群与 Galois 理论
作业 6

陈宏泰

2024011131

清华大学数学科学系

cht24@mails.tsinghua.edu.cn

2025 年 12 月 24 日

目录

用模的观点看线性代数

K 是域, $n \geqslant 1, V$ 是 n 维 K-线性空间, $T \in \mathbf{End}_K(V)$ 是 V 到自身的 K-线性映射. 那么, V 可以被视为 $K[X]$-模:

$$K[X] \times V \to V, \quad P(X) \mapsto (v \mapsto P(T)v).$$

根据主理想整环 $K[X]$ 上的有限生成模的分类定理, 存在唯一的首一多项式 $P_1, \cdots, P_s \in K[X]$, 使得 $P_1 \mid P_2, P_2 \mid P_3, \cdots, P_{s-1} \mid P_s$ 并且有如下 $K[X]$-模的分解:

$$V \simeq {}^{K[X]}\!\big/\!_{(P_1(X))} \oplus {}^{K[X]}\!\big/\!_{(P_2(X))} \oplus \cdots \oplus {}^{K[X]}\!\big/\!_{(P_s(X))}.$$

我们称 $P_1, \cdots, P_s$ 为 T 的**不变因子**.

1. 证明, $\{P \in K[X] \mid P(T) = 0\}$ 为 $K[X]$ 的理想并且由其中唯一的次数最低的首一多项式 $m_T(X)$ 生成. 这个多项式被称作是 T 的**极小多项式**.

证明: 设 $I = \{P \in K[X] \mid P(T) = 0\}$. 对于任意 $P(X), Q(X) \in I$, 有

$$(P(X) + Q(X))(T) = P(T) + Q(T) = 0 + 0 = 0,$$

因此 $P(X) + Q(X) \in I$. 对于任意 $P(X) \in I$ 和 $R(X) \in K[X]$, 有

$$(R(X)P(X))(T) = R(T)P(T) = R(T) \cdot 0 = 0,$$

因此 $R(X)P(X) \in I$. 而显然零多项式属于 I. 综上所述, I 为 $K[X]$ 的理想.

由于 $K[X]$ 是主理想整环, 存在唯一的首一多项式 $m_T(X)$, 使得 $I = (m_T(X))$. 显然, $m_T(X)$ 是 I 中次数最低的首一多项式. 反过来, 设 $Q(X) \in I$ 是次数最低的首一多项式, 则有 $m_T(X) \mid Q(X)$, 从而 $Q(X)$ 与 $m_T(X)$ 相等 (因为它们都是首一多项式). 因此, $m_T(X)$ 是唯一的. □

2. 证明, $m_T(X) = P_s(X)$.

证明: 由 V 的分解可知, 在同构意义下, 对于任意 $v \in V$, 存在 $f_i(X) \in K[X]$, 使得

$$v = \left(f_1(X) + (P_1(X)), f_2(X) + (P_2(X)), \cdots, f_s(X) + (P_s(X))\right).$$

因此, 有

$$P_s(T)v = \left(P_s(X)f_1(X) + (P_1(X)), P_s(X)f_2(X) + (P_2(X)), \cdots, P_s(X)f_s(X) + (P_s(X))\right) = 0.$$

这说明 $P_s(X) \in I$, 因此 $m_T(X) \mid P_s(X)$.

反过来, 设 $Q(X) \in I$, 则对于任意 $v \in V$, 有

$$Q(T)v = \left(Q(X)f_1(X) + (P_1(X)), Q(X)f_2(X) + (P_2(X)), \cdots, Q(X)f_s(X) + (P_s(X))\right) = 0.$$

这说明对于任意 $v \in V, 1 \leqslant i \leqslant s$, 有 $Q(X)f_i(X) \in (P_i(X))$. 特别地, 取 $f_s(X)=1$, 可得 $Q(X) \in (P_s(X))$. 因此, 有 $P_s(X) \mid Q(X)$. 由此可知, $P_s(X) \mid Q(X)$. 因此, 有 $P_s(X) \mid m_T(X)$.

