следовательно, G/H — группа второго порядка и $ab \in aH \cdot bH = H$, т. е. ab есть квадрат.

138. Докажем, что $HK \subseteq KH$. Рассмотрим произвольный элемент $hk \in HK$, где $h \in H$, $k \in K$. Поскольку H — нормальный делитель, то $k^{-1}hk = h' \in H$, поэтому $hk = kh' \in KH$ и $HK \subseteq KH$. Обратное включение $KH \subseteq HK$ доказывается аналогично. Согласно № 66 HK является подгруппой в G.

139. Рассмотрев произведение $(hk)(kh)^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{e\}$, получаем, что $hk = kh$.

140. 1) $K_1 = (2\,3\,4)H$, где $H = \{\varepsilon,\ (1\,4)\}$.
2) K_2 не является смежным классом.
3) K_3 является подгруппой.
4) K_4 не является смежным классом.
5) $K_5 = (1\,2)H$, где $H = \{\varepsilon,\ (1\,5)\,(3\,4)\}$.

142. Предположим противное: некоторый смежный класс $aZ(G)$ является порождающим элементом фактор-группы $G/Z(G)$. Рассмотрим два произвольных элемента g и g' из группы G. Пусть $gZ(G) = (aZ(G))^k = a^kZ(G)$, $g'Z(G) = (aZ(G))^s = a^sZ(G)$. Тогда $g = a^kz$, $g' = a^sz'$ для некоторых $z, z' \in Z(G)$. Поскольку $gg' = a^kza^sz' = z^{k+s}zz' = g'g$, то группа G абелева, что противоречит условию.

144. Гомоморфизм однозначно определяется образом порождающего элемента. Пусть a — порождающий элемент группы G, а b — порождающий элемент группы G'.
1) Один гомоморфизм, образом которого является единичный элемент группы G'.
2) Существует ровно n гомоморфизмов: $\varphi(b) = a^k$, $0 \leq k < n$.

145. Множество представителей различных левых смежных классов:

$$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}, \quad t \in \mathbb{Q} \right\}.$$

Действительно, если $a \neq 0$, то

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \dfrac{c}{a} & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & \dfrac{ad-bc}{a} \end{pmatrix}.$$

Если $a = 0$, то

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & b \end{pmatrix}.$$

Осталось доказать, что различные элементы из предъявленного множества порождают различные левые смежные классы. Пусть A, B — два таких элемента и $AH = BH$. Тогда $A^{-1}B \in H$. Если A и B нижние унитреугольные, то матрица $A^{-1}B$ тоже нижняя унитреугольная. Но в подгруппе H единственной унитреугольной матрицей является единичная, следовательно, $A = B$. Если одной из матриц A или B является $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, то ни $A^{-1}B$, ни $B^{-1}A$ не являются верхними треугольными.

146. Например, группа Q_8 кватернионных единиц (см. № 44).

148. Пусть G — конечная подгруппа в $\mathrm{GL}(\mathbb{Z}, n)$. Тогда утверждение эквивалентно тому, что $G \cap \operatorname{Ker}\varphi = \{E\}$. Предположим, что $A = E + p^r B \in G \cap \operatorname{Ker}\varphi$, $B \in \mathbb{Z}^{n\times n}$, $r \geq 1$, $A^m = E$, и не все элементы матрицы B делятся на p. По формуле бинома

$$A^m - E = (E + p^r B)^m - E = mp^r B + \sum_{k=2}^{m} \binom{m}{k} p^{rk} B^k = 0.$$

Но элементарное арифметическое рассуждение показывает, что при $p > 2$ все числа под знаком суммы делятся на большую степень p, чем mp^r.

149. Знакопеременная группа A_n.

150. $\mathrm{SL}(\mathbb{R}, 2)$.

151. В некоммутативной группе централизатор элемента может не быть подгруппой. Например, централизатором цикла (123) в S_3 является множество $\{e, (123)\}$, которое не является подгруппой.

152. 1) Централизатором матрицы A является множество невырожденных диагональных матриц. Централизатором матрицы B является множество матриц вида

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix},$$

где $a \neq 0$.

2) Централизатором матрицы C является множество матриц вида

$$\begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & a \end{pmatrix},$$

где $ac \neq 0$.

157. *Указание.* Используйте № № 142, 155.

158. То, что группа автоморфизмов циклической группы абелева, очевидно. Ясно, что циклическая группа G, порядок которой больше 2, содержит элемент g такой, что $g^2 \neq e$ (например, таким элементом является любой порождающий элемент группы). При этом отображение $\varphi(x) = x^{-1}$, $x \in G$ является автоморфизмом группы G, отличным от тождественного. Более того, автоморфизм φ^2 является тождественным и порождает подгруппу второго порядка в группе $\operatorname{Aut} G$. Следовательно, порядок группы $\operatorname{Aut} G$ является четным числом.

161. 2) *Указание.* Рассмотреть отображение из Gx в множество левых смежных классов, заданное правилом: $g * x \mapsto g\,\mathrm{St}_G(x)$, и доказать, что оно является биекцией.

