МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**Нижегородский государственный университет
им. Н.И. Лобачевского**

Задачи по теории групп. Часть I

Практикум

Рекомендован методической комиссией механико-математического факультета для студентов ННГУ, обучающихся по специальности 010101 „Математика“, по направлению 010100 „Математика“, по направлению 010200 „Математика и компьютерные науки“

Нижний Новгород
2010

УДК 512.54
ББК 22.144
З-15

З-15. ЗАДАЧИ ПО ТЕОРИИ ГРУПП. ЧАСТЬ I. Составители : Кузнецов М.И., Муляр О.А., Хорева Н.А., Чебочко Н.Г.: Практикум. - Нижний Новгород: Нижегородский госуниверситет, 2010. - 23с.

Рецензент: д.ф.-м.н., профессор **В.М. Галкин.**

Практикум содержит задачи и все необходимые сведения для решения задач по теории групп (части курса "Алгебра") по темам: определение группы, подгруппы, циклические группы, гомоморфизмы групп и факторгруппы. Приводятся подробные решения типовых задач. Практикум предназначен для студентов-математиков второго курса механико-математического факультета.

Практикум издан в рамках развития НИУ „Разработка новых и модернизация существующих образовательных ресурсов“

УДК 512.54
ББК 22.144

Содержание

§1 Понятие группы. Подгруппы

Бинарной алгебраической операцией на множестве M называется любое отображение $* : M \times M \to M$. Результат применения операции $*$ к паре элементов a, b из M будем обозначать $a * b$.

Операция $*$ на множестве M называется ассоциативной, если для любых элементов $a, b, c \in M$ выполняется равенство $(a * b) * c = a * (b * c)$.

Операция $*$ на множестве M называется **коммутативной**, если для любых элементов $a, b \in M$ выполняется равенство $a * b = b * a$.

Определение. Множество G с заданной на нем бинарной операцией $* : G \times G \to G$ называется **группой**, если

1) операция $*$ ассоциативна;

2) в G существует нейтральный элемент, т.е. такой элемент $e \in G$, что $e * g = g * e = g$ для любого $g \in G$;

3) для любого $g \in G$ существует обратный элемент $g^{-1} \in G$, т.е. такой элемент, что $g * g^{-1} = g^{-1} * g = e$.

Для того чтобы подчеркнуть, что множество G рассматривается как группа относительно операции $*$, обычно пишут $(G, *)$.

Если операция в группе обозначается как $+$, то она называется сложением, нейтральный элемент обозначается 0 и называется нулем, обратный элемент к g обозначается $-g$ и называется противоположным к g.

Обычно операцию в группе называют умножением и обозначают знаком $\cdot$, нейтральный элемент называют единичным элементом или единицей группы. В дальнейшем мы будем придерживаться таких обозначений.

Если операция в группе коммутативна, то группу G называют **коммутативной** или **абелевой**. Мощность группы G называется **порядком группы** и обозначается через $|G|$.

В любой группе существует единственный единичный элемент. Для любого элемента группы существует единственный обратный элемент.

Отметим, что $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ (именно в таком порядке).

Определение. Пусть $(G, \cdot)$ - группа. Непустое подмножество H в G называется **подгруппой**, если H является группой относительно операции $\cdot$. Иными словами, H является подгруппой, если выполнены следующие условия:

1) H замкнуто относительно операции $\cdot$ (то есть $a \cdot b \in H$ для любых $a, b \in H$);

2) H замкнуто относительно взятия обратного элемента ($a^{-1} \in H$ для любого $a \in H$).

Рассмотрев любой элемент $a \in H$, получим из свойств 1), 2), что $a \cdot a^{-1} = e \in H$. Т.е любая подгруппа содержит единицу группы G.

Условия 1), 2) можно заменить на одно: $a \cdot b^{-1} \in H$ для любых $a, b \in H$.
Подмножество $H = \{e\}$ и сама группа G всегда являются подгруппами в G.

Упражнения.

1.1. Выяснить, какими свойствами обладает операция $*$ на множестве M, если

а) $M = \mathbb{N},\ x * y = x^y$;
б) $M = \mathbb{N},\ x * y = \text{НОД}(x, y)$;
в) $M = \mathbb{N},\ x * y = 2xy$;
г) $M = \mathbb{Z},\ x * y = x - y$;
д) $M = \mathbb{Z},\ x * y = x^2 + y^2$;
е) $M = \mathbb{R},\ x * y = \sin(x)\sin(y)$;
ж) $M = \mathbb{R}^*,\ x * y = \frac{x}{y}$, где $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$;
з) $M = \mathbb{R} \times \mathbb{R},\ (x, y) * (a, b) = (x, b)$.

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

а) $(G, +)$, где $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
б) $(G, \cdot)$, где $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
в) $(G^*, \cdot)$, где $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (здесь $G^* = G\backslash\{0\}$);
г) $(n\mathbb{Z}, +)$, где $n \in \mathbb{N}$;
д) $(\{-1, 1\}, \cdot)$;
е) $(\{a^n | n \in \mathbb{Z}\}, \cdot)$, где $a \in \mathbb{R}$ и $a \neq 0$;
ж) $(T^1, \cdot)$, где $T^1 = \{z \in \mathbb{C} |\ |z| = 1\}$;
з) $(\{z \in \mathbb{C} |\ |z| > 1\}, \cdot)$.

1.3. Доказать, что $[0, 1)$ с операцией $\oplus$, где $a \oplus b = \{a + b\}$ - дробная часть числа $a + b$, является группой.

1.4. Доказать, что пары $(a,\ b)$ вещественных чисел, $a \neq 0$, составляют группу относительно операции $(a,\ b)(c,\ d) = (ac,\ ad + b)$.

1.5. Пусть $(G, \cdot)$ – группа. Доказать, что G является группой относительно операции $*$, где $a * b = b \cdot a$.

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

а) множество симметрических (кососимметрических) матриц относительно сложения;

б) множество симметрических (кососимметрических) матриц относительно умножения;

в) множество невырожденных матриц относительно сложения;

г) множество невырожденных матриц относительно умножения;

д) множество матриц с фиксированным определителем d относительно умножения;

е) множество диагональных матриц относительно сложения;

ж) множество диагональных матриц относительно умножения;

з) множество диагональных матриц, у которых все элементы на главной диагонали отличны от нуля, относительно умножения;

и) множество всех ортогональных матриц;

к) множество ненулевых матриц вида $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ $(x, y \in \mathbb{R})$ относительно умножения;

л) множество ненулевых матриц вида $\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}$ $(x, y \in \mathbb{R})$, где λ – фиксированное вещественное число, относительно умножения;

м) множество матриц

$$Q_8 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \right\}$$

относительно умножения?

