补充材料

约定. 在下述内容中 F 是域, V 是 F 上的有限维线性空间.

§1 扩展的核核分解定理

定理 1.1 *(扩展的核核分解定理)* 设 $\mathcal{A} \in \mathcal{L}(V), f(t) \in F[t] \setminus \{0\}$ 且 $f(\mathcal{A}) = \mathcal{O}$. 设 $f = q_1 q_2 \cdots q_s$, 其中 $q_1, \ldots, q_s \in F[t]$ 两两互素. 对 $i \in \{1, 2, \ldots, s\}$, 令 $K_i = \ker(q_i(\mathcal{A}))$ 和 $\mathcal{A}_i = \mathcal{A}_{K_i}$. 则

(i) $V = K_1 \oplus \cdots \oplus K_s$.

(ii) 设 $U_i = K_1 + \cdots + K_{i-1} + K_{i+1} + \cdots + K_s$. 则 $q_i(\mathcal{A})$ 在 U_i 上的限制算子是可逆的.

证明. (i) 对 s 归纳. 当 $s = 1$ 时, $V = K_1$. 故结论 (i) 是平凡的.

设 $s > 1$ 且 $s - 1$ 时定理成立. 令 $q = q_2 \cdots q_s$. 则 $\gcd(q_1, q) = 1$. 根据核核分解定理(第二章第二次讲义定理 3.3),

$$V = K_1 \oplus \ker(q(\mathcal{A})). \tag{1}$$

设 $\mathcal{B}$ 是 $\mathcal{A}$ 在 $\ker(q(\mathcal{A}))$ 上的限制映射. 因为 $\ker(q(\mathcal{A}))$ 是 $\mathcal{A}$-子空间(第二章第三次讲义命题 5.5), 所以 $\mathcal{B}$ 是 $\ker(q(\mathcal{A}))$ 上的线性算子. 因为 $q(\mathcal{A})$ 在 $\ker(q(\mathcal{A}))$ 上是把所有向量都映成零向量, 所以 $q(\mathcal{B})$ 是 $\ker(q(\mathcal{A}))$ 上的零算子. 对 $\mathcal{B}$, $\ker(q(\mathcal{A}))$, 和 $q = q_2 \cdots q_s$ 用归纳假设得

$$\ker(q(\mathcal{A})) = \ker(q_2(\mathcal{B})) \oplus \cdots \oplus \ker(q_s(\mathcal{B})).$$

再根据 (1) 得

$$V = K_1 \oplus \ker(q_2(\mathcal{B})) \oplus \cdots \oplus \ker(q_s(\mathcal{B})). \tag{2}$$

下面我们验证 $K_i = \ker(q_i(\mathcal{B}))$, $i = 2, \ldots, s$. 因为 $\mathcal{B}$ 是 $\mathcal{A}$ 的限制算子, 所以

$$\ker(q_2(\mathcal{B})) \subset K_2.$$

反之, 设 $\mathbf{v} \in K_2$. 由 (1) 可知, $\mathbf{v} = \mathbf{v}_1 + \mathbf{w}$, 其中 $\mathbf{v}_1 \in K_1$ 和 $\mathbf{w} \in \ker(q(\mathcal{A}))$. 设 $p = q_1 q_3 \cdots q_s$. 则 $\gcd(p, q_2) = 1$. 由此可知存在 $u, v \in F[t]$ 使得

$$up + vq_2 = 1.$$

于是

$$u(\mathcal{A})p(\mathcal{A}) + v(\mathcal{A})q_2(\mathcal{A}) = \mathcal{E}.$$

把上式作用在 $\mathbf{v}$ 上并利用 $q_2(\mathcal{A})(\mathbf{v})=\mathbf{0}$ 得

$$u(\mathcal{A})p(\mathcal{A})(\mathbf{v}_1+\mathbf{w})=\mathbf{v}.$$

因为 $q_1|p$ 且 $q_1(\mathcal{A})(\mathbf{v}_1)=\mathbf{0}$, 所以 $u(\mathcal{A})p(\mathcal{A})(\mathbf{v}_1)=\mathbf{0}$. 于是, 上式蕴含

