

ЛЕКЦИЯ 6

КОНЕЧНЫЕ АБЕЛЕВЫ ГРУППЫ

СВОБОДНЫЕ АБЕЛЕВЫ ГРУППЫ

СТРУКТУРНАЯ ТЕОРЕМА

КОНЕЧНЫЕ АБЕЛЕВЫ ГРУППЫ

Напомним ключевую лемму, которую мы доказали на прошлой лекции.

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).

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

ТЕОРЕМА 1. 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)

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

2) последовательность элементарных делителей

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

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

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

$$1 \leq c_1 \leq c_2 \leq \dots \leq c_k, \quad 1 \leq c'_1 \leq c'_2 \leq \dots \leq c'_l,$$

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

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,

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

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

$$A = A_1 \oplus \dots \oplus A_{k-1} \oplus A_k,$$

$$A_i = \langle a_i \rangle, \quad O(a_i) = p^{c_i}, \quad 1 \leq c_1 \leq c_2 \leq \dots \leq c_{k-1} \leq c_k,$$

и следовательно,

$$|A| = p^r = p^{c_1+c_2+\dots+c_k}, \quad r = c_1 + \dots + c_k,$$

$$A \cong \mathbb{Z}_{p^{c_1}} \oplus \dots \oplus \mathbb{Z}_{p^{c_k}}.$$

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

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

$$1 \leq c_1 \leq c_2 \leq \dots \leq c_k, \quad 1 \leq c'_1 \leq c'_2 \leq \dots \leq c'_l.$$

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

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

$$A[p] \cong \bigoplus_{i=1}^k (\mathbb{Z}_{p^{c_i}}) [p] \cong \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_k$$

$$A[p] \cong \bigoplus_{j=1}^l (\mathbb{Z}_{p^{d_j}}) [p] \cong \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_l$$

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

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

$$c_{u+1} - c_u \leq c_{u+2} - c_u \leq \dots \leq c_k - c_u$$

(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

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

(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 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 2 (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 , $r_i \geq 1$, $1 \leq i \leq t$, разлагается в прямую сумму примарных циклических групп

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

где

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

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

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

Таким образом,

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

2) Таблица элементарных делителей

$$\begin{aligned} p_1^{c_{11}}, p_1^{c_{12}}, \dots, p_1^{c_{1k_1}}, & \quad 1 \leq c_{11} \leq c_{12} \leq \dots \leq c_{1k_1}, \\ p_2^{c_{21}}, p_2^{c_{22}}, \dots, p_2^{c_{2k_2}}, & \quad 1 \leq c_{21} \leq c_{22} \leq \dots \leq c_{2k_2}, \\ \dots & \\ p_t^{c_{t1}}, p_t^{c_{t2}}, \dots, p_t^{c_{tk_t}}, & \quad 1 \leq c_{t1} \leq c_{t2} \leq \dots \leq c_{tk_t}, \end{aligned}$$

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 1 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

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

Таким образом,

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

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

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

ПОЭТОМУ

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

Отсюда следует, что

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

2) Пусть

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

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

$$\begin{aligned} A = \bigoplus_{i=1}^t \left(\bigoplus_{j=1}^{l_i} A'_{ij} \right), \quad A'_{ij} = \langle a'_{ij} \rangle, \quad O(a'_{ij}) = p_i^{d_{ij}}, \\ n = |A| = p_1^{r_1} \dots p_t^{r_t} = p_1^{d_{11} + \dots + d_{1l_1}} p_2^{d_{21} + \dots + d_{2l_2}} \dots p_t^{d_{t1} + \dots + d_{tl_t}}, \\ r_1 = d_{11} + \dots + d_{1l_1}, \dots, \quad r_t = d_{t1} + \dots + d_{tl_t}. \end{aligned}$$

