



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: 6 октября 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
<b>3</b>	<b>Прямое произведение групп</b>	<b>27</b>
3.1	Внешнее прямое произведение . . . . .	27
3.2	Внутреннее прямое произведение . . . . .	28
3.3	Связь между внутренним и внешним прямым произведением . . . . .	31
<b>4</b>	<b>Конечнопорождённые абелевы группы</b>	<b>33</b>
4.1	Связь между базисами свободной абелевой группы . . . . .	37
4.2	Элементарные преобразования свободных абелевых групп . . . . .	38
4.3	Согласованные базисы свободной абелевой группы и её подгруппы . . . . .	41

# 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.* Для групп конечного порядка, очевидно, выполняется и обратное утверждение: если  $\text{ord } g = |G| < \infty$ , то  $G = \langle g \rangle$ .

Далее циклическую группу порядка  $n$  будем обозначать  $\langle g \rangle_n$ .

**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.

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

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:

$$g^m = (g^k)^q \cdot g^r \implies g^r = (g^k)^{-q} \cdot g^m$$

то есть  $g^r \in H$ , а в силу того, что  $k$  - наименьшее натуральное число такое, что  $g^k \in H$ , имеем  $r = 0$ . Значит,  $g^m = (g^k)^q$ , а отсюда  $H = \langle g^k \rangle$ .

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

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

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

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

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

□

**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).

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

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

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

(Верны аналогичные утверждения для правых смежных классов)

*Доказательство.*

$$1. \text{ Очевидно;}$$

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

Аналогично  $bH \subseteq aH \implies aH = bH$ .

3.  $\implies$ :  $aH = bH \implies a \in bH (a \in aH) \implies \exists h \in H : a = bh \implies b^{-1}a = h \in H$   
 $\impliedby$ :  $b^{-1}a = h \in H \implies a = bh \implies aH = bH$  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:  $a^{-1}a = e \in H \implies a \equiv a \pmod{H}$ ;
- 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:  $a \equiv b, b \equiv c \pmod{H} \implies c^{-1}b, b^{-1}a \in H \implies c^{-1}b \cdot b^{-1}a = c^{-1}a \in H \implies a \equiv c \pmod{H}$ .

Совпадение классов эквивалентности с левыми смежными классами следует из пункта 3 предыдущего утверждения. □

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

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

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

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

**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  $G \simeq V_4$ . □

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

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

**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.

$\square$

**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,  $\forall g \in G : gH = Hg \implies H \trianglelefteq G$ .  $\square$



## 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.  $\square$

## 3 Прямое произведение групп

### 3.1 Внешнее прямое произведение

Пусть  $G_1, \dots, G_k$  - группы.

$$G = G_1 \times \dots \times G_k = \{(g_1, \dots, g_k) | g_i \in G_i\}.$$

$$(g_1, \dots, g_k) \cdot (\tilde{g}_1, \dots, \tilde{g}_k) = (g_1 \tilde{g}_1, \dots, g_k \tilde{g}_k)$$

( $g_i \tilde{g}_i$  перемножаются по правилу бинарной операции на  $G_i$ ).

**Утверждение.**  $(G, \cdot)$  - группа.

*Доказательство.*

1.  $(a_1, \dots, a_k)((b_1, \dots, b_k)(c_1, \dots, c_k)) = (a_1(b_1 c_1), \dots, a_k(b_k c_k)) = ((a_1 b_1) c_1, \dots, (a_k b_k) c_k) = ((a_1, \dots, a_k)(b_1, \dots, b_k))(c_1, \dots, c_k)$
2. Нейтральный элемент -  $(e_1, \dots, e_k)$  ( $e_i$  - нейтральный в  $G_i$ )
3.  $(g_1, \dots, g_k)^{-1} = (g_1^{-1}, \dots, g_k^{-1})$

□

**Определение.** Данная группа  $(G, \cdot)$  называется прямым произведением групп  $G_1, \dots, G_k$ . Обозначается  $G = G_1 \times \dots \times G_k$ ;  $G_i$  называются множителями.

В аддитивной терминологии те же рассуждения определяют прямую сумму  $G = G_1 \oplus \dots \oplus G_k$ , где  $G_i$  - слагаемые.

**Примеры.**

1.  $G_1 = \mathbb{Z}_3, G_2 = S_3, G = G_1 \times G_2$ .  
 $(1, (12)) \cdot (2, (13)) = (1 + 2, (12)(13)) = (0, (132)).$
2.  $D_n(\mathbb{F}) \simeq \underbrace{\mathbb{F}^* \times \dots \times \mathbb{F}^*}_n$  ( $D_n(\mathbb{F})$  - группа диагональных матриц порядка  $n$ ).

**Утверждение.**

1. Если  $(m, n) = 1$ , то  $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{nm}$  - циклическая группа;
2. Если  $(m, n) \neq 1$ , то  $\mathbb{Z}_m \times \mathbb{Z}_n$  - не циклическая.

*Доказательство.*

1. Обозначим за  $[a]_s \in \mathbb{Z}_s$  класс вычетов по модулю  $s$ , содержащий  $a$ .

Рассмотрим отображение  $\varphi : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  такое, что  $\varphi : [a]_{mn} \mapsto ([a]_m, [a]_n)$ . Очевидно, что это гомоморфизм:

$$\varphi([a]_{mn} \cdot [b]_{mn}) = ([ab]_m, [ab]_n) = ([a]_m, [a]_n)([b]_m, [b]_n) = \varphi([a]_{mn})\varphi([b]_{mn})$$

Найдём  $\text{Ker } \varphi$  :

$$\varphi([a]_{mn}) = ([0]_m, [0]_n) \iff \begin{cases} m \mid a \\ n \mid a \end{cases} \xRightarrow{(m,n)=1} mn \mid a \implies \text{Ker } \varphi = \{[0]_{mn}\}$$

По теореме о гомоморфизме  $\text{Im } \varphi = \mathbb{Z}_{mn}/\text{Ker } \varphi = \mathbb{Z}_{mn} \implies |\text{Im } \varphi| = mn$ .

Так как  $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$  и  $\text{Im } \varphi \leq \mathbb{Z}_m \times \mathbb{Z}_n$ ,  $\text{Im } \varphi = \mathbb{Z}_m \times \mathbb{Z}_n$ .

Отсюда  $\varphi$  - биекция (инъекция из  $\text{Ker } \varphi = \{e\}$ ), т.е.  $\varphi$  - изоморфизм.

2. Пусть  $(m, n) = d \neq 1$  ( $m = dk_1, n = dk_2$ ). Тогда  $\forall g = (g_1, g_2) \in \mathbb{Z}_m \times \mathbb{Z}_n$ :

$$(g_1, g_2)^{dk_1k_2} = (g_1^{dk_1k_2}, g_2^{dk_1k_2}) = (0^{k_2}, 0^{k_1}) = (0, 0)$$

Отсюда  $\text{ord } (g_1, g_2) = dk_1k_2 = \frac{mn}{d} < mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$ . Значит,  $\mathbb{Z}_m \times \mathbb{Z}_n$  не является циклической.

