

Глава 6. Теория групп

Группа, подгруппа. Простейшие свойства.

Определение

Пусть G – множество, и определена $\cdot : G \times G \rightarrow G$, удовлетворяющая следующим условиям.

1. Ассоциативность $\forall a, b, c \in G (ab)c = a(bc)$.
 2. Нейтральный элемент. $\exists e \in G$ такой, что $\forall a \in G ae = ea = a$.
 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 $\forall a, b \in G ab = ba$.
- 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 $e_1 = e_1e_2 = e_2$

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 $a_1a = aa_2 = e$, откуда:

$$a_1 = a_1(aa_2) = (a_1a)a_2 = a_2.$$

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 единственный.

Свойство 4

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

Доказательство

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

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:
 $\cdot : H \times H \rightarrow H$ – ассоциативная операция, и для любого элемента существует обратный.
- Пусть $a \in H$. Тогда $a^{-1} \in H \implies e = aa^{-1} \in H$.
- Значит, H – группа с операцией \cdot , то есть, $H < G$.

Лемма 2

Пусть $\{H_i\}_{i \in I}$ – множество подгрупп группы G . Тогда $H = \bigcap_{i \in I} H_i$ – 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.

Подгруппа, порожденная множеством элементов

Определение

Пусть G – группа, $M \subset G$. Тогда

$$\langle M \rangle := t_1 \cdots t_n : \forall i \in \{1, \dots, n\}, t_i \in M \text{ или } t_i^{-1} \in M.$$

(n не фиксировано, может быть любым натуральным числом)

– подгруппа, порожденная M .

Лемма 3

Пусть G – группа, $M \subset G$. Тогда $\langle M \rangle < G$.

Доказательство

- Поскольку группа G замкнута по умножению и взятию обратных элементов, $\langle M \rangle \subset G$. Из $t_i^{-1} \in M \subset G$ следует $t_i = (t_i^{-1})^{-1} \in G$. Из $t_1, \dots, t_n \in G$ следует $t = t_1 \cdots t_n \in G$.)
- Пусть $t, s \in \langle M \rangle$. Тогда $t = t_1 \cdots t_n$ (где $t_i \in M$ или $t_i^{-1} \in M$ для всех i) и $s = s_1 \cdots s_m$ (где $s_i \in M$ или $s_i^{-1} \in M$ для всех i).
- Тогда $ts = t_1 \cdots t_n s_1 \cdots s_m \in \langle M \rangle$.
- $t^{-1} = t_n^{-1} \cdots t_1^{-1} \in \langle M \rangle$, так как для любого i либо $t_i^{-1} \in M$, либо $(t_i^{-1})^{-1} = t_i \in M$.
- По [Лемме 1](#), $\langle M \rangle < G$.

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

- Пусть G – группа, $a \in G$. **Порядок элемента a** (обозначение: $\text{ord}(a)$) – это наименьшее такое $k \in \mathbb{N}$, что $a^k = e$. Если такого k нет, то $\text{ord}(a) = \infty$.
- Порядок группы G** – это количество её элементов (то есть, $|G|$).
 - Если $\text{ord}(a) = 1$, 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:

$$a^k a^n = a^{-1} \dots a^{-1} \text{ (в количестве } |k| \text{)} \cdot a \dots a \text{ (в количестве } n \text{)}.$$

- При $|k| > n$ после сокращения получится:

$$(a^{-1})^{|k|-n} = a^{k+n}.$$

- При $|k| \leq n$ после сокращения получится:

$$a^{n-|k|} = a^{k+n}.$$

- Случай $k > 0, n < 0$ аналогичен.

Лемма 4

- Пусть $G = \langle a \rangle$ – циклическая группа.

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

Доказательство

- В любом случае, по определению $G = \{a^s : s \in \mathbb{Z}\}$.
- Докажем, что $\forall n \in \mathbb{N}$ 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 $0 \leq r \leq k - 1$. 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.
- Если $i, j \in \mathbb{Z}$, $i > j$ и $a^i = a^j$, то аналогично $a^{i-j} = e$, а значит, $\text{ord}(a) = \infty$, противоречие.

