Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ТЕОРИЯ ГРУПП

III СЕМЕСТР

Лектор: *Вадим Владимирович Штепин*

Автор: *Киселев Николай*
Репозиторий на Github

осень 2025

Содержание

1 Введение

1.1 Определения

Определение 1.1. Группа — это множество G с введенным на нем бинарной операцией $*$, удовлетворяющее следующим свойствам:

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

Замечание. В группе нейтральный элемент единственнен

Доказательство. От противного, тогда $e_1 = e_1 * e_2 = e_2$. □

Замечание. В группе обраный элемент единственнен для любого элемента G.

Доказательство. Пусть $\exists b, c : a * b = b * a = e, a * c = c * a = e$. Рассмотрим $b = (c * a) * b = c * (a * b) = c$. □

Замечание. Существует более слабое определение группы — можно не писать **одну** из коммутативностей в пунктах $2, 3$.

Утверждение 1.1. *В группе выполняется правило левого и правого сокращения, т.е. $a * b = c * b \Leftrightarrow a = c$ или $b * a = b * c \Leftrightarrow a = c$ (необходимо домножить на b^{-1} справа или слева).*

Определение 1.2. Группа G называется Абелевой, если операция $*$ **коммутативна**, т.е. $\forall a, b \in G a * b = b * a$.

Определение 1.3. Порядок группы — $|G| \in \mathbb{N} \cup \{\infty\}$ — мощность группы (в случае бесконечной, порядок равен ∞).

Определение 1.4. $a^n = \underbrace{a * a * \cdots * a}_{n}, a^0 = e$.

Определение 1.5. Порядок элемента группы — $\operatorname{ord} a = \min\{n \in \mathbb{N} | a^n = e\}$ (или ∞ в случае пустоты указанного множества).

Определение 1.6. Множество H называется подгруппой G, если $G \subset H$ и H является группой относительно операции $*_G$.

Утверждение 1.2 (Критерий подгруппы). *Непустое подмножество H в группе G является подгруппой ($H \leqslant G$), если*

1. *H замкнуто относительно операции $*$, т.е. $a, b \in H \Rightarrow a * b \in H$*
2. *H замкнуто относительно операции взятия обратного элемента, т.е. $a \in H \Rightarrow a^{-1} \in H$*

Доказательство.

Ассоциативность: следует из ассоциативности группы G и замкнутости относительно операции $*$.

Наличие нейтрального элемента: следует из замкнитости относительно взятия обратного и произведения $a * a^{-1} = e$

Наличие обратного элемента: следует из замкнутости относительно операции взятия нейтрального элемента. □

Определение 1.7. Пусть $(G_1, *), (G_2, \cdot)$ — группы. Гомоморфизмом $G_1 \to G_2$ называется всякое отображение $f : G_1 \to G_2$, такое, что $f(a * b) = f(a) \cdot f(b)$.

Определение 1.8. Изоморфизм — гомоморфизм, являющийся биекцией. Если группы изоморфны, пишут $G \cong H$.

Теорема 1.1 (Кэли). *Всякая конечная группа, порядок которой нравен n, изоморфна некоторой подгруппе группы S_n.*

1.2 Примеры групп

Пример. $(\mathbb{Z}_n, +), |Z_n| = n$

Пример. $(V, +)$

Пример. $GL_n(F)$ — группа невырожденных матриц

Пример. S_n — группа перестановок, $|S_n| = n!$

Пример. Q — группа кватернионов, $|Q| = 8, Q = \{\pm 1, \pm i, \pm j, \pm k\}$,

$$ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$$

1.3 Примеры подгрупп

Пример. $n\mathbb{Z} \leqslant \mathbb{Z}$

Пример. $W \leqslant V$

1.4 Подгруппа, порожденная подмножеством

Пусть $M \subset G$. Рассмотрим $\langle M \rangle = \bigcap_{M \subset H_i \leqslant G} H_i$

Теорема 1.2 (Об описании подгруппы, порожденной множеством). $\langle M \rangle = \{m_1^{\varepsilon_1} m_2^{\varepsilon_2} \dots m_s^{\varepsilon_s} | s \in \mathbb{Z}_{\geqslant 0}\}$.

