Лекция 6

На прошлой лекции мы доказали существование разложения

$$A \cong \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{a_{m_1}}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \ldots \oplus \mathbb{Z}_{p_2^{b_{m_2}}} \oplus \ldots \oplus$$
$$\oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{c_{m_k}}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \quad (1)$$

для произвольной конечно порождчнной абелевой группы A. То есть существование разложения из следующей теоремы. Сейчас докажем единственность. (Доказательство единственности не войдет в вопросы к экзамену.)

Теорема 1 (Теорема о строении конечно порожденных абелевых групп)**.** *Пусть A – конечно порожденная абелева группа. Тогда A изоморфна прямой сумме конечного числа циклических групп. Каждая из этих циклических групп либо является бесконечной циклической группой, либо примарной циклической группой. И такое разложение единственно с точностью до перестановки прямых слагаемых.*

Лемма 1. *Пусть $G_1, \ldots, G_k$ – группы и $g_i \in G_i$. Тогда*

$$\mathrm{ord}(g_1, \ldots, g_k) = \textit{НОК}(\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k)).$$

Доказательство. $m = \mathrm{ord}(g_1, \ldots, g_k)$ – это минимальное натуральное число такое, что $(g_1, \ldots, g_k)^m = (e, \ldots, e)$. Это означает, что $g_i^m = e$ для всех $1 \leq i \leq k$. То есть m делится на все $\mathrm{ord}(g_i)$. Минимальное такое число – это $\text{НОК}(\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k))$. □

Доказательство. (Доказательство теоремы 1) Существование такого разложения в прямую сумму уже доказано (это и есть вторая каноническая форма). Пусть есть два таких разложения одной и той же группы A. Прежде всего докажем, что количество бесконечных циклических слагаемых в обоих разложениях одинаково. Для этого определим следующую подгруппу

Определение 1. Подгруппа кручения $\mathrm{Tor}\, A$ (абелевой) группы A – это подгруппа, состоящая из всех элементов конечного порядка.

Прежде всего нужно объяснить, что множество элементов конечного порядка действительно является подгруппой. Для этого заметим, что если $ka = 0$ и $mb = 0$, то $km(a+b) = 0$. То есть множество $\mathrm{Tor}\, A$ замкнуто относительно сложения. Кроме того $k(-a) = 0$, что означает замкнутость $\mathrm{Tor}\, A$ относительно взятия противоположного. Осталось заметить, что $0 \in \mathrm{Tor}\, A$.

Элементы конечного порядка в разложении (1) имеют вид $(x_1, \ldots, x_N, 0, \ldots, 0)$, где в конечных слагаемых идут любые элементы $x_1, \ldots, x_N$, а в бесконечных слагаемых все элементы – нули. Таким образом,

$$\mathrm{Tor}\, A = \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{a_{m_1}}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \ldots \oplus \mathbb{Z}_{p_2^{b_{m_2}}} \oplus \ldots \oplus$$
$$\oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{c_{m_k}}} \oplus \{0\} \oplus \ldots \oplus \{0\} \subset$$
$$\subset \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{a_{m_1}}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \ldots \oplus \mathbb{Z}_{p_2^{b_{m_2}}} \oplus \ldots \oplus$$
$$\oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{c_{m_k}}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} = A.$$

По теореме о факторизации прямого произведения

$$A/\mathrm{Tor}\, A \cong \{0\} \oplus \ldots \oplus \{0\} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \cong \mathbb{Z}^r.$$

Таким образом, факторгруппа $A/\operatorname{Tor} A$ – это свободная абелева группа ранга r, где r равно количеству прямых слагаемых, изоморфных $\mathbb{Z}$ в разложении (1). Поскольку определение подгруппы кручения не зависит от разложения и ранг свободной абелевой группы определен однозначно, получаем, что если для группы A есть две вторых канонических формы, то количество прямых слагаемых $\mathbb{Z}$ в них одинаково. Назовем это число *рангом* (абелевой) группы A.

