

Введение в теорию групп

Артём Рашевский

2025

Содержание

1	Бинарные операции. Полугруппы, моноиды и группы . .	3
2	Подгруппы. Циклические подгруппы и группы. Порядок элемента	5
3	Смежные классы. Индекс подгруппы. Теорема Лагранжа	8
4	Группы движений	10
5	Группа перестановок	12
6	Нормальные подгруппы. Факторгруппы	15
7	Гомоморфизмы групп. Четверная группа Клейна. Теорема Кэли	17
8	Теорема о гомоморфизме. Классификация циклических групп	21
9	Прямое произведение групп. Теорема о строении конечных абелевых групп	23
10	Экспонента конечной абелевой группы и критерий циклическости	25
11	Кольца и поля	26
	Список литературы	29

1 Бинарные операции. Полугруппы, моноиды и группы

Определение 1.1. Пусть M — непустое множество. *Бинарной операцией* \circ на множестве M называется отображение $\circ : M \times M \rightarrow M$, $\forall a, b \in M: (a, b) \mapsto a \circ b$.

Множество с бинарной операцией обычно обозначают (M, \circ) .

Определение 1.2. Множество с бинарной операцией (M, \circ) называется *полугруппой*, если данная бинарная операция ассоциативна, т.е.

$$\forall a, b, c \in M: a \circ (b \circ c) = (a \circ b) \circ c.$$

Определение 1.3. Полугруппа (M, \circ) называется *моноидом*, если в ней есть *нейтральный элемент*, т.е.

$$\exists e \in M: \forall a \in M: e \circ a = a \circ e = a.$$

Определение 1.4. Моноид (M, \circ) называется *группой*, если для каждого элемента $a \in M$ найдется *обратный элемент*, т.е.

$$\forall a \in M \exists a^{-1} \in M: a \circ a^{-1} = a^{-1} \circ a = e.$$

Определение 1.5. Группа G называется *коммутативной* или *абелевой*, если групповая операция *коммутативна*, т.е.

$$\forall a, b \in G: ab = ba.$$

Определение 1.6. *Порядком* $|G|$ группы G называется число элементов в ней. Группа называется *конечной*, если её порядок конечен, и *бесконечной* иначе.

Примеры.

1. Числовые *аддитивные* группы:

$$\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+, \mathbb{Z}_n^+.$$

2. Числовые *мультипликативные* группы:

$$\mathbb{Q}^\times \setminus \{0\}, \mathbb{R}^\times \setminus \{0\}, \mathbb{C}^\times \setminus \{0\}, \mathbb{Z}_p^\times \setminus \{0\}, p - \text{простое}.$$

3. Группы матриц:

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{R}) \mid \det A \neq 0\} - \text{полная линейная группа};$$

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{R}) \mid \det A = 1\} - \text{специальная линейная группа};$$

$$\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{R}) \mid A \cdot A^T = I\} - \text{ортогональная группа};$$

$$\mathrm{SO}_n(\mathbb{R}) = \mathrm{O}_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R}) - \text{специальная ортогональная группа}.$$

4. Группы перестановок:

симметрическая группа S_n — все перестановки длины n ;

знакопеременная группа A_n — все чётные перестановки длины n .

5. Группы преобразований подобия: гомотетии, движения (осевые и скользящие симметрии, параллельные переносы, повороты).

Определение 1.7. Для описания структур групп часто используются *таблицы Кэли*. Они представляют собой квадратные таблицы, заполненные результатами применения бинарной операции к элементам множества.

Пример. Таблица Кэли для группы $(\{1, 3, 5, 7\}, \times(\bmod 8))$:

\times	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

2 Подгруппы. Циклические подгруппы и группы.

Порядок элемента

Определение 2.1. Подмножество H группы G называется *подгруппой* и обозначается $H < G$, если выполнены следующие условия:

1. $e \in H$;
2. $\forall a, b \in H: ab \in H$;
3. $\forall a \in H: a^{-1} \in H$.

В каждой группе G есть *несобственные* или *тривиальные* подгруппы $H = \{e\}$ и $H = G$. Все прочие подгруппы называются *собственными*.

Примеры.

1. $\mathbb{Z}^+ < \mathbb{Q}^+ < \mathbb{R}^+ < \mathbb{C}^+$
2. $GL_n(\mathbb{R}) > O_n(\mathbb{R}) > SO_n(\mathbb{R}); GL_n(\mathbb{R}) > SL_n(\mathbb{R})$.
3. $S_n > A_n$.

Теорема (Критерий подгруппы). Пусть G — группа, тогда

$$H < G \iff \forall a, b \in H: a \circ b^{-1} \in H.$$

Доказательство. Определим на H вспомогательное отношение $R_H = \{(a, b) \mid a \circ b^{-1} \in H\}$. Покажем, что R_H является отношением эквивалентности. Для этого проверим, что оно рефлексивно (1), симметрично (2) и транзитивно (3):

1. $a \circ a^{-1} = e \in H$;
2. $ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H$;
3. $ab^{-1} \in H, bc^{-1} \in H \implies ac^{-1} = (ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} \in H$.

Рефлексивность R_H определяет наличие нейтрального элемента, симметричность — наличие обратного элемента, транзитивность — ассоциативность заданной бинарной операции. Каждый класс эквивалентности будет ассоциирован с некоторой подгруппой (как с алгебраически замкнутым множеством). ■

Утверждение 2.1. Всякая подгруппа в \mathbb{Z}^+ имеет вид $k\mathbb{Z}$ для некоторого $k \in \mathbb{N}_0$.

