

多元多项式

2022年12月19日 7:00

回忆. 设 F 是域, $f, g \in F[x]$
 $g \neq 0$. 则 $\exists!$ $q, r \in F[x]$

使得 $f = \boxed{q}g + \boxed{r}$, $\deg(r) < \deg(g)$
 $\boxed{q} := \text{quo}(f, g, x)$, $\boxed{r} := \text{rem}(f, g, x)$

余式定理. 设 $\alpha \in F$
 $\underline{f(\alpha)} = \text{rem}(f, \underline{x - \alpha}, x)$

§1.5 多项式的根

定义 设 F 和 K 两个域
 F 是 K 的子域 (K 是 F 的扩域)

设 $\underline{f} \in \underline{(F)[x]}$, $\alpha \in K$

如果 $f(\alpha) = 0$, 则称 α
是 $\underline{f}$ 的一个根 (root)



例: $\underline{f(x)} = x^2 - 2 \in \underline{(Q)[x]}$
 $f(\sqrt{2}) = 0$, $f(\underline{-\sqrt{2}}) = 0$



$$f(\sqrt{2}) = 0, \quad f(-\sqrt{2}) = 0$$

注 $f \in K[x] \rightarrow$ 多项式

命题: 设 F 是域, $f \in F[x]$

$$\deg(f) = n > 0$$

则 $\alpha \in F$ 是 f 的根 $\Leftrightarrow$
 $\text{rem}(f, x - \alpha) = 0$

证: α 是 f 的根

$$\Leftrightarrow f(\alpha) = 0$$

$$\Leftrightarrow \text{rem}(f, x - \alpha) = 0 \quad (\text{余式定理})$$

注

α 是 $f(x)$ 的根 $\Leftrightarrow f(x) = g(x)(x - \alpha)$
 其中 $g(x) \in F[x]$

$$\text{且 } \deg g = n - 1$$

定理 设 F 是域, $f \in F[x]$

且 $\deg(f) = n > 0$. 则

f 在域 F 中至多有 n 个根

证: (1) 对 n 归纳
 $n=1$ $f = \underline{f_1}x + f_0, f_1, f_0 \in F$
且 $f_1 \neq 0$

于是 f 有唯一的根
 $\underline{-f_1^{-1}f_0}$

设 $n > 1$. 且令命题对 $n-1$ 次多项式成立. 如果 f 在 F 中有根. 则命题成立. 否则设
 $\alpha \in F$ 使得 $f(\alpha) = 0$

由上述命题

$$f(x) = g(x)(x - \alpha)$$

设 β 是 f 的另一个根且 $\beta \neq \alpha$

$$0 = f(\beta) = \underbrace{g(\beta)}_{\substack{\in F \\ \neq 0}} \underbrace{(\beta - \alpha)}_{\neq 0}$$

—— 矛盾

$\therefore F$ 中没有零因子

$$\therefore g(b) = 0.$$

$\therefore g$ 的次数至多 $n-1$

$\therefore g$ 至多有 $n-1$ 个互不相同的根

$\Rightarrow f$ 至多有 n 个互不相同的根

另证: 假设 f 有 $n+1$ 个互不相同

的根 $\alpha_1, \alpha_2, \dots, \alpha_{n+1} \in F$

$$\text{设 } f = f_0 + f_1 x + \dots + f_n x^n$$

$$\text{则 } f(\alpha_i) = f_0 + f_1 \alpha_i + \dots + f_n \alpha_i^n = 0 \quad i=1, 2, \dots, n$$

$$(1, \alpha_i, \dots, \alpha_i^n) \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = 0$$

$$\text{即 } \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^n \\ 1 & \alpha_2 & \dots & \alpha_2^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n+1} & \dots & \alpha_{n+1}^n \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$A \in M_{n+1}(F)$$