Разложение (1) состоит из второй канонической формы группы $\operatorname{Tor} A$, к которой добавлены $\operatorname{rk} A$ слагаемых $\mathbb{Z}$. Для того, чтобы доказать, что две вторых канонических формы группы A совпадают, осталось доказать, что для группы $\operatorname{Tor} A$ (то есть для конечной группы) нет двух различных вторых канонических формы.

Пусть B – конечная абелева группа. Для любого натурального числа t можно рассмотреть гомоморфизм $\varphi_t \colon B \to B$, $\varphi_t(b) = tb$. Легко видеть, что если $B = B_1 \oplus B_2$, то $\varphi_t(b_1, b_2) = (tb_1, tb_2) = (\varphi_t|_{B_1}(b_1), \varphi_t|_{B_2}(b_2))$. Фиксируем простое число p. Рассмотрим второе каноническое разложение группы B:

$$\begin{aligned} B = \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \ldots \oplus \mathbb{Z}_{p^2} \oplus \ldots \oplus \mathbb{Z}_{p^k} \oplus \ldots \oplus \mathbb{Z}_{p^k} \oplus \mathbb{Z}_{q_1^{r_1}} \oplus \ldots \oplus \mathbb{Z}_{q_s^{r_s}} = \\ = \mathbb{Z}_p^{m_1} \oplus \mathbb{Z}_{p^2}^{m_2} \oplus \ldots \oplus \mathbb{Z}_{p^k}^{m_k} \oplus \mathbb{Z}_{q_1^{r_1}} \oplus \ldots \oplus \mathbb{Z}_{q_s^{r_s}}. \end{aligned}$$

Возьмем $t = p^\alpha$, где p – простое число. Рассмотрим, ядро гомоморфизма φ_t. Пусть некоторый элемент разложения, умноженный на p^α равен нулю. Тогда его координаты лежат в ядрах ограничений гомоморфизма φ_t на каждое слагаемое. При этом ядра ограничений на $\mathbb{Z}_{q_1^{r_1}}, \ldots, \mathbb{Z}_{q_s^{r_s}}$ равны нулю, так как $t = p^\alpha$ и $q_i^{r_i}$ взаимно просты. В группе $\mathbb{Z}_{p^\beta}$ при умножении на p^α в ноль переходит

– вся группа, если $\beta < \alpha$.

– подгруппа $\langle p^{\beta-\alpha} \rangle \cong \mathbb{Z}_{p^\alpha}$, если $\beta \geq \alpha$.

Отсюда

$$\operatorname{Ker} \varphi_{p^\alpha} = \mathbb{Z}_p^{m_1} \oplus \mathbb{Z}_{p^2}^{m_2} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha-1}}^{m_{\alpha-1}} \oplus \mathbb{Z}_{p^\alpha}^{m_\alpha} \oplus \mathbb{Z}_{p^\alpha}^{m_{\alpha+1}} \oplus \ldots \oplus \mathbb{Z}_{p^\alpha}^{m_k}.$$

Таким образом,

$$|\operatorname{Ker} \varphi_{p^\alpha}| = p^{m_1 + 2m_2 + \ldots + (\alpha-1)m_{\alpha-1} + \alpha(m_\alpha + m_{\alpha+1} + \ldots + m_k)}.$$

Получаем

$$\frac{|\operatorname{Ker} \varphi_{p^\alpha}|}{|\operatorname{Ker} \varphi_{p^{\alpha-1}}|} = p^{m_\alpha + m_{\alpha+1} + \ldots + m_k}.$$

Следовательно,

$$p^{m_\alpha} = \frac{|\operatorname{Ker} \varphi_{p^\alpha}|}{|\operatorname{Ker} \varphi_{p^{\alpha-1}}|} \cdot \frac{|\operatorname{Ker} \varphi_{p^\alpha}|}{|\operatorname{Ker} \varphi_{p^{\alpha+1}}|}$$

