

Теория групп

Артём Рашевский

2025

Содержание

| | | |
|----|--------------------------------------------------------------------------|----|
| 1 | Бинарные операции. Полугруппы, моноиды и группы . . | 4 |
| 2 | Подгруппы. Циклические подгруппы и группы. Порядок элемента | 6 |
| 3 | Смежные классы. Индекс подгруппы. Теорема Лагранжа | 9 |
| 4 | Группы движений | 11 |
| 5 | Группы перестановок | 13 |
| 6 | Нормальные подгруппы. Факторгруппы | 16 |
| 7 | Гомоморфизмы групп. Четверная группа Клейна. Теорема Кэли | 18 |
| 8 | Теорема о гомоморфизме. Классификация циклических групп | 22 |
| 9 | Группы автоморфизмов | 24 |
| 10 | Классы сопряжённости | 27 |
| 11 | Прямое произведение групп | 29 |
| 12 | Свободные абелевы группы | 31 |
| 13 | Структура абелевых групп | 33 |
| 14 | Порождающие элементы | 35 |
| 15 | Коммутант | 36 |
| 16 | Разрешимые группы | 39 |
| 17 | Простые группы | 40 |
| 18 | Действия групп. Формула Бёрнсайда | 41 |

| | |
|------------------------------------------------------|----|
| 19 p -группы. Теоремы Силова | 44 |
| 20 Кольца и поля | 47 |
| 21 Приложения теории групп в криптографии* | 50 |
| 22 Группы Ли* | 51 |
| 23 Введение в гомологическую алгебру* | 52 |
| Список литературы | 53 |

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:

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

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

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

$$\mathbf{SO}_n(\mathbb{R}) = \mathbf{O}_n(\mathbb{R}) \cap \mathbf{SL}_n(\mathbb{R}) — \text{специальная ортогональная группа};$$

$$\mathbf{U}_n = \{A \in \text{Mat}_{n \times n}(\mathbb{C}) \mid A \cdot A^\dagger = I\} — \text{унитарная группа};$$

$$\mathbf{SU}_n = \mathbf{U}_n \cap \mathbf{SL}_n(\mathbb{C}) — \text{специальная унитарная группа}.$$

4. Группы перестановок:

симметрическая группа \mathbf{S}_n — все перестановки длины n ;

знакопеременная группа \mathbf{A}_n — все чётные перестановки длины n .

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

6. *Группа кватернионов*:

Множество $\mathbf{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ с операцией умножения заданной следующим образом: $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$.

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 $(\{1, 3, 5, 7\}, \times(\text{mod } 8))$:

| \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. $n\mathbb{Z}^+ < \mathbb{Z}^+ < \mathbb{Q}^+ < \mathbb{R}^+ < \mathbb{C}^+$;
2. $\mathbf{SO}_n(\mathbb{R}) < \mathbf{O}_n(\mathbb{R}) < \mathbf{GL}_n(\mathbb{R})$;
3. $\mathbf{A}_n < \mathbf{S}_n$.

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

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

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

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

аналогично определяется *правый смежный класс*:

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

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 вычит по простому модулю p , тогда $\bar{a}^{p-1} \equiv 1 \pmod{p}$.

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

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

Доказательство. Пусть $g \in G$ — произвольный не нейтральный 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:

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

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* \mathbf{D}_n :

$$\mathbf{D}_n \stackrel{\text{def}}{=} \text{Isom}(\Delta_n).$$

Утверждение 4.1. $|\mathbf{D}_n| = 2n$.

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:

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

Пример. Таблица Кэли группы \mathbf{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 Группы 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 \mathbf{S}_n , называемую *симметрической группой* или *группой перестановок*.

Утверждение 5.1.

$$|\mathbf{S}_n| = n!$$

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 $\text{sgn}(\sigma) \stackrel{\text{def}}{=} \begin{cases} 1, & \sigma \text{ — чётная} \\ -1, & \sigma \text{ — нечётная.} \end{cases}$

Теорема 5.2.

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

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 $G = \mathbf{S}_3$, $H = \langle (12) \rangle = \{\operatorname{id}, (12)\}$. 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. $H \triangleleft G$;
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 \mathbf{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 \mathbf{S}_4 имеет лишь две нетривиальные нормальные подгруппы — знакопеременную группу \mathbf{A}_4 и четверную группу Клейна \mathbf{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 \mathbf{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.

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

Образ φ определяется как

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

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

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 $\text{Im } \varphi = F$.

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 \mathbf{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 $H < S(G) = \mathbf{S}_n$, 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:

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

Примеры.

1. 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. Если положить $G = (\mathbb{R}^2, +)$, $H = (\mathbb{Z}^2, +)$ и $\varphi : (g, g') \mapsto (e^{2\pi i g}, e^{2\pi i g'})$, то $G/H \cong S^1 \times S^1 \cong \mathbb{T}^2$ — двумерный тор.
2. Пусть $G = \mathbf{GL}_n(\mathbb{R})$, $H = \mathbf{SL}_n(\mathbb{R})$. Построим гомоморфизм $\varphi : \mathbf{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$, $A \mapsto \det A \Rightarrow \ker \varphi = \mathbf{SL}_n(\mathbb{R})$.

