

ЛЕКЦИЯ 3

Конечно порождённые и свободные абелевы группы. Подгруппы свободных абелевых групп. Теорема о согласованных базисах. Алгоритм приведения целочисленной матрицы к диагональному виду.

Всюду в этой и следующей лекции $(A, +)$ — абелева группа с аддитивной формой записи операции. Для произвольного элемента $a \in A$ и целого числа s положим

$$sa = \begin{cases} \underbrace{a + \dots + a}_s, & \text{если } s > 0; \\ 0, & \text{если } s = 0; \\ \underbrace{(-a) + \dots + (-a)}_{|s|}, & \text{если } s < 0. \end{cases}$$

Определение 1. Абелева группа A называется *конечно порождённой*, если найдутся такие элементы $a_1, \dots, a_n \in A$, что всякий элемент $a \in A$ представим в виде $a = s_1 a_1 + \dots + s_n a_n$ для некоторых целых чисел s_1, \dots, s_n . При этом элементы a_1, \dots, a_n называются *порождающими* или *образующими* группы A .

Замечание 1. Всякая конечно порождённая группа конечна или счётна.

Замечание 2. Всякая конечная группа является конечно порождённой.

Определение 2. Конечно порождённая абелева группа A называется *свободной*, если в ней существует *базис*, т. е. такой набор элементов a_1, \dots, a_n , что каждый элемент $a \in A$ единственным образом представим в виде $a = s_1 a_1 + \dots + s_n a_n$, где $s_1, \dots, s_n \in \mathbb{Z}$. При этом число n называется *рангом* свободной абелевой группы A и обозначается $\text{rk } A$.

Пример 1. Абелева группа $\mathbb{Z}^n := \{(c_1, \dots, c_n) \mid c_i \in \mathbb{Z}\}$ является свободной с базисом

$$\begin{aligned} e_1 &= (1, 0, \dots, 0), \\ e_2 &= (0, 1, \dots, 0), \\ &\dots \\ e_n &= (0, 0, \dots, 1). \end{aligned}$$

Этот базис называется *стандартным*. В группе \mathbb{Z}^n можно найти и много других базисов. Ниже мы все их опишем.

Предложение 1. Ранг свободной абелевой группы определён корректно, т. е. любые два её базиса содержат одинаковое число элементов.

Доказательство. Пусть a_1, \dots, a_n и b_1, \dots, b_m — два базиса группы A . Предположим, что $n < m$. Элементы b_1, \dots, b_m однозначно разлагаются по базису a_1, \dots, a_n , поэтому мы можем записать

$$\begin{aligned} b_1 &= s_{11}a_1 + s_{12}a_2 + \dots + s_{1n}a_n, \\ b_2 &= s_{21}a_1 + s_{22}a_2 + \dots + s_{2n}a_n, \\ &\dots \\ b_m &= s_{m1}a_1 + s_{m2}a_2 + \dots + s_{mn}a_n, \end{aligned}$$

где все коэффициенты s_{ij} — целые числа. Рассмотрим прямоугольную матрицу $S = (s_{ij})$ размера $m \times n$. Так как $n < m$, то ранг этой матрицы не превосходит n , а значит, строки этой матрицы линейно зависимы над \mathbb{Q} . Домножая коэффициенты этой зависимости на наименьшее общее кратное их знаменателей, мы найдём такие целые s_1, \dots, s_m , из которых не все равны нулю, что $s_1 b_1 + \dots + s_m b_m = 0$. Поскольку $0 = 0b_1 + \dots + 0b_m$, это противоречит однозначной выразимости элемента 0 через базис b_1, \dots, b_m . \square

Предложение 2. Всякая свободная абелева группа ранга n изоморфна группе \mathbb{Z}^n .

