Алгебра и теория чисел

Курс Жукова И.Б.

Осень 2022 г.

Оглавление

Глава 1

Алгебра линейных операторов

07.09.22

Определение 1.1 (Алгебра). V — линейное пространство над полем K. Линейный оператор на V — линейное отображение $V \to V$ (эндоморфизм линейного пространства V).

Определение 1.2. $\operatorname{End} V = \operatorname{Hom}(V, V)$ — множество линейных операторов.

$$\mathcal{A} \in \operatorname{Hom}(V, W) \quad [\mathcal{A}]_{E,F}$$

Имея два пространства V и W, базисы E и F можно выбрать так, что матрица получится окаймленной единичной.

Теперь же мы имеем одно пространство, соответственно, и один базис и все еще хотим, чтобы матрица была наиболее простой.

Определение 1.3. Говорят, что задана алгебра над полем K, если задано множество A, бинарные операции $+$, $\times$ на нем и отбражение $K \cdot A \to A$, т.ч.:

1. $(A, +, \times)$ - кольцо
2. $(A, +, \cdot)$ - линейное пространство над полем K
3. $\forall \alpha \in K\ \forall a, b \in A : \alpha \cdot (a \times b) = (\alpha \cdot a) \times b = a \times (\alpha \cdot b)$

Пример 1.1. $A = M_n(K)$, $A_0 = \{\alpha E_n | \alpha \in K\}$ — подкольцо скалярных матриц, изоморфное полю K.

Пример 1.2. $A = K[x]$

Пример 1.3. Любая ситуация, где поле $K \subset R$ (R — кольцо) $\implies$ R — K-алгебра.

В обратную сторону тоже верно, если алгебра содержит единицу. Тогда там найдется подкольцо, которое можно отожествить с полем K.

Любая ситуация, где поле $K \subset R$ (R – кольцо) $\implies$ R – K-алгебра. В обратную сторону тоже верно, если алгебра содержит единицу. Тогда там найдется подкольцо, которое можно отожествить с полем .

Почему алгебра с единицей:

Пусть A — алгебра с $1 (\neq 0)$ над полем K. Рассмотрим множество $A_0 = \{\alpha \cdot 1 | \alpha \in K\}$.

$$K \xrightarrow{\varphi} A_0 \quad \alpha \mapsto \alpha_1$$

Идеал в поле либо нулевой, либо все поле. $\varphi(1) \neq 0 \Rightarrow Ker(\varphi) \neq K$. Значит, φ — изоморфизм. A_0 — подкольцо, изоморфное полю K.

Линейные операторы тоже образуют алгебру. Заметим, что в $\mathrm{End}\ V$ есть сложение и композиция операторов, а также умножение на скаляр. $(\mathrm{End}\ V, +)$ — абелева группа. Проверка дистрибутивности операторов:

$$\mathcal{A} \circ (\mathcal{B}_1 + \mathcal{B}_2) = \mathcal{A} \circ \mathcal{B}_1 + \mathcal{A} \circ \mathcal{B}_2$$
$$(\mathcal{A}_1 + \mathcal{A}_2) \circ \mathcal{B} = \mathcal{A}_1 \circ \mathcal{B} + \mathcal{A}_2 \circ \mathcal{B}$$

$(\mathrm{End}\ V, +, \circ)$ — линейное пространство над полем K. Наконец, $(\alpha \cdot \mathcal{A}) \circ \mathcal{B} = \mathcal{A} \circ (\alpha \cdot \mathcal{B}) = \alpha \cdot (\mathcal{A} \circ \mathcal{B})$.

Таким образом, $(\mathrm{End}\ V, +, \circ, \cdot)$ — алгебра над полем K.

Предложение 1.1. Пусть $\dim V = n$. E — базис V. Тогда отображение $\lambda_E : \mathrm{End}\, V \to M_n(K)$, $\mathcal{A} \mapsto [\mathcal{A}]_E$ — изоморфизм алгебр над полем K (т.е. биекция, сохраняющая все операции).

Доказательство. Знаем: λ_E — изоморфизм линейных пространств. $\lambda_E(\mathcal{B} \circ \mathcal{A}) = [\mathcal{B}\mathcal{A}]_E = [\mathcal{B}]_E \cdot [\mathcal{A}]_E = \lambda_E(\mathcal{B})\lambda_E(\mathcal{A})$. ■

Следствие 1.1.1. $\dim \mathrm{End}\ V = (\dim\ V)^2$

lil friendly reminder: $U_E \xrightarrow{\mathcal{A}} V_F \xrightarrow{\mathcal{B}} W_G$, $[\mathcal{B}\mathcal{A}]_{EG} = [\mathcal{B}]_{FG}[\mathcal{A}]_{EF}$ - стандартный случай.

$\mathcal{A} : U_{EE'} \to V_{FF'}$. Как связаны матрицы этого линейного отображения в двух базисах? $[\mathcal{A}]_{EF} = A$ - знаем, $[\mathcal{A}]_{E'F'} = ?$ Нужны матрицы перехода: $M_{E \to E'} = C$, $M_{F \to F'} = D$. Можем записать: $E' = EC$, $E = (e_1, \dots, e_n)$, $C = c_{ij}$ (E - вектор, C - квадратная матрица). Тогда $EC = (c_{11}e_1 + \dots + c_{m1}e_n, c_{12}e_1 + \dots + c_{n2}e_n, \dots)$. Что происходит с матрицей при такой замене базиса?