1.7. Доказать, что множество функций вида $y = \frac{ax+b}{cx+d}$, где $a, b, c, d \in \mathbb{R}$ и $ad - bc \neq 0$, является группой относительно операции композиции функций.

1.8. Доказать, что если $x^2 = e$ для любого элемента группы G, то G абелева.

1.9. Для каждой из групп в задачах 1.2. и 1.6. приведите пример какой-либо подгруппы.

1.10. Доказать, что во всякой группе пересечение любого набора подгрупп является подгруппой.

1.11. Найти две подгруппы в группе из задачи 1.4.

1.12. Найти все подгруппы а) в четверной группе Клейна; б) в S_3; в) в A_4.

§2 Циклические группы

Пусть $(G, \cdot)$ – группа, $g \in G$, $n \in Z$. Введем понятие n-ой степени элемента. Если $n > 0$, то $g^n = \underbrace{gg \cdots g}_{n}$. Если $n = 0$, то $g^n = e$. Если $n < 0$, то $g^n = \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{-n}$.

Если G – группа по сложению, то говорят не о степенях, а о кратных элемента группы. Если $n > 0$, то $ng = \underbrace{g + g + \cdots + g}_{n}$. Если $n = 0$, то $ng = 0$. Если $n < 0$, то $ng = \underbrace{(-g) + (-g) + \cdots + (-g)}_{-n}$.

Свойства степеней:

$$g^m g^n = g^{m+n},$$

$$(g^m)^n = g^{mn}.$$

Рассмотрим множество всех степеней элемента g:

$$< g >= \{g^n | n \in \mathbb{Z}\}.$$

Множество $< g >$ является подгруппой в G и называется **циклической подгруппой**, порожденной элементом g. Элемент g называют **образующим** элементом циклической подгруппы.

Если G – группа по сложению, то циклическая подгруппа – это множество всех кратных элемента g:

$$< g >= \{ng \mid n \in Z\}.$$

Рассмотрим примеры циклических подгрупп.

1) $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ с операцией умножения.

Так как $i^2 = -1, i^3 = -i, i^4 = 1$, то, $< i >= \{1, -1, i, -i\}$, т.е. $< i >$ – подгруппа 4-го порядка. Так как $(-1)^2 = 1$, то $< -1 >= \{1, -1\}$ – подгруппа 2-го порядка.

2) $GL_2(\mathbb{R})$ – группа невырожденных матриц второго порядка с действительными элементами, $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in GL_n(\mathbb{R})$.

Имеем $< A >= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$, т.к. $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$.

Циклическая подгруппа, порождённая A, имеет порядок 2.

Если $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, то $B^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $B^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \ldots, B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

Все натуральные степени матрицы B различны, т.е. циклическая подгруппа $< B >$ содержит бесконечное число элементов.

Группа G называется **циклической**, если существует элемент $g \in G$ такой, что $G =< g >$.

Иными словами, группа – циклическая, если все элементы группы являются степенями некоторого фиксированного элемента этой группы.

Любая циклическая группа абелева, так как любые две степени элемента перестановочны между собой:

$g^m g^n = g^{m+n} = g^n g^m \ \ \forall m, n \in \mathbb{Z}$.

Примеры циклических групп.

1) Пусть $G = (\mathbb{Z}, +)$ - группа целых чисел с операцией сложения. Тогда группа G – бесконечная циклическая. В качестве порождающего элемента можно выбрать 1 или -1. Действительно,

$\forall n \in \mathbb{Z} \ \ n = n \cdot 1 = (-n) \cdot (-1)$. Следовательно, $G =< 1 >=< -1 >$.

Другие элементы из $\mathbb{Z}$ не являются образующими циклической группы $\mathbb{Z}$. Действительно, если $\mathbb{Z} =< t >$, то, в частности, $1 = nt$ для некоторого целого n. Откуда, $n = t = \pm 1$.

2) Пусть G – группа корней n-ой степени из единицы. Группа $G = \{\epsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \mid k = \overline{0, n-1}\}$ имеет порядок n. Очевидно, G – циклическая группа: $\epsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = \left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}\right)^k = \epsilon_1^k$. Следовательно, $G =< \epsilon_1 >$.

3) Пусть $Z_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$ - группа классов вычетов по модулю m. Так как $\bar{t} = \underbrace{\bar{1} + \cdots + \bar{1}}_{t} = t\bar{1}$, то $Z_m =< \bar{1} >$ - циклическая группа.

Пусть G – произвольная группа, $g \in G$.

Порядком элемента g называется наименьшее натуральное число n, такое что $g^n = e$.

Обозначение: $\operatorname{ord} g = n$.

Если такого натурального числа не существует, то говорят, что g имеет бесконечный порядок.

В группе по сложению порядком элемента g называется наименьшее целое положительное число n, такое что $ng = 0$.

Единица группы – единственный элемент порядка 1.

Примеры.

1) $G = \mathbb{Z}$, $\operatorname{ord} 0 = 1$, порядки остальных элементов G бесконечны, так как если кратное $nm = 0$ при $n \neq 0$, то $m = 0$.

2) $G = S_4$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, $g^4 = id$, в меньших положительных степенях мы не получим тождественной подстановки, следовательно, $\operatorname{ord} g = 4$.

3) $G = \mathbb{C}^*$, $g = \dfrac{1}{2} + \dfrac{\sqrt{3}}{2} i = \cos \dfrac{\pi}{3} + i \sin \dfrac{\pi}{3}$. Используя формулу Муавра, получаем, что

$$g^m = \cos \frac{m\pi}{3} + i \sin \frac{m\pi}{3}.$$

Поэтому, $g^m = 1 = \cos 0 + i \sin 0$ тогда и только тогда, когда $\dfrac{m\pi}{3} = 2\pi k$ для некоторого $k \in \mathbb{Z}$, т.е. $m = 6k$. Наименьшее положительное m, кратное 6, это 6. Следовательно, $\mathrm{ord}(\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i)$=6.

В данном примере модуль g равен 1, это необходимое условие, для того, чтобы комплексное число имело конечный порядок. Действительно, при возведении в степень комплексного числа, будет возводиться в степень модуль этого числа. Натуральная степень вещественного положительного числа равна 1, только если это число равно 1. Например, $|1 + i\sqrt{3}| = 2$. Следовательно, $\mathrm{ord}(1 + i\sqrt{3}) = \infty$

Предложение.

(1) $g^m = e \quad \Leftrightarrow \mathrm{ord} g | m$.

(2) $ordg^k = \frac{\mathrm{ord} g}{(k, \mathrm{ord} g)}$.

Доказательство. Пусть $\mathrm{ord} g = n$.