Для каждого простого числа $p_i \in \{p_1, \dots, p_t\}$ 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):

$$\begin{aligned} A_{p_i} = \bigoplus_{j=1}^{k_i} A_{ij} = \bigoplus_{j=1}^{l_i} A'_{ij}, \\ |A_{ij}| = p_i^{c_{ij}}, \quad |A'_{ij}| = p_i^{d_{ij}}, \quad 1 \leq c_{i1} \leq \dots \leq c_{ik_i}, \quad 1 \leq d_{i1} \leq \dots \leq d_{il_i}, \\ |A_{p_i}| = p_i^{r_i} = p_i^{c_{i1} + \dots + c_{ik_i}} = p_i^{d_{i1} + \dots + d_{il_i}}. \end{aligned}$$

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

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

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

СВОБОДНЫЕ АБЕЛЕВЫ ГРУППЫ

Совокупность элементов $\{e_1, \dots, e_m\}$ абелевой группы F называется *базисом*, если:

1) любой элемент $a \in F$ является целочисленной линейной комбинацией

$$a = k_1 e_1 + \dots + k_m e_m, \quad k_i \in \mathbb{Z};$$

2) совокупность элементов $\{e_1, \dots, e_m\}$ линейно независима над \mathbb{Z} :
если

$$l_1 e_1 + \dots + l_m e_m, \quad l_i \in \mathbb{Z},$$

то

$$l_1 = l_2 = \dots = l_m = 0.$$

ЗАМЕЧАНИЕ 1. а) Из условий 1) и 2) следует:
если

$$a = k_1 e_1 + \dots + k_n e_n = k'_1 e_1 + \dots + k'_n e_n, \quad k_i, k'_i \in \mathbb{Z},$$

то

$$k_1 = k'_1, \dots, k_n = k'_n.$$

Действительно,

$$0 = (k_1 - k'_1)e_1 + \dots + (k_n - k'_n)e_n,$$

в силу 2)

$$k_1 - k'_1 = 0, \dots, k_n - k'_n = 0.$$

б) Из 1) и 2') следует 2). *Действительно,*

$$l_1 e_1 + \dots + l_n e_n = 0 = 0 \cdot e_1 + \dots + 0 \cdot e_n,$$

в силу 2')

$$l_1 = 0, \dots, l_n = 0.$$

в) Таким образом, системы условий $\{1), 2)\}$ и $\{1), 2')\}$ равносильны, при этом отображение

$$a = k_1 e_1 + \dots + k_n e_n \in F \mapsto (k_1, \dots, k_n) \in \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n$$

является изоморфизмом,

$$F \cong \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n.$$

Если абелева группа F обладает базисом $\{e_1, \dots, e_n\}$, то она называется *свободной абелевой группой*.

ЛЕММА 2. Если $\{e_1, \dots, e_m\}$ и $\{f_1, \dots, f_n\}$ — два базиса свободной абелевой группы F , то $m = n$ (это число n называется рангом свободной абелевой группы F , обозначение: $m = n = \text{rk}(F)$, $F = F_n$).

Доказательство. Если $f: G \rightarrow G'$ — изоморфизм абелевых групп, то $f(2G) = 2f(G) = 2G'$, и поэтому отображение

$$\bar{f}: G/2G \rightarrow G'/2G', \quad x + 2G \mapsto f(x) + 2G',$$

является изоморфизмом групп.

Так как

$$F \cong \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_m \cong \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n,$$

то

$$2F \cong \underbrace{2\mathbb{Z} \oplus \dots \oplus 2\mathbb{Z}}_m \cong \underbrace{2\mathbb{Z} \oplus \dots \oplus 2\mathbb{Z}}_n,$$

и поэтому

$$F/2F \cong \underbrace{\mathbb{Z}_2 \oplus \dots \oplus \mathbb{Z}_2}_m \cong \underbrace{\mathbb{Z}_2 \oplus \dots \oplus \mathbb{Z}_2}_n.$$

Таким образом, $2^m = 2^n$, следовательно, $m = n$. □

ЛЕММА 3. Пусть $\{e_1, \dots, e_n\}$ — один из базисов свободной абелевой группы F_n ранга n , A — абелева группа, $f, g: F_n \rightarrow A$ — два гомоморфизма такие, что $f(e_i) = g(e_i)$, $1 \leq i \leq n$. Тогда $f = g$.