□

**Следствие.** Пусть  $n = p_1^{s_1} \dots p_k^{s_k}$  - разложение на простые множители. Тогда  $\mathbb{Z}_n = \mathbb{Z}_{p_1^{s_1}} \times \dots \times \mathbb{Z}_{p_k^{s_k}}$ .

*Доказательство.* Очевидно следует из теоремы.

□

**Следствие.** (Китайская теорема об остатках) Если числа  $a_1, \dots, a_n$  попарно взаимно просты, то для любых целых  $r_1, \dots, r_n$  ( $0 \leq r_i < n$ )  $\exists! N$  ( $0 \leq N < a_1 \cdot \dots \cdot a_n$ ) такой, что  $N \equiv r_i \pmod{a_i}$

*Доказательство.* Из теоремы следует, что  $\mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n} \simeq \mathbb{Z}_a$  ( $a = a_1 \cdot \dots \cdot a_n$ ). Это означает, что набор остатков  $(r_1, \dots, r_n) \in \mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n}$  изоморфизм из теоремы однозначно переводит в элемент  $N \in \mathbb{Z}_a$  такой, что  $r_i = [N]_{a_i}$ , что и требовалось.

□

## 3.2 Внутреннее прямое произведение

**Определение.** Пусть  $G$  - группа,  $H_1, \dots, H_k \leq G$ .

$G$  раскладывается в прямое произведение подгрупп  $H_1, \dots, H_k$ , если:

1.  $\forall g \in G \exists! h_i \in H_i : g = h_1 \dots h_k$ ;
2.  $\forall i \neq j : \forall h_i \in H_i, h_j \in H_j \ h_i h_j = h_j h_i$ .

Обозначается  $G = H_1 \times \dots \times H_k$  ( $G = H_1 \oplus \dots \oplus H_k$  в аддитивной терминологии).

*Замечание.* Из определения следует, что  $(h_1 \dots h_k)(\tilde{h}_1 \dots \tilde{h}_k) = (h_1 \tilde{h}_1) \dots (h_k \tilde{h}_k)$ .

**Определение.** Пусть  $H, N \leq G$ . Обозначим  $NH = \{nh | n \in N, h \in H\}$

**Утверждение.** Пусть  $N \trianglelefteq G, H \leq G$ . Тогда  $NH$  - подгруппа в  $G$ , причём  $NH = HN$ .

*Доказательство.* Рассмотрим  $(n_1 h_1)(n_2 h_2) = n_1 \underbrace{(h_1 n_2 h_1^{-1})}_{=\tilde{n}} \underbrace{h_1 h_2}_{=\tilde{h}} = \tilde{n} \tilde{h} \in NH$ .

$e \in N \cap H \implies e \cdot e = e \in NH$ .

$(nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h \in NH$ .

Отсюда  $NH$  - подгруппа. Покажем, что  $NH = HN$ :

$$\forall nh \in NH : nh = (hh^{-1})nh = h(h^{-1}nh) \in HN \implies NH \subseteq HN$$

$$\forall hn \in HN : hn = hn(h^{-1}h) = (hnh^{-1})h \in NH \implies HN \subseteq NH$$

Отсюда  $NH = HN$ . □

**Лемма 1.** Пусть  $H, N \trianglelefteq G, H \cap N = \{e\}$ . Тогда  $\forall h \in H, n \in N \ nh = hn$ .

*Доказательство.* Рассмотрим выражение  $(hn)(nh)^{-1} = hnh^{-1}n^{-1}$ :

$$hnh^{-1}n^{-1} = h(nh^{-1}n^{-1}) \in H; \quad hnh^{-1}n^{-1} = (hnh^{-1})n^{-1} \in N$$

Значит,  $hnh^{-1}n^{-1} \in H \cap N = \{e\} \implies (hn)(nh)^{-1} = e \implies hn = nh$  □

**Теорема 1.** Пусть  $H_1, H_2 \leq G$ . Тогда  $G = H_1 \times H_2 \iff \begin{cases} (1) \ H_1, H_2 \trianglelefteq G \\ (2) \ H_1 \cap H_2 = \{e\} \\ (3) \ G = H_1 H_2 \end{cases}$

*Доказательство.*

$\implies$ : Пусть  $G = H_1 \times H_2$ .

(3) - очевидно из пункта 1 определения.

(1):  $\forall h_1 \in H_1, g \in G : g = \tilde{h}_1 \tilde{h}_2 \ (\tilde{h}_1 \in H_1, \tilde{h}_2 \in H_2) \implies$

$$gh_1 g^{-1} = \tilde{h}_1 (\tilde{h}_2 h_1 \tilde{h}_2^{-1}) \tilde{h}_1^{-1} \underset{(2 \text{ из опр})}{=} \tilde{h}_1 h_1 \tilde{h}_1^{-1} \in H_1$$

Отсюда  $H_1 \trianglelefteq G$  (аналогично  $H_2 \trianglelefteq G$ ).

(2): Пусть  $\exists h \in H_1 \cap H_2$ . Тогда  $h = he = eh$  - два разложения на произведение

элементов подгрупп. Они совпадают только в случае  $h = e$ , т.е.  $H_1 \cap H_2 = \{e\}$ .

$\Leftarrow$ : Пусть даны условия (1) - (3).

По лемме 1 из (1), (2) очевидно следует пункт 2 определения.

Из (3):  $\forall g \in G \exists h_i \in H_i : g = h_1 h_2$ .

Допустим, что это разложение не единственно, т.е.  $h_1 h_2 = \tilde{h}_1 \tilde{h}_2$ .

Тогда  $\tilde{h}_1^{-1} h_1 = \tilde{h}_2 h_2^{-1}$ , а так как  $H_1 \cap H_2 = \{e\}$ , имеем  $h_1 = \tilde{h}_1, h_2 = \tilde{h}_2$ .  $\square$

**Теорема 2.** Пусть  $H_1, \dots, H_k \leq G$ .

$$\text{Тогда } G = H_1 \times \dots \times H_k \iff \begin{cases} (1) H_1, \dots, H_k \leq G \\ (2) \forall i H_i \cap \langle H_j \mid j \neq i \rangle = \{e\} \\ (3) G = H_1 \dots H_k \end{cases}$$

*Доказательство.*

$\Rightarrow$ : Пусть  $G = H_1 \times \dots \times H_k$ .

(3) - очевидно из пункта 1 определения.