3) Поскольку орбиты точек либо совпадают, либо не пересекаются и каждая точка $x \in X$ содержится в некоторой орбите (например, в орбите Gx), то

$$|X| = \sum_{i=1}^{r} |Gx_i| = \sum_{i=1}^{r} \frac{|G|}{\mathrm{St}_G(x_i)}.$$

163. Две орбиты: $\{0\}$ и $\mathbb{R}^n \backslash \{0\}$.

164. 1) G — единственная орбита, все стабилизаторы единичные;
2) G — единственная орбита, все стабилизаторы единичные;
3) орбиты — левые (соответственно правые) смежные классы группы G по подгруппе H, все стабилизаторы единичные.

166. Подсчитаем мощность множества $M = \{(g, x) \mid g * x = x\}$ двумя способами. С одной стороны, $|M| = \sum\limits_{g \in G} |\,\mathrm{Fix}(g)|$, с другой стороны, $|M| = \sum\limits_{x \in X} |\,\mathrm{St}_G(x)|$, поэтому $\sum\limits_{g \in G} |\,\mathrm{Fix}(g)| = \sum\limits_{x \in X} |\,\mathrm{St}_G(x)| = \sum\limits_{x \in X} \frac{|G|}{|Gx|}$. Разделив это равенство на $|G|$, получим $\frac{1}{|G|} \sum\limits_{g \in G} |\,\mathrm{Fix}(g)| = \sum\limits_{x \in X} \frac{1}{|Gx|}$. Поскольку точки из одной орбиты дают одинаковый вклад в последнюю сумму, то эта сумма равна числу орбит.

167. Согласно № 161 порядок группы G равен сумме индексов стабилизаторов элементов, представляющих различные орбиты. Ясно, что каждая орбита длины 1 содержит элемент из центра группы.

168. Применим индукцию по порядку n группы G. Для $n = 2$ теорема верна, поскольку G — циклическая группа второго порядка. Пусть теорема верна для всех групп, порядок которых меньше n, и G — группа порядка n. Пусть сначала G абелева. Рассмотрим произвольный элемент $a \in G$, отличный от единицы e. Его порядок $k > 1$. Если $k \vdots p$, $k = ps$, то элемент a^s имеет порядок p. Если k не делится на p, то порядок фактор-группы G/H, где $H = (a)$, равен $\frac{n}{k} < n$ и делится на p. По предположению индукции G/H содержит элемент bH порядка p, то есть $(bH)^p = H$. Следовательно, $b^p \in H$ и $b^p = a^t$ для некоторого t, откуда $b^{pk} = a^{tk} = e$. Если $b^k = e$, то $(bH)^k = H$ и k делится на порядок p элемента bH, что невозможно. Значит, $b^{kp} = e$, но $b^k \neq e$, то есть элемент b^k имеет порядок p. Пусть теперь G неабелева. Если существует подгруппа $H \neq G$, индекс которой не делится на p, то порядок H меньше n и делится на p. По предположению индукции H содержит элемент порядка p. Если же индексы всех подгрупп группы G, отличных от G, делятся на p, то число элементов, сопряженных любому элементу группы G, не входящему в ее центр $Z(G)$, делится на p (см. № 161). Так как $|G| = n$ делится на p, то $|Z(G)|$ делится на p согласно № 167 и $|Z(G)| < n$, в силу некоммутативности G. По предположению индукции $Z(G)$ содержит элемент порядка p.

169. *Указание.* Используйте № 167.

170. Согласно № 169 центр группы G неединичен. Предположим, что группа G неабелева. Тогда $|Z(G)| = p$ и $|G/Z(G)| = p$. Следовательно, фактор-группа $G/Z(G)$ циклическая, что противоречит № 142. Если G циклическая, то она изоморфна группе вычетов $\mathbb{Z}_{p^2}$. В противном случае группа G содержит по крайней мере два элемента a и b порядка p, порождающие различные циклические подгруппы. Докажем, что группа G порождается этими элементами, т. е. $G = \{a^i b^j \mid 0 \leq i, j < p\}$. Для этого достаточно показать, что все элементы $a^i b^j$ различны. Действительно, если $a^k b^s = a^t b^l$, причем $k \neq t$ или $s \neq l$, то $a^{k-t} = b^{l-s}$. Пусть для определенности $k \neq t$. Тогда элементы a и a^{k-t} порождают одну и ту же циклическую подгруппу порядка p. Следовательно, b^{l-s} порождает ту же подгруппу. Но тогда $s \neq l$ и подгруппы, порожденные элементами a и b совпадают, что противоречит выбору этих элементов. Итак, $G = \{a^i b^j \mid 0 \leq i, j < p\}$. Ясно, что эта группа изоморфна $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

171. *Указание.* Используйте №№ 169, 142.

