回忆 核核分解定理

设 $f \in F[t]$，$f = pg$，其中 $p, g \in F[t]$ 且 $\gcd(p, g) = 1$. 设 $\mathcal{A} \in \mathcal{L}(V)$ 满足 $f(\mathcal{A}) = 0$

则 $\therefore V = K_{p(\mathcal{A})} \oplus K_{g(\mathcal{A})}$

（席南华书P72，定理2.5.1，隐藏在P72，定理3的证明中）

例：设 $\mathcal{A}: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}}_{A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

取 $f(t) = 2t^2 - t - 1$.

求 $f(\mathcal{A})$ 在标准基下的矩阵.

解：设 $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $\quad \mathcal{A}(\vec{x}) = A\vec{x}$

$\mathcal{A}^2 \vec{x} = A^2 \vec{x}$

$f(\mathcal{A}) = 2\mathcal{A}^2 - \mathcal{A} - \mathcal{E}$

$f(\mathcal{A})(\vec{x}) = (2\mathcal{A}^2 - \mathcal{A} - \mathcal{E})(\vec{x})$

$= 2\mathcal{A}^2(\vec{x}) - \mathcal{A}(\vec{x}) - \mathcal{E}(\vec{x})$

$= 2A^2\vec{x} - A\vec{x} - \vec{x}$

$= (2A^2 - A - E)(\vec{x})$

$= f(A)\vec{x}$

于是 $f(\mathcal{A})$ 在标准基下的矩阵是

$$f(A) = 2A^2 - A - E = 2\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2 - \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 12 & 18 \\ 27 & 35 \end{pmatrix}.$$

通过上面类似的计算可证明

$\forall p \in F[t]$，$\mathcal{A} \in \mathcal{L}(V)$，$A \in M_n(F)$ 在 V 的某组基下的矩阵，则 $p(\mathcal{A})$ 在该基下的矩阵是 $p(A)$.

例：设 $A, B \in M_n(F)$，$A \sim_s B$

则 $\forall p \in F[t]$，$p(A) \sim_s p(B)$.

证：设 $A = Q^{-1}BQ$，其中 $Q \in GL_n(F)$

则 $\forall k \in \mathbb{N}$ $\quad A^k = Q^{-1}B^kQ$

设 $p(t)=\alpha_d t^d+\alpha_{d-1}t^{d-1}+\cdots+\alpha_1 t+\alpha_0$, $\alpha_i\in F$

$$\begin{aligned}
p(B) &= \alpha_d B^d+\alpha_{d-1}B^{d-1}+\cdots+\alpha_1 B+\alpha_0 E\\
&= \alpha_d(Q^{-1}AQ)^d+\alpha_{d-1}(Q^{-1}AQ)^{d-1}+\cdots+\alpha_1(Q^{-1}AQ)+\alpha_0 E\\
&= \alpha_d Q^{-1}A^dQ+\alpha_{d-1}Q^{-1}A^{d-1}Q+\cdots+\alpha_1 Q^{-1}AQ+\alpha_0 E\\
&= Q^{-1}(\alpha_d A^d)Q+Q^{-1}(\alpha_{d-1}A^{d-1})Q+\cdots+Q^{-1}(\alpha_1 A)Q+Q^{-1}\alpha_0 Q\\
&= Q^{-1}(\alpha_d A^d+\alpha_{d-1}A^{d-1}+\cdots+\alpha_1 A+\alpha_0 E)Q\\
&= Q^{-1}p(A)Q
\end{aligned}$$

于是 $p(B)\sim_s p(A)$.

例 设 $\mathcal{A}\in\mathcal{L}(V)$ 满足 $\mathcal{A}^2=\mathcal{A}$.

证明: $\operatorname{rank}(\mathcal{A})+\operatorname{rank}(\mathcal{A}-\mathcal{E})=\dim V$

证: 注意到 $\mathcal{A}^2-\mathcal{A}=\mathcal{O}$. 设 $f(t)=t^2-t$

因为 $f(t)=t(t-1)$ 且 $\gcd(t,t-1)=1$

所以 $K_{\mathcal{A}}\oplus K_{\mathcal{A}-\mathcal{E}}=V$

(核核分解定理)

于是 $\dim(K_{\mathcal{A}})+\dim(K_{\mathcal{A}-\mathcal{E}})=\dim V$

(第一章推论7.4)

$\Rightarrow \dim V-\operatorname{rank}(\mathcal{A})+\dim V-\operatorname{rank}(\mathcal{A}-\mathcal{E})=\dim V$

(第一章推论7.1)

$\Rightarrow \operatorname{rank}(\mathcal{A})+\operatorname{rank}(\mathcal{A}-\mathcal{E})=\dim V$ ∎

§2.6 完全正交等方组

(科斯特里金书 §3 第一部分)

设 $V=W_1\oplus W_2\oplus\cdots\oplus W_m$, 其中 W_i 是子空间

则 $\forall \vec{x}\in V$. $\exists!\ \vec{x}_1\in W_1,\cdots,\vec{x}_m\in W_m$

使得 $\vec{x}=\vec{x}_1+\cdots+\vec{x}_m$ (直和的定义)

设: $\pi_i: V\longrightarrow V$, $\vec{x}\longmapsto\vec{x}_i$

由上次讲义关于幂等算子的例子可知

$\pi_i\in\mathcal{L}(V)$, $i=1,\cdots,m$

π_i 称为从由 V 到 W_i 关于上述直和分解的投射.