综上所述, 以及两者都是首一多项式, 有 $m_T(X) = P_s(X)$. □

3. 令 $p_T(X)$ 为 T 的特征多项式. 证明,

$$p_T(X) = P_1(X)P_2(X)\cdots P_s(X).$$

证明: 由于 V 在同构意义下可分解为

$$V \simeq {}^{K[X]}\!\diagup_{(P_1(X))} \oplus {}^{K[X]}\!\diagup_{(P_2(X))} \oplus \cdots \oplus {}^{K[X]}\!\diagup_{(P_s(X))},$$

因此, 在适当选择基的情况下, T 对应的矩阵可以写成如下的块对角矩阵:

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_s \end{pmatrix},$$

其中, 每个块 A_i 对应于 ${}^{K[X]}\!\diagup_{(P_i(X))}$ 上的线性变换.

因此, 有

$$p_T(X) = \det(X\cdot I - A) = \det \begin{pmatrix} X\cdot I_1 - A_1 & 0 & \cdots & 0 \\ 0 & X\cdot I_2 - A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X\cdot I_s - A_s \end{pmatrix},$$

其中 I_i 是与块 A_i 大小相同的单位矩阵. 由行列式的性质可知,

$$p_T(X) = \prod_{i=1}^{s} \det(X\cdot I_i - A_i).$$

注意到 T 在 V 上的作用就等价于 X 在 ${}^{K[X]}\!\diagup_{(P_i(X))}$ 上的作用, 因此, A_i 的特征特征多项式就是 $P_i(X)$. 因此, 有

$$p_T(X) = P_1(X)P_2(X)\cdots P_s(X).$$

□

注: 由此可见, 线性代数中的一些经典结论可以通过模的观点得到更为简洁的证明. 例如, Cayley-Hamilton 定理 (即 $p_T(T)=0$) 可以通过上述结果直接得到, 因为 $p_T(X)$ 显然是 T 的不变因子的乘积, 因此 $p_T(X)$ 整除极小多项式 $m_T(X)$, 从而有 $p_T(T)=0$.

对于 A_i 的特征特征多项式就是 $P_i(X)$ 再做更加具体的说明:

设 $P_i(X)=X^{d_i}+c_{i,d_i-1}X^{d_i-1}+\cdots+c_{i,1}X+c_{i,0}$, 则 $K[X]\big/(P_i(X))$ 的基为 $\{1+(P_i(X)),X+(P_i(X)),\cdots,X^{d_i-1}+(P_i(X))\}$. 在该基下, X 的矩阵表示为

$$A_i=\begin{pmatrix}0&0&\cdots&0&-c_{i,0}\\1&0&\cdots&0&-c_{i,1}\\0&1&\cdots&0&-c_{i,2}\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&-c_{i,d_i-1}\end{pmatrix}.$$

恰为 $P_i(x)$ 的伴随矩阵, 其特征多项式为

$$\det(X\cdot I_i-A_i)=X^{d_i}+c_{i,d_i-1}X^{d_i-1}+\cdots+c_{i,1}X+c_{i,0}=P_i(X).$$

4. 给定 V 的一组基 $\{e_i\}_{1\leqslant i\leqslant n}$, 用 $A=(a_{ij})_{1\leqslant i,j\leqslant n}\in\mathbf{M}_n(K)$ 表示 T 对应的矩阵, 其中, $a_{ij}\in K$; I 为 $n\times n$ 的单位矩阵. 令 $L=X\cdot I-A=\begin{pmatrix}X-a_{11}&-a_{12}&\cdots&-a_{1n}\\-a_{21}&X-a_{22}&\cdots&-a_{2n}\\\vdots&\vdots&\ddots&\vdots\\-a_{n1}&-a_{n2}&\cdots&X-a_{nn}\end{pmatrix}\in\mathbf{M}_n(K[X])$.

我们考虑 $K[X]$-模之间的同态:

$$L:K[X]^n\to K[X]^n,\begin{pmatrix}F_1(X)\\F_2(X)\\\vdots\\F_n(X)\end{pmatrix}\mapsto\begin{pmatrix}X-a_{11}&-a_{12}&\cdots&-a_{1n}\\-a_{21}&X-a_{22}&\cdots&-a_{2n}\\\vdots&\vdots&\ddots&\vdots\\-a_{n1}&-a_{n2}&\cdots&X-a_{nn}\end{pmatrix}\begin{pmatrix}F_1(X)\\F_2(X)\\\vdots\\F_n(X)\end{pmatrix}$$

以及

$$\pi:K[X]^n\to V,\begin{pmatrix}F_1(X)\\F_2(X)\\\vdots\\F_n(X)\end{pmatrix}\mapsto\sum_{i=1}^nF_i(T)\cdot e_i.$$

证明, 我们有 $K[X]$ 一模之间的正合列:

$$K[X]^n\xrightarrow{L}K[X]^n\xrightarrow{\pi}V\to0,$$

即证明 $\mathrm{Ker}(\pi)=\mathrm{Im}\,L$ 并且 $V\simeq K[X]^n/\,\mathrm{Im}\,L$.

