Алгебра и теория чисел

Курс Жукова И.Б.

Осень 2022 г.

Оглавление

Часть I

Линейные операторы

Глава 1

Алгебра линейных операторов

07.09.22

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

Определение 1.2 (Множество линейных операторов)**.** $\operatorname{End} V = \operatorname{Hom}(V, V)$ — 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 (Алгебра)**.** Говорят, что задана алгебра над полем K, если задано множество A, бинарные операции $+$, $\times$ на нем и отображение $\cdot : K \times A \to A$, 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. $A = M_n(K)$, $A_0 = \{\alpha E_n \mid \alpha \in K\}$ — 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.

Почему алгебра с единицей:

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

$$K \underset{\alpha \mapsto \alpha \cdot 1}{\overset{\varphi}{\to}} A_0$$

Идеал в поле либо нулевой, либо все поле. $\varphi(1) \neq 0 \Rightarrow \mathrm{Ker}(\varphi) \neq K$. 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:

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

$(\mathrm{End}\ V, +, \cdot)$ — 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 $EC = (c_{11}e_1 + \dots + c_{n1}e_n, c_{12}e_1 + \dots + c_{n2}e_n, \dots)$. 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.

$$\begin{array}{ccc} U_E & \xrightarrow{\mathcal{A}} & V_F \\ {\scriptstyle \mathscr{E}_U}\uparrow & & \downarrow{\scriptstyle \mathscr{E}_V = id_V} \\ U_{E'} & \xrightarrow[\mathcal{A}]{} & V_{F'} \end{array}$$

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

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

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

$$A = (C^{-1})^{-1}A'C^{-1} \text{ симметричность}$$
$$A'' = D^{-1}A'D = D^{-1}C^{-1}ACD = (CD)^{-1}A(CD)$$

Глава 2

Инвариантные подпространства

Определение 2.1 (Инвариантность пространств относительно оператора)**.** V — линейное конечномерное пространство, $\mathcal{A} \in \operatorname{End} V$. Пусть $W < V$ — линейное подпространство. W — называется инвариантным относительно $\mathcal{A}$, 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, $\mathcal{A}|_W$ можно рассматривать как элемент $\operatorname{End} W$. Более формально, $\exists\, \mathcal{A}_1 \in \operatorname{End} W\ \forall w \in W :$ $\mathcal{A}_1 w = \mathcal{A} w$.

$$W \underset{w \mapsto \mathcal{A}w}{\xrightarrow{\mathcal{A}_1}} W$$

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

Пусть $W < V,\ V/W = \{v + W \mid v \in V\}$ — фактор-пространство. W — $\mathcal{A}$-инвариант. Определим $\mathcal{A}_2$.

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

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. $\mathcal{A}_2 \in \text{End } V/W$

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 $\mathcal{A} \in \text{End } V$, $W < V$, $e_1, \dots, e_m$ — 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 $e_1, \dots, e_m \in W \Rightarrow$

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

14.09.22

Итак, мы выяснили, что если в нашем подпространсве V есть инвариантное подпространство меньшей размерности (ненулевое) $W < V$, 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 $V = W_1 \oplus W_2$ можно получить $\left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right)$.

Предложение 2.3. Пусть $\mathcal{A} \in \mathrm{End}\, V,\ V = W_1 \oplus W_2,\ \underbrace{e_1, \dots, e_m}_{E_1}$ — 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: $\mathcal{A}v = \lambda v \Leftrightarrow \mathcal{A}v - (\lambda\mathscr{E})v = 0 \Leftrightarrow (\mathcal{A} - \lambda\mathscr{E})v = 0 \Leftrightarrow v \in \operatorname{Ker}(\mathcal{A} - \lambda\mathscr{E})$, $\mathscr{E} = \mathrm{id}$.

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

Определение 3.2 (Собственный вектор)**.** 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. $v \in \operatorname{Ker}(\mathcal{A} - \lambda\mathscr{E})\backslash\{0\}$.

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

Определение 3.4 (Диагонализируемость оператора)**.** $\mathcal{A} \in \operatorname{End} V$ 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. $\Rightarrow$:

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

$E = (e_1, \dots, e_n),\ \mathcal{A}e_i = \lambda_i e_i,\ i = 1, \dots, n,\ e_i \neq 0$, 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 $\lambda_i \in K,\ i = 1, \dots, n \Rightarrow [\mathcal{A}]_E = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. ■

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 $\mathcal{A} \Leftrightarrow \operatorname{Ker}(\mathcal{A} - 0\mathscr{E}) \neq 0 \Leftrightarrow \operatorname{Ker} \mathcal{A} \neq 0 \Leftrightarrow \mathcal{A} \notin \mathrm{GL}(V)$. ■

Определение 3.5 (Геометрическая кратность)**.** Пусть λ — собственное значение $\mathcal{A}$. Его геометрической кратностью называется $g_\lambda = \dim \operatorname{Ker}(\mathcal{A} - \lambda\mathscr{E}),\ 1 \leqslant g_\lambda \leqslant n = \dim V$.

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

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

Доказательство. Нужно доказать: если $v_1 + \dots + v_k = v_1' + \dots + v_k'$ (где $v_i,\ v_i' \in V_{\lambda_i}, i = 1, \dots, k$), то $v_1 = v_1', \dots, v_k = v_k'$.

$$(v_1 - v_1') + \dots + (v_k - v_k') = 0 \qquad (**)$$

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

Доказательство. $V_{\lambda_1} + \dots + V_{\lambda_m} < V \Rightarrow \dim(\underbrace{V_{\lambda_1} + \dots + V_{\lambda_m}}_{g_{\lambda_1} + \dots + g_{\lambda_m}}) \leqslant n$
(по следствию 3.3.1). ■

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

Доказательство. $\Rightarrow$: найдется базис E, такой что: $[\mathcal{A}]_E = \operatorname{diag}(\underbrace{\lambda_1, \dots, \lambda_1}_{c_1}, \underbrace{\lambda_2, \dots, \lambda_2}_{c_2}, \dots, \underbrace{\lambda_m, \dots, \lambda_m}_{c_m})$, $c_1, \dots, c_m \geqslant 0$. Первые c_1 векторов — собственные, принадлежащие собственным значениям λ_1. Они ЛНЗ, так как являются часть базиса $\Rightarrow c_1 \leqslant g_{\lambda_1}$. Аналогично, $c_i \leqslant g_{\lambda_i}$, $2 \leqslant i \leqslant m$. $n = c_1 + \dots + c_m \leqslant g_{\lambda_1} + \dots + g_{\lambda_m} \leqslant n \Rightarrow g_{\lambda_1} + \dots + g_{\lambda_m} = n$
$\Leftarrow$: $\dim(V_{\lambda_1} + \dots + V_{\lambda_m}) = g_{\lambda_1} + \dots + g_{\lambda_m} = n \Rightarrow V = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_m}$. 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

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

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 $\mathcal{A} \Leftrightarrow \operatorname{Ker}(\mathcal{A} - \lambda\mathscr{E}) \neq 0 \Leftrightarrow \underbrace{[\mathcal{A} - \lambda\mathscr{E}]_E}_{=A-\lambda E_n} \notin \mathrm{GL}_n(K) \Leftrightarrow |A - \lambda E_n| = 0$. Задача сводится к нахождению таких λ, при которых определитель матрицы равен нулю.

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

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

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

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

Определение 4.1 (Характеристический многочлен)**.** Пусть $A \in M_n(K)$. Ее характеристический многочлен называется $\chi_A = \underbrace{|A - X \cdot E_n|}_{\in M_n(K[x]) \subset M_n(K(x))} \in K[x]$.
$\begin{vmatrix} \ddots & \\ & \ddots \end{vmatrix} = (a_{11} - x)(a_{22} - x)\dots(a_{nn} - x) + G = (-1)^n x^n + (-1)^{n-1} \underbrace{(a_{11} + \dots + a_{nn})}_{\operatorname{Tr} A} x^{n-1} + \dots + |A|$, где $A = (a_{ij})$, $\deg G \leqslant n-2$, $\operatorname{Tr} A$ – 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: $\chi_A = \chi_{A_1}$.

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

$$\chi_{A_1} = |A_1 - XE_n| = |C^{-1}AC - XC^{-1}C| =$$
$$= |C^{-1}AC - C^{-1}XE_nC| = |C^{-1}(A - XE_n)C| = \underbrace{|C^{-1}|}_{|C|^{-1}} |A - XE_n||C| =$$
$$= |A - XE_n| = \chi_A$$

У эквивалентных матриц след одинаков. 21.09.22

Определение 4.3 (Алгебраическая кратность)**.** Кратность корня λ 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; $\mathcal{A}_1 = \mathcal{A}|_W \in \operatorname{End} W$. Тогда $\chi_{\mathcal{A}_1} | \chi_{\mathcal{A}}$.
2. Пусть $V = W_1 \oplus W_2$; W_1, W_2 – $\mathcal{A}$-инвариантны. $\mathcal{A}_1 = \mathcal{A}|_{W_1}$, $\mathcal{A}_2 = \mathcal{A}|_{W_2} \Rightarrow \chi_{\mathcal{A}} = \chi_{\mathcal{A}_1}\chi_{\mathcal{A}_2}$.

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

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

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

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 $A = [\mathcal{A}]_E = \operatorname{diag}(\underbrace{\lambda_1, \dots, \lambda_1}_{g_{\lambda_1}}, \underbrace{\lambda_2, \dots, \lambda_2}_{g_{\lambda_2}}, \dots, \underbrace{\lambda_k, \dots, \lambda_k}_{g_{\lambda_k}})$, 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) $\Rightarrow g_{\lambda_i} = a_{\lambda_i}$.
2 $\Rightarrow$ 1: $\chi_{\mathcal{A}}$ раскладывается на линейные множители $\Rightarrow \chi_{\mathcal{A}} = \pm(x - \lambda_1)^{a_{\lambda_1}} \dots (x - \lambda_k)^{a_{\lambda_k}}$, $g_{\lambda_i} = a_{\lambda_i} \Rightarrow g_{\lambda_1} + \dots + g_{\lambda_k} = a_{\lambda_1} + \dots + a_{\lambda_k} = n \Rightarrow \mathcal{A}$ – 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), $f \in K[X]$. $f = \alpha_n x^n + ... + \alpha_1 x + \alpha_0$. $f(\mathcal{A}) = \alpha_n \mathcal{A}^n + \alpha_{n-1}\mathcal{A}^{n-1} + ... + \alpha_1 \mathcal{A} + \alpha_0 \mathscr{E}_V \in \operatorname{End} V$.

Предложение 5.1. $f, g \in K[X]$

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

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. $v \in \operatorname{Ker} f(\mathcal{A})$, т.е. $f(\mathcal{A})(v) = 0$. Действуем на v оператором $\mathcal{A}$: $f(\mathcal{A})(\mathcal{A}v) = (f(\mathcal{A})\mathcal{A})(v) = (\mathcal{A}f(\mathcal{A}))(v) = \mathcal{A}(0) = 0$. Таким образом, $\mathcal{A}v \in \operatorname{Ker} f(\mathcal{A})$.
$\operatorname{Im} f(\mathcal{A})$ – $\mathcal{A}$-инвариантное подпространство. Пусть $v \in \operatorname{Im} f(\mathcal{A})$. Это означает, что $\exists\ w$: $v = f(\mathcal{A})(w) \Rightarrow \mathcal{A}v = (\mathcal{A}f(\mathcal{A}))(w) = (f(\mathcal{A})\mathcal{A})(w) = f(\mathcal{A})(\mathcal{A}w) \in \operatorname{Im} f(\mathcal{A})$. ■

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

1. I – подгруппа по сложению.

2. $\forall a \in I \; \forall r \in R : ra \in I$.

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

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

Доказательство. Пусть $I \subset K[X]$.
$I = 0$. $I = (0)$.
$I \neq 0$, 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 – ОГИ (область главных идеалов).

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

Определение 5.1 (Аннулятор)**.** 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. $I = \{f \mid f$ – аннулятор $v\}$ – идеал в $K[X]$.

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

Покажем, что ненулевой аннулятор всегда существует. Пусть $\dim V = n$. $v, \mathcal{A}v, \mathcal{A}^2v, \ldots, \mathcal{A}^n v$ – ЛЗС. $f(\mathcal{A})(v) = \alpha_0 v + \alpha_1 \mathcal{A}v + \ldots + \alpha_n \mathcal{A}^n v = 0$, не все $\alpha_i = 0$. $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \neq 0 \Rightarrow f$ – аннулятор v.

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

Есть вектор $v \in V$, можно ли найти минимальное инвариантное подпространство, содержащее этот вектор? Построим искомое W. Пусть $v \in W$, W – инвариант $\Rightarrow \mathcal{A}v \in W \Rightarrow \mathcal{A}^2v \in W \Rightarrow ... \Rightarrow \mathcal{A}^kv \in W,\ \forall k \in \mathbb{N}$. Отсюда понятно, как построить искомое подпрострнство: нужно «натянуть» пространство на все векторы вида $\mathcal{A}^kv \in W$. Тогда пространство представляет собой линейную оболочку и как раз является инвариантным.

Определение 5.2 (Циклическое подпространство)**.** Циклическим подпространством, порожденным v, называется $C_v = \mathrm{Lin}(v, \mathcal{A}v, \mathcal{A}^2v, ...)$.

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

Доказательство. Всякое подпространство – линейная оболочка, это проверять не нужно.
Проверим $\mathcal{A}$-инвариантность: $w \in C_v \Rightarrow w = \alpha_0v + \alpha_1\mathcal{A}v + ... + \alpha_m\mathcal{A}^mv \Rightarrow \mathcal{A}w = \alpha_0\mathcal{A}v + \alpha_1\mathcal{A}^2v + ... + \alpha_m\mathcal{A}^{m+1}v \in C_v$.
Проверим базис. Предположим, $v, \mathcal{A}v, \mathcal{A}^2v, ..., \mathcal{A}^{d-1}v$ – ЛЗС. $g(\mathcal{A})(v) = \beta_0v + \beta_1\mathcal{A}v + ... + \beta_{d-1}\mathcal{A}^{d-1}v = 0$, не все $\beta = 0$.
$g = \beta_0 + \beta_1x + ... + \beta_{d-1}x^{d-1} \neq 0 \Rightarrow g$ – аннулятор $v \Rightarrow g \in (f_0) \Rightarrow f_0|g \Rightarrow \deg g \leqslant d-1$, пришли к противоречию. Таким образом, $v, \mathcal{A}v, \mathcal{A}^2v, ..., \mathcal{A}^{d-1}v$ – ЛНС.
Осталось проверить $C_v = \underbrace{\mathrm{Lin}(v, \mathcal{A}v, \mathcal{A}^2v, ..., \mathcal{A}^{d-1}v)}_{W}$.
Докажем индукцией по k: $\mathcal{A}^kv \in W$.
База: $k = 0, 1, ..., d-1 \Rightarrow \mathcal{A}^kv \in W$ по определению.
Переход: $k \geqslant d$.
По индукционному предположению: $\mathcal{A}^{k-1}v \in W$, т.е. $\mathcal{A}^{k-1}v = \gamma_0v + \gamma_1\mathcal{A}v + ... + \gamma_{d-1}\mathcal{A}^{d-1}v \Rightarrow \mathcal{A}^kv = \underbrace{\gamma_0\mathcal{A}v + \gamma_1\mathcal{A}^2v + ... + \gamma_{d-2}\mathcal{A}^{d-1}v}_{\in W} + \gamma_{d-1}\mathcal{A}^dv$.
$\mathcal{A}^dv \in W$?
$f_0 = \beta_0 + \beta_1x + ... + \beta_{d-1}x^{d-1} + \beta_dx^d$ – минимальный аннулятор, $\beta_d \neq 0$.

$0 = f_0(\mathcal{A})v = \underbrace{\beta_0 v + \beta_1 \mathcal{A}v + ... + \beta_{d-1}\mathcal{A}^{d-1}v}_{\in W} + \beta_d \mathcal{A}^d v \Rightarrow \mathcal{A}^d v \in W \Rightarrow \mathcal{A}^k v \in W, \ \forall\ k \in \mathbb{N}.$

■

28.09.22

Пусть $v \in V$, $\mathcal{A} \in \operatorname{End} V$.

$C_v = \operatorname{Lin}(v, \mathcal{A}v, \mathcal{A}^2 v, ...) = \operatorname{Lin}(v, \mathcal{A}v, \mathcal{A}^2 v, ..., \mathcal{A}^{d-1}v)$, где $d = \deg f_0$, f_0 – минимальный аннулятор v.

Итак, что представляет собой $\chi_{\mathcal{A}|_{C_v}} = ?$

$f_0 = \beta_0 + \beta_1 x + ... + \beta_{d-1}x^{d-1} + \beta_d x^d$, $\beta_d \neq 0$.

Домножив f_0 на ненулевую константу, мы можем считать $\beta_d = 1$.

$E = (v, \mathcal{A}v, \mathcal{A}^2 v, ..., \mathcal{A}^{d-1}v)$ – базис C_v.

Легко видеть:

$$[\mathcal{A}|_{C_v}]_E = \begin{pmatrix} 0 & 0 & 0 & ... & 0 & -\beta_0 \\ 1 & 0 & 0 & ... & 0 & -\beta_1 \\ 0 & 1 & 0 & ... & 0 & -\beta_2 \\ 0 & 0 & 1 & ... & 0 & -\beta_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 0 & -\beta_{d-2} \\ 0 & 0 & 0 & ... & 1 & -\beta_{d-1} \end{pmatrix} = L_{f_0}$$

L_{f_0} – сопровождающая матрица многочлена f_0.

получаем последний столбец

$f_0(\mathcal{A})v = 0 = \beta_0 v + \beta_1 \mathcal{A}v + ... + \beta_{d-1}\mathcal{A}^{d-1}v + \mathcal{A}^d v.$

$\mathcal{A}^d v = -\beta_0 v - \beta_1 \mathcal{A}v - ... - \beta_{d-1}\mathcal{A}^{d-1}v$ – разложение по базису E

получаем последний столбец

$$\chi_{\mathcal{A}|_{C_v}} = \begin{vmatrix} -x & 0 & 0 & \dots & 0 & -\beta_0 \\ 1 & -x & 0 & \dots & 0 & -\beta_1 \\ 0 & 1 & -x & \dots & 0 & -\beta_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -x & -\beta_{d-2} \\ 0 & 0 & 0 & \dots & 1 & -\beta_{d-1} - x \end{vmatrix} =$$

$$= (-1)^{d+1}(-\beta_0) +$$

$$+ (-1)^{d+2}(-\beta_1) \underbrace{\begin{vmatrix} -x & 0 & 0 & \dots & 0 \\ 0 & 1 & -x & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix}}_{-x} +$$

$$+ (-1)^{d+3}(-\beta_2) \underbrace{\begin{vmatrix} -x & 0 & 0 & 0 & \dots & 0 \\ 1 & -x & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & -x & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{vmatrix}}_{x^2} + \dots +$$

$$+ (-1)^{2d-1}(-\beta_{d-2})(-x)^{d-2} +$$

$$+ (-1)^{2d}(-\beta_{d-1} - x)(-x)^{d-1} =$$

$$= (-1)^{d+1} \sum_{i=0}^{d-1} (-1)^i (-\beta_i)(-x)^i + (-x)^d =$$

$$= (-1)^d \left(\sum_{i=0}^{d-1} \beta_i x^i + x^d \right) =$$

$$= (-1)^d f_0$$

Короче, $\chi_{\mathcal{A}|_{C_v}} = (-1)^d f_0$.