То есть

$$\begin{aligned} m_\alpha = \log_p \left(\frac{|\operatorname{Ker} \varphi_{p^\alpha}|^2}{|\operatorname{Ker} \varphi_{p^{\alpha+1}}| \cdot |\operatorname{Ker} \varphi_{p^{\alpha-1}}|} \right) = \\ = 2\log_p(|\operatorname{Ker} \varphi_{p^\alpha}|) - \log_p(|\operatorname{Ker} \varphi_{p^{\alpha+1}}|) - \log_p(|\operatorname{Ker} \varphi_{p^{\alpha-1}}|). \end{aligned}$$

Заметим, что эта формула верна и при $\alpha = 1$, тогда $\varphi_{p^{\alpha-1}} = \mathrm{id}$. Эта формула показывает, что количество слагаемых $\mathbb{Z}_{p^\alpha}$ во втором каноническом разложении конечной абелевой группы B не зависит от этого разложения. Это доказывает теорему.

$\square$

Определение 2. Экспонента группы G – это минимальное натуральное число k такое, что для любого $g \in G$ выполнено $g^k = e$. Если такого числа не существует, то будем говорить, что экспонента G равна бесконечности. Обозначать экспоненту будем $\exp G$.

Лемма 2. *Экспонента группы равна наименьшему общему кратному порядков элементов. (Имеется в виду, что если есть элемент бесконечного порядка или нет конечного общего кратного у всех порядков, то экспонента бесконечна.)*

Доказательство. Если $g^k = e$, то k делится на $\operatorname{ord} g$. Так как $\exp G$ – минимальное натуральное число, что $g^{\exp G} = e$ для всех $g \in G$, получаем, что $\exp G$ – минимальное натуральное число, делящееся на порядки всех элементов. $\square$

Предложение 1 (Критерий цикличности конечной абелевой группы)**.** *Пусть A – конечная абелева группа. Группа A циклическая тогда и только тогда, когда* $\exp A = |A|$.

Доказательство. Пусть A циклическая. Тогда есть элемент, порядок которого равен $|A|$, то есть $\exp A \geq |A|$. Порядки всех элементов – делители $|A|$, значит, $\exp A \leq |A|$. Получаем $\exp A = |A|$.

Пусть наоборот, $\exp A = |A| = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, где p_i – простые числа. Так как $\exp A$ – наименьшее общее кратное порядков всех элементов, для каждого $1 \leq j \leq m$ найдется $b_j \in A$ такое, что $\operatorname{ord} b_j = p_j^{k_j} t$, где t не делится на p_j. Обозначим $a_j = t b_j$. Легко видеть, что $\operatorname{ord} a_j = p_j^{k_j}$. Рассмотрим элемент $a = a_1 + \ldots + a_m$, докажем, что его порядок равен $|A|$. Для этого заметим, что $|A|a = 0$ по теореме Лагранжа, но

$$\frac{|A|}{p_j} a = p_1^{k_1} p_2^{k_2} \dots p_j^{k_j - 1} \dots p_m^{k_m} (a_1 + \ldots + a_j + \ldots a_m) =$$
$$= 0 + \ldots + 0 + p_1^{k_1} p_2^{k_2} \dots p_j^{k_j-1} \dots p_m^{k_m} a_j + 0 + \ldots + 0 = p_1^{k_1} p_2^{k_2} \dots p_j^{k_j-1} \dots p_m^{k_m} a_j \neq 0.$$

А значит, простое число p_j входит в $\operatorname{ord} a$ именно в степени k_j. Так как это выполняется для всех j, порядок a равен $|A|$. Следовательно, группа A циклическая. $\square$

Напомним, что полем называется множество F с двумя бинарными операциями: сложением и умножением, удовлетворяющим следующим аксиомам.

