Алгебра. Глава 6. Теория групп

Д. В. Карпов

2025-2026

Определение

Пусть G — множество, и определена $\cdot : G \times G \to G$, удовлетворяющая следующим условиям.

1) *Ассоциативность* $\forall a, b, c \in G \quad (ab)c = a(bc)$.

2) *Нейтральный элемент.* $\exists e \in G$ такой, что $\forall a \in G \quad ae = ea = a$.

3) *Обратный элемент.* $\forall a \in G\ \exists a^{-1} \in G$ такой, что $a \cdot a^{-1} = a^{-1} \cdot a = e$.

4) *Коммутативность* $\forall a, b \in G \quad ab = ba$.

- Если выполнены условия 1 и 2, то G — *полугруппа*.
- Если выполнены условия 1, 2 и 3, то G — *группа*.
- Если выполнены условия 1, 2, 3 и 4, то G — *абелева группа* (или, что то же самое, *коммутативная группа*).

- Операцию в группе можно обозначать как угодно, как правило, используется символ $\cdot$, но это не обязательно.

Определение

Если G и H — группы с одинаковой операцией $\cdot$ и $H \subset G$, то H — *подгруппа* G. Обозначение: $H < G$.

Свойство 1

Нейтральный элемент единственен

Доказательство. Пусть их два: e_1 и e_2. Тогда $e_1 = e_1 e_2 = e_2$. $\square$

Свойство 2

Для любого $a \in G$, обратный элемент a^{-1} единственен.

Доказательство. Пусть a_1 и a_2 — два обратных элемента к $a \in G$. Тогда $a_1 a = a a_2 = e$, откуда $a_1 = a_1(aa_2) = (a_1 a)a_2 = a_2$. $\square$

Свойство 3

Для любого $a \in G$, $(a^{-1})^{-1} = a$.

Доказательство. Так как $aa^{-1} = a^{-1}a = e$, значит, a является обратным к a^{-1}. По Свойству 2, обратный элемент единственен. $\square$

Свойство 4

Для любых $a, b \in G$ выполнено $(ab)^{-1} = b^{-1}a^{-1}$.

Доказательство. $b^{-1}a^{-1}ab = abb^{-1}a^{-1} = e$. $\square$

Лемма 1

Пусть G — группа, $H \subset G$, причем H замкнуто по умножению и взятию обратного элемента (то есть, $\forall a, b \in H$ выполнено $ab \in H$ и $a^{-1} \in H$). Тогда $H < G$.

Доказательство. • При выполнении этих условий, $\cdot : H \times H \to H$ — ассоциативная операция и для любого элемента существует обратный.

• Пусть $a \in H$. Тогда $a^{-1} \in H \Rightarrow e = aa^{-1} \in H$.

• Значит, H — группа с операцией $\cdot$, то есть, $H < G$. □

Лемма 2

Пусть $\{H_i\}_{i \in I}$ — множество подгрупп группы G. Тогда $H = \bigcap\limits_{i \in I} H_i$ — тоже подгруппа группы G.

Доказательство. • Достаточно проверить замкнутость по умножению и взятию обратного элемента.

• Пусть $a, b \in H$. Тогда для всех $i \in I$ мы имеем $a, b \in H_i$.

• Следовательно, для всех $i \in I$ мы имеем $ab \in H_i$, откуда следует, что $ab \in H$.

• Кроме того, для всех $i \in I$ мы имеем $a^{-1} \in H_i$, откуда следует, что $a^{-1} \in H$. □

Подгруппа, порожденная множеством элементов

Определение

Пусть G — группа, $M \subset G$. Тогда
$\langle M \rangle := \{t_1 \dots t_n \; : \; \forall i \in \{1, \dots, n\} \; t_i \in M$ или $t_i^{-1} \in M.\}$
(n не фиксировано, может быть любым натуральным числом) — *подгруппа, порожденная M*.

Лемма 3

Пусть G — группа, $M \subset G$. Тогда:
1) Если подгруппа $H < G$ такова, что $M \subset H$, то и $\langle M \rangle \subset H$;
2) $\langle M \rangle < G$

Доказательство. 1) Поскольку группа G замкнута по умножению и взятию обратных элементов, $\langle M \rangle \subset H$. (Из $t_i^{-1} \in M \subset H$ следует $t_i = (t_i^{-1})^{-1} \in H$. Из $t_1, \dots, t_n \in H$ следует $t = t_1 \dots t_n \in H$.

2) • Пусть $t, s \in \langle M \rangle$. Тогда $t = t_1 \dots t_n$ (где $t_i \in M$ или $t_i^{-1} \in M$ для всех i) и $s = s_1 \dots s_m$ (где $s_i \in M$ или $s_i^{-1} \in M$ для всех i).

• Тогда $ts = t_1 \dots t_n s_1 \dots s_m \in \langle M \rangle$.

• $t^{-1} = t_n^{-1} \cdot \dots \cdot t_1^{-1} \in \langle M \rangle$, так как для любого i либо $t_i^{-1} \in M$, либо $(t_i^{-1})^{-1} = t_i \in M$.

• По Лемме 1, $\langle M \rangle < G$. $\square$

Система образующих. Циклическая группа

Определение

Пусть G — группа.

1) Если $M \subset G$ таково, что $\langle M \rangle = G$, то M — система образующих группы G.

2) Если $a \in G$ таково, что $\{a\}$ — система образующих G (то есть, $\langle a \rangle = G$), то G — циклическая группа.

Определение

1) Пусть G — группа, $a \in G$. Порядок элемента a (обозначение: $\mathrm{ord}(a)$) — это наименьшее такое $k \in \mathbb{N}$, что $a^k = e$. Если такого k нет, то $\mathrm{ord}(a) = \infty$.

2) Порядок группы G — это количество ее элементов (то есть, $|G|$).

- Если $\mathrm{ord}(a) = 1$, то очевидно, что $a = e$.
- Положим $a^0 = e$. Пусть $k \in \mathbb{N}$, $a \in G$. Тогда положим $a^{-k} := (a^{-1})^k$.

Свойство 1

Для любых $k, n \in \mathbb{Z}$ выполнено $a^{k+n} = a^k a^n$.

Доказательство. • При $k, n \in \mathbb{N}$ утверждение очевидно. как и при $0 \in \{k, n\}$.

- Если $k, n < 0$, то $a^{k+n} = (a^{-1})^{|k|+|n|} = (a^{-1})^{|k|}(a^{-1})^{|n|} = a^k a^n$.
- Пусть $k < 0$, $n > 0$. Тогда $a^k a^n = \underbrace{a^{-1} \dots a^{-1}}_{|k|} \cdot \underbrace{a \dots a}_{n}$.
- При $|k| > n$ после сокращения получится $(a^{-1})^{|k|-n} = a^{k+n}$. При $|k| \le n$ после сокращения получится $a^{n-|k|} = a^{k+n}$.
- Случай $k > 0$, $n < 0$ аналогичен. $\square$

Свойство 2

Для любых $k, n \in \mathbb{Z}$ *выполнено* $(a^k)^n = a^{kn}$.

Доказательство. • При $k = 0$ или $n = 0$ утверждение понятно. При $n \in \mathbb{N}$ утверждение немедленно следует из определения степени.

• При $k > 0$ $(a^k)^{-1} = (\underbrace{a \dots a}_{k})^{-1} = \underbrace{a^{-1} \dots a^{-1}}_{k} = (a^{-1})^k$.

• Следовательно, при $k > 0$ и $n < 0$ имеем
$(a^k)^n = (a^k)^{-|n|} = ((a^k)^{-1})^{|n|} = (a^{-1})^{k|n|} = a^{kn}$.

• Так как $a^{-k} = (a^{-1})^k$ по определению степени, при $k < 0$ аналогично. $\square$

Лемма 4

Пусть $G = \langle a \rangle$ — циклическая группа.

