



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: 19 ноября 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
4.4	Основная теорема о конечнопорождённых абелевых группах	43
<b>5</b>	<b>Действия группы на множестве</b>	<b>51</b>
5.1	Орбиты и стабилизаторы	52
5.2	Действия группы на себе	56
5.3	Классы сопряжённости и централизаторы	58
<b>6</b>	<b>Теоремы Силова</b>	<b>62</b>
6.1	I теорема Силова	62
6.2	II теорема Силова	64
6.3	Нормализатор. III теорема Силова	65
<b>7</b>	<b>Коммутант</b>	<b>67</b>
7.1	Коммутанты некоторых известных групп	68
<b>8</b>	<b>Разрешимые и простые группы</b>	<b>71</b>
8.1	Разрешимые группы	71
8.2	Простые группы	73
8.3	Значение простых групп	74
8.4	Примеры простых групп	75
<b>9</b>	<b>Линейные представления</b>	<b>79</b>
9.1	Матричные представления группы	80
9.2	Приводимость линейных представлений	81
9.3	Сумма линейных представлений группы	86
9.4	Вполне приводимые линейные представления	86

# 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.  
 $|D_n| = 2n$ , т.к.  $n$  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.  $\forall a, b \in G_1 \quad \varphi(a * b) = \varphi(a) \circ \varphi(b)$

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).

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

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

*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.  $A_n \trianglelefteq S_n, S_n/A_n \simeq \mathbb{Z}_2$  (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:

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

- Биективность:

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

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

- 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  $|X'| + |Z'| = k + m - 2$ , 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:  $\pi(W) = 1 \implies W \in \text{Ker } \pi = N$ .

□

**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  $\tilde{W}W^{-1} = 1$  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  $\text{Im } \varphi \simeq \mathbb{Z}_{mn}/\text{Ker } \varphi = \mathbb{Z}_{mn} \implies |\text{Im } \varphi| = mn$ .

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  $\text{ord } (g_1, g_2) \mid dk_1k_2 = \frac{mn}{d} < mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$ . 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  $(n_1 h_1)(n_2 h_2) = n_1 \underbrace{(h_1 n_2 h_1^{-1})}_{=\tilde{n}} \underbrace{h_1 h_2}_{=\tilde{h}} = \tilde{n} \tilde{h} \in NH$ .

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

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

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

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

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 абелевой 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  $B$ , которая содержится в  $\tilde{A}$  (очевидно, что это подгруппа). 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:

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

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:  $\overline{a_i} \rightarrow \overline{a_i} + \lambda \overline{a_j}, \quad i \neq j, \lambda \in \mathbb{Z};$
- 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 Сogласованные 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

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

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

*Замечание.* Для абелевых групп из теоремы 4 прямого произведения получим следующее утверждение: Пусть  $A = A_1 \oplus \dots \oplus A_n$ ,  $B = B_1 \oplus \dots \oplus B_n$ , причём  $B \leq A$ ,  $B_i \leq A_i$

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:  $\tilde{f}_1 = \alpha_1 \tilde{e}_1, \dots, \tilde{f}_m = \alpha_m \tilde{e}_m$ .

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

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.  $\square$

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

**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. □

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

*Доказательство.* В обозначениях следствия 5  $m = 0$ . □

## 4.4 Основная теорема о конечнопорождённых абелевых группах

**Определение.** Группа  $G$  называется периодической, если  $\forall g \in G$   $g$  имеет конечный порядок.

**Определение.** Периодическая группа  $G$  называется  $p$ -группой, где  $p$  - простое, если  $\forall g \in G \exists s \in \mathbb{N} : \text{ord } g = p^s$ .

**Упражнение.**

Доказать, что конечная группа  $G$  является  $p$ -группой  $\iff |G| = p^m$  ( $m \in \mathbb{N}$ ).

*Доказательство.*

$\Leftarrow$  - очевидно, т.к.  $\forall g \in G : \text{ord } g \mid p^m = |G|$ ;

$\Rightarrow$ : на будущих лекциях будет доказательство в терминах силовских подгрупп. □

**Определение.** Группа  $G$  называется примарной, если  $G$  является  $p$ -группой для некоторого простого  $p$ .

**Утверждение.** Существуют конечнопорождённые (не абелевы) бесконечные  $p$ -группы.

*Доказательство.* Без доказательства. □

**Пример.** Не конечнопорождённая примарная абелева группа:

$\mathbb{C}_{p^\infty}$  - группа комплексных корней степеней  $p^m$  из 1.

**Лемма 1.** Пусть  $A$  - конечнопорождённая абелева группа,  $B \leq A$  такая, что  $A/B$  - свободная абелева группа. Тогда  $\exists C \leq A$  - свободная абелева группа такая, что  $A \simeq B \oplus C$ .

*Доказательство.* Пусть  $\bar{e}_1, \dots, \bar{e}_n$  - базис  $\mathbb{Z}^n \simeq A/B$ , и пусть  $\varphi : A/B \rightarrow \mathbb{Z}^n$  - изоморфизм. Тогда  $\varphi^{-1}(\bar{e}_i) = e_i + B$ , где  $e_i \in A$ .

Рассмотрим  $C = \langle e_1, \dots, e_n \rangle$ .

Покажем, что  $e_1, \dots, e_n$  - базис  $C$ , т.е. докажем линейную независимость  $e_1, \dots, e_n$ :

$$\begin{aligned} \lambda_1 e_1 + \dots + \lambda_n e_n = 0 &\implies \lambda_1 e_1 + \dots + \lambda_n e_n + B = B \implies \varphi(\lambda_1 e_1 + \dots + \lambda_n e_n + B) = \\ &= \lambda_1 \bar{e}_1 + \dots + \lambda_n \bar{e}_n = 0 \implies \forall i \lambda_i = 0 \text{ т.к. } \bar{e}_1, \dots, \bar{e}_n \text{ - базис } \mathbb{Z}^n \end{aligned}$$

Покажем, что  $A = B \oplus C$ , или, что равносильно, что  $A = B + C$  и  $B \cap C = \{0\}$ :

- $B \cap C = \{0\}$ : Рассмотрим  $b \in B \cap C$ . Тогда:

$$\begin{aligned} b = \mu_1 e_1 + \dots + \mu_n e_n &\implies \mu_1 e_1 + \dots + \mu_n e_n + B = b + B = B \implies \\ &\implies \varphi(\mu_1 e_1 + \dots + \mu_n e_n + B) = \mu_1 \bar{e}_1 + \dots + \mu_n \bar{e}_n = 0 \implies \forall i \mu_i = 0 \end{aligned}$$

- $A = B + C$ : Рассмотрим произвольный  $a \in A$ .

$\varphi(a + B) = \bar{a} \in \mathbb{Z}^n$ , где  $\bar{a} = \mu_1 \bar{e}_1 + \dots + \mu_n \bar{e}_n$ . Тогда

$$\varphi(a - \sum_i \mu_i e_i + B) = 0 \implies a - \sum_i \mu_i e_i + B = B \implies \exists b \in B : a = b + \sum_i \mu_i e_i$$

□

**Лемма 2.** Все элементы конечного порядка абелевой группы  $A$  образуют подгруппу в  $A$ .

*Доказательство.* Обозначим за  $\text{Tor } A$  множество всех элементов конечного порядка группы  $A$ .

1.  $a, b \in \text{Tor } A \implies \exists n, m \in \mathbb{N} : na = mb = 0 \implies$   
 $\implies (n \cdot m)(a + b) = (n \cdot m)a + (n \cdot m)b = 0 \implies (a + b)$  имеет конечный порядок.
2.  $0 \in \text{Tor } A$  - очевидно.

3.  $\forall a \in \text{Tor } A \implies -a \in \text{Tor } A$ , т.к.  $n(-a) = -na = 0$ .

□

**Определение.** Подгруппа  $\text{Tor } A$  ("torsion subgroup") называется подгруппой кручения группы  $A$ .

**Упражнение.** Доказать, что в группе  $D_\infty = \langle a, b \mid a^2 = 1, aba^{-1} = b^{-1} \rangle$  все элементы конечного порядка не образуют подгруппу.

*Замечание.* Группа Диэдра  $D_n$  отлична от  $D_\infty$  наличием соотношения  $b^n = 1$ , ( $a$  - любая симметрия правильного  $n$ -угольника,  $b$  - поворот на  $\frac{2\pi}{n}$ ).

*Доказательство.* Заметим, что  $\text{ord } ba = 2$  :

$$a = a^{-1} \implies baba = b(aba^{-1}) = bb^{-1} = 1$$

Также  $\text{ord } a = 2 : a^2 = 1$ . При этом  $\text{ord } (ba)a = \text{ord } b = \infty$ . Значит, произведение элементов конечного порядка может быть элементом бесконечного порядка, т.е. все элементы конечного порядка не образуют подгруппу в  $D_\infty$ . □

**Лемма 3.** Пусть  $A$  - абелева группа. Тогда  $A/\text{Tor } A$  - группа без кручения.

*Доказательство.* От противного: пусть  $\bar{a} \in A/\text{Tor } A, \bar{a} \neq 0, \text{ord } \bar{a} = n$ . Тогда  $n\bar{a} = 0$ ,  $a \in \text{Tor } A$ .

$$\begin{aligned} n\bar{a} = 0 &\implies n(a + \text{Tor } A) = \text{Tor } A \implies na \in \text{Tor } A \implies \\ &\implies \exists m \in \mathbb{N} : m(na) = 0 \implies (mn)a = 0 \implies a \in \text{Tor } A \implies \bar{a} = 0 \end{aligned}$$

- противоречие с  $\bar{a} \neq 0$ . Значит,  $A/\text{Tor } A$  - группа без кручения. □

**Лемма 4.** Пусть  $A$  - конечнопорождённая абелева группа. Тогда  $A = \text{Tor } A \oplus C$ , где  $C \leq A$  - свободная абелева группа,  $\text{Tor } A$  - конечная.

*Доказательство.* Пусть  $A = \langle a_1, \dots, a_n \rangle$ .

Тогда  $A/\text{Tor } A = \langle a_1 + \text{Tor } A, \dots, a_n + \text{Tor } A \rangle$ . Кроме того, по лемме 3  $A/\text{Tor } A$  - группа без кручения, а отсюда по следствию 6 из универсального свойства абелевой группы - свободная. Отсюда по лемме 1  $\exists C \leq A$  - свободная абелева группа такая, что  $A \simeq \text{Tor } A \oplus C$ .

Осталось показать, что  $\text{Tor } A$  - конечная:  $\text{Tor } A \simeq A/C = \langle a_1 + C, \dots, a_n + C \rangle \implies \text{Tor } A = \langle b_1, \dots, b_n \rangle$  - конечнопорождённая. Тогда если  $k_i = \text{ord } b_i$ , то  $\forall b \in \text{Tor } A$

$$b = \lambda_1 b_1 + \dots + \lambda_n b_n, \lambda_i \in \mathbb{Z}, 0 \leq \lambda_i < k_i \implies |\text{Tor } A| \leq k_1 \dots k_n$$

□

**Лемма 5.** Пусть  $A$  - конечная абелева группа,  $|A| = p_1^{k_1} \dots p_s^{k_s}$ . Тогда  $A$  раскладывается в прямую сумму  $A_{p_1} \oplus \dots \oplus A_{p_s}$ , где  $A_{p_i}$  -  $p_i$ -подгруппа, причём набор этих подгрупп определён однозначно.

*Доказательство.*

- Существование разложения:

Рассмотрим произвольное простое  $p$  и обозначим за  $A_p$  множество всех элементов  $A$  порядков  $p^m$ . Проверим, что  $A_p$  - подгруппа  $A$ :

1.  $a, b \in A_p, p^{m_1}a = p^{m_2}b = 0 \implies p^{m_1+m_2}(a+b) = p^{m_2} \cdot p^{m_1}a + p^{m_1} \cdot p^{m_2}b = 0$   
Отсюда  $a, b \in A_p \implies a+b \in A_p$ ;
2.  $0 \in A_p$  - очевидно;
3.  $p^m a = 0 \implies p^m(-a) = -p^m a = 0$ . Отсюда  $a \in A_p \implies -a \in A_p$ .

Докажем, что  $A = A_{p_1} \oplus \dots \oplus A_{p_s}$ :

1.  $A_{p_1} \oplus \dots \oplus A_{p_s}$  - прямая сумма.

Из критерия прямой суммы достаточно показать, что  $A_{p_i} \cap \langle A_{p_j} \mid j \neq i \rangle = \{0\}$ . Рассмотрим  $a \in A_{p_i} \cap \langle A_{p_j} \mid j \neq i \rangle$ . Так как  $a \in A_{p_i}$ , то  $p_i^{m_i} a = 0$ . С другой стороны,  $a = \sum_{j \neq i} a_j$ , то есть  $(\prod_{j \neq i} p_j^{m_j}) a = 0$ .

Так как  $\prod_{j \neq i} p_j^{m_j}$  и  $p_i^{m_i}$  взаимно просты, имеем  $1 \cdot a = a = 0$ .

2.  $A = A_{p_1} \oplus \dots \oplus A_{p_s}$ . Рассмотрим произвольный  $a \in A$ . Пусть  $\text{ord } a = n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ . Обозначим  $n_i = \frac{n}{p_i^{\alpha_i}}$ . Так как  $\text{НОД}(n_1, \dots, n_s) = 1, \exists l_i \in \mathbb{Z} : l_1 n_1 + \dots + l_s n_s = 1$ . Отсюда  $a = l_1 n_1 a + \dots + l_s n_s a$ . Так как  $p_i^{\alpha_i} (l_i n_i a) = l_i n a = 0$ , имеем  $l_i n_i a \in A_{p_i}$ . Значит,  $a$  раскладывается в линейную комбинацию элементов  $A_{p_i}$ .

- Единственность разложения - от противного: пусть

$$A = \tilde{A}_{p_1} \oplus \dots \oplus \tilde{A}_{p_s} = A_{p_1} \oplus \dots \oplus A_{p_s}$$

Так как  $A_{p_i}$  - максимальная  $p_i$ -подгруппа в  $A$  (содержит все элементы  $A$  порядка  $p_i^m$ ),  $\tilde{A}_{p_i} \subseteq A_{p_i}$ .

Предположим, что  $\exists a \in A_{p_i} : a \notin \tilde{A}_{p_i}$ . Так как  $a \in A = \tilde{A}_{p_1} \oplus \dots \oplus \tilde{A}_{p_s}$ ,  $a = \tilde{a}_{p_i} + b$ , где  $\tilde{a}_{p_i} \in \tilde{A}_{p_i}, b \in \langle \tilde{A}_{p_j} \mid j \neq i \rangle$ . Тогда  $\text{ord } a = p_i^{m_1}, \text{ord } \tilde{a}_{p_i} = p_i^{m_2} \implies$

$$p_i^{m_1+m_2} a = p_i^{m_1+m_2} \tilde{a}_{p_i} + p_i^{m_1+m_2} b \implies p_i^{m_1+m_2} b = 0, \text{ а также } \prod_{j \neq i} p_j^{\alpha_j} b = 0$$

$\prod_{j \neq i} p_j^{\alpha_j}$  и  $p_i^{m_1+m_2}$  взаимно просты  $\implies b = 0$ , т.е.  $a = \tilde{a}_{p_i} \in \tilde{A}_{p_i}$  - противоречие.

Значит, такого  $a$  не существует, то есть  $A_{p_i} \subseteq \tilde{A}_{p_i}$ . Отсюда  $A_{p_i} = \tilde{A}_{p_i}$ .

□

**Лемма 6.** Пусть  $A$  - конечная абелева  $p$ -группа. Тогда если  $A = A_1 \oplus \dots \oplus A_s = B_1 \oplus \dots \oplus B_t$ , где  $A_i, B_i$  - примарные циклические подгруппы, то  $s = t$  и набор порядков  $|A_1|, \dots, |A_s|$  совпадает с набором порядков  $|B_1|, \dots, |B_t|$  (т.е. разложение единственно с точностью до порядка слагаемых).

*Доказательство.* Индукция по  $|A|$ :

База:  $|A| = p \implies A \simeq \mathbb{Z}_p$  - такое разложение единственно;

Шаг: Пусть  $|A_i| = p^{n_i}, |B_i| = p^{m_i}$ . Упорядочим их: пусть

$$n_1 \geq n_2 \geq \dots \geq n_{\tilde{s}} > n_{\tilde{s}+1} = \dots = n_s = 1$$

$$m_1 \geq m_2 \geq \dots \geq m_{\tilde{t}} > m_{\tilde{t}+1} = \dots = m_t = 1$$

Пусть  $A_i = \langle a_i \rangle_{p^{n_i}}, B_i = \langle b_i \rangle_{p^{m_i}}$ . Рассмотрим множество  $pA = \{pa \mid a \in A\}$ . Очевидно, что  $pA \leq A$ . Тогда:

$$A = \langle a_1 \rangle \oplus \dots \oplus \langle a_{\tilde{s}} \rangle \oplus \langle a_{\tilde{s}+1} \rangle \oplus \dots \oplus \langle a_s \rangle$$

$$\forall a \in A : a = \alpha_1 a_1 + \dots + \alpha_{\tilde{s}} a_{\tilde{s}} + \alpha_{\tilde{s}+1} a_{\tilde{s}+1} + \dots + \alpha_s a_s \implies pa = \alpha_1 pa_1 + \dots + \alpha_{\tilde{s}} pa_{\tilde{s}}$$

( $A_{\tilde{s}+1}, \dots, A_s$  - циклические порядка  $p$ , поэтому  $\alpha_{\tilde{s}+1} pa_{\tilde{s}+1} + \dots + \alpha_s pa_s = 0$ )

Тогда  $pA = \langle pa_1 \rangle \oplus \dots \oplus \langle pa_{\tilde{s}} \rangle$ . При этом  $\text{ord}(pa_1) = p^{n_1-1}, \dots, \text{ord}(pa_{\tilde{s}}) = p^{n_{\tilde{s}}-1}$ .

