Лекции курса «Алгебра», лектор Р. С. Авдеев

ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2015/2016 учебный год

Лекция 3

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

Следующий результат связывает конструкции факторгруппы и прямого произведения.

Теорема о факторизации по сомножителям. Пусть $H_1, \ldots, H_m$ — нормальные подгруппы в группах $G_1, \ldots, G_m$ соответственно. Тогда $H_1 \times \ldots \times H_m$ — нормальная подгруппа в $G_1 \times \ldots \times G_m$ и имеет место изоморфизм групп

$$(G_1 \times \ldots \times G_m)/(H_1 \times \ldots \times H_m) \cong G_1/H_1 \times \ldots \times G_m/H_m.$$

Доказательство. Прямая проверка показывает, что $H_1 \times \ldots \times H_m$ — нормальная подгруппа в $G_1 \times \ldots \times G_m$. Требуемый изоморфизм устанавливается отображением

$$(g_1, \ldots, g_m)(H_1 \times \ldots \times H_m) \mapsto (g_1H_1, \ldots, g_mH_m).$$

□

Теорема 1. *Пусть $n = ml$ — разложение натурального числа n на два взаимно простых множителя. Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_l.$$

Доказательство. Рассмотрим отображение

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_l, \quad k \pmod n \mapsto (k \pmod m, k \pmod l).$$

Поскольку m и l делят n, отображение φ определено корректно. Ясно, что φ — гомоморфизм. Далее, если k переходит в нейтральный элемент $(0, 0)$, то k делится и на m, и на l, а значит, делится на n в силу взаимной простоты m и l. Отсюда следует, что гомоморфизм φ инъективен. Поскольку множества $\mathbb{Z}_n$ и $\mathbb{Z}_m \times \mathbb{Z}_l$ содержат одинаковое число элементов, отображение φ биективно. □

Следствие 1. *Пусть $n \geqslant 2$ — натуральное число и $n = p_1^{k_1} \ldots p_s^{k_s}$ — его разложение в произведение простых множителей (где $p_i \neq p_j$ при $i \neq j$). Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}.$$

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

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

Определение 1. Абелева группа A называется *конечно порождённой*, если найдутся такие элементы $a_1, \ldots, a_n \in A$, что всякий элемент $a \in A$ представим в виде $a = s_1a_1 + \ldots + s_na_n$ для некоторых целых чисел $s_1, \ldots, s_n$. При этом элементы $a_1, \ldots, a_n$ 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 $a_1, \ldots, a_n$, что каждый элемент $a \in A$ единственным образом представим в виде $a = s_1a_1 + \ldots + s_na_n$, где $s_1, \ldots, s_n \in \mathbb{Z}$. При этом число n называется *рангом* свободной абелевой группы A и обозначается $\operatorname{rk} A$.

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

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

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 $s_1b_1 + \ldots + s_mb_m = 0$. Поскольку $0 = 0b_1 + \ldots + 0b_m$, 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

$$\varphi\colon \mathbb{Z}^n \to A, \quad (s_1, \dots, s_n) \mapsto s_1a_1 + \ldots + s_na_n.$$

Легко видеть, что φ — гомоморфизм. Так как всякий элемент $a \in A$ представим в виде $s_1a_1 + \ldots + s_na_n$, 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 $s'_1e'_1 + \ldots + s'_ne'_n = s''_1e'_1 + \ldots + s''_ne'_n$ 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 2. *Всякая подгруппа N свободной абелевой группы L ранга n является свободной абелевой группой ранга $\leqslant n$.*

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

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

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 $m \leqslant n-1$. Зафиксируем в N_1 базис $f_1, \ldots, f_m$.

Рассмотрим отображение

$$\varphi\colon N \to \mathbb{Z}, \quad s_1e_1 + \ldots + s_ne_n \mapsto s_n.$$

Легко видеть, что φ — гомоморфизм и что $\operatorname{Ker}\varphi = N_1$. Далее, $\operatorname{Im}\varphi$ — подгруппа в $\mathbb{Z}$, по предложению 1 из лекции 1 она имеет вид $k\mathbb{Z}$ для некоторого целого $k \geqslant 0$. 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 $f_1, \ldots, f_m, f_{m+1}$ — 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, $f - sf_{m+1} = s_1f_1 + \ldots + s_mf_m$ для некоторых $s_1, \ldots, s_m \in \mathbb{Z}$. Значит, $f = s_1f_1 + \ldots + s_mf_m + sf_{m+1}$ и элементы $f_1, \ldots, f_m, f_{m+1}$ порождают группу N. Осталось доказать, что они образуют базис в N. Предположим, что

$$s_1f_1 + \ldots + s_mf_m + s_{m+1}f_{m+1} = s'_1f_1 + \ldots + s'_mf_m + s'_{m+1}f_{m+1}$$

для некоторых целых чисел $s_1, \ldots, s_m, s_{m+1}, s'_1, \ldots, s'_m, s'_{m+1}$. 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

$$s_1f_1 + \ldots + s_mf_m = s'_1f_1 + \ldots + s'_mf_m.$$

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

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)