1) Если $\mathrm{ord}(a) = k \in \mathbb{N}$, то $G = \{a^0 = e, a, \dots, a^{k-1}\}$ и все эти элементы различны.

2) Если $\mathrm{ord}(a) = \infty$, то $G = \{a^s : s \in \mathbb{Z}\}$ и все эти элементы различны.

Доказательство. • В любом случае, по определению $G = \{a^s : s \in \mathbb{Z}\}$.

1) • Докажем, что $\forall n \in \mathbb{Z}$ мы имеем $a^n \in \{e = a^0, a, a^2, \dots, a^{k-1}\}$.

• Поделим n на k с остатком: $n = qk + r$, где $0 \le r \le k-1$. Тогда $a^n = (a^k)^q \cdot a^r = a^r$, что нам и нужно.

• Пусть $i, j \in \{0, \dots, k-1\}$. Если $a^i = a^j$ и, скажем, $i > j$, то $e = a^i(a^j)^{-1} = a^{i-j}$. Но $i - j < k$, противоречие.

2) Если $i, j \in \mathbb{Z}$, $i > j$ и $a^i = a^j$, то аналогично $a^{i-j} = e$, а значит, $\mathrm{ord}(a) \ne \infty$, противоречие. $\square$

Следствие 1

Для любого $a \in G$ выполнено $\mathrm{ord}(a) = |\langle a \rangle|$.

• Утверждение напрямую следует из Леммы 4.

Лемма 5

Любая подгруппа циклической группы — циклическая.

Доказательство. • Пусть $G = \langle a \rangle$, $H < G$. Если $H = \{e\}$, утверждение очевидно. Далее $H \neq \{e\}$.

• Если $a^m \in H$, то и $a^{-m} = (a^m)^{-1} \in H$. Значит, множество $I = \{m \in \mathbb{N} \ : \ a^m \in H\}$ непусто.

• Рассмотрим минимальное такое $d \in I$ и докажем, что $H = \langle a^d \rangle$.

• Предположим противное, пусть $a^n \in H$ и $n \not\vdots\, d$.

• Поделим n на d с остатком: $n = dq + r$, $0 < r < d$. Тогда $a^n = a^{dq+r} = a^{dq} \cdot a^r \in H$.

• Из $a^d \in H$ следует, что $a^{-dq} \in H$, а значит, и $a^r = a^n \cdot a^{-dq} \in H$. Но $0 < r < d$ противоречит выбору d. $\square$

Определение

Циклическая группа из n элементов обозначается C_n.

Смежные классы

Определение

Пусть G — группа, $H < G$, $a \in G$.

Левый смежный класс — это $aH := \{ah \ : \ h \in H\}$.

Правый смежный класс — это $Ha := \{ha \ : \ h \in H\}$.

Свойство 1

$|H| = |aH| = |Ha|$.

Доказательство. Существует биекция $\varphi : H \to aH$, заданная формулой $\varphi(h) := ah$. Значит, $|H| = |aH|$. Аналогично, $|H| = |Ha|$. $\square$

Свойство 2

$b \in aH \Rightarrow a^{-1}b \in H$.

Доказательство. $b \in aH \Rightarrow b = ah$, где $h \in H$. Тогда $a^{-1}b = h \in H$. $\square$

Свойство 3

$aH = bH \iff a^{-1}b \in H$.

Доказательство. $\Leftarrow$. • Из $a^{-1}b \in H$ следует, что $\forall h \in H$ $a^{-1}b \cdot h \in H \Rightarrow bh = a(a^{-1}bh) \in aH$. Таким образом, $bH \subset aH$.

• Так как $a^{-1}b \in H \Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$, аналогично получаем $aH \subset bH$.

$\Rightarrow$. $aH = bH \Rightarrow b \in aH \Rightarrow a^{-1}b \in H$ по Свойству 2. □

Свойство 4

Если $aH \cap bH \neq \varnothing$, то $aH = bH$.

Доказательство. • Пусть $z \in aH \cap bH$. Тогда $z = ah_1 = bh_2$, где $h_1, h_2 \in H$.

• Следовательно,
$b = ah_1(h_2)^{-1} \Rightarrow a^{-1}b = a^{-1}ah_1(h_2)^{-1} = h_1(h_2)^{-1} \in H$.

• По Свойствам 2 и 3 имеем $aH = bH$. □

Теорема Лагранжа

Определение

Пусть G — группа, $H < G$. Тогда индекс G по H (обозначение: $(G : H)$) — это количество различных смежных классов aH.

• Если множество смежных классов бесконечно, то $(G : H) = \infty$.

Теорема 1

Пусть G — группа, $H < G$. Тогда:

1) $|G| = |H| \cdot (G : H)$;

2) *если G конечна и $a \in G$, то $|G| \mathrel{\vdots} \mathrm{ord}(a)$.*

Доказательство. 1) • Очевидно, $x \in G \Rightarrow x \in xH$.

• По свойству 4 группа G является объединением различных непересекающихся смежных классов по подгруппе H

• Если $|H| = \infty$ или $(G : H) = \infty$, то очевидно, и $|G| = \infty$.

• Пусть $|H| \in \mathbb{N}$, $k := (G : H) \in \mathbb{N}$ и $G = \bigcup\limits_{i=1}^{k} a_i H$, где $a_i \in G$, причем $a_i H \cap a_j H = \varnothing$ при $i \neq j$.

• По Свойству 1 мы имеем $|a_i H| = |H|$ для всех $i \in \{1, \dots, k\}$, следовательно, $|G| = k|H| = (G : H)|H|$.

2) • Если $a \in G$, то G имеет циклическую подгруппу $\langle a \rangle$.

• По пункту 1, $|G| \,\vdots\, |\langle a \rangle| = \mathrm{ord}(a)$ (последнее равенство — по Следствию 1). $\square$

Симметрическая группа

Определение

Пусть $n \in \mathbb{N}$, $I_n = \{1, \dots, n\}$.

1) Подстановка — это биекция $\sigma : I_n \to I_n$. Как правило, мы будем записывать σ как строчку из n чисел: $\sigma(1), \sigma(2), \dots \sigma(n)$ (на k позиции записывается то число, в которое σ переводит k).

2) Симметрическая группа S_n состоит из всех подстановок (в I_n), групповая операция — композиция.

- Как нам известно, композиция ассоциативна.
- Единичным элементом в S_n будет тождественная подстановка id (такая, что $\mathrm{id}(i) = i$ для всех $i \in I_n$.
- Так как $\sigma \in S_n$ — биекция, существует обратная биекция $\sigma^{-1} : I_n \to I_n$).
- Таким образом, S_n — группа.
- Из курса ДМ нам известно, что $|S_n| = n!$.
- Если $k, n \in \mathbb{N}$, $k < n$, мы будем считать, что $S_k < S_n$ (каждую подстановку из S_k отождествим с подстановкой из S_n, так же переставляющей $1, \dots, k$ и оставляющей на месте $k + 1, \dots, n$).

Разложение подстановки на независимые циклы

- Пусть $\sigma \in S_n$. По теореме Лагранжа, $n! = |S_n| \vdots \mathrm{ord}(\sigma)$.
- Значит, существует такое $k \in \mathbb{N}$, что $\sigma^k = \mathrm{id} \iff \forall i \in I_n\, \sigma^k(i) = i$.
- Тогда для каждого $i \in I_n$ существует такое минимальное $k_i \in \mathbb{N}$, что $\sigma^{k_i}(i) = i$.
- Таким образом, σ разбивается на независимые циклы вида $i, \sigma(i), \dots \sigma^{k_i-1}(i)$. (каждый элемент под воздействием σ переходит в следующий, последний переходит в первый).
- В записи каждого цикла главное — циклический порядок, начало не имеет значения.
- Пример. $n = 9$, $\sigma = 643297185$ — стандартная запись.
- Разложение на независимые циклы: $\sigma = (167)(24)(3)(59)(8)$.
- Часто циклы длины 1 в этой записи опускают. Можно записать просто $\sigma = (167)(24)(59)$.