Глава 6

Теорема Гамильтона-Кэли

Теорема 6.1. Пусть $\mathcal{A} \in \operatorname{End} V$, тогда $\chi_{\mathcal{A}}(\mathcal{A}) = 0$.

Доказательство. Рассмотрим $v \in V$. $\chi_{\mathcal{A}|_{C_v}}$ – минимальный аннулятор $v \Rightarrow \chi_{\mathcal{A}|_{C_v}}(\mathcal{A})(v) = 0$. $\chi_{\mathcal{A}|_{C_v}} | \chi_{\mathcal{A}} \Rightarrow \chi_{\mathcal{A}}(\mathcal{A})(v) = 0$, v – любой элемент V. Таким образом, $\chi_{\mathcal{A}}(\mathcal{A}) = 0$. ■

Следствие 6.1.1 (Матричная теорема Гамильтона – Кэли)**.** Допустим, $A \in M_n(K)$, тогда $\chi_A(A) = 0$.

Доказательство. Представим A как $[\mathcal{A}]_E$, тогда $\chi_A = \chi_{\mathcal{A}}$.
$\chi_A(A) = \chi_A([\mathcal{A}]_E) = [\chi_A(\mathcal{A})]_E = [\chi_{\mathcal{A}}(\mathcal{A})]_E = 0$. ■

Как подставляется матрица в многочлен?

Если $f = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n$, $A \in M_n(K)$, то $f(A) = \alpha_0 E_n + \alpha_1 A + ... + \alpha_n A^n$.

Почему мы можем представить матрицу как матрицу какого-то оператора?

1. V – любое пространство с $\dim V = n$, E – фиксированный базис. $\operatorname{End} V \to M_n(K)$, $\beta \mapsto [\beta]_E$ – изоморфизм $\Rightarrow$ существует $\mathcal{A} \in \operatorname{End} V$: $[\mathcal{A}]_E = A$.

2. $V = K^n$, $\mathcal{A}$: $K^n \underset{b \mapsto Ab}{\to} K^n$, E – стандартный базис K^n, $A = [\mathcal{A}]_E$.

Предложение 6.2. Пусть $\mathcal{A} \in \operatorname{End} V$, тогда $I_{\mathcal{A}} = \{f \in K[X] \mid f(\mathcal{A}) = 0\}$ – идеал $K[X]$, где $f(\mathcal{A})$ – нулевой оператор.

Доказательство. $f, g \in I_{\mathcal{A}} \Rightarrow f + g \in I_{\mathcal{A}}$ – очевидно.
$f \in I_{\mathcal{A}}$, $g \in K[X]$: $(gf)(\mathcal{A}) = g(\mathcal{A}) \circ \underbrace{f(\mathcal{A})}_{0} = 0$.
$\chi_{\mathcal{A}} \in I_{\mathcal{A}}$, по теореме Гамильтона–Кэли $\Rightarrow I_{\mathcal{A}} \neq 0$. ■

Образующую $I_{\mathcal{A}}$ называют минимальным многочленом оператора $\mathcal{A}$.

Замечание. $(f) = (g) \Leftrightarrow \begin{cases} f|g \\ g|f \end{cases} \Rightarrow g = \varepsilon f, \varepsilon \in K^*$.

Определение 6.1 (Минимальный многочлен оператора)**.** $\mu_{\mathcal{A}}$ называется минимальным многочленом оператора, если $(\mu_{\mathcal{A}}) = I_{\mathcal{A}}$ (является порождающим идеала $I_{\mathcal{A}}$).

По теореме Гамильтона–Кэли $\mu_{\mathcal{A}} | \chi_{\mathcal{A}}$ ($\chi_{\mathcal{A}} \in I_{\mathcal{A}} = (\mu_{\mathcal{A}})$).
$\mu_{\mathcal{A},v}$ - минимальный аннулятор вектора v.

Предложение 6.3. 1. $\mu_{\mathcal{A},v} | \mu_{\mathcal{A}}$

2. $V = \operatorname{Lin}(v_1, \ldots, v_n)$, тогда $\mu_{\mathcal{A}} = \text{НОК } (\mu_{\mathcal{A},v_1}, \ldots, \mu_{\mathcal{A},v_n})$

Доказательство. 1.

$$\mu_{\mathcal{A}}(\mathcal{A}) = 0 \Rightarrow \mu_{\mathcal{A}}(\mathcal{A})(v) = 0 \Rightarrow \mu_{\mathcal{A}} \in (\mu_{\mathcal{A},v})$$

2.

$$f = \text{НОК } (\ldots)$$
$$\mu_{\mathcal{A},v_i} | f \Rightarrow f(\mathcal{A})(v_i) = 0,\ i = 1, \ldots, n$$
$$v \in V \Rightarrow v = \alpha_1 v_1 + \ldots + \alpha_n v_n$$
$$v_1, \ldots, v_n \in \operatorname{Ker} f(\mathcal{A}) \Rightarrow v \in \operatorname{Ker} f(\mathcal{A})$$

$$f(\mathcal{A}) = 0 \Rightarrow \mu_{\mathcal{A}} \mid f$$
$$1 \Rightarrow \mu_{\mathcal{A},v_i} \mid \mu_{\mathcal{A}},\ i = 1, \dots, n \Rightarrow f \mid \mu_{\mathcal{A}} \Rightarrow f = \varepsilon\mu_{\mathcal{A}},\ \varepsilon \in K^*.$$

■

Глава 7

Примарные подпространства

Определение 7.1 (Примарное подпространство)**.** Допустим, p – неприводимый многочлен, $\mathcal{A} \in \operatorname{End} V$, $W < V$ называется p-примарным, если W – $\mathcal{A}$-инвариантно и $\forall v \in W : \ \mu_{\mathcal{A},v} = p^m,\ m \geqslant 0$. p – неприводимый.

Предложение 7.1. p – неприводимый, $W_p = \{w \in V \mid \mu_{\mathcal{A},w} = p^m,\ m \geqslant 0\}$. W_p – максимальное по включению p-примарное подпространство.

Доказательство. Нужно проверить:

1. $W_p < V$:

$$\lambda \neq 0 \Rightarrow \mu_{\mathcal{A},\lambda w} = \mu_{\mathcal{A},w}.$$
$$w_1,\ w_2 \in W_p$$
$$\mu_{\mathcal{A},w_1} = p^{m_1},\ \mu_{\mathcal{A},w_2} = p^{m_2}$$
$$m = \max(m_1,\ m_2).$$
$$p^m(\mathcal{A})(w_1 + w_2) = p^m(\mathcal{A})(w_1) + p^m(\mathcal{A})(w_2) = 0$$
$$\mu_{\mathcal{A},w_1+w_2} | p^m \Rightarrow \mu_{\mathcal{A},w_1+w_2} = p^l, \text{ где } l \leqslant m \Rightarrow w_1 + w_2 \in W_p$$

2. W_p – $\mathcal{A}$-инвариантно:

$$w \in W_p \Rightarrow \mu_{\mathcal{A},w} = p^m$$
$$p^m(\mathcal{A})(w) = 0$$
$$p^m(\mathcal{A})(\mathcal{A}w) = \mathcal{A}\underbrace{(p^m(\mathcal{A})(w))}_{0} = 0$$
$$\mu_{\mathcal{A},\mathcal{A}w} | p^m \Rightarrow \mu_{\mathcal{A},\mathcal{A}w} = p^l,\ l \leqslant m \Rightarrow \mathcal{A}w \in W_p$$

■

Предложение 7.2. Допустим, $f(\mathcal{A}) = 0,\ f = gh,\ (g,h) = 1$, тогда $V = W_1 \oplus W_2$, где W_1, W_2 – $\mathcal{A}$-инвариантны, $g(\mathcal{A}|_{W_1}) = 0,\ h(\mathcal{A}|_{W_2}) = 0$.

Доказательство. Предположим, $W_1 = \operatorname{Ker} g(\mathcal{A}),\ W_2 = \operatorname{Ker} h(\mathcal{A}),\ W_1, W_2$ – $\mathcal{A}$-инвариантные пространства. $(g,h) = 1 \Rightarrow \exists\ a,\ b \in K[X]$ такие, что $ag + bh = 1$.

1. Проверим, что $W_1 + W_2 = V$:

$$g(\mathcal{A})a(\mathcal{A}) + h(\mathcal{A})b(\mathcal{A}) = \mathscr{E}_V$$
$$\text{Пусть}\ \ v \in V,\ v = \underbrace{g(\mathcal{A})a(\mathcal{A})(v)}_{\in W_2} + \underbrace{h(\mathcal{A})b(\mathcal{A})(v)}_{\in W_1}.$$
$$h(\mathcal{A})(g(\mathcal{A})a(\mathcal{A})(v)) = \underbrace{(hg)}_{f}(\mathcal{A})a(\mathcal{A})(v) = 0$$
$$\Rightarrow g(\mathcal{A})a(\mathcal{A})(v) \in W_2$$

   Аналогично, $h(\mathcal{A})b(\mathcal{A})(v) \in W_1$.

   Таким образом, $\forall v \in W_1 + W_2$.

2. Проверим, что $W_1 \bigcap W_2 = 0$:

$$v \in W_1 \bigcap W_2$$
$$a(\mathcal{A})g(\mathcal{A}) + b(\mathcal{A})h(\mathcal{A}) = \mathscr{E}_V$$
$$a(\mathcal{A})\underbrace{g(\mathcal{A})(v)}_{0} + b(\mathcal{A})\underbrace{h(\mathcal{A})(v)}_{0} = v$$

   Таким образом, $v = 0$.

■

05.10.22

Предложение 7.3. Пусть $f(\mathcal{A}) = 0$, $f = \varepsilon {p_1}^{r_1} \dots {p_s}^{r_s}$, $\varepsilon \in K^*$, p_i попарно неассоциированные неприводимые многочлены. Тогда $V = W_{p_1} \oplus \dots \oplus W_{p_s}$, т.е.

1. $V = W_{p_1} + \dots + W_{p_s}$
2. $0 = w_1 + \dots + w_s$, $w_j \in W_{p_j} \Rightarrow w_1 = \dots = w_s = 0$ (равносильно условию, что V единственным образом представляется в виде суммы $W_{p_1}, \dots, W_{p_s}$: $v = w_1 + \dots + w_s = w_1' + \dots + w_s' \Rightarrow (w_1 - w_1') + \dots + (w_s - w_s') = 0 \Rightarrow w_i - w_i' = 0$).

Доказательство. Индукция по s.
База: $s = 1$. ${p_1}^{r_1}(\mathcal{A}) = 0 \Rightarrow \mu_{\mathcal{A},v} | {p_1}^{r_1} \Rightarrow W_{p_1} = V$.
Переход: $f = gh$, $g = \varepsilon {p_1}^{r_1} \dots {p_{s-1}}^{r_{s-1}}$, $h = {p_s}^{r_s}$, $(g, h) = 1 \Rightarrow V = V' \oplus V''$, $g(\mathcal{A}|_{V'}) = 0$, $h(\mathcal{A}|_{V''}) = 0$ (по предложению 7.2).
По индукционному предположению, $V' = \widetilde{W}_{p_1} \oplus \dots \oplus \widetilde{W}_{p_{s-1}}$.
$\widetilde{W}_{p_j}$ – максимальной p_j-примарное подпространство для $\mathcal{A}|_{V'}$.
$\forall v \in \widetilde{W}_{p_j}$: $\mu_{\mathcal{A}|_{V'},v} = \mu_{\mathcal{A},v} \Rightarrow \widetilde{W}_{p_j} \subset W_{p_j}$.
${p_s}^{r_s}(\mathcal{A}|_{V''}) = 0 \Rightarrow V'' - p_s$-примарное $\Rightarrow V'' \subset W_{p_s}$.
$V = \widetilde{W}_{p_1} \oplus \dots \oplus \widetilde{W}_{p_{s-1}} \oplus V'' \subset W_{p_1} + \dots + W_{p_s}$.
Таким образом, $V = W_{p_1} + \dots + W_{p_s}$.
Предположим, $w_1 + \dots + w_s = 0$, $w_j \in W_{p_j}$, $j = 1, \dots, s$.
Проверим: $w_s = 0$ (аналогично $w_j = 0\ \forall j$).
$w_s = -w_1 - w_2 - \dots - w_{s-1}$.
$w_j \in W_{p_j} \Rightarrow \mu_{\mathcal{A},w_j} = p_j^{l_j}$, $j = 1, \dots, s$.
${p_1}^{l_1} \dots {p_{s-1}}^{l_{s-1}}(\mathcal{A})(w_j) = 0$, $j = 1, \dots, s-1 \Rightarrow$
${p_1}^{l_1} \dots {p_{s-1}}^{l_{s-1}}(\mathcal{A}) \underbrace{(w_1 + \dots + w_{s-1})}_{-w_s} = 0 \Rightarrow {p_s}^{l_s} \mid {p_1}^{l_1} \dots {p_{s-1}}^{l_{s-1}} \Rightarrow$
$l_s = 0 \Rightarrow w_s = 0$. ■

Следствие 7.3.1. Пусть $\mathcal{A} \in \operatorname{End} V$. Тогда $V = \bigoplus_{p | \chi_{\mathcal{A}}} W_p$, p – неприводимый приведеннный.

Замечание. $p \nmid \chi_{\mathcal{A}} \Rightarrow W_p = 0$ (т.к. $\mu_{\mathcal{A},v} \mid \mu_{\mathcal{A}} \mid \chi_{\mathcal{A}}$) $\Rightarrow V = \bigoplus_p W_p$, p – неприводимый приведеннный.

Замечание. $p \mid \chi_{\mathcal{A}} \Rightarrow W_p \neq 0$.

Замечание. Пусть V – p-примарное, тогда $V = \bigoplus_{i=1}^{t} C_{v_i},\ \mu_{\mathcal{A}_i, v_i} = p^{m_i}$.

В частном подходящем базисе:

$[\mathcal{A}]_E = \left(\begin{array}{c|c|c} L_{p^{m_1}} & & \\ \hline & & \\ \hline & & L_{p^{m_t}} \end{array}\right)$, где L_f – сопровождающая матрица многочлена f.

$$f = x^d + \alpha_{d-1}x^{d-1} + ... + \alpha_1 x + \alpha_0 \Rightarrow L_f = \begin{pmatrix} 0 & 0 & ... & -\alpha_0 \\ 1 & 0 & ... & -\alpha_1 \\ 0 & 1 & ... & -\alpha_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & -\alpha_{d-1} \end{pmatrix}$$

Глава 8

Жорданова нормальная форма

Пусть $\mathcal{A} \in \operatorname{End} V$, $\chi_{\mathcal{A}}$ раскладывается на линейные множители.

$p|\chi_{\mathcal{A}}$ неприводимый приведенный $\Rightarrow p = x - \lambda$, λ – собственное значение $\mathcal{A}$.

$W_{x-\lambda} = R_\lambda = \{v \mid \exists j : \ (x-\lambda)^j(\mathcal{A})(v) = 0\} = \{v \mid (\mathcal{A} - \lambda\mathscr{E})^j(v) = 0\}$ – корневые векторы, принадлежащее собственному значению λ.

Определение 8.1 (Корневой вектор и корневое подпространство)**.** Корневым вектором, принадлежащим собственному значению λ называется $v \in V$ такое, что $(\mathcal{A} - \lambda\mathscr{E})^j(v) = 0$ для некоторого j. R_λ – корневое подпространство, принадлежащее собственному значению λ.

Свойства. 1. $V_\lambda \subset R_\lambda$, т.к. $V_\lambda = \operatorname{Ker}(\mathcal{A} - \lambda\mathscr{E})$

2. $R_\lambda \neq 0 \Leftrightarrow \lambda$ – собственное значение $\mathcal{A}$

> **Доказательство.** $\Rightarrow$: $R_\lambda = W_{x-\lambda}$ (по опр.). $R_\lambda \neq 0 \Rightarrow (x-\lambda) \mid \chi_{\mathcal{A}} \Rightarrow \lambda$ – собственное значение.
> $\Leftarrow$: λ – собственное значение $\Rightarrow V_\lambda \neq 0 \Rightarrow R_\lambda \neq 0$ ■

3. $V = \bigoplus_\lambda R_\lambda$ (интерпретация основного определения $V = \bigoplus_{p|\chi_{\mathcal{A}}} W_p$)

Определение 8.2 (Высота корневого вектора)**.** Высота корневого вектора v – это минимальное h такое, что $(\mathcal{A} - \lambda\mathscr{E})^h(v) = 0$.

Корневой вектор высоты 0 – это 0, 1 – собственные векторы, 2 – такие v, что $(\mathcal{A} - \lambda\mathscr{E})(v)$ – собственный вектор, h – $\mathrm{Ker}(\mathcal{A} - \lambda\mathscr{E})^h \setminus \mathrm{Ker}(\mathcal{A} - \lambda\mathscr{E})^{h-1}$.

Очевидно, $R_\lambda = \bigcup_{h\in\mathbb{N}} \underbrace{\mathrm{Ker}(\mathcal{A} - \lambda\mathscr{E})^h}_{:=R_{\lambda,h}}$.

$\underbrace{R_{\lambda,0}}_{=0} \subset \underbrace{R_{\lambda,1}}_{=V_\lambda} \subset R_{\lambda,2} \subset ... \subsetneq R_{\lambda,N_\lambda} = R_{\lambda,N_\lambda+1} \Rightarrow R_\lambda = R_{\lambda,N_\lambda}$.

Предложение 8.1. Пусть N_λ – минимальное натуральное число такое, что $R_\lambda = R_{\lambda,N_\lambda}$, $\lambda_1, ..., \lambda_s$ – все собственные значения $\mathcal{A}$. Тогда $\mu_\mathcal{A} = \underbrace{\prod_{i=1}^{s}(x-\lambda_i)^{N_{\lambda_i}}}_{=f}$.