定义：设 $\sigma_1, \dots, \sigma_m \in \mathcal{L}(V)$，如果它们满足 (i) $\forall i \in \{1, \dots, m\}$. $\sigma_i^2 = \sigma_i$，~~幂等~~ (等方)

(ii) $\forall i, j \in \{1, \dots, m\}, i \neq j$ $\sigma_i \circ \sigma_j = O$ (正交)

则称 $\{\sigma_1, \dots, \sigma_m\}$ 是一个正交等方组.

如果 $\sigma_1, \dots \sigma_m$ 还进一步满足

$$\sigma_1 + \dots + \sigma_m = \varepsilon \quad (\text{完全})$$

则称 $\{\sigma_1, \dots \sigma_m\}$ 是一个完全正交等方组.

例：本节开始的 $\{\pi_1, \dots \pi_m\}$ 是一个完全正交等方组. 验证：

等方. 设 $\vec{x} = \vec{x_1} + \dots + \vec{x_m}$，$\vec{x_i} \in W_i$

$\pi_i(\vec{x}) = \vec{x_i}$ $\quad \pi_i^2(\vec{x}) = \pi_i(\vec{x_i})$

$$\vec{x_i} = \underset{W_1}{\vec{0}} + \dots + \underset{W_{i-1}}{\vec{0}} + \underset{W_i}{\vec{x_i}} + \underset{W_{i+1}}{\vec{0}} + \dots + \underset{W_m}{\vec{0}}$$

$\pi_i(\vec{x_i}) = \vec{x_i} \Rightarrow \pi_i^2(\vec{x}) = \vec{x_i}$

$\Rightarrow \pi_i(\vec{x}) = \pi_i^2(\vec{x}) \Rightarrow \pi_i = \pi_i^2$

定理2.5 设 $\sigma_1, \dots, \sigma_m \in \mathcal{L}(V)$ 构成完全正交等方组. 则

$$V = \mathrm{im}(\sigma_1) \oplus \dots \oplus \mathrm{im}(\sigma_m) \quad (*)$$

且 σ_i 是 V 到 $\mathrm{im}(\sigma_i)$ 关于 $(*)$ 的投影.
$(i = 1, 2, \dots, m)$

~~证~~ 断言1：$V = \mathrm{im}(\sigma_1) + \dots + \mathrm{im}(\sigma_m)$

$\forall \vec{x} \in V$ $\quad \vec{x} = \varepsilon(\vec{x}) = (\sigma_1 + \dots + \sigma_m)(\vec{x}) = \sigma_1(\vec{x}) + \dots + \sigma_m(\vec{x})$ [完全性]

$\because \sigma_i(\vec{x}) \in \mathrm{im}(\sigma_i)$，$i = 1, \dots, m$

$\therefore \vec{x} \in \mathrm{im}(\sigma_1) + \dots + \mathrm{im}(\sigma_m)$

于是 $V \subset \mathrm{im}(\sigma_1) + \dots + \mathrm{im}(\sigma_m)$

而反包含关系显然. 断言1成立

断言2：$\mathrm{im}(\sigma_1) + \dots + \mathrm{im}(\sigma_m)$ 是直和

由第一章命题2.1 只要证

若 $\vec{u_1} \in \mathrm{im}(\sigma_1), \dots \vec{u_m} \in \mathrm{im}(\sigma_m)$ 使得 $\vec{u_1} + \dots + \vec{u_m} = \vec{0}$. 则 $\vec{u_1} = \dots = \vec{u_m} = \vec{0}$

因为 $\vec{u_i} \in \mathrm{im}(\sigma_i)$，所以 $\exists \vec{v_i} \in V$ 使得

$$\vec{u_i} = \sigma_i(\vec{v_i})$$

于是 $\sigma_1(\vec{v_1}) + \cdots + \sigma_m(\vec{v_m}) = \vec{0}$

$\Rightarrow \sigma_1 \circ (\sigma_1(\vec{v_1}) + \sigma_2(\vec{v_2}) + \cdots + \sigma_m(\vec{v_m})) = \vec{0}$

$\sigma_1^2(\vec{v_1}) + \sigma_1 \circ \sigma_2(\vec{v_2}) + \cdots + \sigma_1 \circ \sigma_m(\vec{v_m}) = \vec{0}$

由正交性. $\sigma_1^2(\vec{v_1}) = \vec{0}$

由幂等性 $\sigma_1(\vec{v_1}) = \vec{0} \Rightarrow \vec{u_1} = \vec{0}$

同理 $\vec{u_2} = \cdots = \vec{u_m} = \vec{0}$. 断言2成立.

