

# Общая Алгебра

Адамович Ольга Маратовна

19 декабря 2019 г.

## Содержание

<b>Теория групп</b>	<b>5</b>
1    Лекция №1 . . . . .	5
1.1    Определение группы. Примеры. . . . .	5
1.2    Определение кольца. Примеры. . . . .	6
1.3    Определение поля . . . . .	7
1.4    Область целостности . . . . .	7
1.5    Делимость в области целостности . . . . .	8
1.6    Наибольший общий делитель элементов области це- лостности . . . . .	9
1.7    Евклидово кольцо . . . . .	10
1.8    Алгоритм Евклида . . . . .	10
1.9    Взаимно простые элементы области целостности . .	11
2    Лекция №2 . . . . .	12
2.1    Простые элементы области целостности . . . . .	12
2.2    Разложение на простые множители в евклидовом кольце . . . . .	13
2.3    Факториальное кольцо . . . . .	15
2.4    Аксиомы группы . . . . .	16
2.5    Следствия аксиом группы . . . . .	16
2.6    Порядок группы . . . . .	17
2.7    Таблица Кэли . . . . .	17
2.8    Изоморфизм групп . . . . .	18
3    Лекция №3 . . . . .	18
3.1    Важные примеры групп . . . . .	18
3.2    Кольцо вычетов по модулю $n$ . . . . .	19
3.3    Подгруппа . . . . .	21
3.4    Степень элемента группы . . . . .	22
3.5    Порядок элемента группы . . . . .	23
4    Лекция №4 . . . . .	24
4.1    Циклические группы . . . . .	24

	4.2	Подгруппы циклической группы . . . . .	28
5		Лекция №5 . . . . .	28
	5.1	Симметрическая группа $S_n$ . . . . .	30
6		Лекция №6 . . . . .	34
	6.1	Система порождающих элементов группы . . . . .	35
	6.2	Группа диэдра . . . . .	37
7		Лекция №7 . . . . .	39
	7.1	Группа кватернионов . . . . .	39
	7.2	Сравнение элементов группы по модулю подгруппы . . . . .	41
	7.3	Смежные классы группы по подгруппе. . . . .	41
	7.4	Теорема Лагранжа и следствия из неё: . . . . .	43
8		Лекция №8 . . . . .	45
	8.1	Определение операции на смежных классах . . . . .	45
	8.2	Нормальная подгруппа . . . . .	45
	8.3	Факторгруппа . . . . .	46
	8.4	Гомоморфизм групп . . . . .	47
	8.5	Образ гомоморфизма . . . . .	48
	8.6	Ядро гомоморфизма . . . . .	49
	8.7	Изоморфизм групп . . . . .	50
	8.8	Порядок образа элемента группы при гомоморфизме . . . . .	50
	8.9	Теорема о гомоморфизме . . . . .	51
9		Лекция №9 . . . . .	52
	9.1	Автоморфизм групп . . . . .	52
	9.2	Действия группы на множестве . . . . .	54
	9.3	Действия группы на самой себе $G:G$ . . . . .	54
	9.4	Теорема Кэли . . . . .	55
10		Лекция №10 . . . . .	57
	10.1	Четвёртая группа Клейна $V_4$ . . . . .	59
	10.2	Коммутант . . . . .	61
11		Лекция №11 . . . . .	62
12		Лекция №12 . . . . .	66
	12.1	Прямые произведения(прямые суммы) групп . . . . .	66
	12.2	Внешнее прямое произведения групп . . . . .	66

---

12.3	Внутреннее прямое произведение подгрупп . . . . .	67
13	Лекция №13 . . . . .	70
13.1	Примарные группы ( $p$ - группы) . . . . .	73
13.2	Функция Эйлера . . . . .	74
13.3	Изоморфизм колец индукции . . . . .	74
13.4	Разложение конечнопорождённых абелевых групп в прямую сумму циклических групп . . . . .	75
14	Лекция №14 . . . . .	77
15	Лекция №15 . . . . .	83
15.1	Группы правильных многогранников . . . . .	83

## Теория групп

### 1 Лекция №1

#### 1.1 Определение группы. Примеры.

**Опр.** Группа  $(G, \cdot)$  - множество с бинарной операцией  $\forall g_1, g_2 \in G \mapsto g_1 g_2 \in G$  :

- 1)  $(g_1 g_2) g_3 = g_1 (g_2 g_3) \quad \forall g_1, g_2, g_3 \in G$
- 2)  $\exists e \in G : g \cdot e = e \cdot g = g \quad \forall g \in G$
- 3)  $\forall g \in G \exists g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$

Примеры:

- а)  $(\mathbb{R}^{n \times n}, \cdot)$  не является группой.
- б)  $GL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n} : \det A \neq 0\}$  является группой
- в)  $(V^3, +)$  – коммутативная или абелева группа

**Опр.** Группа  $G$  называется коммутативной (абелевой), если  $a \cdot b = b \cdot a \quad \forall a, b \in G$

**NOTE:**

- 1) Если операция коммутативна, то она чаще называется сложением
- 2) Если операция некоммутативна, то она никогда не называется сложением.

Примеры:

- г)  $V$  – линейное пространство,  $\dim V = n < \infty$   
 $L(V, V)$  - множество линейных операторов на  $V$  - не является группой
- д)  $GL(V, V) = GL(V)$  – множество биективных линейных операторов - группа.  $(GL(V), \cdot)$  – некоммутативная группа

**1.2 Определение кольца. Примеры.**

$A$  – множество с двумя операциями ,  $a, b \in A \mapsto \begin{cases} a + b \in A \\ a \cdot b \in A \end{cases} :$

$$1) \quad a + b = b + a \quad \forall a, b \in A$$

$$2) \quad (a + b) + c = a + (b + c) \quad \forall a, b, c \in A$$

$$3) \quad \exists \bar{0} : a + \bar{0} = \bar{0} + a = a \quad \forall a \in A$$

$$4) \quad \forall a \in A \exists (-a) : a + (-a) = (-a) + a = \bar{0}$$

$$5) \quad \begin{aligned} a(b + c) &= ab + bc \quad \forall a, b, c \in A \\ (a + b)c &= ac + bc \quad \forall a, b, c \in A \end{aligned} \quad \text{дистрибутивность}$$

1)...5)  $\Rightarrow A$  - кольцо

$$6) \quad ab = ba \quad \forall a, b \in A$$

1)...6)  $\Rightarrow A$  - коммутативное кольцо

$$7) \quad (ab)c = a(bc) \quad \forall a, b, c \in A$$

1)...5), 7)  $\Rightarrow A$  - ассоциативное кольцо

$$8) \quad \exists 1 \in A : 1a = a1 = a \quad \forall a \in A$$

1)...5), 8)  $\Rightarrow A$  - кольцо с 1

1)...8)  $\Rightarrow A$  - коммутативное ассоциативное кольцо с 1

Примеры:

- 1)  $(\mathbb{Z}, +, \cdot)$  - коммутативное ассоциативное кольцо с 1
- 2)  $(\mathbb{R}^{n \times n}, +, \cdot)$  - некоммутативное ассоциативное кольцо с 1
- 3)  $\mathbb{R}[x]$  - коммутативное ассоциативное кольцо с 1

### 1.3 Определение поля

**Опр.**  $(A, +, \cdot)$  - поле ,  $a, b \in A \longrightarrow \begin{cases} a + b \in A \\ ab \in A \end{cases}$

1)  $\left. \begin{array}{l} 2) \\ 3) \\ 4) \\ 5) \\ 6) \\ 7) \\ 8) \end{array} \right\} \text{ ————| |————— смотри выше}$

9)  $\forall a \in A \setminus \{\bar{0}\} \exists a^{-1} \in A : aa^{-1} = a^{-1}a = 1$

10)  $|A| > 1 \iff (\bar{0} \neq 1)$  (в  $A$  не менее 2-х элементов)

Примеры: 1)  $\mathbb{Q}$  2)  $\mathbb{R}$  3)  $\mathbb{C}$

### 1.4 Область целостности

**Опр.**  $A$  - кольцо,  $a, b \in A$  называются делителями нуля, если  $\begin{cases} a \neq 0 \\ b \neq 0 \end{cases}$  , но  $ab = \bar{0}$

Пример:  $\mathbb{R}^{2 \times 2} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

**Опр.**

Коммутативное ассоциативное кольцо с 1 без делителей нуля называется областью целостности (целостным кольцом).

Примеры:

- 1)  $\mathbb{Z}$  - область целостности,
- 2)  $\mathbb{R}[x]$  - область целостности

$$\text{Утв. 1. } A \text{ - область целостности } a, b \in A \\ ab = \bar{0} \Rightarrow \begin{cases} a = \bar{0} \\ b = \bar{0} \end{cases}$$

$$\text{Утв. 2. } A \text{ - область целостности } a, b, c \in A \quad \begin{cases} a \neq 0 \\ a \cdot b = a \cdot c \end{cases} \Rightarrow b = c$$

$$\text{Док-во: } a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$$

**Опр.** Пусть  $A$  — ассоциативное кольцо с 1,  $a \in A$  называется обратимым, если  $\exists b \in A : ab = ba = 1$  ( $b = a^{-1}$ )

**Обозначение:**  $A^*$  — множество обратимых элементов кольца

Примеры:  $\mathbb{Z}^* = \{1, -1\}$ ,  $(\mathbb{R}^{n \times n})^* = \{A \in \mathbb{R}^{n \times n} : \det A \neq 0\}$ ,  
 $(\mathbb{R}[x])^* = \{f(x) \in \mathbb{R}[x] : \deg f(x) = 0\}$

**1.5 Делимость в области целостности**

**Опр.**  $A$  — область целостности  
 $a, b \in A$ ,  $a$  делится на  $b$  ( $a : b$ )  $\Leftrightarrow b$  делит  $a$  ( $b \mid a$ ),  
 $\Updownarrow$   
 если  $\exists c \in A : a = c \cdot b$

**Опр.**  $A$  — область целостности,  $a, b \in A$ ,



$a$  ассоциирован с  $b$  ( $a \sim b$ ), если  $\exists q \in A^* : a = q \cdot b$

Пример:  $13 \in \mathbb{Z} \quad -13 \sim 13$

**Утв. 3.**  $a \sim b$  отношение эквивалентности, т.е

- 1)  $a \sim a \quad \forall a \in A$  (рефлексивность)
- 2)  $a \sim b \Rightarrow b \sim a \quad \forall a, b \in A$  (симметричность)
- 3)  $a \sim b, b \sim c \Rightarrow a \sim c \quad \forall a, b, c \in A$  (транзитивность)

**Следствие:** Область целостности разбивается на непересекающиеся классы эквивалентности - классы ассоциированных друг с другом элементов.

Пример:  $\mathbb{Z} = \{\bar{0}\} \cup \{\pm 1\} \cup \{\pm 2\} \dots \cup \{\pm n\} \dots$

**Утв. 4.**  $A$  — область целостности,  $a, b \in A \quad a \sim b \Leftrightarrow \begin{cases} a \mid b \\ b \mid a \end{cases}$

**Док-во:**

$\Rightarrow$

$$a \sim b \quad a = q \cdot b \Rightarrow b \mid a$$

$$b \sim a \quad b = p \cdot a \Rightarrow a \mid b$$

$\Leftarrow$

$$\begin{cases} a \mid b \Rightarrow b = p \cdot a \\ b \mid a \Rightarrow a = q \cdot b \end{cases} \Rightarrow a = q \cdot p \cdot a \Rightarrow \begin{cases} a = 0 \Rightarrow b = 0 \Rightarrow a \sim b \\ a \neq 0 \quad q \cdot p = 1 \Rightarrow q \cdot p \in A^* \Rightarrow a \sim b \end{cases}$$

## 1.6 Наибольший общий делитель элементов области целостности

**Опр.**  $A$  — область целостности,  $a, b, d \in A$   $d$  называется общим делителем  $a$  и  $b$ , если  $\begin{cases} d \mid a \\ d \mid b \end{cases}$

**Опр.**  $A$  – область целостности,  $a, b \in A$ , наибольший общий делитель  $a$  и  $b$   $\text{НОД}\{a, b\} = (a, b)$  – общий делитель  $a$  и  $b$ , который делится на  $\forall$  их общий делитель в  $\mathbb{Z}$ .

Пример:  $(18, 24) = 6$

**Утв. 5.**  $A$  – область целостности,  $a, b \in A$   
Если  $\exists \text{НОД}\{a, b\} = (a, b)$ , то он единственный с точностью до ассоциированности.

**Док-во:** Следует из определения и утверждения 4.

Пример:  $(18, 24) = 6 \sim -6$

## 1.7 Евклидово кольцо

**Опр.** Область целостности  $A$  называется евклидовым кольцом, если  $\exists$  функция, называемая нормой (высотой):  $N : A \setminus \{0\} \rightarrow \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$  :

1)  $N(ab) \geq N(a) \quad \forall a, b \in A$ , причём  $N(ab) = N(a) \Leftrightarrow b \in A^*$

2)  $\forall a, b \in A, \quad b \neq 0$

$\exists q, r \in A : a = qb + r$ , где  $\begin{cases} r = \bar{0} \\ N(r) < N(b) \end{cases}$

Примеры:

1)  $(\mathbb{Z}, +, \cdot)$  – область целостности,  $N(a) = |a|$

2)  $(\mathbb{R}[x], +, \cdot)$  – область целостности,  $N(f(x)) = \deg f(x)$

## 1.8 Алгоритм Евклида

**Теорема**  $A$  – евклидово кольцо  $\Rightarrow$   
 $\Rightarrow \forall a, b \in A \quad \exists (a, b)$  и  $(a, b) = au + bv$ , где  $u, v \in A$

**Док-во:**

$$1) b = 0 \quad (a, b) = (a, 0) = a = 1a + 0b$$

$$2) b|a \quad (a, b) = b = 0a + 1b$$

$$3) b \neq 0, \quad b \nmid a, \quad \text{тогда}$$

$$\begin{aligned} \exists q_1, r_1 \in A : a &= a_1b + r_1, \quad N(r_1) < N(b), \quad r_1 \neq 0, \\ \exists q_2, r_2 \in A : b &= q_2r_1 + r_2, \quad N(r_2) < N(r_1), \quad r_2 \neq 0, \dots \end{aligned} \quad (*)$$

$$\dots\dots\dots r_{n-2} = q_nr_{n-1} + r_n, \quad N(r_n) < N(r_{n-1})$$

$$r_{n-1} = q_{n+1}r_n$$

$$r_n - \text{будет НОД}(a, b), \quad r_n = (a, b)$$

$$(*) \uparrow r_n | r_{n-1} \Rightarrow r_n | r_{n-2} \Rightarrow r_n | r_{n-3} \dots r_n | r_1 \Rightarrow r_n | b \Rightarrow r_n | a$$

$r_n$  - общий делитель  $a, b$

$$(*) \downarrow r_1 = a - q_1b = au_1 + br_1, \quad r_2 = b - q_2r_1 = au_2 + br_2 \dots$$

$$r_3 = \dots, \quad r_n = r_{n-2} - q_nr_{n-1} = au_n + bv_n = au + bv$$

Пусть  $d$  - общий делитель  $a$  и  $b$ ,  $a = dt$ ,  $b = ds$

$$r_n = au + bv$$

$$r_n = d(tu + sv) \Rightarrow d | r_n$$

$r_n$  - общий делитель  $a$  и  $b$ , который делится на любой их общий делитель  $\Rightarrow r_n = (a, b)$

Способ нахождения  $(a, b)$ , описанный в теореме, называется алгоритмом Евклида.

## 1.9 Взаимно простые элементы области целостности

**Опр.**  $A$  - область целостности,  $a, b \in A$  называются взаимно простыми, если  $(a, b) = 1$

**Утв. 6.**  $A$  - евклидово кольцо,  $a, b \in A$   
 $(a, b) = 1 \Leftrightarrow \exists u, v \in A : au + bv = 1$

**Док-во:**

$\Rightarrow$  смотри теорему

⊖ Пусть  $d$  – общий делитель  $a$  и  $b$ :  $a = dt$ ,  $b = ds$

$$au + bv = 1 \Rightarrow d(tu + sv) = 1 \Rightarrow$$

$$\Rightarrow 1 \mid d \Rightarrow d \in A^* \quad d \sim 1 \Rightarrow (a, b) = 1$$

**Утв. 7.**  $A$  – евклидово кольцо,  $a, b, c \in A$ ,  $(a, b) = 1$ ,  $\left. \begin{array}{l} a \mid c \\ b \mid c \end{array} \right\} \Rightarrow$   
 $\Rightarrow ab \mid c$

**Док-во:**

$$c = aq, \quad c = bp, \quad au + bv = 1 \mid \cdot c \quad cau + cbv = c$$

$$abpu + abqv = c \quad ab(pu + qv) = c \quad ab \mid c$$

**Утв. 8.**  $A$  – евклидово кольцо,  $a, b, c \in A$ ,  $(a, b) = 1$ ,  $a \mid bc \Rightarrow a \mid c$

**Док-во:**

$$bc = aq \quad au + bv = 1 \mid \cdot c \quad acu + aqv = c \quad a(cu + qv) = c \Rightarrow a \mid c$$

## 2 Лекция №2

### 2.1 Простые элементы области целостности

**Опр.**  $A$  – область целостности.  $\bar{0} \neq p \in A \setminus A^* (p \in A \setminus (A^* \cup \{0\}))$   
 $p$  – ненулевой необратимый элемент  $A$  называется простым элементом, если его нельзя представить в виде произведения 2-х необратимых элементов, т.е. если  $p = ab$ ,  $a, b \in A \Rightarrow \begin{cases} a \in A^* \\ b \in A^* \end{cases}$

Примеры:

①  $\mathbb{Z}$ ,  $\pm p$ , где  $p \in \mathbb{N}$  – простое число

$\pm 7$  – простые элементы  $\mathbb{Z}$ ,

$\pm 1$ ,  $\bar{0}$ ,  $6 = 2 \cdot 3 = (-2)(-3)$  не являются простыми в  $\mathbb{Z}$ .

②  $K[x]$ ,  $K$  – поле. Простой элемент – неприводимый многочлен

В  $\mathbb{R}[x]$  простые элементы = мн-ны  $\begin{cases} 1\text{-ой степени} \\ 2\text{-ой степени, } D < 0 \end{cases}$   
 В  $\mathbb{C}[x]$  простые элементы = многочлены 1-ой степени

## 2.2 Разложение на простые множители в евклидовом кольце

### Лемма.

$A$  - евклидово кольцо,  $p$  - его простой элемент,  $a_1, \dots, a_n \in A$

$p|a_1, \dots, a_n \Rightarrow \exists i \in \{1, \dots, n\} : p|a_i$

**Док-во:** (индукция по  $n$ )

1)  $n = 2$   $p|a_1a_2$  и пусть  $p \nmid a_1 \Rightarrow (p_1, a_1) = 1$   
 $\Rightarrow p|a_2$

2) Пусть верно для  $n - 1$ . Докажем для  $n$ :

$p|a_1(a_2 \dots a_n) \Rightarrow \begin{cases} p|a_1 \\ p|a_2 \dots a_n \text{ по предположению индукции} \end{cases} \Rightarrow \exists i \in \{2 \dots n\} p|a_i$

### Теорема.

$A$  - евклидово кольцо  $\Rightarrow$

$\forall$  ненулевой необратимый элемент  $A$   $a \in A \setminus (A^* \cup \{0\})$  можно представить в виде  $a = p_1 p_2 \dots p_n$ , где  $p_i$  - простой элемент  $A$   $i = \overline{1, n}$ , причём это разложение единственно с точностью до ассоциированности, то есть если  $a = p_1 \dots p_n = q_1 \dots q_m$  - 2 разложения на простые множители, то  $n = m$  и после перенумерации  $p_1 \sim q_1, p_2 \sim q_2, \dots, p_n \sim q_n$ .

**Опр.** Целостное кольцо с однозначным (в смысле ассоциированности) разложением на простые множители называется факториальным кольцом. (Не путать с факторкольцом!).

Используя этот термин, теорему можно сформулировать так:

**Теорема.**

Евклидово кольцо является факториальным.

**Док-во:**

1)  $\exists$  разложение на простые множители  $\forall a \in A \setminus (A^* \cup 0)$

Докажем от противного:

Пусть  $\exists$  элементы  $\in A \setminus (A^* \cup 0)$ , которые нельзя разложить на простые множители.

Рассмотрим  $c$  - самый маленький по норме  $N$  из этих элементов

$$N : A \setminus \{0\} \longrightarrow \mathbb{Z}_+ = \mathbb{N} \cup \{0\},$$

$c$  не может быть простым  $\Rightarrow c = ab$ , оба  $a$  и  $b$  необратимые и ненулевые.

Если  $a, b$  раскладываются на простые множители  $\Rightarrow c$  раскладывается на множители  $\times \Rightarrow$

$\Rightarrow a$  или  $b$  не раскладывается на простые множители. Например, это элемент  $a$ ,  $N(a) < N(a, b) = N(c) \times \Rightarrow$

$\Rightarrow \nexists$  элемента, который не раскладывается на простые множители.

2) Пусть  $a \in A \setminus (A^* \cup \{0\})$

$a = p_1 \dots p_n = q_1 \dots q_n$  имеет 2 разложения на простые множители.

$$\text{Докажем, что } n = m \text{ и после перенумерации} \left\{ \begin{array}{l} p_1 \sim q_1 \\ p_2 \sim q_2 \\ \cdot \quad \cdot \quad \cdot \\ p_n \sim q_n \end{array} \right.$$

( $a$  однозначно раскладывается на простые с точностью до ассоцииро-

ванности)

индукцией по  $n$ :

Если  $n = 1$

$$p_1 = q_1 \dots q_m$$

$$p_1 - \text{простое} \Rightarrow \begin{cases} m = 1 \\ p_1 = q_1 \end{cases}$$

Пусть утверждение верно для  $n - 1$ , докажем для  $n$ :

$$p_1 \dots p_n = q_1 \dots q_m \Rightarrow p_1 | q_1 \dots q_m \Rightarrow \text{по лемме } \exists i \in \{1, \dots, m\}$$

$p_1 | q_i$ , но  $q_i$  - простой  $\Rightarrow p_1 \sim q_i$  ассоциированы.

Назовём  $q_i = q_1$   $q_1 = \varepsilon p_1$ ,  $\varepsilon \in A^*$

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m = \varepsilon p_1 q_2 \dots q_m = p_1 \tilde{q}_2 \dots q_m \quad (\tilde{q}_2 \sim q_2)$$

$$p_2 \dots p_n = \tilde{q}_2 \dots q_m$$

$$\text{по предположению индукции } n = m \quad \begin{cases} p_2 \sim \tilde{q}_2 \sim q_2 \\ \dots \dots \dots \\ p_n \sim q_m \end{cases}$$

$$\text{Пример: } \mathbb{R}[x] \ni x^2 - 3x + 2 = (x - 1)(x - 2) = 2(x - 1)\left(\frac{x}{2} - 1\right)$$

### 2.3 Факториальное кольцо

**Утв 1.** В факториальном кольце простых элементов бесконечно много.

**Док-во:** Пусть  $p_1, \dots, p_n$  - все простые элементы кольца  $A$ .

Рассмотрим  $c = p_1 p_2 \dots p_n + 1$   $p_i \nmid c \quad \forall i = \overline{1, n} \Rightarrow c \in A \setminus (A^* \cup \{0\})$ .

$A$  - факториальное кольцо  $\Rightarrow c$  должно раскладываться на простые множители  $\Rightarrow c$  - должно делиться на простой элемент  $\times$  Мы пришли к противоречию  $\Rightarrow$  простых элементов бесконечное число.