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 $\varphi : \mathbb{Z} \rightarrow G$, $k \mapsto g^k$.

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

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 Группы автоморфизмов

Утверждение 9.1. Пусть G — группа. Множество её автоморфизмов $\text{Aut}(G)$ несёт каноническую структуру группы с операцией композиции отображений.

Доказательство. Необходимые свойства: ассоциативность верна для композиции любых отображений, в том числе и автоморфизмов; нейтральный элемент — тождественное отображение; обратный элемент существует, так как автоморфизмы биективны. ■

Утверждение 9.2.

1. $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$;
2. $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$.

Доказательство. Пусть $G_1 = \langle g \rangle$. Тогда любой гомоморфизм $\varphi : G_1 \rightarrow G_2$ однозначно определяется образом порождающего элемента $\varphi(g) \in G_2$. В самом деле, $\forall m \in \mathbb{Z} : \varphi(g^m) = \varphi(g)^m$. Пусть $\varphi : G_1 \rightarrow G_1$ — автоморфизм. Тогда, из сюръективности, $\exists k \in \mathbb{Z} : \varphi(g) = g^k$, и это порождающий элемент G .

1. В \mathbb{Z} всего два порождающих. Для каждого из них есть гомоморфизм:

- $\varphi_1 : 1 \mapsto 1$ ($\varphi_1 = \text{id}$);
- $\varphi_1 : 1 \mapsto -1$ ($\varphi_1 = -\text{id}$).

Это автоморфизмы $\Rightarrow |\text{Aut}(\mathbb{Z})| = 2 \Rightarrow \text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

2. В \mathbb{Z}_n порождающие — это \bar{k} : $\text{НОД}(k, n) = 1$.

Построим $\varphi_{\bar{k}} : \bar{1} \mapsto \bar{k}, \bar{m} \mapsto \overline{km}$. Это биекция из множества в само себя, значит, это автоморфизм. Проверим, что отображение $\bar{k} \mapsto \varphi_{\bar{k}}$ сохраняет операцию. Действительно,

$$\varphi_{\bar{s}}(\varphi_{\bar{k}}(\bar{m})) = \overline{skm} = \varphi_{\overline{sk}}(\bar{m}) \Rightarrow \text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times. \quad \blacksquare$$

Определение 9.1. Пусть G — группа, $g \in G$. *Внутренним автоморфизмом* группы G , определяемым g , называется отображение $i_g : G \rightarrow G$, $a \mapsto gag^{-1}$.

Проверим, что это автоморфизм:

$$i_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = i_g(a)i_g(b),$$

обратный к нему существует, и это $i_{g^{-1}}$.

Множество всех внутренних автоморфизмов группы G обозначается как $\text{Inn}(G)$.

Лемма 9.1.

1. $\text{Inn}(G) \triangleleft \text{Aut}(G)$;
2. Отображение $i : G \rightarrow \text{Inn}(G)$, $g \mapsto i_g$ является гомоморфизмом групп.

Доказательство.

1. Поскольку $\text{Inn}(G) = \text{Im } i \subseteq \text{Aut}(G)$, то это подгруппа.

Для проверки нормальности возьмём произвольные $\varphi \in \text{Aut}(G)$ и $i_g \in \text{Inn}(G)$ и сопряжём их:

$$(\varphi i_g \varphi^{-1})(a) = \varphi(g \varphi^{-1}(a) g^{-1}) = \varphi(g) a \varphi(g^{-1}) = i_{\varphi(g)}(a).$$

Таким образом, $\varphi i_g \varphi^{-1} \in \text{Inn}(G) \Rightarrow \text{Inn}(G) \triangleleft \text{Aut}(G)$.

2. $i_{gh}(a) = gha(gh)^{-1} = ghah^{-1}g^{-1} = g(hah^{-1})g^{-1} = i_g(i_h(a)) = (i_g \circ i_h)(a)$, то есть операция сохраняется. ■

Определение 9.2. *Центром* группы G называется множество всех элементов группы, коммутирующих со всеми элементами группы:

$$Z(G) \stackrel{\text{def}}{=} \{g \in G \mid \forall g' \in G: gg' = g'g\}.$$

Замечание. $G = Z(G) \Leftrightarrow G$ абелева.

Лемма 9.2. Пусть G — группа, тогда

1. $Z(G) \triangleleft G$;
2. $\forall i \in \text{Aut}(G): \ker i = Z(G)$.

Доказательство. Достаточно доказать только пункт 2, так как пункт 1 из него следует.

2. Проверим, что $\forall a \in G: i_g(a) = a$:

$$g \in Z(G) \Leftrightarrow \forall a \in G: ga = ag \Leftrightarrow gag^{-1} = a \Leftrightarrow i_g(a) = a. \quad \blacksquare$$

Замечание. $\text{Inn}(G) = e \Leftrightarrow G$ абелева.

