ЛЕКЦИЯ 8

АБЕЛЕВЫ ГРУППЫ БЕЗ КРУЧЕНИЯ

СТРУКТУРНАЯ ТЕОРЕМА

ПОДГРУППЫ СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ

ЗАДАНИЕ АБЕЛЕВОЙ ГРУППЫ ОБРАЗУЮЩИМИ И СООТНОШЕНИЯМИ

АБЕЛЕВЫ ГРУППЫ БЕЗ КРУЧЕНИЯ

Теорема 1 (о свободе конечно порожденной абелевой группы без кручения)**.** *Конечно порожденная абелева группа A является свободной абелевой группой тогда и только тогда, когда A — абелева группа без кручения (другими словами, когда ее периодическая часть равна нулю, $\mathbf{T}(A) = 0$).*

Доказательство. 1) Мы отмечали выше, что свободная абелева группа A не имеет кручения ($\mathbf{T}(A) = 0$).

2) Пусть $A = \langle a_1, \ldots, a_n \rangle$ — конечно порожденная абелева группа и $\mathbf{T}(A) = 0$. Проведем доказательство свободы группы A индукцией по n. Начало индукции: $n = 1$, $A = \langle a_1 \rangle \cong \mathbb{Z} = F_1$, поскольку $O(a_1) = \infty$.

Пусть $n > 1$. Если $\{a_1, \ldots, a_n\}$ — базис абелевой группы A, то $A = F_n$, и наше утверждение доказано.

Допустим теперь, что система образующих $\{a_1, \ldots, a_n\}$ линейно зависима над $\mathbb{Z}$ и

$$k_1 a_1 + \ldots + k_n a_n = 0, \quad k_i \in \mathbb{Z}, — \qquad (*)$$

нетривиальное линейное соотношение между элементами $a_1, \ldots, a_n$ (это означает, что хотя бы один из коэффициентов k_i ненулевой). Пусть $d = \text{НОД}(k_1, \ldots, k_n)$, $k_i = dk_i'$, $i = 1, \ldots, n$. Тогда

$$d(k_1' a_1 + \ldots + k_n' a_n) = 0.$$

Так как $d \neq 0$ и A — абелева группа без кручения, то

$$k_1'a_1 + \ldots + k_n'a_n = 0, \quad (k_1', \ldots, k_n') = 1.$$

Итак, можно считать, что

$$(k_1, k_2, \ldots, k_n) = 1.$$

Если $k_1 = 1$, то

$$a_1 = -(k_2a_2 + \ldots + k_na_n),$$

и поэтому в силу индуктивного предположения абелева группа $A = \langle a_2, \ldots, a_n \rangle$ свободна. Аналогично, A — свободная абелева группа, если $k_1 = -1$.

Далее, мы будем менять систему образующих с целью получить в соотношении между новыми образующими один из коэффициентов равным ± 1.

Если $k_2 = \ldots = k_n = 0$, то $k_1a_1 = 0$, $k_1 \neq 0$, и так как A — группа без кручения, то $a_1 = 0$, и поэтому, в силу индуктивного предположения, $A = \langle a_2, \ldots, a_n \rangle$ — свободная абелева группа.

Итак, допустим, что $|k_1| \geq |k_2| > 0$, и в этом случае заменим образующий a_2 на $a_2' = a_2 + ka_1$, $k \in \mathbb{Z}$ ($a_2 = a_2' - ka_1$). В новой системе образующих $\{a_1, a_2', a_3, \ldots, a_n\}$ наше соотношение $*$ имеет вид

$$(k_1 - kk_2)a_1 + k_2a_2' + k_3a_3 + \ldots + k_na_n = 0.$$

В силу алгоритма деления в кольце целых чисел $\mathbb{Z}$ выберем $k \in \mathbb{Z}$ так, чтобы $|k_1 - kk_2| < |k_2|$, строго уменьшив модуль

коэффициента при a_1. Продолжая этот процесс, мы приходим к рассмотренному случаю, когда $k_1 = \pm 1$, что завершает доказательство. $\square$

Теорема 2 (универсальное свойство свободной абелевой группы конечного ранга)**.** *Пусть $F = F_n$ — свободная абелева группа,* $\mathrm{rk}\,(F) = n$, *$\{e_1, \ldots, e_n\}$ — один из базисов в $F = F_n$.*

Если A — абелева группа, $\varphi\colon \{e_1, \ldots, e_n\} \to A$ — отображение множеств (т. е. заданы элементы $a_1 = \varphi(e_1), \ldots, a_n = \varphi(e_n) \in A$), то существует и единственный гомоморфизм групп $f\colon F_n \to A$ такой, что $f(e_i) = \varphi(e_i)$ для всех $1 \leqslant i \leqslant n$.