172. Пусть подгруппа H группы G имеет индекс p, который является наименьшим простым делителем порядка n группы G. Рассмотрим левое действие подгруппы H на множестве смежных классов $\{gH:\ g\in G\}$, которое элементу $h\in H$ и смежному классу gH ставит в соответствие смежный класс $(hg)H$. Поскольку $|G|=p\cdot|H|$ и длина орбиты является делителем порядка группы H, то длина орбиты любого смежного класса либо равна 1, либо больше или равна p. Но длина орбиты смежного класса eH равна 1, а сумма длин всех орбит равна p (мощности множества смежных классов, на котором действует группа H), поэтому все орбиты имеют длину 1. Таким образом, $(hg)H=gH$ для всех $h\in H$ и $g\in G$, следовательно, $g^{-1}hg\in H$ и H является нормальным делителем в G.

173. Доказательство проведем индукцией по порядку G. Если порядок простой, то утверждение очевидно. Пусть теорема доказана для всех групп, порядок которых меньше $|G|$. Если в G имеется подгруппа H, индекс которой взаимно прост с p, то по предположению индукции H содержит силовскую p-подгруппу, которая является таковой и в G. Поэтому предположим, что у всякой собственной подгруппы индекс делится на p. Тогда согласно формуле классов (см. № 167) $|Z(G)|$ делится на p. Согласно № 168 группа $Z(G)$ содержит циклическую подгруппу H порядка p. Так как $H\subset Z(G)$, то согласно № 141 подгруппа H нормальна в G. Пусть $f:\ G\to G/H$ каноническое отображение. Поскольку p^n — наибольшая степень p, делящая $|G|$, то p^{n-1} делит $|G/H|$. Пусть K' — силовская p-подгруппа в G/H, существующая по предположению индукции, и пусть $K=f^{-1}(K')$. Тогда $H\subset K$ и f отображает K *на* K'. Следовательно, имеет место изоморфизм $K/H\cong K'$ и $|K|=|K'|\cdot|H|=p^{n-1}p=p^n$. Таким образом, K — силовская p-подгруппа в G.

174. Пусть $S\subset G$ — силовская p-подгруппа и S_1 — какая-либо p-подгруппа. Рассмотрим действие S_1 на множестве смежных классов $\{gS:\ g\in G\}$, которое элементу $s\in S_1$ и смежному классу gH ставит в соответствие смежный класс $(sg)H$. Так как длина любой нетривиальной S_1-орбиты делится на p, а мощность множества смежных классов, на котором действует S_1, не делится на p, то существуют одноэлементные орбиты. Пусть gS — неподвижная точка (орбита ее содержит только gS). Тогда для всех $s_1\in S_1$ имеем $s_1gS=gS$, т. е. $g^{-1}s_1g\in S$ или $s_1\in gSg^{-1}$. Таким образом, $S_1\subset gSg^{-1}$, что доказывает первую часть утверждения. Если S_1 — силовская p-подгруппа, то $|S_1|=|S|=|gSg^{-1}|$, следовательно, $S_1=gSg^{-1}$, что доказывает вторую часть утверждения.

175. 1) Пусть $S\subset G$ — силовская p-подгруппа и $C(S)$ — класс подгрупп, сопряженных S. Согласно № 174 это и есть совокупность всех силовских p-подгрупп. При действии G на $C(S)$ сопряжениями стабилизатором любой подгруппы $S'\in C(S)$ является ее нормализатор $N(S')$. Ограничим это действие на S. Тогда множество $C(S)$ как-то разобьется на S-орбиты, которые либо одноэлементны, либо их длина делится на p.

2) Докажем, что единственной одноэлементной орбитой будет подгруппа S, откуда и будет следовать, что $|C(S)|\equiv 1 \pmod p$. Пусть S' — одноэлементная орбита. Это означает, что $sS's^{-1}=S'$ для всех $s\in S$, т. е. $S\subset N(S')$. Тогда S и S' — силовские p-подгруппы в $N(S')$ и, значит, сопряжены в ней. Но S' — нормальный делитель в $N(S')$. Следовательно, $S=S'$.

3) Докажем, что $|C(S)|$ равно индексу $N(S)$ в G. Действительно, отображение, ставящее в соответствие смежному классу $gN(S)$ подгруппу gSg^{-1}, является биекцией. Поэтому $p^nm=|G|=|N(S)|\cdot|C(S)|$. Поскольку S является подгруппой в $N(S)$, то $|N(S)|\vdots p^n=|S|$, следовательно, $|C(S)|$ является делителем m — индекса силовской p-подгруппы S.

176. Если H — единственная силовская p-подгруппа группы G, то согласно № 174 имеем $gHg^{-1}=H$ для всех $g\in G$, т. е. $gH=Hg$, следовательно, H — нормальный делитель в G.