Следствие 1

- Для любого $a \in G$ выполнено $\text{ord}(a) = |\langle a \rangle|$.
- 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 $n \nmid d$.
 - 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 $\varphi : H \rightarrow aH$, заданная формулой $\varphi(h) := ah$. Значит, $|H| = |aH|$. Аналогично, $|H| = |Ha|$.

Свойство 2

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

Доказательство.

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

Свойство 3 смежных классов

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

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 смежные

- Если $aH \cap bH \neq \emptyset$, 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.

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 $|G| \vdash \text{ord}(a)$.

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 $G = \bigcup_{i=1}^k a_i H$, где $a_i \in G$, причем $a_i H \cap a_j H = \emptyset$ 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, $|G| \vdash |\langle a \rangle| = \text{ord}(a)$ (последнее равенство – по [Следствию 1](#)).

Симметрическая группа. Разложение подстановки на независимые циклы и определение ее порядка

Симметрическая группа

Определение

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

- Подстановка — это биекция $\sigma : I_n \rightarrow I_n$. 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).
- 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 $\text{id}(i) = i$ для всех $i \in I_n$).
 - Так как $\sigma \in S_n$ — биекция, существует обратная биекция $\sigma^{-1} : I_n \rightarrow I_n$.
 - 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, $n! = |S_n| \vdash \text{ord}(\sigma)$.
- Значит, существует такое $k \in \mathbb{N}$, что $\sigma^k = \text{id} \Leftrightarrow \forall i \in I_n \sigma^k(i) = i$.
- 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 её 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:

- $\sigma^2 = (17)(68)(234)(5)(9)$,
- $\sigma^3 = (1876)(2)(3)(4)(59)$,
- $\sigma^{-1} = (1876)(234)(59)$.

Лемма 6

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

Доказательство

- $\sigma^\ell = \text{id}$, если и только если каждый элемент I_n остаётся на своём месте.
- Это означает, что каждый цикл длины m_i должен прокрутиться кратное m_i число раз, то есть, $\forall j \in \{1, \dots, k\} \ \ell \dot{:} m_j$.
- $\text{ord}(\sigma)$ по определению — наименьшее такое число ℓ , а это, очевидно, $[m_1, \dots, m_k]$.

Транспозиции.

Определение

1. Подстановка $\sigma \in S_n$ называется **циклом длины k** , если в её 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 $k \rightarrow k + 1$:
 - 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 $1 \leq i \leq k$.
 - 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 τ_1, \dots, τ_ℓ – транспозиции.
 - Тогда $\sigma = \sigma\tau^2 = \sigma'\tau = \tau_1 \dots \tau_\ell\tau$.

Лемма 7

Пусть $\sigma_m \in S_n$ – цикл длины $m \geq 2$: $\sigma_m = (a_1 a_2 \dots a_m)$. 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 $k \rightarrow k + 1$:
 - 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 $1 \leq i \leq k - 1$, $\sigma_k(a_k) = a_1$.
 - 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 $1 \leq i \leq k$ и $\sigma'(a_{k+1}) = a_1$.
 - Значит, $\sigma' = \sigma_{k+1}$.

Четные и нечетные подстановки. Транспозиция меняет четность.

Четные и нечетные подстановки

Определение

Пусть $\sigma \in S_n$.

- Инверсия — это такая пара чисел (i, j) , что $1 \leq i < j \leq n$ и $\sigma(i) > \sigma(j)$.
- Через $I(\sigma)$ обозначается количество инверсий в подстановке σ .
- Подстановка σ называется чётной, если $I(\sigma) \equiv 0 \pmod{2}$, и нечётной, если $I(\sigma) \equiv 1 \pmod{2}$.

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, 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' . Аналогично для пары (ℓ, j) .
 - Если $\ell > j$, то пара (ℓ, j) — инверсия в $\sigma \iff (\ell, i)$ — инверсия в σ' . Аналогично для пары (ℓ, i) .
 - Если $i < \ell < j$, то в каждой из пар (ℓ, i) и (ℓ, j) есть инверсия ровно в одной из подстановок σ и σ' .
- Количество посчитанных выше инверсий в σ и σ' имеют 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.