• Разложение подстановки на независимые циклы позволяет легко возводить ее в степень.

• Так, подстановка σ^ℓ прокручивает каждый цикл σ ровно ℓ раз (нужно передвинуться на ℓ ходов по циклу). При этом, цикл может распадаться на несколько меньших.

• Подстановка σ^{-1} прокручивает каждый цикл σ в обратном порядке.

• Пример. Пусть $\sigma = (1678)(243)(59)$. Тогда $\sigma^2 = (17)(68)(234)(5)(9)$, $\quad \sigma^3 = (1876)(2)(3)(4)(59)$, а $\sigma^{-1} = (1876)(234)(59)$.

Лемма 6

Пусть $\sigma \in S_n$ раскладывается на независимые циклы длин $m_1, \dots, m_k$. Тогда $\mathrm{ord}(\sigma) = [m_1, \dots, m_k]$.

Доказательство. • $\sigma^\ell = \mathrm{id}$, если и только если каждый элемент I_n остается на своем месте.

• Это означает, что каждый цикл длины m_i должен прокрутиться кратное m_i число раз, то есть, $\forall j \in \{1, \dots, k\}\ \ell \,\vdots\, m_j$.

• $\mathrm{ord}(\sigma)$ по определению — наименьшее такое число ℓ, а это, очевидно, $[m_1, \dots, m_k]$. $\square$

Определение

1) Подстановка $\sigma \in S_n$ называется циклом длины k, если в ее разложении на независимые циклы есть один цикл длины k, а все не входящие в него элементы остаются на месте.

2) Транспозиция — это цикл длины 2.

• Транспозиция меняет местами два элемента I_n, а все остальные оставляет на месте.

Теорема 2

При $n \geq 2$, транспозиции — система образующих S_n.

Доказательство. • Индукцией по $2 \leq k \leq n$ докажем, что транспозиции порождают подгруппу $S'_k < S_n$ (все подстановки, оставляющие на местах числа $k+1, \dots, n$). База $k = 2$ очевидна.

Переход $k \to k+1$. • Пусть доказано, что каждая подстановка из S'_k — произведение нескольких транспозиций.

• Рассмотрим $\sigma \in S'_{k+1}$. Если $\sigma(k+1) = k+1$, то $\sigma \in S'_k$ и утверждение для σ доказано.

- Пусть $\sigma(i) = k+1$, где $1 \le i \le k$.
- Рассмотрим транспозицию $\tau = (k+1, i)$ и $\sigma' = \sigma\tau$.
- Тогда $\sigma'(k+1) = \sigma(\tau(k+1)) = \sigma(i) = k+1$.
- Так как и τ, и σ оставляют на местах $\{k+2, \dots, n\}$, σ' тоже эти числа оставляет на местах.
- Значит, $\sigma' \in S'_k$ и по индукционному предположению $\sigma' = \tau_1 \dots \tau_\ell$, где $\tau_1, \dots, \tau_\ell$ — транспозиции.
- Тогда $\sigma = \sigma\tau^2 = \sigma'\tau = \tau_1 \dots \tau_\ell\tau$. □

Лемма 7

Пусть $\sigma_m \in S_n$ — цикл длины $m \ge 2$: $\sigma_m = (a_1 a_2 \dots a_m)$. Тогда $\sigma_m = (a_1 a_2)(a_2 a_3) \dots (a_{m-1} a_m)$.

Доказательство. • Индукция по m. База $m = 2$ очевидна.

Переход $k \to k+1$. • По индукционному предположению, $(a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)(a_k a_{k+1}) = (a_1 a_2 \dots a_k)(a_k a_{k+1})$.

- Цикл $\sigma_k = (a_1 a_2 \dots a_k)$ действует так: $\sigma_k(a_i) = a_{i+1}$ при $1 \le i \le k-1$, $\sigma_k(a_k) = a_1$.
- При домножении на транспозицию $(a_k a_{k+1})$ мы меняем местами эти два числа, значит, если $\sigma' = \sigma_k \cdot (a_k a_{k+1})$, то $\sigma'(a_i) = a_{i+1}$ при $1 \le i \le k$ и $\sigma'(a_{k+1}) = a_1$.
- Значит, $\sigma' = \sigma_{k+1}$. □

Четные и нечетные подстановки

Определение

Пусть $\sigma \in S_n$.

• Инверсия — это такая пара чисел (i, j), что $1 \le i < j \le n$ и $\sigma(i) > \sigma(j)$.

• Через $I(\sigma)$ обозначается количество инверсий в подстановке σ.

• Подстановка σ называется чётной, если $I(\sigma) \,\vdots\, 2$ и нечетной, если $I(\sigma) \not\vdots\, 2$

Лемма 8

Пусть $\sigma, \tau \in S_n$, причем τ — транспозиция, а $\sigma' = \sigma\tau$. Тогда $I(\sigma) \not\equiv I(\sigma') \pmod 2$.

Доказательство. • Пусть τ меняет местами $\sigma(i)$ и $\sigma(j)$, где $i < j$.

• Подсчитаем четность числа пар индексов, образующих инверсию ровно в одной из подстановок σ и σ'. Очевидно, в такой паре должно быть хотя бы одно из чисел i и j.

• Пусть $\ell \notin \{i, j\}$.

• Если $\ell < i$, то пара (ℓ, i) — инверсия в $\sigma \iff (\ell, j)$ — инверсия в σ'.

• Если $\ell > j$, то пара (ℓ, j) — инверсия в $\sigma \iff (\ell, i)$ — инверсия в σ'.

• Пусть $i < \ell < j$. Тогда в каждой из пар (ℓ, i) и (ℓ, j) есть инверсия ровно в одной из подстановок σ и σ'.

• Количества посчитанных выше инверсий в σ и σ' имеет одинаковую четность. Осталась только пара (i, j), которая образует инверсию ровно в одной из подстановок σ и σ' и делает общее число инверсий в них разной четности. $\square$

Свойство 1

Пусть $\sigma = \tau_1 \dots \tau_k$ — разложение $\sigma \in S_n$ в произведение транспозиций. Тогда $I(\sigma) \equiv k \pmod 2$.

Доказательство. • Отметим, что id — четная подстановка.

• Так как σ получена домножением id на транспозицию k раз, четность подстановки меняется в точности k раз по Лемме 8. □

Свойство 2

Произведение подстановок одной четности четно, а произведение подстановок разных четностей нечетно.

Доказательство. • Пусть $\sigma, \sigma' \in S_n$, причем σ представляется как произведение k транспозиций, а σ' — как произведение m транспозиций.

• Тогда $I(\sigma) \equiv k \pmod 2$, $I(\sigma') \equiv m \pmod 2$ и $I(\sigma\sigma') \equiv k + m \pmod 2$, откуда следует доказываемое утверждение. □

Свойство 3

Цикл длины k — четная подстановка, если и только если k нечетно.

Доказательство. По Лемме 7, цикл длины k представляется в виде произведения $k-1$ транспозиций. Далее применяем Свойство 1. □

Свойство 4

Пусть в разложении на независимые циклы подстановки $\sigma \in S_n$ — k циклов, имеющих длины $m_1, \dots, m_k$ (не обязательно различные). Тогда σ — четная, если и только если среди чисел $m_1, \dots, m_k$ — четное количество четных.

Доказательство. Следует из Свойств 2 и 3 □

Свойство 5

$I(\sigma) \equiv I(\sigma^{-1}) \pmod 2$ *для любой* $\sigma \in S_n$.

Доказательство. • Рассмотрим разложение на транспозиции $\sigma = \tau_1\tau_2 \dots \tau_k$.