1) $\forall a, b, c \in F\colon (a + b) + c = a + (b + c)$,
2) $\exists\, 0 \in F\colon \forall x$ выполнено $0 + x = x + 0 = x$,
3) $\forall x \in F\ \exists (-x) : x + (-x) = (-x) + x = 0$,
4) $\forall a, b \in F\colon a + b = b + a$,
5) $\forall a, b, c \in F\colon (a + b)c = ac + bc$,
6) $\forall a, b, c \in F\colon (ab)c = a(bc)$,
7) $\forall a, b \in F\colon ab = ba$,
8) $\exists\, e \in F\colon \forall x$ выполнено $ex = xe = x$,
9) $\forall x \neq 0 \in F\ \exists\, x^{-1} : xx^{-1} = x^{-1}x = e$.

Поле является частным случаем кольца. Мы ранее говорили, что для произвольного кольца R можно рассмотреть группу $(R^\times, \cdot)$, состоящую из всех обратимых по умножению элементов, с операцией множения. Для поля $F^\times = F \setminus \{0\}$ и группа $(F^\times, \cdot)$ называтся *мультипликативной группой поля* F.

Предложение 2. *Конечная подгруппа в мультипликативной группе*

$$F^\times = (F \setminus \{0\}, \cdot)$$

поля F циклическая.

Доказательство. Пусть G – конечная подгруппа в мультипликативной группе поля $F^\times$. Предположим, что G не является циклической. Так как $F^\times$ коммутативна, ее подгруппа G также коммутативна. По предложению 1 экспонента G не равна $|G|$. Значит, $\exp G = k < |G|$. Тогда в поле F у многочлена $x^k - e$ как минимум $|G|$ корней (все элементы группы G являются такими корнями). Однако ненулевой многочлен не может иметь в поле больше корней, чем его степень. В самом деле это следует из того, что, если $f(c) = 0$, то по теореме Безу $f(x)$ делится на $x - c$. Получаем противоречие. Следовательно, исходное предположение, что G не циклическая не верно. □

Очевидным следствием предыдущего предложения является следующее утверждение.

Следствие 1. *Мультипликативная группа конечного поля циклическая.*

Определение 3. Пусть G – группа, а X – множество. *Действием* группы G на множестве X называется отображение $\alpha\colon G \times X \to X$, удовлетворяющее следующим условиям:
1) для любых $g, h \in G$ и $x \in X$ выполнено $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$,
2) для любого $x \in X$ выполнено $\alpha(e, x) = x$.

Если задано действие группы G на множестве X, то говорят, что G *действует* на X и обозначают $G \curvearrowright X$ (в некоторой литературе обозначают $G : X$). При этом $\alpha(g, x)$ называется действием (или применением) элемента g к элементу x, и $\alpha(g, x)$ обозначается $g \cdot x$. В таких обозначениях свойства действия из определения 3 принимают вид:
1) для любых $g, h \in G$ и $x \in X$ выполнено $g \cdot (h \cdot x) = (gh) \cdot x$,
2) для любого $x \in X$ выполнено $e \cdot x = x$.

Заметим, что при фиксированном $g \in G$ отображение $\alpha_g\colon X \to X$, $\alpha_g(x) = \alpha(g, x)$ является биекцией. В самом деле, легко убедиться, что $\alpha_g \circ \alpha_h = \alpha_{gh}$, при этом $\alpha_e = \mathrm{id}$. Это означает, что $\alpha_{g^{-1}}$ – обратное отображение к α_g. Таким образом, мы получаем гомоморфизм φ_α из G в $S(X)$. Напомним, что $S(X)$ – это группа биекций $X \to X$. Гомоморфизм φ_α определяется следующим образом: $\varphi_\alpha(g) = \alpha_g$.

Наоборот, если дан гомоморфизм $\varphi\colon G \to S(X)$, то можно определить действие α_φ группы G на X следующим образом: $g \cdot x = \varphi(g)(x)$.

