Министерство образования Республики Беларусь

Учреждение образования

«Гомельский государственный университет имени Франциска Скорины»

В. С. МОНАХОВ, Д. А. ХОДАНОВИЧ

ТЕОРИЯ ГРУПП

Практическое пособие

для студентов специализации «Алгебра и теория чисел»
математического факультета
специальности 1-31 03 01 «Математика»

Гомель
ГГУ им. Ф. Скорины
2014

УДК 512.542(075.8)
ББК 22.14я73
М 77

Рецензенты:
доктор физико-математических наук, профессор В. Н. Тютянов;
кандидат физико-математических наук А. А. Трофимук;
кафедра алгебры и геометрии учреждения образования
«Гомельский государственный университет им. Ф. Скорины»

Рекомендовано к изданию научно-методическим советом учреждения образования «Гомельский государственный университет имени Франциска Скорины»

Монахов, В. С.
М 77 Теория групп : практ. пособие / В. С. Монахов, Д. А. Ходанович ; М-во образования РБ, Гом. гос. ун-т им. Ф. Скорины. — Гомель: ГГУ им. Ф. Скорины, 2014. — 40 с.
ISBN 978-985-439-888-4

Пособие составлено в дополнение к учебному пособию В. С. Монахова «Введение в теорию конечных групп и их классов» для методического обеспечения индивидуальных занятий по спецкурсу «Теория групп», который читается в рамках специализации «Алгебра и теория чисел».

Адресовано студентам-математикам как для изучения общего курса «Алгебра и теория чисел», так и для освоения начальных фрагментов современной теории групп.

УДК 512.542(075.8)
ББК 22.14я73

ISBN 978-985-439-888-4

Содержание

Предисловие

При изучении дисциплин математических специализаций в рамках университетского образования необходимо ориентировать будущего специалиста на активную индивидуальную работу. Для достижения этой цели в рамках специализации «Алгебра и теория чисел» предлагается настоящее практическое пособие, которое составлено в дополнение к учебному пособию В. С. Монахова «Введение в теорию конечных групп и их классов». Его цель — методическое обеспечение изучения спецкурса «Теория групп».

Данное пособие состоит из шести основных глав, посвященных ключевым разделам начальной теории групп. Каждый раздел содержит вопросы для самоконтроля, индивидуальные задания в пяти вариантах и дополнительные задания, позволяющие студентам в полном объеме усвоить изучаемый материал. Имеется глоссарий, содержащий кроме базовых понятий также и информацию о строении групп малых порядков.

При создании этого учебного издания использованы известные сборники задач по теории групп, а также практический опыт авторов проведения семинарских занятий. При отборе материала преимущество отдавалась задачам о группах, элементами которых являются числа, матрицы, функции, перестановки.

Практическое пособие адресовано студентам математических факультетов университетов для освоения начальных понятий современной теории групп.

Авторы с благодарностью воспримут все отзывы, замечания, пожелания и критические рекомендации.

Монахов Виктор Степанович
Victor.Monakhov@gmail.com

Ходанович Дмитрий Александрович
Hodanovich@gsu.by

Обозначения

Кванторы

$\forall$ — для любого;
$\exists$ — существует.

Числа

p, q — простые числа;
m, n — натуральные числа;
z — комплексное число;
$|z|$ — модуль комплексного числа z.

Множества

$\{\dots\}$ — множество элементов;
$\{\alpha \mid \beta\}$ — множество всех α, для которых выполняется β;
$(X, \circ)$ — множество X с операцией $\circ$;
$X \cap Y$ — пересечение множеств X и Y;
$X \cup Y$ — объединение множеств X и Y;
$X \setminus Y$ — разность множеств X и Y;
$X^* = X \setminus \{0\}$, где X — числовое множество;
$\mathbb{P}$ — множество всех простых чисел;
$\mathbb{N}$ — множество всех натуральных чисел;
$\mathbb{Z}$ — множество всех целых чисел;
$\mathbb{Q}$ — множество всех рациональных чисел;
$\mathbb{R}$ — множество всех действительных чисел;
$\mathbb{R}_+$ — множество всех положительных действительных чисел;
$\mathbb{C}$ — множество всех комплексных чисел;
$m\mathbb{Z}$ — множество целых чисел кратных m;
$\mathbb{Z}_m$ — множество вычетов по модулю m.

Группы

Пусть G — группа. Тогда:
$|G|$ — порядок группы G;
$|x|$ — порядок элемента $x \in G$;
1 — единичный элемент и единичная подгруппа группы G;
$H \le G$ — H является подгруппой группы G;
$H < G$ — H является собственной подгруппой группы G;
$H \lhd G$ — H является нормальной подгруппой группы G;
$|G : H|$ — индекс подгруппы H в группе G;
$C_G(H)$ — централизатор подгруппы H в группе G;
$N_G(H)$ — нормализатор подгруппы H в группе G;
$Z(G)$ — центр группы G;
G' — коммутант группы G;
$\Phi(G)$ — подгруппа Фраттини группы G;
$\langle x \rangle$ — подгруппа, порожденная элементом x;

$\langle X \rangle$ — подгруппа, порожденная множеством X;
$A \times B$ — прямое произведение подгрупп A и B;
$[A]B$ — полупрямое произведение нормальной подгруппы A и подгруппы B;
$[x, y]$ — коммутатор элементов x и y;
E_{p^n} — элементарная абелева группа порядка p^n;
C_n — циклическая группа порядка n;
D_n — диэдральная группа порядка n;
Q_n — группа кватернионов порядка n;
S_n — симметрическая группа степени n;
A_n — знакопеременная группа степени n;
$GL(n, P)$ — полная линейная группа степени n над полем P;
$SL(n, P)$ — специальная линейная группа степени n над полем P;
$PGL(n, P)$ — проективная полная линейная группа степени n над полем P;
$PSL(n, P)$ — проективная специальная линейная группа степени n над P.

Отображения

$\varphi : G \to H$ — отображение группы G в группу H;
$\varphi : x \mapsto y$ — при отображении φ элемент x переходит в y;
$\varphi(x)$ — образ элемента x;
$\varphi^{-1}(y)$ — прообраз элемента y;
$\varphi(G)$ — образ группы G;
$\operatorname{Im}\varphi = \varphi(G)$ — образ гомоморфизма φ;
$\operatorname{Ker}\varphi$ — ядро гомоморфизма φ;
$G \simeq H$ — группы G и H изоморфны.

Греческий алфавит

$\mathrm{A}\,\alpha$	Альфа	$\mathrm{B}\,\beta$	Бета	$\Gamma\,\gamma$	Гамма	$\Delta\,\delta$	Дельта
$\mathrm{E}\,\varepsilon$	Эпсилон	$\mathrm{Z}\,\zeta$	Дзета	$\mathrm{H}\,\eta$	Эта	$\Theta\,\theta$	Тэта
$\mathrm{I}\,\iota$	Йота	$\mathrm{K}\,\kappa$	Каппа	$\Lambda\,\lambda$	Ламбда	$\mathrm{M}\,\mu$	Мю
$\mathrm{N}\,\nu$	Ню	$\Xi\,\xi$	Кси	$\mathrm{O}\,o$	Омикрон	$\Pi\,\pi$	Пи
$\mathrm{P}\,\rho$	Ро	$\Sigma\,\sigma$	Сигма	$\mathrm{T}\,\tau$	Тау	$\Upsilon\,\upsilon$	Ипсилон
$\Phi\,\varphi$	Фи	$\mathrm{X}\,\chi$	Хи	$\Psi\,\psi$	Пси	$\Omega\,\omega$	Омега

1. Группы и их подгруппы

Вопросы для самоконтроля

1. Определение группы с произвольной бинарной алгебраической операцией.

2. Как задать группу?

3. Что значит аддитивная (мультипликативная) группа?

4. Сколько единиц (нулей) в мультипликативной (аддитивной) группе?

5. Сколько противоположных (обратных) имеет элемент в аддитивной (мультипликативной) группе?

6. Что является в аддитивной группе аналогом степени элемента?

7. Определение изоморфизма (мультипликативных) аддитивных групп.

8. Определение изоморфизма, когда одна группа аддитивная, а другая — мультипликативная.

9. Является ли изоморфизм отношением эквивалентности?

10. Является ли мультипликативная группа $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ подгруппой аддитивной группы $\mathbb{R}$?

11. Сформулируйте критерий подгруппы аддитивной группы.

12. В аддитивной группе определите сумму подмножеств и смежный класс.

13. Перечислите свойства смежных классов в аддитивной группе.

Индивидуальные задания

1. Определена ли операция на множестве? Будут ли они группами?

1.1. Операция сложения на

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

1.2. Операция сложения на

$$Q_p = \left\{ \frac{n}{p^m} \mid n \in \mathbb{Z}, m \in \mathbb{N} \right\},$$

p — фиксированное простое число.

1.3. Операция умножения на $S = \{e, (13)(24), (1234), (1432)\}$.

1.4. Операция умножения на $K = \{e, (12)(34), (13)(24), (14)(23)\}$.

1.5. Операция умножения на $L = \{e, (23), (24), (34), (234), (243)\}$.

2. Будет ли подмножество $H \subseteq GL(n, \mathbb{Z}_7)$ подгруппой мультипликативной группы $GL(n, \mathbb{Z}_7)$?

2.1. $n = 4$; $H = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid 1, a, b, c \in \mathbb{Z}_7 \right\}$.

2.2. $n = 4$; $H = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & c & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid 1, a, b, c \in \mathbb{Z}_7 \right\}$.

