



Механико-математический факультет

**АЛГЕБРА, 3 СЕМЕСТР, 2 ПОТОК**

Преподаватель: Куликова Ольга Викторовна

Авторы: Соколов Егор

Группа: 208

Контакт: [Мой телеграм для связи](#)

Москва

Последняя компиляция: 25 сентября 2025 г.

# Содержание

<b>1</b>	<b>Группы</b>	<b>2</b>
1.1	Основные понятия . . . . .	2
1.2	Циклические группы . . . . .	9
1.3	Смежные классы . . . . .	11
1.4	Факторгруппа . . . . .	16
1.5	Гомоморфизмы групп . . . . .	17
<b>2</b>	<b>Свободные группы</b>	<b>20</b>
2.1	Задание группы порождающими и определяющими соотношениями . . . . .	23

# 1 Группы

## 1.1 Основные понятия

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

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

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

Различные формы записи группы:

1. Мультипликативная форма (терминология):  
Операция - "  $\cdot$  " (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  $\forall a, b \in G \quad a \cdot b = b \cdot a$ , 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  $a$  элемент единственный;
3.  $(ab)^{-1} = b^{-1}a^{-1}$ ;
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.  $abb^{-1}a^{-1} = aea^{-1} = e;$

$$b^{-1}a^{-1}ab = b^{-1}eb = e \implies (ab)^{-1} = b^{-1}a^{-1}$$

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  $f : \Omega \rightarrow \Omega$ .

$S(\Omega)$  - множество всех преобразований  $\Omega$  - образует группу относительно композиции.

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

4. Если  $G = \{a_1, \dots, a_n\}$  - 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

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

Обозначается  $H \leq G$ .

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

**Примеры.**

1.  $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$  ( $\mathbb{N} \not\leq \mathbb{Z}$ , т.к. не группа);
2.  $GL_n(F) \geq SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$  - унимодулярная группа.
3.  $GL_n(F) \geq O_n(F) \geq SO_n(F)$  ( $O_n(F)$  - ортогональная группа,  $SO_n(F)$  - специальная ортогональная группа);
4.  $GL_n(F) \geq$  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.

$\text{Isom } \mathcal{E}^2$  - группа изометрий (движений) на  $\mathcal{E}^2$ .

$\text{Isom } \mathcal{E}^2 \geq O_2 \geq SO_2$ , где  $O_2$  - группа движений, сохраняющих точку  $O$ ,  $SO_2$  - группа поворотов вокруг точки  $O$ .

4.  $T \subseteq \mathcal{E}^2$  - некоторая фигура.

$\text{Sym } T = \{f \in \text{Isom } \mathcal{E}^2 \mid f(T) = T\}$  - группа симметрий фигуры  $T$ .

- Если  $T$  - окружность с центром в точке  $O$ , то  $\text{Sym } T = O_2$ ;
- Если  $T$  - правильный  $n$ -угольник с центром в точке  $O$ , то  $\text{Sym } T = D_n$  - группа Диэдра.  
 $|D_n| = 2n$  -  $n$  поворотов и  $n$  симметрий.

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

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

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

**Пример.**  $D_3 \simeq S_3$ .

*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.  $\square$

**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.  $G_1 \simeq G_2 \implies |G_1| = |G_2|$ .

*Замечание.* Обратное утверждение неверно (например,  $S_3 \not\simeq \mathbb{Z}_6$ ).

**Пример.**  $SO_2 \simeq (U, \cdot)$ , 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  $g$ :

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

**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  $\langle g \rangle = \{e, g, g^{-1}, g^2, g^{-2}, \dots\}$ .

**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  $\forall k, m \in \mathbb{Z} : k \neq m \implies g^k \neq g^m$ , то  $\langle g \rangle$  - бесконечная (элемент  $g$  имеет бесконечный порядок).

Если  $\exists k, m \in \mathbb{Z} : k \neq m, g^k = g^m \implies g^{k-m} = e \implies$  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  $\text{ord } g$ .

**Примеры.**

$$1. G = \mathbb{Z} : \text{ord } 2 = \infty;$$

$$2. G = \mathbb{Z}_{12} : \text{ord } 2 = 6;$$

$$3. G = \mathbb{C}^* : \text{ord } 2 = \infty$$

( $\mathbb{C}^*$  - мультипликативная группа поля,  $\mathbb{C} \setminus \{0\}$  относительно умножения).

**Утверждение 1** (Свойства элементов конечного порядка).

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

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

*Доказательство.*

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

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

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

2. Следует из 1.

□

**Следствие.**  $\text{ord } g = |\langle g \rangle|$

*Доказательство.* Если  $\text{ord } g = \infty$  :  $\forall k \neq l \ g^k \neq g^l \implies$  подгруппа  $\langle g \rangle = \{e, g^{\pm 1}, g^{\pm 2}, \dots\}$  бесконечна.

Если  $\text{ord } g = n$  :  $\langle g \rangle = \{e, g^1, \dots, g^{n-1}\}$  - все эти элементы различны из пункта 2 утверждения, а других нет по определению порядка. □

**Примеры.**



1.  $i \in \mathbb{C}^*$  -  $\text{ord } i = 4$ ;

2.  $\sigma \in S_n$ :

Если  $\sigma = (i_1, \dots, i_k)$  - цикл длины  $k$ , то  $\text{ord } \sigma = k$ .

Так как любая подстановка раскладывается в произведение независимых циклов и независимые циклы коммутируют, если  $\sigma = \tau_1 \dots \tau_n$ , где  $\tau_i$  - независимые циклы, то верно:  $\text{ord } \sigma = \text{НОК } \{|\tau_1|, \dots, |\tau_n|\}$ .

Например,  $\sigma = (23)(145) \implies \text{ord } \sigma = 6$ .

**Утверждение 2.** Пусть  $n = \text{ord } g$ . Тогда  $\text{ord } g^k = \frac{n}{\text{НОД}(n,k)}$ .

*Доказательство.* Пусть  $\text{ord } g^k = m$ . Из утверждения 1:  $g^{mk} = e \iff n | mk$ , откуда  $\frac{n}{\text{НОД}(n,k)} | m$ , т.е.  $m \geq \frac{n}{\text{НОД}(n,k)}$ . Очевидно, что при  $m = \frac{n}{\text{НОД}(n,k)}$   $n | mk$ .  $\square$

**Определение.** Множество  $S \subseteq G$  называется порождающим множеством для группы  $G$ , если  $\forall g \in G \exists s_1, \dots, s_k \in S : g = s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}$ , где  $\varepsilon_i = \pm 1$  ( $s_i$  не обязательно различны).

При этом говорят, что  $G$  порождается множеством  $S$ .

Если  $\exists$  конечное множество  $S$  такое, что  $S$  порождает  $G$ , то  $G$  называется конечно порождённой, и бесконечно порождённой иначе.

Обозначается  $\langle S \rangle = \{s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k} | \varepsilon_i = \pm 1\}$  - группа, порождённая  $S$ .