由上述两个断言. $V = \mathrm{im}(\sigma_1) \oplus \cdots \oplus \mathrm{im}(\sigma_m)$

设 π_i 是由 V 到 $\mathrm{im}(\sigma_i)$ 关于上述直和分解的投影. 设 $\vec{x} \in V$

$$\vec{x} = \vec{u_1} + \cdots + \vec{u_m}, \quad \vec{u_i} \in \mathrm{im}(\sigma_i)$$

设 $\vec{u_i} = \sigma_i(\vec{v_i})$，$i=1$. $\vec{v_i} \in V$

$$\vec{x} = \sigma_1(\vec{v_1}) + \cdots + \sigma_m(\vec{v_m})$$

~~由σ1~~

$$\pi_i(\vec{x}) = \sigma_i(\vec{v_i}), \quad i=1,2,\cdots,m.$$

~~由完全性，~~

~~$\vec{x} = \sigma_1(\vec{x}) + \cdots + \sigma_m(\vec{x})$~~

~~由直和分解的唯一性~~

~~$\sigma_i(\vec{x}) = \sigma_i(\vec{v_i}) \Rightarrow$~~

由正交性 $\sigma_i(\vec{x}) = \sigma_i \circ \sigma_1(\vec{v_1}) + \cdots + \sigma_i \circ \sigma_i(\vec{v_i}) + \cdots + \sigma_i \circ \sigma_m(\vec{v_m})$

$= \sigma_i^2(\vec{v_i}) = \sigma_i(\vec{v_i})$，$i=1,\cdots m$.

$\Rightarrow \pi_i(\vec{x}) = \sigma_i(\vec{x}) \Rightarrow \pi_i = \sigma_i$ ▨

关于单位分解的例子

求方程 $3x+5y=2$ 的所有整数解

$\because \gcd(3,5)=1 \quad \therefore \exists u,v \in \mathbb{Z}$ 使得

$$u \times 3 + v \times 5 = 1$$

$$2 \cdot 3 + (-1) \cdot 5 = 1$$

$$4 \cdot 3 + (-2) \cdot 5 = 2$$

于是方程有一组解 $\begin{cases} x_0 = 4 \\ y_0 = -2 \end{cases}$

则 $\begin{cases} 3x+5y=2 \\ 3x_0+5y_0=2 \end{cases} \Rightarrow 3(x-x_0)+5(y-y_0)=0$

$\Rightarrow -3(x-x_0)=5(y-y_0)$

$\Rightarrow 3 \mid 5(y-y_0) \Rightarrow 3 \mid (y-y_0)$

设 $y-y_0=3k \Rightarrow x-x_0=-5k$

于是 $3x+5y=2$ 的所有解是 $\begin{cases} x=x_0-5k=4-5k \\ y=y_0+3k=-2+3k \end{cases}$

§3 不变子空间

定义：设 $\mathcal{A}\in\mathcal{L}(V)$，$U$是$V$的子空间，如果 $\mathcal{A}(U)\subset U$，则称 U是 $\mathcal{A}$的不变子空间，简称 $\mathcal{A}$-子空间.

注：U是$\mathcal{A}$-子空间 $\Leftrightarrow \forall \vec{x}\in U$，$\mathcal{A}(\vec{x})\in U$

设 U是 $\mathcal{A}$-子空间：

$$\mathcal{A}U: \begin{aligned} U &\longrightarrow U \\ x &\longmapsto \mathcal{A}(\vec{u}) \end{aligned}$$

是U上的线性算子.

例. $\{\vec{0}\}$ 和 V 是平凡 $\mathcal{A}$-子空间

例：验证：$\ker(\mathcal{A})$，$\mathrm{im}(\mathcal{A})$是 $\mathcal{A}$-子空间

设 $\vec{x}\in\ker(\mathcal{A})$．$\mathcal{A}(\vec{x})=\vec{0}\in\ker(\mathcal{A})$

于是 $\ker(\mathcal{A})$是 $\mathcal{A}$-子空间.

设 $\vec{x}\in\mathrm{im}(\mathcal{A})$．则$\exists\vec{y}\in V$ 满足

$$\vec{x}=\mathcal{A}(\vec{y})$$

$$\mathcal{A}(\vec{x})=\mathcal{A}(\mathcal{A}(\vec{y}))\in\mathrm{im}(\mathcal{A}).$$

于是 $\mathrm{im}(\mathcal{A})$是 $\mathcal{A}$-子空间.

