

上题作也

$$\begin{aligned}
 i) f &= (x_1 x_2 - 1)^2 + (x_3 x_4 + 1)^2 + 2x_1 x_2 \\
 &= x_1^2 x_2^2 + x_3^2 x_4^2 + 2x_1 x_2 + 2 \\
 \deg f &= 4 \quad \text{not } 10
 \end{aligned}$$

ii)  $f, g \in F[x] \setminus \{0\}$ ,  $F$  是域.  $h$  是  $f, g$  的最大的公因式, 则  $h$  是  $f, g$  的最小公倍式.

证:  $h$  是  $f, g$  最大公因式  $\stackrel{\text{Def}}{\iff} \forall h' \text{ with } f|h', g|h' \Rightarrow h|h'$   
 反证若  $h \nmid h'$ , 由带余除法  $h' = hq + r$   $\deg r < \deg h$   
 注意到  $f|r = h' - hq$   $g|r = h' - hq$  即  $r$  也是  $f, g$  的公因式, 且次数小于  $h$   
 矛盾  $\Rightarrow h|h'$

$$\begin{aligned}
 iii) (x^3 + 2x^2 + 2x + 1, x^2 + 2x) &= (x(x^2 + 2x) + 2x + 1, x^2 + 2x) \\
 &= (2x + 1, x^2 + 2x) \\
 \text{in } \mathbb{Q}[x] &= (2x + 1, (2x + 1)(\frac{1}{2}x + \frac{3}{4}) - \frac{3}{4}) \quad \text{or in } \mathbb{Z}_3[x] = (-x + 1, x^2 - x) \\
 &= (2x + 1, -\frac{3}{4}) = | \quad x - 1 \\
 &= 1
 \end{aligned}$$

iii) 线性映射  $A: F^2 \rightarrow F^2$  在基  $\{e_1, e_2\}$  下的矩阵表示为  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \triangleq A$   
 $f(A) = 0 \iff f(A) = 0$   
 • 对  $f = a_n x^n + \dots + a_0$   $f(A) := a_n A^n + a_{n-1} A^{n-1} + \dots + a_0 I$   $\rightarrow I$  单位阵  
 •  $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \implies f = x^2 + 1$

## 2. 多项式的形式导数

Def:  $D$  为整环.  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in D[x]$ , 记

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$$

称作  $f$  的形式导数

## 3. 形式导数与根的关系

prop: 设  $D$  是整环.  $f(x) \in D[x]$   $a \in D$

(1)  $a$  是  $f(x)$  的  $n$  重根  $\Rightarrow f(a) = f'(a) = \dots = f^{(n-1)}(a) = 0$

(2) 若  $D$  的特征为 0, 则

$$f(a) = \dots = f^{(n-1)}(a) = 0 \quad f^{(n)}(a) \neq 0 \Rightarrow a \text{ 是 } f \text{ 的 } n \text{ 重根}$$

(3) 若  $D$  是域 则  $(f, f') = 1 \Rightarrow f$  在  $D$  上无重根

Pf: (1)  $a$  是  $f$  的  $n$  重根  $\Rightarrow f(x) = (x-a)^n g(x)$

$$\begin{aligned} (x+a)^n &= x^n + n a x^{n-1} + \dots + a^n \\ (x+p)^n &= x^n + n p x^{n-1} + \dots + p^n \end{aligned} \quad \begin{aligned} f'(x) &= n(x-a)^{n-1} g(x) + (x-a)^n g'(x) \\ &= (x-a)^{n-1} (n g(x) + (x-a) g'(x)) \end{aligned}$$

$$\stackrel{\text{对 } n \text{ 归纳}}{\Rightarrow} f(a) = \dots = f^{(n-1)}(a) = 0$$

(2)  $D$  的特征为 0 时.

$$f(x) = f(x-a+a) = b_m (x-a)^m + \dots + b_1 (x-a) + b_0$$

$$\begin{aligned} \text{则 } f(a) &= b_0, f'(a) = b_1, \dots, f^{(m)}(a) = m! b_m \\ \text{char}(D) = 0 &\Rightarrow b_0 = \dots = b_{m-1} = 0 \quad b_m \neq 0 \end{aligned}$$

$$\begin{aligned} \Rightarrow f(x) &= (x-a)^m (b_m + b_{m-1}(x-a) + \dots + b_1(x-a)^{m-1}) \\ &= (x-a)^m g(x) \end{aligned}$$

$$\text{且 } g(a) = b_m \neq 0$$

(3) 若  $a$  为  $f$  的重根, 由 (1), 可得  $x-a \mid (f, f')$

$\swarrow$   $p$  是素数 (特征)