(1) Разделим m с остатком на n: $m = nt + r$, $0 \le r < n$. Тогда $g^m = g^{nt+r} = (g^n)^t g^r = g^r$, так как $g^n = e$ по определению порядка элемента. Далее,

$g^m = e \Leftrightarrow g^r = e \Leftrightarrow$ (так как $r < n$) $r = 0 \Leftrightarrow n|m$.

(2) Пусть $d = (k, n)$, $n = n_1 d$, $k = k_1 d$, $(n_1, k_1) = 1$. Для любого m, $(g^k)^m = e \Leftrightarrow g^{km} = e \Leftrightarrow$ (из (1)) $n|km \Leftrightarrow n_1|k_1 m \Leftrightarrow n_1|m$. Таким образом, $(g^k)^m = e \Leftrightarrow \frac{\mathrm{ord} g}{(k, \mathrm{ord} g)}|m$. Следовательно, $\mathrm{ord} g^k = \frac{\mathrm{ord} g}{(k, \mathrm{ord} g)}$. $\square$

Задача. Найти порядки всех элементов в $\mathbb{Z}_6 = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}$.

Порядок $\overline{0}$ равен 1.

Образующим элементом в $\mathbb{Z}_6$ является, например, $\overline{1}$. Наименьшее положительное t, такое что $t\overline{1} = \overline{0}$ это 6, следовательно, $\mathrm{ord}\overline{1} = 6$.

Согласно утверждению (2) предложения имеем $\mathrm{ord}\overline{2} = \frac{6}{(6,2)} = \frac{6}{2} = 3$, $\mathrm{ord}\overline{3} = \frac{6}{(6,3)} = \frac{6}{3} = 2$, $\mathrm{ord}\overline{4} = \frac{6}{(6,4)} = \frac{6}{2} = 3$, $\mathrm{ord}\overline{5} = \frac{6}{(6,5)} = \frac{6}{1} = 6$.

Покажем, что порядок любой подстановки в $G = S_n$ равен наименьшему общему кратному длин независимых циклов, в произведение которых она раскладывается.

Пусть $\alpha = \alpha_1 \cdots \alpha_s$ – разложение подстановки в произведение независимых циклов длин $k_1, \ldots, k_s$, соответственно. Циклы $\alpha_1, \ldots, \alpha_s$ перестановочны между собой. Поэтому $\alpha^n = \alpha_1^n \cdots \alpha_s^n$. Множества элементов, которые действительно переставляются подстановками $\alpha_1^n, \ldots, \alpha_s^n$, не пересекаются между собой. Следовательно, $\alpha^n = id \Leftrightarrow \alpha_1^n = id, \ldots, \alpha_s^n = id$. Из утверждения (1) предложения следует, что $[\mathrm{ord}\,\alpha_1, \ldots, \mathrm{ord}\,\alpha_s] = \mathrm{ord}\,\alpha$. Так как порядок любого цикла равен длине этого цикла, то мы получаем, что $[k_1, \ldots, k_s] = \mathrm{ord}\,\alpha$.

Задача. Найти порядок подстановки

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 11 & 4 & 5 & 6 & 7 & 3 & 9 & 8 & 10 & 12 & 1 \end{pmatrix}.$$

Так как $\alpha = (1,2,11,12)(3,4,5,6,7)(8,9)$, то $\mathrm{ord}\alpha = [4,5,2] = 20$.

Задача. Сколько элементов порядка 12 содержится в $\mathbb{C}^*$, S_7 или A_7.

Подстановка α имеет порядок 12 тогда и только тогда, когда наименьшее общее кратное длин независимых циклов, в которые она раскладывается равно 12. Так как α – подстановка на множестве из 7 элементов, то α – произведение цикла длины 3 на цикл длины 4. Найдем количество таких подстановок. Выбирая 3 элемента, составляющие цикл длины 3, мы автоматически выбираем 4 элемента (дополнительные к выбранным 3), составляющие независимый цикл длины 4.

Всего таких выборок $C_7^3 = 35$. Для выбранных элементов количество различных циклов длины 3, которые можно составить из данных элементов равно $2 = \dfrac{3!}{3}$. Например, из выборки $2,5,7$ можно составить циклы $(2,5,7) = (5,7,2) = (7,2,5)$ и $(7,5,2) = (5,2,7) = (2,7,5)$. Аналогично, из выбранных четырех чисел можно составить $\dfrac{4!}{4} = 6$ различных циклов длины 4. Следовательно, в S_7 содержится ровно $35 \cdot 2 \cdot 6 = 420$ элементов порядка 12.

Так как произведение цикла длины 3 на цикл длины 4 является нечетной подстановкой, то в A_7 нет элементов порядка 12.

Элементы порядка 12 в $\mathbb{C}^*$ удовлетворяют соотношению $z^{12} = 1$, т.е. они являются корнями из единицы степени 12. По определению порядка наименьшая натуральная степень, при возведении в которую z получается 1, равна 12. Т.е. z является первообразным корнем из 1 единицы степени 12.

Пусть $\varepsilon_k = \cos\dfrac{\pi k}{12} + \sin\dfrac{\pi k}{12}$, $k = 0,1,...,11$ – корни из единицы степени 12. Корень ε_k является первообразным тогда и только тогда, когда k и 12 взаимно просты. Следовательно, первообразными являются $\varepsilon_1, \varepsilon_5, \varepsilon_7, \varepsilon_{11}$. Поэтому в $\mathbb{C}^*$ содержится ровно 4 элемента порядка 12.

Теорема 1. Порядок циклической подгруппы, порожденной элементом g, совпадает с порядком g. Если $ord\, g = n$, то $< g >= \{g^0,\, g^1,\, g^2, \ldots,\, g^{n-1}\}$. $\square$

Следствие 1. Конечная группа G является циклической $\Leftrightarrow$ в G существует элемент порядка $|G|$.

Необходимость следует из теоремы 1. Для доказательства достаточности рассмотрим циклическую подгруппу, порожденную элементом порядка $|G|$. По теореме она состоит из $|G|$ элементов, а, следовательно, совпадает с G.

Следствие 2. Элемент g^k является образующим в группе $< g > \Leftrightarrow k$ взаимно просто с $ord\, g$.

Пусть $G =< g >$, $|G| = \mathrm{ord} g = n$. Из теоремы 1, получаем, что циклическая подгруппа, порожденная элементом g^k, совпадает с G, т.е. состоит из n элементов тогда и только тогда, когда $\mathrm{ord} g^k = n$. Имеем, $\frac{\mathrm{ord} g}{(k, \mathrm{ord} g)} = n$, т.е. $\frac{n}{(k,n)} = n$. Поэтому, g^k является образующим $\Leftrightarrow (k, n) = 1$.