Доказательство. Для любого $x \in F_n$ имеем

$$x = k_1 e_1 + \dots + k_n e_n, \quad k_i \in \mathbb{Z},$$

ПОЭТОМУ

$$f(x) = \sum_{i=1}^n k_i f(e_i) = \sum_{i=1}^n k_i g(e_i) = g(x).$$

Итак, $f = g$. □

ЛЕММА 4. $F = F_m \oplus F_n \cong F_{m+n}$.

Доказательство. Пусть $\{e_1, \dots, e_m\}, \{f_1, \dots, f_n\}$ — базисы свободных абелевых групп F_m и F_n соответственно. Тогда $\{e_1, \dots, e_m, f_1, \dots, f_n\}$ — базис абелевой группы $F_m \oplus F_n$.

Действительно, если $a \in F_m \oplus F_n$, то $a = b + c$, где $b \in F_m$, $c \in F_n$.
Поэтому

$$b = k_1 e_1 + \dots + k_m e_m, \quad c = l_1 f_1 + \dots + l_n f_n, \quad k_i, l_j \in \mathbb{Z},$$

и следовательно,

$$a = b + c = k_1 e_1 + \dots + k_m e_m + l_1 f_1 + \dots + l_n f_n.$$

Если же

$$t_1 e_1 + \dots + t_m e_m + t_{m+1} f_1 + \dots + t_{m+n} f_n = 0,$$

то

$$t_1 e_1 + \dots + t_m e_m = -(t_{m+1} f_1 + \dots + t_{m+n} f_n) \in F_m \cap F_n = 0,$$

и поэтому

$$t_1 = \dots = t_m = t_{m+1} = \dots = t_{m+n} = 0.$$

Таким образом, $\text{rk}(F) = m + n$, $F \cong F_{m+n}$. □

ТЕОРЕМА 3. Свободная абелева группа F (в частности, свободная абелева группа конечного ранга $F = F_n$) является группой без кручения, т. е. $\mathbf{T}(F) = 0$.

Доказательство. Пусть $\{e_1, \dots, e_n\}$ — базис свободной абелевой группы $F = F_n$ и

$$a = k_1 e_1 + \dots + k_n e_n \in \mathbf{T}(F), \quad k_i \in \mathbb{Z}.$$

Если $ra = 0$ для $0 < r \in \mathbb{Z}$, то

$$ra = (rk_1)e_1 + \dots + (rk_n)e_n = 0.$$

Следовательно,

$$rk_1 = \dots = rk_n = 0.$$

Так как $r > 0$, то $k_1 = \dots = k_n = 0$. Таким образом,

$$a = k_1 e_1 + \dots + k_n e_n = 0.$$

Итак, мы показали, что $\mathbf{T}(F_n) = 0$.

В общем случае надо отметить лишь, что если $0 \neq a \in F$, то $a \in F_n \subset F$. □

На самом деле для свободной абелевой группы F_n конечного ранга верно и обратное утверждение.

ТЕОРЕМА 4 (О СВОБОДЕ КОНЕЧНО ПОРОЖДЕННОЙ АБЕЛЕВОЙ ГРУППЫ БЕЗ КРУЧЕНИЯ). *Конечно порожденная абелева группа A является свободной абелевой группой тогда и только тогда, когда A — абелева группа без кручения (другими словами, когда ее периодическая часть равна нулю, $\mathbf{T}(A) = 0$).*

Доказательство. 1) Мы отмечали выше, что свободная абелева группа A не имеет кручения ($\mathbf{T}(A) = 0$).

