**Лекции курса «Алгебра», лектор Р. С. Авдеев**
ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2015/2016 учебный год

## Лекция 4

*Теорема о согласованных базисах. Алгоритм приведения целочисленной матрицы к диагональному виду. Строение конечно порождённых абелевых групп. Конечные абелевы группы.*

В теории абелевых групп операция прямого произведения конечного числа групп обычно называется *прямой суммой* и обозначается символом $\oplus$, так что пишут $A_1 \oplus A_2 \oplus \ldots \oplus A_n$ вместо $A_1 \times A_2 \times \ldots \times A_n$.

Дадим более точное описание подгрупп свободных абелевых групп.

**Теорема о согласованных базисах.** Для всякой подгруппы $N$ свободной абелевой группы $L$ ранга $n$ найдётся такой базис $e_1, \ldots, e_n$ группы $L$ и такие натуральные числа $u_1, \ldots, u_m$, $m \leqslant n$, что $u_1e_1, \ldots, u_me_m$ — базис группы $N$ и $u_i | u_{i+1}$ при $i = 1, \ldots, m-1$.

*Замечание* 1. Числа $u_1, \ldots, u_p$, фигурирующие в теореме о согласованных базисах, называются *инвариантными множителями* подгруппы $N \subseteq L$. Можно показать, что они определены по подгруппе однозначно.

**Следствие 1.** *В условиях теоремы о согласованных базисах имеет место изоморфизм*

$$L/N \cong \mathbb{Z}_{u_1} \times \ldots \times \mathbb{Z}_{u_m} \times \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n-m}.$$

*Доказательство.* Рассмотрим изоморфизм $L \cong \mathbb{Z}^n = \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n}$, сопоставляющий произвольному элементу $s_1e_1 + \ldots + s_ne_n \in L$ набор $(s_1, \ldots, s_n) \in \mathbb{Z}^n$. При этом изоморфизме подгруппа $N \subseteq L$ отождествляется с подгруппой

$$u_1\mathbb{Z} \times \ldots \times u_m\mathbb{Z} \times \underbrace{\{0\} \times \ldots \times \{0\}}_{n-m} \subseteq \mathbb{Z}^n.$$

Теперь требуемый результат получается применением теоремы о факторизации по сомножителям. □

Теперь вернемся к доказательству теоремы о согласованных базисов. Однако это требует некоторой подготовки.

**Определение 1.** *Целочисленными элементарными преобразованиями строк* матрицы называются преобразования следующих трёх типов:

1) прибавление к одной строке другой, умноженной на целое число;

2) перестановка двух строк;

3) умножение одной строки на $-1$.

Аналогично определяются *целочисленные элементарные преобразования столбцов* матрицы.

Прямоугольную матрицу $C = (c_{ij})$ размера $n \times m$ назовём *диагональной* и обозначим $\mathrm{diag}(u_1, \ldots, u_p)$, если $c_{ij} = 0$ при $i \neq j$ и $c_{ii} = u_i$ при $i = 1, \ldots, p$, где $p = \min(n, m)$.

**Предложение 1.** *Всякую прямоугольную целочисленную матрицу $C = (c_{ij})$ с помощью элементарных преобразований строк и столбцов можно привести к виду $diag(u_1, \ldots, u_p)$, где $u_1, \ldots, u_p \geqslant 0$ и $u_i | u_{i+1}$ при $i = 1, \ldots, p-1$.*

*Доказательство.* Если $C = 0$, то доказывать нечего. Если $C \neq 0$, но $c_{11} = 0$, то переставим строки и столбцы и получим $c_{11} \neq 0$. Умножив, если нужно, первую строку на $-1$, добьёмся условия $c_{11} > 0$. Теперь будем стремиться уменьшить $c_{11}$.

Если какой-то элемент $c_{i1}$ не делится на $c_{11}$, то разделим с остатком: $c_{i1} = qc_{11} + r$. Вычитая из $i$-й строки 1-ю строку, умноженную на $q$, и затем переставляя 1-ю и $i$-ю строки, уменьшаем $c_{11}$. Повторяя эту процедуру, в итоге добиваемся, что все элементы 1-й строки и 1-го столбца делятся на $c_{11}$.

Если какой-то $c_{ij}$ не делится на $c_{11}$, то поступаем следующим образом. Вычтя из $i$-й строки 1-ю строку с подходящим коэффициентом, добьёмся $c_{i1} = 0$. После этого прибавим к 1-й строке $i$-ю строку. При этом $c_{11}$ не изменится, а $c_{1j}$ перестанет делиться на $c_{11}$, и мы вновь сможем уменьшить $c_{11}$.