Лемма 3. *Отображения $\Phi\colon \alpha \mapsto \varphi_\alpha$ и $\Psi\colon \varphi \mapsto \alpha_\varphi$ являются взаимно обратными и, следовательно, устанавливают биекцию между действиями G на X и гомоморфизмами из G в $S(X)$.*

Доказательство. Пусть β – некоторое действие G на X. Имеем $\Psi \circ \Phi(\beta) = \Psi(\varphi_\beta)$. По определению, это действие устроено по правилу $g \cdot x = \varphi_\beta(g)(x)$. С другой стороны по определению $\varphi_\beta(g) = \beta_g$, то есть $\varphi_\beta(g)(x) = \beta_g(x) = \beta(g, x)$. Таким образом $\Psi \circ \Phi(\beta) = \beta$, то есть $\Psi \circ \Phi = \mathrm{id}$.

Пусть теперь $\varphi\colon G \to S(X)$ – гомоморфизм. Тогда $\Phi \circ \Psi(\varphi) = \Phi(\alpha_\varphi)$. По определению Φ имеем $\Phi(\alpha_\varphi)(g)(x) = \alpha_\varphi(g, x) = \varphi(g)(x)$. Так как это верно для любого x и для любого g имеем $\Phi \circ \Psi(\varphi) = \varphi$, то есть $\Phi \circ \Psi = \mathrm{id}$. □

Пример 1. *Пусть $X = \{1, 2, \ldots, n\}$. Тогда есть естественное действие симметрической группы S_n на X, заданное по формуле $\sigma \cdot i = \sigma(i)$.*

То, что это действие сводится к проверкам
1) $\sigma \cdot (\delta \cdot i) = \sigma(\delta(i)) = (\sigma \circ \delta)(i) = (\sigma \circ \delta) \cdot i$,
2) $\mathrm{id} \cdot i = \mathrm{id}(i) = i$.

Пример 2. *Пусть K – поле. Тогда зададим действие* $\mathrm{GL}(K) \curvearrowright K^n$ *по следующей формуле. Для* $A \in \mathrm{GL}(K)$ *и* $Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \in K^n$ *положим* $A \cdot Y = AY$. *Доказательство того, что это действие сводится к проверкам*

1) $A \cdot (B \cdot Y) = ABY = (AB) \cdot Y$,

2) $E \cdot Y = EY = Y$.

Такое действие называется тавтологическим.

Важный частный случай действий – это действия группы на себе, то есть случай, когда $X = G$. Есть три естественных действия $G \curvearrowright G$.

Пример 3. *1)* **Действие G на себе левыми сдвигами.**

По определению $g \cdot \overline{g} = g\overline{g}$.

Тогда $g_1 \cdot (g_2 \cdot \overline{g}) = g_1 g_2 \overline{g} = (g_1 g_2) \cdot \overline{g}$ *и* $e \cdot \overline{g} = e\overline{g} = \overline{g}$.

2) **Действие G на себе правыми сдвигами.**

По определению $g \cdot \overline{g} = \overline{g} g^{-1}$. *Проверим, что это действие.*

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (\overline{g} g_2^{-1}) = (\overline{g} g_2^{-1}) g_1^{-1} = \overline{g}(g_1 g_2)^{-1} = (g_1 g_2) \cdot \overline{g},$$
$$e \cdot \overline{g} = \overline{g} \cdot e = \overline{g}.$$

3) **Действие G на себе сопряжениями.**

По определению $g \cdot \overline{g} = g\overline{g}g^{-1}$. *Проверим, что это действие.*

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (g_2 \overline{g} g_2^{-1}) = g_1 g_2 \overline{g} g_2^{-1} g_1^{-1} = (g_1 g_2)\overline{g}(g_1 g_2)^{-1} = (g_1 g_2) \cdot \overline{g}.$$
$$e \cdot \overline{g} = e\overline{g}e^{-1} = \overline{g}.$$

Замечание 1. Заметим, что нельзя определить правое действие (действие правыми сдвигами) таким образом $g \cdot \overline{g} = \overline{g} g$, так как при этом

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (\overline{g} g_2) = \overline{g} g_2 g_1, \qquad (g_1 g_2) \cdot \overline{g} = \overline{g} g_1 g_2.$$

Если группа G не коммутативная, то найдутся два элемента g_1 и g_2 такие, что

$$\overline{g} g_2 g_1 \neq \overline{g} g_1 g_2.$$