ЛЕКЦИЯ 7

ПРИМАРНЫЕ КОМПОНЕНТЫ

КОНЕЧНЫЕ АБЕЛЕВЫ ГРУППЫ

СВОБОДНЫЕ АБЕЛЕВЫ ГРУППЫ

ПРИМАРНЫЕ КОМПОНЕНТЫ

Теорема 1 (о разложении периодической абелевой группы в прямую сумму примарных компонент)**.** *Пусть A — периодическая абелева группа.*

1) *Если p — простое число,*

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

— 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 $n = O(a) = p_1^{k_1} \dots p_r^{k_r}$, где $p_1, \dots, p_r$ — 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, $A'_p = A_p$. $\square$

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

Теорема 2. *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

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

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

Замечание 1. 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 3 (о разложении конечной абелевой группы в прямую сумму примарных компонент)**.** *Пусть A — конечная абелева группа порядка $|A| = n = p_1^{r_1} \ldots p_t^{r_t}$, где $p_1, \ldots, p_t$ — различные простые числа, $r_i \geqslant 1$. Тогда*:

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

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

Доказательство, конечно, непосредственно следует из теоремы 1 о разложении любой периодической абелевой группы в прямую сумму примарных компонент. $\square$

Замечание 2. 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 1. *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 4. 1) *Каждая конечная абелева p-группа A, $|A| = p^r$, $r \geqslant 1$, разлагается в прямую сумму p-примарных циклических групп* (*далее не разложимых в прямую сумму*)

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

2) *последовательность* элементарных делителей

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

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

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

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

Доказательство.

1) В силу доказанной леммы:

$$A = \langle a \rangle \oplus H, \quad a \in A,$$

$O(a)$ — максимальный порядок элементов группы A. Проведем индукцию по $|A|$.

Пусть, в силу индуктивного предположения,

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

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

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

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

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

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 $c_i \leqslant c_u$, 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

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

(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

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

(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 2а). Тем самым мы пришли к противоречию, что завершает доказательство. $\square$

Теперь мы готовы собрать вместе все полученные факты, сформулировать и доказать основную теорему о конечных абелевых группах.

Теорема 5 (о строении и классификации конечных абелевых групп)**.**

1) *Конечная абелева группа* A *порядка* $n = |A| = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$, *где* $\{p_1, p_2, \dots, p_t\}$ *— все различные простые делители числа* n, $r_i \geqslant 1$, $1 \leqslant i \leqslant t$, *разлагается в прямую сумму примарных циклических групп*

$$A = \bigoplus_{i=1}^{t} \Big(\bigoplus_{j=1}^{k_i} A_{ij} \Big), \quad A_{ij} = \langle a_{ij} \rangle, \quad O(a_{ij}) = p_i^{c_{ij}},$$

где

$$\begin{cases} 1 \leqslant c_{11} \leqslant c_{12} \leqslant \ldots \leqslant c_{1k_1}, \\ \ldots \\ 1 \leqslant c_{t1} \leqslant c_{t2} \leqslant \ldots \leqslant c_{tk_t}, \end{cases}$$

$$n = |A| = p_1^{c_{11}+\ldots+c_{1k_1}} p_2^{c_{21}+\ldots+c_{2k_2}} \dots p_t^{c_{t1}+\ldots+c_{tk_t}} = \prod_{i=1}^{t} \prod_{j=1}^{k_i} p_i^{c_{ij}},$$

$$r_1 = c_{11} + \ldots + c_{1k_1}, \dots, \; r_t = c_{t1} + \ldots + c_{tk_t}.$$

Таким образом,

$$A \cong \bigoplus_{i=1}^{t} \Big(\bigoplus_{j=1}^{k_j} \mathbb{Z}_{p_j^{c_{ij}}} \Big).$$

2) *Таблица элементарных делителей*

$$
\begin{array}{ll}
p_1^{c_{11}}, p_1^{c_{12}}, \ldots, p_1^{c_{1k_1}}, & 1 \leqslant c_{11} \leqslant c_{12} \leqslant \ldots \leqslant c_{1k_1}, \\
p_2^{c_{21}}, p_2^{c_{22}}, \ldots, p_2^{c_{2k_2}}, & 1 \leqslant c_{21} \leqslant c_{22} \leqslant \ldots \leqslant c_{2k_2}, \\
\ldots & \\
p_t^{c_{t1}}, p_t^{c_{t2}}, \ldots, p_t^{c_{tk_t}}, & 1 \leqslant c_{t1} \leqslant c_{t2} \leqslant \ldots \leqslant c_{tk_t},
\end{array}
$$

прямого разложения в п. 1) *определена однозначно и однозначно определяет конечную абелеву группу* A (*с точностью до изоморфизма*).

Доказательство.