В итоге добьёмся того, что все элементы делятся на $c_{11}$. После этого обнулим все элементы 1-й строки и 1-го столбца, начиная со вторых, и продолжим процесс с меньшей матрицей. □

Теперь мы готовы доказать теорему о согласованных базисах.

*Доказательство теоремы о согласованных базисах.* Мы знаем, что $N$ является свободной абелевой группой ранга $m \leqslant n$. Пусть $e_1, \dots, e_n$ — базис в $L$ и $f_1, \dots, f_m$ — базис в $N$. Тогда $(f_1, \dots, f_m) = (e_1, \dots, e_n)C$, где $C$ — целочисленная матрица размера $n \times m$ и ранга $m$. Покажем, что целочисленные элементарные преобразования строк (столбцов) матрицы $C$ — это в точности элементарные преобразования над базисом в $L$ (в $N$). Для этого рассмотрим сначала случай строк. Заметим, что каждое из целочисленных элементарных преобразований строк реализуется при помощи умножения матрицы $C$ слева на квадратную матрицу $P$ порядка $n$, определяемую следующим образом:

(1) в случае прибавления к $i$-й строке $j$-й, умноженной на целое число $z$, в матрице $P$ на диагонали стоят единицы, на $(ij)$-м месте — число $z$, а на остальных местах — нули;

(2) в случае перестановки $i$-й и $j$-й строк имеем $p_{ij} = p_{ji} = 1$, $p_{kk} = 1$ при $k \neq i, j$, а на остальных местах стоят нули;

(3) в случае умножения $i$-й строки на $-1$ имеем $p_{ii} = -1$, $p_{jj} = 1$ при $j \neq i$, а на остальных местах стоят нули.

Теперь заметим, что равенство $(f_1, \dots, f_m) = (e_1, \dots, e_n)C$ эквивалентно равенству $(f_1, \dots, f_m) = (e_1, \dots, e_n)P^{-1}PC$. Таким образом, базис $(f_1, \dots, f_m)$ выражается через новый базис $(e'_1, \dots, e'_n) := (e_1, \dots, e_n)P^{-1}$ при помощи матрицы $PC$.

В случае столбцов всё аналогично: каждое из целочисленых элементарных преобразований столбцов реализуется при помощи умножения матрицы $C$ справа на некоторую квадратную матрицу $Q$ порядка $m$ (определяемую почти так же, как $P$). В этом случае имеем $(f_1, \dots, f_m)Q = (e_1, \dots, e_n)CQ$, так что новый базис $(f'_1, \dots, f'_m) := (f_1, \dots, f_m)Q$ выражается через $(e_1, \dots, e_n)$ при помощи матрицы $CQ$.

Воспользовавшись предложением 1, мы можем привести матрицу $C$ при помощи целочисленных элементарных преобразований строк и столбцов к диагональному виду $C'' = \operatorname{diag}(u_1, \dots, u_m)$, где $u_i | u_{i+1}$ для всех $i = 1, \dots, m-1$. С учётом сказанного выше это означает, что для некоторого базиса $e''_1, \dots, e''_n$ в $L$ и некоторого базиса $f''_1, \dots, f''_m$ в $N$ справедливо соотношение $(f''_1, \dots, f''_m) = (e''_1, \dots, e''_n)C''$. Иными словами, $f''_i = u_i e''_i$ для всех $i = 1, \dots, m$, а это и требовалось. □

**Определение 2.** Конечная абелева группа $A$ называется *примарной*, если её порядок равен $p^k$ для некоторого простого числа $p$.

*Замечание* 2. В общем случае (когда группы не предполагаются коммутативными) конечная группа $G$ с условием $|G| = p^k$ ($p$ — простое) называется *$p$-группой*.

Следствие 1 лекции 3 показывает, что каждая конечная циклическая группа разлагается в прямую сумму примарных циклических подгрупп.

**Теорема 1.** *Всякая конечно порождённая абелева группа $A$ разлагается в прямую сумму примарных и бесконечных циклических подгрупп, т. е.*

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}, \tag{1}$$

*где $p_1, \dots, p_s$ — простые числа (не обязательно попарно различные) и $k_1, \dots, k_s \in \mathbb{N}$. Кроме того, число бесконечных циклических слагаемых, а также число и порядки примарных циклических слагаемых определено однозначно.*

Сразу выделим некоторые следствия из этой теоремы.