2.3. $n = 3$; $H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid 1, a, b \in \mathbb{Z}_7 \right\}$.

2.4. $n = 3$; $H = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b & c & 1 \end{pmatrix} \mid 1, b, c \in \mathbb{Z}_7 \right\}$.

2.5. $n = 4$; $H = \left\{ \begin{pmatrix} 1 & a & b & 0 \\ 0 & 1 & c & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid 1, a, b, c \in \mathbb{Z}_7 \right\}$.

3. Будет ли множество $\mathbb{Q}^*$ с указанной операцией $\circ$ группой? Операция $\circ$ коммутативна или нет?

3.1. $a \circ b = 5ab, \quad a, b \in \mathbb{Q}^*$. 3.2. $a \circ b = 2ab, \quad a, b \in \mathbb{Q}^*$.
3.3. $a \circ b = 3ab, \quad a, b \in \mathbb{Q}^*$. 3.4. $a \circ b = 7ab, \quad a, b \in \mathbb{Q}^*$.
3.5. $a \circ b = 4ab, \quad a, b \in \mathbb{Q}^*$.

4. Является ли следующее множество мультипликативной (аддитивной) группой?

4.1. Диагональных $n \times n$-матриц с ненулевыми элементами на диагонали.
4.2. Треугольных $n \times n$-матриц с ненулевыми элементами на диагонали.
4.3. Всех $n \times n$-матриц с нулевыми элементами на диагонали.
4.4. Всех $n \times n$-матриц с определителем, равным 1, -1.
4.5. Всех $n \times n$-матриц с положительным определителем.

5. Будет ли абелевой подгруппой в группе S_4 следующее множество перестановок?

5.1. $\{e$, (12), (13), (23), (123), (132)$\}$.
5.2. $\{e$, (1234), (13)(24), (1432)$\}$.
5.3. $\{e$, (12), (14), (24), (124), (142)$\}$.
5.4. $\{e$, (12)(34), (13)(24), (14)(23)$\}$.

5.5. $\{e, (23), (24), (34), (234), (243)\}$.

6. Составьте таблицу сложения для аддитивной фактор-группы $k\mathbb{Z}$ по подгруппе $t\mathbb{Z}$.

6.1. $k = 2, t = 8$. 6.2. $k = 6, t = 18$.
6.3. $k = 2, t = 6$. 6.4. $k = 5, t = 15$.
6.5. $k = 3, t = 9$.

Дополнительные задания

1. Покажите, что функции

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

определенные на $\mathbb{R}\backslash\{0\}$, с операцией умножения (композиция функций) образуют группу. Постройте таблицу умножения элементов этой группы. Укажите единичный элемент. Для каждого элемента группы найдите обратный.

2. Покажите, что функции

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

$$f_4(x) = \frac{x-1}{x},\ f_5(x) = \frac{x}{x-1},\ f_6(x) = \frac{1}{1-x},$$

определенные на $\mathbb{R}\backslash\{0, 1\}$, с операцией умножения (композиция функций) образуют группу. Укажите единичный элемент. Для каждого элемента группы найдите обратный.

3. Покажите, что функции

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

$$f_5(x) = \frac{x-1}{x+1},\ f_6(x) = \frac{1-x}{x+1},\ f_7(x) = \frac{x+1}{x-1},\ f_8(x) = \frac{x+1}{1-x},$$

определенные на $\mathbb{R}\backslash\{0, \pm 1\}$, с операцией умножения (композиция функций) образуют группу. Укажите единичный элемент. Для каждого элемента группы найдите обратный.

4. Покажите, что совокупность всех аффинных преобразований прямой

$$f_{a,b}(x) = ax + b, \quad a, b \in \mathbb{R}, \quad a \neq 0,$$

с операцией умножения (композиция функций) образуют группу. Укажите единичный элемент и обратные.

5. Покажите, что совокупность всех функций вида

$$f_{a,b,c,d}(x) = \frac{ax+b}{cx+d}, \quad a,b,c,d \in \mathbb{R}, \quad ad \neq bc,$$

с операцией умножения (композиция функций) образуют группу. Укажите единичный элемент и обратные.

6. Пусть M — множество и $S(M)$ — булеан этого множества, т. е. совокупность всех подмножеств. Является ли абелевой группой множество $S(M)$ с операцией Δ, где

$$X\Delta Y = (X \setminus Y) \cup (Y \setminus X), \ X, Y \in S(M)?$$

Если $(S(M), \Delta)$ — группа, то укажите единичный элемент и обратные.

7. Будет ли аддитивной группой множество целых чисел?

8. Будет ли аддитивной группой множество всех четных чисел?

9. Будет ли аддитивной группой множество всех целых чисел, кратных данному натуральному числу n?

10. Будет ли мультипликативной группой множество степеней данного действительного числа a, $a \neq 0$, $a \neq \pm 1$, с целыми показателями?

11. Будет ли аддитивной группой множество неотрицательных целых чисел?

12. Будет ли аддитивной группой множество нечетных целых чисел?

13. Будет ли группой множество целых чисел с операцией вычитания?

14. Будет ли аддитивной группой множество рациональных чисел?

15. Будет ли мультипликативной группой множество рациональных чисел?

16. Будет ли мультипликативной группой множество ненулевых рациональных чисел?

17. Будет ли мультипликативной группой множество положительных рациональных чисел?

18. Будет ли группой множество положительных рациональных чисел с операцией деления?

19. Будет ли аддитивной группой множество рациональных чисел, знаменатели которых являются степенями 2 с целыми неотрицательными показателями?

20. Будет ли аддитивной группой множество всех рациональных чисел, знаменатели которых равны произведениям простых чисел из данного множества M (конечного или бесконечного) с целыми неотрицательными показателями (лишь конечное число которых может быть отлично от нуля)?

21. Будет ли мультипликативной группой множество корней n-й степени из единицы (как действительные, так и комплексные)?

22. Будет ли мультипликативной группой множество корней всех целых положительных степеней из единицы?

23. Будет ли мультипликативной группой множество $n \times n$-матриц с действительными элементами?

24. Будет ли мультипликативной группой множество невырожденных $n \times n$-матриц с действительными элементами?

25. Будет ли мультипликативной группой множество невырожденных $n \times n$-матриц с целыми элементами?

26. Будет ли мультипликативной группой множество $n \times n$-матриц с целыми элементами и определителем, равным единице?

27. Будет ли аддитивной группой множество $n \times n$-матриц с действительными элементами?

28. Будет ли мультипликативной группой множество всех перестановок степени n?

29. Будет ли мультипликативной группой множество всех четных перестановок степени n?

30. Будет ли мультипликативной группой множество всех нечетных перестановок степени n?

31. Будет ли группой множество положительных действительных чисел, если операция задана равенством $a * b = a^b$?

32. Будет ли группой множество положительных действительных чисел, если операция задана равенством $a * b = a^2b^2$?

33. Будет ли аддитивной группой множество действительных многочленов степени $\leq n$ (включая нуль) от неизвестного x?

34. Будет ли аддитивной группой множество действительных многочленов степени n от неизвестного x?

35. Будет ли аддитивной группой множество действительных многочленов любых степеней (включая нуль) от неизвестного x?

2. Циклические группы

Вопросы для самоконтроля

1. Определение порядка элемента группы. Элементы конечного и бесконечного порядков.
2. Определение порядка элемента в аддитивной группе.
3. Конечны ли порядки элементов в конечной группе?
4. Могут ли в группе все элементы иметь бесконечный порядок?
5. Циклическая группа, порожденная элементом конечного порядка.
6. Циклическая группа, порожденная элементом бесконечного порядка.
7. Будут ли равны порядки $|x|$ и $|\langle x\rangle|$, где x — элемент конечной группы?
8. Изоморфизм циклических групп.
9. Подгруппы и фактор-группы бесконечной циклической группы.
10. Подгруппы и фактор-группы конечной циклической группы.
11. Порядок перестановки.
12. Порядки элементов конечной циклической группы.
13. Цикличность группы простого порядка.
14. Абелевость группы порядка p^2, p — простое.

Индивидуальные задания

1. Найдите все элементы циклической подгруппы $\langle g\rangle$ мультипликативной группы $\mathbb{C}^*$.

1.1. $g = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$. 1.2. $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$. 1.3. $g = \frac{1}{2} - \frac{\sqrt{3}}{2}i$.

1.4. $g = \frac{\sqrt{2}}{2} - \frac{1}{\sqrt{2}}i$. 1.5. $g = -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$.

2. Найдите порядок перестановки.

2.1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$. 2.2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} \in S_6$.

2.3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5$. 2.4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 6 & 5 & 1 & 2 & 3 \end{pmatrix} \in S_7$.

2.5. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \in S_5$.

3. В группе $GL(2, \mathbb{C})$ найдите порядки элементов.

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

3.2. $\begin{pmatrix} -i & 0 \\ 1 & i \end{pmatrix}$, $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

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

3.4. $\begin{pmatrix} i & 0 \\ 1 & -i \end{pmatrix}$, $\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.

3.5. $\begin{pmatrix} -i & 1 \\ 0 & i \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} -2+3i & -2+2i \\ 1-i & 3-2i \end{pmatrix}$.

4. В группе $GL(2, \mathbb{Z}_p)$ найдите порядки элементов.

4.1. $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $p = 3$. 4.2. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $p = 5$.

4.3. $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $p = 5$. 4.4. $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$, $p = 3$.

4.5. $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, $p = 3$.