Предложение 1.2. Пусть $\mathcal{A} \in \mathrm{End}\, V, E$ и E' — базисы, $[\mathcal{A}]_E = A$, $M_{E \to E'} = C$, тогда $[\mathcal{A}]_{E'} = C^{-1}AC$.

Доказательство.

$$\begin{tikzcd}
U_E \arrow[r, "\mathcal{A}"] & V_F \arrow[d, "\varepsilon_V = id_V"] \\
U_{E'} \arrow[u, "\varepsilon_U"] & V_{F'} \arrow[l, "\mathcal{A}"]
\end{tikzcd}$$

$$[\mathcal{A}]_{E'F'} = \underbrace{[\varepsilon_V]_{FF'}}_{D^{-1}} \underbrace{[\mathcal{A}]_{EF}}_{A} \underbrace{[\varepsilon_U]_{E'E}}_{C}$$

В нашем случае $(U = V, E = F, E' = F')$. ■

Определение 1.4 (Алгебра)**.** Пусть A' эквивалентно A, если $\exists C \in \mathrm{GL}_n(K)$: $A' = C^{-1}AC$. Проверка симметричности и транзитивности:

$$A = (C^{-1})^{-1}A'C^{-1}$$
$$A'' = D^{-1}A'D = D^{-1}C^{-1}A'CD = (DC)^{-1}A'(CD)$$

Глава 2

Инвариантные подпространства

Определение 2.1. V — линейное конечномерное пространство, $A \in \text{End }\ V$. Пусть $W \subset \ V$ — линейное подпространство. W — называется инвариантным относительно A, если $\forall w \in W$: $\mathcal{A}(w) \in W$.

Свойства.

1. $0, W$ — $\mathcal{A}$-инвариантны
2. $\operatorname{Ker} \mathcal{A}$ — $\mathcal{A}$-инвариантно
3. $\operatorname{Im} \mathcal{A}$ — $\mathcal{A}$-инвариантен

Пусть W — $\mathcal{A}$-инвариант. Следовательно, $A|_W$ можно рассматривать как элемент End W. Более формально, $\exists\ \mathcal{A}_1 \in \text{End }\ W\ \forall w \in W$: $\mathcal{A}_1 w = \mathcal{A} w$

$$W \xrightarrow{\mathcal{A}} W \quad w \mapsto \mathcal{A} w$$

$\mathcal{A}_1$ — оператор индуцированный оператором $\mathcal{A}$ на инвариантном подпространстве W.

$W \subset V,\ V/W = \{v + w | v \in V\}$ — фактор-пространство. W — $\mathcal{A}$-инвариант. Определим $\mathcal{A}_2$.

$$\mathcal{A}_2 : V/W \to V/W \quad v + W \mapsto \mathcal{A}v + W$$

Проверка корректности: пусть $v_1 + W = v_2 + W$, нужно проверить, что $\mathcal{A}v_1 + W = \mathcal{A}v_2 + W$. Так, $\mathcal{A}v_2 = \mathcal{A}(v_1 + (v_2 - v_1)) = \mathcal{A}v_1 + \mathcal{A}\underbrace{(v_2 - v_1)}_{\in W} \Rightarrow \mathcal{A}v_2 + W = \mathcal{A}v_1 + W$.

Предложение 2.1. $\mathcal{A}_2 \in \mathrm{End}\ V/W$

Доказательство. Проверка линейности:

$$\mathcal{A}_2((v_1 + W) + (v_2 + W)) = \mathcal{A}_2((v_1 + v_2) + W) = \\ \mathcal{A}(v_1 + v_2) + W = \mathcal{A}v_1 + \mathcal{A}v_2 + W = \\ (\mathcal{A}v_1 + W) + (\mathcal{A}v_2 + W)$$

$$\mathcal{A}_2(\alpha(v + w)) = \mathcal{A}_2(\alpha v + W) = \\ \mathcal{A}(\alpha v) + W = \alpha\mathcal{A}v + W = \\ \alpha(\mathcal{A}v + W) = \alpha\mathcal{A}_2(v + W)$$

■

$\mathcal{A}_2$ — индуцированный оператор на фактор-пространстве.

Предложение 2.2. Пусть $\mathcal{A} \in \mathrm{End}\ V, W \subset V, e_1, \dots, e_m$ — базис W, $e_{m+1}, \dots, e_n$ — дополнение до базиса V. Тогда эквивалентны 2 утверждения:

1. W — $\mathcal{A}$-инвариант
2. $[\mathcal{A}]_{e_1,\dots,e_n} = \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right)$, $A_1 \in M_m(K)$

При этом $A_1 = [\mathcal{A}_1]_{e_1,\dots,e_m}$, $A_2 = [\mathcal{A}_2]_{e_{m+1}+W,\dots,e_n+W}$, где $\mathcal{A}_1$ и $\mathcal{A}_2$ — соответствующие индуцированные операторы.

