Ответы на вопросы коллоквиума по алгебре

(октябрь 2016, 3-й семестр ПМиИ)

О. Евсеев, А. Константинов

24 декабря 2016 г.

1 ПсО как $K[x]$-модули. Морфизмы ПсО. Матрица ЛО. Замена базисов

Определение. K — поле. *ПсО* — пара $({}_KV, a \in \operatorname{End}_K V)$, где V — *линейное пространство*, a — *линейный оператор*.

Теорема 1. *K — поле.*

а) Если ${}_{K[x]}M$ — модуль, то ему сопоставляется ПсО $({}_KM, a)$.

б) Если $({}_KV, a)$ — ПсО, то ему сопоставляется $K[x]$-модуль ${}_{K[x]}\tilde{V}$.

Доказательство.

а) Положим $l\colon M \to M$, т.ч. $m \in M \xmapsto{l} xm \in M$. Так как $K \subset K[x]$, можем рассмотреть линейное пространство ${}_KM$. Ясно, что $l \in \operatorname{End}_{K[x]} M$, следовательно $l \in \operatorname{End}_K M$, откуда $({}_KM, l)$ — искомое ПсО.

б) Для $f = \sum_{i=0}^n c_i x^i \in K[x]$ и $v \in V$ положим $f \circ v := f(a)(v)$, где $f(a) = \sum_{i=0}^n c_i a^i \in \operatorname{End}_K M$. Такое действие элементов $K[x]$ задает на V структуру $K[x]$ — модуля: ${}_{K[x]}\tilde{V} = (V, \circ)$.

$\square$

Обозначим сопоставления следующим образом:

$$
{}_{K[x]}M \xmapsto{\Phi} ({}_KV, a)
$$
$$
({}_KV, a) \xmapsto{\Psi} {}_{K[x]}\tilde{V}
$$

Определение. *Морфизм ПсО* $\phi\colon ({}_KV, a) \to ({}_KV', a')$ — это K-линейное отображение $\phi\colon V \to V'$, т.ч. $a'\phi = \phi a$.

Замечание. Для того, чтобы ϕ был морфизмом ПсО, нужно, чтобы диаграмма

$$\begin{tikzcd} V \arrow[r, "a"] \arrow[d, "\phi"] & V \arrow[d, "\phi"] \\ V' \arrow[r, "a'"] & V' \end{tikzcd}$$

была коммутативной.

Теорема 2. *K — поле.*

а) Если $\phi\colon {}_{K[x]}M \to {}_{K[x]}N$ — гомоморфизм, то ϕ индуцирует морфизм ПсО $\phi\colon \Phi(M) \to \Phi(N)$.

б) Если $\phi\colon (V,a) \to (V',a')$ — морфизм ПсО, то ϕ можно продолжить до $K[x]$-гомоморфизма $\phi\colon \Psi(V,a) \to \Psi(V',a')$.

Доказательство.

а) Обозначим операторы в $\Phi(M)$ и $\Phi(N)$ через $l^{(M)}$ и $l^{(N)}$ соответственно. Тогда $\phi(l^{(M)}(m)) = \phi(xm) = x\phi(m) = l^{(N)}(\phi(m))$, откуда ясно, что $\phi \circ l^{(M)} = l^{(N)} \circ \phi$. По определению ϕ — морфизм ПсО.

б) Для $v \in {}_{K[x]}V$ и $f \in K[x]$ положим $f \cdot v = \sum_{i=0}^n c_i a^i(v)$. Тогда $\phi(f \cdot v) = \phi(\sum_{i=0}^n c_i a^i(v)) = \sum_{i=0}^n c_i \phi(a^i(v))$ в силу K-линейности ϕ. Таким образом для $K[x]$-линейности ϕ достаточно, чтобы выполнялось $\phi \circ a^i = (a')^i \circ \phi$.

База индукции: $i = 1$ — следует из определения ϕ как морфизма ПсО. Делая ИП, имеем $\phi \circ a^{i+1} = (\phi \circ a^i) \circ a \overset{\text{ИП}}{=} (a')^i \circ \phi \circ a = (a')^i \circ a' \circ \phi = (a')^{i+1} \circ \phi$.

Тогда $\sum_{i=0}^n c_i \phi(a^i(v)) = \sum_{i=0}^n c_i (a')^i(\phi(v)) = f \cdot \phi(v)$, и ϕ — гомоморфизм.

□

Определение. Пусть $({}_KV, a)$ — ПсО. Положим $B = \{u_i\}_{i=1}^n$ — базис ${}_KV$. *Матрицей ЛО a* в базисе B назовем матрицу $[a]_B \coloneqq (a_{ij})$, где $a(v_j) = \sum_{i=1}^n a_{ij} v_j$.

Теорема 3. *Пусть B, B' — базисы $({}_KV, a)$ и C — матрица перехода от B к B'. Тогда $[a']_B = C^{-1}[a]_B C$.*

Доказательство. Следует из более общей теоремы о замене базисов. □

2 Инвариантные подпространства и приведение матрицы оператора к блочно-треугольному виду. Прямая сумма подпространств и блочно-диагональный вид матрицы соответствующего оператора

Определение. Пусть $({}_KV, a)$ — ПсО. $U \le {}_KV$ называется *a-инвариантным*, если $a(U) \le U$.

Теорема 1. *K — поле.*

а) Пусть U — инвариантное подпространство в (V, a). Тогда $\Psi(U, a|_u) \leq \Psi(V, a)$.

б) Пусть ${}_{K[x]}N \leq {}_{K[x]}M$. Тогда $\Phi(N)$ — инвариантное подпространство в $\Phi(M)$ относительно $l^{(M)}$.

Доказательство.

а) Так как ${}_KU \leq {}_KV$, то $\forall u, v \in U\ u + v \in U$. Для $f = \sum_{k=0}^{n} c_k x^k \in K[x]$ и $v \in U$ $f \cdot v = \sum_{k=0}^{n} c_k a^k(v) \in U$ по инвариантности.

б) Для $v \in \Phi(N)$ $l^{(M)}(v) = xv \in N$, так как $N \leq M$.

□

Теорема 2. *Пусть $({}_KV, a)$ — ПсО, ${}_KU \leq {}_KV$ — инвариантное подпространство. Тогда существует базис в ${}_KV$, т.ч. $[a]_B$ имеет блочно-треугольный вид.*

Доказательство. Достаточно выбрать в U базис и дополнить его до базиса V. □

Теорема 3. *K — поле.*

а) Пусть ${}_{K[x]}M = \bigoplus_{i=1}^{n} {}_{K[x]}N_i$, где $N_i \leq M$. Тогда $\Phi(M) = \bigoplus_{i=1}^{n} \Phi(N_i)$.

б) Пусть (V, a) — ПсО, где $V = \bigoplus_{i=1}^{n} U_i$ (U_i — инвариантные подпространства). Тогда $\Phi(V) = \bigoplus_{i=1}^{n} \Psi(U_i)$.

