第二章 线性算子

§1 不同基底下线性映射的矩阵表示

§2 线性算子代数和矩阵相似

小结.

1. 线性映射(算子)与矩阵的对应. 设

$$\begin{array}{rccl}\Phi: & \mathrm{Hom}(V,W) & \longrightarrow & F^{m\times n} \\ & \phi & \mapsto & A, \quad \phi \text{ 在选定基底下的矩阵}\end{array}.$$

则 Φ 是线性同构.

设

$$\begin{array}{rccl}\Phi: & \mathcal{L}(V) & \longrightarrow & \mathrm{M}_n(F) \\ & \phi & \mapsto & A, \quad \phi \text{ 在选定基底下的矩阵}\end{array}.$$

则 Φ 是代数同构.

2. 基底变换与矩阵等价的对应. 设 V 和 W 是 F 上的线性空间, $\mathbf{e}_1,\ldots,\mathbf{e}_n$ 是 V 的一组基, $\epsilon_1,\ldots,\epsilon_m$ 是 W 的一组基.

(i) 设 $\phi\in\mathrm{Hom}(V,W)$ 在 $\mathbf{e}_1,\ldots,\mathbf{e}_n$ 和 $\epsilon_1,\ldots,\epsilon_m$ 下的矩阵是 $A\in F^{m\times n}$. 则 $A\sim_e B$ 当且仅当 B 是 ϕ 在 V 的某组基和 W 的某组基下的矩阵.

(ii) 设 $\mathcal{A}\in\mathcal{L}(V)$ 在 $\mathbf{e}_1,\ldots,\mathbf{e}_n$ 下的矩阵是 $A\in\mathrm{M}_n(F)$. 则 $A\sim_s B$ 当且仅当 B 是 $\mathcal{A}$ 在 V 的某组基下的矩阵.

证明. (i) 设 $A\sim_e B$. 则存在 $P\in\mathrm{GL}_n(F)$ 和 $Q\in\mathrm{GL}_m(F)$ 使得 $B=QAG$. 令

$$(\mathbf{e}_1',\ldots,\mathbf{e}_n')=(\mathbf{e}_1,\ldots,\mathbf{e}_n)P \quad \text{和} \quad (\epsilon_1',\ldots,\epsilon_m')=(\epsilon_1,\ldots,\epsilon_m)Q^{-1}.$$

则 B 是 ϕ 在 $\mathbf{e}_1',\ldots,\mathbf{e}_n'$ 和 $\epsilon_1',\ldots,\epsilon_m'$ 下的矩阵(第二章第一讲定理 1.11). 逆命题是第二章第一讲定理 1.11.

(ii) 设 $A\sim_s B$. 则存在 $P\in\mathrm{GL}_n(F)$ 使得 $P^{-1}AP$. 令 $(\mathbf{e}_1',\ldots,\mathbf{e}_n')=(\mathbf{e}_1,\ldots,\mathbf{e}_n)P$. 由第二章第一讲定理 1.11, B 是 $\mathcal{A}$ 在 $\mathbf{e}_1',\ldots,\mathbf{e}_n'$ 下的矩阵. 逆命题是第二章第一讲定理 1.11 的直接推论. □

§3 单个算子生成的子环

设 $\mathcal{A} \in \mathcal{L}(V)$. 令 $F[\mathcal{A}] = \langle \{\mathcal{A}^k \mid k \in \mathbb{N}\} \rangle$. 则

$$F[\mathcal{A}] = \{\alpha_k \mathcal{A}^k + \alpha_{k-1}\mathcal{A}^{k-1} + \cdots + \alpha_1 \mathcal{A} + \alpha_0 \mathcal{E} \mid k \in \mathbb{N}, \alpha_k, \alpha_{k-1}, \ldots, \alpha_0 \in F\}.$$

注意到 $F[\mathcal{A}] \subset \mathcal{L}(V)$. 对任意 $G, H \in F[\mathcal{A}]$, 我们有 $GH \in F[\mathcal{A}]$. 而且 $\mathcal{O}, \mathcal{E} \in F[\mathcal{A}]$. 于是 $F[\mathcal{A}]$ 是子环. 直接验证可得 $GH = HG$. 于是 $F[\mathcal{A}]$ 是交换环.

我们还可以从另一个角度看出 $F[\mathcal{A}]$ 是交换环. 设 A 是 $\mathcal{A}$ 在 $\mathbf{e}_1, \ldots, \mathbf{e}_n$ 下的矩阵. 则代数同构 $\Phi^{-1} : \mathrm{M}_n(F) \longrightarrow \mathcal{L}(V)$ 把交换环 $F[A]$ 映到 $F[\mathcal{A}]$. 因为 $F[A]$ 是交换环(见上学期第四章第二讲命题 3.4), 所以 $F[\mathcal{A}]$ 是交换环.

可直接验证映射

$$\begin{array}{rccc} \phi : & F & \longrightarrow & F[\mathcal{A}] \\ & \alpha & \mapsto & \alpha\mathcal{E} \end{array}$$

是环同态. 由多项式赋值同态定理, ϕ 可以扩展为一个从 $F[t]$ 到 $F[\mathcal{A}]$ 的环同态 $\phi_{\mathcal{A}}$ 满足 $\phi(t) = \mathcal{A}$. 通过赋值同态得到对任意 $f(t) = f_k t^k + f_{k-1} t^{k-1} + \cdots + f_1 t + f_9 \in F[t]$, 其中 $f_k, f_{k-1}, \ldots, f_1, f_0 \in F$ 得到

$$\phi_{\mathcal{A}}(f) = f_k \mathcal{A}^k + f_{k-1}\mathcal{A}^{k-1} + \cdots + f_1 \mathcal{A} + f_0 \mathcal{E} = f(\mathcal{A}).$$

且对任意 $p, q \in F[t]$, 我们有

$$(p+q)(\mathcal{A}) = p(\mathcal{A}) + q(\mathcal{A}) \quad 和 \quad (pq)(\mathcal{A}) = p(\mathcal{A})q(\mathcal{A}).$$

事实上, 上述赋值同态也可由赋值同态 $\phi_A : F[t] \longrightarrow F[A]$ 与 $\Phi^{-1} : F[A] \longrightarrow F[\mathcal{A}]$ 得到. 赋值同态 ϕ_A 的构造见上学期第五章讲义一命题 2.3.

由上一讲定理 1.9 可知, $\dim(\mathcal{L}(V)) = n^2$. 于是 $\mathcal{E}, \mathcal{A}, \ldots, \mathcal{A}^{n^2}$ 在 F 上必然线性相关. 换言之, 存在 $\alpha_0, \alpha_1, \ldots, \alpha_{n^2} \in F$, 不全为零, 使得

$$\alpha_0 \mathcal{E} + \alpha_1 \mathcal{A} + \cdots + \alpha_{n^2-1}\mathcal{A}^{n^2-1} + \alpha_{n^2}\mathcal{A}^{n^2} = \mathcal{O}.$$

于是 $\mathcal{A}$ 不可能是未定元. 对 $G \in F[\mathcal{A}]$, 我们不能直接定义 $\mathcal{A}$ 的“次数” 和 “系数”.