5. Докажите, что порядки указанных элементов мультипликативной группы равны.

5.1. abc и bca. 5.2. a и $b^{-1}a^{-1}b$. 5.3. ab^{-1} и ba^{-1}.
5.4. a и $b^{-1}ab$. 5.5. ab и ba.

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

6.1. $n = 24$, $k = 6$. 6.2. $n = 100$, $k = 5$.
6.3. $n = 24$, $k = 4$. 6.4. $n = 100$, $k = 20$.
6.5. $n = 36$, $k = 4$.

7. Найдите порядок элемента g, принадлежащего мультипликативной группе G. Вычислите g^{100}.

7.1. $g = \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$, $G = GL(2, \mathbb{C})$. 7.2. $g = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$, $G = \mathbb{C}^*$.

7.3. $g = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$, $G = GL(2, \mathbb{C})$. 7.4. $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$, $G = \mathbb{C}^*$.

7.5. $g = -i$, $G = \mathbb{C}^*$.

Дополнительные задания

1. Найдите циклическую подгруппу из S_5, содержащую точно пять элементов.

2. Найдите циклическую подгруппу из S_6, содержащую точно шесть элементов.

3. Найдите порядки всех элементов группы S_n, $n \leq 7$.

4. Докажите, что порядок нечетной перестановки есть четное число.

5. Элементов какого порядка в симметрической группе S_n больше, четного или нечетного?

6. Докажите, что существуют перестановки любого порядка.

7. Докажите, что группа абелева, если в ней все неединичные элементы имеют порядок 2. Кроме того, если группа конечна, то ее порядок равен 2^n.

8. Могут ли в группе существовать точно два элемента порядка 2?

9. Докажите, что в абелевой группе множество элементов, порядки которых делят фиксированное число n, является подгруппой.

10. Если a — элемент группы порядка 5, то сколько различных элементов находится в группе $< a >$? Каковы порядки каждого из этих элементов?

11. Если a — элемент группы порядка 6, то сколько различных элементов находится в группе $< a >$? Каковы порядки каждого из этих элементов?

12. Если a — элемент группы порядка 6, найдите все подгруппы из $< a >$. Из них все циклические?

13. Если a и b — элементы циклической группы, то следует ли равенство $ab = ba$?

14. Если a — элемент группы и a имеет порядок n, что тогда можно сказать о порядке элемента a^{-1}?

15. Аддитивная группа $\mathbb{Z}$ циклическая, порождённая элементом 1. Если H — подгруппа группы $\mathbb{Z}$ и a — наименьшее положительное целое число в H, то докажите, что $H =< a >$.

16. Если a и b — элементы группы, и $ab = ba$, то докажите, что $a^n b = ba^n$ для всех $n \in \mathbb{Z}$.

17. Если a и b — элементы группы, и $ab = ba$, то докажите, что $a^n b^2 = b^2 a^n$ для всех $n \in \mathbb{Z}$.

18. Если a и b — элементы группы, и $ab = ba$, то докажите, что $a^m b^n = b^n a^m$ для любых $m, n \in \mathbb{Z}$.

19. Если a и b — элементы группы, и $(ab)^2 = a^2 b^2$, то докажите, что $ab = ba$.

20. Докажите, что всякая конечная подгруппа мультипликативной группы $\mathbb{C}^*$ циклическая.

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

22. В мультипликативной группе $\mathbb{C}^*$ найдите все элементы 5-го порядка, 6-го порядка.

23. Докажите, что в абелевой группе нечетного порядка каждый элемент является квадратом некоторого элемента.

24. Докажите, что абелева группа порядка, не делящегося на квадрат простого числа, является циклической.

25. Пусть в абелевой группе G все неединичные элементы имеют один и тот же порядок p. Докажите, что:

1) число p простое;

2) группа G разложима в прямое произведение подгрупп порядка p;

3) порядок группы G равен p^n, где n — число сомножителей в прямом произведении;

4) любая неединичная подгруппа является прямым произведением подгрупп порядка p.

3. Линейные группы

Вопросы для самоконтроля

1. Группы $GL(n, \mathbb{P})$, $SL(n, \mathbb{P})$ и $U(n, \mathbb{P})$.
2. Порядки групп $GL(n, p^m)$, $SL(n, p^m)$ и $U(n, p^m)$.
3. Централизатор элемента в группе и централизатор множества.
4. Центры групп $GL(n, \mathbb{P})$ и $SL(n, \mathbb{P})$.
5. Проективная общая и проективная специальная линейные группы и их порядки над конечными полями.
6. Разложение $GL(2, 2^m)$ в прямое произведение центра и $SL(2, 2^m)$.
7. Вложение группы $PSL(2, p^m)$ в $PGL(2, p^m)$ при нечетном p.
8. Теорема о подгруппах группы $PSL(2, p^m)$.
9. Матрица перестановки. Мономорфизм симметрической группы в полную линейную группу.

Индивидуальные задания

1. Укажите каждому элементу поля $\mathbb{Z}_p$ противоположный и обратный. Вычислите произведения $4 \cdot a$ для всех $a \in \mathbb{Z}_p$. Здесь 4 — элемент поля $\mathbb{Z}_p$.

1.1. $p = 17$. 1.2. $p = 5$. 1.3. $p = 11$. 1.4. $p = 13$. 1.5. $p = 7$.

2. Вычислите противоположную и обратную матрицы над полем $\mathbb{Z}_p$ для матрицы A.

2.1. $p = 7$, $A = \begin{pmatrix} 5 & 3 & 2 \\ 1 & 4 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. 2.2. $p = 5$, $A = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 5 & 3 \\ 3 & 4 & 2 \end{pmatrix}$.

2.3. $p = 11$, $A = \begin{pmatrix} 1 & 4 & 3 \\ 2 & 1 & 3 \\ 5 & 3 & 2 \end{pmatrix}$. 2.4. $p = 7$, $A = \begin{pmatrix} 1 & 4 & 3 \\ 2 & 1 & 3 \\ 5 & 3 & 2 \end{pmatrix}$.

2.5. $p = 5$, $A = \begin{pmatrix} 2 & 5 & 3 \\ 3 & 4 & 2 \\ 3 & 2 & 1 \end{pmatrix}$.

3. Найдите порядки центров групп $GL(3, p^m)$, $SL(3, p^m)$.

3.1. $p^m = 13^2$. 3.2. $p^m = 5^3$. 3.3. $p^m = 2^4$.
3.4. $p^m = 11^2$. 3.5. $p^m = 7^3$.

4. Вычислите порядки групп $GL(3, p^m)$, $SL(3, p^m)$, $PGL(3, p^m)$, $PSL(3, p^m)$.

4.1. $p^m = 17^2$. 4.2. $p^m = 3^4$. 4.3. $p^m = 5^3$.

4.4. $p^m = 11^2$. 4.5. $p^m = 2^5$.

5. Перечислите все подгруппы группы $PSL(2, p^m)$.
5.1. $p^m = 13^2$. 5.2. $p^m = 5^3$. 5.3. $p^m = 3^3$.
5.4. $p^m = 11^3$. 5.5. $p^m = 7^2$.

6. Найдите в группе $GL(3, \mathbb{C})$ централизатор матрицы.

6.1. $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. 6.2. $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. 6.3. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

6.4. $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. 6.5. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

7. В группе $GL(2, 7)$ найдите централизатор множества M, его порядок и индекс. Является ли этот централизатор абелевым?

7.1. $M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Z}_7^* \right\}$. 7.2. $M = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \mid a \in \mathbb{Z}_7 \right\}$.

7.3. $M = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}_7 \right\}$. 7.4. $M = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}_7^* \right\}$.

7.5. $M = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & a \end{pmatrix} \mid a \in \mathbb{Z}_7^* \right\}$.

Дополнительные задания

1. Проверьте, что для невырожденной 2×2-матрицы выполняется равенство:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

2. Является ли группой множество матриц

$$SL^{\pm}(2, \mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = \pm 1 \right\}?$$

3. Является ли группой множество всех диагональных матриц

$$D(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}^* \right\}?$$

4. Является ли группой множество матриц

$$A(1,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}^*,\ b \in \mathbb{R} \right\}?$$

5. Является ли группой множество всех верхних треугольных матриц

$$B(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{C}^*,\ b \in \mathbb{C} \right\}?$$

6. Является ли группой множество всех нижних треугольных матриц

$$B^-(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid a, d \in \mathbb{C}^*, c \in \mathbb{C} \right\}?$$

7. Является ли группой множество всех верхних унитреугольных матриц

$$U(2,\mathbb{C}) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{C} \right\}?$$

8. Является ли группой множество всех нижних унитреугольных матриц

$$U^-(2,\mathbb{C}) = \left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \mid c \in \mathbb{C} \right\}?$$

9. Является ли группой множество всех матриц

$$N(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{C}^* \right\} \cup \left\{ \begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix} \mid a, d \in \mathbb{C}^* \right\}?$$

10. Является ли группой множество матриц

$$A(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{C}, a^2 - b^2 \neq 0 \right\}?$$

11. Является ли группой множество матриц

$$A^-(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{C}, a^2 + b^2 \neq 0 \right\}?$$

12. Проверьте, что для любого натурального $m > 1$ множество

$$\left\{ \begin{pmatrix} \pm 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{Z}_m \right\}$$

является группой диэдра порядка $2m$.