Доказательство. $R_{\lambda_i} = R_{\lambda_i,N_{\lambda_i}} \Rightarrow (x-\lambda_i)^{N_{\lambda_i}}(\mathcal{A}|_{R_{\lambda_i}}) = 0 \Rightarrow f(\mathcal{A}|_{R_{\lambda_i}}) = 0,\ i = 1, ..., s \Rightarrow f(\mathcal{A}) = 0 \Rightarrow \mu_\mathcal{A} | f$.
Докажем: $(x-\lambda_i)^{N_{\lambda_i}} \mid \mu_\mathcal{A},\ i = 1, ..., s$.
$\exists v \in R_{\lambda_i,N_{\lambda_i}} \setminus R_{\lambda_i,N_{\lambda_i}-1}$
$\mu_{\mathcal{A},v} = (x-\lambda_i)^{N_{\lambda_i}},\ \mu_{\mathcal{A},v} \mid \mu_\mathcal{A} \Rightarrow f \mid \mu_\mathcal{A}$. ■

Следствие 8.1.1. Множества корней $\chi_\mathcal{A}$ и $\mu_\mathcal{A}$ совпадают.

Доказательство. $\mu_\mathcal{A}$ делит $\chi_\mathcal{A}$, и у $\chi_\mathcal{A}$ нет других корней, так как $N_{\lambda_i} \geqslant 1$. ■

Определение 8.3 (Жорданова клетка порядка n)**.** Пусть $\lambda \in K$, $n \in \mathbb{N}$. Жордановой клеткой порядка n с собственным значением λ называется

$$\mathcal{J}_n(\lambda) = \begin{pmatrix} \lambda & 0 & \dots & 0 & 0 \\ 1 & \lambda & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \lambda & 0 \\ 0 & 0 & \dots & 1 & \lambda \end{pmatrix}$$

Жорданова матрица – блочно-диагональная матрица, блоки которой – некоторые жордановы клетки.
$\chi_{\mathcal{J}_n(\lambda)} = (\lambda - x)^n = \pm(x - \lambda)^n,\ (a_\lambda = n,\ g_\lambda = 1)$ для оператора умножения на $\mathcal{J}_n(\lambda)$.
Базис E пространства V называется жордановым базисом (для $\mathcal{A}$), если $[\mathcal{A}]_E$ жорданова.

Определение 8.4 (Нильпотентный оператор)**.** $\mathcal{A}$ называется нильпотентным, если $\exists\ N > 0 :\ \mathcal{A}^N = 0$ (т.е. $\mu_\mathcal{A} = x^{\cdots}$).

$V = \bigoplus R_\lambda$
$(x - \lambda)^{N_\lambda}(\mathcal{A}|_{R_\lambda}) = 0 \Rightarrow (\mathcal{A}|_{R_\lambda} - \lambda\mathscr{E}|_{R_\lambda})^{N_\lambda} = 0$. Таким образом, $\mathcal{A}|_{R_\lambda} - \lambda\mathscr{E}_{R_\lambda}$ – нильпотентный. Минимальное N называется индексом нильпотентности $\mathcal{A}$.

Замечание. E – жорданов базис для $\mathcal{A} \Leftrightarrow E$ – жорданов базис для $\mathcal{A} + \alpha\mathscr{E}$.

Доказательство. $[\mathcal{A}+\alpha\mathscr{E}]_E = [\mathcal{A}]_E + [\alpha\mathscr{E}]_E = [A]_E + \mathrm{diag}(\alpha, \dots, \alpha)$.
$\mathcal{J}_n(\lambda) + \alpha E_n = \mathcal{J}_n(\lambda + \alpha)$. ■

Построение жорданового базиса для нильпотентного оператора.
$\mathcal{B}$ – нильпотент, N – индекс нильпотентности.
$\mu_\mathcal{B} = x^N,\ V = R_0 = R_{0,N} \supsetneq R_{0,N-1} \supset \dots \supset R_{0,1} \supset R_{0,0} = \{0\}$
Пусть $e_{N,1}, e_{N,2}, \dots, e_{N,q_N}$ – базис $R_{0,N}$ относительно $R_{0,N-1}$.

Лемма 8.2. Пусть $v_1, \dots, v_s \in R_{0,m}$ ЛНЗ относительно $R_{0,m-1}$. Тогда: $\mathcal{B}v_1, \dots, \mathcal{B}v_s \in R_{0,m-1}$ ЛНЗ относительно $R_{0,m-2}$.

Доказательство. $\mathcal{B}^m v_i = 0 = \mathcal{B}^{m-1}(\mathcal{B}v_i) = 0 \Rightarrow \mathcal{B}v_i \in R_{0,m-1}$. Пусть $\alpha_1\mathcal{B}v_1 + ... + \alpha_s\mathcal{B}v_s \in R_{0,m-2}$. $\mathcal{B}^{m-2}(\alpha_1\mathcal{B}v_1 + ... \alpha_s\mathcal{B}v_s) = \mathcal{B}^{m-1}(\alpha_1 v_1 + ... \alpha_s v_s) = 0 \Rightarrow \alpha_1 v_1 + ... \alpha_s v_s \in \operatorname{Ker}\mathcal{B}^{m-1} = R_{0,m-1} \Rightarrow \alpha_1 = ... = \alpha_s = 0$. ■

12.10.22

Замечание. $\mathcal{B}$ нильпотентный $\Rightarrow$ единственное собственное значение $\mathcal{B}$ – это 0.

Доказательство. Допустим, $\mathcal{B}v = \lambda v,\ \lambda \neq 0$. Тогда $0 = \mathcal{B}^N v = \lambda^N v$ – противоречие. Появляющиеся жордановы клетки имеют собственное значение ноль.

$$\begin{pmatrix} 0 & 0 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & ... & 1 & 0 \end{pmatrix}$$

$$e_l \overset{\mathcal{B}}{\mapsto} e_{l+1} \overset{\mathcal{B}}{\mapsto} ... \overset{\mathcal{B}}{\mapsto} 0$$

Базисные векторы разбиваются на такие цепочки, а последний переходит в ноль. Наша задача строить такие цепочки. ■

$e_{N,1},\ e_{N,2},\ ..., e_{N,q_N}$ – базис $R_{0,N}$ относительно $R_{0,N-1}$. Подействуем на каждый вектор оператором $\mathcal{B}$, соответственно, их высота уменьшится на единицу. $e_{N-1,1},\ e_{N-1,2},\ ..., e_{N-1,q_N} \in R_{0,N-1}$, линейно независимы относительно $R_{0,N-2}$. Дополним этот набор $e_{N-1,q_N+1},\ ..., e_{N-1,q_{N-1}}$, получили базис $R_{0,N-1}$ относительно $R_{0,N-2}$. Повторяем эти действия, пока не дойдем до высоты 1: $e_{1,1},\ e_{1,2},\ ..., e_{1,q_2} \in R_{0,1} = V_0$, линейно независимы относительно $R_{0,0} = \{0\}$. Тогда $e_{1,1},\ e_{1,2},\ ..., e_{1,q_2}$, $e_{1,q_2+1},\ e_{1,q_2+2},\ ..., e_{1,q_1}$ – базис $R_{0,1}$,$e_{1,1},\ e_{1,2},\ ..., e_{1,q_1}$ и $e_{2,1},\ e_{2,2},\ ..., e_{2,q_2}$ в совокупности – базис $R_{0,2}$ [1].

Индукцией по k мы получаем, что $(e_{i,j} \mid 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant q_i)$ – базис $R_{0,k}$. Найденный базис состоит из $\underbrace{(e_{i,j} \mid 1 \leqslant i \leqslant k-1,\ 1 \leqslant j \leqslant q_i)}_{\text{базис } R_{0,k-1} \text{ по ИП}}$ и $\underbrace{(e_{k,j} \mid 1 \leqslant j \leqslant q_k)}_{\text{базис } R_{0,k} \text{ отн. } R_{0,k-1}}$. Следовательно, все $e_{i,j}$ образуют базис $R_{0,N} =$

[1] https://youtu.be/qlrIV2_gFcU?t=760

$R_0 = V$.

Легко видеть, что найденный базис – жорданов.

$$[\mathcal{B}]_E = \operatorname{diag}(\underbrace{\mathcal{J}_N(0), \dots, \mathcal{J}_N(0)}_{q_N}, \underbrace{\mathcal{J}_{N-1}(0), \dots, \mathcal{J}_{N-1}(0)}_{q_{N-1}-q_N}, \dots, \underbrace{\mathcal{J}_1(0), \dots, \mathcal{J}_1(0)}_{q_1-q_2})$$

Пусть $\mathcal{A} \in \operatorname{End} V$, такое что $\chi_{\mathcal{A}} = \pm\prod_{i=1}^{m}(x-\lambda^i)^{\alpha_{\lambda_i}} \Rightarrow V = \bigoplus_{i=1}^{m} R_{\lambda_i}$.

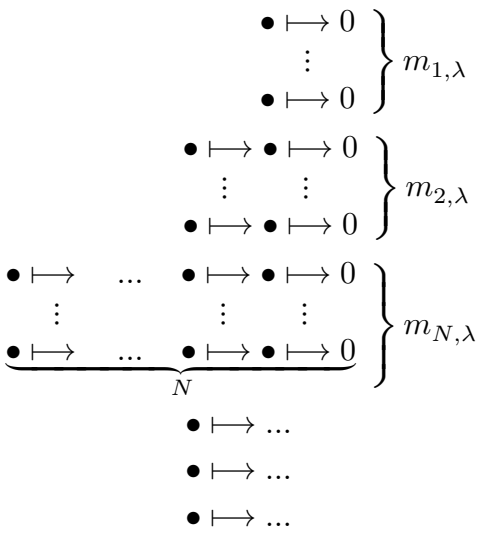
$\mathcal{B}_i = (\mathcal{A} - \lambda_i \mathscr{E})|_{R_{\lambda_i}}$ – нильпотентный $\Rightarrow$ в R_{λ_i} существует жорданов базис для $\mathcal{B}_i \Rightarrow$ для $\mathcal{A}|_{R_{\lambda_i}}$. Объединяя эти базисы, получим жорданов базис для $\mathcal{A}$.

В R_{λ_i} есть базис E_i, такой что $[\mathcal{B}_i]_{E_i} = \operatorname{diag}(\mathcal{J}_m(0), \dots) \Rightarrow [\mathcal{A}|_{R_{\lambda_i}}]_{E_i} = [\mathcal{B}_i + \lambda_i \mathscr{E}_{R_{\lambda_i}}]_{E_i} = [\mathcal{B}_i]_{E_i} + \lambda_i E_{\dim R_{\lambda_i}} = \operatorname{diag}(\mathcal{J}_m(\lambda_i), \dots)$.

Предложение 8.3. Пусть $\chi_{\mathcal{A}}$ раскладывается на линейные множители. Тогда жорданова форма $\mathcal{A}$ определена однозначно с точностью до порядка следования клеток.

Доказательство. λ – собственное значение $\mathcal{A}$. $m_{j,\lambda}$ – количество жордановых клеток вида $\mathcal{J}_j(\lambda)$, докажем, что $m_{j,\lambda}$ – инвариант $\mathcal{A}$. $d_j = \dim R_{\lambda,j}$ – инвариант $\mathcal{A}$. E – жорданов базис $\mathcal{A}$. Переупорядочивая E, считаем, что: $[\mathcal{A}]_E = \operatorname{diag}(\underbrace{\mathcal{J}_1(\lambda), \dots, \mathcal{J}_1(\lambda)}_{m_1,\lambda}, \underbrace{\mathcal{J}_2(\lambda), \dots, \mathcal{J}_2(\lambda)}_{m_2,\lambda}, \dots, \underbrace{\mathcal{J}_N(\lambda), \dots, \mathcal{J}_N(\lambda)}_{m_N,\lambda}, \mathcal{J}_p(\mu), \dots)$.

Посчитаем d_j, для этого рассмотрим оператор $\mathcal{B} = \mathcal{A} - \lambda\mathscr{E}$.



$d_0 = 0$
$d_1 = \dim \operatorname{Ker} \mathcal{B} = m_{1,\lambda} + ... + m_{N,\lambda}$
$d_2 = \dim \operatorname{Ker} \mathcal{B}^2 = m_{1,\lambda} + 2m_{2,\lambda} + ... + 2m_{N,\lambda} = d_1 + m_{2,\lambda} + ... + m_{N,\lambda}$
$d_3 = d_2 + m_{3,\lambda} + ... + m_{N,\lambda}$
... ...
$d_N = d_{N-1} + m_{N,\lambda}$
$d_{N+1} = d_N$

$\Downarrow$

$d_0 = 0$
$d_1 = m_{1,\lambda} + ... + m_{N,\lambda}$
$d_2 - d_1 = m_{2,\lambda} ... + m_{N,\lambda}$
$d_3 - d_2 = m_{3,\lambda} + ... + m_{N,\lambda}$
... ...
$d_N - d_{N-1} = m_{N,\lambda}$
$d_{N+1} = d_N$

$\Downarrow$

$d_1 - (d_2 - d_1) = m_{1,\lambda}$
$(d_2 - d_1) - (d_3 - d_2) = m_{2,\lambda}$
... ...

$(d_{N-1} - d_{N-2}) - (d_N - d_{N-1}) = m_{N-1,\lambda}$

$$m_{k,\lambda} = -d_{k-1} + 2d_k - d_{k+1},\ k = 1, \dots, N$$

■

Замечание. Максимальный порядок жордановой клетки с собственным значением λ равен кратности $(x - \lambda)$ в $\mu_{\mathcal{A}}$.

Доказательство. $e_1, \dots, e_n$ – жорданов базис, $\mu_{\mathcal{A}} = \text{НОК}(\mu_{\mathcal{A},e_i} | i = 1, \dots, n)$. Смотрим, где столбец пересекается с жордановой клеткой. $(\mathcal{A} - \lambda\mathscr{E})^s e_i = 0,\ (\mathcal{A} - \lambda\mathscr{E})^{(s-1)} e_i \neq 0$, где s – количество столбцов, включая i, попавших в эту клетку. Следовательно, $\mu_{\mathcal{A},e_i} = (x-\lambda)^s$, максимальное значение s – максимальный порядок жордановой клетки с собственным значением λ. ■

Часть II

Операторы в евклидовых и унитарных пространствах

Глава 9

Двойственное пространство

19.10.22

Определение 9.1 (Двойственное пространство)**.** V – линейное пространство над полем K, $V^* = \mathrm{Hom}(V, K)$ называется двойственным (дуальным, сопряженным) к V пространством, его элементы – линейные функционалы.

V, W – конечномерные $\Rightarrow \dim \mathrm{Hom}(V, W) = \dim V \dim W$, где $\dim V = n, \dim W = m$. В нашем случае, если $\dim V = n < \infty$, то $\dim V^* = n$.

Пусть $e_1, \dots, e_n$ – базис V. $e^j : \underset{\alpha_1 e_1 + \dots + \alpha_n e_n \mapsto \alpha_j}{V \to K}$ – линейное отображение, тем самым $e^j \in V^*$.

Предложение 9.1. $e^1, \dots, e^n$ – базис V^*.

Доказательство. Проверим линейную независимость:
Пусть $\lambda_1 e^1 + \dots + \lambda_n e^n = 0 \Rightarrow (\lambda_1 e^1 + \dots + \lambda_n e^n)(e_i) = 0$.
Так как $e^j(e_i) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$, $\lambda_1 e^1(e_i) + \dots + \lambda_n e^n(e_i) = \lambda_i$.
Таким образом, $e^1, \dots, e^n$ – ЛНС. ■

Убедимся, что любой линейный функционал раскладывается по такому базису.

Пусть $f \in V^*$.

$$f(e_i) = \lambda_i,\ i = 1, \dots, n$$
$$f_0 = \lambda_1 e^1 + \dots + \lambda_n e^n \in V^*$$
$$f_0(e_i) = \lambda_i,\ i = 1, \dots, n$$

Получается. что у f и f_0 совпадают значения на всех базисных векторах.

Таким образом $f = f_0$. Следовательно, $V^* = \mathrm{Lin}(e^1, \dots, e^n)$.

$e^1, \dots, e^n$ – базис V^*, двойственный к $e_1, \dots, e_n$.

Пример 9.1. $V = \{(a_i) \mid a_i \in K,\ i = 1, 2, \dots,\ a_i = 0$ при достаточно больших $i\}$. Возьмем $W = \{(a_i) \mid a_i \in K, i = 1, 2, \dots\}$.

$$W \underset{(b_i) \mapsto ((a_i) \mapsto \sum_{i=1}^{\infty} a_i b_i)}{\overset{\varepsilon}{\longrightarrow}} V^*$$

Легко понять, что ε – инъективное: если $b_i \neq b_i'$, то в $\varepsilon((b_i))$ и $\varepsilon((b_i'))$ подставим $e_i = (0, \dots, 1_i, \dots, 0) \in V$: $\varepsilon((b_i))(e_i) = b_i \neq \varepsilon((b_i'))(e_i) = b_i'$.

Предложение 9.2. $\varepsilon : V \underset{v \mapsto \varepsilon_v}{\to} V^{**}$ – изоморфизм линейных пространств при условии, что $\dim V = n < \infty$, где $\varepsilon_v : V^* \underset{f \mapsto f(v)}{\to} K$, $V^{**} = (V^*)^*$.

Доказательство. $\mathrm{Ker}\,\varepsilon = 0$? Пусть $v \in \mathrm{Ker}\,\varepsilon$ и $v \neq 0$, дополним до базиса $e_1 = v, e_2, \dots, e_n$. Пусть $e^1, \dots, e^n$ – двойственный базис. $\varepsilon_v(e^1) = e^1(v) = e^1(e_1) = 1 \Rightarrow$ противоречие, так как $\varepsilon_v(e^1) = 0 \Rightarrow$ $\dim \mathrm{Im}\,\varepsilon = \dim V - 0 = n = \dim V^{**} \Rightarrow \mathrm{Im}\,\varepsilon = V^{**}$. ■

$\mathcal{A} \in \mathrm{Hom}(V, W)$, $V \overset{\mathcal{A}}{\to} W \overset{f}{\to} K$.

Определим $\mathcal{A}^T$ (двойственное к $\mathcal{A}$): $W^* \underset{f \mapsto f \circ \mathcal{A}}{\to} V^*$.

Очевидно, $\mathcal{A}^T \in \mathrm{Hom}(W^*, V^*)$.

Предложение 9.3. Пусть E, F - базисы V, W, $\dim E = n$, $\dim F = m$, E', F' – двойственные к ним базисы V^*, W^*, $\dim E' = n$, $\dim F' = m$.
Пусть $\mathcal{A} \in \mathrm{Hom}(V, W)$, $[\mathcal{A}]_{E,F} = A$. Тогда $[\mathcal{A}^T]_{F',E'} = A^T$.

Доказательство. $A = (a_{ij})$, $[\mathcal{A}^T]_{F',E'} = (b_{ij})$.
$\underbrace{\mathcal{A}^T(f^j)}_{=f^j\circ\mathcal{A}} = b_{1j}e^1 + \cdots + b_{n,j}e^n \Rightarrow (f^j \circ \mathcal{A})(e_i) = b_{ij} = f^j(\mathcal{A}e_i) =$
$f^j(a_{1i}f_1 + \cdots + a_{mi}f_m) = a_{ji}$. ■

Глава 10

Двойственность в евклидовых и унитарных пространствах

Будем считать. что V – евклидово или унитарное пространство над полем K ($\mathbb{R}$ или $\mathbb{C}$), $\dim V = n \leqslant \infty$.