(1):  $\forall h_i \in H_i, g \in G : g = \tilde{h}_1 \dots \tilde{h}_k (\tilde{h}_i \in H_i) \Rightarrow$

$$gh_1 g^{-1} = (\tilde{h}_1 \dots \tilde{h}_k) h_i (\tilde{h}_k^{-1} \dots \tilde{h}_1^{-1}) \underset{(2 \text{ из опр})}{=} \tilde{h}_i h_i \tilde{h}_i^{-1} \in H_i$$

Отсюда  $H_i \leq G$ .

(2): Пусть  $\exists h \in H_i \cap \langle H_j \mid j \neq i \rangle$ . Тогда  $h = he = eh$  - два разложения на произведение элементов подгрупп. Они совпадают только в случае  $h = e$ , т.е.  $H_i \cap \langle H_j \mid j \neq i \rangle = \{e\}$ .

$\Leftarrow$ : Пусть даны условия (1) - (3).

По лемме 1 из (1), (2) очевидно следует пункт 2 определения.

Из (3):  $\forall g \in G \exists h_i \in H_i : g = h_1 \dots h_k$ .

Допустим, что это разложение не единственно, т.е.  $h_1 \dots h_k = \tilde{h}_1 \dots \tilde{h}_k$ .

Тогда  $\forall i : \tilde{h}_i^{-1} h_i = \prod_{j \neq i} \tilde{h}_j h_j^{-1}$ , а так как  $H_i \cap \langle H_j \mid j \neq i \rangle = \{e\}$ , имеем  $h_i = \tilde{h}_i$ .  $\square$

**Примеры.**

$$1. V_4 = \{e, a, b, c\} = \{e, a\} \times \{e, b\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2;$$

$$2. \mathbb{C}^* = \mathbb{R}_+ \times U \ (z = r \cdot e^{iy}).$$

3.  $\mathbb{Z}$  не раскладывается в произведение нетривиальных подгрупп.

Предположим противное, т.е.  $\mathbb{Z} = H_1 \times \dots \times H_m$ . Подгруппы  $\mathbb{Z}$  имеют вид  $k\mathbb{Z}$ , т.е.  $\mathbb{Z} = k_1 \mathbb{Z} \times \dots \times k_m \mathbb{Z}, k_i \neq 0$ . Но тогда  $k_1 k_2 \in H_1 \cap H_2$  и  $k_1 k_2 \neq 0$ , что противоречит теореме 2.

### 3.3 Связь между внутренним и внешним прямым произведением

#### Теорема 3.

1. Если группа  $G$  раскладывается в прямое произведение подгрупп  $H_1, \dots, H_k$ , то  $G$  изоморфна прямому произведению групп  $G_1, \dots, G_k$ , где  $\forall i \ G_i \simeq H_i$ ;
2. Если группа  $G$  изоморфна прямому произведению групп  $G_1, \dots, G_k$ , то  $\exists H_i \leq G$  такие, что  $G_i \simeq H_i$  и  $G$  раскладывается в прямое произведение  $H_1, \dots, H_k$ .

*Доказательство.*

1. Имеем:  $H_i \leq G, G = H_1 \times \dots \times H_k$ .

Рассмотрим отображение  $\varphi : G \rightarrow G_1 \times \dots \times G_k$ , где  $G_i = H_i$ , такое, что  $\forall g = h_1 \dots h_k \in G \ \varphi(h_1 \dots h_k) \mapsto (h_1, \dots, h_k)$ . Это изоморфизм:

- Биекция - очевидна;
- Гомоморфизм:

$$\begin{aligned} \varphi((h_1 \dots h_k) \cdot (h'_1 \dots h'_k)) &= \varphi(h_1 h'_1 \dots h_k h'_k) = (h_1 h'_1, \dots, h_k h'_k) = \\ &= (h_1, \dots, h_k) \cdot (h'_1, \dots, h'_k) = \varphi(h_1 \dots h_k) \cdot \varphi(h'_1 \dots h'_k) \end{aligned}$$

2. Имеем:  $G_1, \dots, G_k$  - группы,  $G = \{(g_1, \dots, g_k) \mid g_i \in G_i\}$ .

Тогда  $H_i = \{(e, \dots, e, g_i, e, \dots, e) \mid g_i \in G_i\}$  очевидно является подгруппой  $G$ , изоморфной  $G_i$ .

Покажем, что  $G = H_1 \times \dots \times H_k$ :

- $\forall g = (g_1, \dots, g_k) \in G \ \exists! \ h_i = (e, \dots, e, g_i, e, \dots, e) : g = h_1 \dots h_k$ ;
- $\forall i \neq j, h_i = ((e, \dots, e, a_i, e, \dots, e)) \in H_i, h_j = (e, \dots, e, b_j, e, \dots, e) \in H_j :$

$$h_i h_j = (e, \dots, e, a_i, e, \dots, e, b_j, e, \dots, e) = h_j h_i$$

□

**Теорема 4.** Пусть  $H_i \leq G, G = H_1 \times \dots \times H_k, N_i \leq H_i$ . Тогда:

1.  $N_1 \times \dots \times N_k \leq G$ ;
2.  $G/(N_1 \times \dots \times N_k) \simeq (H_1/N_1) \times \dots \times (H_k/N_k)$ .

*Доказательство.*



1. Очевидно, что  $N_1 \times \dots \times N_k = N \leq G$ .

Покажем нормальность:  $\forall g = h_1 \dots h_k \in G, n = n_1 \dots n_k \in N$

$$gng^{-1} = (h_1 \dots h_k)(n_1 \dots n_k)(h_k^{-1} \dots h_1^{-1}) \underset{(n_i \in H_i)}{=} \overset{\in N_1}{(h_1 n_1 h_1^{-1})} \dots \overset{\in N_k}{(h_k n_k h_k^{-1})} \in N$$

2. Рассмотрим гомоморфизм  $\varphi : G \rightarrow (H_1/N_1) \times \dots \times (H_k/N_k)$  такой, что  $\varphi : h_1 \dots h_k \mapsto (h_1 N_1, \dots, h_k N_k)$ . Это сюръективный гомоморфизм, причём  $\text{Ker } \varphi = N_1 \times \dots \times N_k$ . Отсюда по теореме о гомоморфизме получаем необходимое утверждение.

□

**Следствие.** Если  $G = H_1 \times H_2$ , то  $G/H_1 \simeq H_2, G/H_2 \simeq H_1$ .

## 4 Конечнопорождённые абелевы группы

*Замечание.* В данном разделе используется аддитивная терминология:

$(A, +)$  - абелева группа,  $\forall a \in A, n \in \mathbb{Z}$ :

$$na = \begin{cases} \underbrace{a + \dots + a}_n, & n > 0; \\ 0, & a = 0; \\ \underbrace{(-a) + \dots + (-a)}_{|n|}, & n < 0 \end{cases}$$

**Свойства.**  $(\forall a, b \in A, n, m \in \mathbb{Z})$

$$1. (n + m)a = na + ma;$$

$$2. n(a + b) = na + nb;$$

$$3. (nm)a = n(ma)$$

*Доказательство.* Непосредственный разбор случаев - знаков  $m, n$ . □

**Определение.** (Целочисленной) линейной комбинацией элементов  $a_1, \dots, a_k \in A$  называется выражение  $n_1a_1 + \dots + n_ka_k$  ( $n_i \in \mathbb{Z}$ ).