13. Проверьте, что группой, изоморфной группе S_3, является следующее множество матриц:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \right\}.$$

14. Проверьте, что группой, изоморфной группе S_3, является следующее множество матриц:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 3 & -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 & 1 \\ -3 & -1 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -3 & -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 & -1 \\ 3 & -1 \end{pmatrix} \right\}.$$

15. Проверьте, что группой, изоморфной группе S_3, является следующее множество матриц:

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

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

16. Проверьте, что группой, изоморфной группе кватернионов Q_8, является следующее множество матриц:

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

17. Докажите, что группы порядка 4 исчерпываются с точностью до изо-

морфизма следующими двумя группами матриц:

$$U = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\},$$

$$V = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \times \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle =$$

$$= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

18. Докажите, что группы порядка 4 исчерпываются с точностью до изоморфизма следующими двумя группами перестановок:

$$U_1 =< (1234) >= \{e, (1234), (13)(24), (1432)\},$$

$$V_1 =< (12)(34) > \times < (13)(24) >= \{e, (12)(34), (13)(24), (14)(23)\}.$$

19. Установите изоморфизмы $U \simeq U_1$, $V \simeq V_1$, где U, V, U_1, V_1 — группы из предыдущих двух заданий.

20. Докажите, что аддитивная группа поля P изоморфна мультипликативной группе матриц вида

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

4. Гомоморфизмы групп

Вопросы для самоконтроля

1. Определение гомоморфизма аддитивной (мультипликативной) группы в аддитивную (мультипликативную).

2. Определение гомоморфизма аддитивной (мультипликативной) группы в мультипликативную (аддитивную).

3. Определение мономорфизма, эпиморфизма, изоморфизма.

4. Определение эндоморфизма, автоморфизма.

5. Определение нулевого эндоморфизма, тождественного автоморфизма.

6. Укажите гомоморфизм, который не является ни мономорфизмом, ни эпиморфизмом.

7. Ядро гомоморфизма и его свойства.

8. Образ гомоморфизма и его свойства.

9. Основная теорема о гомоморфизмах групп.

10. Теорема об изоморфизме.

Индивидуальные задания

1. Пусть n, m, r — фиксированные натуральные числа и

$$f : (n\mathbb{Z}, +) \to (m\mathbb{Z}, +)$$

такое отображение, при котором

$$nk \mapsto rk \text{ для всех } k \in \mathbb{Z}.$$

Докажите, что f — гомоморфизм. Найдите ядро и образ f. Будет ли f мономорфизмом, эпиморфизмом, изоморфизмом?

1.1. $n = 2, m = 3, r = 3$. 1.2. $n = 3, m = 6, r = 12$.
1.3. $n = 3, m = 2, r = 4$. 1.4. $n = 2, m = 2, r = 6$.
1.5. $n = 1, m = 2, r = 4$.

2. Докажите, что данные отображения являются гомоморфизмами групп. Найдите ядро и образ.

2.1. $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$, $f(a) = e^a$, $\forall a \in \mathbb{R}$. Здесь e — основание натурального логарифма.

2.2. $f : (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$, $f(a) = \ln a$, $\forall a \in \mathbb{R}^*$.

2.3. $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$, $f(a) = \text{sign } a$, $\forall a \in \mathbb{R}^*$.

2.4. $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$, $f(a) = |a|$, $\forall a \in \mathbb{R}^*$.

2.5. $f : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot)$, $f(a) = |a|$, $\forall a \in \mathbb{C}^*$.

3. Пусть f — отображение группы $(M,*)$ в группу $(N,\cdot)$. Будет ли f мономорфизмом, эпиморфизмом, изоморфизмом? Если f — гомоморфизм, то найдите $\mathrm{Ker} f$ и $\mathrm{Im} f$.

3.1. $*$ и $\cdot$ — умножение,

$$M = \left\{ \begin{pmatrix} a & 5b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{Q},\ a^2+b^2>0 \right\},$$

$$N = \{a+b\sqrt{5} \mid a,b \in \mathbb{Q},\ a^2+b^2>0\},$$

$$f : \begin{pmatrix} a & 5b \\ b & a \end{pmatrix} \mapsto a+b\sqrt{5}.$$

3.2. $*$ и $\cdot$ — сложение,

$$M = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{Z} \right\}, \quad N = \mathbb{Z},$$

$$f : \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mapsto 4a+4b.$$

3.3. $*$ и $\cdot$ — умножение,

$$M = \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{Q},\ a^2+b^2>0 \right\},$$

$$N = \{a+b\sqrt{3} \mid a,b \in \mathbb{Q},\ a^2+b^2>0\},$$

$$f : \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mapsto a+b\sqrt{3}.$$

3.4. $*$ и $\cdot$ — сложение,

$$M = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{Z} \right\}, \quad N = \mathbb{Q},$$

$$f : \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mapsto a-b.$$

3.5. $*$ и $\cdot$ — умножение,

$$M = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a,b \in \mathbb{Q}^* \right\}, \quad N = \mathbb{R}^*,$$

$$f : \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto ab.$$

4. Пусть $f : G \to H$ — гомоморфизм мультипликативной группы G в аддитивную группу H. Докажите следующие утверждения.

4.1. Если 1 — единичный элемент группы G, то $f(1)$ — нулевой элемент группы H.

4.2. Если $a \in G$, то $f(a^{-1}) = -f(a)$.

4.3. Если G_1 — подгруппа группы G, то $f(G_1) = \{f(a) \mid a \in G_1\}$ — подгруппа группы H.

4.4. Если G — абелева группа, то $\mathrm{Im}\ f = \{f(x) \mid x \in G\}$ — абелева подгруппа группы H.

4.5. Если G — циклическая группа, то $\mathrm{Im}\ f = \{f(x) \mid x \in G\}$ — циклическая подгруппа группы H.

5. Пусть $f : G \to H$ — эпиморфизм аддитивной группы G на мультипликативную группу H. Докажите следующие утверждения.

5.1. Порядок G делится на порядок H.

5.2. Если H — неабелева группа, то G — неабелева.

5.3. Если $a \in G$, то $|f(a)|$ делит $|a|$.

5.4. Если $a \in G$, то $f(-a) = f(a^{-1})$.

5.5. Если 0 — нулевой элемент группы G, то $f(0)$ — единичный элемент группы H.

6. Пусть m и n — натуральные числа. Найдите все гомоморфизмы циклической группы порядка m в циклическую группу порядка n.

6.1. $m = 4$, $n = 8$. 6.2. $m = 8$, $n = 4$. 6.3. $m = 6$, $n = 12$.

6.4. $m = 7$, $n = 5$. 6.5. $m = 12$, $n = 6$.

7. Является ли отображение $f : \mathbb{C}^* \to \mathbb{R}^*$ гомоморфизмом мультипликативной группы $\mathbb{C}^*$ в мультипликативную группу $\mathbb{R}^*$?

7.1. $f(z) = |z|$. 7.2. $f(z) = |z|^2$. 7.3. $f(z) = \frac{|z|}{2}$.

7.4. $f(z) = \frac{1}{|z|}$. 7.5. $f(z) = \frac{3}{|z|}$.

8.1. Докажите, что отображение

$$\det : GL(2, \mathbb{R}) \to (\mathbb{R}^*, \cdot),\ a \mapsto \det\ a,\ \forall a \in GL(2, \mathbb{R}),$$

является эпиморфизмом. Найдите ядро. Докажите изоморфизм

$$GL(2, \mathbb{R})/SL(2, \mathbb{R}) \simeq (\mathbb{R}^*, \cdot).$$

8.2. Пусть $SL^{\pm}(2, \mathbb{Q})$ — множество всех 2×2-матриц над полем $\mathbb{Q}$ с определителем ± 1, а $(\mathbb{Q}_+, \cdot)$ — мультипликативная группа положительных рациональных чисел. Проверьте, что $SL^{\pm}(2, \mathbb{Q})$ является нормальной подгруппой группы $GL(2, \mathbb{Q})$. Докажите изоморфизм

$$GL(2, \mathbb{Q})/SL^{\pm}(2, \mathbb{Q}) \simeq (\mathbb{Q}_+, \cdot).$$

8.3. Пусть K — множество всех 2×2-матриц над полем $\mathbb{R}$ с положительным определителем. Проверьте, что K является нормальной подгруппой группы $GL(2, \mathbb{R})$. Докажите изоморфизм

$$GL(2, \mathbb{R})/K \simeq (\{1, -1\}, \cdot).$$

8.4. Пусть L — множество всех 2×2-матриц над полем $\mathbb{C}$ с определителем, по модулю равным 1, а $(\mathbb{R}_+, \cdot)$ — мультипликативная группа положительных действительных чисел. Проверьте, что L является нормальной подгруппой группы $GL(2, \mathbb{C})$. Докажите изоморфизм

$$GL(2, \mathbb{C})/L \simeq (\mathbb{R}_+, \cdot).$$

8.5. Пусть S — множество всех 2×2-матриц над полем $\mathbb{C}$ с положительным действительным определителем, а $\mathbb{C}_1$ — множество всех комплексных чисел, по модулю равных единице. Проверьте, что S является нормальной подгруппой группы $GL(2, \mathbb{C})$, а $\mathbb{C}_1$ с умножением — группа. Докажите изоморфизм

$$GL(2, \mathbb{C})/S \simeq (\mathbb{C}_1, \cdot).$$

Дополнительные задания

1. Найдите все пары (m, n) целых чисел, при которых отображение

$$x \mapsto mx^n, \ \forall x \in \mathbb{Q}^*,$$

является эндоморфизмом мультипликативной группы $\mathbb{Q}^*$.