Доказательство. Пусть A — свободная абелева группа, и пусть a_1, \dots, a_n — её базис. Рассмотрим отображение

$$\varphi: \mathbb{Z}^n \rightarrow A, \quad (s_1, \dots, s_n) \mapsto s_1 a_1 + \dots + s_n a_n.$$

Легко видеть, что φ — гомоморфизм. Так как всякий элемент $a \in A$ представим в виде $s_1 a_1 + \dots + s_n a_n$, где $s_1, \dots, s_n \in \mathbb{Z}$, то φ сюръективен. Из единственности такого представления следует инъективность φ . Значит, φ — изоморфизм. \square

Пусть e'_1, \dots, e'_n — некоторый набор элементов из \mathbb{Z}^n . Выразив эти элементы через стандартный базис e_1, \dots, e_n , мы можем записать

$$(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C,$$

где C — целочисленная квадратная матрица порядка n .

Предложение 3. *Элементы e'_1, \dots, e'_n составляют базис группы \mathbb{Z}^n тогда и только тогда, когда $\det C = \pm 1$.*

Доказательство. Предположим сначала, что e'_1, \dots, e'_n — базис. Тогда элементы e_1, \dots, e_n через него выражаются, поэтому $(e_1, \dots, e_n) = (e'_1, \dots, e'_n)D$ для некоторой целочисленной квадратной матрицы D порядка n . Но тогда $(e_1, \dots, e_n) = (e_1, \dots, e_n)CD$, откуда $CD = E_n$, где E_n — единичная матрица порядка n . Значит, $(\det C)(\det D) = 1$. Учитывая, что $\det C$ и $\det D$ — целые числа, мы получаем $\det C = \pm 1$.

Обратно, пусть $\det C = \pm 1$. Тогда матрица C^{-1} является целочисленной, а соотношение $(e_1, \dots, e_n) = (e'_1, \dots, e'_n)C^{-1}$ показывает, что элементы e_1, \dots, e_n выражаются через e'_1, \dots, e'_n . Но e_1, \dots, e_n — базис, поэтому элементы e'_1, \dots, e'_n порождают группу \mathbb{Z}^n . Осталось доказать, что всякий элемент из \mathbb{Z}^n однозначно через них выражается. Предположим, что $s'_1 e'_1 + \dots + s'_n e'_n = s''_1 e'_1 + \dots + s''_n e'_n$ для некоторых целых чисел $s'_1, \dots, s'_n, s''_1, \dots, s''_n$. Мы можем это переписать в следующем виде:

$$(e'_1, \dots, e'_n) \begin{pmatrix} s'_1 \\ \vdots \\ s'_n \end{pmatrix} = (e'_1, \dots, e'_n) \begin{pmatrix} s''_1 \\ \vdots \\ s''_n \end{pmatrix}.$$

Учитывая, что $(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C$ и что e_1, \dots, e_n — это базис, получаем

$$C \begin{pmatrix} s'_1 \\ \vdots \\ s'_n \end{pmatrix} = C \begin{pmatrix} s''_1 \\ \vdots \\ s''_n \end{pmatrix}.$$

Домножая это равенство слева на C^{-1} , окончательно получаем

$$\begin{pmatrix} s'_1 \\ \vdots \\ s'_n \end{pmatrix} = \begin{pmatrix} s''_1 \\ \vdots \\ s''_n \end{pmatrix}.$$

□

Теорема 1. *Всякая подгруппа N свободной абелевой группы L ранга n является свободной абелевой группой ранга $\leq n$.*

Доказательство. Воспользуемся индукцией по n . При $n = 0$ доказывать нечего. Пусть $n > 0$ и e_1, \dots, e_n — базис группы L . Рассмотрим в L подгруппу

$$L_1 = \langle e_1, \dots, e_{n-1} \rangle := \mathbb{Z}e_1 + \dots + \mathbb{Z}e_{n-1}.$$

Это свободная абелева группа ранга $n - 1$. По предположению индукции подгруппа $N_1 := N \cap L_1 \subseteq L_1$ является свободной абелевой группой ранга $m \leq n - 1$. Зафиксируем в N_1 базис f_1, \dots, f_m .