$w \in V$, $\rho_w : \underset{v \mapsto (v,w)}{V \to K}$, поскольку умножаем справа, отображение линейно: $(\alpha_1 v_1 + \alpha_2 v_2, w) = \alpha_1 (v_1, w) + \alpha_2 (v_2, w)$. Тем самым, $\rho_w \in V^*$.

Предложение 10.1. Пусть V евклидово. Тогда $\rho : \underset{w \mapsto \rho_w}{V \to V^*}$ – изоморфизм линейных пространств.

Доказательство. Знаем, что размерности одинаковы, остается проверить инъективность.
Пусть $w \in \operatorname{Ker} \rho$, тогда $0 = \rho_w(w) = (w, w) \Rightarrow w = 0 \Rightarrow \rho$ – инъективно $\xrightarrow{\text{по пр. Дирихле}} \rho$ – сюръективно. ■

V_1, V_2 – линейные пространства над полем комплексных чисел. $\mathcal{A} : V_1 \to V_2$ – называется полулинейным, если:

1. $\mathcal{A}(v + v') = \mathcal{A}v + \mathcal{A}v'$
2. $\mathcal{A}(\alpha v) = \overline{\alpha} \mathcal{A} v$

Предложение 10.2. Пусть V унитарное. Тогда $\rho : V \underset{w \mapsto \rho_w}{\to} V^*$ – полулинейная биекция.

Доказательство. Полулинейность очевидна, $\operatorname{Ker}\rho = 0$ доказывается таким же образом.
$\tilde{V} = V$, сложение как в V, $\alpha * v = \overline{\alpha}v$. $(\tilde{V},\ +,\ *)$ – линейное пространство над $\mathbb{C}$. Базисы $\tilde{V},\ V$ совпадают $\Rightarrow \dim \tilde{V} = n$. Рассмотрим $\tilde{\rho} : \tilde{V} \underset{w \mapsto \rho_w}{\to} V^*$ – линеное отображение, ядро по-прежнему равняется 0, тогда $\operatorname{Im}\tilde{\rho} = V^*$. ■

$$\mathcal{A} : V \to W$$

$$\begin{array}{ccc} W^* & \xrightarrow{\mathcal{A}^T} & V^* \\ {\scriptstyle \rho_W}\uparrow & & \uparrow{\scriptstyle \rho_V} \\ W & \xrightarrow[\mathcal{A}^*]{} & V \end{array}$$

Пусть $\mathcal{A} \in \operatorname{Hom}(V, W)$. Рассмотрим отображение $\mathcal{A}^* = \rho_V^{-1} \circ \mathcal{A}^T \circ \rho_W$. Тогда $\mathcal{A}^* \in \operatorname{Hom}(W, V)$ называется отображением, сопряженным к $\mathcal{A}$. Очевидно, $\mathcal{A}^*$ – гомоморфизм групп.

$$\begin{gathered} \mathcal{A}^*(\alpha w) = (\rho_V^{-1} \circ \mathcal{A}^T \circ \rho_W)(\alpha w) = (\rho_V^{-1} \circ \mathcal{A}^T)(\overline{\alpha}\rho_W(w)) = \\ = \rho_V^{-1}(\overline{\alpha}(\mathcal{A}^T \circ \rho_W))(w) = \\ = \alpha(\rho_V^{-1} \circ \mathcal{A}^T \circ \rho_W)(w) = \alpha\mathcal{A}^*(w) \end{gathered}$$

Предложение 10.3 (Характеристическое свойство сопряженного отображения)**.** Пусть $\mathcal{A} \in \operatorname{Hom}(V, W)$.

1. $\forall v \in V,\ w \in W :\ (\mathcal{A}v, w) = (v, \mathcal{A}^* w)$
2. Если $\mathcal{B} \in \operatorname{Hom}(W, V)$ такое, что $\forall v \in V,\ w \in W :\ (\mathcal{A}v, w) = (v, \mathcal{B}w)$, то $\mathcal{B} = \mathcal{A}^*$.

Доказательство.

1. $(v, \mathcal{A}^* w) = \rho_{\mathcal{A}^* w}(v) = \rho_V(\mathcal{A}^* w)(v) = \mathcal{A}^T(\rho_W(w))(v) = (\rho_W(w) \circ \mathcal{A})(v) = \rho_w(\mathcal{A}v) = (\mathcal{A}v, w)$
2. Имеем: $\forall v \in V,\ w \in W :\ (\mathcal{A}v, w) = (v, \mathcal{A}^* w) \Rightarrow$

$\Rightarrow (v, (\mathcal{B} - \mathcal{A}^*)(w)) = 0 \Rightarrow \forall w \in W : ((\mathcal{B} - \mathcal{A}^*)w, (\mathcal{B} - \mathcal{A}^*)w) =$
$= 0 \Rightarrow \forall w \in W : (\mathcal{B} - \mathcal{A}^*)(w) = 0$, т.е. $\mathcal{B}w = \mathcal{A}^*w$.

■

Глава 11

Сопряженный оператор

26.10.22

V – евклидово (унитарное) пространство.

Предложение 11.1. $\mathcal{A},\ \mathcal{B} \in \operatorname{End} V,\ \alpha \in K$

1. $(\mathcal{A}+\mathcal{B})^* = \mathcal{A}^* + \mathcal{B}^*$
2. $(\alpha\mathcal{A})^* = \overline{\alpha}\mathcal{A}^*$
3. $(\mathcal{A}\mathcal{B})^* = \mathcal{B}^*\mathcal{A}^*$
4. $\mathcal{A}^{**} = \mathcal{A}$

Каждый раз при доказательстве будем использовать характеристическое свойство.

Доказательство. 1. Достаточно проверить: $\forall v, w \in V:\ ((\mathcal{A}+\mathcal{B})v, w) = (v, (\mathcal{A}^*+\mathcal{B}^*)w)$.
Когда мы это проверим, то окажется, что $(\mathcal{A}+\mathcal{B})$ сопряжены с $(\mathcal{A}^*+\mathcal{B}^*)$, а это как раз то, что нам нужно доказать.

$$((\mathcal{A}+\mathcal{B})v, w) = (\mathcal{A}v + \mathcal{B}v, w) = \\ = (\mathcal{A}v, w) + (\mathcal{B}v, w) = (v, \mathcal{A}^*w) + (v, \mathcal{B}^*w) = \\ = (v, (\mathcal{A}^*+\mathcal{B}^*)w)$$

2. $(\alpha\mathcal{A}v, w) = \alpha(\mathcal{A}v, w) = \alpha(v, \mathcal{A}^*w) = (v, \overline{\alpha}\mathcal{A}^*w)$
3. $((\mathcal{A}\mathcal{B})v, w) = (\mathcal{A}(\mathcal{B}v), w) = (\mathcal{B}v, \mathcal{A}^*w) = (v, \mathcal{B}^*\mathcal{A}^*w)$
4. Достаточно проверить: $\forall v, w \in V : \ (\mathcal{A}^*v, w) = (v, \mathcal{A}w)$.
   $(\mathcal{A}^*v, w) = \overline{(w, \mathcal{A}^*v)} = \overline{(\mathcal{A}w, v)} = (v, \mathcal{A}w)$

■

Теперь рассмотрим характеризацию сопряженного оператора на матричном языке.

Пусть $E = (e_1, \dots, e_n)$ – ортонормированный базис V.

$[\mathcal{A}]_E = A = (a_{ij}),\ [\mathcal{A}^*]_E = B = (b_{ij})$.

Как связаны эти матрицы между собой? Первое означает, что $\mathcal{A}e_j = \sum_{i=1}^n a_{ij}e_i$. Скалярно умножим это равенство на e_k: $(\mathcal{A}e_j, e_k) = a_{kj}$, т.к. базис ортонормированный, с другой стороны $(\mathcal{A}e_j, e_k) = (e_j, \mathcal{A}^*e_k)$. Для e_k запишем: $\mathcal{A}^*e_k = \sum_{i=1}^n b_{ik}e_k$. Подставим это в предыдущее равенство: $(e_j, \mathcal{A}^*e_k) = (e_j, \sum_{i=1}^n b_{ik}e_i) = (e_j, b_{jk}e_j) = \overline{b_{jk}} \Rightarrow b_{jk} = \overline{a_{kj}}$.

Таким образом, $B = \overline{A^T} = A^*$.

Предложение 11.2. Пусть $U \subset V$ инвариантно относительно $\mathcal{A}$. Тогда $U^\perp$ инвариантно относительно $\mathcal{A}^*$.

Доказательство. Нужно проверить: $\forall w \in U^\perp\ \mathcal{A}^*w \in U^\perp$.
$\forall u \in U\ (u, \mathcal{A}^*w) = (\underbrace{\mathcal{A}u}_{\in U},\ \underbrace{w}_{\in U^\perp}) = 0$. Voila! ■

Определение 11.1 (Самосопряженный оператор). $\mathcal{A} \in \operatorname{End} V$ называется самосопряженным, если $\mathcal{A} = \mathcal{A}^*$.

Если $\mathcal{A} = \mathcal{A}^*$, рассмотрим отображение $\mathcal{B} : \underset{(v,w)\mapsto(\mathcal{A}v,w)}{V \times V \to K}$.

$$\mathcal{B}(w, v) = (\mathcal{A}w, v) = (w, \mathcal{A}^*v) = (w, \mathcal{A}v) = \overline{(\mathcal{A}v, w)} = \overline{\mathcal{B}(v, w)}$$

Таким образом, $\mathcal{B}$ – эрмитова форма.

Можно проверить, что все эрмитовы формы так задаются.

Определение 11.2 (Ортогональный оператор). $\mathcal{A} \in \operatorname{End} V$ в евклидовом (унитарном) пространстве называется ортогональным (соответственно, унитарным), если $\mathcal{A}\mathcal{A}^* = \mathscr{E}_V$.

E – ортонормированный базис. Тогда: $\mathcal{A}$ ортогональный (унитарный) $\Leftrightarrow AA^* = E_n$. В ортогональном случае: $AA^T = E_n \Leftrightarrow$ строки A образуют ортонормированный базис $\mathbb{R}^n$.

Замечание. A – ортогональна $\Leftrightarrow A^T$ – ортогональна.

Предложение 11.3. Пусть $\mathcal{A} \in \operatorname{End} V,\ V$ – евклидово. Тогда 3 утверждения эквивалентны:

1. $\mathcal{A}$ – ортогональный.
2. $\forall v,\ w \in V :\ (\mathcal{A}v, \mathcal{A}w) = (v, w)$.
3. $\forall v \in V :\ ||\mathcal{A}v|| = ||v||$.

Доказательство. $1 \Rightarrow 2 :\ (\mathcal{A}v, \mathcal{A}w) = (v, \mathcal{A}^*\mathcal{A}w) = (v, w)$.
$2 \Rightarrow 1 :\ \forall v,\ w : \underbrace{(\mathcal{A}v, \mathcal{A}w)}_{=(v, \mathcal{A}^*\mathcal{A}w)} = (v, w) \Rightarrow (v, \mathcal{A}^*\mathcal{A}w - w) = 0$ (вторая компонента скалярного произведения лежит в ортогональном дополнении ко всему пространству (так как v – любой вектор)).
$2 \Rightarrow 3 : ||\mathcal{A}v|| = \sqrt{(\mathcal{A}v, \mathcal{A}v)} = \sqrt{(v, v)} = ||v||$
$3 \Rightarrow 2 :\ v,\ w \in V,\ ||v + w||^2 = (v + w, v + w) = ||v||^2 + ||w||^2 + 2(v, w),\ ||\mathcal{A}v + \mathcal{A}w||^2 = (\mathcal{A}v + \mathcal{A}w, \mathcal{A}v + \mathcal{A}w) = ||\mathcal{A}v||^2 + ||\mathcal{A}w||^2 + 2(\mathcal{A}v, \mathcal{A}w)$, по свойству 3 слева стоит одно и то же, справа первые два слагаемые попарно равны $\Rightarrow (v, w) = (\mathcal{A}v, \mathcal{A}w)$. ■

Глава 12

Нормальные операторы

Определение 12.1 (Нормальный оператор)**.** Пусть V – евклидово (унитарное) пространство. $\mathcal{A} \in \operatorname{End} V$ называется нормальным, если $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$.

Пример 12.1. 1. Самосопряженный: $\mathcal{A} = \mathcal{A}^*$

2. Ортогональный/унитарный: $\mathcal{A}\mathcal{A}^* = \mathcal{A}\mathcal{A}^{-1} = \mathscr{E}_V = \mathcal{A}^{-1}\mathcal{A} = \mathcal{A}^*\mathcal{A}$

3. Кососимметрический: $\mathcal{A}^* = -\mathcal{A}$

Предложение 12.1. Пусть $\mathcal{A}$ – нормальный, $\alpha \in K$. Тогда $\mathcal{B} = \mathcal{A} - \alpha\mathscr{E}_V$ – тоже нормальный.

Доказательство.

$$\mathcal{B}^* = \mathcal{A}^* - (\alpha\mathscr{E}_V)^* = \mathcal{A}^* - \overline{\alpha}\mathscr{E}_V^* = \mathcal{A}^* - \overline{\alpha}\mathscr{E}_V$$
$$\mathcal{B}\mathcal{B}^* = \mathcal{A}\mathcal{A}^* - \alpha\mathcal{A}^* - \overline{\alpha}\mathcal{A} + |\alpha|^2\mathscr{E}_V$$
$$\mathcal{B}^*\mathcal{B} = \mathcal{A}^*\mathcal{A} - \alpha\mathcal{A}^* - \overline{\alpha}\mathcal{A} + |\alpha|^2\mathscr{E}_V$$

■

Предложение 12.2. Пусть $\mathcal{A}$ – нормальный, $v \in V$ – собственный вектор оператора $\mathcal{A}$, принадлежащий собственному значению λ. Тогда v – собственный вектор оператора $\mathcal{A}^*$, принадлежащий собственному значению $\overline{\lambda}$.

Доказательство. $\underbrace{(\mathcal{A} - \lambda\mathcal{E}_V)}_{\mathcal{B}} v = 0 \Rightarrow (\mathcal{B}v, \mathcal{B}v) = 0 \Rightarrow (v, \mathcal{B}^*\mathcal{B}v) = 0 \Rightarrow (v, \mathcal{B}\mathcal{B}^*v) = 0 \Rightarrow (\mathcal{B}^*v, \mathcal{B}^*v) = 0 \Rightarrow \mathcal{B}^*v = 0 = \mathcal{A}^*v - \overline{\lambda}v \Rightarrow \mathcal{A}^*v = \overline{\lambda}v.$ ■

Теорема 12.3 (Спектральная теорема для нормальных операторов в унитарных пространствах)**.** Пусть V унитарное, $\mathcal{A} \in \operatorname{End} V$ – нормальный. Тогда в V существует ортонормированный базис E, такой что $[\mathcal{A}]_E$ – диагональная.

Доказательство. $v \neq 0 \Rightarrow v_0 = \frac{1}{||v||}v$.
Индукция по $n = \dim V$.
База: $\exists e_1 \in V : \ ||e_1|| = 1$, e_1 – искомый базис.
Переход: $\chi_{\mathcal{A}} \in \mathbb{C}[x]$, $\deg \chi_{\mathcal{A}} = n > 1 \Rightarrow \exists \lambda \in \mathbb{C} : \ \chi_{\mathcal{A}}(\lambda) = 0$, где λ – собственное значение $\mathcal{A}$. v – собственный вектор, принадлежащий собственному значению λ, $e_1 = \frac{1}{||v||}v$. e_1 – собственный для $\mathcal{A} \Rightarrow$ собственный для $\mathcal{A}^*$. $U = \operatorname{Lin}(e_1)$ – инвариантное относительно $\mathcal{A}$ и $\mathcal{A}^*$. $W = U^\perp$ – инвариантно относительно $\mathcal{A}^*$ и $\mathcal{A}^{**} = \mathcal{A}$.
Размерность $U = 1$, $\dim W = \dim V - \dim U = n - 1$.
Применим индукционное предположение. Проверим: $\mathcal{A}_1 = \mathcal{A}|_W$ - нормальный. $\mathcal{A}^*|_W = \mathcal{A}_1^*$?
$\forall v, \ w \in W : \ (\mathcal{A}_1 v, w) = (\mathcal{A}v, w) = (v, \mathcal{A}^*w) = (v, (\mathcal{A}^*|_W)w)$
$\Rightarrow \mathcal{A}_1\mathcal{A}_1^* = \mathcal{A}_1^*\mathcal{A}_1$.
По индукционному предположению в W есть ортонормированный базис $E_1 = (e_2, e_3, \dots, e_n)$, такой что $[\mathcal{A}_1]_{E_1}$ диагональна. $E = (\underbrace{e_1}_{\in U}, \underbrace{e_2, \dots, e_n}_{\in U^\perp})$. $V = U \oplus U^\perp \Rightarrow E$ – базис V. Очевидно, он ортонормированный.

$$[\mathcal{A}]_E = \left(\begin{array}{c|c} \lambda & 0 \dots 0 \\ \hline 0 & \\ \vdots & [\mathcal{A}_1]_{E_1} \\ 0 & \end{array}\right) - \text{диагональная}$$

■

Предложение 12.4. Пусть V – евклидово и унитарное, $\mathcal{A} \in \operatorname{End} V$ – нормальный. $v,\ w \in V$ – собственые векторы $\mathcal{A}$, принадлежащие разным собственным значениям. Тогда $v \perp w$.

Доказательство.

$$\mathcal{A}v = \lambda v$$
$$\mathcal{A}w = \mu w$$
$$\mu \neq \lambda$$
$$\lambda(v,w) = (\lambda v, w) = (\mathcal{A}v, w) = (v, \mathcal{A}^* w) = (v, \overline{\mu} w) = \mu(v,w)$$
$$\Rightarrow (\mu - \lambda)(v,w) = 0$$
$$\Rightarrow (v,w) = 0$$

■

Следствие 12.4.1 (из теоремы)**.** Пусть V – унитарное пространство, $\mathcal{A} \in \operatorname{End} V$. Тогда: $\mathcal{A} = \mathcal{A}^* \Leftrightarrow$ в V существует ортонормированный базис E, такой что $[\mathcal{A}]_E = \operatorname{diag}(c_1, \dots, c_n),\ c_1, \dots, c_n \in \mathbb{R}$.

Доказательство. $\exists$ ортонормированный E, такой что $[\mathcal{A}]_E = A = \operatorname{diag}(c_1, \dots, c_n)$. $\mathcal{A} = \mathcal{A}^* \Rightarrow A = A^* = \operatorname{diag}(\overline{c_1}, \dots, \overline{c_n}) \Rightarrow c_1 = \overline{c_1}, \dots, c_n = \overline{c_n} \Rightarrow c_1, \dots, c_n \in \mathbb{R}$.
Обратно: $c_1, \dots, c_n \in \mathbb{R} \Rightarrow A = \operatorname{diag}(c_1, \dots, c_n) = A^*$ – эрмитова $\Rightarrow \mathcal{A} = \mathcal{A}^*$. ■

Следствие 12.4.2. Пусть V – унитарное пространство, $\mathcal{A} \in \operatorname{End} V$. Тогда: $\mathcal{A}$ – унитарный $\Leftrightarrow$ в V существует ортонормированный базис E, такой что $[\mathcal{A}]_E = \operatorname{diag}(u_1, \dots, u_n),\ |u_1|, \dots, |u_n| = 1$.