**Утв 2.**  $A$  - евклидово кольцо (факториальное кольцо)  $a \in A$

$a = p_1^{k_1} \dots p_n^{k_n}$  - разложение  $a$  на простые  $p_i \neq p_j$  при  $i \neq j$

Тогда  $d | a \Rightarrow d = p_1^{l_1} \dots p_n^{l_n}$ , где  $0 \leq l_i \leq k_i$

**Док-во:**  $d \mid a \Rightarrow a = dc$  разложим  $d$  и  $c$  на простые множители:  
 $d = q_1^{l_1} \dots q_m^{l_m}$ ,  $c = q_{m+1}^{s_{m+1}} \dots q_t^{s_t} \Rightarrow a = p_1^{k_1} \dots p_n^{k_n} = q_1^{l_1} \dots q_m^{l_m} q_{m+1}^{s_{m+1}} \dots q_t^{s_t}$   
однозначно до ассоциированности  $\Rightarrow d = p_1^{l_1} \dots p_m^{l_m}$ ,  $0 \leq l_i \leq k_i$ ,  $i = \overline{1, m}$

**Опр.**  $A$  - область целостности,  $a, b \in A$ , наименьшим общим кратным  $\text{НОК}\{a, b\} = [a, b]$  называется  $c \in A$  :

$$\left\{ \begin{array}{l} a \mid c \\ b \mid c \end{array} \right. \text{ и } \forall \text{ элемент,}$$

который делится на  $a$  и  $b$  (кратный им), делится на  $c$

$$\left( \forall f : \left\{ \begin{array}{l} a \mid f \\ b \mid f \end{array} \right\} \right) \Rightarrow [a, b] \mid f$$

**Утв 3.** В  $\forall$  факториальном кольце  $A$

$$\forall a, b \in A \quad \exists [a, b] \text{ и } [a, b](a, b) = ab$$

**Доказать самим**

$$\text{Группа } (G, \cdot) \quad \forall g_1, g_2 \in G \mapsto g_1 \cdot g_2 \in G :$$

## 2.4 Аксиомы группы

- 1)  $(g_1 g_2) g_3 = g_1 (g_2 g_3) \quad \forall g_1, g_2, g_3 \in G$  ассоциативность
- 2)  $\exists e \in G : g \cdot e = e \cdot g = g \quad \forall g \in G$  ( $\exists$  нейтрального элемента)
- 3)  $\forall g \in G \exists g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$  ( $\exists$  обратного элемента)

## 2.5 Следствия аксиом группы

**Следствия:**

- 1)  $e$  (нейтральный элемент) единственный
- 2)  $\forall g \in G \quad g^{-1}$  единственен
- 3)  $gh_1 = gh_2 \Rightarrow h_1 = h_2 \quad \forall h_1, h_2, g \in G$  возможны сокращения
- 4) Уравнения  $gx = h$  имеет в  $G$  единственное реш.  $x = g^{-1}h \quad \forall g, h \in G$
- 5) Уравнения  $xg = h$  имеет в  $G$  единственное реш.  $x = hg^{-1} \quad \forall g, h \in G$
- 6)  $\forall g_1, g_2 \in G \quad \exists (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$

Доказать самим.



## 2.6 Порядок группы

**Опр.**

Число элементов в группе называется её порядком и обозначается  $|G|$ . Если в группе бесконечное число элементов, то говорят, что её порядок равен бесконечности  $|G| = \infty$ .

Примеры:

1)  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

$(\mathbb{R}^*, \cdot)$  - группа  $|\mathbb{R}^*| = \infty$

2)  $1, -1 \in \mathbb{Z}$

$(\{1, -1\}, \cdot)$  - группа  $|G| = 2$

## 2.7 Таблица Кэли

Таблица Кэли - таблица умножения элементов группы. В любой её строке и любом столбце встречается каждый элемент группы по одному разу.

Пример:  $G_1 = (\{1, -1\}, \cdot)$

$\cdot$	1	-1
1	1	-1
-1	-1	1

$$|G_1| = 2$$

Пусть  $G_2 = \{e, a\}$ ,  $a \neq e$

Если  $a \cdot a = a$ , то  $a = e$ , что противоречит условию  $\Rightarrow$   
 $\Rightarrow aa = e$ .

Таблица Кэли для  $G_2$  аналогична таблице  $G_1$ .

$\cdot$	e	a
e	e	a
a	a	e

## 2.8 Изоморфизм групп

**Опр.**  $(G_1, \cdot)(G_2, *)$  - группы

$f : G_1 \longrightarrow G_2$  - отображение называется изоморфизмом групп, если:

- 1)  $f(a_1 \cdot a_2) = f(a_1) * f(a_2) \quad \forall a_1, a_2 \in G_1$
- 2)  $f$  - биекция

**Опр.** Если  $\exists$  изоморфизм  $f : G_1 \longrightarrow G_2$ , то  $G_1$  и  $G_2$  называются изоморфными группами  $G_1 \simeq G_2$

**NOTE:**

$|G_1| = |G_2| < \infty$

таблицы Кэли одинаковы с точностью до перенумерации элементов  $\left. \vphantom{\begin{matrix} |G_1| = |G_2| < \infty \\ \text{таблицы Кэли одинаковы с точностью до перенумерации элементов} \end{matrix}} \right\} \Leftrightarrow$

$\Leftrightarrow G_1 \simeq G_2$  изоморфизм.

Пример показывает, что с точностью до изоморфизма

$\exists!$  группа  $G : |G| = 2$ .

Эта группа абелева, так как таблица Кэли симметрична относительно главной диагонали.

## 3 Лекция №3

### 3.1 Важные примеры групп

1)  $X$  - множество,  $f : X \longrightarrow X$  - отображение в себя - преобразование  $X$ .

$S(X)$  - множество биективных преобразований множества  $X$

$(S(X), \cdot)$  - группа, так как

$$f_1, f_2 \in S(X) \Rightarrow f_1 f_2 \in S(X)$$

1)  $(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$  ассоциативность (см. 2 семестр)

2)  $\exists e = id \in S(X) : id \circ f = f \circ id = f \quad \forall f \in S(X)$

3)  $\forall f \in S(X) \quad \exists f^{-1} \in S(X) : f^{-1} \circ f = f \circ f^{-1} = id$  (см. 2 семестр)

В частности, если  $X$  конечное множество

$|X| = n$ ,  $X = \{1, 2, \dots, n\}$ ,  $\alpha$  - подстановка,  $\alpha \in S(X)$

$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 2 & 1 & \dots & \dots \end{pmatrix}$ ,  $S(X) = S_n$  - симметрическая группа степени  $n$   
(группа подстановок из  $n$  элементов),  $|S_n| = n!$

**2)**  $E^2$  - евклидова плоскость

$f$  - движение  $E^2$  - биективное преобразование  $E^2$ , сохраняющее расстояние.

Множество всех движений  $E^2$  -

$Isom E^2$  - группа

Аналогично,  $Isom E^3$  - группа

### 3.2 Кольцо вычетов по модулю $n$

**3)**  $(\mathbb{Z}_n, +, \cdot)$  - кольцо вычетов по модулю  $n$ ,

**Опр.**  $a, b \in \mathbb{Z}$  сравнимы по модулю  $n$   $a \equiv b \pmod{n}$ , если  $a - b : n \Leftrightarrow$   
 $a, b$  имеют одинаковые остатки при делении на  $n$ .

$a \equiv b \pmod{n}$  - отношение эквивалентности

1)  $a \sim a$  **рефлексивность**

2)  $a \sim b \Rightarrow b \sim a$  **симметричность**

3)  $a \sim b, b \sim c \Rightarrow a \sim c$  **транзитивность**

$[a] = \{b \in \mathbb{Z} : a \sim b\}$  - класс эквивалентных элементов

$\mathbb{Z}$  разбивается на непересекающиеся классы  $a$  эквивалентности. Классы можно пронумеровать остатками от деления на  $n$ :  $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$

**Опр.** Отношение эквивалентности называется согласованным с операцией  $*$ ,

$$\text{если } \begin{cases} a \sim a_1 \\ b \sim b_1 \end{cases} \Rightarrow a * b \sim a_1 * b_1$$

Тогда можно определить:  $[a] * [b] = [a * b]$

**Докажем**, что сравнимость по  $\text{mod } n$  согласована

с операциями  $+, \cdot$  в  $\mathbb{Z}$

$$\left. \begin{matrix} a \sim a_1 \\ b \sim b_1 \end{matrix} \right\} \Rightarrow \begin{matrix} a + b \sim a + b_1 \sim a_1 + b_1 \\ ab \sim ab_1 \sim a_1 b_1 \end{matrix}$$

**Опр.**  $[a] + [b] = [a + b], \quad [a][b] = [ab]$

$(\mathbb{Z}_n, +, \cdot)$  – ассоциативное коммутативное кольцо с 1

Св-ва операций в  $\mathbb{Z}$ , выражаемые тождествами, наследуются в  $\mathbb{Z}_n$

$(\mathbb{Z}_n, +)$  – группа (аддитивная группа кольца)

$$|\mathbb{Z}_n| = n \quad \mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\} = \{[0], [1], [2], \dots, [n-1]\}$$

Пусть  $\mathbb{Z}_n^*$  – множество обратимых относительно умножения элементов  $\mathbb{Z}_n$

**Утв. 1.**  $\bar{a} \in \mathbb{Z}_n$  является обратимым  $(\bar{a} \in \mathbb{Z}_n^*) \Leftrightarrow (a, n) = 1$

**Док-во:**  $(\bar{a} \in \mathbb{Z}_n^*) \Leftrightarrow \exists \bar{x} \in \mathbb{Z}_n : \bar{a} \bar{x} = \bar{1} \Leftrightarrow ax = 1 + ny$

$$\exists x, y \in \mathbb{Z} : ax + ny = 1 \Leftrightarrow (a, n) = 1$$

Примеры:

$\mathbb{Z}_{12}$

$$\bar{5} \in \mathbb{Z}_{12}^* \text{ т.к. } (5, 12) = 1, \quad \bar{5}^{-1} = \bar{5}$$

$$\bar{6} \notin \mathbb{Z}_{12}^*$$

$$|\mathbb{Z}_n^*| = \varphi(n) = |\{k \in \mathbb{N} : k < n, (k, n) = 1\}| - \text{функция Эйлера}$$

Позже мы докажем, что если  $n = p_1^{s_1} \dots p_e^{s_e}$

$p_1, \dots, p_e$  – простые различные между собой числа, то

$$\varphi(n) = n \left(1 - \frac{1}{p}\right) \dots \left(1 - \frac{1}{p_e}\right)$$

**Лемма:** В поле нет делителей нуля.

**Док-во:**  $F$  – поле  $a, b \in F$  Пусть  $\begin{cases} a \neq 0 \\ b \neq 0 \end{cases} : ab = 0, \exists a^{-1} \in F \Rightarrow$

$a^{-1}ab = a^{-1}0 \Rightarrow b = 0$  противоречие. ✗

**Утв. 2.**  $(\mathbb{Z}_n, +, \cdot)$  является полем  $\Leftrightarrow \begin{cases} n \geq 2 \\ n - \text{простое число} \end{cases}$

**Док-во:**  $\Rightarrow$  Пусть  $n$  – составное,  $n = kl$   
 $\left. \begin{array}{l} \bar{k} \cdot \bar{l} = 0 \\ \bar{k} \neq 0 \quad \bar{l} \neq 0 \end{array} \right\} \Rightarrow \bar{k}, \bar{l} \text{ делители } 0 \text{ в } \mathbb{Z}_n \Rightarrow \mathbb{Z}_n \text{ не поле} \quad \text{✗} \Rightarrow n - \text{простое}$   
 $\Leftrightarrow n - \text{простое} \Rightarrow (n, r) = 1 \quad \forall r - \text{остатка от деления на } n, \quad \bar{r} \in \mathbb{Z}_n^*$   
 $\forall \bar{r} \in \mathbb{Z}_n \setminus \{0\} \Rightarrow \mathbb{Z}_n - \text{поле}$

**Обозначение:**  $n$  – простое  $\Rightarrow \mathbb{Z}_n = \mathbb{F}_n$  ( $\mathbb{Z}_n$  – поле), например,  $\mathbb{Z}_5 = \mathbb{F}_5$

**Утв. 3.**  $(A, +, \cdot)$  – ассоциативное кольцо с 1  $\Rightarrow$   
 $\Rightarrow (A^*, \cdot)$  – группа (мультипликативная группа кольца)  
В частности,  $A$  – поле  $\Rightarrow (A^*, \cdot)$  – мультипликативная группа поля.  
Доказать самим.

### 3.3 Подгруппа

**Опр.**  $(G, \cdot)$  – группа. Непустое подмножество  $G \neq H \subset G$  – называется её подгруппой, если  $H$  является группой, относительно операций, определённых в  $G$  и ограниченных на  $H$ .

**Обозначение:**  $H < G$

$$H < G \Leftrightarrow \begin{cases} 0) h_1, h_2 \in H \Rightarrow h_1 h_2 \in H \quad \forall h_1, h_2 \in H \\ 1) (h_1 h_2) h_3 = h_1 (h_2 h_3) \quad \forall h_1, h_2, h_3 \in H \\ 2) \exists e_H \in H : e_H \cdot h = h \cdot e_H \quad \forall h \in H \\ 3) \forall h \in H \quad \exists h^{-1} \in H : h \cdot h^{-1} = h^{-1} \cdot h = e_H \end{cases}$$

**Утв. 4.** Критерий того, что  $H$  является подгруппой  $G$

$$H < G \Leftrightarrow \begin{cases} \textcircled{1} & e \in H \quad (e \in G) \\ \textcircled{2} & h_1, h_2 \in H \Rightarrow h_1 h_2 \in H \\ \textcircled{3} & \forall h \in H \quad \exists h^{-1} \in H \end{cases}$$

**Док-во:**  $\Rightarrow$  Пусть  $H < G \Rightarrow \textcircled{1}) \Rightarrow \textcircled{2})$

$H \neq \emptyset \Rightarrow \textcircled{1}) \exists e_H \in H$

Рассмотрим  $e_H e_H = e_H$ , так как  $e_H \in G \quad \exists e_H^{-1} \Rightarrow e_H = e \in H$

3)  $\forall h \in H \quad \exists h^{-1} \in H : h h^{-1} = h^{-1} h = e_H = e \Rightarrow \textcircled{3})$

$\Leftarrow \textcircled{1}) \Rightarrow H \neq \emptyset \quad \textcircled{2}) \Rightarrow 0)$

1) ассоциативность следует из ассоциативности в  $G$

2) в качестве  $e_H$  возьмём  $e \in G$

3)  $\Leftarrow \textcircled{3})$  (учитывая, что  $e_H = e$ )

Примеры:

(1)  $(\mathbb{Z}, +) > (2\mathbb{Z}, +)$

1)  $0 \in 2\mathbb{Z}$

2)  $h_1, h_2 \in 2\mathbb{Z} \Rightarrow h_1 + h_2 \in 2\mathbb{Z}$

$h_1 = 2k \quad h_2 = 2l \Rightarrow h_1 + h_2 = 2(k + l)$

3)  $h \in 2\mathbb{Z} \Rightarrow -h \in 2\mathbb{Z}$

(2)  $Isom E^2 > Sym \Omega \quad (\Omega - \text{фигура})$

$Sym \Omega$  - множество движений  $E^2$ , сохраняющих фигуру  $\Omega$ .

Доказать самим.

### 3.4 Степень элемента группы

**Опр.**  $G$  - группа,  $g \in G, \quad \forall n \in \mathbb{Z}$  определено  $g^n$

1)  $n = m \in \mathbb{N} \quad g^n = g^m = g \dots g \text{ (} n \text{ раз)}$

2)  $n = 0 \quad g^0 = e$

3)  $n = -m \quad g^n = g^{-m} = (g^{-1})^m = g^{-1} \dots g^{-1} \text{ (} m \text{ раз)}$

**NOTE:**  $g^n = g^m \Leftrightarrow g^{n-m} = e \quad g \in G$

### Свойства

- 1)  $g^m g^k = g^{m+k}$ ,
- 2)  $(g^m)^{-1} = g^{-m}, \quad \forall m, k \in \mathbb{Z}$
- 3)  $(g^m)^k = g^{mk}$

Доказать самим.

### 3.5 Порядок элемента группы

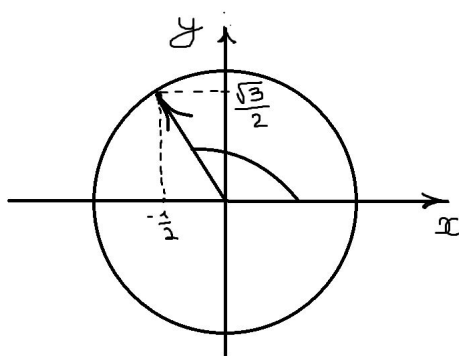
**Опр.**  $G$  - группа,  $g \in G$ ,  $\text{ord } g$  - наименьшее натуральное число  $n$ :  $g^n = e$

Если не существует  $n \in \mathbb{N} : g^n = e$ ,  $\text{ord } g = \infty$

(В адитивной записи  $(G, +)$   $g \in G$   $\text{ord}_+ g = n$ , если  $n$  - наименьшее натуральное число :  $ng = g + \dots + g = 0$ )

Примеры:

- ①  $(\mathbb{Z}, +)$   $\text{ord}_+ 1 = \infty$ ,  $\text{ord}_+ 0 = 1$
- ②  $(\mathbb{R}^*, \cdot)$   $\text{ord } 1 = 1$ ,  $\text{ord}(-1) = 2$
- ③  $(\mathbb{C}^*, \cdot)$   $\text{ord } i = 4$ ,  $\text{ord}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = \text{ord } e^{i\frac{2\pi}{3}} = 3$



## 4 Лекция №4

### 4.1 Циклические группы

$G$  – группа,  $g \in G$   $\langle g \rangle = \{g^n, n \in \mathbb{Z}\}$   $\langle G \rangle$  – циклическая подгруппа, порождённая  $g$ .

Если  $\exists g \in G : G = \langle g \rangle$ , то  $G$  – циклическая группа, порождаемая  $g$ .

Пример:  $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$

Note:  $G = \langle g \rangle$  является абелевой, так как  $g^k \cdot g^l = g^{k+l} = g^l \cdot g^k$

**Опр.**  $G$  – группа,  $n \in \mathbb{N}$  называется порядком  $g \in G$ , если  $n$  – min натуральное число:  $g^n = e$ ,

**Обозначение:**  $n = \text{ord } g$

Если  $\nexists n \in \mathbb{N} : g^n = e$ , то  $\text{ord } g = \infty$

**Утв. 1.**  $G$  – группа  $\text{ord } g = \infty \Rightarrow g^m \neq g^k$  при  $m \neq k$

**Док-во:** Пусть  $g^m = g^k$ , при  $m \neq k$  и пусть  $m > k \Rightarrow g^{m-k} = e$   
 $m - k \in \mathbb{N} \quad \text{и} \quad \text{ord } g = \infty \Rightarrow$  Все степени различны

**Следствие.** Если в группе  $G \exists g \in G : \text{ord } g = \infty \Rightarrow |G| = \infty$

**Утв. 2.**  $G$  – группа  $\text{ord } g = n < \infty \quad g^m = e \Leftrightarrow m : n (\Leftrightarrow n | m)$

**Док-во:**  $\Rightarrow$

1)  $m = 0 \quad g^m = g^0 = e \quad 0 : n$

2) Заметим, что  $g^m = e \Rightarrow g^{-m} = (g^m)^{-1} = e \Rightarrow$  можно считать  $m \in \mathbb{N}$

$\exists S, r \in \mathbb{Z}_+ \quad m = ns + r$ , где  $\begin{cases} r = 0 \Leftrightarrow m : n \\ 0 < r < n \end{cases}$

Пусть  $0 < r < n \quad g^m = g^{ns+r} = g^{ns} \cdot g^r = (e^s)g^r = g^r = e \Rightarrow$  противоречит тому, что  $\text{ord } g = n > r \Rightarrow m : n$

$\Leftarrow m : n \Leftrightarrow m = ns \quad g^m = g^{ns} = (g^n)^s = (e)^s = e$



**УТВ.3**  $G$  – группа,  $g \in G$  :  $\text{ord } g = n < \infty$   
 $g^m = g^l \Leftrightarrow m \equiv l \pmod{n} \Leftrightarrow (m-l):n$

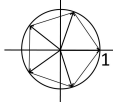
**Док-во:**  $g^m = g^l \Leftrightarrow g^{m-l} = e \Leftrightarrow (m-l):n \Leftrightarrow m \equiv l \pmod{n}$

**УТВ.4**  $G = \langle g \rangle \Rightarrow |G| = |\langle g \rangle| = \text{ord } g$

**Док-во:** 1)  $\text{ord } g = \infty$   $\langle g \rangle = \{g^n, n \in \mathbb{Z}\}$ , причём  $g^m \neq g^l$  при  $m \neq l \Rightarrow |\langle g \rangle| = \infty$   
 2)  $\text{ord } g = n < \infty$   $\langle g \rangle = \{g^n, n \in \mathbb{Z}\} = \{g^0 = e, g^1, g^2, \dots, g^{n-1}\}$  – все различные между собой  
**УТВ.3\***  $\forall$  степень  $g^k$ , совпадает с одним из этих элементов  $\Rightarrow$   
 $\Rightarrow |\langle g \rangle| = n = \text{ord } G$

Примеры:

- ①  $(\mathbb{Z}, +) = (\langle 1 \rangle, +)$   $\text{ord}_+ 1 = \infty$   $|(\mathbb{Z}, +)| = \infty$
- ②  $2 \in \mathbb{R}^*$ ,  $(\langle 2 \rangle, \cdot) = \{2^n, n \in \mathbb{Z}\}$   $\text{ord } 2 = \infty$   $|(\langle 2 \rangle, \cdot)| = \infty$
- ③  $(\mathbb{Z}_n, +)$   $\text{ord}_+ 1 = n$   $|(\mathbb{Z}_n, +)| = n = \text{ord } 1$
- ④  $(\mathbb{C}_n, \cdot)$   $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\} = \{z = 1 e^{i \frac{2\pi k}{n}}, k = 0, 1, \dots, n-1\}$  -

циклическая группа  $\text{ord } e^{i \frac{2\pi k}{n}} = n$ ,  $|(\mathbb{C}_n, \cdot)| = n$  

**УТВ.5**  $G = \langle g \rangle$ ,  $|\langle g \rangle| = \infty \Rightarrow (G, \cdot) \cong (\mathbb{Z}, +)$

**Док-во:** Построим изоморфизм  $f : (\mathbb{Z}, +) \rightarrow (G, \cdot)$  :  
 $\forall n \in \mathbb{Z} \ f(n) = g^n \in G$   
 1)  $f$  – сюръекция, т.к.  $\forall g^k \in \langle g \rangle \ \exists k \in \mathbb{Z} : f(k) = g^k$   
 2)  $f$  – инъекция, т.к.  $f(k) = f(m) \Leftrightarrow g^k = g^m \Rightarrow k = m$  ( $\text{ord } g = \infty$ )  
 1), 2)  $\Rightarrow f$  – биекция  
 3)  $f(m+n) = g^{m+n} = g^m g^n = f(m)f(n) \Rightarrow f$  – гомоморфизм  
 1), 2), 3)  $\Rightarrow f$  – изоморфизм