Доказательство. Очевидно, что все подмножества вида $k\mathbb{Z}$ являются подгруппами в \mathbb{Z} . Пусть $H < \mathbb{Z}$. Если $H = \{0\}$, то $H = 0\mathbb{Z}$. Иначе положим $k = \min(H \cap \mathbb{N}) \neq 0$ (это множество непусто, т.к. $\forall x \in H \cap \mathbb{N}: -x \in H$), тогда $k\mathbb{Z} \subseteq H$. Покажем, что $k\mathbb{Z} = H$. Пусть $a \in H$ — произвольный элемент. Поделим его на k с остатком:

$$a = qk + r, \text{ где } k \in H, 0 \leq r < k \Rightarrow r = a - qk \in H.$$

В силу выбора k получаем: $r = 0 \Rightarrow a = qk \in k\mathbb{Z}$. ■

Определение 2.2. Пусть G — группа, $g \in G$ и $n \in \mathbb{Z}$. *Степень* элемента g определяется следующим образом:

$$g^n = \begin{cases} \underbrace{g \dots g}_n, & n > 0 \\ e, & n = 0 \\ \underbrace{g^{-1} \dots g^{-1}}_n, & n < 0 \end{cases}$$

и обладает свойствами:

$$\forall m, n \in \mathbb{Z} :$$

1. $g^m \cdot g^n = g^{m+n}$;
2. $(g^m)^{-1} = g^{-m}$;
3. $(g^m)^n = g^{mn}$.

Определение 2.3. Пусть G — группа и $g \in G$. *Циклической подгруппой*, порожденной элементом g , называется подмножество $\{g^n \mid n \in \mathbb{Z}\} \subseteq G$.

Циклическая подгруппа, порождённая элементом g , обозначается $\langle g \rangle$. Элемент g называется *порождающим* или *образующим* для подгруппы $\langle g \rangle$.

Пример. Подгруппа $2\mathbb{Z} < \mathbb{Z}^+$ является циклической, и в качестве порождающего элемента в ней можно взять $g = 2$ или $g = -2$. Другими словами, $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$.

Определение 2.4. Группа G называется *циклической*, если

$$\exists g \in G: G = \langle g \rangle.$$

Циклическая группа порядка n обозначается C_n .

Примеры. \mathbb{Z}^+ ; \mathbb{Z}_n^+ , $n \geq 1$.

Определение 2.5. Пусть G — группа и $g \in G$. *Порядком* элемента g называется наименьшее $m \in \mathbb{N}$: $g^m = e$. Если такого натурального числа m не существует, говорят, что порядок элемента g равен бесконечности. Порядок элемента обозначается $\text{ord}(g)$.

Замечание.

$$\text{ord}(g) = 1 \iff g = e.$$

Утверждение 2.2. Если G — группа и $g \in G$, то $\text{ord}(g) = |\langle g \rangle|$.

Доказательство. Заметим, что если $g^k = g^s$, то $g^{k-s} = e$. Поэтому если элемент g имеет бесконечный порядок, то все элементы g^n , $n \in \mathbb{Z}$, попарно различны, и подгруппа $\langle g \rangle$ содержит бесконечно много элементов. Если же $\text{ord}(g) = m$, то из минимальности числа m следует, что элементы $e = g^0, g^1, g^2, \dots, g^{m-1}$ попарно различны. Далее, $\forall n \in \mathbb{Z}: n = mq + r$, где $0 \leq r \leq m-1$, и

$$g^n = g^{mq+r} = (g^m)^q g^r = e^q g^r = g^r.$$

Следовательно, $\langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\}$ и $|\langle g \rangle| = m$. ■

Очевидно, что всякая циклическая группа коммутативна и не более чем счётна.

3 Смежные классы. Индекс подгруппы. Теорема Лагранжа

Определение 3.1. *Левым смежным классом* элемента g группы G по подгруппе H называется подмножество

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

аналогично определяется *правый смежный класс*:

$$Hg = \{hg \mid h \in H\}.$$

Лемма 3.1. *Пусть G — конечная подгруппа, тогда $\forall g \in G: |gH| = |H|$.*

Доказательство. Поскольку $gH = \{gh \mid h \in H\}$, в gH элементов не больше, чем в H . Если $gh_1 = gh_2$, то домножив слева на g^{-1} , получаем $h_1 = h_2$. Значит, все элементы вида gh , где $h \in H$, попарно различны, откуда $|gH| = |H|$. ■

Определение 3.2. Пусть G — группа, $H < G$. *Индексом* подгруппы H в группе G называется число левых смежных классов G по H .

Индекс группы G по подгруппе H обозначается $[G : H]$.

Теорема (Лагранж). *Пусть G — конечная группа, $H < G$. Тогда*

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

Доказательство. Каждый элемент группы G лежит в (своём) левом смежном классе по подгруппе H , разные смежные классы не пересекаются (по следствию из доказательства критерия подгруппы) и каждый из них содержит по $|H|$ элементов (по предыдущей лемме). ■

Следствие 3.1. $|G| \div |H|$.

Следствие 3.2. $|G| \div \text{ord}(g)$.

Доказательство. Вытекает из следствия 1 и того, что $\text{ord}(g) = |\langle g \rangle|$. ■

Следствие 3.3. $g^{|G|} = e$.