Если элемент  $b \in A$  равен некоторой линейной комбинации  $a_1, \dots, a_k \in A$ , то говорят, что  $b$  выражается через  $a_1, \dots, a_k$ .

**Определение.** Система элементов  $a_1, \dots, a_k$  называется линейно зависимой, если  $\exists n_1, \dots, n_k \in \mathbb{Z}$ , не все равные 0, такие, что  $n_1a_1 + \dots + n_ka_k = 0$ .

В противном случае система  $a_1, \dots, a_k$  называется линейно независимой.

**Пример.**  $A = \mathbb{Z}_3 \oplus \mathbb{Z}_4$ . Система из одного элемента  $(1, 1)$  - линейно зависима:  $12 \cdot (1, 1) = (0, 0)$

**Определение.** Пусть  $A$  - абелева группа,  $a_1, \dots, a_k \in A$ .

Будем обозначать  $\langle a_1, \dots, a_k \rangle = \{n_1a_1 + \dots + n_ka_k \mid n_i \in \mathbb{Z}\}$

(для бесконечного числа  $a_k$  - всевозможные конечные линейные комбинации)

**Утверждение.**  $\langle a_1, \dots, a_k \rangle$  - наименьшая подгруппа  $A$ , содержащая  $a_1, \dots, a_k$ .

*Доказательство.* Пусть  $H$  - наименьшая подгруппа, содержащая  $a_1, \dots, a_k$ . Тогда с одной стороны  $\langle a_1, \dots, a_k \rangle \subseteq H$  по определению подгруппы, а с другой стороны  $\langle a_1, \dots, a_k \rangle$ , очевидно, подгруппа в  $A$ . Значит,  $H = \langle a_1, \dots, a_k \rangle$  □

**Определение.** Если  $A = \langle a_1, \dots, a_k \rangle$ , то говорят, что  $A$  порождается  $a_1, \dots, a_k$ . Элементы  $a_1, \dots, a_k$  называются порождающими (образующими).

**Определение.** Если  $\exists$  конечное множество элементов  $a_1, \dots, a_k \in A$ , что  $A = \langle a_1, \dots, a_k \rangle$ , то  $A$  называется конечнопорождённой.

**Примеры.**

1.  $\mathbb{Q}$  - не конечнопорождённая;
2.  $U$  (комплексные корни из 1) - не конечнопорождённая;
3.  $\mathbb{Z}, \mathbb{Z}_n$  - конечнопорождённые (циклические);
4.  $\mathbb{Z} \oplus \mathbb{Z}$  - конечнопорождённая, не циклическая (примеры систем порождающих -  $(1, 0), (0, 1)$  или  $(3, 0), (4, 5), (0, 1)$ )

**Определение.** Линейно независимая система порождающих группы  $A$  называется базисом (или свободной системой порождающих).

**Утверждение.** (не было в лекции)

$a_1, \dots, a_k$  - базис  $\iff$  любой элемент  $A$  выражается через  $a_1, \dots, a_k$  единственным образом.

*Доказательство.*

$\implies$ : Из определения базиса любой элемент имеет разложение по базису.

$$\alpha_1 e_1 + \dots + \alpha_n e_n = a = \alpha'_1 e_1 + \dots + \alpha'_n e_n \implies (\alpha_1 - \alpha'_1) e_1 + \dots + (\alpha_n - \alpha'_n) e_n = 0$$

Отсюда из линейной независимости  $\alpha_i = \alpha'_i \forall i$ , т.е. разложение единственно.

$\impliedby$ : Любой элемент  $a \in A$  имеет разложение по  $a_1, \dots, a_n$  - система  $a_1, \dots, a_n$  порождает  $A$ . Разложение любого элемента единственно  $\implies 0$  имеет только тривиальное разложение  $\implies a_1, \dots, a_n$  линейно независимы.  $\square$

**Пример.**  $\mathbb{Z}_3 \oplus \mathbb{Z}_4$  - не имеет базиса: любая система элементов в ней линейно зависима ( $12 \cdot a = 0 \forall a \in A$ ).

**Определение.** Конечнопорождённая абелева группа, имеющая базис, называется свободной абелевой группой. По определению  $A = \{0\}$  - свободная абелева группа.

**Пример.**  $\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n$  - свободная абелева группа;

Базис -  $(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)$ . Проверим это:

1. Линейная независимость:

$$\alpha_1 e_1 + \dots + \alpha_n e_n = 0 \implies (\alpha_1, \dots, \alpha_n) = (0, \dots, 0) \implies \alpha_i = 0 \quad \forall i$$

2. Порождаемость группы:

$$\forall a \in \mathbb{Z}^n : a = (a_1, \dots, a_n) = a_1 e_1 + \dots + a_n e_n$$

**Лемма.** (Основная лемма о линейной зависимости для абелевых групп)

Если абелева группа  $A$  обладает базисом из  $n$  элементов, то любая система из  $m > n$  элементов линейно зависима.

*Доказательство.* Пусть  $e_1, \dots, e_n$  - базис группы  $A$ ,  $a_1, \dots, a_m \in A$  - произвольные элементы. Тогда из определения базиса:

$$\begin{cases} a_1 = \alpha_{11}e_1 + \dots + \alpha_{1n}e_n \longrightarrow (\alpha_{11}, \dots, \alpha_{1n}) \\ \vdots \\ a_m = \alpha_{m1}e_1 + \dots + \alpha_{mn}e_n \longrightarrow (\alpha_{m1}, \dots, \alpha_{mn}) \end{cases}$$

Строки  $\bar{\alpha}_i = (\alpha_{i1}, \dots, \alpha_{in})$  можно рассматривать как векторы из пр-ва  $\mathbb{Q}^n$  над  $\mathbb{Q}$ . Так как  $m > n$ , по ОЛЛЗ для векторных пространств система  $\bar{\alpha}_1, \dots, \bar{\alpha}_m$  линейно зависима, т.е.  $\exists \lambda_1, \dots, \lambda_m \in \mathbb{Q}$ , не все равные нулю, что  $\lambda_1 \bar{\alpha}_1 + \dots + \lambda_m \bar{\alpha}_m = 0$ .

Тогда если  $d$  - НОК знаменателей ненулевых  $\lambda_i$ , то  $(d\lambda_1)\bar{\alpha}_1 + \dots + (d\lambda_m)\bar{\alpha}_m = 0$  - нетривиальная целочисленная линейная комбинация, равная нулю.