Доказательство. $\Rightarrow$: в некотором ортонормированном базисе E $[\mathcal{A}]_E = A = \operatorname{diag}(u_1, \dots, u_n)$, $AA^* = E_n \Rightarrow u_1\overline{u_1} = \dots = u_n\overline{u_n} = 1 \Rightarrow |u_1| = \dots = |u_n| = 1$.
$\Leftarrow$: $A = \operatorname{diag}(u_1, \dots, u_n)$, $|u_1| = \dots = |u_n| = 1 \Rightarrow AA^* = E_n$, A – матрица $\mathcal{A}$ в ортонормированном базисе $\Rightarrow \mathcal{A}\mathcal{A}^* = \mathscr{E}$. ■

всем героям, проверяющим конспект, мерси ♥
я стараюсь делать поменьше ошибок, честно

Глава 13

Комплексификация

02.11.22

V – линейное пространство над полем $\mathbb{R}$. Построим $V_{\mathbb{C}}$ – линейное пространство над полем $\mathbb{C}$. Неформально: $V_{\mathbb{C}} = \{v + iw \mid v,\ w \in V\}$ (сложение: вещественные части и мнимые отдельно, умножение на скаляр: $(\alpha + i\beta)(v + iw) = (\alpha v - \beta w) + i(\beta v + \alpha w)$).

$V_{\mathbb{C}} = V \times V$. На этом множестве введем сложение и умножение на комплексные скаляры.

$$(v_1, w_1) + (v_2, w_2) := (v_1 + v_2, w_1 + w_2)$$
$$(\alpha + i\beta)(v, w) := (\alpha v - \beta w, \beta v + \alpha w)$$

Нетрудно проверить, что $(V_{\mathbb{C}}, +, \cdot)$ – линейное пространство над $\mathbb{C}$.

1. Рассмотрим подмножество $V' = \{(v, 0) \mid v \in V\}$ – замкнуто относительно сложения и умножения на вещественные скаляры ($(\alpha + i0)(v, w) = (\alpha v, 0)$).

   $V \underset{v \mapsto (v,0)}{\xrightarrow{\sim}} V'$ – изоморфизм линейных пространств над $\mathbb{R}$. Следовательно, V' можно рассматривать как линейное пространство над $\mathbb{R}$. Можно от отожествить v с $(v, 0)$.

2. Можно ли сделать что-то с $(0, w)$? Оказывается, что можно: $(0, w) = i(w, 0)$.

3. Таким образом, $(v, w) = (v, 0) + i(w, 0) = v + iw$.

$V_{\mathbb{C}}$ – комплексификация V.

Следствие 13.0.1. Пусть $e_1, \dots, e_n$ – базис V. Тогда $e_1, \dots, e_n$ – базис $V_{\mathbb{C}}$, где $e_k = e_k + i0,\ 1 \leqslant k \leqslant n$.

Доказательство. Рассмотрим $u \in V_{\mathbb{C}}$.

$$u = v + iw,\ v,\ w \in V$$
$$v = \alpha_1 e_1 + \dots + \alpha_n e_n$$
$$w = \beta_1 e_1 + \dots + \beta_n e_n$$
$$\Rightarrow u = (\alpha_1 + i\beta_1)e_1 + \dots + (\alpha_n + i\beta_n)e_n \in \mathrm{Lin}_{V_{\mathbb{C}}}(e_1, \dots, e_n)$$

Предположим, $u = (\alpha_1 + i\beta_1)e_1 + \dots + (\alpha_n + i\beta_n)e_n = 0$. $u = \alpha_1 e_1 + \dots + \alpha_n e_n + i(\beta_1 e_1 + \dots \beta_n e_n) \Rightarrow \begin{cases} \alpha_1 e_1 + \dots + \alpha_n e_n = 0 \\ \beta_1 e_1 + \dots + \beta_n e_n = 0 \end{cases} \Rightarrow$

$\begin{cases} \alpha_1 = \dots = \alpha_n = 0 \\ \beta_1 = \dots = \beta_n = 0 \end{cases}$ ■

Следствие 13.0.2. $\dim V_{\mathbb{C}} = \dim V$

По $\mathcal{A} \in \mathrm{End}\, V$ построим $\mathcal{A}_{\mathbb{C}} \in \mathrm{End}\, V_{\mathbb{C}}$.

$$\mathcal{A}_{\mathbb{C}} : \underset{v+iw \mapsto \mathcal{A}v + i\mathcal{A}w}{V_{\mathbb{C}} \to V_{\mathbb{C}}}$$

Предложение 13.1. $\mathcal{A}_{\mathbb{C}} \in \mathrm{End}\, V_{\mathbb{C}}$

Доказательство.

$$\mathcal{A}_{\mathbb{C}}((v_1 + iw_1) + (v_2 + iw_2)) = \mathcal{A}(v_1 + v_2) + i\mathcal{A}(w_1 + w_2) =$$
$$= \mathcal{A}v_1 + \mathcal{A}v_2 + i\mathcal{A}w_1 + i\mathcal{A}w_2 = \mathcal{A}_{\mathbb{C}}(v_1 + iw_1) + \mathcal{A}_{\mathbb{C}}(v_2 + iw_2)$$

$$\alpha \in \mathbb{R},\ \mathcal{A}_{\mathbb{C}}(\alpha(v + iw)) = \mathcal{A}(\alpha v) + i\mathcal{A}(\alpha w) =$$
$$= \alpha(\mathcal{A}v + i\mathcal{A}w) = \alpha\mathcal{A}_{\mathbb{C}}(v + iw)$$

$$\mathcal{A}_{\mathbb{C}}(i(v + iw)) = \mathcal{A}_{\mathbb{C}}(-w + iv) =$$
$$= \mathcal{A}(-w) + i\mathcal{A}v = i(\mathcal{A}v + i\mathcal{A}w) = i\mathcal{A}_{\mathbb{C}}(v + iw)$$

$\Rightarrow \mathcal{A}_{\mathbb{C}}((\alpha+i\beta)(v+iw)) = (\alpha+i\beta)\mathcal{A}_{\mathbb{C}}(v+iw)$ ■

Предложение 13.2. Пусть E – базис V. Тогда $[\mathcal{A}_{\mathbb{C}}]_E = [\mathcal{A}]_E$.

Доказательство. $[\mathcal{A}]_E = (a_{kj})$, $\mathcal{A}e_j = \sum_{k=1}^n a_{kj}e_k$. $\mathcal{A}_{\mathbb{C}}e_j = \sum_{k=1}^n a_{kj}e_k + i0 = \sum_{k=1}^n (a_{kj}+i0)e_k$. ■

Следствие 13.2.1. $\chi_{\mathcal{A}_{\mathbb{C}}} = \chi_{\mathcal{A}}$.

Предложение 13.3. Пусть $\mathcal{A} \in \operatorname{End} V$, λ – собственное значение $\mathcal{A}_{\mathbb{C}}$, $\lambda \notin \mathbb{R}$; $v_1+iw_1, \dots, v_l+iw_l$ – базис V_λ. Тогда $\overline{\lambda}$ – собственное значение $\mathcal{A}_{\mathbb{C}}$ и $v_1-iw_i, \dots, v_l-iw_l$ – базис $V_{\overline{\lambda}}$.

Доказательство.

$$\chi_{\mathcal{A}_{\mathbb{C}}} = \chi_{\mathcal{A}} \in \mathbb{R}[X]$$
$$\chi_{\mathcal{A}}(\lambda) = 0 \Rightarrow \chi_{\mathcal{A}}(\overline{\lambda}) = 0$$

Замечание. $u \in V_{\mathbb{C}},\ \gamma \in \mathbb{C} \Rightarrow \overline{\gamma u} = \overline{\gamma}\cdot\overline{u}$. $\overline{u} = \overline{v+iw} = v-iw$. Проверка: пусть $\gamma = \alpha+i\beta,\ u = v+iw$, тогда $\overline{(\alpha+i\beta)(v+iw)} = \overline{\alpha v - \beta w + i(\alpha w+\beta v)} = \alpha v - \beta w - i(\alpha w+\beta v) = (\alpha+i\beta)(v-iw) = \alpha v - \beta w - i(\beta v+\alpha w)$.

$$\underbrace{\mathcal{A}_{\mathbb{C}}(v_j+iw_j)}_{\mathcal{A}v_j+i\mathcal{A}w_j} = \lambda(v_j+iw_j)$$
$$\mathcal{A}_{\mathbb{C}}(v_j-iw_j) = \mathcal{A}v_j - i\mathcal{A}w_j = \overline{(\mathcal{A}v_j+i\mathcal{A}w_j)} =$$
$$= \overline{\lambda(v_j+iw_j)} = \overline{\lambda}(v_j-iw_j)$$

Таким образом, $v_1-iw_1, \dots, v_l-iw_l \in V_{\overline{\lambda}}$.
Проверим линейную независимость. Предположим, $\gamma_1(v_1-iw_1) + \dots + \gamma(v_l-iw_l) = 0 \Rightarrow \overline{\gamma}(v_1+iw_1) + \dots + \overline{\gamma}(v_l+iw_l) = 0 \Rightarrow \overline{\gamma_1} = \dots = \overline{\gamma_l} = 0 \Rightarrow \gamma_1 = \dots = \gamma_l = 0 \Rightarrow \dim V_{\overline{\lambda}} \geqslant \dim V_\lambda$.
Аналогично, $\dim V_\lambda \geqslant \dim V_{\overline{\lambda}} \Rightarrow \dim V_\lambda = \dim V_{\overline{\lambda}} = l \Rightarrow v_1 - iw_i, \dots, v_l-iw_l$ – базис $V_{\overline{\lambda}}$. ■

Далее V – евклидово пространство. Введем на $V_{\mathbb{C}}$ отображение $V_{\mathbb{C}} \times V_{\mathbb{C}} \to \mathbb{C}$, где $\mathcal{B}(v+iw, v'+iw') = (v,v')+(w,w')+i((w,v')-(v,w'))$.
$\underset{(u,u')\mapsto\mathcal{B}(u,u')}{}$

lil friendly reminder: сопряженный к $i = -i$, и при выносе скаляра из правой части, нужно брать его с сопряжением.

Предложение 13.4. $\mathcal{B}$ – скалярное произведение на $V_{\mathbb{C}}$

Доказательство. Полуторалинейность – непосредственная проверка.
$\mathcal{B}(v'+iw', v+iw) = \overline{\mathcal{B}(v+iw, v'+iw')}$.
$\mathcal{B}(v+iw, v+iw) = (v,v)+(w,w) \geqslant 0$, $(= 0$ только при $v = w = 0)$.
Таким образом, $(V_{\mathbb{C}}, \mathcal{B})$ – унитарное пространство. ■

Замечание. $e_1, \dots, e_n$ – базис V. Тогда: $e_1, \dots, e_n$ – ортонормированный базис $V \Leftrightarrow e_1, \dots, e_n$ – ортонормированный базис $V_{\mathbb{C}}$.

Предложение 13.5. Пусть $\mathcal{A} \in \operatorname{End} V$. Тогда $(\mathcal{A}_{\mathbb{C}})^* = (\mathcal{A}^*)_{\mathbb{C}}$.

Доказательство. Нужно проверить: $\forall u,\ u' \in V_{\mathbb{C}}\ (\mathcal{A}_{\mathbb{C}}u, u') = (u, (\mathcal{A}^*)_{\mathbb{C}}u')$. Пусть $u = v+iw,\ u' = v'+iw'$.

$$
\begin{aligned}
(\mathcal{A}_{\mathbb{C}}u, u') &= (\mathcal{A}v + i\mathcal{A}w, v'+iw') = \\
&= (\mathcal{A}v, v') + (\mathcal{A}w, w') + i((\mathcal{A}w, v') - (\mathcal{A}v, w')) = \\
&= (v, \mathcal{A}^*v') + (w, \mathcal{A}^*w') + i((w, \mathcal{A}^*v') - (v, \mathcal{A}^*w)) = \\
&= (v, \mathcal{A}^*v' + i\mathcal{A}^*w') + (w, \mathcal{A}^*w' - i\mathcal{A}^*v') = \\
&= (v, \underbrace{\mathcal{A}^*v + i\mathcal{A}^*w'}_{(\mathcal{A}^*)_{\mathbb{C}}u'}) + (iw, \underbrace{i(\mathcal{A}^*w' - i\mathcal{A}^*v')}_{((\mathcal{A}^*)_{\mathbb{C}}u')}) = (u, (\mathcal{A}^*)_{\mathbb{C}}u').
\end{aligned}
$$

■

Глава 14

Нормальные операторы в евклидовом пространстве

V – евклидово пространство, $\mathcal{A} \in \operatorname{End} V$ – нормальный.

$\mathcal{A}_{\mathbb{C}}$ – нормальный. $\mathcal{A}_{\mathbb{C}}\mathcal{A}_{\mathbb{C}}^* = \mathcal{A}_{\mathbb{C}}(\mathcal{A}^*)_{\mathbb{C}} = (\mathcal{A}\mathcal{A}^*)_{\mathbb{C}} = (\mathcal{A}^*\mathcal{A})_{\mathbb{C}} = \mathcal{A}_{\mathbb{C}}^*\mathcal{A}_{\mathbb{C}}$.

$\underbrace{\chi_{\mathcal{A}}}_{\in\mathbb{R}[X]} = \chi_{\mathcal{A}_{\mathbb{C}}} = \prod_{i=1}^{s}(x-\lambda_i)^{g_i}\prod_{i=1}^{t}(x-\mu_i)^{h_i}(x-\overline{\mu_i})^{h_i},\ \lambda_i \in \mathbb{R},\ \mu_i \notin \mathbb{R}$.

$V_{\mathbb{C}} = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_s} \oplus \underbrace{V_{\mu_1} \oplus V_{\overline{\mu_1}}}_{W_1} \oplus \ldots \oplus \underbrace{V_{\mu_t} \oplus V_{\overline{\mu_t}}}_{W_t}$. 09.11.22

Что мы сейчас делаем? В каждом из подпространств существует свой ортонормированный базис, объедивнишись, они составят ортонормированный базис всего пространства, так как собственные векторы, принадлежащие разным собственным значениям, между собой ортогональны. Мы же будем строить базис только из вещественных векторов.

Пусть v – собственное значение $\mathcal{A}_{\mathbb{C}}$, $V_v = \operatorname{Ker}(\mathcal{A}_{\mathbb{C}} - v\mathscr{E}_{V_{\mathbb{C}}})$.

$W = W_l = V_{\mu_l} \oplus V_{\overline{\mu_l}}$. Выберем в V_{μ_l} какой-нибудь ортонормированный базис: $v_1 + iw_1, \ldots, v_q + iw_q \Rightarrow v_1 - iw_1, \ldots, v_q - iw_q$ – базис $V_{\overline{\mu_l}}$.

$\mu_l \neq \overline{\mu_l} \Rightarrow (v_j - iw_j) \perp (v_k + iw_k),\ j,k = 1, \ldots, q$.

$W = V_{\mu_l} + V_{\overline{\mu_l}} = \operatorname{Lin}(v_1 + iw_1, \ldots, v_q + iw_q, v_1 - iw_1, \ldots, v_q - iw_q) = \operatorname{Lin}(v_1, \ldots, v_q, w_1, \ldots, w_q)$.

$\subset$: очевидно, $\supset$: $\dim W = 2q \Rightarrow \dim \operatorname{Lin}(v_1, \ldots, v_q, w_1, \ldots, w_q) \geqslant 2q$ ($\supset W,\ \dim W = 2q$) $\Rightarrow \dim \underbrace{\operatorname{Lin}(v_1, \ldots, v_q, w_1, \ldots, w_q)}_{=W} = 2q$ (с другой сторо-

ны, $v_1 = \frac{1}{2}((v_1 + iw_1) + (v_1 - iw_1))$ и т.д.) $\Rightarrow v_1, \dots, v_q, w_1, \dots, w_q$ – базис W.

При $j \neq k$:

$$(v_j + iw_j, v_k \pm iw_k) = (v_j, v_k) \pm (w_j, w_k) + i((v_k, w_j) \mp (v_j, w_k)) = 0 \Rightarrow$$
$$\Rightarrow \begin{cases} (v_j, v_k) + (w_j, w_k) = 0 \\ (v_j, v_k) - (w_j, w_k) = 0 \\ (v_k, w_j) - (v_j, w_k) = 0 \\ (v_k, w_j) + (v_j, w_k) = 0 \end{cases} \Rightarrow \begin{cases} (v_j, v_k) = 0 \\ (w_j, w_k) = 0 \\ (v_k, w_j) = 0 \\ (v_j, w_k) = 0 \end{cases}$$

$$\begin{matrix} (v_j + iw_j, v_j + iw_j) = 1 \\ (v_j + iw_j, v_j - iw_j) = 0 \end{matrix} \Rightarrow \begin{cases} (v_j, v_j) + (w_j, w_j) + i((v_j, w_j) - (v_j, w_j)) = 1 \\ (v_j, v_j) - (w_j, w_j) + i((v_j, w_j) + (v_j, w_j)) = 0 \end{cases} \Rightarrow$$
$$\Rightarrow \begin{cases} (v_j, v_j) + (w_j, w_j) = 1 \\ (v_j, v_j) - (w_j, w_j) = 0 \\ 2(v_j, w_j) = 0 \end{cases} \Rightarrow \begin{cases} (v_j, v_j) = \frac{1}{2} \\ (w_j, w_j) = \frac{1}{2} \\ (v_j, w_j) = 0 \end{cases}$$

Таким образом, $v_1, \dots, v_q, w_1, \dots, w_q$ – ортогональный базис W; $(v_j, v_j) = (w_j, w_j) = \frac{1}{2}$.

$\widetilde{v_j} = \sqrt{2}v_j$, $\widetilde{w_j} = \sqrt{2}w_j \Rightarrow \widetilde{v_1}, \widetilde{w_1}, \dots, \widetilde{v_q}, \widetilde{w_q}$ – ортонормированный базис W.

