

# Механико-математический факультет

### Алгебра, 3 семестр, 2 поток

Преподаватель: Куликова Ольга Викторовна

Авторы: Соколов Егор

Группа: 108

Контакт: Мой телеграм для связи

Последняя компиляция: 1 сентября 2025 г.

# Содержание

1 Группы 2

# 1 Группы

**Определение.** Пусть G - множество. Бинарной операцией на G называется отображение  $*: G \times G \to G$ .

**Определение.** Множество G с бинарной операцией \* называется группой, если выполнены следующие аксиомы:

- 1.  $\forall a, b, c \in G \ a * (b * c) = (a * b) * c;$
- 2.  $\exists e \in G : \forall a \in G \ a * e = e * a = a;$
- 3.  $\forall a \in G \ \exists b \in G : a * b = b * a = e$

Различные формы записи группы:

1. Мультипликативная форма (терминология):

Операция - " · " (умножение);

Нейтральный элемент - единичный (1);

Элемент из аксиомы 3 - обратный  $(a^{-1}$  для  $a \in G)$ ;

2. Аддитивная форма (терминология):

Операция - " + " (сложение);

Нейтральный элемент - нулевой (0);

Элемент из аксиомы 3 - противоположный (-a для  $a \in G)$ ;

**Определение.** Если G - группа и  $\forall a,b \in G \ a \cdot b = b \cdot a,$  то G - абелева (коммутативная) группа.

Замечание. Обычно для обозначения абелевых групп будем использовать аддитивную форму записи, для иных - мультипликативную.

Утверждение (Простейшие свойства групп).

- 1. Единичный элемент единственный;
- 2.  $\forall a \in G$  обратный к а элемент единственный;
- $\beta. (ab)^{-1} = b^{-1}a^{-1};$
- 4. Если  $a,b \in G$ , то решение уравнения  $ax = b \ (xa = b)$  единственно.

Доказательство.

- 1. (От противного) Допустим, что  $\exists e_1, e_2 \in A$  единичные. Тогда  $e_1 = e_1 * e_2 = e_2$  по определению единичного элемента.
- 2. Допустим  $\exists b_1, b_2$  обратные к a элементы:  $b_1 \neq b_2$  В силу ассоциативности:

$$b_1 * (a * b_2) = (b_1 * a) * b_2$$
  
 $b_1 * e = e * b_2$   
 $b_1 = b_2$ 

3. 
$$abb^{-1}a^{-1} = aea^{-1} = e;$$
  
 $b^{-1}a^{-1}ab = b^{-1}eb = e \Longrightarrow (ab)^{-1} = b^{-1}a^{-1}$ 

4. 
$$ax = b \iff a^{-1}ax = a^{-1}b \iff x = a^{-1}b;$$
  
 $xa = b \iff xaa^{-1} = ba^{-1} \iff x = ba^{-1};$ 

**Определение.** Мощность множества G называется порядком группы G. Обозначается |G|.

Если  $|G| < \infty$ , то группа называется конечной, иначе бесконечной.

## Примеры.

- 1.  $(\mathbb{Z}, +), (\mathbb{Z}_n, +);$
- 2.  $GL_n(F)$  группа невырожденных матриц порядка n с коэффициентами из поля F;
- 3. Пусть  $\Omega$  множество. Преобразованиями  $\Omega$  назовём биекции  $f:\Omega \to \Omega$ .  $S(\Omega)$  множество всех преобразований  $\Omega$  образует группу относительно композиции.

Если  $\Omega = \{1, ..., n\}$ , то  $S(n) = S_n$  - группа подстановок.

4. Если  $G = \{a_1, ..., a_n\}$  - конечная группа, то её можно задать с помощью таблицы умножения (таблицы Кэли).

Например, для  $Z_2 = \{0, 1\}$ :

	0	1
0	0	1
1	1	0

П

5. Группа кватернионов:  $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ Таблица Кэли для кватернионов:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	i	-1

**Определение.** Подмножество  $H\subseteq G$  называется подгруппой группы G, если:

- 1.  $\forall a, b \in H \ ab \in H$ ;
- $2. \ \forall a \in H \ a^{-1} \in H;$
- 3.  $1 \in H$  (можно заменить на  $H \neq \varnothing$ )

Обозначается  $H \leqslant G$ .

**Утверждение.** Подгруппа H группы G является группой относительно бинарной операции группы G.

#### Примеры.

- 1.  $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C} \ (\mathbb{N} \nleq \mathbb{Z}$ , т.к. не группа);
- 2.  $GL_n(F) \geqslant SL_n(F) = \{A \in GL_n(F) | \det A = 1\}$  унимодулярная группа.
- 3.  $GL_n(F) \geqslant O_n(F) \geqslant SO_n(F) \ (O_n(F)$  ортогональная группа,  $SO_n(F)$  специальная ортогональная группа);
- 4.  $GL_n(F) \ge$  группа строго треугольных матриц.

**Определение.** Любая подгруппа группы  $S(\Omega)$  называется группой преобразований множества  $\Omega$ .

## Примеры.

- 1. GL(V) ( $\leq S(V)$ ) группа всех невырожденных линейных операторов векторного пространства V;
- 2.  $Aff(\mathbb{A})$  группа всех невырожденных аффинных преобразований аффинного пространства  $\mathbb{A}$ ;

3.  $\mathcal{E}^2$  - аффинно-евклидово двумерное пространство. Isom  $\mathcal{E}^2$  - группа изометрий (движений) на  $\mathcal{E}^2$ . Isom  $\mathcal{E}^2\geqslant O_2\geqslant SO_2$ , где  $O_2$  - группа движений, сохраняющих точку O,  $SO_2$  - группа поворотов вокруг точки O.