Доказательство. $1 \Rightarrow 2$: векторы $e_1, \dots, e_n \in W \Rightarrow \mathcal{A}e_1, \dots, \mathcal{A}e_m \in W = \mathrm{Lin}(e_1, \dots, e_m) \Rightarrow [\mathcal{A}]_{e_1,\dots,e_n} = \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right)$
Очевидно, $[\mathcal{A}_1]_{e_1,\dots e_m} = A_1$.

Пусть $[\mathcal{A}]_{e_1,\dots,e_n} = (a_{ij})$.
$\mathcal{A}e_j = \underbrace{a_{1j}e_1 + \dots + a_{mj}e_m}_{\in W} + a_{m+1j}e_{m+1} + \dots + a_{nj}e_n$, $j \geqslant m+1$

$\underbrace{\mathcal{A}e_j + W}_{=\mathcal{A}_2(e_j+W)} = \underbrace{a_{m+1j}e_{m+1} + \dots + a_{nj}e_n + W}_{=a_{m+1j}(e_{m+1}+W)+\dots+a_{nj}(e_n+W)}$ (первые m элементов станут нулевым классом). Таким образом, $[\mathcal{A}_2]_{e_{m+1}+W,\dots,e_n+W} = \begin{pmatrix} a_{m+1m+1} & \dots & a_{m+1n} \\ \vdots & \ddots & \vdots \\ a_{nm+1} & \dots & a_{nn} \end{pmatrix} = A_2$

$2 \Rightarrow 1$: $[\mathcal{A}_1]_{e_1,\dots,e_n} = \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right) \Rightarrow \mathcal{A}e_1, \dots, \mathcal{A}e_m \in \operatorname{Lin}(e_1, \dots, e_m) \in W$. Пусть $w \in W \Rightarrow w = \beta_1 e_1 + \dots + \beta_m e_m \Rightarrow \mathcal{A}w = \beta_1 \underbrace{\mathcal{A}_1 e_1}_{\in W} + \dots + \beta_m \underbrace{\mathcal{A}_m e_m}_{\in W} \in W$. ■

14.09.22

Итак, мы выяснили, что если в нашем подпространсве V есть инвариантное подпространство меньшей размерности (ненулевое) $W \subset V$, то это позволяет нам составить блочно-треугольную матрицу $\left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right)$, где A_1, A_2 – квадратные матрицы, $A_1 \in M_m(K)$, $m = \dim W$.

В ситуации $V = W_1 \bigoplus W_2$ можно получить $\left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right)$.

Предложение 2.3. Пусть $\mathcal{A} \in \operatorname{End} V$, $V = W_1 \bigoplus W_2$, $\underbrace{e_1, \dots, e_m}_{E_1}$ — базис W_1, $\underbrace{e_{m+1}, \dots, e_n}_{E_2}$ — базис W_2, $E = E_1 + E_2$. Тогда эквивалентны 2 утверждения:

1. $W_1, W_2 - \mathcal{A}$-инвариантны
2. $[\mathcal{A}]_E = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right)$, $A_1 \in M_m(K)$, $A_2 \in M_{n-m}(K)$. При этом $A_1 = [\mathcal{A}|_{W_1}]_{E_1}$, $A_2 = [\mathcal{A}|_{W_2}]_{E_2}$

Доказательство. Аналогично предыдущему предложению.
$1 \Rightarrow 2$: $\mathcal{A}e_1, \dots, \mathcal{A}e_m \in W_1 \Rightarrow \left(\begin{array}{c|c} A_1 & \\ \hline 0 & \end{array}\right)$, $\mathcal{A}e_{m+1}, \dots, \mathcal{A}e_n \in W_2 \Rightarrow \left(\begin{array}{c|c} & 0 \\ \hline & A_2 \end{array}\right)$.

$2 \Rightarrow 1$: $\left(\begin{array}{c|c} & \\ \hline 0 & \end{array}\right) \Rightarrow \mathcal{A}e_1, \dots, \mathcal{A}e_m \in \mathrm{Lin}(e_1, \dots, e_m) = W_1 \Rightarrow \forall w \in W_1,\ \mathcal{A}w \in W_1,\ W_1$ — $\mathcal{A}$-инвариант.
$\left(\begin{array}{c|c} & 0 \\ \hline & \end{array}\right) \Rightarrow \mathcal{A}e_{m+1}, \dots, \mathcal{A}e_n \in \mathrm{Lin}(e_{m+1}, \dots, e_n) = W_2 \Rightarrow \forall w \in W_2,\ \mathcal{A}w \in W_2,\ W_2$ — $\mathcal{A}$-инвариант. ■

Что означает в терминах оператора, что матрица получилась диагональной? Например, образ первого базисного вектора будет прямо пропорционален первому базисному вектору: $\mathcal{A}e_1 = \lambda_1 e_1,\ \mathcal{A}e_2 = \lambda_2 e_2$ и т.д.