Доказательство. Оба пункта следуют из совпадения рассмотренных подмодулей и инвариантных подпространств как абелевых групп. □

Теорема 4. *Пусть $({}_KV, a)$ — ПсО, ${}_KV = \bigoplus_{i=1}^{n} U_i$, где U_i — инвариантные подпространства. Тогда существует базис в ${}_KV$, т.ч. $[a]_B$ имеет блочно-диагональный вид.*

Доказательство. Достаточно выбрать базис в каждом из инвариантных подпространств. □

3 Формулировка теоремы о жордановой нормальной форме матрицы линейного оператора

Теорема. *K — алгебраически замкнутое поле. Пусть $({}_KV, a)$ — ПсО. Тогда существует базис B в ${}_KV$, т.ч. матрица $[a]_B$ имеет вид* ***жордановой нормальной формы****, то есть:*

$$[a]_B = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_t \end{pmatrix},$$

где $\forall i \ A_i \in M_{k_i}(K)$ *имеет вид* ***жордановой клетки:***

$$A_i = \begin{pmatrix} \lambda_i & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix},$$

причем такая матрица определена однозначно с точностью до порядка жордановых клеток. Соответствующий базис B *в таком случае называют* ***жордановым базисом****.*

4 Циклические модули, циклические ПсО. Аннуляторы (элемента, модуля). Простые модули. Лемма Шура

Определение. Модуль ${}_RM$ называется циклическим, если $\exists m \in M \colon M = {}_R\langle m\rangle$.

Определение. ${}_RM$ — модуль. *Аннулятор элемента* $x \in M$ — это $(0 : x) \coloneqq \{r \in R \mid rx = 0\}$. *Аннулятор модуля* M — это $(0 : M) \coloneqq \{r \in R \mid rM = \{0\}\}$.

Замечание. Легко видеть, что $(0 : x) \leq R$, $(0 : M) \lhd R$.

Определение. Пусть $({}_KV, a)$ — ПсО, ${}_{K[x]}\tilde{V}$ — соответствующий $K[x]$-модуль. Так как $K[x]$ — ОГИ, то $\forall x \in V \ (0 : x) = {}_{K[x]}\langle \mu_x\rangle$, где $\mu_x \in K[x]$. Аналогично $(0 : \tilde{V}) = {}_{K[x]}\langle \mu_a\rangle$. Считаем, что μ_x и μ_a унитальны. μ_x и μ_a называются *минимальными аннулирующими многочленами* соответственно элемента x и оператора a.

Определение. Пусть R — а.к. с единицей. Модуль ${}_RM$ называется простым, если $M \neq \{0\}$ и не содержит нетривиальных подмодулей.

Лемма. (Шура) Пусть ${}_RM$, ${}_RN$ — простые модули. Тогда:

а) Любой гомоморфизм $f \colon {}_RM \to {}_RN$ либо нулевой, либо является изоморфизмом.

б) $\operatorname{End} {}_RM$ — тело.

Доказательство.

а) НУО считаем, что f ненулевой. Так как $\ker f \leq {}_RM$ и M прост, то $\ker f = \{0\}$. Так как $\operatorname{im} f \leq {}_RN$ и N прост, то $\operatorname{im} f = N$. Отсюда следует, что f — изоморфизм.

б) Явным образом следует из предыдущего пункта (все ненулевые элементы обратимы).

$\square$

5 Определение и свойства фактормодуля

Определение. R — а.к. с единицей. Пусть $N \leq {}_R M$. На факторгруппе $\bar{M} \coloneqq M/N$ рассмотрим действие элементов из R $\mu\colon R \times \bar{M} \to \bar{M}$, т.ч. $\mu(r, \bar{m}) = \overline{rm}$.

Модуль $(\bar{M}, \mu)$ назовем фактормодулем.

Замечание. Определение μ корректно, т.к. если $m_1 \in \bar{m}$, то $m_1 - m \in N$ и, соответственно, $r(m_1 - m) \in N$, откуда $\overline{rm_1} = \overline{rm}$.

Теорема. *R — а.к. с единицей. Пусть $N \leq {}_R M$. Тогда:*

а) $(\bar{M}, \mu)$ — левый R-модуль.

б) Каноническое отображение $\pi\colon M \to \bar{M}$ — эпиморфизм.

в) Существует биекция между множеством подмодулей M, содержащих N, и множеством всех подмодулей $\bar{M}$.

Доказательство.

а) Очевидно.

б) Очевидно.

в) Положим $\Phi \coloneqq \{K \mid K \leq M\colon N \subset K\}$, $\Psi \coloneqq \left\{P \mid P \leq \bar{M}\right\}$. Введем отображения α и β между Φ и Ψ и обратно соответственно, т.ч. $\alpha(K) = \pi(K)$, $\beta(P) = \pi^{-1}(P)$.

Пусть $K \leq {}_R M$, тогда $K \leq M$ как группа. Для $r \in R$, $\bar{x} \in \alpha(K)$ имеем $r\bar{x} = \overline{rx} \in \alpha(K)$ (в силу того, что $rx \in K$). Так, $\alpha(K) \leq {}_R \bar{M}$. Аналогично доказывается, что $\beta(P) \in {}_R M$.

Очевидно, что $\alpha(\beta(P)) = \pi(\pi^{-1}(P)) = P$, т.к. π — сюръекция. Пусть $x \in \beta(\alpha(k))$, тогда $\exists k \in K\colon \pi(x) = \pi(k)$, откуда $\pi(x - k) = 0$ и, следовательно, $x - k \in \ker \pi = N \subset K \Rightarrow x - k \in K \Rightarrow x \in K$. Мы доказали, что $\beta(\alpha(K)) \subset K$; обратное включение очевидно.

Так как $\alpha \circ \beta = \mathrm{id}_\Psi$ и $\beta \circ \alpha = \mathrm{id}_\Phi$, то α и β взаимно обратны.

□

6 Теоремы об изоморфизмах для модулей

Теорема 1. *(I теорема об изоморфизме) Пусть $f\colon {}_R M \to {}_R N$ — гомоморфизм R-модулей. Тогда $\operatorname{im} f \simeq M/\ker f$.*

Доказательство. Положим $\phi : M/\ker f \to \operatorname{im} f$, т.ч. $\bar{x} \mapsto x$. По IТоИ для групп ϕ — изоморфизм $M/\ker f$ и $\operatorname{im} f$ как групп, при этом очевидна R-линейность ϕ. Таким образом, ϕ — соответствующий изоморфизм модулей. □

Теорема 2. *${}_R M$ — модуль, $N \leq {}_R M$. Пусть $\psi\colon M \to M_1$ — гомоморфизм модулей, т.ч. $N \subset \ker \psi$. Тогда $\exists! \psi'\colon M/N \to M_1$, т.ч. $\psi' \pi = \psi$.*

Доказательство. Положим $\psi'(\bar{x}) = \psi(x)$. По теореме о продолжении группового гомоморфизма на факторгруппу ψ' — единственный групповой гомоморфизм $M/N \to M_1$, т.ч. $\psi'\pi = \psi$.

$$\begin{tikzcd} M \arrow[r, "\pi"] \arrow[dr, "\psi"'] & M/N \arrow[d, dashed, "\psi'"] \\ & M_1 \end{tikzcd}$$

При этом очевидна R-линейность ψ'. Таким образом, ψ' — искомый гомоморфизм модулей. $\square$

Теорема 3. *(II теорема об изоморфизме) Пусть $N, S \leq {}_RM$ и $N \subset S$. Тогда $M/S \simeq (M/N)/(S/N)$.*

Доказательство. Пусть $\psi\colon M \to M/S$ — проекция. Тогда $\ker\psi = S$, но $N \subset S$; таким образом $\exists!\psi'\colon M/N \to M/S$, т.ч. $\ker\psi' = S/N$.

$$\begin{tikzcd} M \arrow[r, two heads, "\psi"] \arrow[dr, "\pi"'] & M/S \\ & M/N \arrow[u, "\psi'"'] \end{tikzcd}$$

При этом ψ — эпиморфизм, следовательно, $\forall\bar{x} \in M/S\ \exists y \in M\colon \psi(y) = \bar{x} \Rightarrow \psi'(\pi(y)) = \psi(y) = \bar{x} \Rightarrow \exists z = \pi(y)\colon \psi'(z) = \bar{x}$ и ψ' — эпиморфизм.