Значит,  $|pA| = p^{n_1+\dots+n_{\tilde{s}}-\tilde{s}} < |A|$ .

Аналогично  $pA = \langle pb_1 \rangle \oplus \dots \oplus \langle pb_{\tilde{t}} \rangle, |pA| = p^{m_1+\dots+m_{\tilde{t}}-\tilde{t}} < |A|$ .

Тогда по предположению индукции разложения  $pA$  совпадают (порядок слагаемых одинаковый в силу упорядоченности), то есть

$$\tilde{s} = \tilde{t}; \quad \forall i = \overline{1 \dots \tilde{s}} : n_i - 1 = m_i - 1 \implies n_i = m_i$$

При этом  $|A| = |A_1| \cdot \dots \cdot |A_{\tilde{s}}| \cdot |A_{\tilde{s}+1}| \cdot \dots \cdot |A_s| = p^{n_1+\dots+n_{\tilde{s}}+s-\tilde{s}}$ , а с другой стороны  $|A| = |B_1| \cdot \dots \cdot |B_{\tilde{t}}| \cdot |B_{\tilde{t}+1}| \cdot \dots \cdot |B_t| = p^{m_1+\dots+m_{\tilde{t}}+t-\tilde{t}}$ . Отсюда

$$n_1 + \dots + n_{\tilde{s}} + s - \tilde{s} = m_1 + \dots + m_{\tilde{t}} + t - \tilde{t}; \quad \tilde{s} = \tilde{t}; \quad n_i = m_i \implies s = t$$

□

**Теорема.** (Основная т. о конечнопорождённых абелевых группах)

Пусть  $A$  - конечнопорождённая абелева группа. Тогда  $A$  изоморфна прямой



сумме (конечных) примарных циклических подгрупп и бесконечных циклических подгрупп:

$$A \simeq \mathbb{Z}_{p_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{s_k}} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_m$$

причём число  $m$  и набор  $p_1^{s_1}, \dots, p_k^{s_k}$  определены однозначно для группы  $A$ .

*Доказательство.*

- **Существование разложения**

Из следствия 4 универсального свойства абелевой группы для  $A$  имеем:

$$A \simeq A_0/B_0 \simeq \mathbb{Z}_{\alpha_1} \oplus \dots \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n-m}$$

Также из аналога китайской теоремы об остатках знаем, что если  $\alpha = q_1^{\nu_1} \dots q_\mu^{\nu_\mu}$ , где  $q_i$  - различные простые, то  $\mathbb{Z}_\alpha = \mathbb{Z}_{q_1^{\nu_1}} \oplus \dots \oplus \mathbb{Z}_{q_\mu^{\nu_\mu}}$ . Отсюда из разложения выше получаем искомое разложение.

- **Единственность разложения**

По лемме 4 для  $A$  имеет место разложение  $A = \text{Tor } A \oplus C$ , где  $\text{Tor } A$  - конечная,  $C$  - свободная. Заметим, что  $\text{rk } C = \text{rk } A/\text{Tor } A$ . Так как  $\text{Tor } A$  - инвариант  $A$ , то  $A/\text{Tor } A$ , а тогда и  $\text{rk } C$  - инварианты  $A$ .

Так как  $C \simeq \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$ , а  $\mathbb{Z}_{p_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{s_k}}$  - конечная, имеем  $C = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_m$ , то есть  $m = \text{rk } C$ , а отсюда  $m$  однозначно определено для  $A$ .

Пусть  $B = \text{Tor } A$ . По лемме 5  $B \simeq A_{\tilde{p}_1} \oplus \dots \oplus A_{\tilde{p}_l}$ , причём это разложение на примарные подгруппы единственно с точностью до порядка слагаемых. А из леммы 6 каждая  $A_{\tilde{p}_i}$  раскладывается на циклические примарные однозначно с точностью до порядка слагаемых. Значит, набор порядков  $p_1^{s_1}, \dots, p_k^{s_k}$  определён однозначно для  $A$ .

□

**Пример.** Все абелевы группы порядка 8 с точностью до изоморфизма:

$$8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2 \implies A_1 \simeq \mathbb{Z}_8; A_2 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2; A_3 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

**Пример.**  $V_4 = \{e, a, b, c\}$

$V_4 = \langle a \rangle_2 \oplus \langle b \rangle_2 = \langle b \rangle_2 \oplus \langle c \rangle_2$ , но разложение из теоремы единственно:  $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

*Замечание.* Для не конечнопорождённых абелевых групп утверждение теоремы неверно, контрпримером служит следующее упражнение:

**Упражнение.** Доказать, что  $\mathbb{Q}$  не раскладывается в прямую сумму циклических (вообще говоря, произвольных) подгрупп.

*Доказательство.* Пусть  $H_1, H_2 \trianglelefteq \mathbb{Q}$  - нетривиальные нормальные подгруппы  $\mathbb{Q}$ . Тогда  $\exists h_1 \in H_1, h_2 \in H_2 : h_1, h_2 \neq 0$ . Тогда:

$$h_1 = \frac{m_1}{n_1}, h_2 = \frac{m_2}{n_2} \implies m_2 n_1 h_1 = m_1 n_2 h_2 \in H_1 \cap H_2$$

то есть  $H_1 \cap H_2 \neq \{0\}$ . Отсюда  $\mathbb{Q}$  не раскладывается в прямую сумму подгрупп.  $\square$

**Определение.** Экспонентой (периодом, показателем) конечной группы  $G$  называется наименьшее общее кратное порядков элементов группы  $G$ .

Обозначается  $\exp G$ .

**Утверждение.** Если  $G$  конечна, то  $\exp G \mid |G|$

*Доказательство.* Для конечных групп знаем, что порядок группы является общим кратным всех порядков элементов группы. Так как наименьшее общее кратное набора чисел делит любое общее кратное этого набора, получаем необходимое утверждение.  $\square$

**Утверждение.** Конечная абелева группа  $A$  циклическая  $\iff \exp A = |A|$ .

*Доказательство.*

$\implies$ :  $A = \langle a \rangle \implies \text{ord } a = |A| \implies \exp A \geq |A| \implies \exp A = |A|$  (т.к.  $\exp A \mid |A|$ ).

$\impliedby$ : От противного: пусть  $\exp A = |A|$ , но  $A$  - не циклическая. По основной теореме о конечнопорождённых абелевых группах  $A \simeq \mathbb{Z}_{p_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p_m^{s_m}}$ . Если все  $p_1, \dots, p_m$  различны, то  $A$  циклическая по аналогу китайской теоремы об остатках - противоречие. Если среди них есть совпадающие, то можем без ограничения общности считать, что  $p_1 = p_2, s_1 \leq s_2$ . Обозначим  $\mathbb{Z}_{p_i^{s_i}} = \langle a_i \rangle \implies \forall a \in A : a = \sum_{i=1}^m \alpha_i a_i$ . Тогда если в равенстве  $|A| = p_1^{s_1} p_2^{s_2} \dots p_m^{s_m}$  обозначить  $t = p_2^{s_2} \dots p_m^{s_m}$ ,

то  $\forall a \in A : ta = \sum_{i=1}^m \alpha_i t a_i = 0$ .

(очевидно, что  $t a_i = 0$  для  $i \neq 1$ , а  $t a_1 = 0$  в силу  $p_1 = p_2, s_1 \leq s_2$ )

Тогда  $t$  - общее кратное всех порядков элементов  $A$ , то есть  $\exp A \mid t$ , но  $t < |A| = \exp A$  - противоречие. Значит,  $A$  - циклическая.  $\square$

**Теорема.** Пусть  $\mathbb{F}$  - произвольное поле,  $A$  - конечная подгруппа в  $\mathbb{F}^*$ . Тогда  $A$  - циклическая.

*Доказательство.* (мультипликативная терминология)

Из определения поля  $F^*$  - абелева группа, а значит,  $A$  также абелева.

От противного: пусть  $A$  не циклическая, т.е.  $\exp A < |A|$ . Тогда если  $\exp A = n$ , то  $\forall a \in A \ a^n = 1$ . Рассмотрим многочлен  $x^n - 1$  над полем  $\mathbb{F}$ . Его степень равна  $n$ , а число его корней в  $\mathbb{F}$  хотя бы  $|A|$ , что больше  $n$  по предположению - противоречие.  $\square$

**Пример.**  $\mathbb{F} = \mathbb{Z}_p$  :  $A = F^*$  - циклическая. Например,  $\mathbb{Z}_5^* = \langle 3 \rangle_4$ .

**Следствие.** *Мультипликативная группа любого конечного поля - циклическая.*

## 5 Действия группы на множестве

**Определение.** Пусть  $X$  - произвольное множество. Биективное отображение  $f : X \rightarrow X$  называется преобразованием множества  $X$ .

Множество всех преобразований  $X$  обозначается  $S(X)$ .

**Утверждение.**  $S(X)$  - группа относительно композиции.

*Доказательство.*

1. Ассоциативность - очевидно;
2. Нейтральный элемент - тождественное преобразование;
3. Обратный элемент - обратное преобразование (существует, т.к. биекция)

□

**Определение.** Группа  $S(X)$  называется группой всех преобразований  $X$ .  
Произвольная  $H \leq S(X)$  называется группой преобразований множества  $X$ .

**Пример.**  $GL(V)$  - группа невырожденных линейных операторов векторного пространства  $V : GL(V) \leq S(V)$ .

**Определение.** Пусть  $G$  - произвольная группа,  $X$  - произвольное множество. Действием группы  $G$  на множестве  $X$  называется гомоморфизм  $\alpha : G \rightarrow S(X)$ .  
Обозначается  $G \curvearrowright X$  (или  $G : X$ )

Элементы множества  $X$  при этом называются точками.

$\forall g \in G : g \mapsto \alpha(g)$  - преобразование множества  $X$ , т.е. биекция  $X \rightarrow X$ .

Равенство  $\alpha(g)(x) = y (x \in X)$  записывают как  $\alpha(g)x = y$  или  $gx = y$ .

Так как  $\alpha$  - гомоморфизм, имеем:

$$\forall g_1, g_2 \in G : \alpha(g_1 g_2) = \alpha(g_1) \alpha(g_2) \implies \alpha(g_1 g_2)x = (\alpha(g_1) \alpha(g_2))x = \alpha(g_1)(\alpha(g_2)x)$$

Отсюда  $(g_1 g_2)x = g_1(g_2 x)$ . Аналогично:

$$\forall g \in G : \alpha(g^{-1}) = (\alpha(g))^{-1} \implies \alpha(g^{-1})x = (\alpha(g)x)^{-1}$$

Отсюда  $g^{-1}x = y \iff gy = x$ .

Если  $H \leq S(X)$ , то определено "тавтологическое" действие  $H$  на  $X : \alpha(h) = h$   
- вложение  $H \rightarrow S(X)$ .

**Пример.**  $GL(V) \curvearrowright V : \alpha(g)x = g(x) \forall g \in GL(V), x \in X$

В общем случае:  $\alpha : G \rightarrow S(X)$  - гомоморфизм, то есть  $\text{Im } \alpha \leq S(X)$ ,  $\text{Ker } \alpha \trianglelefteq G$ .

**Определение.**  $\text{Ker } \alpha$  называется ядром неэффективности действия группы  $G$  на  $X$ .

Если  $\text{Ker } \alpha = \{e\}$ , то действие называется эффективным.

*Замечание.* Всякое действие группы  $G$  на множестве  $X$  индуцирует и другие действия. Например:

1.  $G \curvearrowright 2^X$ ;

2. Если  $Y \subset X$  - инвариантное подмножество относительно  $G$ , то  $G \curvearrowright Y$ .

**Пример.** Пусть  $K$  - равносторонний треугольник,  $G = \text{Sym } K \leq S(X)$ , где  $X$  - множество точек треугольника.

Тогда если  $Y = \{v_1, v_2, v_3\}$  - вершины треугольника, а  $Z = \{e_1, e_2, e_3\}$  - стороны треугольника, то действие  $G \curvearrowright X$  индуцирует также и действия  $G \curvearrowright Y, G \curvearrowright Z$

**Пример.** Пусть задано  $G \curvearrowright X$ ,  $\mathbb{F}$  - поле,  $Y = \{f : X \rightarrow \mathbb{F}\}$  - алгебра всех функций  $X \rightarrow \mathbb{F}$ . Рассмотрим  $\alpha : G \rightarrow S(Y) : \forall g \in G \alpha(g)f = \tilde{f}$  такое, что  $\tilde{f}(x) = f(g^{-1}x) \forall x \in X$ . Покажем, что  $\alpha$  - гомоморфизм:

$$\begin{aligned} \forall g_1, g_2 \in G : (\alpha(g_1 g_2)f)(x) &= f((g_1 g_2)^{-1}(x)) = f(g_2^{-1}(g_1^{-1}x)) = (\alpha(g_2)f)(g_1^{-1}x) = \\ &= \alpha(g_1)(\alpha(g_2)f)(x) = (\alpha(g_1)\alpha(g_2)f)(x) \end{aligned}$$

*Замечание.* Если  $G \curvearrowright X, H \leq G$ , то определено также действие  $H \curvearrowright X$  - ограничение действия на подгруппу.

**Пример.**  $G = S_3$ ;  $G \curvearrowright X$ , где  $X = \{1, 2, 3\}$  - действуют как подстановки.  $H = \langle (1, 2, 3) \rangle \leq G$  - определено действие  $H \curvearrowright X$  как ограничение  $G \curvearrowright X$ .

## 5.1 Орбиты и стабилизаторы

**Утверждение.** Отношение, заданное правилом  $x \sim y \iff \exists g \in G : gx = y$ , является отношением эквивалентности.

*Доказательство.*

- Рефлексивность:  $\forall x \in X : ex = x \implies x \sim x$ ;
- Симметричность:

$$x \sim y \implies \exists g \in G : gx = y \implies g^{-1}gx = g^{-1}y \implies g^{-1}y = x \implies y \sim x$$

- Транзитивность:

$$\begin{cases} x \sim y \\ y \sim z \end{cases} \implies \exists g_1, g_2 \in G : \begin{cases} y = g_1 x \\ z = g_2 y \end{cases} \implies z = g_2(g_1 x) = (g_2 g_1) x \implies x \sim z$$

□

**Определение.** Классы эквивалентности относительно этого отношения называются орбитами относительно действия  $G \curvearrowright X$ .

Обозначается  $\text{Orb}(x) = \{y \in X \mid \exists g \in G : y = gx\}$

**Пример.** Пусть  $G$  - группа поворотов плоскости  $\mathcal{E}^2$  вокруг точки  $o$ .

Тогда при  $G \curvearrowright E^2$   $\text{Orb}(x)$  - окружность с центром в точке  $o$  радиуса  $|ox|$ .

**Определение.** Если  $\text{Orb}(x) = \{x\}$ , то  $x$  называется неподвижной точкой.

**Определение.** Если  $\text{Orb}(x) = X$ , то действие называется транзитивным.

*Замечание.* Это именно характеристика действия, так как  $\exists x : \text{Orb}(x) = X \implies \forall x \in X \text{ Orb}(x) = X$ .

**Пример.**  $G$  - группа сдвигов (параллельных переносов)  $\mathcal{E}^2$ .

Тогда  $G \curvearrowright \mathcal{E}^2$  - транзитивное (из любой точки можно получить любую другую сдвигом на вектор, их соединяющий).

**Утверждение.** Если  $y \in \text{Orb}(x)$ , то  $\text{Orb}(y) = \text{Orb}(x)$ .

*Доказательство.* Напрямую следует из определения орбиты. □

**Определение.** Стабилизатором (стационарной подгруппой) точки  $x$  называется множество  $\text{St}(x) = \{g \in G \mid gx = x\}$ .

**Утверждение.**  $\text{St}(x) \leq G$ .

*Доказательство.*

- $g_1, g_2 \in \text{St}(x) \implies g_1 x = g_2 x = x$   
 $(g_1 g_2) x = g_1(g_2 x) = g_1 x = x \implies g_1 g_2 \in \text{St}(x);$
- $ex = x \implies e \in \text{St}(x);$
- Пусть  $g \in \text{St}(x)$ . Тогда  $g(x) = x$ , а также  $g(g^{-1}x) = ex = x$ . Так как образ  $g$  при действии - биекция, имеем  $x = g^{-1}x$ , то есть  $g^{-1} \in \text{St}(x)$

□

**Утверждение.** Если  $y = gx$ , то множество  $M_y = \{h \in G \mid y = hx\}$  совпадает с множеством  $g\text{St}(x)$ .

*Доказательство.* Покажем оба включения:

$g\text{St}(x) \subset M_y : \forall \tilde{g} \in g\text{St}(x) : \tilde{g} = g \cdot g', \text{ где } g' \in \text{St}(x). \text{ Тогда: } \tilde{g}x = (gg')x = g(g'x) = gx = y \implies \tilde{g} \in M_y. \text{ Отсюда } g\text{St}(x) \subset M_y.$

$M_y \subset g\text{St}(x) : \forall h \in M_y : y = hx. \text{ Также } y = gx \implies gx = hx \implies (g^{-1}h)x = g^{-1}(hx) = x \implies g^{-1}h \in \text{St}(x) \implies h \in g\text{St}(x). \text{ Отсюда } M_y \subset g\text{St}(x). \quad \square$

**Теорема.** Отображение  $\psi : \text{Orb}(x) \rightarrow G/\text{St}(x)$  (множество левых смежных классов, не факторгруппа!) такое, что  $gx \mapsto g\text{St}(x)$ , является биекцией.

