

# ЛЕКЦИЯ 9

ЗАДАНИЕ АБЕЛЕВОЙ ГРУППЫ ОБ-  
РАЗУЮЩИМИ И СООТНОШЕНИЯМИ

ДЕЙСТВИЯ ГРУППЫ НА МНОЖЕ-  
СТВЕ (ПОЛИГОНЫ)

ПРИМЕРЫ ДЕЙСТВИЙ

ЦЕНТР  $p$ -ГРУППЫ

## ЗАДАНИЕ ГРУППЫ ОБРАЗУЮЩИМИ И СООТНОШЕНИЯМИ

В комбинаторной теории групп один из основных способов задания групп — это задание группы образующими и соотношениями между ними. Наиболее прозрачный сюжет в этой области — это задание конечно порожденной абелевой группы образующими и соотношениями, поскольку для конечно порожденной абелевой группы  $A = \langle a_1, \dots, a_n \rangle$  каждый элемент  $x \in A$  записывается (в аддитивной форме) как

$$X = k_1 a_1 + \dots + k_n a_n, \quad k_i \in \mathbb{Z}.$$

ЗАМЕЧАНИЕ 1 (О ЗАДАНИИ КОНЕЧНО ПОРОЖДЕННОЙ АБЕЛЕВОЙ ГРУППЫ ОБРАЗУЮЩИМИ И СООТНОШЕНИЯМИ). Пусть  $A = \langle a_1, \dots, a_n \rangle$  — конечно порожденная абелева группа,  $\{a_1, \dots, a_n\}$  — одна из ее систем образующих;

$$\pi: F_n = \langle e_1, \dots, e_n \rangle \rightarrow A = \langle a_1, \dots, a_n \rangle$$

— сюръективный гомоморфизм из свободной абелевой группы  $F_n$  с базисом  $\{e_1, \dots, e_n\}$  в группу  $A$ , для которого  $\pi(e_i) = a_i$ ,  $1 \leq i \leq n$ ,

$$B = \ker \pi \subseteq F_n = \langle e_1, \dots, e_n \rangle,$$

$B$  — свободная абелева группа,  $\{b_1, \dots, b_m\}$  — ее базис,  $m \leq n$ ;  
 $b_j = \sum_{i=1}^n r_{ij} e_i$ ,  $r_{ij} \in \mathbb{Z}$ ,  $R = (r_{ij}) \in \mathbf{M}_{n,m}(\mathbb{Z})$  — матрица соотношений между образующими  $a_1, \dots, a_n$ .

Тогда целочисленная матрица  $R = (r_{ij}) \in \mathbf{M}_{n,m}(\mathbb{Z})$  полностью определяет абелеву группу  $A$  как фактор-группу:

$$\begin{aligned} A &\cong F_n / \ker \pi = F_n / B = \langle e_1, \dots, e_n \rangle / \langle b_1, \dots, b_m \rangle, \\ F_n &= \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n, \quad B = \mathbb{Z}b_1 \oplus \dots \oplus \mathbb{Z}b_m, \\ b_j &= \sum_{i=1}^n r_{ij}e_i \in \ker \pi, \quad 1 \leq j \leq m. \end{aligned}$$

Так как  $b_j \in \ker \pi$ , то  $\pi(b_j) = 0$ ,  $1 \leq j \leq m$ , и поэтому

$$0 = \pi(b_j) = \pi\left(\sum_{i=1}^n r_{ij}e_i\right) = \sum_{i=1}^n r_{ij}\pi(e_i) = \sum_{i=1}^n r_{ij}a_i$$

является соотношением между элементами  $a_1, \dots, a_n$ . При этом если

$$k_1a_1 + \dots + k_na_n = 0$$

— любое другое соотношение между группами  $a_1, \dots, a_n$ , то

$$\pi(k_1e_1 + \dots + k_ne_n) = k_1a_1 + \dots + k_na_n = 0,$$

и поэтому

$$k_1e_1 + \dots + k_ne_n \in \ker \pi = \langle b_1, \dots, b_m \rangle.$$

Следовательно, элемент  $k_1e_1 + \dots + k_ne_n$  является линейной комбинацией элементов  $b_1, \dots, b_m$ . Таким образом, соотношения  $b_1, \dots, b_m$  определяют все соотношения между элементами  $a_1, \dots, a_n$ .  $\square$

ЗАМЕЧАНИЕ 2. Основная идея доказательства теоремы о классификации конечно порожденных абелевых групп связана с заменой базисов в свободных абелевых группах  $F_n$  и  $\ker \pi$ ,

$$0 \rightarrow \ker \pi \rightarrow F_n \rightarrow A = \langle a_1, \dots, a_n \rangle \rightarrow 0,$$

а именно, с переходом от исходных базисов  $\{e_1, \dots, e_n\}$  и  $\{b_1, \dots, b_m\}$  соответственно к новым базисам  $\{e'_1, \dots, e'_n\}$  и  $\{b'_1, \dots, b'_m\}$ , в которых матрица соотношений  $R'$  уже будет иметь диагональный вид.

