

5. 在 $K[x]$ 中, $f_1(x), f_2(x), \dots, f_s(x)$ 两两互素, 证明对于任意的 $r_1(x), r_2(x), \dots, r_s(x) \in K[x]$, 同余方程组

$$\begin{cases} g(x) \equiv r_1(x) \pmod{f_1(x)} \\ g(x) \equiv r_2(x) \pmod{f_2(x)} \\ \vdots \\ g(x) \equiv r_s(x) \pmod{f_s(x)} \end{cases}$$

在 $K[x]$ 中有解, 且若 $c(x), d(x)$ 均为解, 则 $c(x) \equiv d(x) \pmod{f_1 f_2 \dots f_s}$.

7.4

考虑 $c-d \equiv 0 \pmod{f_i}$

考虑 $\begin{cases} g_1 \equiv 1 \pmod{f_1} \\ g_1 \equiv 0 \pmod{f_2} \end{cases}, \begin{cases} g_2 \equiv 0 \pmod{f_1} \\ g_2 \equiv 1 \pmod{f_2} \end{cases}$

$r_1 g_1 + r_2 g_2$ 即为原问题的一个解.

• 不可约多项式

• 唯一因式分解定理; 这里唯一性的意义是?

例题

1. 证明, 数域 K 上的一个次数大于零的多项式 f 与 $K[x]$ 中某一不可约多项式的正整数次幂相伴的充分必要条件是, 对于任意 $g(x) \in K[x]$, 必有 $(f(x), g(x)) = 1$, 或者存在一个整数数 m , 使得 $f(x) | g^m(x)$.

$f \sim p^m$, 必要性: 考虑 $p | g$ 或 $p \nmid g$

充分性, 取 f 的不可约因子 p_i

$(f, p_i) \neq 1 \Rightarrow f | p_i^m$

$\begin{cases} g_i \equiv 1 \pmod{f_i} \\ g_i \equiv 0 \pmod{f_1 \dots f_s} \end{cases}$

7.5 等

• 重因式

• 复数域上的不可约多项式只有一次的

• 实数域上的不可约多项式都是一次的, 或判别式小于零的二次多项式

• 有理数域上的不可约多项式可以是任意次数的

例题

1. 证明, $K[x]$ 中一个 n 次 ($n \geq 1$) 多项式 $f(x)$, 能被它的导数整除的充分必要条件是 $f(x)$ 与一个一次因式的 n 次幂相伴.

充分性显然

必要性: (f, f') 是 f 的所有不可约因式的乘积 (只出现一次)

$(f, f') = f' \Rightarrow f = (ax+b) f'$

$f = a p_1^{l_1} \dots p_s^{l_s}$

$f' = p_1^{l_1-1} \dots p_s^{l_s-1} h(x)$

2. 设 K 是一个数域, R 是 K 的一个交换扩环, 设 $a \in R$, 其中 $J_a \neq 0$,

$J_a = \{f(x) \in K[x] | f(a) = 0\}$

$(h(x)) \equiv c$

$f' | f \Rightarrow f = f' p_1 p_2 \dots p_s$

$\Rightarrow ax+b$ 是 f 唯一的不可约因子.

证明:

必要性方法二, 对 n 数学归纳.

$n=1$ 成立

假设 $n=k-1$ 成立, $n=k$ 时, $k > 1$

$f = (ax+b) f'$

$$f' = af' + (ax+b)f''$$

$$f' = \frac{1}{1-a}(ax+b)f''$$

$$\text{归纳: } \Rightarrow f' \text{ 为 } c(ax+b)^{k-1} \Rightarrow f = c(ax+b)^k$$

(1) J_a 中存在唯一的首项系数为 1 的多项式 $m(x)$, 使得 J_a 的元素都是 $m(x)$ 的倍式.

取次数最小的多项式为 $\tilde{m}(x)$

$$\forall f \in J_a, f(x) = \tilde{m}(x)p(x) + r(x) \quad \deg r < \deg \tilde{m}$$

$$\Rightarrow r(a) = f(a) - \tilde{m}(a)p(a) = 0. \quad r(x) \in J_a$$

(2) 如果 R 是无零因子环, 则 $m(x)$ 在 $K[x]$ 中不可约.

若 m 可约, $m = pq$

$$0 = m(a) = p(a)q(a), \quad p(a), q(a) \neq 0.$$

因为 $\deg p < \deg m$

$$\deg q < \deg m$$

(3) 取 $K = C, R = C[A]$, 其中

唯一性, m_1, m_2 次数相同. 首一

$$m_1 | m_2, m_2 | m_1$$

$$\Rightarrow m_1 = m_2$$

$m(x)$ 为 A 的最小多项式

求 J_A 中的 $m(x)$, 并判断 $C[A]$ 是无零因子环么?

特征多项式 $f(x) \in J_A$

$$A \text{ 的特征多项式, } |xI - A| = \begin{vmatrix} x-1 & 1 \\ -1 & x-1 \end{vmatrix} = (x-1)^2 + 1$$

$\Rightarrow m(x) | f(x)$

易见 $\deg m > 1, \Rightarrow m(x) = (x-1)^2 + 1$, 在 $C[x]$ 中可约.

3. 在复数域上求下述循环矩阵的全部特征值以及行列式

$C[A]$ 有零因子.

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ a_3 & a_4 & a_5 & \cdots & a_2 \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 1 & & & & 0 \end{bmatrix}, \quad A = a_1 I + a_2 C + \cdots + a_n C^{n-1}$$

$$= f(C), \quad f(x) = a_1 + a_2 x + \cdots + a_n x^{n-1}$$

C 的特征多项式 $x^n - 1$, 特征值为 $e^{\frac{2\pi k i}{n}}$, 记为 $\zeta^k, k=0, \dots, n-1$.

则 A 的特征值为 $f(\zeta^k), k=0, \dots, n-1$.

$$\text{解释: } |\lambda I - f(C)| = (-1)^n |C - z_1 I| |C - z_2 I| \cdots |C - z_n I|$$

\downarrow

$$\Rightarrow = (-1)^{n+n^2} |z_1 I - C| \cdots |z_n I - C| \quad \begin{matrix} (n+1)ls \\ (-1) \end{matrix}$$

$$\text{考虑多项式 } \lambda - f(x) = -(\lambda - z_1)(\lambda - z_2) \cdots (\lambda - z_n)$$

$$\text{已知 } g(\lambda) = |\lambda I - C| = (\lambda - \lambda_1)^{l_1} \cdots (\lambda - \lambda_s)^{l_s} \quad (\lambda - f(\lambda_1))^{l_1} \cdots (\lambda - f(\lambda_s))^{l_s}$$

$$\Rightarrow |\lambda I - f(C)| = (-1)^{n+n^2} |z_1 I - C| \cdots |z_n I - C| = (-1)^{n+n^2} (z_1 - \lambda_1)^{l_1} \cdots (z_n - \lambda_s)^{l_s} \\ = (\lambda - f(\lambda_1))^{l_1} \cdots (\lambda - f(\lambda_s))^{l_s} \quad \begin{matrix} (z_1 - \lambda_1)^{l_1} & \cdots & (z_1 - \lambda_s)^{l_s} \\ (z_2 - \lambda_1)^{l_1} & \cdots & (z_2 - \lambda_s)^{l_s} \\ \vdots & & \vdots \\ (z_n - \lambda_1)^{l_1} & \cdots & (z_n - \lambda_s)^{l_s} \end{matrix}$$