Примеры:

$$\mathbb{R}^* > (< 2 >, \cdot) \simeq (\mathbb{Z}, +)$$

$$\mathbb{Z} > (< 2 >, +) = 2\mathbb{Z} \simeq (\mathbb{Z}, +)$$

**Утв. 6**  $G = \langle g \rangle$  (циклическая группа),  
 $|\langle g \rangle| = n \Rightarrow (G, \cdot) \cong (\mathbb{Z}_n, +)$

**Док-во:** Построим изоморфизм.  $f : (\mathbb{Z}_n, +) \longrightarrow (G, \cdot)$

Положим:  $\bar{k} \in \mathbb{Z}_n$   $f(\bar{k}) = g^k$

Это определение корректно, т.к.

$$\bar{k} = \bar{l} \Leftrightarrow k \equiv l \pmod{n} \Rightarrow g^k = g^l \Leftrightarrow f(\bar{k}) = f(\bar{l})$$

$$1) f - \text{сюръективно, т.к. } \forall g^k \in \langle g \rangle \exists \bar{k} \in \mathbb{Z}_n : f(\bar{k}) = g^k$$

$$2) f - \text{инъективно, т.к. } f(\bar{k}) = f(\bar{l}) \Leftrightarrow k \equiv l \pmod{n} \Leftrightarrow \bar{k} = \bar{l}$$

$$3) f(\bar{k} + \bar{l}) = f(\overline{k+l}) = g^{k+l} = g^k g^l = f(\bar{k}) f(\bar{l}) \Rightarrow f - \text{гомоморфизм}$$

$$1), 2) \Rightarrow \text{биекция.} \quad 1), 2), 3) \Rightarrow \text{изоморфизм.}$$

$$(G, \cdot) \cong (\mathbb{Z}_n, +)$$

Пример:  $(\mathbb{C}_n, \cdot) \cong (\mathbb{Z}_n, +)$

$$Rot \bigcirc = \langle \varphi_{\frac{2\pi}{6}} = \varphi_{\frac{\pi}{3}} \rangle \quad |Rot \bigcirc| = 6$$

$$ord \varphi_{\frac{\pi}{3}} = 6 \quad Rot \bigcirc \simeq (\mathbb{Z}_6, +) \simeq (\mathbb{C}_6, \cdot)$$

**Утв. 7.**  $G$  - группа  $ord g = n < \infty \Rightarrow ord g^k = \frac{n}{(n, k)}$

**Док-во:**  $k = 0. \quad ord g^k = ord g^0 = ord 1 = 1 = \frac{n}{n}, \quad n = (n, 0)$

$$k \neq 0. \quad \text{Пусть } (n, k) = d \Rightarrow \begin{cases} n = dn_1 \\ k = dk_1 \\ (n_1, k_1) = 1 \end{cases} \Rightarrow n_1 = \frac{n}{d} = \frac{n}{(n, k)}$$

Пусть  $(g^k)^m = e$

$$(g^k)^m = g^{km} = e \Rightarrow km : n \Leftrightarrow km = ns$$

$$k = dk_1, \quad n = dn_1, \quad n_1 \in \mathbb{N} \Rightarrow dk_1 m = dn_1 s \Rightarrow k_1 m = n_1 s$$

$$\left. \begin{array}{l} (n_1, k_1) = 1 \\ k_1 m : n_1 \end{array} \right\} \Rightarrow m : n_1 \Rightarrow m = n_1 t$$

$$(g^k)^m = e \Rightarrow (g^k)^{-m} = ((g^k)^m)^{-1} = e \Rightarrow \text{можно}$$

рассматривать  $m \in \mathbb{N} \quad m = n_1 t \Rightarrow t \in \mathbb{N}$

$$\text{ord } g^k = \min\{m \in \mathbb{N} : (g^k)^m = e\} = \min\{n_1 t \in \mathbb{N} : (g^k)^{n_1 t} = e\} =$$

$$= n_1 = \frac{n}{(n_1 k)}$$

Проверим, что  $(g^k)^{n_1} = e$

$$(g^k)^{n_1} = g^{kn_1} = g^{dk_1 n_1} = g^{(dn_1)k_1} = (g^n)^{k_1} = e^{k_1} = e, \text{ т.к. } n = \text{ord } g$$

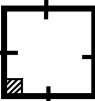
**УТВ.8** Пусть  $|G| = n < \infty$ , тогда

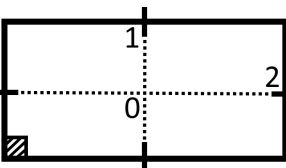
$G$  является циклической группой  $\Leftrightarrow \exists g \in G : \text{ord } g = n$

$$\ominus \left. \begin{array}{l} |\langle g \rangle| = \text{ord } g = n = |G| \\ \langle g \rangle < G \end{array} \right\} \Rightarrow G = \langle g \rangle$$

$$\oplus \quad G = \langle g \rangle \Rightarrow |G| = \text{ord } g = n$$

Примеры:

(1)   $\text{Rot } \square = \langle \varphi_{\frac{2\pi}{4}} = \varphi_{\frac{\pi}{4}} \rangle \simeq \{\mathbb{Z}_4, +\}$

(2)   $\text{Sym } \square = \langle id, s_1, s_2, \varphi_\pi \rangle$

$$\text{ord } id = 1$$

$$\text{ord } s_1 = \text{ord } s_2 = \text{ord } \varphi_\pi = 2$$

$|\text{Sym } \square| = 4$ ,  $\nexists$  элемента порядка 4.  $\text{Sym } \square$  не является циклической.

Эта группа называется четверная группа Клейна

**NOTE:** Порождающим элементом циклической группы является элемент, порядок которого совпадает с её порядком.

**Следствие 1:**  $G = \langle g \rangle \quad \text{ord } g = n = |G|$   
 $g^k$  является порождающим элементом  $G \Leftrightarrow (n, k) = 1$ .

**Следствие 2:** Количество различных порождающих элементов в группе  $\langle g \rangle$ :  $\text{ord } g = n$  равно  $\varphi(n)$  - значению функции Эйлера от  $n$ .

**Следствие 3:** В  $\langle g \rangle$ :  $\text{ord } g = n \quad \forall$  элемент является порождающим  $\Leftrightarrow n$  - простое.

## 4.2 Подгруппы циклической группы

**Утв. 9.** Любая подгруппа циклической группы циклическая.

**Док-во:**  $H < G = \langle g \rangle$

1)  $H = \langle e \rangle = \langle g^0 \rangle$  циклическая

2)  $\exists g^k \in H : g^k \neq e$

$\Rightarrow g^{-k} \in H$ , так как  $g^{-1} = (g^k)^{-1} \in H \Rightarrow$  можно считать  $k \in \mathbb{N}$

$m = \min\{k \in \mathbb{N} : g^k \in H\} \Rightarrow \langle g^m \rangle = H$

Докажем это:

$$k = ms + r \begin{cases} r = 0 \Rightarrow g^k = g^{ms} = (g^m)^s \\ 0 < r < m \Rightarrow g^k = g^{ms+r} = \text{ord } g^k = \frac{n}{(k, n)} = d \end{cases}$$

## 5 Лекция №5

$0 < r < m \Rightarrow g^k \in H \quad g^m \in H \Rightarrow (g^m)^s \in H \Rightarrow g^{-ms} \in H \Rightarrow$

$\Rightarrow g^{-ms} g^k = g^r \in H \quad \overset{0}{X} \text{ выбору } m \Rightarrow r = 0 \Rightarrow k = ms$

$g^k = g^{ms} = (g^m)^s \quad g^k \in \langle g^m \rangle \Rightarrow H = \langle g^m \rangle$

**Утв. 10**  $G = \langle g \rangle \quad |G| = n \Rightarrow \forall k \in \mathbb{N} : n:k \quad \exists! H < G : |H| = k$

**Док-во:**

⊖ **Док-во существования:**  $n = km$

Рассмотрим  $H = \langle g^m \rangle \quad \text{ord } g^m = \frac{n}{m, n} = \frac{n}{m} = k \Rightarrow |H| = k$

Ⓢ **Док-во единственности:** Пусть  $H_1 < G : |H_1| = k$

$$|H_1| = \langle g^s \rangle \quad \text{ord } g^s = \frac{n}{n, s} = k \quad n = k(n, s) \Rightarrow (n, s) = m,$$

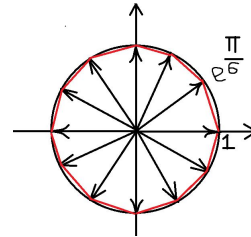
$$\text{где } (l, k) = 1 \quad g^s = (g^m)^l \in H = \langle g^m \rangle$$

$$\left. \begin{array}{l} H_1 \subset H \\ |H_1| = |H| \end{array} \right\} \Rightarrow H_1 = H$$

$$\text{Пример: } \mathbb{C}_{12} = \{z \in \mathbb{C} : z^{12} = 1\} = \{e^{\frac{2\pi k}{12}i}, k = \overline{0, 11}\} = \langle e^{\frac{2\pi}{12}i} = e^{\frac{\pi}{6}i} \rangle$$

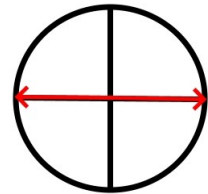
$$|\mathbb{C}_{12}| = 12 \quad \text{Дел } 12 : k = 1, 2, 3, 4, 6, 12$$

$$\left. \begin{array}{l} k = 1 \quad H_1 = \langle 1 \rangle \quad H_1 = 1 \\ k = 12 \quad H_2 = \mathbb{C}_{12} \quad H_2 = 12 \end{array} \right\} \begin{array}{l} \text{тривиальные} \\ \text{(несобственные)} \\ \text{подгруппы} \end{array}$$

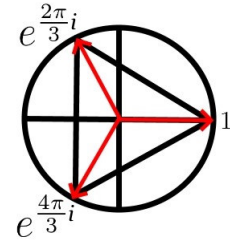


Собственные подгруппы:

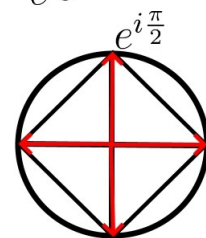
$$k = 2 \quad |H_3| = 2 \quad H_3 = \langle e^{\frac{\pi 6i}{6}} \rangle = \langle e^{\pi i} \rangle = \{1, -1\} \cong (\mathbb{Z}_2, +)$$



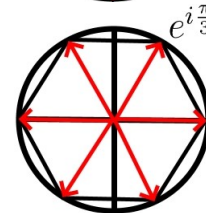
$$k = 3 \quad |H_4| = 3 \quad H_4 = \langle e^{\frac{\pi 4i}{6}} \rangle = \langle e^{\frac{2\pi}{3}i} \rangle \cong (\mathbb{Z}_3, +)$$



$$k = 4 \quad |H_5| = 4 \quad H_5 = \langle e^{\frac{i\pi 3}{6}} \rangle = \langle e^{\frac{\pi}{2}i} \rangle \cong (\mathbb{Z}_4, +)$$



$$k = 6 \quad |H_6| = 6 \quad H_6 = \langle e^{\frac{i\pi 2}{6}} \rangle = \langle e^{\frac{\pi}{3}i} \rangle \cong (\mathbb{Z}_6, +)$$



### 5.1 Симметрическая группа $S_n$

**Опр.** Пусть  $X$  - конечное множество,  $|X| = n$ ,  $X = \{1, 2, \dots, n\}$

$S(X)$  - группа биективных преобразований  $X$  называется симметрической группой степени  $n$  (группой подстановок) и обозначается  $S_n$

$\alpha \in S(X) = S_n$ ,  $\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$  - подстановка из  $n$  элементов

$$|X| = n \Rightarrow S(X) = S_n \Rightarrow |S_n| = n!$$

$$\begin{aligned} \alpha &= \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} & \beta &= \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \\ \beta\alpha &= \beta \circ \alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \\ &= \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} \end{aligned}$$

Пример:  $\alpha, \beta \in S_5$   $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$ ,  $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$

$$\begin{aligned} \beta\alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} 2 & 3 & 5 & 4 & 1 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \end{aligned}$$

В  $S_n$  нейтральный элемент  $id = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ ,

$$\forall \alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \Rightarrow \alpha^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Пример:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} \Rightarrow \alpha^{-1} = \begin{pmatrix} 2 & 3 & 5 & 4 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$$

Название "симметрическая группа" связано с действием  $S_n$  на многочлены от  $n$  переменных

$$f \in \mathbb{R}[x_1, x_2, \dots, x_n] \quad \alpha \in S_n \quad (\alpha f) = f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}) \in \mathbb{R}[x_1, x_2, \dots, x_n]$$

$$f = x_1 x_2 x_3^2, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \Rightarrow \alpha f = x_1 x_3 x_2^2$$

$$f \in \mathbb{R}[x_1, x_2, \dots, x_n] \text{ - симметрический многочлен} \Leftrightarrow \alpha f = f \quad \forall \alpha \in S_n$$

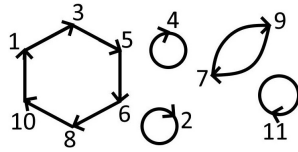
Например:

$x_1 x_2 \dots x_n$  - симметрический многочлен,

$x_1 + x_2 + \dots + x_n$  - симметрический многочлен

Пример:

$$\alpha \in S_{11} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 2 & 5 & 4 & 6 & 8 & 9 & 10 & 7 & 1 & 11 \end{pmatrix} = (1\ 3\ 5\ 6\ 8\ 10)(4)(7\ 3)(2)(11)$$



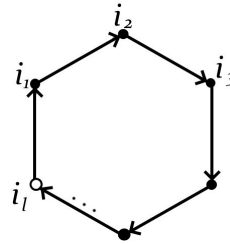
**Утв. 1.**  $\forall \alpha \in S_n$  можно разложить в произведения независимых циклов.

**Утв. 2.** Независимые циклы перестановочны между собой (коммутируют).

**Утв. 3** Разложение подстановки в произведение независимых циклов единственно (с точностью до перестановки циклов).

**Утв. 4**

$\alpha = (i_1, i_2, \dots, i_l)$  – цикл длины  $l$   
 $\text{ord } \alpha = \text{ord}(i_1, \dots, i_l) = l$



**Док-во:**  $\alpha(i_k) = i_{k+1}$      $\alpha(i_l) = i_1$      $\alpha^s(i_k) = i_{k+s}$      $\alpha^l(i_k) = i_k$

**Опр.** Цикленным типом подстановки  $\alpha \in S_n$  называется набор длин независимых циклов, в произведение которых раскладывается  $\alpha$ .

$$\{\alpha\} = \{l_1, l_2, \dots, l_s\}$$

$$l_1 \geq l_2 \geq \dots \geq l_s, \quad l_1 + l_2 + \dots + l_s = n$$

**Утв.5**  $\{\alpha\} = \{l_1, l_2, \dots, l_s\} \Rightarrow \text{ord } \alpha = \text{НОК}\{l_1, l_2, \dots, l_s\}$

**Док-во:** Пусть  $\alpha = \beta_1 \beta_2 \dots \beta_s$  – разложение  $\alpha$  в произведение независимых циклов  $\alpha^k = \beta_1^k \beta_2^k \dots \beta_s^k = id$      $\beta_i^k = id$      $i = \overline{1, s}$      $k : l_i$      $i = \overline{1, s}$   
 $k : \text{НОК}\{l_1, \dots, l_s\}$      $\text{ord } \alpha = \text{НОК}\{l_1, \dots, l_s\}$

**Опр.**

$\alpha = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$  называется чётной, если  $[i_1, i_2, \dots, i_n] + [j_1, j_2, \dots, j_n]$  – чётное число, нечётной в противном случае.

**NOTE:** Это определение корректно,

тк  $\forall$  подстановку  $\alpha$  можно записать в виде  $\begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$ , с точностью до перестановки пары столбцов. При перестановке столбцов, происходит изменение четности верхней и нижней перестановок.  $\Rightarrow$  чётность суммарного числа инверсий не изменятся.

**Опр.**



Пусть  $\alpha = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$ .

Знаком подстановки  $\alpha$  называется число  $\operatorname{sgn} \alpha = (-1)^{[i_1, i_2, \dots, i_n] + [j_1, j_2, \dots, j_n]}$ .

$\operatorname{sgn} \alpha = 1 \Leftrightarrow \alpha$  – чётная;  $\operatorname{sgn} \alpha = -1 \Leftrightarrow \alpha$  – нечётная.

**УТВ. 6.**  $\forall \alpha, \beta \in S_n \quad \operatorname{sgn} (\alpha\beta) = \operatorname{sgn} \alpha \cdot \operatorname{sgn} \beta$

**Док-во:**  $\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$ .

$$\alpha = \begin{pmatrix} j_1 & \dots & j_n \\ k_1 & \dots & k_n \end{pmatrix}$$

$$\operatorname{sgn} \alpha = (-1)^{[j_1, \dots, j_n] + [k_1, \dots, k_n]} \quad \operatorname{sgn} \beta = (-1)^{[1, \dots, n] + [j_1, \dots, j_n]}$$

$$\alpha\beta = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ k_1 & j_2 & \dots & k_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

$$\begin{aligned} \operatorname{sgn}(\alpha\beta) &= (-1)^{[1, \dots, n] + [k_1, \dots, k_n]} = \\ &= (-1)^{([1, \dots, n] + [j_1, \dots, j_n]) + ([j_1, \dots, j_n] + [k_1, \dots, k_n])} = \\ &= (-1)^{[1, \dots, n] + [j_1, \dots, j_n]} (-1)^{[j_1, \dots, j_n] + [k_1, \dots, k_n]} = \\ &= \operatorname{sgn} \beta \operatorname{sgn} \alpha \end{aligned}$$

Пусть  $A_n = \{\alpha \in S_n : \operatorname{sgn} \alpha = 1\}$  – множество чётных подстановок.

**УТВ. 7.**  $A_n < G$

**Док-во:** 1)  $id \in A_n$ , т.к.  $id = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}, \quad \operatorname{sgn}(id) = 1$

2)  $\alpha, \beta \in A_n$ , то есть  $\operatorname{sgn} \alpha = 1, \operatorname{sgn} \beta = 1 \Rightarrow \operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha) \operatorname{sgn}(\beta) = 1 \cdot 1 = 1 \Rightarrow \alpha\beta \in A_n$

3)  $\alpha \in A_n, \quad \alpha = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \quad \operatorname{sgn} \alpha = (-1)^{[i_1, \dots, i_n] + [j_1, \dots, j_n]} = 1 \Rightarrow$

$$\Rightarrow \operatorname{sgn} \alpha^{-1} = (-1)^{[j_1, \dots, j_n] + [i_1, \dots, i_n]} = (-1)^{[i_1, \dots, i_n] + [j_1, \dots, j_n]} = 1.$$

**Опр.**  $A_n$  называется знакопеременной группой

$\left( A_n \text{ сохраняет знакопеременный многочлен } \prod_{1 \leq i < j \leq n} (x_i - x_j) \right).$

**Утв. 8.**  $|A_n| = \frac{n!}{2}$

**Док-во:**  $\alpha \in A_n \Leftrightarrow \alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} : [i_1, i_2, \dots, i_n] - \text{чётное, так}$

как  $[1, 2, \dots, n] = 0$ ,

то есть  $(i_1, i_2, \dots, i_n) - \text{чётная перестановка. Их число } \frac{n!}{2}.$

**Опр.** Подстановка  $(i, j)$  называется транспозицией.

$$(ij)^{-1} = (ji) \quad \text{ord}(ij) = 2$$

$(ij) - \text{нечётная перестановка,}$

$$(ij) = \begin{pmatrix} 1 & \dots & i-1 & i & \dots & j-1 & j & \dots & n \\ 1 & \dots & i-1 & \mathbf{j} & \dots & j-1 & \mathbf{i} & \dots & n \end{pmatrix}$$

$$\text{sgn}(ij) = -1$$

$$\text{NOTE: } \alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

$$\begin{aligned} (i_k i_l)\alpha &= \begin{pmatrix} 1 & 2 & \dots & i_k & \dots & i_l & j & \dots & n \\ 1 & 2 & \dots & i_l & \dots & i_k & j & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \\ &= \begin{pmatrix} i_1 & \dots & i_k & \dots & i_l & \dots & i_n \\ i_1 & \dots & i_l & \dots & i_k & \dots & i_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & i_k & \dots & i_l & \dots & n \\ i_1 & i_2 & \dots & i_l & \dots & i_k & \dots & n \end{pmatrix} \end{aligned}$$

**Утв. 9.**  $\forall \alpha \in S_n$  можно представить в виде произведения транспозиций.

## 6 Лекция №6

**Док-во:**

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}, \quad (j_1 1)\alpha = \begin{pmatrix} 1 & 2 & \dots & l & \dots & n \\ 1 & j_2 & \dots & j_1 & \dots & j_n \end{pmatrix}, \quad \tau_1 = (j_1 1) \Rightarrow$$

$$\Rightarrow \exists \tau_1, \tau_2, \dots, \tau_s : \tau_s, \dots, \tau_3, \tau_2, \tau_1 \alpha = id$$

$$\alpha = (\tau_s, \dots, \tau_2, \tau_1)^{-1} id = \tau_1, \tau_2, \dots, \tau_s$$

**Утв. 10.** Чётная подстановка представляется в виде чётного числа

транспозиций; нечётная - нечётного;

**Док-во:**  $\alpha = \tau_1, \tau_2, \dots, \tau_s \quad \text{sgn } \alpha = \text{sgn } \tau_1 \text{sgn } \tau_2, \dots, \text{sgn } \tau_s = (-1)^s$   
 $\alpha$  – чётная подстановка  $\Leftrightarrow s$  – чётное число,  
 $\alpha$  – нечётная подстановка  $\Leftrightarrow s$  – нечётное число.

**Утв. 11.**  $\alpha = (i_1, \dots, i_k) \in S_n \Rightarrow \text{sgn } \alpha = (-1)^{k-1}$

**Док-во:**  $(i_1, i_2, \dots, i_k) =$   
 $= (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$  - произведение  $(k-1)$  транспозиций

**Утв. 12.**  $\alpha \in S_n$ , цикленный тип  $\{\alpha\} = \{k_1, k_2, \dots, k_l\}, \Rightarrow$   
 $\Rightarrow \text{sgn } \alpha = (-1)^{n-l}$

**Док-во:**  $\alpha = (i_1, \dots, i_{k_1}) \dots (i_1 \dots i_{k_l})$   
 $\text{sgn } \alpha = (-1)^{(k_1-1)+\dots+(k_l-1)} = (-1)^{(k_1+\dots+k_l)-l} = (-1)^{n-l}$

**Утв. 13.**  $\forall \alpha \in A_n$  при  $n \geq 3$  можно представить в виде произведения тройных циклов.

**Док-во:**  $\forall \alpha \in A_n < S_n$  представляется в виде чётного числа транспозиций

Докажем, что  $(i, j)(k, l)$  – можно представить в виде тройных циклов.

- 1)  $(i, j)(j, k) = (kij)$ ,  $i, j, k$  различны
- 2)  $(i, j)(k, l) = (i, j)(j, k)(j, k)(k, l) = (kij)(ljk)$ ,  $((j, k)(j, k) = id)$ .  
 $i, j, k, l$  различны

## 6.1 Система порождающих элементов группы

Пусть  $G$  – группа,  $\emptyset \neq S \subset G$ ,  
 $\langle S \rangle = \{g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k}, k \in \mathbb{N}, \varepsilon_i = \pm 1, i = \overline{1, k}\} \Rightarrow \langle S \rangle \subset G$

**УТВ. 1.**  $\langle S \rangle \leq G$

**Док-во:**

$$1) \exists g \in S \Rightarrow gg^{-1} = e \in \langle S \rangle$$

$$2) h_1 = g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k} \in S, h_2 = g_1^{\varepsilon_1} \dots g_m^{\varepsilon_m} \in S \Rightarrow h_1 h_2 = g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k} g_1^{\varepsilon_1} \dots g_m^{\varepsilon_m} \in \langle S' \rangle$$

$$3) h = g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k} \in \langle S \rangle \Rightarrow h^{-1} = g_k^{-\varepsilon_k} \dots g_1^{-\varepsilon_1} \in \langle S \rangle$$

**NOTE:**

$\langle S \rangle$  минимальная по включению подгруппа, содержащее мн-во  $S$ , т.к.  $S \subset \langle S \rangle$ , а вместе с  $S$  в подгруппу должны войти все произведения нужного вида.