Глава 3

Собственные значения и собственные векторы

Пусть $\mathcal{A} \in \operatorname{End} V$. Скаляр $\lambda \in K$ называется собственным значением оператора $\mathcal{A}$, если $\exists v \in V,\ v \neq 0 : \mathcal{A}v = \lambda v$. Можно написать иначе: $\mathcal{A}v = \lambda v \Leftrightarrow \mathcal{A}v - (\lambda\varepsilon)v = 0 \Leftrightarrow (\mathcal{A} - \lambda\varepsilon)v = 0 \Leftrightarrow v \in \operatorname{Ker}(\mathcal{A} - \lambda\varepsilon)$, $\varepsilon = \mathrm{id}$.

Определение 3.1. Таким образом, λ — собственное значение $\mathcal{A} \Leftrightarrow \operatorname{Ker}(\mathcal{A} - \lambda\varepsilon) \neq 0$. Если K — числовое поле, то «собственное число $=$ собственное значение».

Определение 3.2. Пусть $v \in V$, λ — собственное значение $\mathcal{A}$. Говорят, что v — собственный вектор $\mathcal{A}$, принадлежащий собственному значению λ, если $v \neq 0$ и $\mathcal{A}v = \lambda v$, т.е. $v \in \operatorname{Ker}(\mathcal{A} - \lambda\varepsilon) \setminus \{0\}$.

Определение 3.3. $V_\lambda = \operatorname{Ker}(\mathcal{A} - \lambda\varepsilon)$ — собственное подпространство, принадлежащее собственному значению λ.

Определение 3.4. $\mathcal{A} \in \operatorname{End} V$ называется диагонализируемым, если в V существует базис E, такой что $[\mathcal{A}]_E$ диагональна.

Предложение 3.1. Пусть $\mathcal{A} \in \operatorname{End} V$. Тогда: $\mathcal{A}$ диагонализируем $\Leftrightarrow$ в V существует базис из собственных векторов $\mathcal{A}$.

Доказательство.

$$[\mathcal{A}]_E = diag(\lambda_1, \dots, \lambda_n) = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix}$$

$E = (e_1, \dots, e_n),\ \mathcal{A}e_i = \lambda_i e_i,\ i = 1, \dots, n,\ e_i \neq 0$, так как входит в базис $\Rightarrow e_i$ — собственный.
$\Leftarrow$: Пусть $E = (e_1, \dots, e_n)$ — базис из собственных векторов. $\mathcal{A}e_i = \lambda_i e_i$ для некоторых $\lambda_i \in K,\ i = 1, \dots, n \Rightarrow [\mathcal{A}]_E = diag(\lambda_1, \dots, \lambda_n)$. ■

Лемма 3.2. Пусть $\mathcal{A} \in \operatorname{End} V$. Тогда: 0 — собственное значение $\mathcal{A} \Leftrightarrow \mathcal{A} \notin \mathrm{GL}(V)$.

Доказательство. 0 — собственное значение оператора $\mathcal{A} \Leftrightarrow \operatorname{Ker}(\mathcal{A} - 0\varepsilon) \neq 0 \Leftrightarrow \operatorname{Ker} \mathcal{A} \neq 0 \Leftrightarrow \mathcal{A} \notin \mathrm{GL}(V)$. ■

Определение 3.5. Пусть λ — собственное значение $\mathcal{A}$. Его геометрической кратностью называется $g_\lambda = \dim \operatorname{Ker}(\mathcal{A} - \lambda\varepsilon),\ \lambda \leqslant g_\lambda \leqslant n = \dim V$.

Предложение 3.3. Пусть $\lambda_1, \dots, \lambda_k$, где k — конечное число, — различные собственные значения $\mathcal{A}$. $v_1, \dots, v_k$ — принадлежащие им собственные векторы. Тогда $v_1, \dots, v_k$ — ЛНЗ.

Доказательство. Индукция по k.
База: $k = 1$. По определению $v_1 \neq 0 \Rightarrow v_1$ — ЛНЗ.
Переход: $k - 1 \to k$. Пусть $v_1, \dots, v_k$ — собственные векторы, принадлежащие $\lambda_1, \dots, \lambda_k$. Предположим, $\alpha_1 v_1 + \dots + \alpha_k v_k = 0 (*)$. $\mathcal{A}(\lambda_1 v_1 + \dots + \lambda_k v_k) = \alpha_1 \lambda_1 v_1 + \dots + \alpha_k \lambda_k v_k = 0$. Домножим $(*)$ на λ_k: $\alpha_1 \lambda_k v_1 + \dots + \alpha_k \lambda_k v_k = 0$. Вычтем: $\alpha_1(\lambda_1 - \lambda_k)v_1 + \dots + \alpha_{k-1}(\lambda_{k-1} - \lambda_k)v_{k-1} = 0$
По индукционному предположению: $v_1, \dots, v_{k-1}$ — ЛНС $\Rightarrow$

$\alpha_1 \underbrace{(\lambda_1 - \lambda_k)}_{\neq 0} = ... = \alpha_{k-1} \underbrace{(\lambda_{k-1} - \lambda_k)}_{\neq 0} = 0 \Rightarrow \alpha_1 = ... = \alpha_{k-1} = 0 \Rightarrow$
$\alpha_k v_k = 0$ ($v_k \neq 0$, т.к. собственный вектор) $\Rightarrow \alpha_k = 0 \Rightarrow v_1, ..., v_k$ — ЛНЗ. ■

Следствие 3.3.1. Пусть $\lambda_1, ..., \lambda_k$ — различные собственные значения $\mathcal{A}$. Тогда $V_{\lambda_1} + ... + V_{\lambda_k} = V_{\lambda_1} \oplus ... \oplus V_{\lambda_k}$.