Доказательство. Для элемента

$$x = k_1 e_1 + \ldots + k_n e_n \in F_n, \quad k_i \in \mathbb{Z},$$

положим

$$f(x) = k_1 a_1 + \ldots + k_n a_n \in A.$$

Если

$$y = l_1 e_1 + \ldots + l_n e_n \in F_n, \quad l_i \in \mathbb{Z},$$

то

$$\begin{aligned} &x + y = (k_1 + l_1)e_1 + \ldots + (k_n + l_n)e_n, \\ &f(y) = l_1 a_1 + \ldots + l_n a_n \in A, \\ &f(x + y) = (k_1 + l_1)a_1 + \ldots + (k_n + l_n)a_n = \\ &\quad = (k_1 a_1 + \ldots + k_n a_n) + (l_1 a_1 + \ldots + l_n a_n) = f(x) + f(y). \end{aligned}$$

Таким образом, f — гомоморфизм групп. Ясно, что $f(e_i) = a_i = \varphi(e_i)$ для всех $1 \leq i \leq n$.

Так как любой гомоморфизм $g\colon F_n \to A$ однозначно определяется значениями $g(e_1), \ldots, g(e_n)$, то условием условием $f(e_i) = \varphi(e_i)$ для всех $1 \leq i \leq n$ гомоморфизм f определен однозначно. $\square$

Теорема 3 (накрывающее свойство свободной абелевой группы конечного ранга)**.** *Пусть $A = \langle a_1, a_2, \ldots, a_n \rangle$ — конечно порожденная абелева группа, $\{a_1, a_2, \ldots, a_n\}$ — одна из ее систем образующих. Тогда*:

1) *существует сюръективный гомоморфизм $f\colon F_n \to A$;*

2) *группа A изоморфна фактор-группе $F_n/\ker f$.*

Доказательство. Пусть $F = F_n$ — свободная абелева группа с базисом $\{e_1, \ldots, e_n\}$. В силу предыдущей теоремы существует гомоморфизм $f\colon F_n \to A$, для которого $f(e_i) = a_i$, $1 \leqslant i \leqslant n$. Так как $\{a_1, \ldots, a_n\}$ — система образующих группы A, $A = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$, то $\operatorname{Im} f = A$. В силу теоремы о гомоморфизме $F_n/\ker f \cong A$. $\square$

Теорема 4 (расщепляющее свойство свободной абелевой группы)**.** *Пусть A — абелева группа, F_n — свободная абелева группа ранга n, $f\colon A \to F_n$ — сюръективный гомоморфизм. Тогда*:

1) *существует гомоморфизм $h\colon F_n \to A$, для которого $fh = 1$ (т. е. имеем ретракт $f : A \to F_n$, $h : F_n \to A$, $fh = 1_{F_n}$);*

2) *для некоторой подгруппы B в A $A = B \oplus \ker f$, $B \cong F_n$.*

Доказательство. Пусть $\{e_1, \ldots, e_n\}$ — один из базисов свободной абелевой группы F_n, $n = \operatorname{rk}(F_n)$.

Так как $f\colon A \to F_n$ — сюръективное отображение, то выберем такие элементы $\{a_1, \ldots, a_n\}$ в A, что $f(a_i) = e_i$, $1 \leqslant i \leqslant n$.

Отображение $\{e_1, \ldots, e_n\} \to \{a_1, \ldots, a_n\}$, $e_i \to a_i$, продолжается до гомоморфизма $h\colon F_n \to A$, для которого $h(e_i) = a_i$.

Так как для $(fh)\colon F_n \to F_n$ имеем

$$(fh)(e_i) = f\big(h(e_i)\big) = f(a_i) = e_i = 1_{F_n}(e_i),$$

то $fh = 1_{F_n}$. Итак, получили ретракт, $fh = 1_{F_n}$.

В силу леммы о ретракте $A = \operatorname{Im} h \oplus \ker f$. Полагая $B = \operatorname{Im} h = \langle a_1, \ldots, a_n \rangle$, получаем $A = B \oplus \ker f$.

Так как $f(B) = f(A) = F_n$, то $f|_B$ — сюръективное отображение, при этом

$$\ker(f|_B) = \ker f \cap B = \ker f \cap \operatorname{Im} h = 0.$$

Итак, $f|_B\colon B \to F_n$ — изоморфизм групп, $B \cong F_n$. $\square$

СТРУКТУРНАЯ ТЕОРЕМА

Теорема 5. *Пусть A — конечно порожденная абелева группа.*

1) *Тогда имеет место прямое разложение*

$$A = \mathbf{T}(A) \oplus A',$$

где периодическая часть $\mathbf{T}(A)$ является конечной абелевой группой, $|\mathbf{T}(A)| < \infty$, и $\mathbf{T}(A)$ выделяется в A прямым слагаемым, подгруппа A' является свободной абелевой группой конечного ранга $r < \infty$ и определена однозначно (с точностью до изоморфизма), $A' \cong A/\mathbf{T}(A) \cong F_r$, $r = \operatorname{rk}\big(A/\mathbf{T}(A)\big)$ — инвариант группы A.