Утверждение 9.3. Пусть G — группа, тогда $\text{Inn}(G) \cong G/Z(G)$.

Доказательство. Рассмотрим гомоморфизм $i: G \rightarrow \text{Aut}(G), g \mapsto i_g$. Тогда $\text{Im } i = \text{Inn}(G), \ker i = Z(G)$ по предыдущей лемме. По теореме о гомоморфизме, $\text{Im } i = \text{Inn}(G) \cong G/\ker i = G/Z(G)$. \blacksquare

Примеры.

1. $Z(\mathbf{S}_n) = \begin{cases} \mathbf{S}_n, & n \leq 2, \\ \{e\}, & n \geq 3. \end{cases}$
- $Z(\mathbf{A}_n) = \begin{cases} \mathbf{A}_n, & n \leq 3, \\ \{e\}, & n \geq 4. \end{cases}$
2. $Z(\mathbf{GL}_n(\mathbb{R})) = \{\lambda I \mid \lambda \in \mathbb{R} \setminus \{0\}\}.$
3. $Z(\mathbf{D}_n) = \begin{cases} \{e, R_\pi\}, & n = 2k, \\ \{e\}, & n = 2k + 1. \end{cases}$
4. $Z(Q_8) = \{\pm 1\}.$

Определение 9.3. Множество внешних автоморфизмов группы G определяется как

$$\text{Out}(G) \stackrel{\text{def}}{=} \text{Aut}(G)/\text{Inn}(G).$$

10 Классы сопряжённости

Определение 10.1. Пусть G — группа. Элементы $a, b \in G$ называются *сопряжёнными* и обозначаются $a \sim b$, если $\exists g \in G: a = bgb^{-1}$.

Определение 10.2. *Классом сопряжённости* элемента a группы G называется множество

$$C_G(a) \stackrel{\text{def}}{=} \{b \in G \mid a \sim b\}.$$

Лемма 10.1. Пусть G — группа.

1. Отношение сопряжённости является отношением эквивалентности.
2. $C_G(a) = \{a\} \Leftrightarrow a \in Z(G)$.

Доказательство.

1. Проверим свойства отношения эквивалентности:

- Рефлексивность: $a = eae^{-1} \Rightarrow a \sim a$;
- Симметричность: $a = gba^{-1} \Leftrightarrow b = g^{-1}ag$;
- Транзитивность:
 $(a = bgb^{-1}, b = hch^{-1} \Rightarrow a = ghch^{-1}g^{-1}) \Rightarrow (a \sim b, b \sim c \Rightarrow a \sim c)$.

2. $C_G(a) = \{a\} \Leftrightarrow \forall g \in G: gag^{-1} = a \Leftrightarrow a \in Z(G)$. ■

Лемма 10.2. Пусть G — группа, $a, b \in G$.

Тогда $b \in C_G(a) \Rightarrow \text{ord}(b) = \text{ord}(a)$.

Доказательство. Пусть $b = gag^{-1}$, $a^n = e$.

Тогда $b^n = (gag^{-1})^n = ga^n g^{-1} = gg^{-1} = e$ и наоборот из симметричности сопряжённости \Rightarrow минимальные показатели совпадают. ■

Определение 10.3. *Централизатором* элемента a группы G называется множество

$$Z_G(a) \stackrel{\text{def}}{=} \{g \in G \mid ga = ag\}.$$

Замечание. $Z_G(a) < G$.

Утверждение 10.1. Пусть G — конечная группа, $a \in G$. Тогда $|C_G(a)| = \frac{|G|}{|Z_G(a)|}$. В частности, $|G| : |C_G(a)|$.

Доказательство. Пусть $G/Z_G(a)$ — множество левых смежных классов (не факторгруппа, т.к. $Z_G(a)$ не обязательно нормальна). Достаточно установить биекцию $G/Z_G(a) \leftrightarrow C_G(a)$.

Определим отображение $G/Z_G(a) \rightarrow C_G(a)$, $gZ_G(a) \mapsto gag^{-1}$. Проверим:

1. Корректность:

$$\begin{aligned} h \in Z_G(a) &\Rightarrow ghZ_G(a) \mapsto (gh)a(gh)^{-1} = ghah^{-1}g^{-1} = gahh^{-1}g^{-1} = \\ &= gag^{-1} \mapsto gZ_G(a); \end{aligned}$$

2. Сюръективность: по построению;

3. Инъективность:

$$gag^{-1} = g'a(g')^{-1} \Leftrightarrow ag^{-1}g' = g^{-1}g'a \Leftrightarrow g^{-1}g' \in Z_G(a) \Leftrightarrow g' \in Z_G(a).$$

■

11 Прямое произведение групп

Определение 11.1. *Прямым произведением групп G_1, \dots, G_m называется группа*

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

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 11.2. 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 11.1. 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

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

12 Свободные абелевы группы

Определение 12.1. Кручением или периодической частью группы G называется множество элементов конечного порядка

$$\text{Tor}(G) \stackrel{\text{def}}{=} \{g \in G \mid \text{ord}(g) < \infty\}.$$

Лемма 12.1. Если группа A — абелева, то $\text{Tor}(A) < A$.

