ЛЕКЦИЯ 7

ПОДГРУППЫ СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ

ПРЕОБРАЗОВАНИЯ БАЗИСА

ДЕЙСТВИЯ ГРУПП НА МНОЖЕСТВАХ

ОРБИТЫ, СТАБИЛИЗАТОРЫ

ПРИМЕРЫ ДЕЙСТВИЙ

ПОДГРУППЫ СВОБОДНЫХ АБЕЛЕВЫХ ГРУПП

Рассмотрим подгруппы свободной абелевой группы конечного ранга (это расширяет нашу информацию о подгруппах бесконечной циклической группы).

Теорема 1. *Ненулевая подгруппа B свободной абелевой группы F_n конечного ранга n является свободной абелевой группой ранга m, $B \cong F_m$, где $1 \leq m \leq n$.*

Доказательство. проведем индукцией по n.

Случай $n = 1$: $F_1 \cong \mathbb{Z}$; ненулевая подгруппа B в $\mathbb{Z}$ имеет вид $\mathbb{Z}k$, $0 \neq k \in \mathbb{Z}$, поэтому $B \cong \mathbb{Z}$, и следовательно, B является свободной абелевой группой ранга $m = 1 = n$.

Пусть наше утверждение верно для всех рангов $n' < n$, $n > 1$, B — ненулевая подгруппа группы

$$F_n = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1} \oplus \mathbb{Z}e_n,$$

где $\{e_1, \ldots, e_n\}$ — один из базисов свободной абелевой группы F_n. Рассмотрим короткую точную последовательность абелевых групп

$$0 \to \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1} \xrightarrow{i} F_n \xrightarrow{\pi} \mathbb{Z}e_n \to 0,$$

где i — естественное вложение, $\pi(k_1e_1 + \ldots + k_ne_n) = k_ne_n$ (т. е. π — естественная проекция на прямое слагаемое $\mathbb{Z}e_n$, $\ker\pi = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1}$). Рассмотрим ограничение $\pi|_B\colon B \to \mathbb{Z}e_n$ гомоморфизма π на подгруппу B. Так как

$$\ker(\pi|_B) = B \cap \ker\pi = B \cap (\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1}),$$

то короткая точная последовательность абелевых групп

$$0 \to B \cap (\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n) \to B \xrightarrow{\pi|_B} \pi(B) \to 0$$

является точной.

В силу индуктивного предположения для подгруппы $B \cap (\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1})$ группы $F_{n-1} = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1}$ имеем

$$B \cap (\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1}) \cong F_l,$$

где $l \leq n-1$.

Если $\pi(B) = 0$, то

$$B \subseteq \ker \pi = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1},$$

и в силу нашего индуктивного предположения для $n' = n-1 < n$: $B \cong F_m$, $m \leq n-1 < n$.

Если

$$0 \neq \pi(B) \subseteq \mathbb{Z}e_n \cong \mathbb{Z} = F_1,$$

то

$$\pi(B) \cong \mathbb{Z}t \subseteq \mathbb{Z}, \quad 0 \neq t \in \mathbb{Z},$$

и поэтому $\pi(B) \cong \mathbb{Z} = F_1$ — свободная абелева группа ранга 1. В силу расщепляющего свойства свободной абелевой группы:

$$B = C \oplus \big(B \cap (\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1})\big),$$

где $C \cong \pi(B) \cong F_1$. Итак, $B \cong F_1 \oplus F_l = F_{l+1}$, где $l+1 \leq (n-1)+1 = n$. $\square$

Важным следствием из доказанной теоремы является следующее утверждение о строении подгрупп конечно порожденных абелевых групп.

Теорема 2 (о подгруппах конечно порожденных абелевых групп). *Пусть $A = \langle a_1, \ldots, a_n \rangle$ — конечно порожденная абелева группа с системой образующих $\{a_1, \ldots, a_n\}$ из n элементов. Тогда любая подгруппа H группы A является конечно порожденной абелевой группой, при этом группа A обладает системой образующих из m элементов, где $m \leq n$.*

Доказательство. Рассмотрим свободную абелеву группу F_n ранга n с базисом $\{e_1, \ldots, e_n\}$ и сюръективный гомоморфизм

$$F_n \xrightarrow{\pi} A \to 0,$$

для которого $\pi(e_i) = a_i$, $1 \le i \le n$. Так как $H \subseteq A$, то рассмотрим подгруппу $B = \pi^{-1}(H)$ свободной абелевой группы F_n. В силу теоремы 1 $B \cong F_m$, где $m \le n$.