• Так как $\tau_i^{-1} = \tau_i$, мы имеем $\sigma^{-1} = \tau_k \dots \tau_2\tau_1$.

• По Свойству 1, $I(\sigma) \equiv k \equiv I(\sigma^{-1}) \pmod 2$. □

- A_n — множество всех четных подстановок.

Теорема 3

При $n \geq 2$ выполняется:

1) $A_n < S_n$;

2) $|A_n| = \frac{n!}{2}$.

Доказательство. 1) • По Свойству 5, если $\sigma \in A_n$, то и $\sigma^{-1} \in A_n$.

- Пусть $\sigma, \sigma' \in A_n$. По Свойству 2, $\sigma\sigma' \in A_n$.
- По Лемме 1, $A_n < S_n$.

2) • Докажем, что четных и нечетных подстановок в S_n поровну.

• Определим отображение $f : S_n \to S_n$ формулой $f(\sigma) := \sigma \cdot (12)$.

• Отметим, что $f(f(\sigma)) = \sigma \cdot (12)^2 = \sigma$.

• По Лемме 8, подстановки σ и $f(\sigma)$ всегда разной четности.

• Пусть $A_n = \{\sigma_1, \dots, \sigma_k\}$ и $f(\sigma) = \sigma'$. Тогда все подстановки σ'_1, ..., σ'_k — различны и нечетны.

• Если $\sigma' \in S_n$ — нечетная подстановка, то $f(\sigma')$ — четная и $f(f(\sigma')) = \sigma'$.

• Следовательно, $S_n \setminus A_n = \{\sigma'_1, \dots, \sigma'_k\}$.

• Таким образом, $|A_n| = |S_n \setminus A_n|$, откуда следует, что $|A_n| = \frac{n!}{2}$. $\square$

Гомоморфизм групп

Определение

• Пусть G, H — группы. Отображение $f : G \to H$ называется гомоморфизмом, если $\forall\, a, b \in G \quad f(ab) = f(a)f(b)$.

Ядро гомоморфизма f — это $\mathrm{Ker}(f) = \{x \in G \ : \ f(x) = e_H\}$.

Образ гомоморфизма f — это
$\mathrm{Im}(f) = \{y \in H \ : \ \exists x \in G : f(x) = y\}$.

Свойство 1

Если $f : G \to H$ гомоморфизм, то $f(e_G) = e_H$.

Доказательство. $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$. Умножая левую и правую части $(f(e_G))^{-1}$, получаем $f(e_G) = e_H$. □

Свойство 2

Если $f : G \to H$ гомоморфизм, то $f(a^{-1}) = (f(a))^{-1}$.

Доказательство. • $e_H = f(e_G) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$.

• Аналогично, $f(a^{-1}) \cdot f(a) = e_H$. Значит, $f(a^{-1}) = (f(a))^{-1}$. □

Лемма 9

Пусть G, H — группы, $f : G \to H$ — гомоморфизм групп. Тогда:

1) $\mathrm{Ker}(f) < G$.

2) $\mathrm{Im}(f) < H$.

Доказательство. Достаточно проверить условия из Леммы 1.

1) • Пусть $a, b \in \mathrm{Ker}(f)$. Тогда $f(ab) = f(a)f(b) = e_H \cdot e_H = e_H$, следовательно, $ab \in \mathrm{Ker}(f)$.

• $f(a^{-1}) = (f(a))^{-1} = e_H^{-1} = e_H$, следовательно, $a^{-1} \in \mathrm{Ker}(f)$.

2) • Пусть $y, y' \in \mathrm{Im}(f)$, а $x, x' \in G$ таковы, что $f(x) = y$ и $f(x') = y'$.

• Тогда $yy' = f(x)f(x') = f(xx') \in \mathrm{Im}(f)$.

• $y^{-1} = (f(x))^{-1} = f(x^{-1}) \in \mathrm{Im}(f)$. □

Следствие 2

Если $f : G \to H$ гомоморфизм, а $N < G$, то $f(N) = \{f(x) : x \in N\} < H$.

Доказательство. • Очевидно, f индуцирует гомоморфизм $f|_N : N \to H$.

• По Лемме 9 мы имеем $f(N) = \mathrm{Im}(f|_N) < H$. □

Типы гомоморфизмов

- G, H — группы, $f : G \to H$ — гомоморфизм групп.
- Если f — инъекция, то f — мономорфизм.
- Если f — сюръекция (то есть, $\mathrm{Im}(f) = H$), то f —эпиморфизм.
- Если f — биекция, то f — изоморфизм.
- Изоморфизм = мономорфизм + эпиморфизм.

Лемма 10

Пусть $f : G \to H$ — гомоморфизм групп. Тогда f — мономорфизм, если и только если $\mathrm{Ker}(f) = \{e_G\}$.

Доказательство. $\Rightarrow$ • Если f — мономорфизм, то f — инъекция.

• Пусть $a \in \mathrm{Ker}(f)$. Из $f(a) = e_H = f(e_G)$ следует, что $a = e_G$ (так как f — инъекция).

$\Leftarrow$ • Пусть $f(a) = f(b)$. Тогда
$f(a \cdot b^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot (f(b))^{-1} = f(b) \cdot (f(b))^{-1} = e_H$.

• Значит, $a \cdot b^{-1} \in \mathrm{Ker}(f) = \{e_G\}$, откуда $a \cdot b^{-1} = e_G$ и $a = b$.
Таким образом, f — инъекция, а значит, мономорфизм. $\square$

Лемма 11

Пусть $f : G \to H$ — изоморфизм групп. Тогда и $f^{-1} : H \to G$ — изоморфизм групп.

Доказательство. • Достаточно доказать, что f^{-1} — гомоморфизм (так как отображение, обратное к биекции — биекция).

• Рассмотрим любые $a, b \in H$.

• Так как f — гомоморфизм,
$f(f^{-1}(ab)) = ab = f(f^{-1}(a)) \cdot f(f^{-1}(b)) = f(f^{-1}(a) \cdot f^{-1}(b))$.

• Из того, что f — биекция, следует, что
$f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b)$. А это и значит, что f^{-1} — гомоморфизм групп. □

Определение

Если существует изоморфизм групп $f : G \to H$, то говорят, что эти группы изоморфны. Обозначение: $G \simeq H$.

Теорема 4

$\simeq$ — отношение эквивалентности на множестве всех групп.

Доказательство. • Рефлексивность очевидна: тождественное отображение $\mathrm{id} : G \to G$ (заданное формулой $\mathrm{id}(x) = x$ для всех $x \in G$), очевидно, является изоморфизмом.

• Симметричность доказана в Лемме 11.

• Докажем транзитивность. Пусть F, G, H — группы, $F \simeq G$ и $G \simeq H$.

• Тогда существуют изоморфизмы $\varphi : F \to G$ и $\psi : G \to H$. Докажем, что их композиция $\psi\varphi : F \to H$ (заданная правилом $(\psi\varphi)(a) := \psi(\varphi(a))$) также является изоморфизмом.

• Композиция биекций ψ и φ, очевидно, является биекцией.

• Проверим, что $\psi\varphi$ — гомоморфизм групп:

$\psi\varphi(ab) = \psi(\varphi(ab)) = \psi(\varphi(a) \cdot \varphi(b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b)) = (\psi\varphi)(a) \cdot (\psi\varphi)(b).$ $\square$

Автоморфизмы группы

Определение

Пусть G группа.

• **Автоморфизм** группы G — это изоморфизм $\varphi : G \to G$.

• Множество всех автоморфизмов группы G обозначим через $\mathrm{Aut}(G)$.

Лемма 12

$\mathrm{Aut}(G)$ — *группа относительно композиции.*

Доказательство. • Ассоциативность композиции нам известна.

• Очевидно, тождественное отображение id подходит в качестве нейтрального элемента.