Доказательство. Пусть $\text{ord}(a) = n$, $\text{ord}(b) = m$, $a, b \in A$. Тогда $nm(a + b) = 0 \implies \text{ord}(a + b) = 0$. ■

Замечание. В неабелевой группе элементы конечного порядка не всегда образуют подгруппу.

Определение 12.2. Группа A называется *конечнопорождённой*, если $\forall a \in A \exists a_1, \dots, a_n \in A$: $a = k_1 a_1 + \dots + k_n a_n$ для некоторых $k_1, \dots, k_n \in \mathbb{Z}$. Такой набор $\{a_1, \dots, a_n\}$ называется *системой образующих* или *порождающих*.

Примеры.

1. Любая конечная абелева группа конечнопорождена.

2. Решётка $\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n \text{ раз}} = \{(c_1, \dots, c_n) \mid c_i \in \mathbb{Z}\}$. Системой порождающих будет *стандартный базис*

$$\{e_1 = (1, 0, \dots, 0), e_2 = (0, 1, \dots, 0), \dots, e_n = (0, 0, \dots, 1)\}.$$

Определение 12.3. Система порождающих $\{a_1, \dots, a_n\}$ группы A называется *базисом*, если $\forall a \in A$ запись $a = k_1 a_1 + \dots + a_n k_n$ единственна. Группа, обладающая базисом, называется *свободной*. Число элементов в базисе называется *рангом* и обозначается $\text{rank } A$.

Утверждение 12.1. Все базисы свободной абелевой группы содержат одно и то же число элементов.

Лемма 12.2. Свободная абелева группа A ранга n изоморфна \mathbb{Z}^n .

Доказательство. Если $\{e_1, \dots, e_n\}$ — базис в A , то $a = k_1e_1 + \dots + k_ne_n \leftrightarrow (k_1, \dots, k_n) \in \mathbb{Z}^n$. Для этого отображения простым образом проверяются корректность, биективность и сохранение операции. ■

Теорема 12.1. Всякая подгруппа B свободной абелевой группы A ранга n является свободной абелевой группой ранга $\leq n$.

Утверждение 12.2. Пусть A — свободная абелева группа с базисом $\{e_1, \dots, e_n\}$, D — произвольная абелева группа, $d_1, \dots, d_n \in D$ — произвольные элементы. Тогда $\exists!$ гомоморфизм

$$\varphi : A \rightarrow D, \quad \varphi(e_i) = d_i, \quad i = \overline{1, n}.$$

Доказательство. $\forall a \in A: a = k_1e_1 + \dots + k_ne_n$.

Положим $\varphi(a) = k_1\varphi(e_1) + \dots + k_n\varphi(e_n)$. Это гомоморфизм, что проверяется очевидным образом. ■

Следствие. Для любой конечнопорождённой абелевой группы D существует эпиморфизм $\varphi : A \twoheadrightarrow D$ из некоторой свободной абелевой группы A .

Доказательство. Пусть $\{d_1, \dots, d_n\}$ — порождающие элементы группы D . Положим $A = \mathbb{Z}^n$ и определим φ условием $\varphi(e_i) = d_i$, где $\{e_1, \dots, e_n\}$ — стандартный базис в \mathbb{Z}^n . Тогда φ сюръективен, т.к. d_1, \dots, d_n — порождающие. ■

13 Структура абелевых групп

Определение 13.1. Конечная абелева группа A называется *примарной*, если $|A| = p^k$ для некоторого $k \in \mathbb{N}$, где p — простое.

Теорема 13.1. Любая конечнопорождённая абелева группа A изоморфна прямой сумме примарных циклических групп и бесконечных циклических групп:

$$A \cong \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{k_t}},$$

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).

Определение 13.2. Экспонентой конечной группы G называется число

$$\exp G \stackrel{\text{def}}{=} \min\{m \in \mathbb{N} \mid \forall g \in G: mg = 0\}.$$

Замечание.

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

Примеры.

1. $\exp(\mathbb{Z}_n) = n$;
2. $\exp(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 2$;
3. $\exp(\mathbf{S}_3) = 6$.

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. ■

14 Порождающие элементы

Определение 14.1. Подгруппа в группе G называется порождённой подмножеством S , если эта группа есть множество элементов вида $g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k}$, где $g_{i_p} \in S, \varepsilon_p \in \{\pm 1\}$. Легко заметить, что это наименьшая подгруппа в G , содержащая S .

Утверждение 14.1. Группа A_n порождается:

1. парами транспозиций;
2. тройными циклами;
3. парами независимых транспозиций при $n \geq 5$.

Доказательство.