**Примеры.**

1.  $S_n = \langle \text{все транспозиции} \rangle$ ;

2.  $GL_n(F) = \langle \text{все элементарные матрицы} \rangle$

3.  $Q_8 = \langle i, j \rangle$ ;

4.  $D_n = \langle \alpha, s \rangle$ , где  $\alpha$  - поворот на  $\frac{2\pi}{n}$ , а  $s$  - любая из симметрий.

5. Группа Клейна:  $H = \{\text{id}, a = (12)(34), b = (13)(24), c = (14)(23)\} \leq S_4$

Это группа симметрий прямоугольника, не являющегося квадратом:  $a, c$  - симметрии относительно средних линий,  $b$  - поворот на  $\pi$  вокруг центра.

Таблица Кэли для группы Клейна:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Отсюда  $\{e, a, b, c\} = \langle a, b \rangle$ .

6.  $\mathbb{Q}$  - бесконечно порождённая.

## 1.2 Циклические группы

**Определение.** Группа  $G$  называется циклической, если  $G$  порождается одним элементом, т.е.  $\exists g \in G : \forall h \in G \exists k \in \mathbb{Z} : h = g^k$ . Элемент  $g$  также называется образующим элементом группы  $G$ .

**Примеры.**

1.  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ ,  $\mathbb{Z}_n = \langle 1 \rangle$ ;

2.  $U_n$  - множество всех комплексных корней степени  $n$  из 1.

$U_n$  - группа относительно умножения, причём  $U_n = \langle \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \rangle$ .

**Утверждение 3.** Если  $G = \langle g \rangle$ , то  $|G| = \text{ord } g$ .

*Доказательство.* Очевидно из определения порождающего множества. □

*Замечание.* Далее циклическую группу порядка  $n$  обозначаем  $\langle g \rangle_n$

**Утверждение 4.** Пусть  $G = \langle g \rangle_n$ . Тогда  $G = \langle g^k \rangle \iff \text{НОД}(k, n) = 1$ .

*Доказательство.* Из утверждения 3  $|G| = \text{ord } g$ . Тогда:

$$G = \langle g^k \rangle \iff \text{ord } g^k = \frac{n}{\text{НОД}(n, k)} = n \iff \text{НОД}(n, k) = 1$$

□

**Теорема 1** (Классификация циклических групп).

1. Если циклическая группа  $G$  бесконечна, то  $G \simeq \mathbb{Z}$ ;

2. Если циклическая группа  $G$  конечна и имеет порядок  $n$ , то  $G \simeq \mathbb{Z}_n$ .

*Доказательство.*

1. Пусть  $\text{ord } g = \infty, \forall h \in G \exists k \in \mathbb{Z} : h = g^k$

Рассмотрим отображение  $\varphi : G \rightarrow \mathbb{Z}$  такого вида:  $\varphi : g^k \mapsto k$ . Очевидно, что  $\varphi$  - сюръекция (в  $k \in \mathbb{Z}$  перешёл  $g^k \in G$ ).

$\varphi(g^k) = \varphi(g^m) \implies k = m \implies g^k = g^m$  - отсюда  $\varphi$  - инъекция.

Проверим сохранение операции:

$$\varphi(g^k \cdot g^m) = \varphi(g^{k+m}) = k + m = \varphi(g^k) + \varphi(g^m)$$

Отсюда  $\varphi$  - изоморфизм.

2. Пусть  $\text{ord } g = n$ . Рассмотрим отображение  $\varphi : \mathbb{Z}_n \rightarrow G$  такого вида:  $\varphi : k \mapsto g^k$ . Очевидно, что  $\varphi$  - сюръекция (в  $g^k \in G$  перешёл  $k \in \mathbb{Z}_n$ ).  
 $k \equiv m \pmod{n} \iff g^k = g^m$  - отсюда  $\varphi$  - инъекция.  
 Сохранение операции - аналогично пункту 1.  
 Отсюда  $\varphi$  - изоморфизм.

□

**Следствие.** Если  $G_1, G_2$  - циклические группы, то  $G_1 \simeq G_2 \iff |G_1| = |G_2|$ .

*Доказательство.*

$\implies$ : верно всегда;

$\impliedby$ : из теоремы: если  $G_1$  бесконечна, то  $G_1 \simeq \mathbb{Z} \simeq G_2$ , иначе  $G_1 \simeq \mathbb{Z}_n \simeq G_2$ , где  $n = |G_1| = |G_2|$ . □

## Теорема 2.

1. Любая подгруппа циклической группы является циклической.
2. Подгруппы циклической группы  $G$  порядка  $n$  находятся во взаимно однозначном соответствии с делителями  $n$ , т.е.

$$\forall H \leq G \ |H| \mid n \text{ и } \forall d \mid n \ \exists! H \leq G : |H| = d$$

3. Подгруппы группы  $\mathbb{Z}$  исчерпываются группами  $k\mathbb{Z} = \langle k \rangle$ , где  $k \in \mathbb{N} \cup \{0\}$ .

*Доказательство.*

1. Пусть  $G = \langle g \rangle, H \leq G$ . Если  $H = \{e\}$ , то  $H = \langle e \rangle$ .  
 При  $H \neq \{e\} : \forall h \in H \ \exists k \in \mathbb{Z} : h = g^k$ . Так как  $g^k \in H \implies g^{-k} \in H$  и в  $H$  есть элемент, отличный от  $e$ ,  $\exists$  наименьшее  $k \in \mathbb{N} : g^k \in H$ .  
 Докажем, что  $H = \langle g^k \rangle$ . Рассмотрим произвольный  $g^m \in H$ . Разделим  $m$  на  $k$  с остатком:  $m = kq + r, 0 \leq r < k$ . Тогда:

$$g^m = (g^k)^q \cdot g^r \implies g^r = (g^k)^{-q} \cdot g^m \implies r = 0, \text{ т.к. } k - \text{наименьшее} \in \mathbb{N}$$

2.  $G = \langle g \rangle_n, H \leq G \implies_{(1)} H = \langle g^k \rangle$ .

Так как  $g^n = e \in H$ , то в силу рассуждений пункта 1 при  $m = n$  получаем  $k \mid n \implies n = kq$ .

Отсюда  $H = \{e, g^k, g^{2k}, \dots, g^{(q-1)k}\} \implies |H| = q$ , где  $q \mid n$ .

Обратно,  $\forall d \mid n \ \exists! H = \langle g^{\frac{n}{d}} \rangle$  (в силу описания выше других подгрупп такого порядка нет).

3. Из пункта 1 в аддитивной форме получаем, что  $H \leq \mathbb{Z} = \langle 1 \rangle \implies H = \langle k \cdot 1 \rangle$

□

**Следствие.** В циклической группе простого порядка существуют ровно две подгруппы - тривиальная и сама группа.

**Примеры.**

1.  $H \leq \mathbb{Z}_5 \implies H = \{0\}, H = \mathbb{Z}_5;$

2.  $H \leq \mathbb{Z}_6 \implies H = \{0\}, H = \langle 2 \rangle, H = \langle 3 \rangle, H = \mathbb{Z}_6.$

### 1.3 Смежные классы

**Определение.** Пусть  $(G, \cdot, e)$  - произвольная группа,  $H \leq G, g \in G$ .

Рассмотрим множества:

$gH = \{gh | h \in H\}$  - левый смежный класс  $G$  по  $H$  с представителем  $g$

$Hg = \{hg | h \in H\}$  - правый смежный класс  $G$  по  $H$  с представителем  $g$

**Утверждение** (Свойства смежных классов).

1.  $\forall a \in G \ a \in aH;$

2. если  $a \in bH$ , то  $bH = aH$ ; в частности, любые два смежных класса либо не пересекаются, либо совпадают.