2. Пусть S — множество всех комплексных чисел из мультипликативной группы $\mathbb{C}^*$, лежащих на действительной и мнимой осях, а $\mathbb{C}_1$ — мультипликативная группа всех комплексных чисел с модулем, равным 1. Докажите, что S — нормальная подгруппа и $\mathbb{C}^*/S \simeq \mathbb{C}_1$.

3. Докажите, что аддитивная группа целых чисел не является эпиморфным образом аддитивной группы рациональных чисел.

4. Докажите изоморфизм мультипликативных групп

$$\mathbb{C}^* \simeq \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}, \ a^2 + b^2 > 0 \right\}.$$

5. Следующий набор групп разбейте на классы попарно изоморфных групп: $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Z}, +)$, $(m\mathbb{Z}, +)$, $m \in \mathbb{N}$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

6. Найдите группы автоморфизмов циклической группы порядка 5, циклической группы порядка 6.

7. Докажите, что группа всех автоморфизмов циклической группы абелева.

8. Докажите, что группа автоморфизмов конечной циклической группы простого порядка p является конечной циклической группой порядка $p-1$.

9. Докажите, что группа H тогда и только тогда является гомоморфным образом конечной циклической группы G, когда H также циклическая и $|H|$ делит $|G|$.

10. Докажите, что не существует группы, у которой группа автоморфизмов является конечной циклической группой нечетного порядка.

11. Докажите, что группа автоморфизмов бесконечной циклической группы является конечной группой порядка 2.

12. Докажите, что группа автоморфизмов конечной абелевой нециклической группы не является абелевой группой.

13. Докажите, что группа автоморфизмов неабелевой группы не может быть циклической группой.

14. Докажите, что группа автоморфизмов группы S_3 изоморфна S_3.

15. Докажите, что группа автоморфизмов группы S_4 изоморфна S_4.

16. Докажите, что фактор-группа S_n/A_n изоморфна аддитивной фактор-группе $\mathbb{Z}/2\mathbb{Z}$.

17. Пусть G — абелева группа и $f(a) = a^2$, $\forall a \in G$. Будет ли $f : G \to G$ гомоморфизмом, мономорфизмом, автоморфизмом?

18. Пусть G — абелева группа и $f(a) = a^{-1}$, $\forall a \in G$. Будет ли $f : G \to G$ гомоморфизмом, мономорфизмом, автоморфизмом?

19. Докажите, что группа автоморфизмов нециклической группы порядка 4 изоморфна S_3.

20. Докажите, что если центр группы G равен 1, то центр ее группы автоморфизмов также равен 1.

21. Пусть G и H — группы взаимно простых порядков и отображение $f : G \to H$ — гомоморфизм. Докажите, что $\mathrm{Ker}\, f = G$.

22. Докажите, что аддитивная группа $\mathbb{Z}$ целых чисел эпиморфно отображается на конечную циклическую группу $< a >$ порядка n, если положить $f : k \mapsto a^k$, $\forall k \in \mathbb{Z}$. Найдите ядро этого эпиморфизма.

23. Пусть группа G обладает автоморфизмом f порядка 2 без неподвижных точек, т. е. $f(x) \neq x$, $\forall x \in G \setminus \{1\}$. Докажите, что G — абелева группа нечетного порядка.

24. Пусть $(G, \cdot)$ — мультипликативная группа и $t \in G$ — фиксированный элемент. На множестве G введем новую операцию $*$ полагая $a * b = atb$. Докажите, что $(G, *)$ — группа, изоморфная группе $(G, \cdot)$.

25. Найдите все изоморфизмы групп $(\mathbb{Z}_4, +)$ и $(\mathbb{Z}_5, \cdot)$.

26. Зафиксируем рациональное число $t \neq 0$. Докажите, что отображение $f : x \mapsto xt$, $\forall x \in \mathbb{Q}$, является автоморфизмом аддитивной группы $(\mathbb{Q}, +)$.

5. Центр и коммутант

Вопросы для самоконтроля

1. Коммутатор элементов, коммутант группы.
2. Коммутант и нормальная подгруппа с абелевой фактор-группой.
3. Коммутант фактор-группы.
4. n–ый коммутант группы, n–ый коммутант фактор-группы.
5. Разрешимые группы. Примеры разрешимых групп.
6. Подгруппы и фактор-группы разрешимых групп.
7. Прямые произведения разрешимых групп.
8. Теорема о разрешимости группы с разрешимой нормальной подгруппой и разрешимой фактор-группой по ней.
9. Центр группы и его свойства.
10. Абелевость группы с циклической фактор-группой по центру.

Индивидуальные задания

1. В группе $GL(2, \mathbb{Z}_5)$ найдите коммутаторы матриц

$$x = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ y = \begin{pmatrix} 1 & 2 \\ 4 & 4 \end{pmatrix},\ z = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}.$$

1.1. $[x, y]$, $[x^{-1}, y]$. 1.2. $[x, z]$, $[x, z^{-1}]$. 1.3. $[y, z]$, $[y^{-1}, z]$.
1.4. $[z, x]$, $[x^{-1}, z]$. 1.5. $[z, y]$, $[z^{-1}, y]$.

2. В группе $GL(3, \mathbb{C})$ найдите коммутаторы матриц

$$u = \begin{pmatrix} i & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix},\ v = \begin{pmatrix} i & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\ w = \begin{pmatrix} 0 & 0 & i \\ 0 & 2 & 0 \\ 3 & 0 & 0 \end{pmatrix}.$$

2.1. $[u, v]$. 2.2. $[u, w]$. 2.3. $[v, w]$. 2.4. $[w, u]$. 2.5. $[v, u]$.

3. В симметрической группе S_4 для элементов

$$\tau_1 = (12),\ \tau_2 = (123),\ \tau_3 = (1234),\ \tau_4 = (13)(24)$$

найти коммутаторы α и β и пересечение централизаторов этих коммутаторов.
3.1. $\alpha = [\tau_1, \tau_2]$, $\beta = [\tau_3, \tau_4]$. 3.2. $\alpha = [\tau_1, \tau_3]$, $\beta = [\tau_2, \tau_4]$.
3.3. $\alpha = [\tau_1, \tau_4]$, $\beta = [\tau_4, \tau_3]$. 3.4. $\alpha = [\tau_2, \tau_3]$, $\beta = [\tau_3, \tau_1]$.
3.5. $\alpha = [\tau_4, \tau_2]$, $\beta = [\tau_3, \tau_2]$.

4. Пусть в группе G коммутант содержится в центре группы, т. е. $G' \subseteq \subseteq Z(G)$. Докажите, что для любых x, y и $z \in G$ справедливы следующие равенства.

4.1. $[xy, z] = [x, z][y, z]$. 4.2. $[x^2, y] = [x, y^2] = [x, y]^2$.

4.3. $[x, yz] = [x, y][x, z]$. 4.4. $(xy)^2 = x^2y^2[y, x]$.

4.5. $[x, [y, z]][y, [z, x]] = [z, [x, y]] = e$.

5. Докажите, что для любых a, b и $c \in G$ справедливы следующие равенства.

5.1. $[a^{-1}, b] = a[b, a]a^{-1}$. 5.2. $[a, b]^{-1} = [b, a]$.

5.3. $[ab, c] = b^{-1}[a, c]b[b, c]$.

5.4. $[a, bc] = [a, c][a, b]^c = [a, c][a, b][[a, b], c]$.

5.5. $[ab, c] = [a, c]^b[b, c] = [a, c][[a, c], b][b, c]$.

6.1. Докажите, что в симметрической группе S_n любой коммутатор принадлежит знакопеременной группе A_n.

6.2. Пусть элемент z группы G является коммутатором. Докажите, что при любом $x \in G$ элементы xzx^{-1} и $x^{-1}zx$ также будут коммутаторами.

6.3. Пусть в группе все коммутаторы совпадают с единичным элементом. Докажите, что группа абелева.

6.4. Каковы коммутаторы всех элементов абелевой группы?

6.5. Докажите, что коммутант группы $GL(n, \mathbb{R})$ содержится в $SL(n, \mathbb{R})$.

Дополнительные задания

1. Найдите центр и коммутант абелевой группы.

2. Найдите центр и коммутант симметрической группы S_3.

3. Найдите центр и коммутант знакопеременной группы A_4.

4. Найдите центр и коммутант симметрической группы S_4.

5. Найдите центр и коммутант симметрической группы S_n и знакопеременной группы A_n, $n \geq 5$.

6. Найдите центр и коммутант группы кватернионов.

7. Найдите центр и коммутант группы диэдра.

8. В группе $GL(2, \mathbb{C})$ найдите централизаторы элементов

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

9. В группе $GL(3, \mathbb{Z}_5)$ найдите централизатор элемента

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

10. Пусть в группе порядок коммутанта равен 2. Докажите, что коммутант содержится в центре группы.

11. Пусть в группе порядок коммутанта равен 2. Докажите, что индекс коммутанта — четное число.

12. Пусть H — нормальная подгруппа группы и $H \cap G' = 1$. Докажите, что $H \subseteq Z(G)$ и $Z(G/H) = Z(G)/H$.

13. Докажите, что всякая минимальная нормальная подгруппа группы содержится либо в коммутанте, либо в центре.

14. Докажите, что если $G = G'$, то $Z(G/Z(G)) = 1$.

15. Докажите, что если $a \in G$ и $< a >$ — нормальная подгруппа группы G, то $G' \subseteq C_G(a)$.

16. Пусть H — нормальная подгруппа группы G, $a, b \in G$. Докажите, что если $ab \in H$, то $ba \in H$ и $a^{-1}b^{-1} \in H$.

