Введение в алгебру

Линдеманн Никита, МФТИ

31 августа 2021 г.

Содержание

1 Программа **2**

2 Понятие группы **3**

3 Смежные классы и теорема Лагранжа **7**

4 Нормальные подгруппы **8**

5 Отображения групп **10**

6 Факторгруппа **14**

7 Основная теорема о гомоморфизме **16**

8 Прямое произведение групп **17**

9 Группы малых порядков **19**

10 Другие алгебраические структуры **19**

Литература **21**

1 Программа

1. Основные свойства групп. Абелевы группы. Понятие подгруппы.
2. Правые и левые смежные классы по подгруппе. Теорема Лагранжа и следствия из нее.
3. Нормальные подгруппы, их свойства.
4. Отображения. Инъкция, сюръекция, биекция. Отображения групп: гомоморфизм и изоморфизм. Теорема о соответствии подгрупп при гомоморфизмах.
5. Отношение эквивалентности и факторгруппа.
6. Основная теорема о гомоморфизме.
7. Прямое произведение групп. Критерий разложимости группы в прямое произведение своих подгрупп.
8. Классификация групп малых порядков с точностью до изоморфизма.
9. Поле комплексных чисел. Алгебраическая, тригонометрическая и показательная запись комплексных чисел. Формула Муавра. Корни из комплексных чисел. Мультипликативная группа C^* и ее подгруппы.
10. Алгебраические структуры. Кольцо, поле, линейное пространство, алгебра.

2 Понятие группы

Рассмотрим преобразования плоскости, сохраняющие правильный треугольник (то есть переводящие треугольник в себя, лишь меняя местами его вершины). Всего есть два типа таких преобразований[1]: поворот вокруг центра треугольника (центр парвильного треугольника это точка пересечения его медиан) на угол кратный 120° и отражение относительно любой медианы. Тогда для треугольника ABC существуют всего 6 таких преобразований: Id, $\mathrm{R}_{2\pi/3}$, $\mathrm{R}_{4\pi/3}$, S_1, S_2, S_3, где Id – тождественное преобразование, R_α – поворот против часовой стрелки вокруг центра треугольника на угол α, S_n – симметрия относительно прямой l_n:

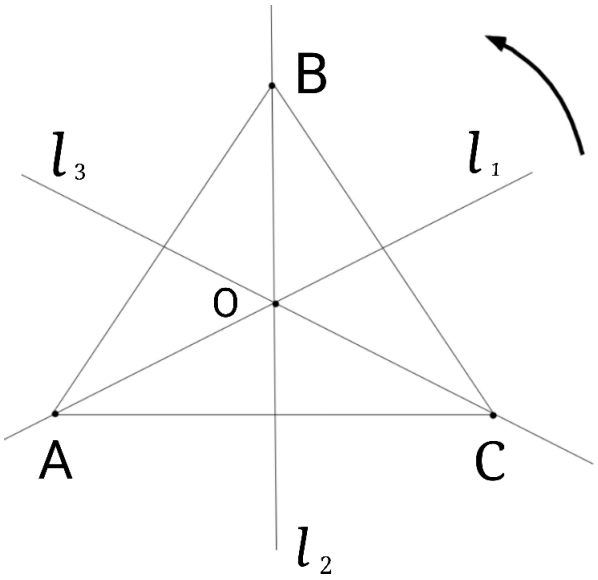

Рис. 1: Оси симметрии правильного треугольника.

Заметим, что других изометрий, переводящих треугольник в себя нет (это можно показать, используя лемму о трех гвоздях) и что комозиция любых двух описанных выше преобразований тоже является одним из этих преобразований. Заполним таблицу Кэли, считая, что сначала выполняется преобразование из верхней строки, потом из правого столбца (прямые l_1, l_2, l_3 при всех преобразованиях остаются на месте):

	Id	$\mathrm{R}_{\frac{2\pi}{3}}$	$\mathrm{R}_{\frac{4\pi}{3}}$	S_1	S_2	S_3
Id	Id	$\mathrm{R}_{\frac{2\pi}{3}}$	$\mathrm{R}_{\frac{4\pi}{3}}$	S_1	S_2	S_3
$\mathrm{R}_{\frac{2\pi}{3}}$	$\mathrm{R}_{\frac{2\pi}{3}}$	$\mathrm{R}_{\frac{4\pi}{3}}$	Id	S_2	S_3	S_1
$\mathrm{R}_{\frac{4\pi}{3}}$	$\mathrm{R}_{\frac{4\pi}{3}}$	Id	$\mathrm{R}_{\frac{2\pi}{3}}$	S_3	S_1	S_2
S_1	S_1	S_3	S_2	Id	$\mathrm{R}_{\frac{4\pi}{3}}$	$\mathrm{R}_{\frac{2\pi}{3}}$
S_2	S_2	S_1	S_3	$\mathrm{R}_{\frac{2\pi}{3}}$	Id	$\mathrm{R}_{\frac{4\pi}{3}}$
S_3	S_3	S_2	S_1	$\mathrm{R}_{\frac{4\pi}{3}}$	$\mathrm{R}_{\frac{2\pi}{3}}$	Id

Определение 2.1. Непустое множество G с заданной на нем внутренней бинарной операцией $* : G \times G \to G$ называется группой $(G, *)$, если выполнены следующие аксиомы:

1. Ассоциативность: $\forall\, a, b, c \in G$ выполнено $(a * b) * c = a * (b * c)$.

[1]На самом деле их гораздо больше, но мы рассматриваем только те преобразования, которые сохраняют расстояние между точками. Такие преобразования метрических пространств называются изометриями.

2. Наличие нейтрального элемента: $\exists\, e \in G : \forall\, a \in G$ выполнено $e * a = a * e = a$.

3. Наличие обратного элемента: $\forall\, a \in G\ \exists\, a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$.

Примеры групп:

1. Множество целых чисел относительно сложения – $(\mathbb{Z}, +)$.

2. Множество рациональных чисел без нуля относительно умножения – $(\mathbb{Q}^*, \cdot)$.

3. Множество матриц порядка n над полем вещественных чисел относительно операции матричного умножения – общая линейная группа $GL_n(\mathbb{R})$.

4. Множество квадртатных матриц порядка n над полем вещественных чисел с единичным определителем относительно матричного умножения – специальная линейная группа $SL_n(\mathbb{R})$.

5. Множество симметрий правильного n-угольника относительно композиции – группа диэдра D_n.

6. Множество перестановок из n элементов относительно композиции – симетрическая группа перестановок S_n.

7. Множество комплексных чисел относительно сложения $(\mathbb{C}, +)$.

8. Множество остатков от деления на n относительно сложения – группа $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0,1,\ldots,n-1\}$.

Утверждение 2.1. *Для всех элементов a и b группы G выполнено $(ab)^{-1} = b^{-1}a^{-1}$.*

Утверждение 2.2. *Единичный элемент в группе единственен.*

Утверждение 2.3. *Для заданного элемента g группы G существует единственный обратный к нему.*

Утверждение 2.4. *Если квадрат любого элемента группы равен единичному элементу, то группа абелева.*

Доказательство. Действительно, если $\forall\, a \in G \hookrightarrow a \cdot a = e$, то каждый элемент группы является обратным к самому себе: $a = a^{-1}$. Тогда $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ для любых $a, b \in G$, откуда и следует коммутативность группы. □

Определение 2.2. Непустое подмножество H группы $(G, *)$ называется подгруппой, что обозначается $H < G$ если:

1. Для любых $h_1, h_2 \in H$ верно $h_1 * h_2 \in H$.

2. Для любого $h \in H$ выполнено $h^{-1} \in H$.

