Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев

ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2014/2015 учебный год

Лекция 4

Строение конечно порождённых абелевых групп. Конечные абелевы группы. Экспонента конечной абелевой 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 $A_1 \times A_2 \times \ldots \times A_n$.

Определение 1. Конечная абелева группа A называется *примарной*, если её порядок равен p^k для некоторого простого числа p.

Замечание 1. В общем случае (когда группы не предполагаются коммутативными) конечная группа G с условием $|G| = p^k$ (p — простое) называется *p-группой.*

Следствие 2 лекции 2 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.*

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

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

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

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

Ясно, что φ 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 $u_1e_1, \ldots, u_me_m$ — базис группы N. Тогда имеем

$$\begin{array}{ccccccccccccc} L & = & \langle e_1\rangle & \oplus & \ldots & \oplus & \langle e_m\rangle & \oplus & \langle e_{m+1}\rangle & \oplus & \ldots & \oplus & \langle e_n\rangle, \\ N & = & \langle u_1e_1\rangle & \oplus & \ldots & \oplus & \langle u_me_m\rangle & \oplus & \{0\} & \oplus & \ldots & \oplus & \{0\}. \end{array}$$

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 2 из лекции 2.

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

$$a = r_1c_1 + \ldots + r_mc_m + r_{m+1}c_{m+1} + \ldots + r_nc_n$$

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 $A/\operatorname{Tor} A \cong \mathbb{Z}^t$. 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).

Далее, для каждого простого числа p определим в A *подгруппу p-кручения*

$$\mathrm{Tor}_p\, A := \{a \in A \mid p^k a = 0 \text{ для некоторого } k \in \mathbb{N}\}. \tag{4}$$

Ясно, что $\mathrm{Tor}_p\, A \subset \mathrm{Tor}\, A$. Выделим подгруппу $\mathrm{Tor}_p\, A$ в разложении (3). Легко видеть, что $\langle c_i \rangle_{p_i^{k_i}} \subseteq \mathrm{Tor}_p\, A$ для всех i с условием $p_i = p$. Если же $p_i \neq p$, то по следствию 2 из теоремы Лагранжа (см. лекцию 1) порядок любого ненулевого элемента $x \in \langle c_i \rangle_{p_i^{k_i}}$ является степенью числа p_i, а значит, $p^k x \neq 0$ для всех $k \in \mathbb{N}$. Отсюда следует, что $\mathrm{Tor}_p\, A$ является суммой тех конечных слагаемых в разложении (3), порядки которых суть степени p. Поэтому доказательство теперь сводится к случаю, когда A — примарная группа. Пусть $|A| = p^k$ и

$$A = \langle c_1 \rangle_{p^{k_1}} \oplus \ldots \oplus \langle c_r \rangle_{p^{k_r}}, \quad k_1 + \ldots + k_r = k.$$

Докажем индукцией по k, что набор чисел $k_1, \ldots, k_r$ не зависит от разложения.

Если $k = 1$, то $|A| = p$, но тогда $A \cong \mathbb{Z}_p$ по следствию 5 из теоремы Лагранжа (см. лекцию 1). Пусть теперь $k > 1$. Рассмотрим подгруппу $pA := \{pa \mid a \in A\}$. В терминах равенства (4) имеем

$$pA = \langle pc_1 \rangle_{p^{k_1 - 1}} \oplus \ldots \oplus \langle pc_r \rangle_{p^{k_r - 1}}.$$

В частности, при $k_i = 1$ соответствующее слагаемое равно $\{0\}$ (и тем самым исчезает). Так как $|pA| = p^{k-r} < p^k$, то по предположению индукции группа pA разлагается в прямую сумму примарных циклических подгрупп однозначно с точностью до порядка слагаемых. Следовательно, ненулевые числа в наборе $k_1 - 1, \ldots, k_r - 1$ определены однозначно (с точностью до перестановки). Отсюда мы находим значения k_i, отличные от 1. Количество тех k_i, которые равны 1, однозначно восстанавливается из условия $k_1 + \ldots + k_r = k$. $\square$

Следствие 1. *Всякая конечная абелева группа разлагается в прямую сумму примарных циклических подгрупп, причём число и порядки примарных циклических слагаемых определено однозначно.*

Заметим, что теорема о согласованных базисах даёт нам другое разложение конечной абелевой группы A:

$$A = \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}, \quad \text{где } u_i | u_{i+1} \text{ при } i = 1, \ldots, m-1. \tag{5}$$

Числа $u_1, \ldots, u_m$ называют *инвариантными множителями* конечной абелевой группы A.

Определение 2. *Экспонентой* конечной абелевой группы A называется число $\exp A$, равное наименьшему общему кратному порядков элементов из A.

Замечание 2. Легко видеть, что $\exp A = \min\{n \in \mathbb{N} \mid ma = 0 \text{ для всех } a \in A\}$.

Предложение 1. *Экспонента конечной абелевой группы A равна её последнему инвариантному множителю u_m.*

Доказательство. Обратимся к разложению (5). Так как $u_i | u_m$ для всех $i = 1, \ldots, m$, то $u_m a = 0$ для всех $a \in A$. Это означает, что $\exp A \leqslant u_m$ (и тем самым $\exp A \,|u_m$). С другой стороны, в A имеется циклическая подгруппа порядка u_m. Значит, $\exp A \geqslant u_m$. $\square$

Следствие 2. *Конечная абелева группа A является циклической тогда и только тогда, когда* $\exp A = |A|$.

Доказательство. Группа A является циклической тогда и только тогда, когда в разложении (5) присутствует только одно слагаемое, т. е. $A = \mathbb{Z}_{u_m}$ и $|A| = u_m$. $\square$

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)