177. Пусть N_p, N_q — число силовских p-подгрупп и q-подгрупп соответственно. Тогда согласно

№ 175 имеем $N_p \equiv 1 \pmod p$, $N_q \equiv 1 \pmod q$, $q \vdots N_p$, $p \vdots N_q$. Откуда следует, что $N_q = 1$ и поскольку $q - 1$ не делится на p, то $N_p = 1$. Пусть G_p — силовская p-подгруппа, а G_q — силовская q-подгруппа, которые являются циклическими. Согласно № 176 G_p и G_q являются нормальными делителями в G. Ясно, что $G_p \cap G_q = \{e\}$, поэтому согласно № 68 $|G_pG_q| = |G_p| \cdot |G_q| = pq$. Следовательно, $G = G_pG_q$. Далее, согласно № 139 имеем $ab = ba$ для всех $a \in G_p, b \in G_q$. Рассмотрев произвольные элементы $g_1 = a_1b_1$, $g_2 = a_2b_2 \in G$, имеем $g_1g_2 = (a_1b_1)(a_2b_2) = a_1(b_1a_2)b_2 = a_1(a_2b_1)b_2 = (a_1a_2)(b_1b_2) = (a_2a_1)(b_2b_1) = a_2(a_1b_2)b_1 = a_2(b_2a_1)b_1 = g_2g_1$. Таким образом, G — абелева группа. Если x, y — порождающие элементы подгрупп G_p и G_q соответственно, то xy — порождающий элемент группы G. Это следует, например, из № 91.

178. *Указание.* Воспользуйтесь № 175 и докажите, что $G = G_3G_5$, где G_3 — силовская 3-подгруппа порядка 9, G_5 — силовская 5-подгруппа и используйте тот факт, что группа порядка 9 абелева (№ 170).

179. 1) Неассоциативное кольцо (кольцо Ли).
2) Кольцо (коммутативное, если K коммутативно).
3) В общем случае кольцом не является, так как не имеет место дистрибутивность $a(b + c) = ab + ac$ (но справедливо, что $(a + b)c = ac + bc$).
4) Кольцо (коммутативное, если K коммутативно).
5) Кольцо (в общем случае некоммутативное, даже если K — коммутативное).
6) Кольцо Ли (в общем случае неассоциативное).
7) Коммутативное кольцо, в общем случае неассоциативное.

180. $\dfrac{1}{a + bi + cj + dk} = \dfrac{1}{a^2 + b^2 + c^2 + d^2} \cdot (a - bi - cj - dk)$.

181. 1) Полем не является.
2) Делители нуля — числа вида dy, где $y \in \mathbb{R}$, и только они.
3)

$$f'(x) = \frac{(x + dy)^n - f(x)}{dy} = \frac{x^n + nx^{n-1}dy + \sum\limits_{k=2}^{n} \binom{n}{k} x^{n-k}d^ky^k - x^n}{dy} = nx^{n-1}.$$

182. 1) Полем не является.
2) Делители нуля — числа вида $x + xj$, где $x \in \mathbb{R}$, и только они.

183. 6) Тело кватернионов является линейной алгеброй (размерности 4) над полем $\mathbb{R}$. Над полем $\mathbb{C}$ алгеброй не является.

184. 1) Не является кольцом; 2) является полем.

188. *Указание.* См. № 9.

189. Нет, так как в $\mathbb{Z}_2$ все элементы являются квадратами.

191. p^2.

192. 1) Не является кольцом, так как 2^X относительно операции объединения не есть группа.
2) Кольцо. Является полем, если и только если $|X| = 1$.

194. Является полукольцом. Кольцом не является (если $|X| \neq 1$), так как X относительно операции $\downarrow$ не является группой.

197. В кольце матриц вида

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

где $a, b \in \mathbb{R}$, левыми единицами являются все матрицы

$$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix},$$

где $c \in \mathbb{R}$.

209. 1) $D = 0$;

2) $f(x)D$, $f(x) \in \mathbb{Z}[x]$, где D — обычное дифференцирование;

3) $\sum\limits_{i=1}^{n} f_i D_i$, $f_i \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, где D_i — частное дифференцирование по переменной x_i.

210. Обозначим через X множество правых обратных к элементу x. Рассмотрим отображение $\varphi_y : X \to X$, задаваемое правилом $\varphi_y(z) = y + zx - 1$, где y — некоторый фиксированный элемент из X. Поскольку x не имеет левых обратных, то $y \notin \varphi_y(X)$. С другой стороны, отображение φ_y инъективно, так как равенство $\varphi_y(a) = \varphi_y(b)$ влечет $ax = bx$, откуда вытекает $a = b$. Таким образом, отображение φ_y инъективно, но не сюръективно, что возможно только в случае, когда множество X бесконечно.

211. Если $xy = 1$ и $yx \neq 1$, то элемент $y + yx - 1 \neq y$ является правым обратным для x.

215. 1) Для произвольного $a \in K$ рассмотрим множество $aK = \{ax : x \in K\}$. Поскольку K конечно и не содержит делителей нуля, то $aK = K$ и найдется такой элемент x, что $ax = a$. Докажем, что x — правая единица. Поскольку $Ka = K$, то для произвольного $b \in K$ найдется такой y, что $b = ya$. Тогда $bx = (ya)x = y(ax) = ya = b$. Аналогично доказывается, что K содержит левую единицу.

2) Элемент a, обратимый справа, не является правым делителем нуля, поэтому $Ka = K$, следовательно, существует элемент x такой, что $xa = 1$, т. е. a обратим и слева.

3) Пусть a — левый делитель нуля, т. е. $ab = 0$ для некоторого $b \neq 0$. Предположив, что a не является правым делителем нуля, имеем $Ka = K$ и $xa = 1$ для некоторого $x \in K$. Но тогда $b = (xa)b = 0$ — противоречие.