证明: 首先, 证明 $\mathrm{Im}\,L\subseteq\mathrm{Ker}(\pi)$. 对于任意 $\mathbf{F}(X)=\begin{pmatrix}F_1(X)\\F_2(X)\\\vdots\\F_n(X)\end{pmatrix}\in K[X]^n$, 有

$$L(\mathbf{F}(X))=\Big(\ (XI-A)\cdot\mathbf{F}(X)\ \Big).$$

因此, 有

$$\pi(L(\mathbf{F}(X))) = \sum_{i=1}^{n} ((XI - A) \cdot \mathbf{F}(X))_i (T) \cdot e_i.$$

注意到 $(XI - A) \cdot \mathbf{F}(X)$ 的第 i 个分量为

$$(X - a_{ii})F_i(X) - \sum_{j \neq i} a_{ij} F_j(X),$$

因此, 有

$$\pi(L(\mathbf{F}(X))) = \sum_{i=1}^{n} \left((T - a_{ii} I) F_i(T) - \sum_{j \neq i} a_{ij} F_j(T) \right) \cdot e_i.$$

由于 $T(e_i) = \sum_{j=1}^{n} a_{ji} e_j$, 可得

$$\begin{aligned} \pi(L(\mathbf{F}(X))) &= \sum_{i=1}^{n} \left(T(F_i(T) \cdot e_i) - \sum_{j=1}^{n} a_{ij} F_j(T) \cdot e_i \right) \\ &= \sum_{i=1}^{n} T(F_i(T) \cdot e_i) - \sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_{ij} F_j(T) \cdot e_i \right) \\ &= T\left(\sum_{i=1}^{n} F_i(T) \cdot e_i \right) - T\left(\sum_{j=1}^{n} F_j(T) \cdot e_j \right) \\ &= 0. \end{aligned}$$

这说明 $L(\mathbf{F}(X)) \in \operatorname{Ker}(\pi)$. 因此, 有 $\operatorname{Im} L \subseteq \operatorname{Ker}(\pi)$.

再证明 $\mathrm{Ker}\pi \subset \mathrm{Im}L$. $\forall \mathbf{F}(X) \in \mathrm{Ker}\pi$, 将其按照 X 的次数展开:

$$\mathbf{F}(X) = \sum_{k=0}^{m} \mathbf{X}^k v_k = X^m v_m + X^{m-1} v_{m-1} + \cdots + X v_1 + v_0,$$

其中, $v_k \in K^n$. 利用代数恒等式 $X^k \cdot I - A^k = (X \cdot I - A)(X^{k-1} + X^{k-2}A + \cdots + XA^{k-2} + A^{k-1})$, 可得

$$X^k \cdot I \equiv A^k \pmod{\mathrm{Im}L}.$$

因此, 有

$$\mathbf{F}(X) \equiv \sum_{k=0}^{m} A^k v_k \pmod{\mathrm{Im}L}.$$

由于 $\mathbf{F}(X) \in \mathrm{Ker}(\pi)$, 以及 $\mathrm{Im}L \subset \mathrm{Ker}(\pi)$, 可知 $G(X) := \sum_{k=0}^{m} A^k v_k \in \mathrm{Ker}(\pi)$. 注意到 $G(X)$ 是常数向量, 不妨设为 $(r_1, r_2, \cdots, r_n)^T$, 于是

$$\pi(G(X)) = \sum_{i=1}^{n} r_i e_i = 0.$$

又由于 $\{e_i\}$ 是 V 的一组基, 可知 $r_i = 0$ 对任意 i 成立, 即 $G(X) = 0$. 于是有 $\mathbf{F}(X) \in \mathrm{Im}L$. 因此, 有 $\mathrm{Ker}(\pi) \subset \mathrm{Im}L$.

综上所述, 有 $\mathrm{Ker}(\pi)=\mathrm{Im}\,L$. 由同态基本定理可知, $V\simeq {K[X]^n}/{\mathrm{Ker}(\pi)}\simeq {K[X]^n}/{\mathrm{Im}\,L}$.

