

第五章 复数域和多项式

1 一元多项式

符号约定: 在本节中 $(R, +, 0, \cdot, 1)$ 是交换环.

1.1 一元多项式环的构造

设 R 是交换环. 令

$$\tilde{R} = \{(r_0, r_1, r_2, \dots, r_n, \dots) \mid r_n \in R, \text{有限多个非零}\}.$$

我们定义

$$\begin{aligned} + : \quad & \tilde{R} \times \tilde{R} && \longrightarrow && \tilde{R} \\ & ((\dots, r_n, \dots), (\dots, s_n, \dots)) && \mapsto && (\dots, r_n + s_n, \dots) \end{aligned}$$

注意到两个只有有限多个非零元的无穷序列之和仍是一个只有有限多个非零元的无穷序列. 故加法是良定义的. 可直接验证 $(\tilde{R}, +, \tilde{0})$ 是交换群, 其中 $\tilde{0}$ 代表由 0 组成的无穷序列.

再定义

$$\begin{aligned} \cdot : \quad & \tilde{R} \times \tilde{R} && \longrightarrow && \tilde{R} \\ & ((\dots, r_n, \dots), (\dots, s_n, \dots)) && \mapsto && (\dots, \sum_{i+j=n} r_i s_j, \dots) \end{aligned}$$

\uparrow_n

设 $w \in \mathbb{N}$ 使得 $r_w = r_{w+1} = \cdots = 0$ 和 $s_w = s_{w+1} = \cdots = 0$. 则当 $\ell \geq 2w$ 时, $\sum_{i+j=\ell} r_i s_j = 0$. 故乘法是良定义的. 下面我们验证 $(\tilde{R}, \cdot, \tilde{1})$ 是交换的含么半群, 其中

$$\tilde{1} = (1, 0, 0, \dots).$$

交换性成立来自 R 是交换环和

$$\sum_{k=0}^n r_k s_{n-k} = \sum_{k=0}^n r_{n-k} s_k.$$

下面我们来验证结合律. 设 $\tilde{a}, \tilde{b}, \tilde{c} \in \tilde{R}$, 其中

$$\tilde{a} = (a_0, a_1, \dots), \quad \tilde{b} = (b_0, b_1, \dots), \quad \tilde{c} = (c_0, c_1, \dots).$$

我们要证明 $(\tilde{a}\tilde{b})\tilde{c} = \tilde{a}(\tilde{b}\tilde{c})$. 为此, 我们假设

$$\tilde{p} = \tilde{a}\tilde{b}, \quad \tilde{q} = (\tilde{a}\tilde{b})\tilde{c}, \quad \tilde{u} = \tilde{b}\tilde{c}, \quad \tilde{v} = \tilde{a}(\tilde{b}\tilde{c}).$$

则

$$q_n = \sum_{i+j=n} p_i c_j = \sum_{i+j=n} \left(\sum_{k+l=i} a_k b_l \right) c_j = \sum_{k+l+j=n} a_k b_l c_j.$$

类似地,

$$v_n = \sum_{k+i=n} a_k u_i = \sum_{k+i=n} a_k \left(\sum_{\ell+j=i} b_\ell c_j \right) = \sum_{k+\ell+j=n} a_k b_\ell c_j.$$

故 $q_n = v_n$. 由此可知结合律成立.

我们再来验证乘法单位

$$\tilde{r}\tilde{1} = (r_0, r_1, r_2, \dots)(1, 0, 0, \dots) = (r_0, r_1, r_2, \dots) = \tilde{r}.$$

故 $(\tilde{R}, \cdot, \tilde{1})$ 是交换的含幺半群.

最后我们验证分配律. 设 $\tilde{f} = \tilde{a}(\tilde{b} + \tilde{c})$ 和 $\tilde{g} = \tilde{a}\tilde{b} + \tilde{a}\tilde{c}$. 则

$$\begin{aligned} f_n &= \sum_{i+j=n} a_i(b_j + c_j) = \sum_{i+j=n} (a_i b_j + a_i c_j) \\ &= \left(\sum_{i+j=n} a_i b_j \right) + \left(\sum_{i+j=n} a_i c_j \right) \\ &= g_n. \end{aligned}$$

故分配律成立. 我们证明了下述命题.