• Для каждого $\varphi \in \mathrm{Aut}(G)$ по Лемме 11 мы имеем $\varphi^{-1} \in \mathrm{Aut}(G)$. $\square$

Сопряжения

Определение

Пусть G группа, $a \in G$.

- Сопряжение элементом a — это отображение $I_a : G \to G$, заданное формулой $I_a(x) := a^{-1}xa$.
- Обозначим через $\mathrm{Inn}(G)$ множество всех сопряжений группы G.
- Очевидно, $I_e = \mathrm{id}$.
- Если группа G абелева, то $\forall a \in G \quad I_a = \mathrm{id}$.

Лемма 13

Для любой группы G $\mathrm{Inn}(G) < \mathrm{Aut}(G)$.

Доказательство. • Сначала докажем, что $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$. Пусть $a \in G$.

• Очевидно, $a^{-1}xa = a^{-1}ya \iff x = y$, поэтому, I_a — биекция.

• Так как $I_a(x)I_a(y) = a^{-1}xaa^{-1}ya = I_a(xy)$, I_a — гомоморфизм, а значит, $I_a \in \mathrm{Aut}(G)$.

• По Лемме 1, достаточно проверить замкнутость $\mathrm{Inn}(G)$ по умножению и взятию обратного элемента.

• Пусть $a, b \in G$. Тогда $(I_a \cdot I_b)(x) = a^{-1}(b^{-1}xb)a = (ba)^{-1}x(ba) = I_{ba}(x)$. Таким образом, $I_a \cdot I_b = I_{ba}$.

• Теперь для $a \in G$ несложно проверить, что $I_a \cdot I_{a^{-1}} = I_{a^{-1}a} = I_e = \mathrm{id}$ и, аналогично, $I_{a^{-1}} \cdot I_a = \mathrm{id}$. □

Нормальные подгруппы

Определение

Пусть G — группа, $H < G$. Тогда H — **нормальная подгруппа** G, если $I_a(H) = \{I_a(h) \,:\, h \in H\} = H$ для любого $a \in G$. Обозначение: $H \lhd G$.

Лемма 14

Пусть G — группа, $H < G$. Тогда $H \lhd G$, если и только если $aH = Ha$ для любого $a \in G$.

Доказательство. • Пусть $a \in G$. Тогда

$I_a(H) = H \iff \{a^{-1}ha \,:\, h \in H\} = \{h \,:\, h \in H\} \iff \{ha \,:\, h \in H\} = \{ah \,:\, h \in H\} \iff Ha = aH$

(второе равенство множеств получается из первого умножением на a слева, а это — биекция).

• Поэтому,

$H \lhd G \iff \forall a \in G \; I_a(H) = H \iff \forall a \in G \; aH = Ha.$ $\square$

Критерий нормальности

Лемма 15

Пусть G — группа, $H < G$. Тогда $H \lhd G$, если и только если для любых $a \in G$ и $h \in H$ выполнено $I_a(h) \in H$ (или, что то же самое, $I_a(H) \subset H$).

Доказательство. • По определению,
$H \lhd G \iff \forall a \in G\ I_a(H) = H$.

• Поэтому, $\Rightarrow$ очевидна.

$\Leftarrow$. • Для любого $a \in G$ мы знаем, что $I_a(H) \subset H$.

• Так как $a^{-1} \in G$, мы знаем и $I_{a^{-1}}(H) \subset H$. Подействуем на это включение обратной биекцией I_a:

$H = (I_a \cdot I_{a^{-1}})(H) = I_a(I_{a^{-1}}(H)) \subset I_a(H)$.

• Таким образом, для любого $a \in G$ мы знаем, что $I_a(H) \subset H$ и $H \subset I_a(H)$, то есть, $I_a(H) = H$. □

Лемма 16

Пусть G — группа, а $\{H_i\}_{i\in I}$ — нормальные подгруппы G. Тогда $H = \bigcap\limits_{i\in I} H_i \lhd G$.

Доказательство. • Проверим условие из Леммы 15.

• Пусть $a \in G$, $h \in H$. Тогда для любого $i \in I$ мы имеем $h \in H_i$. Так как $H_i \lhd G$, мы имеем $I_a(h) \in H_i$.

• Таким образом, $\forall a \in G$, $\forall h \in H$ $I_a(h) \in H$, откуда $H \lhd G$. □

Лемма 17

Пусть G, H — группы, а $f : G \to H$ — гомоморфизм. Тогда $\ker(f) \lhd G$.

Доказательство. • Проверим условие из Леммы 15.

• Пусть $x \in G$, $a \in \ker(f)$. Тогда

$$f(x^{-1}ax) = f(x^{-1})f(a)f(x) = f(x^{-1}) \cdot e_H \cdot f(x) = f(x^{-1})f(x) = f(x^{-1}x) = f(e_G) = e_H,$$

следовательно, $x^{-1}ax \in \ker(f)$. □

Факторгруппа

• Пусть G — группа, $H \lhd G$. Будем использовать обозначение $\overline{a} := aH$.

• Факторгруппа $G/H = \{\overline{a} \; : \; a \in G\}$. Умножение определим так:
$\overline{a} \cdot \overline{b} := \overline{ab}$.

• Напомним, что для множеств $A, B \subset G$ мы используем обозначение $A \cdot B := \{ab \; : \; a \in A, \; b \in B\}$.

• Если G — группа, а $H < G$, то нетрудно понять, что $H \cdot H = H$ (так как умножение не выводит за пределы H и $H \cdot H \supset eH = H$).

Лемма 18

Пусть G — группа, $H \lhd G$. Тогда умножение в G/H определено корректно.

Доказательство. • Так как $H \lhd G$, для любого $b \in G$ мы имеем $bH = Hb$.

• Поэтому, $\overline{a} \cdot \overline{b} = aH \cdot bH = a \cdot (Hb) \cdot H = a \cdot (bH) \cdot H = ab \cdot (H \cdot H) = abH = \overline{ab}$.

Лемма 19

Пусть G — группа, $H \lhd G$. Тогда G/H — группа.

Доказательство. Ассоциативность умножения: $\forall \overline{a}, \overline{b}, \overline{c} \in G/H$
$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{abc} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

Нейтральный элемент — это $\overline{e}$.

Проверка: $\overline{e} \cdot \overline{a} = \overline{ea} = \overline{a} = \overline{ae} = \overline{a} \cdot \overline{e}$.

Обратный элемент: $(\overline{a})^{-1} := \overline{a^{-1}}$.

Проверка: $\overline{a} \cdot \overline{a^{-1}} = \overline{a \cdot a^{-1}} = \overline{e}$ и $\overline{a^{-1}} \cdot \overline{a} = \overline{a^{-1} \cdot a} = \overline{e}$. □

Лемма 20

Пусть G — группа, $F \lhd G$, $H' < G/F$. Пусть $H = \{x \in G \ : \ \overline{x} \in H'\}$. Тогда $H < G$, причем $|H| = |H'||F|$.

Доказательство. • Пусть $x, y \in H$. Тогда $\overline{x}, \overline{y} \in H'$, а значит, $\overline{xy} = \overline{x} \cdot \overline{y} \in H'$ (так как H' — группа). Следовательно, $xy \in H$.

• Пусть $x \in H$. Тогда $\overline{x} \in H'$, а значит, $\overline{x^{-1}} = (\overline{x})^{-1} \in H'$ (так как H' — группа). Следовательно, $x^{-1} \in H$.

• По Лемме 1, $H < G$.

• Каждый $\overline{x} \in H'$ — это смежный класс xF, содержащий ровно $|F|$ элементов, и все они при факторизации переходят в $\overline{x}$. Поэтому, $|H| = |H'||F|$. □

Теорема 5

Пусть $f : G \to H$ *— гомоморфизм групп. Тогда* $G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$.