1. $\forall \sigma \in S_n: \sigma = \tau_1 \dots \tau_k$, где τ_i — транспозиция. Если σ чётная, то $k = 2s$. Из этого следует, что $\sigma = (\tau_1 \tau_2) \dots (\tau_{2s-1} \tau_{2s})$.
2. Выразим пары транспозиций через тройные циклы:

$$(ij)(ij) = e, (ij)(jk) = (ijk), (ij)(kl) = (ijk)(jkl).$$

3. Выразим пару зависимых транспозиций через пары независимых транспозиций:

$$(ij)(jk) = ((ij)(lm))((jk)(lm)), \quad l, m \in \{i, j, k\}. \quad \blacksquare$$

Определение 14.2. *Задание (копредставление или генетический код) группы* — один из методов описания группы. Пусть подмножество S группы G порождает её. При такой кодировке конкатенация слов соответствует умножению элементов группы, а значит, теоретически вся групповая структура задаётся информацией о том, какие пары таких слов представляют один и тот же элемент группы G . Такие пары называются *соотношениями*. Метод состоит в том, чтобы указать (по возможности небольшой) список R определяющих соотношений, которого, с учётом заранее оговоренных правил вывода, хватит для хранения полной информации о группе. В этом случае пишут $G \cong \langle S \mid R \rangle$.

15 Коммутант

Определение 15.1. Пусть G — группа. Коммутатором двух элементов $x, y \in G$ называется $[x, y] \stackrel{\text{def}}{=} xyx^{-1}y^{-1} \in G$.

Замечание.

1. $[x, y] = e \iff xy = yx$;
2. $xy = [x, y]yx$, поэтому $[x, y]$ называют *корректирующим множителем*;
3. $[x, x] = e$;
4. $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$.

Определение 15.2. Коммутантом или производной подгруппой группы G называется подгруппа G' (или $[G, G]$) $\leq G$, порождённая всеми коммутаторами в G .

Замечание. $[G, G] = \{e\} \iff G$ — абелева.

Пример. $G = \mathbf{S}_n \Rightarrow [\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ — чётная $\Rightarrow G' \leq \mathbf{A}_n$. С другой стороны, \mathbf{A}_n порождается тройными циклами, которые, в свою очередь, представимы как коммутаторы:

$$(ijk) = (ij)(ik)(ij)(ik) = (ij)(ik)(ij)^{-1}(ik)^{-1} = [(ij), (ik)] \Rightarrow \mathbf{A}_n \leq G' \Rightarrow \\ \Rightarrow \mathbf{A}_n = G'.$$

Утверждение 15.1. Пусть G — группа, тогда:

1. $G' \triangleleft G$;
2. G/G' абелева;
3. если $N \triangleleft G$, то G/N абелева $\iff G' \leq N$;
4. если $G' \leq K \leq G$, то $K \triangleleft G$.

Доказательство. Достаточно доказать только факты 3 и 4, из которых сразу следуют 2 и 1, соответственно.

$$\begin{aligned} 3. \quad \forall g, h \in G: (gN)(hN) &= (hN)(gN) \Leftrightarrow (gN)(hN)(gN)^{-1}(hN)^{-1} = \\ &= (ghg^{-1}h^{-1}N) = eN \Leftrightarrow ghg^{-1}h^{-1} \in N \Leftrightarrow \\ &\Leftrightarrow N \text{ содержит все коммутаторы} \Leftrightarrow G' \leq N. \end{aligned}$$

$$4. \quad \text{Если } g \in G, k \in K, \text{ то } gkg^{-1} = gkg^{-1}k^{-1}k = [g, k]k. \quad \text{Так как} \\ [g, k] \in K, \text{ то } gkg^{-1} \in K \Rightarrow K \triangleleft G. \quad \blacksquare$$

Лемма 15.1. Пусть $\varphi : G_1 \rightarrow G_2$ — гомоморфизм. Тогда $\varphi(G'_1) \leq G'_2$. Если φ сюръективен, то $\varphi(G'_1) = G'_2$.

Доказательство.

$$\begin{aligned} \varphi([x, y]) &= \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x^{-1})\varphi(y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = \\ &= [\varphi(x), \varphi(y)] \in G'_2 \Rightarrow \varphi(G'_1) \leq G'_2. \end{aligned}$$

Если φ сюръективен и $a, b \in G_2$, то $\exists x, y \in G_1: a = \varphi(x), b = \varphi(y)$. Тогда $[a, b] = [\varphi(x), \varphi(y)] = \varphi([x, y]) \in \varphi(G'_1) \Rightarrow G'_2 \leq \varphi(G'_1) \Rightarrow \varphi(G'_1) = G'_2. \quad \blacksquare$

Определение 15.3. Пусть G — группа. Подгруппа $H \leq G$ называется *характеристической*, если она устойчива относительно всех автоморфизмов, т.е. $\forall \varphi \in \text{Aut}(G): \varphi(H) = H$.

Замечание. Центр группы является характеристической подгруппой.

Утверждение 15.2. Коммутант группы является характеристической подгруппой.

Доказательство. Достаточно проверить, что $\forall \varphi \in \text{Aut}(G): \varphi([x, y]) \in G'$.
 $\varphi([x, y]) = [\varphi(x), \varphi(y)] \in G'. \quad \blacksquare$

Замечание. Если $H \leq G$, то $H' \subseteq G'$.

