§5 **Доказательство теоремы о примарном циклическом разложении.**

Шаг 1. Примарное разложение

Из разложения

$$\ker \mu_{\mathcal{A}}(t) = \bigoplus_{i=1}^{r} \ker f_i(t)$$

, где $\mu_{\mathcal{A}}(t) = \prod_{i=1}^{r} f_i(t),\ (f_i, f_j) = 1 \forall\ i \neq j$(откуда $f_i = p_i(t)^k$, p_i - неприводим) следует, что достаточно доказать только то, что примарное пространство раскладывается в сумму циклических.

Поэтому будем считать, что $\mu_{\mathcal{A}}(t) = p^k(t)$, где p - неприводим

Шаг 2. Циклическое разложение.

Существует вектор v, такое что $p^k(\mathcal{A})v = 0$ и $p^{k-1}(\mathcal{A})v \neq 0$(если бы такого вектора не было, то это p^{k-1} аннулировал бы V, что противоречит минимальности p^k).

Возьмем инвариантное подпространство L наибольшой размерности, такое что $L \cap \langle v \rangle_{\mathcal{A}} = 0$. Мы хотим показать, что $V = L \oplus \langle v \rangle_{\mathcal{A}}$. Будем доказывать от противного - предположим, что существует $u_0 \in V \setminus (L \oplus \langle v \rangle_{\mathcal{A}})$.

Рассмотрим последовательность $u_0, p(\mathcal{A})u_0, ..., p^k(\mathcal{A})u_0 = 0$. Последний ее элемент равен 0, то есть он лежит в $L \oplus \langle v \rangle_{\mathcal{A}}$. Теперь возьмем $u = p^l(\mathcal{A})u_0$, такой что $p^l(\mathcal{A})u_0 \notin L \oplus \langle v \rangle_{\mathcal{A}}$, а $p^{l+1}(\mathcal{A})u_0 \in L \oplus \langle v \rangle_{\mathcal{A}}$(такое l существует, потому что при $l = 0$ вектор u_0 не лежит в $L \oplus \langle v \rangle_{\mathcal{A}}$, а при $l = k$ вектор 0 лежит в $L \oplus \langle v \rangle_{\mathcal{A}}$)

Будем "подправлять вектор"$u \to u'$, чтобы $(\langle u' \rangle_{\mathcal{A}} + L) \cap \langle v \rangle_{\mathcal{A}} = 0$

$p\mathcal{A}(u) = l + x$, $l \in L$, $x \in \langle v \rangle_{\mathcal{A}}$, $\exists f(t) :\ x = f(\mathcal{A})v$.(в первом равенстве пользуемся тем фактом, что вектор $p(\mathcal{A})(u)$ лежит в прямой сумме, во втором - тем что вектор x лежит в циклическом подпространстве.)

ФАКТ: $p(t)|f(t)$, то есть $f(t) = p(t)g(t)$

Доказательство:

Применяя теорему о линейном представлении НОД, получаем, что если $(f(t), p(t)) = 1$, то $(f(t), p^k(t)) = 1$, а значит

$a(\mathcal{A})f(\mathcal{A}) + b(\mathcal{A})p^k(\mathcal{A}) = Id$

$(a(\mathcal{A})f(\mathcal{A}) + b(\mathcal{A})p^k(\mathcal{A}))v = (Id)v$

$a(\mathcal{A})f(\mathcal{A})v + b(\mathcal{A})p^k(\mathcal{A})v = v$

$a(\mathcal{A})x = v$

(в предпоследней строчке мы пользовались тем, что $x = f(\mathcal{A})v$ и тем, что $p^k(\mathcal{A})v = 0$)

$p^{k-1}f(\mathcal{A})x = v \neq 0$, значит $p^{k-1}(\mathcal{A})x \neq 0$.