$$\mathbf{v}=u(\mathcal{A})p(\mathcal{A})(\mathbf{w}).$$

因为 $\mathbf{w}\in\ker(q(\mathcal{A}))$ 且 $\ker(q(\mathcal{A}))$ 是 $\mathcal{A}$-不变的, 所以 $u(\mathcal{A})p(\mathcal{A})(\mathbf{w})\in\ker(q(\mathcal{A}))$. 由此可知, $\mathbf{v}\in\ker(q(\mathcal{A}))$. 故 $\mathcal{B}(\mathbf{v})$ 是良定义的. 因为 $q_2(\mathcal{A})(\mathbf{v})=\mathbf{0}$ 蕴含 $q_2(\mathcal{B})(\mathbf{v})=\mathbf{0}$, 所以 $\mathbf{v}\in\ker(q_2(\mathcal{B}))$, 即

$$K_2\subset\ker(q_2(\mathcal{B})).$$

故 $K_2=\ker(q_2(\mathcal{B}))$. 同理可知, $K_i=\ker(q_i(\mathcal{B}))$, $i=3,\ldots,s$. 再根据 (2), (i) 成立.

(ii) 我们沿用证明 (i) 时的记号来证明 $q_1(\mathcal{A})$ 在 U_1 上的限制算子是 U_1 上的可逆算子. 因为 $\gcd(q_1,q)=1$, 所以存在 $a,b\in F[t]$ 使得

$$a(t)q_1(t)+b(t)q(t)=1.$$

于是,

$$a(\mathcal{A})q_1(\mathcal{A})+b(\mathcal{A})q(\mathcal{A})=\mathcal{E}. \tag{3}$$

由 (i) 的证明可知, $U_1=\ker(q(\mathcal{A}))$. 对任意 $\mathbf{u}\in U_1$, 我们把 (3) 作用在 $\mathbf{u}$ 上得

$$a(\mathcal{A})q_1(\mathcal{A})(\mathbf{u})=\mathbf{u},$$

即 $a(\mathcal{A})q(\mathcal{A})$ 在 U_1 上是恒同映射. 于是, $q(\mathcal{A})|_U$ 的逆算子是 $a(\mathcal{A})$. 通过置换下标，我们可以推出 (ii) 对 $i=2,3,\ldots,s$ 都成立. □

推论 1.2 *设 $\mathcal{A}\in\mathcal{L}(V)$, $\mu_{\mathcal{A}}=p_1^{m_1}\cdots p_s^{m_s}$ 是 $\mu_{\mathcal{A}}$ 在 $F[t]$ 上的不可约因式分解. 则设 $K_i=\ker(p_i^{m_i}(\mathcal{A}))$, $\quad i=1,2,\ldots,s$. 则*

(i) $V=K_1\oplus\cdots\oplus K_s$.

(ii) *设 $U_i=K_1+\cdots+K_{i-1}+K_{i+1}+\cdots+K_s$. 则 $p_i(\mathcal{A})$ 在 U_i 上的限制算子是可逆的, $i=1,\ldots,s$.*

(iii) *$\mathcal{A}$ 在 K_i 上的限制算子的极小多项式是 $p_i^{m_i}$, $i=1,\ldots,s$.*

证明. (i) 设扩展的核核分解定理中 $f=\mu_{\mathcal{A}}$, $q_i=p_i^{m_i}$, $i=1,\ldots,s$. 则扩展的核核分解定理蕴含 (i) 和 $q_i(\mathcal{A})$ 在 U_i 上可逆. 因为 $q_i(\mathcal{A})$ 限制在 U_i 上是单射, 所以 $p_i(\mathcal{A})$ 限制在 U_i 上也是单射.