Тогда  $(d\lambda_1)a_1 + \dots + (d\lambda_m)a_m = 0$ , т.е.  $a_1, \dots, a_m$  линейно зависимы.  $\square$

**Теорема 1.** Все базисы свободной абелевой группы  $A$  равномощны.

*Доказательство.* Очевидно следует из ОЛЛЗ для абелевых групп.  $\square$

**Определение.** Число элементов в базисе свободной абелевой группы  $A$  называется рангом группы  $A$ . Обозначается  $\text{rk } A$ . По определению  $A = \{0\} \implies \text{rk } A = 0$ .

**Теорема 2.** Все свободные абелевы группы ранга  $n$  изоморфны между собой (в частности, изоморфны  $\mathbb{Z}^n$ ).

*Доказательство.*

Пусть  $A$  - свободная абелева группа,  $\text{rk } A = n$ ,  $e_1, \dots, e_n$  - базис. Рассмотрим отображение  $\varphi : A \rightarrow \mathbb{Z}^n$  такое, что  $\forall a = \alpha_1 e_1 + \dots + \alpha_n e_n \in A \quad \varphi(a) = (\alpha_1, \dots, \alpha_n)$ . Покажем, что  $\varphi$  - изоморфизм:

1. Биекция - следует из единственности разложения по базису;
2. Гомоморфизм: пусть  $a = \alpha_1 e_1 + \dots + \alpha_n e_n, b = \beta_1 e_1 + \dots + \beta_n e_n$ . Тогда:

$$\begin{aligned}\varphi(a+b) &= \varphi((\alpha_1 + \beta_1)e_1 + \dots + (\alpha_n + \beta_n)e_n) = ((\alpha_1 + \beta_1), \dots, (\alpha_n + \beta_n)) = \\ &= (\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = \varphi(a) + \varphi(b)\end{aligned}$$

Отсюда  $A \simeq \mathbb{Z}^n$ .

Если  $\text{rk } A = \text{rk } B = n$ , то  $A \simeq \mathbb{Z}^n \simeq B \implies A \simeq B$ . □

**Теорема 3.** Любая подгруппа  $B$  свободной абелевой группы  $A$  ранга  $n$  является свободной абелевой, причём  $\text{rk } B \leq n$ .

*Доказательство.* Случай  $n = 0$  очевиден. Индукция по  $n$ :

База:  $n = 1 \implies A \simeq \mathbb{Z} \implies A = \langle e \rangle$ .

Знаем, что любая подгруппа циклической группы - циклическая.

Пусть  $B = \langle ke \rangle, k \in \mathbb{N} \cup \{0\}$ . Тогда:

$$k = 0 \implies B = \{0\} \implies \text{rk } B = 0 < 1 = \text{rk } A$$

$$k \neq 0 \implies B = \langle ke \rangle \simeq \mathbb{Z} \implies \text{rk } B = 1 = \text{rk } A$$

Шаг: пусть  $e_1, \dots, e_n$  - базис свободной группы  $A$ .

Рассмотрим  $\tilde{A} = \langle e_1, \dots, e_{n-1} \rangle \leq A$  - свободная абелева ранга  $n - 1$ .

Рассмотрим  $\tilde{B} = B \cap \tilde{A}$  - подгруппу  $B$  в  $\tilde{A}$ . По предположению индукции  $\tilde{B}$  - свободная абелева, причём  $\text{rk } \tilde{B} \leq \text{rk } \tilde{A} = n - 1$ .

Если  $B = \tilde{B}$ , то теорема доказана.

Иначе рассмотрим гомоморфизм (проекцию на  $\langle e_n \rangle$ )

$$\pi : A \rightarrow \mathbb{Z} : \forall a = \alpha_1 e_1 + \dots + \alpha_n e_n \in A \quad \pi(a) = \alpha_n \quad (\text{Ker } \pi = \tilde{A}, \text{Im } \pi = \mathbb{Z}).$$

Знаем, что  $\pi(B)$  - подгруппа в  $\mathbb{Z} \implies \pi(B) = \langle k \rangle$  ( $k \neq 0$  из  $B \neq \tilde{B}$ ).

Рассмотрим  $b_0 \in B$  такой, что  $\pi(b_0) = k$ , т.е.  $b_0 = \beta_1 e_1 + \dots + \beta_{n-1} e_{n-1} + k e_n$ .

Докажем, что если  $b_1, \dots, b_s$  - базис  $\tilde{B}$ , то  $b_0, b_1, \dots, b_s$  - базис  $B$  (тогда  $B$  - свободная абелева,  $\text{rk } B \leq n$ )

1. Проверим линейную независимость:

$$\lambda_0 b_0 + \dots + \lambda_s b_s = 0 \implies \pi(\lambda_0 b_0 + \dots + \lambda_s b_s) = 0 \implies \lambda_0 \pi(b_0) + \dots + \lambda_s \pi(b_s) = 0 \implies$$

$$\lambda_0 k = 0 \implies \lambda_0 = 0$$

Линейная комбинация  $\lambda_1 b_1 + \dots + \lambda_s b_s = 0$  тривиальна, так как  $b_1, \dots, b_s$  - базис  $\tilde{B}$ . Отсюда  $b_0, b_1, \dots, b_s$  линейно независимы.

2.  $\langle b_0, b_1, \dots, b_s \rangle \stackrel{?}{=} B$ :

Рассмотрим произвольный  $b \in B$ .  $\pi(b) \in \langle k \rangle \implies \pi(b) = tk, t \in \mathbb{Z}$ .

Пусть  $\tilde{b} = b - tb_0$ . Тогда  $\pi(\tilde{b}) = \pi(b) - t\pi(b_0) = tk - tk = 0 \implies \tilde{b} \in \text{Ker } \pi = \tilde{A} \implies \tilde{b} \in \tilde{A} \cap B = \tilde{B} \implies \tilde{b} = t_1 b_1 + \dots + t_s b_s \implies b = tb_0 + t_1 b_1 + \dots + t_s b_s$ .

□

## 4.1 Связь между базисами свободной абелевой группы

**Определение.** Пусть  $A$  - свободная абелева группа,  $\mathcal{E} = \{e_1, \dots, e_n\}$ ,  $\tilde{\mathcal{E}} = \{\tilde{e}_1, \dots, \tilde{e}_n\}$  - базисы  $A$ .

$$\begin{cases} \tilde{e}_1 = c_{11}e_1 + \dots + c_{n1}e_n \\ \vdots \\ \tilde{e}_n = c_{1n}e_1 + \dots + c_{nn}e_n \end{cases} \implies (\tilde{e}_1, \dots, \tilde{e}_n) = (e_1, \dots, e_n)C, \quad C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix}$$

Такая  $C \in M_n(\mathbb{Z})$  называется матрицей перехода от  $\mathcal{E}$  к  $\tilde{\mathcal{E}}$ .