例 3.1 设 $\mathcal{A}$ 是数乘算子 $\lambda\mathcal{E}$, $f(t) = t^2 - 3t - \lambda^2$. 则

$$f(\mathcal{A}) = \mathcal{A}^2 - 3\mathcal{A} - \lambda^2\mathcal{E} = -3\mathcal{A} = -2\lambda\mathcal{E}. \quad \square$$

注解 3.2 赋值同态 $f(t) \mapsto f(\mathcal{A})$ 是交换环 $F[t]$ 到 $F[\mathcal{A}]$ 的满同态. 于是

$$F[\mathcal{A}] = \{p(\mathcal{A}) \mid p \in F[t]\} \quad 且 \quad F[A] = \{p(A) \mid p \in F[t]\}.$$

定理 3.3 *(核核分解)* 设 $\mathcal{A} \in \mathcal{L}(V)$, $p, q \in F[t]$ 互素. 如果 $(pq)(\mathcal{A}) = \mathcal{O}$, 则

$$V = \ker(p(\mathcal{A})) \oplus \ker(q(\mathcal{A})).$$

证明. 由 Bezout 关系, 存在 $u, v \in F[t]$ 使得 $u(t)p(t) + v(t)q(t) = 1$. 于是,

$$u(\mathcal{A})p(\mathcal{A}) + v(\mathcal{A})q(\mathcal{A}) = \mathcal{E}. \tag{1}$$

设 $\mathbf{x} \in V$. 则

$$\begin{aligned}
\mathbf{x} = \mathcal{E}(\mathbf{x}) &= (u(\mathcal{A})p(\mathcal{A}) + v(\mathcal{A})q(\mathcal{A}))(\mathbf{x}) \quad (\because\ (1)) \\
&= (u(\mathcal{A})p(\mathcal{A}))(\mathbf{x}) + (v(\mathcal{A})q(\mathcal{A}))(\mathbf{x}) \quad (\text{映射加法的定义}) \\
&= (p(\mathcal{A})u(\mathcal{A}))(\mathbf{x}) + (q(\mathcal{A})v(\mathcal{A}))(\mathbf{x}) \quad (F[\mathcal{A}]\ \text{是交换环}) \\
&= p(\mathcal{A})(\underbrace{u(\mathcal{A}))(\mathbf{x})}_{\mathbf{y}}) + q(\mathcal{A})(\underbrace{v(\mathcal{A})(\mathbf{x})}_{\mathbf{z}}). \quad (\text{乘法即复合}) \\
&= p(\mathcal{A})(\mathbf{y}) + q(\mathcal{A})(\mathbf{z}).
\end{aligned}$$

因为 $(pq)(\mathcal{A}) = \mathcal{O}$, 所以 $p(\mathcal{A})q(\mathcal{A}) = \mathcal{O}$. 于是 $q(\mathcal{A})(p(\mathcal{A})(\mathbf{y})) = \mathbf{0}$, 即 $p(\mathcal{A})(\mathbf{y}) \in \ker(q(\mathcal{A}))$. 类似可知 $q(\mathcal{A})(\mathbf{z}) \in \ker(p(\mathcal{A}))$. 我们得到 $\mathbf{x} \in \ker(p(\mathcal{A})) + \ker(q(\mathcal{A}))$. 由 $\mathbf{x}$ 的任意性推出 $V = \ker(p(\mathcal{A})) + \ker(q(\mathcal{A}))$.

再设 $\mathbf{x} \in \ker(p(\mathcal{A})) \cap \ker(q(\mathcal{A}))$. 则由 (1) 得出

$$\mathbf{x} = \mathcal{E}(\mathbf{x}) = u(\mathcal{A})p(\mathcal{A})(\mathbf{x}) + v(\mathcal{A})q(\mathcal{A})(\mathbf{x}) = \mathbf{0}.$$

从而 $V = \ker(p(\mathcal{A})) \oplus \ker(q(\mathcal{A}))$. □

例 3.4 设 $\mathcal{A} \in \mathcal{L}(A)$ 满足 $\mathcal{A}^2 = \mathcal{E}$. 证明: 当 F 的特征不等于 2 时,

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

证明. 由核像版的对偶公式*(第一章第二讲命题 4.15 (iii) 和上一讲注释 1.16)*, 我们只要证明

$$\dim(\ker(\mathcal{A} - \mathcal{E})) + \dim(\ker(\mathcal{A} + \mathcal{E})) = \dim(V).$$

设 $f(t) = t^2 - 1$. 则 $f(\mathcal{A}) = \mathcal{A}^2 - \mathcal{E} = \mathcal{O}$. 设 $p = (t-1)$, $q = (t+1)$. 因为 $pq = f$, 所以 $(pq)(\mathcal{A}) = \mathcal{O}$. 因为 F 的特征不等于 2, 所以 $\gcd(p, q) = 1$. 由核核分解定理可知

$$V = \ker(p(\mathcal{A})) \oplus \ker(q(\mathcal{A})).$$

又因为 $p(\mathcal{A}) = \mathcal{A} - \mathcal{E}$ 和 $q(\mathcal{A}) = \mathcal{A} + \mathcal{E}$, 所以

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

(直和维数的基本性质—第一章第二讲命题 4.16). □

满足 $\mathcal{A}^2=\mathcal{E}$的算子称为对合算子. 典型例子是矩阵

$$\begin{pmatrix} E_k & O \\ O & -E_\ell \end{pmatrix}.$$

定理 3.5 *(核像分解 I)*[1] 设 $\mathcal{A}\in\mathcal{L}(V)$. 则

$$V=\ker(\mathcal{A})\oplus\operatorname{im}(\mathcal{A}) \iff \operatorname{rank}(\mathcal{A})=\operatorname{rank}(\mathcal{A}^2).$$

证明. 断言. 对任意 $\mathcal{A}\in\mathcal{L}(V)$, $\ker(\mathcal{A})\subset\ker(\mathcal{A}^2)$, $\operatorname{im}(\mathcal{A})\supset\operatorname{im}(\mathcal{A}^2)$.

断言的证明. 设 $\mathbf{v}\in\ker(\mathcal{A})$. 则 $\mathcal{A}^2(\mathbf{v})=\mathcal{A}(\mathcal{A}(\mathbf{v}))=\mathcal{A}(\mathbf{0})=\mathbf{0}$. 设 $\mathbf{y}\in\operatorname{im}(\mathcal{A}^2)$. 则存在 $\mathbf{z}\in V$ 使得 $\mathbf{y}=\mathcal{A}^2(\mathbf{z})$. 于是 $\mathbf{y}=\mathcal{A}(\mathcal{A}(\mathbf{z}))\in\operatorname{im}(\mathcal{A})$. 断言成立.