*Доказательство.*

- Корректность: Пусть  $y = g_1x = g_2x$ . Тогда:

$$\begin{aligned} g_1x = g_2x &\implies (g_2^{-1}g_1)x = (g_2^{-1}g_2)x = x \implies g_2^{-1}g_1 \in \text{St}(x) \implies \\ &\implies g_1 \in g_2\text{St}(x) \implies g_1\text{St}(x) = g_2\text{St}(x) \implies \psi(g_1x) = \psi(g_2x) \end{aligned}$$

- Сюръективность - очевидна ( $\forall g \in G$   $g\text{St}(x)$  будет образом точки  $gx$ );
- Инъективность: Пусть  $\psi(g_1) = \psi(g_2)$ . Тогда:

$$g_1\text{St}(x) = g_2\text{St}(x) \implies g_2^{-1}g_1 \in \text{St}(x) \implies (g_2^{-1}g_1)x = x \implies g_1x = g_2x$$

$\square$

**Следствие 1.**  $|\text{Orb}(x)| = |G/\text{St}(x)| = |G : \text{St}(x)|$ .

**Следствие 2.** Если  $G$  - конечная группа, то  $|\text{Orb}(x)| = \frac{|G|}{|\text{St}(x)|}$ .

**Пример.** Пусть  $K \in \mathcal{E}^3$  - куб,  $G = \text{Sym}^+(K) = \{g \in \text{Isom}^+(\mathcal{E}^3) \mid gK = K\}$  - группа вращений  $K$ .

Найдём  $|G|$ . Так как  $G \leq S(X)$ , где  $X = \{v_1, \dots, v_8\}$  - множество вершин куба,  $|G| < \infty$ . Значит, если рассмотреть индуцированное действие  $G \curvearrowright X$ , то  $|G| = |\text{Orb}(v_1)| \cdot |\text{St}(v_1)|$ .

$\text{Orb}(v_1) = X$  (вершина может перейти в любую)  $\implies |\text{Orb}(v_1)| = 8$ ;

$|\text{St}(v_1)| = 3$  (id и два поворота вокруг большой диагонали, содержащей  $v_1$ );

Отсюда  $|G| = 8 \cdot 3 = 24$ .

Более того, покажем, что  $G \simeq S_4$ . Рассмотрим множество диагоналей куба  $Y = \{d_1, d_2, d_3, d_4\}$ . Так как при собственном движении диагонали переходят в диагонали, можем рассмотреть действие  $G \curvearrowright Y \implies \exists \alpha : G \rightarrow S(Y) \simeq S_4$  -

гомоморфизм. Из  $|G| = |S_4| = 24$  для доказательства того, что  $\alpha$  - изоморфизм, достаточно показать сюръективность, а для этого достаточно показать, что все транспозиции диагоналей можно получить вращениями (достаточно, т.к.  $S_4$  порождается транспозициями, а  $\text{Im } \alpha \leq S(Y)$ ).

Такая транспозиция - это поворот на  $\pi$  относительно прямой, проходящей через середины двух рёбер, соединяющих концы диагоналей.

**Упражнение.** Доказать, что если  $L$  - правильный тетраэдр, то  $\text{Sym}(L) \simeq S_4$ .

*Доказательство.* Будем действовать аналогично - пусть  $X = \{v_1, \dots, v_4\}$  - множество вершин тетраэдра, тогда действие  $\text{Sym}(L) \curvearrowright E^3$  индуцирует действие  $\text{Sym}(L) \curvearrowright X$ , а отсюда  $|\text{Sym}(L)| = |\text{Orb}(v_1)| \cdot |\text{St}(v_1)|$ .

$\text{Orb}(v_1) = X$  (вершина может перейти в любую)  $\implies |\text{Orb}(v_1)| = 4$ ;

$|\text{St}(v_1)| = 6$  (любые перестановки вершин на грани, не содержащей  $v_1$ );

(проверка существования всех этих движений непосредственная)

Отсюда  $|G| = 4 \cdot 6 = 24$ .

Так как  $S(X) \simeq S_4$ , достаточно показать, что гомоморфизм действия - изоморфизм, а из равенства порядков достаточно сюръективности. Транспозиция любых двух вершин может быть получена симметрией относительно плоскости, проходящей через середину ребра, соединяющего вершины, и противоположное ребро.  $\square$

**Определение.** Элементы  $a, b \in G$  называются сопряжёнными, если  $\exists g \in G$  такой, что  $b = g^{-1}ag$ . Обозначается  $b = a^g$ .

*Замечание.* Такое обозначение не случайно: многие свойства возведения в степень присущи и операции сопряжения. Однако в данном курсе эти свойства пока не понадобятся.

**Определение.** Подгруппы  $L, K \leq G$  называются сопряжёнными, если  $\exists g \in G$  такой, что  $K = g^{-1}Lg = \{g^{-1}lg \mid l \in L\}$ .

**Утверждение.** Пусть  $y = gx$ . Тогда  $g\text{St}(x)g^{-1} = \text{St}(y)$ .

*Доказательство.*

- $g\text{St}(x)g^{-1} \stackrel{?}{\subseteq} \text{St}(y)$ :  
 $\forall h \in \text{St}(x) : ghg^{-1}(y) = ghg^{-1}(gx) = gh(g^{-1}g)x = ghx = gx = y \implies ghg^{-1} \in \text{St}(y)$ ;



- $\text{St}(y) \stackrel{?}{\subseteq} g\text{St}(x)g^{-1}$ : (аналогичные рассуждения, т.к.  $y = gx \iff x = g^{-1}y$ )  
 $\forall h \in \text{St}(y) : g^{-1}hg(x) = g^{-1}hg(g^{-1}y) = g^{-1}h(gg^{-1})y = g^{-1}hy = g^{-1}y =$   
 $x \implies g^{-1}hg \in \text{St}(x) \implies h \in g\text{St}(x)g^{-1}.$

□

## 5.2 Действия группы на себе

Пусть  $G$  - группа,  $X = G$ . Рассмотрим основные действия  $G \curvearrowright G$  и покажем некоторые их свойства:

1. Действие  $G \curvearrowright G$  левыми сдвигами:

$\alpha : G \rightarrow S(G)$  такое, что  $\forall g \in G, h \in G : \alpha(g)h = gh$ .

Покажем, что  $\alpha$  - гомоморфизм:

$$\forall g_1, g_2 \in G : \alpha(g_1g_2)h = (g_1g_2)h = g_1(g_2h) = \alpha(g_1)(\alpha(g_2)h) = (\alpha(g_1)\alpha(g_2))h$$

$g \in \text{Ker } \alpha \implies \forall h \in G : gh = h \implies g = e \implies \text{Ker } \alpha = \{e\}$  - действие эффективно.

Значит, по теореме о гомоморфизме  $G \simeq \text{Im } \alpha \leq S(G)$ .

**Следствие.** (Теорема Кэли)

Пусть  $|G| = n$ . Тогда  $G$  изоморфна некоторой подгруппе  $S_n$ .

*Доказательство.* Рассмотрим гомоморфизм  $\alpha : G \rightarrow S(G)$ , приведённый выше. Тогда  $G \simeq \text{Im } \alpha \leq S(G) \simeq S_n$ , т.к.  $|G| = n$ . □

2. Действие  $G \curvearrowright G$  правыми сдвигами:

$\alpha : G \rightarrow S(G)$  такое, что  $\forall g \in G, h \in G : \alpha(g)h = hg^{-1}$ .

Покажем, что  $\alpha$  - гомоморфизм:

$$\forall g_1, g_2 \in G : \alpha(g_1g_2)h = hg_2^{-1}g_1^{-1} = \alpha(g_1)(hg_2^{-1}) = (\alpha(g_1)\alpha(g_2))h$$

$g \in \text{Ker } \alpha \implies \forall h \in G : hg^{-1} = h \implies g = e \implies \text{Ker } \alpha = \{e\}$  - действие эффективно.

3. Действие  $G \curvearrowright G$  сопряжениями:

$\alpha : G \rightarrow S(G)$  такое, что  $\forall g \in G, h \in G : \alpha(g)h = ghg^{-1}$ .

Покажем, что  $\alpha$  - гомоморфизм:

$$\forall g_1, g_2 \in G : \alpha(g_1g_2)h = (g_1g_2)h(g_1g_2)^{-1} = g_1(g_2hg_2^{-1})g_1^{-1} = \alpha(g_1)(\alpha(g_2)h)$$

**Утверждение.**  $\forall g \in G : \alpha(g) : G \rightarrow G$  - автоморфизм, т.е. изоморфизм  $G$  на себя.

*Доказательство.* Биективность  $\alpha(g)$  следует из  $\alpha(g) \in S(G)$ . Докажем, что  $\alpha(g)$  - гомоморфизм:

$$\alpha(g)(h_1 h_2) = g h_1 h_2 g^{-1} = (g h_1 g^{-1})(g h_2 g^{-1}) = (\alpha(g)h_1)(\alpha(g)h_2)$$

Значит,  $\alpha(g)$  - автоморфизм  $G$ . □

**Определение.** Такой автоморфизм называется внутренним автоморфизмом группы  $G$  (относительно элемента  $g$ ).

**Утверждение.**

1. Множество  $\text{Aut } G$  всех автоморфизмов группы  $G$  - группа относительно композиции, причём  $\text{Aut } G \leq S(G)$ .
2. Множество  $\text{Int } G$  всех внутренних автоморфизмов группы  $G$  - группа относительно композиции, причём  $\text{Int } G \trianglelefteq \text{Aut } G$ .

*Доказательство.*

1. Достаточно проверить, что  $\text{Aut } G \leq S(G)$ :

- $\alpha_1, \alpha_2 \in \text{Aut } G \implies (\alpha_1 \alpha_2) \in \text{Aut } G$ ;
- $\text{id} \in \text{Aut } G$ ;
- $\alpha \in \text{Aut } G \implies \alpha^{-1} \in \text{Aut } G$  (изоморфизм обратим).

2. Для определения группы достаточно проверить, что  $\text{Int } G \leq \text{Aut } G$ :

- $\alpha_1, \alpha_2 \in \text{Int } G \implies \exists g_1, g_2 \in G : \alpha_i$  - сопряжение относительно  $g_i$ . Тогда  $(\alpha_1 \alpha_2)$  - сопряжение относительно  $g_1 g_2$ , т.е.  $(\alpha_1 \alpha_2) \in \text{Int } G$ ;
- $\text{id} \in \text{Int } G$  - сопряжение относительно  $e$ ;
- $\alpha \in \text{Int } G \implies \alpha$  - сопряжение относительно  $g \in G \implies \alpha^{-1}$  - сопряжение относительно  $g^{-1} \implies \alpha^{-1} \in \text{Int } G$ .

Проверим, что  $\text{Int } G \trianglelefteq \text{Aut } G$ , т.е.  $\forall \varphi \in \text{Aut } G, g \in G : \varphi \alpha(g) \varphi^{-1} \in \text{Int } G$ :

$$\begin{aligned} (\varphi \alpha(g) \varphi^{-1})(h) &= \varphi(\alpha(g)(\varphi^{-1}(h))) = \varphi(g \varphi^{-1}(h) g^{-1}) = \varphi(g) \varphi(\varphi^{-1}(h)) \varphi(g^{-1}) \\ &= \varphi(g) h (\varphi(g))^{-1} = \alpha(\varphi(g))(h) \implies \varphi \alpha(g) \varphi^{-1} = \alpha(\varphi(g)) \in \text{Int } G \end{aligned}$$

□

**Определение.**  $\text{Aut } G$  называется группой аутизмов<sub>1</sub> группы  $G$ .  
 $\text{Int } G$  называется группой внутренних автоморфизмов группы  $G$ .

Пусть  $\alpha$  - действие  $G \curvearrowright G$  сопряжениями. Тогда  $\text{Ker } \alpha = \{g \in G \mid \alpha(g)h = h \forall h \in G\} = \{g \in G \mid ghg^{-1} = h \forall h \in G\} = \{g \in G \mid gh = hg \forall h \in G\}$ , а  $\text{Im } \alpha = \text{Int } G$ .

**Определение.** Множество  $Z(G) = \{g \in G \mid gh = hg \forall h \in G\}$  называется центром группы  $G$ .

**Свойства.**

1.  $Z(G) = \text{Ker } \alpha$ , где  $\alpha$  - действие  $G \curvearrowright G$  сопряжениями;
2.  $Z(G) \trianglelefteq G$ ;
3.  $\forall H \leq Z(G) : H \trianglelefteq G$ ;
4.  $Z(G) = G \iff G$  - абелева

*Доказательство.*

1. Доказано выше;
2. Следует из (1) ( $\text{Ker } \alpha \trianglelefteq G$  - свойство гомоморфизма);
3.  $\forall h \in H \leq Z(G), g \in G : ghg^{-1} = gg^{-1}h = h \in H \implies H \trianglelefteq G$ ;
4. Очевидно из определения абелевой группы.

□

### 5.3 Классы сопряжённости и централизаторы

**Определение.** Пусть  $\alpha$  - действие  $G \curvearrowright G$  сопряжениями.

Классом сопряжённости  $x \in G$  называется орбита  $x$  относительно  $\alpha$ .

Централизатором элемента  $x \in G$  называется стабилизатор  $x$  относительно  $\alpha$ .

Класс сопряжённости обозначается как  $x^G = \{y \in G \mid \exists g \in G : y = gxg^{-1}\}$ .

Централизатор обозначается как  $C(x) = \{g \in G \mid gxg^{-1} = x\}$ .

**Утверждение 1.** Если  $|G| < \infty$ , то  $|x^G| = \frac{|G|}{|C(x)|}$ .

*Доказательство.* Очевидно следует из утверждения  $|\text{Orb}(x)| = \frac{|G|}{|\text{St}(x)|}$ .

□

**Утверждение 2.**  $x^G = \{x\} \iff x \in Z(G)$ .

*Доказательство.* Очевидно следует из свойства 1 центра группы. □

**Определение.** Группа  $G$  называется тривиальной, если  $G = \{e\}$ .

**Теорема.** Центр любой конечной нетривиальной  $p$ -группы нетривиален ( $p$  - простое).

*Доказательство.* Пусть  $|G| = p^s$ . Рассмотрим случаи:

1.  $G$  - абелева  $\implies Z(G) = G$ .

2.  $G$  - неабелева. Тогда  $G$  разбивается на несколько непересекающихся классов сопряжённости:  $G = \bigsqcup_{i=1}^k x_i^G$ .

По утверждению 2  $|x_i^G| = 1 \iff x_i \in Z(G)$ , а по утверждению 1  $|x_i^G| = \frac{|G|}{|C(x_i)|}$

Так как  $G$  -  $p$ -группа, для  $x_i \notin Z(G)$  :  $|x_i^G| = p^{s_i}, s_i \geq 1$ .

Без ограничения общности пусть только  $x_1, \dots, x_m \in Z(G)$  (всегда будет хотя бы один, так как  $e \in Z(G)$ ). Тогда:

$$|G| = \underbrace{|x_1^G| + \dots + |x_m^G|}_{|Z(G)|} + |x_{m+1}^G| + \dots + |x_k^G| \implies p^s = |Z(G)| + p^{s_{m+1}} + \dots + p^{s_k}$$

Отсюда  $p \mid |Z(G)|$ , а значит,  $|Z(G)| \geq p > 1$  - центр нетривиален. □

*Замечание.*  $\exists$  бесконечная (конечнопорождённая)  $p$ -группа с тривиальным центром (монстр Тарского).

**Следствие.** Если  $|G| = p^2$ , где  $p$  - простое, то  $G$  - абелева.

*Доказательство.*  $G$  -  $p$ -группа  $\implies Z(G) \neq \{e\}$ .

Предположим, что  $G$  неабелева, т.е. что  $Z(G) \neq G$ .

Тогда, так как  $|Z(G)| \mid |G| = p^2$  и  $|Z(G)| \neq 1, p^2$ , имеем  $|Z(G)| = p$ .

Рассмотрим группу  $G/Z(G)$ . Её порядок равен  $\frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p \implies G/Z(G)$  - циклическая, а значит,  $G/Z(G) = \langle aZ(G) \rangle$ . Тогда  $\forall g \in G \exists t \in \mathbb{Z} : g \in a^t Z(G)$ .

Рассмотрим два произвольных элемента  $g_1, g_2 \in G$  и докажем, что  $g_1 g_2 = g_2 g_1$ :

$$\exists t_1, t_2 \in \mathbb{Z} : g_1 = a^{t_1} Z(G), g_2 = a^{t_2} Z(G) \implies \exists z_1, z_2 \in Z(G) : g_1 = a^{t_1} z_1, g_2 = a^{t_2} z_2$$

Так как элементы центра коммутируют со всеми элементами  $G$ , имеем:

$$g_1 g_2 = a^{t_1} z_1 a^{t_2} z_2 = a^{t_1+t_2} z_1 z_2 = a^{t_2+t_1} z_2 z_1 = a^{t_2} z_2 a^{t_1} z_1 = g_2 g_1$$

а значит,  $G$  - абелева, что противоречит предположению.

Отсюда  $G$  не может быть неабелевой, т.е.  $G$  - абелева.  $\square$

**Лемма 1.** Пусть  $X$  - произвольное множество,  $G \leq S(X)$ . Тогда если  $\varphi \in G$  т.ч.  $\varphi : x \mapsto y$ , то  $\forall \psi \in G : \psi \circ \varphi \circ \psi^{-1} : \psi(x) \mapsto \psi(y)$ .

*Доказательство.* Применим преобразование  $\psi \circ \varphi \circ \psi^{-1}$ :

$$(\psi \circ \varphi \circ \psi^{-1})(\psi(x)) = \psi(\varphi(\psi^{-1}(\psi(x)))) = \psi(\varphi(x)) = \psi(y)$$

$\square$

**Утверждение 3.** Пусть  $\sigma, \tilde{\sigma} \in S_n$ . Тогда  $\sigma, \tilde{\sigma}$  сопряжены в  $S_n \iff \sigma, \tilde{\sigma}$  имеют одинаковые цикловые структуры, т.е. наборы длин независимых циклов в разложении  $\sigma, \tilde{\sigma}$  совпадают.