Утверждение 2.5. ***(Критерий подгруппы)*** *Непустое подмножество H группы G является подгруппой тогда и только тогда, когда $ab^{-1} \in H$ для всех $a, b \in H$.*

Определение 2.3. Центр группы G – множество элементов данной группы, которые коммутируют со всеми её элементами: $Z(G) = \{g \in G \mid \forall\, x \in G\ gx = xg\}$.

Определение 2.4. Пусть A – некоторое множество. Его подмножества A и $\varnothing$ называются несобственными или тривиальными подмножествами.

Задача 2.1. Образует ли группу относительно сложения:

1. Множество всех действительных чисел.

   Да, так как из аксиоматического определения $\mathbb{R}$ следует, что вещественные числа являются абелевой группой по сложению (более того $\mathbb{R}$ – поле, а значит у него есть аддитивная и мультипликативная группы поля).

2. Множество всех неотрицательных действительных чисел.

   Нет, так как ни для одного элемента из этого множества (кроме 0) нет противоположного.

3. Множество всех рациональных чисел.

   Да, так как выполнены все аксиомы группы: сумма двух рациональных чисел есть рациональное число, для каждого рационального $q \in \mathbb{Q}$ существует противоположное $-q \in \mathbb{Q}$, и в $\mathbb{Q}$ есть нейтральный по сложению элемент 0 (как и в случае с вещественными числами, $\mathbb{Q}$ – поле).

4. Множество всех нечетных чисел.

   Очевидно, что это множество не является группой, так как сумма двух нечетных чисел есть четное число.

5. Множество всех чисто мнимых чисел с нулем.

   Да, так как это множество с точки зрения теории групп ничем не отличается от аддитивной группы вещественных чисел (то есть они изоморфны: $\mathbb{C}_i \cong \mathbb{R}$, здесь $\mathbb{C}_i = \{ai \mid a \in \mathbb{R}\}$).

Задача 2.2. Образует ли группу относительно умножения:

1. Множество всех рациональных чисел.

   Нет, так как в этом множестве присутствует необратимый элемент: $0 \in \mathbb{Q}$ (это единственная причина, почему это множество не является группой по умножению: $\mathbb{Q}^* = \mathbb{Q} \setminus 0$ уже является мультипликативной группой).

2. Множество всех положительных действительных чисел.

   Да, так как выполнены все аксиомы мультипликативной группы: произведение двух положительных действительных чисел есть положительное вещественное число, для каждого $a \in \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$ существует обратный $\dfrac{1}{a} \in \mathbb{R}_+$, и этому множеству принадлежит еденица $1 \in \mathbb{R}_+$.

3. Множество всех ненулевых комплексных чисел.

   Да, так как $\mathbb{C}$ – поле, то $\mathbb{C}^*$ – его мультипликативная группа.

4. Множество всех комплексных чисел, равных по модулю 1.

   Да: из того, что $z_1, z_2 \in \mathbb{C}_1 = \{z \in \mathbb{C} \mid |z| = 1\}$, следует, что $z_1 z_2 \in \mathbb{C}_1$ так как $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$; если $z \in \mathbb{C}_1$, то $z^{-1} \in \mathbb{C}_1$ так как $|z^{-1}| = |z|^{-1}$, и в этом множестве есть нейтральный по умножению элемент $1 \in \mathbb{C}_1$.

5. Множество всех ненулевых чисто мнимых комплексных чисел.

   Нет, так как произведение двух чисто мнимых комплексных чисел всегда вещественное число.

Задача 2.3. Образует ли группу данное множество квадратных матриц порядка n:

1. Относительно сложения:

   (a) Множество всех верхних треугольных матриц.

   Да, так как сумма двух верхних треугольных матриц тоже является верхней треугольной матрицей, обратная к такой матрице тоже верхняя треугольная, и нулевая матрица, являющаяся нулем группы тоже частный случай верхней треугольной матрицы.

   (b) Множество всех матриц с нулевым следом.

   Да, так как достаточно очевидно, что если $\mathrm{tr}(A) = 0, \mathrm{tr}(B) = 0$, то $\mathrm{tr}(A+B) = 0$, если $\mathrm{tr}(A) = 0$, то $\mathrm{tr}(-A) = 0$. Нейтральный элемент – нулевая матрица.

   (c) Множество всех вырожденных матриц.

   Нет, так как суммой двух вырожденных матриц может быть матрица с ненулевым определителем:
   $$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

2. Относительно умножения:

   (a) Множество всех невырожденных матриц.

   Да, так как по свойству определителя $|A^{-1}| = |A|^{-1}$, $|A \cdot B| = |A| \cdot |B|$, и нейтральный элемент по умножению E принадлежит этому множеству.

   (b) Множество всех матриц, в каждой строке и столбце которых один элемент равен 1, а все остальные – нулю.

   Да, так как матричное умножение ассоциативно, в этом множестве есть единичная матрица, и любая матрица, в каждой строке и столбце которой ровно один элемент равен 1, а все остальные равны нулю, обратима (определитель таких матриц равен ± 1 в зависимости от четности перестановки столбцов единичной матрицы E).

Утверждение 2.6. *Если a, b, c – элементы группы $(G, +)$, то $a + c = b + c \Leftrightarrow a = b$.*

Доказательство. $\boxed{\Leftarrow}$ Если $a = b$, то
$$a = a \Rightarrow a + c = a + c = \big|a = b\big| = b + c.$$
$\boxed{\Rightarrow}$ Обратно, пусть $a + c = b + c = A$, тогда
$$A = A \Rightarrow A - c = A - c \Rightarrow (a + c) - c = (b + c) - c \Rightarrow a = b.$$
□

Задача 2.4. Является ли на множестве $\mathbb{Z}$ операция
$$a \circ b = \begin{vmatrix} 0 & a \\ b & 0 \end{vmatrix} = -ab$$
бинарной, коммутативной, ассоциативной? Обладает ли система $(\mathbb{Z}, \circ)$ нейтральным элементом, если да, то каким? Является ли заданная операция обратимой?

Задача 2.5. Найти порядок элемента $\begin{pmatrix} 2 & -1 \\ 3 & -2 \end{pmatrix}$ в группе $GL_2(\mathbb{C})$.

Задача 2.6. Доказать, что $(\mathbb{Z}, \circ)$, гдt $m \circ n = (1 + m)(1 + n) - 1$, – коммутативная полугруппа. Найти все обратимые элементы.

3 Смежные классы и теорема Лагранжа

Определение 3.1. Порядком группы G называется количество элементов в группе и обозначается $|G|$.

Определение 3.2. Порядком элемента группы $g \in G$ называется

$$|g| = \mathrm{ord}(g) = \min_{n \in \mathbb{N}} \{n \mid g^n = e\}.$$

Определение 3.3. Пусть $H < G$ и $g \in G$, тогда

$gH = \{gh \mid h \in H\}$ – левый смежный класс элемента $g \in G$ по подгруппе H.

$Hg = \{hg \mid h \in H\}$ – правый смежный класс элемента $g \in G$ по подгруппе H.

Определение 3.4. Пусть $H < G$, тогда

G/H – множество всех левых смежных классов группы G по подгруппе H.

$H\backslash G$ – множество всех правых смежных классов группы G по подгруппе H.

Утверждение 3.1. *Пусть $a, b \in G$ и $H < G$. Тогда $aH \cap bH \neq \emptyset \Rightarrow aH = bH$.*

Доказательство. Пусть $aH \cap bH \neq \emptyset$, это значит, что $\exists\, h_1, h_2 \in H : ah_1 = bh_2 \Rightarrow$

$$a = bh_2h_1^{-1} \Rightarrow a \in bH \Rightarrow \forall\, h \in H \hookrightarrow ah \in bH \Rightarrow aH \subseteq bH.$$

$$b = ah_1h_2^{-1} \Rightarrow b \in aH \Rightarrow \forall\, h \in H \hookrightarrow bh \in aH \Rightarrow bH \subseteq aH.$$

Из последних двух вложений получаем, что $aH = bH$. □

Утверждение 3.2. *Для любого элемента группы $g \in G$ и подгруппы $H < G$ выполнено $|gH| = |H|$.*

Утверждение 3.3. *Для любой подгруппы $H < G$ количество всех левых смежных классов и правых смежных классов группы G по подгруппе H совпадают:*

$$|G/H| = |H\backslash G| = |G : H|,$$

и это количество называется индексом группы G по подгруппе H.

