一元多项式

2022年12月14日 7:05

回忆 设 $(R,+,0,\cdot,1)$ 是交换环

$\tilde{R}=\{(r_0,r_1,r_2\cdots)\mid r_n\in R,\ 有限个非零\}$

$(\tilde{R},+,\tilde{0},\cdot,\tilde{1})$ 是交换环

$R \hookrightarrow \tilde{R}$

$r \longmapsto \underline{(r,0,0\cdots)}$

$\Rightarrow (\tilde{R},+,\underline{0},\cdot,\underline{1})$ 是交换环

$r_0+r_1x+\cdots+r_nx^n$

$r_0=0,r_1=1,\ r_2=\cdots=r_n=\cdots 0$

令 $x=(0,1,0,0\cdots)$

断言 $\forall n\in\mathbb{Z}^+$

$x^n=(\underbrace{0,0\cdots0}_{n},\underset{n}{1},0\cdots0)$

证: $n=1$. ✓

设 $n-1$ 时断言成立

$x^{n-1}=(\underbrace{0,\cdots0}_{n-1}\ 1\ 0\ 0\cdots0\cdots)$

$x^n=x\,x^{n-1}=\underbrace{(0,1\ 0\cdots0\cdots)}_{r_1}(\underbrace{0\cdots0}_{n-1}\underset{S_{n-1}}{1},0\cdots)$

$=(\underbrace{0,\cdots0}_{n}\ 1\ 0\cdots)$ ☐

$\forall\ \tilde{r}=(r_0,r_1,\cdots r_N,0\ 0\cdots)$

$$\forall\ \tilde{r} = (r_0, r_1, \cdots r_N, 0, 0 \cdots\ )$$

$$\tilde{r} = r_0(1, 0, 0 \cdots 0) + r_1(0, 1, 0 \cdots 0 \cdots) + \cdots + r_N(\underbrace{0, 0 \cdots 0}_{N}\ 1\ 0 \cdots)$$

$$= r_0 x^0 + r_1 x + \cdots + r_N x^N$$

$\forall\ \tilde{r} \in \tilde{R}\ \exists!\ r_0, r_1, \cdots r_N \cdots$ 使得

$$\tilde{r} = r_0 x^0 + r_1 x + \cdots + r_N x^N$$

$$[\ x^0 := 1\ ]$$

特别地.

$$\boxed{\begin{aligned} &\tilde{r} = r_0 + r_1 x + \cdots + r_N x^N = 0 \\ &\iff r_0 = r_1 = \cdots = r_N = 0 \end{aligned}}$$

$$p(x) = p_d x^d + p_{d-1} x^{d-1} + \cdots + p_0 = 0$$

$p_i \in R$. 则 $p_d = p_{d-1} = \cdots = p_0 = 0$

$$R = \mathbb{Z}_2$$

x. 未定元 indeterminate

$$\tilde{R} := R[x] = \left\{ r_0 + r_1 x + \cdots + r_n x^n \ \middle|\ \begin{matrix} r_i \in R \\ n \in \mathbb{N} \end{matrix} \right\}$$

幂次

系数

如 $r_n \neq 0$, 则 n 称为

定义：如果 $r_n \neq 0$，则 n 称为

$$r := r_0 + r_1 x + \cdots + r_n x^n$$

的次数 记为 $\deg_x(r)$

或 $\deg(r)$

且 r_n 称为 r 的首项系数

(leading coefficient) 记为

$lc_x(r)$ 或 $lc(r)$

如果 $r = 0$，则

$$\deg(0) := -\infty$$

$$lc(0) := 0.$$

§1.2 加法与乘法

命题，设 $p, q \in R[x]$

则 $\deg(p+q) \leq \max(\deg(p), \deg(q))$

当 $\deg(p) \neq \deg(q)$，等式成立

$$p = p_m x^m + p_{m-1} x^{m-1} + \cdots + p_1$$

$$q = q_n x^n + q_{n-1} x^{n-1} + \cdots + q_0$$

不妨设 $m \geq n$

$$p+q = p_m x^m + \cdots + p_{n+1} x^{n+1} + \underline{(p_n + q_n)} x^n + \underline{(p_{n-1} + q_{n-1})} x^{n-1} + \cdots + \underline{p_0 + q_0}$$

$(p+q) = m$

$+ (p_{n-1}+g_{n-1})$ ——

若 $m>n$. $\deg(p+g)=m$

若 $m=n$ $\deg(p+g)\le m$ 丌

[分段 p或g为零. 则(命题成立)