Количество натуральных чисел не превосходящих n и взаимно простых с n равно значению функции Эйлера $\varphi(n)$. Следовательно, количество образующих в циклической группе порядка n равно $\varphi(n)$.

Пример. Пусть $G = Z_{20}$. Количество образующих равно $\varphi(20) = 8$. Так как $Z_{20} =< \bar{1} >$, то $\bar{t} = t\bar{1}$ - образующий, тогда и только тогда, когда $(t, 20) = 1$. Т.е. образующими являются $\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}$.

Задача. В циклической группе порядка 20 найти все элементы a, такие что $a^5 = e$ и все элементы порядка 5.

Пусть $G =< g >= \{e, g, g^2, ..., g^{19}\}$. Имеем, $(g^k)^5 = e \Leftrightarrow 20|5k$, т.е. $4|k$. Откуда, $k = 0, 4, 8, 12, 16$. Следовательно, элементы, которые в пятой степени равны единичному, это $g^0 = e, g^4, g^8, g^{12}, g^{16}$.

Так как $\mathrm{ord} g^k = \dfrac{\mathrm{ord} g}{(k, \mathrm{ord} g)} = \dfrac{20}{(k, 20)}$, то $\mathrm{ord} g^k = 5 \Leftrightarrow \dfrac{20}{(k, 20)}=5$, т.е. $(k, 20) = 4$. Следовательно, $k = 4, 8, 12, 16$. Т.е. элементы порядка 5 в G это g^4, g^8, g^{12}, g^{16}.

Теорема 2.

(1) Любая подгруппа циклической группы сама является циклической.

(2) Существует взаимно-однозначное соответствие между всеми подгруппами конечной циклической группы и всеми делителями порядка группы. $\square$

Если $G =< g >$ и H - нееденичная подгруппа в G, то $H =< g^m >$, где $m = \min\limits_{g^k \in H}\{k > 0\}$. Если G – конечная группа, то число m является делителем $n = |G|$. Более точно, $|H| = \dfrac{n}{m}$.

Задача. Найти все подгруппы в $\mathbb{Z}_{15}$.

В группе классов вычетов образующим элементом всегда является класс вычетов 1, но мы выберем другой образующий: $\bar{2}$, $\mathbb{Z}_{15} =< \bar{2} >$.

Делителями 15 являются 1, 3, 5, 15. Подгруппами в $\mathbb{Z}_{15}$ являются $H_1 =< m_1\bar{2} >$, $H_2 =< m_2\bar{2} >$, $H_3 =< m_3\bar{2} >$, $H_4 =< m_4\bar{2} >$, где $m_1 = \dfrac{15}{1} = 15$, $m_2 = \dfrac{15}{3} = 5$, $m_3 = \dfrac{15}{5} = 3$, $m_4 = \dfrac{15}{15} = 1$. Таким образом, $H_1 = \{\bar{0}\}$,

$H_2 =< 5(\bar{2}) >=< \overline{10} >= \{\bar{0}, \overline{10}, 2(\overline{10})\} = \{\bar{0}, \bar{5}, \overline{10}\}$, $H_3 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}\}$, $H_4 = G$.

Задача. Найти все подгруппы в $\mathbb{Z}$.

$\mathbb{Z}$ - бесконечная циклическая группа с операцией сложения, образующим является 1 и -1. Т.е. $\mathbb{Z} =< 1 >$. Любая подгруппа, согласно теореме 2, имеет вид $< a >$, где a - некоторое кратное 1, т.е. $a = m1 = m,\ m \in \mathbb{N}$ или $a = 0$. Таким образом, подгруппы в $\mathbb{Z}$ это $< m >= \{..., -2m, -m, 0, m, 2m, ...\} = m\mathbb{Z}$, где $m \in \mathbb{N} \cup \{0\}$.

Упражнения.

2.1. Доказать, что $\mathrm{ord}xy = \mathrm{ord}yx$ и $\mathrm{ord}x = \mathrm{ord}yxy^{-1}$.

2.2. Найти порядок элемента группы:

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

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 5 & 4 & 1 & 6 & 2 & 3 & 9 & 8 & 11 & 12 & 10 \end{pmatrix} \in S_{12}$;

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

д) $g = 5 + 6i \in \mathbb{C}^*$; е) $g = \cos\dfrac{5\pi}{12} + i\sin\dfrac{5\pi}{12} \in \mathbb{C}^*$;

ж) $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{C})$; з) $\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{C})$;

и) $\begin{pmatrix} \frac{1}{2} & -\frac{i\sqrt{3}}{2} \\ -\frac{i\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \in GL_2(\mathbb{C})$; к) $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in GL_3(\mathbb{R})$;

л) $\begin{pmatrix} \overline{1} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix} \in GL_2(\mathbb{Z}_5)$; м) $\begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{2} \end{pmatrix} \in GL_2(\mathbb{Z}_3)$.

2.3. Сколько элементов порядка 6 содержится в группе:

а) $\mathbb{C}^*$; б) S_5; в) A_5.

2.4. Сколько элементов порядка 2 содержится в группе:

а) S_5; б) A_5.

2.5. Найти порядок каждого элемента в группах $\mathbb{Z}_{12}$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}^*$, $\mathbb{Z}_8^*$, $\mathbb{Z}_7^*$ (здесь через K^* обозначена группа обратимых элементов кольца K).

2.6. В циклической группе порядка 24 найти все элементы a, такие что $a^6 = e$, и все элементы порядка 6.

2.7. Найти все образующие группы $\mathbb{Z}_{14}$.

2.8. Для каждой из следующих групп определите, является ли она циклической группой: $\mathbb{Z}$, $8\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{Z}_{10}^*$, $\mathbb{Z}_{13}^*$, S_n $(n \geq 3)$.

2.9. Найдите в группе $\mathbb{C}^*$ циклическую подгруппу, порожденную элементом $-\frac{\sqrt{3}}{2} + \frac{1}{2}i$.

2.10. Найдите в группе $\mathbb{Z}_{30}$ циклическую подгруппу, порожденную элементом $\overline{25}$; в группе $\mathbb{Z}_{42}$ – циклическую подгруппу, порожденную элементом $\overline{30}$.

2.11. Найдите в группе $\mathbb{Z}_{14}^*$ циклическую подгруппу, порожденную элементом $\overline{5}$.

2.12. Найти все подгруппы в $\mathbb{Z}_{10}$, в $\mathbb{Z}_{24}$, в $\mathbb{Z}_{100}$.

2.13. Найти все конечные подгруппы в $\mathbb{R}^*$ и $\mathbb{C}^*$.