**Опр.** Если  $G = \langle S \rangle$ , то говорят, что  $G$  порождается системой  $S$ , или  $S$  – система порождающих  $G$ .

Примеры:

$$\textcircled{1} G = \langle g \rangle = \{g^k, k \in \mathbb{Z}\}$$

$$\text{а) } k \in \mathbb{N} \quad g^k = g \dots g \quad (k - \text{раз})$$

$$\text{б) } k = 0 \quad g^0 = e = gg^{-1}$$

$$\text{в) } k = -m \quad g^k = g^{-m} = g^{-1} \dots g^{-1} \quad (m - \text{раз}) \quad m \in \mathbb{N}$$

$\textcircled{2}$  УТВ.9 означает, что мн-во всевозможных транспозиций из  $n$  элементов

$$(i, j) \quad i \neq j \quad i, j = \overline{1, n} \text{ - система порождающих } S_n$$

( $S_n$  порождается транспозициями)

$$\text{Например, } S_3 = \{(1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2), id\} = \langle (1, 2), (1, 3), (2, 3) \rangle$$

$\textcircled{3}$  Утверждение 13 означает, что  $A_n$  порождается тройными циклами

$$\text{Например, } A_3 = \{(1, 2, 3), (1, 3, 2), id\} = \langle (1, 2, 3) \rangle$$

## 6.2 Группа диэдра

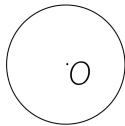
$$O_2 \subset Isom E^2$$

$O_2$  - множество движений плоскости, оставляющих на месте начальную точку  $O$ .  $O_2 < Isom E^2$ .  $O_2$  - ортогональная группа.

$F$  - фигура на плоскости.  $\Rightarrow Sym F < Isom E^2$

$F$  - фигура с центром  $\Rightarrow Sym F < O_2 < Isom E^2$

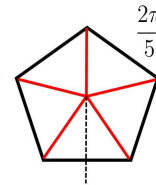
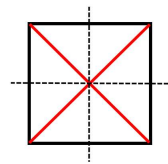
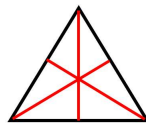
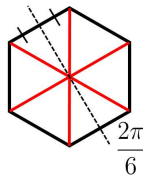
Пример:



$F$  - окружность с центром в точке  $O$ ,  $Sym F = O_2$

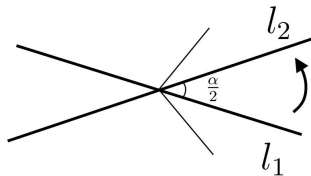
$F$  - правильный  $n$ -угольник,  $n \geq 3$

$Sym F = Sym \hat{n} = D_n$  - группа диэдра



В  $D_n$  входят повороты на углы  $\frac{2\pi}{n}k$ ,  $k = \overline{0, n-1}$  (или  $k = \overline{1, n}$ ) и отражения относительно прямых, соединяющих центр и одну из вершин или центр и середину одной из сторон.

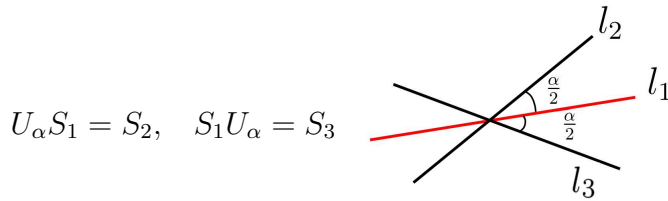
$$|D_n| = 2n \text{ (} n \text{ отражений и } n \text{ поворотов)}$$



$S_1$  - отражение относительно  $l_1$ ,

$S_2$  - отражение относительно  $l_2$ .

$S_2 S_1 = U_\alpha$  - поворот на  $\alpha$



$$U_\alpha S_1 = S_2, \quad S_1 U_\alpha = S_3$$

$D_n$  - некоммутативная группа

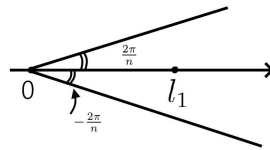
$$D_n = \{id, U_{\frac{2\pi}{n}}, U_{\frac{2\pi}{n}2}, \dots, U_{\frac{2\pi}{n}(n-1)}, S_1, \dots, S_n\} = \langle U_{\frac{2\pi}{n}}, S_1 \rangle$$

$U_{\frac{2\pi}{n}}, S_1$  - система порождающих  $D_n$ ,

где  $U_{\frac{2\pi}{n}}$  - поворот на  $\frac{2\pi}{n}$  против часовой стрелки,

$S_1$  - одно из отражений (симметрий).

$$\text{ord } U_{\frac{2\pi}{n}} = n, \quad \text{ord } S_1 = 2, \quad S_1 U_{\frac{2\pi}{n}} S_1 = U_{-\frac{2\pi}{n}} = U_{\frac{2\pi}{n}}^{-1}$$



**Теорема (достаточное условие того, что группа изоморфна группе диэдра):**

Если  $G = \langle a, b \rangle$ ,  $\text{ord } a = n$ ,  $n \geq 3$ ,  $\text{ord } b = 2$ ,  $bab = a^{-1}$ , то  $G \cong D_n$

**Док-во:**

$$1) b^{-1} = b, \quad ab = ba^{-1}(*), \quad a^{-1}b = ba(**)$$

2) Покажем, что все элементы группы  $G$

имеют вид  $a^k$ ,  $k = 0, 1, \dots, n$  или  $ba^k$ ,  $k = 0, 1, \dots, n$ .

Если в выражении  $g$  через  $a, b$  встречается только  $a \Rightarrow g = a^k$ ,

где  $k = \overline{0, n-1}$

Если в выражении  $g$  через  $a$  и  $b$  встречается  $b^{-1}$ , заменим его на  $b$

Все  $b$  можно вытащить вперёд, пользуясь  $(*)$ ,  $(**)$ ,  $b^2 = e \Rightarrow$  впереди  $b$  останется только в первой степени (или исчезнет).

$$3) \text{ а) } g_1 = a^k, \quad g_2 = a^m, \quad k, m = \overline{0, n-1}, \Rightarrow g_1 g_2 = a^{k+m}$$

$$б) \text{ } g_1 = a^k, \quad k = \overline{0, n-1}, \quad g_2 = ba^l, \quad l = \overline{0, n-1} \Rightarrow$$

$$\Rightarrow g_1 g_2 = a^k ba^l = ba^{-k} a^l = ba^{l-k},$$

$$g_2 g_1 = ba^l a^k = ba^{l+k}$$

$$в) \text{ } g_1 = ba^k, \quad k = \overline{0, n-1}, \quad g_2 = ba^l, \quad l = \overline{0, n-1}$$

$$g_1 g_2 = ba^k \cdot ba^l = b^2 a^{-k} a^l = a^{l-k}$$

Ясно, что таблица Кэли группы определяется однозначно  $\Rightarrow$  с точностью до изоморфизма имеется ровно одна группа  $G$ , удовлетворяющая данным условиям  $\Rightarrow G \cong D_n$ .

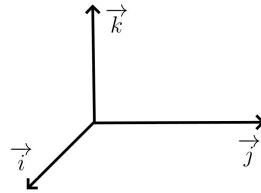
Пример:  $|D_3| = 6, \quad |\mathbb{Z}_6| = 6, \quad D_3 \not\cong \mathbb{Z}_6 \simeq \mathbb{C}_6, \quad |S_3| = 6, \quad S_3 \simeq D_3$

## 7 Лекция №7

### 7.1 Группа кватернионов

Пусть  $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

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



Умножение символов  $i, j, k$  происходит так же, как векторное умножение векторов базиса  $\langle \vec{i}, \vec{j}, \vec{k} \rangle$ ,  $i^2 = j^2 = k^2 = -1$ .

$Q_8$  можно реализовать в виде группы матриц  $\{\pm E, \pm I, \pm J, \pm K\}$ .

$$\begin{aligned} 1 \rightarrow E &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & -1 \rightarrow -E &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} & i \rightarrow I &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\ -i \rightarrow -I &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} & j \rightarrow J &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & -j \rightarrow -J &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ k \rightarrow K &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & -k \rightarrow -K &= \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \text{ord } 1 = 1, \quad \text{ord}(-1) = 2, \quad (-1)^{-1} = 1, \quad \text{ord}(\pm i) = 4, \quad i^{-1} = -i, \quad (-i)^{-1} = i, \\ \text{ord}(\pm j) = 4, \quad j^{-1} = -j, \quad \text{ord}(\pm k) = 4, \quad k^{-1} = k. \end{aligned}$$

$Q_8$  — некоммутативная группа:  $|Q_8| = 8$

$\exists$  ещё некоммутативная группа:  $|G| = 8 \quad G = D_4 \quad Q_8 \not\cong D_4$

Сравним количество элементов определенного порядка в этих группах.

$$Q_8 :$$

Порядок	1	1	6
Количество	1	2	4

$$D_4 :$$

Порядок	1	5	2
Количество	1	2	4

$$Q_8 = \langle i, j \rangle = \langle i, k \rangle = \langle j, k \rangle$$

Покажем, что  $Q_8 = \langle i, j \rangle$ ,  $\text{ord } i = 4$ ,  $i^2 = j^2$

$$\begin{aligned} ((j)^{-1}ij) = -jij = kj = -i = i^{-1} \quad 1 = i \cdot i \cdot i \cdot i = i(-i) = i(i)^{-1} \quad -1 = i \cdot i \\ i = i; \quad -i = (i)^{-1}; \quad j = j \quad (-j) = (j)^{-1} = -j; \quad k = ij; \quad -k = ji \end{aligned}$$

**Теорема(достаточное условие того, что группа изоморфна группе кватернионов):**

Если  $G = \langle a, b \rangle$ ,  $\text{ord } a = 4$ ,  $a^2 = b^2$ ,  $b^{-1}ab = a^{-1}$ , то  $G \cong Q_8$

**Док-во:**

$$1) \text{ord } b = 4 \Rightarrow b^{-1} = b^3, \quad ab = ba^{-1} = ba^3(*) \quad \text{ord } a = 4 \Rightarrow a^{-1} = a^3$$

2)  $g \in G$  выражается через порождающие  $a, b$ . Заменим в его выражении  $a^{-1}$  на  $a^3$ ,  $b^{-1}$  на  $b^3$ ,  $a^2$  на  $b^2 \Rightarrow$  В его выражении через  $a$  и  $b$  могут встречаться  $aa^{-1} = e, a^2, b, a^3 \quad (*) \Rightarrow b$  можно вынести вперёд.

$$a^3b = a^2ba^3 = aba^3a^3 = ba^3a^3a^3 = ba$$

$$bab = bba^3 = a^5 = a$$

$$ba^2b = baba^3 = bba^3a^3 = b^2a^6 = a^8$$

$$ba^3b = ba^2ba^3 = baba^6 = b^2a^9 = a^{11} = a^3$$

$$G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}, \quad |G| = 8$$

Таблица Кэли определяется однозначно.



$e$	$a$	$a^2$	$a^3$	$b$	$ba$	$ba^2$	$ba^3$
$a$	$a^2$	$a^3$	$e$	$ba^3$	$b$	$ba$	$ba^2$
$a^2$	$a^3$	$e$	$a$	$ba^2$	$ba^3$	$b$	$ba$
$a^3$	$e$	$a$	$a^2$	$ba$	$ba^2$	$ba^3$	$b$
$b$	$ba$	$ba^2$	$ba^3$	$a^2$	$a^3$	$e$	$a$
$ba$	$ba^2$	$ba^3$	$b$	$a$	$a^2$	$a^3$	$e$
$ba^2$	$b^3$	$b$	$ba$	$e$	$a$	$a^2$	$a^3$
$ba^3$	$b$	$ba$	$ba^2$	$a^3$	$e$	$a$	$a^2$

$\Rightarrow$  С точностью до изоморфизма  $\exists!$  такая группа  $G$ . Но мы знаем такую группу -  $Q_8 \Rightarrow G \cong Q_8$

## 7.2 Сравнение элементов группы по модулю подгруппы

**Опр.**  $G$  - группа,  $H < G$ ,  $g_1, g_2 \in G$  называются сравнимыми по  $\text{mod } H$

$g_1 \equiv g_2 (\text{mod } H)$ , если  $g_1^{-1}g_2 \in H$ .

(в аддитивной записи  $(-g_1) + g_2 \in H$ )

**Утв. 1.** Сравнимость по  $\text{mod } H$  - отношение эквивалентности.

1)  $g \equiv g (\text{mod } H)$ , (**рефлексивность**),

т.к.  $g^{-1}g = e \in H$

2)  $g_1 \equiv g_2 (\text{mod } H) \Rightarrow g_2 \equiv g_1 (\text{mod } H)$ , (**симметричность**),

т.к.  $g_1^{-1}g_2 \in H \Rightarrow (g_1^{-1}g_2)^{-1} = g_2^{-1}g_1 \in H \Rightarrow g_2 \equiv g_1 (\text{mod } H)$

3)  $g_1 \equiv g_2 (\text{mod } H), g_2 \equiv g_3 (\text{mod } H) \Rightarrow g_1 \equiv g_3 (\text{mod } H)$ , (**транзитивность**),

т.к.  $g_1^{-1}g_2 \in H, g_2^{-1}g_3 \Rightarrow (g_1^{-1}g_2)(g_2^{-1}g_3) = g_1^{-1}g_3 \in H \Rightarrow g_1 \equiv g_3 (\text{mod } H)$

## 7.3 Смежные классы группы по подгруппе.

Отношение эквивалентности разбивает группу  $G$  на непересекающиеся классы эквивалентности - **левые смежные классы** группы  $G$  по подгруппе  $H$   $Lg_1 = \{g \in G : g_1 \equiv g (\text{mod } H)\}$

**УТВ. 2.**  $Lg_1 = g_1H = \{g \in G : \exists h \in H : g = g_1h\}$

**Док-во:**  $g \in Lg_1 \Leftrightarrow g_1 \equiv g(mod H) \Leftrightarrow g^{-1}g \in H \Leftrightarrow \exists h \in H : g^{-1}g = h \Leftrightarrow g \in g^{-1}H$

Если рассмотрим другое отношение эквивалентности  $g_1 \equiv g_2(mod H) \Leftrightarrow g_1g_2^{-1} \in H$  получим **правые смежные классы** группы  $G$  по подгруппе  $H : Rg_1 = Hg_1$ .

### Обозначения:

- 1) Мно-во всех левых смежных классов группы  $G$  по подгруппе  $H$  обозначим  $G/H$
- 2) Мно-во всех правых смежных классов группы  $G$  по подгруппе  $H$  обозначим  $H \backslash G$

### Пример:

$$S_3 = \{id, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}$$

$$H = \langle (1, 2) \rangle = \{id, (1, 2)\} < G$$

$$L_{(1,3)} = (1, 3)H = \{(1, 3), (1, 3)(1, 2) = (2, 3, 1)\} = (2, 3, 1)H = L_{(2,3,1)} = L_{(1,2,3)}$$

$$L_{(2,3)} = (2, 3)H = \{(2, 3), (2, 3)(1, 2) = (2, 1, 3)\} = (2, 1, 3)H = L_{(2,1,3)} = L_{(1,3,2)}$$

$$R_{(1,3)} = H(1, 3) = \{(1, 3), (1, 2)(1, 3) = (3, 2, 1)\} = H(3, 2, 1) = R_{(3,2,1)} = R_{(1,3,2)}$$

$$R_{(2,3)} = H(2, 3) = \{(2, 3), (1, 2)(2, 3) = (3, 1, 2)\} = H(3, 1, 2) = R_{(3,1,2)} = R_{(1,2,3)}$$

$$S_3 / \langle (1,2) \rangle \neq \langle (1,2) \rangle \backslash S_3$$

**УТВ. 3.** В абелевой группе  $G/H = H \backslash G$

**Док-во:**  $gh = hg \quad Lg = gH = Hg = Rg$

**УТВ. 4.**  $\exists$  взаимно-однозначное соответствие между  $G/H$  и  $H \backslash G$

**Док-во:** Рассмотрим  $f : G \rightarrow G$ ,  $f(g) = g^{-1} \Rightarrow f$  - биекция  
 $\forall gh \in gH \xrightarrow{f} (gh)^{-1} = h^{-1}g^{-1} \in Hg^{-1} \Rightarrow gH \xrightarrow{f} Hg^{-1}$ ,  
 $Lg \xrightarrow{f} Rg^{-1}$ ,  $f : G/H \rightarrow H \backslash G$  - биекция, т.к.  
 1)  $\forall Rg \exists Lg^{-1} : f(Lg^{-1}) = Rg$ ,  
 2) Если  $f(Lg_1) = f(Lg_2)$ , т.е.  $Rg_1^{-1} = Rg_2^{-1} \Leftrightarrow g_1^{-1}g_2 \in H \Leftrightarrow Lg_1 = Lg_2$ .

**Опр.** Количество левых (правых) смежных классов группы  $G$  по подгруппе  $H$  называется индексом подгруппы  $H$  в группе  $G$  и обозначается  $|G : H|$ .

**Утв. 5.**

$G$  - группа,  $H < G : |G : H| = 2 \Rightarrow \forall g \in G \quad Lg = Rg$

**Док-во:**  $g \notin H \quad G = H \cup Lg, \quad H \cap Lg = \emptyset$ ,  
 $G = H \cup Rg, \quad H \cap Rg = \emptyset \Rightarrow Lg = Rg$

**Утв. 6.**

$G$  - группа,  $H < G : |H| = n < \infty \Rightarrow \forall g \in G \quad |gH| = |H| = n$

**Док-во:**

$H = \{e, h_1, h_2, \dots, h_{n-1}\}, \quad h_k \neq h_m, \quad k \neq m, \quad k, m = \overline{1, n-1}$   
 $gH = \{g, gh_1, gh_2, \dots, gh_{n-1}\}$ , где  
 $gh_k \neq gh_m, \quad k \neq m, \quad k, m = \overline{1, n-1}$ ,  
 т.к.  $h_k \neq h_m$

## 7.4 Теорема Лагранжа и следствия из неё:

**Теорема Лагранжа.**

$G$  - группа,  $|G| < \infty, \quad H < G \Rightarrow$   
 $|G| = |H| \cdot |G : H|$

**Док-во:** Рассмотрим разбиения  $G$  на левые смежные классы по  $H$ .  
 Их количество -  $|G : H|$ . Количество элементов в  $\forall$  классе -  $|H|$ .

**Следствие 1.**  $\left. \begin{array}{l} |G| < \infty \\ H < G \end{array} \right\} \Rightarrow |G| : |H| \quad (|H| \mid |G|)$

**Следствие 2.**  $|G| < \infty \Rightarrow \forall g \in G \quad |G| : \text{ord } g \quad (\text{ord } g \mid |G|)$

**Док-во:**  $\forall g \in G$  рассмотрим  $H = \langle g \rangle$ ,  $|H| = \text{ord } g \Rightarrow$   
 $\Rightarrow |G| : |H| = \text{ord } g$

**Следствие 3.**  $|G| = p$  - простое число  $\Rightarrow G$  - циклическая группа

**Док-во:**  $g \in G \left[ \begin{array}{l} \text{ord } g = 1 \Leftrightarrow g = e \\ \text{ord } g = p = |G| \Rightarrow \langle g \rangle = G \end{array} \right.$

**Следствие 4.**  $|G| = n < \infty \Rightarrow \forall g \in G \quad g^n = e$

**Док-во:** Пусть  $\text{ord } g = m \Rightarrow$   
 $\Rightarrow n : m \Rightarrow n = mk \Rightarrow g^n = g^{mk} = (g^m)^k = e^k = e$

**Следствие 5. Малая теорема Ферма.**

$p$  - простое,  $a \in \mathbb{Z}$ ,  $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

**Док-во:**  $\bar{a} \in \mathbb{Z}_p^*$ ,  $\mathbb{Z}_p^*$  - группа,  $|\mathbb{Z}_p^*| = p - 1 \Rightarrow$   
 $\Rightarrow \bar{a}^{p-1} = \bar{1}$  в  $\mathbb{Z}_p^* \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$  в  $\mathbb{Z}$

**Следствие 6. Теорема Эйлера.**

$\left. \begin{array}{l} n \in \mathbb{N}, a \in \mathbb{Z} \\ (a, n) = 1 \end{array} \right\} \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

**Док-во:**  $\bar{a} \in \mathbb{Z}_n^*$ ,  $\mathbb{Z}_n^*$  - группа,  $|\mathbb{Z}_n^*| = \varphi(n) \Rightarrow$   
 $\Rightarrow \bar{a}^{\varphi(n)} = \bar{1}$  в  $\mathbb{Z}_n^* \Leftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

**Следствие 7. Теорема Вильсона**

$p \in \mathbb{N}$  – простое число  $\Rightarrow (p-1)! \equiv -1 \pmod{p}$

**Док-во:**  $p$  – простое число  $\Rightarrow \mathbb{Z}_p = \mathbb{F}_p$  – поле

$$\bar{1}, \bar{2}, \dots, \overline{p-1} \in \mathbb{F}_p^* = \mathbb{Z}_p^* \quad |\mathbb{Z}_p^*| = |\mathbb{F}_p^*| = p-1$$

$\forall x \in \mathbb{Z}_p \quad x^{p-1} = \bar{1} \Rightarrow \bar{1}, \bar{2}, \dots, \overline{p-1}$  – корни многочлена  $x^{p-1} - \bar{1}$  над  $\mathbb{F}_p \Rightarrow$   
 $x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) \dots (x - \overline{p-1})$  над  $\mathbb{F}_p$ ,

Сравним свободные члены левой и правой части

$$-\bar{1} = (-1)^{p-1} \bar{1} \cdot \bar{2} \dots \overline{p-1} = \bar{1} \cdot \bar{2} \dots \overline{p-1} \text{ при } p \neq 2, \quad 1! = 1 \equiv -1 \pmod{2}$$

$$(p-1)! \equiv -1 \pmod{p} \quad \forall p \in \mathbb{N} \text{ - простого}$$

**8 Лекция №8****8.1 Определение операции на смежных классах**

Пусть  $H < G$ . Хотим определить операцию на  $G/H$ :

$$(g_1 H)(g_2 H) = g_1 g_2 H. \quad \text{Это можно сделать корректно} \Leftrightarrow$$

$\Leftrightarrow$  Отношение сравнения по  $\text{mod } H$  согласовано с операцией в  $G$ ,

$$\text{т.е.} \quad \left. \begin{array}{l} g_1 \equiv \tilde{g}_1 \pmod{H} \\ g_2 \equiv \tilde{g}_2 \pmod{H} \end{array} \right\} \Rightarrow g_1 g_2 \equiv \tilde{g}_1 \tilde{g}_2 \pmod{H}$$

Критерий согласованности отношения сравнения по  $\text{mod } H$  с операцией в  $G$ .

$$\left. \begin{array}{l} g_1 g_2 \equiv \tilde{g}_1 \tilde{g}_2 \pmod{H}, \text{ если} \\ \tilde{g}_1 \in g_1 H, \text{ т.е. } \tilde{g}_1 = g_1 h_1 \\ \tilde{g}_2 \in g_2 H, \text{ т.е. } \tilde{g}_2 = g_2 h_2 \end{array} \right\} \Leftrightarrow (g_1 g_2)^{-1} \tilde{g}_1 \tilde{g}_2 \in H \Leftrightarrow$$

$$\Leftrightarrow g_2^{-1} g_1^{-1} g_1 h_1 g_2 h_2 \in H \Leftrightarrow g_2^{-1} h_1 g_2 h_2 \in H \Leftrightarrow g_2^{-1} h_1 g_2 \in H \Leftrightarrow$$

$$\Leftrightarrow g h g^{-1} \in H \quad \forall h \in H \quad \forall g \in G$$

**8.2 Нормальная подгруппа**

**Опр.** Подгруппа  $H < G$  называется нормальной подгруппой (нормальным делителем), если  $g h g^{-1} \in H \quad \forall h \in H, \quad \forall g \in G$

**Обозначение:**  $H \triangleleft G \quad (G \triangleright H)$

**Утв. 1.** Следующие условия эквивалентны:

- 1)  $ghg^{-1} \in H, \quad \forall h \in H \quad \forall g \in G$
- 2)  $gHg^{-1} = H \quad \forall g \in G$
- 3)  $gH = Hg \quad \forall g \in G$

**Док-во:**  $1) \Leftrightarrow gHg^{-1} \subset H \quad (1) \quad \forall g \in G \Rightarrow$   
 $\Rightarrow g^{-1}(gHg^{-1})g \subset g^{-1}Hg \quad \forall g \in G \Rightarrow H \subset g^{-1}Hg(2)$   
 $\Rightarrow (1), (2) \Rightarrow H = gHg^{-1}$   
 $1) \Leftrightarrow 2) \Leftrightarrow 3)$

### 8.3 Факторгруппа

**Утв. 2.** Пусть  $H \triangleleft G$ . Тогда множество  $G/H (= H \backslash G)$  с операцией  $(g_1H)(g_2H) = g_1g_2H$  является группой.