Доказательство. Нужно доказать: если $v_1 + ... + v_k = v'_1 + ... + v'_k$ (где $v_1,\ v'_1 \in V_{\lambda_i}, i = 1, ..., k$). Таким образом, $v_1 = v'_1, ..., v_k = v'_k$.

$$(v_1 - v'_1) + ... + (v_k - v'_k) = 0 \qquad (**)$$

Предположим, $\exists i : v_i \neq v'_i$. Тогда в $(**)$ есть ненулевое слагаемое: $v_i - v'_i \in V_{\lambda_i}$. Оставим в $(**)$ только ненулевые слагаемые, получится, что сумма собственных векторов из разных собственных подпространств будет равна нулю - противоречие с линейной независимостью. ■

Следствие 3.3.2. Пусть $\dim V = n,\ \mathcal{A} \in \operatorname{End} V$. Тогда у $\mathcal{A}$ есть $\leqslant n$ собственных значений (для каждого собственного значению по собственному вектору, прямо следует из предложения).

Следствие 3.3.3. Пусть $\lambda_1, ..., \lambda_m$ — все собственные значение $\mathcal{A}$. Тогда $g_{\lambda_1} + ... + g_{\lambda_m} \leqslant n = \dim V$.

Доказательство. $V_{\lambda_1} + ... + V_{\lambda_m} < V \Rightarrow \dim(\underbrace{V_{\lambda_1} + ... + V_{\lambda_k}}_{g_{\lambda_1} + ... + g_{\lambda_m}}) \leq n$

(по следствию 3.3.1). ■

Предложение 3.4. Критерий диагонализируемости оператора в терминах геометрических кратностей.
Пусть $\mathcal{A} \in \operatorname{End} V,\ \lambda_1, ..., \lambda_m$ — все его собственные значения, $\dim V = n$. Тогда $\mathcal{A}$ диагонализируем $\Leftrightarrow g_{\lambda_1} + ... + g_{\lambda_m} = n$.

Доказательство. $\Rightarrow$: найдется базис E, такой что: $[\mathcal{A}]_E =$

$diag(\underbrace{\lambda_1, \dots, \lambda_1}_{c_1}, \underbrace{\lambda_2, \dots, \lambda_2}_{c_2}, \dots, \underbrace{\lambda_m, \dots, \lambda_m}_{c_m})$, $c_1, \dots, c_m \geq 0$. Первые c_1 векторов — собственные, принадлежащие собственным значениям λ_1. Они ЛНЗ, так как являются часть базиса $\Rightarrow c_1 \leq g_{\lambda_1}$. Аналогично, $c_i \leq g_{\lambda_i},\ m \leq i \leq 2$. $n = c_1 + \dots + c_m \leq g_{\lambda_1} + \dots + g_{\lambda_m} = n \Rightarrow g_{\lambda_1} + \dots + g_{\lambda_m} = n$
$\Leftarrow$: $\dim(V_{\lambda_1} + \dots + V_{\lambda_m}) = g_{\lambda_1} + \dots + g_{\lambda_m} = n \Rightarrow V = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_m}$. E_1 — любой базис V_{λ_1}, ..., E_m — любой базис V_{λ_m}. E — диагонализирующий базис для $\mathcal{A}$. ■

Замечание. При этом получили, если

$$[\mathcal{A}]_E = diag(\underbrace{\lambda_1, \dots, \lambda_1}_{c_1}, \underbrace{\lambda_2, \dots, \lambda_2}_{c_2}, \dots, \underbrace{\lambda_m, \dots, \lambda_m}_{c_m}),$$

то $c_1 = g_{\lambda_1}, \dots, c_m = g_{\lambda_m}$.

Глава 4

Характеристический многочлен оператора

$\mathcal{A} \in \operatorname{End} V$, $[\mathcal{A}]_E = A$. Задача: найти собственное значение $\mathcal{A}$. λ – собственое значение $\mathcal{A} \Leftrightarrow \operatorname{Ker}(\mathcal{A} - \lambda\varepsilon) \neq 0 \Leftrightarrow \underbrace{[\mathcal{A} - \lambda\varepsilon]_E}_{=A-\lambda E_n} \notin \mathrm{GL}_n(K) \Leftrightarrow$ $|\mathcal{A} - \lambda\varepsilon| = 0$. Задача сводится к нахождению таких λ, при которых определитель матрицы равен нулю.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

$$A - \lambda E_n| = \begin{pmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \ddots & \ddots & \vdots & a_{1n} \\ a_{n1} - \lambda & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Например, $\begin{pmatrix} a_{11} - \lambda & a_{12} \\ a_{21} & a_{22} - \lambda \end{pmatrix} = (a_{11} - \lambda)(a_{22} - \lambda) - a_{12}a_{21} = \lambda^2 - \lambda(a_{11} + a_{22}) + a_{11}a_{22} - a_{12}a_{21}$.

Определитель обращается в ноль, когда λ является корнем этого многочлена.