17. Пусть G — группа, $a, b \in G$. Докажите, что $a^{-n}b^{-n}(ab)^n \in G'$ для любого натурального n.

18. Пусть в группе G имеются две различные абелевы максимальные подгруппы M_1 и M_2. Докажите, что их пересечение $M_1 \cap M_2$ содержится в центре группы G.

19. Пусть M — максимальная подгруппа группы G. Докажите, что для любой подгруппы H из группы G либо $Z(H) \subseteq M$, либо $Z(H) \cap M$ — нормальная подгруппа группы G.

20. Пусть G — группа и $< g^G >= \{g^x \mid x \in G\} \neq G$ для всех $g \in G$. Докажите, что $G' \neq G$.

6. Группы, порожденные двумя элементами

Вопросы для самоконтроля

1. Определение инволюции. Примеры инволюций в группах функций, в симметрической группе S_n, в полной линейной группе $GL(2, \mathbb{C})$.
2. Подгруппа, порожденная множеством.
3. Диэдральная группа и ее основные свойства.
4. Группы простого порядка.
5. Группы порядка p^2.
6. Группы порядка 8.
7. Группы порядка p^3.
8. Группы порядка pq.
9. Группы порядка pqr.
10. Группы порядка p^2q.
11. Группы порядка p^2q^2.
12. Число неизоморфных групп порядка ≤ 15.

Индивидуальные задания

1. Пусть τ и σ — элементы симметрической группы S_5.
а) Докажите, что $\tau^n \sigma = \sigma \tau^n$ для всех $n \in \mathbb{Z}$.
б) Заполните таблицу

	σ	τ^i	$\sigma\tau^j$
σ			
τ^k			
$\sigma\tau^l$			

.

в) Перечислите все элементы подгруппы $\langle \tau, \sigma \rangle$ и укажите порядок каждого элемента этой подгруппы.
г) Найдите индекс подгруппы $\langle \tau, \sigma \rangle$ в группе S_5.
1.1. $\tau = (235)$, $\sigma = (14)$. 1.2. $\tau = (124)$, $\sigma = (35)$.
1.3. $\tau = (134)$, $\sigma = (25)$. 1.4. $\tau = (234)$, $\sigma = (15)$.
1.5. $\tau = (125)$, $\sigma = (34)$.

2. Пусть γ и δ — элементы симметрической группы S_4.
а) Перечислите все элементы подгруппы $H = \langle \gamma, \delta \rangle$ и укажите порядок каждого элемента этой подгруппы.

б) Найдите разложение группы S_4 на правые смежные классы по подгруппе H.

в) Установите изоморфизм $H \simeq S_3$.

2.1. $\gamma = (234)$, $\delta = (34)$. 2.2. $\gamma = (124)$, $\delta = (12)$.
2.3. $\gamma = (134)$, $\delta = (13)$. 2.4. $\gamma = (234)$, $\delta = (23)$.
2.5. $\gamma = (132)$, $\delta = (12)$.

3. В диэдральной группе $D = \langle a, b \mid a^4 = b^2 = e, a^b = a^3 \rangle$ порядка 8 перечислите все элементы и найдите их порядки. Укажите все классы сопряженности. Найдите коммутант, центр и подгруппу Фраттини. Вычислите следующие произведения.

3.1. a^3ba^2b. 3.2. a^3bab. 3.3. a^2bab. 3.4. a^2ba^3b. 3.5. aba^3b.

4. В группе кватернионов $Q = \langle a, b \mid a^4 = e, b^2 = a^2, a^b = a^3 \rangle$ порядка 8 перечислите все элементы и найдите их порядки. Укажите все классы сопряженности. Найдите коммутант, центр и подгруппу Фраттини. Вычислите следующие произведения.

4.1. a^2bab^3. 4.2. $a^3ba^3b^2$. 4.3. $abab^2$. 4.4. a^4b^3ab. 4.5. a^7b^3ab.

5. В группе $R = \langle a, b \mid a^9 = b^3 = e, a^b = a^4 \rangle$ порядка 27 найдите коммутант, центр и подгруппу Фраттини. Вычислите порядок элемента x. Будет ли $\langle b, x \rangle$ собственной подгруппой?

5.1. $x = a^5ba^2b^2$. 5.2. $x = a^2ba^3b^2$. 5.3. $x = aba^5b^2$.
5.4. $x = a^3b^2a^2b$. 5.5. $x = a^3b^2ab$.

6. В группе $T = \langle a, b, c \mid a^3 = b^3 = c^3 = e, ab = bac, ac = ca, bc = cb \rangle$ порядка 27 найдите коммутант, центр и подгруппу Фраттини. Вычислите порядок элемента x. Докажите, что $T = \langle a, b \rangle$. Будет ли $\langle a, x \rangle$ собственной подгруппой?

6.1. $x = a^2bab^2$. 6.2. $x = a^2bab$. 6.3. $x = a^2b^2a^2b$.
6.4. $x = aba^2b^2$. 6.5. $x = ab^2ab$.

Дополнительные задания

1. В диэдральной группе $D = \langle a, b \mid a^8 = b^2 = e, a^b = a^3 \rangle$ порядка 16 перечислите все элементы и найдите их порядки. Укажите все классы сопряженности. Найдите коммутант, центр и подгруппу Фраттини. Вычислите произведение a^3ba^2b.

2. В группе кватернионов $Q = \langle a, b \mid a^8 = 1, b^2 = a^4, a^b = a^7 \rangle$ порядка 16 перечислите все элементы и найдите их порядки. Укажите все классы сопряженности. Найдите коммутант, центр и подгруппу Фраттини. Вычислите произведение a^2bab^3.

3. В полудиэдральной группе $S = \langle a, b \mid a^8 = b^2 = e, a^b = a^3 \rangle$ порядка 16 перечислите все элементы и найдите их порядки. Укажите все классы со-

пряженности. Найдите коммутант, центр и подгруппу Фраттини. Вычислите произведение a^2ba^2b.

4. В диэдральной группе $D = \langle a, b \mid a^5 = b^2 = e, a^b = a^4\rangle$ порядка 10 перечислите все элементы и найдите их порядки. Укажите все классы сопряженности. Найдите коммутант, центр и подгруппу Фраттини. Вычислите произведение a^3ba^2b.

5. Проверьте, что $S_4 = HK$, где $H \simeq S_3$, а

$$K = \{e, (12)(34), (13)(24), (14)(23)\}.$$

6. Проверьте, что $S_4 = LM$, где $L = \langle(1234)\rangle$ — циклическая группа порядка 4, а $M \simeq S_3$.

7. Докажите, что диэдральная группа порядка 16 не является произведением двух подгрупп порядка 4.

8. Докажите, что полудиэдральная группа порядка 16 не является произведением двух подгрупп порядка 4.

9. Пусть группа G порождается элементом a порядка n и элементом b порядка 2, которые связаны соотношением $ab = ba^{-1}$.

a) Докажите, что группа G состоит из $2n$ элементов.

b) Докажите, что каждый элемент вида ba^r имеет порядок 2.

10. Представьте каждый элемент из S_3 как произведение транспозиций. Докажите, что $S_3 = \langle(12), (13), (23)\rangle$.

11. Докажите, что множество всех транспозиций из S_n порождает группу S_n.

12. Вычислите произведение $(1a)(1b)(1a)$ и установите, что множество транспозиций $\{(12), (13), \ldots, (1n)\}$ порождает группу S_n.

13. Докажите, что все циклы длины 3 порождают A_n.

14. Пусть

$$M = \left\{ \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \mid b \in \mathbb{Z}_5,\ a \in \{\bar{1}, \bar{4}\} \subseteq \mathbb{Z}_5 \right\}.$$

Докажите, что M — подгруппа группы $GL(2, 5)$ и M изоморфна диэдральной группе порядка 10. Будет ли M нормальной подгруппой в группе $GL(2, 5)$?

15. Докажите, что подгруппа $\langle(12), (13)(24)\rangle$ группы S_4 является диэдральной. Укажите ее порядок и индекс.

16. Докажите, что подгруппа $\langle(12), (124)\rangle$ группы S_4 является диэдральной. Укажите ее порядок и индекс в группе S_4.

17. Докажите, что подгруппа

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

группы $GL(2,\mathbb{C})$ является диэдральной. Укажите ее порядок.

18. Докажите, что подгруппа

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

группы $GL(2,\mathbb{C})$ является диэдральной. Укажите ее порядок.

19. Докажите, что подгруппа

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

группы $GL(2,\mathbb{C})$ является группой кватернионов. Укажите ее порядок.

20. Проверьте, что в группе $GL(2,\mathbb{C})$ подгруппа

$$\left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle$$

изоморфна группе кватернионов

$$Q_8 = \langle a, b \mid a^4 = b^4 = 1,\ a^2 = b^2,\ a^b = a^{-1} \rangle$$

порядка 8. Она содержит в точности три максимальные подгруппы:

$$M_1 = \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\rangle,\ M_2 = \left\langle \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle,\ M_3 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

Глоссарий

Группа

В математике наиболее часто используются две формы записи алгебраической операции: аддитивная и мультипликативная. При *аддитивной* записи операцию называют *сложением* и пишут $c = a+b$. При *мультипликативной* записи операцию называют *умножением* и пишут $c = a \cdot b$ или $c = ab$. Связь между аддитивной и мультипликативной записями операций представлена в таблице 1.

Таблица 1.