$\square$

注: 个人认为, 利用代数恒等式 $X^k\cdot I-A^k=(X\cdot I-A)(X^{k-1}+X^{k-2}A+\cdots+XA^{k-2}+A^{k-1})$ 是证明 $\mathrm{Ker}(\pi)\subset \mathrm{Im}L$ 的关键所在.

如果记性好, 能够想起高代中同样代表带余除法的引理, 参看《高等代数学》(谢启鸿姚慕生吴泉水) 中的引理 7.1.1.

如果存在可逆的 $P\in\mathbf{End}_K(V)$, 使得 $P\circ S\circ P^{-1}=T$, 就称 S 与 T 是 (通过 P) **相似的**.

另外, 根据 S 和 T 可分别在 V 上定义出 (两个)$K[X]$ 一模的结构. 第一个记作 V_S :

$$K[X]\times V\to V,\quad P(X)\mapsto (v\mapsto P(S)v);$$

第二个记作 V_T :

$$K[X]\times V\to V,\quad P(X)\mapsto (v\mapsto P(T)v).$$

5. 证明, 若 S 与 T 是通过 P 相似的, 则以下映射是 $K[X]$-模同构:

$$V_S\longrightarrow V_T,\quad v\mapsto P(v).$$

证明: 记此映射为 φ. 由于 $P\in\mathbf{End}_K(V)$, φ 是双射. 对于任意 $v\in V_S$ 和 $Q(X)\in K[X]$, 有

$$\varphi(Q(X)\cdot v)=\varphi(Q(S)v)=P(Q(S)v)=Q(T)P(v)=Q(X)\cdot\varphi(v).$$

因此, φ 是 $K[X]$-模同构. $\square$

6. 证明, S 与 T 相似当且仅当 $K[X]$-模 V_S 与 V_T 同构.

证明: 必要性: 由题 5 的结论可知.

充分性: 设 $\varphi: V_S\longrightarrow V_T$ 为 $K[X]$-模同构. 由于 φ 是双射, 因此, 存在 $P=\varphi\in\mathrm{End}_K(V)$ 使得对于任意 $v\in V$, 有 $\varphi(v)=P(v)$. 对于任意 $v\in V$, 有

$$P(S(v))=P(X\cdot v)=X\cdot P(v)=T(P(v))=T(\varphi(v))=T(P(v)).$$

因此, 有 $P\circ S=T\circ P$, 即 $P\circ S\circ P^{-1}=T$. 这说明 S 与 T 相似. $\square$

7. 证明, S 与 T 相似当且仅当 S 与 T 具有同样的不变因子.

证明: 由于 $K[X]$-模 V_S 与 V_T 同构, 由有限生成模的分类定理的唯一性可知, S 与 T 具有同样的不变因子. 于是由题 6, S 与 T 相似当且仅当 $K[X]$-模 V_S 与 V_T 同构, 当且仅当 S 与 T 具有同样的不变因子 $\square$

8. 给定 V 一组基使得 S 和 T 可以用矩阵表示 (仍然记作 S 和 T) 证明, S 与 T 相似当且仅当 $X\cdot I-S$ 与 $X\cdot I-T$ 在 $\mathbf{M}_n(K[X])$ 中共轭, 即存在 $P\in\mathbf{GL}(n;K[X])$, 使得 $P\cdot(X\cdot I-S)\cdot P^{-1}=X\cdot I-T$.

证明: 必要性: 设 S 与 T 相似, 则有 $P\cdot S\cdot P^{-1}=T$. 同时 $P\cdot X\cdot I\cdot P^{-1}=X\cdot I$. 因此, 有

$$P\cdot(X\cdot I-S)\cdot P^{-1}=X\cdot I-T.$$

充分性: 设存在 $P\in\mathbf{GL}(n;K[X])$, 使得 $P\cdot(X\cdot I-S)\cdot P^{-1}=X\cdot I-T$. 类似题 4 的带余除法, 可知 P 可以写成 $P=Q\cdot(X\cdot I-S)+R$, 其中 $Q\in\mathbf{M}_n(K[X])$ 且 $R\in\mathbf{M}_n(K)$. 于是有

$$\begin{aligned}&P\cdot(X\cdot I-S)=(X\cdot I-T)\cdot P\\ \Rightarrow\ &(Q\cdot(X\cdot I-S)+R)\cdot(X\cdot I-S)=(X\cdot I-T)\cdot(Q(X\cdot I-S)+R)\\ \Rightarrow\ &(Q\cdot(X\cdot I-S)+R-(X\cdot I-T)\cdot Q)\cdot(X\cdot I-S)=(X\cdot I-T)\cdot R.\end{aligned}$$