Определение 4.1. Пусть $A \in M_n(K)$. Есть характеристический многочлен называется $\chi_A = \underbrace{|A - X \cdot E_n|}_{\in M_n(K[x]) \subset M_n(K(x))} \in K[x]$.
$\begin{vmatrix} \ddots & \\ & \ddots \end{vmatrix} = (a_{11} - x)(a_{22} - x) \dots (a_{nn} - x) + G = (-1)^{n-1} x^n + (-1)^{n-1} \underbrace{(a_{11} + \dots + a_{nn})}_{\operatorname{Tr} A} x^{n-1} + \dots + |A|$, где $A = (a_{ij}),\ \deg G \leq n - 2,\ \operatorname{Tr} A$ - след матрицы.

Определение 4.2. Пусть $\mathcal{A} \in \operatorname{End} V$. Его характеристическим многочленом $\chi_{\mathcal{A}}$ называется $\chi_{[\mathcal{A}]_E}$, где E — любой базис V.

Проверка корректности независимости выбора базиса: пусть $A = [\mathcal{A}]_E,\ A_1 = [\mathcal{A}]_{E_1},\ C = M_{E \to E_1}$. Нужно: $\chi_{\mathcal{A}} = \chi_{\mathcal{A}_1}$.

$$A_1 = C^{-1} A C$$

$$\begin{aligned} &\chi_{\mathcal{A}_1} = |A_1 - XE_n| = |C^{-1}AC - XC^{-1}C| = \\ &= |C^{-1}AC - C^{-1}XE_nC| = |C^{-1}(A - XE_n)C| = \underbrace{|C^{-1}}_{|C|^{-1}}|A - XE_n||C| = \\ &\qquad = |A - XE_n| = \chi_{\mathcal{A}} \end{aligned}$$

У эквивалентных матриц след одинаков. 21.09.22

Определение 4.3. Кратность корня λ у многочлена $\chi_{\mathcal{A}}$ называется алгебраической кратностью собственного значения λ (обозначается a_λ).

Предложение 4.1. Пусть $\mathcal{A} \in \operatorname{End} V$

1. Пусть $W|_{\mathcal{A}}$ – инвариантное подпространство V, $\mathcal{A}_1 = \mathcal{A}|_w \in W$. Тогда $\chi_{\mathcal{A}_1} | \chi_{\mathcal{A}}$.
2. Пусть $V = W_1 \bigoplus W_2$; $W_1,\ W_2$ – $\mathcal{A}$-инвариант. $\mathcal{A}_1 = \mathcal{A}|_{W_1},\ \mathcal{A}_2 = \mathcal{A}|_{W_2} \Rightarrow \chi_{\mathcal{A}} = \chi_{\mathcal{A}_1}\chi_{\mathcal{A}_2}$.

Доказательство. 1: E – базис V, начальная часть которого – базис W.

$[\mathcal{A}]_E = \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right),\ A_1 = [\mathcal{A}_1]_{E_1},\ E_1$ – начальная часть E.
$\chi_{\mathcal{A}} = |\left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right) - XE_m| = |\left(\begin{array}{c|c} A_1 - XE_m & B \\ \hline 0 & A_2 - XE_{n-m} \end{array}\right)| =$
$|A_1 - XE_m||A_2 - XE_{n-m}| = \underbrace{\chi_{A_1}}_{=\chi_{\mathcal{A}_1}} \chi_{A_2}$.
2: аналогично, $[\mathcal{A}]_E = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right) : A_1 = [\mathcal{A}_1]_{E_1},\ A_2 = [\mathcal{A}_2]_{E_2} \Rightarrow$
$\chi_{\mathcal{A}} = \chi_{A_1}\chi_{A_2} = \chi_{\mathcal{A}_1}\chi_{\mathcal{A}_2}$. ■

Следствие 4.1.1. Допустим, λ – собственное значение $\mathcal{A}$, тогда $g_\lambda \le a_\lambda$.

Доказательство. Применим предложение к $W = V_\lambda$. Очевидно, W – $\mathcal{A}$-инвариантно $\Rightarrow \chi_{\mathcal{A}|_{V_\lambda}} | \chi_{\mathcal{A}}$.
В любом базисе $[\mathcal{A}|_{V_\lambda}] = diag(\underbrace{\lambda, \lambda, \dots, \lambda}_{g_\lambda}) \Rightarrow \chi_{\mathcal{A}|_{V_\lambda}} =$
$|diag(\underbrace{\lambda - x, \dots, \lambda - x}_{g_\lambda})| = (\lambda - x)^{g_\lambda} \Rightarrow (\lambda - x)^{g_\lambda} | \chi_{\mathcal{A}} \Rightarrow a_\lambda \ge g_\lambda$. ■

Теорема 4.2. Пусть $\mathcal{A} \in \operatorname{End} V$. Тогда эквивалентны 2 условия:

1. $\mathcal{A}$ – диагонализируем.
2. $\chi_{\mathcal{A}}$ – раскладывается на линейные множители, и для любого собственного значения λ выполнено $g_\lambda = a_\lambda$.