Свойства четных и нечетных подстановок.

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 — чётная подстановка.
- Так как σ получена домножением id на транспозицию k раз, чётность подстановки меняется в точности k раз по Лемме 8.

□

Свойство 2 четности

Произведение подстановок одной чётности чётно, а произведение подстановок разных чётностей нечётно.

Доказательство

- Пусть $\sigma, \sigma' \in S_n$, причём 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 – чётная подстановка, если и только если k нечётно.

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 – чётная, если и только если среди чисел m_1, \dots, m_k – чётное количество чётных.

Доказательство

- Следует из Свойств 2 и 3.

Свойство 5 четности

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

Группа A_n .

- 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 чётных и нечётных подстановок в S_n поровну.

- Определим отображение $f : S_n \rightarrow S_n$ 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 чётности.
- Пусть $A_n = \{\sigma_1, \dots, \sigma_k\}$ и $f(\sigma) = \sigma'$. Тогда все подстановки $\sigma'_1, \dots, \sigma'_k$ – различные и нечётны.
- Если $\sigma' \in S_n$ – нечётная подстановка, то $f(\sigma')$ – чётная 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 $|A_n| = \frac{n!}{2}$.

Гомоморфизм групп, ядро и образ. Свойства

Гомоморфизм групп

Определение

- Пусть G, H – группы. Отображение $f : G \rightarrow H$ называется **гомоморфизмом**, если $\forall a, b \in G$ $f(ab) = f(a)f(b)$.
- Ядро гомоморфизма f – это $\text{Ker}(f) = \{x \in G : f(x) = e_H\}$.
- Образ гомоморфизма f – это $\text{Im}(f) = \{y \in H : \exists x \in G : f(x) = y\}$.

Свойство 1

- Если $f : G \rightarrow H$ – 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 на $(f(e_G))^{-1}$, получаем $f(e_G) = e_H$.

Свойство 2

- Если $f : G \rightarrow H$ – 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, $f : G \rightarrow H$ – гомоморфизм групп. Тогда:
 1. $\text{Ker}(f) < G$;
 2. $\text{Im}(f) < H$.

Доказательство

Достаточно проверить условия из [Леммы 1](#).

1.

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

2.

- Пусть $y, y' \in \text{Im}(f)$, а $x, x' \in G$ таковы, что $f(x) = y$ и $f(x') = y'$.
- Тогда $yy' = f(x)f(x') = f(xx') \in \text{Im}(f)$.
- $y^{-1} = (f(x))^{-1} = f(x^{-1}) \in \text{Im}(f)$.

Следствие 2

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

Доказательство

- Очевидно, f индуцирует гомоморфизм $f|_N : N \rightarrow H$.
- По [Лемме 9](#) мы имеем $f(N) = \text{Im}(f|_N) < H$.

Типы гомоморфизмов. Свойства.

Типы гомоморфизмов

Определение

- Пусть G, H – группы, $f : G \rightarrow H$ – гомоморфизм групп.
- Если f – инъекция, то f – **мономорфизм**.
- Если f – сюръекция (то есть, $\text{Im}(f) = H$), то f – **эпиморфизм**.
- Если f – биекция, то f – **изоморфизм**.
- Изоморфизм = мономорфизм + эпиморфизм.

Лемма 10

- Пусть $f : G \rightarrow H$ – гомоморфизм групп. Тогда f – мономорфизм, если и только если $\text{Ker}(f) = \{e_G\}$.

Доказательство

- (\Rightarrow)
 - Если f – мономорфизм, то f – инъекция.
 - Пусть $a \in \text{Ker}(f)$. 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, $a \cdot b^{-1} \in \text{Ker}(f) = \{e_G\}$, откуда $a \cdot b^{-1} = e_G$ и $a = b$.
 - Таким образом, f – инъекция, а значит, мономорфизм.

Лемма 11

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

Доказательство обратимости

- 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.

Отображение, обратное к изоморфизму. Изоморфные группы.