上式右边是次数小于等于 1 的矩阵多项式, 因此左边也必须是次数小于等于 1 的矩阵多项式. 这说明 $Q\cdot(X\cdot I-S)+R-(X\cdot I-T)\cdot Q$ 也是一个常数矩阵, 记为 U. 于是有

$$U\cdot(X\cdot I-S)=(X\cdot I-T)\cdot R.$$

整理上式, 可得

$$X\cdot(U-R)=T\cdot R-U\cdot S.$$

再比较次数, 可知 $U=R, US=TR$. 于是只需要证明 R 是可逆的即可. 由于 P 是可逆的, 存在 $P^{-1}\in\mathbf{M}_n(K[X])$, 使得

$$P\cdot P^{-1}=I.$$

同样地, 设 $P^{-1}=Q'\cdot(X\cdot I-S)+R'$, 其中 $Q'\in\mathbf{M}_n(K[X])$ 且 $R'\in\mathbf{M}_n(K)$. 于是有

$$(Q\cdot(X\cdot I-S)+R)\cdot(Q'\cdot(X\cdot I-S)+R')=I.$$

展开上式, 可得

$$(Q\cdot(X\cdot I-S)\cdot Q')(X\cdot I-S)=I-R\cdot R'.$$

比较次数, 可知 $R\cdot R'=I$. 这说明 R 是可逆的. 综上所述, 有 S 与 T 相似. □

注: 参看《高等代数学》(谢启鸿姚慕生吴泉水) 中的定理 7.1.2.

9. 应用: 试计算 $\mathbf{GL}\,(2;\mathbb{F}_3)$ 的共轭类的个数.

证明: 设 $K=\mathbb{F}_3$. 根据有限生成模的分类定理, $\mathbf{GL}\,(2;K)$ 中的每个元素 T 的不变因子有以下几种可能:

1. $P_1(X)=X-a, P_2(X)=X-a$, 其中 $a\in K^\times$. 共有 2 种可能.

2. $P_1(X)=(X-a)^2$, 其中 $a\in K^\times$. 共有 2 种可能.

3. $P_1(X)=(X-a)(X-b)$, 其中 $a,b\in K^\times$ 且 $a\neq b$. 共有 2 种可能.

4. $P_1(X)=Q(X)$, 其中 $Q(X)\in K[X]$ 为次数为 2 的首一不可约多项式. 共有 $3^2-3-2-2=2$ 种可能.

综上所述, $\mathbf{GL}\,(2;\mathbb{F}_3)$ 的共轭类的个数为 $2+2+2+2=8$. □

10. 应用: 给定域扩张 L/K 以及 $A,B\in\mathbf{M}_n(K)$. 证明, 若存在 $P\in\mathbf{GL}(n;L)$ 使得 $PAP^{-1}=B$, 则存在 $Q\in\mathbf{GL}(n;K)$ 使得 $QAQ^{-1}=B$. (提示: 参考 Smith 标准型唯一性的证明)

证明: 设 $X\cdot I-A$ 在 $\mathbf{M}_n(K[X])$ 中的 Smith 标准型为

$$D_A=\operatorname{diag}\left(P_1(X),P_2(X),\cdots,P_n(X)\right),$$

其中, $P_i(X)\in K[X]$ 且 $P_i(X)\mid P_{i+1}(X)$. 同理, 设 $X\cdot I-B$ 在 $\mathbf{M}_n(K[X])$ 中的 Smith 标准型为

$$D_B=\operatorname{diag}\left(Q_1(X),Q_2(X),\cdots,Q_n(X)\right),$$

其中, $Q_i(X)\in K[X]$ 且 $Q_i(X)\mid Q_{i+1}(X)$. 由题 8 的结论可知, D_A 与 D_B 在 $\mathbf{M}_n(L[X])$ 中共轭. 由 Smith 标准型的唯一性可知, 有 $P_i(X)=Q_i(X)$ 对任意 $1\leqslant i\leqslant n$ 成立. 因此, $D_A=D_B$, 即 A 与 B 具有相同的不变因子. 由题 7 的结论可知, 存在 $Q\in\mathbf{GL}(n;K)$ 使得 $QAQ^{-1}=B$.