- 4.  $T\subseteq \mathcal{E}^2$  некоторая фигура. Sym  $T=\{f\in \mathrm{Isom}\ \mathcal{E}^2\|\ f(T)=T\}$  - группа симметрий фигуры T.
  - Если T окружность с центром в точке O, то Sym  $T = O_2$ ;
  - Если T правильный n-угольник с центром в точке O, то Sym  $T=D_n$  группа Диэдра.

 $|D_n| = 2n$  - n поворотов и n симметрий.

**Определение.** Пусть  $(G_1,*,e_1),(G_2,,e_2)$  - группы. Отображение  $\varphi:G_1\to G_2$  - изоморфизм, если

- 1.  $\varphi$  биекция;
- 2.  $\forall a, b \in G_1 \ \varphi(a * b) = \varphi(a) * \varphi(b)$

Если между  $G_1$  и  $G_2$  существует изоморфизм, то  $G_1$  и  $G_2$  называются изоморфными. Обозначается  $G_1\cong G_2$ .

Пример.  $D_3 \cong S_3$ .

Доказательство.  $D_3$  - группа движений, переводящая равносторонний треугольник в себя. Если пронумеровать вершины изначального треугольника, то каждый элемент группы  $D_3$  будет соответствовать подстановке, переводящей старый порядок вершин в новый. Определение изоморфизма проверяется очевидно.

**Утверждение.** Изоморфность групп - отношение эквивалентности на множестве групп.

Утверждение (Свойства изоморфизмов).

- 1.  $\varphi(e_1) = e_2;$
- 2.  $\varphi(a^{-1}) = (\varphi(a))^{-1}$ ;
- 3.  $G_1 \cong G_2 \Longrightarrow |G_1| = |G_2|$ .

Замечание. Обратное утверждение неверно (например,  $S_3 \ncong \mathbb{Z}_6$ ).

**Пример.**  $SO_2 \cong (U, \cdot)$ , где  $U = \{z \in \mathbb{C} : |z| = 1\}$ .

**Определение.** Пусть  $(G, \cdot, e)$  - группа,  $k \in \mathbb{Z}, g \in G$ . Мультипликативный термин - элемент g в степени k:

$$g^{k} = \begin{cases} \underbrace{g \cdot g \cdot \dots \cdot g}_{k}, k > 0 \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{-k}, k < 0 \\ e, k = 0 \end{cases}$$

**Определение.** Пусть (G, +, e) - группа,  $k \in \mathbb{Z}, g \in G$ . Аддитивный термин - кратное элемента g:

$$kg = \begin{cases} \underbrace{g + g + \dots + g, k > 0}_{k} \\ \underbrace{(-g) + (-g) + \dots + (-g)}_{-k}, k < 0 \\ e, k = 0 \end{cases}$$

**Утверждение** (Свойства  $(k, m \in \mathbb{Z}, g \in G)$ ).

1. 
$$g^k \cdot g^m = g^{k+m}$$
;

2. 
$$(g^k)^m = g^{km}$$
;

3. 
$$(g^k)^{-1} = g^{-k}$$
.

**Утверждение.** Множество всех элементов  $g^k$ , где  $k \in \mathbb{Z}$ ,  $g \in G$ , образует подгруппу в G. Обозначается  $\langle g \rangle = \{e, g, g^{-1}, g^2, g^{-2}, ...\}$ .

**Определение.**  $\langle g \rangle$  - циклическая подгруппа. порождённая элементом g.

#### Примеры.

1. 
$$G=\mathbb{Z}:\langle 2\rangle=2\mathbb{Z}$$
 - чётные целые числа;

2. 
$$G = \mathbb{Z}_6 : \langle 2 \rangle = \{0, 2, 4\};$$

3. 
$$G = \mathbb{C} : \langle i \rangle = \{\pm 1, \pm i\}$$

Пусть  $(G, \cdot, e)$  - группа,  $g \in G$ . Если  $\forall k, m \in \mathbb{Z} : k \neq m \Longrightarrow g^k \neq g^m$ , то  $\langle g \rangle$  - бесконечная (элемент g имеет бесконечный порядок).

Если  $\exists k, m \in \mathbb{Z} : k \neq m, g^k = g^m \Longrightarrow g^{k-m} = e \Longrightarrow$  существует наименьшее  $n \in \mathbb{N}$  такое, что  $g^n = e$  (элемент g имеет порядок n)

**Определение.** Порядком элемента  $g \in G$  называется наименьшее натуральное число n такое, что  $g^n = e$ , если такое существует. Иначе говорят, что элемент g имеет бесконечный порядок. Обозначается ord g.

#### Примеры.

- 1.  $G = \mathbb{Z}$ : ord  $2 = \infty$ ;
- 2.  $G = \mathbb{Z}$  : ord 2 = 6;
- 3.  $G=\mathbb{C}^*: \mathrm{ord}\ 2=\infty$  ( $\mathbb{C}^*$  мультипликативная группа поля,  $\mathbb{C}\setminus\{0\}$  относительно умножения).

Утверждение (Свойства).

1. 
$$g^m = e \iff \text{ord } g \mid m;$$

2. 
$$g^m = g^l \iff k \equiv l \pmod{g}$$

Доказательство.

1. Разделим m на  $n = \operatorname{ord} g$  с остатком: m = nq + r, где  $0 \leqslant r < n$ . Тогда:

$$e = g^m = (g^n)^q \cdot g^r = g^r \Longrightarrow r = 0$$

так как r < n, где n - минимальное натуральное число такое, что  $g^n = 0$ .

2. Следует из 1.