Определение

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

Теорема 4

\simeq — отношение эквивалентности на множестве всех групп.

Доказательство

- **Рефлексивность** очевидна: тождественное отображение $\text{id} : G \rightarrow G$ (заданное формулой $\text{id}(x) = x$ для всех $x \in G$), очевидно, является изоморфизмом.
- **Симметричность** доказана в [Лемме 11](#).
- **Транзитивность:**
 - Пусть F, G, H — группы, $F \simeq G$ и $G \simeq H$.
 - Тогда существуют изоморфизмы $\varphi : F \rightarrow G$ и $\psi : G \rightarrow H$.
 - Докажем, что их композиция $\psi\varphi : F \rightarrow H$ (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:
 - $\psi\varphi(ab) = \psi(\varphi(ab)) = \psi(\varphi(a) \cdot \varphi(b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b)) = (\psi\varphi)(a) \cdot (\psi\varphi)(b)$.

Автоморфизмы и сопряжения группы.

Автоморфизмы группы

Определение

- Пусть G — группа.
- Автоморфизм группы G — это изоморфизм $\varphi : G \rightarrow G$.
- Множество всех автоморфизмов группы G обозначим через $\text{Aut}(G)$.

Лемма 12

- $\text{Aut}(G)$ – группа относительно композиции.

Доказательство

- Ассоциативность композиции нам известна.
- Очевидно, тождественное отображение id подходит в качестве нейтрального элемента.
- Для каждого $\varphi \in \text{Aut}(G)$ по [Лемме 11](#) мы имеем $\varphi^{-1} \in \text{Aut}(G)$.

Сопряжения

Определение

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

Лемма 13

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

Доказательство

- Сначала докажем, что $\text{Inn}(G) \subset \text{Aut}(G)$. Пусть $a \in G$.
- Очевидно, $a^{-1}xa = a^{-1}ya \iff x = y$, поэтому I_a – биекция.
- Так как $I_a(x)I_a(y) = a^{-1}xa a^{-1}ya = I_a(xy)$, I_a – гомоморфизм, а значит, $I_a \in \text{Aut}(G)$.
- По [Лемме 1](#), достаточно проверить замкнутость $\text{Inn}(G)$ 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:
 - $I_a \cdot I_{a^{-1}} = I_{a^{-1}a} = I_e = \text{id}$ и, аналогично, $I_{a^{-1}} \cdot I_a = \text{id}$.

Нормальные подгруппы. Критерий нормальности.

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: $H \triangleleft G$.

Лемма 14

- Пусть G – группа, $H < G$. Тогда $H \triangleleft G$, 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:
 - $H \triangleleft G \iff \forall a \in G I_a(H) = H \iff \forall a \in G aH = Ha$.

Критерий нормальности

Лемма 15

- Пусть G – группа, $H < G$. Тогда $H \triangleleft G$, 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:
 - $H \triangleleft G \iff \forall a \in G I_a(H) = H$.
- 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, $I_a(H) = H$.

Нормальность пересечения нормальных подгрупп. Нормальность ядра гомоморфизма.

Лемма 16

- Пусть G – группа, а $\{H_i\}_{i \in I}$ – нормальные подгруппы G .
- Тогда $H = \bigcap_{i \in I} H_i \triangleleft G$.

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 $H_i \triangleleft G$, мы имеем $I_a(h) \in H_i$.
- Таким образом, $\forall a \in G, \forall h \in H I_a(h) \in H$, откуда $H \triangleleft G$.

Лемма 17

- Пусть G, H – группы, а $f : G \rightarrow H$ – гомоморфизм.
- Тогда $\ker(f) \triangleleft G$.

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. Лемма о подгруппе факторгруппы.

Факторгруппа

Определение

- Пусть G – группа, $H \triangleleft G$. Будем использовать обозначение $\bar{a} := aH$.
- Факторгруппа $G/H = \{\bar{a} : a \in G\}$. Умножение определим так:
 - $\bar{a} \cdot \bar{b} := \overline{ab}$.
- 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, $H \triangleleft G$. Тогда умножение в G/H определено корректно.