Лемма 15.2. $D'_n = \begin{cases} \langle R_{\frac{2\pi}{n}} \rangle, & n = 2s + 1, \\ \langle R_{\frac{2\pi}{s}} \rangle, & n = 2s. \end{cases}$

Доказательство. Коммутаторы вращений тривиальны.

$$R_\varphi S_v R_{-\varphi} S_v = S_{R_\varphi v} S_v = R_{2\varphi}.$$

$S_1 S_2 S_1 S_2 = R_{2\varphi} R_{2\varphi} = R_{4\varphi}$, где φ — угол между осями симметрий.

Таким образом, $D'_n = \{R_{2 \cdot \frac{2\pi k}{n}}\}_{k=0}^{n-1} = \begin{cases} \langle R_{\frac{2\pi}{n}} \rangle, & n = 2s + 1, \\ \langle R_{\frac{2\pi}{s}} \rangle, & n = 2s. \end{cases}$ ■

Лемма 15.3. $A'_n = \begin{cases} e, & n \leq 3, \\ V_4, & n = 4, \\ A_n, & n \geq 5. \end{cases}$

Доказательство. При $n \leq 3$ A_n абелева.

При $n = 4$: $V_4 \triangleleft A_n$, $|A_4/V_4| = \frac{12}{4} = 3$ — простое число $\Rightarrow A_4/V_4 \cong \mathbb{Z}_3$ — абелева $\Rightarrow A'_4 \leq V_4$. С другой стороны, $A'_4 \neq \{e\}$, т.к. A_4 не абелева. Но A_4 состоит из двух классов сопряжённости \Rightarrow в V_4 нет собственных подгрупп, нормальных в $A_4 \Rightarrow A'_4 = V_4$.

При $n \geq 5$: применяя вышеописанные рассуждения к произвольной четвёрке индексов i, j, k, l , увидим, что любая пара независимых транспозиций лежит в A'_n . Такие пары порождают A_n , значит, $A'_n = A_n$. ■

Лемма 15.4. $GL'_n(F) = SL_n(F)$ при $|F| \geq 4$, $n \geq 2$.

Доказательство. $\det[A, B] = \det(ABA^{-1}B^{-1}) = 1 \Rightarrow GL'_n(F) \subseteq SL_n(F)$.

С другой стороны, $SL'_n(F) = SL_n(F) \subseteq GL'_n(F)$. Значит, $GL'_n(F) = SL_n(F)$. ■

16 Разрешимые группы

17 Простые группы

18 Действия групп. Формула Бёрнсайда

Определение 18.1. Пусть G — группа, X — произвольное множество. *Действием* группы G на множестве X называется гомоморфизм $\alpha : G \rightarrow S(X)$, где $S(X)$ — группа биекций на X . Альтернативное определение заключается в том, что действие — отображение $G \times X \rightarrow X$, $(g, x) \mapsto gx$, удовлетворяющее условиям:

1. $\forall x \in X: ex = x$;
2. $\forall g, h \in G \forall x \in X: g(hx) = (gh)x$.

Действие G на X обозначается $G \curvearrowright X$ или $G : X$.

Замечание. Эти определения эквивалентны.

Определение 18.2. *Орбитой* точки $x \in X$ называется множество

$$Orb(x) \stackrel{\text{def}}{=} \{gx \mid g \in G\} \subseteq X.$$

Определение 18.3. *Стабилизатором (стационарной подгруппой, подгруппой изотропии)* точки $x \in X$ называется множество

$$St(x) \stackrel{\text{def}}{=} \{g \in G \mid gx = x\} \subseteq G.$$

Замечание. $St(x) < G$.

Определение 18.4. Действие

- *транзитивно*, если $\forall x, y \in X \exists g \in G: y = gx$ (т.е. X состоит из одной орбиты);
- *свободно*, если $\exists x \in X: gx = x$ влечёт $St(x) = \{e\}$;
- *эффективно*, если $\forall x \in X: gx = x$ влечёт $g = e$ (т.е. действие инъективно).

Определение 18.5. *Ядром неэффективности действия α* называется множество

$$\ker \alpha \stackrel{\text{def}}{=} \{g \in G \mid \forall x \in X: gx = x\}.$$

Замечание. От действия $G \curvearrowright X$ можно перейти к действию $G/\ker \alpha \curvearrowright X : g \ker \alpha = gx$, которое будет эффективным.

Примеры.

1. $\mathbf{SO}_n(\mathbb{R}) \curvearrowright \mathbb{R}^n, (A, v) \mapsto Av$.

Орбитами этого действия при $n = 2$ будут концентрические окружности с центром в начале координат (а также сама точка начала координат, считающаяся окружностью с нулевым радиусом). В общем случае это сферы с центром в начале координат, а также сама точка начала координат.