Если $\{f_1, \ldots, f_m\}$ — базис свободной абелевой группы $B \cong F_m$, то

$$H = \pi\big(\pi^{-1}(H)\big) = \pi(B) = \pi(\langle f_1, \ldots, f_m\rangle) = \langle \pi(f_1), \ldots, \pi(f_m)\rangle. \qquad \square$$

ЗАДАНИЕ 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 $A = \langle a_1, \ldots, a_n\rangle$ каждый элемент $x \in A$ записывается (в аддитивной форме) как

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

Замечание 1 (о задании конечно порожденной абелевой группы образующими и соотношениями). Пусть $A = \langle a_1, \ldots, a_n\rangle$ — конечно порожденная абелева группа, $\{a_1, \ldots, a_n\}$ — одна из ее систем образующих;

$$\pi\colon F_n = \langle e_1, \ldots, e_n\rangle \to A = \langle a_1, \ldots, a_n\rangle —$$

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

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

B — свободная абелева группа, $\{b_1, \ldots, b_m\}$ — ее базис, $m \le n$; $b_j = \sum\limits_{i=1}^{n} r_{ij} e_i$, $r_{ij} \in \mathbb{Z}$, $R = (r_{ij}) \in \mathbf{M}_{n,m}(\mathbb{Z})$ — матрица соотношений между образующи-

ми $a_1, \ldots, a_n$. Тогда целочисленная матрица $R = (r_{ij}) \in \mathbf{M}_{n,m}(\mathbb{Z})$ полностью определяет абелеву группу A как фактор-группу:

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

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 $a_1, \ldots, a_n$. При этом если

$$k_1 a_1 + \ldots + k_n a_n = 0 —$$

любое другое соотношение между группами $a_1, \ldots, a_n$, то

$$\pi(k_1 e_1 + \ldots + k_n e_n) = k_1 a_1 + \ldots + k_n a_n = 0,$$

и поэтому

$$k_1 e_1 + \ldots + k_n e_n \in \ker \pi = \langle b_1, \ldots, b_m \rangle.$$

Следовательно, элемент $k_1 e_1 + \ldots + k_n e_n$ является линейной комбинацией элементов $b_1, \ldots, b_m$. Таким образом, соотношения $b_1, \ldots, b_m$ определяют все соотношения между элементами $a_1, \ldots, a_n$. □

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

$$0 \to \ker \pi \to F_n \to A = \langle a_1, \ldots, a_n \rangle \to 0,$$

а именно, с переходом от исходных базисов $\{e_1, \ldots, e_n\}$ и $\{b_1, \ldots, b_m\}$ соответственно к новым базисам $\{e'_1, \ldots, e'_n\}$ и $\{b'_1, \ldots, b'_m\}$, 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 $A \in \mathrm{GL}_n(\mathbb{Z})$. □

Пример 1. Следующие матрицы называются *элементарными матрицами* в группе $\mathrm{GL}_n(\mathbb{Z})$:

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

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

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

1) матрица $e_{ij}A$ 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 $\mathrm{diag}\,(d_1, \ldots, d_m)A$ получается из матрицы A умножением i-й строки на d_i, $1 \leq i \leq m$, $d_i = \pm 1 \in \mathbb{Z}$. □

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

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

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

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

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

Доказательство.

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

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

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

1б) Если

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

то

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

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

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

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

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

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

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

Тогда

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

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

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

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

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

Пусть $\{e_1, \ldots, e_n\}$, $\{e'_1, \ldots, e'_n\}$ — 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 $\{e_1, \ldots, e_n\}$ ко второму базису $\{e'_1, \ldots, e'_n\}$ в F_n.

Рассмотрим эндоморфизм $\xi\colon F_n \to F_n$, $\xi \in \operatorname{End}(F_n)$, для которого

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

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

Лемма 3. *Пусть F_n — свободная абелева группы конечного ранга n, $\{e_1, \ldots, e_n\}$ и $\{e'_1, \ldots, e'_n\}$ — 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 $\{e_1, \ldots, e_n\}$ к базису $\{e'_1, \ldots, e'_n\}$, $\alpha \in \operatorname{End}(F_n)$, $A = (a_{ij}) \in \mathbf{M}_n(\mathbb{Z})$ — его матрица в базисе $\{e_1, \ldots, e_n\}$, $A' = (a'_{ij}) \in \mathbf{M}_n(\mathbb{Z})$ — его матрица в базисе $\{e'_1, \ldots, e'_n\}$. Тогда

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

Доказательство. Так как для автоморфизма

$$\xi \colon F_n \to F_n, \quad \xi(e_j) = e'_j, \quad j = 1, \ldots, n,$$

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

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

то матрица эндоморфизма $\xi^{-1}\alpha\xi$ в базисе $\{e_1, \ldots, e_n\}$ 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 $A = U^{-1}BV^{-1}$, $U^{-1} \in \mathrm{GL}_m(\mathbb{Z})$, $V^{-1} \in \mathrm{GL}_n(\mathbb{Z})$, и поэтому $A \sim B$;

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

$$C = U'BV' = U'(UAV)V' = (U'U)A(VV'),$$

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

Теорема 3 (алгоритм приведения прямоугольной целочисленной матрицы к каноническому эквивалентному диагональному виду).