Для реализации этой программы нам понадобятся некоторые сведения о целочисленных матрицах и о матрицах эндоморфизмов свободных абелевых групп, похожие на известные нам сведения о матрицах линейных преобразований линейных пространств над полем.

**Лемма 1.** Пусть  $A = (a_{ij}) \in \mathbf{M}_n(\mathbb{Z})$  — квадратная  $(n \times n)$ -матрица с элементами  $a_{ij} \in \mathbb{Z}$ . Тогда  $A \in \mathrm{GL}_n(\mathbb{Z})$  (т. е. матрица  $A$  обратима, это означает существование матрицы  $B \in \mathbf{M}_n(\mathbb{Z})$ , для которой  $AB = E = BA$ ) в том и только в том случае, если  $|A| = \pm 1$  (иными словами,  $|A| \in \mathbf{U}(\mathbb{Z}) = \{1, -1\}$ ).

*Доказательство.*

1) Если  $AB = E$ , то  $|A| \cdot |B| = |AB| = |E| = 1$ , и поэтому  $|A| \in \mathbf{U}(\mathbb{Z}) = \{1, -1\}$ .

2) Если  $|A| = \pm 1$ , то для  $B = (b_{ij} = A_{ji}/|A|) \in \mathbf{M}(\mathbb{Z})$  имеем  $AB = E = BA$ , поэтому  $A \in \mathrm{GL}_n(\mathbb{Z})$ .  $\square$

ПРИМЕР 1. Следующие матрицы называются *элементарными матрицами* в группе  $GL_n(\mathbb{Z})$ :

1)  $e_{ij}^r = E + rE_{ij}$ ,  $i \neq j$ ,  $r \in \mathbb{Z}$ ,  $|e_{ij}^r| = 1$ ;

2) матрица  $t_{ij}$ ,  $i \neq j$ , получаемая из единичной матрицы  $E$  перестановкой  $i$ -й и  $j$ -й строк,  $|t_{ij}| = -1$ ;

3)  $\text{diag}(d_1, \dots, d_n) = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$ , где  $d_i = \pm 1$ ,  $|\text{diag}(d_1, \dots, d_n)| = d_1 \dots d_n = \pm 1$ .

Их называют элементарными, поскольку они реализуют элементарные преобразования строк или столбцов.

1. *Элементарные преобразования строк* прямоугольной  $(m \times n)$ -матрицы  $A \in \mathbf{M}_{m,n}(\mathbb{Z})$  при умножении *слева* на элементарные матрицы  $e_{ij}^r, t_{ij}, \text{diag}(d_1, \dots, d_m) \in GL_n(\mathbb{Z})$ :

1) матрица  $e_{ij}^r A$  получается из матрицы  $A$  прибавлением к  $i$ -й строке  $j$ -й строки, умноженной на  $r \in \mathbb{Z}$ ;

2) матрица  $t_{ij} A$  получается из матрицы  $A$  перестановкой  $i$ -й и  $j$ -й строк;

3) матрица  $\text{diag}(d_1, \dots, d_m) A$  получается из матрицы  $A$  умножением  $i$ -й строки на  $d_i$ ,  $1 \leq i \leq m$ ,  $d_i = \pm 1 \in \mathbb{Z}$ .  $\square$

2. *Элементарные преобразования столбцов* прямоугольной  $(m \times n)$ -матрицы  $A \in \mathbf{M}_{m,n}(\mathbb{Z})$  при умножении *справа* на элементарные матрицы  $e_{ij}^r, t_{ij}, \text{diag}(d_1, \dots, d_n) \in GL_n(\mathbb{Z})$ :

1) матрица  $A e_{ij}^r$  получается из матрицы  $A$  прибавлением к  $j$ -му столбцу  $i$ -го столбца, умноженного на  $r \in \mathbb{Z}$ ;

2) матрица  $A t_{ij}$  получается из матрицы  $A$  перестановкой  $i$ -го и  $j$ -го столбцов;

3) матрица  $A \text{diag}(d_1, \dots, d_n)$  получается из матрицы  $A$  умножением  $j$ -го столбца на  $d_j = \pm 1 \in \mathbb{Z}$ ,  $1 \leq j \leq n$ .  $\square$

**Лемма 2.** Эндоморфизм  $\alpha \in \text{End}(F_n)$  свободной абелевой группы  $F_n$  с базисом  $\{e_1, \dots, e_n\}$  тогда и только тогда является автоморфизмом,  $\alpha \in \text{Aut}(F_n)$ , когда образ  $\{\alpha(e_1), \dots, \alpha(e_n)\}$  базиса  $\{e_1, \dots, e_n\}$  при  $\alpha$  также является базисом абелевой группы  $F_n$ .

*Доказательство.*

1а) Если  $\alpha \in \text{Aut}(F_n)$ ,  $\alpha\beta = 1_{F_n} = \beta\alpha$ ,  $\beta \in \text{Aut}(F_n)$ ,  $x \in F_n$ ,  $\beta(x) = \sum_{i=1}^n l_i e_i$ ,  $l_i \in \mathbb{Z}$ , то

$$x = 1_F(x) = (\alpha\beta)(x) = \alpha(\beta(x)) = \alpha\left(\sum_{i=1}^n l_i e_i\right) = \sum_{i=1}^n l_i \alpha(e_i).$$

Таким образом,  $\{\alpha(e_1), \dots, \alpha(e_n)\}$  — система образующих абелевой группы  $F_n$ .