*Доказательство.*

$\implies$ : Пусть  $\sigma, \tilde{\sigma}$  сопряжены в  $S_n \implies \exists \tau \in S_n : \tilde{\sigma} = \tau \sigma \tau^{-1}$ .

Пусть  $\sigma = (i_1 i_2 \dots i_s)(j_1 j_2 \dots j_t) \dots$  - разложение  $\sigma$  в независимые циклы. Тогда  $\sigma : i_1 \mapsto i_2, i_2 \mapsto i_3, \dots, i_s \mapsto i_1$ , а тогда по лемме 1  $\tau \sigma \tau^{-1} : \tau(i_1) \mapsto \tau(i_2), \tau(i_2) \mapsto \tau(i_3), \dots, \tau(i_s) \mapsto \tau(i_1)$ . Аналогичное рассуждение можно провести для всех независимых циклов  $\sigma$ , а значит,  $\tau \sigma \tau^{-1} = (\tau(i_1) \tau(i_2) \dots \tau(i_s))(\tau(j_1) \tau(j_2) \dots \tau(j_t)) \dots$  - длины циклов сохраняются.

$\impliedby$ : Пусть  $\sigma, \tilde{\sigma}$  имеют одинаковые цикловые структуры. Можем поменять порядок циклов так, чтобы длины  $i$ -х циклов в  $\sigma$  и  $\tilde{\sigma}$  совпадали, т.е.

$$\sigma = (i_1 i_2 \dots i_s)(j_1 j_2 \dots j_t) \dots; \quad \tilde{\sigma} = (\tilde{i}_1 \tilde{i}_2 \dots \tilde{i}_s)(\tilde{j}_1 \tilde{j}_2 \dots \tilde{j}_t) \dots$$

Тогда если  $\tau = \begin{pmatrix} i_1 & i_2 & \dots & i_s & j_1 & j_2 & \dots & j_t & \dots \\ \tilde{i}_1 & \tilde{i}_2 & \dots & \tilde{i}_s & \tilde{j}_1 & \tilde{j}_2 & \dots & \tilde{j}_t & \dots \end{pmatrix}$ , то по лемме 1  $\tilde{\sigma} = \tau \sigma \tau^{-1}$ .  $\square$

**Примеры.**  $\sigma = (12)(345)(6)(7), \tilde{\sigma} = (15)(243)(6)(7)$  - сопряжены в  $S_7$ :

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 2 & 4 & 3 & 6 & 7 \end{pmatrix} \text{ (из построения в теореме);}$$

$$\sigma = (123)(45), \tau = (135) \implies \tau \sigma \tau^{-1} = (325)(41).$$

**Следствие.**  $Z(S_n) = \{\text{id}\}$  при  $n \geq 3$ .

*Доказательство.* Допустим, что в  $Z(G)$  есть  $\sigma \neq \text{id}$ . Разложим в независимые циклы:  $\sigma = (ij...)\dots$ . Так как  $n \geq 3, \exists k \neq i, j$ . Тогда при  $\tau = (jk) : \tau\sigma\tau^{-1} = (ik...)\dots$  - не совпадёт с  $\sigma$  ( $\tau\sigma\tau^{-1}(i) \neq \sigma(i)$ ) - противоречие.  $\square$

**Упражнение.** Докажите, что  $Z(A_n) = \{\text{id}\}$  при  $n \geq 4$ .

*Доказательство.* Допустим, что в  $Z(G)$  есть  $\sigma \neq \text{id}$ . Разложим в независимые циклы:  $\sigma = (ij...)\dots$ . Так как  $n \geq 4, \exists k, l : k, l, i, j$  попарно различны. Тогда при  $\tau = (jkl) : \tau\sigma\tau^{-1} = (ik...)\dots$  - не совпадёт с  $\sigma$  ( $\tau\sigma\tau^{-1}(i) \neq \sigma(i)$ )- противоречие.  $\square$

**Утверждение.**

$$H \trianglelefteq G \iff \begin{cases} H \leq G \\ H - \text{объединение нескольких классов сопряжённости } G \end{cases}$$

*Доказательство.*

$\implies$ : Пусть  $H \trianglelefteq G$ . Очевидно, что  $H \leq G$ .

Если  $h \in H$ , то  $\forall g \in G \ ghg^{-1} \in H$  -  $H$  содержит классы сопряжённости всех её элементов  $\implies H = \bigcup_{h \in H} h^G$ .

$\impliedby$ : Пусть  $H \leq G$  и  $H$  - объединение классов сопряжённости. Тогда  $\forall h \in H, g \in G : ghg^{-1} \in H$  ( $H$  содержит весь класс сопряжённости  $h^G$ )  $\implies H \trianglelefteq G$ .  $\square$

## 6 Теоремы Силова

Пусть  $G$  - конечная группа,  $|G| = p^s \cdot m$ , где  $p$  - простое,  $(p, m) = 1$ .

**Определение.** Подгруппа  $H \leq G$  называется силовской  $p$ -подгруппой, если  $|H| = p^s$ .

*Замечание.* Несложно видеть, что определение корректно: если  $H$  - силовская  $p$ -подгруппа, то  $H$  -  $p$ -подгруппа; более того, это доказано в [упражнении](#) п. 4.4

**Теорема 1.** (Первая теорема Силова - о существовании)

*Силовская  $p$ -подгруппа существует.*

*Замечание.* Напомним, что более общее утверждение  $k \mid |G| \implies \exists H \leq G : |H| = k$  неверно - в  $A_4$  нет подгруппы порядка 6.

**Теорема 2.** (Вторая теорема Силова - о сопряжённости)

*Любая  $p$ -подгруппа лежит в некоторой силовской  $p$ -подгруппе.*

*Все силовские  $p$ -подгруппы сопряжены.*

**Теорема 3.** (Третья теорема Силова - о количестве)

Пусть  $N_p$  - число силовских  $p$ -подгрупп в  $G$ . Тогда 
$$\begin{cases} N_p \equiv 1 \pmod{p} \\ N_p \mid m \end{cases}$$

**Примеры.**

1.  $G = S_3, |G| = 6 = 2 \cdot 3$ . Силовские 2-подгруппы:  $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$ .

2.  $G = S_4, |G| = 24 = 2^3 \cdot 3$ . Найдём силовские 2-подгруппы:

Доказывалось, что  $S_4 \simeq \text{Sym}^+ K$  - группа вращений куба. Можем рассмотреть сечение куба плоскостью, параллельной некоторой паре противоположных граней - вращения, оставляющие квадрат сечения на месте, образуют подгруппу, очевидно изоморфную  $D_4$  (по определению  $D_4$ ). Такая подгруппа будет иметь порядок 8, и таких подгрупп будет 3 - столько же, сколько пар противоположных граней - по III теореме Силова это все силовские  $p$ -подгруппы в  $G$ .

### 6.1 I теорема Силова

Пусть  $G$  - группа,  $|G| = p^s m$ , где  $p$  - простое,  $(p, m) = 1$ . Тогда  $\exists$  силовская  $p$ -подгруппа в  $G$ .

*Доказательство.* Рассмотрим случаи:

1.  $G$  - абелева  $\implies G \simeq \langle a_1 \rangle_{p_1^{s_1}} \times \dots \times \langle a_k \rangle_{p_k^{s_k}}$ . Без ограничения общности  $p_1 = \dots = p_t = p$ ,  $p_{t+1}, \dots, p_k \neq p$ . Тогда  $H \simeq \langle a_1 \rangle_{p^{s_1}} \times \dots \times \langle a_t \rangle_{p^{s_t}}$  - искомая силовская  $p$ -подгруппа: очевидно, что  $H$  является  $p$ -подгруппой, а также  $p^s m = |G| = |H| \cdot |G/H|$ , где  $p \nmid |G/H| \implies p^s \mid |H| \implies |H| = p^s$ .
2. Общий случай ( $G$  - неабелева). Индукция по  $|G|$ :

База:  $n = 1$  - очевидно;

Шаг: Пусть  $G = Z(G) \sqcup x_1^G \sqcup \dots \sqcup x_k^G$  - разложение  $G$  на классы сопряжённости, где  $x_i \notin Z(G)$ , то есть  $|x_i^G| > 1$ . Вновь рассмотрим случаи:

- (a)  $\exists i = \overline{1, \dots, k} : p \nmid |x_i^G|$ . Знаем, что  $|C(x_i)| = \frac{|G|}{|x_i^G|}$ . По предположению индукции в  $C(x_i)$   $\exists$  силовская  $p$ -подгруппа  $H \implies |H| = p^s$  (так как степень вхождения  $p$  в порядок группы не уменьшилась), т.е.  $H$  - силовская  $p$ -подгруппа и для  $G$ ;
- (b)  $\forall i = \overline{1, \dots, k} : p \mid |x_i^G|$ . Тогда  $p \mid |Z(G)| \implies |Z(G)| = p^{s_0} m_0$  ( $(p, m_0) = 1$ ). Так как  $Z(G)$  - абелева, по 1 случаю  $\exists$  силовская  $p$ -подгруппа  $S_0 \leq Z(G)$ ,  $|S_0| = p^{s_0}$ .

По свойству центра  $S_0 \leq Z(G) \implies S_0 \trianglelefteq G$  - можем рассмотреть  $G/S_0$ . Так как  $|G/S_0| < |G|$ , по предположению индукции  $\exists$  силовская  $p$ -подгруппа  $S \leq G/S_0$ .  $|G/S_0| = p^{s-s_0} m \implies |S| = p^{s-s_0}$

Рассмотрим натуральный гомоморфизм  $\pi : G \rightarrow G/S_0$ , и  $\tilde{S} = \pi^{-1}(S)$  - полный прообраз  $S$  при этом гомоморфизме.

$S_0 \subset \tilde{S}$ , так как  $\forall s_0 \in S_0 : \pi(s_0) = eS_0$ , причём  $S_0 \trianglelefteq G \implies S_0 \trianglelefteq \tilde{S}$ , т.е. можем рассмотреть ограничение  $\pi|_{\tilde{S}} : \tilde{S} \rightarrow \tilde{S}/S_0$ .  $\pi|_{\tilde{S}}$  - натуральный гомоморфизм с ядром  $S_0$  и образом  $\pi(\tilde{S}) = S$ .

Натуральный гомоморфизм сюръективен, а отсюда по теореме о гомоморфизме  $|\tilde{S}| = |S_0| \cdot |S| = p^{s_0} \cdot p^{s-s_0} = p^s \implies \tilde{S}$  - искомая силовская  $p$ -подгруппа  $G$ .

□

**Следствие.** Пусть  $|G| < \infty$ . Тогда  $G$  -  $p$ -группа  $\iff |G| = p^s (s \in \mathbb{N})$ .

*Доказательство.*

$\Leftarrow$  - доказано ранее;

$\implies$ : От противного: пусть  $|G|$  содержит простой множитель  $q \neq p$ . Тогда по I теореме Силова  $\exists$  силовская  $q$ -подгруппа в  $G$ , причём в ней хотя бы  $q$  элементов.



Значит, в ней есть элемент порядка  $q^k (k \geq 1)$ , что противоречит определению  $p$ -группы. Отсюда у  $|G|$  нет простых делителей, отличных от  $p \implies |G| = p^s$ .  $\square$

## 6.2 II теорема Силова

Пусть  $G$  - группа,  $|G| = p^s m$ , где  $p$  - простое,  $(p, m) = 1$ .

Тогда любая  $p$ -подгруппа группы  $G$  лежит в некоторой силовой  $p$ -подгруппе. Все силовые  $p$ -подгруппы группы  $G$  сопряжены.

*Доказательство.* Пусть  $|G| = p^s m$ , где  $p$  - простое,  $(p, m) = 1$ .

По I теореме Силова  $\exists$  силовая  $p$ -подгруппа  $S \leq G$ . Рассмотрим  $H \leq G$  - произвольную нетривиальную  $p$ -подгруппу (случай  $H = \{e\}$  очевиден).

Рассмотрим множество  $X = \{g_1 S, \dots, g_m S\}$  смежных классов  $G$  по  $S$  и действие  $H \curvearrowright X$ , заданное по правилу  $\alpha(h)g_i S = hg_i S$ .

$$|\text{Orb}(g_i S)| \mid |H| \implies \begin{cases} |\text{Orb}(g_i S)| = 1 \\ p \mid |\text{Orb}(g_i S)| \end{cases} \quad (|H| = p^m \text{ по следствию из I т. Силова}).$$

Предположим, что  $\forall i = \overline{1, \dots, m} : p \mid |\text{Orb}(g_i S)|$ . Тогда  $p \mid \sum_i |\text{Orb}(g_i S)| = |X|$ .

Однако  $|X| = m$  - взаимно просто с  $p$ . Противоречие.

Отсюда  $\exists i = \overline{1, \dots, m} : |\text{Orb}(g_i S)| = 1$ , т.е. точка  $g_i S$  неподвижна при  $H \curvearrowright X$ . Значит,  $\forall h \in H \quad hg_i S = g_i S \implies h \in g_i S g_i^{-1} \implies H \leq g_i S g_i^{-1}$ . Так как  $|g_i S g_i^{-1}| = |S|$ ,  $g_i S g_i^{-1}$  - силовая  $p$ -подгруппа, т.е.  $H$  лежит в силовой  $p$ -подгруппе  $G$ .

Заметим, что в доказательстве выше подгруппа  $S$  зафиксирована.

Если рассмотреть  $H$  - произвольную силовую  $p$ -подгруппу  $G$ , то  $|H| = p^s$ . Так как  $H \leq g_i S g_i^{-1}$ ,  $|g_i S g_i^{-1}| = p^s \implies H = g_i S g_i^{-1}$  - любая силовая  $p$ -подгруппа сопряжена с  $S$ . Значит, все силовые  $p$ -подгруппы сопряжены.  $\square$

**Следствие.** Пусть  $G$  - группа,  $|G| = p^s m$ , где  $p$  - простое,  $(p, m) = 1$ .

Тогда силовая  $p$ -подгруппа в  $G$  единственна  $\iff$  эта подгруппа нормальна.

*Доказательство.*

$\Leftarrow$ : Пусть  $S \trianglelefteq G$  - силовая  $p$ -подгруппа. По II теореме Силова все силовые  $p$ -подгруппы сопряжены с  $S$ , а из нормальности совпадают с  $S$ .

(из нормальности следует включение  $g S g^{-1} \subseteq G$ , а также  $|g S g^{-1}| = |S| = p^s$ )

$\implies$ : Если  $S$  - единственная, то  $\forall g \in G : g S g^{-1} = S$ , т.к. сопряженной к силовой  $p$ -подгруппе должна быть силовая  $p$ -подгруппа. Отсюда  $S \trianglelefteq G$ .  $\square$

### 6.3 Нормализатор. III теорема Силова

Пусть  $G$  - группа,  $H \leq G$ ,  $X = \{gHg^{-1} \mid g \in G\}$ .

Рассмотрим действие  $G \curvearrowright X : \alpha(\tilde{g})(gHg^{-1}) = \tilde{g}(gHg^{-1})\tilde{g}^{-1}$

Для точки  $H \in X : \text{Orb}(H) = X$ ,  $\text{St}(H) = \{\tilde{g} \in G \mid \tilde{g}H\tilde{g}^{-1} = H\} \leq G$

**Определение.** Стабилизатор  $H$  относительно этого действия называется нормализатором группы  $H$ . Обозначается  $N_G(H)$ .

**Утверждение 1.** Если  $|G| < \infty$ , то  $|G| = |X| \cdot |N_G(H)|$ , где  $X$  - число подгрупп, сопряжённых с  $H$ . В частности,  $|X| = |G : N_G(H)|$ .

*Доказательство.* Очевидно следует из утверждения  $|\text{Orb}(x)| = \frac{|G|}{|\text{St}(x)|}$ . □

**Утверждение 2.**  $N_G(H)$  - наибольшая (по включению) подгруппа  $G$ , содержащая  $H$  как нормальную подгруппу.

*Доказательство.* Из определения  $N_G(H)$  очевидно, что  $H \trianglelefteq N_G(H)$ .

Пусть  $H \trianglelefteq K \leq G$ . Тогда  $\forall g \in K \ gHg^{-1} = H \implies g \in N_G(H)$ .

Отсюда  $K \leq N_G(H)$ . □

#### III теорема Силова

Пусть  $G$  - группа,  $|G| = p^s m$ , где  $p$  - простое,  $(p, m) = 1$ .

Пусть  $N_p$  - число силовских  $p$ -подгрупп в  $G$ . Тогда  $N_p \equiv 1 \pmod{p}$ ,  $N_p \mid m$ .

*Доказательство.*

Пусть  $S$  - произвольная силовская  $p$ -подгруппа  $G$  (хотя бы одна существует по I теореме Силова). Рассмотрим  $X = \{gSg^{-1} \mid g \in G\}$ . По II теореме Силова все силовские  $p$ -подгруппы  $G$  сопряжены, а также порядок любой подгруппы вида  $gSg^{-1}$  равен  $|S|$ , т.е.  $gSg^{-1}$  - также силовская  $p$ -подгруппа. Отсюда  $X$  - множество всех силовских подгрупп  $G$ .

$|X| = N_p \implies$  по утверждению 1 получаем  $N_p \mid |G|$ . Осталось показать, что  $N_p \equiv 1 \pmod{p}$  (если это так, то  $N_p \mid |G| = p^s m \implies N_p \mid m$ ).