引理3.1 设 $\mathcal{A},\mathcal{B}\in\mathcal{L}(V)$．~~如果~~ $\mathcal{A}\circ\mathcal{B}=\mathcal{B}\circ\mathcal{A}$，则 $\ker(\mathcal{B})$ 和 $\mathrm{im}(\mathcal{B})$ 都是 $\mathcal{A}$-子空间.

证：设 $\vec{x}\in\ker(\mathcal{B})$.

$\mathcal{B}(\mathcal{A}(\vec{x}))=\mathcal{B}\circ\mathcal{A}(\vec{x})=\mathcal{A}\circ\mathcal{B}(\vec{x})=\mathcal{A}(\mathcal{B}(\vec{x}))$

$=\mathcal{A}(\vec{0})=\vec{0}$

$\Rightarrow \mathcal{A}(\vec{x})\in\ker(\mathcal{B})$

$\Rightarrow \ker(\mathcal{B})$是 $\mathcal{A}$-子空间.

设 $\vec{z} \in \mathrm{im}(\mathcal{B})$. $\exists \vec{y} \in V$ 使得 $\vec{z} = \mathcal{B}(\vec{y})$

$$\mathcal{A}(\vec{z}) = \mathcal{A} \circ \mathcal{B}(\vec{y}) = \mathcal{B} \circ \mathcal{A}(\vec{y}) = \mathcal{B}(\mathcal{A}(\vec{y})) \in \mathrm{im}(\mathcal{B})$$

于是 $\mathrm{im}(\mathcal{B})$ 是 $\mathcal{A}$-子空间 ▨

推论3.1 设 $\mathcal{A} \in \mathcal{L}(V)$, $p \in F[t]$

则 $\ker(p(\mathcal{A}))$ 和 $\mathrm{im}(p(\mathcal{A}))$ 都是 $\mathcal{A}$-子空间.

证: $\because$ $\mathcal{A} \circ p(\mathcal{A}) = p(\mathcal{A}) \circ \mathcal{A}$

推论由引理3.1得证 ▨

命题3.1 设 $\mathcal{A} \in \mathcal{L}(V)$, U 是 $\mathcal{A}$-子空间,

$\vec{e_1}, \dots, \vec{e_d}$ 是 U 的基, $\vec{e_1}, \dots, \vec{e_d}, \vec{e_{d+1}}, \dots, \vec{e_n}$

是 V 的基 则 $\mathcal{A}$ 在

$\vec{e_1}, \dots, \vec{e_d}, \vec{e_{d+1}}, \dots, \vec{e_n}$ 下的矩阵是

$$A = \begin{pmatrix} B & C \\ O & D \end{pmatrix}$$

其中 $B \in M_d(F)$, $C \in F^{d \times (n-d)}$, $D \in M_{n-d}(F)$

证: $\forall j \in \{1, 2, \dots, d\}$

$\because$ U 是 $\mathcal{A}$-子空间 $\therefore$ $\mathcal{A}(\vec{e_j}) \in U$

$\exists$ $\beta_{1j}, \dots \beta_{dj} \in F$ 使得

$$\mathcal{A}(\vec{e_j}) = \sum_{i=1}^{d} \beta_{ij} \vec{e_i}$$

$\forall j \in \{d+1, \dots, n\}$. $\exists$ $\alpha_{1j}, \dots \alpha_{nj} \in F$ 使得

$$\mathcal{A}(\vec{e_j}) = \sum_{i=1}^{n} \alpha_{ij} \vec{e_i}$$

于是

$$(\mathcal{A}(\vec{e_1}), \dots \mathcal{A}(\vec{e_d}), \mathcal{A}(\vec{e_{d+1}}), \dots \mathcal{A}(\vec{e_n})) =$$

$$(\vec{e_1}, \dots, \vec{e_d}, \vec{e_{d+1}}, \dots, \vec{e_n}) \begin{pmatrix} \beta_{11} & \cdots & \beta_{1d} & \alpha_{1,d+1} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & & & \\ \beta_{d1} & \cdots & \beta_{dd} & \alpha_{d,d+1} & \cdots & \alpha_{d,n} \\ & & & \alpha_{d+1,d+1} & \cdots & \alpha_{d+1,n} \\ & O & & & \vdots & \\ & & & \alpha_{n,d+1} & \cdots & \alpha_{n,n} \end{pmatrix}$$

▨

命题3.2 设 $\mathcal{A}\in\mathcal{L}(V)$，$U, W$ 是 $\mathcal{A}$-子空间

且 $V=U\oplus W$.

设 $\vec{e}_1,\cdots,\vec{e}_d$ 是 U 的基，$\vec{e}_{d+1},\cdots,\vec{e}_n$ 是 W 的基. 则在 V 的基底

$\vec{e}_1,\cdots,\vec{e}_d,\ \vec{e}_{d+1},\cdots,\vec{e}_n$

下 $\mathcal{A}$ 的矩阵可写为 $\begin{pmatrix} B & O \\ O & C \end{pmatrix}$

其中 $B\in M_d(F)$，$C\in M_{n-d}(F)$.