Утверждение 3.4. *Пусть $H < G$, тогда группа G представима в виде дезъюнктного объединения левых смежных классов группы G по подгруппе H:*

$$G = \bigsqcup_{g \in G} gH.$$

Теорема 3.1 (Лагранжа). *Пусть $H < G$, тогда порядок группы G равен произведению порядка подгруппы H на индекс группы G по подгруппе H:*

$$|G| = |H| \cdot |G : H|.$$

Задача 3.1. Пусть $K < H < G$, доказать, что $|G : K| = |G : H| \cdot |H : K|$.

Утверждение 3.5. *Пусть g – элемент группы G, тогда $g^{|G|} = e$.*

Доказательство. Рассмотрим циклическую подгруппу $H = \langle g \rangle < G$, ее порядок равен порядку элемента g: $|H| = |g|$. Согласно теореме Лагранжа

$$g^{|G|} = g^{|H| \cdot |G:H|} = (g^{|H|})^{|G:H|} = e^{|G:H|} = e.$$

□

Определение 3.5. Функция Эйлера – целочисленная функция $\varphi(n)$ от натурального агрумента n, значение которой равно количеству натуральных чисел, не превышающих n и взаимно простых с ним.

Теорема 3.2. ***(Эйлера)*** *Если натуральные числа a и n взаимно просты, то*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Доказательство. Рассмотрим мультипликативную группу $\mathbb{Z}_n^* = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ обратимых элементов кольца $\mathbb{Z}_n$. Очевидно, что ее порядок равен функции Эйлера от числа n: $|\mathbb{Z}_n^*| = \varphi(n)$ (это следует из определения функции Эйлера). Так как $(a, n) = 1$, то соответствующий $a \in \mathbb{R}$ элемент $\overline{a}\mathbb{Z}_n$ является обратимым и принадлежит группе $\mathbb{Z}_n^*$, при этом элемент $\overline{a}$ порождает циклическую подгруппу $H = \langle \overline{a} \rangle$. Согласно теореме Лагранжа порядок подгруппы H делит порядок группы $\mathbb{Z}_n^*$, равный $\varphi(n)$, откуда следует, что $\overline{a}^{\varphi(n)} = \overline{1}$. □

Задача 3.2. Пусть G – циклическая группа порядка 20. Найти все элементы $a \in G$ такие, что $a^5 = e$.

Задача 3.3. В циключеской группе порядка 24 найти все элементы a, удовлетворяющие условию $a^6 = e$ и все элементы порядка 6.

Задача 3.4. Пусть X – группа симметрий прямоугольника (не являющегося квадратом), а H – подгруппа, состоящая из поворотов. Найти левые и правые смежные классы группы X по подгруппе H.

4 Нормальные подгруппы

Определение 4.1. Подгруппа $H < G$ является нормальной, что обозначается как $H \triangleleft G$, если для всех $g \in G$ выполнено $gH = Hg$, то есть $G/H = H\backslash G$.

Примеры нормальных подгрупп:

1. $H \triangleleft G$, если G – абелева группа и $H < G$.
2. $G \triangleleft G$, $\{e\} \triangleleft G$.

Утверждение 4.1. *Если $H_1 \triangleleft G$ и $H_2 \triangleleft G$, то $H_1 \cap H_2 \triangleleft G$.*

Утверждение 4.2. *Если $H_1 \triangleleft G$ и $H_2 < G$, то $H_1 H_2 = \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\} < G$.*

Утверждение 4.3. *Если $H_1 \triangleleft G$ и $H_2 \triangleleft G$, то $H_1 H_2 \triangleleft G$.*

Теорема 4.1 (Критерий нормальной подгруппы). *Подгруппа $H < G$ является нормальной тогда и только тогда, когда для всех элементов группы $g \in G$ выполнено*

$$gHg^{-1} = H.$$

Задача 4.1. Найти порядки элементов и подгрупп в группах:

1. $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

   Очевидно, что 1 – порождающий элемент, значит $\langle 1\rangle = \mathbb{Z}_6$ и $|\langle 1\rangle| = |\mathbb{Z}_6| = 6$. Двойка образует подгруппу четных чисел: $\langle 2\rangle = \{0, 2, 4\} \lhd \mathbb{Z}_6$ (все подгруппы данной группы нормальные так как сама группа абелева), а значит, $|\langle 2\rangle| = |\langle 4\rangle| = 3$. Следующая подгруппа – подгруппа состоящая из двух элементом $\langle 3\rangle = \{0, 3\} \Rightarrow |\langle 3\rangle| = 2$. И последняя подгруппа – подгруппа с образующим элементом 5: $\langle 5\rangle = \langle 1\rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$, следовательно, $|\langle 5\rangle| = 6$. Заметим, что порядки всех подгрупп делят порядок группы, в соответствии с теоремой Лагранжа.

2. $\left(\mathbb{Z}/7\mathbb{Z}\right)^* = \{1, 2, 3, 4, 5, 6\}$.

   Здесь уже не так очевидно, какие элементы являются образующими. Будем строить подгруппы, выбирая каждый раз в качестве образующего новый элемент, начиная с двойки:
   $2 \to 4 \to 1$, значит, $\langle 2\rangle = \langle 4\rangle = \{1, 2, 4\}$.
   $3 \to 2 \to 6 \to 4 \to 5 \to 1$, значит, элементы 5 и 3 – образующие: $\langle 3\rangle = \langle 5\rangle = \left(\mathbb{Z}/7\mathbb{Z}\right)^*$.
   $6 \to 1$, следовательно, $\langle 6\rangle = \{1, 6\}$.

Определение 4.2. Пусть x, g – элементы группы G, тогда элемент $g^x = x^{-1}gx \in G$ называется сопряженным к g с помощью x.

Задача 4.2. Доказать, что порядки сопряженных элементов g и g^x равны.

Задача 4.3. Доказать, что

1. $g^{xy} = (g^x)^y$.
2. $(g_1g_2)^x = g_1^x g_2^x$.
3. $(g^{-1})^x = (g^x)^{-1}$.

Задача 4.4. Определить разбиение симметрической группы $S_3 = \{e, (12), (13), (23), (123), (321)\}$ на левые и правые смежные классы

1. По подгруппе $H = \{e, (23)\}$.

   По определению правый смежный класс группы S_3 по подгруппе H – это множество, состоящее из множеств вида $Hg = \{hg \mid h \in H\}$ (аналогично определяется и левый смежный класс), где представитель смежного класса g пробегает всю группу S_3.

   Пусть $g \in S_3 = \{e, (12), (13), (23), (123), (321)\}$. Построим смежные классы по подгруппе H с разными представителями:

$$g = e \Rightarrow \quad He = eH = H$$

$$g = (12) \Rightarrow \quad H(12) = \{(12), (132)\},\ \ (12)H = \{(12), (231)\}$$
$$g = (13) \Rightarrow \quad H(13) = \{(13), (123)\},\ \ (12)H = \{(12), (213)\}$$
$$g = (23) \Rightarrow \quad H(23) = \{(23), e\},\ \ (23)H = \{(23), e\}$$
$$g = (123) \Rightarrow \quad H(123) = \{(123), (13)\},\ \ (123)H = \{(123), (21)\}$$
$$g = (321) \Rightarrow \quad H(321) = \{(321), (12)\},\ \ (321)H = \{(321), (13)\}$$

2. По подгруппе $K = \{e, (123), (321)\}$.