Рассмотрим действие  $S \curvearrowright X$  сопряжениями. Очевидно,  $S$  - неподвижная точка относительно него. Также  $N_p = |X| = \sum_{i=1}^k |\text{Orb}(x_i)|$ . При этом

$$|\text{Orb}(x_i)| \mid |S| = p^s \implies \begin{cases} |\text{Orb}(x_i)| = 1 \\ p \mid |\text{Orb}(x_i)| \end{cases}$$

Значит, достаточно показать, что  $S$  - единственная неподвижная точка относительно данного движения (тогда  $|X| = \sum_{i=1}^k |\text{Orb}(x_i)| \equiv |\text{Orb}(S)| = 1 \pmod{p}$ )

Допустим, что  $\tilde{S}$  - неподвижная точка  $\implies \forall g \in S \ g\tilde{S}g^{-1} = \tilde{S}$ .

Рассмотрим нормализатор  $N_G(\tilde{S})$ . Знаем, что  $\tilde{S} \subseteq N_G(\tilde{S})$ , а из неподвижности точки  $\tilde{S}$  имеем  $S \subseteq N_G(\tilde{S})$ . Также  $N_G(\tilde{S}) \leq G$ , то есть степень вхождения  $p$  в  $|N_G(\tilde{S})|$  также равна  $s$ . Значит,  $S, \tilde{S}$  - силовские  $p$ -подгруппы в  $N_G(\tilde{S})$ . Тогда по II теореме Силова  $S$  и  $\tilde{S}$  сопряжены в  $N_G(\tilde{S})$ , т.е.  $S = g\tilde{S}g^{-1}, g \in N_G(\tilde{S})$ , а тогда по определению нормализатора  $S = \tilde{S}$ . Значит,  $S$  - единственная неподвижная точка.  $\square$

**Упражнение.** Доказать, что любая группа порядка 15 циклическая.

*Доказательство.* Пусть  $G$  - группа порядка 15. По I теореме Силова в ней есть силовские подгруппы порядка 3 и порядка 5. Притом по III теореме Силова:

$$N_3 \equiv 1 \pmod{3}, \quad N_3 \mid 5 \implies N_3 = 1$$

$$N_5 \equiv 1 \pmod{5}, \quad N_5 \mid 3 \implies N_5 = 1$$

Таким образом, в  $G$  есть по одной силовской подгруппе порядка 3 и 5, а по следствию из III теоремы Силова они обе нормальны в  $G$ . Так как их порядки простые, обе эти подгруппы циклические, т.е. изоморфны  $\mathbb{Z}_3$  и  $\mathbb{Z}_5$  соответственно.

Остаётся заметить, что эти подгруппы пересекаются тривиально (у остальных элементов разные порядки), т.е. некоторая подгруппа  $G$  раскладывается в их прямое произведение, а так как  $15 = 3 \cdot 5$ , эта подгруппа - вся  $G$ . Отсюда  $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$  - циклическая.  $\square$

## 7 Коммутант

**Определение.** Пусть  $G$  - произвольная группа,  $x, y \in G$ .

Коммутатором элементов  $x, y$  называется элемент  $[x, y] = xyx^{-1}y^{-1}$ .

**Свойства.**

1.  $[x, y] = e \iff xy = yx$ ;
2.  $[x, y]^{-1} = [y, x]$ ;
3.  $\forall g \in G \quad g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$ .

*Доказательство.* 1, 2 - очевидно;

$$3 : [gxg^{-1}, gyg^{-1}] = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = gxyx^{-1}y^{-1}g^{-1} = g[x, y]g^{-1}$$

□

**Определение.** Коммутантом группы  $G$  называется подгруппа, порождённая всеми коммутаторами элементов группы  $G$ . Обозначается  $[G]$  или  $G'$ .

$$G' = \left\{ \prod_{i=1}^k [x_i, y_i] \mid x_i, y_i \in G \right\}.$$

**Утверждение.**  $G' = \{e\} \iff G$  - абелева.

*Доказательство.* Очевидно из свойства 1 коммутатора.

□

**Утверждение.**  $G' \trianglelefteq G$

*Доказательство.*

$$\begin{aligned} \forall g \in G, g' \in G' : g' = [x_1, y_1][x_2, y_2] \dots [x_k, y_k] \in G' : gg'g^{-1} &= g[x_1, y_1][x_2, y_2] \dots [x_k, y_k]g^{-1} = \\ &= (g[x_1, y_1]g^{-1})(g[x_2, y_2]g^{-1}) \dots (g[x_k, y_k]g^{-1}) = [gx_1g^{-1}, gy_1g^{-1}] \dots [gx_kg^{-1}, gy_kg^{-1}] \end{aligned}$$

Отсюда  $\forall g \in G, g' \in G' : gg'g^{-1} \in G' \implies G' \trianglelefteq G$ .

□

**Утверждение.** Если  $H \leq G$  и  $G' \leq H$ , то  $H \trianglelefteq G$ .

*Доказательство.*  $\forall g \in G, h \in H : ghg^{-1} = (ghg^{-1}h^{-1})h \in H$ .

□

**Утверждение.** Пусть  $N \trianglelefteq G$ . Тогда  $G/N$  абелева  $\iff G' \subseteq N$ .

*Доказательство.*

$\implies$ : Пусть  $G/N$  абелева. Тогда  $\forall g_1, g_2 \in G : (g_1N)(g_2N) = (g_2N)(g_1N) \implies g_1g_2N = g_2g_1N \implies g_1g_2g_1^{-1}g_2^{-1} = [g_1, g_2] \in N$ . Значит, любой коммутатор  $\in N$ , а значит и все произведения коммутаторов  $\in N$ , то есть  $G' \subseteq N$ .

$\impliedby$ : Пусть  $G' \subseteq N$ . Тогда  $\forall g_1, g_2 \in G : [g_1, g_2] = g_1g_2g_1^{-1}g_2^{-1} \in N \implies g_1g_2N = g_2g_1N \implies (g_1N)(g_2N) = (g_2N)(g_1N)$ .

□

## 7.1 Коммутанты некоторых известных групп

**Лемма 1.**

1.  $A_n$  порождается циклами длины 3;
2. Если  $n \geq 5$ , то  $A_n$  порождается произведениями пар независимых транспозиций;

*Доказательство.*  $\forall \sigma \in A_n \quad \sigma = \prod_{i=1}^k \tau_i$ , где  $\tau_i$  - транспозиции,  $k$  - чётное, т.е. транспозиции разбиваются на пары - в паре транспозиции могут быть зависимы либо независимы.

Если  $i, j, k, l$  - различные (случай  $n \leq 3$  очевиден), то

$$(ij)(jk) = (ijk); \quad (ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$$

то есть  $\sigma$  представима как произведение тройных циклов.

Если  $n \geq 5$ , то  $\exists i, j, k, l, m$  - различные, а тогда  $(ij)(jk) = ((ij)(lm))((lm)(jk))$ . Таким образом можно избавиться от пар зависимых транспозиций, то есть  $\sigma$  представима как произведение пар независимых транспозиций.  $\square$

**Утверждение.**  $S'_n = A_n$ .

*Доказательство.*  $|S_n/A_n| = 2 \implies S_n/A_n$  - абелева  $\implies S'_n \subseteq A_n$ . Значит, достаточно доказать (по лемме 1), что  $\forall i, j, k$  (различных)  $(ikj) \in S'_n$ .

$$[(ij), (jk)] = (ij)(jk)(ij)^{-1}(jk)^{-1} = (ik)(kj) = (ikj)$$

$\square$

**Утверждение.**

1.  $n = 1, 2, 3 \implies A'_n = \{\text{id}\};$
2.  $n = 4 \implies A'_n = V_4;$
3.  $n \geq 5 \implies A'_n = A_n.$

*Доказательство.*

1.  $n = 1, 2, 3$  -  $A'_n = \{\text{id}\}$ , т.к.  $A_n$  - абелева;
2.  $n = 4$ :  $V_4 \trianglelefteq A_4, |V_4| = 4 \implies |A_4/V_4| = 3$  - абелева. Значит,  $A'_4 \subseteq V_4$ .

$$[(ijk), (ijm)] = (ijk)(ijm)(ijk)^{-1}(ijm)^{-1} = (jkm)(imj) = (ij)(km)$$

3.  $n \geq 5$ : По пункту 2 леммы 1  $A_n$  порождается парами независимых транспозиций. Аналогично  $[(ijk), (ijm)] = (ij)(km)$ , а значит, все элементы  $A_n$  принадлежат  $A'_n$ .

□

**Лемма 2.** *Группа  $SL_n(\mathbb{F})$  порождается элементарными матрицами, соответствующими преобразованиям  $I$  типа  $(a_i \mapsto a_i + \lambda a_j)$ .*

*Доказательство.* Покажем, что  $\forall A \in SL_n(\mathbb{F})$  приводится к  $E$  за конечное число операций  $I$  типа (над строками):

Индукция по  $n$ . База  $n = 1$  очевидна ( $\det A = a_{11} = 1 \implies A = E$ )

Шаг: Так как  $\det A \neq 0$ ,  $\exists i : a_{i1} \neq 0$ .

Если  $a_{11} = 0$ , то прибавим  $i$ -ю строку к первой - сделаем  $a_{11} \neq 0$ . Пусть  $n \geq 2$  (случай  $n = 1$ )

Если  $a_{11} \neq 1$ , то сделаем  $a_{12} \neq 0$  аналогично  $a_{11}$ , а далее прибавим к первой строке вторую, умноженную на  $\frac{1-a_{11}}{a_{12}}$  - сделаем  $a_{11} = 1$ . Далее с помощью первой строки сможем занулить оставшиеся элементы первого столбца. По предположению индукции подматрицу полученной матрицы без первой строки и первого столбца можно привести к единичному виду. Сделаем это, а далее с помощью  $i$ -й строки занулим  $a_{1i}$ .

Значит,  $\forall A \in SL_n(\mathbb{F})$  приводится к  $E$  за конечное число операций  $I$  типа над строками, то есть раскладывается в произведение соответствующих элементарных матриц.

□

**Утверждение.** Пусть  $|\mathbb{F}| > 3$ . Тогда  $GL_n(\mathbb{F})' = SL_n(\mathbb{F})' = SL_n(\mathbb{F})$ .

*Доказательство.* Заметим, что  $GL_n(\mathbb{F})/SL_n(\mathbb{F}) = \mathbb{F}^*$  из теоремы о гомоморфизме для  $\alpha : GL_n(\mathbb{F}) \rightarrow \mathbb{F}^*$  такого, что  $\alpha(A) = \det A$ . Отсюда  $GL_n(\mathbb{F})/SL_n(\mathbb{F})$  - абелева (как мультипликативная группа поля), т.е.  $GL_n(\mathbb{F})' \subseteq SL_n(\mathbb{F})$ .

Если  $|\mathbb{F}| > 3$ , то  $\exists \lambda \in \mathbb{F} : \lambda \neq 0, 1, -1$ .

$$n = 2 : \left[ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (\lambda^2 - 1)a \\ 0 & 1 \end{pmatrix} \quad (\lambda \neq 0)$$

Любое ур-е  $(\lambda^2 - 1)a = \mu$  решается для  $a$ , так как  $\lambda \neq \pm 1$  - отсюда все верхнетреугольные элементарные матрицы  $I$  типа принадлежат  $GL_n(\mathbb{F})'$ . Аналогично для нижнетреугольных - все элементарные матрицы  $I$  типа, а отсюда и  $SL_n(\mathbb{F})$ , принадлежат  $GL_n(\mathbb{F})'$ .

Случай  $n > 2$  аналогичен: необходимо рассмотреть коммутатор

$$[E + (\lambda - 1)E_{ii} + (\lambda^{-1} - 1)E_{jj}, E + aE_{ij}] = E + (\lambda^2 - 1)aE_{ij} \quad (i \neq j)$$

Все рассуждения верны и для доказательства  $SL_n(\mathbb{F}) \subseteq SL_n(\mathbb{F})'$ , т.к. определители всех рассматриваемых при взятии коммутаторов матриц равны 1.  $\square$

## 8 Разрешимые и простые группы

### 8.1 Разрешимые группы

**Определение.** Кратный коммутант группы  $G$ :

$$G^{(1)} = G; \quad G^{(k+1)} = [G^{(k)}, G^{(k)}] = (G^{(k)})'$$

Очевидно, что  $G \geq G^{(1)} \geq G^{(2)} \geq \dots$

**Определение.** Группа  $G$  называется разрешимой, если  $\exists m \in \mathbb{N} : G^{(m)} = \{e\}$ .

**Утверждение.**  $G$  - абелева  $\implies G$  - разрешимая.

*Доказательство.*  $G$  - абелева  $\implies G' = \{e\}$ . □

**Утверждение.**

1.  $S_n$  - разрешимая  $\iff n \leq 4$ ;

2.  $A_n$  - разрешимая  $\iff n \leq 4$ .

*Доказательство.*  $S'_n = A_n$ , поэтому  $S_n$  - разрешимая  $\iff A_n$  - разрешимая.

$A_2 = \{\text{id}\}$ ,  $A_3 \simeq \mathbb{Z}_3$  - абелева,  $A'_4 = V_4$  - абелева  $\implies$  при  $n \leq 4$   $A_n$  разрешима.

При  $n \geq 5$   $A'_n = A_n$ , то есть  $A_n$  - не разрешимая. □

**Утверждение.** Пусть  $\mathbb{F}$  - поле,  $|\mathbb{F}| > 3$ . Тогда  $GL_n(\mathbb{F})$  и  $SL_n(\mathbb{F})$  не разрешимы.

*Доказательство.*  $GL_n(\mathbb{F})' = SL_n(\mathbb{F})' = SL_n(\mathbb{F})$ . □

**Утверждение.**

1.  $G$  - разрешимая,  $H \leq G \implies H$  - разрешимая;

2.  $G$  - разрешимая,  $H \trianglelefteq G \implies G/H$  - разрешимая;

3.  $H \trianglelefteq G$ ,  $H$  и  $G/H$  - разрешимые  $\implies G$  - разрешимая.

*Доказательство.*

1. Для начала заметим, что  $H \leq G \implies H' \leq G'$ , так как любой коммутатор элементов из  $H$  - также коммутатор элементов из  $G$ . Значит,  $H^{(m)} \leq G^{(m)}$ .  
 $G$  разрешима  $\implies \exists m : G^{(m)} = \{e\} \implies H^{(m)} = \{e\} \implies H$  разрешима.



2. Рассмотрим натуральный гомоморфизм  $\pi : G \rightarrow G/H$ . Очевидно, что образ коммутатора при гомоморфизме - коммутатор:

$$\alpha([x, y]) = \alpha(xy x^{-1} y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} = [\alpha(x), \alpha(y)]$$

то есть  $\pi(G') \subseteq (G/H)'$ . При этом натуральный гомоморфизм сюръективен, а прообраз коммутатора - также коммутатор (аналогично), то есть  $\pi(G') = (G/H)'$ . Аналогично  $\pi(G^{(m)}) = (G/H)^{(m)}$ .

$G$  разрешима  $\implies \exists m : G^{(m)} = \{e\} \implies \pi(G^{(m)}) = (G/H)^{(m)} = \{e\}$ .

3.  $(G/H)$  разрешима  $\implies \exists k : (G/H)^{(k)} = \{e\} \implies \pi(G^{(k)}) = \{e\} \implies G^{(k)} \subseteq H$ .  
Также  $H$  разрешима  $\implies \exists l : H^{(l)} = \{e\} \implies (G^{(k)})^{(l)} = G^{(k+l)} = \{e\}$ .  
Значит,  $G$  разрешима.

□

**Утверждение.** Группа  $T_n(\mathbb{F})$  невырожденных верхнетреугольных матриц порядка  $n$  с коэффициентами из поля  $\mathbb{F}$  разрешима.

*Доказательство.* Индукция по  $n$ :

База:  $n = 1 \implies T_1(\mathbb{F}) \simeq \mathbb{F}^*$  - абелева, а значит, разрешима;

Шаг: пусть  $T_{n-1}(\mathbb{F})$  разрешима. Рассмотрим гомоморфизм  $\varphi : T_n \rightarrow T_{n-1}$ :

$$\varphi : \left( \begin{array}{ccc|c} a_{11} & & * & a_{1n} \\ & \ddots & & a_{2n} \\ 0 & & a_{n-1n-1} & a_{n-1n} \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right) \mapsto \left( \begin{array}{ccc|c} a_{11} & & * & \\ & \ddots & & \\ 0 & & a_{n-1n-1} & \end{array} \right)$$

Этот гомоморфизм, очевидно, сюръективен, т.е по теореме о гомоморфизме  $T_n/\text{Ker } \varphi \simeq T_{n-1}$ . Так как  $T_{n-1}$  разрешима по предположению индукции, по пункту 3 предыдущего утверждения достаточно доказать разрешимость группы

$$\text{Ker } \varphi = \left\{ \left( \begin{array}{ccc|c} & & & a_{1n} \\ & \text{E} & & a_{2n} \\ & & & a_{n-1n} \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right) : a_{in} \in \mathbb{F}, a_{nn} \neq 0 \right\}$$

Аналогично, рассмотрим гомоморфизм  $\psi : \text{Ker } \varphi \rightarrow \mathbb{F}^*$ :

$$\psi : \left( \begin{array}{ccc|c} & & & a_{1n} \\ & \text{E} & & a_{2n} \\ & & & a_{n-1n} \\ \hline 0 & \dots & 0 & a_{nn} \end{array} \right) \mapsto a_{nn}$$

Заметим, что  $\text{Im } \psi = \mathbb{F}^*$  - абелева, а  $\text{Ker } \psi$  состоит из матриц  $\text{Ker } \varphi$  с  $a_{nn} = 1$ .

$$\left( \begin{array}{c|c} \text{E} & \begin{matrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{n-1n} \end{matrix} \\ \hline 0 & 1 \end{array} \right) \cdot \left( \begin{array}{c|c} \text{E} & \begin{matrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{n-1n} \end{matrix} \\ \hline 0 & 1 \end{array} \right) = \left( \begin{array}{c|c} \text{E} & \begin{matrix} a_{1n} + b_{1n} \\ a_{2n} + b_{2n} \\ \vdots \\ a_{n-1n} + b_{n-1n} \end{matrix} \\ \hline 0 & 1 \end{array} \right)$$

Отсюда несложно видеть, что  $\text{Ker } \psi$  - также абелева, то есть разрешимая группа. Значит,  $\text{Ker } \varphi$  разрешима, а отсюда и  $T_n(\mathbb{F})$  - разрешимая группа.  $\square$

**Утверждение 1.** *Всякая конечная примарная группа  $G$  разрешима.*

*Доказательство.* Пусть  $p$  - простое, для которого  $G$  является  $p$ -группой.