1) В силу теоремы о разложении конечной абелевой группы A, $|A| = p_1^{r_1} \dots p_t^{r_t}$, имеем

$$A = \bigoplus_{i=1}^{t} A_{p_i}, \quad |A_{p_i}| = p_i^{r_i}.$$

Применяя к каждой конечной абелевой p_i-группе A_{p_i} теорему 4 о строении конечных абелевых p-групп, получаем

$$A_{p_i} = \bigoplus_{j=1}^{k_i} A_{ij}, \quad A_{ij} = \langle a_{ij} \rangle, \quad O(a_{ij}) = p_i^{c_{ij}},$$

где

$$1 \leqslant c_{i1} \leqslant c_{i2} \leqslant \ldots \leqslant c_{ik_i}, \quad |A_{p_i}| = p_i^{c_{i1}+\ldots+c_{ik_i}} = p_i^{r_i}.$$

Таким образом,

$$A = \bigoplus_{i=1}^{t} \Big(\bigoplus_{j=1}^{k_i} A_{ij} \Big), \quad A_{ij} = \langle a_{ij} \rangle, \quad O(a_{ij}) = p_i^{c_{ij}},$$

$$\begin{cases} 1 \leqslant c_{11} \leqslant c_{12} \leqslant \ldots \leqslant c_{1k_1}, \\ \ldots \\ 1 \leqslant c_{t1} \leqslant c_{t2} \leqslant \ldots \leqslant c_{tk_t}, \end{cases}$$

$$n = |A| = p_1^{r_1} \dots p_t^{r_t} = p_1^{c_{11}+\ldots+c_{1k_1}} p_2^{c_{21}+\ldots+c_{2k_2}} \dots p_t^{c_{t1}+\ldots+c_{tk_t}},$$

поэтому

$$r_1 = c_{11} + \ldots + c_{1k_1}, \ldots, \; r_t = c_{t1} + \ldots + c_{tk_t}.$$

Отсюда следует, что

$$A \cong \bigoplus_{i=1}^{t} \Big(\bigoplus_{j=1}^{k_i} \mathbb{Z}_{p_i^{c_{ij}}} \Big).$$

2) Пусть

$$\begin{aligned}
&p_1^{d_{11}}, p_1^{d_{12}}, \ldots, p_1^{d_{1l_1}}, \quad 1 \leqslant d_{11} \leqslant d_{12} \leqslant \ldots \leqslant d_{1l_1},\\
&p_2^{d_{21}}, p_2^{d_{22}}, \ldots, p_2^{d_{2l_2}}, \quad 1 \leqslant d_{21} \leqslant d_{22} \leqslant \ldots \leqslant d_{2l_2},\\
&\ldots\\
&p_t^{d_{t1}}, p_t^{d_{t2}}, \ldots, p_t^{d_{tl_t}}, \quad 1 \leqslant d_{t1} \leqslant d_{t2} \leqslant \ldots \leqslant d_{tl_t},
\end{aligned}$$

— таблица элементарных делителей другого разложения конечной абелевой группы A в прямую сумму примарных циклических групп,

$$A = \bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{l_i} A'_{ij} \right), \quad A'_{ij} = \langle a'_{ij} \rangle, \quad O(a'_{ij}) = p_i^{d_{ij}},$$

$$n = |A| = p_1^{r_1} \ldots p_t^{r_t} = p_1^{d_{11}+\ldots+d_{1l_1}} p_2^{d_{21}+\ldots+d_{2l_2}} \ldots p_t^{d_{t1}+\ldots+d_{tl_t}},$$

$$r_1 = d_{11} + \ldots + d_{1l_1}, \ldots, \; r_t = d_{t1} + \ldots + d_{tl_t}.$$

Для каждого простого числа $p_i \in \{p_1, \ldots, p_t\}$ вычислим однозначно определенную p_i-примарную компоненту A_{p_i} конечной абелевой группы A_i по первому и второму разложениям (см. теорему о единственности разложения в сумму примарных абелевых групп по разным простым числам):

$$A_{p_i} = \bigoplus_{j=1}^{k_i} A_{ij} = \bigoplus_{j=1}^{l_i} A'_{ij},$$

$$|A_{ij}| = p_i^{c_{ij}}, \;\; |A'_{ij}| = p_i^{d_{ij}}, \;\; 1 \leqslant c_{i1} \leqslant \ldots \leqslant c_{ik_i}, \;\; 1 \leqslant d_{i1} \leqslant \ldots \leqslant d_{il_i},$$

$$|A_{p_i}| = p_i^{r_i} = p_i^{c_{i1}+\ldots+c_{ik_i}} = p_i^{d_{i1}+\ldots+d_{il_i}}.$$

К p_i-примарной конечной абелевой группе A_{p_i} применим теорему о единственности последовательности элементарных делителей):

$$k_i = l_i, \quad c_{i1} = d_{i1}, \ldots, \ c_{ik_i} = d_{ik_i} = d_{il_i}.$$

Таким образом, таблица элементарных делителей, определяющая разложение конечной абелевой группы в прямую сумму примарных циклических групп, определена однозначно. Ясно, что две прямые суммы примарных циклических групп с одной и той же таблицей элементарных делителей изоморфны. $\square$