Доказательство

- Так как $H \triangleleft G$, для любого $b \in G$ мы имеем $bH = Hb$.
- Поэтому:
 - $\bar{a} \cdot \bar{b} = aH \cdot bH = a \cdot (Hb) \cdot H = a \cdot (bH) \cdot H = ab \cdot (H \cdot H) = abH = \overline{ab}$.

Лемма 19

- Пусть G – группа, $H \triangleleft G$. Тогда G/H – группа.

Доказательство

- **Ассоциативность умножения:**
 - $\forall a, b, c \in G/H \quad \bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot \bar{bc} = \overline{abc} = \overline{ab} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$.
- **Нейтральный элемент** – это \bar{e} .
 - Проверка: $\bar{e} \cdot \bar{a} = \overline{ea} = \bar{a} = \overline{ae} = \bar{a} \cdot \bar{e}$.
- **Обратный элемент:**
 - $(\bar{a})^{-1} := \overline{a^{-1}}$.
 - Проверка: $\bar{a} \cdot \overline{a^{-1}} = \bar{e}$ и $\overline{a^{-1}} \cdot \bar{a} = \bar{e}$.

Лемма 20

- Пусть G – группа, $F \triangleleft G$, $H' < G/F$. Пусть $H = \{x \in G : \bar{x} \in H'\}$. Тогда $H < G$, причем $|H| = |H'| \cdot |F|$.

Доказательство

- Пусть $x, y \in H$. Тогда $\bar{x}, \bar{y} \in H'$, а значит, $\bar{xy} = \bar{x} \cdot \bar{y} \in H'$ (так как H' – группа). Следовательно, $xy \in H$.
- Пусть $x \in H$. Тогда $x \in H'$, а значит, $\overline{x^{-1}} = (\bar{x})^{-1} \in H'$ (так как H' – группа). Следовательно, $x^{-1} \in H$.
- По [Лемме 1](#), $H < G$.
- Каждый $\bar{x} \in H'$ – это смежный класс xF , содержащий ровно $|F|$ элементов, и все они при факторизации переходят в \bar{x} . Поэтому, $|H| =$

$$|H'| \cdot |F|.$$

Теорема о гомоморфизме групп

Теорема 5

- Пусть $f : G \rightarrow H$ – гомоморфизм групп. Тогда $G/\text{Ker}(f) \simeq \text{Im}(f)$.

Доказательство

- Зададим отображение $\bar{f} : G/\text{Ker}(f) \rightarrow \text{Im}(f)$ формулой $\bar{f}(\bar{a}) := f(a)$.
- **Корректность определения \bar{f} :**
 - Пусть $a, b \in G$ таковы, что $\bar{a} = \bar{b}$. По [свойству 3](#) смежных классов, тогда $a^{-1}b \in \text{Ker}(f)$.
 - Следовательно:
 - $\bar{f}(\bar{b}) = f(b) = f(a \cdot a^{-1}b) = f(a)f(a^{-1}b) = f(a) \cdot e_H = \bar{f}(\bar{a})$
- **\bar{f} – гомоморфизм групп:**
 - $\bar{f}(\bar{a} \cdot \bar{b}) = \bar{f}(\bar{ab}) = f(ab) = f(a)f(b) = \bar{f}(\bar{a}) \cdot \bar{f}(\bar{b})$.
- $\text{Im}(\bar{f}) = \text{Im}(f)$: для любого $y \in \text{Im}(f)$ существует такой $x \in G$, что $\bar{f}(\bar{x}) = f(x) = y$.
- **\bar{f} – мономорфизм:**
 - Проверка: пусть $\bar{a} \in \text{Ker}(\bar{f})$. Тогда $f(a) = \bar{f}(\bar{a}) = e_H$, следовательно, $a \in \text{Ker}(f)$, а значит, $\bar{a} = \bar{e}$.
 - Таким образом, $\text{Ker}(\bar{f}) = \{\bar{e}\}$.
- Таким образом, \bar{f} – изоморфизм, а значит, $G/\text{Ker}(f) \simeq \text{Im}(f)$.