Доказательство. Из предыдущего следствия получаем:
 $|G| = \text{ord}(g) \cdot s, s \in \mathbb{N} \implies g^{|G|} = (g^{\text{ord}(g)})^s = e^s = e$. ■

Следствие 3.4 (Малая теорема Ферма). Пусть \bar{a} — ненулевой вычет по простому модулю p , тогда $\bar{a}^{p-1} \equiv 1 \pmod{p}$.

Доказательство. Достаточно применить следствие 3 к группе $\mathbb{Z}_p^\times \setminus \{0\}$ ■

Следствие 3.5. Пусть $|G|$ — простое число, тогда G — циклическая группа, порождённая любым своим ненулевым элементом.

Доказательство. Пусть $g \in G$ — произвольный ненулевой элемент. Тогда циклическая подгруппа $\langle g \rangle$ содержит более одного элемента и $|\langle g \rangle|$ делит $|G|$ по следствию 1. Значит, $|\langle g \rangle| = |G|$, откуда $G = \langle g \rangle$. ■

4 Группы движений

Определение 4.1. Упорядоченная пара (M, d) , состоящая из множества M и отображения $d : M \times M \rightarrow \mathbb{R}$, называется *метрическим пространством*, если $\forall x, y \in M$:

1. $d(x, y) = 0 \Leftrightarrow x = y$ (*аксиома тождества*);
2. $d(x, y) \geq 0$ (*аксиома неотрицательности*);
3. $d(x, y) = d(y, x)$ (*аксиома симметричности*);
4. $d(x, y) + d(y, z) \geq d(x, z)$ (*аксиома или неравенство треугольника*).

Определение 4.2. Пусть X и Y — метрические пространства. Отображение $f : X \rightarrow Y$ называется *изометрией*, если оно сохраняет расстояние между точками:

$$\forall x, x' \in X: |f(x) - f(x')|_Y = |x - x'|_X,$$

Если $X = Y$, f называют *движением*.

Определение 4.3. Движение называют *собственным*, если оно сохраняет *ориентацию* пространства.

Определение 4.4. Пусть E — евклидово аффинное пространство и $F \subseteq E$ — геометрическая фигура. Группой движений (изометрий) $\text{Isom}(F)$ фигуры F называется множество тех движений аффинного пространства E , которые переводят фигуру F в себя:

$$\text{Isom}(F) = \{\varphi : E \rightarrow E \mid \varphi \text{ — движение, } \varphi(F) = F\}.$$

В качестве групповой операции рассматривается операция композиции движений.

Замечание. Группа собственных движений $\text{Isom}(F)^+$ является подгруппой группы движений $\text{Isom}(F)$ фигуры F .

Определение 4.5. Группа движений правильного n -угольника $\Delta_n \subset \mathbb{R}^2$ называется *диэдральной группой* D_n :

$$D_n = \text{Isom}(\Delta_n).$$

Утверждение 4.1. $|D_n| = 2n$.

Доказательство. Есть всего 2 вида движений:

1. n вращений относительно центра на угол, кратный $\frac{2\pi}{n}$ (вращение на угол φ обозначается R_φ);
2. n симметрий относительно осей симметрии (симметрия относительно прямой l обозначается S_l).

В случае нечётного n любая ось симметрии проходит через центр Δ_n и одну из вершин, в случае чётного n любая ось симметрии проходит либо через противоположные вершины, либо через середины противоположных сторон. ■

Замечание. Группа собственных движений Δ_n содержит только повороты:

$$\text{Isom}(D_n)^+ = \{R_{\frac{2\pi k}{n}}\}, \quad k = \overline{0, n-1}.$$

Пример. Таблица Кэли группы D_4 квадрата $ABCD$:

\circ	id	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	S_h	S_v	S_{AC}	S_{BD}
id	id	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	S_h	S_v	S_{AC}	S_{BD}
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	id	S_{BD}	S_{AC}	S_h	S_v
R_π	R_π	$R_{\frac{3\pi}{2}}$	id	$R_{\frac{\pi}{2}}$	S_v	S_h	S_{BD}	S_{AC}
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	id	$R_{\frac{\pi}{2}}$	R_π	S_{AC}	S_{BD}	S_v	S_h
S_h	S_h	S_{AC}	S_v	S_{BD}	id	R_π	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
S_v	S_v	S_{BD}	S_h	S_{AC}	R_π	id	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$
S_{AC}	S_{AC}	S_v	S_{BD}	S_h	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$	id	R_π
S_{BD}	S_{BD}	S_h	S_{AC}	S_v	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	R_π	id

5 Группа перестановок

Определение 5.1. Пусть задано множество $X = \{1, 2, \dots, n\}$, $n \in \mathbb{N}$. Множество всех возможных биекций $X \leftrightarrow X$ с операцией композиции образует группу S_n , называемую *симметрической группой* или *группой перестановок*.

Утверждение 5.1.

$$|S_n| = n!$$

Доказательство. Символ 1 можно подходящей перестановкой σ перевести в любой другой символ $\sigma(1)$, для чего существует в точности n различных возможностей. Но зафиксировав $\sigma(1)$, в качестве $\sigma(2)$ можно брать лишь один из оставшихся $n - 1$ символов и т.д. Всего возможностей выбора $\sigma(1), \sigma(2), \dots, \sigma(n)$, значит и всех перестановок будет $n(n - 1) \dots 2 \cdot 1 = n!$. ■

Утверждение 5.2. Любая перестановка может быть представлена в виде композиции независимых циклов единственным образом с точностью до порядка множителей.

