# Алгебра. Глава 6. Теория групп

Д. В. Карпов

2022-2023

## 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 $e_1 = e_1 e_2 = e_2$. □

## 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 $a_1 = a_1(a a_2) = (a_1 a) a_2 = a_2$. □

## Свойство 3

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

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

## 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, $\cdot : H \times H \to H$ — 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 $\langle M \rangle < G$.*

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 $t = t_1 \dots t_n \in G$.

• 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, $\langle M \rangle < G$.

# 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 $\operatorname{ord}(a) = 1$, 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 $|k| \leq n$ после сокращения получится $a^{n-|k|} = a^{k+n}$.

• Случай $k > 0$, $n < 0$ аналогичен. □

## 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 $(a^k)^n = (a^k)^{-|n|} = \left((a^k)^{-1}\right)^{|n|} = (a^{-1})^{k|n|} = a^{kn}$.

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

## Лемма 4

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

1) *Если $\mathrm{ord}(a) = k \in \mathbb{N}$, то $G = \{a^0 = e, a, \ldots, a^{k-1}\}$ 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 $\forall n \in \mathbb{N}$ мы имеем $a^n \in \{e = a^0, a, a^2, \ldots, a^{k-1}\}$.

• 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 $i, j \in \{1, \ldots, k-1\}$. 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, $\mathrm{ord}(a) \neq \infty$, противоречие. □

## 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 $d$. □

# 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, $|H| = |Ha|$. □

## 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

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

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* $|G| \vdots \operatorname{ord}(a)$.

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 $i \in \{1, \ldots, k\}$, следовательно, $|G| = k|H| = (G : H)|H|$.

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

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

# Симметрическая группа

## Определение

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

1) Подстановка — это биекция $\sigma : I_n \to I_n$. Как правило, мы будем записывать $\sigma$ как строчку из $n$ чисел: $\sigma(1), \sigma(2), \ldots \sigma(n)$ (на $k$ позиции записывается то число, в которое $\sigma$ 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 $\mathrm{id}$ (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 $1, \ldots, k$ и оставляющей на месте $k+1, \ldots, n$).

# Разложение подстановки на независимые циклы

- Пусть $\sigma \in S_n$. По теореме Лагранжа, $n! = |S_n| \vdots \operatorname{ord}(\sigma)$.
- 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, $\sigma$ разбивается на независимые циклы вида $i, \sigma(i), \ldots \sigma^{k_i-1}(i)$. (каждый элемент под воздействием $\sigma$ 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 $\sigma^\ell$ прокручивает каждый цикл $\sigma$ ровно $\ell$ раз (нужно передвинуться на $\ell$ ходов по циклу). При этом, цикл может распадаться на несколько меньших.

• Подстановка $\sigma^{-1}$ прокручивает каждый цикл $\sigma$ в обратном порядке.

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

## Лемма 6

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

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, $\forall j \in \{1, \ldots, k\}\ \ell \vdots m_j$.

• $\operatorname{ord}(\sigma)$ по определению — наименьшее такое число $\ell$, а это, очевидно, $[m_1, \ldots, m_k]$.

## 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 $k+1, \ldots, n$). 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 $\sigma$ 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 $\tau$, и $\sigma$ оставляют на местах $\{k+2, \ldots, n\}$, $\sigma'$ тоже эти числа оставляет на местах.

• Значит, $\sigma' \in S'_k$ и по индукционному предположению $\sigma' = \tau_1 \ldots \tau_\ell$, где $\tau_1, \ldots, \tau_\ell$ — транспозиции.

• Тогда $\sigma = \sigma\tau^2 = \sigma'\tau = \tau_1 \ldots \tau_\ell\tau$. □

## Лемма 7

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

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

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

• Цикл $\sigma_k = (a_1 a_2 \ldots a_k)$ 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



## 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 $\sigma$.
- Подстановка $\sigma$ называется чётной, если $I(\sigma) \vdots 2$ и нечетной, если $I(\sigma) \not\vdots 2$

## Лемма 8

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

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

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

• Пусть $\ell \notin \{i, j\}$.

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

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

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

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

## 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 $\mathrm{id}$ — четная подстановка.

• Так как $\sigma$ получена домножением $\mathrm{id}$ 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 $\sigma$ представляется как произведение $k$ транспозиций, а $\sigma'$ — 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 $m_1, \ldots, m_k$ (не обязательно различные). Тогда $\sigma$ — четная, если и только если среди чисел $m_1, \ldots, m_k$ — 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 $\sigma = \tau_1 \tau_2 \ldots \tau_k$.

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

• 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 $\sigma$ и $f(\sigma)$ всегда разной четности.

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

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

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

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

# 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 $\psi$ и $\varphi$, очевидно, является биекцией.

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

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

□