Доказательство. 1 $\Rightarrow$ 2: существует базис E, такой что $A = [\mathcal{A}]_E = diag(\underbrace{\lambda_1, \dots, \lambda_1}_{g_{\lambda_1}}, \underbrace{\lambda_2, \dots, \lambda_2}_{g_{\lambda_2}}, \dots, \underbrace{\lambda_k, \dots, \lambda_k}_{g_{\lambda_m}})$, где $\lambda_1, \dots, \lambda_k$ – различные собственные значения. $\chi_{\mathcal{A}} = (\lambda_1 - x)^{g_{\lambda_1}} \dots (\lambda_k - x)^{g_{\lambda_k}}$ – раскладывается на линейные множители (кратность – степень). $g_{\lambda_i} = a_{\lambda_i}$.
2 $\Rightarrow$ 1: $\chi_{\mathcal{A}}$ раскладывается на линейные множители $\Rightarrow \chi_{\mathcal{A}} = \pm(x - \lambda_1)^{a_{\lambda_1}} \dots (x - \lambda_k)^{a_{\lambda_k}},\ g_{\lambda_i} = a_{\lambda_i} \Rightarrow g_{\lambda_1} + \dots + g_{\lambda_k} = a_{\lambda_1} + \dots + a_{\lambda_k} = n \Rightarrow \chi$ – диагонализируем. ■

Теорема указывает на два обстоятельства, которые мешают оператору быть диагонализируемым: многочлен может не раскладываться на линейные множители (т.е. не только не быть диагонализируемым, но и не иметь собственных значений), геометрическая и алгебраическиая кратности могут не совпадать.

Пример 4.1. 1. $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\chi_{\mathcal{A}} = \begin{vmatrix} -x & -1 \\ 1 & -x \end{vmatrix} = x^2 + 1$ $(K = \mathbb{R})$.

2. $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $\chi_{\mathcal{A}} = \begin{vmatrix} -x & 0 \\ 1 & -x \end{vmatrix} = x^2$, единственное собственное значение – 0, $a_0 = 2$ и $g_0 = 1$.

Глава 5

Многочлены от операторов

Пусть $\mathcal{A} \in \operatorname{End} V$ (V над K), $f \in K[x]$. $f = \alpha_n x^n + ... + \alpha_1 x + \alpha_0$. $f(\mathcal{A}) = \alpha_n \mathcal{A}^n + \alpha_{n-1}\mathcal{A}^{n-1} + ... + \alpha_1 \mathcal{A} + \alpha_0 \varepsilon_V \in \operatorname{End} V$.

Предложение 5.1. $f, g \in K[x]$

1. $(f+g)(\mathcal{A}) = f(\mathcal{A}) + g(\mathcal{A})$.
2. $(fg)(\mathcal{A}) = f(\mathcal{A})g(\mathcal{A}) = g(\mathcal{A})f(\mathcal{A}) = gf(\mathcal{A})$.

Доказательство. Непосредственная проверка. ■

Следствие 5.1.1. Пусть $\mathcal{A} \in \operatorname{End} V$, $f \in K[x]$, тогда $\operatorname{Ker} f(\mathcal{A}), \operatorname{Im} f(\mathcal{A})$ – $\mathcal{A}$-инвариантные подпространства.

Доказательство. $v = \operatorname{Ker} f(\mathcal{A})$, т.е. $f(\mathcal{A})(v) = 0$. $f(\mathcal{A})(\mathcal{A}v) = (f(\mathcal{A})\mathcal{A})(v) = (\mathcal{A}f(\mathcal{A}))(v) = \mathcal{A}(v) = 0$. Таком образом, $\mathcal{A}v \in \operatorname{Ker} f(\mathcal{A})$. $\operatorname{Im} f(\mathcal{A})$ – $\mathcal{A}$-инвариантное подпространство. Пусть $v \in \operatorname{Im} f(\mathcal{A}) \Rightarrow \exists w$: $v = f(\mathcal{A})(w)$. $\mathcal{A}v = (\mathcal{A}f(\mathcal{A}))(w) = (f(\mathcal{A})\mathcal{A})(w) = f(\mathcal{A})(\mathcal{A}w) \in \operatorname{Im} f(\mathcal{A})$. ■

R – коммутативное ассоциативное кольцо с 1. Подмножество $I \subset R$ называется идеалом, если

1. I – подгруппа по сложению

2. $\forall a \in I\ \forall r \in \mathbb{R} : ra \in I$.

Пусть $c \subset R$, $(c) = \{cx | x \in K\}$ – идеал в R, главный идеал, порожденный c.

Следствие 5.1.2. В $K[x]$, где K – поле, все идеалы главные.

Доказательство. Пусть $I \subset K[x]$, $I = 0 \Rightarrow I = (0)$. $I \neq 0$, h - многочлен наименьшей степени, входящий в $I \setminus \{0\}$. Докажем: $I = (h)$. $h \in I \Rightarrow (h) \subset I$. Осталось: $I \subset (h)$. $f \in I \Rightarrow f = hq + r$, где $\deg r < \deg h \Rightarrow r = \underbrace{f}_{\in I} - \underbrace{h}_{\in I} q \in I \Rightarrow r = 0 \Rightarrow f = hq \in (h)$. ∎

Замечание. Аналогично доказывается, что любая евклидова область - ОГЦ (область главных идеалов).