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

(Верны аналогичные утверждения для правых смежных классов)

*Доказательство.*

1. Очевидно;

2.  $a \in bH \implies \exists h \in H : a = bh \implies \forall \tilde{h} \in H \ a\tilde{h} = b\tilde{h} \in bH \implies aH \subseteq bH.$   
Аналогично  $bH \subseteq aH \implies aH = bH.$

3.  $\implies: aH = bH \implies a \in bH (a \in aH) \implies \exists h \in H : a = bh \implies b^{-1}a = h \in H$   
 $\iff: b^{-1}a = h \in H \implies a = bh \implies aH = bH$  по пункту 2.

□

**Утверждение.** Отношение  $a \equiv b \pmod{H} \Leftrightarrow b^{-1}a \in H$  является отношением эквивалентности, причём классы эквивалентности совпадают с левыми смежными классами (аналогично  $ab^{-1} \in H$  для правых).

*Доказательство.*

- Рефлексивность:  $a^{-1}a = e \in H \Rightarrow a \equiv a \pmod{H}$ ;
- Симметричность:  $a \equiv b \pmod{H} \Rightarrow b^{-1}a \in H \Rightarrow a^{-1}b = (b^{-1}a)^{-1} \in H \Rightarrow b \equiv a \pmod{H}$ ;
- Транзитивность:  $a \equiv b, b \equiv c \pmod{H} \Rightarrow c^{-1}b, b^{-1}a \in H \Rightarrow c^{-1}b \cdot b^{-1}a = c^{-1}a \in H \Rightarrow a \equiv c \pmod{H}$ .

Совпадение классов эквивалентности с левыми смежными классами следует из пункта 3 предыдущего утверждения.  $\square$

**Утверждение.** Если  $G$  - абелева, то  $\forall a \in G : aH = Ha$ .  
(В общем случае данное утверждение неверно).

*Доказательство.*  $\forall a \in G : \{ah : h \in H\} = \{ha : h \in H\} \Rightarrow aH = Ha$ .  $\square$

**Примеры.**

1.  $H = \langle (12) \rangle \leq S_3$  ( $H = \{id, (12)\}$ ),  $g = (13)$ .  
 $(13)(12) = (123)$ ;  $(12)(13) = (132)$ .  
Тогда  $\{(13), (123)\} = gH \neq Hg = \{(13), (132)\}$ .
2.  $H = 3\mathbb{Z} \leq \mathbb{Z}$ . Смежные классы -  $3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$ .
3.  $H = \mathbb{R} \leq \mathbb{C}$ . Смежные классы -  $a + bi + \mathbb{R} = bi + \mathbb{R}$ .

**Утверждение.** Множество  $\{aH : a \in G\}$  находится во взаимно однозначном соответствии с множеством  $\{Ha : a \in G\}$ .

*Доказательство.*  $gH \leftrightarrow Hg^{-1} : x = gh \in gH \leftrightarrow x^{-1} = h^{-1}g^{-1} \in Hg^{-1}$ .  $\square$

**Следствие.**  $|\{aH : a \in G\}| = |\{Ha : a \in G\}|$

**Определение.** Мощность множества левых смежных классов группы  $G$  по подгруппе  $H$  называется индексом  $H$  в  $G$ . Обозначение:  $|G : H|$

**Пример.**  $|\mathbb{Z} : 3\mathbb{Z}| = 3$ , т.к. смежные классы -  $\{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$ .

**Теорема.** (Теорема Лагранжа)

Пусть  $G$  - конечная группа,  $H \leq G$ . Тогда  $|G| = |H| \cdot |G : H|$ .

*Доказательство.* Так как  $|G| < \infty$ , то  $|H| < \infty$ , т.е.  $H = \{h_1, \dots, h_k\}$ .

$\forall g \in G, gH = \{gh_1, \dots, gh_k\}$ , причем  $gh_i = gh_j \Rightarrow h_i = h_j \Rightarrow |gH| = |H|$ .

Отсюда, если  $|G : H| = n$ :

$$G = \bigsqcup_{i=1}^n a_i H \implies |G| = \sum_{i=1}^n |a_i H| = |G : H| \cdot |H|$$

□

**Следствие 1.** Если  $G$  - конечная группа,  $H \leq G$ , то  $|H| \mid |G|$ .

(Обратное утверждение неверно).

**Упражнение.** Пусть  $G = A_4$  (группа чётных перестановок).

$|A_4| = \frac{4!}{2} = 12$ . Докажем, что в  $A_4$  нет подгруппы порядка 6.

Предположим, что  $H \leq A_4$  и  $|H| = 6$ .  $A_4$  состоит из элемента  $id$ , 3 элементов вида  $(ab)(cd)$  и восьми элементов вида  $(abc)$ . Значит,  $H$  содержит хотя бы один элемент вида  $(abc)$  (с точностью до перенумерования -  $(123)$ ). Тогда  $H$  содержит и  $(123)^{-1} = (132)$ . Также знаем, что группа чётного порядка содержит элемент порядка 2 (иначе в группе все элементы, кроме  $e$ , разбиваются на пары обратных, и элементов нечётное число), поэтому  $H$  содержит  $\sigma = (**)(**)$ .

Рассмотрим  $\omega = \sigma(123)\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$  (это равенство легко проверить, подставив в него  $\sigma(1), \dots, \sigma(4)$ ). Очевидно, что это цикл длины 3, не оставляющий на месте 4 (т.к.  $\sigma$  не оставляет на месте 4). Значит,  $\omega$  и  $\omega^{-1}$  принадлежат  $H$  и не совпадают с предыдущими элементами (и друг с другом), т.е.

$$H = \{id, (123), (132), \sigma, \omega, \omega^{-1}\}$$

Осталось перебрать возможные значения  $\sigma$ :

- $\sigma = (12)(34) \implies (123)(12)(34)(132) = (14)(23) \notin H$ ;
- $\sigma = (13)(24) \implies (123)(13)(24)(132) = (12)(34) \notin H$ ;
- $\sigma = (14)(23) \implies (123)(14)(23)(132) = (13)(24) \notin H$ ;

Отсюда таких  $H$  не существует.

**Следствие 2.** Если  $G$  - конечная группа, то  $\forall g \in G : \text{ord } g \mid |G|$

*Доказательство.*  $\text{ord } g = |\langle g \rangle| \mid |G|$ .

□

**Следствие 3.** Если  $G$  - конечная группа порядка  $n$ , то  $\forall g \in G : g^n = e$  в  $G$ .

*Доказательство.* По следствию 2:  $n = \text{ord } g \cdot k \Rightarrow g^n = g^{(\text{ord } g) \cdot k} = e^k = e$ .