($\Longleftarrow$) 因为 $\operatorname{rank}(\mathcal{A})=\operatorname{rank}(\mathcal{A}^2)$, 所以 $\dim(\ker(\mathcal{A}))=\dim(\ker(\mathcal{A}^2))$. 这是因为 $\dim(\ker(\mathcal{A}))+\operatorname{rank}(\mathcal{A})=\dim(\ker(\mathcal{A}^2))+\operatorname{rank}(\mathcal{A}^2)$ (上一讲注释 1.16). 由断言可知 $\ker(\mathcal{A})=\ker(\mathcal{A}^2)$. 设 $\mathbf{x}\in\ker(\mathcal{A})\cap\operatorname{im}(\mathcal{A})$. 则存在 $\mathbf{y}\in V$ 使得 $\mathbf{x}=\mathcal{A}(\mathbf{y})$ 且 $\mathcal{A}(\mathbf{x})=\mathbf{0}$. 于是 $\mathcal{A}^2(\mathbf{y})=\mathbf{0}$. 因为 $\ker(\mathcal{A})=\ker(\mathcal{A}^2)$, 所以 $\mathbf{y}\in\ker(\mathcal{A})$. 于是 $\mathbf{x}=\mathbf{0}$. 即 $\ker(\mathcal{A})+\operatorname{im}(\mathcal{A})$ 是直和. 于是 $\dim(\ker(\mathcal{A})+\operatorname{im}(\mathcal{A}))=\dim(\ker(\mathcal{A}))+\dim(\operatorname{im}(\mathcal{A}))=\dim(V)$. 我们得出 $V=\ker(\mathcal{A})\oplus\operatorname{im}(\mathcal{A})$.

($\Longrightarrow$) 由断言和推论 1,14 可知, 我们只要证明 $\operatorname{im}(\mathcal{A})\subset\operatorname{im}(\mathcal{A}^2)$ 即可. 设 $\mathbf{x}\in\operatorname{im}(\mathcal{A})$. 则存在 $\mathbf{y}\in V$ 使得 $\mathbf{x}=\mathcal{A}(\mathbf{y})$. 因为 $V=\ker(\mathcal{A})+\operatorname{im}(\mathcal{A})$, 所以存在 $\mathbf{u}\in\ker(\mathcal{A})$, $\mathbf{v}\in\operatorname{im}(\mathcal{A})$ 使得 $\mathbf{y}=\mathbf{u}+\mathbf{v}$ 且 $\mathbf{v}=\mathcal{A}(\mathbf{w})$, 其中 $\mathbf{w}$ 是 V 中某个向量. 于是 $\mathbf{x}=\mathbf{u}+\mathcal{A}(\mathbf{w})$, 从而 $\mathbf{x}=\mathcal{A}(\mathbf{y})=\mathcal{A}(\mathbf{u})+\mathcal{A}^2(\mathbf{w})=\mathcal{A}^2(\mathbf{w})\in\operatorname{im}(\mathcal{A}^2)$. 我们有 $\operatorname{im}(\mathcal{A})\subset\operatorname{im}(\mathcal{A}^2)$. □

注解 3.6 由上述定理和证明中的断言可知, 以下结论是彼此等价的.

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

(ii) $\operatorname{rank}(\mathcal{A})=\operatorname{rank}(\mathcal{A}^2)$;

(iii) $\operatorname{im}(\mathcal{A})=\operatorname{im}(\mathcal{A}^2)$;

(iv) $\ker(\mathcal{A})=\ker(\mathcal{A}^2)$;

(v) $\dim(\ker(\mathcal{A}))=\dim(\ker(\mathcal{A}^2))$.

例 3.7 设 $\mathcal{A}\in\mathcal{L}(V)$ 满足 $\mathcal{A}^2=\mathcal{A}$. 证明

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

证明. 因为 $\mathcal{A}^2=\mathcal{A}$, 所以 $\operatorname{rank}(\mathcal{A}^2)=\operatorname{rank}(\mathcal{A})$. 由上述核像分解定理可知结论成立. □

例 3.8 设 $\mathcal{D}$ 是 $\mathbb{R}[x]_n$ 上的导数算子. 则 $\ker(\mathcal{D})=\mathbb{R}$ 且 $\operatorname{im}(\mathcal{D})=\mathbb{R}[x]_{n-1}$. 因为 $\mathbb{R}\subset\mathbb{R}[x]_{n-1}$, 所以 $\ker(\mathcal{D})+\operatorname{im}(\mathcal{D})$ 不是直和.

[1]袁力, 沈洁. 常州工学院学报 27 卷第二期, 2014 年 4 月.

§4 算子和矩阵的极小多项式

定义 4.1 设 $f \in F[t]$, $\mathcal{A} \in \mathcal{L}(V)$. 如果 $f(\mathcal{A}) = \mathcal{O}$, 则称 f 是关于 $\mathcal{A}$ 的零化多项式. 关于 $\mathcal{A}$ 的非零的零化多项式中次数最小的称为 $\mathcal{A}$ 的极小多项式. 为明确起见, 我们设极小多项式是首一的.

类似地, 对 $A \in \mathrm{M}_n(F)$, 我们有关于 A 的零化多项式和极小多项式的概念.

引理 4.2 设 $\mathcal{A} \in \mathcal{L}(V)$, $f(t) \in F[t]$, $p(t)$ 是 $\mathcal{A}$ 的极小多项式. 则

$$f(\mathcal{A}) = \mathcal{O} \iff p|f.$$

证明. 由多项式除法可知 $f(t) = q(t)p(t) + r(t)$, 其中 $q, r \in F[t]$ 且 $\deg(r) < \deg(p)$. 由赋值同态定理 $f(\mathcal{A}) = q(\mathcal{A})p(\mathcal{A}) + r(\mathcal{A})$. 因为 $p(\mathcal{A}) = \mathcal{O}$, 所以 $f(\mathcal{A}) = r(\mathcal{A})$.

如果 $f(\mathcal{A}) = \mathcal{O}$, 则 $r(\mathcal{A}) = \mathcal{O}$. 由极小多项式的定义可知, $r(t) = 0$. 如果 $r(t) = 0$, 则 $r(\mathcal{A}) = \mathcal{O}$. 于是, $f(\mathcal{A}) = \mathcal{O}$. □

命题 4.3 设 $\mathcal{A} \in \mathcal{L}(V)$. 则 $\mathcal{A}$ 的极小多项式存在且唯一. 极小多项式的次数不大于 n^2.

证明. 因为 $\dim(\mathcal{L}(V)) = n^2$, 所以 $1, \mathcal{A}, \ldots, \mathcal{A}^{n^2}$ 在 F 上线性相关. 由此可知, $\mathcal{A}$ 有非零的次数不高于 n^2 的零化多项式. 于是, 极小多项式存在且次数不高于 n^2. 设 p, q 是 $\mathcal{A}$ 的两个极小多项式. 则 $\deg(p) = \deg(q)$. 由引理 4.2, $p|q$ 且 $q|p$. 于是 $p = cq$, 其中 $c \in F \setminus \{0\}$. 因为 p 和 q 都首一, 所以 $c = 1$. □

注解 4.4 以上结论对 $A \in \mathrm{M}_n(F)$ 同样成立.