По IТоИ $M/S = \operatorname{im}\psi' \simeq (M/N)/\ker\psi' = (M/N)/(S/N)$. $\square$

Теорема 4. *(III теорема об изоморфизме) Пусть $L, K \leq {}_RM$. Тогда $(L+K)/K \simeq L/(L \cap K)$.*

Доказательство. Рассмотрим $\phi\colon L \to (L+K)/K$, т.ч. $\phi(l) = \bar{l}$. Очевидно, что ϕ — гомоморфизм.

Пусть $t = l + k \in L + K$, тогда $\bar{t} = t + K = l + K = \bar{l}$, откуда $\phi(l) = \bar{t}$. Ясно, что ϕ — эпиморфизм.

Пусть $l \in \ker\psi$. Тогда $\bar{l} = \bar{0} \Rightarrow l \in K \to l \in L \cap K$. Пусть $t \in L \cap K$, тогда $t \in K \Rightarrow \phi(t) = 0 \Rightarrow t \in \ker\psi$. Отсюда следует, что $L \cap K = \ker\psi$.

Дальнейшее очевидно по IТоИ. $\square$

7 Определение свободного модуля. Конструкция свободного модуля

Определение. Пусть $X \neq \varnothing$, $X \subset {}_RM$, $i\colon X \to M$ — вложение. Модуль ${}_RM$ называется свободным, если для любого R-модуля N и любого теоретико-множественного отображения $f\colon X \to N$ существует единственный R-гомоморфизм $\phi\colon M \to N$, т.ч. $\phi i = f$.

Рассмотрим следующее множество формальных конечных сумм:

$$F_X \coloneqq \left\{ \sum_{x \in X} r_x x \mid r_x \in R, \text{п.в. } r_x = 0 \right\}$$

Введем операции:

$$\sum_{x \in X} r_x x + \sum_{x \in X} s_x x \coloneqq \sum_{x \in X} (r_x + s_x) x$$
$$r \cdot \sum_{x \in X} r_x x \coloneqq \sum_{x \in X} (r r_x) x$$

Теорема. *F_X — свободный R-модуль, определяемый X.*

Доказательство.

а) Пусть $\phi_0 \colon X \to {}_R M$, где ${}_R M$ — произвольный R-модуль. Рассмотрим $\phi \colon F_X \to M$, т.ч. $\phi(\sum_{x \in X} r_x x) \coloneqq \sum_{x \in X} r_x \phi_0(x) \in M$. Очевидно, что ϕ — гомоморфизм, при этом $\phi \circ i = \phi|_X = \phi_0$.

б) Предположим, что существует еще один гомоморфизм $\tilde{\phi} \colon F_X \to M$, т.ч. $\tilde{\phi} i = \phi_0$. Тогда $\tilde{\phi}(\sum_{x \in X} r_x x) = \sum_{x \in X} r_x \tilde{\phi}(x) = \sum_{x \in X} r_x \phi_0(x) = \phi(\sum_{x \in X} r_x x)$, откуда $\tilde{\phi} \equiv \phi$.

□

8 Существование эпиморфизма из свободного модуля в данный

Теорема. *Пусть ${}_R M$ — модуль. Тогда существует эпиморфизм $\phi \colon F \to M$, где F — некоторый свободный модуль.*

Доказательство. Пусть $M = {}_R \langle X \rangle$. Рассмотрим диаграмму:

$$\begin{tikzcd} F\langle X \rangle \arrow[r, two heads, "\phi"] & M \\ X \arrow[u, hook, "i"] \arrow[ur, hook, "j"'] & \end{tikzcd}$$

По универсальному свойству свободного модуля $\exists! \phi \colon F\langle X \rangle \to M$, т.ч. $\phi \circ i = j$. Пусть $m \in M$, тогда $m = \sum_{x \in X} r_x x = \sum_{x \in X} r_x j(x) = \sum_{x \in X} r_x \phi(i(x)) = \phi \underbrace{\left(\sum_{x \in X} r_x i(x) \right)}_{=: z \in F\langle X \rangle}$.

Так, $\exists z \in F\langle X \rangle \colon \phi(z) = m$, откуда ϕ — эпиморфизм. □

Следствие. *Пусть ${}_R M = {}_R \langle X \rangle$. Тогда ${}_R M \simeq F\langle X \rangle / P$, где P — некоторый подмодуль ${}_R F\langle X \rangle$.*

Доказательство. Согласно теореме, существует эпиморфизм $\phi \colon F\langle X \rangle \to M$. По ITоИ ${}_R M \simeq F\langle X \rangle / \ker \phi$. При этом $\ker \phi$ — искомый подмодуль P. □

9 Инвариантность ранга при изоморфизме свободных модулей

Теорема. *R — к.к. с единицей. Пусть X, Y — непустые конечные множества. Тогда если $F\langle X\rangle \simeq F\langle Y\rangle$, то $\#X = \#Y$.*

Доказательство. Отождествим $F\langle X\rangle$ и $F\langle Y\rangle$ и будем обозначать их как F. Пусть $X = \{x_i\}_{i=1}^n$. Т.к. R — к.к. с единицей, то существует максимальный двусторонний идеал $P \lhd R$. Положим $K \coloneqq R/P$. Так как P максимальный, K — поле.

Рассмотрим $P\cdot F \coloneqq \left\{\sum_{i\in I} p_i f_i \mid p_i \in P, f_i \in F, \text{п.в. } p_i = 0\right\}$. Ясно, что $P\cdot F \le {}_R F$. Рассмотрим дополнительно $\bar{F} \coloneqq F/(P\cdot F)$. Пусть $\pi\colon F \to \bar{F}$ — проекция. Введем на $\bar{F}$ структуру K-линейного пространства: $\bar{r}\cdot\bar{f} \coloneqq r\bar{f} = \overline{rf}$. Оределение корректно: если $\bar{r} = \bar{k}$, то $k = r - p$, где $p \in P$, и тогда $\bar{k}\cdot\bar{f} = \overline{rf} - \overline{pf} = \overline{rf} - \bar{0} = \overline{rf}$.