$\underbrace{V_{\lambda_l}}_{\lambda_l \in \mathbb{R}} = \mathrm{Lin}(v_1 + iw_1, \dots, v_p + iw_p)$ для некоторых векторов $v_1, \dots, v_p, w_1, \dots, w_p$.

$$\underbrace{\mathcal{A}_{\mathbb{C}}(v_j + iw_j)}_{= \lambda_l(v_j + iw_j) = \lambda_l v_j + i\lambda_l w_j} = \mathcal{A}v_j + i\mathcal{A}w_j \Rightarrow$$
$$\Rightarrow \mathcal{A}v_j = \lambda_l v_j,\ \mathcal{A}w_j = \lambda_l w_j \Rightarrow v_j, w_j \in V_{\lambda_l} \Rightarrow$$
$$\Rightarrow V_{\lambda_l} = \mathrm{Lin}(v_1, \dots, v_p, w_1, \dots, w_p)\ (\subset\text{: очевидно}, \supset\text{: т.к. } v_j, w_j \in V_{\lambda_l})$$

Выбрав из $v_1, \dots, v_p, w_1, \dots, w_p$ базис V_{λ_l} и применив к нему процесс ортогонализации Грамма-Шмидта, получим ортонормированный базис V_{λ_l} из вещественных векторов. Объединив базисы все V_{λ_l} и W_l, получим ортонормированный вещественный базис $V_{\mathbb{C}}$. $V_{\lambda_l} \perp V_{\lambda_k}$ $(k \neq l)$, $W_l \perp W_k$ $(k \neq l)$, $W_l \perp V_{\lambda_k}$.

Его элементы – ЛНС в $V_{\mathbb{C}} \Rightarrow$ ЛНС в $V \Rightarrow$ базис V, т.к. количество векторов $= \dim V_{\mathbb{C}} = \dim V$.

Теперь посмотрим на матрицу оператора в найденном базисе.

$$v \in V_{\lambda_l} \Rightarrow \underbrace{\mathcal{A}_{\mathbb{C}} v}_{\mathcal{A}v} = \lambda_l(v + i0) = \lambda_l v$$

$$\begin{pmatrix} \lambda_l & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_l \end{pmatrix} = \operatorname{diag}(\underbrace{\lambda_l, \dots, \lambda_l}_{p}) \text{ – соответствует } V_{\lambda_l}$$

$$W = V_{\mu_l} \oplus V_{\overline{\mu_l}},\ \widetilde{v_1}, \widetilde{w_1}, \dots, \widetilde{v_q}, \widetilde{w_q}$$
$$\mathcal{A}_{\mathbb{C}}(v_j + iw_j) = \mu_l(v_j + iw_j)$$
$$\mu_l = \alpha + i\beta,\ \alpha, \beta \in \mathbb{R},\ \beta \neq 0$$
$$\mathcal{A}v_j + i\mathcal{A}w_j = \alpha v_j - \beta w_j + i(\alpha w_j + \beta v_j) \Rightarrow \begin{cases} \mathcal{A}v_j = \alpha v_j - \beta w_j \\ \mathcal{A}w_j = \alpha w_j + \beta v_j \end{cases} \Rightarrow$$
$$\Rightarrow \begin{cases} \mathcal{A}\widetilde{v_j} = \alpha\widetilde{v_j} - \beta\widetilde{w_j} \\ \mathcal{A}\widetilde{w_j} = \alpha\widetilde{w_j} + \beta\widetilde{v_j} \end{cases} \quad \begin{pmatrix} & & \vdots & \vdots & \\ \dots & \dots & \alpha & \beta & \dots \\ \dots & \dots & -\beta & \alpha & \dots \\ & & \vdots & \vdots & \end{pmatrix}$$

Теорема 14.1 (Спектральная теорема для нормальных операторов в евклидовом пространстве)**.** V – евклидово, $\mathcal{A} \in \operatorname{End} V$ – нормальный. Тогда в V есть ортонормированный базис E, т.ч. $[\mathcal{A}]_E$ – блочно-диагональная матрица с блоками $1 \times 1,\ 2 \times 2$ вида $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix}$ (оператор = самосопряж. + кососим.)

$\mathcal{A}$ называется ортогональным, если $\mathcal{A}\mathcal{A}^* = \mathscr{E} = E_n \Leftrightarrow A = [\mathcal{A}]_E \in O_n$, где E – ортонормированный базис V.

$$A = \operatorname{diag}(\dots, \lambda, \dots, \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}, \dots)$$
$$A^T = \operatorname{diag}(\dots, \lambda, \dots, \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}, \dots)$$
$$AA^T = \operatorname{diag}(\dots, \lambda^2, \dots, \begin{pmatrix} \alpha^2 + \beta^2 & 0 \\ 0 & \alpha^2 + \beta^2 \end{pmatrix}, \dots)$$
$$A \in O_n \Leftrightarrow \text{ все } \lambda^2 = 1 \text{ и все } \alpha^2 + \beta^2 = 1$$

$R_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$ (матрица поворота плоскости), φ, т.ч. $\beta = -\sin\varphi,\ -\beta = \sin\varphi$.

Следствие 14.1.1. Пусть $\mathcal{A} \in \operatorname{End} V$ – ортогональный. Тогда в V существует ортонормированный базис E, т.ч. $[\mathcal{A}]_E = \operatorname{diag}(R_{\varphi_1}, \dots, R_{\varphi_t}, \pm 1, \dots, \pm 1)$.

Следствие 14.1.2 (Теорема Эйлера)**.** Пусть V – трехмерное евклидово пространство, $\mathcal{A} \in \operatorname{End} V$ – ортогональный. Тогда в некотором ортонормированном базисе его матрица имеет вид $\begin{pmatrix} & & 0 \\ & R_\varphi & \vdots \\ & & 0 \\ 0 & \dots 0 & \pm 1 \end{pmatrix}$.

$\dim V$ нечетный: $[\mathcal{A}]_E = \operatorname{diag}(R_{\varphi_1}, \dots, R_{\varphi_s}, \pm 1)$
$\dim V$ четный, $|\mathcal{A}| = 1$: $[\mathcal{A}]_E = \operatorname{diag}(R_{\varphi_1}, \dots, R_{\varphi_s})$
$\dim V$ четный, $|\mathcal{A}| = -1$: $[\mathcal{A}]_E = \operatorname{diag}(R_{\varphi_1}, \dots, R_{\varphi_s}, 1, -1)$

Глава 15

Самосопряженные операторы

Предложение 15.1. Пусть V – евклидово или унитарное пространство, $\mathcal{A} \in \operatorname{End} V$. Тогда $\mathcal{A} = \mathcal{A}^* \Leftrightarrow$ в V существует ортонормированный базис E, такой что $[\mathcal{A}]_E = \operatorname{diag}(\alpha_1, \dots, \alpha_n),\ \alpha_1, \dots, \alpha_n \in \mathbb{R}$.

Доказательство. $\Leftarrow$:

$$\begin{array}{ccc} [\mathcal{A}]_E^* & = & [\mathcal{A}]_E \\ \| & & \\ [\mathcal{A}^*]_E & \Longrightarrow & \mathcal{A}^* = \mathcal{A} \end{array}$$

$\Rightarrow$: для унитарных доказано ранее.

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}^T = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} \Rightarrow \beta = 0$$

■

16.11.22

Далее V – евклидово пространство.
Пусть $\mathcal{A} \in \operatorname{End} V,\ \mathcal{A} = \mathcal{A}^*$. $V \times V \xrightarrow[(v,w)\mapsto(\mathcal{A}v,w)]{\mathcal{B}} \mathbb{R}$.

Предложение 15.2. $\mathcal{B}$ – симметрическая билинейная форма.

Доказательство. 1. биленейность очевидна.

2. $\mathcal{B}(w,v) = (\mathcal{A}w, v) = (w, \mathcal{A}^*v) = (w, \mathcal{A}v) = (\mathcal{A}v, w) = \mathcal{B}(v,w)$

■

Замечание. Для любой симметрической билинийной формы $\mathcal{B}$ на V существует единственный $\mathcal{A} \in \operatorname{End} V,\ \mathcal{A} = \mathcal{A}^*$, т.ч. $\mathcal{B}(v,w) = (\mathcal{A}v, w)$.

упражнение

если E – ортонормированный базис V, то $[\mathcal{A}]_E = [\mathcal{B}]_E$

упражнение

Пусть V – евклидово пространство, $\mathcal{A} \in \operatorname{End} V$ – самосопряженный. $\mathcal{A}$ называется положительно определенным, если $\forall v \in V,\ v \neq 0 :$ $(\mathcal{A}v, v) > 0$. 16.11.22

Предложение 15.3. Следующие 2 условия эквивалентны:

1. $\mathcal{A}$ положительно определенный.
2. В V существует ортонормированный базис E, такой что $[\mathcal{A}]_E = \operatorname{diag}(\lambda_1, \dots, \lambda_n),\ \lambda_i > 0,\ i = 1, \dots, n$.

Доказательство. $1 \Rightarrow 2$: существует ортонормированный E, такой что $[\mathcal{A}]_E = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. $\mathcal{A}e_i = \lambda_i e_i$. $\underbrace{(\mathcal{A}e_i, e_i)}_{>0} = (\lambda_i e_i, e_i) = \lambda_i(e_i, e_i) = \lambda_i$.
$2 \Rightarrow 1$: $v = \alpha_1 e_1 + \dots + \alpha_n e_n,\ \exists i :\ \alpha_i \neq 0$. $\mathcal{A}v = \alpha_1\lambda_1 e_1 + \dots + \alpha_n\lambda_n e_n$.
$(\mathcal{A}v, v) = \alpha_1^2\lambda_1 + \dots + \alpha_n^2\lambda_n > 0$. ■

Предложение 15.4. Пусть $\mathcal{A}$ – положительно определенный на V. Тогда существует единственный $\mathcal{B} \in \operatorname{End} V$, такой что $\mathcal{A} = \mathcal{B}^2$ и $\mathcal{B}$ – положительно определенный.

Доказательство. Существование: есть ортонормированный базис E: $[\mathcal{A}]_E = \operatorname{diag}(\lambda_1, \dots, \lambda_n),\ \lambda_i \geqslant 0$. $\mathcal{B}(e_i) = \sqrt{\lambda_i} e_i$. $[\mathcal{B}]_E = \operatorname{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}) = B$. $B^* = B \Rightarrow \mathcal{B} = \mathcal{B}^*;\ \mathcal{B}^2 = \mathcal{A}$.
Единственность: пусть $\mathcal{B}_1 = \mathcal{B}_1^*,\ \mathcal{B}_1^*$ положительно определен,

$\mathcal{B}_1^2 = \mathcal{A}$. Существует ортонормированный F, $[\mathcal{B}_1]_F$ – диагональная. Пусть $\mu_1, \dots, \mu_k$ – все собственные значения $\mathcal{B}_1$, $g_{\mathcal{B}_1\mu_1}, \dots, g_{\mathcal{B}_1\mu_k}$ – их геометричсекие кратности.

$$g_{\mathcal{B}_1\mu_1} + \dots + g_{\mathcal{B}_1\mu_k} = n = \dim V$$
$$V_{\mathcal{B}_1\mu_j} = \operatorname{Ker}(\mathcal{B}_1 - \mu_j\mathscr{E})$$
$$\mathcal{B}_1|_{V_{\mathcal{B}_1\mu_j}} = \mu_j\mathscr{E}|_{\dots}$$
$$\Rightarrow \mathcal{B}_1^2|_{V_{\mathcal{B}_1\mu_j}} = \mu_j^2\mathscr{E}|_{\dots}$$
$$\Rightarrow \mathcal{A}|_{V_{\mathcal{B}_1\mu_j}} = \mu_j^2\mathscr{E}|_{\dots}$$
$$\Rightarrow V_{\mathcal{B}_1\mu_j} \subset V_{\mathcal{A}\mu_j^2}$$
$$g_{\mathcal{B}_1\mu_j} \leqslant g_{\mathcal{A}\mu_j^2}$$
$$n = g_{\mathcal{B}_1\mu_1} + \dots + g_{\mathcal{B}_1\mu_k} \leqslant g_{\mathcal{A}\mu_1} + \dots + g_{\mathcal{A}\mu_k} \leqslant n$$

$\Rightarrow g_{\mathcal{B}_1\mu_j} = g_{\mathcal{A}\mu_j^2}$ и из $\mathcal{A}$ нет собственных значений, кроме $\mu_1^2, \dots, \mu_k^2$

Таким образом, $V_{\mathcal{B}_1\mu_j} = V_{\mathcal{A}_1\mu_j^2} \Rightarrow$

$\Rightarrow (\mathcal{A}e = \lambda e \Rightarrow \mathcal{B}_1 e = \sqrt{\lambda}e)$. В частности, $\mathcal{B}_1 e_i = \sqrt{\lambda_i}e_i = \mathcal{B}e_i$

■

Теорема 15.5 (Полярное разложение)**.** Пусть V – евклидово, $\mathcal{A} \in \mathrm{GL}(V)$. Тогда существуют единственные $\mathcal{C}, \mathcal{O} \in \operatorname{End} V$, такие что $\mathcal{C}$ – положительно определенный, $\mathcal{O}$ ортогональный и $\mathcal{A} = \mathcal{C}\mathcal{O}$.

$\mathcal{A} \in \mathrm{GL}(V) \Rightarrow \mathcal{A}^* \in \mathrm{GL}(V)$ $(\mathcal{A}\mathcal{B} = \mathscr{E} \Rightarrow \mathcal{B}^*\mathcal{A}^* = \mathscr{E})$

Доказательство. $(\mathcal{A}\mathcal{A}^*)^* = (\mathcal{A}^*)^*\mathcal{A}^* = \mathcal{A}\mathcal{A}^*$. $\mathcal{A}\mathcal{A}^*$ положительно определенный: $v \neq 0$, $(\mathcal{A}\mathcal{A}^*v, v) = (\underbrace{\mathcal{A}^*v}_{\neq 0}, \mathcal{A}^*v) > 0 \Rightarrow \mathcal{A}\mathcal{A}^* = \mathcal{C}^2$, $\mathcal{C} \in \operatorname{End} V$ – положительно определенный.
$\mathcal{O} = \mathcal{C}^{-1}\mathcal{A}$, $\mathcal{A} = \mathcal{C}\mathcal{O}$.
$\mathcal{C}^2 = \mathcal{A}\mathcal{A}^* = \mathcal{C}\mathcal{O}\mathcal{O}^*\mathcal{C}^* = \mathcal{C}\mathcal{O}\mathcal{O}^*\mathcal{C} \Rightarrow \mathscr{E} = \mathcal{O}\mathcal{O}^*$.
$\mathcal{A} = \mathcal{C}_1\mathcal{O}_1 = \mathcal{C}_2\mathcal{O}_2$
$\mathcal{C}_1, \mathcal{C}_2$ – полож. опред., $\mathcal{O}_1, \mathcal{O}_2$ – ортог.
$\mathcal{A}\mathcal{A}^* = \mathcal{C}_1\mathcal{O}_1\mathcal{O}_1^*\mathcal{C}_1 = \mathcal{C}_1^2$.
$\mathcal{A}\mathcal{A}^* = \mathcal{C}_2\underbrace{\mathcal{O}_2\mathcal{O}_2^*}_{=\mathscr{E}}\mathcal{C}_2 = \mathcal{C}_2^2$.
По предыдущему предложению: $\mathcal{C}_1 = \mathcal{C}_2$, $\mathcal{O}_1 = \mathcal{O}_2$. ■

Часть III

Элементы теории полей

Глава 16

Факторкольца и гомоморфизмы колец

R – коммутативное (ассоциативность подразумевается) кольцо с 1.

$I \subset R$ называется идеалом, если I – подгруппа R относительно сложения и $RI \subset I$.

$(a) = \{ax \mid x \in R\}$

$R = (1),\ 0 = (0)$.

Предложение 16.1. R – поле $\Leftrightarrow$ в R ровно 2 идеала.

Доказательство. $\Rightarrow$: $\underbrace{(1)}_{1\in} \neq \underbrace{(0)}_{1\in}$, т.к. $1 \neq 0$. Пусть I – идеал в R, $I \neq 0 \Rightarrow \exists c \in I\backslash\{0\} \Rightarrow 1 = cc^{-1} \Rightarrow 1 \in I \Rightarrow I = R$ $(r = r \cdot 1)$.
$\Leftarrow$: если $0 = 1$, $r = r \cdot 1 = r \cdot 0 = 0 \Leftarrow$ нет двух идеалов.
Проверим обратимость: $c \in R\backslash\{0\},\ (c) \neq 0 \Rightarrow (c) = R \Rightarrow 1 \in (c) \Rightarrow c \in R^*$. ■

Пусть R – коммутативное кольцо, I – идеал в R.

Рассмотрим факторгруппу R/I и введем на ней умножение: $(R/I) \times (R/I) \to R/I$.
$(a+I, b+I) \mapsto ab+I$

Проверка корректности:

$$\left.\begin{array}{l} a+I=a'+I \\ b+I=b'+I \end{array}\right\} \Rightarrow ab+I=a'b'+I$$

$$\left.\begin{array}{l} a'=a+s,\ s\in I \\ b'=b+s,\ t\in I \\ a'b'=ab+\underset{\in I}{\underbrace{at}}+\underset{\in I}{\underbrace{bs}}+\underset{\in I}{\underbrace{st}} \Rightarrow a'b'-ab\in I \end{array}\right\} \Rightarrow a'b'+I=ab+I$$

Предложение 16.2. $(R/I,+,\cdot)$ – коммутативное кольцо с 1.

Доказательство. Непосредственная проверка. ■

Теорема 16.3. Пусть R – ОГИ, $a\in R$. Тогда $R/(a)$ – поле $\Leftrightarrow$ a неприводимый.

Замечание. $R/(a)$ поле $\Leftrightarrow \forall b\in R,\ a\notin R^*$: $b\notin(a)\Rightarrow \exists c\in R:\ \overline{b}\overline{c}=\overline{1}$ $(\overline{b}=b+(a))\Leftrightarrow \forall b\in R:\ a\nmid b\Rightarrow \exists c\in R:\ bc=1+ax,\ x\in R$.

Доказательство. Антипрямо: пусть a неприводим. Тогда $a\nmid b\Rightarrow (a,b)=1\Rightarrow ax+by=1$ для некоторых $x,\ y\in R\Rightarrow by=1-ax$. Таким образом, $R/(a)$ – поле.
Антиобратно, $R/(a)$ – поле $\Rightarrow R/(a)\neq 0$, т.е. $a\notin R^*$ и $1=bc-ax$, т.е. $a\nmid b\Rightarrow (a,b)=1\Rightarrow a$ – неприводим. ■

Пример 16.1. 1. $\mathbb{R}[x]/(x^2+1)=\mathbb{C}$

2. $\mathbb{F}_2=\mathbb{Z}/(2)$, $\mathbb{F}_2[x]/(x^2+x+1)=\{0,1,\overline{x},1+\overline{x}\}=\mathbb{F}_4$

Определение 16.1 (Гомоморфизм)**.** Пусть $R,\ S$ – кольца с 1. $\varphi: R\to S$ называется гоморфизмом, если:

1. $\varphi(a+b)=\varphi(a)+\varphi(b),\ \forall a,\ b\in R$
2. $\varphi(ab)=\varphi(a)\varphi(b),\ \forall a,\ b\in R$
3. $\varphi(1_R)=1_S$

Пример 16.2. $\underset{a\mapsto a+I}{R\to R/I}$

Теорема 16.4 (О гомоморфизме для колец)**.** Пусть $\varphi : R \to S$ – гомоморфизм колец. Тогда:

1. $\operatorname{Ker}\varphi$ – идеал в R.
2. $\operatorname{Im}\varphi$ – подкольцо в S.
3. Существует изоморфизм: $\overline{\varphi} = R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$.
$$a+\operatorname{Ker}\varphi \mapsto \varphi(a)$$

Доказательство. 1. $\operatorname{Ker}\varphi$ – подгруппа R. Пусть $a \in \operatorname{Ker}\varphi$, $r \in R \Rightarrow \varphi(ra) = \varphi(r)\underbrace{\varphi(a)}_{0} = 0 \Rightarrow ra \in \operatorname{Ker}\varphi$.