证：$\forall j\in\{1,\cdots,d\}$

$\mathcal{A}(\vec{e}_j)\in U \Rightarrow \exists\, \alpha_{1j},\cdots\alpha_{dj}\in F$ 使得

$$\mathcal{A}(\vec{e}_j)=\alpha_{1j}\vec{e}_1+\cdots+\alpha_{dj}\vec{e}_d$$

$\forall j\in\{d+1,\cdots,n\}$

$\mathcal{A}(\vec{e}_j)\in W \Rightarrow \exists\, \beta_{d+1,j},\cdots\beta_{nj}\in F$ 使得

$$\mathcal{A}(\vec{e}_j)=\beta_{d+1,j}\vec{e}_{d+1}+\cdots+\beta_{nj}\vec{e}_n$$

于是

$$(\mathcal{A}(\vec{e}_1),\cdots,\mathcal{A}(\vec{e}_d),\mathcal{A}(\vec{e}_{d+1}),\cdots\mathcal{A}(\vec{e}_n))$$
$$=(\vec{e}_1,\cdots,\vec{e}_d,\vec{e}_{d+1},\cdots,\vec{e}_n)\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1d} & & O & \\ \alpha_{d1} & \cdots & \alpha_{dd} & & & \\ & & & \beta_{d+1,d+1} & \cdots & \beta_{d+1,n} \\ & O & & \vdots & & \\ & & & \beta_{n,d+1} & \cdots & \beta_{n,n} \end{pmatrix}$$

$\boxed{/\!/}$

例：设 $\mathcal{A}\in\mathcal{L}(V)$，$\mathcal{A}^2=\mathcal{A}$

由上周讲义 p6 例

$$V=\ker(\mathcal{A})\oplus \operatorname{im}(\mathcal{A}).$$

设 $\vec{e}_1,\cdots,\vec{e}_d$ 是 $\ker(\mathcal{A})$ 的一组基

$\vec{e}_{d+1},\cdots,\vec{e}_n$ 是 $\operatorname{im}(\mathcal{A})$ 的一组基.

$\forall j\in\{1,\cdots,d\}$，$\mathcal{A}(\vec{e}_j)=0$

$\forall j\in\{d+1,\cdots,n\}$ $\exists\, \vec{u}_j\in V$

$$\vec{e}_j=\mathcal{A}(\vec{u}_j)$$

$$\mathcal{A}(\vec{e}_j)=\mathcal{A}^2(\vec{u}_j)=\mathcal{A}(\vec{u}_j)=\vec{e}_j$$

于是 $\mathcal{A}$ 在 $\vec{e}_1, \dots, \vec{e}_d, \vec{e}_{d+1}, \dots, \vec{e}_n$ 下的矩阵

是 $$\begin{pmatrix} O & O \\ O & E_{n-d} \end{pmatrix}$$

例：设 $A \in M_n(F)$ 满足 $A^2 = A$

证明 $tr(A) = rank(A)$

证：设 $\mathcal{A}: F^n \longrightarrow F^n$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$\because A^2 = A \quad \therefore \mathcal{A}^2 = \mathcal{A}$

设 $r = rank(A)$. 则 $r = rank(\mathcal{A}) = \dim(\mathrm{im}(\mathcal{A}))$.

由上例可知

$$A \sim_s \underbrace{\begin{pmatrix} O & O \\ O & E_r \end{pmatrix}}_{B}$$

$$\Rightarrow \underbrace{tr(A) = tr(B)}_{\text{命题 } 2.1} = r \quad \boxed{}$$

引理 3.2 设 $\mathcal{A} \in \mathcal{L}(V)$, U, W 是 $\mathcal{A}$-子空间. 则

$U \cap W$, $U + W$

也是 $\mathcal{A}$-子空间

证：$\forall \vec{x} \in U \cap W$, $\Rightarrow \mathcal{A}(\vec{x}) \in U$, $\mathcal{A}(\vec{x}) \in W$

$\Rightarrow \mathcal{A}(\vec{x}) \in U \cap W$

$\Rightarrow U \cap W$ 是 $\mathcal{A}$-子空间 [illegible]

$\forall \vec{x} \in U + W$, $\exists \vec{y} \in U$, $\vec{z} \in W$ 使得

$$\vec{x} = \vec{y} + \vec{z}$$

$$\mathcal{A}(\vec{x}) = \underset{\underset{U}{\cap}}{\mathcal{A}(\vec{y})} + \underset{\underset{W}{\cap}}{\mathcal{A}(\vec{z})} \in U + W.$$

$\Rightarrow U + W$ 是 $\mathcal{A}$-子空间

定理3.1 设 $\mathcal{A} \in \mathcal{L}(V)$, $U_1, \cdots U_m$

是 $\mathcal{A}$-子空间且

$$V = U_1 \oplus \cdots \oplus U_m$$

设 $\vec{e}_{k1},\dots,\vec{e}_{kd_k}$ 是 U_k 的基底，$k=1,2,\dots,m$

则 $\mathcal{A}$ 在 V 的基底

$\vec{e}_{11},\dots,\vec{e}_{1d_1},\dots,\vec{e}_{m,1},\dots,\vec{e}_{m,d_m}$

下的矩阵可写成

$$A=\begin{pmatrix} A_1 & & O \\ & \ddots & \\ O & & A_m \end{pmatrix}，其中 A_i\in M_{d_i}(F)$$

$i=1,\dots,m.$

证：对 m 归纳：$m=1$ 显然

设 $m-1$ 时定理成立.

