5 Лекция 11.04

Доказательство теоремы о согласованных базисах

Определение 26. *Элементарные целочисленные преобразования матрицы $C = (c_{ij})$ над строками (и столбцами) бывают 3 типов:*

1. *Прибавить к i-ой строке j-ую, умноженную на λ*
2. *Перестановка i-ой и j-ой строки*
3. *Умножение строки на ± 1*

Определение 27. *Матрица C размером (n, m) диагональна, если она имеет вид*

$$C = \begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix}$$

то есть если $i \neq j$, то $c_{ij} = 0$. Обозначается как $\operatorname{diag}(u_1, \dots, u_p)$, *где* $p = \min(n, m)$.

Предложение 6. Любую прямоугольную целочисленную матрицу C элементарными преобразованиями строк и столбцов можно привести к диагональному виду $\operatorname{diag}(u_1, \dots, u_p)$, где $u_1 \geq 0, \dots, u_p \geq 0, \forall i : u_i \mid u_{i+1}$.

Доказательство. Без ограничения общности считаем, что $c_{11} > 0$. Хотим, чтобы любой элемент 1 строки и 1 столбца делился на c_{11}. Разберем для строки. Будем делать что-то наподобие алгоритма Евклида. Пусть c_{1i} не делится на c_{11}. Представим $c_{1i} = c_{11}q + r$, тогда q раз вычтем из c_{1i} число c_{11}. Затем поменяем местами столбцы i и 1. Тогда за конечное число шагов мы сделаем так, что c_{1i} делится на c_{11}. После этого мы можем занулить все элементы 1 строки и 1 столбца, кроме c_{11}.

Теперь мы хотим, чтобы все элементы c_{ij} делились на c_{11}. Пусть какой-то c_{ij} не делится на c_{11}. Поднимем его в первый столбец и запустим для него процедуру из 1 абзаца.

После этого мы получим матрицу вида:

$$C = \begin{pmatrix} c_{11} & \\ & c_{11} \cdot C' \end{pmatrix}$$

Теперь для матрицы C' продолжим это рассуждение по индукции. Далее получим:

$$C = \begin{pmatrix} c_{11} & & \\ & c_{22} & \\ & & c_{22} \cdot C'' \end{pmatrix}$$

где c_{22} делится на c_{11} и так далее. □

Доказательство. Теперь вернемся к доказательству теоремы. Пусть $e_1, \dots, e_n$ — базис в N, $f_1, \dots, f_m$ — базис в L. Мы знаем, что $(f_1, \dots, f_m) = (e_1, \dots, e_n) \cdot C$, где C имеет размеры $n \times m$. Заметим, что целочисленные элементарные преоразования строк (столбцов) соответствуют заменам базиса в L (или в N, если делали преобразования столбцов).

Пример. При замене строк мы меняем базис f, столбцов — e.

$$(f_1, f_2) = (e_1, e_2, e_3) \cdot \begin{pmatrix} 1 & 0 \\ 2 & -2 \\ 3 & 7 \end{pmatrix}$$

Цепочкой преобразований строк и столбцов приведем C к диагональному виду. Получим

$$(f'_1, \dots, f'_m) = (e'_1, \dots, e'_n) \cdot \operatorname{diag}(u_1, \dots, u_m)$$

Из этого следует, что

$$f'_1 = u_1 e'_1$$
$$f'_2 = u_2 e'_2$$
$$\vdots$$
$$f'_m = u_m e'_m$$

Что и требовалось.

□

Следствие 8. $L/N \cong \mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_m} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n-m \text{ раз}}$

Доказательство. Выберем согласованные базисы $e_1, \dots, e_m, e_{m+1}, \dots, e_n$ и $u_1 e_1, \dots, u_m e_m$. Тогда

$$L/N = \frac{\mathbb{Z} \oplus \dots \oplus \mathbb{Z} \oplus \mathbb{Z} \dots \oplus \mathbb{Z}}{u_1\mathbb{Z} \oplus \dots \oplus u_m\mathbb{Z} \oplus \{0\} \oplus \dots \oplus \{0\}} \cong$$
$$\mathbb{Z}/u_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/u_m\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/\{0\} \oplus \dots \oplus \mathbb{Z}/\{0\} \cong$$
$$\mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_m} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$$

□

Определение 28. *Числа $u_1, \dots, u_m$ называют инвариантными множителями для пары (L, N). Они не зависят от выбора базиса.*

Определение 29. *Конечная абелева группа A называется примарной, если $|A| = p^k$, где p — простое, а $k \in \mathbb{N}$. Для конечной неабелевой группы говорят p-группа.*

Теорема 8. *Всякая конечно порожденная абелева группа A разлагается в прямую сумму примарных и бесконечных циклических групп. Формально*

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$$

где $p_1, \dots, p_s$ — простые (не обязательно различные), а $k_i \in \mathbb{N}$. Кроме того, число бесконечных слагаемых и число и порядки примарных слагаемых определены однозначно.

Пример.

$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}$$

Но 6 — не примарное число, поэтому $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ не является контрпримером.

Доказательство. Пусть $a_1, \dots, a_n$ — система порождающих группы A. Тогда рассмотрим гомоморфизм $\varphi : \mathbb{Z}^n \to A$, причем $(s_1, \dots, s_n) \mapsto^{\varphi} (s_1 a_1, \dots, s_n a_n)$. Заметим, что φ — сюръективен, потому что любой элемент A представим в виде линейной комбинации. Вспомним, что

$$A = \operatorname{Im}\varphi \cong \mathbb{Z}^n / \ker\varphi = L/N \cong \mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_n} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$$

Каждое u_i разложим на простые множители, $u_i = p_{1i}^{k_{1i}} \cdot \dots \cdot p_{si}^{k_{si}}$. Тогда

$$\mathbb{Z}_{u_i} \cong \mathbb{Z}_{p_{1i}^{k_{1i}}} \oplus \dots \oplus \mathbb{Z}_{p_{si}^{k_{si}}}$$

Таким образом доказали существование. Единственность доказывается технически и является факультативным материалом. □

Следствие 9. Каждая конечная абелева группа изоморфна $\mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}} \cong \mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_m}$, где $u_i \mid u_{i+1}$.

Определение 30. *Экспонента конечной абелевой группы A — такое число* $\exp(A)$*, равное НОК всех порядков элементов в A.*

Упражнение. Показать, что $\exp(A) = \min\{m \mid \forall a \in A : ma = 0\}$.

Предложение 7. Если $A = \mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_m}$, то $\exp(A) = u_m$.

Доказательство. Возьмем $a = (\vec{c_1}, \dots, \vec{c_m})$, где $c_i \in Z_{u_i}$. Тогда $u_m a = (\vec{0}, \dots, \vec{0})$. С другой стороны $(\vec{0}, \dots, \vec{0}, \vec{1})$ имеет порядок u_m. Из первого получаем, что $\exp(A) \leq u_m$, из второго — что $\exp(A) \geq u_m$, то есть $\exp(A) = u_m$. □

Следствие 10. A — циклическая $\Leftrightarrow |A| = \exp(A)$.

Доказательство. A — циклическая $\Leftrightarrow$ в разложении $\mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_m}$ только одно слагаемое, пусть $\mathbb{Z}_k$. По предложению (7) получаем, что $\exp(A) = k$. □