2.14. Доказать, что в группе кватернионов Q_8 все подгруппы, кроме самой Q_8, являются циклическими.

* * *

2.15. Доказать, что в группе четного порядка имеется элемент порядка 2.

2.16. Доказать, что любая бесконечная группа имеет бесконечное число подгрупп.

2.17. Доказать, что циклическая группа не может иметь более одного элемента порядка 2.

§3 Гомоморфизмы групп

Пусть $(G, *)$ и $(H, \circ)$ - группы. Отображение $f : G \to H$ называется **гомоморфизмом групп,** если для любых $a, b \in G$

$$f(a * b) = f(a) \circ f(b).$$

Ядром гомоморфизма групп $f : G \to H$ называется множество

$$Kerf = \{g \in G \mid f(a) = e\},$$

где e - единица в H.

Образом гомоморфизма f называется множество всех элементов вида $f(g)$:

$$Imf = \{b \in H \mid \exists\ a \in G, f(a) = b\}.$$

Инъективный гомоморфизм называется **мономорфизмом**, сюръективный - **эпиморфизмом**, биективный - **изоморфизмом.**

Примеры.

1. Пусть $G = (\mathbb{R}^n, +),\ H = (\mathbb{R}^m, +),\ f : \mathbb{R}^n \to \mathbb{R}^m -$ линейное отображение. Тогда $f-$ гомоморфизм групп.

2. Пусть $(G, *)$ и $(H, \circ)$ - произвольные группы. Отображение $f : G \to H$ определим следующим образом: $f(g) = e$ для любого элемента $g \in G$. Здесь $e-$ единица в H. Покажем, что $f-$ гомоморфизм групп. Действительно,

$$f(a * b) = e = e \circ e = f(a) \circ f(b).$$

Ядро гомоморфизма $Kerf = G$, а образ $Imf = \{e\}$.

3. Пусть $G = (\mathbb{R}, +),\ H = (\mathbb{R}^*, \cdot),\ f : G \to H,\ f(x) = 2^x$. Покажем, что $f-$ гомоморфизм. Действительно,

$$f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y).$$

Так как $2^x = 1$ только при $x = 0$, то $Kerf = \{0\}$ и, следовательно, $f-$ мономорфизм.

Как известно, $2^x \in \mathbb{R}^+$ для любого $x \in \mathbb{R}$. Поэтому $Imf \subseteq \mathbb{R}^+$. Кроме того, любое положительное число y можно записать в виде $y = 2^x = f(x)$, где $x = \log_2 y \in \mathbb{R}$. Следовательно, $Imf = \mathbb{R}^+$.

4. Пусть $G = (GL_n(\mathbb{R}), \cdot),\ H = (\mathbb{R}^*, \cdot),\ f : G \to H,\ f(A) = \det A$. Покажем, что $f-$ гомоморфизм групп. В самом деле,

$$f(A \cdot B) = \det(A \cdot B) = \det A \cdot \det B = f(A) \cdot f(B).$$

Найдем ядро и образ гомоморфизма f :

$$Kerf = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} = SL_n(\mathbb{R});\ Imf = \mathbb{R}^*.$$

В самом деле, для любого ненулевого действительного числа $\alpha \in \mathbb{R}^*$ существует невырожденная матрица A с определителем, равным α, например, такая:

$$A = \begin{pmatrix} \alpha & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{pmatrix}.$$

Таким образом, f – эпиморфизм.

Свойства гомоморфизмов групп

Пусть $(G, *)$ и $(H, \circ)$ – группы, $f : G \to H$ – гомоморфизм групп.

(1) Единица группы G переходит в единицу группы H, то есть $f(e) = e$.

(2) Для любого элемента $a \in G$ справедливо: $f(a^{-1}) = (f(a))^{-1}$.

(3) Для любого элемента $a \in G$ выполняется: $f(a^n) = (f(a))^n$.

(4) Гомоморфизм f инъективен тогда и только тогда, когда ядро $Kerf$ тривиально, то есть состоит только из нейтрального элемента.

(5) Ядро гомоморфизма является нормальной подгруппой в G, образ гомоморфизма является подгруппой в H.

(6) Композиция гомоморфизмов групп является гомоморфизмом групп.

(7) Если $f : G \to H$ – изоморфизм групп, то $f^{-1} : H \to G$ – тоже изоморфизм групп (существует в силу биективности).

Изоморфизм $f : G \to G$ называется **автоморфизмом**. Множество $Aut(G)$ всех автоморфизмов группы G образует группу относительно операции композиции отображений.

Пример. Пусть G – группа. Для произвольного элемента $g \in G$ зададим отображение $\tau_g : G \to G$ правилом $\tau_g(x) = gxg^{-1}$. Отображение τ_g является автоморфизмом группы G. Такие автоморфизмы называются внутренними.

Например, если $G = S_n$, $\alpha \in S_n$, $\sigma = (i_1, i_2, \ldots, i_k) \in S_n$, то $\tau_\alpha(\sigma) = (\alpha(i_1), \alpha(i_2), \ldots, \alpha(i_k))$. Т.е. автоморфизм τ_α сохраняет структуру независимых циклов в разложении подстановки.

Автоморфизм, который не является внутренним, называется внешним. Например, $\Phi : GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$, $\Phi(A) = (A^{-1})^t$ является внешним автоморфизмом. Действительно, при внутреннем автоморфизме характеристические числа не меняются. Матрицы $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ и $\Phi(A) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$ имеют различные характеристические числа, поэтому Φ не является внутренним автоморфизмом $GL_2(\mathbb{R})$

Если существует изоморфизм $f : G \to H$, то группы G и H называются изоморфными. Обозначение: $G \cong H$.

Предложение.

Пусть $f : G \to H$ – гомоморфизм групп. Тогда:

1) для любого $g \in G$ порядок элемента $f(g)$ делит порядок g;

2) если f – изоморфизм, то порядки g и $f(g)$ совпадают;

3) циклические группы одного порядка изоморфны.

Доказательство. 1) Пусть g – любой элемент группы G. Обозначим порядок g через k : $\operatorname{ord} g = k$. Тогда $g^k = e$, где e – единица группы G. Рассмотрим элемент $f(g^k)$. С одной стороны, $f(g^k) = f(e) = e$ – единица группы H, по свойству (1) гомоморфизмов групп. С другой стороны, $f(g^k) = f(g)^k$ по свойству (3) гомоморфизмов групп. Таким образом, $f(g)^k = e$. Согласно предложению из §2 $\operatorname{ord}(f(g))$ делит $k = \operatorname{ord} g$.