设 $W=U_2\oplus\cdots\oplus U_m$

由引理3.2 W 是 $\mathcal{A}$-子空间

$\therefore V=U_1\oplus W$

$\vec{e}_{11},\dots,\vec{e}_{1d_1}$ 是 U_1 的一组基

$\vec{e}_{21},\dots,\vec{e}_{2d_2},\dots,\vec{e}_{m1},\dots,\vec{e}_{md_k}$ 是 W 的基. 由命题3.2

~~$\mathcal{A}$ 在~~ 该基下的矩阵是

$$A=\begin{pmatrix} A_1 & O \\ O & C \end{pmatrix}，其中 A_1\in M_{d_1}(F)，C\in M_{n-d_1}(F)$$

~~由中~~ 对 $\mathcal{A}_W$ 和 W 利用归纳假设

$\mathcal{A}_W$ 在 $\vec{e}_{21},\dots,\vec{e}_{2d_2},\dots,\vec{e}_{m1},\dots,\vec{e}_{md_k}$

下的矩阵 ~~是~~ 可以写成

$$C=\begin{pmatrix} A_2 & & \\ & \ddots & \\ & & A_m \end{pmatrix}，其中 A_i\in M_{d_i}(F)$$

于是

$$A=\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_m \end{pmatrix}.$$ $\boxed{}$

§4 极小多项式

定义：设 $\mathcal{A} \in \mathcal{L}(V)$，$f \in F[t]$

如果 $f(\mathcal{A}) = \mathcal{O}$，则称 f 零化 $\mathcal{A}$。

设 $A \in M_n(F)$，如果

$f(A) = O$，则称 f 零化 A。

引理 4.1 (i) 设 $\mathcal{A} \in \mathcal{L}(V)$，则存在 $f \in F[t] \setminus \{0\}$ 零化 $\mathcal{A}$。(ii) 设 $A \in M_n(F)$，则存在 $f \in F[t] \setminus \{0\}$ 零化 A

证：(i) 由定理 3.2，$\mathcal{L}(V)$ 和 $M_n(F)$ 线性同构。于是

$$\dim \mathcal{L}(V) = \dim M_n(F) = n^2$$

于是 $\mathcal{A}^0 = \mathcal{E}, \mathcal{A}, \mathcal{A}^2, \cdots, \mathcal{A}^{n^2}$ 在 F 上线性相关。即

$\exists\, \alpha_0, \alpha_1, \cdots, \alpha_{n^2} \in F$，不全为零

满足

$$\alpha_0 \mathcal{E} + \alpha_1 \mathcal{A} + \cdots + \alpha_{n^2} \mathcal{A}^{n^2} = \mathcal{O}$$

设 $f(t) = \alpha_{n^2} t^{n^2} + \cdots + \alpha_1 t + \alpha_0 \in F[t] \setminus \{0\}$

满足 $f(\mathcal{A}) = \mathcal{O}$。 ☒

(ii) 类似。

定义：设 $\mathcal{A} \in \mathcal{L}(V)$，$A \in M_n(F)$。$F[t]$ 中非零且零化 $\mathcal{A}$ (A) 多项式中次数极小者称为 $\mathcal{A}$ (A) 的极小多项式

记为 $\mu_{\mathcal{A}}$ (μ_A)

通常：~~$\mu_{\mathcal{A}}$~~ 设：$\mu_{\mathcal{A}}$ 和 μ_A 首一。

引理 4.2 设 $f \in F[t]$

(i) 设 $\mathcal{A} \in \mathcal{L}(V)$ 且 f 零化 $\mathcal{A}$，则 $\mu_{\mathcal{A}}(t) \mid f(t)$