   Пусть $g \in S_3 = \{e, (12), (13), (23), (123), (321)\}$. Аналогично предыдущему пункту построим смежные классы по подгруппе K с разными представителями:

$$g = e \Rightarrow \quad Ke = eK = K$$

$$g = (12) \Rightarrow \quad K(12) = \{(12), (13), (23)\},\ (12)K = \{(12), (23), (13)\}$$
$$g = (13) \Rightarrow \quad K(13) = \{(13), (32), (12)\},\ (13)K = \{(13), (21), (23)\}$$
$$g = (23) \Rightarrow \quad K(23) = \{(23), (21), (31)\},\ (23)K = \{(23), (13), (21)\}$$
$$g = (123) \Rightarrow \quad K(123) = \{(123), (132), e\},\ (123)K = \{(123), (132), e\}$$
$$g = (213) \Rightarrow \quad K(213) = \{(213), e, (123)\},\ (213)K = \{(213), e, (123)\}$$

   Так как $\forall\, g \in S_3$ правые и левые межные классы по подгруппе K совпадают: $gK = Kg$, то, по определению, K является нормальной подгруппой в S_3: $S_3 \rhd K$.

Утверждение 4.4. *Группа простого порядка циклическая.*

Доказательство. Пусть группа G имеет простой порядок $p = |G|$. Пусть $g \neq e \in G$: $|g| = n$, если $1 \leq n < p$, то $\{e, g, g^2, \ldots, g^{n-1}\} \leq G$ и тогда, в силу теоремы Лагранжа, p кратно n. Но так как p – простое, то либо $|g| = 1$, либо $|g| = p$. А так как $g \neq e$, то $|g| > 1$.

Заметим, что любой элемент (кроме нейтрального) группы простого порядка является порождающим. □

Задача 4.5. Доказать, что если $H < G$ и $|G : H| = 2$, то $H \lhd G$.

5 Отображения групп

Определение 5.1. Отображение $f : X \to Y$ – инъекция, если из того, что $f(x) = f(y)$ следует, что $x = y$, то есть разные элементы X отображаются в разные элементы в Y.

Определение 5.2. Отображение $f : X \to Y$ – сюръекция, если для всех $y \in Y$ найдется $x \in X$ такой, что $f(x) = y$, то есть каждый элемент из Y образ некоторого элемента из X.

Определение 5.3. Отображение $f : X \to Y$ – биекция (взаимно-однозначное отображение), если f одновременно является сюръективным и инъективным отображением.

Определение 5.4. Пусть $(G, \cdot)$ и $(S, *)$ – группы, отображение $f : G \to S$ называется гомоморфизмом, если для всех $a, b \in G$ выполнено $f(a \cdot b) = f(a) * f(b)$.

Определение 5.5. Эпиморфизм – это сюръективный гомоморфизм.

Определение 5.6. Мономорфизм – это инъективный гомоморфизм.

Определение 5.7. Изоморфизм – это биективный гомоморфизм.

Определение 5.8. Эндоморфизм – это гомоморфизм группы в себя

Определение 5.9. Автоморфизм – это изоморфизм группы в себя.

Определение 5.10. Образом отображения двух групп $\varphi : G \to S$ называется множество

$$\operatorname{Im} \varphi = \{\varphi(g) \mid g \in G\} = \varphi(G).$$

Определение 5.11. Ядром отображения двух групп $\varphi : G \to S$ называется множество

$$\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = e_S\} = \varphi^{-1}(e_S).$$

Примеры отображения групп:

1. Отображение $\varphi : G \to S$, которое всем элементам $g \in G$ сопоставляет нейтральный элемент $e_S \in S$ по формуле $\varphi(g) = e_S$, называется тривиальным гомоморфизмом.

2. Для произвольной группы G можно определить тривиальный изоморфизм из группы в себя $\varphi : G \to G$ правилом $\varphi(g) = g$.

3. Отображение $\varphi : \mathbb{R} \to \mathbb{R}^*$, заданное правилом $\varphi(x) = e^x$, является изоморфизмом из аддитивной группы вещественных чисел в мультипликативную группу вещественных чисел.

4. Определитель как полилинейное кососимметричное отображение, действующее из группы невырожденных матриц над полем $\mathbb{F}$ в мультипликативную группу поля $\mathbb{F}^*$, $det : GL_n(\mathbb{F}) \to \mathbb{F}^*$ является гомоморфизмом.

5. Пусть x – фиксированный элемент группы G, тогда отображение $\varphi_x(g) = x^{-1}gx$ является автоморфизмом группы G.

6. Пусть n – некоторое натуральное число. Отображение $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, сопоставляющее целому числу его остаток от деления на n, является эпиморфизмом.

Задача 5.1. Доказать, что в примерах, приведенных выше, заданы соответствующие отображения групп и найти ядро и образ для каждого отображения.

Утверждение 5.1. *При гомоморфизме групп $\varphi : G \to S$ нейтральный элемент первой группы переходит в нейтральный элемент второй группы: $\varphi(e_G) = e_S$, а так же $\forall\, g \in G$ верно $\varphi(g^{-1}) = \varphi(g)^{-1}$.*

Доказательство. Рассмторим произвольный элемент $a \in G$, для него выполнено $\varphi(a) = \varphi(e_G \cdot a) = \varphi(e_G)\varphi(a)$, значит $\varphi(e_G) \in S$ – нейтральный элемент в группе S, то есть $\varphi(e_G) = e_S$.

Для доказательства второго факта положим $\varphi(g) = s \in S$ и рассмотрим $e_S = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = s\varphi(g^{-1})$, откуда следует, что $\varphi(g^{-1}) = s^{-1} = \varphi(g)^{-1}$. □

Утверждение 5.2. *Пусть $\varphi : G \to S$ – гомоморфимз, тогда $\operatorname{Im}\varphi < S$ и $\operatorname{Ker}\varphi < G$.*

Задача 5.2. Доказать, что ядро изоморфизма тривиально.

Задача 5.3. Изоморфны ли мультипликативные группы $\mathbb{R}^*$ и $\mathbb{C}^*$?

Утверждение 5.3. *Ядро гомоморфизма является нормальной подгруппой в группе, из которой он действует.*

Доказательство. Пусть $\varphi : G \to S$ – заданный гомоморфизм групп. По определению $\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = e_S \in S\}$. Покажем, что ядро – подгруппа: действительно, $\forall\, k_1, k_2 \in \operatorname{Ker}\varphi$ верно, что $k_1k_2, k_1^{-1} \in \operatorname{Ker}\varphi$ так как если $\varphi(k_1) = \varphi(k_2) = e_S$, то $\varphi(k_1k_2) = \varphi(k_1)\varphi(k_2) = e_S \in \operatorname{Ker}\varphi$ и $\varphi(k_1^{-1}) = \varphi(k_1)^{-1} = e_S^{-1} = e_S \in \operatorname{Ker}\varphi$. Нормальность этой подгруппы следует из того факта, что нейтральный элемент коммутирует со всеми элементами группы: $\forall\, g \in G$ и $\forall\, k \in \operatorname{Ker}\varphi$ верно, что $gk = kg$, так как $\varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)e_S = \varphi(g)$ и аналогично $\varphi(kg) = \varphi(k)\varphi(g) = e_S\varphi(g) = \varphi(g)$, это и означает, что $\operatorname{Ker}\varphi \lhd G$. □

Задача 5.4. Доказать, что композиция гомоморфизмов групп $\psi \circ \varphi$, где $\varphi : G \to H$ и $\psi : H \to K$, – гомоморфизм.

Задача 5.5. Доказать, что матрицы вида $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$, где $x, y \in \mathbb{R}$ образуют аддитивную группу, изоморфную $(\mathbb{C}, +)$, а ненулевые матрицы того же вида – мультипликативную группу, изоморфную $(\mathbb{C}^*, \cdot)$.