Утверждение 5.3. Независимые циклы коммутируют.

Утверждение 5.4. Порядок цикла равен его длине.

Утверждение 5.5. Порядок перестановки равен НОК длин циклов в его цикловом разложении.

Определение 5.2. Цикл длины 2 называется *транспозицией*.

Лемма 5.1. Любая перестановка является произведением транспозиций.

Доказательство. Достаточно доказать это для циклов непосредственной проверкой:

$$(i_1 i_2 i_3 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k). \quad \blacksquare$$

Определение 5.3. *Инверсией* в перестановке называется пара индексов $k < s$, таких что $i_k > i_s$.

Определение 5.4. *Чётностью* перестановки называется чётность числа инверсий в ней.

Лемма 5.2. Пусть (ij) — произвольная транспозиция, тогда $\forall \sigma \in S_n$ чётности перестановок σ и $\sigma(ij)$ различны.

Доказательство. Рассмотрим два случая:

1. $(ij) = (i \ i + 1)$ — число инверсий изменилось на одну, чётность изменилась.
2. (ij) — любая, тогда

$$(ij) = (j - 1 \ j) \dots (i + 1 \ i + 2)(i \ i + 1)(i + 1 \ i + 2) \dots (j - 1 \ j), \quad (1)$$

что подтверждается непосредственной проверкой. ■

Следствие. Любая перестановка является композицией произведением соседних элементов.

Доказательство. В разложении (1) $2(j - i - 1) + 1$ сомножителей, т.е, нечётное число. При перемене чётности нечётное число раз, она изменится, что доказывает следствие. ■

Теорема 5.1. В S_n число чётных перестановок равно числу нечётных перестановок.

Доказательство. Пусть $\sigma_1, \dots, \sigma_k$ — все чётные перестановки длины n , тогда $\sigma_1(12), \dots, \sigma_k(12)$ — нечётные перестановки. Если σ — чётная, то $\sigma(12)$ — нечётная $\implies \sigma = (\sigma(12))(12) = \sigma(12)^2 = \sigma \text{ id} = \sigma \implies$ среди $\sigma_1, \dots, \sigma_k$ встретятся все нечётные перестановки. Значит, мы установили биекцию между множеством чётных и множеством нечётных перестановок \implies эти множества равномощны. ■

Определение 5.5. Знак перестановки $\text{sgn}(\sigma) = \begin{cases} 1, & \sigma \text{ — чётная} \\ -1, & \sigma \text{ — нечётная.} \end{cases}$

Теорема 5.2.

$$\forall \sigma, \tau \in S_n: \operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau).$$

Доказательство. Пусть $\sigma = \sigma_1, \dots, \sigma_k$, $\tau = \tau_1, \dots, \tau_s$ — произведение транспозиций. Тогда $\operatorname{sgn}(\sigma) = (-1)^k$, $\operatorname{sgn}(\tau) = (-1)^s$.

$$\sigma\tau = \sigma_1, \dots, \sigma_k\tau_1, \dots, \tau_s \implies \operatorname{sgn}(\sigma\tau) = (-1)^{k+s}. \quad \blacksquare$$

Следствие.

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1}).$$

Доказательство.

$$\operatorname{sgn}(\sigma) \operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn}(\operatorname{id}) = 1. \quad \blacksquare$$

Пример. Пусть $G = S_3$, $H = \langle (12) \rangle = \{\operatorname{id}, (12)\}$. Найдём все левые и правые смежные классы G по H (произвольный элемент обозначим a):

a	aH	Ha
id	aH	Ha
(12)	$\{(12), \operatorname{id}\}$	$\{(12), \operatorname{id}\}$
(13)	$\{(13), (123)\}$	$\{(13), (132)\}$
(23)	$\{(23), (132)\}$	$\{(23), (123)\}$
(123)	$\{(123), (13)\}$	$\{(123), (23)\}$
(132)	$\{(132), (23)\}$	$\{(132), (13)\}$

6 Нормальные подгруппы. Факторгруппы

Определение 6.1. Подгруппа H группы G называется *нормальной*, если

$$\forall g \in G: gH = Hg.$$

Обозначается $H \triangleleft G$.

Утверждение 6.1. Пусть H — подгруппа группы G , тогда следующие условия эквивалентны:

1. H нормальна;
2. $\forall g \in G: gHg^{-1} = H$;
3. $\forall g \in G: gHg^{-1} \subseteq H$.

Доказательство.

$$(1) \implies (2): gH = Hg \mid \cdot g^{-1} \implies gHg^{-1} = H.$$

$$(2) \implies (3): \text{очевидно.}$$

$$(3) \implies (2): gHg^{-1} \subseteq H \implies gHg^{-1} \subseteq H \mid \cdot g \implies gH \subseteq Hg.$$

$$\text{Если } g = g^{-1}, \text{ то } g \cdot \mid g^{-1}Hg \subseteq H \implies Hg \subseteq gH \implies gH = Hg. \quad \blacksquare$$

Рассмотрим множество смежных классов по нормальной подгруппе, обозначенной G/H . Определим на G/H бинарную операцию, полагая, что $(g_1H)(g_2H) = (g_1g_2)H$.

