ЛЕКЦИЯ 5

ТОЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

ПЕРИОДИЧЕСКАЯ ЧАСТЬ

ПРИМАРНЫЕ КОМПОНЕНТЫ

КОНЕЧНЫЕ АБЕЛЕВЫ ГРУППЫ

ТОЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ (ПРОДОЛЖЕНИЕ)

Лемма 1 (о ретракте абелевых групп). *Пусть G и G' — абелевы группы.*

1) *Если $f\colon G \to G'$, $h\colon G' \to G$ — гомоморфизмы и $fh = 1_{G'}$ (пара f, h — ретракт), то*:

а) $\ker h = 0$;

б) $\operatorname{Im} f = G'$;

в) $\operatorname{Im} h \oplus \ker f = G$.

2) *Если $f\colon G \to G'$ — гомоморфизм,*

$$\operatorname{Im} f = G' \text{ и } A \oplus \ker f = G$$

для некоторой подгруппы $A \subseteq G$, то существует гомоморфизм $h\colon G' \to G$, для которого $fh = 1_{G'}$.

3) *Если $h\colon G' \to G$ — гомоморфизм,*

$$\ker h = 0 \text{ и } \operatorname{Im} h \oplus B = G$$

для некоторой подгруппы $B \subseteq G$, то существует гомоморфизм $f\colon G \to G'$, для которого $fh = 1_{G'}$.

Доказательство.

1а) Если $y \in \ker h \subseteq G$, то $h(y) = 0$, и поэтому

$$y = 1_{G'}(y) = (fh)(y) = f\bigl(h(y)\bigr) = f(0) = 0.$$

Итак, $\ker h = 0$.

1б) Если $y \in G'$, то

$$y = 1_{G'}(y) = (fh)(y) = f\bigl(h(y)\bigr) \in \operatorname{Im} f.$$

Итак, $\operatorname{Im} f = G'$.

1в) Если $x \in G$, то $x = h\bigl(f(x)\bigr) + \bigl(x - (hf)(x)\bigr)$, при этом, поскольку $fh = 1_{G'}$,

$$f\bigl(x - (hf)(x)\bigr) = f(x) - (fhf)(x) = f(x) - f(x) = 0,$$

поэтому $x - (hf)(x) \in \ker f$, $h\bigl(f(x)\bigr) \in \operatorname{Im} h$. Таким образом, $G = \operatorname{Im} h + \ker f$.

Если $z \in \operatorname{Im} h \cap \ker f$, то $z = h(y)$ для $y \in G'$ и $f(z) = 0$, поэтому

$$y = 1_{G'}(y) = (fh)(y) = f\bigl(h(y)\bigr) = f(z) = 0.$$

Таким образом, $\operatorname{Im} h \cap \ker f = 0$.

Итак, $G = \operatorname{Im} h \oplus \ker f$.

2) Так как для $f|_A \colon A \to G'$ имеем

$$\begin{gathered} f|_A(A) = f(A \oplus \ker f) = f(G) = G', \\ \ker(f|_A) = \ker f \cap A = 0, \end{gathered}$$

то $f|_A \colon A \to G'$ — изоморфизм.

Положим

$$h = (f|_A)^{-1} \colon G' \to A \subseteq G.$$

Тогда

$$fh = f(f|_A)^{-1} = 1_{G'}.$$

3) Гомоморфизм $h \colon G' \to \operatorname{Im} h$ является изоморфизмом, поскольку $\ker h = 0$. Рассмотрим изоморфизм $h^{-1} \colon \operatorname{Im} h \to G'$. Пусть $\pi \colon G = \operatorname{Im} h \oplus B \to \operatorname{Im} h$ — проекция на первое прямое слагаемое. Рассмотрим гомоморфизм

$$f = h^{-1}\pi \colon G = \operatorname{Im} h \oplus B \xrightarrow{\pi} \operatorname{Im} h \xrightarrow{h} G'.$$

Тогда для $g' \in G'$ имеем

$$(fh)(g') = f\bigl(h(g')\bigr) = h^{-1}\Bigl(\pi\bigl(h(g')\bigr)\Bigr) = h^{-1}\bigl(h(g')\bigr) = g'.$$