Положим $\bar{X} \coloneqq \pi(X), \bar{Y} \coloneqq \pi(Y)$. Так как $t \in \bar{F}$ представимо в виде $t = \overline{\sum_{z\in X} r_z z} = \sum_{z\in X} \overline{r_z z} = \sum_{z\in X} \underbrace{\bar{r_z}}_{\in K} \cdot \underbrace{\bar{z}}_{\in \bar{X}}$, то $\bar{F} = {}_K\langle \bar{X}\rangle$.

Предположим, что $\sum_{i=1}^n \bar{r_i}\bar{x_i} = \bar{0}$, $\bar{r_i} \in K$. Тогда $\sum_{i=1}^n r_i x_i \in P\cdot F \Rightarrow \sum_{i=1}^n r_i x_i = \sum_{i=1}^n p_i x_i$, где $p_i \in P$. Так как X — базис, то $\forall i\ r_i = p_i$. Таким образом, в K $\bar{r_i} = \bar{0}$.

Из вышесказанного следует, что $\bar{X}$ — базис $\bar{F}$, аналогично $\bar{Y}$ — базис $\bar{F}$. Их мощности совпадают и равны $\dim_K \bar{F}$.

$\pi\colon X \to \bar{X}$ сюръективно по определению и инъективно в силу линейной независимости $\bar{X}$; аналогично $\pi\colon Y \to \bar{Y}$ — биекция. Так, $\#X = \#\bar{X} = \#\bar{Y} = \#Y$. $\square$

10 Однозначная определенность ранга свободной группы

Теорема. *Пусть X, Y — непустые конечные множества. Тогда если $F\langle X\rangle \simeq F\langle Y\rangle$, то $\#X = \#Y$.*

Доказательство. Отождествим $F\langle X\rangle$ и $F\langle Y\rangle$ и обозначим их как F. Рассмотрим $\bar{F} \coloneqq F/[F,F]$ — абелизацию F (она, естественно, коммутативна). Пусть $\pi\colon F \to \bar{F}$ — проекция. Положим $\bar{X}$ и $\bar{Y}$ — образы X и Y соответственно.

Докажем, что $\pi_0 \coloneqq \pi|_X\colon X \to \bar{X}$ инъективно. Для фиксированного $x \in X$ число вхождений x в $w \in \bar{x}$ нечетно, а для $y \in X \setminus \{x\}$ — четно, отсюда очевидна инъективность; аналогично для Y и $\bar{Y}$.

Рассмотрим диаграмму:

$$\begin{tikzcd}
X \arrow[rr, "\pi_0", "\sim"'] \arrow[dd, hook, "i"'] & & \bar{X} \arrow[dl, "\phi_0"'] \arrow[dd, hook, "j"] \\
& {}_{\mathbb{Z}}M & \\
F\langle X\rangle \arrow[ur, dashed, "\psi"] \arrow[rr, two heads, "\pi"] & & \bar{F} \arrow[ul, dashed, "\phi"']
\end{tikzcd}$$

Докажем, что ${}_{\mathbb{Z}}\bar{F}$ — свободный модуль с базисом $\bar{X}$. Пусть даны ${}_{\mathbb{Z}}M$ и $\phi_0\colon \bar{X} \to M$. Тогда для отображения $\phi_0\pi_0$ по универсальному свойству ${}_{\mathbb{Z}}F\langle X\rangle$ существует единственный гомоморфизм ψ, т.ч. $\phi_0\pi_0 = \psi i$. Так как ${}_{\mathbb{Z}}M$ коммутативна, то существует единственный гомоморфизм ϕ, т.ч. $\phi\pi = \psi$. Получаем $\phi_0\pi_0 = \psi i = \phi\pi i = \phi j\pi_0$, откуда в силу того, что π_0 — сюръекция, $\phi_0 = \phi j$. Отсюда следует, что ${}_{\mathbb{Z}}\bar{F}$ — свободный модуль с базисом $\bar{X}$. Аналогичным образом утверждение доказывается для базиса $\bar{Y}$.

Имеем $\#X = \#\bar{X} = \#\bar{Y} = \#Y$. □

11 Замена базисов в свободном модуле конечного ранга над коммутативным кольцом. Матрица перехода

Теорема. *Пусть R — к.к. с единицей, F — свободный R-модуль с базисом $X = \{x_i\}_{i=1}^n$, C — квадратная матрица над R (**матрица перехода**). Дополнительно положим $x'_j \coloneqq \sum_{i=1}^n c_{ij}x_i$. Равносильны следующие утверждения:*

а) $X' \coloneqq \left\{x'_j\right\}_{j=1}^n$ — базис ${}_RF$.

б) $C \in M_n(R)^*$.

Доказательство. <u>(a) ⇒ (б)</u>. Так как X' — базис, то $\forall k$ имеем $x_k = \sum_{s=1}^n d_{sk}x'_s = \sum_{s=1}^n d_{sk}\sum_{i=1}^n c_isx_i = \sum_{i=1}^n \underbrace{\left(\sum_{s=1}^n c_{is}d_{sk}\right)}_{=(CD)_{ik}} x_i$. Так как X — базис, $(CD)_{ik} = \delta_{ik}$, или $CD = E_n$, откуда следует, что C обратима.

<u>(б) ⇒ (а)</u> Предположим, что $\sum_{t=1}^n p_tx'_t = 0$. Тогда $\sum_{t=1}^n p_t\sum_{i=1}^n c_{it}x_i = 0$. Так как X — базис, то $\forall i\, \sum_{t=1}^n c_{it}p_t = 0$. Пусть $P = (p_1, \dots, p_n)^T$, тогда $CP = \mathbf{0} \Rightarrow P = \mathbf{0} \Rightarrow \forall t\ p_t = 0$. □

13 Конечно порожденные модули над нетеровыми кольцами

Лемма. R — а.к. с единицей. Пусть $N \le {}_RM$, ${}_R\bar{M} \coloneqq M/N$. Если ${}_RN$ и ${}_R\bar{M}$ конечно порожденные, то ${}_RM$ конечно порожденные.

Доказательство. Пусть ${}_RN = {}_R\langle x_1, \dots, x_m\rangle$, ${}_RM = {}_R\langle \bar{y}_1, \dots, \bar{y}_n\rangle$. Докажем, что ${}_RM = {}_R\langle x_1, \dots, x_m, y_1, \dots, y_n\rangle$. Положим $m \in M$, тогда $\bar{m} \in \bar{M}$. $\bar{m}$ представимо в виде $\bar{m} = \sum_{j=1}^n s_j\bar{y}_j = \overline{\sum_{j=1}^n s_jy_j}$. Отсюда $m - \sum_{j=1}^n s_jy_j \in N \Rightarrow m - \sum_{j=1}^n s_jy_j = \sum_{k=1}^n r_kx_k \Rightarrow m = \sum_{j=1}^n s_jy_j + \sum_{k=1}^n r_kx_k$. Таким образом m представим в виде линейной комбинации конечного числа элементов. □

Теорема 1. *R — нётерово слева кольцо, ${}_RM$ — конечно порожденный модуль. Пусть $N \le {}_RM$, тогда ${}_RN$ — конечно порожденный.*

Доказательство. Считаем, что M ненулевой (тривиальный случай). Положим $M = {}_R\langle a_1, \dots, a_n\rangle$, где n — наименьшая возможная мощность множества образующих.