记号. 设 $\mathcal{A} \in \mathcal{L}(V)$, $A \in \mathrm{M}_n(F)$. 它们的极小多项式分别记为 $\mu_{\mathcal{A}}$ 和 μ_A.

注解 4.5 设 $\mathcal{A} \in \mathcal{L}(V)$, A 是 $\mathcal{A}$ 在 V 某组基下的矩阵. 则 $\mu_{\mathcal{A}} = \mu_A$. 这是因为 $F[\mathcal{A}]$ 和 $F[A]$ 代数同构.

例 4.6 设 $\mathcal{A} \in \mathcal{L}(V)$. 证明 $\deg(\mu_{\mathcal{A}}) = 1$ 当且仅当 $\mathcal{A}$ 是数乘算子.
证明. 设 $\mathcal{A} = \lambda\mathcal{E}$, $\lambda \in F$. 则 $\mu_{\mathcal{A}} = t - \lambda$. 反之, 设 $\mu_{\mathcal{A}} = t - \lambda$. 则 $\mathcal{O} = \mu_{\mathcal{A}}(\mathcal{A}) = \mathcal{A} - \lambda\mathcal{E}$. 于是, $\mathcal{A} = \lambda\mathcal{E}$. □

特别地, $\mu_{\mathcal{O}} = t$, $\mu_{\mathcal{E}} = t - 1$.

例 4.7 设 $\mathcal{A} \in \mathcal{L}(V)$ 是幂零算子. 证明 $\mu_{\mathcal{A}}$ 是 t 的幂次.
证明. 设 $\mathcal{A}^k = \mathcal{O}$. 则 t^k 零化 $\mathcal{A}$. 由引理 *4.2*, $\mu_{\mathcal{A}}|t^k$. 于是 $\mu_{\mathcal{A}}$ 是 t 的幂次. □

引理 4.8 设 $A, B \in \mathrm{M}_n(F), P \in \mathrm{GL}_n(F)$ 使得 $B = P^{-1}AP$. 设 $f \in F[t]$. 则

$$f(B) = P^{-1}f(A)P.$$

特别地, $A \sim_s B \implies f(A) \sim_s f(B)$.

证明. 直接计算得对任意 $i \in \mathbb{N}$,

$$B^i = \underbrace{(P^{-1}AP)(P^{-1}AP)\cdots(P^{-1}AP)(P^{-1}AP)}_{i} = P^{-1}A^iP.$$

设 $f(t) = f_kt^k + f_{k-1}t^{k-1} + \cdots + f_1t + f_0$. 则

$$f(B) = f_kP^{-1}A^kP + f_{k-1}P^{-1}A^{k-1}P + \cdots + f_1P^{-1}AP + f_0P^{-1}EP = P^{-1}f(A)P. \quad \square$$

命题 4.9 设 $A, B \in \mathrm{M}_n(F)$. 如果 $A \sim_s B$, 则 $\mu_A = \mu_B$.

证明. 由引理 4.8 和 $\mu_A(A) = O$ 可知, $\mu_A(B) = O$. 于是 $\mu_B|\mu_A$ (引理 4.2). 同理 $\mu_A|\mu_B$. 因为 μ_A 和 μ_B 都首一, 所以 $\mu_A = \mu_B$. $\square$

例 4.10 设

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

问 A 和 B 是否相似?

解. 注意到 $\mu_A = t - 1$. 因为 B 不是数乘矩阵, 所以 $\deg(\mu_B) > 1$ *(例 4.6)*. 于是, $\mu_A \neq \mu_B$. 故 $A \nsim_s B$. $\square$

例 4.11 设 $A, B \in \mathrm{M}_n(F)$, A 是数乘矩阵, B 是幂零矩阵. 则

$$A \sim_s B \iff A = B = O.$$

证明. 由例 *4.6* 和 例 *4.7* 可知, $\mu_A = t - \lambda$, $\mu_B = t^k$, 其中 $\lambda \in F, k \in \mathbb{Z}^+$. 设 $A \sim_s B$. 则 $\mu_A = \mu_B$ *(命题 4.9)*. 于是 $\lambda = 0$ 且 $k = 1$. 由此得出 $A = O$ 和 $B = O$. 另一个方向是平凡的. $\square$

命题 4.12 设 $\mathcal{A} \in \mathcal{L}(V)$. 则 $\dim(F[\mathcal{A}]) = \deg(\mu_{\mathcal{A}})$ 且 $\mathcal{A}$ 可逆当且仅当 $\mu_{\mathcal{A}}(0) \neq 0$.

证明. 设 $d = \deg_t(\mu_{\mathcal{A}})$. 我们来证明 $\mathcal{E}, \mathcal{A}, \ldots, \mathcal{A}^{d-1}$ 是 $F[\mathcal{A}]$ 的一组基.

设 $\alpha_0, \alpha_1, \ldots, \alpha_{d-1} \in F$ 使得

$$\alpha_0\mathcal{E} + \alpha_1\mathcal{A} + \cdots + \alpha_{d-1}\mathcal{A}^{d-1} = \mathcal{O}.$$

令 $p(t)=\alpha_0+\alpha_1 t+\cdots+\alpha_{d-1}t^{d-1}\in F[t]$. 则 $p(\mathcal{A})=\mathcal{O}$. 因为 $\deg_t(p)<d$, 所以 $p=0$. 于是, $\alpha_0=\alpha_1=\cdots=\alpha_{d-1}=0$. 我们推出 $\mathcal{E}$, $\mathcal{A}$, $\ldots$, $\mathcal{A}^{d-1}$ 线性无关.

设 $G\in F[\mathcal{A}]$. 则存在 $g\in F[t]$ 使得 $G=g(\mathcal{A})$. 由多项式带余除法可知, 存在 $q,r\in F[t]$, $\deg_t(r)<d$ 使得

$$g(t)=q(t)\mu_{\mathcal{A}}(t)+r(t).$$

于是

$$G=g(\mathcal{A})=q(\mathcal{A})\mu_{\mathcal{A}}(\mathcal{A})+r(\mathcal{A})=r(\mathcal{A}).$$

即 G 是 $\mathcal{E},\mathcal{A},\ldots,\mathcal{A}^{d-1}$ 在 F 上的线性组合. 于是 $\mathcal{E}$, $\mathcal{A}$, $\ldots$, $\mathcal{A}^{d-1}$ 是 $F[\mathcal{A}]$ 的一组基. 特别地, $\dim(F[\mathcal{A}])=d$.