命题: 设 $p, g \in R[x]$

$\deg(pg)\le \deg(p)+\deg(g)$

$lc(p)lc(g)\neq 0 \Longleftrightarrow$ 等号成立

证: 设 $\deg p=m$. $\deg g=n$

$p=p_m x^m+p_{m-1}x^{m-1}+\cdots+p_0$

$g=g_n x^n+g_{n-1}x^{n-1}+\cdots+g_0$

$pg=(p_m x^m+p_{m-1}x^{m-1}+\cdots+p_0)(g_n x^n+g_{n-1}x^{n-1}+\cdots+g_0)$

$=p_m g_n x^{m+n}+$ 次数低于 $m+n$ 的项

$\deg(pg)\le m+n$ 且

$p_m g_n\neq 0 \Longleftrightarrow \deg(pg)=m+n$ 曰

例: 设 $f=\bar{2}x^2+\bar{3}x+\bar{1}$

$g=\bar{3}x+\bar{4}$ 是

$\mathbb{Z}_6[x]$ 中的多项式

计算 $f+g$, $f\cdot g$

计算 $f+g$, ...

解 $f+g=\bar{2}x^2+(\bar{3}+\bar{3})x+\bar{1}+\bar{4}$

$=\bar{2}x^2+\bar{5}$

$fg=f(\bar{3}x+\bar{4})$

$=\bar{3}fx+\bar{4}f$

$=\bar{3}(\bar{2}x^2+\bar{3}x+\bar{1})x+\bar{4}(\bar{2}x^2+\bar{3}x+\bar{1})$

$=\underbrace{\bar{6}x^3}_{=\bar{0}}+\bar{9}x^2+\bar{3}x+\bar{8}x^2+\underbrace{\bar{12}x}_{=\bar{0}}+\bar{4}$

$=\underline{\bar{5}x^2}+\underline{\bar{3}x}+\bar{4}$

定理. 设 D 是整环, 则 $D[x]$ 也是整环.

证: 设 $p, q\in D[x]$ 都非零

则 $lc(p), lc(q)\in D$ 都非零

于是 $lc(p)lc(q)\neq 0$

故 $\deg(pq)=\deg(p)+\deg(q)$

$\Rightarrow pq\neq 0$ $\square$

注 $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$

$\mathbb{Z}_p[x]$. 中是素数

二、分式域的概念 $D(x)$

四 分式域的概念 $D(x)$

$D[x]$ 分式域 $F_r(D[x])=\left\{\frac{f(x)}{g(x)} \middle| \begin{matrix} f, g\in D[x] \\ g\neq 0 \end{matrix}\right\}$

特别地，当 $D=\mathbb{R}$

$\mathbb{R}(x)$ 称为 $\mathbb{R}$ 上的有理~~函数域~~

对于任意的域 $F \longrightarrow F[x]$

$F(x)$ F 上的有理分式域

x^{-1} $\frac{1}{x}\in F(x)$

$\frac{1}{x^2}+\frac{1}{x}+2+x+4x^2$

$\mathbb{Z}_p(x)$ 的特征是 p

1.3 求值定理

$f(x)=x^2-4\in\mathbb{R}[x]$

$f(3)=3^2-4=5$

$f(x)=(x-2)(x+2)$

$f(3)=(3-2)(3+2)=5$

$f(\bar{5})=\bar{5}^2-\bar{4}$

$f(A)$ A^2-4E

... 是交换环

定理 设 S 是交换环，

$\varphi: R \to S$ 是环同态

且 $s \in S$ ∃! 环同态

$\varphi_s: R[x] \longrightarrow S$

满足 $\varphi_s|_R = \varphi$. $\varphi_s(x) = s$

证明：存在性。定义

$\varphi_s: R[x] \longrightarrow S$

$\sum_{i=0}^{n} r_i x^i \longmapsto \sum_{i=0}^{n} \varphi(r_i) s^i$

$r_i \in R$

良定义 OK

设 $f = \sum_{i=0}^{k} f_i x^i$, $g = \sum_{j=0}^{l} g_j x^j$

$k \geq l$

$f + g = f_k x^k + \cdots + f_{l+1} x^{l+1} + \sum_{i=0}^{l} (f_i + g_i) x^i$

$\varphi_s(f+g) = \varphi(f_k) s^k + \cdots + \varphi(f_{l+1}) s^{l+1}$

$+ \sum_{i=0}^{l} (\varphi(f_i) + \varphi(g_i)) s^i$

$$+\sum_{j=0}$$

$$=\sum_{i=0}^{k}\varphi(p_i)s^i+\sum_{j=0}^{l}\varphi(q_j)s^j$$

$$=\varphi_s(p)+\varphi_s(q)$$

$$\varphi_s((p_ix^i)(q_jx^j))=\varphi_s(p_iq_jx^{i+j})$$

$$=\varphi(p_iq_j)s^{i+j}$$

$$\varphi_s(p_ix^i)\varphi_s(q_jx^j)$$

$$=\varphi(p_i)s^i\varphi(q_j)s^j$$

$$=\varphi(p_i)\varphi(q_j)s^{i+j}$$ [∵ S 是交换环]