Индукция по  $n = |G|$ :

База:  $n = 1 \implies G = \{e\}$  - разрешима;

Шаг:  $G \neq \{e\} \implies Z(G) \neq \{e\}$  (из примарности). Знаем, что  $Z(G) \trianglelefteq G$  - рассмотрим  $G/Z(G)$ . Это также  $p$ -группа, причём порядка  $\frac{|G|}{|Z(G)|}$ , что меньше  $n$ . Значит,  $G/Z(G)$  разрешима по предположению индукции, а также  $Z(G)$  разрешима, так как абелева. Отсюда  $G$  разрешима.  $\square$

**Утверждение 2.** *Всякая группа  $G$  порядка  $pq$ , где  $p, q$  простые, разрешима.*

*Доказательство.* Случай  $p = q$  очевиден из утверждения 1.

Пусть  $p \neq q$  - без ограничения общности  $p > q$ .

По I теореме Силова  $\exists$  силовская  $p$ -подгруппа  $H \leq G$ .

$$\text{По III теореме Силова } \begin{cases} N_p \mid q \\ N_p \equiv 1 \pmod{p} \end{cases} \implies N_p = 1$$

(не может равняться  $q$  в силу  $q < p$ )

Тогда по следствию из II теоремы Силова единственная силовская  $p$ -подгруппа  $H$  нормальна в  $G$ . Притом  $|H| = p \implies H \simeq \mathbb{Z}_p$  и  $|G/H| = q \implies G/H \simeq \mathbb{Z}_q$  - абелевы. Значит,  $H$  и  $G/H$  разрешимы, а отсюда  $G$  разрешима.  $\square$

## 8.2 Простые группы

**Определение.** Подгруппа  $H \leq G$  называется собственной, если  $H \neq \{e\}, G$ .

**Определение.** Группа  $G$  называется простой, если  $G \neq \{e\}$  и в  $G$  нет собственных нормальных подгрупп.

**Утверждение 1.** *Абелева группа  $G$  - простая  $\iff G \simeq \mathbb{Z}_p$ , где  $p$  - простое.*

*Доказательство.*

$\Leftarrow$  - очевидно ( $\mathbb{Z}_p$  - циклическая, т.е. нет собственных подгрупп);

$\Rightarrow$ : Пусть  $G$  - абелева и простая группа.

Тогда  $G$  циклическая, так как  $\forall g \neq e : \langle g \rangle \trianglelefteq G$  (т.к. абелева) и  $g \notin \{e\}$ , т.е.  $\langle g \rangle = G$ . Теперь, если  $G$  бесконечна, то  $G \simeq \mathbb{Z}$ , но  $2\mathbb{Z} \triangleleft \mathbb{Z}$  - противоречие, т.е.  $G$  конечна. А если  $|G|$  составное, то  $G \simeq \mathbb{Z}_{mn}$ , где  $\langle m \rangle \triangleleft \mathbb{Z}_{mn}$  ( $m, n \neq 1$ ). Значит,  $|G|$  простое, т.е.  $G \simeq \mathbb{Z}_p$ .  $\square$

**Утверждение 2.** Если  $G$  - разрешимая и простая, то  $G \simeq \mathbb{Z}_p$ , где  $p$  - простое.

*Доказательство.* Так как  $G$  разрешима,  $G' \neq G$ . Притом  $G' \trianglelefteq G$ , а отсюда из простоты  $G' = \{e\}$ . Значит,  $G$  - абелева, а тогда  $\simeq \mathbb{Z}_p$  из утверждения 1.  $\square$

*Замечание.* Таким образом, всякая простая группа либо изоморфна  $\mathbb{Z}_p$ , либо не абелева и не разрешима.

### 8.3 Значение простых групп

**Определение.** Субнормальной матрёшкой называется последовательность

$$G = G_0 \geq G_1 \geq \dots \geq G_m = \{e\}; \quad G_{i+1} \trianglelefteq G_i \quad \forall i = \overline{0 \dots m-1}$$

**Пример.**  $G = A_4, H = V_4, K = \langle (12)(34) \rangle$ . Тогда  $H \trianglelefteq G, K \trianglelefteq H$ , то есть  $G \geq H \geq K \geq \{\text{id}\}$  - субнормальная матрёшка.

**Теорема.** Группа  $G$  разрешима  $\iff G$  обладает субнормальной матрёшкой такой, что  $G_i/G_{i+1}$  - абелева  $\forall i = \overline{0 \dots m-1}$ .

*Доказательство.* Без доказательства.  $\square$

**Определение.** Композиционным рядом называется субнормальная матрёшка такая, что  $\forall i = \overline{0 \dots m-1} : G_i \neq G_{i+1}$  и  $G_i/G_{i+1}$  - простая группа.

**Утверждение 3.** Всякая конечная группа  $G$  обладает композиционным рядом.

*Доказательство.* Если  $G$  - простая, то  $G \geq \{e\}$  - композиционный ряд.

Если  $G$  - не простая, то  $\exists$  собственная подгруппа  $N \trianglelefteq G$ , т.е.  $G \geq N \geq \{e\}$  - субнормальная матрёшка. Будем уплотнять эту матрёшку следующим образом:

Предположим, что в субнормальной матрёшке  $G_0 \geq \dots \geq G_m$  группа  $G_i/G_{i+1}$  - не простая. Тогда  $\exists$  собственная  $\tilde{N} \trianglelefteq G_i/G_{i+1}$ .

Рассмотрим натуральный гомоморфизм  $\pi : G_i \rightarrow G_i/G_{i+1}$ . Тогда  $\pi^{-1}(\tilde{N}) = \tilde{N}$

- собственная нормальная подгруппа  $G_i$ , содержащая  $G_{i+1}$ , то есть в матрёшке кусок "...  $\supseteq G_i \supseteq G_{i+1} \supseteq \dots$ " заменяем на "...  $\supseteq G_i \supseteq \tilde{N} \supseteq G_{i+1} \supseteq \dots$ ". Очевидно, что процесс таких уплотнений конечен, так как количество членов матрёшки явно не превышает  $|G|$  (порядок строго убывает). Значит, за конечное число уплотнений сможем построить композиционный ряд для  $G$ .  $\square$

**Теорема.** (Жордана - Гёльдера)

Если группа  $G$  обладает композиционным рядом, то набор факторгрупп в нём определён однозначно с точностью до перестановки.

*Доказательство.* Без доказательства.  $\square$

**Пример.** Пусть  $G = \langle a \rangle_{12}$ . Композиционные ряды:

$$\langle a \rangle_{12} > \langle a_6 \rangle > \langle a_3 \rangle > \{e\} \quad - \quad \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3;$$

$$\langle a \rangle_{12} > \langle a_6 \rangle > \langle a_2 \rangle > \{e\} \quad - \quad \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2;$$

$$\langle a \rangle_{12} > \langle a_4 \rangle > \langle a_2 \rangle > \{e\} \quad - \quad \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2;$$

*Замечание.* Группа  $G$  не задаётся однозначно набором простых факторов композиционного ряда: пусть набор факторов -  $\mathbb{Z}_2, \mathbb{Z}_2$ , тогда возможны композиционные ряды  $0 < \mathbb{Z}_2 < \mathbb{Z}_4$  и  $0 < \mathbb{Z}_2 < \mathbb{Z}_2 \oplus \mathbb{Z}_2 \simeq V_4$ .

## 8.4 Примеры простых групп

**Упражнение.** Если  $|G| < 60$  и  $|G|$  - не простое, то  $G$  - не простая группа.

*Доказательство.* (довольно объёмное и вряд ли пригодится)

Всё в лучших традициях - докажем несколько лемм:

**Лемма 1.** Всякая неабелева примарная группа не является простой.

*Доказательство.* Очевидно из нетривиальности центра - он не совпадает со всей группой из неабелевости, а значит является собственной нормальной подгруппой  $G$   $\square$

**Лемма 2.** Пусть  $G$  - неабелева группа,  $|G| = p^l m$ , где  $p \nmid m$ ,  $p^l \nmid (m-1)!$ . Тогда  $G$  - не простая группа.

*Доказательство.* Случай  $m = 1$  очевиден из леммы 1.

Пусть  $m > 1$ . Рассмотрим действие  $G \curvearrowright G/S$  левыми сдвигами ( $G/S$  - множество левых смежных классов). Таких смежных классов ровно  $m$  (из теоремы

Лагранжа), причём каждый элемент  $g$  переводит разные смежные классы в разные - отсюда каждый элемент  $G$  соответствует некоторой подстановке из  $S_m$ , то есть определён гомоморфизм  $\alpha : G \rightarrow S_m$ . Если  $G$  простая, то  $\text{Ker } \alpha = \{e\}$  либо  $G$  - второе, очевидно, невозможно (класс  $g_1S$  в класс  $g_2S$  переводит элемент  $g_2g_1^{-1}$ ). Значит,  $G \simeq \alpha(G) \leq S_m$  из теоремы о гомоморфизме. Отсюда  $|G| \mid |S_m| \implies p^l m \mid m! \implies p^l \mid (m-1)!$  - противоречие.  $\square$

*Замечание.* Данная лемма очень сильна при решении некоторых упражнений - например, из неё несложными рассуждениями следует непростота (а по индукции и разрешимость) групп порядков  $2p^k, 3p^k, 4p^k$  ( $p$  - простое).

Остаётся лишь перебор случаев составных чисел  $< 60$  - целиком его несложно провести самому, поэтому здесь он приведён не будет в целях сохранения моего морального и физического благополучия.

В результате под лемму 2 не попадут порядки 30, 40 и 56 - разберём их:

- $|G| = 40 = 2^3 \cdot 5$ : По III теореме Силова в  $G$  единственная подгруппа порядка 5 ( $N_5 \mid 8, N_5 \equiv 1 \pmod{5}$ ) - она нормальна;
- $|G| = 30 = 2 \cdot 3 \cdot 5$ : По III теореме Силова число силовских 5-подгрупп в  $G$  либо 1, либо 6 ( $N_5 \mid 6, N_5 \equiv 1 \pmod{5}$ ). Если такая подгруппа единственна - то она нормальна, и  $G$  не простая. Аналогично силовских 3-подгрупп либо 1, либо 10 - случай единственности очевиден. Остаётся заметить, что порядки самих силовских подгрупп простые, то есть эти подгруппы циклические - значит, различные 3- и 5-подгруппы пересекаются тривиально. Значит, в  $G$  есть  $6 \cdot (5-1) = 24$  различных элементов порядка 5 и  $10 \cdot (3-1) = 20$  различных элементов порядка 3, что невозможно для группы порядка 30.
- $|G| = 56 = 2^3 \cdot 7$ : По III теореме Силова силовских 7-подгрупп в  $G$  либо 1, либо 8 ( $N_7 \mid 8, N_7 \equiv 1 \pmod{7}$ ). Случай  $N_7 = 1$  очевиден, а иначе по рассуждениям выше силовские 7-подгруппы пересекаются тривиально, а значит в  $G$  есть хотя бы  $8 \cdot (7-1) = 48$  различных элементов порядка 7. При этом в  $G$  есть силовская 2-подгруппа, которой принадлежат 8 элементов порядка  $2^k$  - либо она единственна, то есть нормальна, либо их больше одной, что невозможно в группе порядка  $56 = 48 + 8$ .

Все случаи разобраны.  $\square$

**Теорема.** Если  $G$  - простая и  $|G| = 60$ , то  $G \simeq A_5$ .

*Доказательство.* Без доказательства.  $\square$

**Пример.**  $A_2 = \{\text{id}\}$ ,  $A_3 \simeq \mathbb{Z}_3$  - простая,  $A_4$  - не простая ( $V_4 \trianglelefteq A_4$ ).

**Лемма.** Пусть  $n \geq 5$ ,  $N \leq A_n$ ,  $N \neq \{\text{id}\}$ ,  $N \trianglelefteq S_n$ . Тогда  $A_n = N$ .

*Доказательство.* Так как  $N \neq \{\text{id}\}$ , то  $\exists \sigma \in N, \sigma \neq \text{id}$ . Разложим  $\sigma$  в независимые циклы:  $\sigma = c_1 c_2 \dots c_k$ . Рассмотрим случаи:

1.  $\exists i$  такой, что длина  $c_i \geq 3$ , то можем считать, что  $c_1 = (i_1 \dots i_k), k \geq 3$ . Так как  $N \trianglelefteq S_n, \forall \tau \in S_n : \tau \sigma \tau^{-1} \in N$ . Рассмотрим  $\tau = (i_1 i_2)$ :

$$\tau \sigma \tau^{-1} \sigma^{-1} \in N; \tau \sigma \tau^{-1} \sigma^{-1} = \tau c_1 \tau^{-1} c_1^{-1} = (i_2 i_1 i_3 \dots i_k)(i_k \dots i_1) = (i_1 i_2 i_3)$$

( $\tau \sigma \tau^{-1} \sigma^{-1} = \tau c_1 \tau^{-1} c_1^{-1}$ , так как остальные циклы в  $\sigma$  независимы с  $\tau$ , т.е. коммутируют с  $\tau$ )

Тогда в  $N$  содержатся все тройные циклы -  $A_n = N$ .

2. Если же  $\forall i$  длина  $c_i$  равна 2, то  $k$  - чётно, т.е.  $\sigma = (i_1 i_2)(i_3 i_4) c_3 \dots c_k$ .

Тогда при аналогичных рассуждениях и  $\tau = (i_2 i_3)$ :

$$\begin{aligned} \tau \sigma \tau^{-1} \sigma^{-1} &= (i_2 i_3)(i_1 i_2)(i_3 i_4)(i_2 i_3)(i_1 i_2)(i_3 i_4) = \\ &= (i_1 i_3)(i_2 i_4)(i_1 i_2)(i_3 i_4) = (i_1 i_4)(i_2 i_3) \in N \end{aligned}$$

Так как в  $S_n$  все произведения пар независимых транспозиций сопряжены, все пары независимых транспозиций  $\in N$ . Так как  $n \geq 5$ ,  $A_n$  порождается парами независимых транспозиций, а значит,  $N = A_n$ .

□

**Теорема.**  $A_n$  - простая при  $n \geq 5$ .

*Доказательство.* Рассмотрим произвольную нормальную подгруппу  $N \trianglelefteq A_n$ .

Если  $N \trianglelefteq S_n$ , то по лемме 1  $N = A_n$ . Иначе:  $|S_n : A_n| = 2, S_n = A_n \sqcup (12)A_n$ .

Пусть  $N$  не нормальна в  $S_n$ . Обозначим  $N_1 = N, N_2 = (12)N_1(12)$ . Если  $N_1 = N_2$ , то  $N$  при сопряжении любой  $\sigma \in S_n$  не изменится, т.е.  $N \trianglelefteq S_n$  - противоречие. Поэтому  $N_1 \neq N_2$ , причём  $|N_1| = |N_2|$ .

Докажем, что  $A_n = N_1 \times N_2$  (отсюда получим, что  $|A_n| = |N|^2$ ):

1.  $N_1 \trianglelefteq A_n$  - уже имеем;

2.  $N_2 \trianglelefteq A_n$ :

$$\begin{aligned} \forall \sigma \in A_n : \sigma N_2 \sigma^{-1} &= \sigma (12) N_1 (12) \sigma^{-1} = \underset{=\tilde{\sigma}}{(12)(12)} \sigma (12) N_1 (12) \underset{=\tilde{\sigma}^{-1}}{\sigma^{-1}(12)(12)} = \\ &= (12) \tilde{\sigma} N_1 \tilde{\sigma}^{-1} (12) = (12) N_1 (12) = N_2 \end{aligned}$$

3.  $N_1 \cap N_2 = \{id\}$ : Пусть  $K = N_1 \cap N_2 \leq A_n$ . Тогда  $K \trianglelefteq S_n$ :

- $\forall \sigma \in A_n : \sigma K \sigma^{-1} \subseteq N_1, N_2$  из  $N_1, N_2 \trianglelefteq A_n$ , то есть  $\sigma K \sigma^{-1} \subseteq K$ ;
- $(12)K(12) \subseteq N_2$  из  $K \subseteq N_1$ ,  $(12)K(12) \subseteq N_1$  из  $K \subseteq N_2 \implies \implies (12)K(12) \subseteq K$

Значит,  $K$  не изменится при сопряжении любой подстановкой из  $S_n$ , то есть  $K \trianglelefteq S_n$ . Тогда по лемме 1 и  $K \neq A_n$  имеем  $K = \{id\}$ .

4.  $N_1 N_2 = A_n$ : Пусть  $L = N_1 N_2 \leq A_n$  Тогда  $L \trianglelefteq S_n$ :

- $\forall \sigma \in A_n : \sigma L \sigma^{-1} = \sigma N_1 N_2 \sigma^{-1} = \sigma N_1 \sigma^{-1} \sigma N_2 \sigma^{-1} = N_1 N_2$ ;
- $(12)L(12) = (12)N_1 N_2(12) = (12)N_1(12)(12)N_2(12) = N_2 N_1 = N_1 N_2$

При этом  $L \neq id$  - по лемме 1  $L = A_n$ .