设 $\mu_{\mathcal{A}}=\beta_0+\beta_1 t+\cdots+\beta_{d-1}t^{d-1}+t^d$, 其中 $\beta_0,\beta_1,\ldots,\beta_{d-1}\in F$. 则

$$\mathcal{O}=\beta_0\mathcal{E}+\beta_1\mathcal{A}+\cdots+\beta_{d-1}\mathcal{A}^{d-1}+\mathcal{A}^d.$$

如果 $\mu_{\mathcal{A}}(0)\neq 0$, 则 $\beta_0\neq 0$. 于是

$$\mathcal{A}\underbrace{(-\beta_1\mathcal{E}-\cdots+\beta_{d-1}\mathcal{A}^{d-2}-\mathcal{A}^{d-1})\beta_0^{-1}}_{\mathcal{A}^{-1}}=\mathcal{E}. \tag{2}$$

即 $\mathcal{A}$ 可逆. 设 $\mathcal{A}$ 可逆. 如果 $\mu_{\mathcal{A}}(0)=0$, 则 $\beta_0=0$. 于是

$$\mu_{\mathcal{A}}(t)=t(\beta_1+\beta_2 t+\cdots+\beta_{n-1}t^{n-2}+t^{n-1}).$$

于是

$$\mathcal{O}=\mathcal{A}(\beta_1\mathcal{E}+\beta_2\mathcal{A}+\cdots+\beta_{d-1}\mathcal{A}^{d-2}+\mathcal{A}^{d-1}).$$

把上述等式两边同乘以 $\mathcal{A}^{-1}$. 则

$$\mathcal{O}=\beta_1\mathcal{E}+\beta_2\mathcal{A}+\cdots+\beta_{d-1}\mathcal{A}^{d-2}+\mathcal{A}^{d-1}.$$

我们看到非零多项式 $\beta_1+\beta_2 t+\cdots+\beta_{d-1}t^{d-2}+t^{d-1}$ 零化 $\mathcal{A}$. 矛盾. □

注解 4.13 由 (2) 可知, 当 $\mathcal{A}$ 可逆时, $\mathcal{A}^{-1}\in F[\mathcal{A}]$.

§5 $F[t]$ 中的最小公倍式(复习与加细)

设 $p_1,\ldots,p_k,p\in F[t]\setminus\{0\}$. 如果 $p_i|p$, $i=1,2,\ldots,k$, 则称 p 是 $p_1,\ldots,p_k$ 的公倍式. 设 $q\in F[t]$ 是 $p_1,\ldots,p_k$ 的公倍式且它们的任何公倍式都被 q 整除, 则称 q 是 $p_1,\ldots,p_k$ 是最小公倍式.

命题 5.1 设 $p_1,\dots,p_k\in F[t]\setminus\{0\}$. 则它们的最小公倍式存在, 它们的两个最小公倍式在 F 上相伴(即它们在 F 上线性相关).

证明. 显然 $p_1p_2\cdots p_k$ 是 $p_1,\dots,p_k$ 的公倍式. 设 q 是 $p_1,\dots,p_k$ 的公倍式中次数最小的. 再设 p 是 $p_1,\dots,p_k$ 的公倍式. 由多项式带余除法

$$p=fq+r,$$

其中 $f,r\in F[t]$, 且 $\deg(r)<\deg(q)$. 因为 $p_i|p, p_i|q$, 所以 $p_i|r$ (见上学期第五章讲义一引理 2.5 (ii)), $i=1,2,\dots,k$. 于是, $q|r$. 因为 $\deg(q)>\deg(r)$, 所以 $r=0$. 即 $q|p$, q 是 $p_1,\dots,p_k$ 的最小公倍式.

再设 h 是 $p_1,\dots,p_k$ 的另一个公倍式. 则 $h|q$ 且 $q|h$. 于是 h 和 q 在 F 上相伴. □.

设 $p_1,\dots,p_k\in F[t]\setminus\{0\}$. 它们的(首一的)极小公倍式)记为 $\operatorname{lcm}(p_1,\dots,p_k)$.

命题 5.2 设 $p_1,\dots,p_k\in F[t]\setminus\{0\}$, 其中 $k>2$. 则

$$\operatorname{lcm}(p_1,\dots,p_{k-1},p_k)=\operatorname{lcm}(\operatorname{lcm}(p_1,\dots,p_{k-1}),\,p_k).$$

证明. 设

$$f=\operatorname{lcm}(p_1,\dots,p_{k-1},p_k)\quad 和 \quad g=\operatorname{lcm}(\operatorname{lcm}(p_1,\dots,p_{k-1}),\,p_k).$$

因为 $\operatorname{lcm}(p_1,\dots,p_{k-1})|f$ 和 $p_k|f$, 所以 $g|f$. 反之 $p_i|\operatorname{lcm}(p_1,\dots,p_{k-1})$, $i=1,2,\dots,k-1$, 和 $\operatorname{lcm}(p_1,\dots,p_{k-1})|g$ 蕴含 $p_i|g$, $i=1,\dots,k-1$. 再由 $p_k|g$, 我们得到 g 是 $p_1,\dots,p_{k-1},p_k$ 的公倍式. 于是, $f|g$. 再利用首一性可知, $f=g$. □

定理 5.3 设 $f,g\in F[t]\setminus\{0\}$. 则 $\operatorname{lcm}(f,g)=fg/\gcd(f,g)$.

证明. 设 $h=\gcd(f,g)$. 则存在 $a,b\in F[t]$ 使得 $f=ah$, $g=bh$ 且 $\gcd(a,b)=1$. 令 $\ell=fg/h$. 则

$$\ell=ag=bf. \tag{3}$$

于是, ℓ 是 f 和 g 的公倍式.

再设 w 是 f 和 g 的公倍式. 则存在 $p,q\in F[t]$ 使得 $w=pf=qg$. 由 Bezout 关系, 存在 $u,v\in F[t]$ 使得

$$ua+vb=1\implies uaw+vbw=w\implies uaqg+vbpf=w\overset{(3)}{\implies}\ell(uq+vp)=w\implies\ell|w.$$

于是, $\ell=\operatorname{lcm}(f,g)$. □

推论 5.4 设 $f,g\in F[t]\setminus\{0\}$ 且 $\gcd(f,g)=1$. 则 $\operatorname{lcm}(f,g)=fg$.

引理 5.5 设 $p_1,\dots,p_k\in F[t]\setminus\{0\}$ 两两互素. 则 $p_1\cdots p_{k-1}$ 与 p_k 互素.

证明. 由 Bezout 关系, 存在 $u_i, v_i \in F[t]$ 使得 $u_ip_i + v_ip_k = 1$, $i = 1, \ldots, k-1$. 于是

$$1 = \prod_{i=1}^{k-1}(u_ip_i + v_ip_k) = (u_1 \cdots u_{k-1})(p_1 \cdots p_{k-1}) + vp_k,$$

其中 v 是 $F[t]$ 中某个多项式. 于是, $p_1 \cdots p_{k-1}$ 与 p_k 互素. □

命题 5.6 设 $p_1, \ldots, p_k \in F[t] \setminus \{0\}$ 两两互素. 则 $\mathrm{lcm}(p_1, \ldots, p_{k-1}, p_k) = p_1 \cdots p_{k-1}p_k$.