□

11. 给定 $\lambda\in K$. 证明, λ 是特征值等价于 $X-\lambda\mid p_T(\lambda)$, 即 λ 为 $p_T(\lambda)$ 的根. 令 V_λ 为 λ 对应的特征子空间 (若 λ 不是特征值, 则 $V_\lambda=0$). 令 $\mu_a(\lambda)$ 为 λ 作为 $p_T(\lambda)$ 的根的重数, 我们称它为 λ 的**代数重数**; 令 $\mu_g(\lambda)=\dim_K V_\lambda$, 我们称它为 λ 的**几何重数**.

证明: λ 是特征值等价于存在非零向量 $v\in V$, 使得 $T(v)=\lambda v$. 这等价于 $(\lambda I-T)(v)=0$, 即 $v\in\operatorname{Ker}(\lambda I-T)$. 这等价于 $\det(\lambda I-T)=0$. 由于 $p_T(X)=\det(XI-T)$ 是 T 的特征多项式, $\det(\lambda I-T)=0$ 等价于 $X-\lambda\mid p_T(X)$. 因此, 有 λ 是特征值等价于 $X-\lambda\mid p_T(X)$. □

12. 证明, $\mu_g(\lambda)=|\{i\mid X-\lambda \text{ 乘除 } P_i(X)\}|$, 其中, $\{P_i\}_{i\leqslant s}$ 为 T 的不变因子. (提示: 可以将 $K[X]$-模 V 进一步分解为

$$V\simeq\left(\bigoplus_{\text{有限}}K[X]\big/(X-\lambda)^e\right)\oplus\left(\bigoplus_{\text{有限和},\,Q\text{ 不可约},\,Q(\lambda)\neq0}K[X]\big/(Q(X))^e\right)$$

并研究 $X-\lambda$ 在分量上的作用)

证明: 由于 V 在同构意义下可分解为

$$V\simeq\bigoplus_{i=1}^{s}K[X]\big/(P_i(X)),$$

再考虑每个分量 $K[X]\big/(P_i(X))$ 的进一步分解. 设 $P_i(X)$ 在 $K[X]$ 中的分解为

$$P_i(X)=(X-\lambda)^{e_i}(Q_{i,1}(X))^{e_{i,1}}\cdots(Q_{i,k_i}(X))^{e_{i,k_i}},$$

其中, $Q_{i,j}(X)$ 为不可约多项式且 $Q_{i,j}(\lambda)\neq 0$. 由中国剩余定理可知, 在同构意义下, 有环同构

$$K[X]/(P_i(X)) \simeq K[X]/(X-\lambda)^{e_i} \oplus K[X]/(Q_{i,1}(X))^{e_{i,1}} \oplus \cdots \oplus K[X]/(Q_{i,k_i}(X))^{e_{i,k_i}},$$

故也可视为 $K[X]$-模同构 (由商环性质保证). 由此可知, 在同构意义下, 有

$$\begin{aligned} V &\simeq \bigoplus_{i=1}^{s}\left(K[X]/(X-\lambda)^{e_i} \oplus K[X]/(Q_{i,1}(X))^{e_{i,1}} \oplus \cdots \oplus K[X]/(Q_{i,k_i}(X))^{e_{i,k_i}}\right) \\ &\simeq \left(\bigoplus_{i=1}^{s} K[X]/(X-\lambda)^{e_i}\right) \oplus \left(\bigoplus_{\text{有限和},\, Q\text{ 不可约},\, Q(\lambda)\neq 0} K[X]/(Q(X))^{e}\right). \end{aligned}$$

由题 11 的结论可知, $V_\lambda = \mathrm{Ker}(\lambda I - T)$. 注意到 $\lambda I - T$ 在 V 上的作用就等价于 $X-\lambda$ 在上述分解的各个分量上的作用. 于是有

$$V_\lambda \simeq \bigoplus \mathrm{Ker}\left(X-\lambda \text{ 作用在} K[X]/(X-\lambda)^e\right) \oplus \bigoplus \mathrm{Ker}\left(X-\lambda \text{ 作用在} K[X]/(Q(X))^e\right).$$