Стабилизатор ненулевого вектора $St(v) \cong \mathbf{SO}_{n-1}(\mathbb{R})$ — все специальные ортогональные преобразования в ортогональной плоскости к v . Если же $v = 0$, то $St(v) = \mathbf{SO}_n(\mathbb{R})$. Действие не транзитивно (длина сохраняется), не свободно (хотя при $n = 2$ очень к этому близко) и эффективно.

2. $\mathbf{S}_n \curvearrowright \{1, \dots, n\}, i \mapsto \sigma(i)$.

Действие транзитивно и эффективно, но не свободно при $n \geq 3$, т.к. $St(i) \cong \mathbf{S}_{n-1}$.

3. $\sigma \in \mathbf{S}_n, G = \langle \sigma \rangle \curvearrowright \{1, \dots, n\} = X$.

Орбиты соответствуют независимым циклам в разложении σ .

Действие транзитивно $\Leftrightarrow \sigma$ — цикл длины n .

4. $G = \mathbf{GL}_n(F)$ или $\mathbf{SL}_n(F)$ ($n \geq 2$) $\curvearrowright F^n \setminus \{0\}$, $(A, v) \mapsto Av$.

Орбиты: (для $\mathbf{SL}_n(F)$ при $n > 1$) $F^n \setminus \{0\}$ и $\{0\}$.

5. $G = \mathbf{GL}_n(\mathbb{C}) \curvearrowright \text{Mat}_{n \times n}(\mathbb{C}) = X, (g, M) \mapsto gMg^{-1}$.

Орбиты — матрицы одного оператора в разных базисах: $GM = \{M' \mid \mathcal{J}(M') = \mathcal{J}(M)\}$, где $\mathcal{J}(M)$ — жорданова нормальная форма M .

$$St(M) = Z_{\mathbf{GL}_n(\mathbb{C})}(M) = \{g \mid gM = Mg\}.$$

6. $G = \mathbf{GL}_n(F) \curvearrowright \text{Mat}_{n \times n}(\mathbb{C}) = X, (g, M) \mapsto gMg^T$.

Орбиты GM — матрицы одной билинейной формы.

Три важных действия $G \curvearrowright G$:

1. *левые сдвиги*: $(g, x) \mapsto gx$;
2. *правые сдвиги*: $(g, x) \mapsto xg$;
3. *сопряжения*: $(g, x) \mapsto gxg^{-1}$.

Определение 18.6. Подгруппы $H_1, H_2 < G$ называются *сопряжёнными*, если $\exists g \in G: gH_1g^{-1} = H_2$.

Теорема (формула Бёрнсайда). Пусть G — конечная группа, X — конечное множество, $G \curvearrowright X$. Тогда число орбит действия равно

$$\frac{1}{|G|} \sum_{g \in G} |X^g|, \text{ где } X^g \stackrel{\text{def}}{=} \{x \in X \mid gx = x\}.$$

19 p -группы. Теоремы Силова

Определение 19.1. Пусть p — простое число. Конечная группа G называется p -группой, если $|G| = p^k$ для некоторого $k \in \mathbb{N}$.

Примеры.

1. $|\mathbf{D}_4| = 2^3$ — 2-группа;
2. $|\mathbf{Q}_8| = 2^3$ — 2-группа.

Теорема 19.1.

1. Нетривиальная p -группа имеет нетривиальный центр.
2. Любая p -группа разрешима.

Доказательство.

1. $|G| = p^k$, $G = \bigsqcup C_G(g) \Rightarrow |G| = \sum |C_G(g)|$.
Но $|C_G(g)| = \frac{|G|}{|Z_G(g)|} = p^l$, $l \leq k$. При этом $|C_G(g)| = 1 \Leftrightarrow g \in Z(G)$.
Поэтому
$$p^k = |G| = |Z(G)| + \sum_{l_i > 0} p^{l_i} \Rightarrow p \cdot |Z(G)| \Rightarrow |Z(G)| \neq 1 \Rightarrow Z(G) \neq \{e\}.$$

2. Индукция по k :

- При $k = 0$: $|G| = 1 \Rightarrow G = \{e\} \Rightarrow G$ разрешима.
- При $k > 0$: $Z(G) \neq \{e\}$, $Z(G) \triangleleft G \Rightarrow |G/Z(G)| = p^l < p^k$. По предположению индукции, $G/Z(G)$ разрешима. Сам $Z(G)$ абелев, в частности, разрешим. Значит, и G разрешима. ■

Лемма 19.1. Пусть G — некоммутативная группа, тогда $G/Z(G)$ не циклическая.

Доказательство. Предположим, что $G/Z(G)$ — циклическая. Тогда $\exists a \in G$: $G/Z(G) = \langle aZ(G) \rangle$. Отсюда $\forall g \in G$: $g = a^k z$, где $k \in \mathbb{Z}$, $z \in Z(G)$. Но $(a^{k_1} z_1)(a^{k_2} z_2) = a^{k_1+k_2} z_1 z_2$. Получаем противоречие с некоммутативностью группы. ■

Теорема 19.2. Любая группа порядка $|p^2|$ абелева.

Доказательство. Пусть G — группа и $|G| = p^2$. Каким может быть центр?