Мультипликативная запись операции	Аддитивная запись операции
умножение	сложение
произведение ab $\prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n$	сумма $a+b$ $\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$
единичный элемент e $ae = ea = a$	нулевой элемент 0 $a + 0 = 0 + a = a$
обратный элемент a^{-1} $aa^{-1} = a^{-1}a = e$	противоположный элемент $-a$ $a + (-a) = -a + a = 0$
ассоциативность $(ab)c = a(bc)$	ассоциативность $(a+b)+c = a+(b+c)$
коммутативность $ab = ba$	коммутативность $a+b = b+a$
степень a^n при $n > 0$ $a^n = \underbrace{a \ldots a}_{n \text{ раз}}$	кратное na при $n > 0$ $na = \underbrace{a + \ldots + a}_{n \text{ раз}}$
степень a^n при $n < 0$ $a^n = \underbrace{a^{-1} \ldots a^{-1}}_{-n \text{ раз}}$	кратное na при $n < 0$ $na = \underbrace{(-a) + \ldots + (-a)}_{-n \text{ раз}}$
$a^n = e$ при $n = 0$	$na = 0$ при $n = 0$
$a^n a^m = a^{n+m}$	$na + ma = (n+m)a$
$(a^n)^m = a^{nm}$	$m(na) = (mn)a$
$(ab)^n = a^n b^n$, если $ab = ba$	$n(a+b) = na + nb$, если $a+b = b+a$

В дальнейшем все определения и результаты формулируются для мультипликативной записи операции.

Группой называется непустое множество G с бинарной алгебраической операцией (умножением), которая удовлетворяет следующим требованиям:

1) операция определена на G, т. е. $ab \in G$ для всех $a, b \in G$;

2) операция ассоциативна, т. е. $a(bc) = (ab)c$ для любых $a, b, c \in G$;

3) в G существует единичный элемент, т. е. такой элемент $e \in G$, что $ae = ea = a$ для всех $a \in G$;

4) каждый элемент обладает обратным, т. е. для любого $a \in G$ существует такой элемент $a^{-1} \in G$, что $aa^{-1} = a^{-1}a = e$.

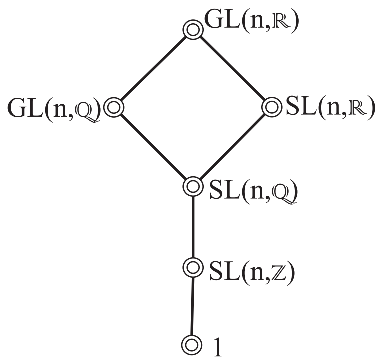
Приведенное определение группы легко переносятся с соответствующим изменением терминологии как указано в таблице на множества с аддитивной записью операции.

Подгруппа

Подмножество H группы G называется *подгруппой*, если H — группа относительно той же операции, которая определена на G. Запись $H \leq G$ означает, что H — подгруппа группы G, а $H < G$, что H — собственная подгруппа группы G, т. е. $H \leq G$ и $H \neq G$.

Критерий подгруппы: Непустое подмножество H группы G будет подгруппой тогда и только тогда, когда $h_1h_2 \in H$ и $h_1^{-1} \in H$ для всех $h_1, h_2 \in H$.

В группе $GL(n, \mathbb{R})$ содержатся следующие подгруппы.



Изоморфизм групп

Две группы G и G_1 называются *изоморфными*, если существует биекция $f : G \to G_1$ такая, что $f(ab) = f(a)f(b)$ для всех $a, b \in G$. Для обозначения изоморфизма используется запись $G \simeq G_1$.

Свойства изоморфных групп: Пусть $f : G \to G_1$ — изоморфизм группы G на группу G_1. Тогда:

1) $f(e)$ — единичный элемент группы G_1, где e — единичный элемент группы G;

2) $f(a^{-1})$ — обратный элемент к $f(a)$ в группе G_1 для любого $a \in G$;

3) отношение "быть изоморфными группами" является отношением эквивалентности.

Смежные классы

Пусть G — группа, H — ее подгруппа и $g \in G$. *Правым смежным классом* группы G по подгруппе H называется множество

$$Hg = \{hg \ | \ h \in H\}$$

всех элементов группы G вида hg, где h "пробегает" все элементы подгруппы H. Аналогично определяется *левый смежный класс*

$$gH = \{gh \ \mid \ h \in H\}.$$

Свойства смежных классов: Пусть G — группа, H — подгруппа. Тогда:
1) $H = He$;
2) $g \in Hg$ для каждого $g \in G$;
3) если $a \in H$, то $Ha = H$; если $b \in Ha$, то $Hb = Ha$;
4) $Ha = Hb$ тогда и только тогда, когда $ab^{-1} \in H$;
5) два смежных класса либо совпадают, либо их пересечение пусто;
6) если H — конечная подгруппа, то $\mid Hg \mid = \mid H \mid$ для всех $g \in G$.

Если G — конечная группа, то число различных правых смежных классов по H также будет конечно, оно называется *индексом подгруппы* H в G и обозначается через $\mid G : H \mid$.

Теорема Лагранжа: Если H — подгруппа конечной группы G, то $\mid G \mid = \mid H \mid\mid G : H \mid$. В частности, порядок конечной группы делится на порядок каждой своей подгруппы.

Нормальные подгруппы и фактор-группы

Подгруппа H называется *нормальной подгруппой* группы G, если $xH = Hx$ для всех $x \in G$. Запись $H \lhd G$ читается: "H — нормальная подгруппа группы G". Равенство $xH = Hx$ означает, что для любого элемента $h_1 \in H$ существует элемент $h_2 \in H$ такой, что $xh_1 = h_2x$.

Критерий нормальной подгруппы: Для подгруппы H группы G следующие утверждения эквивалентны:

1) H — нормальная подгруппа;

2) подгруппа H вместе с каждым своим элементом содержит все ему сопряженные элементы, т. е. $h^x \in H$ для всех $h \in H$ и всех $x \in G$;

3) подгруппа H совпадает с каждой своей сопряженной подгруппой, т. е. $H = H^x$ для всех $x \in G$.

Пусть H — нормальная подгруппа группы G. Обозначим через $\overline{G}$ совокупность всех левых смежных классов группы G по подгруппе H, т. е. $\overline{G} = \{xH \mid x \in G\}$. Множество $\overline{G}$ с умножением $(xH)(yH) = xyH$ будет группой, которую называют *фактор-группой группы G по подгруппе H* и обозначают через G/H. Если группа G конечна, то фактор-группа G/H также будет конечной и

$$\mid G/H \mid = \mid G : H \mid = \mid G \mid / \mid H \mid .$$

Произведение подгрупп

Пусть H и K — подгруппы группы G. *Двойной смежный класс*

$$HgK = \{hgk \mid h \in H, \ k \in K\}$$

группы G по подгруппам H и K обладает свойствами, аналогичными свойствам смежных классов группы по подгруппе. При $g = e$ двойной смежный класс превращается в произведение подгрупп H и K:

$$HK = \{hk \mid h \in H,\ k \in K\}.$$

В общем случае HK не является подгруппой. Говорят, что подгруппы H и K *перестановочны*, если $HK = KH$.

Произведение двух подгрупп является подгруппой тогда и только тогда, когда эти подгруппы перестановочны.

Тождество Дедекинда: Если A, B и C — подгруппы группы G и $A \leq C$, то $C \cap AB = A(C \cap B)$.

Порядок элемента

Пусть a — элемент группы G. Если все степени элемента a различны, т. е. $a^m \neq a^n$ для всех целых $m \neq n$, то говорят, что элемент a имеет *бесконечный порядок.*

Предположим, что имеются совпадения $a^m = a^n$ при $m \neq n$. Если, например, $m > n$, то $m - n > 0$ и $a^{m-n} = e$, т. е. существуют натуральные степени элемента a, равные единичному элементу. Наименьшее натуральное число k, при котором $a^k = e$, называют *порядком* элемента a и пишут: $\mid a \mid = k$.

Если a — элемент порядка n, то элемент a^m имеет порядок $n/(n, m)$. В частности, элемент a^m имеет порядок n тогда и только тогда, когда n и m взаимно просты.

Циклические группы

Зафиксируем в группе G элемент a. Пересечение всех подгрупп группы G, содержащих элемент a, назовем *циклической подгруппой, порожденной элементом* a, и обозначим через $\langle a \rangle$. Таким образом,

$$\langle a \rangle = \bigcap_{a \in H \leq G} H.$$

Циклическая подгруппа $\langle a \rangle$, порожденная элементом a, состоит из всевозможных целых степеней элемента a, т. е. $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Если в группе G существует элемент a такой, что $G = \langle a \rangle$, то группу G называют *циклической.*

Все подгруппы бесконечной циклической группы $G = \langle a \rangle$ исчерпываются единичной подгруппой $E = \{e\}$ и бесконечными циклическими подгруппами $\langle a^m \rangle$ для каждого натурального m.

Все фактор-группы бесконечной циклической группы $\langle a \rangle$ исчерпываются бесконечной циклической группой $\langle a \rangle / E \simeq \langle a \rangle$ и конечными циклическими группами $\langle a \langle a^m \rangle \rangle$ порядка m для каждого натурального m.

Все подгруппы конечной циклической группы $\langle a\rangle$ порядка n исчерпываются циклическими подгруппами $\langle a^m\rangle$ порядка n/m для каждого натурального m, делящего n.

Все фактор-группы конечной циклической группы $\langle a\rangle$ порядка n исчерпываются конечными циклическими группами $\langle a\langle a^m\rangle\rangle$ порядка m для каждого натурального m делящего n.