**Док-во:**

- 1) ассоциативность в  $G/H$  наследуется из ассоциативности в  $G$   
 $((g_1H)(g_2H))(g_3H) = (g_1g_2H)(g_3H) = (g_1g_2)g_3H = g_1(g_2g_3)H = (g_1H)(g_2g_3H) =$   
 $= (g_1H)(g_2H)(g_3H)$
  - 2)  $e_{G/H} = H$  - нейтральный элемент, так как  $H = eH \quad \begin{cases} gHeH = gH & \forall gH \in G/H \\ eHgH = gH \end{cases}$
  - 3)  $\forall gH \in G/H \quad \exists (gH)^{-1} = g^{-1}H \in G/H$   
 $(gH)g^{-1}H = gg^{-1}H = H$   
 $(g^{-1}H)(gH) = g^{-1}gH = H$
- 1), 2), 3) -  $G/H$  - группа.

**Опр.**  $G \triangleleft H$ ,  $G/H$  с операцией  $(g_1H)(g_2H) = g_1g_2H$  называется факторгруппой группы  $G$  по подгруппе  $H$ .

Пример:  $G = (\mathbb{Z}, +) = \langle 1 \rangle$  абелева  
 $H = m\mathbb{Z} = \langle m \rangle \quad H \triangleleft G \quad m\mathbb{Z} \triangleleft \mathbb{Z} \quad \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$

Утверждения 3-6 доказать самим.

**УТВ. 3.**  $G$  - абелева группа,  $H < G \Rightarrow H \triangleleft G$ .

**УТВ. 4.**  $G$  - группа,  $H < G$ ,  $|G : H| = 2 \Rightarrow H \triangleleft G$ .

**УТВ. 5.**  $G$  - абелева группа,  $H < G \Rightarrow G/H$  - абелева группа.

**УТВ. 6.**  $G$  - циклическая группа,  $H < G \Rightarrow G/H$  - циклическая группа.

#### 8.4 Гомоморфизм групп

**Опр.** Пусть  $(G, \cdot), (H, *)$  - группы.

Отображение  $f : G \rightarrow H$  называется гомоморфизмом групп, если  $f(g_1 \cdot g_2) = f(g_1) * f(g_2) \quad \forall g_1, g_2 \in G$

( $f(g_1 g_2) = f(g_1) f(g_2)$ , если обозначить операции в группах  $G$  и  $H$  одинаково).

Примеры:

1)  $f : G \rightarrow H \quad G = GL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n} : \det A \neq 0\}$ .

$f(A) = \det A, \quad H = \mathbb{R}^*$

$f : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$  - гомоморфизм, так как  $\det(AB) = \det(A)\det(B)$

2)  $f : S_n \rightarrow \mathbb{R}^* \quad f(\alpha) = \operatorname{sgn}(\alpha)$  гомоморфизм,

т.к.  $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$

**УТВ. 7.**  $f : G \rightarrow H$  гомоморфизм групп  $\Rightarrow f(e_G) = e_H$

**Док-во:**  $e_G e_G = e_G \Rightarrow f(e_G) f(e_G) = f(e_G) \in H$

$\exists (f(e_G))^{-1} \Rightarrow f(e_G) = e_H$

**Утв. 8.**  $f : G \longrightarrow H$  гомоморфизм групп  $\Rightarrow$   
 $\Rightarrow \forall g \in G \quad f(g^{-1}) = (f(g))^{-1}$

**Док-во:**  $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$   
 $f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_H$

### 8.5 Образ гомоморфизма

**Опр.**  $f : G \longrightarrow H$  гомоморфизм групп.  
 Образом гомоморфизма  $f$  называется множество  
 $Im f = \{h \in H : \exists g \in G : f(g) = h\}$ .

**Утв. 9.**  $Im f < H$

**Док-во:** 1)  $e_H \in Im f$ , так как  $f(e_G) = e_H$   
 2)  $h_1, h_2 \in Im f$ , т.е.  $\exists g_1, g_2 \in G : \left. \begin{array}{l} h_1 = f(g_1) \\ h_2 = f(g_2) \end{array} \right\} \Rightarrow$   
 $\Rightarrow f(g_1g_2) = f(g_1)f(g_2) = h_1h_2 \Rightarrow h_1h_2 \in Im f$   
 3)  $\forall h \in Im f$ , т.е.  $\exists g \in G : f(g) = h, \Rightarrow h^{-1} = f(g^{-1}) \in Im f$

Очевидно

**Утв. 10.**  $f : G \longrightarrow H$  гомоморфизм является сюръективным

$$\begin{array}{c} \Updownarrow \\ Im f = H \end{array}$$

**Опр.** Сюръективный гомоморфизм групп называется эпиморфизмом.



## 8.6 Ядро гомоморфизма

**Опр.**  $f : G \longrightarrow H$  гомоморфизм групп.

Ядром гомоморфизма  $f$  называется множество

$$\text{Ker } f = \{g \in G : f(g) = e_H\}.$$

**Утв. 11.**  $\text{Ker } f < G$

**Док-во:** 1)  $e_G \in \text{Ker } f$ , т.к.  $f(e_G) = e_H$

2)  $g_1, g_2 \in \text{Ker } f$ , т.е.  $f(g_1) = f(g_2) = e_H \Rightarrow f(g_1 g_2) = f(g_1) f(g_2) = e_H e_H = e_H \Rightarrow g_1 g_2 \in \text{Ker } f$

3)  $g \in \text{Ker } f$ , т.е.  $f(g) = e_H \Rightarrow f(g^{-1}) = (f(g))^{-1} = e_H^{-1} = e_H \Rightarrow g^{-1} \in \text{Ker } f$

**Утв. 12.**  $f : G \longrightarrow H$  гомоморфизм групп  $\Rightarrow \text{Ker } f \triangleleft G$

**Док-во:**  $\forall \tilde{g} \in \text{Ker } f$

$$f(g \tilde{g} g^{-1}) = f(g) f(\tilde{g}) f(g^{-1}) = f(g) e_H f(g^{-1}) = e_H \Rightarrow g \tilde{g} g^{-1} \in \text{Ker } f \quad \forall g \in G$$

Примеры:

(1)  $f : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*, \quad f(A) = \det A$

$$\text{Ker } f = SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R}), \quad \text{Im } f = \mathbb{R}^*$$

(2)  $f : S_n \rightarrow \mathbb{R}^*, \quad f(\alpha) = \text{sgn } \alpha \quad \text{Ker } f = A_n \triangleleft S_n, \quad \text{Im } f = \mathbb{C}_2$

**Утв. 13.**  $f : G \rightarrow H$  гомоморфизм групп.

$$f(g_1) = f(g_2) \Leftrightarrow g_1 \equiv g_2 \pmod{\text{Ker } f} \Leftrightarrow g_1^{-1} g_2 \in \text{Ker } f$$

**Док-во:**  $f(g_1) = f(g_2) \Leftrightarrow (f(g_1))^{-1} f(g_2) = e_H \Leftrightarrow f(g_1^{-1}) f(g_2) = e_H \Leftrightarrow f(g_1^{-1} g_2) = e_H \Leftrightarrow g_1^{-1} g_2 \in \text{Ker } f$

Очевидно

**Утв. 14.**  $f : G \rightarrow H$  гомоморфизм является инъективным

$$\begin{array}{c} \Updownarrow \\ \text{Ker } f = \{e_G\} \end{array}$$

**Опр.** Инъективный гомоморфизм групп называется мономорфизмом.

### 8.7 Изоморфизм групп

**Утв. 15.**  $f : G \rightarrow H$  гомоморфизм групп является изоморфизмом  $\Leftrightarrow \begin{cases} \text{Im } f = H \\ \text{Ker } f = \{e_G\} \end{cases}$

**Док-во:**  $f$  - гомоморфизм является изоморфным  $\Leftrightarrow f$  - биекция  $\Leftrightarrow \begin{cases} f \text{ - сюръективно} \\ f \text{ - инъективно} \end{cases} \Leftrightarrow \begin{cases} f \text{ - эпиморфизм} \\ f \text{ - мономорфизм} \end{cases} \Leftrightarrow \begin{cases} \text{Im } f = H \\ \text{Ker } f = \{e_G\} \end{cases}$

### 8.8 Порядок образа элемента группы при гомоморфизме

**Утв. 16.** Пусть  $f : G \rightarrow H$  гомоморфизм групп,  $g \in G : \text{ord } g = n < \infty$ , тогда  $\text{ord } f(g) \mid \text{ord } g = n$

**Док-во:**  $(f(g))^n = f(g^n) = f(e_G) = e_H \Rightarrow n : \text{ord } f(g) \Leftrightarrow \text{ord } f(g) \mid \text{ord } g$

**Утв. 17.** Если  $f : G \rightarrow H$  изоморфизм групп,  $g \in G : \text{ord } g = n < \infty$ , то  $\text{ord } f(g) = \text{ord } g$

**Док-во:** Следует из утв. 16 для  $f$  и  $f^{-1}$ .

**Утв. 18.** Если  $f : G \rightarrow H$  изоморфизм,  $g \in G : \text{ord } g = \infty$ , то  $\text{ord } f(g) = \infty$

**Док-во:** Если  $\text{ord } f(g) < \infty$ , то  $\text{ord } g = f^{-1}(f(g)) = \text{ord } f(g)$ .

$$\left. \begin{array}{l} \text{УТВ. 17.} \\ \text{УТВ. 18.} \end{array} \right\} \Rightarrow \text{Следствие: } \begin{array}{l} f : G \rightarrow H \text{ изоморфизм} \Rightarrow \\ \Rightarrow \text{ord } g = \text{ord } f(g) \quad \forall g \in G \end{array}$$

### 8.9 Теорема о гомоморфизме

$$f : G \rightarrow H \text{ гомоморфизм} \Rightarrow G/\text{Ker } f \simeq \text{Im } f$$

**Док-во:**  $\text{Ker } f \triangleleft G \quad \exists G/H$  - факторгруппа с операцией  
 $(g_1 \text{Ker } f)(g_2 \text{Ker } f) = g_1 g_2 \text{Ker } f$

Построим  $F : G/\text{Ker } f \rightarrow \text{Im } f$

Определим  $F(g \text{Ker } f) = f(g) \in \text{Im } f$

Определение корректно:  $g_1 \equiv g_2 \pmod{\text{Ker } f} \xrightarrow{\text{УТВ. 13}} F(g_1 \text{Ker } f) = F(g_2 \text{Ker } f)$

$$\begin{array}{ccc} \parallel & & \parallel \\ f(g_1) & & f(g_2) \end{array}$$

1)  $F$  - гомоморфизм

$$F(g_1 \text{Ker } f \cdot g_2 \text{Ker } f) = F(g_1 g_2 \text{Ker } f) = f(g_1 g_2) = f(g_1) f(g_2) = F(g_1 \text{Ker } f) F(g_2 \text{Ker } f)$$

2)  $F$  - эпиморфизм

$$\forall h \in \text{Im } f \quad \exists g \in G : f(g) = h \Rightarrow \exists g \text{Ker } f \in G/\text{Ker } f : F(g \text{Ker } f) = f(g) = h$$

3)  $F$  - мономорфизм

$$\text{Ker } F = \{g \text{Ker } f : F(g \text{Ker } f) = f(g) = e_H\}$$

$$\text{Ker } F = \{\text{Ker } f\} = \{e_{G/\text{Ker } f}\}$$

$F$  - изоморфизм групп  $G/\text{Ker } f$  и  $\text{Im } f$ , т.е.  $G/\text{Ker } f \simeq \text{Im } f$

**Примеры:**

(1)  $f : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$

$$f(A) = \det A \quad \forall A \in GL_n(\mathbb{R}).$$

$f$  - гомоморфизм, т.к.  $\det(A_1 A_2) = \det A_1 \det A_2$ ,

$$\text{Ker } f = SL_n(\mathbb{R})$$

$\text{Im } f = \mathbb{R}^*$ , так как  $\forall \lambda \in \mathbb{R}^* \exists A \in GL_n(\mathbb{R}) : \det A = \lambda$ ,

$$\text{например, } A = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$$

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$$

$$(2) f : S_n \rightarrow \mathbb{R}^*, \quad f(\alpha) = \text{sgn } \alpha,$$

$f$  - гомоморфизм,  $\text{Ker } f = A_n$ ,

$$\text{Im } f = \{-1, 1\} \simeq \mathbb{C}_2 \simeq \mathbb{Z}_2$$

$$S_n/A_n \simeq \mathbb{Z}_2 \simeq \mathbb{C}_2$$

**NOTE:**  $\forall N \triangleleft G \quad \exists \varphi : G \rightarrow G/N$  - естественный (канонический) гомоморфизм :  $\text{Ker } \varphi = N$ , а именно  $\varphi(g) = gN$   
 $\varphi$  - гомоморфизм, т.к.  $\varphi(g_1 g_2) = (g_1 g_2)N = g_1 N g_2 N = \varphi(g_1) \varphi(g_2)$   
 $\text{Ker } \varphi = \{g \in G : gN = N\} = N$

**NOTE:** Если  $f : G \rightarrow H$  - эпиморфизм, то  
 $\exists$  естественный  $\varphi : G \rightarrow G/\text{Ker } f \simeq H \Rightarrow \exists!$  эпиморфизм  $G$  в  $H$

## 9 Лекция №9

### 9.1 Автоморфизм групп

**Опр.**  $f : G \rightarrow G$  - гомоморфизм группы в себя называется эндоморфизмом.

Пример:  $\forall g \in G \quad f(g) = e \Rightarrow f$  - эндоморфизм (тривиальный)

**Опр.**  $f : G \rightarrow G$  - изоморфизм группы на себя называется автоморфизмом.

Множество всех автоморфизмов  $G \rightarrow G$  обозначается  $Aut G$

Примеры:

(1)  $G = GL_n(\mathbb{R})$   $f_1 : G \rightarrow G$   $f_1(A) = A^{-1}$  - биекция  
 $f_1(AB) = (AB)^{-1} = B^{-1}A^{-1}$ ,  $f_1(A)f_1(B) = A^{-1}B^{-1}$   
 $f_1$  не является гомоморфизмом, т.к.  $G$  некоммутативная группа  
 $f_1 \notin Aut GL_n(\mathbb{R})$ .

(2)  $G = GL_n(\mathbb{R})$ ,  $f_2 : G \rightarrow G$ ,  $f_2(A) = A^T$  - биекция  
 $f_2(AB) = (AB)^T = B^T A^T$ ,  $f_2(A)f_2(B) = A^T B^T$   
 $f_2 \notin Aut GL_n(\mathbb{R})$ , т.к.  $G$  некоммутативная группа.

(3)  $G = GL_n(\mathbb{R})$   $f_3 = f_2 \circ f_1 : G \rightarrow G$  биекция  $f_3(A) = (A^{-1})^T$   
 $f_3(AB) = ((AB)^{-1})^T = (B^{-1}A^{-1})^T = (A^{-1})^T(B^{-1})^T = f_3(A)f_3(B)$   
 $f_3 \in Aut GL_n(\mathbb{R})$

**Утв. 1.**  $G$  - группа  $\Rightarrow Aut G$  - группа

**Док-во:**  $Aut G \subset S(G)$ , где  $S(G)$  - группа всех биективных отображений  $G$  в  $G$ .

Докажем:  $Aut G < S(G)$

1)  $id \in Aut G$

2)  $f_1, f_2 \in Aut G$

$$\left. \begin{aligned} f_1(g_1g_2) &= f_1(g_1)f_1(g_2) \\ f_2(g_1g_2) &= f_2(g_1)f_2(g_2) \end{aligned} \right\} \Rightarrow (f_1f_2)(g_1g_2) = f_1(f_2(g_1g_2)) =$$
  

$$= f_1(f_2(g_1)f_2(g_2)) = f_1(f_2(g_1))f_1(f_2(g_2)) = (f_1f_2)(g_1)(f_1f_2)(g_2) \Rightarrow$$
  

$$\Rightarrow f_1f_2 - \text{гомоморфизм}$$

$$\left. \begin{aligned} f_1 \\ f_2 \end{aligned} \right\} - \text{биекция} \Rightarrow f_1f_2 - \text{биекция} \Rightarrow f_1f_2 \in Aut G$$

3)  $f \in Aut G$   $f$  - биекция  $\Rightarrow \exists f^{-1} : G \rightarrow G$  - биекция

$f$  - гомоморфизм, т.е.  $f(g_1g_2) = f(g_1)f(g_2) \Rightarrow$

$\Rightarrow f^{-1}(g_1g_2) = f^{-1}(f(f^{-1}(g_1)f^{-1}(g_2))) =$   
 $= (f^{-1}f)(f^{-1}(g_1)f^{-1}(g_2)) = f^{-1}(g_1)f^{-1}(g_2) \Rightarrow$

$\Rightarrow f^{-1}$  - гомоморфизм.  $\Rightarrow f^{-1} \in \text{Aut } G$

$$\left. \begin{array}{l} 1) \\ 2) \\ 3) \end{array} \right\} \text{Aut } G < S(G) \Rightarrow \text{Aut } G \text{ - группа}$$

## 9.2 Действия группы на множестве

$G$  - группа,  $X$  - мн-во,

$S(X)$  - группа всех биективных преобразований  $X$

$\varphi : G \rightarrow S(X)$  - гомоморфизм групп.

$\varphi(g) \in S(X) \quad \varphi(g)(x) = \varphi(g)x = gx \quad \forall x \in X$

$\text{Im } \varphi < S(X)$  - группа преобразований  $X$

$G/\text{Ker } \varphi \simeq \text{Im } \varphi < S(X)$

**Опр.** Если задан  $\varphi : G \rightarrow S(X)$  гомоморфизм, говорят

$G$  действует на  $X \quad G : X$

Элементы мн-ва  $X$  называются точками.

**Опр.**  $\text{Ker } \varphi$  - ядро неэффективности, если  $\text{Ker } \varphi = \{e\}$  тривиально, то говорят, что действие группы на  $X$  эффективно.

## 9.3 Действия группы на самой себе $G:G$

### (1) Действие левыми сдвигами

$G$  - группа  $S(G)$  группа биективных отображений  $G$  в  $G$

$l : G \rightarrow S(G) : l(g)(x) = gx \quad \forall g \in G, \quad \forall x \in G$

**Утв. 2.**  $l : G \rightarrow S(G)$  - гомоморфизм

**Док-во:**

0)  $l(g)$  - биекция.

а)  $l(g)$  - сюръекция, т.к.  $\forall y \in G \exists x \in G : y = l(g)(x) = l(g)x = gx$ , а именно  $x = g^{-1}g \in G$ .

б)  $l(g)$  - инъекция, т.к.  $l(g)x_1 = l(g)x_2 \Leftrightarrow gx_1 = gx_2 \Leftrightarrow$   
 $\Leftrightarrow x_1 = x_2 \quad \forall x_1, x_2 \in G \Rightarrow$   
 а), б)  $\Rightarrow l : G \rightarrow S(G)$

1)  $l(g_1g_2)x = (g_1g_2)x = g_1(g_2x) = l(g_1)(l(g_2)(x)) = l(g_1) \circ l(g_2)(x)$   
 $l : G \rightarrow S(G)$  - гомоморфизм

**NOTE:**  $l(g)$  не является автоморфизмом,  $l(g) \notin \text{Aut}(G)$ , если  $g \neq e$   
 $l(g)$  - биекция, но  $l(g)$  не гомоморфизм, т.к.

$$l(g)(x_1x_2) = g(x_1x_2) \quad gx_1x_2 = gx_1gx_2 \Leftrightarrow e = g$$

$$l(g)(x_1)l(g)(x_2) = gx_1gx_2$$

**УТВ. 3.**  $l : G \rightarrow S(G)$  мономорфизм

**Док-во:**  $\text{Ker } l = \{g \in G : l(g) = id\} =$   
 $= \{g \in G : l(g)x = x \quad \forall x \in G\} = \{g \in G : gx = x \quad \forall x \in G\} = \{e\}$

**Следствие:**  $G \simeq \text{Im } l$

**Док-во:** по теореме о гомоморфизме  
 $l : G \rightarrow S(G)$  гомоморфизм является мономорфизмом,  $\text{Ker } l = \{e\}$   
 $G/\text{Ker } l \simeq \text{Im } l \Rightarrow G \simeq \text{Im } l$

## 9.4 Теорема Кэли

$\forall$  конечная группа порядка  $n$  изоморфна некоторой подгруппе в группе  $S_n$ .