216. Если $xy = 1$, то $(yx - 1)y = 0$, следовательно, $yx = 1$.

217. 2) См. № 216.

4) $(1 + xy)^{-1} = 1 - x(1 + yx)^{-1}y$

222. *Указание.* Используйте № 220.

224. 1) $x = 1$, $y = 0$, $z = 0$.

2) $x = 1 + t$, $y = t$, $z = t$, где $t \in \mathbb{Z}_5$.

225. 1) $x = 0$, $y = 3$, $z = 1$.

2) Система не совместна.

226. 1) $x^2 + 1$.

2) 1.

227. 1) 1.

2) $x + 1$.

3) 1.

228. 1) $x^2 + 2x$.

2) $x^3 + x + 3$.

3) $x^3 + 2x + 4$.

4) $x - 1$.

229. $p^m(p - 1)$.

230. 1) x^2, $x^2 + 1 = (x + 1)^2$, $x^2 + x = x(x + 1)$, $x^2 + x + 1$ — неприводимый.

2) x^3, $x^3+1=(x+1)(x^2+x+1)$, $x^3+x=x(x+1)^2$, x^3+x+1 неприводим, $x^3+x^2=x^2(x+1)$, x^3+x^2+1 неприводим, $x^3+x^2+x=x(x^2+x+1)$, $x^3+x^2+x+1=(x+1)^3$.

231. 1) x^2+1, x^2+x+2, x^2+2x+2.

2) x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+2x^2+1, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+x+1, x^3+2x^2+2x+2.

232. 1) $(x+1)^3(x^2+x+1)$.

2) $(x^2+1)(x^3+2x^2+2x+2)$.

3) $(x+1)(x^2+2x+4)(x^2+4x+2)$.

233. 1) $(x+1)x^2(x^2+1)$.

2) $(x+1)(x^2+4x+2)(x^2+x+2)$.

3) $(x+1)(x^2+x+3)(x^2+6x+3)$.

4) $(x+1)(x^4-2x^2+9)$.

234. Над $\mathbb{Q}$ многочлен неприводим.

235. 2) Многочлены x и $x+p$ взаимно просты над $\mathbb{Q}$, но не являются таковыми над $\mathbb{Z}_p$.

236. 2) Многочлен $px^2+(p+1)x+1=(x+1)(px+1)$ приводим над $\mathbb{Q}$, но над $\mathbb{Z}_p$ равен $x+1$ и, следовательно, неприводим.

3) Докажем, что x^4+1 приводим над $\mathbb{Z}_p$ при любом простом p. Так как

$$x^4+1=x^4-(-1)=(x^2+1)^2-2x^2=(x^2-1)^2-(-2)x^2,$$

то достаточно доказать, что одно из чисел: -1, 2 или -2 — является квадратом в $\mathbb{Z}_p$. Однако если ни 2, ни -2 не является квадратом в $\mathbb{Z}_p$, то, согласно № 137, квадратом является их произведение $2\cdot(-2)=4\cdot(-1)$, и, следовательно, квадратом является -1.

237. x^4+x^3+x+1.

238. 1) 4, 7; 2) нет решений; 3) 3, 4; 4) 10 (двукратный корень); 5) нет решений;

6) 2; 7) все ненулевые элементы (по малой теореме Ферма);

8) при любом a единственное решение.

239. 1) все элементы поля (малая теорема Ферма); 2) a.

240. 1) Не является подгруппой аддитивной группы.

2) Идеал.

3) Подкольцо, но не идеал.

4) Подкольцо, но не идеал.

5) Подгруппа аддитивной группы, но не подкольцо.

6) Идеал.

7) Подкольцо, но не идеал.

8) Идеал.

9) Идеал.

243. *Указание.* Воспользуйтесь тем, что для ненулевой матрицы X найдутся такие матрицы A и B, что $AXB=E_{11}+\ldots+E_{rr}$, где E_{ii} — матрица, у которой элемент, находящийся на пересечении i-й строки и i-го столбца равен единице, а остальные элементы нулевые.

244. *Указание.* Используя факт, что $E_{ii}AE_{jj}=a_{ij}E_{ij}$, вывести, что множество элементов всех матриц из идеала кольца $K^{n\times n}$ образует идеал в K.

245. Каждый идеал образуют все матрицы вида $\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}$, где элементы a_k образуют в $\mathbb{Z}$ идеал I_k ($k=1,2,3$), причем $I_1\subseteq I_2$ и $I_3\subseteq I_2$.

246. Нулевой идеал, всё кольцо, все матрицы с нулевым первым (вторым) столбцом, все матрицы с одинаковыми столбцами.

248. *Указание.* Рассмотреть идеал, порожденный элементом $a \neq 0$. Наличие единицы существенно. Рассмотрим кольцо с нулевым умножением, аддитивная группа которого является циклической простого порядка. Такое кольцо не имеет нетривиальных идеалов, но полем не является.