Пусть $g'_1H = g_1H$ и $g'_2H = g_2H$, тогда $g'_1 = g_1h_1$, $g'_2 = g_2h_2$, где $h_1, h_2 \in H$.

$$\begin{aligned} (g'_1H)(g'_2H) &= (g'_1g'_2)H = (g_1h_1g_2h_2)H = (g_1g_2 \underbrace{g_2^{-1}h_1g_2}_{\in H} h_2)H \subseteq (g_1g_2)H \implies \\ &\implies (g'_1g'_2)H = (g_1g_2)H. \end{aligned}$$

Утверждение 6.2. G/H является группой.

Доказательство. Проверим аксиомы группы:

1. Ассоциативность очевидна.
2. Нейтральный элемент — eH .
3. Обратный к gH — $g^{-1}H$. ■

Определение 6.2. Множество G/H с указанной операцией называется *факторгруппой* группы G по нормальной подгруппе H .

Пример. Если $G = \mathbb{Z}^+$ и $H = n\mathbb{Z}$, то G/H — группа вычетов \mathbb{Z}_n^+

7 Гомоморфизмы групп. Четверная группа Клейна.

Теорема Кэли

Определение 7.1. Пусть (G, \circ) и $(F, *)$ — группы.

Отображение $\varphi : G \rightarrow F$ называется *гомоморфизмом*, если

$$\forall g_1, g_2 \in G: \varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2).$$

Замечание. Пусть $\varphi : G \rightarrow F$ — гомоморфизм групп, и пусть e_G, e_F — нейтральные элементы групп G и F соответственно, тогда:

1. $\varphi(e_G) = e_F$
2. $\forall g \in G: \varphi(g^{-1}) = \varphi(g)^{-1}$

Доказательство.

1. $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) \varphi(e_G).$

Домножив обе крайние части равенства на $\varphi(e_G)^{-1}$, получим $e_F = \varphi(e_G).$

2. $\varphi(g * g^{-1}) = e_F = \varphi(g) \varphi(g^{-1}).$

Умножив обе части на $\varphi(g)^{-1}$, получаем необходимое. ■

Определение 7.2. Гомоморфизм групп $\varphi : G \rightarrow F$ называется

- *эндоморфизмом*, если $F = G$;
- *мономорфизмом*, если φ инъективно;
- *эпиморфизмом*, если φ сюръективно;
- *изоморфизмом*, если φ биективно;
- *автоморфизмом*, если φ является эндоморфизмом и изоморфизмом.

Группы G и F называются *изоморфными*, если между ними существует изоморфизм. Обозначается: $G \cong F$.

Пример. Четверная группа Клейна — ациклическая коммутативная группа четвёртого порядка, задающаяся следующей таблицей Кэли:

\cdot	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Порядок каждого элемента, отличного от нейтрального, равен 2.

Обозначается V или V_4 (от нем. *Viererguppe* — четверная группа).

Любая группа четвёртого порядка изоморфна либо циклической группе, либо четверной группе Клейна, наименьшей по порядку нециклической группе. Симметрическая группа S_4 имеет лишь две нетривиальные нормальные подгруппы — знакопеременную группу A_4 и четверную группу Клейна V_4 , состоящую из перестановок $\text{id}, (12)(34), (13)(24), (14)(23)$.

Несколько примеров изоморфных ей групп:

- прямая сумма $\mathbb{Z}_2 \oplus \mathbb{Z}_2$;
- диэдральная группа D_2 ;
- множество $\{0, 1, 2, 3\}$ с операцией XOR;
- группа симметрий ромба $ABCD$ в трёхмерном пространстве, состоящая из 4 преобразований: $\text{id}, R_\pi, S_{AC}, S_{BD}$;
- группа поворотов тетраэдра на угол π вокруг всех трёх рёберных медиан (вместе с тождественным поворотом).

Определение 7.3. Ядром гомоморфизма $\varphi : G \rightarrow F$ называется множество всех элементов G , которые отображаются в нейтральный элемент F , т.е.

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_F\}.$$

Образ φ определяется как

$$\operatorname{Im} \varphi = \varphi(G) = \{f \in F \mid \exists g \in G: \varphi(g) = f\}.$$

Очевидно, что $\ker \varphi < G$ и $\operatorname{Im} \varphi < F$.

Лемма 7.1. Гомоморфизм групп $\varphi : G \rightarrow F$ инъективен тогда и только тогда, когда $\ker \varphi = \{e_G\}$.

Доказательство. Ясно, что если φ инъективен, то $\ker \varphi = \{e_G\}$.

Обратно, пусть $g_1, g_2 \in G$ и $\varphi(g_1) = \varphi(g_2)$. Тогда $g_1^{-1}g_2 \in \ker \varphi$, поскольку $\varphi(g_1^{-1}g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_2) = e_F$. Отсюда $g_1^{-1}g_2 = e_G$ и $g_1 = g_2$. ■

Следствие. Гомоморфизм групп $\varphi : G \rightarrow F$ является изоморфизмом тогда и только тогда, когда $\ker \varphi = \{e_G\}$ и $\operatorname{Im} \varphi = F$.

Утверждение 7.1. Пусть $\varphi : G \rightarrow F$ гомоморфизм групп, тогда $\ker \varphi \triangleleft G$.

Доказательство. Достаточно проверить, что

$$\forall g \in G \quad \forall h \in \ker \varphi: g^{-1}hg \in \ker \varphi.$$

Это следует из цепочки равенств:

$$\varphi(g_1^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})e_F\varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_F.$$

■

Теорема (Кэли). Любая конечная группа G порядка n изоморфна некоторой подгруппе S_n .