Теорема о сокращении.

Теорема 6

- Пусть G – группа, $H, F \triangleleft G$, причем $F < H$. Тогда выполнены следующие утверждения:
 1. $F \triangleleft H$.
 2. $H/F \triangleleft G/F$.
 3. $G/H \simeq (G/F)/(H/F)$.

Доказательство

1. $F \triangleleft G \implies \forall a \in G \quad I_a(F) = F \implies \forall a \in H \quad I_a(F) = F \implies F \triangleleft H$.
2.
 - Из $H \triangleleft G$ следует, что для любых $a \in G$ и $h \in H$ выполнено $a^{-1}ha \in H$.
 - Пусть $\bar{a} := aF$. Тогда для любых $\bar{a} \in G/F$ и $\bar{h} \in H/F$ выполнено $(\bar{a})^{-1} \cdot \bar{h} \cdot \bar{a} = \overline{a^{-1}ha} \in H/F$.
 - Следовательно, $H/F \triangleleft G/F$.
3.
 - Для $a \in G$ положим $\tilde{a} := aH$. По свойству смежных классов, $\bar{a} = \bar{b} \implies a^{-1}b \in F \implies a^{-1}b \in H \implies \tilde{a} = \tilde{b}$.
 - Определим отображение $f : G/F \rightarrow G/H$ формулой $f(\bar{a}) := \tilde{a}$.
 - Так как из $\bar{a} = \bar{b}$ следует, что $\tilde{a} = \tilde{b}$, определение f корректно.
 - **f – гомоморфизм групп:**
 - $f(\bar{a} \cdot \bar{b}) = f(\bar{ab}) = \tilde{ab} = \tilde{a} \cdot \tilde{b} = f(\bar{a})f(\bar{b})$.
 - $\text{Ker}(f) = H/F$. Доказательство:
 - $\bar{a} \in \text{Ker}(f) \iff \tilde{a} = f(\bar{a}) = \tilde{a} \iff a \in H \iff \bar{a} \in H/F$.
 - $\text{Im}(f) = G/H$. Действительно, для любого $\tilde{a} \in G/H$, очевидно, $\bar{a} \in G/F$ и $f(\bar{a}) = \tilde{a}$.
 - По [Теореме 5](#):
 - $G/H = \text{Im}(f) \simeq (G/F)/\text{Ker}(f) = (G/F)/(H/F)$.

Коммутаторы и коммутант. Свойства.

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, $[a, b] \cdot [b, a] = e$.

Обозначение

- 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

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

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

- $[G, G] \triangleleft G$.

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](#), $[G, G] \triangleleft G$.

Теорема об абелевой факторгруппе.

Теорема 7

- Пусть G – группа, $H \triangleleft G$. Тогда G/H абелева, если и только если $[G, G] < H$.

Доказательство

- Пусть $\bar{a} := aH$.
- Группа G/H абелева, если и только если для любых $a, b \in G$ выполнено $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$. Преобразуем это условие:
 - $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} \iff \bar{e} = [\bar{a}, \bar{b}] = \overline{[a, b]} \iff [a, b] \in H$.
- Таким образом, группа G/H абелева, если и только если:
 - $\forall a, b \in G [a, b] \in H \iff [G, G] \subset H \iff [G, G] < H$.

Действие группы на множестве.

Примеры действий.

Действие группы на множестве

Определение

- Пусть G – группа, M – множество. Отображение $\cdot : G \times M \rightarrow M$ называется действием группы G на множестве M , если выполнены следующие условия:
 1. $\forall a, b \in G, \forall x \in M (ab)x = a(bx)$;
 2. $\forall x \in M ex = x$.

Примеры действий

1. S_n действует на $\{1, 2, \dots, n\}$.
2. Если G – группа, то $\text{Aut}(G)$ действует на G (здесь G выступает в качестве множества).
3. Если G – группа, то G (как группа) действует на G (как множество) левыми умножениями:

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

Стабилизатор: определение и свойства.

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

Свойство 1

- Для любого $N \subset M$ выполнено $St(N) < G$.