Доказательство. Для доказательства изоморфности аддитивных групп построим в явном виде изоморфизм $\varphi : (M_2, +) \to (\mathbb{C}, +)$, где $(M_2, +)$ – группа, состоящая из матриц указанного вида. Сопоставим каждому комплексному числу матрицу по правилу: $\varphi(z) = \varphi(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$. Биективность такого отображения очевидна, проверим, что это гомоморфизм:

$$\varphi(z_1 + z_2) = \varphi((x_1 + iy_1) + (x_2 + iy_2)) = \varphi((x_1 + x_2) + (y_1 + y_2)i) = \begin{pmatrix} x_1 + x_2 & -y_1 - y_2 \\ y_1 + y_2 & x_1 + x_2 \end{pmatrix} =$$

$$= \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix} = \varphi(z_1) + \varphi(z_2).$$

Аналогично докажем второй факт. Покажем, что отображение $\varphi(z) = \varphi(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ является гомоморфизмом и мультипликативных групп $(M_2, \cdot)$ и $(\mathbb{C}, \cdot)$. Действительно:

$$\varphi(z_1 z_2) = \varphi((x_1 + iy_1)(x_2 + iy_2)) = \varphi((x_1x_2 - y_1y_2) + (x_2y_1 + x_1y_2)i) =$$
$$\begin{pmatrix} x_1x_2 - y_1y_2 & -x_1y_2 - x_2y_1 \\ x_2y_1 + x_1y_2 & x_1x_2 - y_1y_2 \end{pmatrix} = \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix} = \varphi(z_1)\varphi(z_2).$$

□

Утверждение 5.4. *Множество автоморфизмов группы G, которое обозначается как $\mathrm{Aut}(G)$, образует группу относительно операции композиции.*

Утверждение 5.5. *Пусть $\varphi : G \to H$ – гомоморфизм и $g \in G$, тогда $|\varphi(g)|$ делит $|g|$.*

Задача 5.6. Доказать, что не существует эпиморфизма $\varphi : C_5 \to C_3$ (C_n – циклическая группа порядка n).

Теорема 5.1. ***(Критерий инъективности)*** *Гомоморфизм $\varphi : G \to H$ является мономорфизмом тогда и только тогда, когда $\mathrm{Ker}\,\varphi = \{e_G\}$.*

Доказательство. Пусть φ – инъкция. Тогда из того, что $\varphi(x) = \varphi(y)$ следует, что $x = y$ для всех $x, y \in G$. Пусть $g \in \mathrm{Ker}\,\varphi$, тогда $\varphi(g) = e_H$, но при этом, так как φ – гомоморфизм, то $\varphi(e_G) = e_H$. Следовательно, $g = e_G$, то есть $\mathrm{Ker}\,\varphi = \{e_G\}$.

Обратно, пусть $\mathrm{Ker}\,\varphi = \{e_G\}$. Пусть при этом $\varphi(x) = \varphi(y)$ для некоторых $x, y \in G$, тогда

$$e_H = \varphi(x)(\varphi(y))^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) \Rightarrow xy^{-1} \in \mathrm{Ker}\,\varphi \Rightarrow xy^{-1} = e_G \Rightarrow x = y.$$

Это означает, что φ – инъекция, то есть мономорфизм. □

Задача 5.7. Доказать, что гомоморфизм $\varphi : G \to H$ является эпиморфизмом тогда и только тогда, когда $\mathrm{Im}\,\varphi = H$.

Утверждение 5.6. *Пусть $H < G$, тогда существует гомоморфизм φ, такой, что* $\operatorname{Im}\varphi = H$.

Доказательство. Пусть $\varphi : G \to G$ – автоморфизм группы G, заданный правилом $\varphi(g) = g$ для всех $g \in G$. Тогда сужение $\varphi\big|_H$ – искомый гомоморфизм, образом которого является H. □

Теорема 5.2. *Пусть $\varphi : G \to H$ – гомоморфизм и $K = \operatorname{Ker}\varphi$. Тогда для всех $g \in G$ выполнено*

$$\varphi^{-1}(\varphi(g)) = gK = Kg,$$

где $\varphi^{-1}(h) = \{g \in G \mid \varphi(g) = h\}$ – полный прообраз элемента $h \in H$.

Доказательство. Пусть $a \in G$, тогда

$$a \in \varphi^{-1}(\varphi(g)) \Leftrightarrow \varphi(a) = \varphi(g) \Leftrightarrow e_H = (\varphi(g))^{-1}\varphi(a) = \varphi(g^{-1}a) \Leftrightarrow g^{-1}a \in K \Leftrightarrow a \in gK.$$

Аналогично показывается, что $a \in Kg$. Так как $a \in \varphi^{-1}(\varphi(g)) \Leftrightarrow a \in Kg$, $a \in gK$, то $\varphi^{-1}(\varphi(g)) = gK = Kg$. □

Таким образом мы показали, что образом гомоморфизма может быть любая подгруппа, а ядром только нормальная.

Задача 5.8. Доказать, что существует ровно одна (с точностью до изоморфизма) группа G простого порядка p.

Задача 5.9. Доказать, что группа диэдра D_4 степени 4 (группа преобразований плоскости, сохранющих квадрат) и мультипликативная группа кватернионов Q_8 не изоморфны.

Доказательство. Известно, что $Q_8 = \{\pm 1, \pm i, \pm j, \pm k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\}$ и $D_4 = \{\mathrm{Id}, \mathrm{R}_{\frac{\pi}{2}}, \mathrm{R}_{\pi}, \mathrm{R}_{\frac{3\pi}{2}}, \mathrm{S}_1, \mathrm{S}_2, \mathrm{S}_3, \mathrm{S}_4\}$, где Id – тождественное преобразование, R_α – поворот вокруг центра квадрата на угол α, а $\mathrm{S}_1, \mathrm{S}_2, \mathrm{S}_3, \mathrm{S}_4$ – четыре отражения (два относительно диоганалей и два относительно серединных перпедикуляров квадрата).

Рассмотрим порядки элементов в группе Q_8: $|\pm i| = |\pm j| = |\pm k| = 4$, $|-1| = 2$. Для группы D_4: $|\mathrm{S}_1| = |\mathrm{S}_2| = |\mathrm{S}_3| = |\mathrm{S}_4| = 2$, $|\mathrm{R}_{\frac{\pi}{2}}| = 4$, $|\mathrm{R}_{\pi}| = 2$, $|\mathrm{R}_{\frac{3\pi}{2}}| = 4$. Из того факта, что в Q_8 только один элемент порядка два, в то врямя как в группе D_4 целых пять элементов второго порядка, делаем вывод, что данные группы не могут быть изоморфны: $D_4 \ncong Q_8$. □

Задача 5.10. Доказать, что мультипликативная группа $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$ не изоморфна аддитивной группе $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}_4$, хотя в обеих группах по 4 элемента.