Произведем индукцию по n. База индукции — $n = 1$. В таком случае ${}_RM$ — циклический модуль, что эквивалентно тому, что $M \simeq {}_RR/I$, где $I \leq {}_RR$ — некоторый идеал. Считаем, что $M = {}_RR/I$. Так как $N \leq {}_RM$, то по биекции между подмодулями M и подмодулями R, содержащими I, имеем $N = \pi(J)$, где π — проекция, $I \subset J \leq {}_RR$. Так как R нетерово, любой его идеал конечно порожден. В то же время $N = \pi(J) = J/I$, откуда очевидна конечнопорожденность N.

Сделаем индукционное предположение. Рассмотрим $M' \coloneqq {}_R\langle a_1, \dots, a_{n-1}\rangle \lneq {}_RM$. Заметим, что в этом случае фактормодуль M/M' ненулевой и цикличен. Рассмотрим $M' \cap N \leq M'$. Очевидно, что в нем не более $n-1$ образующих. Тогда, по ИП, $M' \cap N$ конечно порожден. По IIIТоИ $N/(N \cap M') \simeq (N + M')/M' \leq M/M'$, где последний цикличен. Тогда первый конечно порожден, а, следовательно (по лемме), конечно порожден и N. □

14 Периодическая часть модуля над областью целостности. Свойства

Определение. R — область целостности, ${}_RM$ — модуль. *Периодическая часть* (или *кручение*) модуля M — это $tM \coloneqq \{m \in M \mid \exists r \in R \setminus \{0\}\colon rm = 0\}$.

Если $tM = \{0\}$, то M называется модулем без кручения.

Если $tM = M$, то M называется периодическим модулем.

Теорема 1. *Пусть R — о.ц., ${}_RM$ — модуль. Тогда:*

а) $tM \leq {}_RM$

б) M/tM — модуль без кручения.

Доказательство.

а) Пусть $m_1, m_2 \in tM$, тогда $\exists r_1, r_2 \in R \setminus \{0\}\colon r_1m_1 = r_2m_2 = 0 \Rightarrow r_1r_2(m_1 + m_2) = 0 \Rightarrow m_1 + m_2 \in tM$. При этом $\forall r \in R$ имеем $r_1(rm_1) = r(r_1m_1) = 0 \Rightarrow rm_1 \in tM$. Отсюда $tM \leq {}_RM$.

б) Пусть $\bar{m} \in t(M/tM)$. Тогда $\exists r \in R \setminus \{0\}\colon r \cdot \bar{m} = \overline{rm} = 0$. Отсюда $rm \in tM$, то есть $\exists s \in R \setminus \{0\}\colon srm = 0$. Но $sr \neq 0$, то есть $m \in tM$, или, что эквивалентно, $\bar{m} = \bar{0}$.

□

Теорема 2. *Пусть R — о.ц., $\{M_i\}_{i \in I}$ — семейство R-модулей. Тогда $t(\bigoplus_{i\in I} M_i) = \bigoplus_{i \in I} tM_i$.*

Доказательство. Обозначим за LHS и RHS левую и правую часть соответственно.

а) Пусть $(x_i)_{i\in I} \in LHS$. Тогда $\exists r \in R \setminus \{0\}\colon r(x_i)_{i\in I} = 0 \Rightarrow \forall i\ rx_i = 0 \Rightarrow \forall i\ x_i \in tM_i \Rightarrow (x_i)_{i\in I} \in RHS$.

б) Пусть $(x_i)_{i\in I} \in RHS$. Так как $(x_i)_{i\in I}$ по определению содержит лишь конечное число ненулевых элементов и при этом $\forall i \in I$, т.ч. $x_i \neq 0$, $\exists r_i \neq 0\colon r_i x_i = 0$, можем положить $r \coloneqq \prod_{i\in I \text{ т.ч. } x_i\neq 0} r_i$. Ясно, что $r(x_i)_{i\in I} = 0$, откуда $(x_i)_{i\in I} \in LHS$.

Прямое и обратное включение доказаны; таким образом, $LHS = RHS$. □

16 Канонический вид матрицы над евклидовым кольцом (форма Смита)

Теорема. *R — евклидово кольцо с нормой $\nu : R \setminus \{0\} \to \mathbb{N}_0$. Пусть $A \in M_{m,n}(R)$, тогда существует последовательность ЭП над строками и столбцами, приводящая ее к виду* $\mathrm{diag}(d_1, \dots, d_k, 0, \dots, 0)$*, где $\forall i\ d_i \mid d_{i+1}$.*

Доказательство. Считаем, что матрица A ненулевая (тривиальный случай).

Положим $\nu\colon M_{m,n}(R) \setminus \{0\} \to \mathbb{N}_0$, т.ч. $X = (x_{ij}) \mapsto \min\{\nu(x_{ij}) \mid x_{ij} \neq 0\}$. Рассмотрим на $M_{m,n}(R)$ отношение эквивалентности $X \sim Y \Leftrightarrow$ существует последовательность ЭП, приводящая X к Y. Обозначим класс эквивалентности A относительно $\sim$ как $[A]$.

Выберем $x \in [A]$ с наименьшим возможным значением $\nu(x) =: \nu_0$ Переобозначим $A \coloneqq X$. НУО считаем, что $\nu(a_{11}) = \nu_0$. Обозначим $d \coloneqq a_{11}$.

Докажем, что $\forall i > 1\ d \mid a_{i1}$. Предположим, что это не так и $\exists i > 1\colon a_{i1} \not\vdots\, d$. Тогда $a_{i1} = qd + r$, где $q, r \in R$ и $\nu(r) < \nu(d) = \nu_0$. Выполнив ЭП вида

$$ⓘ - q \cdot ① \longmapsto ⓘ, \tag{1}$$

получим $\tilde{A} \in [A]$, для которой $\nu(\tilde{A}) \leq \nu(R) < \nu_0$, что противоречит выбору A. Аналогичным образом доказывается, что $\forall j > 1\ d \mid a_{1j}$.

Выполняя для $i = 2 \dots m$ ЭП вида (1) и аналогичные им ЭП над столбцами, получаем матрицу вида:

$$\left(\begin{array}{c|c} d & \mathbf{0} \\ \hline \mathbf{0} & A' \end{array}\right), A' = (a'_{ij}) \in M_{m-1,n-1}(R) \tag{2}$$

Докажем, что $\forall i, j > 1\ a'_{ij} \vdots\, d$. Предположим, что это не так, и $\exists i, j > 1\colon a'_{ij} \not\vdots\, d$. Тогда выполнив ЭП вида $\boxed{1} + \boxed{j} \longmapsto \boxed{1}$ получим матрицу из $[A]$, у которой элемент на позиции $(i, 1)$ не делится на d, что невозможно по предыдущему рассуждению.

Аналогичный процесс применим к A'. Так как количество ненулевых элементов в A конечно, то процесс обрывается, сходясь к искомой форме. □

17 Гомоморфизмы между свободными модулями конечного ранга над евклидовым кольцом

Теорема. *R — е.к. Пусть $\alpha\colon F \to G$ — гомоморфизм R-модулей конечного ранга. Тогда:*

а) $\ker\alpha$ *и* $\operatorname{im}\alpha$ *свободны.*

б) $F \simeq \ker\alpha \oplus \operatorname{im}\alpha$.