249. *Указание.* Доказать, что полные правые делители нуля (т. е. элементы $a \in K$, для которых $Ka = 0$) образуют левый идеал и поэтому не могут быть отличными от нуля. Если же $ba \neq 0$, то $Ka = K$. Вывести отсюда, что в K нет делителей нуля и отличные от нуля элементы кольца образуют группу по умножению.

252. Не является полем.

253. 1) Изоморфно полю $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$.

2) Изоморфно полю $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : \ a, b, c, d \in \mathbb{Q}\}$.

254. 1) Кольцо из 4 элементов. Не является полем.

2) Поле из 9 элементов.

255. Поле из p^n элементов.

258. 1) Фактор-кольцо $\mathbb{Z}_4[x]/I = \{(ax + b) + I \ : \ a, b \in \mathbb{Z}_4\}$. Группа обратимых элементов $G = \{1 + I, 3 + I, (2x + 1) + I, (2x + 3) + I, x + I, (x + 2) + I, 3x + I, (3x + 2) + I\}$.

259. 1) $\varphi n = 0$;

2) $\varphi n = n$ и $\varphi n = 0$;

3) $\varphi n = 0$;

4) $\varphi n = ne_i$, где e_i — идемпотент в кольце матриц; всего восемь гомоморфизмов, соответствующих идемпотентам 0, E, E_{11}, E_{22}, $E_{11} + E_{12}$, $E_{21} + E_{22}$, $E_{11} + E_{21}$, $E_{12} + E_{22}$.

260. $2^{\omega(n) - \omega(n/\text{НОД}(m,n))}$, где $\omega(a)$ — число различных простых делителей числа a.

261. Докажем, что $\mathbb{Z}_m \cong K$, где $K = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \mathbb{Z}_{m_s}$. Для этого рассмотрим гомоморфизм $\varphi : \ \mathbb{Z} \to K$, определяемый формулой

$$\varphi x = (x \bmod m_1, \ x \bmod m_2, \ \ldots, \ x \bmod m_s).$$

Так как $m_1, m_2, \ldots, m_s$ — попарно взаимно простые, то $\operatorname{Ker} \varphi = n\mathbb{Z}$.

Покажем теперь, что $\operatorname{Im} \varphi = K$. Существуют разные доказательства, например, на основе принципа ящиков Дирихле. Приведем другое. Рассмотрим произвольный $r = (r_1, r_2, \ldots, r_s) \in K$ и покажем, что для него найдется x, такой, что $\varphi x = r$. Пусть

$$\alpha_i = \left(\frac{m}{m_i}\right)^{\varphi(m_j)} \qquad (j = 1, 2, \ldots, s).$$

По теореме Эйлера (см. № 119),

$$\alpha_i \equiv 1 \ (\text{mod } p_i), \quad \alpha_i \equiv 1 \ (\text{mod } p_j) \quad (i \neq j),$$

поэтому в качестве x можно взять

$$x = \alpha_1 r_1 + \alpha_2 r_2 + \ldots + \alpha_s r_s.$$

Теперь по теореме о гомоморфизме получаем $\mathbb{Z}_m \cong \operatorname{Im} \varphi = K$.

262. 1) Целостное кольцо.

2) Целостное кольцо.

3) Целостное тогда и только тогда, когда $n = \pm 1$.

4) Целостное кольцо.

5) Целостное кольцо (вытекает из предыдущего).
6) Целостное тогда и только тогда, когда n — простое.
7) Не является целостным кольцом.

264. 1) В качестве нормы взять модуль числа.
2) В качестве нормы взять степень многочлена.
3) *Указание.* В качестве $N(a)$ взять $|a|^2$. Для доказательства возможности деления с остатком в качестве q взять целое гауссово число, ближайшее к a/b.

265. *Указание.* Разделить a на ab с остатком.

267. *Указание.* Использовать алгоритм Евклида.

270. *Указание.* Использовать № 268.

271. *Указание.* Для доказательства единственности разложения воспользоваться № 270 (1).

272. $2 = (1+i)(1-i) = -i(1+i)^2$, 3 — простое, $4 = -(1+i)^4$, $5 = (1+2i)(1-2i)$.

273. $6 = 2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$.

274. В указанных кольцах есть числа, допускающие по два разложения на простые:
1) $10 = 2 \cdot 5 = (1+i\sqrt{3})(1-i\sqrt{3})$.
2) $6 = 2 \cdot 3 = -(4+\sqrt{10})(4-\sqrt{10})$.

276. *Указание.* В идеале I разделить произвольный элемент на минимальный.

277. 1) Является факториальным кольцом согласно теореме Гаусса: если K — факториальное кольцо, то $K[x]$ также является факториальным кольцом.
2) Не является кольцом главных идеалов. Например, идеал $(2, x)$, состоящий из всех многочленов с четным свободным членом, не является главным.
3) Не является евклидовым кольцом.