Таким образом, $fh = 1_{G'}$. $\square$

Теорема 1 (условия расщепления короткой точной последовательности абелевых групп). *Пусть*

$$0 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 0 \text{ — }$$

короткая точная последовательность абелевых групп ($\ker i = 0,\ \operatorname{Im} i = \ker \pi,\ \operatorname{Im} \pi = C$). *Тогда эквивалентны следующие условия*:

1) *существует гомоморфизм* $j\colon B \to A$, *для которого* $ji = 1_A$ (*расщепляемость последовательности слева*);

2) *существует гомоморфизм* $\rho\colon C \to B$, *для которого* $\pi\rho = 1_C$ (*расщепляемость последовательности справа*).

Доказательство. а) Пусть выполнено условие 1). Тогда в силу леммы о ретракте (п. 1с) для ретракта

$$i : A \to B,\ j : B \to A, \quad ji = 1_A,$$

имеем:

$$\operatorname{Im} i \oplus \ker j = B.$$

Так как $\operatorname{Im} i = \ker \pi$, то

$$\ker \pi \oplus \ker j = B.$$

Это позволяет применить к гомоморфизму $\pi\colon B \to C$ ($\operatorname{Im} \pi = C$, $\ker j \oplus \ker \pi = B$) лемму о ретракте. Тогда существует гомоморфизм $\rho\colon C \to B$, для которого $\pi\rho = 1_C$. Таким образом, из 1) следует 2).

б) Пусть выполнено условие 2). Применяя к ретракту

$$\pi : B \to C,\ \rho : C \to B, \quad \pi\rho = 1_C,$$

лемму о ретракте (п. 1с), имеем $\operatorname{Im} \rho \oplus \ker \pi = B$. Так как $\operatorname{Im} i = \ker \pi$, то $\operatorname{Im} i \oplus \operatorname{Im} \rho = B$. Это позволяет применить к гомоморфизму $i\colon A \to B$ ($\ker i = 0,\ \operatorname{Im} i \oplus \operatorname{Im} \rho = B$) лемму о ретракте (п. 3). Тогда существует гомоморфизм $j\colon B \to A$, для которого $ji = 1_A$. Таким образом, из 2) следует 1). □

ПЕРИОДИЧЕСКАЯ ЧАСТЬ АБЕЛЕВОЙ ГРУППЫ

Как мы видели, совокупность

$$\mathbf{T}(G) = \{g \in G \mid O(g) < \infty\}$$

элементов некоммутативной группы может не быть подгруппой (например, $\mathbf{T}(\operatorname{GL}_2(\mathbb{Z}))$). Для абелевых групп A элементы конечного порядка образуют подгруппу, называемую *периодической частью* группы A. Периодическая часть $\mathbf{T}(A)$ абелевой группы — важный инвариант группы A.

Если $\mathbf{T}(A) = 0$ (в группе A все ненулевые элементы имеют бесконечный порядок), то будем говорить, что группа A — без кручения.

Теорема 2. *Пусть A — абелева группа,*

$$\mathbf{T}(A) = \{a \in A \mid O(a) < \infty\} -$$

ее периодическая часть. Тогда:

1) $\mathbf{T}(A)$ — *периодическая подгруппа группы* A;

2) $\mathbf{T}\big(A/\mathbf{T}(A)\big) = 0$ (*другими словами,* $A/\mathbf{T}(A)$ — *группа без кручения*).

Доказательство. 1) Если $a, b \in \mathbf{T}(A)$, $ra = 0 = sb$, $r > 0$, $s > 0$, $r, s \in \mathbb{N}$, то

$$rs(a + b) = s(ra) + r(sb) = 0 + 0 = 0, \quad r, s > 0,$$
$$r(-a) = -ra = 0, \quad r > 0,$$

и поэтому $a + b \in \mathbf{T}(A)$, $-a \in \mathbf{T}(A)$. Таким образом, $\mathbf{T}(A)$ — подгруппа группы A. Конечно, $\mathbf{T}(A)$ — периодическая группа.