Таким образом, конечно порожденная абелева группа A является прямой суммой конечной абелевой группы $\mathbf{T}(A)$ и свободной абелевой группы $A' \cong F_r$ конечного ранга r; если $A = \mathbf{T}(A) \oplus A' = \mathbf{T}(A) \oplus A''$, то $A' \cong A''$.

2) *Это прямое разложение единственно в следующем смысле*: *если*

$$A = B \oplus C = B' \oplus C',$$

где B и B' — конечные абелевы группы, $C \cong F_r$ и $C' \cong F_s$ — свободные абелевы группы конечных рангов r и s соответственно, то

$$B = B' = \mathbf{T}(A), \quad C \cong C' \cong F_r \quad (r = s = \operatorname{rk}(A/\mathbf{T}(A))).$$

Доказательство.

1) Если $A = \langle a_1, \ldots, a_n \rangle$ — конечно порожденная абелева группа, то

$$A/\mathbf{T}(A) = \langle \bar{a}_1, \ldots, \bar{a}_n \rangle,$$
$$\bar{a}_i = a_i + \mathbf{T}(A) \in A/\mathbf{T}(A), \quad \mathbf{T}\big(A/\mathbf{T}(A)\big) = 0,$$

и поэтому $A/\mathbf{T}(A)$ — конечно порожденная абелева группа без кручения. В силу теоремы **??** $A/\mathbf{T}(A)$ — свободная абелева группа конечного ранга, $A/\mathbf{T}(A) \cong F_r$, где $r = \operatorname{rk}\big(A/\mathbf{T}(A)\big)$. В силу расщепляющего свойства свободной абелевой группы (см. теорему 4) имеем: $A = \mathbf{T}(A) \oplus A'$, где A' — подгруппа в A, $A' \cong A/\mathbf{T}(A) \cong F_r$ ($r < \infty$, поскольку $A/\mathbf{T}(A)$ — конечно порожденная абелева группа).

Так как $\mathbf{T}(A) \cong A/A'$ — конечно порожденная периодическая абелева группа, то в силу теоремы прошлой лекции $|\mathbf{T}(A)| < \infty$. Итак, $\mathbf{T}(A)$ — конечная абелева группа.

Если $A = \mathbf{T}(A) \oplus A' = \mathbf{T}(A) \oplus A''$, то $A' \cong A/\mathbf{T}(A) \cong A''$.

2) Если

$$A = B \oplus C = B' \oplus C', \quad |B| < \infty, \ \ |B'| < \infty, \ \ C \cong F_r, \ \ C' \cong F_s,$$

то

$$\mathbf{T}(B) = B, \quad \mathbf{T}(C) = 0, \quad \mathbf{T}(B') = B', \quad \mathbf{T}(C') = 0,$$

и поэтому

$$B = \mathbf{T}(B) = \mathbf{T}(B) \oplus \mathbf{T}(C) = \mathbf{T}(B \oplus C) = \mathbf{T}(A) = \\ = \mathbf{T}(B' \oplus C') = \mathbf{T}(B') \oplus \mathbf{T}(C') = \mathbf{T}(B') = B'.$$

Следовательно, $B = \mathbf{T}(A) = B'$. Поэтому

$$F_r \cong C \cong A/B = A/\mathbf{T}(A) = A/B' \cong C' \cong F_s,$$

и следовательно, $r = s$. $\square$

ПОДГРУППЫ СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ

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

Теорема 6. *Ненулевая подгруппа B свободной абелевой группы F_n конечного ранга n является свободной абелевой группой ранга m, $B \cong F_m$, где $1 \leqslant m \leqslant n$.*

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 $l \leqslant n-1$.

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 $n' = n-1 < n$: $B \cong F_m$, $m \leqslant n-1 < n$.

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 $l+1 \leqslant (n-1)+1 = n$. $\square$

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 $A = \langle a_1, \ldots, a_n \rangle$ 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 $\pi(e_i) = a_i$, $1 \leqslant i \leqslant n$,

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

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

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

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

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

$$k_1a_1 + \ldots + k_na_n = 0$$

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

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

и поэтому

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

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

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

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

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.

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, $1 \leqslant i \leqslant m$, $d_i = \pm 1 \in \mathbb{Z}$. □

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

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

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

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

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

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

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

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

Тогда

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

для всех $1 \leqslant i \leqslant n$, 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 $1 \leqslant i \leqslant n$, 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,

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

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*

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

— 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 $1 \leqslant j \leqslant n$

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

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 7 (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*

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

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

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* $D = \operatorname{diag}(d_1, \ldots, d_u)$ *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, придём 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 найдётся 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 $D = \operatorname{diag}(d_1, d_2, \ldots, d_u) \in \mathbf{M}_{m,n}(\mathbb{Z})$, где $d_1 \mid d_2 \mid \ldots \mid d_u$.

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

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 $1 \leqslant i \leqslant u$;

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

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

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

Таким образом,

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

Итак, последовательно:

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

(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 $d'_2 = \ldots = d'_u = d_2 = \ldots = d_u = 0$).

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