命题 1.1 五元组 $(\tilde{R}, +, \tilde{0}, \cdot, \tilde{1})$ 是交换环.

引理 1.2 设 $(R, +, 0, \cdot, 1)$ 是交换环. 则

$$\begin{aligned} \phi: R &\longrightarrow \tilde{R} \\ r &\mapsto (r, 0, 0, \dots) \end{aligned}$$

是单环同态.

证明. 由 \tilde{R} 中运算的定义可知, 对任意 $r, s \in R$,

$$\phi(r + s) = (r + s, 0, 0, \dots) = \phi(r) + \phi(s),$$

$$\phi(rs) = (rs, 0, 0, \dots) = \phi(r)\phi(s),$$

和

$$\phi(1) = (1, 0, 0, \dots) = \tilde{1}.$$

故 ϕ 是环同态. 如果 $\phi(r) = \tilde{0}$, 则 $(r, 0, 0, \dots) = (0, 0, 0, \dots)$. 故 $r = 0$. 根据第四章第二讲引理 2.46, ϕ 是单射. \square

于是, R 与 \tilde{R} 的子环 $\{(r, 0, 0, \dots) \mid r \in R\}$ 同构. 我们可以把 $(r, 0, 0, \dots)$ 简记为 r .

对于任意 $r \in R$, $\tilde{s} = (s_0, s_1, \dots, s_n, \dots) \in \tilde{R}$,

$$r\tilde{s} = (r, 0, 0, \dots)(s_0, s_1, \dots, s_n, \dots) = (rs_0, rs_1, rs_2, \dots).$$

令

$$x = (0, 1, 0, 0, \dots).$$

我们用数学归纳法来证明: 对任意 $n \in \mathbb{Z}^+$

$$x^n = \underbrace{(0, \dots, 0, 1, 0, 0, \dots)}_n. \quad (1)$$

当 $n=1$ 时, 结论显然成立. 设 $n>1$ 且结论对 $n-1$ 成立. 则

$$\begin{aligned} x^n &= xx^{n-1} = x\underbrace{(0, \dots, 0, 1, 0, 0, \dots)}_{n-1} \\ &= (0, 1, 0, 0, \dots)\underbrace{(0, \dots, 0, 1, 0, 0, \dots)}_{n-1} \\ &= \underbrace{(0, \dots, 0, 1, 0, 0, \dots)}_n. \end{aligned}$$

归纳法完成.

由此得出对任意 $\tilde{r} = (r_0, r_1, r_2, \dots, r_n, 0, 0, \dots) \in \tilde{R}$,

$$\tilde{r} = r_0 + r_1x + r_2x^2 + \cdots + r_nx^n.$$

故

$$\tilde{R} = \left\{ \sum_{k=0}^n r_k x^k \mid n \in \mathbb{N}, r_k \in R \right\} := R[x].$$

我们称 $(R[x], +, 0, \cdot, 1)$ 是 R 上关于未定元 x 的一元多项式环. 命题 1.1 说明 $(R[x], +, 0, \cdot, 1)$ 是良定义的交换环. 根据引理 1.2, 我们可以认为 $R \subset R[x]$.

注解 1.3 由 x 的定义和 (1) 可知, 对任意 $r_0, r_1, \dots, r_n \in R$,

$$r_0 + r_1x + \cdots + r_nx^n = 0 \iff r_0 = r_1 = \cdots = r_n = 0.$$

1.2 加法与乘法

定义 1.4 设 $p = p_nx^n + p_{n-1}x^{n-1} + \cdots + p_0 \in R[x]$, 其中 $p_n, p_{n-1}, \dots, p_0 \in R$. 如果 $p_n \neq 0$, 则称 n 是 p 的次数 (*degree*), 记为 $\deg(p)$; p_n 是 p 的首项系数 (*leading coefficient*), 记为 $\text{lc}(p)$. 当 $p = 0$ 时, 它的次数定义为 $-\infty$ 而其首项系数定义为 0.

