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

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

Лекция 5

Строение конечно порождённых абелевых груп (продолжение). Экспонента конечной абелевой группы. Действие группы на множестве. Орбиты и стабилизаторы.

Продолжим доказательство теоремы с прошлой лекции.

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. На прошлой лекции мы доказали существование разложения и то, что количество бесконечных циклических групп $\mathbb{Z}$ определено однозначно. Для этого мы вводили понятие *подгруппы кручения*:

$$\operatorname{Tor} A = \langle c_1 \rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_s \rangle_{p_s^{k_s}}. \tag{2}$$

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

$$\operatorname{Tor}_p A := \{a \in A \mid p^k a = 0 \text{ для некоторого } k \in \mathbb{N}\}. \tag{3}$$

Ясно, что $\operatorname{Tor}_p A \subset \operatorname{Tor} A$. Выделим подгруппу $\operatorname{Tor}_p A$ в разложении (2). Легко видеть, что $\langle c_i \rangle_{p_i^{k_i}} \subseteq \operatorname{Tor}_p A$ для всех i с условием $p_i = p$. Если же $p_i \neq p$, то по следствию 2 из теоремы Лагранжа (см. лекцию 2) 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 $\operatorname{Tor}_p A$ является суммой тех конечных слагаемых в разложении (2), 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 2). Пусть теперь $k > 1$. Рассмотрим подгруппу $pA := \{pa \mid a \in A\}$. В терминах равенства (3) 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 $k_1 + \ldots + k_r = k$. □

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

$$A = \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}, \quad \text{где } u_i | u_{i+1} \text{ при } i = 1, \ldots, m-1. \tag{4}$$

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

Определение 1. *Экспонентой* конечной абелевой группы A называется число $\exp A$, равное наименьшему общему кратному порядков элементов из A. Легко заметить, что это равносильно следующему условию:

$$\exp A = \min\{n \in \mathbb{N} \mid na = 0 \text{ для всех } a \in A\}$$

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

Доказательство. Обратимся к разложению (4). 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, $\exp A \geqslant u_m$. □

Следствие 1. *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 (4) присутствует только одно слагаемое, т. е. $A = \mathbb{Z}_{u_m}$ и $|A| = u_m$. □

Пусть G — произвольная группа и X — некоторое множество.

Определение 2. *Действием* группы G на множестве X называется отображение $G \times X \to X$, $(g, x) \mapsto gx$, удовлетворяющее следующим условиям:

1) $ex = x$ для любого $x \in X$ (e — нейтральный элемент группы G);

2) $g(hx) = (gh)x$ для всех $g, h \in G$ и $x \in X$.

Обозначение: $G : X$.

Если задано действие группы G на множестве X, то каждый элемент $g \in G$ определяет биекцию $a_g \colon X \to X$ по правилу $a_g(x) = gx$ (обратным отображением для a_g будет $a_{g^{-1}}$). Обозначим через $S(X)$ группу всех биекций (перестановок) множества X с операцией композиции. Тогда отображение $a \colon G \to S(X)$, $g \mapsto a_g$, является гомоморфизмом групп. Действительно, для произвольных элементов $g, h \in G$ и $x \in X$ имеем

$$a_{gh}(x) = (gh)x = g(hx) = ga_h(x) = a_g(a_h(x)) = (a_g a_h)(x).$$

Можно показать, что задание действия группы G на множестве X равносильно заданию соответствующего гомоморфизма $a \colon G \to S(X)$.

Пример 1. Симметрическая группа S_n естественно действует на множестве $X = \{1, 2, \ldots, n\}$ по формуле $\sigma x = \sigma(x)$ ($\sigma \in S_n$, $x \in X$). Условие 1) здесь выполнено по определению тождественной подстановки, условие 2) выполнено по определению композиции подстановок.

Пусть задано действие группы G на множестве X.

Определение 3. *Орбитой* точки $x \in X$ называется подмножество

$$Gx = \{x' \in X \mid x' = gx \text{ для некоторого } g \in G\} = \{gx \mid g \in G\}.$$

Замечание 1. Для точек $x, x' \in X$ отношение «x' лежит в орбите Gx» является отношением эквивалентности:

(1) (рефлексивность) $x \in Gx$ для всех $x \in X$: это верно, так как $x = ex \in Gx$ для всех $x \in X$;

(2) (симметричность) если $x' \in Gx$, то $x \in Gx'$: это верно, так как из условия $x' = gx$ следует $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x' \in Gx'$;

(3) (транзитивность) если $x' \in Gx$ и $x'' \in Gx'$, то $x'' \in Gx$: это верно, так как из условий $x' = gx$ и $x'' = hx'$ следует $x'' = hx' = h(gx) = (hg)x \in Gx$.

Отсюда вытекает, что множество X разбивается в объединение попарно непересекающихся орбит действия группы G.

Определение 4. *Стабилизатором* (*стационарной подгруппой*) точки $x \in X$ называется подгруппа $\mathrm{St}(x) := \{g \in G \mid gx = x\}$.

Упражнение 1. Проверьте, что множество $\mathrm{St}(x)$ действительно является подгруппой в G.

Лемма 1. *Пусть конечная группа G действует на множестве X. Тогда для всякого элемента $x \in X$ справедливо равенство*

$$|Gx| = |G|/|\mathrm{St}(x)|.$$

В частности, число элементов в (любой) орбите делит порядок группы G.

Доказательство. Рассмотрим множество[1] $G/\mathrm{St}(x)$ левых смежных классов группы G по подгруппе $\mathrm{St}(x)$ и определим отображение $\psi \colon G/\mathrm{St}(x) \to Gx$ по формуле $g\mathrm{St}(x) \mapsto gx$. Это определение корректно, поскольку для любого другого представителя g' левого смежного класса $g\mathrm{St}(x)$ имеем $g' = gh$, где $h \in \mathrm{St}(x)$, и тогда $g'x = (gh)x = g(hx) = gx$. Сюръективность отображения ψ следует из определения орбиты Gx. Проверим инъективность. Предположим, что $g_1\mathrm{St}(x) = g_2\mathrm{St}(x)$ для некоторых $g_1, g_2 \in G$. Тогда $g_1x = g_2x$. Подействовав на левую и правую части элементом g_2^{-1}, получим $(g_2^{-1}g_1)x = x$, откуда $g_2^{-1}g_1 \in \mathrm{St}(x)$. Последнее и означает, что $g_1\mathrm{St}(x) = g_2\mathrm{St}(x)$. Итак, мы показали, что отобржание ψ является биекцией. Значит, $|Gx| = |G/\mathrm{St}(x)| = [G : \mathrm{St}(x)]$ и требуемое равенство вытекает из теоремы Лагранжа (см. лекцию 1). □

[1] Это множество может не быть факторгруппой, так как подгруппа $\mathrm{St}(x)$ не обязана быть нормальной в G.

Пример 2. Рассмотрим действие группы $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ на множестве $\mathbb{C}$, заданное формулой $(z, w) \mapsto zw$, где $z \in S^1$, $w \in \mathbb{C}$, а zw — обычное произведение комплексных чисел. Для этого действия орбитами будут множества вида $|z| = c$, где $c \in \mathbb{R}_{\geqslant 0}$, — это всевозможные окружности с центром в нуле, а также отдельная орбита, состоящая из нуля. Имеем

$$\mathrm{St}(z) = \begin{cases} \{1\}, & \text{если } z \neq 0; \\ S^1, & \text{если } z = 0. \end{cases}$$

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 10, § 3)
[2] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 1, § 3)
[3] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 13, § 57)