Если применить $p^{k-1}(\mathcal{A})$ к равенству $p\mathcal{A}(u) = l + x$, то получим, что $p^k\mathcal{A}(u) = p^{k-1}(\mathcal{A})l + p^{k-1}(\mathcal{A})x$, то есть $0 = p^{k-1}(\mathcal{A})l + p^{k-1}(\mathcal{A})x$. Второе слогаемое на равно 0, значит мы получили нетривиальное представление 0 в прямой сумме, чего не может быть. Значит наибольший общий делитель не равен 1, в силу простоты p получаем, что он равен p. $\square$.

Теперь, достаточно взять $u' = u - g(\mathcal{A})v$. u' не лежит в $L \oplus \langle v \rangle_{\mathcal{A}}$, потому что u тоже не нем не лежит, и при этом $p(\mathcal{A})u' = l \in L$.

Замечание:

$\mu_{\mathcal{A},x}(t) = \frac{p^k(t)}{\gcd(f(t),p^k(t))} = \frac{\mu_{\mathcal{A},x}(t)}{\gcd(f(t),\mu_{\mathcal{A},x}(t))}$

Эта формула является прямой аналогией теоретико-групповой формулы:

$ord(g^k) = \frac{ord(g)}{gcd(ord(g),k)}$

Задача(разбиралась на практике):

$L = L_1 \oplus L_2$.

Доказать, что $\mu_{\mathcal{A},L} = LCM(\mu_{\mathcal{A},L_1}, \mu_{\mathcal{A},L_2})$

Докажем, что $(\langle u' \rangle_{\mathcal{A}} + L) \cap \langle v \rangle_{\mathcal{A}} = 0$

От противного, пусть пересечение не пусто, тогда $\exists \varphi(t), g(t), l'$, такие что:

$\varphi(\mathcal{A})u' + l' = g(\mathcal{A})v$.

Тогда:

$\varphi(\mathcal{A})u' = g(\mathcal{A})v - l'$.

Первый случай, $(\varphi(t), p(t)) = 1$:

$\psi\varphi(\mathcal{A})u'\gamma p^k(\mathcal{A})u' = Idu'$

$\psi\varphi(\mathcal{A})u' = u'$

$\psi\varphi(\mathcal{A})u' = \psi(g(\mathcal{A})v - l')$

$u' = \psi(\mathcal{A})g(\mathcal{A})v - \psi\mathcal{A}l'$.

В силу инвариантности $\psi(\mathcal{A})g(\mathcal{A})v \in \langle v \rangle_{\mathcal{A}}$, $\psi\mathcal{A}l' \in L$, но u' по предположению не лежит в $L \oplus \langle v \rangle_{\mathcal{A}}$. Противоречие

Второй случай $(\varphi(t), p(t)) = p(t)$, то есть $\varphi(t) = ph(t)$, так как $p(\mathcal{A})u' = l$, то $\varphi(\mathcal{A})u' = ph(\mathcal{A})u' = h(\mathcal{A})l$, то есть $h(\mathcal{A})l = g(\mathcal{A})v - l'$. Получили два разложения в прямую сумму, чего не может быть. $\square$.

Замечание:

$V = \bigoplus_{i=1}^{r} \mathbb{K}[t]/(p_i^{k_i}(t))$.

Набор $\{\{(p_i, k_i)\dots\}\}$ - неприводимые многочлены со степенями(пары могут повторятся) определен однозначно. Без доказательства.

§ **Алгоритм построения Жорданова базиса в случае базового поля C**

Пусть $(V, \mathcal{A})$ - векторное пространство над $\mathbb{C}$ с оператором $\mathcal{A}$. Тогда:

$\chi_{\mathcal{A}}(t) = \prod_{i=1}^{r}(t-\lambda_i)^{k_i}$, где $\lambda_i \neq \lambda_j$ при $i \neq j$.