命题 1.5 设 $p, q \in R[x]$. 则 $\deg(p+q) \leq \max(\deg(p), \deg(q))$. 当 p, q 次数不同时, 等号成立.

证明. 设 $p = \sum_{i=0}^k p_i x^i$ 和 $q = \sum_{j=0}^{\ell} q_j x^j$, 其中 $p_i, q_j \in R$ 且 $p_k \neq 0$ 和 $q_{\ell} \neq 0$. 不妨设 $k \geq \ell$. 于是

$$p + q = p_k x^k + \cdots + p_{\ell+1} x^{\ell+1} + \sum_{i=0}^{\ell} (p_i + q_i) x^i.$$

故 $\deg(p + q) \leq k$ 且 $k > \ell$ 时等号成立. 当 $p = 0$ 或 $q = 0$ 时结论自然成立. \square

命题 1.6 设 $p, q \in R[x]$. 则 $\deg(pq) \leq \deg(p) + \deg(q)$. 当 $\text{lc}(p)\text{lc}(q) \neq 0$ 时, 等号成立且 $\text{lc}(pq) = \text{lc}(p)\text{lc}(q)$.

证明. 设 $p = \sum_{i=0}^k p_i x^i$ 和 $q = \sum_{j=0}^{\ell} q_j x^j$, 其中 $p_i, q_j \in R$ 且 $p_k \neq 0$ 和 $q_{\ell} \neq 0$. 于是

$$pq = (p_k q_{\ell}) x^{k+\ell} + (p_k q_{\ell-1} + p_{k-1} q_{\ell}) x^{k+\ell-1} + \text{低次项}.$$

故 $\deg(pq) \leq k + \ell$ 且 $p_k q_{\ell} \neq 0$ 时等号成立且 $\text{lc}(pq) = p_k q_{\ell}$. 当 $p = 0$ 或 $q = 0$ 时结论自然成立. \square

例 1.7 设 $f = \bar{2}x^2 + \bar{3}x + \bar{1}$ 和 $g = \bar{3}x + \bar{4}$ 是 $\mathbb{Z}_6[x]$ 中的多项式. 计算 $f + g$ 和 fg .

解. 直接计算得

$$f + g = \bar{2}x^2 + \bar{6}x + \bar{5} = \bar{2}x^2 + \bar{5}.$$

利用分配律计算得

$$fg = f\bar{3}x + f\bar{4} = (\bar{6}x^3 + \bar{9}x^2 + \bar{3}x) + (\bar{8}x^2 + \bar{12}x + \bar{4}) = \bar{5}x^2 + \bar{3}x + \bar{4}.$$

定理 1.8 设 D 是整环. 则 $D[x]$ 是整环. 特别地, 当 F 是域时, $F[x]$ 是整环.

证明. 设 $p, q \in D[x] \setminus \{0\}$. 则 $\text{lc}(p)$ 和 $\text{lc}(q)$ 都不等于 0. 因为 D 是整环, 所以 $\text{lc}(p)\text{lc}(q) \neq 0$. 根据命题 1.6, $\text{lc}(pq) \neq 0$. 故 $pq \neq 0$. \square

例 1.9 设 F 是域. 则 $F[x]$ 的分式域记为 $F(x)$. 特别地, $\mathbb{R}(x)$ 是实系数的有理函数构成的域. 设 p 是素数. 则 $\mathbb{Z}_p(x)$ 是特征为正的无限域.

1.3 赋值定理

本节说明如何把多项式看成“函数”.