Теперь индукцией по  $n \leq 5$  докажем, что  $A_n$  - простая.

База:  $n = 5 - |A_5| = 60$  - не точный квадрат, то есть невозможна ненормальность  $N$  в  $S_n$ , а отсюда  $A_n$  - простая;

Шаг: Пусть  $A_{n-1}$  - простая. Обозначим  $A_n \geq H = \{\sigma \in A_n \mid \sigma(n) = n\} \simeq A_{n-1}$ .

Предположим, что  $N_1 \neq N_2 \implies A_n = N_1 \times N_2 \implies H \leq N_1 \times N_2$ . Тогда  $H \cap N_2 \trianglelefteq H$ , т.к.  $N_2 \trianglelefteq A_n$  и  $H \cap N_2 \subseteq H$ .

Так как  $H$  - простая, то  $H \cap N_2$  равно либо  $H$ , либо  $id$ .

Если  $H \cap N_2 = H$ , то  $H \subseteq N_2 \implies |H| \leq |N_2| = |N|$ .

Если  $H \cap N_2 = \{id\}$ , то рассмотрим гомоморфизм  $\varphi : A_n = N_1 \times N_2 \rightarrow N_1$ .

$\text{Кер } \varphi = N_2 \implies H \simeq \varphi(H) \leq N_1 \implies |H| \leq |N_1| = |N|$ .

В каждом случае  $|H| = |A_{n-1}| \leq |N|$ . Тогда из предположения

$$|A_n| = |N|^2 \geq |A_{n-1}|^2 \implies \frac{n!}{2} \geq \frac{((n-1)!)^2}{4} \implies 2n \geq (n-1)!$$

Последнее неравенство, очевидно, неверно при  $n \geq 5$ . □

**Теорема.**  $SO_3$  - простая.

*Доказательство.* Без доказательства. □

## 9 Линейные представления

Пусть  $V$  - векторное пространство над полем  $\mathbb{F}$ ,  $GL(V)$  - группа обратимых линейных операторов над  $V$ ,  $G$  - произвольная группа.

**Определение.** Произвольный гомоморфизм  $\Phi : G \rightarrow GL(V)$  (действие  $G \curvearrowright V$ ) называется линейным представлением группы  $G$ .

$V$  называется пространством линейного представления,  $\dim V$  - размерность (степень) линейного представления. Если  $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ , то линейное представление называется рациональным, вещественным или комплексным соответственно.

Из определения  $\Phi(e) = I$  - тождественный оператор,  $\Phi(g_1 g_2) = \Phi(g_1) \Phi(g_2)$ .

**Определение.**  $\forall g \in G$   $\Phi(g)$  называется оператором линейного представления. Обозначается  $\forall v \in V$   $\Phi(g)v := \Phi(g)(v)$ .

**Определение.** Если  $\text{Ker } \Phi = \{e\}$ , то линейное представление называется точным. В этом случае  $G \simeq \text{Im } \Phi \leq GL(V)$ .

**Определение.** Если  $G \leq GL(V)$ , то тождественное линейное представление  $\Phi = \text{id} : G \rightarrow GL(V)$  называется тавтологическим линейным представлением  $G$ .

### Примеры.

1.  $\dim V = 1 : GL(V) \simeq \mathbb{F}^*$ , то есть  $\Phi : G \rightarrow GL(V) \simeq \mathbb{F}^*$ ;

(a)  $\mathbb{F} = \mathbb{R}, G = \mathbb{R} : \Phi(t) = e^t$ ;

(b)  $\mathbb{F} = \mathbb{R}, G = S_n : \Phi(\sigma) = \text{sgn } \sigma$ ;

(c)  $G = GL_n(\mathbb{F}) : \Phi(A) = \det A$ .

2.  $V = M_n(\mathbb{C}), G = \mathbb{R}$ . Если зафиксировать матрицу  $B \in M_n(\mathbb{C})$ , то определено линейное представление  $\Phi(t) = e^{tB}$ .

3. Пусть задано линейное представление  $\Phi : G \rightarrow GL(V)$  и задан гомоморфизм  $\Psi : H \rightarrow G$ . Тогда  $\tilde{\Phi} = \Phi \circ \Psi : H \rightarrow GL(V)$  - линейное представление группы  $H$ .

4. Пусть  $X$  - некоторое множество, задано  $G \curvearrowright X$ .

Рассмотрим векторное пространство функций  $\mathcal{F}(X, \mathbb{F}) = \{f : X \rightarrow \mathbb{F}\} = V$

Тогда  $\Phi : G \rightarrow GL(V) : \forall g \in G$   $\Phi(g)f = \tilde{f}$ , где  $\tilde{f}(x) = f(gx)$  - линейное представление группы  $G$ :

$$\forall g_1, g_2 \in G : \Phi(g_1 g_2)f(x) = f(g_1 g_2 x) = \Phi(g_1)f(g_2 x) = \Phi(g_1)\Phi(g_2)f(x)$$



## 9.1 Матричные представления группы

**Определение.** Произвольный гомоморфизм  $\Phi : G \rightarrow GL_n(\mathbb{F})$  называется матричным представлением группы  $G$  размерности  $n$  над полем  $\mathbb{F}$ .

Заметим, что линейные и матричные представления связаны между собой:

1. Если задано матричное представление  $G$ , то есть гомоморфизм  $\Phi : G \rightarrow GL_n(\mathbb{F})$ , то  $GL_n(\mathbb{F}) \underset{\psi}{\simeq} GL(\mathbb{F}^n) \implies \tilde{\Phi} = \psi \circ \Phi : G \rightarrow GL(\mathbb{F}^n)$  - линейное представление  $G$ .
2. Если задано  $n$ -мерное линейное представление  $G$ , то есть гомоморфизм  $\Phi : G \rightarrow GL(V) : \forall g \in G \ g \mapsto \Phi(g) = \varphi_g$  - линейный оператор. Если фиксировать базис  $\mathcal{E} = \{e_1, \dots, e_n\}$ , то  $\varphi_g \leftrightarrow A_g$  - матрица  $\varphi_g$  в базисе  $\mathcal{E}$ . Отсюда  $GL(V) \underset{\tilde{\psi}}{\simeq} GL_n(\mathcal{E})$  - получим матричное представление группы  $G$ .

Поэтому при фиксированном базисе  $V$  имеет место взаимно однозначное соответствие между линейными представлениями  $G \rightarrow GL(V)$  и матричными представлениями  $G \rightarrow GL_n(\mathbb{F})$ , где  $n = \dim V$ .

**Напоминание.** Если  $\varphi : V \rightarrow V$  - линейный оператор,  $A$  и  $\tilde{A}$  - его матрицы в базисах  $\mathcal{E}$  и  $\tilde{\mathcal{E}}$  соответственно, то  $\tilde{A} = C^{-1}AC$ , где  $C$  - матрица перехода от  $\mathcal{E}$  к  $\tilde{\mathcal{E}}$ .

Здесь и далее: если вдруг не вспоминается - см. [конспект](#) линейной алгебры.

**Определение.** Матричные представления  $\Phi_1, \Phi_2$  группы  $G$  размерности  $n$  над полем  $\mathbb{F}$  называются эквивалентными (изоморфными, подобными), если  $\exists C \in GL_n(\mathbb{F}) : \forall g \in G : \Phi_2(g) = C^{-1}\Phi_1(g)C$ . Обозначается  $\Phi_1 \approx \Phi_2$ .

*Замечание.* Эквивалентные матричные представления группы  $G$  соответствуют одному и тому же линейному представлению  $G$  относительно разных базисов.

**Определение.** Пусть  $V_1, V_2$  - векторные пространства над полем  $\mathbb{F}$ . Линейные представления  $\Phi_1 : G \rightarrow GL(V_1)$  и  $\Phi_2 : G \rightarrow GL(V_2)$  называются эквивалентными (изоморфными, подобными), если  $\exists \varphi : V_1 \rightarrow V_2$  - изоморфизм такой, что  $\forall g \in G : \Phi_2 = \varphi^{-1} \circ \Phi_1 \circ \varphi$ . Обозначается  $\Phi_1 \approx \Phi_2$ .

*Замечание.* Если  $\Phi_1 \approx \Phi_2$  и  $\mathcal{E}_1 = \{e_1, \dots, e_n\}$  - базис  $V_1$ , то в базисе  $\mathcal{E}_2 = \{\varphi(e_1), \dots, \varphi(e_n)\}$  (где  $\varphi$  - изоморфизм  $V_1$  и  $V_2$  из определения  $\Phi_1 \approx \Phi_2$ ) для любого  $g$  матрица линейного оператора  $\Phi_2(g)$  равна матрице оператора  $\Phi_1(g)$  в базисе  $\mathcal{E}_1$ .

## 9.2 Приводимость линейных представлений

**Напоминание.** Пусть  $\varphi : V \rightarrow V$  - линейный оператор. Подпространство  $U \subseteq V$  называется инвариантным относительно  $\varphi$ , если  $\forall u \in U : \varphi(u) \in U$ .

**Определение.** Пусть  $\Phi : G \rightarrow GL(V)$  - линейное представление группы  $G$ . Подпространство  $U \subseteq V$  называется инвариантным относительно  $\Phi$ , если  $\forall g \in G$   $U$  инвариантно относительно оператора  $\Phi(g)$ , то есть  $\forall g \in G, u \in U : \Phi(g)u \in U$ .

**Замечание.** Подпространства  $\{0\}, V$ , очевидно, всегда инвариантны - они называются тривиальными инвариантными подпространствами.

**Утверждение.** Сумма и пересечение инвариантных подпространств - инвариантное подпространство (как для оператора, так и для линейного представления).

*Доказательство.* Очевидно из определений инвариантности. □

**Напоминание.** Если  $U \subseteq V$  - инвариантное подпространство относительно линейного оператора  $\varphi$  и  $\{e_1, \dots, e_n\}$  - базис  $V$  такой, что  $\{e_1, \dots, e_m\}$  - базис  $U$ , то матрица линейного оператора в базисе  $\{e_1, \dots, e_n\}$  имеет вид  $A = \left( \begin{array}{c|c} A_u & * \\ \hline 0 & * \end{array} \right)$ , где  $A_u$  - матрица  $\varphi|_U$  (ограничения на инвариантное подпространство).

**Утверждение.** Если  $U \subseteq V$  - инвариантное подпространство относительно линейного представления  $\Phi : G \rightarrow GL(V)$  и  $\{e_1, \dots, e_n\}$  - базис  $V$  такой, что  $\{e_1, \dots, e_m\}$  - базис  $U$ , то  $\forall g \in G$  матрица линейного оператора  $\Phi(g)$  в базисе  $\{e_1, \dots, e_n\}$  имеет вид  $A_g = \left( \begin{array}{c|c} A_{g,u} & * \\ \hline 0 & * \end{array} \right)$ .

**Определение.** Если  $U \subseteq V$  - инвариантное подпространство относительно линейного  $\Phi : G \rightarrow GL(V)$ , то ограничением линейного представления  $\Phi$  на  $U$  называется линейное представление  $\Phi|_U : G \rightarrow GL(U)$  такое, что  $\forall g \in G : \Phi|_U(g) = \Phi(g)|_U$

**Определение.** Линейное представление  $\Phi : G \rightarrow GL(V)$  называется неприводимым, если:

1.  $V \neq \{0\}$ ;
2.  $\Phi$  не имеет нетривиальных инвариантных подпространств.

В противном случае  $\Phi$  называется приводимым.

### Примеры.

1. Любое одномерное линейное представление неприводимо;
2. Пусть  $G = \mathbb{R}$ ,  $V = \mathcal{E}^2$  - двумерное евклидово пространство;  
 $\Phi : G \rightarrow GL(\mathcal{E}^2)$  такое, что  $\Phi(g)$  в ортонормированном базисе  $\{e_1, e_2\}$  имеет матрицу  $\begin{pmatrix} \cos g & -\sin g \\ \sin g & \cos g \end{pmatrix}$  (т.е.  $\Phi(g)$  - поворот евклидова пространства).  
Над  $\mathbb{R}$  данное линейное представление неприводимо, так как не имеет одномерных инвариантных подпространств (геометрически очевидно).  
Однако над  $\mathbb{C}$  нетривиальные инвариантные подпространства есть: они будут собственными подпространствами  $\langle e_1 + ie_2 \rangle$ ,  $\langle e_1 - ie_2 \rangle$  - поэтому  $\Phi$  приводимо над  $\mathbb{C}$ .
3. Пусть  $G = \langle a \rangle_k$ ,  $V = \mathcal{E}^2$  - двумерное евклидово пространство;  
 $\Phi : G \rightarrow GL(\mathcal{E}^2)$  такое, что  $\Phi(a^m)$  в ортонормированном базисе  $\{e_1, e_2\}$  - поворот на  $\frac{2\pi m}{k}$ . Абсолютно аналогично примеру (2) доказывается, что  $\Phi$  неприводимо над  $\mathbb{R}$  и приводимо над  $\mathbb{C}$ ;
4. Пусть  $G = D_n (n \geq 3)$ ,  $V = \mathcal{E}^2$  - двумерное евклидово пространство;  
По определению  $D_n = \text{Sym } N \subset O_2 \subset GL(\mathcal{E}^2)$  (где  $N$  - правильный  $n$ -угольник) - можем задать тавтологическое линейное представление  $\Phi$ .  
 $\Phi$  неприводимо над  $\mathbb{R}$ , так как нет одномерных инвариантных подпространств относительно поворотов.  
Также  $\Phi$  неприводимо над  $\mathbb{C}$ , так как все одномерные инвариантные подпространства относительно поворотов - это  $\langle e_1 + ie_2 \rangle$ ,  $\langle e_1 - ie_2 \rangle$ , которые не инвариантны относительно симметрий.
5. Пусть  $G = S_4$ ,  $V = \mathcal{E}^3$  - трёхмерное евклидово пространство;  
Ранее доказывали, что  $S_4 \simeq \text{Sym}^+ K \subset O_3 \subset GL(\mathcal{E}^3)$  (где  $K$  - куб) - задали линейное представление  $\Phi$ .  
 $\Phi$  неприводимо над  $\mathbb{R}$ , так как одномерных инвариантных подпространств не может быть из геометрических соображений, а двумерных не может быть, так как если  $U$  - инвариантное, то  $U^\perp$  инвариантно из ортогональности  $\Phi(g)$  для всех  $g$ , а  $U^\perp$  одномерно.  
Также  $\Phi$  неприводимо над  $\mathbb{C}$ : любое одномерное инвариантное подпространство над  $\mathbb{C}$  соответствует двумерному инвариантному подпространству над  $\mathbb{R}$  (либо одномерному, если оно полностью вещественное) - значит,

таковых нет; двумерных инвариантных подпространств не может быть из рассуждений об ортогональности (как выше).

6. Пусть  $G = S_4$ ,  $V = \mathcal{E}^3$  - трёхмерное евклидово пространство;  
 Ранее доказывали, что  $S_4 \simeq \text{Sym } T \subset O_3 \subset GL(\mathcal{E}^3)$  (где  $T$  - правильный тетраэдр)- задали линейное представление  $\Phi$ .  
 Абсолютно аналогично примеру (5) доказывается, что  $\Phi$  неприводимо над  $\mathbb{R}$  и над  $\mathbb{C}$ .

7. Пусть  $G = S_n$ ,  $V$  - векторное пространство размерности  $n$  над полем  $\mathbb{F}$  ( $\text{char } \mathbb{F} = 0$ ). Зададим *мономиальное* линейное представление  $S_n$ : зафиксируем базис  $\mathcal{E} = \{e_1, \dots, e_n\}$  в  $V$  и определим  $M : G \rightarrow GL(V)$  так, что  $\forall \sigma \in G : M(\sigma)e_i = e_{\sigma(i)}$  (очевидно, что для любой подстановки такой оператор существует и единственный)

Заметим, что  $M$  приводимо - оно имеет одномерное инвариантное подпространство  $U = \langle e_1 + \dots + e_n \rangle$  и  $n - 1$ -мерное инвариантное подпространство  $W = \{x = \sum x_i e_i \mid \sum x_i = 0\}$  (оно  $n - 1$ -мерно, т.к. любой его элемент однозначно задаётся первыми  $n - 1$  координатами).

Более того, докажем, что  $V = U \oplus W$ :

- $\dim V = \dim U + \dim W$ ;
- Если  $x \in U \cap W$ , то  $x = k(e_1 + \dots + e_n)$ , причём сумма его координат равна нулю, т.е.  $k = 0 \implies x = 0$ . Значит,  $U \cap W = \{0\}$ .

Однако ограничение  $M|_W = M_W$  неприводимо - докажем это:

Пусть  $\tilde{U} \subset W$  - нетривиальное инвариантное подпространство.

Тогда  $\exists x \in \tilde{U}, x \neq 0$ . Так как  $x \in W$ ,  $\sum x_i = 0 \implies \exists i, j : x_i \neq x_j$ .

Рассмотрим  $(ij) \in S_n$ :

$$M(ij)x \in \tilde{U} \implies x - M(ij)x = (x_i - x_j)(e_i - e_j) \in \tilde{U} \implies e_i - e_j \in \tilde{U}$$

Отсюда из инвариантности  $\tilde{U} \forall \sigma \in S_n : e_{\sigma(i)} - e_{\sigma(j)} \in \tilde{U} \implies \forall k, m : e_k - e_m \in \tilde{U} \implies \tilde{U} = W$  (т.к.  $W = \langle e_1 - e_2, \dots, e_1 - e_n \rangle$ )

**Теорема.** (*Лемма Шура*).

Пусть  $\mathbb{F}$  - алгебраически замкнутое поле,  $V$  - векторное пространство над  $\mathbb{F}$ ,  $G$  - произвольная группа,  $\Phi : G \rightarrow GL(V)$  - неприводимое линейное представление. Тогда если  $\varphi : V \rightarrow V$  - линейный оператор такой, что  $\forall g \in G : \varphi \circ \Phi(g) = \Phi(g) \circ \varphi$ , то  $\varphi$  - скалярный оператор (т.е.  $\varphi = \lambda I$ ).