Доказательство. $\forall a \in G$ рассмотрим отображение $L_a : G \rightarrow G$, определённое формулой $L_a(g) = ag$.

Если e, g_2, \dots, g_n — все элементы G , то a, ag_2, \dots, ag_n будут теми же элементами, но расположенными в каком-то другом порядке. Значит, L_a — биекция, обратной к которой будет $L_a^{-1} = L_{a^{-1}}$, тождественным отображением является L_e . Тогда $L_{ab}(g) = (ab)g = a(bg) = L_a(L_b(g))$, т.е. $L_{ab} = L_a L_b$. Следовательно множество $L_e, L_{g_2}, \dots, L_{g_n}$ образует подгруппу $H < S(G) = S_n$, а $L : a \mapsto L_a$ является изоморфизмом. ■

8 Теорема о гомоморфизме. Классификация циклических групп

Теорема (О гомоморфизме). Пусть $\varphi : G \rightarrow F$ — гомоморфизм групп, тогда

$$\text{Im } \varphi \cong G / \ker \varphi.$$

Доказательство. Рассмотрим отображение $\psi : G / \ker \varphi \rightarrow \text{Im } \varphi$, заданное формулой $\psi(g \ker \varphi) = \varphi(g)$.

Достаточно проверить определение изоморфизма для ψ . Для этого покажем, что заданное отображение корректно определено, биективно и гомоморфно.

1. Проверим корректность ψ :

$$\exists h_1, h_2 \in \ker \varphi : g_1 \ker \varphi = g_2 \ker \varphi \implies g_1 h_1 = g_2 h_2;$$

$$\psi(g_1 \ker \varphi) = \varphi(g_1) = \varphi(g_1 h_1) = \varphi(g_2 h_2) = \varphi(g_2) = \psi(g_2 \ker \varphi).$$

2. Докажем, что ψ — гомоморфизм:

$$\begin{aligned} \psi((g_1 \ker \varphi)(g_2 \ker \varphi)) &= \psi((g_1 g_2) \ker \varphi) = \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = \\ &= \psi(g_1 \ker \varphi) \psi(g_2 \ker \varphi). \end{aligned}$$

3. Сюръективность видна из построения.

4. Инъективность:

$$\begin{aligned} \psi(g_1 \ker \varphi) = \psi(g_2 \ker \varphi) &\implies \varphi(g_1) = \varphi(g_2) \implies \varphi(g_1) \varphi(g_2)^{-1} = e_F \implies \\ \implies \varphi(g_1 g_2^{-1}) &= e_F \implies g_1 g_2^{-1} \in \ker \varphi \implies g_1 \ker \varphi = g_2 \ker \varphi. \quad \blacksquare \end{aligned}$$

Пример. Пусть $G = \mathbb{R}^+$ и $H = \mathbb{Z}^+$. Рассмотрим группу $F = \mathbb{C}^\times \setminus \{0\}$ и гомоморфизм $\varphi : G \rightarrow F$, $g \mapsto e^{2\pi i g} = \cos(2\pi g) + i \sin(2\pi g)$. Тогда $\ker \varphi = H$ и факторгруппа G/H изоморфна окружности S^1 , рассматриваемой как подгруппа в F , состоящей из комплексных чисел с модулем равным 1.

Теорема (О классификации циклических групп). Пусть G — циклическая группа.

1. Если $|G| = \infty$, то $G \cong \mathbb{Z}^+$.
2. Если $|G| = n < \infty$, то $G \cong \mathbb{Z}_n^+$.

Доказательство. Пусть $G = \langle g \rangle$. Рассмотрим отображение $\varphi : \mathbb{Z} \rightarrow G, \quad k \mapsto g^k$.

$$\varphi(k+l) = g^{k+l} = g^k g^l = \varphi(k)\varphi(l), \text{ поэтому } \varphi \text{ — гомоморфизм.}$$

Из определения циклической группы следует, что φ сюръективен, т.е. $\text{Im } \varphi = G$. По теореме о гомоморфизме получаем $G \cong \mathbb{Z} / \ker \varphi$, т.к. $\ker \varphi < \mathbb{Z} \implies \exists m \geq 0: \ker \varphi = m\mathbb{Z}$ (любая подгруппа \mathbb{Z} имеет вид $k\mathbb{Z}$). Если $m = 0$, то $\ker \varphi = \{0\}$, откуда $G \cong \mathbb{Z} / \{0\} \cong \mathbb{Z}$. Если $m > 0$, то $G \cong \mathbb{Z} / m\mathbb{Z} = \mathbb{Z}_m$. ■

9 Прямое произведение групп. Теорема о строении конечных абелевых групп

Определение 9.1. *Прямым произведением групп G_1, \dots, G_m называется группа*

$$G_1 \times \dots \times G_m = \{(g_1, \dots, g_m) \mid g_1 \in G_1, \dots, g_m \in G_m\}$$

с операцией $(g_1, \dots, g_m)(g'_1, \dots, g'_m) = (g_1g'_1, \dots, g_mg'_m)$.

Ясно, что эта операция ассоциативна, обладает нейтральным элементом $(e_{G_1}, \dots, e_{G_m})$ и для каждого элемента (g_1, \dots, g_m) есть обратный элемент $(g_1^{-1}, \dots, g_m^{-1})$.