Доказательство. • Зададим отображение $\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ формулой $\overline{f}(\overline{a}) := f(a)$.

• Корректность определения $\overline{f}$.

• Пусть $a, b \in G$ таковы, что $\overline{a} = \overline{b}$. По Свойству 3 смежных классов, тогда $a^{-1}b \in \ker(f)$.

• Следовательно, $\overline{f}(\overline{b}) = f(b) = f(a \cdot a^{-1}b) = f(a)f(a^{-1}b) = f(a) \cdot e_H = f(a) = \overline{f}(\overline{a})$.

• $\overline{f}$ — гомоморфизм групп: $\overline{f}(\overline{a} \cdot \overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a)f(b) = \overline{f}(\overline{a}) \cdot \overline{f}(\overline{b})$.

• $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$: для любого $y \in \mathrm{Im}(f)$ существует такой $x \in G$, что $\overline{f}(\overline{x}) = f(x) = y$.

• $\overline{f}$ — монофорфизм. Проверка: пусть $\overline{a} \in \mathrm{Ker}(\overline{f})$. Тогда $f(a) = \overline{f}(\overline{a}) = e_H$, следовательно, $a \in \mathrm{Ker}(f)$, а значит, $\overline{a} = \overline{e}$. Таким образом, $\mathrm{Ker}(\overline{f}) = \{\overline{e}\}$.

• Таким образом, $\overline{f}$ — изофорфизм, а значит, $G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$.

Теорема 6

Пусть G — группа, $H, F \lhd G$, причем $F < H$. Тогда выполнены следующие утверждения.

1) $F \lhd H$.
2) $H/F \lhd G/F$.
3) $G/H \simeq (G/F)/(H/F)$.

Доказательство. 1) $F \lhd G \Rightarrow \forall a \in G \quad I_a(F) = F \Rightarrow$

$\Rightarrow \forall a \in H \quad I_a(F) = F \Rightarrow F \lhd H$.

2) • Из $H \lhd G$ следует, что для любых $a \in G$ и $h \in H$ выполнено $a^{-1}ha \in H$.

• Пусть $\overline{a} := aF$. Тогда для любых $\overline{a} \in G/F$ и $\overline{h} \in H/F$ выполнено $(\overline{a})^{-1} \cdot \overline{h} \cdot \overline{a} = \overline{a^{-1}ha} \in H/F$.

• Следовательно, $H/F \lhd G/F$.

3) • Для $a \in G$ положим $\tilde{a} := aH$. По Свойству 3 смежных классов, $\quad \overline{a} = \overline{b} \Rightarrow a^{-1}b \in F \Rightarrow a^{-1}b \in H \Rightarrow \tilde{a} = \tilde{b}$.

- Определим отображение $f : G/F \to G/H$ формулой $f(\overline{a}) := \tilde{a}$.
- Так как из $\overline{a} = \overline{b}$ следует, что $\tilde{a} = \tilde{b}$, определение f корректно.
- f — гомоморфизм групп: $f(\overline{a} \cdot \overline{b}) = f(\overline{ab}) = \widetilde{ab} = \tilde{a} \cdot \tilde{b} = f(\overline{a})f(\overline{b})$.
- $\mathrm{Ker}(f) = H/F$. Доказательство:
- $\overline{a} \in \mathrm{Ker}(f) \iff \tilde{e} = f(\overline{a}) = \tilde{a} \iff a \in H \iff \overline{a} \in H/F$.
- $\mathrm{Im}(f) = G/H$. Действительно, для любого $\tilde{a} \in G/H$, очевидно, $\overline{a} \in G/F$ и $f(\overline{a}) = \tilde{a}$.
- По Теореме 5, $G/H = \mathrm{Im}(f) \simeq (G/F)/\mathrm{Ker}(f) = (G/F)/(H/F)$. $\square$

Определение

Пусть G — группа. Коммутатор элементов $a, b \in G$ — это $[a, b] = a^{-1}b^{-1}ab$.

Свойство 1

$[a, b] = e \iff ab = ba$ (в этом случае говорят, что элементы a и b коммутируют).

Доказательство. $e = a^{-1}b^{-1}ab \iff ba = ab$. □

Свойство 2

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

Доказательство. $[b, a] \cdot [a, b] = b^{-1}a^{-1}ba \cdot a^{-1}b^{-1}ab = e$. Аналогично, $[a, b] \cdot [b, a] = e$. □

- Для $a, x \in G$ будем применять обозначение $a^x := I_x(a) = x^{-1}ax$.
- Нетрудно проверить, что $(a^x)^{-1} = (a^{-1})^x$.

Свойство 3

$[a, b]^x = [a^x, b^x]$.

Доказательство. $[a, b]^x = x^{-1}(a^{-1}b^{-1}ab)x = (x^{-1}a^{-1}x)(x^{-1}b^{-1}x)(x^{-1}ax)(x^{-1}bx) = (a^{-1})^x(b^{-1})^x a^x b^x = (a^x)^{-1}(b^x)^{-1}a^x b^x = [a^x, b^x]$. □

Определение

Пусть G — группа. Коммутант $[G, G]$ — это подгруппа G, порожденная множеством коммутаторов.

Свойство 4

$[G, G]$ состоит из всех произведений коммутаторов элементов G.

Доказательство. • По определению $[G, G]$ состоит из всех произведений вида $t_1 \dots t_n$, где каждый t_i — коммутатор двух элементов G, или обратный к такому коммутатору.

• По Свойству 2, обратный элемент к коммутатору также является коммутатором. □

Свойство 5

$[G, G] \lhd G$.

Доказательство. • Пусть $x \in G$, $y \in [G, G]$. Тогда $y = [a_1, b_1] \dots [a_n, b_n]$, где $a_1, b_1, \dots, a_n, b_n \in G$.

• Тогда $y^x = ([a_1, b_1] \dots [a_n, b_n])^x = [a_1, b_1]^x \dots [a_n, b_n]^x = [a_1^x, b_1^x] \dots [a_n^x, b_n^x] \in [G, G]$.

• По Лемме 15, $[G, G] \lhd G$. □

Теорема 7

Пусть G — группа, $H \lhd G$. Тогда G/H абелева, если и только если $[G,G] < H$.

Доказательство. • Пусть $\overline{a} := aH$.

• Группа G/H абелева, если и только если для любых $a, b \in G$ выполнено $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$. Преобразуем это условие:

$$\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} \iff \overline{e} = [\overline{a}, \overline{b}] = \overline{[a,b]} \iff [a,b] \in H.$$

• Таким образом, группа G/H абелева, если и только если

$$\forall a, b \in G \; [a,b] \in H \iff [G,G] \subset H \iff [G,G] < H. \qquad \square$$

Действие группы на множестве

Определение

Пусть G — группа, M — множество. Отображение $\cdot : G \times M \to M$ называется действием группы G на множестве M, если выполнены следующие условия:

1) $\forall a, b \in G$, $\forall x \in M \quad (ab)x = a(bx)$;

2) $\forall x \in M \quad ex = x$.

Примеры действий.

1) S_n действует на $\{1, 2, \dots, n\}$.

2) Если G группа, то $\mathrm{Aut}(G)$ действует на G (здесь G выступает в качестве множества).

3) Если G группа, то G (как группа) действует на G (как множестве) левыми умножениями:

$\forall a \in G \ \forall x \in G \quad ax := ax$ (первое умножение — действие, а второе — умножение в группе).

Определение

Пусть группа G действует на множестве M.

1) Орбита элемента $x \in M$ — это

$\langle x \rangle = \{ax \ : \ a \in G\}$.

2) Для $a \in G$ и $N \subset M$ положим $aN := \{ax \ : \ x \in N\}$.

3) Стабилизатор подмножества $N \subset M$ — это

$\mathrm{St}(N) := \{a \in G \ : \ aN = N\}$.