□

**Пример.** Пусть  $G = \mathbb{Z}_p^*$ ,  $p$  - простое,  $|\mathbb{Z}_p^*| = p - 1$ . По следствию 3:  
 $\forall a \in \mathbb{Z}_p^* : a^{p-1} = 1$  в  $\mathbb{Z}_p^*$ , отсюда  $\forall a \in \mathbb{Z}, p \nmid a : a^{p-1} \equiv 1 \pmod{p}$  - малая теорема Ферма.

**Следствие 4.** Любая группа  $G$  простого порядка  $p$  является циклической.

*Доказательство.*  $\forall a \in G, a \neq e : \text{ord } a \neq 1, \text{ord } a \mid |G| = p \Rightarrow \text{ord } a = |G| \Rightarrow G = \langle a \rangle$ .  $\square$

**Упражнение.** Доказать, что с точностью до изоморфизма существует ровно две группы порядка 4 -  $\mathbb{Z}_4$  и  $V_4$ .

*Доказательство.* Пусть  $G$  - группа порядка 4. Заметим, что по следствию 2 порядок неединичного элемента в  $G$  может быть равен либо 2, либо 4. Если в  $G$  есть элемент порядка 4, то  $G$  циклическая, а тогда по теореме о классификации циклических групп  $G \simeq \mathbb{Z}_4$ .

Пусть  $G = \{e, a, b, c\}, \text{ord } a = \text{ord } b = \text{ord } c = 2$ . Посмотрим, чему может быть равно  $ab$ :

- $ab = e \Rightarrow aab = a \Rightarrow b = a$  - противоречие;
- $ab = a \Rightarrow aab = aa \Rightarrow b = e$  - противоречие;
- $ab = b \Rightarrow abb = bb \Rightarrow a = e$  - противоречие.

Отсюда  $ab = c$  - аналогично произведение любых двух различных неединичных элементов равно третьему. Отсюда таблица Кэли для  $G$  имеет вид

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

откуда видно, что  $G \simeq V_4$ .  $\square$

**Упражнение.** Доказать, что если в группе  $G$  все неединичные элементы имеют порядок 2, то  $G$  - абелева.

*Доказательство.*  $\text{ord } a = 2 \Rightarrow a = a^{-1} \Rightarrow \forall a, b \in G : ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ .  $\square$

**Пример.**  $H = \langle (12) \rangle \leq S_3, g = (13) \Rightarrow gH \neq Hg$

**Определение.** Подгруппа  $H$  группы  $G$  называется нормальной, если

$$\begin{aligned} \forall g \in G : gH = Hg &\iff \forall g \in G : gHg^{-1} = H \iff \\ &\iff \forall g \in G : gHg^{-1} \subseteq H \iff \forall g \in G, \forall h \in H : ghg^{-1} \in H \end{aligned}$$

Обозначение:  $H \trianglelefteq G$ .

*Эквивалентность определений:*

- $1 \iff 2$  - очевидно;
- $2 \iff 3$ :  
 $\Leftarrow$ :  $gHg^{-1} \subseteq H \Leftrightarrow H \subseteq g^{-1}Hg$  - из условия на всевозможные  $g$  получаем равенство;  
 $\Rightarrow$  - очевидно;
- $3 \iff 4$  - из определения смежного класса.

□

**Примеры.**

1.  $A_n \trianglelefteq S_n$ , так как  $\forall \sigma \in S_n, \forall \tau \in A_n : \sigma\tau\sigma^{-1} \in A_n$ .
2.  $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$ , так как  $\forall A \in GL_n(\mathbb{R}), \forall B \in SL_n(\mathbb{R}) : \det(ABA^{-1}) = \det B = 1 \Rightarrow ABA^{-1} \in SL_n(\mathbb{R})$ .

**Утверждение.** В абелевой группе любая подгруппа является нормальной.

**Упражнение.** Докажите, что если  $|G : H| = 2$ , то  $H \trianglelefteq G$  для произвольной группы  $G$  и произвольной подгруппы  $H \leq G$ .

*Доказательство.* Если  $|G : H| = 2$ , то  $G$  разбивается на два непересекающихся левых (правых) смежных класса по  $H$ . Очевидно, что один из этих классов в обоих случаях - сама подгруппа  $H$ . Тогда  $\forall g \in G \setminus H$  группа  $G$  разбивается на левые смежные классы  $H$  и  $gH$ , а также на правые смежные классы  $H$  и  $Hg$ , откуда  $gH = Hg$ . Также очевидно, что  $\forall h \in H : hH = H = Hh$ . Значит,  $\forall g \in G : gH = Hg \implies H \trianglelefteq G$ . □



## 1.4 Факторгруппа

**Утверждение.** Пусть  $G$  - группа,  $H \trianglelefteq G$ . Тогда множество всех смежных классов  $G$  по  $H$  :  $G/H = \{eH, aH, \dots\}$  образует группу относительно операции  $aH \cdot bH = abH$ .

*Доказательство.*

1. Проверим корректность операции, т.е.  $\begin{cases} aH = \tilde{a}H \\ bH = \tilde{b}H \end{cases} \implies abH = \tilde{a}\tilde{b}H$ .

Действительно, если  $\begin{cases} a = \tilde{a}h_a \\ b = \tilde{b}h_b \end{cases}$  из равенства смежных классов, то:

$$\forall x \in abH \implies \exists h \in H : x = abh = \tilde{a}h_a\tilde{b}h_bh = \tilde{a}\tilde{b}h'h_bh \in \tilde{a}\tilde{b}H$$

$$(H \trianglelefteq G \implies Hb = bH \implies \exists h' \in H : h_a\tilde{b} = \tilde{b}h')$$

2. Проверим, что это группа:

- Ассоциативность:

$$aH(bH \cdot cH) = aH(bcH) = a(bc)H = (ab)cH = (abH)cH = (aH \cdot bH)cH$$

- Нейтральный элемент:

$$eH = H : aH \cdot eH = aeH = aH = eaH = eH \cdot aH$$

- Обратный элемент:

$$\forall aH \exists a^{-1}H : aH \cdot a^{-1}H = eH = a^{-1}H \cdot aH$$

□

**Определение.** Группа  $G/H$  называется факторгруппой  $G$  по  $H$ .

*Замечание.* Если  $H \not\trianglelefteq G$ , то операция  $aH \cdot bH = abH$  некорректна:

$$\langle (12) \rangle \leq S_3 : (13)H = (132)H, (23)H = (123)H;$$

$$(13)(23)H = (132)H \neq H = (123)(123)H$$

**Примеры.**

1.  $\mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}_3 = \{0, 1, 2\}$ ;
2.  $S_n \trianglelefteq A_n, S_n/A_n \simeq \mathbb{Z}_2$  (по чётности);
3.  $\mathbb{R} \trianglelefteq \mathbb{C}, \mathbb{C}/\mathbb{R} \simeq \mathbb{R}$  ( $bi + \mathbb{R} \mapsto b$ ).

## 1.5 Гомоморфизмы групп

**Определение.** Пусть  $(G, \cdot, e), (\tilde{G}, \cdot, \tilde{e})$  - группы. Отображение  $\varphi : G \rightarrow \tilde{G}$  называется гомоморфизмом групп  $G$  и  $\tilde{G}$ , если  $\forall a, b \in G \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ .

*Замечание.* В частности, изоморфизм - биективный гомоморфизм.

**Утверждение** (Свойства гомоморфизмов).

1.  $\varphi(e) = \tilde{e}$ ;
2.  $\varphi(a^{-1}) = (\varphi(a))^{-1}$

**Определение.** Множество  $\text{Im } \varphi = \{b \in \tilde{G} \mid \exists a \in G : \varphi(a) = b\}$  - образ гомоморфизма. Множество  $\text{Ker } \varphi = \{a \in G \mid \varphi(a) = \tilde{e}\}$  - ядро гомоморфизма.

**Утверждение 1.**

1.  $\text{Im } \varphi \leq \tilde{G}$ ;
2.  $\text{Ker } \varphi \leq G$ .

*Доказательство.*

1.  $\text{Im } \varphi \subseteq \tilde{G}$ 
  - $x, y \in \text{Im } \varphi \Rightarrow \exists a, b \in G : x = \varphi(a), y = \varphi(b) \Rightarrow xy = \varphi(a)\varphi(b) = \varphi(ab) \in \text{Im } \varphi$ ;
  - $\tilde{e} = \varphi(e) \in \text{Im } \varphi$ ;
  - $\forall x \in \text{Im } \varphi \exists a \in G : \varphi(a) = x \Rightarrow x^{-1} = (\varphi(a))^{-1} = \varphi(a^{-1}) \in \text{Im } \varphi$

Отсюда  $\text{Im } \varphi \leq \tilde{G}$ .

2.  $\text{Ker } \varphi \subseteq G$ 
  - $\forall a, b \in \text{Ker } \varphi : \varphi(a) = \varphi(b) = \tilde{e} \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = \tilde{e} \Rightarrow ab \in \text{Ker } \varphi$ ;
  - $\tilde{e} = \varphi e \Rightarrow e \in \text{Ker } \varphi$ ;
  - $\forall a \in \text{Ker } \varphi \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1} = \tilde{e}^{-1} = \tilde{e} \Rightarrow a^{-1} \in \text{Ker } \varphi$

Отсюда  $\text{Ker } \varphi \leq G$ .

$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = \tilde{e} \Rightarrow ghg^{-1} \in \text{Ker } \varphi \Rightarrow \text{Ker } \varphi \trianglelefteq G$ .

□

**Утверждение 2.**  $\varphi(a) = \varphi(b) \iff a\text{Ker } \varphi = b\text{Ker } \varphi$ .

В частности,  $\varphi$  инъективно  $\iff \text{Ker } \varphi = \{e\}$ .

*Доказательство.*

$$\varphi(a) = \varphi(b) \iff \varphi(a)\varphi(b)^{-1} = \tilde{e} \iff \varphi(ab^{-1}) = \tilde{e} \iff$$

$$ab^{-1} \in \text{Ker } \varphi \iff a\text{Ker } \varphi = b\text{Ker } \varphi$$

□

**Пример.**  $\varphi : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^* : \varphi(A) = \det A$ .

$$\text{Ker } \varphi = SL_n(\mathbb{R}), \text{Im } \varphi = \mathbb{R}^* \implies \mathbb{R}^* \simeq GL_n(\mathbb{R})/SL_n(\mathbb{R}).$$

**Теорема** (О гомоморфизме). Пусть  $G, \tilde{G}$  - группы,  $\varphi : G \rightarrow \tilde{G}$  - гомоморфизм. Тогда  $G/\text{Ker } \varphi \simeq \text{Im } \varphi$ .

*Доказательство.* Для начала заметим, что  $\text{Ker } \varphi \trianglelefteq G$ , поэтому факторгруппа  $G/\text{Ker } \varphi$  определена.

Рассмотрим  $\psi : g\text{Ker } \varphi \mapsto \varphi(g)$ :

- Корректность:

$$\text{По утверждению 2: } g_1\text{Ker } \varphi = g_2\text{Ker } \varphi \implies \varphi(g_1) = \varphi(g_2);$$

- Биективность:

$$\text{Сюръективность: } \forall b \in \tilde{G} \exists a \in G : \varphi(a) = b \implies \psi(a\text{Ker } \varphi) = b;$$

$$\text{Инъективность: по утверждению 2: } \psi(a\text{Ker } \varphi) = \psi(b\text{Ker } \varphi) \implies \varphi(g_1) = \varphi(g_2) \implies a\text{Ker } \varphi = b\text{Ker } \varphi;$$

- Сохранение операции:

$$\begin{aligned} \psi((g_1\text{Ker } \varphi)(g_2\text{Ker } \varphi)) &= \psi(g_1g_2\text{Ker } \varphi) = \varphi(g_1g_2) = \\ &= \varphi(g_1)\varphi(g_2) = \psi(g_1\text{Ker } \varphi)\psi(g_2\text{Ker } \varphi) \end{aligned}$$

Отсюда  $\psi : G/\text{Ker } \varphi \rightarrow \text{Im } \varphi$  - изоморфизм.

□

**Пример.** Пусть  $G = S_n, \tilde{G} = \mathbb{R}^*, \varphi(\sigma) = \text{sgn } \sigma$ .

Тогда из теоремы о гомоморфизме:

$$\text{Im } \varphi = \{\pm 1\}, \text{Ker } \varphi = A_n \implies S_n/A_n \simeq \{\pm 1\} \simeq \mathbb{Z}_2$$

**Следствие 1.** Гомоморфизм  $\varphi : G \rightarrow \tilde{G}$  - изоморфизм  $\iff \begin{cases} \text{Ker } \varphi = \{e\} \\ \text{Im } \varphi = \tilde{G} \end{cases}$

*Доказательство.*

$\implies$  - очевидно из биективности;

$\impliedby$  - изоморфизм из теоремы совпадёт с  $\varphi$ . □

**Следствие 2.** Если  $|G| < \infty$ , то  $|G| = |\text{Ker } \varphi| \cdot |\text{Im } \varphi|$ .

*Доказательство.*  $|G| = |G/\text{Ker } \varphi| \cdot |\text{Ker } \varphi| = |\text{Im } \varphi| \cdot |\text{Ker } \varphi|$ . □

**Утверждение.** Пусть  $G$  - группа,  $H \trianglelefteq G$ . Тогда  $\exists$  такая группа  $\tilde{G}$ , что  $\exists$  сюръективный гомоморфизм  $\pi : G \rightarrow \tilde{G}$ , причём  $\text{Ker } \pi = H$ .

*Доказательство.* Подходят  $\tilde{G} = G/H, \pi : g \mapsto gH$ . □

**Определение.** Приведённый выше гомоморфизм  $\pi : G \mapsto G/H$  называется естественным (натуральным) гомоморфизмом из  $G$  в  $G/H$ .

**Определение.** Эпиморфизм - сюръективный гомоморфизм.

**Утверждение.** Пусть  $\varphi : G \rightarrow \tilde{\tilde{G}}$  - произвольный эпиморфизм с ядром  $H$ . Тогда  $\exists$  изоморфизм  $\psi : G/H \rightarrow \tilde{\tilde{G}}$  такой, что  $\varphi = \psi \circ \pi$ , где  $\pi$  - натуральный гомоморфизм из  $G$  в  $G/H$ .