**Док-во:**  $G$  - группа,  $|G| = n < \infty$   $l : G \rightarrow S(G) = S_n$   
 $G \simeq \text{Im } l < S_n$

### (2) Действие группы на себя правыми сдвигами

$r(g) : G \rightarrow G : r(g)(x) = xg \quad \forall g \in G, \quad \forall x \in G \dots$  аналогично (1)

**(3) Действие группы на себя сопряжениями**

$$a(g) : G \rightarrow G \quad x \in G \quad a(g)x = gxg^{-1} \in G$$

**УТВ. 4.**  $a : G \rightarrow S(G)$  гомоморфизм

**Док-во:**

1)  $a(g)$  - биекция

а)  $a(g)$  - сюръекция, т.к.  $\forall y \in G \quad \exists x \in G : y = a(g)x = gxg^{-1}$ ,

а именно  $x = g^{-1}yg \in G$

б)  $a(g)$  - инъекция, т.к.  $a(g)x_1 = a(g)x_2 \Leftrightarrow gx_1g^{-1} = gx_2g^{-1} \Leftrightarrow x_1 = x_2$

а), б)  $\Rightarrow a : G \rightarrow S(G)$

2)  $a : G \rightarrow S(G)$  - гомоморфизм

$$a(g_1g_2)(x) = (g_1g_2)x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} = g^{-1}(a(g_2)(x))g^{-1} =$$

$$= a(g_1)(a(g_2)(x)) = (a(g_1)a(g_2))x \quad \forall x \in G \Rightarrow$$

$$\Rightarrow a(g_1g_2) = a(g_1)a(g_2)$$

**УТВ. 5.**  $a(g) \in \text{Aut } G \quad \forall g \in G$

**Док-во:**

1)  $a(g)$  - биекция  $\forall g \in G$  (см. УТВ. 4)

$$2) a(g)(x_1x_2) = g(x_1x_2)g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = a(g)(x_1) \cdot a(g)(x_2)$$

$\Rightarrow a(g)$  - эндоморфизм

$$\left. \begin{array}{l} 1) \\ 2) \end{array} \right\} \Rightarrow \begin{array}{l} a(g) - \text{изоморфизм } G \text{ в себя,} \\ \text{т.е. автоморфизм } a(g) \in \text{Aut } G \end{array}$$

**Опр.**  $a(g)$  называется внутренним автоморфизмом  $\forall g \in G$ .

Мн-во всех внутренних автоморфизмов обозначается  $\text{Int } G$ .

**NOTE:**  $\text{Int } G = \text{Im } a < S(G) \Rightarrow \text{Int } G$  - группа

$$\text{Int } G \subset \text{Aut } G \Rightarrow \text{Int } G < \text{Aut } G < S(G)$$

**Опр.** Центром группы  $G$  называется

$$Z(G) = \{h \in G : gh = hg \quad \forall g \in G\}.$$



**УТВ.6**  $\text{Ker } a = Z(G)$

**Док-во:**  $\text{Ker } a = \{g \in G : a(g) = id\} =$   
 $= \{g \in G : gxg^{-1} = x \quad \forall x \in G\} =$   
 $= \{g \in G : gx = gx \quad \forall x \in G\} = Z(G)$

**УТВ. 7.**  $G/Z(G) \simeq \text{Int } G$

**Док-во:**  $a : G \rightarrow S(G)$  - гомоморфизм  $\Rightarrow$   
 $\Rightarrow G/\text{Ker } a \simeq \text{Im } a$ , т.е.  $G/Z(G) \simeq \text{Int } G$

**УТВ. 8.**  $\forall n \geq 3 \quad Z(S_n) = \{id\}$

**Док-во:**  $\forall \alpha \in S_n \quad \alpha \neq id \quad \exists \beta \in S_n : \alpha\beta \neq \beta\alpha$

Пусть  $\alpha(i) = j \quad i \neq j$

Рассмотрим  $\beta = (j, k), \quad k \neq i, j$  (это возможно при  $n \geq 3$ )

$$\left. \begin{aligned} (\alpha\beta)(i) &= \alpha(\beta(i)) = \alpha(i) = j \\ (\beta\alpha)(i) &= \beta(\alpha(i)) = \beta(j) = k \end{aligned} \right\} \Rightarrow (\alpha\beta)(i) \neq (\beta\alpha)(i) \Rightarrow \alpha\beta \neq \beta\alpha \Rightarrow$$
  
 $Z(S_n) = \{id\}$  при  $n \geq 3$

## 10 Лекция №10

**Следствие:**  $\text{Int } S_n = S_n$  при  $n \geq 3$

**Док-во:**

$\text{Int } G = \{a_g \in \text{Aut } G : a_g(x) = gxg^{-1} \quad \forall x \in G\}$

$\text{Int } G \simeq G/Z(G), \quad G = S_n \quad Z(S_n) = \{id\} \quad n \geq 3$

$\text{Int } S_n \simeq S_n/\{id\} = S_n$

**УТВ. 1.**  $\text{Aut } S_3 = S_3$

**Док-во:**  $T = \{(12), (13), (23)\}$  - мн-во всех элементов второго порядка

группы  $S_3$

$f \in \text{Aut } S_3 \Rightarrow f$  - сохраняет порядок элемента  $\Rightarrow f : T \rightarrow T$

Можно определить  $\Phi : \text{Aut } S_3 \rightarrow S(T) \simeq S_3$

Автоморфизм  $f$  однозначно задаётся своим действием на  $T$ ,

поскольку  $S_3 = \langle (12), (13), (23) \rangle \Rightarrow \Phi$  - мономорфизм

$$|\text{Aut } S_3| \leq |S(T)| = |S_3| \quad (1)$$

$$S_3 \simeq \text{Int } S_3 < \text{Aut } S_3 \quad |S_3| \leq |\text{Aut } S_3| \quad (2)$$

$$\left. \begin{array}{l} (1) \\ (2) \end{array} \right\} \Rightarrow |\text{Aut } S_3| = |S_3| \Rightarrow \text{Aut } S_3 = \text{Int } S_3 \simeq S_3$$

**УТВ. 2.**  $\text{Aut } \mathbb{Z} \simeq \mathbb{Z}_n^*$

**Док-во:**  $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  - эндоморфизм :  $f(\bar{1}) = \bar{k} \in \mathbb{Z}$

$$f(\bar{x}) = f(\underbrace{\bar{1} + \dots + \bar{1}}_x) = \underbrace{f(\bar{1}) + \dots + f(\bar{1})}_x = xf(\bar{1}) = f(\bar{1})\bar{x} = \bar{k}\bar{x}$$

$f$  - биекция  $\Leftrightarrow \exists f^{-1} : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  эндоморфизм

$$f(\bar{1}) = \bar{k} \quad \exists f^{-1}(\bar{1}) = \bar{l} \quad (f^{-1}f)(\bar{1}) = f^{-1}(f(\bar{1})) = f^{-1}(\bar{k}) = \bar{l} \cdot \bar{k}$$

$$(f^{-1}f)(\bar{1}) = \text{id}(1) = \bar{1} \quad \bar{l} \cdot \bar{k} = 1 \Leftrightarrow \bar{k} \in \mathbb{Z}^*$$

$f$  - автоморфизм  $f(1) = k \Leftrightarrow \bar{k} \in \mathbb{Z}^*$

Рассмотрим:  $\Phi : \text{Aut } \mathbb{Z}_n \rightarrow \mathbb{Z}_n^*$

$$\forall f \in \text{Aut } \mathbb{Z}_n \quad \Phi(f) = f(\bar{1}) \in \mathbb{Z}_n^*$$

**1)**  $\Phi$  - гомоморфизм

$$\begin{aligned} \Phi(f_1 \circ f_2) &= (f_1 \circ f_2)(1) = f_1(f_2(1)) = f_1(f_2(\bar{1})) = \\ &= f_1(\bar{1})f_2(\bar{1}) = \Phi(f_1) \cdot \Phi(f_2) \Rightarrow \Phi(f_1 \circ f_2) = \Phi(f_1) \circ \Phi(f_2) \end{aligned}$$

$$\begin{aligned} \mathbf{2)} \quad \text{Ker } \Phi &= \{f \in \text{Aut } \mathbb{Z}_n : \Phi(f) = \bar{1}\} = \{f \in \text{Aut } \mathbb{Z}_n : f(\bar{1}) = \bar{1}\} = \\ &= \{f \in \text{Aut } \mathbb{Z}_n : f(\bar{x}) = f(\bar{1})\bar{x} = \bar{x} \quad \forall x \in \mathbb{Z}_n\} = \\ &= \{f \in \text{Aut } \mathbb{Z}_n : f(x) = x \quad \forall x \in \mathbb{Z}_n\} = \{\text{id}\} \end{aligned}$$

**3)**  $\text{Im } \Phi = \mathbb{Z}_n^*$

а)  $\text{Im } \Phi \subset \mathbb{Z}_n^*$

б)  $\forall \bar{k} \in \mathbb{Z}_n^* \quad \exists f \in \text{Aut } \mathbb{Z}_n$ , а именно

$$\left. \begin{array}{l} f(\bar{1}) = \bar{k}, \text{ т.е. } \Phi(f) = \bar{k} \quad \mathbb{Z}_n^* \subset Im \Phi \quad \left. \begin{array}{l} \text{а)} \\ \text{б)} \end{array} \right\} \Rightarrow Im \Phi = \mathbb{Z}_n^* \Leftrightarrow \Phi \text{ -эпиморфизм} \\ \left. \begin{array}{l} 1) \\ 2) \\ 3) \end{array} \right\} \Rightarrow \Phi \text{ - эпиморфизм} \quad Aut \mathbb{Z} \simeq \mathbb{Z}_n^*$$

**NOTE:**  $Int \mathbb{Z}_n = \{id\}$ , т.к.  $\mathbb{Z}_n$  - абелева

**УТВ. 3.**  $G$  - группа  $\Rightarrow Int\,G \triangleleft Aut\,G$

$$\begin{aligned} \text{Док-во: } & \forall a_g \in \text{Int } G \quad \forall f \in \text{Aut } G \quad \forall x \in G \\ & (f a_g f^{-1})(x) = f(a_g(f^{-1}(x))) = f(g f^{-1}(x) g^{-1}) = \\ & f(g) f(f^{-1}(x)) f(g^{-1}) = f(g) x f(g)^{-1} = a_{f(g)}(x) \\ & \forall a_g \in \text{Int } G \quad \forall f \in \text{Aut } G \\ & f a_g f^{-1} = a_{f(g)} \in \text{Int } G \Rightarrow \text{Int } G \triangleleft \text{Aut } G \end{aligned}$$

**NOTE:**  $\exists Aut^G/Int(G)$  - (группа внешних автоморфизмов).

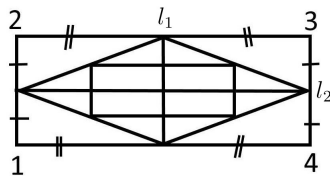
**NOTE:**  $G$  - группа,  $H < G$

$$H \triangleleft G \Leftrightarrow a_q(H) = H \quad \forall a_q \in \text{Int}G$$

т.е.  $H$  инвариантна относительно всех внутренних автоморфизмов группы  $G$

$$a_q(H) = gHg^{-1} = H$$

### 10.1 Четвёртая группа Клейна $V_4$



Группа симметрий прямоугольника  $Sym_R \square = \{id, u_\pi, s_1, s_2\} =$   
 $=$  группе симметрий ромба  $Sim \diamond$

$$V_4 < S_4 \text{ - четвёртая группа Клейна} \qquad u_\pi \longmapsto (1\,3)(2\,4)$$

$$s_1 \mapsto (1\ 4)(2\ 3)$$

$$s_2 \mapsto (1\ 2)(3\ 4)$$

$$\text{Sym } \square \simeq V_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

**УТВ. 4.**  $V_4 \triangleleft S_4$  и  $S_4/V_4 \simeq S_3$

**Док-во:** Рассмотрим многочлены от  $x_1, x_2, x_3, x_4$

$$P_1 = x_1x_2 + x_3x_4 \quad P_2 = x_1x_3 + x_2x_4 \quad P_3 = x_1x_4 + x_2x_3$$

$S_4$  действует на мн-ве  $P = \{P_1, P_2, P_3\}$

$\alpha \in S_4$   $\alpha P_1 = x_{\alpha(1)}x_{\alpha(2)} + x_{\alpha(3)}x_{\alpha(4)}$  аналогично определяются  $\alpha P_2, \alpha P_3$ .

$S_4 = \langle (12), (13), (14) \rangle$

$$(1\ 2) \mapsto \vartheta_{p_1}, \quad p_2 \leftrightarrow p_3$$

$$(1\ 3) \mapsto \vartheta_{p_2}, \quad p_1 \leftrightarrow p_3$$

$$(1\ 4) \mapsto \vartheta_{p_3}, \quad p_1 \leftrightarrow p_2$$

$$\Phi: S_4 \rightarrow S(P) = S_3$$

1)  $\Phi$  - гомоморфизм

2)  $\text{Im } \Phi = S_3$  а)  $\text{Im } \Phi \subset S_3$  б)  $\forall$  транспозицию  $(p_1, p_2), (p_2, p_3), (p_1, p_3)$

можно получить с помощью  $\Phi$

$$\Phi(1\ 4) = (p_1, p_2), \quad \Phi(1\ 3) = (p_1, p_3), \quad \Phi(1\ 2) = (p_2, p_3)$$

Вся группа  $S(P) = S_3$  порождается этими транспозициями

По теореме о гомоморфизме  $S_4/\text{Ker } \Phi \simeq \text{Im } \Phi = S_3$

$$\text{Ker } \Phi = \{\alpha \in S_4 : \alpha(p_i) = p_i \quad i = 1, 2, 3\}$$

Очевидно,  $V_4 = \{id, (12)(34), (13)(24), (14)(23)\} \subset \text{Ker } \Phi$

Из т.о гомоморфизме  $|S_n| = |\text{Im } \Phi| |\text{Ker } \Phi| = |S_3| |\text{Ker } \Phi|$

$$|\text{Ker } \Phi| = \frac{|S_4|}{|S_3|} = 4 \quad |V_4| = 4 \Rightarrow V_4 = \text{Ker } \Phi \Rightarrow V_4 \triangleleft S_4, \quad S_4/V_4 \simeq S_3$$

**NOTE:**  $V_4 < A_4 \triangleleft S_4 \Rightarrow V_4 \triangleleft A_4$ , т.к  $H \triangleleft G$

$$H < K < G \Rightarrow H \triangleleft K$$

$$gHg^{-1} \in H \quad \forall h \in H \quad \forall g \in G \quad \forall h \in H \quad \forall k \in K < G$$

$$V_4 \triangleleft A_4 \quad |A_4/V_4| = \frac{12}{4} = 3 \quad A_4/V_4 \simeq \mathbb{C}_3 \simeq \mathbb{Z}_3$$

## 10.2 Коммутант

**Опр.**  $G$  - группа,  $\forall a, b \in G$ , коммутатор  $a, b$   $[a, b] = aba^{-1}b^{-1}$

**Утв. 5.**  $[a, b] = e \Leftrightarrow ab = ba$

**Док-во:**  $aba^{-1}b^{-1} = e \Leftrightarrow ab = ba$

**Утв. 6.**  $[a, b]^{-1} = [b, a]$

**Док-во:**  $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = (a^{-1}b^{-1})^{-1}(ab)^{-1} = bab^{-1}a^{-1} = [b, a]$

**Опр.** Подгруппа группы  $G$ , порождённая всеми коммутаторами её элементов, называется коммутантом группы  $G$  и обозначается  $G'([G, G])$

**NOTE:** В выражении  $g \in G'$  через коммутаторы можно использовать только положительные степени.

**Утв. 7.**  $G, H$  - группы  $f : G \rightarrow H$  гомоморфизм  
 $\forall a, b \in G \quad f([a, b]) = [f(a), f(b)]$

**Док-во:**  $f([a, b]) = f(aba^{-1}b^{-1}) = f(a)f(b)f(a^{-1})f(b^{-1}) = f(a)f(b)(f(a))^{-1}(f(b))^{-1} = [f(a), f(b)]$

**Следствие 1.**  $f : G \rightarrow H$  - гомоморфизм  $\Rightarrow f(G') < H'$

**Следствие 2.**  $f : G \rightarrow H$  - эпиморфизм  $\Rightarrow f(G') = H'$

**Следствие 3.**  $G' \triangleleft G$

**Док-во:**  $\forall a_g \in \text{Int } G, \quad a_g : G \rightarrow G, \quad a_g(G') = G' \Rightarrow G' \triangleleft G$

## 11 Лекция №11

$$\text{Утв. 1. } \left. \begin{array}{l} H < G \\ G' < H \end{array} \right\} \Rightarrow H \triangleleft G$$

**Док-во:**  $\forall g \in G \quad \forall h \in H \quad ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]h \in H \Rightarrow H \triangleleft G$   
 $[g, h] \in G' < H$

**Следствие:**  $G' \triangleleft G$  (2-ое док-во нормальности  $G'$ )

**Теорема:**  $G' \triangleleft G$  - наименьшая по включению нормальная подгруппа  $G$ , факторгруппа, по которой абелева, т.е:

$$\left. \begin{array}{l} 1) G/G' - \text{абелева группа} \\ 2) H \triangleleft G, \quad G/H - \text{абелева группа} \end{array} \right\} \Rightarrow G' < H$$

**Док-во:**  $G' \triangleleft G$

1) Пусть  $\Psi : G \rightarrow G/G'$  - естественный (канонический) гомоморфизм

$\forall g \in G \quad \Psi(g) = gG'$  эпиморфизм  $\Rightarrow \Psi(G') = (G/G')'$

по определению  $\Psi(G') = e_{G/G'}$

$(G/G')' = \{e_{G/G'}\} \Leftrightarrow G/G' - \text{абелева группа}$

2) Пусть  $H \triangleleft G$

$\Psi : G \rightarrow G/H$  - естественный (канонический) гомоморфизм

$\Psi(g) = gH$  эпиморфизм  $\Rightarrow \Psi(G') = (G/H)'$

$G/H - \text{абелева группа} \Leftrightarrow (G/H)' = \{e_{G/H}\} = \{H\}$

$\Psi(G') = \{H\} \Rightarrow G' < H$

**Утв. 2.**

$A_n$  при  $n \geq 3$  порождается тройными циклами  $((ijk))$

$A_n$  при  $n \geq 5$  порождается парой независимых транспозиций  $((ij)(kl))$

**Док-во:**  $A_n < S_n$

$\forall$  подстановка  $\alpha \in S_n$  может быть разложена в произведение транспозиций.  $\alpha \in A_n$  раскладывается в чётное число транспозиций  $\Rightarrow \alpha \in A_n$

раскладывается в произведение пар транспозиций.

1) пара зависимых транспозиций  $(ij)(jk) = (kij) = (ijk)$

2) пара независимых транспозиций  $(ij)(kl) = ((ij)(jk)) = ((jk)(kl)) = (ijk)(jkl)$

$i, j, k, l$  различны

1)  $\left. \begin{array}{l} 1) \\ 2) \end{array} \right\} \Rightarrow A_n$  при  $n \geq 3$  порождается тройными циклами

$k \geq 5$  3) пара зависимых транспозиций  $(ij)(jk) = (ij)(lm)(jk)(lm) = ((ij)(lm))((jk)(lm))$

$i, j, k, l, m$  - различны

3)  $\Rightarrow$  при  $n \geq 5$   $A_n$  порождается парами независимых транспозиций

**УТВ. 3.**  $Z(A_n) = \{id\}$  при  $n \geq 4$

**Док-во:**

Пусть  $\left. \begin{array}{l} \alpha \in Z(A_n) \\ \alpha \neq id \end{array} \right\} \alpha(i) = j \quad i \neq j \quad \exists \beta \in A_n : \quad \alpha\beta = \beta\alpha$

$n \geq 4$  рассмотрим  $\beta = (j, k, l)$   $j, k, l$  различные и не равны  $i$

$(\alpha\beta)(i) = \alpha(\beta(i)) = \alpha(j) = k$   
 $(\beta\alpha)(i) = \beta(\alpha(i)) = \beta(j) = k$   $j \neq k \Rightarrow \alpha\beta = \beta\alpha \Rightarrow \nexists \alpha \in Z(A_n)$   
 $\Rightarrow Z(A_n) = \{id\} \quad n \geq 4$

**NOTE.**  $A_3 = \{(123)(132)id\} \simeq \mathbb{Z}_3$  абелева  $\Rightarrow$   
 $\Rightarrow Z(A_3) = A_3 \quad A'_3 = \{id\}$

**УТВ. 4.**  $H \triangleleft G, |H| = 2 \Rightarrow H < Z(G)$

**Док-во:**  $H = \{e, h\} \quad h \neq e$

$H \triangleleft G \Leftrightarrow \forall g \in G \quad ghg^{-1} \in H \Rightarrow ghg^{-1} = \begin{cases} e \Rightarrow h = e \\ h \Rightarrow gh = hg \Rightarrow h \in Z(G) \end{cases} \Rightarrow$

$\Rightarrow H < Z(G)$

**УТВ. 5.**  $n \geq 3 \quad S'_n = A_n$

**Док-во:**

1)  $A_n \triangleleft S_n \quad |S_n/A_n| = 2 \Rightarrow S_n/A_n \simeq \mathbb{Z}_2$  - абелева группа.

$\Rightarrow S'_n < A_n$

2)  $S_3 \triangleright A_3 > S'_3, \quad |A_3| = 3 \Rightarrow |S'_3| = \begin{bmatrix} 1 \\ 3 \end{bmatrix} \Leftrightarrow S'_3 = \begin{bmatrix} \{id\} \\ A_3 \end{bmatrix} \Leftrightarrow S_3$  - абелева  $\times$

$S'_3 = A_3 = \{(123), (132), id\}$  включает все тройные циклы из 3-х элементов

3)  $S'_n$  содержит все тройные циклы,

$A_n$  порождается тройными циклами при  $n \geq 3 \Rightarrow A_n < S'_n$

1), 3)  $\Rightarrow S'_n = A_n \quad n \geq 3$ .

**NOTE.**

$A'_3 = \{id\}$ , т.к.  $A_3$  - абелева

**УТВ. 6.**

$A'_4 = V_4$

$A'_n = A_n \quad n \geq 5$

**Док-во:**

1)  $A_4 \triangleright V_4, \quad |A_4/V_4| = 12/4 = 3 \Rightarrow$

$\Rightarrow A_4/V_4 \simeq \mathbb{Z}_3$  - абелева  $\Rightarrow A'_4 < V_4$

$|V_4| = 4 \Rightarrow |A'_4| \mid 4 \Rightarrow |A'_4| = \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} \Rightarrow$

$A'_4 = \begin{bmatrix} \{id\} \Rightarrow A_4 \text{ - абелева, } \times \\ A'_4 \triangleleft V_4, \quad |A'_4| = Z \Rightarrow A'_4 \in Z(A_4) = \{id\} \\ V_4 \end{bmatrix} \quad \times$

$A'_4 = V_4 = \{(12)(34), (13)(24), (14)(23)\}$  содержит всевозможные произведения пар независимых транспозиций из 4-х элементов

2)  $A'_n$  содержит всевозможные произведения пар независимых транспо-



зиций 4-х элементов

$A_n$  при  $n \geq 5$  порождается произведениями пар независимых транспозиций  $\Rightarrow$

$$\left. \begin{array}{l} \Rightarrow A_n < A'_n \quad n \geq 5 \\ \text{очевидно, } A'_n < A_n \end{array} \right\} \Rightarrow A'_n = A_n \quad \text{при } n \geq 5$$

**Опр.**  $G^{(1)} = G'$ ,  $G^{(2)} = (G')' \dots G^{(k)} = (G^{(k-1)})'$  - кратные коммутанты  
 $G > G^{(1)} > G^{(2)} > \dots > G^{(k)} > \dots$

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

**Примеры.**

(1)  $S_3$

$$S_3^{(1)} = S'_3 = A_3$$

$$S_3^{(2)} = (S'_3)' = A'_3 = \{id\}$$

$S_3$  - разрешима.

(2)  $S_4$

$$S'_4 = A_4$$

$$S_4^{(2)} = A'_4 = V_4$$

$$S_4^{(3)} = A_4^{(2)} = V'_4 = \{id\}, \text{ т.к. } V_4 - \text{абелева.}$$

$S_4$  - разрешима.

(3)  $S_n, \quad n \geq 5$

$$S_n^{(1)} = S'_n = A_n$$

$$S_n^{(2)} = A'_n = A_n$$

$$S_n^{(3)} = A'_n = A_n$$

$n \geq 3 \quad S_n$  неразрешима.