由范德蒙行列式可知

$$\det(A) \neq 0$$

$$\Rightarrow f_0 = f_1 = \dots = f_n = 0$$

$$\rightarrow \leftarrow \deg(f) = n. \quad \square$$

$$\langle \text{例} \rangle \quad f(x) = x^2 \in \mathbb{R}[x]$$

$$\in \mathbb{R} \left[\underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_A \right]$$

$$0 \ 0) \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\forall \alpha \in \mathbb{R} \quad f(\alpha A) = 0$$

§* 期末总结

矩阵部分

设 F 是域

1. 方阵

(a) $(M_n(F), +, \cdot, 0, \cdot, E)$

是非交换环. $\square$

$$\forall \lambda \in F, \quad A, B \in M_n(F)$$

$$\lambda(A+B) = \lambda A + \lambda B$$

$$\lambda(AB) = (\lambda A)B = A(\lambda B)$$

(b) A 可逆 $\Leftrightarrow$ A 满秩

(c) A 是左(右)零因子 $\Leftrightarrow A$ 不满足且 $A \neq 0$

(d) A 是中心元 $\Leftrightarrow A = \lambda E$
 $(\forall B \in M_n(F), AB = BA)$ [证明略]

$\underline{U_R}$

(e) $(M_n(F), +, 0, \cdot, E)$

所有可逆元的集 $\underline{GL_n(F)}$

$$\underline{(A^{-1})^{-1} = A} \quad \underline{(AB)^{-1} = B^{-1}A^{-1}}$$

2 初等矩阵

(a) 第 I, II, III 类初等矩阵
 (它们的逆是同类型初等矩阵)

(b) 行列引理

(c) 可逆矩阵是初等矩阵

之和

矩阵求逆的方法

$GL_n(F)$
 是一组生成元
 是所有的初等

可逆

3 矩阵求逆

(a) 行变换法

(b) 多项式法

设 $A \in M_n(F)$. 则 $\exists$
 $f \in F[x], f \neq 0$. 使得

$$f(A) = 0 \quad (*)$$

设 f 是满足 (*) 次数最小
的多项式. 则

$$A \text{ 可逆} \Leftrightarrow f(0) \neq 0$$

若 $f(0) \neq 0$, 则 A^{-1} 可以
写为 $F[A]$ 中的元素

$$\Rightarrow B \text{ 是 } F[A] \text{ 中的元素} \\ \Leftrightarrow \text{rank}(B) = n.$$

4. 矩阵分块

1. 证明及计算. 利用矩阵

分块矩阵秩的不等式. 不考)

行列式部分

1. 定义与性质

$$(a) \det \left((a_{i,j})_{n \times n} \right)$$

$$= \sum_{\sigma \in S_n} \varepsilon_{\sigma} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$$

行列式的定义只需要行列式性质

(b) 多重线性. 行列对称.

且. 如果有两行或两列相同则行列式的值为零

$$(c) \det(A) = \det(A^t)$$

(d) 行列式乘积定理

$$\det(A^{-1}) = \det(A)^{-1}$$

$$\left[\begin{array}{l} \det: GL_n(F) \rightarrow (F^*, \cdot, 1) \\ A \mapsto \det(A) \end{array} \right.$$

是群同态]

2. 行列式计算

- (a) 利用初等变换化为上(下)三角
- (b) 按一行或一列展开. 用初等法
- (c) 利用分块矩阵.

3. 行列式的性质

- (a) 伴随矩阵和原矩阵的关系

$$(AB)^V = B^V A^V \quad \text{不考}$$

- (b) Cramer 法则 (不专门考)

- (c) 矩阵的秩和它的子式的关系

[它说明秩的概念与行列式性质有关]

群. 环. 域

- 1. 抽象 = 无运算不考
同余运算必考

群

环. 域

(a) 群, 同态, 同构, 子群 ...
子群判定法

(b) 最低阶非循环群 $\mathbb{Z}_2 \times \mathbb{Z}_2$
... 交换群. S_3

$GL_n(F), S_n$

(c) 群和子群的生成

(d) 群中元素的阶

(e) 循环群的分类, 有限循环群
的所有子群

(f) Lagrange 定理和 Cayley 定理
—— 不考 ——

3 环

(a) 环, 同态, 同构, 子环, 整环
环特征.

