

# Теория групп. Лекция 1

Штепин Вадим Владимирович

5 сентября 2019 г.

Опр. **Группа** — множество  $G$  с определённой на нём операцией  $*$ , удовлетворяющей условиям:

1. Ассоциативность:  $(a * b) * c = a * (b * c)$
2. Существование нейтрального элемента:  $\exists e \in G \forall a \in G \ a * e = e * a = a$
3. Существование обратного элемента:  $\forall a \in G \ \exists a^{-1} \in G \ a * a^{-1} = a^{-1} * a = e$

Опр. Если выполнено свойство коммутативности ( $\forall a, b \in G \ a * b = b * a$ ), то группа называется **абелевой**

Опр. **Подгруппа** — непустое подмножество  $H \subset G$ , являющееся группой.

**Теорема (критерий подгруппы).** Доказывалась на 1 курсе.

Непустое подмножество  $H \subset G$  это подгруппа в  $G$ , если верны следующие условия:

1.  $H$  замкнуто относительно групповой операции:  $\forall a, b \in H \ a * b \in H$
2.  $H$  замкнуто относительно взятия обратного элемента:  $\forall a \in H \ a^{-1} \in H$

**Примеры групп:**

1.  $(Z, +), (Z_n, +)$
2. Если  $F$  — поле, то  $(F, +)$  — аддитивная группа поля,  $(F^*, *)$  — мультипликативная группа поля
3. Если  $V$  — лин. пр-во, то  $(V, +)$  — абелева группа
4.  $GL_n(F)$  — полная линейная группа над полем  $F$ , т.е. группа невырожденных матриц относительно умножения
5.  $S_n$  — симметрическая группа степени  $n$ , т.е. группа биекций множества  $\{1, 2, \dots, n\}$  на себя относительно композиции.

Опр. **Порядок группы** — число элементов в группе

Опр. **Порядок элемента группы**  $g$  — наименьшее ненулевое число  $n$ , в что  $g^n = e$

**Примеры подгрупп (знаком  $\leq$  обозначают отношение "быть подгруппой"):**

1.  $nZ \leq Z$  — группа кратных  $n$  чисел
2. Если  $W, V$  — лин. пространства и  $W \leq V$  (подпространство), то верно что  $W$  — подгруппа  $V$
3.  $SL_n(F) \leq GL_n(F), A \in SL_n(F) \leftrightarrow \det(A) = 1$
4.  $O_n \leq GL_n(\mathbb{R})$  — группа ортогональных матриц,  $U_n \leq GL_n(\mathbb{C})$  — группа унитарных матриц
5.  $A_n \leq S_n$  — четные подстановки

## 1 Группа, порожденная подмножеством

Опр. Пусть  $G$  — группа относительно умножения и  $M \subset G$ . Тогда  $\langle M \rangle = \bigcap_{H \leq G, M \subset H} H$  — подгруппа, **порожденная**  $M$

Опр. Подгруппа, **порожденная**  $M$  — наименьшая по включению подгруппа  $G$ , содержащая  $M$

$$\text{Утв. } \langle M \rangle = \{m_1^{\epsilon_1} * m_2^{\epsilon_2} * \dots * m_s^{\epsilon_s} \mid m_i \in M, \epsilon_i \in \{0, 1, -1\}\}$$

## 2 Циклическая группа

Опр. Пусть  $\exists a \in G, G = \langle a \rangle$ , тогда  $G$  — **циклическая группа** с порождающим элементом  $a$ .

**Теорема (об элементе конечного порядка)** Пусть  $a \in G, \text{ord}(a) < \infty, \text{ord}(a) = n$ . Тогда  $\langle a \rangle$  — конечная группа порядка  $n$  и  $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$

**Теорема (об изоморфизме циклических групп)** Все циклические группы одного порядка (в том числе и бесконечные) изоморфны между собой

### Следствие

1. Если  $|G| = n < \infty$  и  $G$  — циклическая, то  $G \simeq Z_n$
2. Если  $|G| = \infty$  и  $G$  — циклическая, то  $G \simeq Z$

**Теорема** Всякая подгруппа циклической группы сама циклическая

**Теорема** Пусть  $G$  — циклическая группа, порожденная  $a$  и  $\text{Div}(G)$  — множество делителей  $n = \text{ord}(a)$ , тогда  $\forall d \in \text{Div}(G) \exists H_d \leq G, H_d = \{e, a^d, a^{2d}, \dots, a^{(\frac{n}{d}-1)d}\}$  и

1.  $H_d$  — циклическая подгруппа порядка  $\frac{n}{d}$
2. Если  $d_1, d_2 \in \text{Div}(G), d_1 \neq d_2$ , то  $H_{d_1} \neq H_{d_2}$
3. Всякая подгруппа группы  $G$  имеет вид  $H_d$  для некоторого  $d$

### 3 Произведение подмножеств в группе

Опр. Если  $A, B \subset G$ , то  $AB = \{ab \mid a \in A, b \in B\}$ . Если  $A = a$ ,  $B = H \leq G$ , то  $AB = aH = \{ah \mid h \in H\}$  — левый смежный класс  $a$  по подгруппе  $H$ .  $Ha = \{ha \mid h \in H\}$  — правый смежный класс. Причем верно  $\forall A, B, C \subset G (AB)C = A(BC)$

**Теорема (критерий подгруппы, переформулировка)** Пусть  $H \subset G$  и  $H \neq \emptyset$ . Тогда  $H \leq G \Leftrightarrow$