Доказательство.

- $\subset$ Заметим, что полученное множество является подгруппой по критерию подгруппы ($(m_1^{\varepsilon_1} \dots m_s^{\varepsilon_s})^{-1} = m_s^{-\varepsilon_1} \dots m_1^{-\varepsilon_1}$).
- $\supset$ Все представленные элементы обязаны лежать в $\langle M \rangle$, т.к. они лежат в каждой группе, содержащей M.

□

Определение 1.9. $G = \langle M \rangle$ — тогда говорят, что G порождается множеством M. Тогда элементы из M называются порождающими элементами.

Определение 1.10. Пусть $a \in G$. Тогда группа $\langle a \rangle$ называется циклической.

Теорема 1.3 (Об элементе конечного порядка)**.** *Пусть* $a \in G, \operatorname{ord} a = n$. *Тогда* $\langle a \rangle$ *конечна и* $|\langle a \rangle| = n$ *и* $\langle a \rangle = \{e, a, a^2, \dots a^{n-1}\}$

Теорема 1.4. *Все циклические группы одного и того же порядка (в том числе и бесконечного) изоморфны.*

Доказательство. 1. $\operatorname{ord} \in \mathbb{N}$. Тогда эта группа изоморфна $(Z_n, +)$

2. $\operatorname{ord} = \infty$. Тогда эта группа изоморфна $(Z, +)$

□

1.5 Описание подгрупп циклических групп

Теорема 1.5. *Всякая подгруппа циклической группы является циклической*

Теорема 1.6. *Если* $G = \langle a \rangle \cong C_n$ *и* $H_d = \langle a^d \rangle, d|n$, *то*

1. $H_d \leqslant G, |H_d| = \frac{n}{d}$
2. $d_1 \neq d_2 \Rightarrow H_{d_1} \neq H_{d_2}$
3. *У группы* G *не существует никаких других подгрупп, кроме* $H_d, d|n$.

Определение 1.11. Пусть $A, B \subset G$. $A \cdot B = \{ab | a \in A, b \in B\}$.

Замечание. $A(BC) = (AB)C$

Определение 1.12. Если H — подгруппа в $G, x \in G$, то xH называется левым смежным классом, а Hx — правым смежным классом.

1.6 Свойства правых и левых смежных классов

Утверждение 1.3. $y \in xH \Rightarrow xH = yH$

Доказательство. $\exists h \in G : yh = x \Rightarrow yH = x(hH) = xH$. □

Следствие. Любые два смежных класса либо совпадают, либо не пересекаются.

Следствие. $\forall H \leqslant G, G = \bigsqcup x_i H$ для некоторых x_i

Доказательство. $x \in xH \Rightarrow G = \bigcup_{x \in G} xH$. Оставим в данном объединении только по одному представителю каждого смежного класса. Получили желаемое. □

Аналогичные свойства верны и для правых смежных классов.

Теорема 1.7 (Лагранжа)**.** *Порядок любой подгруппы* H *конечной группы* G *является делителем порядка группы.*

Доказательство. Разложим G по H. Получим, что $G = \bigsqcup x_i H \Rightarrow |G| = \sum_i |H|$. □

Определение 1.13. $(G : H) = |G : H| = \frac{|G|}{|H|}$, если $H \leqslant G$.

Следствие. $a \in G \Rightarrow \operatorname{ord} a |\ |G|$.

Следствие. $|G| = p \Rightarrow G$ — циклическая

Следствие. Существует единственная с точностью до изоморфизма группа порядка p.

Следствие (Теорема Эйлера)**.** Пусть $(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv_n 1$

Следствие (Малая Теорема Ферма)**.** Пусть $a^p \equiv_p a$