Замечание. $\mathbb{Z}[x]$ - не ОГЦ. Например, $I = \{f | f(0) \vdots 2\} \neq (2),\ \neq (x),\ \neq (1)$.

Определение 5.1. Пусть $\mathcal{A} \in \operatorname{End} V : v \in V$. $f \in K[x]$ называется аннулятором v по отношению к оператору $\mathcal{A}$, если $f(\mathcal{A})(v) = 0$.

Лемма 5.2. $I = \{f | f$ – аннулятор $v\}$ – идеал в $K[x]$.

Доказательство. $f, g \in I,\ (f-g)(\mathcal{A})(v) = (f(\mathcal{A}) - g(\mathcal{A}))(v) = f(\mathcal{A})(v) - g(\mathcal{A})(v) = 0$. $f \in I,\ h \in K[x]$.
$(hf)(\mathcal{A})(v) = h(\mathcal{A})(\underbrace{f(\mathcal{A})(v)}_{0}) = 0 \Rightarrow hf \in I$. ∎

Пусть $dimV = n$. $v, \mathcal{A}v, \mathcal{A}^2v, \dots, \mathcal{A}^nv$ - ЛЗС. $f(\mathcal{A})(v) = \alpha_1 v + \dots + \lambda_n \mathcal{A}^n v = 0$, не все $\alpha_i = 0$. $f = \alpha_0 + \alpha_1 x + \dots + \alpha_n x^n \neq 0 \Rightarrow f$ – аннулятор v.

I – главный идеал $\Rightarrow I = (f_0), f_0 \neq 0$. f_0 - минимальный аннулятор v (минимальный аннулирующий многочлен).

$v \in V$, $v \in W$ – инвариант $\Rightarrow \mathcal{A}v \in W \Rightarrow \mathcal{A}^2 v \in W \Rightarrow \dots \Rightarrow \forall \mathcal{A}^k v \in W$.

Определение 5.2. Циклическим подпространством, порожденным V, называется $C_v = Lin(v, \mathcal{A}v, \mathcal{A}^2v, \dots)$.

Предложение 5.3. Пусть f_0 – минимальный аннулятор v, $d = deg f_0$. Тогда C_v – $\mathcal{A}$-инвартное подпространство с базисом $v, \mathcal{A}v, \mathcal{A}^2v, \dots, \mathcal{A}^{d-1}v$.

Доказательство. $w \in C_v \Rightarrow w = \alpha_0 v + \alpha_1 \mathcal{A}v + \dots + \alpha_m \mathcal{A}^m v \Rightarrow \mathcal{A}w = \alpha_0 \mathcal{A}v + \alpha_1 \mathcal{A}^2 v + \dots + \alpha_m \mathcal{A}^{m+1} v \in C_v$.
Предположим, $v, \mathcal{A}v, \mathcal{A}^2v, \dots, \mathcal{A}^{d-1}v$ – ЛЗС. $g(\mathcal{A})(v) = \beta_0 v + \beta_1 \mathcal{A}v + \dots + \beta_{d-1}\mathcal{A}^{d-1} = 0$, не все $\beta = 0$.
$g = \beta_0 + \beta_1 v + \dots + \beta_{d-1} v^{d-1} \neq 0 \Rightarrow g$ – аннулятор $v \Rightarrow g \in (f_0) \Rightarrow f_0 | g \Rightarrow deg g < deg f_0$, пришли к противоречию. Таким образом, $v, \mathcal{A}v, \mathcal{A}^2v, \dots, \mathcal{A}^{d-1}v$ – ЛНС.
Осталось проверить $C_v = \underbrace{Lin(v, \mathcal{A}v, \mathcal{A}^2v, \dots, \mathcal{A}^{d-1}v)}_{W}$.
Докажем индукцией по k: $\mathcal{A}^k v \in W$.
База: $k = 0, 1, \dots, d-1 \Rightarrow \mathcal{A}^k \in W$ по определению.
Переход: $k \geq d$.
По индукционному предположению: $\mathcal{A}^{k-1}v \in W$, т.е. $\mathcal{A}^{k-1}v = \gamma_0 v + \gamma_1 \mathcal{A}v + \dots + \gamma_{d-1}\mathcal{A}v \Rightarrow \mathcal{A}^k v = \underbrace{\gamma_0 \mathcal{A}v + \gamma_1 \mathcal{A}^2 v + \dots + \gamma_{d-2}\mathcal{A}^{d-1}v}_{W} + \gamma_{d-1}\mathcal{A}^d v$.
$\mathcal{A}^d v \in W$?
$f_0 = \beta_0 + \beta_1 x + \dots \beta_{d-1}x^{d-1} + \beta_d x^d$ - минимальный аннулятор, $B_d \neq 0$.
$f_0(\mathcal{A})v = \underbrace{\beta_0 v + \beta_1 \mathcal{A}v + \dots + \beta_{d-1}\mathcal{A}^{d-1}v}_{\in W} + \beta_d \mathcal{A}^d v \Rightarrow \mathcal{A}^d v \in W \Rightarrow \mathcal{A}^k v \in W \ \forall k \in \mathbb{N}$.

■