2) Пусть $A = \langle a_1, \dots, a_n \rangle$ — конечно порожденная абелева группа и $\mathbf{T}(A) = 0$. Проведем доказательство свободы группы A индукцией по n . Начало индукции: $n = 1$, $A = \langle a_1 \rangle \cong \mathbb{Z} = F_1$, поскольку $O(a_1) = \infty$.

Пусть $n > 1$. Если $\{a_1, \dots, a_n\}$ — базис абелевой группы A , то $A = F_n$, и наше утверждение доказано.

Допустим теперь, что система образующих $\{a_1, \dots, a_n\}$ линейно зависима над \mathbb{Z} и

$$k_1 a_1 + \dots + k_n a_n = 0, \quad k_i \in \mathbb{Z}, \quad (*)$$

нетривиальное линейное соотношение между элементами a_1, \dots, a_n (это означает, что хотя бы один из коэффициентов k_i ненулевой). Пусть $d = \text{НОД}(k_1, \dots, k_n)$, $k_i = dk'_i$, $i = 1, \dots, n$. Тогда

$$d(k'_1 a_1 + \dots + k'_n a_n) = 0.$$

Так как $d \neq 0$ и A — абелева группа без кручения, то

$$k'_1 a_1 + \dots + k'_n a_n = 0, \quad (k'_1, \dots, k'_n) = 1.$$

Итак, можно считать, что

$$(k_1, k_2, \dots, k_n) = 1.$$

Если $k_1 = 1$, то

$$a_1 = -(k_2 a_2 + \dots + k_n a_n),$$

и поэтому в силу индуктивного предположения абелева группа $A = \langle a_2, \dots, a_n \rangle$ свободна. Аналогично, A — свободная абелева группа, если $k_1 = -1$.

Далее, мы будем менять систему образующих с целью получить в соотношении между новыми образующими один из коэффициентов равным ± 1 .

Если $k_2 = \dots = k_n = 0$, то $k_1 a_1 = 0$, $k_1 \neq 0$, и так как A — группа без кручения, то $a_1 = 0$, и поэтому, в силу индуктивного предположения, $A = \langle a_2, \dots, a_n \rangle$ — свободная абелева группа.

Итак, допустим, что $|k_1| \geq |k_2| > 0$, и в этом случае заменим образующий a_2 на $a'_2 = a_2 + k a_1$, $k \in \mathbb{Z}$ ($a_2 = a'_2 - k a_1$). В новой системе образующих $\{a_1, a'_2, a_3, \dots, a_n\}$ наше соотношение * имеет вид

$$(k_1 - k k_2) a_1 + k_2 a'_2 + k_3 a_3 + \dots + k_n a_n = 0.$$

В силу алгоритма деления в евклидовом кольце целых чисел \mathbb{Z} выберем $k \in \mathbb{Z}$ так, чтобы $|k_1 - kk_2| < |k_2|$, строго уменьшив модуль коэффициента при a_1 . Продолжая этот процесс, мы приходим к рассмотренному случаю, когда $k_1 = \pm 1$, что завершает доказательство. \square

ТЕОРЕМА 5 (УНИВЕРСАЛЬНОЕ СВОЙСТВО СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ КОНЕЧНОГО РАНГА). Пусть $F = F_n$ — свободная абелева группа, $\text{rk}(F) = n$, $\{e_1, \dots, e_n\}$ — один из базисов в $F = F_n$.

Если A — абелева группа, $\varphi: \{e_1, \dots, e_n\} \rightarrow A$ — отображение множеств (т. е. заданы элементы $a_1 = \varphi(e_1), \dots, a_n = \varphi(e_n) \in A$), то существует и единственный гомоморфизм групп $f: F_n \rightarrow A$ такой, что $f(e_i) = \varphi(e_i)$ для всех $1 \leq i \leq n$.