(ii) 设 $A \in M_n(F)$ ⋯⋯ A 则 $\mu_A(t) \mid f(t)$

证：(ii) 设 $p\in F[t]$ 满足 $p(A)=O_{n\times n}$

由多项式除法

$$p(t)=q(t)\mu_A(t)+r(t)$$

其中 $q,r\in F[t]$，$\deg r<\deg \mu_A$

则 $P(A)=q(A)\mu_A(A)+r(A)$

∵ $P(A)=O$，$\mu_A(A)=O$

∴ $r(A)=O$

由极小多项式定义，$r(t)=0$. ▨

(i) 类似

例：零算子 O 的极小多项式是 t

恒同算子的极小多项式是 $t-1$

例：设 $A\in M_n(F)$. 如果 μ_A 的次数为1

则 $A=\alpha E$，~~其中~~ $\alpha\in F$

证：设 $\mu_A=t-\alpha$，$\alpha\in F$

$$\mu_A(A)=A-\alpha E=O$$

$$A=\alpha E$$ ▨

例：设 $\mathcal{A}\in\mathcal{L}(V)$，$\mathcal{A}\neq\mathcal{O}$，$\mathcal{A}\neq\mathcal{E}$，$\mathcal{A}^2=\mathcal{A}$

则 $\mu_{\mathcal{A}}=t^2-t$.

证：设 $p(t)=t^2-t$.

则 $\mu_{\mathcal{A}}\mid p(t)$.

若 $\mu_{\mathcal{A}}(t)=t-\alpha$，则 $\mathcal{A}=\alpha\mathcal{E}$ (见上例)

$$\mathcal{A}^2=\mathcal{A}\Rightarrow \alpha^2\mathcal{E}=\alpha\mathcal{E}$$

$$\Rightarrow \alpha(\alpha-1)\mathcal{E}=\mathcal{O}$$

$\Rightarrow \alpha=0$，或 $\alpha=1$

$\Rightarrow \mathcal{A}=\mathcal{E}$ 或 $\mathcal{A}=\mathcal{O}$. →←

于是 $\mu_{\mathcal{A}}=t^2+\alpha t+\beta$，$\alpha,\beta\in F$

∵ $\mu_{\mathcal{A}}\mid p$ ∴ $\mu_{\mathcal{A}}=t^2-t$.

例：$\mathcal{D}: \mathbb{R}_n[x] \longrightarrow \mathbb{R}_n[x]$

$p(x) \longmapsto p'(x)$

$\mathcal{D}^n = \mathcal{O}$，但 $\mathcal{D}^{n-1}(x^{n-1}) \neq 0$

$\mu_{\mathcal{D}}(t) = t^n$.

~~命题~~4.1 设 $\mathcal{A} \in \mathcal{L}(V)$，$A$ 是 $\mathcal{A}$ 在 V 的某组基下的矩阵 则

(i) $\forall f \in F[t]$，$f(\mathcal{A}) = \mathcal{O} \Longleftrightarrow f(A) = O$

(ii) 特别地，$\mu_{\mathcal{A}} = \mu_A$

证：设 $\Phi: \mathcal{L}(V) \longrightarrow M_n(F)$ 为代数同构 满足 $\Phi(\mathcal{A}) = A$

（见定理2.2）

(i) $f(\mathcal{A}) = \mathcal{O} \Longleftrightarrow \Phi(f(\mathcal{A})) = \Phi(\mathcal{O})$

$\Longleftrightarrow f(\Phi(\mathcal{A})) = O_{n\times n}$

$\Longleftrightarrow f(A) = O_{n\times n}$

(ii)：由 (i) $\mu_{\mathcal{A}}(A) = O$，$\mu_A(\mathcal{A}) = O$

由引理4.2. $\mu_{\mathcal{A}} \mid \mu_A$，$\mu_A \mid \mu_{\mathcal{A}}$

$\because$ μ_A 和 $\mu_{\mathcal{A}}$ 都首一 $\therefore$ $\mu_A = \mu_{\mathcal{A}}$ ∎