**Утверждение.**

Пусть  $C \in M_n(\mathbb{Z})$ . Тогда  $C$  - матрица перехода  $\iff \det C = \pm 1$ .

*Доказательство.*

$\implies$ : Пусть  $C$  - матрица перехода от  $\mathcal{E}$  к  $\tilde{\mathcal{E}}$ ,  $D$  - от  $\tilde{\mathcal{E}}$  к  $\mathcal{E}$ . Тогда:

$$\begin{cases} (\tilde{e}_1, \dots, \tilde{e}_n) = (e_1, \dots, e_n)C \\ (e_1, \dots, e_n) = (\tilde{e}_1, \dots, \tilde{e}_n)D \end{cases} \implies CD = DC = E \implies D = C^{-1}$$

$$\det C \cdot \det D = \det CD = \det E = 1$$

Так как  $C, D \in M_n(\mathbb{Z})$ ,  $\det C, \det D \in \mathbb{Z} \implies \det C = \pm 1$ .

$\Leftarrow$ :  $C \in M_n(\mathbb{Z})$ ,  $\det C = \pm 1$ . Рассмотрим некоторый базис  $\mathcal{E} = \{e_1, \dots, e_n\}$  и докажем, что  $(\tilde{e}_1, \dots, \tilde{e}_n) = (e_1, \dots, e_n)C$  - базис.

1. Проверим линейную независимость:

Если  $\lambda_1 \tilde{e}_1 + \dots + \lambda_n \tilde{e}_n = 0$ , то линейная комбинация столбцов  $C$  с теми же  $\lambda_i$  также равна 0. Из  $\det C \neq 0$  столбцы линейно независимы, т.е.  $\lambda_i = 0 \forall i$ .

2.  $\langle \tilde{e}_1, \dots, \tilde{e}_n \rangle \stackrel{?}{=} A$ :

Так как  $\det C = \pm 1$ ,  $\exists D = C^{-1} \in M_n(\mathbb{Z})$  (из формулы явного выражения элементов обратной матрицы элементы  $D$  целые)  $\implies (e_1, \dots, e_n) = (\tilde{e}_1, \dots, \tilde{e}_n)D$ .

$\forall a \in A$  целочисленно выражается через  $e_1, \dots, e_n$ , каждый  $e_i$  целочисленно выражается через  $\tilde{e}_1, \dots, \tilde{e}_n \implies a$  целочисленно выражается через  $\tilde{e}_1, \dots, \tilde{e}_n$

□

## 4.2 Элементарные преобразования свободных абелевых групп

**Определение.** (ЭП свободных абелевых групп)

Пусть  $A$  - свободная абелева группа,  $e_1, \dots, e_n$  - базис  $A$ .

- ЭП1:  $\tilde{e}_i = e_i + ke_j, i \neq j, k \in \mathbb{Z}; \quad \tilde{e}_s = e_s, s \neq i;$
- ЭП2:  $\tilde{e}_i = e_j; \quad \tilde{e}_j = e_i; \quad \tilde{e}_s = e_s, s \neq i, j (i \neq j);$
- ЭП3:  $\tilde{e}_i = -e_i; \quad \tilde{e}_s = e_s, s \neq i;$

Матрицы перехода при этих ЭП:

ЭП1:

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \lambda & \\ & & & \ddots & \\ & & & & 1 \\ & & & & & 1 \end{pmatrix}$$

ЭП2:

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & & \ddots & \\ & & 1 & 0 & \\ & & & & 1 \end{pmatrix}$$

ЭП3:

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & -1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

называются (целочисленными) элементарными матрицами.

**Определение.** (ЭП строк целочисленных матриц)

- ЭП1:  $\overline{a_i} \rightarrow \overline{a_i} + \lambda \overline{a_j}, \quad i \neq j, k \in \mathbb{Z};$
- ЭП2:  $\overline{a_i} \leftrightarrow \overline{a_j}, \quad i \neq j;$
- ЭП3:  $\overline{a_i} \rightarrow (-1)\overline{a_i};$

(Аналогично определены ЭП над столбцами матрицы)

**Приведение целочисленной матрицы с помощью целочисленных ЭП к "диагональному" виду**

Пусть  $A = (a_{ij}) \in M_{n \times m}(\mathbb{Z})$ . Будем говорить, что матрица  $A$  имеет "диагональный" вид, если либо  $A = 0$ , либо  $a_{ii} = \alpha_i \in \mathbb{N}, i = \overline{1, l}$  и  $a_{ij} = 0$  иначе.

$$A = \left( \begin{array}{ccc|c} \alpha_1 & & 0 & 0 \\ & \ddots & & \\ 0 & & \alpha_l & 0 \\ \hline & & 0 & 0 \end{array} \right)$$

**Лемма.** Любую матрицу  $M \in M_{n \times m}(\mathbb{Z})$  за конечное число целочисленных ЭП над строками и столбцами можно привести к "диагональному" виду.

*Доказательство.* Индукция по  $n$  - числу строк матрицы. При фиксированном  $n$  индукция по  $\nu(M)$  - наименьшему по модулю ненулевому элементу  $M$ .

Если  $M = 0$ , то утверждение доказано, поэтому далее  $M \neq 0$ .

База индукции:  $n = 1 \implies M = (a_{11}, \dots, a_{1m})$ .

База внутренней индукции:  $\nu(M) = 1$  - очевидна (если в строке есть 1, то с помощью неё можно занулить все оставшиеся элементы).

Шаг внутренней индукции: Пусть  $\nu(M) = |a_{1j}|$ . Если  $a_{1j} < 0$ , то применим ЭП3 к столбцу  $j$ ; если  $j > 1$ , то применением ЭП2 поменяем 1-й и  $j$ -й столбцы местами. После этих операций  $\nu(M) = a_{11}$ .

$\forall j > 1 : a_{1j} = a_{11}q_j + r_j$ , где  $0 \leq r_j < a_{11}$ . Вычитая с помощью ЭП1 из  $j$ -го столбца 1-й, умноженный на  $q_j$ , получим строку  $\tilde{M} = (a_{11}, r_2, \dots, r_m)$ .

Если все  $r_j = 0$ , то диагональный вид получен, иначе можно воспользоваться предположением индукции ( $\nu(\tilde{M}) < \nu(M)$ ).

Шаг индукции: Пусть  $\nu(M) = |a_{ij}|$ . Сначала сделаем  $a_{ij}$  положительным (ЭП3), затем переставим его в верхний левый угол (ЭП2).

Случай 1:  $M = \left( \begin{array}{c|ccc} a_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbb{C} & \\ 0 & & & \end{array} \right)$  - по предположению индукции приводим



$C$  к диагональному виду;

Случай 2:  $\exists j > 1 : a_{1j} \neq 0$ . Тогда, аналогично базе индукции, с помощью ЭП1 приводим верхнюю строчку к виду  $\forall j > 1 : a_{1j} = 0$ .