1.  $HH = H$
2.  $H^{-1} = H$ , где  $H^{-1} = \{a^{-1} \mid a \in H\}$

**Свойства левых смежных классов:**

1. Всякий левый смежный класс порождается любым своим элементом  $y \in xH, H \leq G \Rightarrow yH = xH$

**Доказательство:**  $y \in xH, H \leq G \Rightarrow \exists h \in H : y = xh \Rightarrow yH = xhH = xH$ , так как если  $h \in H$ , то  $hH = H$

2. Всякие два левых смежных класса по подгруппе  $H$  либо не пересекаются, либо совпадают

**Доказательство:** Пусть  $xH \cap yH \neq \emptyset \Rightarrow \exists z \in xH \cap yH \Rightarrow zH = xH \quad zH = yH \Rightarrow xH = yH$

3.  $G = \sqcup_{i \in I} x_i H$  — левостороннее разложение группы  $G$  по подгруппе  $H$ , где объединение дизъюнктное, то есть объединяются непересекающиеся множества

**Доказательство** Очевидно, что  $G = \cup_{x \in G} xH$ . Из каждого семейства совпадающих смежных классов оставим ровно по одному представителю. По предыдущему свойству они не пересекаются.

Аналогично доказывается существование правостороннего разложения  $G = \sqcup_{i \in I} Hx$

Наличие этих разложений — следствие того, что отношение "х и у принадлежат одному левому(правому) смежному классу" — это отношение эквивалентности на  $G$ , и верна теорема о классах эквивалентности

**Теорема (критерий принадлежности двух элементов одному левому смежному классу)** Элементы  $x, y \in G$  принадлежат одному левому смежному классу по подгруппе  $H$  тогда, и только тогда, когда верно одно из след. эквивалентных условий:

1.  $x^{-1}y \in H$
2.  $y^{-1}x \in H$
3.  $xH = yH$
4.  $x \in yH$
5.  $y \in xH$
6.  $xH \cap yH \neq \emptyset$

**Доказательство.** Покажем эквивалентность с первым условием:

1. Необходимость  $x, y \in zH \Rightarrow \exists h_1, h_2 \in H \ x = zh_1, \ y = zh_2 \Rightarrow x^{-1}y = h_1^{-1} * z^{-1} * z * h_2 = h_1^{-1} * h_2 \in H$
2. Достаточность  $x^{-1}y \in H \Rightarrow x^{-1}y = h \in H \Rightarrow y = xh \Rightarrow y \in xH \Rightarrow xH = yH$

**Упражнение:** Доказать остальные эквивалентности и придумать аналогичный критерий для правых смежных классов

**Теорема (Лагранж)** Порядок любой подгруппы конечной группы является делителем порядка группы

**Доказательство**  $G = \sqcup_{i \in I} x_i H$  и  $|xH| = |H|$  по свойствам группы. Значит,  $|G| = |I| |H|$ , так как объединение дизъюнктное. Тогда  $|G| : |H|$

Опр.

$G/H$  — множество левых смежных классов в разложении

$|G/H|$  — индекс подгруппы

$H \backslash G$  — множество правых смежных классов в разложении

$$|G/H| = |H \backslash G| = \frac{|G|}{|H|} = |G : H|$$

Следствие Порядок любого элемента конечной группы — делитель порядка группы

Следствие Если  $p$  — простое, то любая группа порядка  $p$  — циклическая

**Доказательство** Если  $p$  — простое, то  $p \geq 2$  и в группе есть элемент, отличный от нейтрального. Обозначим его  $a \in G, \ a \neq e$ . По теореме Лагранжа  $|G| : |\langle a \rangle|$ . Так как  $p$  простое, то  $|\langle a \rangle| = p$  и  $\langle a \rangle = G$

Следствие  $\forall p$  — простое  $\exists!$  с точностью до изоморфизма группа порядка  $p$

**Доказательство**  $|G| = p \Rightarrow G$  изоморфно  $C_p$  — абстрактная циклическая группа порядка  $p$

Следствие (теорема Эйлера) Если  $a \in Z, \ n \in N, \ gcd(a, n) = 1$ , то  $a^{\phi(n)} \equiv 1 \pmod{n}$ , где  $\phi(n)$  — функция Эйлера, т.е. количество простых чисел, меньших  $n$ .

Свойства функции Эйлера:

1.  $\phi(nm) = \phi(n)\phi(m)$ , если  $gcd(n, m) = 1$
2. Если  $n = p_1^{\alpha_1} * \dots * p_s^{\alpha_s}$  — каноническое разложение на простые множители, то  $\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s})$

**Доказательство**  $Z_n^*$  — группа вычетов, взаимно простых с  $n$ . По условию  $a \in Z_n^*$  и  $|Z_n^*| = \phi(n)$ . Значит, если  $ord(a) = k$ , то  $\phi(n) : k$  и  $a^{\phi(n)} \equiv 1 \pmod{n}$

Следствие (Малая теорема Ферма)  $a \in N, p$  — простое, то  $a^p \equiv a \pmod{p}$

**Доказательство** Если  $НОД(a, p) = 1$ , то  $a^{\phi(p)} \equiv 1 \pmod{p}$ , то есть  $a^{p-1} \equiv 1 \pmod{p}$ .

Домножение равенства на  $a$  доказывает следствие. Если  $НОД(a, p) \neq 1$ , то  $a : p$  и  $a^p \equiv a \equiv 0 \pmod{p}$