Свойство 1

Для любого $N \subset M$ $\quad \mathrm{St}(N) < G$.

Доказательство. • Достаточно проверить условия из Леммы 1.

• Пусть $a, b \in \mathrm{St}(N)$. Тогда $(ab)N = a(bN) = aN = N$, то есть, $ab \in \mathrm{St}(N)$.

• Пусть $a \in \mathrm{St}(N)$. Тогда
$a^{-1}N = a^{-1}(aN) = (a^{-1}a)N = eN = N$, то есть,
$a^{-1} \in \mathrm{St}(N)$. $\square$

Свойство 2

Пусть $a \in G$, $N \subset M$. *Тогда* $\mathrm{St}(aN) = I_{a^{-1}}(\mathrm{St}(N))$.

Доказательство.

$$x \in \mathrm{St}(aN) \iff (xa)N = x(aN) = aN \iff$$
$$a^{-1}((xa)N) = a^{-1}(aN) \iff$$
$$I_a(x)N = (a^{-1}xa)N = (a^{-1}a)N = eN = N \iff$$
$$I_a(x) \in \mathrm{St}(N).$$

• Таким образом, $\mathrm{St}(aN) = \{x : I_a(x) \in \mathrm{St}(N)\} = \{I_{a^{-1}}(y) : y \in \mathrm{St}(N)\} = I_{a^{-1}}(\mathrm{St}(N))$. □

Свойство 3

Для любого $x \in M$ *выполнено* $x \in \langle x \rangle$.

Доказательство. $ex = x \Rightarrow x \in \langle x \rangle$. □

Свойство 4

Пусть $x, y \in M$, $\langle x \rangle \cap \langle y \rangle \neq \varnothing$. *Тогда* $\langle x \rangle = \langle y \rangle$.

Доказательство. • Пусть $a, b \in G$ таковы, что $ax = by$.

• Тогда $y = (b^{-1}b)y = (b^{-1}a)x$, то есть, $y \in \langle x \rangle$.

• Пусть $z \in \langle y \rangle$, тогда $z = cy$, где $c \in G$ и $z = (cb^{-1}a)x \in \langle x \rangle$

• Таким образом, $\langle y \rangle \subset \langle x \rangle$. Аналогично, $\langle x \rangle \subset \langle y \rangle$. □

Теорема 8

Пусть группа G действует на множестве M, а $x \in M$. Тогда $|\langle x\rangle| \cdot |\mathrm{St}(x)| = |G|$.

Доказательство. • Для $a, b \in G$

$$ax = bx \iff (b^{-1}a)x = b^{-1}(ax) = b^{-1}(bx) = x \iff$$
$$b^{-1}a \in \mathrm{St}(x) \iff b \cdot \mathrm{St}(x) = a \cdot \mathrm{St}(x).$$

(в последнем равенстве мы воспользовались Свойством 3 смежных классов).

• Таким образом, элементы G, одинаково действующие на x, образуют смежный класс по подгруппе $\mathrm{St}(x)$.

• Следовательно, $|\langle x\rangle| = (G : \mathrm{St}(x))$ (количеству смежных классов по подгруппе $\mathrm{St}(x)$).

• Теперь Теорема 8 следует из Теоремы 1 (теоремы Лагранжа). □

Определение

Для любого множества M через S_M обозначим группу всех перестановок множества M (то есть, биекций из M в M) относительно композиции.

- S_M — группа для любого множества M (доказательство аналогично случаю S_n).
- Если M — конечное множество, то $S_M \simeq S_{|M|}$.

Теорема 9

(A. Cayley.) *Любая группа G изоморфна подгруппе группы S_G.*

Доказательство. • Для $g \in G$ определим отображение $f_g : G \to G$ формулой $f_g(x) := gx$.

• Проверим, что f_g — биекция:
$gx = f_g(x) = f_g(y) = gy \iff x = y$ (можно умножить $gx = gy$ слева на g^{-1}).

• Таким образом, $f_g \in S_G$.

- Определим отображение $f : G \to S_G$ формулой $f(a) := f_a$.
- Проверим, что f — гомоморфизм групп: пусть $a, b \in G$. Тогда

$\forall x \in G$ имеем
$f_{ab}(x) = abx = a(bx) = f_a(f_b(x)) = (f_a f_b)(x)$.

- Следовательно, $\forall a, b \in G$ $f(ab) = f(a)f(b)$ и f — гомоморфизм.
- Пусть $a \in \ker(f)$. Тогда $f_a = f(a) = \mathrm{id}$, то есть, $\forall x \in G$ $ax = f_a(x) = x$, откуда очевидно следует, что $a = e$.
- Таким образом, $\ker(f) = \{e\}$.
- По теореме о гомоморфизме групп (Теореме 5) мы имеем

$G \simeq G/\{e\} = G/\ker(f) \simeq \mathrm{Im}(f) < S_G$. $\square$

Центр группы

Определение

Центр группы G — это множество всех элементов группы, которые коммутируют со всеми элементами G:

$Z(G) := \{a \in G \ : \ \forall x \in G \ ax = xa\}$.

- Если G абелева, то $Z(G) = G$.

Свойство 1

$a \in Z(G) \iff I_a = \mathrm{id}$.

Доказательство. $a \in Z(G) \iff \forall x \in G \ ax = xa \iff \forall x \in G \ x = a^{-1}xa = I_a(x) \iff I_a = \mathrm{id}$. □

Свойство 2

$a \in Z(G) \iff \forall x \in G \quad I_x(a) = a$.

Доказательство. $a \in Z(G) \iff \forall x \in G \ ax = xa \iff \forall x \in G \ I_x(a) = x^{-1}ax = a$. □

Лемма 21

1) *$Z(G) < G$.*

2) *Если $H < Z(G)$, то $H \lhd G$.*

Доказательство. 1) • Пусть $a, b \in Z(G)$, $x \in G$. Тогда $(ab)x = axb = x(ab)$, а значит, $ab \in Z(G)$.

• Пусть $a \in Z(G)$, $x \in G$. Тогда
$a^{-1}x = xa^{-1} \iff a(a^{-1}x)a = a(xa^{-1})a \iff xa = ax$.
Значит, $a^{-1} \in Z(G)$.

• По Лемме 1, $Z(G) < G$.

2) • Пусть $a \in H$, $x \in G$. По Свойству 2 тогда $x^{-1}ax = a \in H$.

• По Лемме 15, $H \lhd G$. □

Теорема 10

Для любой группы G выполнено $G/Z(G) \simeq \mathrm{Inn}(G)$.

Доказательство. • Определим $f : G \to \mathrm{Inn}(G)$ формулой $f(a) := I_{a^{-1}}$.

• Так как для любого $x \in G$

$I_{a^{-1}}(I_{b^{-1}}(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = I_{(ab)^{-1}}(x)$,

мы имеем $f(a)f(b) = f(ab)$, то есть, f — гомоморфизм групп.

• По Свойству 1 центра и так как $Z(G) < G$,

$a \in \mathrm{Ker}(f) \iff I_{a^{-1}} = \mathrm{id} \iff a^{-1} \in Z(G)$

$\iff a \in Z(G)$.

• Таким образом, $\mathrm{Ker}(f) = Z(G)$.

• Очевидно, $\mathrm{Im}(f) = \mathrm{Inn}(G)$.

• По теореме о гомоморфизме (Теореме 5)

$G/Z(G) = G/\ker(f) \simeq \mathrm{Im}(f) = \mathrm{Inn}(G)$. □

Определение

Пусть $p \in \mathbb{P}$. Конечная группа G с $|G| = p^n$, где $n \in \mathbb{N}$ называется p-группой.

Теорема 11

Пусть $p \in \mathbb{P}$, а G — p-группа. Тогда $|Z(G)| \vdots p$.

Доказательство. • Рассмотрим действие $\mathrm{Inn}(G)$ на G.