1б) Если

$$\sum_{i=1}^n k_i \alpha(e_i) = 0,$$

то

$$0 = \sum_{i=1}^n k_i \alpha(e_i) = \alpha\left(\sum_{i=1}^n k_i e_i\right),$$

и, поскольку  $\alpha \in \text{Aut}(F_n)$ ,

$$\sum_{i=1}^n k_i e_i = 0,$$

поэтому  $k_1 = k_2 = \dots = k_n = 0$ . Таким образом,  $\{\alpha(e_1), \dots, \alpha(e_n)\}$  — линейно независимая система элементов абелевой группы  $F_n$ .

Итак, 1а) и 1б) означают, что  $\{\alpha(e_1), \dots, \alpha(e_n)\}$  — базис в  $F_n$ .

2) Если  $\{\alpha(e_1), \dots, \alpha(e_n)\}$  — базис абелевой группы  $F_n$  для  $\alpha \in \text{End}(F_n)$ , то рассмотрим  $\beta \in \text{End}(F_n)$ , для которого

$$\beta(\alpha(e_i)) = e_i, \quad 1 \leq i \leq n.$$

Тогда

$$(\beta\alpha)(e_i) = \beta(\alpha(e_i)) = e_i$$

для всех  $1 \leq i \leq n$ , и поэтому  $\beta\alpha = 1_{F_n}$ ;

$$(\alpha\beta)(\alpha(e_i)) = \alpha((\beta\alpha)(e_i)) = \alpha(1_{F_n}(e_i)) = \alpha(e_i)$$

для всех  $1 \leq i \leq n$ , и поэтому  $\alpha\beta = 1_{F_n}$ .

Итак,  $\alpha\beta = 1_{F_n} = \beta\alpha$ ,  $\beta = \alpha^{-1} \in \text{Aut}(F_n)$ . □

Пусть  $\{e_1, \dots, e_n\}$ ,  $\{e'_1, \dots, e'_n\}$  — два базиса свободной абелевой группы  $F_n$ ,

$$e'_j = \sum_{i=1}^n c_{ij}e_i, \quad c_{ij} \in (\mathbb{Z}), \quad 1 \leq j \leq n.$$

Квадратная целочисленная  $(n \times n)$ -матрица  $C = (c_{ij}) \in \mathbf{M}_n(\mathbb{Z})$  называется *матрицей перехода* от первого базиса  $\{e_1, \dots, e_n\}$  ко второму базису  $\{e'_1, \dots, e'_n\}$  в  $F_n$ .

Рассмотрим эндоморфизм  $\xi: F_n \rightarrow F_n$ ,  $\xi \in \text{End}(F_n)$ , для которого

$$\xi(e_j) = e'_j = \sum_{i=1}^n c_{ij}e_i.$$

Так как  $\xi(\{e_1, \dots, e_n\}) = \{e'_1, \dots, e'_n\}$  — базис в  $F_n$ , то  $\xi$  — автоморфизм,  $\xi \in \text{Aut}(F_n)$ , при этом  $C$  — матрица автоморфизма  $\xi$  в базисе  $\{e_1, \dots, e_n\}$ .

**Лемма 3.** Пусть  $F_n$  — свободная абелева группы конечного ранга  $n$ ,  $\{e_1, \dots, e_n\}$  и  $\{e'_1, \dots, e'_n\}$  — базисы в  $F_n$ , при этом

$$C = (c_{ij}) \in \mathbf{M}(\mathbb{Z}), \quad e'_j = \sum_{i=1}^n c_{ij} e_i, \quad 1 \leq j \leq n,$$

— матрица перехода от базиса  $\{e_1, \dots, e_n\}$  к базису  $\{e'_1, \dots, e'_n\}$ ,  $\alpha \in \text{End}(F_n)$ ,  $A = (a_{ij}) \in \mathbf{M}_n(\mathbb{Z})$  — его матрица в базисе  $\{e_1, \dots, e_n\}$ ,  $A' = (a'_{ij}) \in \mathbf{M}_n(\mathbb{Z})$  — его матрица в базисе  $\{e'_1, \dots, e'_n\}$ . Тогда

$$A' = C^{-1}AC.$$

*Доказательство.* Так как для автоморфизма

$$\xi: F_n \rightarrow F_n, \quad \xi(e_j) = e'_j, \quad j = 1, \dots, n,$$

с матрицей  $C = (c_{ij})$  в базисе  $\{e_1, \dots, e_n\}$  имеем для любого  $1 \leq j \leq n$

$$\begin{aligned} (\xi^{-1}\alpha\xi)(e_j) &= \xi^{-1}\left(\alpha(\xi(e_j))\right) = \xi^{-1}(\alpha(e'_j)) = \\ &= \xi^{-1}\left(\sum_{i=1}^n a'_{ij} e'_i\right) = \sum_{i=1}^n a'_{ij} \xi^{-1}(e'_i) = \sum_{i=1}^n a'_{ij} e_i, \end{aligned}$$

то матрица эндоморфизма  $\xi^{-1}\alpha\xi$  в базисе  $\{e_1, \dots, e_n\}$  равна  $A'$ , а с другой стороны, она равна  $C^{-1}AC$ .