Example: in  $F_p[x]$   $f = (x^p+1)(x^p-1)$   $f' = p x^{p-1}(x^p-1) + p x^{p-1}(x^p+1) = 0$

but  $f = (x-1)^p (x+1)^p$

$\pm 1$  是  $f$  的  $p$  重根. (结合 (2) 中, 特征  $p \neq 0$  时的反例.)



4. 设  $p$  为素数  $f \in \mathbb{Z}[X]$ ,  $p \nmid f$ , 则  $\bar{f}$  在  $\mathbb{Z}_p[X]$  不可约  $\Rightarrow f$  在  $\mathbb{Z}[X]$  不可约

pf: 反证即可

rank:  $f(x) = a_n x^n + \dots + a_0 \quad \bar{f}(x) := \bar{a}_n x^n + \dots + \bar{a}_0 \in \mathbb{F}_p[X]$

5. (练习) 设  $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[X]$   $\deg f = n$ . 若存在素数  $p$ , 整数  $k$ , s.t.

$p \nmid a_n \quad p \nmid a_0 \quad p \mid a_i \quad (0 \leq i \leq k-1) \quad p^2 \nmid a_0$

则  $f(x)$  在  $\mathbb{Z}[X]$  中必存在次数  $\geq k$  的不可约因子

pf: (本质上类似于 Eisenstein 判别的证明)

反证 设  $f = \alpha_1 \dots \alpha_s \quad \deg \alpha_i \leq k$

设  $\alpha_i(x) = \alpha_i^{d_i} x^{d_i} + \alpha_i^{d_i-1} x^{d_i-1} + \dots + \alpha_i^0 \quad d_i = \deg \alpha_i \leq k$

$\bullet p \nmid a_0 = \alpha_1^{d_1} \alpha_2^{d_2} \dots \alpha_s^{d_s} \Rightarrow p \nmid \alpha_i^{d_i} \quad (\alpha_i^{d_i} \text{ 中 } d_i \text{ 是指标, 不是幂次})$

ie  $p \nmid f(x) \Rightarrow p \nmid \alpha_i(x) \quad \deg \alpha_i = \deg \alpha_i$

$\bullet p^2 \nmid a_0, p \mid a_0, a_0 = \alpha_1^{d_1} \alpha_2^{d_2} \dots \alpha_s^{d_s} \Rightarrow$  不妨设  $p \mid \alpha_1, p^2 \nmid \alpha_1, p \nmid \alpha_2, \dots, p \nmid \alpha_s$

$\bullet$  考虑模  $p$  在  $\mathbb{Z}_p[X]$

$\bar{f} = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \dots + \bar{a}_k x^k$

$\bar{\alpha}_1 = \bar{a}_1^{d_1} x^{d_1} + \dots + \bar{a}_1^0 x^0$

$\bar{\alpha}_i = \bar{a}_i^{d_i} x^{d_i} + \dots + \bar{a}_i^0 x^0 + \bar{a}_i^0$

注意到  $x^k \mid \bar{f} = \bar{\alpha}_1 \dots \bar{\alpha}_s \quad x \nmid \bar{\alpha}_2, \dots, \bar{\alpha}_s \quad x$  是  $\mathbb{Z}_p[X]$  中素元

$\Rightarrow x^k \mid \bar{\alpha}_1 \Rightarrow \deg \alpha_1 \geq k$  矛盾  $\square$

6. (拉格朗日)  $D$  是整环  $f \in D[X]$   $\deg f = n \Rightarrow f$  在  $D$  中的根不超过  $n$  个.

rank: 若  $D$  不是交换环, 则上述命题不成立.

Example: 四元数体  $H = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \mid i^2 = j^2 = k^2 = -1 \quad ij = -ji = k, jk = -kj = i, ki = -ik = j\}$

$x^2 + 1$  在  $H[X]$  有无数个根  $b + ic + dk$  with  $b^2 + c^2 + d^2 = 1$ .