Доказательство.

а) Пусть $B_1 = \{u_j\}_{j=1}^n$ и $B_2 = \{v_i\}_{i=1}^m$ — базисы, т.ч. $[\alpha]_{B_1B_2}$ имеет форму Смита. Тогда:

$$\alpha(u_i) = \begin{cases} \alpha_i v_i, 1 \le i \le k \\ 0, i > k \end{cases}$$

Докажем, что $u_{k+1}, \dots, u_n$ — базис $\ker\alpha$. Пусть $x = \sum_{i=1}^n \lambda_i u_i \in \ker\alpha$, $\lambda_i \in R$. Тогда $0 = \alpha(x) = \sum_{i=1}^n \lambda_i \alpha(u_i) = \sum_{i=1}^k (\lambda_i\alpha_i)v_i$. По линейной независимости $\forall i = 1 \dots k$ имеем $\lambda_i\alpha_i = 0$. Но $\alpha_i \ne 0 \Rightarrow \forall i \le k\ \lambda_i = 0$, откуда $x \in {}_R\left\langle \{u_j\}_{j=k+1}^n \right\rangle$. Мы доказали, что $\ker\alpha \subset {}_R\left\langle \{u_j\}_{j=k+1}^n \right\rangle$, обратное включение очевидно, отсюда $\ker\alpha$ — свободный модуль.

б) $\operatorname{im}\alpha = {}_R\left\langle \{\alpha_i v_i\}_{i=1}^k \right\rangle \simeq {}_R\left\langle \{v_i\}_{i=1}^k \right\rangle \simeq {}_R\left\langle \{u_i\}_{i=1}^k \right\rangle$, откуда $\operatorname{im}\alpha$ — свободный модуль.

$F = {}_R\left\langle \{u_i\}_{i=1}^k \right\rangle \oplus {}_R\langle \{u_i\}_{i=k+1}^n \rangle$, откуда $F \sim \operatorname{im}\alpha \oplus \ker\alpha$.

□

18 Подмодули свободных модулей. Согласованные базисы

Теорема. *R — е.к., ${}_RF$ — свободный R-модуль конечного ранга. Пусть $U \le {}_RF$, тогда:*

а) U *— свободный R-модуль.*

б) $\operatorname{rk} U \le \operatorname{rk} F$.

Доказательство. Так как R — нетерово кольцо, а ${}_RF$ — конечно порожденный модуль, то ${}_RU$ также конечно порожден. При этом существует эпиморфизм $\pi\colon {}_RG \to {}_RU$, где G — некоторый свободный модуль.

Рассмотрим $\alpha = i \circ \pi$ (i — вложение):

$$\begin{tikzcd} G \arrow[r, two heads, "\pi"] \arrow[dr, dashed, "\alpha"'] & U \arrow[d, hook, "i"] \\ & F \end{tikzcd}$$

Очевидно, что $\operatorname{im}\alpha = U$. Тогда U свободен как образ гомоморфизма свободных модулей. При этом $\operatorname{rk} U = \operatorname{rk}(\operatorname{im}\alpha) \le \operatorname{rk} F$. $\square$

Следствие. *В $_RF$ существует базис $\{u_i\}_{i=1}^n$, т.ч. $U = {}_R\left\langle \{d_i u_i\}_{i=1}^k \right\rangle$, где $d_i \in R \setminus \{0\}$ и $\forall i\ d_i \mid d_{i+1}$.*

Доказательство. Рассмотрим $i\colon U \to F$ — вложение. Возьмем в U и F базисы $B_1 = \{t_i\}_{i=1}^k$ и $B_2 = \{u_i\}_{i=1}^n$, т.ч. $[i]_{B_1,B_2}$ имеет форму Смита. Тогда $t_i = i(t_i) = d_i u_i$. $\square$

19 Строение конечно порожденных модулей над евклидовым кольцом. Свобода конечно порожденных модулей без кручения. «Инвариантные множители» для конечно порожденного периодического модуля

Лемма. R — а.к. с единицей, $_RX = {}_RY \oplus {}_RZ$. Пусть $_RY' \le {}_RY$, $_RZ' \le {}_RZ$ и $X' \coloneqq Y' \oplus Z' \le {}_RX$. Тогда $X/X' \simeq Y/Y' \oplus Z/Z'$.

Доказательство. Рассмотрим $f\colon X/X' \to Y/Y' \oplus Z/Z'$, т.ч. $x + X' = y + z + X' \mapsto (y + Y', z + Z')$ $(x \in X, y \in Y, z \in Z)$. Очевидно, что f — изоморфизм. $\square$

Теорема. *R — е.к. Пусть $_RM$ — конечно порожденный модуль, тогда $_RM \simeq tM \oplus M_0$, где M_0 — свободный R-модуль конечного ранга.*

Доказательство. Можно считать, что $_RM = F/U$, где F — свободный модуль конечного ранга, $U \le {}_RF$. По теореме о согласованных базисах существует базис $_RF$ $\{u_i\}_{i=1}^n$ т.ч. $\{d_i u_i\}_{i=1}^k$ (где $d_i \in R \setminus \{0\}$ и $\forall i\ d_i \mid d_{i+1}$) — базис $_RU$.

Тогда $F \simeq \bigoplus_{i=1}^n Ru_i$, $U \simeq \bigoplus_{i=1}^k Rd_iu_i$. Отсюда по лемме с использованием ММИ:

$$M = F/U \simeq \underbrace{\left(\bigoplus_{i=1}^{k} Ru_i/Rd_iu_i\right)}_{=:M_1} \oplus \underbrace{\left(\bigoplus_{i=k+1}^{n} Ru_i\right)}_{=:M_0} \tag{1}$$

Для M_0 факторизация по $\{0\}$ тождественна и ей можно пренебречь. Ясно, что M_0 — свободный R-модуль.

Положим $d \coloneqq \prod_{i=1}^k d_i \ne 0$. Тогда $\forall x \in M_1\ dx = 0$, откуда M_1 — периодический. Его кручение $tM = t(M_1 \oplus M_0) = tM_1 \oplus tM_0 = M_1 \oplus \{0\} = M_1$, откуда $M = tM \oplus M_0$, где M_0 — свободный. $\square$

Следствие 1. *Пусть R — е.к., тогда любой конечно порожденный R-модуль ${}_RM$ без кручения свободен.*

Доказательство. По теореме $M \simeq tM \oplus M_0$, где M_0 свободен. Но $tM = \{0\}$. □

Следствие 2. *R — е.к. Пусть ${}_RM$ — конечно порожденный периодический модуль, тогда $M \simeq \bigoplus_{i=1}^t R/\langle d_i \rangle$, где $d_i \in R \setminus \{0\}$ и $\forall i\ d_i \mid d_{i+1}$.*

Доказательство. Заметим, что $R/\langle d_i \rangle \sim Ru_i/Rd_iu_i$. Тогда утверждение следует из (1). □

20 Разложение периодического модуля над евклидовым кольцом в прямую сумму примарных компонент

Определение. Пусть R — е.к., $P =< p >$ — максимальный идеал в R. *P-примарной компонентой модуля ${}_RM$* назовем $M_P \coloneqq \{x \in m \mid \exists n \in N \colon p^n x = 0\}$. Ясно, что $M_P \leq {}_RM$. При этом сам ${}_RM$ называется *P-примарным*, если $M = M_P$.