证明. 对 k 归纳. 当 $k = 2$ 时, 结论是推论 5.4. 设 $k > 2$ 且结论对 $k-1$ 个两两互素的多项式成立. 根据命题 5.1,

$$\mathrm{lcm}(p_1, \ldots, p_{k-1}, p_k) = \mathrm{lcm}(\mathrm{lcm}(p_1, \ldots, p_{k-1}), p_k) = \mathrm{lcm}(p_1 \cdots p_{k-1}, p_k) = p_1 \cdots p_{k-1}p_k. \quad \square$$

§6 不变子空间

定义 6.1 设 $\mathcal{A} \in \mathcal{L}(V)$, U 是 V 的子空间. 如果 $\mathcal{A}(U) \subset U$, 即 $\forall \mathbf{u} \in U, \mathcal{A}(\mathbf{u}) \in U$, 则称 U 是 $\mathcal{A}$ 的不变子空间.

设 U 是 $\mathcal{A}$ 的不变子空间. 则 $A|_U$ 可以看做 U 上的线性算子. 为简明起见, 记限制映射 $A|_U$ 为 $\mathcal{A}_U$. 注意到 $\mathcal{A}_U \in \mathcal{L}(U)$.

例 6.2 设 $\mathcal{D}$ 是 $\mathbb{R}[x]_n$ 上的导数算子. 则 $\mathbb{R}[x]_k$ 是 $\mathcal{D}$ 的不变子空间, $k = 1, 2, \ldots, n$. 但 $\langle x^k \rangle$ 不是, $k = 0, 1, \ldots, n-1$.

设 $\lambda \in F$, 则 V 的每个子空间都是 $\lambda\mathcal{E}$ 的不变的.

命题 6.3 设 $\mathcal{A} \in \mathcal{L}(V)$, U 是 $\mathcal{A}$ 的 d 维不变子空间, $0 < d < n$. 则存在 V 的一组基使得 $\mathcal{A}$ 在该基下的矩阵为

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

其中 $B \in \mathrm{M}_d(F)$ 是 $\mathcal{A}_U$ 的某个矩阵表示. 进而 $\mu_{\mathcal{A}_U} | \mu_{\mathcal{A}}$, $\mu_B | \mu_A$, $\mu_D | \mu_A$.

证明. 设 $\mathbf{e}_1, \ldots, \mathbf{e}_d$ 是 U 的一组基. 把它扩充为 V 的一组基 $\mathbf{e}_1, \ldots, \mathbf{e}_d, \mathbf{e}_{d+1}, \ldots, \mathbf{e}_n$. 因为 U 是 $\mathcal{A}$ 的不变子空间, 所以当 $j \in \{1, 2, \ldots, d\}$ 时, $\mathcal{A}(\mathbf{e}_j)$ 是 $\mathbf{e}_1, \ldots, \mathbf{e}_d$ 的线性组合, 即 $\mathcal{A}(\mathbf{e}_j)$ 关于 $\mathbf{e}_{d+1}, \ldots, \mathbf{e}_n$ 的坐标都等于零. 于是 $\mathcal{A}$ 在 $\mathbf{e}_1, \ldots, \mathbf{e}_d, \mathbf{e}_{d+1}, \ldots, \mathbf{e}_n$ 下的矩阵如命题所述形式, 且 B 是 $\mathcal{A}_U$ 在 $\mathbf{e}_1, \ldots, \mathbf{e}_d$ 下的矩阵.

直接计算可验证对任意 $k \in \mathbb{N}$

$$A^k = \begin{pmatrix} B^k & * \\ O & D^k \end{pmatrix},$$

其中 $*$ 是某个 $n\times(n-d)$ 阶的矩阵. 于是, 对任意 $f\in F[t]$.

$$f(A)=\begin{pmatrix} f(B) & * \\ O & f(D)\end{pmatrix}.$$

因为 $\mu_A(A)=O_{n\times n}$, 所以 $\mu_A(B)=O_{d\times d}$, $\mu_A(D)=O_{(n-d)\times(n-d)}$. 由引理 4.2, $\mu_B|\mu_A$, $\mu_D|\mu_A$, 且 $\mu_{\mathcal{A}_U}|\mu_{\mathcal{A}}$. □

给定 $\mathcal{A}\in\mathcal{L}(V)$, $\{\mathbf{0}\}$ 和 V 是 $\mathcal{A}$ 的平凡的不变子空间. 下面的引理指出如何寻找 $\mathcal{A}$ 的非平凡的子空间.

引理 6.4 *设 $\mathcal{A},\mathcal{B}\in\mathcal{L}(V)$ 满足 $\mathcal{AB}=\mathcal{BA}$. 则 $\ker(\mathcal{B})$ 和 $\mathrm{im}(\mathcal{B})$ 是 $\mathcal{A}$ 的不变子空间.*

证明. 设 $\mathbf{x}\in\ker(B)$. 则 $\mathcal{B}(\mathcal{A}(\mathbf{x}))=(\mathcal{BA})(\mathbf{x})=(\mathcal{AB})(\mathbf{x})=\mathcal{A}(\mathcal{B}(\mathbf{x}))=\mathcal{A}(\mathbf{0})=\mathbf{0}$. 于是 $\mathcal{A}(\mathbf{x})\in\ker(\mathcal{B})$. 即 $\ker(\mathcal{B})$ 是 $\mathcal{A}$ 不变的. 设 $\mathbf{x}\in\mathrm{im}(\mathcal{B})$. 则存在 $\mathbf{y}\in V$ 使得 $\mathbf{x}=\mathcal{B}(\mathbf{y})$. 于是 $\mathcal{A}(\mathbf{x})=\mathcal{A}(\mathcal{B}(\mathbf{y}))=\mathcal{B}(\mathcal{A}(\mathbf{y}))\in\mathrm{im}(\mathcal{B})$. □

命题 6.5 *设 $\mathcal{A}\in\mathcal{L}(V)$, $f\in F[t]$. 则 $\ker(f(\mathcal{A}))$ 和 $\mathrm{im}(f(\mathcal{A}))$ 都是 $\mathcal{A}$ 的不变子空间.*

证明. 因为 $\mathcal{A}f(\mathcal{A})=f(\mathcal{A})\mathcal{A}$, 所以 $\ker(f(\mathcal{A}))$ 和 $\mathrm{im}(f(\mathcal{A}))$ 都是 $\mathcal{A}$ 的不变子空间(引理 6.4). □

为了简单起见, 当 U 是 $\mathcal{A}$ 的不变子空间时, 我们说 U 是 $\mathcal{A}$-不变的或许 $\mathcal{A}$-子空间.