278. Пусть $K[x]$ — кольцо главных идеалов. Для произвольного ненулевого элемента $a \in K$ рассмотрим идеал $I = \langle x, a\rangle$. Поскольку I – главный идеал и $a \in K$, то $I = \langle b\rangle$ для некоторого $b \in K$. Так как $x \in I$, то $x = (dx)b$ для некоторого $d \in K$. Следовательно, $bd = 1$ и $d = b^{-1} \in K$, поэтому по определению идеала $1 = db \in I$ и $I = K[x]$. Таким образом, $1 = u(x)x + v(x)a$, $u(x), v(x) \in K[x]$ и $1 = v(0)a$, т. е. элемент a обратим. Следовательно, K — поле.

279. 1) Является факториальным кольцом согласно теореме Гаусса.
2) Не является кольцом главных идеалов. Например, идеал (x, y), состоящий из всех многочленов без свободного члена, не является главным.
3) Не является евклидовым кольцом.

280. *Указание.* Доказать, что $(a, b) = (d)$, где $d = \text{НОД}\,\{a, b\}$.

284. Степень расширения равна степени многочлена $f(x)$.

286. 1) *Указание.* Рассмотреть $F[x]/(p(x))$, где $p(x)$ — неприводимый множитель многочлена $f(x)$.

289. 1) *Указание.* Рассмотреть гомоморфизм $\varphi:\ F[x] \to L$, заданный формулой $\varphi(g(x)) = g(\alpha)$. Доказать, что $\operatorname{Im}\varphi = F(\alpha)$, и воспользоваться теоремой о гомоморфизме.

292. 1) $x^4 - 14x^2 + 39$;
2) $x^3 - 3x^2 - 3x - 1$;
3) $x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$.

293. $x^2 - 6x + 13$.

294. Очевидно, что элементы поля F алгебраичны над F. Пусть α и β — два алгебраических над F элемента с минимальными многочленами

$$f(x) = x^m + \sum_{i=0}^{m-1} f_i x^i \quad \text{и} \quad g(x) = x^n + \sum_{i=0}^{n-1} g_i x^i$$

соответственно. Тогда $\alpha^m = -\sum\limits_{i=0}^{m-1} f_i\alpha^i$, $\beta^n = -\sum\limits_{i=0}^{n-1} g_i\beta^i$. Рассмотрим вектор

$$v = (1, \alpha, \ldots, \alpha^{m-1}, \beta, \alpha\beta, \ldots, \alpha^{m-1}\beta, \ldots, \beta^{n-1}, \alpha\beta^{n-1}, \ldots, \alpha^{m-1}\beta^{n-1})^\top.$$

Нетрудно видеть, что существуют матрицы A и B с коэффициентами из F такие, что $Av = \alpha v$, $Bv = \beta v$. Далее $(A+B)v = (\alpha+\beta)v$, $(AB)v = \alpha\beta v$. Таким образом, элементы $\alpha+\beta$ и $\alpha\beta$ являются собственными числами матриц $A+B$ и AB соответственно, поэтому они являются корнями их характеристических многочленов, следовательно, $\alpha+\beta$ и $\alpha\beta$ алгебраичны над F. Осталось доказать, что α^{-1} алгебраичен над F, если $\alpha \neq 0$. Разделив обе части равенства

$$\alpha^m + \sum_{i=0}^{m-1} f_i\alpha^i = 0$$

на $f_0\alpha^m$ ($f_0 \neq 0$, поскольку $f(x)$ неприводим), получим

$$f_0^{-1} + \sum_{i=1}^{m-1} f_0^{-1} f_i (\alpha^{-1})^{m-i} + (\alpha^{-1})^m = 0,$$

что доказывает алгебраичность элемента α^{-1}.

295. Рассмотрим произвольный многочлен, коэффициенты которого — алгебраические числа. Над полем комплексных чисел он раскладывается на линейные множители и, следовательно, каждый его комплексный корень является алгебраическим числом.

299. 1) 0; 2) p; 3) p.

300. Да. Например, поле частных над кольцом $\mathbb{Z}_p[x]$ (см. № 204).

304. *Указание.* Рассмотреть мультипликативную группу поля и воспользоваться № 117.

306. *Указание.* Воспользоваться тем, что F является линейным пространством над полем из p элементов.

308. *Указание.* Воспользоваться № 304.

309. Рассмотрим поле L разложения многочлена $f(x) = x^q - x \in \mathbb{Z}_p[x]$. Так как $f'(x) = -1$, то $f(x)$ и $f'(x)$ взаимно просты и $f(x)$ не имеет кратных корней. Рассмотрим $F = \{\alpha_1, \alpha_2, \ldots, \alpha_q\} \subseteq L$ — множество всех корней этого многочлена. Имеем тождества

$$(a+b)^q = a^q + b^q, \quad (ab)^q = a^q b^q, \quad (a^{-1})^q = (a^q)^{-1},$$

справедливые для любых a и b из F (первое равенство следует из № 302 (1), так как $q = p^n$, а характеристика поля L равна p), откуда получаем, что F — поле. Оно содержит $q = p^n$ элементов.

310. Предположим, что F_1 и F_2 — два поля порядка p^n. Для некоторого $\alpha \in F_1$ имеем $F_1 = \mathbb{Z}_p(\alpha)$. Аналогично, для некоторого $\beta \in F_1$ имеем $F_2 = \mathbb{Z}_p(\beta)$. $F_1 = \mathbb{Z}_p(\alpha)$ и $F_2 = \mathbb{Z}_p(\beta)$ являются (минимальными) полями разложения многочлена $f(x) = x^{p^n} - x$, поэтому, согласно № 291, эти поля изоморфны.