Замечание. Группа $G_1 \times \dots \times G_m$ коммутативна тогда и только тогда, когда коммутативна каждая из групп G_1, \dots, G_m .

Замечание. Если все группы G_1, \dots, G_m конечны, то $|G_1 \times \dots \times G_m| = |G_1| \dots |G_m|$.

Определение 9.2. Говорят, что группа G *раскладывается в прямое произведение* своих подгрупп H_1, \dots, H_m , если отображение $H_1 \times \dots \times H_m \rightarrow G$, $(h_1, \dots, h_m) \mapsto h_1 \dots h_m$ является изоморфизмом.

Теорема 9.1. Пусть $n = pq$ — разложение натурального числа n на два взаимно простых сомножителя. Тогда имеет место изоморфизм групп

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q.$$

Доказательство. Рассмотрим отображение

$$\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q, \quad \varphi(a \bmod n) = (a \bmod p, a \bmod q).$$

1. Корректность следует из того, что $n : p$, $n : q$.
2. φ — гомоморфизм, т.к.

$$\varphi((a + b) \bmod n) = \varphi(a \bmod n) + \varphi(b \bmod n).$$

3. φ инъективен:

Если $\varphi(a \bmod n) = (0, 0)$, то $a : p$, $a : q$. Но так как $\text{НОД}(p, q) = 1$, получаем, что $a \mid n$. Тогда $a \equiv 0 \pmod{n}$, т.е. $\ker \varphi = \{0\}$.

4. φ сюръективен, т.к. $|\mathbb{Z}_n| = n = p \cdot q = |\mathbb{Z}_p \times \mathbb{Z}_q|$. ■

Следствие. Пусть $n \geq 2$ — натуральное число и $n = p_1^{k_1} \dots p_s^{k_s}$ — его разложение в произведение простых множителей ($p_i \neq p_j$ при $i \neq j$). Тогда имеет место изоморфизм групп

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_s^{k_s}}.$$

Определение 9.3. Конечная абелева группа A называется *примарной*, если $|A| = p^k$ для некоторого $k \in \mathbb{N}$, где p — простое.

Теорема (О строении конечных абелевых групп). Пусть A — конечная абелева группа. Тогда $A \cong \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_t^{k_t}}$, где p_1, \dots, p_t — простые числа (не обязательно различные) и $k_1, \dots, k_t \in \mathbb{N}$. Более того, набор примарных циклических множителей $\mathbb{Z}_{p_1^{k_1}}, \dots, \mathbb{Z}_{p_t^{k_t}}$ определен однозначно с точностью до перестановки (в частности, число этих множителей определено однозначно).

10 Экспонента конечной абелевой группы и критерий цикличности

Определение 10.1. *Экспонентой* конечной абелевой группы A называется число

$$\exp A = \min\{m \in \mathbb{N} \mid \forall a \in A: ma = 0\}.$$

Замечание.

1. Из того, что $\forall a \in A \forall m \in \mathbb{Z}: ma = 0 \iff m : \text{ord}(a)$, определение экспоненты можно переписать в виде $\exp A = \text{НОК}\{\text{ord}(a) \mid a \in A\}$.
2. Из того, что $\forall a \in A: |A| : \text{ord}(a)$, следует, что $|A|$ — общее кратное множества $\{\text{ord}(a) \mid a \in A\}$, а значит, $|A| : \exp A$. В частности, $\exp A \leq |A|$.

Теорема (Критерий цикличности). *Группа A является циклической тогда и только тогда, когда $\exp A = |A|$.*

Доказательство. Пусть $|A| = n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$ — разложение на простые множители, где p_i — простое и $k_s \in \mathbb{N}$ ($p_i \neq p_j$ при $i \neq j$).

Необходимость. Если $A = \langle a \rangle$, то $\text{ord}(a) = n$, откуда $\exp A = n$.

Достаточность. Если $\exp A = n$, то для $i = 1, \dots, s$ $\exists c_i \in A: \text{ord}(c_i) = p_i^{k_i} m_i$, $m_i \in \mathbb{N}$. Для каждого $i = 1, \dots, s$ положим $a_i = m_i c_i$, тогда $\text{ord}(a_i) = p_i^{k_i}$. Рассмотрим элемент $a = a_1 + \dots + a_s$ и покажем, что $\text{ord}(a) = n$. Пусть $\exists m \in \mathbb{N}: ma = 0$, т.е. $ma_1 + \dots + ma_s = 0$. При фиксированном $i \in \{1, \dots, s\}$ умножим обе части последнего равенства на $n_i = n/p_i^{k_i}$. Видно, что $\forall i \neq j: mn_i a_j = 0$, поэтому в левой части останется только слагаемое $mn_i a_i$, откуда $mn_i a_i = 0 \implies mn_i : p_i^{k_i}$, а т.к. $n_i : p_i$, то $m : p_i^{k_i}$. В силу произвольности выбора i отсюда вытекает, что $m : n$, и т.к. $na = 0$, то окончательно получаем $\text{ord}(a) = n$. Значит, $A = \langle a \rangle$ — циклическая группа. ■

11 Кольца и поля

Определение 11.1. *Кольцо* — это множество R , на котором заданы две бинарные операции « $+$ » (сложение) и « \cdot » (умножение), удовлетворяющее следующим условиям:

1. $(R, +)$ — абелева группа;
2. (R, \cdot) — алгебраическая структура;
3. $\forall a, b, c \in R: a(b + c) = ab + ac$ и $(a + b)c = ac + bc$.