**Следствие 2.** *Абелева группа $A$ является конечно порождённой тогда и только тогда, когда $A$ разлагается в прямую сумму циклических подгрупп.*

*Доказательство.* В одну сторону следует из теоремы. В другую сторону: пусть $A = A_1 \oplus \dots \oplus A_m$, где $A_i$ — циклическая подгруппа, то есть $A_i = \langle a_i \rangle$, $a_i \in A$. Тогда $\{a_1, \dots, a_m\}$ — набор порождающих элементов для группы $A$. □

**Следствие 3.** *Всякая конечная абелева группа разлагается в прямую сумму примарных циклических подгрупп, причём число и порядки примарных циклических слагаемых определено однозначно.*

Теперь преступим к доказательству самой теоремы.

*Доказательство.* Пусть $a_1, \ldots, a_n$ — конечная система порождающих группы $A$. Рассмотрим гомоморфизм

$$\varphi\colon \mathbb{Z}^n \to A, \quad (s_1, \ldots, s_n) \mapsto s_1 a_1 + \ldots + s_n a_n.$$

Ясно, что $\varphi$ сюръективен. Тогда по теореме о гомоморфизме получаем $A \cong \mathbb{Z}^n/N$, где $N = \operatorname{Ker}\varphi$. По теореме о согласованных базисах существует такой базис $e_1, \ldots, e_n$ группы $\mathbb{Z}^n$ и такие натуральные числа $u_1, \ldots, u_m$, $m \leqslant n$, что $u_1 e_1, \ldots, u_m e_m$ — базис группы $N$. Тогда имеем

$$\begin{array}{rcccccccccccc} L & = & \langle e_1\rangle & \oplus & \ldots & \oplus & \langle e_m\rangle & \oplus & \langle e_{m+1}\rangle & \oplus & \ldots & \oplus & \langle e_n\rangle, \\ N & = & \langle u_1 e_1\rangle & \oplus & \ldots & \oplus & \langle u_m e_m\rangle & \oplus & \{0\} & \oplus & \ldots & \oplus & \{0\}. \end{array}$$

Применяя теорему о факторизации по сомножителям, мы получаем

$$\mathbb{Z}^n/N \cong \mathbb{Z}/u_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/u_m\mathbb{Z} \oplus \underbrace{\mathbb{Z}/\{0\} \oplus \ldots \oplus \mathbb{Z}/\{0\}}_{n-m} \cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n-m}.$$

Чтобы добиться разложения (1), остаётся представить каждое из циклических слагаемых $\mathbb{Z}_{u_i}$ в виде прямой суммы примарных циклических подгрупп, воспользовавшись следствием 1 из лекции 3.

Перейдём к доказательству единственности разложения (1). Пусть $\langle c\rangle_q$ обозначает циклическую группу порядка $q$ с порождающей $c$. Пусть имеется разложение

$$A = \langle c_1\rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_s\rangle_{p_s^{k_s}} \oplus \langle c_{s+1}\rangle_\infty \oplus \ldots \oplus \langle c_{s+t}\rangle_\infty \tag{2}$$

(заметьте, что мы просто переписали в другом виде правую часть соотношения (1)). Рассмотрим в $A$ так называемую *подгруппу кручения*

$$\operatorname{Tor} A := \{a \in A \mid ma = 0 \text{ для некоторого } m \in \mathbb{N}\}.$$

Иными словами, $\operatorname{Tor} A$ — это подгруппа в $A$, состоящая из всех элементов конечного порядка. Выделим эту подгруппу в разложении (2). Рассмотрим произвольный элемент $a \in A$. Он представим в виде

$$a = r_1 c_1 + \ldots + r_m c_m + r_{m+1} c_{m+1} + \ldots + r_n c_n$$

для некоторых целых чисел $r_1, \ldots, r_n$. Легко видеть, что $a$ имеет конечный порядок тогда и только тогда, когда $r_{m+1} = \ldots = r_m = 0$. Отсюда получаем, что

$$\operatorname{Tor} A = \langle c_1\rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_s\rangle_{p_s^{k_s}}. \tag{3}$$

Применяя опять теорему о факторизации по сомножителям, мы получаем $A/\operatorname{Tor} A \cong \mathbb{Z}^t$, где $t$ — количество бесконечных циклических подгрупп в разложении (1). Отсюда следует, что число $t$ однозначно выражается в терминах самой группы $A$ (как ранг свободной абелевой группы $A/\operatorname{Tor} A$). Значит, $t$ не зависит от разложения (2).

Однозначность числа и порядков примарных циклических групп будет доказана на следующей лекции.

□

## Список литературы


[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 9, § 1)

[2] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 2, § 3)

[3] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 13, § 60)