2) Если $a + \mathbf{T}(A) \in \mathbf{T}(A/\mathbf{T}(A))$, то

$$s\big(a + \mathbf{T}(A)\big) = sa + \mathbf{T}(A) = \bar{0} = \mathbf{T}(A), \quad s > 0,$$

поэтому $sa \in \mathbf{T}(A)$. Следовательно,

$$r(sa) = (rs)a = 0, \quad r > 0.$$

Так как $rs > 0$, то $a \in \mathbf{T}(A)$, и поэтому $a + \mathbf{T}(A) = \mathbf{T}(A) = \bar{0}$. Итак, $\mathbf{T}\big(A/\mathbf{T}(A)\big) = \bar{0}$. □

Замечание 1. Эта теорема объясняет, почему структурная теория абелевых групп разбивается на три части:

1-я часть посвящена изучению периодических абелевых групп (когда $\mathbf{T}(A) = A$);

2-я часть заключается в изучении абелевых групп A без кручения (когда $\mathbf{T}(A) = 0$);

3-я часть анализирует в общем случае расширение

$$0 \to \mathbf{T}(A) \to A \to A/\mathbf{T}(A) \to 0$$

периодической группы A с помощью группы $A/\mathbf{T}(A)$ без кручения.

ПРИМАРНЫЕ КОМПОНЕНТЫ

Теорема 3 (о разложении периодической абелевой группы в прямую сумму примарных компонент). *Пусть A — периодическая абелева группа.*

1) *Если p — простое число,*

$$A_p = \{a \in A \mid O(a) = p^k,\ k \geq 1\} -$$

p-примарная компонента *группы A, то A_p — подгруппа группы A*;

2) $A = \bigoplus\limits_p A_p$;

3) *если $A = \bigoplus\limits_p A'_p$, где A'_p — абелева p-группа (т. е. все ненулевые элементы группы A'_p имеют порядки, являющиеся степенями простого числа p), то $A'_p = A_p$.*

Доказательство.

1) Если $x, y \in A_p$, $p^m x = 0$, $p^n y = 0$, $m \geq 1$, $n \geq 1$, $t = \max(m, n)$, то:

$$\begin{aligned} p^t(x+y) &= p^t x + p^t y = 0 + 0 = 0, \\ p^m(-x) &= -p^m x = 0, \end{aligned}$$

и поэтому $x + y, -x \in A_p$. Таким образом, A_p — подгруппа группы A.

2) Если $a \in A$ и $n = O(a) = p_1^{k_1} \ldots p_r^{k_r}$, где $p_1, \ldots, p_r$ — различные простые числа, то числа $\langle n_i = n/p_i^{k_i} \rangle$ взаимно просты, и поэтому

$$1 = t_1 n_1 + \ldots + t_r n_r, \quad t_i \in \mathbb{Z}.$$

Тогда

$$a = 1 \cdot a = \sum_{i=1}^{r} t_i(n_i a),$$

где $n_i a \in A_{p_i}$, поскольку $p_i^{k_i}(n_i a) = na = 0$. Таким образом,

$$a \in \sum_{i=1}^{r} A_{p_i} \subseteq \sum_{p} A_p.$$

Итак, $A = \sum\limits_{p} A_p$.

Если

$$b \in A_{p_1} + \ldots + A_{p_k},$$

то

$$O(b) = \prod_{i=1}^{k} p_i^{l_i}, \quad l_i \geq 0.$$

Если $q \notin \{p_1, \ldots, p_k\}$ — другое простое число, отличное от p_i, то

$$A_q \cap (A_{p_1} + \ldots + A_{p_k}) = 0.$$

Итак,

$$A = \bigoplus_{p} A_p$$

3) Ясно, что $A'_p \subseteq A_p$ для любого простого числа p (A_p содержит все элементы, порядки которых являются степенями простого числа p).

Если $0 \neq x \in \bigoplus\limits_p A'_p$, то

$$x = x_{p_1} + \ldots + x_{p_k} \in \sum_i A'_{p_i}, \quad x_{p_i} \neq 0,$$

и поэтому $O(x) = p_1^{l_1} \ldots p_k^{l_k}$, $l_i \geq 1$. Если $0 \neq x \notin A'_p$, то найдется $p_i \neq p$ (иначе $x = x_p \in A'_p$), и тогда $x \notin A_p$, поскольку в A_p все элементы имеют своими порядками степени простого числа p.