于是 φ_s 保持单项式的乘法

$$\varphi_s(pq)=\varphi_s\left(\left(\sum_{i=0}^{k}p_ix^i\right)\left(\sum_{j=0}^{l}q_jx^j\right)\right)$$

$$=\varphi_s\left(\sum_{i=0}^{k}\sum_{j=0}^{l}(p_ix^i)(q_jx^j)\right)$$

$$=\sum_{i=0}^{k}\sum_{j=0}^{l}\varphi_s((p_ix^i)(q_jx^j))$$

$$=\sum_{i=0}^{k}\sum_{j=0}^{l}\varphi(p_i)s^i\varphi(q_j)s^j$$

$$\ldots)\left(\sum^{l}\varphi(q_j)s^j\right)$$

$\quad i=0 \quad j=0$

$$= \left(\sum_{i=0}^{k} \varphi(p_i) s^i\right)\left(\sum_{j=0}^{l} \varphi(q_j) s^j\right)$$

$$= \varphi(p)\,\varphi(q)$$

$$\varphi_s(1) = \varphi(1) = 1_S \quad \checkmark$$

φ_s 是环同态

唯一性见讲义 $\square$

注

$$\begin{tikzcd} R[x] \arrow[dr, "\varphi_s\ (\exists!)"] & \\ R \arrow[u] \arrow[r, "\varphi"] & S \end{tikzcd}$$

φ 被提升为 $\varphi_s : R[x] \to S$

lifting

例: 设 $f(x) = x^2 - 4 \in \mathbb{Z}[x]$

求 $f(15)$

$$\begin{tikzcd} \mathbb{Z}[x] \arrow[dr, "\varphi_{15}"] & \\ \mathbb{Z} \arrow[u] \arrow[r, "id_{\mathbb{Z}}"'] & \mathbb{Z} \end{tikzcd}$$

$$(p_i x^i) \quad , \quad p_i \in \mathbb{Z}$$

$$\mapsto \sum^{k} id_{\mathbb{Z}}(p_i)\, 15^i = \sum_{i=0}^{k} p_i\, 15^i$$

$= \sum_{i=0}^{k} \pi_{\mathbb{Z}}(p_i) \overline{15}^{i}$ $i=0$

$f(15) = 15^2 - 4 = 221$

$f(x) = (x-2)(x+2)$

$f(15) = (15-2)(15+2) = 221.$

例 设 $\pi: \mathbb{Z} \to \mathbb{Z}_n$ 是环同态
$m \mapsto \overline{m}$

$\forall\ p = p_k x^k + \cdots + p_1 x + p_0 \in \mathbb{Z}[x]$, $p_i \in \mathbb{Z}$

取 $p(\overline{m}) = \pi(p_k)\overline{m}^k + \cdots + \pi(p_1)\overline{m} + \pi(p_0)\overline{1}$

例 设 $g = (179x - 286)(413x - 567)$

计算 $g(\overline{3})$，其中 $\overline{3} \in \mathbb{Z}_5$

$g(\overline{3}) = (\overline{179}\ \overline{3} - \overline{286})(\overline{413}\ \overline{3} - \overline{567})$

$= (\overline{4} \cdot \overline{3} - \overline{1})(\overline{3}\ \overline{3} - \overline{2})$

$= \overline{2}$

推论：设 F 是域，$A \in M_n(F)$

则 $\rho_A: F[x] \to F[A]$
$\sum_{i=0}^{k} p_i x^i \mapsto \underline{\sum_{i=0}^{k} p_i A^i}$

$(p_i \in F)$

是环同态。

$(F[A], +, \cdot, O, E)$

✓ 环

是环同态.

