0.1 其他

定理 0.1

设 $\mathbb{F}$ 是一个域,$m_i, a_i \in \mathbb{F}[x], i = 1, 2, \cdots, n$, 且 $\gcd\left(m_i, m_j\right) \mid \left(a_i - a_j\right), i, j \in \{1, 2, \cdots, n\}$, 则存在 $f \in \mathbb{F}[x]$ 使得

$$f(x) \equiv a_i(x) \pmod{m_i(x)}, i = 1, 2, \cdots, n,$$

即存在 $k_i \in \mathbb{F}[x]$ 使得

$$f(x) = k_i(x)m_i(x) + a_i(x), i = 1, 2, \cdots, n.$$

♡

证明

□

例题 0.1 设 $\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_m \in M_n(\mathbb{K})$,$g(x) \in \mathbb{K}[x]$, 使得 $g(\boldsymbol{A}_1), g(\boldsymbol{A}_2), \cdots, g(\boldsymbol{A}_m)$ 都是非异阵. 试用两种方法证明: 存在 $h(x) \in \mathbb{K}[x]$, 使得 $g(\boldsymbol{A}_i)^{-1} = h(\boldsymbol{A}_i)$ 对所有的 $1 \le i \le m$ 都成立.

证明 证法一:由命题**??**可知, 对 $\forall i \in \{1, 2, \cdots, m\}$, 存在 $h_i \in \mathbb{K}[x]$, 使得

$$g^{-1}(A_i) = h_i(A_i). \tag{1}$$

记 A_i 的极小多项式为 $n_i(x)$,$i = 1, 2, \cdots, m$. 考虑 $\gcd(n_i, n_j)(i, j \in \{1, 2, \cdots, m\})$, 设 $x_0 \in \mathbb{C}$ 是 $\gcd(n_i, n_j)$ 的根, 则 $(x - x_0)|n_i, n_j$, 即 x_0 是 A_i 和 A_j 的公共特征值. 由命题**??**和命题**??**可知,$h_i(x_0)$ 是 $h_i(A_i)$ 的特征值,$\dfrac{1}{g(x_0)}$ 是 $g^{-1}(A_i)$ 的特征值. 再由(1)式可知

$$g^{-1}(A_i) = h_i(A_i) \Longrightarrow \frac{1}{g(x_0)} = h_i(x_0), \quad i = 1, 2, \cdots, m.$$

于是

$$h_i(x_0) - h_j(x_0) = \frac{1}{g(x_0)} - \frac{1}{g(x_0)} = 0.$$

因此 $(x - x_0)|(h_i - h_j)$. 故在 $\mathbb{C}$ 上就有 $\gcd(n_i, n_j)|(h_i - h_j)$. 又因为整除不随数域扩张而改变, 所以在 $\mathbb{K}$ 上也有 $\gcd(n_i, n_j)|(h_i(x) - h_j(x))$. 于是由中国剩余定理的推广可知, 方程

$$h(x) \equiv h_i(x) \pmod{n_i(x)}, \quad i = 1, 2, \cdots, m$$

在 $\mathbb{K}$ 上有解. 故存在 $h \in \mathbb{K}[x]$, 使得

$$h(A_i) = h_i(A_i) = g^{-1}(A_i), \quad i = 1, 2, \cdots, m.$$

证法二:记 A_i 的极小多项式为 $n_i(x)$,$i = 1, 2, \cdots, m$, 由命题**??**可知

$$(n_i, g) = 1, i = 1, 2, \cdots, m.$$

从而 $(n_1 n_2 \cdots n_m, g) = 1$. 因此存在 $h, k \in \mathbb{F}[x]$, 使得

$$h(x) g(x) + n_1(x) n_2(x) \cdots n_m(x) k(x) = 1.$$

从而

$$h(A_i) = g^{-1}(A_i), i = 1, 2, \cdots, m.$$

□

例题 0.2

证明

□