$V = \bigoplus_{i=1}^{r} \ker(\mathcal{A} - \lambda_i Id)^{k_i}$

Дадим алгоритм построение базиса в каждом пространстве $\ker(\mathcal{A} - \lambda Id)^k$

Предложение. Имеет место следующий алгоритмы(метод спуска):

$\ker(\mathcal{A} - \lambda Id)^k \subset \ker(\mathcal{A} - \lambda Id)^{k-1} \subset \dots \ker \mathcal{A} - \lambda Id$

Шаг I. Находим базис $\ker(\mathcal{A}-\lambda Id)^k$ по модулю $(\mathcal{A}-\lambda Id)^{k-1}$: $v_1^k, v_2^k, ...v_{i_1}^k$. Применим к ним $\mathcal{A} - \lambda Id$.

Лемма. Если $v_1, \dots, v_k \in \ker B^k$ - линейно независимые $mod\ B^{k-1}$, то $(B(v_1), \dots, B(v_k)) \in \ker B^{k-1}$ - линейно независимые $mod\ B^{k-2}$.

Замечание Следующие три условия равносильные($U \subset V$, $v_1, \dots, v_k$ - набор векторов):

1. $\exists u_1, \dots, u_n$ - базис, такой что $u_1, \dots, u_n, v_1, \dots, v_k$ - линейно независимые

2. $\forall u_1, \dots, u_n$ - базис, такой что $u_1, \dots, u_n, v_1, \dots, v_k$ - линейно независимые

3. если $\sum \alpha_i v_i \in U$, то $\alpha_1 = \alpha_2 \cdots = \alpha_n = 0$.

(доказательство предлагается проделать в уме)

Доказательство леммы

Если $B(v_1), \dots, B(v_k)$ - линейно зависимые по модулю $\ker B^{k-2}$, то $\exists \alpha_i : \sum \alpha_i B(v_i) \in \ker B^{k-2} \Rightarrow B(\sum \alpha_i v_i) \in \ker B^{k-2} \Rightarrow \sum \alpha_i v_i \in \ker B^{k-1}$. Получили противоречие с линейной независимостью $mod\ B^{k-1}$.

Шаг II $B\mathcal{A} - \lambda Id$ - нильпотентный оператор, $B^k = 0$.

$Bv_1^k, Bv_2^k, ...Bv_{i_1}^k$ дополним до относительного базиса в $\ker Bk - 1 \mod \ker B^{k-2}$: $v_1^{k-1}, \dots, v_{i_1}^{k-1}, v_{i_1+1}^{k-1}, \dots, v_{i_1+i_2}^{k-1}$

III Повторять эту процедуру до конца.

$$
\begin{array}{llll}
v_1^k & \xrightarrow{\mathcal{B}} v_1^{k-1} & \xrightarrow{\mathcal{B}} \dots \xrightarrow{\mathcal{B}} & v_1^1 \\
v_2^k & \xrightarrow{\mathcal{B}} v_2^{k-1} & \xrightarrow{\mathcal{B}} \dots \xrightarrow{\mathcal{B}} & v_2^1 \\
\vdots & & & \vdots \\
v_{i_1}^k & \xrightarrow{\mathcal{B}} v_{i_1}^{k-1} & \xrightarrow{\mathcal{B}} \dots \xrightarrow{\mathcal{B}} & \vdots \\
 & v_{i_1+1}^{k-1} & \xrightarrow{\mathcal{B}} \dots \xrightarrow{\mathcal{B}} & \vdots \\
 & \vdots & & \\
 & v_{i_1+i_2}^{k-1} & \xrightarrow{\mathcal{B}} \dots \xrightarrow{\mathcal{B}} & \vdots \\
 & & & v_{i_1+\dots i_k}
\end{array}
$$

Лемма Правые s рядов образуют базис $\ker B^s$.

Доказаельство:

переход от s к $s+1$

Каждый ряд линейно независимая. Допустим суммарно они линейно зависимые. Тогда применим B^s к комбинации линейной зависимости. Получим линейную комбинацию для векторов из $s+1$ ряда равную нулю $\Rightarrow$ все ее коэфициенты равны 0. Значит исходная комбинация была их векторов из правых s рядов чего не может быть по предположению индукции