Итак,  $A' = C^{-1}AC$ . □

Пусть  $A, B \in \mathbf{M}_{m,n}(\mathbb{Z})$ . Скажем, что матрица  $B$  эквивалентна матрице  $A$ , если существуют такие обратимые матрицы  $U \in \mathrm{GL}_m(\mathbb{Z})$  и  $V \in \mathrm{GL}_n(\mathbb{Z})$ , что

$$B = UAV$$

(обозначение:  $B \sim A$ ).

Действительно, это отношение  $B \sim A$  является отношением эквивалентности:

1)  $A \sim A$ , поскольку  $A = E_m A E_n$ ,  $E_m \in \mathrm{GL}_m(\mathbb{Z})$ ,  $E_n \in \mathrm{GL}_n(\mathbb{Z})$ ;

2) если  $B \sim A$ ,  $B = UAV$ ,  $U \in \mathrm{GL}_m(\mathbb{Z})$ ,  $V \in \mathrm{GL}_n(\mathbb{Z})$ , то  $A = U^{-1} B V^{-1}$ ,  $U^{-1} \in \mathrm{GL}_m(\mathbb{Z})$ ,  $V^{-1} \in \mathrm{GL}_n(\mathbb{Z})$ , и поэтому  $A \sim B$ ;

3) если  $C \sim B$ ,  $C = U' B V'$ ,  $B \sim A$ ,  $B = UAV$ ,  $U, U' \in \mathrm{GL}_m(\mathbb{Z})$ ,  $V, V' \in \mathrm{GL}_n(\mathbb{Z})$ , то

$$C = U' B V' = U' (U A V) V' = (U' U) A (V V'),$$

$U' U \in \mathrm{GL}_m(\mathbb{Z})$ ,  $V V' \in \mathrm{GL}_n(\mathbb{Z})$ , и поэтому  $C \sim A$ . □



Первый шаг редукции заключается в приведении матрицы  $A$  к эквивалентной целочисленной  $(m \times n)$ -матрице  $C \in \mathbf{M}_{m,n}(\mathbb{Z})$  специального вида I:

$$C = \left( \begin{array}{c|ccc} d_1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & C^* & \\ 0 & & & \end{array} \right),$$

где  $C^* \in \mathbf{M}_{(m-1),(n-1)}(\mathbb{Z})$  и  $d_1$  делит каждый элемент матрицы  $C^*$ .

Опишем конечное число элементарных преобразований строк и столбцов матрицы, которые:

1) либо приводят к матрице вида I;

2) либо приводят к матрице  $B = (b_{ij}) \in \mathbf{M}_{m,n}(\mathbb{Z})$ , удовлетворяющей условию

$$|b_{11}| < |a_{11}| \quad (*)$$

(повторяя эту процедуру, после конечного числа шагов придем к виду I).

Если  $A$  — нулевая матрица, то мы уже имеем вид I.

Если  $A$  — ненулевая матрица, то, переставляя строки и столбцы при необходимости, можно считать, что  $a_{11} \neq 0$ .

Имеются три следующие возможности.

СЛУЧАЙ 1: существует такой элемент  $a_{1j}$  в первой строке, что  $a_{11} \mid a_{1j}$ , пусть  $a_{1j} = a_{11}q + r$ ,  $|r| < |a_{11}|$ . Вычитая из  $q$ -го столбца 1-й столбец, умноженный на  $q$ , и переставляя 1-й и  $q$ -й столбцы, приходим к матрице  $B = (b_{ij})$ , в которой

$$|b_{11}| = |r| < |a_{11}|,$$

т. е. выполнено условие (\*).

СЛУЧАЙ 2: в первом столбце существует такой элемент  $a_{i1}$ , что  $a_{11} \mid a_{i1}$ . Поступая как и в случае 1, но со строками, приходим к матрице  $B = (b_{ij})$ , где

$$|b_{11}| = |r| < |a_{11}|$$

(т. е. выполнено условие (\*)).

СЛУЧАЙ 3: элемент  $a_{11}$  делит все элементы 1-й строки и все элементы 1-го столбца. Совершая соответствующие элементарные преобразования первого типа со строками и столбцами, приходим к матрице вида

$$\left( \begin{array}{c|ccc} a_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & D^* & \\ 0 & & & \end{array} \right).$$

Если элемент  $a_{11}$  делит все элементы матрицы  $D^*$ , то мы пришли к матрице вида I. В противном случае найдется элемент  $d_{ij}$  такой, что  $a_{11} \nmid d_{ij}$ ,  $1 < i$ ,  $1 < j$ . Прибавляя  $i$ -ю строку к 1-й строке, мы приходим к случаю 1.

После конечного числа шагов приходим к матрице вида I.