(iii) 设 μ_i 是 $\mathcal{A}$ 在 K_i 上的限制算子的极小多项式, $i=1,\ldots,s$. 则第二章第二讲引理 4.2 蕴含

$$\mu_i | p_i^{m_i}, \quad i=1,\ldots,s. \tag{4}$$

再根据第二章第三讲定理 5.9,

$$\mu_{\mathcal{A}} = \mathrm{lcm}(\mu_1,\ldots,\mu_s).$$

将上式对比 $\mu_{\mathcal{A}}$ 的不可约分解

$$\mu_{\mathcal{A}} = p_1^{m_1}\cdots p_s^{m_s}$$

和 (4), 我们得到 (iii). □

§2 关于算子和向量的极小多项式

设 $\mathcal{A}\in\mathcal{L}(V), \mathbf{v}\in V, f(t)\in F[t]$. 如果 $f(\mathcal{A})(\mathbf{v})=\mathbf{0}$, 则称 $f(t)$ 是通过 $\mathcal{A}$ 零化 $\mathbf{v}$ 的多项式. 非零、次数最小的通过 $\mathcal{A}$ 零化 $\mathbf{v}$ 的多项式称为通过 $\mathcal{A}$ 零化 $\mathbf{v}$ 的极小多项式. 该极小多项式记为 $\mu_{\mathcal{A},\mathbf{v}}$, 它通常是首一的.

注意到 $\mu_{\mathcal{A}}(\mathcal{A})(\mathbf{v})=\mathcal{O}(\mathbf{v})=\mathbf{0}$. 于是, $\mu_{\mathcal{A},\mathbf{v}}$ 存在. 设 $f(\mathcal{A})(\mathbf{v})=\mathbf{0}$. 由多项式带余除法可知

$$f(t)=q(t)\mu_{\mathcal{A},\mathbf{v}}(t)+r(t),$$

其中 $q,r\in F[t]$, $\deg(r)<\deg(\mu_{\mathcal{A},\mathbf{v}})$. 带入 $\mathcal{A}$ 得 $\mathcal{O}=q(\mathcal{A})\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})+r(\mathcal{A})$. 两侧同时作用在 $\mathbf{v}$ 上得到

$$\mathbf{0}=q(\mathcal{A})\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v})+r(\mathcal{A})(\mathbf{v})=\mathbf{0}+r(\mathcal{A})(\mathbf{v}).$$

于是, $r(\mathcal{A})(\mathbf{v})=\mathbf{0}$. 因为 $\deg(r)<\deg(\mu_{\mathcal{A},\mathbf{v}})$, 所以 $r(t)=0$. 由此得出 $\mu_{\mathcal{A},\mathbf{v}}|f$. 特别地, $\mu_{\mathcal{A},\mathbf{v}}|\mu_{\mathcal{A}}$.

下面的结论有重要的应用.

命题 2.1 *设 $\mathcal{A}\in\mathcal{L}(V)$. 则存在 $\mathbf{v}\in V$ 使得 $\mu_{\mathcal{A},\mathbf{v}}=\mu_{\mathcal{A}}$.*

为了证明该命题, 我们先证明一个局部结果.

引理 2.2 *设 $\mathcal{A}\in\mathcal{L}(V)$ 且 $\mu_{\mathcal{A}}=p^k$, 其中 $p\in F[t]$ 不可约和首一. 则存在 $\mathbf{v}\in V$ 使得*

$$\mu_{\mathcal{A},\mathbf{v}}=\mu_{\mathcal{A}}.$$

证明. 因为 $\mu_{\mathcal{A},\mathbf{v}}|\mu_A$ 且 p 不可约, 所以 $\mu_{\mathcal{A},\mathbf{v}}=p^{m_\mathbf{v}}$, 其中 $1\le m_\mathbf{v}\le k$. 假设不存在 $\mathbf{v}$ 使得 $m_\mathbf{v}=k$. 则对任意 $\mathbf{v}\in V$, $m_\mathbf{v}\le k-1$. 于是 $p^{k-1}=q_\mathbf{v}\mu_{\mathcal{A},\mathbf{v}}$, 其中 $q_\mathbf{v}\in F[t]$. 我们有

$$p^{k-1}(\mathcal{A})=q_\mathbf{v}(\mathcal{A})\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A}) \implies p^{k-1}(\mathcal{A})(\mathbf{v})=q_\mathbf{v}(\mathcal{A})\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v})=q_\mathbf{v}(\mathcal{A})\left(\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v})\right)=\mathbf{0}.$$

由 $\mathbf{v}$ 的任意性得出 $p^{k-1}(\mathcal{A})=\mathcal{O}$, 与 $\mu_{\mathcal{A}}=p^k$ 矛盾. □

其次, 我们给出从局部结果过渡到整体结果的工具. 注意到第二章第二次讲义命题 6.5 说明对任意 $f\in F[t]$, $\ker(f(\mathcal{A}))$ 是 $\mathcal{A}$-不变的.