Итак, $A'_p = A_p$. □

В силу доказанной теоремы теория периодических абелевых групп сводится к теории примарных абелевых групп.

Теорема 4. *Конечно порожденная периодическая* абелева *группа конечна.*

Доказательство. Пусть $A = \langle a_1, \ldots, a_n \rangle$ — периодическая абелева группа, порожденная элементами $a_1, \ldots, a_n$, $O(a_i) = m_i < \infty$. Если $a \in A$, то

$$a = k_1 a_1 + \ldots + k_n a_n, \quad 0 \leq k_i < m_i,$$

и поэтому $|A| \leq m_1 m_2 \ldots m_n$. □

Замечание 2. Для неабелевых периодических групп одной из основных была следующая проблема Бернсайда: конечна ли конечно порожденная группа G, в которой $x^n = e$ для всех $x \in G$? Отрицательное решение было получено С. И. Адяном и П. С. Новиковым.

КОНЕЧНЫЕ АБЕЛЕВЫ ГРУППЫ

Классификация (с точностью до изоморфизма) конечных абелевых групп воспринималась как один из триумфов алгебры XIX века и сразу нашла приложения в алгебре, теории чисел, топологии, комбинаторике. В каком-то смысле это уникальный факт теории абелевых групп, то, что удалось конструктивно описать строение конечных объектов. Совсем не такая простая ситуация с классификацией конечных объектов как в теории некоммутативных групп (отметим лишь один из самых крупных математических проектов, связанный с классификацией конечных простых групп), так и в теории колец (описание строения конечных полей — это лишь начало загадочной истории об описании строения конечных колец).

Теорема 5 (о разложении конечной абелевой группы в прямую сумму примарных компонент). *Пусть* A *— конечная абелева группа порядка* $|A| = n = p_1^{r_1} \dots p_t^{r_t}$, *где* $p_1, \dots, p_t$ *— различные простые числа,* $r_i \geq 1$. *Тогда*:

1) $A = A_{p_1} \oplus \dots \oplus A_{p_t}$, *где* $|A_{p_i}| = p_i^{r_i}$;

2) *это прямое разложение конечной абелевой группы* A *единственно, а именно если* $A = B_1 \oplus \dots \oplus B_t$, *где* $|B_i| = p_i^{r_i'}$, *то* $r_i' = r_i$ *для всех* $1 \leq i \leq t$, *и* $B_i = A_{p_i}$.

Доказательство, конечно, непосредственно следует из теоремы 3 о разложении любой периодической абелевой группы в прямую сумму примарных компонент. □

Замечание 3. Данная теорема сводит изучение конечных абелевых групп к рассмотрению их примарных компонент, являющихся конечными примарными абелевыми группами.

В следующей ключевой лемме мы сосредоточим внимание уже на конечной примарной абелевой группе.

Лемма 2. *Пусть A — конечная абелева p-группа, $a \in A$ — элемент с максимальным порядком $O(a) = p^r$ в группе A. Тогда $A = \langle a \rangle \oplus H$ для некоторой подгруппы H (другими словами, циклическая подгруппа $\langle a \rangle$, порожденная элементом a, является прямым слагаемым группы A).*

Доказательство. Выберем в нашей конечной группе A максимальную подгруппу H среди всех подгрупп со свойством $H \cap \langle a \rangle = 0$.

Рассмотрим подгруппу $\langle H, a \rangle = H \oplus \langle a \rangle = A_0$. Если $A_0 = A$, то наша лемма доказана.