当 $X-\lambda$ 作用在 $K[X]/(X-\lambda)^e$ 上时, 显然 $\mathrm{Ker}\left(X-\lambda \text{ 作用在} K[X]/(X-\lambda)^e\right)$ 的基为 $\{(X-\lambda)^{e-1}+((X-\lambda)^e)\}$, 因此, 有

$$\dim_K \mathrm{Ker}\left(X-\lambda \text{ 作用在} K[X]/(X-\lambda)^e\right) = 1.$$

另一方面, 由于 $X-\lambda$ 在 $K[X]/(Q(X))^e$ 上是可逆的 (因为 $\gcd(X-\lambda, Q(X)) = 1$, 由 Bezout 定理可知), 因此, 有

$$\mathrm{Ker}\left(X-\lambda \text{ 作用在} K[X]/(Q(X))^e\right) = 0.$$

综上所述, 有

$$\begin{aligned} \mu_g(\lambda) &= \dim_K V_\lambda \\ &= \dim_K \bigoplus \mathrm{Ker}\left(X-\lambda \text{ 作用在} K[X]/(X-\lambda)^e\right) \\ &\quad + \dim_K \bigoplus \mathrm{Ker}\left(X-\lambda \text{ 作用在} K[X]/(Q(X))^e\right) \\ &= \left|\left\{i \mid K[X]/(X-\lambda)^{e_i}, \text{其中} e_i \geqslant 1\right\}\right| + 0 \\ &= \left|\left\{i \mid X-\lambda \text{ 乘除} P_i(X)\right\}\right|. \end{aligned}$$

□

13. 证明, $\mu_g(\lambda) \leqslant \mu_a(\lambda)$ 并且 $\sum_\lambda \mu_g(\lambda) \leqslant \dim_K V$.

证明: 由题 12 的结论可知, 有

$$\mu_g(\lambda) = \left|\left\{i \mid X-\lambda \text{ 乘除} P_i(X)\right\}\right|.$$

另一方面,

$$\begin{aligned}\mu_a(\lambda) &= \ X-\lambda \text{ 作为 } p_T(X) \text{ 的根的重数}\\ &= \ X-\lambda \text{ 作为} \prod_{i=1}^{s} P_i(X) \text{ 的根的重数}\\ &= \sum_{i=1}^{s} \ X-\lambda \text{ 作为 } P_i(X) \text{ 的根的重数}\\ &\geqslant \left|\left\{i \mid X-\lambda \text{ 乘除} P_i(X)\right\}\right| = \mu_g(\lambda).\end{aligned}$$

这说明 $\mu_g(\lambda) \leqslant \mu_a(\lambda)$.

进一步有

$$\sum_{\lambda} \mu_g(\lambda) \leqslant \sum_{\lambda} \mu_a(\lambda) = \deg p_T(X) = \dim_K V.$$

□

注: 对于不同特征值 $\lambda \neq \mu$, 其对应的特征子空间 V_λ, V_μ 的和为直和. 这是因为假设 $\exists\ v \in V_\lambda \cap V_\mu$, 则

$$Tv = \lambda v = \mu v \Rightarrow (\lambda - \mu)v = 0 \Rightarrow v = 0.$$

因此, 有

$$\sum_{\lambda} \mu_g(\lambda) = \sum_{\lambda} \dim_K V_\lambda \leqslant \dim_K V.$$

14. 证明, T 可被对角化当且仅当其极小多项式 $m_T(X)$ 分裂成一次多项式的乘积.

证明: 充分性: 设 $m_T(X)$ 分裂成一次多项式的乘积, 即

$$m_T(X) = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_k),$$

其中, λ_i 为 T 的特征值. 由题 13 的过程可知, 对于每个特征值 λ_i , 有 $\mu_g(\lambda_i) = \mu_a(\lambda_i)$. 因此, 有

$$\sum_{i=1}^{k} \mu_g(\lambda_i) = \sum_{i=1}^{k} \mu_a(\lambda_i) = \dim_K V.$$

这说明 V 可以写成特征子空间的直和:

$$V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \cdots \oplus V_{\lambda_k}.$$

因此, T 可被对角化.

必要性: 设 T 可被对角化, 则存在基 $\{v_1, v_2, \cdots, v_n\}$, 使得对于每个 v_i , 有

$$T(v_i) = \lambda_i v_i,$$

其中, λ_i 为 T 的特征值. 因此, 有

$$m_T(X) = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n).$$

这说明 $m_T(X)$ 分裂成一次多项式的乘积. □