**Утв. 7.**  $G$  - разрешима  $\Rightarrow$  любая её подгруппа разрешима.

**Доказать самим.**

**Утв. 8.**  $G$  - разрешима,  $H \triangleleft G \Rightarrow G/H$  разрешима.  
Доказать самим.

## 12 Лекция №12

### 12.1 Прямые произведения(прямые суммы) групп

### 12.2 Внешнее прямое произведения групп

$G_1, G_2, \dots, G_k$  - группы

$$G_1 \times G_2 \times \dots \times G_k = \{(g_1, g_2, \dots, g_k), g_i \in G, i = \overline{1, k}\}$$

$$(g_1, g_2, \dots, g_k)(\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_k) = (g_1\tilde{g}_1, g_2\tilde{g}_2, \dots, g_k\tilde{g}_k) \in G_1 \times G_2 \times \dots \times G_k$$

Очевидны утв. 1,2,3

**Утв. 1.**  $G_1 \times G_2 \times \dots \times G_k$  - группа

**Утв. 2.**  $G_1 \times G_2 \times \dots \times G_k$  - коммутативная группа  $\Leftrightarrow$   
 $\Leftrightarrow G_i$  - коммутативная группа  $\forall i = \overline{1, k}$

**Утв. 3.**  $|G_1 \times G_2 \times \dots \times G_k| = |G_1| \cdot |G_2| \cdot \dots \cdot |G_k|$

В случае абелевой группы можно говорить о прямой сумме

$$G_1 \oplus G_2 \oplus \dots \oplus G_k$$

$$\mathbb{C}_3 \times \mathbb{C}_2 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_3$$

$$\mathbb{Q}_8 \times \mathbb{Z}_2$$

**Утв. 4.**  $g = (g_1, g_2, \dots, g_k) \in G_1 \times G_2 \times \dots \times G_k \Rightarrow$   
 $\Rightarrow \text{ord } g = \text{НОК}\{\text{ord } g_1, \text{ord } g_2, \dots, \text{ord } g_k\}$

**Док-во:**  $g^n = e \in G \Leftrightarrow$

$$\Leftrightarrow \begin{cases} g_1^n = e_1 \\ g_2^n = e_2 \\ \vdots \\ g_k^n = e_k \end{cases} \Leftrightarrow \begin{cases} n \vdots \text{ord } g_1 \\ n \vdots \text{ord } g_2 \\ \dots \\ n \vdots \text{ord } g_k \end{cases} \Rightarrow n \text{ кратно } \text{ord } g_1, \text{ord } g_2, \dots, \text{ord } g_k \Rightarrow \\ \Rightarrow n = \text{ord } g \Leftrightarrow n = \text{НОК} \{ \text{ord } g_1, \text{ord } g_2, \dots, \text{ord } g_k \}$$

**УТВ. 5.**

Если  $G_1 = \langle g_1 \rangle$ ,  $G_2 = \langle g_2 \rangle$

$|G_1| = m$ ,  $|G_2| = n$ ,

то  $G_1 \times G_2$  - циклическая группа  $\Leftrightarrow (m, n) = 1$

**Док-во:**  $|G_1 \times G_2| = |G_1| \cdot |G_2| = m \cdot n$

$\text{ord}(\tilde{g}_1, \tilde{g}_2) = \text{НОК}\{\text{ord } \tilde{g}_1, \text{ord } \tilde{g}_2\} \leq \text{ord } \tilde{g}_1 \cdot \text{ord } \tilde{g}_2 \leq m \cdot n$

$G_1 \times G_2$  - цикл.  $\Leftrightarrow \exists (\tilde{g}_1, \tilde{g}_2) \in G_1 \times G_2 : \text{ord}(\tilde{g}_1, \tilde{g}_2) = |G_1 \times G_2| = m \cdot n \Leftrightarrow$

$\Leftrightarrow (m, n) = 1$ .

В этом случае

$$G_1 \times G_2 = \langle (g_1, g_2) \rangle$$

Примеры.

(1)  $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$ , т.к.  $(2, 3) = 1$

(2)  $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\simeq \mathbb{Z}_4$

В  $\mathbb{Z}_2 \times \mathbb{Z}_2$  нет элементов 4-го порядка.

Наибольший порядок элемента в  $\mathbb{Z}_2 \times \mathbb{Z}_2$  - 2. В  $\mathbb{Z}_4$  порождающий элемент имеет порядок 4.

**12.3 Внутреннее прямое произведение подгрупп**

**Опр.**  $G$  - группа.  $G_1, G_2, \dots, G_k < G$

Говорят, что  $G$  является внутренним прямым произведением своих подгрупп, если

$$\left[ \begin{array}{l} 1) \forall g \in G - \text{однозначно представляется в виде произведения} \\ \qquad \qquad \qquad g_1, g_2, \dots, g_k \text{ где } g_i \in G^i, \quad i = \overline{1, k} \\ 2) g_i g_j = g_j g_i \quad i \neq j \quad i, j = \overline{1, k} \end{array} \right.$$

**УТВ. 6.**

Если группа  $G$  является внутренним прямым произведением своих подгрупп  $G_1, G_2, \dots, G_k < G$ , то  $G \simeq G_1 \times G_2 \times \dots \times G_k$

**Док-во:**

Рассмотрим отображение  $\psi : G_1 \times G_2 \times \dots \times G_k \rightarrow G$

$$\psi((g_1, g_2, \dots, g_k)) = g_1 g_2 \dots g_k \in G$$

1)  $\psi$  - гомоморфизм.

$$\begin{aligned} \psi((g_1 \tilde{g}_1, g_2 \tilde{g}_2, \dots, g_k \tilde{g}_k)) &= g_1 \tilde{g}_1 g_2 \tilde{g}_2 \dots g_k \tilde{g}_k = g_1 g_2 \dots g_k \cdot \tilde{g}_1 \tilde{g}_2 \dots \tilde{g}_k = \\ &= \psi((g_1, g_2, \dots, g_k)) \cdot \psi((\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_k)) \end{aligned}$$

2)  $\psi$  - эпиморфизм. ( $Im \psi = G$ )

$\forall g \in G$  можно представить в виде.

$$g = g_1 \cdot g_2 \cdot \dots \cdot g_k, \text{ где } g_i \in G_i, \quad i = \overline{1, k} \Rightarrow$$

$$\Rightarrow \exists (g_1, g_2, \dots, g_k) \in G_1 \times G_2 \times \dots \times G_k;$$

$$\psi((g_1, g_2, \dots, g_k)) = g_1 g_2 \dots g_k = g \Rightarrow g \in Im \psi$$

$\Rightarrow \psi$  - эпиморфизм

3)  $\psi$  - мономорфизм

$$\psi((g_1, g_2, \dots, g_k)) = \psi((\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_k)) \Rightarrow$$

$$\Rightarrow g_1 g_2 \dots g_k = \tilde{g}_1 \tilde{g}_2 \dots \tilde{g}_k$$

$$\Rightarrow \begin{cases} g_1 = \tilde{g}_1 \\ g_2 = \tilde{g}_2 \\ \dots \\ g_k = \tilde{g}_k \end{cases} \Rightarrow (g_1, g_2, \dots, g_k) = (\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_k) \Rightarrow$$

$$\Rightarrow \psi - \text{мономорфизм} \Leftrightarrow Ker \psi = \{(e_1, \dots, e_k)\} - \text{тривиальное}$$

По теореме о гомоморфизме

$$G_1 \times G_2 \times \dots \times G_k / \text{Ker } \psi \simeq \text{Im } \psi$$

$$G_1 \times G_2 \times \dots \times G_k \simeq G$$

**Утв. 7.**  $G = G_1 \times G_2 \times \dots \times G_k$  - внешнее произведение,  
 $\widetilde{G}_i = \{(e_1, e_2, \dots, e_{i-1}, g^i, e_{i+1}, \dots, e_k), g_i \in G_i\} < G$ ;  $\widetilde{G}_i \simeq G_i, i = \overline{1, k}$   
 $G$  является внутренним прямым произведением своих подгрупп  $\widetilde{G}_i, i = \overline{1, k}$

**Док-во:**

1)  $\widetilde{G}_i$  - подгруппа  $G_1 \times G_2 \times \dots \times G_k = G$  по критерию подгруппы  $i = \overline{1, k}$

2)  $\varphi : \widetilde{G}_i \rightarrow G_i$

$$\varphi((e_1, e_2, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_k)) = g_i$$

$$\left. \begin{array}{l} \varphi - \text{гомоморфизм} \\ \varphi - \text{эпиморфизм} \\ \varphi - \text{мономорфизм} \\ \widetilde{G}_i = G_i \end{array} \right\} \Rightarrow \varphi - \text{изоморфизм}$$

3)  $G = G_1 \times \dots \times G_n$  является внутренним прямым произведением  $\widetilde{G}_1, \widetilde{G}_2, \dots, \widetilde{G}_k$

1)  $\forall (g_1, g_2, \dots, g_k) \in G_1 \times G_2 \times \dots \times G_k$

$$(g_1, g_2, \dots, g_k) = (g_1, e_2, \dots, e_k)(e_1, g_2, \dots, e_k) \dots (e_1, \dots, e_{k-1}, g_k)$$

единственным образом представляется в виде произведения элементов

$$\widetilde{G}_1, \widetilde{G}_2, \dots, \widetilde{G}_k$$

$$\begin{aligned} 2) (e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_k)(e_1, \dots, e_{j-1}, g_j, e_{j+1}, \dots, e_k) &= (e_1, \dots, g_i \dots g_j \dots e_k) = \\ &= (e_1 \dots g_1 \dots e_k)(e_1 \dots g_j \dots e_k) \end{aligned}$$

Утв. 6 и 7 показывают тесную связь между понятиями внешнего и внутреннего произведений групп. Поэтому употребляются одинаковые обозначения для этих произведений.

$$G = G_1 \times G_2 \times \dots \times G_k$$

$$\begin{aligned} & \text{УТВ. 8. } G - \text{ группа, } G_1, G_2, \dots, G_k < G, \quad G = G_1 \times G_2 \times \dots \times G_k \Leftrightarrow \\ & \Leftrightarrow \begin{cases} 1) \forall g \in G \text{ единственным образом представляется в виде} \\ \quad g = g_1 g_2 \dots g_k, \quad g_i \in G_i, \quad i = \overline{1, k} \\ 2) G_i \triangleleft G \quad i = \overline{1, k} \end{cases} \end{aligned}$$

### 13 Лекция №13

**Опр.**  $G$ - группа

$$G_1, G_2, \dots, G_k < G$$

$G_1 \times G_2 \times \dots \times G_k$  если

$$\begin{cases} 1) \forall g \in G \text{ единственным образом представляется в виде } g = g_1 g_2 \dots g_k \\ \quad g_i \in G_i \quad i = \overline{1, k} \\ 2) g_i g_j = g_j g_i \quad i \neq j \quad i, j = \overline{1, k} \end{cases}$$

**УТВ. 8.**  $G > G_1, G_2, \dots, G_k$

$$G = G_1 \times G_2 \times \dots \times G_k \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 1) \forall g \in G \text{ единственным образом представляется} \\ \quad \text{в виде } g = g_1 g_2 \dots g_k g_i \in G_i \quad i = \overline{1, k} \\ 2) G_i \triangleleft G \quad \forall i = \overline{1, k} \end{cases}$$

**Док-во:**  $\Rightarrow$

$$1) = 1)' \quad \left. \begin{matrix} 1) \\ 2) \end{matrix} \right\} \Rightarrow 2)'$$

$$G_i \triangleleft G \Leftrightarrow \forall \tilde{g}_i \in G_i \quad \forall g \in G \quad g \tilde{g}_i g^{-1} \in G_i$$

$$1) \Rightarrow g = g_1 g_2 \dots g_i \dots g_k$$

$$g \tilde{g}_i g^{-1} = g_1 g_2 \dots g_i \dots g_k \tilde{g}_i g_k^{-1} \dots g_i^{-1} \dots g_1^{-1} =$$

$$= g_1 g_2 \dots g_i \dots \tilde{g}_i g_k g_k^{-1} \dots g_i^{-1} \dots g_1^{-1} =$$

$$g_1 g_2 \dots g_i \tilde{g}_i g_i^{-1} \dots g_2^{-1} g_1^{-1} =$$

$$g_1 g_2 \dots \tilde{g}_i \dots g_2^{-1} g_1^{-1} =$$

$$= \tilde{g}_i \in G_i \quad \forall \tilde{g}_i \in G_i \quad \forall g \in G \Rightarrow G_i \triangleleft G$$

$$\tilde{g}_i \in G_i$$

$$\oplus$$

$$\left. \begin{array}{l} 1)' = 1)' \\ 2)' \end{array} \right\} \Rightarrow 2)$$

$$g_i \in G \quad g_j \in G_j \quad i \neq j$$

$$g = g_i g_j g_i^{-1} g_j^{-1} = (g_i g_j g_i^{-1}) g_j = \tilde{g}_j g_j = \tilde{g}_j \in G_i$$

$$g_i g_j g_i^{-1} g_j^{-1} = g_i (g_j g_i^{-1} g_j^{-1}) = g_i \tilde{g}_i = \tilde{g}_i \in G_j$$

$$g = e \dots \tilde{g}_i e \dots e = e \dots \tilde{g}_j \dots e$$

$$i \neq j \quad \tilde{g}_i = \tilde{g}_j = e \quad g_i g_j g_i^{-1} g_j^{-1} = e \Leftrightarrow g_i g_j = g_j g_i \quad i \neq j, \quad i = \overline{1, k}$$

**Утв. 9.** В случае 2-х подгрупп  $G_1, G_2 < G$

$\forall g$  единственным образом представляется

$$\text{в виде } g = g_1 g_2, \quad g_1 \in G_1 \quad g_2 \in G_2 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 1) G = G_1 G_2 \\ 2) G_1 \cap G_2 = \{e\} \end{cases}$$

**Док-во:**  $\oplus$

Пусть  $g$  един обр предствл. ??

$$g = g_1 g_2$$

Пусть  $g \in G_1 \cap G_2 \quad g \in G_1, G_2$

$$g = ge = eg \Rightarrow g = e \Rightarrow G_1 \cap G_2 = \{e\}$$

$\oplus$  Пусть  $g = g_1 g_2 = \tilde{g}_1 \tilde{g}_2$

$$g_1 g_2 = \tilde{g}_1 \tilde{g}_2$$

$$G_1 \ni \tilde{g}_1^{-1} g_1 = \tilde{g}_2 g_2^{-1} \in G_2$$

$$\text{т.к. } G_1 \cup G_2 = \{e\} \Rightarrow \begin{cases} \tilde{g}_1^{-1} g_1 = e \\ \tilde{g}_2 g_2^{-1} = e \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} g_1 = \tilde{g}_1 \\ g_2 = \tilde{g}_2 \end{cases}$$

**Следствие.**  $G$  - группа  $G_1, G_2 < G \quad G = G_1 \times G_2 \Leftrightarrow$

$$\Leftrightarrow \left\{ \begin{array}{l} 1) G = G_1 G_2 \\ 2) G_1 \cap G_2 = \{e\} \\ 3) g_1 g_2 = g_2 g_1, \quad g_1 \in G_1, g_2 \in G_2 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} 1) G = G_1 G_2 \\ 2) G_1 \cap G_2 = \{e\} \\ 3) G_1, G_2 \triangleleft G \end{array} \right.$$

Примеры:

(1)  $(\mathbb{Z}, +)$  нельзя разложить в прямое произведение(сумму) подгрупп.

т.к. являются подгруппами  $H < \mathbb{Z}$  имеет вид  $H = m\mathbb{Z}$

$\forall H_1, H_2 < \mathbb{Z}$ , т.е.  $m\mathbb{Z}, k\mathbb{Z} < \mathbb{Z}$  имеют нетривиальное пересечение

$$m\mathbb{Z} \cap k\mathbb{Z} = [m, k]\mathbb{Z} \quad [m, k] = \text{НОК}\{m, k\}$$

$$(2) \mathbb{C}^* = \mathbb{R}_+^* \times \mathbb{U}$$

$$z \in \mathbb{C}^* \quad z = \rho e^{i\varphi} \text{ единственным образом } (\mathbb{R}_+^* \cap \mathbb{U} = \{1\})$$

$$\rho \in \mathbb{R}_+^*, \quad e^{i\varphi} \in \mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$$

$$\mathbb{R}_+^*, \mathbb{U} \triangleleft \mathbb{C}^*, \text{ т.к. } \mathbb{C} - \text{абнлнва группа ??}$$

$$\text{УТВ. 10. } G = G_1 \times G_2 \Rightarrow$$

$$G/G_1 \simeq G_2, \quad G/G_2 \simeq G_1$$

**Док-во:**

$$\varphi_1 : G \rightarrow G_2$$

$$\varphi_1((g_1, g_2)) = g_2$$

$$1) \varphi_1 \text{ гомоморфизм}$$

$$2) \text{Ker } \varphi_1 = G_1 \times \{e_2\} \simeq G_1$$

$$3) \text{Im } \varphi_1 = G_2$$

$$G/G_1 \simeq G_2$$

$$\left. \begin{array}{l} \varphi_1 : G \rightarrow G_2 \\ \varphi_1((g_1, g_2)) = g_2 \\ 1) \varphi_1 \text{ гомоморфизм} \\ 2) \text{Ker } \varphi_1 = G_1 \times \{e_2\} \simeq G_1 \\ 3) \text{Im } \varphi_1 = G_2 \end{array} \right\} \Rightarrow \text{по теореме о гомоморфизме}$$

$$\varphi_2 : G \rightarrow G_1$$

$$\varphi_2((g_1, g_2)) = g_1$$

$$- \parallel -$$

$$- \parallel -$$

$$- \parallel -$$

$$\left. \begin{array}{l} - \parallel - \\ - \parallel - \\ - \parallel - \end{array} \right\} \Rightarrow G/G_2 \simeq G_1$$

**NOTE:** обратное утверждение неверно.



$$\mathbb{Z}_4/\mathbb{Z}_2 \simeq \mathbb{Z}_2 \quad \mathbb{Z}_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

### 13.1 Примарные группы (р - группы)

**Опр.** Группа называется примарной или р-группой, если её порядок равен  $p^k$ ,  $k \in \mathbb{N}$ ,  $p$  - простое.

**Утв. 1.**  $\forall$  циклическая конечномерная группа является прямым произведением примарных циклических групп.

**Док-во:**

$$|G| = n < \infty$$

$$n = p_1^{s_1} p_2^{s_2} \dots p_m^{s_m}$$

$p_i$  - простые числа,  $p_i \neq p_j$  при  $i \neq j$   $i, j = \overline{1, m}$

индукция  $m$

1)  $m = 1$

$$n = p_1^{s_1}$$

$\mathbb{Z}_n = \mathbb{Z}_{p^{s_1}}$  - примарная?? группа

2) Пусть утверждение верно для  $m-1$ , докажем для  $m$

$$n = (p_1^{s_1} p_2^{s_2} \dots p_m^{s_m}) p_m^s$$

$\mathbb{Z}_{mn}$  - циклическая группа раскладывается в прямое произведение

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \Leftrightarrow (m, n) = 1$$

$$(p_1^{s_1} \dots p_{m-1}^{s_{m-1}}, p_m^{s_m}) = 1$$

$$\mathbb{Z}_{p_1^{s_1} \dots p_{m-1}^{s_{m-1}}} \times \mathbb{Z}_{p_m^{s_m}} \simeq \mathbb{Z}_n \Rightarrow \text{по предположению индукции}$$

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{s_{m1}}} \times \dots \times \mathbb{Z}_{p_{m-1}^{s_{m-1}}} \times \mathbb{Z}_{p_m^{s_m}}$$

Пример:  $60 = 2^2 \cdot 3 \cdot 5$

$$\mathbb{Z}_{60} = \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

**Утв. 2.** Примарную циклическую группу нельзя представить в виде прямого произведения 2-х нетривиальных подгрупп.

**Док-во:**

$$|G| = p^S$$

$$G \simeq \mathbb{Z}_{p^S}$$

$$\text{Пусть } G = H_1 \times H_2 \quad H_1, H_2 < G \quad |H_1|, |H_2| \mid p^S$$

$$\Rightarrow \begin{cases} |H_1| = p^k & k < S \\ |H_2| = p^l & l < S \end{cases}$$

$$H_1 \simeq \mathbb{Z}_{p^k} \quad H_2 \simeq \mathbb{Z}_{p^l}$$

$$\mathbb{Z}_{p^S} \simeq \mathbb{Z}_{p^k} \times \mathbb{Z}_{p^l}$$

Наибольший порядок элемента?? в  $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^l}$

$p^{\max\{k,l\}} < p^S$  - наибольший порядок элемента в  $\mathbb{Z}_{p^S} \not\simeq$

### 13.2 Функция Эйлера

$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$  ( $m, n = 1$  изоморфизм групп порождает и изоморфизм колец

$f$  - изоморфизм

$$f(\overline{S}) = f(\overline{1} + \dots + \overline{1}) \text{ (S - раз)} = f(\overline{1}) + \dots + f(\overline{1}) \text{ (S - раз)}$$

$$f(\overline{St}) = f(\overline{1} + \dots + \overline{1}) \text{ (St - раз)} =$$

$$= f(\overline{1}) + \dots + f(\overline{1}) \text{ (t - раз)} f(\overline{1}) + \dots + f(\overline{1}) \text{ (S - раз)}$$

### 13.3 Изоморфизм колец индукции

$$\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$

группы обратимых элементов по умножению

$$\varphi(n) = |\mathbb{Z}_n^*|$$

$$|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*| |\mathbb{Z}_n^*|$$

$$\varphi(mn) = \varphi(m)\varphi(n)$$

$$n = p_1^{s_1} p_2^{s_2} \dots p_m^{s_m} \text{ - разложение на простые множители } p_i \neq p_j$$

$$i \neq j \quad i, j = \overline{1, m}$$

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{s_1}} \times \mathbb{Z}_{p_2^{s_2}} \times \dots \times \mathbb{Z}_{p_m^{s_m}}$$

$$\mathbb{Z}_n^* = \mathbb{Z}_{p_1^{s_1}}^* \times \mathbb{Z}_{p_2^{s_2}}^* \times \dots \times \mathbb{Z}_{p_m^{s_m}}^*$$

$$\varphi(n) = \varphi(p_1^{s_1}) \varphi(p_2^{s_2}) \dots \varphi(p_m^{s_m})$$

$$\varphi(p^S) = p^S - p^{S-1} = p^S \left(1 - \frac{1}{p}\right)$$

$$\begin{aligned} \varphi(n) &= p_1^{s_1} \left(1 - \frac{1}{p_1}\right) p_2^{s_2} \left(1 - \frac{1}{p_2}\right) \dots p_m^{s_m} \left(1 - \frac{1}{p_m}\right) = \\ &= p_1^{s_1} p_2^{s_2} \dots p_m^{s_m} \prod_{i=1}^m \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^m \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

### 13.4 Разложение конечнопорождённых абелевых групп в прямую сумму циклических групп

**Теорема:**  $\forall$  конечнопорождённая абелева группа является прямым произведением бесконечных циклических подгрупп и примарных циклических групп, причём набор порядков этих групп определён однозначно.

Пример:

$$G_1 \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5$$

$$G_2 \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$G_1 \not\simeq G_2$$

**Теорема:**  $\forall$  конечная абелева группа является прямым произведением примарных циклических групп, причём набор порядков этих групп

определён однозначно.

Пример:

Перечислим все абелевы группы  $|G| = 36$

$$36 = 2^3 \cdot 3^2$$

1)  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

2)  $\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3$

3)  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$

4)  $\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$

Все эти группы не изоморфны.

Пример:

Изоморфны ли группы?