Доказательство. Для элемента

$$x = k_1 e_1 + \dots + k_n e_n \in F_n, \quad k_i \in \mathbb{Z},$$

положим

$$f(x) = k_1 a_1 + \dots + k_n a_n \in A.$$

Если

$$y = l_1 e_1 + \dots + l_n e_n \in F_n, \quad l_i \in \mathbb{Z},$$

то

$$\begin{aligned} x + y &= (k_1 + l_1)e_1 + \dots + (k_n + l_n)e_n, \\ f(y) &= l_1 a_1 + \dots + l_n a_n \in A, \\ f(x + y) &= (k_1 + l_1)a_1 + \dots + (k_n + l_n)a_n = \\ &= (k_1 a_1 + \dots + k_n a_n) + (l_1 a_1 + \dots + l_n a_n) = f(x) + f(y). \end{aligned}$$

Таким образом, f — гомоморфизм групп. Ясно, что $f(e_i) = a_i = \varphi(e_i)$ для всех $1 \leq i \leq n$.

Так как любой гомоморфизм $g: F_n \rightarrow A$ однозначно определяется значениями $g(e_1), \dots, g(e_n)$, то условием $f(e_i) = \varphi(e_i)$ для всех $1 \leq i \leq n$ гомоморфизм f определен однозначно. \square

ТЕОРЕМА 6 (НАКРЫВАЮЩЕЕ СВОЙСТВО СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ КОНЕЧНОГО РАНГА). Пусть $A = \langle a_1, a_2, \dots, a_n \rangle$ — конечно порожденная абелева группа, $\{a_1, a_2, \dots, a_n\}$ — одна из ее систем образующих. Тогда:

- 1) существует сюръективный гомоморфизм $f: F_n \rightarrow A$;
- 2) группа A изоморфна фактор-группе $F_n / \ker f$.

Доказательство. Пусть $F = F_n$ — свободная абелева группа с базисом $\{e_1, \dots, e_n\}$. В силу предыдущей теоремы существует гомоморфизм $f: F_n \rightarrow A$, для которого $f(e_i) = a_i$, $1 \leq i \leq n$. Так как $\{a_1, \dots, a_n\}$ — система образующих группы A , $A = \mathbb{Z}a_1 + \dots + \mathbb{Z}a_n$, то $\text{Im } f = A$. В силу теоремы о гомоморфизме $F_n / \ker f \cong A$. \square

ТЕОРЕМА 7 (РАСЩЕПЛЯЮЩЕЕ СВОЙСТВО СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ). Пусть A — абелева группа, F_n — свободная абелева группа ранга n , $f: A \rightarrow F_n$ — сюръективный гомоморфизм. Тогда:

- 1) существует гомоморфизм $h: F_n \rightarrow A$, для которого $fh = 1$ (т. е. имеем ретракт $f: A \rightarrow F_n$, $h: F_n \rightarrow A$, $fh = 1_{F_n}$);
- 2) для некоторой подгруппы B в A $A = B \oplus \ker f$, $B \cong F_n$.

Доказательство. Пусть $\{e_1, \dots, e_n\}$ — один из базисов свободной абелевой группы F_n , $n = \text{rk}(F_n)$. Так как $f: A \rightarrow F_n$ — сюръективное отображение, то выберем такие элементы $\{a_1, \dots, a_n\}$ в A , что $f(a_i) = e_i$, $1 \leq i \leq n$. Отображение $\{e_1, \dots, e_n\} \rightarrow \{a_1, \dots, a_n\}$, $e_i \rightarrow a_i$, продолжается до гомоморфизма $h: F_n \rightarrow A$, для которого $h(e_i) = a_i$. Так как для $(fh): F_n \rightarrow F_n$ имеем

$$(fh)(e_i) = f(h(e_i)) = f(a_i) = e_i = 1_{F_n}(e_i),$$

то $fh = 1_{F_n}$. Итак, получили ретракт, $fh = 1_{F_n}$.