Доказательство. Мы знаем, что $\left(\mathbb{Z}/8\mathbb{Z}\right)^* = \{1, 3, 5, 7\}$ и $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Установить отсутствие изоморфизма можно, перебрав все возможные $4! = 24$ взаимно-однозначные отображения (биекции) между группами, но мы поступим более рационально. Пусть все-таки изоморфизм $\varphi : \mathbb{Z}_4 \to \left(\mathbb{Z}/8\mathbb{Z}\right)^*$ существует, тогда $\varphi(0) = 1$. Рассмотрим, куда может отображаться $1 \in \mathbb{Z}_4$. Очевидно, что $1 + 1 = 2 \neq 0 \in \mathbb{Z}_4$, но это значит, что $1 \in \mathbb{Z}_4$ не может при изоморфизме переходить ни в один элемент группы $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$: если $\varphi(1) = 3$, то $\varphi(1+1) = \varphi(2) = \varphi(1)\varphi(1) = 3 \cdot 3 = 1$, что при биекции невозможно, так как в единицу группы $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$ переходит ноль группы $\mathbb{Z}_4$, если предположить, что $\varphi(1) = 5$, то тоже легко прийти к противоречию таким же способом $\varphi(1+1) = \varphi(2) = \varphi(1)\varphi(1) = 5 \cdot 5 = 1$, аналогично и при $\varphi(1) = 7$ противоречие – $\varphi(1+1) = \varphi(2) = \varphi(1)\varphi(1) = 7 \cdot 7 = 1$. Значит, $\left(\mathbb{Z}/8\mathbb{Z}\right)^* \ncong \mathbb{Z}/4\mathbb{Z}$ □

Теорема 5.3 (Теорема о соответствии подгрупп при гомоморфизмах.). *Пусть $\varphi : G \to K$ – гомоморфизм. Тогда, если $H < G$, то $S = \varphi(H) = \{\varphi(h) \mid h \in H\}$ – подгруппа в группе K.*

Доказательство. Воспользуемся критерием подгруппы, согласно которому $S < K \Leftrightarrow ab^{-1} \in S$ для всех $a, b \in S$. Пусть $a = \varphi(h_1)$, $b = \varphi(h_2) \in S$, тогда, в силу того, что $H < G$ и φ – гомоморфимз, получим

$$ab^{-1} = \varphi(h_1)\big(\varphi(h_2)\big)^{-1} = \varphi(h_1)\varphi(h_2^{-1}) = \varphi(h_1 h_2^{-1}) = \varphi(h) \in S,\ h \in H.$$

□

Задача 5.11. Постороить изоморфизм мультипликативной группы матриц вида $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, где $k \in \mathbb{Z}$, в аддитивную группу целых чисел.

6 Факторгруппа

Определение 6.1. Отношение эквивалентности $\sim$ на множестве X – это бинарное отношение, такое, что для всех $a, b, c \in X$ выполнены аксиомы

1. $a \sim a$ – рефлексивность.
2. $a \sim b \Rightarrow b \sim a$ – симметричность.
3. $a \sim b$, $b \sim c \Rightarrow a \sim c$ – транзитивность.

Примеры отношений эквивалентности:

1. Равенство чисел.
2. Подобие треугольников.
3. Параллельность прямых.
4. Изоморфизм групп.

Задача 6.1. На множестве $\mathbf{M}$ квадратных матриц порядка n задано отношение $A \sim B \Leftrightarrow$ существует обратимая матрица $S \in \mathbf{M}$ такая, что $B = S^{-1}AS$. Доказать, что заданое отношение $\sim$ является отношением эквивалентности.

Задача 6.2. Доказать, что изоморфизм групп является отношением эквивалентности.

Определение 6.2. Пусть на множестве X задано отношение эквивалентности $\sim$ и $x \in X$, тогда $[x] = \{y \in X \mid x \sim y\}$ – класс эквивалентности элемента $x \in X$, а x называют представителем класса эквивалентности $[x]$.

Теорема 6.1. *Заданное на мнжестве X отношение эквивалентности $\sim$ разбивает множество X на непересекающиеся классы.*

Доказательство. Так как отношение эквивалентности рефлексивно, то множество X можно представить в виде

$$X = \bigcup_{x \in X} [x].$$

Докажем, что классы эквивалентности $[x]$ и $[y]$ либо не пересекаются, либо совпадают. Пусть $[x] \cap [y] \neq \emptyset$, тогда существует элемент a такой, что

$$\begin{cases} a \in [x], \\ a \in [y]. \end{cases} \Rightarrow \begin{cases} a \sim x, \\ a \sim y. \end{cases} \Rightarrow x \sim y \Rightarrow [x] = [y].$$

□

Определение 6.3. Пусть на множестве X задано отношение эквивалентности $\sim$. Множество всех классов эквивалентности, отвечающее отношению эквивалентности $\sim$, называется фактормножеством относительно $\sim$ и обозначается $X/\sim$.

Утверждение 6.1. *Пусть $H \triangleleft G$, тогда множество всех левых смежных классов G/H образуют группу.*

Доказательство. Используя нормальность подгруппы H, определим на множестве левых смежных классов операцию произведения

$$g_1H \cdot g_2H = g_1(Hg_2)H = g_1(g_2H)H = g_1g_2H.$$

Проверим, что для этой операции выполнены все аксиомы группы:

1. Так как $H \triangleleft G$, то $(g_1H)(g_2H)(g_3H) = g_1g_2g_3H$.
2. В роли нейтрального элемента выступает $eH = H$.
3. Для каждого смежного класса существует обратный элемент равный $(gH)^{-1} = g^{-1}H$.

□

Определение 6.4. Пусть $H \triangleleft G$, тогда множество всех левых смежных классов G/H называется факторгруппой группы G по нормальной подгруппе H и обозначается как G/H.

Теорема 6.2. *Любая нормальная подгруппа является ядром некоторого гомоморфизма.*

Доказательство. Пусть $H \triangleleft G$, рассмотрим отображение $\pi : G \to G/H$, заданное правилом $\pi(g) = gH$. Ввиду нормальности подгруппы H для всех $g_1, g_2 \in G$ выполнено

$$\pi(g_1g_2) = g_1g_2K = g_1Hg_2H = \pi(g_1)\pi(g_2).$$

Так как смежный класс gH является образом $\pi(g)$, то можно заключить, что π - сюръекция.

Докажем, что $H = \operatorname{Ker}\pi$. Действительно, $\pi(g) = gH$ по построению π и при этом

$$g \in \operatorname{Ker}\pi \Leftrightarrow gH = \pi(g) = e_H = H \Leftrightarrow g \in H \Leftrightarrow H = \operatorname{Ker}\pi.$$

□

Задача 6.3. Пусть G – группа. Доказать, что $G/G \cong G$.

Задача 6.4. Построить факторгруппу группы $\mathbb{Z}_{12}$ классов вычетов по модулю 12 по ее подгруппе $H = \{0, 4, 8\}$.

Определение 6.5. Пусть $G \triangleright H$, тогда отображение $\pi : G \to G/H$, заданное правилом $\pi(g) = gH$, называется естественным (каноническим) эпиморфизмом.

7 Основная теорема о гомоморфизме

Теорема 7.1. *(**Основная теорема о гомоморфизме**) Пусть $\varphi : G \to H$ – гомоморфизм, тогда*

$$\operatorname{Im}\varphi \cong {}^{G}\!/_{\operatorname{Ker}\varphi}.$$

Доказательство. Зададим отображение $\theta : \operatorname{Im}\varphi \to {}^{G}\!/_{\operatorname{Ker}\varphi}$ правилом $\theta(\varphi(g)) = gK$, где $K = \operatorname{Ker}\varphi \triangleleft G$. Это отображение является гомоморфизмом:

$$\theta(\varphi(g_1)\varphi(g_2)) = \theta(\varphi(g_1g_2)) = g_1g_2K = g_1Kg_2 = g_1KKg_2 = g_1Kg_2K = \theta(\varphi(g_1))\theta(\varphi(g_2)).$$

θ – сюръекция, так как любой смежный класс $gK \in {}^{G}\!/_{K}$ является образом некоторого элемента: $gK = \theta(\varphi(g))$. Так же θ является инъективным отображением, так как его ядро тривиально:

$$\theta(\varphi(g)) = K \Leftrightarrow gK = K \Leftrightarrow g \in K \Leftrightarrow \varphi(g) = \varphi(e),$$

то есть в нейтральный элемент переходит только нейтральный элемент.

Таким образом, θ – искомый изоморфизм, существование которого и утверждает теорема.