Допустим теперь, что $A_0 \neq A$, и приведем это предположение к противоречию. Так как $A_0 \neq A$, то выберем в $A \setminus A_0$ элемент x *наименьшего порядка.* Так как в p-группе A

$$O(px) = \frac{O(x)}{p} < O(x),$$

то $px \in A_0 = \langle a \rangle \oplus H$, и поэтому

$$px = la + y, \quad l \in \mathbb{Z}, \quad y \in H.$$

Так как p^r — наибольший порядок элементов нашей p-группы A, то

$$p^{r-1}la + p^{r-1}y = p^{r-1}(px) = p^r x = 0.$$

Следовательно,

$$p^{r-1}la = -p^{r-1}y \in \langle a \rangle \cap H = 0.$$

Поэтому $p^{r-1}l$ делится на $p^r = O(a)$, и тогда $l = pq$. Таким образом,

$$px = la + y = pqa + y,$$

и поэтому

$$p(x - qa) = y \in H.$$

Но $x - qa \notin H$, поскольку если $x - qa \in H$, то

$$x \in qa + H \subseteq \langle a \rangle + H = A_0,$$

что противоречит выбору элемента $x \notin A_0$.

Итак,

$$H < \langle x - qa \rangle + H,$$

поэтому в силу максимальности выбора подгруппы H

$$(\langle x - qa\rangle + H) \cap \langle a\rangle \neq 0.$$

Следовательно, найдутся числа $k, m \in \mathbb{Z}$ и элемент $y' \in H$, для которых

$$m(x - qa) + y' = ka \neq 0.$$

Отсюда следует, что

$$mx - mqa + y' = ka,$$

и поэтому

$$mx = (mq + k)a - y' \in \langle a\rangle + H = A_0.$$

Если p делит число m, $m = pt$, то, поскольку

$$p(x - qa) = y \in H,$$

имеем

$$m(x - qa) = tp(x - qa) = ty \in H,$$

и поэтому

$$ka = m(x - qa) + y' \in H + H = H.$$

Итак, $ka \in \langle a\rangle \cap H = 0$, но это противоречит тому, что $ka \neq 0$.

Следовательно, m не делится на p, и поэтому

$$1 = (p, m) = up + vm, \quad u, v \in \mathbb{Z}.$$

Поскольку $px \in A_0$ и $mx \in A_0$, приходим к противоречию с выбором элемента x:

$$x = (up + vm)x = u(px) + v(mx) \in A_0 + A_0 = A_0. \qquad \square$$

В качестве непосредственного следствия леммы получаем теорему о строении конечной абелевой p-группы.

Теорема 6. 1) *Каждая конечная абелева p-группа A, $|A| = p^r$, $r \geq 1$, разлагается в прямую сумму p-примарных циклических групп (далее не разложимых в прямую сумму)*

$$A = A_1 \oplus \ldots \oplus A_k, \quad A_i = \langle a_i \rangle, \quad O(a_i) = p_i^{c_i}, \quad 1 \leq c_1 \leq c_2 \leq \ldots \leq c_k,$$
$$|A| = p^r = p^{c_1+c_2+\ldots+c_k}, \quad r = c_1 + c_2 + \ldots + c_k,$$
$$A \cong \mathbb{Z}_{p^{c_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{c_k}}.$$

2) *последовательность* элементарных делителей

$$p^{c_1}, \ldots, p^{c_k}, \quad c_1 \leq c_2 \leq \ldots \leq c_k$$

(*совпадающая в этом случае с последовательностью* инвариантных множителей $1 \leq d_1 = p^{c_1} \mid d_2 = p^{c_2} \mid \ldots \mid d_k = p^{c_k}$) *определена однозначно, а именно*: *если*

$$A \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p^{c_i}} \cong \bigoplus_{j=1}^{l} \mathbb{Z}_{p^{c'_j}},$$
$$1 \leq c_1 \leq c_2 \leq \ldots \leq c_k, \quad 1 \leq c'_1 \leq c'_2 \leq \ldots \leq c'_l,$$

то $k = l$, $c_1 = c'_1, \ldots, c_k = c'_k$.

Доказательство.