Случай 3:  $\exists j > 1 : a_{j1} \neq 0$  - аналогично случаю 2 (ЭП строк вместо столбцов).

□

**Упражнение.** Доказать, что с помощью конечного числа целочисленных ЭП над строками и столбцами

$$M \sim \left( \begin{array}{ccc|c} \alpha_1 & & 0 & 0 \\ & \ddots & & \\ 0 & & \alpha_l & 0 \\ \hline & 0 & & 0 \end{array} \right)$$

где  $\alpha_l \mid \alpha_{l-1}, \alpha_{l-1} \mid \alpha_{l-2}, \dots, \alpha_2 \mid \alpha_1$ .

*Доказательство.* По лемме можем с помощью ЭП привести  $M$  к диагональному виду. Индукция по  $l$  - числу ненулевых  $\alpha$  в диагональном виде:

База:  $l = 0, 1$  - очевидно;

Шаг: Из теории чисел знаем, что для чисел  $\alpha_1, \alpha_i$  существуют  $a, b \in \mathbb{Z}$ , что  $a\alpha_1 + b\alpha_i = d_i = \text{НОД}(\alpha_1, \alpha_i)$ . Значит, с помощью ЭП1 можно сделать  $a_{1i} = d_i$ . Тогда следующими операциями:

$$\begin{aligned} \begin{pmatrix} \alpha_1 & \cdots & 0 & \cdots & 0 \\ & \ddots & & & \\ 0 & & \alpha_i & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} &\sim \begin{pmatrix} \alpha_1 & \cdots & d_i & \cdots & 0 \\ & \ddots & & & \\ 0 & & \alpha_i & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \sim \begin{pmatrix} \alpha_1 & \cdots & d_i & \cdots & 0 \\ & \ddots & & & \\ k\alpha_1 & & 0 & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \sim \\ &\sim \begin{pmatrix} 0 & \cdots & d_i & \cdots & 0 \\ & \ddots & & & \\ k\alpha_1 & & 0 & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \sim \begin{pmatrix} k\alpha_1 & \cdots & 0 & \cdots & 0 \\ & \ddots & & & \\ 0 & & d_i & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \end{aligned}$$

можем сделать так, чтобы  $\alpha_i \mid \alpha_1$ . Причём  $\alpha_1$  при этих операциях домножается на  $k \in \mathbb{Z}$ , а значит, делимость на все предыдущие  $\alpha_j$  сохраняется. Тогда за  $l - 1$  таких наборов операций можно сделать  $\alpha_1$  общим кратным всех  $\alpha$ , а матрица без первой строки и первого столбца приводится к нужному виду по предположению индукции.

□

**Пример.**  $(12, 10, 6) \sim (6, 10, 12) \sim (6, 4, 0) \sim (4, 6, 0) \sim (4, 2, 0) \sim (2, 4, 0) \sim (2, 0, 0)$ .

(По сути - обобщённый алгоритм Евклида, остаётся НОД чисел 12, 10 и 6).

### 4.3 Согласованные базисы свободной абелевой группы и её подгруппы

#### Теорема 1.

Пусть  $A$  - свободная абелева группа ранга  $n$ ,  $B \leq A$  - подгруппа ранга  $m$ .

Тогда  $\exists$  базисы  $\tilde{e}_1, \dots, \tilde{e}_n$  группы  $A$  и  $\tilde{f}_1, \dots, \tilde{f}_m$  подгруппы  $B$  такие, что  $\tilde{f}_i = \alpha_i \tilde{e}_i$ ,  $\alpha_i \in \mathbb{N}$ .

*Доказательство.* Пусть  $e_1, \dots, e_n$  и  $f_1, \dots, f_m$  - некоторые базисы  $A$  и  $B$  соответственно. Так как  $f_i \in A$ ,  $(f_1, \dots, f_m) = (e_1, \dots, e_n)C$ , где  $C \in M_{n \times m}(\mathbb{Z})$ .

Если  $\tilde{f}_1, \dots, \tilde{f}_m$  - другой базис  $B$ , то  $(f_1, \dots, f_m) = (\tilde{f}_1, \dots, \tilde{f}_m)T$ , где  $T \in M_{m \times m}(\mathbb{Z})$

Если  $\tilde{e}_1, \dots, \tilde{e}_n$  - другой базис  $A$ , то  $(e_1, \dots, e_n) = (\tilde{e}_1, \dots, \tilde{e}_n)S$ , где  $S \in M_{n \times n}(\mathbb{Z})$  ( $\det T, S = \pm 1$ ). Отсюда

$$(\tilde{f}_1, \dots, \tilde{f}_m)T = (\tilde{e}_1, \dots, \tilde{e}_n)SC \implies (\tilde{f}_1, \dots, \tilde{f}_m) = (\tilde{e}_1, \dots, \tilde{e}_n)\tilde{C}, \quad \tilde{C} = SCT^{-1}$$

Тогда если  $S, T^{-1}$  - элементарные матрицы, то  $SC$  - ЭП над строками  $C$ , а  $CT^{-1}$  - ЭП над столбцами  $C$ . По лемме 1  $C$  с помощью ЭП можно привести к виду

$$\tilde{C} = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_m \\ & & & 0 \end{pmatrix} \quad (\text{нулей среди } \alpha_i \text{ не будет, т.к. векторы базиса } f \text{ ЛНЗ}). \text{ Отсюда}$$

и получаем требуемое равенство  $\tilde{f}_i = \alpha_i \tilde{e}_i$ ,  $\alpha_i \in \mathbb{N}$ . □

#### Теорема. (не было в лекции)

Пусть  $G = G_1 \times \dots \times G_s$ ,  $H = H_1 \times \dots \times H_s$ , причём  $H \subseteq G$  и  $H_i \trianglelefteq G_i$ .

Тогда  $H \trianglelefteq G$  и  $G/H = G_1/H_1 \times \dots \times G_s/H_s$ .

*Доказательство.*

Будем работать с внешним прямым произведением. Рассмотрим отображение

$$\varphi : G \rightarrow G_1/H_1 \times \dots \times G_s/H_s$$

$$\varphi(g_1, \dots, g_s) = (g_1 H_1, \dots, g_s H_s)$$

$\varphi$  - гомоморфизм, так как по  $i$ -й компоненте  $\varphi$  реализует естественный гомоморфизм  $G \rightarrow G/H_i$ .

Ядро  $\varphi$  - наборы  $(g_1, \dots, g_s)$ , которые отображаются в нейтральный элемент, т.е. в  $(H_1, \dots, H_s)$ . Получаем

$$\varphi(g_1, \dots, g_s) = (H_1, \dots, H_s) \iff g_i \in H_i, \quad \forall i = 1, \dots, s$$

Таким образом,  $\text{Ker } \varphi = H_1 \times \dots \times H_s$ .