В силу леммы о ретракте $A = \text{Im } h \oplus \ker f$. Полагая $B = \text{Im } h = \langle a_1, \dots, a_n \rangle$, получаем $A = B \oplus \ker f$.

Так как $f(B) = f(A) = F_n$, то $f|_B$ — сюръективное отображение, при этом

$$\ker(f|_B) = \ker f \cap B = \ker f \cap \operatorname{Im} h = 0.$$

Итак, $f|_B: B \rightarrow F_n$ — изоморфизм групп, $B \cong F_n$. □

Рассмотрим теперь подгруппы свободной абелевой группы конечно-го ранга (это расширяет нашу информацию о подгруппах бесконечной циклической группы).

ТЕОРЕМА 8. *Ненулевая подгруппа B свободной абелевой группы F_n конечно-го ранга n является свободной абелевой группой ранга m , $B \cong F_m$, где $1 \leq m \leq n$.*

Доказательство. проведем индукцией по n .

Случай $n = 1$: $F_1 \cong \mathbb{Z}$; ненулевая подгруппа B в \mathbb{Z} имеет вид $\mathbb{Z}k$, $0 \neq k \in \mathbb{Z}$, поэтому $B \cong \mathbb{Z}$, и следовательно, B является свободной абелевой группой ранга $m = 1 = n$.

Пусть наше утверждение верно для всех рангов $n' < n$, $n > 1$, B — ненулевая подгруппа группы

$$F_n = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1} \oplus \mathbb{Z}e_n,$$

где $\{e_1, \dots, e_n\}$ — один из базисов свободной абелевой группы F_n . Рассмотрим короткую точную последовательность абелевых групп

$$0 \rightarrow \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1} \xrightarrow{i} F_n \xrightarrow{\pi} \mathbb{Z}e_n \rightarrow 0,$$

где i — естественное вложение, $\pi(k_1e_1 + \dots + k_n e_n) = k_n e_n$ (т. е. π — естественная проекция на прямое слагаемое $\mathbb{Z}e_n$, $\ker \pi = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1}$). Рассмотрим ограничение $\pi|_B: B \rightarrow \mathbb{Z}e_n$ гомоморфизма π на подгруппу B . Так как

$$\ker(\pi|_B) = B \cap \ker \pi = B \cap (\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1}),$$

то короткая точная последовательность абелевых групп

$$0 \rightarrow B \cap (\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1}) \rightarrow B \xrightarrow{\pi|_B} \pi(B) \rightarrow 0$$

является точной.

В силу индуктивного предположения для подгруппы $B \cap (\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1})$ группы $F_{n-1} = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1}$ имеем

$$B \cap (\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1}) \cong F_l,$$

где $l \leq n - 1$.

Если $\pi(B) = 0$, то

$$B \subseteq \ker \pi = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1},$$

и в силу нашего индуктивного предположения для $n' = n - 1 < n$: $B \cong F_m$, $m \leq n - 1 < n$.

Если

$$0 \neq \pi(B) \subseteq \mathbb{Z}e_n \cong \mathbb{Z} = F_1,$$

то

$$\pi(B) \cong \mathbb{Z}t \subseteq \mathbb{Z}, \quad 0 \neq t \in \mathbb{Z},$$

и поэтому $\pi(B) \cong \mathbb{Z} = F_1$ — свободная абелева группа ранга 1. В силу расщепляющего свойства свободной абелевой группы:

$$B = C \oplus (B \cap (\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_{n-1})),$$

где $C \cong \pi(B) \cong F_1$. Итак, $B \cong F_1 \oplus F_l = F_{l+1}$, где $l+1 \leq (n-1)+1 = n$. \square

СТРУКТУРНАЯ ТЕОРЕМА

ТЕОРЕМА 9. Пусть A — конечно порожденная абелева группа.