1) В силу доказанной леммы: $A = \langle a \rangle \oplus H$, $a \in A$, $O(a)$ — максимальный порядок элементов группы A. Проведем индукцию по $|A|$. Пусть, в силу индуктивного предположения,

$$H = A_1 \oplus \ldots \oplus A_{k-1}, \quad A_i = \langle a_i \rangle, \quad O(a_i) = p^{c_i}, \quad 1 \leq c_1 \leq \ldots \leq c_{k-1},$$

при этом $p^{c_{k-1}} \leq O(a)$. Полагая $a_k = a$, $p^{c_k} = O(a)$, $A_k = \langle a \rangle$, получаем, что

$$A = A_1 \oplus \ldots \oplus A_{k-1} \oplus A_k,$$
$$A_i = \langle a_i \rangle, \quad O(a_i) = p^{c_i}, \quad 1 \leq c_1 \leq c_2 \leq \ldots \leq c_{k-1} \leq c_k,$$

и следовательно,

$$|A| = p^r = p^{c_1+c_2+\ldots+c_k}, \quad r = c_1 + \ldots + c_k,$$
$$A \cong \mathbb{Z}_{p^{c_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{c_k}}.$$

Как мы отмечали, прямые слагаемые $A_i \cong \mathbb{Z}_{p^{c_i}}$, являющиеся примарными циклическими группами, далее в нетривиальную прямую сумму уже не разлагаются.

2а) Пусть

$$A \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p^{c_i}} \cong \bigoplus_{j=1}^{l} \mathbb{Z}_{p^{c'_j}},$$
$$1 \le c_1 \le c_2 \le \ldots \le c_k, \quad 1 \le c'_1 \le c'_2 \le \ldots \le c'_l.$$

Для доказательства равенства $k = l$ вычислим, используя эти два прямых разложения, подгруппу $A[p] = \{x \in A \mid px = 0\}$ группы A, зная, что

$$\left(\bigoplus_{i=1}^{k} A_i\right)[p] = \bigoplus_{i=1}^{k} A_i[p]$$

и

$$(\mathbb{Z}_{p^t})[p] \cong \mathbb{Z}_p$$

(см. **??**):

$$A[p] \cong \bigoplus_{i=1}^{k} (\mathbb{Z}_{p^{c_i}})[p] \cong \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{k},$$
$$A[p] \cong \bigoplus_{j=1}^{l} (\mathbb{Z}_{p^{d_j}})[p] \cong \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{l}.$$

Поэтому $|A[p]| = p^k = p^l$, и следовательно, $k = l$.

2б) Допустим противное, т. е. что последовательности $(c_1, \ldots, c_k)$ и $(c'_1, \ldots, c'_k)$, $k = l$, различны. Пусть u — такой индекс, что $c_1 = c'_1, \ldots$, $c_{u-1} = c'_{u-1}$, $c_u \neq c'_u$, скажем $c_u < c'_u$. Так как $p^{c_u}\mathbb{Z}_{p^{c_i}} = 0$ для $c_i \le c_u$, то, используя первое разложение и **??**, получаем

$$p^{c_u} A \cong \bigoplus_{i=1}^{k} p^{c_u} \mathbb{Z}_{p^{c_i}} \cong \bigoplus_{i=u+1}^{k} \mathbb{Z}_{p^{c_i - c_u}},$$

где

$$c_{u+1} - c_u \le c_{u+2} - c_u \le \ldots \le c_k - c_u$$

(здесь $k-u$ ненулевых прямых слагаемых). Поскольку $c_i = c'_i$ для $i < u$ и $c_u < c'_u$, то, используя второе разложение, получаем

$$p^{c_u} A \cong \bigoplus_{j=1}^{k=l} p^{c_u} \mathbb{Z}_{p^{c'_j}} \cong \bigoplus_{i=u}^{k=l} \mathbb{Z}_{p^{c'_j - c_u}},$$

где

$$1 \leq c'_u - c_u \leq c'_{u+1} - c_u \leq \ldots \leq c'_k - c_u, \quad k = l$$

(здесь $k-(u-1) = (k-u)+1$ ненулевых прямых слагаемых).

Таким образом, для конечной абелевой p-группы $p^{c_u} A$ получили два разложения в прямую сумму ненулевых p-примарных циклических групп, содержащих разное число слагаемых ($k-u$ и $(k-u)+1$ соответственно), что невозможно в силу уже доказанного утверждения 2a). Тем самым мы пришли к противоречию, что завершает доказательство. $\square$