命题 6.6 *设 $\mathcal{A}\in\mathcal{L}(V)$, U_1,U_2 是 $\mathcal{A}$-子空间. 则 U_1+U_2 和 $U_1\cap U_2$ 都是 $\mathcal{A}$-子空间.*

证明. 设 $\mathbf{x}\in U_1+U_2$. 则存在 $\mathbf{x}_1\in U_1$, $\mathbf{x}_2\in U_2$ 使得 $\mathbf{x}=\mathbf{x}_1+\mathbf{x}_2$. 于是,

$$\mathcal{A}(\mathbf{x})=\mathcal{A}(\mathbf{x}_1)+\mathcal{A}(\mathbf{x}_2)\in U_1+U_2.$$

设 $\mathbf{x}\in U_1\cap U_2$, 则 $\mathcal{A}(\mathbf{x})\in U_1$ 且 $\mathcal{A}(\mathbf{x})\in U_2$. 由此可知, $\mathcal{A}(\mathbf{x})\in U_1\cap U_2$. □

引理 6.7 *设 $\mathcal{A}\in\mathcal{L}(V)$, U_1,U_2 是非平凡 $\mathcal{A}$-子空间, 且 $V=U_1\oplus U_2$. 设 $\epsilon_1,\ldots,\epsilon_{d_1}$ 是 U_1 的基, $\delta_1,\ldots,\delta_{d_2}$ 是 U_2 的基则在 V 的基底 $\epsilon_1,\ldots,\epsilon_{d_1},\delta_1,\ldots,\delta_{d_2}$ 下 $\mathcal{A}$ 的矩阵是*

$$A=\begin{pmatrix} A_1 & O \\ O & A_2\end{pmatrix},$$

其中 $A_i\in\mathrm{M}_{d_i}(F)$ 是 $\mathcal{A}_{U_i}$ 在对应基下的矩阵, $i=1,2$. 进而 $\mu_{\mathcal{A}}=\mathrm{lcm}(\mu_{\mathcal{A}_{V_1}},\mu_{\mathcal{A}_{V_2}})$ (取首一的最小公倍式).

证明. 注意到 $V=U_1\oplus U_2$ 蕴含 $d_1+d_2=n(=\dim(V))$ 且 $\epsilon_1,\ldots,\epsilon_{d_1},\delta_1,\ldots,\delta_{d_2}$ 线性无关. 所以 $\epsilon_1,\ldots,\epsilon_{d_1},\delta_1,\ldots,\delta_{d_2}$ 是 V 的一组基. 对 $i\in\{1,2,\ldots,d_1\}$, $\mathcal{A}(\epsilon_i)\in U_1$, $\mathcal{A}(\epsilon_i)$ 是 $\epsilon_1,\ldots,\epsilon_{d_1}$ 的线性组合, 它关于 $\delta_1,\ldots,\delta_{d_2}$ 的坐标都是零. 于是, 存在 $A_1\in\mathrm{M}_{d_1}(F)$ 使得

$$(\mathcal{A}(\epsilon_1),\ldots,\mathcal{A}(\epsilon_{d_1}))=(\epsilon_1,\ldots,\epsilon_{d_1})A_1.$$

类似地, 存在 $A_2 \in \mathrm{M}_{d_1}(F)$ 使得

$$(\mathcal{A}(\delta_1), \dots, \mathcal{A}(\delta_{d_1})) = (\delta_1, \dots, \delta_{d_2})A_2.$$

于是 A_i 是 $\mathcal{A}_{U_i}$ 在对应基底下的矩阵, $i = 1, 2$. 进而, $\mathcal{A}$ 在 V 的基底 $\epsilon_1, \dots, \epsilon_{d_1}, \delta_1, \dots, \delta_{d_2}$ 下的矩阵等于 A.

设 $p = \mathrm{lcm}(\mu_{\mathcal{A}_{U_1}}, \mu_{\mathcal{A}_{U_2}})$. 由引理 6.3, $\mu_{\mathcal{A}_{U_1}} | \mu_{\mathcal{A}}, \mu_{\mathcal{A}_{U_2}} | \mu_{\mathcal{A}}$. 于是 $p | \mu_{\mathcal{A}}$. 又因为 $\mu_{\mathcal{A}_{U_1}} | p, \mu_{\mathcal{A}_{U_2}} | p$, 所以 $p(\mathcal{A}_{U_1}) = \mathcal{O}$ 和 $p(\mathcal{A}_{U_2}) = \mathcal{O}$ (引理 6.4). 于是

$$p(A) = \begin{pmatrix} p(A_1) & O \\ O & p(A_2) \end{pmatrix} = \begin{pmatrix} O & O \\ O & O \end{pmatrix}.$$

由此和引理 6.4, $\mu_{\mathcal{A}} | p$. 再利用首一性得出 $p = \mu_{\mathcal{A}}$. □

例 6.8 设

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

计算 μ_A.

解. 由上述引理 $\mu_A = \mathrm{lcm}(\mu_{(1)}, \mu_{(0)}) = \mathrm{lcm}(t-1, t) = (t-1)t$. □

以下内容将在下次大课中讲.

定理 6.9 设 $\mathcal{A} \in \mathcal{L}(V)$, $U_1, \dots, U_k$ 是非平凡 $\mathcal{A}$-子空间满足 $V = U_1 \oplus \cdots \oplus U_k$. 设 Z_i 是 U_i 的一组基, $i = 1, \dots, k$. 则 $\mathcal{A}$ 在 V 的基底 $Z_1 \cup \cdots \cup Z_k$ 下的矩阵

$$A = \begin{pmatrix} A_1 & O & \cdots & O \\ O & A_2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_k \end{pmatrix},$$

其中 A_i 是 $\mathcal{A}_{U_i}$ 在 Z_i 下的矩阵, $i = 1, 2, \dots, k$. 进而, $\mu_{\mathcal{A}} = \mathrm{lcm}(\mu_{\mathcal{A}_{U_1}}, \dots, \mu_{\mathcal{A}_{U_k}})$.

证明. 对 k 归纳. 当 $k = 1$ 时, 定理显然成立. 设 $k > 1$ 且 $k-1$ 时定理成立. 设 $W = U_1 \oplus \cdots \oplus U_{k-1}$. 则 $V = W \oplus U_k$, $Y = Z_1 \cup \cdots \cup Z_{k-1}$ 是 W 的基. 由引理 6.7, $\mathcal{A}$ 在基底 $W \cup Z_k$ 下的矩阵是

$$A = \begin{pmatrix} B & O \\ O & A_k \end{pmatrix},$$

其中 B 是 $\mathcal{A}_W$ 在 Y 下的矩阵, A_k 是 $\mathcal{A}_{U_k}$ 在 Z_k 下的矩阵, 且 $\mu_{\mathcal{A}} = \mathrm{lcm}(\mu_{\mathcal{A}_W}, \mu_{A_{U_k}})$.