1. $|Z(G)| = 1$ — противоречие с пунктом 1 предыдущей теоремы.
2. $|Z(G)| = p \Rightarrow |G/Z(G)| = p \Rightarrow G/Z(G)$ — циклическая — противоречие с предыдущей леммой.
3. $|Z(G)| = p^2 \Rightarrow G = Z(G) \Rightarrow G$ абелева. ■

Следствие. Если $|G| = p^2$, то либо $G \cong \mathbb{Z}_{p^2}$, либо $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Определение 19.2. Пусть G — конечная группа, p — простое число. Тогда $|G| = p^k m$, где $k \in \mathbb{N}$, $\text{НОД}(m, p) = 1$. Силовской p -подгруппой в G называется подгруппа H_p порядка p^k .

Пример. $G = \mathbf{S}_4 \Rightarrow |G| = 24 = 2^3 \cdot 3$

- $p = 2 \Rightarrow |H_p| = 8 \Rightarrow H_p \cong \mathbf{D}_4$.
- $p = 3 \Rightarrow |H_p| = 3$. Например, $H_p = \langle (123) \rangle$.
- $p \geq 5 \Rightarrow |H_p| = 1 \Rightarrow H_p = \{e\}$.

Теорема (первая теорема Силова). В любой конечной группе G для любого простого p силовская p -подгруппа существует.

Замечание. Первая теорема Силова — это частичное обращение теоремы Лагранжа.

Теорема (вторая теорема Силова).

1. Любая p -подгруппа в G содержится в некоторой силовской p -подгруппе.
2. Все силовские p -подгруппы в G сопряжены.

Следствие. Пусть $H \leq G$ — силовская p -подгруппа. Тогда $H \triangleleft G \Leftrightarrow H$ — единственная силовская p -подгруппа.

Определение 19.3. Пусть G — группа, $H \leq G$. Нормализатором подгруппы H в G называется множество

$$N_G(H) \stackrel{\text{def}}{=} \{g \in G \mid gHg^{-1} = H\}.$$

При этом $H \triangleleft N_G(H)$.

Теорема (третья теорема Силова). Если за n_p обозначить число силовских p -подгрупп в G , то $n_p \equiv 1 \pmod{p}$ и $n_p | m$, где m — индекс силовской p -подгруппы.

Следствие. Группа G порядка pq , где p, q — простые, $p > q$, разрешима степени ≤ 2 .

20 Кольца и поля

Определение 20.1. *Кольцо* — это множество R , на котором заданы две бинарные операции « $+$ » (сложение) и « \cdot » (умножение), удовлетворяющее следующим условиям:

1. $(R, +)$ — абелева группа;
2. (R, \cdot) — полугруппа;
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 20.2. Кольцо R называется *коммутативным*, если

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

Определение 20.3. Говорят, что кольцо R *содержит единицу*, если

$$\exists 1 \in R \forall a \in R: 1 \times a = a \times 1 = a.$$

Определение 20.4. Элемент a кольца R называется *обратимым*, если

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

Замечание. Все обратимые элементы кольца образуют группу по умножению.

Определение 20.5. 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 20.6. Элемент a кольца R называется *нильпотентным* (*нильпотентом*), если $a \neq 0$ и $\exists n \in \mathbb{N}: a^n = 0$.

Замечание. Всякий нильпотент является делителем нуля.

Определение 20.7. Кольцо называется *телом*, если оно содержит $1 \neq 0$, и любой ненулевой элемент обратим.

Пример. \mathbb{H} — тело кватернионов.

Определение 20.8. Тело называется *полем*, если оно коммутативно.

Примеры. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{A}, \mathbb{Z}_p, \mathbb{Q}_p$ для простых p .

Замечание. В полях не существует делителей нуля.

Определение 20.9. *Характеристикой* $\text{char } F$ поля F называется такое $n \in \mathbb{N}$, что $\underbrace{1 + \dots + 1}_{n \text{ раз}} = 0$.

Теорема 20.1. *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. ■

Утверждение 20.1. *Любая конечная подгруппа мультипликативной группы поля является циклической.*

Доказательство. Пусть F — поле, $A \leq F^\times$ — конечная подгруппа, $m = \exp(A)$. Тогда $\forall a \in A: a^m = 1$. Но уравнение $x^m - 1 = 0$ имеет над полем $\leq m$ корней $\implies |A| \leq m$. С другой стороны, $|A| : m \implies m = |A| \Leftrightarrow A$ — циклическая. ■

Следствие. *Если поле F конечно, то F^\times — циклическая.*

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

21 Приложения теории групп в криптографии*

22 Группы Ли*

23 Введение в гомологическую алгебру*

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] [Брагилевский В.Н. и др. Теория категорий](#)
- [16] [Савватеев А.В. Геометрия и группы](#)
- [17] [Савватеев А.В. Конечные поля](#)
- [18] [Савватеев А.В. Теория Галуа](#)
- [19] [Элементарное введение в теорию групп \(для физиков\)](#)