Теорема. *R — е.к. Пусть ${}_RM$ — периодический модуль, Π — множество всех максимальных идеалов в R. Тогда $M = \bigoplus_{P \in \Pi} M_P$.*

Доказательство.

а) (представимость в виде суммы) Пусть $x \in M \setminus \{0\}$. Рассмотрим $I \coloneqq (0 \colon x) \neq 0$ (такой I существует, так как M периодичен). $I \leq {}_RR$, но R евклидово $\Rightarrow I = {}_R\langle a \rangle$, где $a \in R \setminus \{0\}$. Применим к a ОТА и получим разложение в виде $a = \epsilon \prod_{i=1} tp_i^{\alpha_i}$. НУО считаем, что $\epsilon = 1$. По теореме о представлении циклического модуля в виде фактормодуля имеем:

$$Rx \simeq R/I = R/_R\langle a \rangle \overset{\text{КТО}}{\simeq} \bigoplus_{i=1}^{t} R/_R\langle p_i^{\alpha_i} \rangle$$

Положим $P_i = {}_R\langle p_i \rangle \in \Pi$. Отождествим Rx и прямую сумму справа. Имеем $R/_R\langle p_i^{\alpha_i} \rangle \subset M_{P_i} \Rightarrow Rx \subset \bigoplus_{i=1}^t M_{P_i} \subset \bigoplus_{P \in \Pi} M_P \Rightarrow M \subset \bigoplus_{P \in \Pi}$. Обратное включение очевидно.

б) :(

□

21 Конечномерные ПсО и конечно порожденные периодические модули над $K[x]$

Теорема. *K — поле, $({}_KV, a)$ — ПсО, ${}_{K[x]}\tilde{V}$ — соответствующий модуль. Пусть $\dim {}_KV < \infty$, тогда ${}_{K[x]}\tilde{V}$ — конечно порожденный периодический модуль.*

Доказательство.

а) Так как $K \subset K[x]$, очевидна конечнопорожденность ${}_{K[x]}\tilde{V}$. Пусть $v \in {}_{K[x]}\tilde{V}$. Рассмотрим семейство $\left\{a^i(v)\right\}_{i\in\mathbb{N}_0} = \left\{x^i \cdot v\right\}_{i\in\mathbb{N}_0}$. Так как ${}_KV$ конечномерно, $\exists n \in \mathbb{N}_0$, т.ч. это семейство линейно зависимо. Тогда существует ненулевой $f = \sum_{i=0}^n c_i x^i$, т.ч. $fv = 0$, то есть f принадлежит $t_{K[x]}\tilde{V}$, то есть модуль периодический.

б) Пусть ${}_{K[x]}\tilde{V} = {}_{K[x]}\left\langle \{v_i\}_{i=1}^m \right\rangle$, где m — минимально возможное количество образующих.

Произведем индукцию по m. База: $m = 1$, тогда ${}_{K[x]}\tilde{V}$ — циклический, откуда ${}_{K[x]}\tilde{V} \simeq {}_{K[x]}K[x]/\langle f\rangle = {}_KK[x]/\langle f\rangle$. При этом, если $\deg f = n$, то $\{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}$ — базис ${}_KK[x]/\langle f\rangle$, откуда ${}_KV$ конечномерно.

Сделаем индукционное предположение. Рассмотрим ${}_{K[x]}U \coloneqq {}_{K[x]}\langle\{v_1, \dots, v_{m-1}\}\rangle \lneq {}_{K[x]}\tilde{V}$. Тогда ${}_{K[x]}V/U$ циклический, откуда по БИ ${}_KV/U$ конечномерно, при этом ${}_KU$ конечномерно по ИП. Так, ${}_KV$ конечномерно.

□

22 Первая каноническая форма (Фробениуса) матрицы линейного оператора

Теорема. *Пусть K — поле, $({}_KV, a)$ — конечномерное ПсО. Тогда существует базис B в ${}_KV$, т.ч.* $[a]_B = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_t \end{pmatrix}$, *где $A_i = A^{(h_i)}$ — сопровождающая матрица неприводимого над K унитального многочлена $h_i = p_i^{l_i}$.*

Доказательство. «В общем. Есть у нас конечномерное ПсО $({}_KV, a)$. Берем соответствующий $K[x]$-модуль M, он будет конечнопорождённым и периодическим. По следствию теоремки о примарном разложении его можно рассыпать в прямую сумму циклических примарных модулей $K[x]/\left\langle p_i^{l_i}\right\rangle$, где p_i — неприводимые, l_i — натуральная степень. Произведем отождествление по изоморфизму и будем считать, что $M = \bigoplus K[x]/\left\langle p_i^{l_i}\right\rangle$.

Каждому из этих прямых слагаемых соответствует некоторое a-инвариантное циклическое подпространство U_i в ${}_KV$. Т.к. прямая сумма подмодулей и прямая сумма соответствующих a-инвариантных подпространств совпадают, то $V = \bigoplus V_i$ — прямая сумма циклических a-инвариантных подпространств. Т.к. они a-инвариантны, то матрица $[a]$ в базисе, составленном из базисов U_i, будет блочно-диагональной. Т.е. достаточно выбрать базис U_i так, чтобы соответствующая клетка имела нужный вид. Подпространства циклические. Заметим, что для каждого из них аннулятор — это соответствующий $\left\langle p_i^{l_i}\right\rangle$, т.е. для каждого из них минимальным многочленом является $p_i^{l_i}$. Теперь юзаем теоремку о том, что в циклическом ПсО можно выбрать базис, в котором матрица оператора совпадает с сопровождающей матрицей минимального многочлена. Получаем нужный вид клетки.

q.e.d.» $\square$

24 Характеристический многочлен оператора. Собственные числа и собственные векторы оператора. Связь с с.ч. и с.в. матрицы оператора. Собственное подпространство оператора

Определение. K — поле, $({}_KV, a)$ — конечномерное ПсО. *Характеристический многочлен* a — это $\chi_a \coloneqq \chi_A = \det(A - xE)$, где A — матрица a в некотором базисе B.

Определение. $\lambda \in K$ называется *собственным числом* a, если $\exists v \in V \setminus \{\mathbf{0}\} \colon a(v) = \lambda v$. При этом такой v называется *собственным вектором* a, принадлежащим λ.

Теорема 1. *K — поле. $a \in \operatorname{End}_K V$, где V конечномерно. Пусть B — базис ${}_KV$, $A \coloneqq [a]_B$, $\lambda \in K$. Тогда равносильны:*

а) λ — с.ч. a.

б) λ — с.ч. A.

в) λ — с.ч. χ_a

Доказательство. Равносильность двух последних пунктов доказывалась ранее.