2) Пусть теперь $f : G \to H$ – изоморфизм групп. Если $h = f(g)$, то $f^{-1}(h) = g$. По 1) пункту $\operatorname{ord} h$ делит $\operatorname{ord} g$. По свойству (7) $f^{-1} : H \to G$ – тоже изоморфизм групп. Следовательно, по 1) $\operatorname{ord}(f^{-1}(h))$ делит $\operatorname{ord} h$. Но $f^{-1}(h) = g$, то есть $\operatorname{ord} g$ делит $\operatorname{ord} h$. Таким образом, получаем, что $\operatorname{ord} h | \operatorname{ord} g$ и $\operatorname{ord} g | \operatorname{ord} h$. Поскольку порядок – натуральное число, то $\operatorname{ord} g = \operatorname{ord} h$.

3) Пусть $G =< g >$, $H =< h >$, $|G| = |H|$. Тогда $f : G \to H$, $f(g^k) = h^k$ – изоморфизм. $\square$

Задача. Найти все гомоморфизмы из $\mathbb{Z}_n$ в $\mathbb{Z}_m$.

Пусть $f : \mathbb{Z}_n \to \mathbb{Z}_m$ гомоморфизм. Рассмотрим любой образующий в циклической группе $\mathbb{Z}_n$, например, $\overline{1}$. Имеем, $f(\overline{1}) = \overline{t} \in \mathbb{Z}_m$. Тогда по свойству (3) гомоморфизмов $f(\overline{k}) = kf(\overline{1}) = k\overline{t}$ для любого $\overline{k} \in \mathbb{Z}_n$. Поэтому для задания гомоморфизма f достаточно указать образ $\overline{1}$.

Так как порядок $\overline{1}$ в $\mathbb{Z}_n$ равен n, то согласно предложению $\mathrm{ord} f(\overline{1})$ делит n. Из предложения §2 имеем $\mathrm{ord}\overline{t} = \frac{m}{(m,t)}$. Таким образом, если $f : \mathbb{Z}_n \to \mathbb{Z}_m$ – гомоморфизм и $f(\overline{1}) = \overline{t}$, то $\frac{m}{(m,t)}|n$.

Условие $\mathrm{ord}\overline{t}|n$ является достаточным для того, чтобы отображение $f : \mathbb{Z}_n \to \mathbb{Z}_m$, заданное правилом $f(\overline{k}) = k\overline{t}$, было определено корректно и являлось гомоморфизмом. Действительно, если $\overline{k} = \overline{s}$, то $n|(k - s)$. Так как $\mathrm{ord}\overline{t}|n$, то $\mathrm{ord}\overline{t}|(k - s)$. Тогда из предложения §2 имеем $(k - s)\overline{t} = \overline{0}$ и, следовательно, $f(\overline{k}) = f(\overline{s})$. Поэтому отображение определено корректно. Так как $f(\overline{k_1} + \overline{k_2}) = f(\overline{k_1 + k_2}) = (k_1 + k_2)\overline{t} = k_1\overline{t} + k_2\overline{t} = f(\overline{k_1}) + f(\overline{k_2})$, то f является гомоморфизмом.

Например, найдем все гомоморфизмы из $\mathbb{Z}_3$ в $\mathbb{Z}_{36}$. Согласно сказанному выше, если $f(\overline{1}) = \overline{t}$, то $\frac{36}{(36,t)}|3$. Поэтому $(36, t) = 36$ или $(36, t) = 12$, где $0 \le t \le 35$. Следовательно, $\overline{t} \in \{\overline{0},\ \overline{12}, \overline{24}\}$. Таким образом, существует всего 3 гомоморфизма из $\mathbb{Z}_3$ в $\mathbb{Z}_{36}$: f_1, f_2 и f_3, где $f_1 \equiv \overline{0}$,
$f_2(\overline{0}) = \overline{0}$, $f_2(\overline{1}) = \overline{12}$, $f_2(\overline{2}) = \overline{24}$,
$f_3(\overline{0}) = \overline{0}$, $f_3(\overline{1}) = \overline{24}$, $f_2(\overline{2}) = \overline{12}$.

Упражнения.

3.1. Проверить какие из отображений групп $f : \mathbb{C}^* \to \mathbb{R}^*$ являются гомоморфизмами:

а) $f(z) = |z|$; б) $f(z) = 2|z|$; в) $f(z) = \frac{1}{|z|}$;
г) $f(z) = 1 + |z|$; д) $f(z) = |z|^2$; е) $f(z) = 1$;
ж) $f(z) = 2$.

3.2. Проверить какие из отображений являются гомоморфизмами групп:
а) $f : \mathbb{R} \to \mathbb{R}^*$, где $f(x) = e^x$;
б) $f : \mathbb{R} \to \mathbb{C}^*$, где $f(x) = \cos 2\pi x + i \sin 2\pi x$;
в) $f : M_n(\mathbb{R}) \to \mathbb{R}^*$, где $f(A) = a_{11}$;
г) $f : T_n(\mathbb{R}) \to D_n(\mathbb{R})$, где $f(\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}) =$

$$= \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}.$$

3.3. Найти ядро и образ гомоморфизмов из задач 3.1 и 3.2.

3.4. Какие из отображений задачи 3.1 являются изоморфизмами?

3.5. Для каких групп G отображение $f : G \to G$, определенное правилом (а) $f(x) = x^2$ или (б) $f(x) = x^{-1}$, является гомоморфизмом? При каком условии эти отображения являются изоморфизмами?

3.6. Построить изоморфизм между группами:

а) $\mathbb{Z}$ и $n\mathbb{Z}$;

б) $\mathbb{C}$ и $G = \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R}\}$ (относительно сложения).

3.7. Доказать, что не существует эпиморфизма $f : \mathbb{Q} \to \mathbb{Z}$ аддитивных групп.

3.8. Доказать, что $\mathbb{R}^+ \cong \mathbb{R}$ и $\mathbb{Q}^+ \ncong \mathbb{Q}$. (Здесь $\mathbb{R}^+ = \{a \in \mathbb{R} \mid a > 0\}$).

3.9. Доказать, что

а) группа 4-го порядка либо циклическая, либо изоморфна четверной группе Клейна;

б) группа 6-го порядка либо абелева, либо изоморфна S_3.

3.10. Выяснить, какие из перечисленных циклических групп $< a >$, порожденных элементом $a \in G$, изоморфны:

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

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

в) $G = \mathbb{C}^*,\ a = 2 - i$;

г) $G = GL_2(\mathbb{C}),\ a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;

д) $G = S_6,\ a = (3\ 2\ 6\ 5\ 1)$;

е) $G = \mathbb{Z},\ a = 3$;

ж) $G = \mathbb{R}^*,\ a = 10$.