Рассмотрим отображение

$$\varphi: N \rightarrow \mathbb{Z}, \quad s_1 e_1 + \dots + s_n e_n \mapsto s_n.$$

Легко видеть, что φ — гомоморфизм и что $\text{Ker } \varphi = N_1$. Далее, $\text{Im } \varphi$ — подгруппа в \mathbb{Z} , по предложению 1 из лекции 1 она имеет вид $k\mathbb{Z}$ для некоторого целого $k \geq 0$. Если $k = 0$, то $N \subseteq L_1$, откуда $N = N_1$ и всё доказано. Если $k > 0$, то пусть f_{m+1} — какой-нибудь элемент из N , для которого $\varphi(f_{m+1}) = k$. Докажем, что f_1, \dots, f_m, f_{m+1} — базис в N . Пусть $f \in N$ — произвольный элемент, и пусть $\varphi(f) = sk$, где $s \in \mathbb{Z}$. Тогда $\varphi(f - sf_{m+1}) = 0$, откуда $f - sf_{m+1} \in N_1$ и, следовательно, $f - sf_{m+1} = s_1 f_1 + \dots + s_m f_m$ для некоторых $s_1, \dots, s_m \in \mathbb{Z}$. Значит, $f = s_1 f_1 + \dots + s_m f_m + sf_{m+1}$ и элементы f_1, \dots, f_m, f_{m+1} порождают группу N . Осталось доказать, что они образуют базис в N . Предположим, что

$$s_1 f_1 + \dots + s_m f_m + s_{m+1} f_{m+1} = s'_1 f_1 + \dots + s'_m f_m + s'_{m+1} f_{m+1}$$

для некоторых целых чисел $s_1, \dots, s_m, s_{m+1}, s'_1, \dots, s'_m, s'_{m+1}$. Рассмотрев образ обеих частей этого равенства при гомоморфизме φ , получаем $s_{m+1}k = s'_{m+1}k$, откуда $s_{m+1} = s'_{m+1}$ и

$$s_1 f_1 + \dots + s_m f_m = s'_1 f_1 + \dots + s'_m f_m.$$

Но f_1, \dots, f_m — базис в N_1 , поэтому $s_1 = s'_1, \dots, s_m = s'_m$. □

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, \dots, e_n группы L и такие натуральные числа u_1, \dots, u_m , $m \leq n$, что $u_1 e_1, \dots, u_m e_m$ — базис группы N и $u_i | u_{i+1}$ при $i = 1, \dots, m-1$.

Доказательство этой теоремы потребует некоторой подготовки.

Определение 3. 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 $n \times t$ назовём *диагональной* и обозначим $\text{diag}(u_1, \dots, u_p)$, если $c_{ij} = 0$ при $i \neq j$ и $c_{ii} = u_i$ при $i = 1, \dots, p$, где $p = \min(n, t)$.

Предложение 4. Всякую прямоугольную целочисленную матрицу $C = (c_{ij})$ с помощью элементарных преобразований строк и столбцов можно привести к виду $\text{diag}(u_1, \dots, u_p)$, где $u_1, \dots, u_p \geq 0$ и $u_i | u_{i+1}$ при $i = 1, \dots, p-1$.

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: $c_{i1} = qc_{11} + r$. Вычтя 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. \square

Теперь мы готовы доказать теорему о согласованных базисах.

Доказательство теоремы о согласованных базисах. Мы знаем, что N является свободной абелевой группой ранга $m \leq n$. 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 целочисленных 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 4, мы можем привести матрицу C при помощи целочисленных элементарных преобразований строк и столбцов к диагональному виду $C'' = \text{diag}(u_1, \dots, u_m)$, 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. \square

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

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

Доказательство. Рассмотрим изоморфизм $L \cong \mathbb{Z}^n = \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_n$, сопоставляющий произвольному элементу $s_1 e_1 + \dots + s_n e_n \in L$ набор $(s_1, \dots, s_n) \in \mathbb{Z}^n$. При этом изоморфизме подгруппа $N \subseteq L$ отождествляется с подгруппой

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

Теперь требуемый результат получается применением теоремы о факторизации по сомножителям. \square

Замечание 3. Числа u_1, \dots, u_r , фигурирующие в теореме о согласованных базисах, называются *инвариантными множителями* подгруппы $N \subseteq L$. Можно показать, что они определены по подгруппе однозначно.

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)