1)  $\mathbb{Z}_{24} \times \mathbb{Z}_9$  и  $\mathbb{Z}_4 \times \mathbb{Z}_{54}$

$$24 = 2^3 \cdot 3 \quad 54 = 2 \cdot 3^3$$

$$\mathbb{Z}_{24} = \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2} \not\simeq \mathbb{Z}_4 \times \mathbb{Z}_{54} = \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^3}$$

2)  $\mathbb{Z}_6 \times \mathbb{Z}_{36}$  и  $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$

$$6 = 2 \cdot 3 \quad 12 = 2^2 \cdot 3$$

$$36 = 2^2 \cdot 3^2 \quad 18 = 2 \cdot 3^2$$

$$\mathbb{Z}_6 \times \mathbb{Z}_{36} = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$$

$$\mathbb{Z}_{12} \times \mathbb{Z}_{18} = \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$$

$$\mathbb{Z}_6 \times \mathbb{Z}_{36} \simeq \mathbb{Z}_{12} \times \mathbb{Z}_{18}$$

## 14 Лекция №14

$G$  - группа

$\varphi$  - гомоморфизм.

$\varphi : G \rightarrow S(x)$

$G : X \xrightarrow{\varphi} \forall x \in X \text{ опр. } \varphi(g)x = gx$

**Опр.** Пусть  $G : X, x, y \in X$  называются эквивалентными относительно действия  $G$   $x \sim_G y$ , если  $\exists g \in G : y = gx$

**Утв. 1**  $x \sim_G y$  - отношение эквивалентности (Проверить самим)

**Опр.** Смежные классы эквивалентности  $x \sim y$  называются орбитами действия  $G$  на  $X$

$$G(x) = \{y \in X : y = gx \forall g \in G\}$$

**Опр.** Действие  $G$  на  $X$  (или сама группа  $G$ ) называется транзитивным, если:  $\forall x, y \in X \exists g \in G : y = gx$ , т.е  $\exists$  всего одна орбита действия группы  $G$ .

**Опр.** Стабилизатором точки  $x \in X$  называется

$$G_x = \{g \in G : gx = x\}$$

**Утв. 2**  $G_x < G$  (док-ть самим, используя критерий подгрупп)

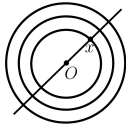
Примеры:

(1)  $G = \text{Isom } E^2 \quad \exists t_{\overline{xy}} \in \text{Isom } E^2$  - пара переносов на  $\overline{xy}$

$$\begin{array}{ccc} & & y \\ & \nearrow t & \\ x & & \end{array} \quad t_{\overline{xy}}x = y$$

транзитивное действие  $G(x) = E^2, \quad G_x = O_2$

(2)  $G = O_2 : E^2 \quad G(O) = O \quad G_O = O_2$



$G(x)$  - окружность, проходящая через  $x$  с центром  $O$

$$G_x = \{id, S_{Ox}\}$$

(3)  $G : G$  сопряжение

$$x, y \in G \quad y = gxg^{-1} \quad \forall g \in G$$

$$x \in Z(G) \quad gxg^{-1} = x \quad \forall g \in G \quad G_x = G = Z(x) \quad G(x) = x = C(x)$$

$$x \notin Z(G) \text{ орбита } G(x) = \{y \in G : y = gxg^{-1}\} =$$

$= C(x)$  - класс сопряжений.

$$G_x = \{g \in G : gxg^{-1} = x\} = Z(x)$$

(4)  $S_n : S_n$  сопряжение

$G(\alpha) = C(\alpha)$  - все элементы, имеющие циклический тип  $\{\alpha\}$ , и только они

$$G_\alpha = Z(\alpha)$$

**УТВ. 3.**  $G : x$

$$G_{gx} = gG_xg^{-1}$$

**Док-во:**

$$1) h \in G_x \quad ghg^{-1}(gx) = g(h(x)) = g(x) = gx \Rightarrow ghg^{-1} \in G_{gx},$$

$$\text{т.е. } gG_xg^{-1} \subset G_{gx}$$

$$2) x = g^{-1}(gx)$$

$$g^{-1}G_{gx}g \subset G_x$$

$$gg^{-1}G_{gx}gg^{-1} \subset gG_xg^{-1}$$

$$G_{gx} \subset gG_xg^{-1}$$

$$\left. \begin{array}{l} 1) \\ 2) \end{array} \right\} \Rightarrow G_{gx} = gG_xg^{-1}$$

**Теорема:**  $G : X$

$$x \in X \quad f : G(x) \rightarrow G/G_x : \quad f(gx) = gG_x \quad f - \text{биекция}$$

**Док-во:**

0) Опр  $f$  корректно

$$g_1x = g_2x \Rightarrow x = g_1^{-1}g_2x \Rightarrow g_1^{-1}g_2 \in G_x \Rightarrow g_1G_x = g_2G_x$$

1)  $f$  - инъективно, т.к

$$f(g_1x) = f(g_2x) \Rightarrow g_1G_x = g_2G_x \Rightarrow g_1^{-1}g_2 \in G_x \Rightarrow g_1^{-1}g_2x = x \Rightarrow g_1x = g_2x$$

2)  $f$  - сюръективно, т.к

$$\forall gG_x \in G/G_x \quad \exists gx \in G(x) : f(gx) = gG_x \quad f - \text{биекция}$$

**Опр.** Длиной орбиты  $|G(x)|$  называется количество точек в ней.

$$\textbf{Следствие 1.} \quad |G| < \infty, G : X \Rightarrow \forall x \in X \quad |G(x)| = |G : G_x|$$

$$\textbf{Следствие 2.} \quad |G| < \infty, G : X \Rightarrow \forall x \in X \quad |G| = |G_x| \cdot |G(x)|$$

$$\textbf{Следствие 3.} \quad |G| < \infty, G : X \Rightarrow \forall x \in X \quad |G(x)| \mid |G|$$

$$\textbf{Следствие 4.} \quad |G| < \infty, G : X \Rightarrow \forall x \in X \quad |G| = |Z(x)| |C(x)|$$

В частн, в т.р №4  $G = S_4$

$$|G(\alpha)| = |C(x)| = N_{\{\alpha\}}$$

$$|G_\alpha| = |Z(\alpha)|$$

$$|Z(\alpha)| \cdot |C(x)| = |Z(\alpha)| N_{\{\alpha\}} = |S_n| = n!$$

**Утв. 4.** Примарная группа имеет нетривиальный центр.

$$|G| = p^m \quad (p - \text{простое число}, m \in \mathbb{N}) \Rightarrow Z(G) \neq \{e\}$$

**Док-во:** Рассмотрим  $G : G$  сопряж.

$$G = Z(G) \cup G(x_1) \cup G(x_2) \cup \dots \cup G(x_k) = Z(G) \cup C(x_1) \cup C(x_2) \cup \dots \cup C(x_k)$$

$$x_i \notin Z(G) \quad x_i \neq x_j \quad i, j = \overline{1, k}$$

$$|C(x_i)| \mid |G| \quad \forall i = \overline{1, k} \Rightarrow |C(x_i)| = p^{l_i} \quad 1 \leq l_i \leq m$$

$$|G| = |Z(G)| + \sum_{i=1}^k |C(x_i)|$$

$$1 \leq |Z(G)| = |G| - \sum_{i=1}^k |C(x_i)| = p^m - \sum_{i=1}^k p^{l_i} \quad \vdots p$$

$$\Rightarrow |Z(G)| : p \Rightarrow Z(G) \neq \{e\}$$

**Утв. 5**  $|G| < \infty$   $G/Z(G)$  - цикл. группа  $\Rightarrow G$  - абелева группа

**Док-во:** Пусть  $G/Z(G) = \langle aZ(G) \rangle$   $a \in G$   
 $\forall g \in G$  имеет  $a^k z$ , где  $z \in Z(G)$ , но элементы такого вида коммутируют  
 $g_1 = a^{k_1} z_1, g_2 = a^{k_2} z_2$   
 $g_1 g_2 = a^{k_1} z_1 a^{k_2} z_2 = a^{k_1+k_2} z_1 z_2 = a^{k_2} a^{k_1} z_2 z_1 = a^{k_2} z_2 a^{k_1} z_1 = g_2 g_1 \Rightarrow$   
 $\Rightarrow G$  - абелева

**Утв. 6.**  $|G| = p^2$ ,  $p$  - простое  $\Rightarrow G$  - абелева.

**Док-во:**

Пусть  $G$  не является абелевой, т.е.  $G \neq Z(G)$ ,  
 $\Rightarrow 1 \neq |Z(G)| = p \Rightarrow |G/Z(G)| = p \Rightarrow G/Z(G) \simeq \mathbb{Z}_p$  (цикл)  
 $\Rightarrow G = Z(G) \Rightarrow G$  - абелева.

**Утв. 7.**  $G$  - неабелева

$|G| = 2p$ ,  $p$  - простое  $\Rightarrow$   
 $\Rightarrow G \simeq D_p$

**Док-во:**

$$\forall g \in G \text{ } ord\,g \mid 2p$$

Если  $\exists g \in G : ord\,g = 2p \Rightarrow G$  - циклическая  $\Rightarrow$  абелева.  $\times$

Если  $\forall g \in G, g \neq e, ord\,g = 2 \Rightarrow G$  - абелева.  $\times$

$$\exists u \in G : ord\,u = p$$

Рассмотрим  $H = \langle u \rangle$   $|G : H| = 2$

$$G = H \cup bH$$

$$b \notin \langle u \rangle$$

$$H \triangleleft G \quad G/H \simeq \mathbb{Z}_2$$

$$(bH)(bH) = H \Rightarrow b^2 \in H$$



$$ord b = \begin{cases} 2p \Rightarrow G - \text{циклическая} \Rightarrow \text{абелева.} \times \\ p \Rightarrow b = bb^p = b^{p+1} = b^{2m} = (b^2)^m \in H \times \\ 2 \end{cases}$$

$$b \notin H \Rightarrow ord b = 2 \Rightarrow$$

$$\Rightarrow ba \notin H \Rightarrow ord ba = 2$$

$$ba ba = e \Rightarrow bab = a^{-1}$$

$$\left. \begin{array}{l} G = \langle a, b \rangle \\ ord a = p \\ ord b = z \\ bab = a^{-1} \end{array} \right\} \Rightarrow G \simeq D_p$$

**Утв. 8.**  $G$  - неабелева группа,

$$|G| = 8 \Rightarrow G \simeq \begin{bmatrix} Q_4 \\ Q_8 \end{bmatrix}$$

**Док-во:**

Если  $\exists g \in G : ord g = 8 \Rightarrow G$  - циклическая  $\Rightarrow$  абелева.  $\times$

Если  $\forall g \in G, g \neq e, ord g = 2 \Rightarrow G$  - абелева.  $\times$

$$\exists a \in G : ord a = 4$$

Рассмотрим  $H = \langle a \rangle : |G : H| = 2 \Rightarrow H \triangleleft G$

$$G/Z(G) \simeq \mathbb{Z}_2$$

$$|G| = 2^3 \Rightarrow Z(G) \neq \{e\}$$

$$|Z(G)| = \begin{cases} 8 \Rightarrow G - \text{абелева.} \times \\ 4 \Rightarrow |G/Z(G)| = 2 \Rightarrow G/Z(G) - \text{циклическая} \Rightarrow G - \text{абелева} \\ 2 \end{cases}$$

$$Z(G) = \{e, z\}$$

$$\text{Если } z \notin H \quad G = H \cup zH$$

$$\Rightarrow \forall g = a^k z, \quad z \in Z(G) \Rightarrow G - \text{абелева.} \times$$

$$\Rightarrow z \in H, \quad ord z = z, \quad z = a^2$$

$$\exists b \notin \langle a \rangle, \quad Z(G)$$

$$\Rightarrow G = H \cup bH \Rightarrow$$

$$\Rightarrow G = \langle a, b \rangle$$

$$bab^{-1} \in H = \langle a \rangle, \text{ т.к. } H \triangleleft G$$

$$bab^{-1} = a \Rightarrow ba = ab \Rightarrow G - \text{абелева. } \times$$

$$bab^{-1} = a^3 = a^{-1}$$

$$1) \text{ ord } b = 2$$

$$\left. \begin{array}{l} G = \langle a, b \rangle \\ \text{ord } a = 4 \\ \text{ord } b = 2 \\ bab^{-1} = a^{-1} \end{array} \right\} \Rightarrow G \simeq D_4$$

$$2) \text{ ord } b = 4, \quad c = b^{-1}, \quad \text{ord } c = 4$$

$$\left. \begin{array}{l} G = \langle a, b \rangle = \langle a, c \rangle \\ \text{ord } a = 2 \\ a^2 = z = c^2 \\ c^{-1}ac = a^{-1} \end{array} \right\} \Rightarrow G \simeq Q_8$$

Группы малых порядков

$ G $	абелева	неабелева
1	$\{e\} \simeq \mathbb{Z}_1$	—
2 - простое	$\mathbb{Z}_2$	—
3 - простое	$\mathbb{Z}_3$	—
$4 = 2^2$	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq V_4$	—
5 - простое	$\mathbb{Z}_5$	—
$6 = 2 \cdot 3$	$\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$	$D_3 \simeq S_3$
7 - простое	$\mathbb{Z}_7$	—
$8 = 2^3$	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4, Q_8$
$9 = 3^2$	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$	—
$10 = 2 \cdot 5$	$\mathbb{Z}_2 \times \mathbb{Z}_5$	$D_5$
11 - простое	$\mathbb{Z}_{11}$	—

## 15 Лекция №15

### 15.1 Группы правильных многогранников

Правильные многогранники:

- 1) тетраэдр
- 2) куб (гексаэдр) (двойственен 3)
- 3) октаэдр (двойственен 2)
- 4) додекаэдр (двойственен 5)
- 5) аксаэдр (двойственен 4)

Центры граней двойственных многогранников являются вершинами другого двойственного многогранника.

Тетраэдр двойственен сам себе.

$$(Rot M) \sim Sym_+ M < Sym M = \{\alpha \in Isom E^3 : \alpha(M) = M\} < O_3$$

Название	Число граней	Число рёбер	Число вершин	$ Sym M $	$ Sym_+ M $
тетраэдр	4	$\frac{4 \cdot 3}{6} = 6$	4	24	12
куб	6	$\frac{6 \cdot 4}{2}$	8	48	24
октаэдр	8	$\frac{8 \cdot 3}{2} = 12$	6	48	24
додекаэдр	12	$\frac{12 \cdot 5}{2} = 30$	$\frac{12 \cdot 5}{3} = 20$	120	60
искосаэдр	20	$\frac{20 \cdot 3}{2} = 30$	$\frac{20 \cdot 3}{5} = 12$	120	60

Найдём  $|Sym M|$

$T$  - тетраэдр.

$$G = Sym T$$

$G$  : множество вершин ( $t$  - top)

транзитивно

$$|G| = |G(t)| |G_t| = 4 \cdot 6 = 24$$

$$|G(t)| = 4$$

$G_t$  : множество рёбер, исходящих из вершины  $t$  ( $e$  - *edge*)

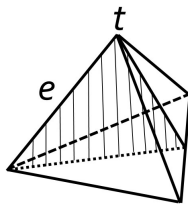
действие транзитивно

$$|G_t| = |G_t(e)||G_{t_e}| = 3 \cdot 2 = 6$$

$$|G_t(e)| = 3$$

$$G_{t_e} = \{id, S\}$$

$S$  - отражение относительно плоскости,  
проходящей через ребро  $e$  и центр  $T$



$$|G_{t_e}| = 2$$

Найдём  $|Sym_+ M|$

$T$  - тетраэдр.

$$G = Sym_+ T$$

$G$  : множество вершин  $t$

транзитивно

$$|G| = |G(t)||G_t| = 4 \cdot 3 = 12$$

$$|G(t)| = 4$$

$G_t$  : множество рёбер, исходящих из вершины  $t$  ( $e$  - *edge*)

действие транзитивно

$$|G_t| = |G_t(e)||G_{t_e}| = 3 \cdot 1 = 3$$

$$|G_t(e)| = 3$$

$$G_{t_e} = \{id\}$$

Найдём  $|Sym M|$

$K$  - куб.

$$G = Sym K$$

$G$  : множество вершин  $t$

транзитивно

$$|G| = |G(t)| |G_t| = 8 \cdot 6 = 48$$

$$|G(t)| = 8$$

$G_t$  : множество рёбер, исходящих из вершины  $t$  ( $e$  - edge)

действие транзитивно

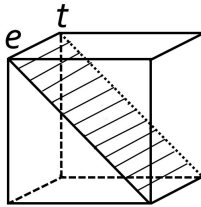
$$|G_t| = |G_t(e)| |G_{te}| = 3 \cdot 2 = 6$$

$$|G_t(e)| = 3$$

$$G_{te} = \{id, S\} \Rightarrow |G_{te}| = 2$$

$S$  - отражение относительно плоскости,

проходящей через ребро  $e$  и центр



Найдём  $|Sym_+ M|$

$K$  - куб.

$$G = Sym_+ T$$

$G$  : множество вершин  $t$

транзитивно

$$|G| = |G(t)| |G_t| = 8 \cdot 3 = 24$$

$$|G(t)| = 8$$

$G_t$  : множество рёбер, исходящих из вершины  $t$  ( $e$  - edge)

действие транзитивно

$$|G_t| = |G_t(e)| |G_{te}| = 3 \cdot 2 = 6$$

$$|G_t(e)| = 3$$

$$G_{te} = \{id\} \Rightarrow |G_{te}| = 2$$

ОКТАЭДРА В ЛЕКЦИИ НЕ БЫЛО

Найдём  $|Sym M|$

$T$  - октаэдр.

Найдём  $|Sym_+ M|$

$T$  - октаэдр.

Найдём  $|Sym M|$

$M = D$  - додекаэдр.

$G = Sym D$

$G$  : множество вершин  $t$

транзитивно

$$|G| = |G(t)| |G_t| = 20 \cdot 6 \cdot 2 = 240$$

$$|G(t)| = 20$$

$G_t$  : множество рёбер, исходящих из вершины  $t$  ( $e$  - *edge*)

действие транзитивно

$$|G_t| = |G_t(e)| |G_{t_e}| = 6 \cdot 2 = 12$$

$$|G_t(e)| = 3 \cdot 2 = 6$$

$$G_{t_e} = \{id, S\} \Rightarrow |G_{t_e}| = 2$$

$Sym_+ M$  содержит повороты относительно осей, проходящих через центр и граничную точку.

[ вершина  
середина ребра  
центр грани

$Sym_+ T$

1 шт. 1)  $id$

$4 \cdot 2 = 8$  шт. 2) поворот, относительно проходящий через вершину и центр

(и через центр  $y$ )

на  $\frac{2\pi}{3}, \frac{2\pi \cdot 2}{3}$

$\frac{G}{2} = 3$  3) поворот относительно оси, проходящей через середину ребра и центр (и середину противоположного ребра) на  $\pi$

$Sym_+ K$

1 шт. 1)  $id$

$\frac{8}{2} \cdot 2 = 8$  шт. 2) поворот, относительно проходящий через вершину и центр (и через противоположную вершину)

на  $\frac{2\pi}{3}, \frac{2\pi \cdot 2}{3}$

$\frac{12}{2} \cdot 1 = 6$  3) поворот относительно оси, проходящей через середину ребра и центр (и середину противоположного ребра) на  $\pi$

$\frac{6}{2} \cdot 1 = 9$  (всего 24) 4) поворот относительно оси проходящей через центр

грани (и центр противоположной грани) на  $\frac{2\pi}{4}, \frac{2\pi \cdot 2}{4}, \frac{2\pi \cdot 3}{4}$

$Sym_+ D$

1 шт. 1)  $id$

$\frac{20}{2} \cdot 2 = 20$  шт. 2) поворот, относительно проходящий через вершину и центр (и через противоположную вершину)

на  $\frac{2\pi}{3}, \frac{2\pi \cdot 2}{3}$

$\frac{30}{2} \cdot 1 = 15$  3) поворот относительно оси, проходящей через середину ребра и центр (и середину противоположного ребра) на  $\pi$

$\frac{12}{2} \cdot 4 = 24$  (24) 4) поворот относительно оси проходящей через центр

грани (и центр противоположной грани) на  $\frac{2\pi}{5}, \frac{2\pi \cdot 2}{5}, \frac{2\pi \cdot 3}{5}, \frac{2\pi \cdot 4}{5}$

**Задача:**

Посчитать  $|Sym M|$  и  $|Sym_+ M|$

Рассмотрим действия

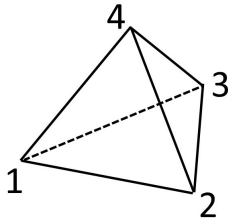
- 1) на мн-во ребер
- 2) на мн-во граней (граней - face)

**УТВ. 1**  $Sym T \simeq S_4$

**Док-во:**

$$F : Sym T \rightarrow S_4 \quad f \in Sym T$$

$F(f) = \alpha$ , которые осуществляет ту же перестановку вершин тетраэдра



Очевидно,  $F$  - гомоморфизм

$$F(f_2 f_1) = F(f_2) F(f_1)$$

$F$  - сюръективно

$$S_4 = \langle (1\ 2), (1\ 3), (1\ 4) \rangle$$

$$\exists f_1 \in Sym T : F(f_1) = (1\ 2)$$

$f_1$  - отражение относительно пл-ти, проходящей через  $e_{34}$  и центр  $T$

$$\exists f_2 \in Sym T : F(f_2) = (1\ 3)$$

$f_2$  - отражение относительно пл-ти, проходящей через  $e_{24}$  и центр  $T$

$$\exists f_3 \in Sym T : F(f_3) = (1\ 4)$$

$f_3$  - отражение относительно пл-ти, проходящей через  $e_{23}$  и центр  $T$

$\Rightarrow F$  - сюръективно

$F$  - инъективно т.к  $|Sym T| = |S_4| = 4! = 24$

$\Rightarrow F$  - изоморфизм

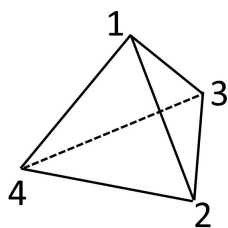
**УТВ. 2**  $Sym_+ T \simeq A_4$

**Док-во:**

$$F : Sym T \rightarrow A_4 \quad f \in Sym T$$

$F(f) = \alpha$ , которые осуществляет ту же перестановку вершин тетраэдра





Очевидно,  $F$  - гомоморфизм

$$F(f_2 f_1) = F(f_2) F(f_1)$$

$F$  - сюръективно

$$A_4 = \langle (1\ 2), (1\ 3), (1\ 4) \rangle$$

$$\exists f_1 \in \text{Sym } T : F(f_1) = (1\ 2\ 3)$$

$f_1$  - поворот относительно прямой, проходящей через  $t_4$  и центр, на  $\frac{2\pi}{3}$

.....

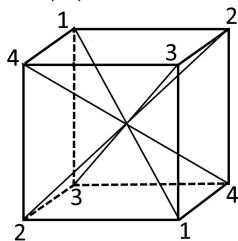
$F$  - сюръективна

$F$  - инъективна

$$|\text{Sym}_+ T| = |Au| = 12 \Rightarrow F \text{ - изоморфизм}$$

**Утв. 3.**  $\text{Sym}_+ K \simeq S_4$

**Док-во:**



$$F : \text{Sym}_+ K \rightarrow S_u \quad \forall f \in \text{Sym}_+ K$$

$F(t) = \alpha \in S_u$ , которая осуществляет ту же перестановку диагоналей (доделать самим)

**Утв. 4.**  $\text{Sym}_+ D \simeq A_5$  (доказать самим)