*Завершение редукции:* элементарные преобразования строк и столбцов матрицы  $C^*$  реализуются элементарными преобразованиями строк и столбцов матрицы  $C$ , все новые элементы в последующих преобразованиях матрицы  $C^*$  делятся на  $d_1$ . Таким образом приходим к матрице  $D = \text{diag}(d_1, d_2, \dots, d_u) \in \mathbf{M}_{m,n}(\mathbb{Z})$ , где  $d_1 \mid d_2 \mid \dots \mid d_u$ .

2) Пусть  $1 \leq i \leq \min(m, n) = u$ .

Рассмотрим идеал  $J_i(A)$  кольца целых чисел  $\mathbb{Z}$ , порожденный всеми  $(i \times i)$ -минорами (т. е. определителями  $(i \times i)$ -подматриц) матрицы  $A$ . Тогда:

(1) если  $B \sim A$ , то  $J_i(A) = J_i(B)$  для всех  $1 \leq i \leq u$ ;

(2)  $J_i(A) = J_i(D) = \mathbb{Z}(d_1 d_2 \dots d_i)$  (используя диагональную форму матрицы).

Если  $u = \min(m, n)$ ,  $D' = \text{diag}(d'_1, d'_2, \dots, d'_u) \in \mathbf{M}_{m,n}(\mathbb{Z})$ ,  $D' \sim A$ ,  $d'_1 \mid d'_2 \mid \dots \mid d'_u$ ,  $d'_i \in \mathbb{N} \cup \{0\}$ , то  $D' \sim A \sim D_i$ , и поэтому  $D' \sim D_i$ , следовательно,

$$\mathbb{Z}(d'_1 d'_2 \dots d'_i) = J_i(D') = J_i(D) = \mathbb{Z}(d_1 d_2 \dots d_i).$$

Таким образом,

$$d'_1 d'_2 \dots d'_i = d_1 d_2 \dots d_i \text{ для всех } 1 \leq i \leq u.$$

Итак, последовательно:

$$d'_1 = d_1; \quad d'_1 d'_2 = d_1 d_2, \dots$$

(при этом если  $d'_1 = d_1 \neq 0$ , то из этого следует, что  $d'_2 = d_2$ , если же  $d'_1 = d_1 = 0$ , то все кратные  $d'_2 = \dots = d'_u = d_2 = \dots = d_u = 0$ ).

В итоге получаем, что всегда  $d'_1 = d_1, d'_2 = d_2, \dots, d'_u = d_u$ .  $\square$

## ДЕЙСТВИЯ ГРУППЫ НА МНОЖЕСТВЕ (ПОЛИГОНЫ)

Различные группы преобразований дают естественные и многочисленные примеры действия групп на множествах. Это обосновывает рассмотрение *левого полигона  $M$  над группой  $G$*  (или *левого  $G$ -полигона*, обозначение  $M_G$ ): множества  $M$  и отображения  $G \times M \rightarrow M$ , при котором  $(g, t) \rightarrow gt$ ,  $t \in M$ ,  $g \in G$ , при этом

- 1)  $(gh)t = g(ht)$  для всех  $t \in M$ ,  $g, h \in G$ ;
- 2)  $et = t$  для  $t \in M$  и нейтрального элемента  $e \in G$ .

Если  $\mathbf{S}(M)$  — группа подстановок на множестве  $M$ , т. е. группа всех биекций  $\sigma: M \rightarrow M$  с операцией композиции, то задание структуры полигона  $M_G$  равносильно заданию гомоморфизма групп

$$\varphi: G \rightarrow \mathbf{S}(M).$$

**ОПРЕДЕЛЕНИЕ 1.** *Орбитой* элемента  $t$  полигона  $M_G$  над группой  $G$  назовем следующее подмножество в  $M$ :

$$\text{Orb}(t) = \{gt \mid g \in G\} (= Gt).$$

**ЗАМЕЧАНИЕ 3.**  $y \in \text{Orb}(t) \iff \text{Orb}(y) = \text{Orb}(t)$ .

Действительно, если  $y = gt$ , то  $hy = hgt$  для  $h \in G$ , т. е.  $Gy \subseteq Gt$ . Так как  $t = g^{-1}y$ , то  $Gt \subseteq Gy$ . Итак,  $Gy = Gt$ . Если  $Gy = Gt$ , то  $y = ey \in Gy = Gt$ .

ЗАМЕЧАНИЕ 4. Отношение  $y \sim x \iff y = gx, g \in G$  (т. е.  $y \sim x \iff \text{Orb}(y) = \text{Orb}(x)$ ) является отношением эквивалентности.

Действительно,

1)  $x = ex$ , т. е.  $x \sim x$ ;

2) если  $z \sim y, y \sim x$ , т. е.  $z = hy, y = gx, h, g \in G$ , то  $z = hgx$ , т. е.  $z \sim x$ ;

3) если  $y \sim x$ , т. е.  $y = gx, g \in G$ , то  $x = g^{-1}y$ , т. е.  $x \sim y$ .

**Теорема 2** (разбиение на непересекающиеся орбиты). Если  $M_G$  — полигон над группой  $G$ , то  $M_G$  является объединением непересекающихся орбит:  $M_G = \bigcup_i \text{Orb}(m_i)$ , где  $m_i$  — представители орбит (т. е. выбранные по одному элементу в каждой орбите).