1) *Любая прямоугольная целочисленная $(m \times n)$-матрица $A \in \mathbf{M}_n(\mathbb{Z})$ эквивалентна диагональной $(m \times n)$-матрице*

$$D = \mathrm{diag}\,(d_1, \ldots, d_u) = {}_m \overset{n}{\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_u \end{pmatrix}}_{u=m\le n} = \text{или} =$$

$$= {}_m \overset{n}{\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_u \\ & & \end{pmatrix}}_{u=n\le m} \in \mathbf{M}_n(\mathbb{Z}),$$

где $u = \min\{m, n\}$ и $d_1 \mid d_2 \mid \ldots \mid d_u$, $d_i \in \mathbb{N} \cup \{0\}$ ($D \sim A$, D — канонический вид матрицы A).

2) *Канонический вид $D = \mathrm{diag}\,(d_1, \ldots, d_u)$ матрицы A определен однозначно.*

Доказательство. теоремы является, фактически, описанием алгоритма приведения целочисленной прямоугольной матрицы к каноническому диагональному виду. Ключевой момент этого алгоритма — алгоритм Евклида в кольце целых чисел $\mathbb{Z}$ (другими словами, $\mathbb{Z}$ — евклидово кольцо с евклидовой функцией $\mathbb{Z} \ni n \mapsto |n| \in \mathbb{N} \cup \{0\}$).

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

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

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

Если A — нулевая матрицы, 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, придчм 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 найдчтся элемент d_{ij} такой, что $a_{11} \mid d_{ij}$, $1 < i, 1 < j$. 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 $D = \operatorname{diag}(d_1, d_2, \dots, d_u) \in \mathbf{M}_{m,n}(\mathbb{Z})$, 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 $u = \min(m, n)$, $D' = \operatorname{diag}(d'_1, d'_2, \dots, d'_u) \in \mathbf{M}_{m,n}(\mathbb{Z})$, $D' \sim A$, $d'_1 \mid d'_2 \mid \dots \mid d'_u$, $d'_i \in \mathbb{N} \cup \{0\}$, 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,

$$d'_1 d'_2 \dots d'_i = d_1 d_2 \dots d_i$$

для всех $1 \leq i \leq u$.

Итак, последовательно:

$$\begin{aligned} d'_1 &= d_1; \\ d'_1 d'_2 &= d_1 d_2, \end{aligned}$$

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 $d'_2 = \ldots = d'_u = d_2 = \ldots = d_u = 0$;

$$\vdots$$

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

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 $G \times M \to M$, при котором $(g, m) \to gm$, $m \in M$, $g \in G$, при этом

1) $(gh)m = g(hm)$ для всех $m \in M$, $g, h \in G$;
2) $em = m$ для $m \in M$ и нейтрального элемента $e \in G$.

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

$$\varphi\colon G \to \mathbf{S}(M).$$

Определение 1. Орбитой элемента m полигона M_G над группой G назовем следующее подмножество в M:

$$\mathrm{Orb}\,(m) = \{gm \mid g \in G\}\ (= Gm).$$

Замечание 3. $y \in \operatorname{Orb}(m) \iff \operatorname{Orb}(y) = \operatorname{Orb}(m)$.

Действительно, если $y = gm$, то $hy = hgm$ для $h \in G$, т. е. $Gy \subseteq Gm$. Так как $m = g^{-1}y$, то $Gm \subseteq Gy$. Итак, $Gy = Gm$. Если $Gy = Gm$, то $y = ey \in Gy = Gm$.

Замечание 4. Отношение $y \sim x \iff y = gx,\ g \in G$ (т. е. $y \sim x \iff \operatorname{Orb}(y) = \operatorname{Orb}(x)$) 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 4 (разбиение на непересекающиеся орбиты). *Если M_G — полигон над группой G, то M_G является объединением непересекающихся орбит: $M_G = \dot{\bigcup\limits_i} \operatorname{Orb}(m_i)$, где m_i — представители орбит (т. е. выбранные по одному элементу в каждой орбите).*

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

$$|M_G| = |\operatorname{Orb}(m_1)| + \ldots + |\operatorname{Orb}(m_k)|,$$

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

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

Замечание 5. Если $M_G = \operatorname{Orb}(m)$, $m \in G$ (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:

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

Теорема 5. *Пусть $p \in M_G$. Тогда():*

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

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

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

Доказательство.

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

2) Если $a, b \in G$, то

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

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

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

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

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

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

Доказательство.

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

$$gp = p' \iff gp = ap \iff a^{-1}gp = p \iff a^{-1}g \in \mathrm{St}\,(p) \iff g \in a\,\mathrm{St}\,(p).$$

2) Действительно,

$$g \in \mathrm{St}\,(p') \iff gap = ap \iff a^{-1}gap = p \iff a^{-1}ga \in \mathrm{St}\,(p) \iff g \in a\,\mathrm{St}\,(p)a^{-1}.$$

□

ПРИМЕРЫ ПОЛИГОНОВ

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

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