对 $\mathcal{A}_W$, W, $U_1, \dots, U_{k-1}$ 用归纳假设得

$$B = \begin{pmatrix} A_1 & O & \cdots & O \\ O & A_2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_{k-1} \end{pmatrix},$$

其中 A_i 是 $\mathcal{A}_{U_i}$ 在 Z_i 下的矩阵, $i = 1, 2, \dots, k-1$. 进而, $\mu_{\mathcal{A}_W} = \mathrm{lcm}(\mu_{\mathcal{A}_{U_1}}, \dots, \mu_{\mathcal{A}_{U_{k-1}}})$. 于是, A 是所要求得形式. 注意到

$$\mathrm{lcm}\left(\mu_{\mathcal{A}_{U_1}}, \dots, \mu_{\mathcal{A}_{U_k}}\right) = \mathrm{lcm}\left(\mathrm{lcm}\left(\mu_{\mathcal{A}_{U_1}}, \dots, \mu_{\mathcal{A}_{U_{k-1}}}\right), \mu_{\mathcal{A}_{U_k}}\right) = \mathrm{lcm}(\mu_{\mathcal{A}_W}, \mu_{\mathcal{A}_{U_k}}) = \mu_{\mathcal{A}}. \quad \square$$

定理 6.10 *(核像分解 II)*[2] 设 $\mathcal{A} \in \mathcal{L}(V)$. 则

$$V = \ker(\mathcal{A}) \oplus \mathrm{im}(\mathcal{A}) \iff t^2 \nmid \mu_{\mathcal{A}}.$$

证明. 设 $K = \ker(\mathcal{A})$ 和 $I = \mathrm{im}(\mathcal{A})$.

($\Longrightarrow$) 设 $V = K \oplus I$. 如果 $K = \{\mathbf{0}\}$, 则 $\mathcal{A}$ 是单射(第一章第一讲命题 2.3). 于是, $\mathcal{A}$ 可逆(第二章第一讲推论 1.19). 根据命题 4.12, $\mu_{\mathcal{A}}(0) \neq 0$, 从而 $t^2 \nmid \mu_{\mathcal{A}}$. 设 $K_{\mathcal{A}} = V$. 则 $\mathcal{A} = \mathcal{O}$. 此时 $\mu_{\mathcal{A}} = t$. 于是 $t^2 \nmid \mu_{\mathcal{A}}$.

设 K 和 I 都是非平凡的. 则 $\mathcal{A}_K$ 是零算子. 于是 $\mu_{\mathcal{A}_K} = t$. 设 $\mathbf{v} \in I$. 如果 $\mathcal{A}_I(\mathbf{v}) = \mathbf{0}$, 则 $\mathcal{A}(\mathbf{v}) = \mathbf{0}$. 于是, $\mathbf{v} \in K \cap I$. 有直和条件可知, $\mathbf{v} = \mathbf{0}$. 即 $\mathcal{A}_I$ 是双射(第二章第一讲推论 1.19). 根据命题 4.12, $t \nmid \mu_{\mathcal{A}_I}(0) \neq 0$. 我们得到

$$\mu_{\mathcal{A}} = \mathrm{lcm}(\mu_{\mathcal{A}_K}, \mu_{\mathcal{A}_I}) = t\mu_{\mathcal{A}_I}.$$

于是, $t^2 \nmid \mu_{\mathcal{A}}$.

($\Longleftarrow$) 如果 $t \nmid \mu_{\mathcal{A}}$, 则 $\mathcal{A}$ 可逆(命题 4.12). 如果 $\mu_{\mathcal{A}} = t$, 则 $\mathcal{A} = \mathcal{Q}$. 在这两种情形下, $V = K \oplus I$ 显然成立.

设 $\mu_{\mathcal{A}} = tp$ 满足 $\gcd(t, p) = 1$. 由核核分解定理 $V = K \oplus \ker(p(\mathcal{A}))$. 下面我们验证 $I = \ker(p(\mathcal{A}))$. 设 $\mathbf{x} \in I$. 则存在 $\mathbf{y} \in V$ 使得 $\mathbf{x} = \mathcal{A}(\mathbf{y})$. 于是,

$$p(\mathcal{A})(\mathbf{x}) = p(\mathcal{A})(\mathcal{A}(\mathbf{y})) = (p(\mathcal{A})\mathcal{A})(\mathbf{y}) = (tp)(\mathcal{A})(\mathbf{y}) = \mu_{\mathcal{A}}(\mathcal{A})(\mathbf{y}) = \mathbf{0}.$$

由此得出 $I \subset \ker(p(\mathcal{A}))$. 另一方面, 由直和分解的性质和核像维数公式可知

$$\dim(\ker(p(\mathcal{A}))) = \dim(V) - \dim(K) = \dim(I).$$

我们推出 $I = \ker(p(\mathcal{A}))$. $\square$

[2]袁力, 沈洁. 常州工学院学报 27 卷第二期, 2014 年 4 月.

例 6.11 设 $\mathcal{A} \in \mathcal{L}(V)$ 满足 $\mathcal{A}^3 - \mathcal{A}^2 - \mathcal{A} = \mathcal{O}$. 证明: $\ker(\mathcal{A}) \oplus \operatorname{im}(\mathcal{A}) = V$.

证明. 设 $f(t) = t^3 - t^3 - t$. 则 $f(\mathcal{A}) = \mathcal{O}$. 由引理 *4.2*, $\mu_{\mathcal{A}}(t) | f(t)$. 因为 $t^2 \nmid f$, 所以 $t^2 \nmid \mu_{\mathcal{A}}(t)$. 由上述定理, $\ker(\mathcal{A}) \oplus \operatorname{im}(\mathcal{A}) = V$. □

例 6.12 设 $\mathcal{A} \in \mathcal{L}(V)$ 满足 $\ker(\mathcal{A}) \oplus \operatorname{im}(\mathcal{A}) = V$. 设 $\mathbf{e}_1, \ldots, \mathbf{e}_r$ 是 $\operatorname{im}(\mathcal{A})$ 的一组基, $\mathbf{e}_{r+1}, \ldots, \mathbf{e}_n$ 是 $\operatorname{im}(\mathcal{A})$ 的一组基. 则 $\mathbf{e}_1, \ldots, \mathbf{e}_r, \mathbf{e}_{r+1}, \ldots, \mathbf{e}_n$ 是 V 的一组基. 因为 $\operatorname{im}(\mathcal{A})$ 和 $\ker(\mathcal{A})$ 都是 $\mathcal{A}$-子空间, 且 $\mathcal{A}(\mathbf{e}_j) = \mathbf{0}$, $j = r+1, r+2, \ldots, n$, 所以 $\mathcal{A}$ 在该基底下的矩阵是

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

其中 $B \in \mathrm{M}_r(F)$ 满秩. 当 $r = n$ 时, $B = A$. 否则, $\mu_A = \operatorname{lcm}(\mu_B, t)$.