2. $a',\ b' \in \operatorname{Im}\varphi \Rightarrow a' = \varphi(a),\ b' = \varphi(b)$
$a' - b' = \varphi(a) - \varphi(b) = \varphi(a-b) \in \operatorname{Im}\varphi$
$a'b' = \varphi(a)\varphi(b) = \varphi(ab)$
$1_S = \varphi(1_R) \in \operatorname{Im}\varphi$

3. Из ТГ знаем:

   a) $\overline{\varphi}$ определено корректно.

   b) $\overline{\varphi}$ – изоморфизм групп.

   $\overline{\varphi}((a + \operatorname{Ker}\varphi)(b + \operatorname{Ker}\varphi)) = \overline{\varphi}(ab + \operatorname{Ker}\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a + \operatorname{Ker}\varphi)\overline{\varphi}(b + \operatorname{Ker}\varphi)$
   $\overline{\varphi}(1_{R/\operatorname{Ker}\varphi}) = \varphi(1_R) = 1_S = 1_{\operatorname{Im}\varphi}$

■

Глава 17

Простые поля

23.11.22

Определение 17.1 (Подполе)**.** Пусть K – поле. Подполем K называется подкольцо $F \subset K$, такое что F – поле.

Определение 17.2 (Простое поле)**.** Поле K называется простым, если в нем нет собственных подполей

Пример 17.1. $\mathbb{Q}$ – простое поле.

Пусть $F \subset \mathbb{Q}$ – подполе. $1 \in F \Rightarrow \mathbb{N} \subset F \Rightarrow \mathbb{Z} \subset F \Rightarrow \forall n \in \mathbb{N} : n^{-1} \in F \Rightarrow F = \mathbb{Q}$.

Пример 17.2. Пусть p – простое. Тогда $\mathbb{F}_p = \underbrace{\mathbb{Z}/(p)}_{\mathbb{Z}/p\mathbb{Z}}$ – простое поле.

$F \subset \mathbb{F}_p$ – подполе. $1 \in F \Rightarrow \quad \forall k \in \mathbb{N} : \underbrace{1 + ... + 1}_{k} \in F \Rightarrow F = \mathbb{F}_p$

$(1 = \overline{1},\ 2 := 1 + 1$ и т. д.)

Определение 17.3 (Характеристика кольца)**.** R – кольцо с единицей.

$$\operatorname{char} R = \begin{cases} \min\{n : \underbrace{1 + ... + 1}_{n} = 0 \text{ в } R\} \\ 0, \quad \text{если } \forall n \in \mathbb{N} : \underbrace{1 + ... + 1}_{n} \neq 0 \end{cases}$$

Лемма 17.1. Пусть F – поле. Тогда $\operatorname{char} F$ является простым числом или $= 0$.

Доказательство. Будем доказывать от противного. Пусть $l = \operatorname{char} F = mn,\ m,\ n > 1$. $0 = \underbrace{1 + ... + 1}_{l} = \underbrace{(1 + ... + 1)}_{\substack{m \\ \neq 0,\ \text{т.к. } m<l}} \underbrace{(1 + ... + 1)}_{\substack{n \\ \neq 0,\ \text{т.к. } n<l}}$ – невозможно в поле. ■

Предложение 17.2. Пусть F_1, F_2 – поля, $\alpha : F_1 \to F_2$ – гомоморфизм. Тогда α отображает F_1 изоморфно на подполе $\alpha(F_1)$ (индуцирует изоморфизм на свой образ).

Доказательство.

$$\operatorname{Ker}\alpha \text{ – идеал в } F_1$$

$$\Rightarrow \left[\begin{array}{c} \operatorname{Ker}\alpha = 0 \\ \operatorname{Ker}\alpha = F_1 \Rightarrow \underbrace{\alpha(1)}_{=1} = 0 \neq 1 \text{ - не реализуется} \end{array}\right.$$

$$\Rightarrow \alpha \text{ инъективно}$$

$$\Rightarrow \alpha \text{ индуцирует изоморфизм } F_1 \xrightarrow{\sim} \alpha(F_1)$$

$$F_1 \text{ поле } \Rightarrow \alpha(F_1) \text{ поле}$$

■

Термин гоморфизм полей не используется, так как он всегда инъективен, говорят «вложение».

Теорема 17.3. Пусть F – простое поле.

1. Если $\operatorname{char} F = 0$, то $F \cong \mathbb{Q}$.
2. Если $\operatorname{char} F = p > 0$, то $F \cong \mathbb{F}_p$.

Доказательство. 1. Будем строить $\alpha : \mathbb{Q} \to F$.

$$\begin{gathered} n \in \mathbb{N} \quad \alpha(n) := \underbrace{1 + ... 1}_{n} \text{ в } F \\ \alpha(0) := 0 \\ \alpha(-n) := -\underbrace{(1 + ... + 1)}_{n} \end{gathered} \qquad (*)$$

$\alpha\left(\frac{a}{b}\right) := \frac{\alpha(a)}{\alpha(b)}$, $\alpha(b) \neq 0$, т.е. $\alpha(b) = \underbrace{1 + ... + 1}_{b} \neq 0$, т.к. $\operatorname{char} F = 0$

Проверка корректности:

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b$$
$$\Rightarrow \underbrace{\alpha(ab')}_{=\alpha(a)\alpha(b')\neq 0} = \underbrace{\alpha(a'b)}_{=\alpha(a')\alpha(b)\neq 0}$$
$$\Rightarrow \frac{\alpha(a)}{\alpha(b)} = \frac{\alpha(a')}{\alpha(b')}$$

Непосредственно проверяется, что α – гомоморфизм.

$$\Rightarrow \alpha(\mathbb{Q}) \text{ – подполе } F, \text{ изоморфное } \mathbb{Q}$$
$$\Rightarrow \alpha(\mathbb{Q}) = F$$
$$\Rightarrow F \cong \mathbb{Q}$$

2. $\mathbb{Z} \xrightarrow{\alpha} F$. Зададим α формулами $(*)$. Легко видеть: α – гомоморфизм. $\operatorname{Ker}\alpha$ – идеал в $\mathbb{Z}$.

$$\operatorname{char} F = p \Rightarrow \begin{cases} p \in \operatorname{Ker}\alpha \\ 1, ..., p-1 \notin \operatorname{Ker}\alpha \end{cases} \Rightarrow \operatorname{Ker}\alpha = (p)$$

По теореме о гомоморфизме α – индуцированный изоморфизм. $\overline{\alpha}: \mathbb{Z}/(p) \xrightarrow{\sim} \operatorname{Im}\alpha$, p – простое $\Rightarrow \mathbb{Z}/(p)$ – поле $\Rightarrow \operatorname{Im}\alpha$ – поле $\Rightarrow \operatorname{Im}\alpha = F \Rightarrow \overline{\alpha}: \mathbb{F}_p \xrightarrow{\sim} F$.

■

Предложение 17.4. Пусть K – поле. Тогда в K содержится единственное простое подполе.

Доказательство. $F_0 := \bigcap_{F - \text{подполе } K} F$ – подполе K. $F_1 \subset F_0$– подполе $\Rightarrow F_1$– подполе $K \Rightarrow F_0 \subset F_1 \Rightarrow F_1 = F_0$.
F_0' – еще одно простое подполе $\Rightarrow F_0 \subset F_0' \Rightarrow F_0' = F_0$. ■

Глава 18

Расширения полей

Определение 18.1. Говорят, что задано расширение поля L/K (читается L над K), если задано поле L и подполе K.

Пример 18.1. 1. $\mathbb{C}/\mathbb{R}$

2. $\mathbb{R}/\mathbb{Q}$

3. K/K для любого K

4. $K(X)/K$ для любого K

Если L/K – расширение, то L можно рассматривать как линейное пространство над K. L/K называется конечным расширением, если $\dim_K L < \infty$. $[L : K] = \dim_K L$ – степень расширения L/K. В противном случае L/K называются бесконечным.

Пример 18.2. 1. $[\mathbb{C} : \mathbb{R}] = 2$

2. $[\mathbb{R} : \mathbb{Q}] = \infty$

3. $[K : K] = 1$

4. $[K(X) : K] = \infty$

Предложение 18.1. Пусть $L/K, M/L$ – конечные расширения. Тогда M/K – тоже конечное расширение и $[M : K] = [M : L] \cdot [L : K]$. $M/L/K$ – башня полей.

Доказательство. Пусть $e_1, \dots, e_l$ – базис L как линейного пространстнства $/K$. $f_1, \dots, f_n$ – базис M как линейного пространства $/L$. Проверим, $(e_i f_j \mid 1 \leqslant i \leqslant l, 1 \leqslant j \leqslant m)$ – базис M/K. Пусть $c \in M \Rightarrow c = b_1 f_1 + \dots + b_m f_m,\ b_1, \dots, b_m \in L \Rightarrow c = (a_{11}e_1 + \dots + a_{1l}e_l)f_1 + \dots + (a_{m1}e_1 + \dots + a_{ml}e_l)f_m =$
$= \sum_{i=1}^{m} \sum_{j=1}^{l} a_{ij} e_j f_i,\ a_{ij} \in K \Rightarrow \mathrm{Lin}(e_j f_i \mid 1 \leqslant j \leqslant l, 1 \leqslant i \leqslant m) = M.$
Пусть $\sum_{i,j} a_{ij} e_i f_j = 0 = \sum_j \left(\underbrace{\sum_i a_{ij} e_i}_{\in L} \right) \cdot f_j,\ f_1, \dots, f_m$ – базис M/L
$\Rightarrow \sum_i a_{ij} e_i = 0,\ j = 1, \dots, m,\ e_1, \dots, e_l$ – базис $L/K \Rightarrow$ все $a_{ij} = 0$. ■

Определение 18.2 (Алгебраический элемент)**.** Пусть L/K – расширение, $a \in L$. a называется алгебраическим над K, если существует $f \in K[X],\ f \neq 0$, такой что $f(a) = 0$. В противном случае, a называется трансцендентным $/K$.

Пример 18.3. $\sqrt{2}$ алгебраичен над $\mathbb{Q},\ f = X^2 - 2$

L/K называется алгебраическим, если все его элементы алгебраичны $/K$. В противном случае, L/K называется трансцендентным.

Пример 18.4.

1. $\mathbb{C}/\mathbb{R}$ – алгебраическое.
2. $\mathbb{R}/\mathbb{Q}$ – трансцендентное, например, π – трансцендентное над $\mathbb{Q}$. Без примера: рациональных чисел счетное множество и многочленов с рациональными коэффициентами тоже. У каждого многочлена конечное число корней. Таким образом, алгебраические числа (в $\mathbb{R}$) образуют счетное множество. Однако $\mathbb{R}$ несчетно.
3. $K(X)/K$ – трансцендентное, X – трансцендентный, $f(X) = \frac{f(X)}{1}$.

Предложение 18.2. Любое конечное расширение поля – алгебраично.

Доказательство. Пусть $[L : K] = d$.

$$a \in L,\ \underbrace{1, a, a^2, \dots, a^d}_{d+1}$$
$$\Rightarrow \exists b_0, b_1, \dots, b_d \in K : b_0 + b_1 a + \dots b_d a^d = 0 \text{ и не все } b_i = 0$$
$$f := b_d X^d + \dots + b_1 X + b_0 \neq 0$$
$$f(a) = 0 \Rightarrow a \text{ – алгебраическое}$$

■

Предложение 18.3. Пусть L/K расширение, $a \in L$ – алгебрический. Тогда $\{f \in K[X] \mid f(a) = 0\} = (p),\ p$ – неприводимый многочлен из $K[X]$.

Доказательство. $I = \{f \in K[X] | f(a) = 0\}$ – подгруппа в $K[X]$.

$$\begin{matrix} f \in I \\ g \in K[X] \end{matrix} \Rightarrow (gf)(a) = g(a) \underbrace{f(a)}_{0} = 0 \Rightarrow gf \in I$$

Таким образом, I – идеал $\Rightarrow I = (p)$ в $K[X]$.
Проверим, что p – неприводимый.

$$p = fg,\ p(a) = 0 \Rightarrow f(a)g(a) = 0 \Rightarrow \left[\begin{matrix} f(a) = 0 \\ g(a) = 0 \end{matrix}\right.$$
$$\Rightarrow \left[\begin{matrix} f \in I = (p) \\ g \in I = (p) \end{matrix}\right. \Rightarrow \left[\begin{matrix} f \sim p \\ g \sim p \end{matrix}\right.$$

■

Такой многочлен p будем обозначать $\operatorname{Irr}_K a$. Например $\operatorname{Irr}_{\mathbb{R}} i = x^2+1$.

Определение 18.3. Пусть L/K; $\quad a_1, \dots, a_m \in L$. $K(a_1, \dots, a_m) := \bigcap_{\substack{F \text{ подполе } L \\ K \subset F \\ a_1, \dots, a_m \in F}} F$ – подполе L. Назовем его расширением K, порожденным $a_1, \dots, a_m$.

Определение 18.4. Пусть L/K – расширение, если $\exists\ a_1, \dots, a_m \in L$, т.ч. $K(a_1, \dots, a_m) = L$, то L/K называется конечно порожденным.

Предложение 18.4. Пусть L/K – конечное расширение, тогда L/K конечно порожденное.

Доказательство. $e_1, \dots, e_n$ – базис L/K. $a_1e_1 + \dots + a_ne_n \in K(e_1, \dots, e_n) \Rightarrow K(e_1, \dots, e_n) = L$. ■

Замечание. Обратное неверно. $K(X)/K$ – порождается одним элементом (x), но не конечное, так как трансцендентное.

Определение 18.5 (Простое расширение)**.** L/K называется простым, если $\exists\ a \in L$, т.ч. $L = K(a)$.

Предложение 18.5. Пусть L/K – простое алгебраическое расширение, то есть $L = K(a)$, a – алгебраический над K. Тогда $L \cong K[X]/(p)$, где $p = \operatorname{Irr}_K a$.

Доказательство.

$$K[X] \xrightarrow[f \mapsto f(a)]{\alpha} L$$

$$\operatorname{Ker}\alpha = (p)$$

$$\left.\begin{array}{c} \Rightarrow \operatorname{Im}\alpha \cong K[X]/(p),\ p \text{ – неприводимый} \Rightarrow \operatorname{Im}\alpha \text{ – поле} \\ K \subset \operatorname{Im}\alpha, \text{ т.к. } \alpha(c) = c\ (c \in K) \\ a \in \operatorname{Im}\alpha \text{ т.к. } \alpha(X) = a \end{array}\right\} \Rightarrow$$

$$\Rightarrow \operatorname{Im}\alpha \supset K(a) = L$$

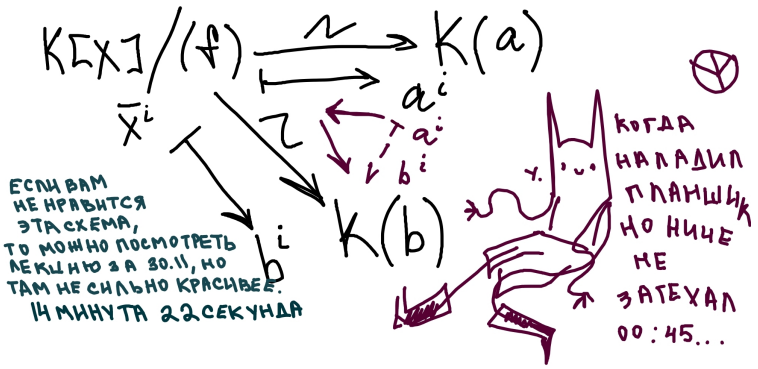
Таким образом, $L \cong K(X)/(p)$. ■

30.11.22

Следствие 18.5.1. 1. Если f – минимальный многочлен a, $\deg f = d$, то $[K(a) : K] = d$, и базисом $K(a)$, как линейного пространства над K, служит семейство $1, a, a^2, \dots, a^{d-1}$.

2. Если есть еще одно расширение $K(b)/K$, и минимальный многочлен b также f, то существует изоморфизм $K(a) \to K(b) \quad (\alpha_i \in K)$.
$\sum_{i=0}^{d-1} \alpha_i a^i \mapsto \sum_{i=0}^{d-1} \alpha_i b^i$

Доказательство. 1. Есть изоморфизм $K[X]/(f) \xrightarrow{\sim} K(a)$ – изоморфизм полей и линейных пространств $/K$. Рассмотрим первое пространство: $K[X]/(f) = \{\overline{\alpha_0 + \alpha_1 X + \dots + \alpha_{d-1} X^{d-1}} \mid \alpha_0, \dots, \alpha_{d-1} \in K\} = \{\alpha_0 \overline{1} + \alpha_1 \overline{X} + \dots + \alpha_{d-1} \overline{X^{d-1}} \mid \alpha_0, \dots, \alpha_{d-1} \in K\}$. Очевидно, $\overline{1}, \overline{X}, \dots, \overline{X^{d-1}}$ – линейно независимые ($\alpha_0 + \alpha_1 X + \dots + \alpha_{d-1} X^{d-1} \not\equiv 0 \mod f$, если $\exists\, i : \alpha_i \neq 0$). Таким образом, $\overline{1}, \overline{X}, \dots, \overline{X^{d-1}}$ – базис $K[X]/(f)$ $\Rightarrow 1, a, a^2, \dots, a^{d-1}$ – базис $K(a)$.



2.

■

Предложение 18.6. Пусть $f \in K[X]$ – неприводимый. Тогда существует расширение $K(a)/K$, такое что $\mathrm{Irr}_K(a) = f$.

Доказательство. $L = K[X]/(f)$ – поле, так как f неприводим. $K \underset{c \mapsto \overline{c}}{\hookrightarrow} L$ отожествляет c с $\overline{c}$. Очевидно, $L = K(\underbrace{\overline{X}}_{a:=})$, любой эле-

мент этого поля представим в виде $\overline{\sum \alpha_i x^i} = \sum \overline{\alpha_i}\overline{X^i} = \sum \alpha_i \overline{X^i}$. $\operatorname{Irr}_K X = f$, так как $f(\overline{x}) = \overline{f} = 0$ и f неприводим. ■

Предложение 18.7. Пусть a трансцендентен над K. Тогда $K(a) \cong K(X)$.