**Следствие 1.** Если  $|M_G| < \infty$ , то

$$|M_G| = |\text{Orb}(m_1)| + \dots + |\text{Orb}(m_k)|,$$

где  $m_1, \dots, m_k$  — представители орбит.

*Доказательство.* вытекает из рассмотрения отношения эквивалентности:  $y \sim x \iff \text{Orb}(y) = \text{Orb}(x)$ . □

ЗАМЕЧАНИЕ 5. Если  $M_G = \text{Orb}(m), m \in G$  (т. е. имеется единственная орбита), то будем говорить, что группа  $G$  действует транзитивно.

ОПРЕДЕЛЕНИЕ 2. Если  $p \in M_G$ , то стабилизатором элемента  $p$  назовем следующее подмножество группы  $G$ :

$$\text{St}(p) = \{g \in G \mid gp = p\}.$$

**Теорема 3.** Пусть  $p \in M_G$ . Тогда():

1) стабилизатор  $\text{St}(p)$  элемента  $p \in G$  является подгруппой группы  $G$ ;

2) соответствие между смежными классами  $\text{St}(p)a$ ,  $a \in G$ , и элементами  $pa \in Gp = \text{Orb}(p)$  является биекцией;

3) если  $|G| = n < \infty$ , то  $|G| = |\text{Orb}(p)| \cdot |\text{St}(p)|$  (и следовательно,  $|\text{Orb}(p)|$  и  $|\text{St}(p)|$  — делители числа  $n = |G|$ , при этом  $|\text{Orb}(p)| = \frac{|G|}{|\text{St}(p)|}$ ).

*Доказательство.*

1) Если  $g, h \in \text{St}(p)$  т. е.  $gp = p$  и  $hp = p$ , то  $hgp = hp = p$ , и поэтому  $hg \in \text{St}(p)$ . Если  $g \in \text{St}(p)$ , т. е.  $gp = p$ , то  $g^{-1}p = g^{-1}gp = ep = p$ , и поэтому  $g^{-1} \in \text{St}(p)$ . Ясно, что  $ep = p$ , т. е.  $e \in \text{St}(p)$ , т. е.  $\text{St}(p) \neq \emptyset$ . Таким образом,  $\text{St}(p)$  — подгруппа группы  $G$ .

2) Если  $a, b \in G$ , то

$$ap = bp \iff b^{-1}ap = p \iff b^{-1}a \in \text{St}(p) \iff a \text{St}(p) = b \text{St}(p).$$

Таким образом, установлена биекция между различными элементами орбиты  $Gp = \text{Orb}(p)$  и множеством различных смежных классов  $a \text{St}(p)$  по подгруппе  $\text{St}(p)$ :  $ap \leftrightarrow a \text{St}(p)$ .

В силу 2) число различных смежных классов по подгруппе  $\text{St}(p)$  совпадает с  $|\text{Orb}(p)|$ . Применяя теорему Лагранжа, получаем:  $|G| = |\text{Orb}(p)| \cdot |\text{St}(p)|$ . В частности,  $|\text{Orb}(p)| = \frac{|G|}{|\text{St}(p)|}$ .  $\square$

**Лемма 4.** Если  $p' = ap \in \text{Orb}(p)$ ,  $p \in M_G$ , то:

1)  $a \text{St}(p) = \{g \in G \mid gp = p'\}$ ;

2)  $\text{St}(p') = a \text{St}(p)a^{-1}$  (т. е.  $\text{St}(p')$  — подгруппа, сопряженная с подгруппой  $\text{St}(p)$ ).

*Доказательство.*

1) Фактически, это уже было проверено в предыдущей теореме:

$$\begin{aligned} gp = p' &\iff gp = ap \iff a^{-1}gp = p \iff \\ &\iff a^{-1}g \in \text{St}(p) \iff g \in a \text{St}(p). \end{aligned}$$

2) Действительно,

$$\begin{aligned} g \in \text{St}(p') &\iff gap = ap \iff a^{-1}gap = p \iff \\ &\iff a^{-1}ga \in \text{St}(p) \iff g \in a \text{St}(p)a^{-1}. \quad \square \end{aligned}$$

## ПРИМЕРЫ ПОЛИГОНОВ

ПРИМЕР 2.  $M_G = \{1, 2, \dots, n\}_{S_n}$ , где  $\sigma i$  — значение подстановки  $\sigma \in S_n$  на элементе  $i$  из  $\{1, 2, \dots, n\}$ . Так как  $i(i, j) = j$  для цикла  $(i, j)$ , то это действие группы  $\mathbf{S}_n$  на  $\{1, 2, \dots, n\}$  транзитивно. Ясно, что, например,  $\text{St}(n) = \mathbf{S}_{n-1}$ . Более общим образом, для любого множества  $M$  и группы всех биекций  $\mathbf{S}(M)$  имеем полигон  $M_{\mathbf{S}(M)}$ .

ПРИМЕР 3. Пусть  $\sigma \in \mathbf{S}_n$ ,  $(\sigma)$  — циклическая подгруппа в  $\mathbf{S}_n$ , порожденная подстановкой  $\sigma$ . Тогда:  $\{1, 2, \dots, n\}_{(\sigma)}$  — полигон над группой  $(\sigma)$ , его различные орбиты — это в точности непересекающиеся циклы подстановки  $(\sigma)$ , перестановочные между собой.