Из определения  $\varphi$  очевидна сюръективность, т.е.  $\text{Im } \varphi = G_1/H_1 \times \dots \times G_s/H_s$ , а значит, из теоремы о гомоморфизме получаем необходимое утверждение. □

*Замечание.* Для абелевых групп из теоремы получим следующее утверждение:

Пусть  $A = A_1 \oplus \dots \oplus A_n$ ,  $B \leq A$ ,  $B = B_1 \oplus \dots \oplus B_n$ .

Тогда  $A/B = (A_1 \oplus \dots \oplus A_n)/(B_1 \oplus \dots \oplus B_n) \simeq A_1/B_1 \oplus \dots \oplus A_n/B_n$

**Следствие 1.** В условиях теоремы 1:

$$A/B \simeq \mathbb{Z}_{\alpha_1} \oplus \dots \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n-m}$$

*Доказательство.* По теореме 1:  $\tilde{f}_1 = \alpha_1 \tilde{e}_1, \dots, \tilde{f}_m = \alpha_m \tilde{e}_m$ .

$$A = \langle \tilde{e}_1 \rangle \oplus \dots \oplus \langle \tilde{e}_m \rangle \oplus \langle \tilde{e}_{m+1} \rangle \oplus \dots \oplus \langle \tilde{e}_n \rangle; \quad B = \langle \alpha_1 \tilde{e}_1 \rangle \oplus \dots \oplus \langle \alpha_m \tilde{e}_m \rangle \oplus \langle 0 \rangle \oplus \dots \oplus \langle 0 \rangle$$

Тогда из замечания выше:

$$\begin{aligned} A/B &\simeq \langle \tilde{e}_1 \rangle / \langle \alpha_1 \tilde{e}_1 \rangle \oplus \dots \oplus \langle \tilde{e}_m \rangle / \langle \alpha_m \tilde{e}_m \rangle \oplus \langle \tilde{e}_{m+1} \rangle / \langle 0 \rangle \oplus \dots \oplus \langle \tilde{e}_n \rangle / \langle 0 \rangle \simeq \\ &\simeq \mathbb{Z}_{\alpha_1} \oplus \dots \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n-m} \end{aligned}$$

□

**Следствие 2.** В условиях теоремы 1:  $\text{rk } A = \text{rk } B \iff |A : B| < \infty$ .

*Доказательство.* По определению  $|A : B| = |A/B|$ .

Из следствия 1 видно, что если  $\text{rk } A = \text{rk } B$ , то  $A/B \simeq \mathbb{Z}_{\alpha_1} \oplus \dots \oplus \mathbb{Z}_{\alpha_n}$ , и  $|A/B| < \infty$ , а иначе в прямой сумме встретится слагаемое  $\mathbb{Z}$ , то есть найдётся элемент бесконечного порядка. □

**Утверждение 1.** (Универсальное свойство абелевой группы)

Пусть  $S = \{a_1, \dots, a_n\}$  - система порождающих абелевой группы  $A$ .

Тогда следующие утверждения эквивалентны:

1.  $A$  - свободная с базисом  $S$ ;
2.  $\forall$  абелевой группы  $D$ ,  $\forall d_1, \dots, d_n \in D \exists!$  гомоморфизм  $\varphi : A \rightarrow D$  т.ч.  
 $\varphi : a_i \mapsto d_i \forall i$ .

*Доказательство.*

$1 \implies 2$  :  $S$  - базис  $A \implies \forall a \in A \exists! \alpha_i \in \mathbb{Z} : a = \alpha_1 a_1 + \dots + \alpha_n a_n$ .

Рассмотрим отображение  $\varphi : A \rightarrow D$ , заданное как  $a = \alpha_1 a_1 + \dots + \alpha_n a_n \mapsto \alpha_1 d_1 + \dots + \alpha_n d_n$ . Оно корректно вследствие единственности разложения по базису, а также очевидно является гомоморфизмом с нужным свойством.

$2 \implies 1$ . Рассмотрим свободную группу  $D$  ранга  $n$ , в ней рассмотрим базис

$d_1, \dots, d_n$ . По условию  $\exists!$  гомоморфизм  $\varphi : A \rightarrow D$ , причём  $a_i \mapsto d_i$ .

Предположим, что  $a_1, \dots, a_n$  линейно зависимы. Тогда

$$\lambda_1 a_1 + \dots + \lambda_n a_n = 0 \implies \varphi(\lambda_1 a_1 + \dots + \lambda_n a_n) = \lambda_1 d_1 + \dots + \lambda_n d_n = 0$$

Противоречие с линейной независимостью  $d_1, \dots, d_n$ . Значит,  $a_1, \dots, a_n$  - базис.  $\square$

**Следствие 3.** *Любая конечнопорождённая абелева группа изоморфна свободной абелевой группе по некоторой её подгруппе  $B$ .*

*Доказательство.* Пусть  $D = \langle d_1, \dots, d_n \rangle$ . Рассмотрим свободную абелеву группу  $A$  ранга  $n$  с базисом  $a_1, \dots, a_n$ .

По утверждению 1  $\exists$  гомоморфизм  $\varphi : A \rightarrow D$  такой, что  $\varphi(a_i) = d_i$ .

Из порождаемости гомоморфизм сюръективен, а значит, по теореме о гомоморфизме  $D = \text{Im } \varphi \simeq A/\text{Ker } \varphi$ , где  $\text{Ker } \varphi \leq A$ .  $\square$

**Следствие 4.** *Любая конечнопорождённая абелева группа раскладывается в сумму циклических подгрупп.*

*Доказательство.*  $D \simeq A/B \simeq \mathbb{Z}_{\alpha_1} \oplus \dots \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n-m}$   $\square$

**Следствие 5.** *Любая конечнопорождённая абелева группа  $D$  раскладывается в прямую сумму конечной абелевой группы и свободной абелевой группы.*

*Доказательство.*  $D \simeq (\mathbb{Z}_{\alpha_1} \oplus \dots \oplus \mathbb{Z}_{\alpha_m}) \oplus \mathbb{Z}^{n-m}$   $\square$

**Определение.** Группа, в которой каждый неединичный элемент имеет бесконечный порядок, называется группой без кручения.

**Упражнение.** Если  $A$  - свободная абелева, то  $A$  - без кручения.

*Доказательство.* Предположим, что  $b \in A$  - элемент конечного порядка  $m$ . По определению свободной группы  $b = \alpha_1 a_1 + \dots + \alpha_n a_n$ , причём не все  $\alpha_i$  равны 0. Тогда  $m\alpha_1 a_1 + \dots + m\alpha_n a_n = mb = 0$  - противоречие с линейной независимостью базиса.  $\square$

**Следствие 6.** *Если  $A$  - конечнопорождённая абелева группа без кручения, то  $A$  - свободная абелева группа.*

*Доказательство.* В обозначениях следствия 5  $m = 0$ .  $\square$