命题 2.1 的证明. 利用上述推论 1.2 中的记号, 对 $i\in\{1,2,\ldots,s\}$, 令 $\mathcal{A}_i$ 记 $\mathcal{A}$ 在 K_i 上的限制算子. 则 $\mathcal{A}_i\in\mathcal{L}(K_i)$. 根据推论 1.2, $\mu_{\mathcal{A}_i}$ 是 $F[t]$ 中一个不可约多项式的幂次. 根据引理 2.2, 存在 $\mathbf{v}_i\in K_i$ 使得 $\mu_{\mathcal{A}_i}=\mu_{\mathcal{A}_i,\mathbf{v}_i}$.

令 $\mathbf{v}=\mathbf{v}_1+\cdots+\mathbf{v}_s$. 则,

$$\mathbf{0}=\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v})=\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v}_1)+\cdots+\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v}_s).$$

因为 $V=K_1\oplus\cdots\oplus K_s$, 且每个 K_i 都是 $\mathcal{A}$ 不变的, 所以 $\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v}_i)\in K_i$. 由直和的基本性质(见第一章第一讲定理 1.11 (ii)), $\mu_{\mathcal{A},\mathbf{v}}(\mathcal{A})(\mathbf{v}_i)=\mathbf{0}$. 于是, $\mu_{\mathcal{A}_i,\mathbf{v}_i}|\mu_{\mathcal{A},\mathbf{v}}$, $i=1,2,\ldots,s$. 由此可知, $\mu_{\mathcal{A}_i}|\mu_{\mathcal{A},\mathbf{v}}$, $i=1,2,\ldots,s$. 从而 $\mu_{\mathcal{A}}=\operatorname{lcm}(\mu_{\mathcal{A}_1},\ldots,\mu_{\mathcal{A}_s})|\mu_{\mathcal{A},\mathbf{v}}$. 又因为 $\mu_{\mathcal{A},\mathbf{v}}|\mu_{\mathcal{A}}$. 我们有 $\mu_{\mathcal{A}}=\mu_{\mathcal{A},\mathbf{v}}$. □

§3 广义特征子空间分解

设 $\dim(V)=n>0$ 和 $\mathcal{A}\in\mathcal{L}(V)$. 令

$$\mu_{\mathcal{A}}=p_1^{m_1}\cdots p_s^{m_s},$$

其中 $p_1,\ldots,p_s\in F[t]\setminus F$, 首一, 不可约且两两互素, $m_1,\ldots,m_s\in\mathbb{Z}^+$. 令

$$V(p_i)=\ker(p_i^{m_i}(\mathcal{A})),\quad i=1,2,\ldots,s.$$

我们称 $V(p_i)$ 是算子 $\mathcal{A}$ 关于不可约因子 p_i 的广义特征子空间. 则推论 1.2 可重述为

定理 3.1 *(广义特征子空间分解–极小多项式版)* *利用上述记号,*

(i) $V=V(p_1)\oplus\cdots\oplus V(p_s)$.

(ii) *设* $U_i=V(p_1)+\cdots+V(p_{i-1})+V(p_{i+1})+\cdots+V(p_s)$. *则* $p_i(\mathcal{A})$ *在* U_i *上的限制算子是可逆的,* $i=1,\ldots,s$.

(iii) $\mathcal{A}$ *在* $V(p_i)$ *上的限制算子的极小多项式是* $p_i^{m_i}$, $i=1,\ldots,s$.

引理 3.2 *利用上述记号, 设* $k,\ell\in\mathbb{Z}^+$ *满足* $k<m_i<\ell$. *则*

$$\ker(p_i(\mathcal{A})^k)\subsetneq V(p_i)=\ker(p_i(\mathcal{A})^\ell).$$

证明. 根据线性映射的复合, 我们有

$$\ker(p_i(\mathcal{A})^k) \subset V(p_i) \subset \ker(p_i(\mathcal{A})^\ell).$$

设 $\mathcal{A}_i$ 是 $\mathcal{A}$ 在 $V(p_i)$ 上的限制算子, μ_i 是 $\mathcal{A}_i$ 的极小多项式, $i = 1, \ldots, s$.