(b) 广义分配律

(c) 子环的判定: $\mathbb{R}[A]$
 $\mathbb{Z}[\sqrt{2}]$

(d) 左和右逆同时存在

环中可逆元构成乘法群

$(\mathbb{Z}_n, +, \cdot, \bar{0}, \bar{1})$ 中的可逆
 元和零因子是什么
 FCA 中的可逆元和零因子?

- (e) 环中消去律
- (f) 同态与环的特征
- (g) 零因子, 零零矩阵 不考

4 域

- (a) 域, 同态, 同构, 子域, 域的特征
- (b) 子域的经验:
- (c) 整环的分式域 (不考证明)
- (d) 域的嵌入
- (e) 域上的线性代数

一元多项式

1. 未定元的引入不考

2. 在 $R[x]$ 中, R 交换环

(a) 次数, 首项系数

(b) $+$, $\cdot$, $-$, $\div$ (证明不考)

(c) 赋值例证. (10002.24)

3. 设 F 是域

(a) $F[x]$ 是整环.

(b) $F[x]$ 中的乘法

✓ (c) 设 $f \in F[x]$, $A \in M_n(F)$
计算 $f(A)$

§2 多元多项式

$$x^2 + y^2 - 1$$

$$\begin{array}{ccccc} R & \subset & R[x] & \subset & \underline{R[x][y]} \\ \downarrow & & \downarrow & & \downarrow \\ \text{交换环} & & \text{一元多项式环} & & \text{二元多项式环} \end{array}$$

例

$$f = \underbrace{(x^2+1)}_v y^3 - (x+1)y^2 + x^5 + 2x \in \mathbb{Z}[x][y]$$

$\deg_y(f) = 3, \quad lc_y(f) = x^2+1$
 $\deg(f, y) \quad lc(f, y)$

$$= -\underbrace{x^5}_v + \underbrace{y^3}_{\deg_x(f)=5} x^2 + \underline{(2-y^2)} x + \underline{y^3 - y^2}$$

$lc_x(f) = -1$

$$= x^2 y^3 + y^3 - x y^2 - y^2 - x^5 + 2x$$

$$= \frac{x^2y^3 + y^3 - xy - y - x - 1 - 2x}{\text{分布式}}$$

§2.1 多元多项式环

定义：设 R 是交换环，交换环 $R[x_1][x_2]\dots[x_n]$ 称 R 上的 n 元多项式环

由分布式观点 我们可以把 $R[x_1][x_2]\dots[x_n] = R[x_1, x_2, \dots, x_n]$

定理 如果 R 是整环，则 $R[x_1, x_2, \dots, x_n]$ 也是

证：对 n 归纳证明。

$n=1$ $R[x_1]$ 是整环 [已证]
设 n 成立，则 $R[x_1, \dots, x_{n-1}]$ 是整环

再用一次上节的结果

$R[x_1, \dots, x_{n-1}][x_n]$ 是整环

注: 设 F 是域

$$F(x_1, \dots, x_n) := \left\{ \frac{f}{g} \mid f, g \in F[x_1, \dots, x_n], g \neq 0 \right\}$$

是域 (多元有理分式域) ✓

定义: 设 $R[x_1, \dots, x_n]$ 是交换环 R 上的多元多项式环. 令

$$X_n = \{ x_1^{d_1} x_2^{d_2} \dots x_n^{d_n} \mid d_1, d_2, \dots, d_n \in \mathbb{N} \}$$

称 X_n 中的元素为单项式

(monomial)

设 $M = x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$

$$\deg(M) := d_1 + d_2 + \dots + d_n$$

称为 M 的总次数

M 关于 x_i 的次数 d_i 记为 $\deg_{x_i}(M)$

证 设 $M, N \in X_n$
 则 $MN \in X_n$ 且

$$\deg(MN) = \deg(M) + \deg(N)$$

引理 设 $M_1, \dots, M_k \in X_n$ 互不同
 又 $\alpha_1, \dots, \alpha_k \in R$

如果 $\alpha_1 M_1 + \dots + \alpha_k M_k = 0$

则 $\alpha_1 = \dots = \alpha_k = 0$

证 对 n 归纳.