$(F[A],+,\cdot,E)$ 交换

记 $\rho: F \longrightarrow F[A]$

$\lambda \longmapsto \lambda E$

可直接验证: ρ 是环同态

则由赋值定理, $\exists!$

$$\rho_A: F[x] \longrightarrow F[A]$$

$$\sum_{i=0}^{k} p_i x^i \longmapsto \underline{\sum_{i=0}^{k} \rho(p_i) A^i}$$

$$\sum_{i=0}^{k} \rho(p_i) A^i = \sum_{i=0}^{k} (p_i E) A^i = \sum_{i=0}^{k} p_i A^i$$ $\boxtimes$

例: 设 $f = x^2 - 4 \in \mathbb{R}[x]$

$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ $\rho(4) = 4E$ 计算 $f(A)$

$[\underline{A^2 - 4}]$

解 $f(A) = A^2 - 4E$

$= \begin{pmatrix} 4 & 4 \\ 0 & 4 \end{pmatrix} - 4E = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$

$f(x) = (x-2)(x+2)$

$f(A) = (A-2E)(A+2E)$

$= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$

$f(x) \in \mathbb{Z}[x]$

$m \in \mathbb{Z}$

$\varphi_m \quad (f(m))$

$$\begin{tikzcd} \mathbb{Z}[x] \arrow[dr, "\varphi_m"] & \\ \mathbb{Z} \arrow[u, "\iota"] \arrow[r, "\mathrm{id}"] & \mathbb{Z} \end{tikzcd}$$

$$\begin{tikzcd} \mathbb{Z}[x] \arrow[dr, "\varphi_A"] & \\ \mathbb{Z} \arrow[u, "j"] \arrow[r, "\varphi"] & \mathbb{Z}[A] \end{tikzcd}$$

$A \in M_n(\mathbb{Z})$

$\lambda \longmapsto \lambda E$

$$\mathbb{Z} \xrightarrow{id_{\mathbb{Z}}} \mathbb{Z}$$

$$\mathbb{Z}[x] \qquad \varphi_{\overline{m}} \quad f(\overline{m})$$

$$\downarrow f$$

$$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n$$

$$\overline{m}$$

$$\lambda \longmapsto \lambda E$$

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots \overline{p-1}\} \qquad card(\mathbb{Z}_p) = p$$

$\mathbb{Z}_p[x]$ 整环

$$\mathbb{Z}_p(x) = \left\{ \frac{\alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_0}{\beta_m x^m + \beta_{m-1} x^{m-1} + \dots + \beta_0} \;\middle|\; \begin{array}{l} \alpha_i, \beta_j \in \mathbb{Z}_p \\ n, m \in \mathbb{N} \end{array} \right\}$$

$\hookrightarrow$ 无限域 $char(\mathbb{Z}_p(x)) = p$.

例 设 $A, B \in M_n(F)$

证明: $(AB)^\vee = B^\vee A^\vee$

证: 当 A 和 B 都可逆时

证明与作业中的证明一样.

假设 A 或 B 不可逆

令 x 是 F 上的未定元

$A_x = xE + A$. $\quad B_x = xE + B$

$F(x)$

则 $\det(A_x)$ 是关于 x 的 n 次多项式

$\Rightarrow \det(A_x) \neq 0$

$\Rightarrow A_x$ 可逆

同理 B_x 也可逆

由可逆时的结论可知

$$\underset{\substack{\| \\ C_x = (c_{ij}(x))}}{(A_x B_x)^\vee} = \underset{\substack{\| \\ D_x = (d_{ij}(x))}}{B_x^\vee A_x^\vee}$$

则 $c_{ij}(x) = d_{ij}(x)$. $\because c_{ij}(x), d_{ij}(x) \in F(x)$

$\Longrightarrow c_{ij}(0) = d_{ij}(0)$

可直接验证(知同时代入 $x=0$ 是同态)

$c_{ij}(0)$ 是 $(AB)^\vee$ 中第 i 行第 j 列的元素

$d_{ij}(0)$ 是 $B^\vee A^\vee$ 中 ......