如果 $\ker(p_i(\mathcal{A})^k) = V(p_i)$, 则 $p_i(\mathcal{A}_i)^k$ 在 $V(p_i)$ 上是零算子. 由此得出 $\mu_i(t)|p_i(t)^k$ (第二章第二讲引理 4.2). 根据上述定理 (iii), $p_i^{m_i}|p_i^k$. 故 $m_i \le k$, 矛盾. 由此推出,

$$\ker(p_i(\mathcal{A})^k) \subsetneq V(p_i).$$

再假设 $\mathbf{v} \in \ker(p_i(\mathcal{A})^\ell) \backslash V(p_i)$. 由上述定理 (i) 可知, 存在 $\mathbf{v}_i \in V(p_i)$ 和 $\mathbf{u}_i \in U_i \backslash \{\mathbf{0}\}$ 使得

$$\mathbf{v} = \mathbf{v}_i + \mathbf{u}_i.$$

将上式两侧同时作用 $p_i(\mathcal{A})^\ell$ 并利用 $m_i < \ell$ 得 $p_i(\mathcal{A})^\ell(\mathbf{u}_i) = \mathbf{0}$. 由上述定理 (ii) 可知, $p_i(\mathcal{A})$ 在 U_i 上的限制算子可逆. 故 $p_i(\mathcal{A})^\ell$ 在 U_i 上的限制算子也可逆. 由此得出 $\mathbf{u}_i = \mathbf{0}$. 矛盾. 由此得到

$$V(p_i) = \ker(p_i(\mathcal{A})^\ell). \quad \square$$

定理 3.3 *(广义特征子空间分解–特征多项式版)* 设 $\mathcal{A} \in \mathcal{L}(V)$, 且

$$\chi_{\mathcal{A}}(t) = p_1^{n_1} \cdots p_s^{n_s},$$

其中 $p_1, \ldots, p_s \in F[t] \setminus F$, 首一, 不可约, 两两互素. 则

(i) $V = V(p_1) \oplus \cdots \oplus V(p_s)$.

(ii) 设 $U_i = V(p_1) + \cdots + V(p_{i-1}) + V(p_{i+1}) + \cdots + V(p_s)$. 则 $p_i(\mathcal{A})$ 在 U_i 上的限制算子是可逆的, $i = 1, \ldots, s$.

(iii) $\mathcal{A}$ 在 $V(p_i)$ 上的限制算子的特征多项式是 $p_i^{n_i}$, $i = 1, \ldots, s$. 特别地,

$$\dim(V(p_i)) = n_i \deg(p_i).$$

证明. 根据加强版的 Hamilton-Cayley 定理(第二章第五讲定理 10.2), $\mu_{\mathcal{A}}$ 在 $F[t]$ 中的不可约分解是

$$\mu_{\mathcal{A}} = p_1^{m_1} \cdots p_s^{m_s},$$

其中 $0 < m_i \le n_i$, $i = 1, 2, \ldots, s$. 根据定理 3.1 (i) 和 (ii), 以及引理 3.2, 结论 (i) 和 (ii) 成立.

设 $\mathcal{A}_i$ 是 $\mathcal{A}$ 在 $V(p_i)$ 上的限制算子, $i = 1, 2, \ldots, s$. 根据定理 3.1 (iii), $\mu_{\mathcal{A}_i} = p_i^{m_i}$. 再根据加强版的 Hamilton-Cayley 定理, $\chi_{\mathcal{A}_i} = p_i^{\ell_i}$. 由第二章第三讲例 7.14 可知,

$$\chi_{\mathcal{A}} = \chi_{\mathcal{A}_1} \cdots \chi_{\mathcal{A}_s} = p_i^{\ell_1} \cdots p_s^{\ell_s}.$$

根据多项式不可约分解的唯一性, 我们得到 $\ell_i = n_i$, $i = 1, 2, \ldots, s$. 进而,

$$\dim(V(p_i)) = \deg(\chi_{A_i}) = n_i \deg(p_i),$$

$i = 1, 2, \ldots, n$. $\square$