*Доказательство.* Так как  $\mathbb{F}$  алгебраически замкнуто,  $\varphi$  имеет хотя бы одно собственное значение  $\lambda$  и собственное подпространство  $V_\lambda = \{v \in V \mid \varphi(v) = \lambda v\}$ . Докажем, что  $V_\lambda$  - инвариантное подпространство, т.е. что  $\forall g \in G, v \in V_\lambda : \Phi(g)v \in V_\lambda$ , что равносильно  $\varphi(\Phi(g)v) = \lambda \Phi(g)v$ :

$$\varphi(\Phi(g)v) = (\varphi \circ \Phi(g))v = (\Phi(g) \circ \varphi)v = \Phi(g)(\varphi(v)) = \Phi(g)(\lambda v) = \lambda \Phi(g)v$$

Т.к.  $V_\lambda \neq \{0\}$  и  $\Phi$  неприводимо,  $V_\lambda = V \implies \forall v \in V : \varphi(v) = \lambda v \implies \varphi = \lambda I$ .  $\square$

**Следствие.** Пусть  $\mathbb{F}$  - алгебраически замкнутое поле,  $V$  - векторное пространство над  $\mathbb{F}$ ,  $G$  - абелева группа,  $\Phi : G \rightarrow GL(V)$  - неприводимое линейное представление. Тогда  $\dim V = 1$ , т.е.  $\Phi$  - одномерное линейное представление.

*Доказательство.*  $\forall g, h \in G : gh = hg \implies \Phi(gh) = \Phi(hg) \implies \Phi(g)\Phi(h) = \Phi(h)\Phi(g)$ . Тогда если обозначить  $\Phi(h) = \varphi$ , то условия леммы Шура выполняются, а отсюда  $\forall h : \Phi(h)$  - скалярный оператор. Но для скалярного оператора любое подпространство  $V$  инвариантно, а значит любое подпространство  $V$  инвариантно для  $\Phi$ . Тогда из неприводимости  $\Phi$  любое нетривиальное подпространство  $V$  совпадает с  $V$ , а отсюда  $\dim V = 1$ .  $\square$

### Неприводимые лин. представления конечных абелевых групп над $\mathbb{C}$

Пусть  $G$  - конечная абелева группа,  $\mathbb{F} = \mathbb{C}$ . По следствию из леммы Шура любое неприводимое линейное представление  $G$  имеет одномерное пространство представления, то есть  $GL(V) \simeq \mathbb{C}^*$ .

**Утверждение.** Для конечной абелевой группы  $G$  существует ровно  $|G|$  различных комплексных неприводимых линейных представлений  $G$ .

*Доказательство.* Опишем все гомоморфизмы  $\Phi : G \rightarrow \mathbb{C}^*$ :

Так как  $G$  - конечная абелева, по основной теореме о конечнопорождённых абелевых группах  $G \simeq \langle a_1 \rangle_{n_1} \times \dots \times \langle a_k \rangle_{n_k}$ . Пусть  $\Phi(a_i) = c_i$ . Тогда  $c_i^{n_i} = \Phi(a_i^{n_i}) = \Phi(e) = 1$ , то есть  $c_i$  - комплексный корень степени  $n_i$  из единицы. Так как  $a_1, \dots, a_k$  порождают  $G$ , очевидно, что гомоморфизм однозначно задаётся выбором  $c_1, \dots, c_k$ . Способов выбрать  $c_i$  ровно  $n_i$  (количество комплексных корней степени  $n_i$  из единицы) - отсюда гомоморфизмов  $n_1 \cdot \dots \cdot n_k = |G|$ .  $\square$

**Пример.**  $V_4 = \langle a \rangle_2 \times \langle b \rangle_2 \implies \Phi(a) = \pm 1, \Phi(b) = \pm 1$ .

	e	a	b	ab
$\Phi_1 = I$	1	1	1	1
$\Phi_2$	1	-1	1	-1
$\Phi_3$	1	1	-1	-1
$\Phi_4$	1	-1	-1	1

### Одномерные комплексные лин. представления произвольной группы

Пусть  $G$  - произвольная группа.

Знаем, что коммутант  $G' \trianglelefteq G$  - подгруппа такая, что  $G/G'$  абелева. Рассмотрим канонический гомоморфизм  $\pi : G \rightarrow G/G'$ :

**Утверждение.** Если  $\Psi : G/G' \rightarrow \mathbb{C}^*$  - одномерное комплексное линейное представление  $G/G'$ , то  $\Phi = \psi \circ \pi : G \rightarrow \mathbb{C}^*$  - одномерное комплексное линейное представление  $G$ .

*Доказательство.* Очевидно (композиция гомоморфизмов - гомоморфизм).  $\square$

**Утверждение.** Пусть  $G$  - произвольная группа,  $\Phi : G \rightarrow \mathbb{C}^*$  - произвольное одномерное комплексное линейное представление  $G$ . Тогда  $\exists$  линейное представление  $\Psi : G/G' \rightarrow \mathbb{C}^*$  такое, что  $\Phi = \Psi \circ \pi$ .

*Доказательство.* Заметим, что  $\text{Im } \Phi \leq \mathbb{C}^* \implies \text{Im } \Phi$  - абелева.

Из теоремы о гомоморфизме  $\text{Im } \Phi \simeq G/\text{Ker } \Phi$ , то есть  $G/\text{Ker } \Phi$  - абелева, а тогда  $G' \subseteq \text{Ker } \Phi$  (свойство коммутанта).

Отсюда  $\forall g \in G, h \in G' : \Phi(gh) = \Phi(g)$ , то есть значения  $\Phi$  на всех элементах левого смежного класса  $g$  по  $G'$  совпадают. Поэтому корректно отображение  $\Psi : G/G' \rightarrow \mathbb{C}^*$ , заданное по правилу  $gG' \mapsto \Phi(g)$ . Это гомоморфизм:

$$\Psi(g_1G' \cdot g_2G') = \Psi(g_1g_2G') = \Phi(g_1g_2) = \Phi(g_1)\Phi(g_2) = \Psi(g_1G')\Psi(g_2G')$$

При этом  $\forall g \in G : g \xrightarrow{\pi} gG' \xrightarrow{\Psi} \Phi(g)$ , то есть  $\Phi = \Psi \circ \pi$ .  $\square$

**Следствие.** Если  $G$  конечна, то одномерных комплексных линейных представлений  $G$  ровно  $|G/G'|$ .

*Доказательство.* Из двух предыдущих утверждений имеем взаимно однозначное соответствие между одномерными комплексными линейными представлениями  $G$  и  $G/G'$ . Если  $G$  конечна, то  $G/G'$  - конечная абелева, а тогда она имеет ровно  $|G/G'|$  представлений.  $\square$

## 9.3 Сумма линейных представлений группы

### 1. Внутренняя сумма линейных представлений

Пусть  $\Phi : G \rightarrow GL(V)$  - линейное представление  $G$ , и пусть  $V = U \oplus W$ , где  $U$  и  $W$  инвариантны относительно  $\Phi$ . Тогда говорят, что  $\Phi$  есть сумма (внутренняя) представлений  $\Phi|_U$  и  $\Phi|_W$ .

Заметим, что если выбрать базисы  $\mathcal{E}_U = \{e_1, \dots, e_m\}$  в  $U$ ,  $\mathcal{E}_W = \{e_{m+1}, \dots, e_n\}$  в  $W$ , то в базисе  $\mathcal{E}_V = \{e_1, \dots, e_n\}$  пространства  $V$  матрица оператора  $\Phi(g)$  для любого  $g \in G$  имеет вид  $A_g = \left( \begin{array}{c|c} A_{U,g} & 0 \\ \hline 0 & A_{W,g} \end{array} \right)$ , где  $A_{U,g}$  - матрица  $\Phi|_U$  в базисе  $\mathcal{E}_U$ , а  $A_{W,g}$  - матрица  $\Phi|_W$  в базисе  $\mathcal{E}_W$ .

### 2. Внешняя сумма линейных представлений

Пусть  $U, W$  - векторные пространства над полем  $\mathbb{F}$ , и пусть заданы линейные представления  $\Psi_1 : G \rightarrow GL(U)$  и  $\Psi_2 : G \rightarrow GL(W)$ . Обозначим  $V = U \oplus W$  - внешняя прямая сумма  $U$  и  $W$ . Тогда линейное представление  $\Phi : G \rightarrow GL(V)$ , заданное по правилу  $\Phi(g)(u, w) = (\Psi_1(g)u, \Psi_2(g)w)$  (очевидно, что это гомоморфизм), называется суммой линейных представлений  $\Psi_1, \Psi_2$  и обозначается  $\Phi = \Psi_1 + \Psi_2$ .

Аналогично, если выбрать базисы  $\mathcal{E}_U = \{e_1, \dots, e_m\}$  в  $U$ ,  $\mathcal{E}_W = \{e_{m+1}, \dots, e_n\}$  в  $W$ , то в базисе  $\mathcal{E}_V = \{(e_1, 0), \dots, (e_m, 0), (0, e_{m+1}), \dots, (0, e_n)\}$  пространства  $V$  матрица оператора  $\Phi(g)$  для любого  $g \in G$  имеет вид  $\left( \begin{array}{c|c} A_{\Psi_1} & 0 \\ \hline 0 & A_{\Psi_2} \end{array} \right)$ , где  $A_{\Psi_1}$  - матрица  $\Psi_1$  в базисе  $\mathcal{E}_U$ , а  $A_{\Psi_2}$  - матрица  $\Psi_2$  в базисе  $\mathcal{E}_W$ .

## 9.4 Вполне приводимые линейные представления

**Определение.** Линейное представление  $\Phi : G \rightarrow GL(V)$  называется вполне приводимым, если для любого подпространства  $U \subseteq V$ , инвариантного относительно  $\Phi$ , существует такое подпространство  $W \subseteq V$ , инвариантное относительно  $\Phi$ , что  $V = U \oplus W$ .

*Замечание.* Любое неприводимое линейное представление вполне приводимо - для него есть только инвариантные подпространства  $V$  и  $\{0\}$ , причём  $V \oplus \{0\} = V$ .

**Примеры.** (Напомним, что при фиксированном базисе  $V$  линейные представления взаимно однозначно соответствуют матричным, где в соответствие каждому оператору поставлена его матрица).

1.  $\Phi : \mathbb{R} \rightarrow GL_2(\mathbb{C})$   $\Phi(t) = \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix}$  - вполне приводимо.

(поворот унитарного пространства - ортогональный оператор, то есть если  $U$  инвариантно, то  $U^\perp$  инвариантно, причём  $V = U \oplus U^\perp$ )

2.  $\Phi : \mathbb{R} \rightarrow GL_2(\mathbb{C})$   $\Phi(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$  - приводимо, но не вполне приводимо:

Рассмотрим базис  $\tilde{C} = \{e_1, e_2\}$  двумерного пространства линейного представления  $V$ , в котором записаны матрицы операторов.

Заметим, что  $\langle e_1 \rangle$  - инвариантное подпространство относительно  $\Phi$ . Однако никакое подпространство  $W = \langle \mu e_1 + e_2 \rangle$  не инвариантно:

$$\forall t > 0 : \Phi(t) \begin{pmatrix} \mu \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ 1 \end{pmatrix} = \begin{pmatrix} \mu + t \\ 1 \end{pmatrix} \neq \lambda \begin{pmatrix} \mu \\ 1 \end{pmatrix}$$

**Определение.** Пусть  $\Phi : G \rightarrow GL(V)$  - линейное представление  $G$ . Линейное представление  $\tilde{\Phi}$  называется подпредставлением  $\Phi$ , если  $\exists \tilde{V} \subseteq V$  - такое подпространство, инвариантное относительно  $\Phi$ , что  $\tilde{\Phi} = \Phi|_{\tilde{V}} : G \rightarrow GL(\tilde{V})$ .

**Лемма 1.** Любое подпредставление вполне приводимого представления вполне приводимо.

*Доказательство.* Пусть  $\Phi : G \rightarrow GL(V)$  - вполне приводимое линейное представление,  $\tilde{\Phi} : G \rightarrow GL(\tilde{V})$  - его подпредставление ( $\tilde{V}$  - подпространство  $V$ ). Рассмотрим произвольное подпространство  $U \subseteq \tilde{V}$ , инвариантное относительно  $\tilde{\Phi}$ .  $U$  является подпространством и для  $V$ , а тогда  $\exists$  инвариантное относительно  $\Phi$  подпространство  $W \subseteq V$  такое, что  $V = U \oplus W$  (т.к.  $\Phi$  вполне приводимо). Тогда если обозначить  $\tilde{W} = W \cap \tilde{V}$ , то  $\tilde{W}$  - подпространство  $\tilde{V}$ , инвариантное относительно  $\tilde{\Phi}$ .

Осталось показать, что  $\tilde{V} = U \oplus \tilde{W}$ , то есть что  $\forall x \in \tilde{V}$  единственным образом раскладывается как  $x = u + \tilde{w}$ ,  $u \in U$ ,  $\tilde{w} \in \tilde{W}$ . Действительно, из  $V = U \oplus W$  знаем, что  $x$  как элемент  $V$  единственно раскладывается в сумму  $x = u + w$ , где  $u \in U$ ,  $w \in W$ , однако  $w = x - u \in \tilde{V}$ , то есть  $w \in \tilde{V} \cap W = \tilde{W}$ . Значит, такое разложение существует и единственно, что и требовалось.  $\square$

**Лемма 2.** Пусть  $\Phi : G \rightarrow GL(V)$  - вполне приводимое линейное представление. Тогда  $\Phi$  раскладывается в сумму неприводимых линейных представлений (возможно, одного).

*Доказательство.* Индукция по  $n = \dim V$ :

База:  $n = 1 \implies \Phi$  неприводимо;



Шаг: Пусть  $V_1$  - минимальное ненулевое инвариантное подпространство линейного представления  $\Phi$ . Так как  $\Phi$  вполне приводимо,  $\exists$  инвариантное дополнение  $W : V = V_1 \oplus W \implies \Phi = \Phi_{V_1} + \Phi_W$ . При этом  $\Phi_{V_1}$  неприводимо из минимальности  $V_1$  (нет нетривиальных инвариантных подпространств меньшей размерности), а  $\Phi_W$  по лемме 1 вполне приводимо, и притом меньшей размерности - раскладывается в искомую сумму по предположению индукции. Значит,  $\Phi$  также раскладывается в искомую сумму.  $\square$

**Пример.** Если  $\dim V = n > 1$  и  $\Phi : G \rightarrow GL(n)$  такое, что  $\Phi(g) = I \forall g \in G$ , то все подпространства  $V$  являются инвариантными для  $\Phi$ , откуда  $\Phi$  вполне приводимо. Тогда  $\Phi$  раскладывается в сумму одномерных представлений, причём не единственным образом - в зависимости от выбора базиса:

$$\mathcal{E} = \{e_1, \dots, e_n\} \implies V = \langle e_1 \rangle \oplus \dots \oplus \langle e_n \rangle \implies \Phi = \Phi_1 + \dots + \Phi_n;$$

$$\tilde{\mathcal{E}} = \{\tilde{e}_1, \dots, \tilde{e}_n\} \implies V = \langle \tilde{e}_1 \rangle \oplus \dots \oplus \langle \tilde{e}_n \rangle \implies \Phi = \tilde{\Phi}_1 + \dots + \tilde{\Phi}_n;$$

**Лемма 3.** Пусть  $V = V_1 + \dots + V_k$ , где  $V_i$  - минимальные ненулевые подпространства, инвариантные относительно линейного представления  $\Phi : G \rightarrow GL(V)$ . Тогда  $\Phi$  вполне приводимо, причём для произвольного инвариантного подпространства  $U \subseteq V$  существует инвариантное дополнение вида  $W = \sum_{i \in I} V_i$  для некоторого  $I \subseteq \{1, \dots, k\}$ .

*Доказательство.* Обозначим  $V_I = \sum_{i \in I} V_i$ , где  $I \subseteq \{1, \dots, k\}$ . Очевидно, что  $V_I$  - инвариантное подпространство (как сумма инвариантных). Рассмотрим произвольное инвариантное  $U \subseteq V$  и возьмём  $I = \{i \mid U \cap V_i = \{0\}\}$ . Докажем, что  $V = U \oplus V_I$  (по построению  $U \cap V_I = \{0\}$ , поэтому достаточно  $V = U + V_I$ ): Рассмотрим  $j \notin I$ . Тогда  $V_{I \cup \{j\}} = V_I + V_j$ , а также  $U \cap V_{I \cup \{j\}} \neq 0 \implies \exists u \in U : u = \sum_{i \in I} v_i + v_j$ , причём  $v_j \neq 0$ . Тогда  $v_j = u - \sum_{i \in I} v_i \in U + V_I$ , то есть  $V_j \cap (U + V_I) \neq \{0\}$ . При этом пересечение инвариантных подпространств инвариантно, то есть  $V_j \cap (U + V_I)$  - инвариантное подпространство в  $V_j$ . Тогда из минимальности  $V_j$  это подпространство совпадает с  $V_j$ , а значит  $V_j \subseteq U + V_I$ . Проведя такое рассуждение для всех  $j \in \{1, \dots, k\} \setminus I$ , получим  $V \subseteq U + V_I$ , а отсюда уже  $V = U \oplus V_I$ .  $\square$