ПРИМЕР 4 (РЕГУЛЯРНОЕ ПРЕДСТАВЛЕНИЕ ЛЕВЫМИ УМНОЖЕНИЯМИ). Пусть  $M_G = G_G$  с умножением  $(g, x) \rightarrow gx$  для  $x \in G$ ,  $g \in G$ . Ясно, что:  $(hg)x = h(gx)$  (для  $x, g, h \in G$ , ассоциативность умножения в группе);  $ex = x$  для единицы  $e$  группы  $G$ .

Если  $p, x \in G$ , то  $\text{St}(p) = \{g \in G \mid gp = p\} = \{e\}$  и  $\text{Orb}(x) = Gx = G$  (т. е. это действие транзитивно).

Если  $g \in G$ , то рассмотрим отображение  $\rho_g: G \rightarrow G$ ,  $\rho_g x = gx$ . Так как из  $gx = gy$  для  $x, y \in G$  следует (умножим на  $g^{-1}$  справа в группе  $G$ ), что  $x = y$ , то  $\rho_g$  — мономорфизм. Так как для любого  $z \in G$  имеем  $z = gg^{-1}z$ , то  $\rho_g$  — сюръекция.

Итак,  $\rho_g \in \mathbf{S}(G)$ .

Так как для  $x, g, h \in G$  имеем

$$\rho_{hg}x = (hg)x = h(gx) = \rho_h(\rho_g x),$$

т. е.  $\rho_{hg} = \rho_h \rho_g$ , то отображение  $\rho: G \rightarrow \mathbf{S}^r(G)$ ,  $\rho(g) = \rho_g$ , является гомоморфизмом групп.

Если  $g, g' \in G$  и  $\rho_g = \rho(g) = \rho(g') = \rho_{g'}$ , то  $g = eg = eg' = g'$ .

Таким образом,  $\rho$  — инъективный гомоморфизмом.

Итак, мы доказали следующее утверждение.

**Теорема 4** (Кэли). *Регулярное представление группы  $G$  правыми умножениями*

$$G \xrightarrow{\rho} \mathbf{S}^{\Gamma}(G) = \mathbf{S}(G), \quad g \rightarrow \rho_g, \quad \rho_g x = gx,$$

*является инъективным гомоморфизмом.*

**Следствие 2.** *Всякая группа  $G$  изоморфна некоторой подгруппе  $G'$  группы подстановок  $\mathbf{S}(G)$  на множестве  $G$ .*

**Следствие 3.** *Если  $n = |G| < \infty$ , то группа  $G$  изоморфна некоторой подгруппе  $G'$  группы подстановок  $\mathbf{S}_n$ . С точностью до изоморфизма существует лишь конечное число групп порядка  $n$ .*

**ЗАМЕЧАНИЕ 6.** К сожалению,  $|\mathbf{S}_n| = n!$ , и подгрупп в  $\mathbf{S}_n$  из  $n$  элементов достаточно много.

ПРИМЕР 5. Пусть  $H$  — подгруппа группы  $G$ , рассмотрим полигон

$$M_H = G_H, \quad (hx) \rightarrow hx \text{ для } x \in G, h \in H.$$

Если  $p, x \in G$ , то

$$\text{St}(p) = \{h \in H \mid hp = p\} = \{e\}$$

и  $\text{Orb}(x) = Hx$  — левый смежный класс  $Hx$  по подгруппе  $H$ , порожденный элементом  $x \in G$ .

Таким образом, в этом частном случае полигона  $G_H$  разбиение на орбиты превращается в хорошо знакомое нам разбиение группы в объединение непересекающихся различных левых смежных классов  $G = \dot{\bigcup} Hx$ , и как следствие подсчета элементов по орбитам имеем

$$|G| = \sum |\text{Orb}(x)| = \sum |Hx| = [G : H]|H|$$

(т. е. теорему Лагранжа).

ПРИМЕР 6 (ДЕЙСТВИЕ ГРУППЫ  $G$  ЛЕВЫМИ УМНОЖЕНИЯМИ НА МНОЖЕСТВЕ ПРАВЫХ СМЕЖНЫХ КЛАССОВ). Пусть  $H$  — подгруппа группы  $G$ ,

$$M_G = \{xH, x \in G\}, \quad g(xH)g = gxH \quad \text{для } x, g \in G.$$

Это умножение корректно:

если  $xH = x'H$ , то  $x' = xh$ ,  $h \in H$ , и поэтому  $gx' = gxh$ , тогда  $gx'H = gxH$ .

Если  $x, g_1, g_2 \in G$ , то  $(g_1g_2)(xH) = g_1(g_2(xH))$  и  $e(xH) = xH$ , т. е.  $M_G = \{xH \mid x \in G\}_G$  — правый полигон над группой  $G$ .

Так как  $\text{Orb}(xH) = M_G$ , то это действие группы  $G$  транзитивно.