$n=1$. 设 $M_1 = x_1^{e_1}, \dots, M_k = x_1^{e_k}$

且 $e_1 < e_2 < \dots < e_k$

则 $\alpha_1 x_1^{e_1} + \dots + \alpha_k x_1^{e_k} = 0$

$\therefore x_1$ 是 R 上非零元

$\therefore \alpha_1 = \dots = \alpha_k = 0$ ✓

设 $n > 1$. 且 假设对 $n-1$ 成立

$$d = \max(\deg_{x_n}(M_1), \dots, \deg_{x_n}(M_k))$$

$\therefore d \geq 1$ 则 x_n 在 $M_1, \dots, M_k$ 中

如果 $d=0$. 则 x_n 在 $M_1, \dots, M_k$ 中
都不出现. 则由归纳假设

$$\alpha_1 = \dots = \alpha_k = 0$$

设 $d > 0$ 不妨设 $\alpha_1, \dots, \alpha_k$ 都不为 0

再设 $\deg_{x_n}(M_1) < d, \dots, \deg(M_{i-1}) < d$
 $\deg_{x_n}(M_i) = \dots = \deg_{x_n}(M_k) = d$

$$M_i = N_i x_n^d, \dots, M_k = N_k x_n^d$$

$$\text{其中 } N_i, \dots, N_k \in X_{n-1}$$

$$\left[\begin{array}{c} \underbrace{(x_1^3)}_{N_1} \underbrace{x_2^6}_{\sim} \\ \underbrace{(x_1^2)}_{N_2} \underbrace{x_2^6}_{\sim} \end{array} \right]$$

$$0 = \alpha_1 M_1 + \dots + \alpha_{i-1} M_{i-1} + \alpha_i N_i x_n^d + \dots + \alpha_k N_k x_n^d$$

$$= \underbrace{\alpha_1 M_1 + \dots + \alpha_{i-1} M_{i-1}}_{\in R[x_1, \dots, x_{n-1}]} + (\alpha_i N_i + \dots + \alpha_k N_k) x_n^d$$

右边是一个 $R[x_1, \dots, x_{n-1}][x_n]$ 中的多项式

首项系数是 $\alpha_i N_i + \dots + \alpha_k N_k$

$$\Rightarrow \alpha_i N_i + \dots + \alpha_k N_k = 0$$

$\therefore M_2, \dots, M_k$ 两两不同
 $\therefore N_2, \dots, N_k$ 两两不同

由归纳假设 $\alpha_2 = \dots = \alpha_k = 0$
 与 $\alpha_k \neq 0$. $\rightarrow \leftarrow$ 矛盾

定理 设 $p \in R[x_1, \dots, x_n]$ 且 $p \neq 0$

则 $\exists!$ 两两不同的单项式

$M_1, \dots, M_k \in X_n$

和非零元素 $(\neq 0) \alpha_1, \dots, \alpha_k \in R$

使得

$$p = \alpha_1 M_1 + \dots + \alpha_k M_k$$

证: 显然 p 由 $R[x_1, \dots, x_n]$ 中运算
 可得 即 $p \in R$.

设 $p = \beta_1 N_1 + \dots + \beta_l N_l$

$\beta_1, \dots, \beta_l \in R$. 非零

且 $N_1, \dots, N_l \in X_n$ 的
 两两不同

要证: $k=l$. 适当安排非零项后

证: $k=2$. 适当安排 $1 \sim n$

$$\alpha_1 = \beta_1, \quad M_1 = N_1$$

$$\alpha_k = \beta_k, \quad M_k = N_k$$

□