*Доказательство.* По теореме о гомоморфизме  $G/\text{Ker } \varphi \simeq \text{Im } \varphi$ .

Так как  $\varphi$  - сюръекция,  $\text{Im } \varphi = \tilde{\tilde{G}}$ , также по условию  $\text{Ker } \varphi = H$ . Тогда  $\psi : G/H \rightarrow \tilde{\tilde{G}}$  - изоморфизм, заданный в доказательстве теоремы о гомоморфизме:  $\psi : gH \mapsto \varphi(g)$ .

Взяв этот изоморфизм, получим  $\varphi = \psi \circ \pi$  (так как  $g \xrightarrow{\pi} gH \xrightarrow{\psi} \varphi(g)$ ). □

## 2 Свободные группы

**Определение.** Тривиальные (групповые) соотношения - соотношения, которые выводятся из аксиом группы (и, соответственно, есть в любой группе).

Построим группу, в которой нет других соотношений.

**Определение.** Пусть  $A$  - множество символов (букв),  $A^{-1}$  - множество символов (букв)  $a^{-1}$ , где  $a \in A$ .

Условия на эти множества:

$$1. \forall a^{-1} \in A^{-1} \implies a^{-1} \notin A;$$

$$\forall a \in A \implies a \notin A^{-1};$$

$$2. (a^{-1})^{-1} = a;$$

Буквы  $a, a^{-1}$  назовём взаимно обратными.

Множество  $A^{\pm 1} = A \sqcup A^{-1}$  называется алфавитом.

Слово в алфавите  $A^{\pm 1}$  - конечная последовательность букв  $X = x_1 \dots x_k$ , где  $x_i \in A^{\pm 1}$ .

Длина слова  $X$  (обозначается  $|X|$ ) - количество букв в  $X$ .

**Пример.**  $A = \{a, b\} : X = abaab^{-1} \Rightarrow |X| = 5$ .

**Определение.** Слово  $X = x_1 \dots x_k$  - сократимое, если  $\exists i \in \overline{1, \dots, k-1} : x_i = x_{i+1}^{-1}$ .

Сокращением взаимно обратных букв назовём вычёркивание пары  $x_i, x_{i+1}$  из  $X$  (получим слово длины  $|X| - 2$ ).

За конечное число сокращений получим слово  $\tilde{X}$ , не являющееся сократимым - такое  $\tilde{X}$  называется результатом полного сокращения слова  $X$ .

**Определение.** Рассмотрим множество  $F(A)$  всех несократимых слов в  $A^{\pm 1}$ .

Введём бинарную операцию на  $F(A)$ : пусть  $X = x_1 \dots x_k, Y = y_1 \dots y_m$ .

Если  $x_k \neq y_1^{-1}$ , то  $XY$  - конкатенация (приписывание)  $X$  и  $Y$ :

$$XY = x_1 \dots x_k y_1 \dots y_m, |XY| = k + m.$$

Если  $x_k = y_1^{-1}$ , то  $XY$  - результат полного сокращения слова  $x_1 \dots x_k y_1 \dots y_m$ .

**Пример.**  $(abcd a^{-1} b)(b^{-1} a d^{-1} a a b) = abcaab$ .

**Определение.** Если  $|X| = 0$ , то  $X$  называется пустым словом (обозначим  $\lambda$ ).

Пустое слово по определению несократимо и лежит в  $F(A)$ .

**Теорема.**  $F(A)$  с приведённой выше бинарной операцией - группа.

*Доказательство.*

1. Ассоциативность:

Пусть  $X = x_1 \dots x_k, Z = z_1 \dots z_m$ .

Случай  $|Y| = 0 \implies Y = \lambda$  очевиден ( $XZ = XZ$ );

Индукция по длине слова  $Y$ :

База индукции:  $|Y| = 1 \implies Y = a \in A^{\pm 1}$ . Индукция по  $|X| + |Z|$ :

База внутренней индукции:

$|X| + |Z| = 0$  - очевидно ( $a = a$ );

$|X| + |Z| = 1$  - очевидно (одно из слов  $X, Z$  пустое);

Шаг внутренней индукции ( $k + m - 2 \rightarrow k + m$ ) - рассмотрим случаи:

- $a^{-1} \neq x_k, a^{-1} \neq z_1 : X(YZ) = x_1 \dots x_k a z_1 \dots z_m = (XY)Z$ ;
- $a^{-1} = x_k, a^{-1} \neq z_1 : X(aZ) = X(a z_1 \dots z_m) =$   
= результат полного сокращения  $x_1 \dots x_{k-1} a^{-1} a z_1 \dots z_m =$   
= результат полного сокращения  $x_1 \dots x_{k-1} z_1 \dots z_m = (Xa)Z$ ;
- $a^{-1} \neq x_k, a^{-1} = z_1$  - аналогично предыдущему;
- $a^{-1} = x_k, a^{-1} = z_1$ : пусть  $X = X' a^{-1}, Z = a^{-1} Z'$ . Тогда:  
 $X(aZ) = X(a(a^{-1} Z')) = XZ' = (X' a^{-1}) Z'$   
 $(Xa)Z = (X' a^{-1} a)Z = X' Z = X'(a^{-1} Z')$   
При этом  $|X'| + |Y'| = k + m - 2$ , то есть  $X'(a^{-1} Z') = (X' a^{-1}) Z'$  по предположению внутренней индукции.

Во всех случаях  $X(aZ) = (Xa)Z \implies$  база доказана.

Шаг индукции: Пусть  $Y = y_1 \dots y_l$ . Тогда:

$$\begin{aligned} X(YZ) &= X(y_1 \dots y_l \cdot Z) = X((y_1 \dots y_{l-1} \cdot y_l)Z) \stackrel{1}{=} X((y_1 \dots y_{l-1}) \cdot (y_l Z)) \stackrel{2}{=} \\ &\stackrel{2}{=} ((X \cdot y_1 \dots y_{l-1}) y_l) Z \stackrel{3}{=} (X \cdot y_1 \dots y_l) Z = (XY)Z \end{aligned}$$

1, 3 - из утверждения базы индукции; 2 - по предположению индукции.

2.  $\lambda$  - нейтральный элемент;

3. обратный элемент к  $x_1 \dots x_k$  - элемент  $x_k^{-1} \dots x_1^{-1}$ .

□

**Определение.** Построенная группа  $F(A)$  называется свободной группой с базисом  $A$ . ( $A$  также называется свободной порождающей системой группы).

Любая группа, изоморфная  $F(A)$ , также называется свободной.

**Утверждение.** Пусть  $H \leq SL_2(\mathbb{Z}) : H = \langle \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \rangle$ .

Тогда  $H \simeq F(A)$  с базисом  $A = \{a, b\}$ .