Заметим, что $\theta(\varphi(g)) = gK = \pi(g)$, то есть представленная на рисунке 2 диаграмма является коммутативной. Это означает, что отображение φ можно представить в виде $\varphi = \theta^{-1} \circ \pi$.

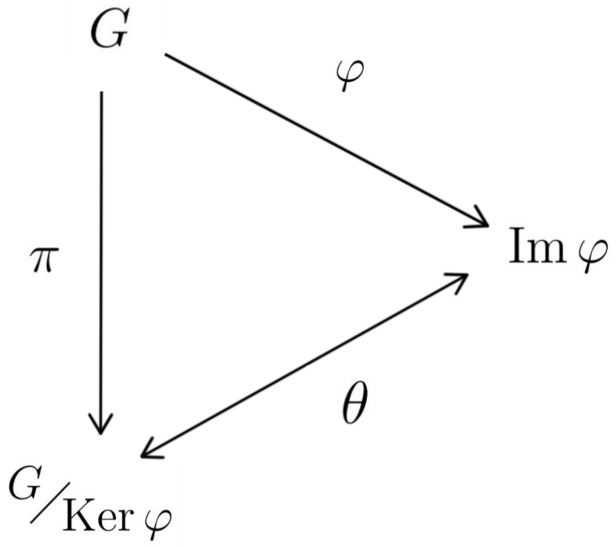

Рис. 2: Иллюстрация к доказательству основной теоремы о гомоморфизме.

□

Задача 7.1. Установить изоморфизмы групп:

1. ${}^{\mathbb{C}}\!/_{\mathbb{R}} \cong \mathbb{R}$.

   Воспользуемся основной теоремой о гомоморфизме, которая гласит, что гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма. Постороим такой гомоморфизм $\varphi : \mathbb{C} \to \mathbb{R}$, чтобы его ядро совпадало со множеством вещественных чисел $\operatorname{Ker}\varphi = \mathbb{R}$. Нетрудно видеть, что эпиморфизм (сюръективный гомоморфизм), заданный правилом $\varphi(z) = \varphi(x + iy) = y$ удовлетворяет этому условию, причем $\varphi(\mathbb{C}) = \mathbb{R}$. Тогда по основной теореме о гомоморфизме $\varphi(\mathbb{C}) \cong {}^{\mathbb{C}}\!/_{\operatorname{Ker}\varphi}$, что равносильно тому, что $\mathbb{R} \cong {}^{\mathbb{C}}\!/_{\mathbb{R}}$.

2. $\mathbb{C}^*/U \cong \mathbb{R}_+$ (здесь $U = \{z \in \mathbb{C} \mid |z| = 1\}$, а $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$).

   Опять же воспользуемся основной теоремой о гомоморфизме. Пусть $\varphi : \mathbb{C}^* \to \mathbb{R}_+$ задано правилом $\varphi(z) = \varphi(x+iy) = x^2+y^2$. Проверим, что это гомоморфизм: $\varphi(z_1z_2) = \varphi((x_1+iy_1)(x_2+iy_2)) = \varphi((x_1x_2-y_1y_2)+i(x_1y_2+x_2y_1)) = (x_1x_2-y_1y_2)^2+(x_1y_2+x_2y_1)^2 = x_1^2(x_2^2+y_2^2) + y_1^2(x_2^2+y_2^2) = (x_1^2+y_1^2)(x_2^2+y_2^2) = \varphi(z_1)\varphi(z_2)$, причем $\varphi(\mathbb{C}^*) = \mathbb{R}_+$. Ядро этого гомоморфизма – все элементы, переходящие в единицу, то есть $\operatorname{Ker}\varphi = U$. Значит, $\varphi(\mathbb{C}^*) \cong \mathbb{C}^*/\operatorname{Ker}\varphi$ по основной теореме о гомоморфизме, а следовательно $\mathbb{C}^*/U \cong \mathbb{R}_+$.

3. $U/U_n \cong U$ (здесь U_n – группа комплексных корней n-ой степени из единицы).

   Зададим гомоморфизм $\varphi : U \to U$ правилом $\varphi(z) = z^n$. Очевидно, что $\operatorname{Ker}\varphi = U_n$ и $\varphi(U) = U$. Значит, по основной теореме о гомоморфизме, $U/U_n \cong U$.

4. $\mathbb{Z}_{36}/\mathbb{Z}_6 \cong \mathbb{Z}_6$.

   Построим гомоморфизм $\varphi : \mathbb{Z}_{36} \to \mathbb{Z}_6$ следующим образом: $\varphi(n) = \dfrac{n}{36} \mod 6$, где mod означает взятие остатка от деления (в данном случае на 6). Нетрудно видеть, что $\operatorname{Ker}\varphi = \mathbb{Z}_6$ и $\varphi(\mathbb{Z}_{36}) = \mathbb{Z}_6$, значит, по основной теореме о гомоморфизме, $\mathbb{Z}_{36}/\mathbb{Z}_6 \cong \mathbb{Z}_6$.

Задача 7.2. Пусть F – поле, доказать, что $GL_n(F)/SL_n(F) \cong F^*$.

Задача 7.3. Построить факторгруппу $\mathbb{C}^*/\mathbb{R}_+$.

8 Прямое произведение групп

Определение 8.1. Пусть A, B – множества, их декартовым произведением называется множество

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Определение 8.2. Пусть G и H - группы, их (внешним) прямым произведением называется множество

$$G \times H = \{(g, h) \mid g \in G, h \in H\}.$$

Задача 8.1. Доказать, что прямое произведение групп $G \times H$ является группой относительно операции $(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2)$.

Задача 8.2. Доказать, что $G \times H \cong H \times G$.

Задача 8.3. Доказать, что множество $\{(g, e_H) \mid g \in G\}$ является подгруппой группы $G \times H$.

Утверждение 8.1. *Подгруппа $\{(g, e_H) \mid g \in G\}$ является нормальной в группе $G \times H$.*

Доказательство. Обозначим $A = G \times H$, тогда $B = \{(g, e_H) \mid g \in G\} < A$. По определению B – нормальная подгруппа, если $aB = Ba$ для всех $a \in A$. Пусть $a = (\tilde{g}, \tilde{h}) \in A$, рассмотрим

$$aB = (\tilde{g}, \tilde{h}) \cdot (g, e_H) = (\tilde{g}g, \tilde{h}e_H) = (\tilde{g}g, \tilde{h}),$$

$$aB = (g, e_H) \cdot (\tilde{g}, \tilde{h}) = (g\tilde{g}, e_H\tilde{h}) = (g\tilde{g}, \tilde{h}).$$

Так как $\{g\tilde{g}\} = G\tilde{g} = G = \tilde{g}G = \{\tilde{g}g\}$, то можно заключить, что $aB = Ba$ для всех $a \in A$. Следовательно, $\{(g, e_H) \mid g \in G\} \triangleleft G \times H$. □

Утверждение 8.2. *Координатная функция $\varphi_G : G\times H \to G$ заданная правилом $\varphi_G\big((g,h)\big) = g$ является гомоморфизмом.*

Доказательство. Действительно, это отображение сохраняет операцию для всех (g_1, h_1) и (g_2, h_2) из $G \times H$

$$\varphi_G\big((g_1,h_1)\cdot(g_2,h_2)\big) = \varphi_G\big((g_1g_2, h_1h_2)\big) = g_1g_2 = \varphi_G\big((g_1,h_1)\big)\varphi_G\big((g_2,h_2)\big).$$

□

Задача 8.4. Доказать, что подгруппа $\{(g, e_H) \mid g \in G\}$ группы $G \times H$ изоморфна группе G.

Задача 8.5. Доказать, что внешнее прямое произведение ассоциативно, то есть, что для любых трех групп A, B, C выполнено $(A \times B) \times C \cong A \times (B \times C)$.