Гомоморфизм

Пусть G и Γ — мультипликативные группы. Отображение $\varphi : G \to \Gamma$ называется *гомоморфизмом* группы G в группу Γ, если

$$\varphi(xy) = \varphi(x)\varphi(y)$$

для любых x и $y \in G$. Если M — подмножество группы G, то

$$\varphi(M) = \{\varphi(m) \mid m \in M\} -$$

образ M при гомоморфизме φ, а $\varphi(G)$ — *образ гомоморфизма* φ. Образ гомоморфизма φ также обозначают через $\operatorname{Im}\varphi$. Ядром гомоморфизма φ называется множество

$$\operatorname{Ker}\varphi = \{x \in G \mid \varphi(x) = \varepsilon\},$$

где ε — единичный элемент группы Γ. Другими словами, в ядре собраны все элементы группы G, переходящие при отображении φ в единичный элемент группы Γ, т. е. $\operatorname{Ker}\varphi = \varphi^{-1}(\{\varepsilon\})$.

Основная теорема о гомоморфизме: При гомоморфизме $\varphi : G \to \Gamma$ групп фактор-группа по ядру изоморфна образу:

$$G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi.$$

Гомоморфизм $\varphi : G \to \Gamma$ называется *мономорфизмом*, если $\operatorname{Ker}\varphi = \{\varepsilon\}$. Гомоморфизм φ является мономорфизмом тогда и только тогда, когда отображение φ — инъекция. Если $\operatorname{Im}\varphi = \Gamma$, то гомоморфизм $\varphi : G \to \Gamma$ называется *эпиморфизмом*. Ясно, что в этом случае φ — сюръекция. Гомоморфизм, который одновременно является мономорфизмом и эпиморфизмом, будет *изоморфизмом*.

Теоремы Силова

Пусть конечная группа G имеет порядок $p^m s$, где p — простое число и p не делит s. Тогда справедливы следующие утверждения:

1) в группе G существует подгруппа порядка p^i для каждого $i = 1, 2, \ldots, m$;

2) если H — p-подгруппа и P — подгруппа порядка p^m, то существует такой элемент $a \in G$, что $H \le P^a$;

3) любые две подгруппы порядка p^m сопряжены;

4) число подгрупп порядка p^m в группе G сравнимо с единицей по модулю p и делит s.

Силовской p-подгруппой конечной группы G называют такую p-подгруппу, индекс которой не делится на p.

Для конечной группы G и ее силовской p-подгруппы P справедливы следующие утверждения:

1) если K — нормальная подгруппа группы G, то $P \cap K$ — силовская p-подгруппа в K, а PK/K — силовская p-подгруппа в G/K;

2) $N_{G/K}(PK/K) = N_G(P)K/K$;

3) если K_1 и K_2 — нормальные подгруппы группы G, то $K_1K_2 \cap P = (K_1 \cap P)(K_2 \cap P)$ и $K_1P \cap K_2P = (K_1 \cap K_2)P$;

4) пусть $p_1, p_2, \ldots, p_n$ — все простые делители порядка группы G, $p_i \neq p_j$ при $i \neq j$, и $P_1, P_2, \ldots, P_n$ — соответствующие им силовские подгруппы. Тогда $G = \langle P_1 \cup P_2 \cup \ldots \cup P_n \rangle$, а если $n = 2$, то $G = P_1P_2$.

Диэдральная группа

Элемент порядка 2 называется *инволюцией. Диэдральной группой* называется группа, порожденная двумя различными инволюциями.

Для группы G следующие утверждения эквивалентны:

1) G — диэдральная группа;

2) $G = [A]B$, где $A = \langle a \rangle$, $B = \langle b \rangle$, $\mid B \mid = 2$, $a^b = a^{-1}$.

Диэдральную группу порядка $2n$ записывают так:

$$D_{2n} = \langle a, b \mid a^n = b^2 = 1,\ a^b = a^{-1} \rangle.$$

При $n = 2$ диэдральная группа порядка 4 абелева:

$$D_4 = \langle a, b \mid a^2 = b^2 = 1,\ a^b = a \rangle = \langle a \rangle \times \langle b \rangle.$$

При $n = 3$ получаем: $D_6 = \langle a, b \mid a^3 = b^2 = 1,\ a^b = a^2 \rangle$. Диэдральная группа порядка 6 имеет следующую таблицу умножения:

$\mathbf{D_6}$	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	a^2b	ab	1	a^2	a
ab	ab	b	a^2b	a	1	a^2
a^2b	a^2b	ab	b	a^2	a	1

Группа D_6 изоморфна симметрической группе S_3 степени 3.

Для диэдральной группы порядка 8 получаем следующую таблицу умножения:

$\mathbf{D_8}$	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

Группа кватернионов

Группу $Q_8 = \langle a, b \mid a^4 = b^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1} \rangle$ называют *группой кватернионов.* Для этой группы получаем следующую таблицу умножения:

$\mathbf{Q_8}$	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2

Группы Q_8 и D_8 исчерпывают все неабелевые группы порядка 8.

Группы малых порядков

Из теоремы Лагранжа следует, что группа простого порядка циклическая.

Группа порядка p^2 или циклическая, или элементарная абелева.

Группа порядка $2p$ или циклическая, или диэдральная.

Если $p > q$, то каждая группа G порядка pq содержит нормальную подгруппу порядка p. Кроме того, если q не делит $p - 1$, то G циклическая.

Неабелевы группы порядка p^3, $p > 2$, могут быть двух типов:

$$\langle a, b \mid a^{p^2} = b^p = 1,\ a^b = a^{1+p} \rangle,$$

$$\langle a, b, c \mid a^p = b^p = c^p = 1,\ ab = bac,\ ca = ac,\ cb = bc \rangle.$$

Неабелева группа порядка 8 или диэдральная, или кватернионная.

Каждая неабелева группа порядка 12 изоморфна или A_4, или D_{12}, или группе $T = \langle a, b \mid a^6 = 1,\ b^2 = a^3 = (ab)^2 \rangle$.

В следующей таблице через $g(n)$ обозначается число неизоморфных групп порядка n.

n	$g(n)$	n	$g(n)$	n	$g(n)$	n	$g(n)$
1	1	11	1	21	2	31	1
2	1	12	5	22	2	32	51
3	1	13	1	23	1	33	1
4	2	14	2	24	15	34	2
5	1	15	1	25	2	35	1
6	2	16	14	26	2	36	14
7	1	17	1	27	5	37	1
8	5	18	5	28	4	38	2
9	2	19	1	29	1	39	2
10	2	20	5	30	4	40	14

Литература

1. Белоногов, В. А. Задачник по теории групп / В. А. Белоногов. — М.: Наука, 2000. — 239 с.

2. Беняш–Кривец, В. В. Лекции по алгебре: группы, кольца, поля / В. В. Беняш–Кривец, О. В. Мельников. — Минск: БГУ, 2009. — 115 с.

3. Кострикин, А. И. Введение в алгебру: в 3 ч. / А. И. Кострикин. — М.: Физматлит, 2001. — Ч. 3. — 272 с.

4. Ляпин, Е. С. Упражнения по теории групп / Е. С. Ляпин, А. Я. Айзенштат, М. М. Лесохин. — М.: Наука, 1967. — 264 с.

5. Монахов, В. С. Алгебра и теория чисел: учебное пособие / В. С. Монахов, А. В. Бузланов. – Минск: Изд. центр БГУ, 2007. — 264 с.

6. Монахов, В. С. Введение в теорию конечных групп и их классов / В. С. Монахов. — Минск: Вышэйш. шк., 2006. — 207 с.

7. Монахов, В. С. Числовые функции и классы вычетов : практикум / В. С. Монахов, А. А. Трофимук. — Брестский гос. ун–т им. А. С. Пушкина. — Брест: БрГУ имени А. С. Пушкина, 2011. — 88 с.

8. Проскуряков, И. В. Сборник задач по линейной алгебре / И. В. Проскуряков. — 9-е изд. — М.: Дрофа, 2005. — 383 с.

9. Сборник задач по алгебре / под ред. А. И. Кострикина. — М.: Наука, 1987. — 352 с.

10. Чехлов, А. Р. Упражнения по основам теории групп / А. Р. Чехлов. — Томский гос. ун–т. — Томск: Изд-во ТГУ, 2004. — 276 с.

11. Ledermann, W. Introduction to group theory / W. Ledermann, A. J. Weir. — Addison Wesley Longman, 1996. — 271 p.

12. Rotman, J. An introduction to the theory of groups / J. Rotman. — New York: Springer-Verlag, 1994. — 540 p.

Производственно-практическое издание

МОНАХОВ Виктор Степанович,
ХОДАНОВИЧ Дмитрий Александрович

ТЕОРИЯ ГРУПП

Практическое пособие

для студентов специализации «Алгебра и теория чисел»
математического факультета
специальности 1-31 03 01 «Математика»

Редактор В. И. Шкредова
Корректор В. В. Калугина

Подписано в печать 29.05.2014. Формат 60x84 1/16.
Бумага офсетная. Ризография. Усл. печ. л. 2,3.
Уч.-изд. л. 2,5. Тираж 70 экз. Заказ 363.

Издатель и полиграфическое исполнение:
учреждение образования
«Гомельский государственный университет
имени Франциска Скорины».

Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий № 1/87 от 18.11.2013.
Специальное разрешение (лицензия) № 02330 / 450 от 18.12.2013.
Ул. Советская, 104, 246019, Гомель.