*Доказательство.* Без доказательства. □

**Утверждение.** Все базисы свободной группы равномощны.

*Доказательство.* Без доказательства. □

**Определение.** Ранг свободной группы - мощность её базиса.

*Замечание.* Заметим, что в  $F(A)$  результат умножения определён однозначно  $\implies$  однозначно определён элемент  $x_1 \cdot \dots \cdot x_k$ , где  $x_i \in A^{\pm 1}$ .

Тогда если считать слово  $x_1 \dots x_k$  результатом умножения  $x_1 \cdot \dots \cdot x_k$ , то можно опускать знак умножения, и в этом смысле работать и с сократимыми словами.

**Пример.**  $abb^{-1}ba^{-1}a = a \cdot b \cdot b^{-1} \cdot b \cdot a^{-1} \cdot a = ab \in F(A)$ .

**Теорема 1** (Универсальное свойство свободной группы).

Пусть  $G$  - группа,  $\{g_i \mid i \in I\} \subset G$  - произвольное множество её элементов.

Рассмотрим свободную группу  $F(A)$  с базисом  $A = \{a_i \mid i \in I\}$ .

Тогда отображение  $\varphi : a_i \mapsto g_i$  продолжается до гомоморфизма  $\varphi : F(A) \rightarrow G$ , причём единственным образом.

*Доказательство.* Пусть  $W = a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k}$  - несократимое слово из  $F(A)$ , где  $\varepsilon_i = \pm 1, a_{i_j} \in A$ . Зададим  $\varphi : F(A) \rightarrow G$  по правилу  $\varphi(W) = g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k}$ .

Проверим, что  $\varphi$  - гомоморфизм ( $W, \tilde{W} \in F(A), W = a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k}, \tilde{W} = a_{j_1}^{\tau_1} \dots a_{j_m}^{\tau_m}$ ):

$$\begin{aligned} \varphi(W\tilde{W}) &= \varphi(a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k} \cdot a_{j_1}^{\tau_1} \dots a_{j_m}^{\tau_m}) = g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k} \cdot g_{j_1}^{\tau_1} \dots g_{j_m}^{\tau_m} = \\ &= (g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k}) \cdot (g_{j_1}^{\tau_1} \dots g_{j_m}^{\tau_m}) = \varphi(W)\varphi(\tilde{W}) \end{aligned}$$

Единственность такого гомоморфизма очевидна:

$\varphi(a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k}) = \varphi(a_{i_1})^{\varepsilon_1} \dots \varphi(a_{i_k})^{\varepsilon_k} = g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k}$  - определено однозначно. □

**Пример.** (несвободной группы)

$S_3 = \langle (12), (123) \rangle : \forall g \in S_3 \ g^6 = id$ . Попытаемся продолжить до гомоморфизма  $S_3 \rightarrow Q_8$  отображение  $\varphi : (12) \mapsto i, (123) \mapsto j$ :

$-1 = i^2 = \varphi((12))^2 = \varphi((12)^2) = \varphi(id) = 1$  - противоречие.

**Следствие 1.** Пусть  $G$  - группа,  $M = \{g_i \mid i \in I\}$  - порождающее множество  $G$ ,  $F(A)$  - свободная группа с базисом  $A = \{a_i \mid i \in I\}$ .

Тогда  $\exists!$  сюръективный гомоморфизм  $\varphi : F(A) \rightarrow G$  такой, что  $\forall i \in I : \varphi(a_i) = g_i$ .

*Доказательство.* Достаточно показать, что в этом случае гомоморфизм из доказательства теоремы сюръективен - это следует из того, что множество  $\{g_i \mid i \in I\}$  порождает группу  $G$  (каждый элемент представим как  $g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k} = \varphi(a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k})$ ).  $\square$

**Следствие 2.** Любая группа  $G$  изоморфна факторгруппе некоторой свободной группы по некоторой её нормальной подгруппе.

*Доказательство.* Пусть  $\varphi : F(A) \rightarrow G$  - гомоморфизм из следствия 1.

Так как  $\text{Ker } \varphi \trianglelefteq F(A)$ , из теоремы о гомоморфизме  $G = \text{Im } \varphi \simeq F(A)/\text{Ker } \varphi$ .  $\square$

**Определение.** Сюръективный гомоморфизм  $\varphi : F(A) \rightarrow G$  - из следствия 1 называется копредставлением группы  $G$ .

*Замечание.* Копредставление зависит от выбора порождающего множества  $M$ .

## 2.1 Задание группы порождающими и определяющими соотношениями

По следствию 2:  $G \simeq F(A)/N$ , где  $N \trianglelefteq F(A)$ . Отсюда задание группы  $G$  сводится к заданию  $A$  и  $N$ .

$N$  - нормальная  $\implies \forall f \in F(A), \forall h \in N : fhf^{-1} \in N$ .

**Определение.** Пусть  $\mathcal{R} \subseteq F(A)$ . Нормальным замыканием множества  $\mathcal{R}$  в группе  $F(A)$  называется наименьшая (по включению) нормальная подгруппа, содержащая  $\mathcal{R}$ . Обозначается  $\langle\langle \mathcal{R} \rangle\rangle^{F(A)}$

**Утверждение.**

$$\langle\langle \mathcal{R} \rangle\rangle^{F(A)} = \{(f_1 r_1^{\varepsilon_1} f_1^{-1}) \dots (f_k r_k^{\varepsilon_k} f_k^{-1}) \mid r_i \in \mathcal{R}, f_i \in F(A), \varepsilon_i = \pm 1\}$$

*Доказательство.*

Пусть  $\{(f_1 r_1^{\varepsilon_1} f_1^{-1}) \dots (f_k r_k^{\varepsilon_k} f_k^{-1}) \mid r_i \in \mathcal{R}, f_i \in F(A), \varepsilon_i = \pm 1\} = H$ . Тогда:

$$\langle\langle \mathcal{R} \rangle\rangle^{F(A)} \trianglelefteq F(A) \implies \forall r_i \in \mathcal{R}, f_i \in F(A), \varepsilon_i \in \{\pm 1\} : f_i r_i^{\varepsilon_i} f_i^{-1} \in \langle\langle \mathcal{R} \rangle\rangle^{F(A)} \implies H \subseteq \langle\langle \mathcal{R} \rangle\rangle^{F(A)}. \text{ Осталось показать, что } H \trianglelefteq F(A):$$

$$\begin{aligned} \forall h \in H, g \in F(A) : ghg^{-1} &= g(f_1 r_1^{\varepsilon_1} f_1^{-1}) \dots (f_k r_k^{\varepsilon_k} f_k^{-1}) g^{-1} = \\ &= ((gf_1) r_1^{\varepsilon_1} (f_1^{-1} g^{-1})) \dots ((gf_k) r_k^{\varepsilon_k} (f_k^{-1} g^{-1})) = \\ &= ((gf_1) r_1^{\varepsilon_1} (gf_1)^{-1}) \dots ((gf_k) r_k^{\varepsilon_k} (gf_k)^{-1}) \in H \end{aligned}$$

Отсюда минимальная группа, содержащая  $\mathcal{R}$ , в точности равна  $H$ .  $\square$



**Утверждение.** Любую нормальную подгруппу  $N \trianglelefteq F(A)$  можно задать как  $N = \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$  для подходящего  $\mathcal{R} \subset F(A)$ .