1) Тогда имеет место прямое разложение

$$A = \mathbf{T}(A) \oplus A',$$

где периодическая часть $\mathbf{T}(A)$ является конечной абелевой группой, $|\mathbf{T}(A)| < \infty$, и $\mathbf{T}(A)$ выделяется в A прямым слагаемым, подгруппа A' является свободной абелевой группой конечного ранга $r < \infty$ и определена однозначно (с точностью до изоморфизма), $A' \cong A/\mathbf{T}(A) \cong$

F_r , $r = \text{rk}(A/\mathbf{T}(A))$ — инвариант группы A .

Таким образом, конечно порожденная абелева группа A является прямой суммой конечной абелевой группы $\mathbf{T}(A)$ и свободной абелевой группы $A' \cong F_r$ конечного ранга r ; если $A = \mathbf{T}(A) \oplus A' = \mathbf{T}(A) \oplus A''$, то $A' \cong A''$.

2) Это прямое разложение единственно в следующем смысле: если

$$A = B \oplus C = B' \oplus C',$$

где B и B' — конечные абелевы группы, $C \cong F_r$ и $C' \cong F_s$ — свободные абелевы группы конечных рангов r и s соответственно, то

$$B = B' = \mathbf{T}(A), \quad C \cong C' \cong F_r \quad (r = s = \text{rk}(A/\mathbf{T}(A))).$$

Доказательство.

1) Если $A = \langle a_1, \dots, a_n \rangle$ — конечно порожденная абелева группа, то

$$A/\mathbf{T}(A) = \langle \bar{a}_1, \dots, \bar{a}_n \rangle, \quad \bar{a}_i = a_i + \mathbf{T}(A) \in A/\mathbf{T}(A), \quad \mathbf{T}(A/\mathbf{T}(A)) = 0,$$

и поэтому $A/\mathbf{T}(A)$ — конечно порожденная абелева группа без кручения. В силу теоремы ?? $A/\mathbf{T}(A)$ — свободная абелева группа конечного ранга, $A/\mathbf{T}(A) \cong F_r$, где $r = \text{rk}(A/\mathbf{T}(A))$. В силу расщепляющего свойства свободной абелевой группы (см. теорему 7) имеем: $A = \mathbf{T}(A) \oplus A'$, где A' — подгруппа в A , $A' \cong A/\mathbf{T}(A) \cong F_r$ ($r < \infty$, поскольку $A/\mathbf{T}(A)$ — конечно порожденная абелева группа).

Так как $\mathbf{T}(A) \cong A/A'$ — конечно порожденная периодическая абелева группа, то в силу теоремы прошлой лекции $|\mathbf{T}(A)| < \infty$. Итак, $\mathbf{T}(A)$ — конечная абелева группа.

Если $A = \mathbf{T}(A) \oplus A' = \mathbf{T}(A) \oplus A''$, то $A' \cong A/\mathbf{T}(A) \cong A''$.

2) Если

$$A = B \oplus C = B' \oplus C', \quad |B| < \infty, \quad |B'| < \infty, \quad C \cong F_r, \quad C' \cong F_s,$$

то

$$\mathbf{T}(B) = B, \quad \mathbf{T}(C) = 0, \quad \mathbf{T}(B') = B', \quad \mathbf{T}(C') = 0,$$

и поэтому

$$\begin{aligned} B = \mathbf{T}(B) &= \mathbf{T}(B) \oplus \mathbf{T}(C) = \mathbf{T}(B \oplus C) = \mathbf{T}(A) = \\ &= \mathbf{T}(B' \oplus C') = \mathbf{T}(B') \oplus \mathbf{T}(C') = \mathbf{T}(B') = B'. \end{aligned}$$

Следовательно, $B = \mathbf{T}(A) = B'$. Поэтому

$$F_r \cong C \cong A/B = A/\mathbf{T}(A) = A/B' \cong C' \cong F_s,$$

и следовательно, $r = s$. □