3.11. Найти все гомоморфные отображения:

а) $\mathbb{Z}_6 \to \mathbb{Z}_6$; б) $\mathbb{Z}_6 \to \mathbb{Z}_{18}$; в) $\mathbb{Z}_{18} \to \mathbb{Z}_6$;

г) $\mathbb{Z}_{12} \to \mathbb{Z}_{15}$; д) $\mathbb{Z}_6 \to \mathbb{Z}_{25}$; е) $\mathbb{Z}_5 \to S_3$;

ж) $\mathbb{Z}_6 \to S_3$; з) $S_3 \to \mathbb{Z}_6$.

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

3.13. Найти группу автоморфизмов группы:

а) $\mathbb{Z}_5$; б) $\mathbb{Z}_6$; в) $\mathbb{Z}_8$; г) $\mathbb{Z}_9$.

3.14. Найти порядок группы автоморфизмов группы $Aut(Aut(Aut\ \mathbb{Z}_9))$.

3.15. Найти группу автоморфизмов группы:

а) $\mathbb{Z}$; б) $\mathbb{Z}_p$; в) S_3;

г) $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$;
д) Q_8 (группа кватернионов).

§4 Факторгруппа. Теоремы о гомоморфизмах

Пусть G – группа, H – подгруппа в G. **Левым смежным классом** элемента $g \in G$ называется множество $gH = \{gh|\ h \in H\} = \overline{g}$. **Правым смежным классом** элемента g называется множество $Hg = \{hg|\ h \in H\}$. Любой элемент из смежного класса называется его представителем.

Левые смежные классы либо не пересекаются, либо совпадают, причем $gH = \widetilde{g}H$ тогда и только тогда, когда $g^{-1}\widetilde{g} \in H$. Группа G является объединением непересекающихся левых смежных классов.

Все левые смежные классы группы G по подгруппе H имеют одинаковую мощностьравную мощности подгруппы H. Отсюда следует

Теорема Лагранжа. Пусть G − конечная группа. H − подгруппа в G. Тогда порядок подгруппы H делит порядок группы G.$\square$

Соответствие $gH \mapsto Hg^{-1}$ является биекцией между множеством левых смежных классов и множеством правых смежных классов, следовательно, количество левых смежных классов равно количеству правых смежных классов группы G по подгруппе H. Оно называется **индексом** группы G по подгруппе H и обозначается $(G : H)$.

Следствие. G − конечная группа. H − подгруппа в G, тогда $|G| = (G : H)|H|$. $\square$

Подгруппа $H \subset G$ называется **нормальной подгруппой**, если для любого $g \in G$
$gH = Hg$.

Подгруппа H в группе G нормальна тогда и только тогда, когда для любого $g \in G$ и любого $h \in H$ $ghg^{-1} \in H$. Т. е. нормальная подгруппа – это подгруппа, которая сохраняется относительно любого внутреннего автоморфизма группы G.

Задача. Доказать, что $SL_n(\mathbb{R})$ нормальная подгруппа в $GL_n(\mathbb{R})$.

Возьмем $A \in GL_n(\mathbb{R})$ и $B \in SL_n(\mathbb{R})$. Найдем определитель матрицы ABA^{-1}.
$\det ABA^{-1} = \det A \cdot \det B \cdot \det A^{-1} = \det A \cdot (\det A)^{-1} = 1$. Получаем, что $ABA^{-1} \in SL_n(\mathbb{R})$. Таким образом, $SL_n(\mathbb{R})$ – нормальная подгруппа.

Пусть H – нормальная подгруппа в G. Введем бинарную операцию на множестве смежных классов следующим образом: $\bar{a} \cdot \bar{b} = \overline{ab}$. Множество смежных классов с введенной операцией является группой, которая называется **факторгруппой** группы G по подгруппе H и обозначается через

G/H.

Отображение $p : G \to G/H : a \mapsto \overline{a}$ является эпиморфизмом групп и называется **канонической проекцией**. Ядро канонической проекции совпадает с подгруппой H.

Подгруппа $H = \{e\}$ нормальна в G. Так как $Kerp = H = \{e\}$, то каноническая проекция в данном случае является изоморфизмом между G и $G/\{e\}$. Смежный класс $\overline{g}$ любого элемента g по подгруппе H по определению состоит из одного элемента g: $\overline{g} = \{g\}$, поэтому G и $G/\{e\}$ отождествляют. Аналогично, G/G отождествляют с $\{e\}$.

Основная теорема о гомоморфизмах. Пусть $\varphi : G \to K$ – гомоморфизм групп с ядром $H = Ker\varphi$. Существует единственный гомоморфизм $\varphi^* : G/H \to K$, для которого коммутативна следующая диаграмма

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "p"'] & K \\ G/H \arrow[ur, "\varphi^*"'] & \end{tikzcd}$$

$\varphi^* \circ p = \varphi$. Гомоморфизм φ^* инъективен. Если φ сюръективно, то φ^* изоморфизм. $\square$

Задача. Доказать, что $GL_n(\mathbb{C})/H \cong \mathbb{R}^+$, где H подгруппа матриц модуль определителя которых равен 1.

Отметим, что H – нормальная подгруппа в $GL_n(\mathbb{C})$. Рассмотрим отображение $f : GL_n(\mathbb{C}) \to \mathbb{R}^+$, $f(A) = |\det(A)|$. Так как $|\det(AB)| = |\det(A)||\det(B)|$, то f является гомоморфизмом групп. Для любого положительного вещественного числа r существует матрица A из $GL_n(\mathbb{C})$, например,

$$\begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

такая что $f(A) = |\det(A)| = r$. Следовательно, f – эпиморфизм групп. При этом $Kerf = H$. Тогда по основной теореме о гомоморфизмах $GL_n(\mathbb{C})/H \cong \mathbb{R}^+$.

Вторая теорема о гомоморфизмах. Пусть G – группа, H, K – подгруппы в G и K – нормальная подгруппа в G. Тогда:

1) $HK = KH$ – подгруппа, содержащая K;

2) $H \cap K$ – нормальная подгруппа в H;

3) $HK/K \cong H/H \cap K$. $\square$

Задача. Найти факторгруппу S_4/V_4, где $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ – четверная группа Клейна.

В §3 было показано, что внутренние автоморфизмы сохраняют цикловую структуру подстановки, следовательно, V_4 – нормальная подгруппа в S_4. Рассмотрим подгруппу H в S_4, состоящую из подстановок, оставляющих на месте 4,
$H = \{e, (12), (13), (23), (123), (132)\} \subset S_4$. Нетрудно видеть, что $S_4 = H \cdot V_4$ ($|S_4| = 24$, а $|S_3| = 6$, $|V_4| = 4$). По второй теореме о гомоморфизмах $H \cdot V_4/V_4 \cong H/H \cap V_4$, $H \cap V_4 = \{e\}$, поэтому $S_4/V_4 \cong H \cong S_3$.