Доказательство

- Достаточно проверить условия из [Леммы 1](#).
- Пусть $a, b \in St(N)$. Тогда $(ab)N = a(bN) = aN = N$, то есть $ab \in St(N)$.
- Пусть $a \in St(N)$. Тогда $a^{-1}N = a^{-1}(aN) = (a^{-1}a)N = eN = N$, то есть $a^{-1} \in St(N)$.

Свойство 2 центра

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

Доказательство

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

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

Орбита: определение и свойства. Связь мощностей орбиты и стабилизатора элемента.

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

Свойство 3

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

Доказательство

- $ex = x \implies x \in \langle x \rangle$.

Свойство 4 орбит

- Пусть $x, y \in M$, $\langle x \rangle \cap \langle y \rangle \neq \emptyset$. 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 $|\langle x \rangle| \cdot |St(x)| = |G|$.

Доказательство

- Для $a, b \in G$:
 - $ax = bx \iff (b^{-1}a)x = b^{-1}(ax) = b^{-1}(bx) = x \iff b^{-1}a \in St(x) \iff b \cdot St(x) = a \cdot St(x)$.
 - (в последнем равенстве мы воспользовались [Свойством 3 смежных классов](#)).
- Таким образом, элементы G , одинаково действующие на x , образуют смежный класс по подгруппе $St(x)$.
- Следовательно, $|\langle x \rangle| = (G : St(x))$ (количество смежных классов по подгруппе $St(x)$).
- Теперь Теорема 8 следует из [Теоремы 1](#) (теоремы Лагранжа).

Теорема Кэли.

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 $f_g : G \rightarrow G$ 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 $f : G \rightarrow S_G$ 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 $f_a = f(a) = \text{id}$, 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

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

Центр группы. Свойства.

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

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

Доказательство

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

Свойство 2

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

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 $H \triangleleft G$.

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](#), $H \triangleleft G$.

Связь центра с группой сопряжений.

Теорема 10

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

Доказательство

- Определим $f : G \rightarrow \text{Inn}(G)$ 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 $Z(G) < G$:
 $a \in \ker(f) \iff I_{a^{-1}} = \text{id} \iff a^{-1} \in Z(G) \iff a \in Z(G)$.
- Таким образом, $\ker(f) = Z(G)$.
- Очевидно, $\text{Im}(f) = \text{Inn}(G)$.
- По теореме о гомоморфизме ([Теореме 5](#)):
 $G/Z(G) = G/\ker(f) \simeq \text{Im}(f) = \text{Inn}(G)$.

Центр p -группы.

Определение

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

Теорема 11

- Пусть $p \in P$, а G – p -группа. Тогда $|Z(G)| \nmid p$.

Доказательство

- Рассмотрим действие $\text{Inn}(G)$ на G .

- По [Теореме 10](#) мы имеем $\text{Inn}(G) \cong G/Z(G)$, откуда следует, что

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

- Значит, $|\text{Inn}(G)| = p^k$, где $k \leq n$.
- По [Свойству 4](#) орбиты множества G разбиваются на орбиты под действием $\text{Inn}(G)$.
- По [Теореме 8](#), $|\text{Inn}(G)| = p^k$ 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 $\text{Inn}(G)$ образуют в точности элементы из $Z(G)$.
- Так как $|G| \vdash p$, количество одноэлементных орбит делится на p . Следовательно, $|Z(G)| \vdash p$.

Элемент порядка p в абелевой группе.

Лемма 22

- Пусть $p \in P$, а H – абелева группа конечного порядка, $|H| \vdash p$. Тогда H имеет элемент порядка p .

Доказательство

- Индукция по $|H|$.