$\Longrightarrow \underline{(AB)^\vee = B^\vee A^\vee}$ □

"x" 未定元. indeterminate

§1.4 多项式的除法

引理 设 $f, g \in R[x]$ 且 $g \neq 0$

再设 $lc(g)$ 是 R 中的可逆元

则 $\exists!$ 多项式 $q, r \in R[x]$

满足

$f = qg + r$ 和 $\deg(r) < \deg(g)$

$$f = q\,g + r$$

$q \to \mathrm{quo}(f, g, x)$, $r \to \mathrm{rem}(f, g, x)$

<u>证明</u>（存在性）当 $\deg(f) < \deg(g)$

取 $q = 0$, $r = f$ 即可

设 $f = f_{n+k}x^{n+k} + \cdots + f_1 x + f_0$

$g = g_n x^n + \cdots + g_1 x + g_0$

<u>其中</u> f_i, $g_j \in R$, $k \geq 0$, $f_{n+k} \neq 0$

$g_n \neq 0$ 且可逆

对 k 归纳. $k = 0$

$$f = \underline{f_n x^n} + f_{n-1}x^{n-1} + \cdots + f_0$$

$$g = \underline{g_n x^n} + g_{n-1}x^{n-1} + \cdots + g_0$$

$$f - \underbrace{\boxed{g_n^{-1} f_n}}_{q}\, g$$

$$= f - \left(f_n x^n + g_n^{-1} f_n g_{n-1} x^{n-1} + \cdots + g_n^{-1} f_n g_0\right)$$

$$= \underbrace{(f_{n-1} - g_n^{-1} f_n g_{n-1})x^{n-1} + \text{低次项}}_{r}$$

$f = q\,g + r$ 且 $\deg(r) \leq n-1$. ✓

设 $k > 0$. 且对 $n, n+1, \ldots, n+k-1$ 存在性成立

$$h := f - g_n^{-1} f_{n+k} x^k g$$

$$= (f_{n+k} - f_{n+k} g_n^{-1} g_n) x^{n+k}$$

$$+ (f_{n+k-1} - f_{n+k} g_n^{-1} g_{n-1}) x^{n+k-1}$$

$+ \cdots$ 低次式

$$\deg(h) \le n+k-1$$

由归纳假设可知

$\exists\ \tilde{q}, \tilde{r} \in R[x]$ 使得

$$h = \tilde{q} g + \tilde{r}$$

且 $\deg(\tilde{r}) < \deg(g)$

$$f_{n+k} = \underbrace{(g_n^{-1} f_{n+k} x^k + \tilde{q})}_{q} g + \underbrace{\tilde{r}}_{r}$$

存在性成立

(唯一性) 设 $f = q g + r$

$$f = p g + a$$

其中 $q, p, r, a \in R[x]$

$\deg(r) < \deg(g)$, $\deg(a) < \deg(g)$

则 $(q - p) g = a - r \quad (*)$

如果 $q - p \neq 0$. 则 $\deg((q-p) g)$

$= \deg(q-p) + \deg(g) > \deg(a-r)$

[$\because$ $lc(g)$ 可逆] 与 $(*)$ 矛盾

故 $q = p \Rightarrow a = r$. 证

定理 设 $f, g \in F[x]$，其中 F 是域

如果 $g \neq 0$，则 $\exists q, r \in F[x]$

使得 $f = qg + r$

且 $\deg(r) < \deg(g)$

证：$\because$ F 中非零元都可逆

例：设 $f = x^3 + 3x + 1$，$g = 2x^2 + 1 \in \mathbb{Q}[x]$

求 $\mathrm{rem}(f, g, x)$

解

$$
\begin{array}{r|l}
 & \frac{1}{2}x \\
\hline
2x^2+1 & x^3 + 3x + 1 \\
 & x^3 + \frac{1}{2}x \\
\hline
 & \frac{5}{2}x + 1
\end{array}
$$

$\Rightarrow \mathrm{rem}(f, g, x) = \frac{5}{2}x + 1$

例 设 $f = \bar{3}x^3 + \bar{2}x^2 + \bar{1}$

$g = \bar{2}x^2 + \bar{4}$

是 $\mathbb{Z}_5[x]$ 中的多项式

计算 $\mathrm{quo}(f, g, x)$，$\mathrm{rem}(f, g, x)$

解：$\bar{2}^{-1} = \bar{3}$

$$
\begin{array}{r}
\bar{4}x+\bar{1} \\
\bar{2}x^2+\bar{4} \;\big)\; \bar{3}x^3+\bar{2}x^2+\bar{1} \\
\bar{3}x^3+x \\
\hline
\bar{2}x^2+\bar{4}x+\bar{1} \\
\bar{2}x^2+\bar{4} \\
\hline
\bar{4}x+\bar{2}
\end{array}
$$

$\mathrm{quo}(f,g)=\bar{4}x+\bar{1}$. $\mathrm{rem}(f,g)=\bar{4}x+\bar{2}$ □

定理 设 $a\in R$. $f(x)\in R[x]$

则 $\mathrm{rem}(f, \underline{x-a}) = f(a)$

证: $x-a$ 的首项系数可逆

$f(x)=q(x)(x-a)+r$. $r\in R$

$f(a)=q(a)(a-a)+r$

$=r$ □