• По Теореме 10 мы имеем $\mathrm{Inn}(G) \simeq G/Z(G)$, откуда следует, что

$|\mathrm{Inn}(G)| = |G/Z(G)| = (G : Z(G)) = \frac{|G|}{|Z(G)|}$.

• Значит, $|\mathrm{Inn}(G)| = p^k$, где $k \le n$.

• По Свойству 4 орбит G разбивается на орбиты под действием $\mathrm{Inn}(G)$.

• По Теореме 8, $|\mathrm{Inn}(G)| = p^k$ делится на размеры всех этих орбит. Следовательно, размер каждой орбиты либо равен 1, либо делится на p.

• По Свойству 2 центра одноэлементные орбиты под действием $\mathrm{Inn}(G)$ образуют в точности элементы из $Z(G)$.

• Так как $|G| \vdots p$, количество одноэлементных орбит делится на p. Следовательно, $|Z(G)| \vdots p$. $\square$

Лемма 22

Пусть $p \in \mathbb{P}$, а H — абелева группа конечного порядка, $|H| \vdots p$. Тогда H имеет элемент порядка p.

Доказательство. • Индукция по $|H|$.

• База $|H| = p$: по теореме Лагранжа (Теореме 1) в группе H могут быть только элемент порядка 1 (это e) и p. Значит, элемент порядка p есть.

Переход. Пусть для групп меньших порядков лемма доказана.

• Пусть $a \in H$. Рассмотрим два случая.

Случай 1: $\mathrm{ord}(a) \vdots p$.

• Пусть $\mathrm{ord}(a) = np$. Тогда $\mathrm{ord}(a^n) = p$.

Случай 2: $\mathrm{ord}(a) \not\vdots p$.

• Пусть $F = \langle a \rangle$. Тогда $|F| = k$, $(k, p) = 1$.

• Очевидно, $F \lhd H$ (любая подгруппа абелевой группы нормальна).

- Рассмотрим группу H/F. Тогда $|H/F| = (H : F) = \frac{|H|}{k} \vdots p$.
- По индукционному предположению существует элемент $\overline{b} \in H/F$ с $\mathrm{ord}(\overline{b}) = p$.
- Рассмотрим $b \in H$. Мы знаем, что $b^p \in F$ и $b^s \notin F$ при $s < p$.
- Пусть $\mathrm{ord}(b) = m = qp + r$, где $0 \le r < p$.
- Тогда $F \ni e = b^{qp+r} = (b^p)^q \cdot b^r$, откуда следует, что $b^r \in F$, а значит, $r = 0$ и $m \vdots p$.
- Итак, $\mathrm{ord}(b) \vdots p$ и по Случаю 1 в H есть элемент порядка p. $\square$

Первая теорема Силова

Определение

Пусть G — конечная группа, $H < G$, $p \in \mathbb{P}$, $p^k \parallel |G|$. Тогда H — силовская p-подгруппа G, если $|H| = p^k$.

Теорема 12

Пусть G — конечная группа, $p \in \mathbb{P}$, $p^k \parallel |G|$. Тогда G имеет подгруппу порядка p^k.

Доказательство. • Индукция по $|G|$. База для $|G| \not\vdots\, p$ очевидна.

Переход. Пусть для групп меньших порядков теорема доказана, а $|G| = np^k$, где $k \ge 1$ и $n \not\vdots\, p$.

• Рассмотрим два случая.

Случай 1: $|Z(G)| \vdots\, p$.

• По Лемме 22, существует $a \in Z(G)$ с $\mathrm{ord}(a) = p$.

• Тогда $|\langle a\rangle| = p$ по Следствию 1.

• По Лемме 21, $\langle a\rangle \lhd G$. Рассмотрим $G' := G/\langle a\rangle$, тогда $|G'| = (G : \langle a\rangle) = np^{k-1}$ и по индукционному предположению существует подгруппа $H' < G'$ с $|H'| = p^{k-1}$.

• Пусть $H = \{x \in G \ : \ \overline{x} \in H'\}$. По Лемме 20, $H < G$ и $|H| = |H'||\langle a\rangle| = p^k$, что нам и нужно.

Случай 2: $|Z(G)| \not\vdots\, p$.

• Тогда рассмотрим действие G на G сопряжениями: для любых $g \in G$ и $x \in G$ положим $(g, x) \to gxg^{-1} = I_{g^{-1}}(x)$.

• Нетрудно проверить, что это действие. Множество G разбивается этим действием на орбиты.

• Очевидно, орбиты каждого элемент $x \in Z(G)$ одноэлементная. Объединение всех таких орбит равно $Z(G)$ и имеет некратное p число элементов.

• Так как $|G| \vdots\, p$, существует такой элемент $a \in G \setminus Z(G)$, что $|\langle a \rangle| \not\vdots\, p$ (здесь $\langle a \rangle$ — орбита элемента a).
• Вспомним, что $\mathrm{St}(a) < G$ и по Теореме 8 мы знаем, что $|\mathrm{St}(a)| \cdot |\langle a \rangle| = |G|$.
• Тогда $p^k \parallel |\mathrm{St}(a)|$. Из $a \notin Z(G)$ следует, что $|\langle a \rangle| > 1$, а значит, $|\mathrm{St}(a)| < |G|$.
• По индукционному предположению, существует такая $H < \mathrm{St}(a)$, что $|H| = p^k$. Тогда $H < G$ и теорема доказана. $\square$

Следствие 3

(Теорема Коши.) *Пусть G — конечная группа, $p \in \mathbb{P}$, $|G| \vdots p$. Тогда существует такой $a \in G$, что $\mathrm{ord}(a) = p$.*

Доказательство. • Пусть $p^k \parallel |G|$. По Теореме 12, существует $H < G$, $|H| = p^k$. По Теореме 11 мы имеем $|Z(H)| \vdots p$.

• Так как $Z(H)$ — абелева группа, по Лемме 22 существует $a \in Z(H)$, $\mathrm{ord}(a) = p$. $\square$

Вторая теорема Силова

Теорема 13

Пусть G — конечная группа, $p \in \mathbb{P}$, $|G| \vdots p$. Тогда выполнены следующие утверждения.

1) *Если $P < G$ — силовская p-подгруппа, то все силовские p-подгруппы G — это в точности все подгруппы вида $I_a(P)$, где $a \in G$.*

2) *Любая p-подгруппа группы G является подгруппой одной из силовских p-подгрупп.*

Доказательство. • По Следствию 2, все множества вида $I_a(P)$ — подгруппы G.

• Так как I_a — биекция, все они имеют $|P|$ элементов, то есть, являются силовсими p-подгруппами.

• Пусть $H < G$ — p-подгруппа (не обязательно силовская). Достаточно доказать, что $\exists a \in G$, для которого $H < I_a(P)$ (если H — силовская, то мы получим как раз $H = I_a(P)$).

• H действует левыми сдвигами на множестве левых смежных классов $M = \{aP \ : \ a \in G\}$ (это не обязательно фактор-группа!):

$$\text{для } x \in H,\ aP \in M \text{ положим } x \cdot aP := (xa)P$$

(условия из определения действия проверяются очевидно).

• Множество M разбивается на орбиты, размеры которых по Теореме 8 делят $|H| = p^s$, а значит, длина каждой орбиты либо делится на p, либо равна 1.

• Так как $|M| = \frac{|G|}{|P|} \not\vdots\ p$, есть одноэлементная орбита $\{aP\}$.

• Таким образом, $\forall x \in H\ xaP = aP \Rightarrow x \cdot aPa^{-1} = aPa^{-1}$.

• Так как $aPa^{-1} < G$, это означает, что $x \in aPa^{-1}$.

• Таким образом, $H \subset aPa^{-1} \Rightarrow H < aPa^{-1}$, что мы и доказывали. $\square$