База

- $|H| = p$: по теореме [Лагранжа \(Теореме 1\)](#) в группе H могут быть только элементы 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: $\text{ord}(a) \mid p$

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

Случай 2: $\text{ord}(a) \nmid p$

- Пусть $F = \langle a \rangle$. Тогда $|F| = k$, $(k, p) = 1$.
- Очевидно, $F \triangleleft H$ (любая подгруппа абелевой группы нормальна).
- Рассмотрим группу H/F . Тогда

$$|H/F| = (H : F) = \frac{|H|}{k} \mid p.$$

- По индукционному предположению существует элемент $\bar{b} \in H/F$ с $\text{ord}(\bar{b}) = p$.
- Рассмотрим $b \in H$. Мы знаем, что $b^p \in F$ и $b^s \notin F$ при $s < p$.
- Пусть $\text{ord}(b) = m = qp + r$, где $0 \leq r < p$.
- 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 $m \mid p$.
- Итак, $\text{ord}(b) \mid p$ и по Случаю 1 в H есть элемент порядка p .

Первая теорема Силова и теорема Коши об элементе порядка p .

Первая теорема Силова

Определение

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

Теорема 12

- Пусть G – конечная группа, $p \in P$, $p^k \mid |G|$. Тогда G имеет подгруппу порядка p^k .

Доказательство

- Индукция по $|G|$.

База

- Для $|G| \nmid p$ очевидна.

Переход

- Пусть для групп меньших порядков теорема доказана, а $|G| = np^k$, где $k \geq 1$ и $n \nmid p$.

Случай 1: $|Z(G)| \nmid p$

- По [Лемме 22](#), существует $a \in Z(G)$ с $\text{ord}(a) = p$.
- Тогда $|\langle a \rangle| = p$ по Следствию 1.
- По [Лемме 21](#), $\langle a \rangle \triangleleft G$. 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 $H = \{x \in G : x \in H'\}$. По Лемме 20, $H < G$ и

$$|H| = |H'||\langle a \rangle| = p^k,$$

что нам и нужно.

Случай 2: $|Z(G)| \mid p$

- Тогда рассмотрим действие G на G сопряжениями: для любых $g \in G$ и $x \in G$ положим

$$(g, x) \rightarrow gxg^{-1} = I_{g^{-1}}(x).$$

- Нетрудно проверить, что это действие. Множество G разбивается этим действием на орбиты.
- Очевидно, орбиты каждого элемента $x \in Z(G)$ одноэлементные. Объединение всех таких орбит равно $Z(G)$ и имеет некратное p число элементов.
- Так как $|G| \nmid p$, существует такой элемент $a \in G \setminus Z(G)$, что $|\langle a \rangle| \nmid p$ (здесь $\langle a \rangle$ – орбита элемента a).
- Вспомним, что $\text{St}(a) < G$ и по Теореме 8 мы знаем, что

$$|\text{St}(a)| \cdot |\langle a \rangle| = |G|.$$

- Тогда $p^k \parallel |\text{St}(a)|$. Из $a \notin Z(G)$ следует, что $|\langle a \rangle| > 1$, а значит, $|\text{St}(a)| < |G|$.
- По индукционному предположению, существует такая $H < \text{St}(a)$, что $|H| = p^k$. Тогда $H < G$ и теорема доказана.

Следствие 3

- (Теорема Коши.) Пусть G – конечная группа, $p \in P$, $|G| \nmid p$. Тогда существует такой $a \in G$, что $\text{ord}(a) = p$.

Доказательство

- Пусть $p^k \parallel |G|$. По Теореме 12, существует $H < G$, $|H| = p^k$. По Теореме 11 мы имеем $|Z(H)| \nmid p$.
- Так как $Z(H)$ – абелева группа, по [Лемме 22](#) существует $a \in Z(H)$, $\text{ord}(a) = p$.

Вторая теорема Силова

Вторая теорема Силова

Теорема 13

- Пусть G – конечная группа, $p \in P$, $|G| \dot{:} p$. 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 силовскими 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!):
 - Для $x \in H$, $aP \in M$ 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 $|M| = \frac{|G|}{|P|} \dot{:} p$, есть одноэлементная орбита $\{aP\}$.
 - Таким образом, $\forall x \in H \quad xaP = aP \implies x \cdot aPa^{-1} = aPa^{-1}$.
 - Так как $aPa^{-1} < G$, это означает, что $x \in aPa^{-1}$.
 - Таким образом, $H \subset aPa^{-1} \implies H < aPa^{-1}$, что мы и доказывали.