~~命题~~4.2 设 $A, B \in M_n(F)$，$A \sim_s B$

则 $\mu_A = \mu_B$

证：设 $\mu_A(t) = t^d + \alpha_{d-1}t^{d-1} + \dots + \alpha_0$

$A = P^{-1}BP$，其中 $P \in GL_n(F)$

直接归纳得可知

$\forall k \in \mathbb{N} \quad A^k = P^{-1}B^kP$

$O = \mu_A(A) = A^d + \alpha_{d-1}A^{d-1} + \dots + \alpha_0 E$

$= P^{-1}B^dP + \alpha_{d-1}P^{-1}B^{d-1}P + \dots + \alpha_0 P^{-1}P$

$= P^{-1}(B^d + \alpha_{d-1}B^{d-1} + \dots + \alpha_0 E)P$

$\Rightarrow \quad B^d + \alpha_{d-1}B^{d-1} + \dots + \alpha_0 E = O$

即 $\mu_A(B)=O$. 同理 $\mu_B(A)=O$

由引理4.2 $\mu_A \mid \mu_B$ 且 $\mu_B \mid \mu_A$

于是 $\mu_A=\mu_B$ ▨

例：证明：$A=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$

不相似

证：$\mu_A=t-1$, μ_B 的次数不可能

是一次. 否则 $B=\alpha A$. $\Rightarrow \mu_A\neq\mu_B$

$\Rightarrow A \nsim_s B$

例：设 $A\in M_n(F)$，则 $\mu_A=\mu_{A^t}$

证：设 $\mu_A=t^d+\alpha_{d-1}t^{d-1}+\cdots+\alpha_1 t+\alpha_0$

$\mu_A(A)=A^d+\alpha_{d-1}A^{d-1}+\cdots+\alpha_1 A+\alpha_0 E=O$

$\left(A^d+\alpha_{d-1}A^{d-1}+\cdots+\alpha_1 A+\alpha_0 E\right)^t=O^t=O$

$\Rightarrow$

$(A^d)^t+\alpha_{d-1}(A^{d-1})^t+\cdots+\alpha_1 A^t+\alpha_0 E=O$

$\because \forall k\in\mathbb{N}$ $(A^d)^t=(A^t)^d$

$\therefore (A^t)^d+\alpha_{d-1}(A^t)^{d-1}+\cdots+\alpha_1 A^t+\alpha_0 E=O$

即 $\mu_A(A^t)=O \Rightarrow \mu_A \mid \mu_{A^t}$, $\mu_{A^t} \mid \mu_A$

同理 $\mu_{A^t}(A)=O$

$\Rightarrow \mu_A=\mu_{A^t}$.

~~命题4.3 设 $\mathcal{A}\in\mathcal{L}(V)$, $U\subset V$~~

~~是 $\mathcal{A}$-子空间. f 是 $\mathcal{A}|_U$ 的最小多项式~~

~~则 $f \mid \mu_{\mathcal{A}}$~~

引理4.3 设 $A=\begin{pmatrix}A_1&A_2\\O&A_3\end{pmatrix}\in M_n(F)$

其中 $A_1\in M_d(F)$. 设 $f\in F[t]$

则 $f(A)=\begin{pmatrix}B_1&B_2\\O&B_3\end{pmatrix}\in M_n(F)$

且 $B_1=f(A_1)$, $B_3=f(A_3)$

证：由矩阵分块的乘法

$$\begin{pmatrix} A_1 & A_2 \\ O & A_3 \end{pmatrix}^k = \begin{pmatrix} A_1^k & * \\ O & A_3^k \end{pmatrix}$$

设 $f = \sum_{i=0}^{d} \alpha_i t^i$

$$f(A) = \sum_{i=0}^{d} \alpha_i A^i = \sum_{i=0}^{d} \alpha_i \begin{pmatrix} A_1 & A_2 \\ O & A_3 \end{pmatrix}^i$$

$$= \sum_{i=0}^{d} \alpha_i \begin{pmatrix} A_1^i & * \\ O & A_3^i \end{pmatrix}$$

$$= \cancel{\sum} \begin{pmatrix} \sum_{i=0}^{d} \alpha_i A_1^i & \\ O & \sum_{i=0}^{d} \alpha_i A_3^i \end{pmatrix} = \begin{pmatrix} f(A_1) & * \\ O & f(A_3) \end{pmatrix} \boxtimes$$

~~定理4.1~~

引理4.4 ~~设~~

(i) 设 $A = \begin{pmatrix} A_1 & A_2 \\ O & A_3 \end{pmatrix}$

则 $\mu_{A_1} \mid \mu_A$, $\mu_{A_3} \mid \mu_A$

(ii) 设 $A = \begin{pmatrix} A_1 & O \\ O & A_3 \end{pmatrix}$

则 $\mu_A = \operatorname{lcm}(\mu_{A_1}, \mu_{A_3})$

<u>证：</u> (i) 由引理4.3

$$\mu_A(A) = \begin{pmatrix} \mu_A(A_1) & * \\ O & \mu_A(A_3) \end{pmatrix} = \begin{pmatrix} O & * \\ O & O \end{pmatrix}$$

$\Rightarrow \mu_A(A_1) = O$, $\mu_A(A_3) = O$

$\Rightarrow \mu_{A_1} \mid \mu_A$, $\mu_{A_3} \mid \mu_A$ (引理4.2)

(ii) 由 (i) μ_A 是 μ_{A_1} 和 μ_{A_3} 的公倍式. 设 $p = \operatorname{lcm}(\mu_{A_1}, \mu_{A_3})$，首一

则 $p(t) = f(t)\mu_{A_1}(t) = g(t)\mu_{A_3}(t)$，~~其中 $f, g \in F[t]$~~

$$p(A) = \begin{pmatrix} p(A_1) & O \\ O & p(A_3) \end{pmatrix} = \begin{pmatrix} f(A)\mu_{A_1}(A_1) & O \\ O & g(A)\mu_{A_3}(A_3) \end{pmatrix}$$

引理4.3

$$= \begin{pmatrix} O & O \\ O & O \end{pmatrix}$$

$\Rightarrow p(A) = O \Rightarrow \mu_{A}(t) \mid p(t)$ 由引理4.2

$\Rightarrow \mu_A(t) = p(t)$. $\boxtimes$