Замечание.

1. $\forall a \in R: 0 \cdot a = a \cdot 0 = 0$;
2. Если $|R| > 1$, то $1 \neq 0$.

Доказательство.

1. $a0 = a(0 + 0) = a0 + a0 \implies 0 = a0$.
2. Следует из условий выше. ■

Примеры.

1. Числовые кольца $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
2. Кольцо \mathbb{Z}_n вычетов по модулю n ;
3. Кольцо матриц $\text{Mat}_{n \times n}(\mathbb{R})$;
4. Кольцо многочленов $\mathbb{R}[x]$ от переменной x с коэффициентами из \mathbb{R} ;
5. Кольцо функций $F(M, \mathbb{R})$ из множества M в \mathbb{R} с поэлементными операциями сложения и умножения:

$$\forall m \in M: (f_1 + f_2)(m) = f_1(m) + f_2(m), \quad (f_1 \cdot f_2)(m) = f_1(m) \cdot f_2(m).$$

Определение 11.2. Кольцо R называется *ассоциативным*, если

$$\forall a, b, c \in R: (ab)c = a(bc).$$

Определение 11.3. Кольцо R называется *коммутативным*, если

$$\forall a, b \in R: ab = ba.$$

Определение 11.4. Элемент a кольца R называется *обратимым*, а кольцо *содержащим единицу*, если

$$\exists b \in R: ab = ba = 1.$$

Замечание. Все обратимые элементы кольца образуют группу по умножению.

Определение 11.5. Элемент a кольца R называется *левым* (соответственно *правым*) *делителем нуля*, если $a \neq 0$ и $\exists b \neq 0 \in R: ab = 0$ (соответственно $ba = 0$).

Замечание. Если кольцо коммутативно, то множества левых и правых делителей нуля совпадают. Тогда левые и правые делители нуля называются просто «делителями нуля».

Замечание. Все делители нуля в кольце необратимы.

Доказательство. Пусть R — кольцо; $a \neq 0$, $b \neq 0$. Если $ab = 0$ и $\exists a^{-1}$, то $a^{-1}ab = a^{-1}0 \implies b = 0$ — противоречие. ■

Определение 11.6. Элемент a кольца R называется *нильпотентным* (*нильпотентом*), если $a \neq 0$ и $\exists n \in \mathbb{N}: a^n = 0$.

Замечание. Всякий nilпотент является делителем нуля.

Определение 11.7. Кольцо называется *телом*, если оно ассоциативно, содержит $1 \neq 0$, и любой ненулевой элемент обратим.

Пример. \mathbb{H} — тело кватернионов.

Определение 11.8. Тело называется *полем*, если оно коммутативно.

Замечание. В поле не существует делителей нуля.

Примеры. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{A}, \mathbb{Z}_2$.

Теорема 11.1. *Кольцо вычетов \mathbb{Z}_p является полем тогда и только тогда, когда p — простое число.*

Доказательство.

Необходимость. Если $n = 1$, то $\mathbb{Z}_n = \{0\}$ — не поле.

Если $n > 1$ и $n = m \cdot k$, где $1 < m, k < n$, то $\overline{m} \cdot \overline{k} = \overline{0} \implies$ в \mathbb{Z}_n есть делитель нуля $\implies \mathbb{Z}_n$ — не поле.

Достаточность. Пусть p — простое, $\bar{a} \in \mathbb{Z}_p \setminus \{\bar{0}\}$.

Тогда $\text{НОД}(a, p) = 1 \implies \exists k, l \in \mathbb{Z}: ak + pl = 1$. Значит, $\bar{a} \cdot \bar{k} + \bar{p} \cdot \bar{l} = \bar{1} \implies a \cdot k \equiv 1 \pmod{p} \implies a$ обратим, противоречие. ■

Теорема (Ваддербёрн). *Всякое конечное тело является полем.*

Список литературы

- [1] Алексеев В.Б. *Теорема Абеля в задачах и решениях*: МЦНМО, 2024.
- [2] Артин Э. *Теория Галуа*: МЦНМО, 2004.
- [3] Атья М., Макдональд И. *Введение в коммутативную алгебру*: МЦНМО, 2021.
- [4] Верещагин Н.К., Шень А. *Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств*: МЦНМО, 2024.
- [5] Винберг Э.Б. *Курс алгебры*: МЦНМО, 2019.
- [6] Кострикин А.И. *Введение в алгебру*: МЦНМО, 2020.
- [7] Курош А.Г. *Курс высшей алгебры*: Лань, 2007.
- [8] Линдон Р., Шупп П. *Комбинаторная теория групп*: Мир, 1980.
- [9] Маклейн С. *Категории для работающего математика*: Физматлит, 2004.
- [10] [Авдеев Р.С. Алгебра](#)
- [11] [Аржанцев И.В. Алгебра. Часть 1](#)
- [12] [Аржанцев И.В. Алгебра. Часть 2](#)
- [13] [Аржанцев И.В. Алгебра. Часть 3](#)
- [14] [Аржанцев И.В. Конечные поля](#)
- [15] [Савватеев А.В. Конечные поля](#)
- [16] [Савватеев А.В. Геометрия и группы](#)
- [17] [Савватеев А.В. Теория Галуа](#)
- [18] [Брагилевский В.Н. и др. Теория категорий](#)
- [19] [Элементарное введение в теорию групп \(для физиков\)](#)