311. Приведем два доказательства. 1-*е доказательство*. Согласно № 93, порядок любого элемента группы G делит $m = \max\limits_{g\in G} |g| = |g_0|$. Таким образом, $g^m = e$ для всех $g \in G$. Поскольку уравнение $x^m = e$ в поле имеет не более m корней, то $|G| \leq m$. С другой стороны, $m \leq |G|$, поскольку порядок любого элемента в группе не превосходит числа элементов группы. Поэтому $m = |G|$ и элемент g_0 порядка m является порождающим в G.

2-*е доказательство*. Пусть $|G| = n$ и $g \in G$, $|g| = d$, тогда d — делитель числа n и $\{x : x^d - 1 = 0\} = \{1, g, g^2, \ldots, g^{d-1}\} = (g)$. Но все элементы подгруппы G порядка d удовлетворяют равенству $x^d - 1 = 0$ и, следовательно, принадлежат (g), поэтому количество элементов порядка d в G равно $\varphi(d)$. Отсюда получаем, что

$$\sum_{d \in A} \varphi(d) = n,$$

где $A = \{|a| : a \in G\}$. Но так как любой элемент в A есть делитель числа n и

$$\sum_{d|n} \varphi(d) = n,$$

то A содержит все такие делители, и, в частности, $n \in A$.

313. Для простых чисел вида $8k \pm 3$ и только для них.

314. Согласно № 311 группа $\mathbb{Z}_p^*$ циклическая. Пусть a_0 — порождающий элемент этой группы. Поскольку $a_0^{p^{m-1}} \equiv a_0 \pmod{p}$, то целое число $a = a_0^{p^{m-1}}$ также является порождающим элементом в $\mathbb{Z}_p^*$. С другой стороны, $a^{p-1} = a_0^{p^{m-1}(p-1)} = a_0^{\varphi(p^m)} \equiv 1 \pmod{p^m}$. Значит, смежный класс $\overline{a} = a + \mathbb{Z}_{p^m}$ порождает в $\mathbb{Z}_{p^m}^*$ циклическую подгруппу порядка $p - 1$. Далее,

$$(1+p)^p = \sum_{i=0}^{p} \binom{p}{i} p^i = 1 + p^2 + \frac{1}{2}(p-1)p^3 + \sum_{i \geq 3} \binom{p}{i} p^i.$$

Так как $p > 2$, то $(1+p)^p \equiv 1+p^2 \pmod{p^3}$. Предположив по индукции, что $(1+p)^{p^j} \equiv 1+p^{j+1} \pmod{p^{j+2}}$, мы находим

$$(1+p)^{p^{j+1}} = \left(1 + (1+sp)p^{j+1}\right)^p = \sum_{i=0}^{p} \binom{p}{i} (1+sp)^i p^{(j+1)i} =$$

$$= 1 + (1+sp)p^{j+2} + \frac{1}{2}(p-1)(1+sp)^2 p^{2(j+1)+1} + \ldots,$$

откуда

$$(1+p)^{p^{j+1}} \equiv 1 + p^{j+2} \pmod{p^{j+3}}.$$

В частности,

$$(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m},$$

но

$$(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \pmod{p^m}$$

и поэтому $(1+p)^{p^{m-2}}$ не сравнимо с 1 по модулю p^m, и, стало быть, смежный класс $\overline{b} = 1+p+\mathbb{Z}_{p^m}$ с представителем $b = 1+p$ порождает в $\mathbb{Z}_{p^m}^*$ циклическую группу порядка p^{m-1}. Согласно № 91 элементы $\overline{a}$, $\overline{b}$ взаимно простых порядков $p-1$, p^{m-1} порождают циклическую группу порядка $p^{m-1}(p-1) = \varphi(p^m) = |\mathbb{Z}_{p^m}^*|$.

Литература

1. *Белоногов В. А.* Задачник по теории групп. — М.: Наука, 2000. — 239 с.
2. *Винберг Э. Б.* Курс алгебры. — 2-е изд., испр. и доп. — М.: Факториал Пресс, 2001. — 544 с.
3. *Курош А. Г.* Курс высшей алгебры. — М.: Наука, 1971. — 432 с.
4. *Ляпин Е. С., Айзенштат А. Я., Лесохин М. М.* Упражения по теории групп. — М.: Наука, 1967. — 264 с.
5. *Окунев Л. Я.* Сборник задач по высшей алгебре. — М.: Просвещение, 1964. — 184 с.
6. *Фаддеев Д. К.* Лекции по алгебре. — М.: Наука, 1984. — 416 с.
7. *Фаддеев Д. К., Соминский И. С.* Сборник задач по высшей алгебре. — М.: Наука, 1977. — 288 с.
8. *Dummit D. S., Foote R. M.* Abstract Algebra. — 3 ed. — Wiley, 2004. — 945 p.