Доказательство.

$$K(X) \xrightarrow{\mathscr{E}} K(a)$$
$$\underbrace{\frac{f}{g}}_{g \neq 0} \mapsto \underbrace{\frac{f(a)}{g(a)}}_{g(a) \neq 0, \text{ т.к. } a \text{ тр.}}$$
$$\operatorname{Im}\mathscr{E} \text{ – подполе в } K(a)$$
$$K \subset \operatorname{Im}\mathscr{E} \ (c = \mathscr{E}(c))$$
$$a \in \operatorname{Im}\mathscr{E} \ (a = \mathscr{E}(X))$$
$$\Rightarrow \operatorname{Im}\mathscr{E} = K(a)$$

■

Пример 18.5. Пусть $K = \mathbb{F}_2,\ f = x^2 + x + 1,\ L = \mathbb{F}_2(a)$, где a – корень f. Составим таблицы сложения и умножения:

$+$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\cdot$	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	$1+a$	1
$1+a$	0	$1+a$	1	a

Определение 18.6. Расширение L поля K называется полем разложения многочлена $f \in K[X]$, если:

1. В $L[X]$ f раскладывается на линейные множители.
2. $L = K(a_1, \ldots, a_m),\ a_1, \ldots, a_m$ – все корни f в L.

Пример 18.6.

1. $\mathbb{C}/\mathbb{R}$ – поле разложения $X^2 + 1$.
2. $K = \mathbb{Q}(\sqrt[4]{2})$ – не поле разложения $X^4 - 2$ над $\mathbb{Q}$. В $K[X]$ $X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$.
3. $K' = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ – поле разложения $X^4 - 2$ над $\mathbb{Q}$.

Предложение 18.8. Пусть K поле, $f \in K[X]$. Тогда у f существует поле разложения над K.

Доказательство. Индукция по $d = \deg f$.
$d \leqslant 1$: K – поле разложения f.
$d > 1$: p – неприводимый делитель f. $L = K(a),\ p(a) = 0$. $f(a) = 0 \xrightarrow{\text{т. Безу}} f = (X-a)g$. $g \in L[X],\ \deg g = d-1$.
По индукционному предположению существует M/L – поле разложения g. В $M[X]$ $g = c(X-a_1)\dots(X-a_{d-1}) \Rightarrow f = c(X-a)(X-a_1)\dots(X-a_{d-1})$. $M = L(a_1,\dots,a_{d-1}) = K(a)(a_1,\dots,a_{d-1}) = K(a,a_1,\dots,a_{d-1})$. ■

Изоморфизмом между расширениями L_1/K и L_2/K – это изоморфизм σ: $L_1 \backsimeq L_2$ такой, что $\forall\ a \in K:\ \sigma(a) = a$.

Предложение 18.9. L/K – расширение. Тогда 2 условия эквивалентны:

1. L/K конечно.
2. $L = K(a_1,\dots,a_n),\ a_1,\dots,a_n$ – алгебраические над K.

Доказательство. $1 \Rightarrow 2$: Пусть $\theta_1,\dots,\theta_n$ – базис L над $K \Rightarrow K(\theta_1,\dots,\theta_n) = L$, все элементы L алгебраичны над K.
$2 \Rightarrow 1$: Индукция по n. $n = 0 \Rightarrow L = K$. $n > 0 \Rightarrow L = K'(a_n),\ K' = K(a_1,\dots,a_{n-1}), [K' : K] < \infty$ по ИП, $[L : K'] = d,\ d = \deg \operatorname{Irr}_{K'} a_n < \infty, [L : K] = [L : K'][K' : K] < \infty$. ■

Следствие 18.9.1. Пусть $a,\ b$ – алгебраичны над K. Тогда $a+b,\ ab$ – алгебраичны над K.

Доказательство. $a,\ b$ – алгебраичны над $K \Rightarrow K(a,b)/K$ – конечное $\Rightarrow$ алгебраическое. $a+b,\ ab \in K(a,b) \Rightarrow a+b,\ ab$ – алгебраичны над K. ■

Глава 19

Конечные поля

Предложение 19.1. Пусть k – поле, $|k| = q$, K/k – расширение, $[K : k] = m$. Тогда $|K| = q^m$.

Доказательство. $K \cong k^m$ как линейное пространство $\Rightarrow |K| = |k^m| = |k|^m = q^m$. ■

Следствие 19.1.1. Пусть K – конечное поле, $\mathrm{char} K = p$. Тогда $|K| = p^m$ для некоторого $m \in \mathbb{N}$.

Доказательство. k – простое подполе $K \Rightarrow k \cong \mathbb{F}_p$, $|k| = p \Rightarrow |K| = p^m$, где $m = [K : k]$. ■

Предложение 19.2. Пусть K – поле, $|K| = q$. Тогда $\forall a \in K : a^q = a$.

Доказательство. $a = 0$ – очевидно. $a \neq 0 : |K^*| = q - 1 \Rightarrow \forall c \in K^* : \ \mathrm{ord}\ c \mid q - 1 \Rightarrow c^{q-1} = 1,\ a \in K^* \Rightarrow a^{q-1} = 1 \Rightarrow a^q = a$. ■

Следствие 19.2.1. Пусть $|K| = q$. Тогда K – поле разложения $X^q - X$ над любым подполем.

Доказательство. По предыдущему предложению: $\forall\ a \in K\ f(a) = 0,\ f = X^q - X.\ \deg\ f = q \Rightarrow f = \prod_{a \in K}(X - a).\ k$ – подполе, $k(a \mid f(a) = 0) = k(K) = K.$ ■

Лемма 19.3. Пусть $\mathrm{char}\ K = p > 0;\ \alpha, \beta \in K$. Тогда $\forall m \in \mathbb{N}:$ $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$.

Доказательство. Достаточно рассмотреть $m = 1$.

$$(\alpha + \beta)^p = \alpha^p + \beta^p + \sum_{i=1}^{p-1} C_p^i \alpha^i \beta^{p-i}$$

$$C_p^i = \frac{p!}{i!(p-i)!} = 0 \text{ в } K$$

■

Теорема 19.4 (О существовании конечных полей)**.** Пусть p – простое, $n \in \mathbb{N}$. Тогда существует поле K: $|K| = p^n$.

Доказательство. Пусть F – поле разложения $X^q - X$ над $\mathbb{F}_p,\ q = p^n$. Проверим, что у него нет кратных корней: $(X^q - X)' = qX^{q-1} - 1 = -1 \Rightarrow$ в $F:\ X^q - X = \prod_{i=1}^{q}(X - a_i),\ a_1, \ldots, a_q$ – различны.

$$K = \{a_1, \ldots, a_q\},\ \forall\ i:\ a_i^q = a_i$$

$$a_i, a_j \in K\ (a_i + a_j)^q = (a_i + a_j)^{p^n} = a_i^{p^n} + a_j^{p^n} = a_i + a_j$$

$$\Rightarrow a_i + a_j \in K$$

$$a \in K\ (-a)^q = \begin{cases} -a^q, & q \text{ неч.} \\ a^q, & q \text{ чет.} \end{cases} \Rightarrow -a \in K$$

$$a,\ b \in K \Rightarrow (ab)^q = a^q b^q = ab \Rightarrow ab \in K$$

$$\underbrace{a \in K}_{a \neq 0} \Rightarrow a^q = a \Rightarrow (a^{-1})^q = a^{-q} = (a^q)^{-1} = a^{-1}$$

Таким образом, K – поле, $|K| = q = p^n$. ■

07.12.22

Лемма 19.5. Пусть K/k – расширение конечных полей (K – конечное). Тогда это простое расширение.

Доказательство. Конечная подгруппа в мультипликативной группе поля – циклическая (из ТГ). K^* – циклическая, т.е. $K^* = \langle\theta\rangle$. Тогда $K = k(\theta)$. ■

Теорема 19.6. Пусть $K_1,\ K_2$ – конечные поля, $|K_1| = |K_2| = p^n$. Тогда K_1 и K_2 изоморфны.

Доказательство. По лемме $K_1 = \mathbb{F}_p(\theta_1)$. Многочлен $g = \operatorname{Irr}_{\mathbb{F}_p}\theta_1,\ \deg g = [K_1 : \mathbb{F}_p] = n$. θ_1 – корень $X^{p^n} - X \Rightarrow g | X^{p^n} - X$. В K_2 все элементы – корни $X^{p^n} - X \Rightarrow$ в $K_2[X]$ $X^{p^n} - X$ – раскладывается на линейные множители $\Rightarrow g$ раскладывается в $K_2[X]$ на линейные множители $\Rightarrow \exists\theta_2 \in K_2 :\ g(\theta_2) = 0 \Rightarrow [\mathbb{F}_p(\theta_2) : \mathbb{F}_p] = \deg g = n$, но $[K_2 : \mathbb{F}_p] = n \Rightarrow K_2 = \mathbb{F}_p(\theta_2) \Rightarrow K_2 \cong K_1 (\cong \mathbb{F}_p[X]/(g))$. ■

Теорема 19.7.

1. Пусть K – подполе $\mathbb{F}_{p^n}$ (поле из p^n элементов). Тогда $|K| = p^m,\ m \mid n$.
2. Пусть $m \mid n$. Тогда в $\mathbb{F}_{p^n}$ есть единственное подполе из p^m элементов.

Доказательство.

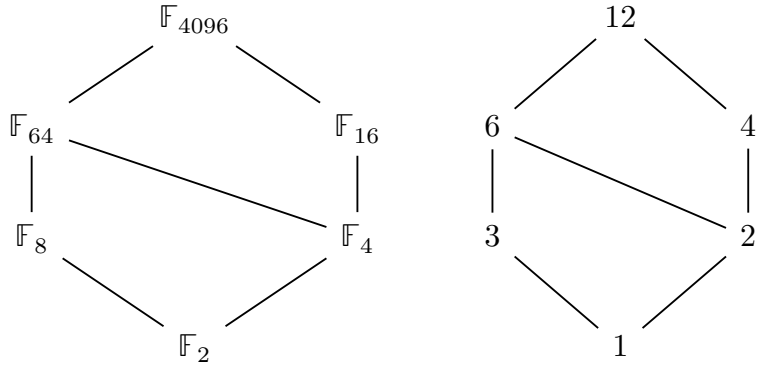
1. $|K| = q,\ [\mathbb{F}_{p^n} : K] = l \Rightarrow q^l = p^n \Rightarrow q = p^m,\ p^{ml} = p^n \Rightarrow m \mid n$.
2. $m \mid n \Rightarrow (p^m - 1) \mid (p^n - 1)$. $n = ml \Rightarrow p^n - 1 = (p^m)^l - 1^l = (p^m - 1)(...) \Rightarrow (X^{p^m-1} - 1) | (X^{p^n-1} - 1),\ (p^n - 1) = r(p^m - 1) \Rightarrow (X^{p^m} - X) | (X^{p^n} - X)$.

   $X^{p^n} - X$ раскладывается на линейные множители в $\mathbb{F}_p[X] \Rightarrow$ $X^{p^m} - X$ раскладывается на линейные множители в $\mathbb{F}_p[X]$.

   $F = \{a \mid a^{p^m} - a = 0\}$ – искомое подполе.

Пусть F' – другое подполе, такое что $|F'| \neq 0,\ F' \neq F\, \forall a \in F' :\ a^{p^m} - a = 0 \Rightarrow \forall a \in F \cup F' :\ a^{p^m} - a = 0,\ |F \cup F'| > p^m$. ■

Пример 19.1. $\mathbb{F}_{p^n},\ d \mid n \Rightarrow$ в $\mathbb{F}_{p^n}$ есть ровно одно поле из p^d элементов.



Глава 20

Автоморфизм конечных полей

Лемма 20.1 (Автоморфизм Фробениуса)**.** Пусть p – простое, $n \in \mathbb{N}$. Тогда отображение $\mathbb{F}_{p^n} \underset{a \mapsto a^p}{\to} \mathbb{F}_{p^n}$ является автоморфизмом $\mathbb{F}_{p^n}$.

Доказательство.

$$(a+b)^p = a^p + b^p$$
$$(ab)^p = a^p b^p$$
$$1^p = 1$$

Таким образом, это вложение полей. Оно инъективно $\Rightarrow$ сюръективно. ■

$\mathrm{Aut}(K)$ – группа автоморфизмов поля K.

Пусть L/K – расширение. $\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}\, L \mid \forall a \in K : \sigma(a) = a\}$.

Пример 20.1. $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id},\ \text{комплексное сопряжение}\}$.

$K,\ F$ – поля, $\sigma : K \hookrightarrow F$ – вложение.

$$f \in K[X]$$
$$f = a_n X^n + \dots a_1 X + a_0$$
$$f^\sigma = \sigma(a_n)X^n + \dots + \sigma(a_1) + \sigma(a_0) \in F[X]$$

Предложение 20.2. Пусть $\sigma : K \hookrightarrow F$ – вложение, $L = K(x)$ – простое алгебраическое расширение, $f = \operatorname{Irr}_K x,\ y_1, \dots, y_n$ – все корни f^σ в F. Тогда у σ есть ровно n продолжений $\sigma_1, \dots, \sigma_n$ на L, причем $\sigma_i(x) = y_i,\ i = 1, \dots, n$.

Пусть L/K – расширение. Вложение $\tau : L \hookrightarrow F$ называется продолжением вложения $\sigma : K \hookrightarrow F$, если $\tau|_K = \sigma$.

Доказательство. Построим σ_i. Можно считать $L = K[X]/(f)$.

$$K[X] \xrightarrow[g \mapsto g^\sigma(y_i)]{\alpha_i} F$$
$$K[X] \to F[X] \to F$$
$$g \mapsto g^\sigma \mapsto g^\sigma(y_i)$$
$$f \in \operatorname{Ker} \alpha_i, \text{ т.е. } f(y_i) = 0$$
$$\operatorname{Ker} \alpha_i = (h) \Rightarrow h \mid f \Rightarrow h = f$$

По теореме о гомоморфизме α_i индуцирует вложение $L \xhookrightarrow[x=\overline{X} \mapsto y_i]{\sigma_i} F$. $\sigma_i|_K = \sigma$, т.к. $\alpha_i(c) = c^\sigma = \sigma(c)$, при $c \in K$.
Осталось проверить, что других продолжений нет. Пусть $\tau : L \hookrightarrow F,\ \tau|_K = \sigma$. $f^\sigma(\tau(x)) = f^\tau(\tau(x)) = \tau(f(x)) = \tau(0) = 0 \Rightarrow \exists i : \tau(x) = y_i = \sigma_i(x),\ \forall c \in K : \tau(c) = \sigma(c) = \sigma_i(c) \Rightarrow (L = \{\alpha_0 + \alpha_1 x + \dots + \alpha_{d-1} x^{d-1} \mid \alpha_0, \dots, \alpha_{d-1} \in K\}) \Rightarrow \tau = \sigma_i$. ■

Следствие 20.2.1. Пусть $\sigma : K \hookrightarrow F$ – вложение. L/K – конечное расширение. Тогда у σ есть $\leqslant [L : K]$ продолжений на L.

Доказательство. $L = K(x_1, \dots, x_m)$.
Индукция по m. $m = 0 : [L : K] = 1$, у σ одно продолжение.
Переход. $L_0 = K(x_1, \dots, x_{m-1})$. По ИП у σ есть $\leqslant d_0$ продолжений на L_0, где $d_0 = [L_0 : K] : \sigma_1 \dots, \sigma_l,\ l \leqslant d_0$. У каждого σ_i есть

$\leqslant [L : L_0]$ продолжений на $L \Rightarrow$ у σ есть $\leqslant l \cdot [L : L_0]$ продоолжений на L, т.к. $[\underbrace{L}_{L_0(x_m)} : L_0] = \deg \operatorname{Irr}_{L_0} x_m$. $l \cdot [L : L_0] \leqslant d_0 \cdot [L : L_0] = [L : K]$. ■

Следствие 20.2.2. Пусть L/K – конечное расширение. Тогда $|\operatorname{Aut}(L/K)| \leqslant [L : K]$.

Доказательство. Автоморфизм L/K – вложение $L \hookrightarrow L$, продолжающее $K \underset{a \mapsto a}{\hookrightarrow} L$. $[L : K] < \infty \Rightarrow$ любое вложение $L \hookrightarrow L$ над K – биекция. ■

Теорема 20.3 (О группе автоморфизмов конечных полей)**.** Пусть p – простое, $n \in \mathbb{N}$, $K = \mathbb{F}_{p^n}$. Тогда $\operatorname{Aut}(K) = \langle \mathrm{Fr} \rangle$, где Fr – автоморфизм Фробениуса и $|\operatorname{Aut}(K)| = n$.

Доказательство. Хотим узнать степень Fr. $(Fr)^n = \mathrm{id}_K$. $\forall x \in K : \ x^{p^n} = x \Rightarrow \mathrm{ord} Fr \leqslant n$. Предположим, $\exists d < n : Fr^d = \mathrm{id}_K \Rightarrow \forall x \in K : \ x^{p^d} = x \Rightarrow x$ – корень $X^{p^d} - X$. Однако, у $X^{p^d} - X$ не может быть p^n корней. Таким образом, $ord\,\mathrm{Fr} = n \Rightarrow |\langle \mathrm{Fr} \rangle| = n = [K : \mathbb{F}_p] \geqslant \operatorname{Aut}(K/\mathbb{F}_p) = \operatorname{Aut}(K)$ $(c \in \mathbb{F}_p : \ \sigma(c) = c = \{1 + ... + 1\})$ (на простом подполе любой автоморфизм тождественный) $\Rightarrow \langle \mathrm{Fr} \rangle = \operatorname{Aut} K$. ■

Пример 20.2 (Ужасный пример)**.** $\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. У $X^3 - 2$ один корень в $\mathbb{Q}(\sqrt[3]{2}) \Rightarrow |\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$.

Алгебраическое расширение L/K сепарабельно, если $\forall x \in L : \operatorname{Irr}_K x$ не имеет кратных корней в L.

Есть кратный корень $\Rightarrow (f, f') \neq$ в $L[X]$, $(f, f') \neq$ в $K[X]$, но f неприводим.

Определение 20.1. Конечное расширение L/K называется расширением Галуа, если оно нормальное и сепарабельное ($\Leftrightarrow \operatorname{Aut}(L/K) = [L : K]$).

L/K – расширение Галуа, $G = \operatorname{Aut}(L/K)$.

$$
\begin{array}{ccccc}
L & & \{M - \text{промежуточное поле в } L/K\} & & \{H \mid H < G\} \\
\Big| & & & & \\
M & & & M \longmapsto \mathrm{Aut}(L/M) < \mathrm{Aut}(L/K) & \\
\Big| & & & & \\
K & & \underbrace{L^H}_{=\{a \in L \mid \forall \sigma \in H\colon\ a^\sigma = a\}} & \longmapsto & H
\end{array}
$$

– две взаимно обратные функции, образующие включения.