*Доказательство.* Очевидно, подойдёт  $\mathcal{R} = N$ . □

**Элементарные преобразования над словами в  $F(A)$ :**

(под словами в  $F(A)$  подразумеваются любые произведения букв, а не только элементы  $F(A)$ )

- ЭП1:  $W = W_1 a^\varepsilon a^{-\varepsilon} W_2 \mapsto \tilde{W} = W_1 W_2$ , где  $a \in A, \varepsilon = \pm 1$ ;
- ЭП2:  $W = W_1 r^\varepsilon W_2 \mapsto \tilde{W} = W_1 W_2$ , где  $r \in \mathcal{R}, \varepsilon = \pm 1$ ;
- ЭП1' - обратное к ЭП1;
- ЭП2' - обратное к ЭП2;

**Определение.** Назовём слова  $W$  и  $\tilde{W}$   $\mathcal{R}$ -эквивалентными, если от  $W$  можно с помощью ЭП перейти к  $\tilde{W}$ .

**Утверждение.**  $\mathcal{R}$ -эквивалентность - отношение эквивалентности.

*Доказательство.*

- Рефлексивность - очевидно;
- Симметричность - следует из обратимости каждого ЭП;
- Транзитивность - очевидно;

□

**Теорема 2.** Следующие условия эквивалентны:

1.  $W \in \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$ ;
2.  $W$   $\mathcal{R}$ -эквивалентно пустому слову  $\lambda$ ;
3. Если для произвольной группы  $G$  с порождающим множеством  $M = \{g_i \mid i \in I\}$  (т.е. заданным копредставлением  $\varphi : F(A) \rightarrow G$ ) верно, что  $\forall r \in \mathcal{R} : \varphi(r) = 1$  в  $G$ , то  $\varphi(W) = 1$  в  $G$ .

*Доказательство.*

- $1 \implies 2$  :  $W \in \langle\langle \mathcal{R} \rangle\rangle^{F(A)} \implies W = (f_1 r_1^{\varepsilon_1} f_1^{-1}) \dots (f_k r_k^{\varepsilon_k} f_k^{-1}) \xRightarrow{\text{ЭП2}} W \sim \tilde{W} = (f_1 f_1^{-1}) \dots (f_k f_k^{-1}) \xRightarrow{\text{ЭП1}} \lambda$ ;

- $2 \implies 3$  Пусть  $\varphi : F(A) \rightarrow G$  взят из условия теоремы. Покажем, что при ЭП образ слова не меняется:

1.  $\varphi(W_1 a^\varepsilon a^{-\varepsilon} W_2) = \varphi(W_1) \varphi(a)^\varepsilon \varphi(a)^{-\varepsilon} \varphi(W_2) = \varphi(W_1) \varphi(W_2) = \varphi(W_1 W_2)$ ;
2.  $\varphi(W_1 r^\varepsilon W_2) = \varphi(W_1) \varphi(r)^\varepsilon \varphi(W_2) = \varphi(W_1) \cdot 1^\varepsilon \cdot \varphi(W_2) = \varphi(W_1 W_2)$ ;

При ЭП, обратных этим, образ слова аналогично не изменяется.

Тогда если  $W \underset{\text{ЭП}}{\sim} \lambda$ , то  $\varphi(W) = \varphi(\lambda) = 1$ .

- $3 \implies 1$  :  $\forall r \in \mathcal{R} : \varphi(r) = 1 \implies r \in \text{Ker } \varphi$ ;  $\varphi(W) = 1 \implies W \in \text{Ker } \varphi$ .

Рассмотрим в качестве  $G$  группу  $F(A)/N$ , где  $N = \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$ , а в качестве  $\varphi$  -  $\pi$  (естественный гомоморфизм  $F(A) \rightarrow F(A)/N$ ).

$r \in N \implies \pi(r) = 1$ . Тогда по условию 3:  $\pi(W) = 1 \implies W \in \text{Ker } \varphi = N$ .

□

**Определение.** Если  $W \in F(A)$  удовлетворяет любому из условий теоремы 2, то говорят, что соотношение  $W = 1$  следует из соотношений  $\{r = 1 \mid r \in \mathcal{R}\}$  или является следствием соотношений  $\mathcal{R}$ .

**Определение.** Рассмотрим копредставление произвольной группы  $G$ , т.е.  $\varphi : F(A) \rightarrow G$ , где  $A = \{a_i \mid i \in I\}$ . Пусть слово  $W \in F(A)$  ( $W = a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k}$ ) такое, что  $\varphi(W) = g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k} = 1$  в  $G$ .

Тогда говорят о соотношении  $W = 1$ .

(Для упрощения записи вместо  $g_i$  пишут  $a_i$ ).

**Определение.** Множество  $\mathcal{R} \subset F(A)$  называется определяющим множеством соотношений группы  $G$ , если любое соотношение группы  $G$  следует из  $\mathcal{R}$ .

При этом элементы  $\mathcal{R}$  называются определяющими соотношениями  $G$ . Обозначается  $G = \langle A \mid \mathcal{R} \rangle$  (данная запись также называется копредставлением  $G$ ).

**Примеры.**

1.  $\mathbb{Z}_3 = \langle a \mid a^3 = 1 \rangle$ ;  $a^{12} = 1$  - следствие;
2.  $V_4 = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$ ;  $(ab)^2 = 1$  - следствие.

**Теорема** (Теорема Дика).

Пусть  $G$  - группа, заданная копредставлением  $\langle A \mid R \rangle$ , где  $A = \{a_i \mid i \in I\}$ .

Пусть  $H$  - произвольная группа,  $\{h_i \mid i \in I\} \subset H$  - произвольное множество её элементов.

Тогда отображение  $\varphi$  на порождающих  $\varphi : a_i \mapsto h_i \forall i \in I$  продолжается до

гомоморфизма  $\varphi : G \rightarrow H$  тогда и только тогда, когда  $\forall r \in \mathcal{R} : \varphi(r) = 1$  в  $H$ .

*Доказательство.* Если  $\varphi : a_i \mapsto h_i$  и  $\varphi$  - гомоморфизм, то должно выполняться  $\varphi(a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k}) = h_{i_1}^{\varepsilon_1} \dots h_{i_k}^{\varepsilon_k}$ . Если это отображение корректно, то очевидно, что оно является искомым гомоморфизмом. Покажем корректность:

Пусть  $W = \tilde{W}$  в  $G$ . Тогда  $\tilde{W}W^{-1} = 1$  в  $G \implies \tilde{W}W^{-1} \in \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$  (так как по определению копредставления соотношение  $\tilde{W}^{-1}W = 1$  следует из  $R$ ).

Отсюда  $\tilde{W}W^{-1} \sim \lambda \implies W \sim \tilde{W}W^{-1}W = \tilde{W}$ . Из размышлений доказательства перехода  $2 \implies 3$  теоремы 2 видно, что из условия  $\forall r \in \mathcal{R} : \varphi(r) = 1$  в  $H$  следует, что образ не изменяется при ЭП, то есть  $\varphi(W) = \varphi(\tilde{W})$ , т.е. отображение корректно.  $\square$