Задача 8.6. Пусть $A_1 < A$ и $B_1 < B$. Доказать, что $A_1 \times B_1 < A \times B$.

Задача 8.7. Пусть $A_1 \lhd A$ и $B_1 \lhd B$. Доказать, что $A_1 \times B_1 \lhd A \times B$.

Утверждение 8.3. *Пусть $A_1 \lhd A$ и $B_1 \lhd B$. Доказать, что $A \times B \big/ A_1 \times B_1 \cong A \big/ A_1 \times B \big/ B_1$.*

Доказательство. Рассмотрим отображение $\varphi : A \times B \to A \big/ A_1 \times B \big/ B_1$ заданное правилом $\varphi\big((a,b)\big) = (aA_1, bB_1)$. Это гомоморфизм: ввиду того, что $A_1 \lhd A$ и $B_1 \lhd B$, для всех $a, c \in A$ и $b, d \in B$ выполнено

$$\varphi\big((a,b)(c,d)\big) = \varphi\big((ac,bd)\big) = (acA_1, bdB_1) = (aA_1cA_1, bB_1dB_1) = (aA_1A_1c, bB_1B_1d) =$$

$$= (aA_1cA_1, bB_1dB_1) = (aA_1, bB_1)(cA_1, dB_1) = \varphi\big((a,b)\big)\varphi\big((c,d)\big).$$

Так как нейтральный элемент в группе $A \big/ A_1 \times B \big/ B_1$ – это $\{(a_1, b_1) \mid a_1 \in A_1, b_1 \in B_1\}$, то ядро рассматриваемого отображения равно

$$\operatorname{Ker}\varphi = \{(a,b) \mid (aA_1, bB_1) = (A_1, B_1)\} = A_1 \times B_1.$$

Образ гомоморфизма тоже легко найти

$$\operatorname{Im}\varphi = \varphi(A \times B) = \{(aA_1, bB_1) \mid a \in A, b \in B\} = A \big/ A_1 \times B \big/ B_1.$$

Тогда по основной теореме о гомоморфизме

$$\operatorname{Im}\varphi \cong A \times B \big/ \operatorname{Ker}\varphi \Leftrightarrow A \big/ A_1 \times B \big/ B_1 \cong A \times B \big/ A_1 \times B_1.$$

□

Теорема 8.1 (Критерий разложимости группы в прямое произведение). *Пусть A, B – подгруппы группы G. В таком случае $G \cong A \times B$ тогда и только тогда, когда A, B – нормальные подгруппы группы G, $A \cap B = \{e\}$ и $AB = G$.*

Доказательство. Пусть $G = A \times B$, где $A < G$ и $B < G$. Тогда, так как $A \cong A \times \{e\} \lhd A \times B$ и $B \cong \{e\} \times B \lhd A \times B$, □

9 Группы малых порядков

Рассмотрим (с точностью до изоморфизма) группы малых порядков G_i^j (нижний индекс обозначает порядок группы, а верхний номер рассмариваемой группы данного порядка):

1. $G_1^1 = \{e\} \cong (\{0\}, +) \cong (\{1\}, \cdot) \cong (\{\mathrm{Id}\}, \circ)$ – абелева, циклическая, тривиальная группа.

2. $G_2^1 = \{e, a\} \cong \mathbb{Z}_2 = (\{0, 1\}, +) \cong (\{-1, 1\}, \cdot)$ – циклическая абелева группа.

3. $G_3^1 = \{e, a, b\} \cong (\{0, 1, 2\}, +) \cong \mathbb{Z}_4^*$ – циклическая абелева группа с таблицей Кэли

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

4. $G_4^1 = \{e, a, b, c\} \cong (\{0, 1, 2, 3\}, +)$ – циклическая абелева группа с таблицей Кэли

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

$G_4^2 = \{e, a, b, c\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = (\{(0, 0), (0, 1), (1, 0), (1, 1)\}, +)$ – нециклическая абелева группа с таблицей Кэли

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

Задача 9.1. Доказать, что существует ровно по одной (с точностью до изоморфизма) группе порядков 5 и 7. Выписать их таблицы Кэли.

Задача 9.2. Доказать, что существует ровно две неизоморфные группы 6 порядка. Выписать их таблицы Кэли.

10 Другие алгебраические структуры

Определение 10.1. Кольцо – это непустое множество с двумя внутренними бинарными операциями $+ : R \times R \to R$ и $\cdot : R \times R \to R$, такими, что

1. $(R, +)$ – абелева группа.

2. Операция умножения дистрибутивна относительно сложения: для всех a,b,$c \in R$ выполнено $a(b+c) = ab + ac$ и $(a+b)c = ac + bc$.

Задача 10.1. Пусть $(R, +, \cdot)$ – кольцо. Доказать, что для всех $a, b \in R$ выполнено

1. Нейтральный элемент относительно умножения, если он существует, единственен.
2. $a \cdot 0 = 0 \cdot a = 0$.
3. $-b = (-1) \cdot b$.
4. $(-a) \cdot b = (-ab)$.
5. $(-a) \cdot (-b) = ab$.

Примеры колец:

1. Множество целых чисел относительно сложения и умножения – $(\mathbb{Z}, +, \cdot)$.
2. Кольцо многочленов с рациональными коэффициентами.
3. $\mathbb{Z}_n$ – конечное кольцо вычетов по модулю натурального числа n.
4. Кольцо 2^X всех подмножеств множества X – кольцо, элементами которого являются подмножества в X. Операция сложения – симметрическая разность, а умножение – пересечение подмножеств.

Задача 10.2. Проверить, что множество 2^X является кольцом относительно операций симметрической разности и пересечения.

Задача 10.3. Доказать, что множество эндоморфизмов абелевой группы является кольцом.

Определение 10.2. Поле – это коммутативное ассоциативное кольцо с единицей, каждый ненулевой элемент которого обратим.

Определение 10.3. Линейное (векторное) пространство над полем F – это непустое множество V со внутренней бинарной операцией $+ : V \times V \to V$ и внешней бинарной операцией $\cdot : F \times V \to V$ такими, что для всех $\alpha, \beta \in F$ и $x, y \in V$ выполнено

1. $(V, +)$ – абелева группа.
2. $(\alpha\beta)x = \alpha(\beta x)$.
3. Для единицы поля $1 \in F$ выполнено $1 \cdot x = x$.
4. $(\alpha + \beta)x = \alpha x + \beta x$.
5. $\alpha(x + y) = \alpha x + \alpha y$.

Определение 10.4. Алгебра над полем F – это линейное пространство V над полем F с заданным на нем отображением $\times : V \times V \to V$, таким, что для всех $x, y, z \in V$ и для всех $\alpha, \beta \in F$ выполнено

1. $(x + y) \times z = x \times z + y \times z$.
2. $x \times (y + z) = x \times y + x \times z$.
3. $(\alpha x) \times (\beta y) = (\alpha\beta)(x \times y)$.

Список литературы

[1] И.И. Богданов. Курс видеолекций «Теория групп». https://www.youtube.com/playlist?list=PLyBWNG-pZKx6pWlAfPRo2X_kPWyzq1ebj.

[2] А.В. Савватеев. Курс видеолекций «Теория групп». https://www.youtube.com/playlist?list=PLgqZ7cC8KvvZcMjXYLP53SaXCG35hF_E8.

[3] Т.М. Банникова, Н.А. Баранова. Теория групп в задачах и упражнениях.

[4] К.Ю. Федоровский. Алгебра. Введение в теорию групп.

[5] А.И. Мальцев. Современная алгебра.

[6] П. Кон. Универсальная алгебра.

[7] С.Н. Тронин. Введение в универсальную и категорную алгебру.

[8] Б.Л. Ван-дер-Варден. Алгебра.

[9] А.Г. Курош. Общая алгебра