Докажем равносильность первых двух пунктов. $a(v) = \lambda v \Rightarrow [a]_B[v]_B = \lambda[v]_B \Rightarrow Au = \lambda u$, где u — ненулевой вектор. $\square$

Определение. $a \in \operatorname{End}_K V$, λ — с.ч. a. Множество $L_a(\lambda) \coloneqq \{v \in V \mid a(v) = \lambda v\}$ называется *собственным подпространством*, принадлежащим λ.

Теорема. *$L_a(\lambda)$ — a-инвариантное подпространство в ${}_KV$.*

Доказательство. Пусть $u, v \in L_a(\lambda)$, $c \in K$. Тогда:

- $a(u) = \lambda u$, $a(v) = \lambda v \Rightarrow a(u + v) = \lambda(u + v) \Rightarrow u + v \in L_a(\lambda)$.
- $a(cu) = ca(u) = c\lambda u = \lambda(cu) \Rightarrow L_a(\lambda)$.

Таким образом, $a(L_a(\lambda)) \subset L_a(\lambda)$. $\square$

25 Характеристический многочлен оператор с матрицей в форме Фробениуса. Характеристический многочлен циклического ПсО

Теорема. *K — поле, $({}_K V, a)$ — конечномерное ПсО. Пусть B — базис ${}_K V$, т.ч. $[a]_b$ имеет вид $\begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_t \end{pmatrix}$, где A_i — сопровождающая матрица $h_i = p_i^{l_i}$ (p_i — неприводимый унитальный многочлен). Тогда $\chi_a = (-1)^n \prod_{i=1}^t p_i^{l_i}$, где $n = \dim {}_K V$.*

Доказательство. Так как $A \coloneqq [a]_B$ — по определению блочно-диагональная матрица, то $\chi_a = \prod_{i=1}^t \chi_{A_i}$. Таким образом, достаточно рассмотреть случай одной клетки, то есть циклического ПсО $({}_K V, a)$.

A будет иметь следующий вид:

$$\begin{pmatrix} 0 & & & -\alpha_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -\alpha_{r-2} \\ & & 1 & -\alpha_{r-1} \end{pmatrix}, \quad h \coloneqq p^l = \sum_{i=0}^{r} \alpha_i x^i,\ \alpha_r = 1$$

Тогда характеристический многочлен a будет иметь вид:

$$\chi_a = \chi_A = \begin{vmatrix} -x & & & -\alpha_0 \\ 1 & \ddots & & \vdots \\ & \ddots & -x & -\alpha_{r-2} \\ & & 1 & -\alpha_{r-1} - x \end{vmatrix}$$

Применяя последовательно $1 + x^{i-1} i \longmapsto 1$ для i от 2 до r, получаем:

$$\chi_a = \chi_A = \begin{vmatrix} 0 & & & & -h \\ 1 & -x & & & \vdots \\ & \ddots & \ddots & & \vdots \\ & & \ddots & -x & \vdots \\ & & & 1 & \vdots \end{vmatrix} = (-1)^{r+1} \cdot (-h) \cdot \underbrace{1}_{\text{минор верхнетреуг.}} = (-1)^r h$$

□

Следствие. *$({}_K V, a)$ — циклическое ПсО. Пусть μ_a — минимальный многочлен a. Тогда $\chi_a = (-1)^n \mu_a$, где $n = \dim {}_K V$.*

Доказательство. Следует из доказательства теоремы о первой форме Фробениуса, т.к. p^l — это и есть μ_a. □

26 Теорема Гамильтона-Кэли для операторов и матриц

Теорема. *K — поле, $({}_KV, a)$ — конечномерное ПсО. Пусть χ_a — характеристический мн-н a, тогда $\chi_a(a) = 0$.*

Доказательство. Так как $({}_KV, a)$ конечномерно, то $\Psi(V, a)$ — конечномерный периодический $K[x]$-модуль. По структурной теореме для конечнопорожденных периодических модулей имеем $\Psi(V, a) = \bigoplus_{i=1}^t N_i$, где N_i — циклические периодические подмодули.

Тогда $V = \bigoplus_{i=1}^t U_i$, где $U_i = \Phi(N_i) \leq V$ — циклические a-инвариантные подпространства.

Рассмотрим $a_i \in \operatorname{End}_K U_i$ — сужение a на U_i. Имеем $\chi_a = \prod_{i=1}^t \chi_{a_i}$, где $\chi_{a_i} = \pm\mu_{a_i}$ — соответствующие минимальные многочлены. Для любого $v \in U_i$ имеем $\chi_a(a_i)(v) = 0$, откуда $\forall v \in U_i$ $\chi_a(a)(v) = 0$. При этом любой $m \in V$ представим в виде $m = \sum_{i=1}^t u_i$, где $u_i \in U_i$.

Имеем $\chi_a(a)(m) = \sum_{i=1}^t \chi_a(a)(u_i)$, но $\forall i$ $\chi_a(a)(u_i) = 0$, откуда $\chi_a(a) = 0$. □

Следствие 1. *K — поле. Пусть A — квадратная матрица над K размера $n \times n$. Тогда $\chi_A(A) = \mathbf{0}$.*

Доказательство. Рассмотрим $a\colon K^n \to K^n$, т.ч. $a(x) = Ax$. Пусть $\chi_a = \chi_A = \sum_{i=0}^n c_i x^i$, $\mathbf{e}$ — стандартный базис K^n. Имеем $\chi_a(a) = 0$, откуда $\left[\sum_{i=0}^n c_i a^i\right]_{\mathbf{e}} = \mathbf{0} \Rightarrow \sum_{i=0}^n c_i [a]_{\mathbf{e}}^i = \sum_{i=0}^n c_i A^i = \chi_A(A) = \mathbf{0}$ □

Следствие 2. *Пусть $a \in \operatorname{End}_K V$. Тогда $\mu_a \mid \chi_a$.*

Доказательство. По теореме $\chi_a(a) = 0$, откуда $a \in (0 : \Psi(V, a)) = {}_{K[x]}\langle \mu_a \rangle$. Очевидно, $\mu_a \mid \chi_a(a)$. □

27 «Сильная» теорема о ЖНФ

Теорема. *K — поле, $({}_KV, a)$ — конечномерное ПсО. Пусть χ_a раскладывается в $K[x]$ на линейные множители, тогда существует B — базис ${}_KV$, в котором $[a]_B$ имеет вид ЖНФ (см. ранее).*

Доказательство. Известно, что существует базис B такой, что

$$[a]_B = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_t \end{pmatrix},$$

где A_i имеет вид

$$A_i = \begin{pmatrix} \boxed{D_i} & & & \\ 1 & \boxed{D_i} & & \\ & \ddots & \ddots & \\ & & 1 & \boxed{D_i} \end{pmatrix},$$

где D_i — сопровождающая матрица неприводимого унитального многочлена p_i.

При этом (по теореме о характеристическом многочлене оператора с матрицей в форме Фробениуса) $p_i \mid \chi_a$. По условию χ_a раскладывается в произведение неприводимых линейных многочленов, откуда следует, что все p_i линейны, а все D_i — это матрицы, состоящие из одного элемента. Следовательно, все A_i являются жордановыми клетками. $\square$