Теорема о соответствии. Пусть $\varphi : G \to K$ – эпиморфизм, тогда:

1) $\sigma : H \mapsto \varphi(H)$ – взаимно-однозначное соответствие между множеством подгрупп в G, содержащих ядро φ, и множеством подгрупп в K;

2) Если H – нормальная подгруппа в G, то $\varphi(H)$ – нормальная подгруппа в K;

3) H – нормальная подгруппа в G, содержащая ядро φ, то $G/H \cong K/\varphi(H)$. $\square$

Задача. Найти факторгруппу $d\mathbb{Z}/n\mathbb{Z}$, где $n = md$.

Возьмем в теореме о соответствии $G = \mathbb{Z}$, $K = d\mathbb{Z}$. Отображение $\varphi : \mathbb{Z} \to d\mathbb{Z} : \ \varphi(k) = dk$ – эпиморфизм. Пусть $H = m\mathbb{Z}$, тогда $\varphi(H) = dm\mathbb{Z} = n\mathbb{Z}$. По теореме о соответствии $d\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.

Терема о сокращении. Пусть G – группа, H, K – подгруппы в G и K – нормальная подгруппа в G, $K \subset H$. Тогда:

1) H/K – подгруппа в G/K;

2) Существует взаимно-однозначное соответствие между подгруппами в G, содержащими K и подгруппами в G/K;

3) Если H – нормальная подгруппа в G, то H/K – нормальная подгруппа в G/K и $G/H \cong (G/K)/(H/K)$. $\square$

Упражнения.

4.1. Найти левые и правые смежные классы:

а) группы S_3 по подгруппе $\{e, (12)\}$;

б) группы S_4 по подгруппе $H = \{e, (12), (13), (23), (123), (132)\}$;

в) группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}^+$;

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

д) группы $\mathbb{C}^*$ по подгруппе $\mathbb{T}^1 = \{z \in \mathbb{C} | |z| = 1\}$.

4.2. Доказать, что подгруппа H нормальна в G, если

а) G – абелева, H – любая ее подгруппа;

б) $G = S_n, H = A_n$;

в) G – произвольная группа, H – подгруппа индекса 2 в G;

г) $G = \{(a,b) \mid a,\ b \in \mathbb{Z}\}$ с операцией $(a,b)(c,d) = (a+(-1)^b c, b+d)$, $H = \{(a,0) \mid a \in \mathbb{Z}\}$;

д) $G = GL_n(\mathbb{R})$, $H = \{A \in GL_n(\mathbb{R}) | \det(A) > 0\}$;

е) $G = GL_n(\mathbb{C})$, $H = \{A \in GL_n(\mathbb{C}) | \det(A) \in \mathbb{R}^+\}$.

4.3. Доказать, что ядро гомоморфизма $f : G \to H$ является нормальной подгруппой в G.

4.4. Найти факторгруппы:

а) $\mathbb{R}^*/\mathbb{R}^+$;

б) $\mathbb{C}^*/\mathbb{R}^+$;

в) $\mathbb{C}^*/\mathbb{T}^1$, где $\mathbb{T}^1 = \{z \in \mathbb{C} || z| = 1\}$;

г) $\mathbb{T}^1/\mathbb{U}_n$, где $\mathbb{U}^n = \{z \in \mathbb{C} | z^n = 1\}$;

д) $\mathbb{C}^*/H_n$, где $H_n = \{z \in \mathbb{C} | arg(z) = \frac{2\pi k}{n}, k \in \mathbb{Z}\}$;

е) $\mathbb{C}^*/\mathbb{U}_n$;

ж) $H_n/\mathbb{R}^+$;

з) $H_n/\mathbb{U}_n$.

4.5. Доказать, что

а) $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$;

б)$GL_n(\mathbb{C})/SL_n(\mathbb{C}) \cong \mathbb{C}^*$;

в) $GL_n(\mathbb{R})/H \cong \mathbb{Z}_2$, где $H = \{A \in GL_n(\mathbb{R}) | \det(A) > 0\}$;

г) $GL_n(\mathbb{C})/H \cong \mathbb{T}^1$, где $H = \{A \in GL_n(\mathbb{C}) | \det(A) \in \mathbb{R}^+\}$;

д) $GL_n(\mathbb{R})/H \cong \mathbb{R}^+$, где $H = \{A \in GL_n(\mathbb{R}) || \det(A)| = 1\}$;

4.6. Доказать, что если $f : G \to H$ – эпиморфизм групп, то $|H|$ делит $|G|$.

4.7. Найти факторгруппы: а) $4\mathbb{Z}/12\mathbb{Z}$; б) $\mathbb{Z}_{12}$ по подгруппе порядка 3.

4.8. В факторгруппе $\mathbb{Q}/\mathbb{Z}$ найти наименьший неотрицательный представитель и порядок смежных классов:

а) $\overline{30,3}$; б) $\overline{-\frac{47}{5}}$; в) $\overline{1,37}$; г)$\overline{-1,25}$.

* * *

4.9. Доказать, что подгруппа, индекс которой есть наименьший простой делитель порядка группы, нормальна.

4.10. Доказать, что в факторгруппе $\mathbb{Q}/\mathbb{Z}$

а) каждый элемент имеет конечный порядок;

б) для каждого $n \in \mathbb{N}$ существует единственная подгруппа порядка n.

Список литературы

[1] Сборник задач по алгебре. Семестр 3./ Сост. С.А. Кириллов. - Н.Новгород: ННГУ, 1997.-34 с.

[2] Сборник задач по алгебре./Под ред. А.И. Кострикина. - М.: ФИЗМАТЛИТ, 2001. - 464 с.

[3] Кострикин А. И. Введение в алгебру. - М.: Наука, 1977. - 496 с.

ЗАДАЧИ ПО ТЕОРИИ ГРУПП. ЧАСТЬ I

Составители:
Михаил Иванович **Кузнецов**
Ольга Александровна **Муляр**
Надежда Александровна **Хорева** и др.

Практикум

Государственное образовательное учреждение высшего профессионального образования "Нижегородский государственный университет им. Н.И. Лобачевского".
603950, Нижний Новгород, пр. Гагарина, 23.
Подписано в печать . Формат 60x84 1/16.
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл.печ.л. Уч.-изд.л.
Заказ № . Тираж 100 экз.
Отпечатано в типографии Нижегородского госуниверситета им. Н.И. Лобачевского
603600, г. Нижний Новгород, ул. Большая Покровская, 37
Лицензия ПД № 18-0099 от 14.05.01