ПРИМЕР 7 (ДЕЙСТВИЕ ГРУППЫ  $G$  НА ГРУППЕ  $G$  СОПРЯЖЕНИЕМ). Пусть  $M_G = G_G$ ,  $(g, m) \rightarrow gmg^{-1} = \alpha_g m$  для  $m, g \in G$ .

Так как для  $m, g, h \in G$  имеем

$$m\alpha_{hg} = (hg)m(hg)^{-1} = h(gmg^{-1})h^{-1} = \alpha_h(\alpha_g m),$$

т. е.  $\alpha_{hg} = \alpha_h\alpha_g$ ,

$$\alpha_e m = em e^{-1} = m,$$

то  $M_G = G_G$  с сопряжением — левый  $G$ -полигон.

## КЛАССЫ СОПРЯЖЕННЫХ ЭЛЕМЕНТОВ

Если  $x \in G$ , то при сопряжении орбита элемента

$$\text{Orb}(x) = \{gxg^{-1} \mid g \in G\}$$

— это класс сопряженных элементов элемента  $x$ .

Ясно, что  $\text{Orb}(e) = \{e\}$ . Более того,  $|\text{Orb}(x)| = 1 \iff x \in \mathbf{Z}(G)$ , т. е. одноэлементные орбиты — это в точности элементы центра, поскольку  $gxg^{-1} = x$  для всех  $g \in G$  равносильно тому, что  $xg = gx$  для всех  $g \in G$ , т. е. тому, что  $x \in \mathbf{Z}(G)$ .

Ясно, что

$$\text{St}(x) = \{g \mid gxg^{-1} = x\} = \mathbf{C}(x),$$

где  $\mathbf{C}(x) = \{y \in G \mid xy = yx\}$  — централизатор элемента  $x \in G$ .

Таким образом, теорема о разбиении на орбиты в данном случае означает следующее.

**Теорема 5** (о разбиении на классы сопряженных элементов). Пусть  $G$  — группа, тогда:

1) группа является объединением орбит — непересекающихся различных классов сопряженных элементов (т. е. отношение сопряженности  $y \sim x$ , если  $y = gxg^{-1}$ , является отношением эквивалентности);

2) число элементов конечной группы  $G$ , сопряженных с элементом  $x \in G$ , равно индексу централизатора  $\mathbf{C}(x)$  элемента  $x \in G$  в группе (поскольку  $|G| = |\text{Orb}(x)| \cdot |\text{St}(x)| = \{\text{число сопряженных с } x \text{ элементов}\} \cdot |\mathbf{C}(x)|$ ), т. е. числу  $|G|/|\mathbf{C}(x)|$ , и является делителем числа  $|G|$ .  $\square$

## ЦЕНТР КОНЕЧНОЙ $p$ -ГРУППЫ

**Теорема 6.** *Фактор неабелевой группы по ее центру не может быть циклической группой.*

*Доказательство.* Предположим, что это не так, т. е. существует некоторая неабелева группа  $G$  такая, что  $G/\mathbf{Z}(G) = G/Z$  — циклическая группа. Пусть тогда  $G/Z = \langle gZ \rangle$ . В этом случае любой элемент группы  $G$  представляется в виде произведения  $g^k z$ , где  $z \in Z$ .

Рассмотрим два произвольных элемента группы  $G$  —  $g^k z_1$  и  $g^l z_2$ . Они коммутируют, так как элементы центра коммутируют со всеми элементами группы, а степени элемента  $g$  коммутируют между собой.

Таким образом, группа  $G$  — абелева, что противоречит предположению.  $\square$

**Теорема 7.** *Пусть  $G$  — конечная  $p$ -группа, т. е.  $|G| = p^k$ , где  $p$  — простое число,  $k \in \mathbb{N}$ . Тогда ее центр нетривиален, т. е.  $|\mathbf{Z}(G)| > 1$ .*

*Доказательство.* Рассмотрим разбиение группы  $G$  на классы сопряженных элементов. Одноэлементный класс — это в точности элемент центра (один из них  $\{e\}$ ). Содержащий больше одного элемента класс сопряженных элементов содержит  $p^l$  элементов, где  $l > 1$  (как нетривиальный делитель числа  $|G| = p^k$ ). Отсюда следует, что  $|\mathbf{Z}(G)| > 1$  (в противном случае  $p^k = 1 + pq$ ).  $\square$

**Теорема 8** (о коммутативности группы из  $p^2$  элементов). Пусть  $G$  — конечная группа,  $|G| = p^2$ , где  $p$  — простое число. Тогда  $G$  — абелева группа.

*Доказательство.* В силу предыдущей теоремы  $|\mathbf{Z}(G)| > 1$ , т. е.  $|\mathbf{Z}(G)| = p$  или  $|\mathbf{Z}(G)| = p^2$ . Но первый случай ( $|\mathbf{Z}(G)| = p$ ) невозможен, поскольку тогда  $|G/\mathbf{Z}(G)| = p^2/p = p$ , и поэтому  $G/\mathbf{Z}(G)$  — циклическая группа, что невозможно. Итак,  $|\mathbf{Z}(G)| = p^2$ , т. е.  $G = \mathbf{Z}(G)$ , и поэтому группа  $G$  коммутативна.  $\square$