定理 1.10 设 S 是交换环, $\phi : R \rightarrow S$ 是环同态, 且 $s \in S$. 则存在唯一的环同态 $\phi_s : R[x] \rightarrow S$ 满足

$$\phi_s|_R = \phi \quad \text{和} \quad \phi_s(x) = s.$$

证明. 定义:

$$\begin{aligned} \phi_s : R[x] &\longrightarrow S \\ \sum_{i=0}^n r_i x^i &\mapsto \sum_{i=0}^n \phi(r_i) s^i. \end{aligned}$$

下面验证 ϕ_s 是环同态. 设 $p = \sum_{i=0}^k p_i x^i$ 和 $q = \sum_{j=0}^{\ell} q_j x^j$, 其中 $p_i, q_j \in R$. 不妨设 $k \geq \ell$. 于是

$$p + q = p_k x^k + \cdots + p_{\ell+1} x^{\ell+1} + \sum_{i=0}^{\ell} (p_i + q_i) x^i.$$

则

$$\begin{aligned}\phi_s(p+q) &= \phi(p_k)s^k + \cdots + \phi(p_{\ell+1})s^{\ell+1} + \sum_{i=0}^{\ell} \phi(p_i+q_i)s^i \quad (\phi_s \text{ 的定义}) \\ &= \phi(p_k)s^k + \cdots + \phi(p_{\ell+1})s^{\ell+1} + \sum_{i=0}^{\ell} (\phi(p_i) + \phi(q_i))s^i \quad (\phi \text{ 保持加法}) \\ &= \left(\sum_{i=0}^k \phi(p_i)s^i \right) + \left(\sum_{j=0}^{\ell} \phi(q_j)s^j \right) \quad (\text{加法交换律}) \\ &= \phi_s(p) + \phi_s(q) \quad (\phi_s \text{ 的定义})\end{aligned}$$

再计算:

$$\begin{aligned}\phi_s((p_i x^i)(p_j x^j)) &= \phi_s((p_i p_j) x^{i+j}) \\ &= \phi(p_i p_j) s^{i+j} \quad (\phi_s \text{ 的定义}) \\ &= \phi(p_i) \phi(p_j) s^{i+j} \quad (\phi \text{ 保持乘法}) \\ &= (\phi(p_i) s^i) (\phi(p_j) s^j) \quad (S \text{ 中乘法交换}).\end{aligned}$$

于是,

$$\begin{aligned}\phi_s(pq) &= \phi_s \left(\left(\sum_{i=0}^k p_i x^i \right) \left(\sum_{j=0}^{\ell} q_j x^j \right) \right) \\ &= \phi_s \left(\sum_{i=0}^k \sum_{j=0}^{\ell} (p_i x^i)(q_j x^j) \right) \quad (\text{广义分配律}) \\ &= \sum_{i=0}^k \sum_{j=0}^{\ell} \phi_s((p_i x^i)(q_j x^j)) \quad (\phi_s \text{ 保持加法}) \\ &= \sum_{i=0}^k \sum_{j=0}^{\ell} (\phi(p_i) s^i) (\phi(q_j) s^j) \quad (\text{上述计算}) \\ &= \left(\sum_{i=0}^k \phi(p_i) s^i \right) \left(\sum_{j=0}^{\ell} \phi(q_j) s^j \right) \quad (\text{广义分配律}) \\ &= \phi_s(p) \phi_s(q) \quad (\phi_s \text{ 的定义}).\end{aligned}$$

最后,

$$\phi_s(1_R) = \phi_s(1_R x^0) = \phi(1_R) s^0 = 1_S s^0 = 1_S.$$

故 ϕ_s 是环同态. 对任意 $r \in R$,

$$\phi_s(r) = \phi_s(r x^0) = \phi(r) s^0 = \phi(r) \implies \phi_s|_R = \phi.$$

存在性成立.

设 $\psi : R[x] \longrightarrow S$ 是环同态满足 $\psi|_R = \phi$ 和 $\psi(x) = s$.

则

$$\begin{aligned}\psi(p) &= \sum_{i=0}^k \psi(p_i)\psi(x)^i \quad (\psi \text{ 是环同态}) \\ &= \sum_{i=0}^k \phi(p_i)s^i \quad (\psi \text{ 的性质}) \\ &= \phi(p) \quad (\phi \text{ 的定义}).\end{aligned}$$

唯一性成立. \square

我们称上述定理中的环同态 ϕ_s 称为关于 ϕ 在 s 处的赋值同态. 当 $S = R$ 且 $\phi = \text{id}_R$ 时, ϕ_s 就是通常的从 $R[x]$ 到 R 的在 s 处的赋值映射: $f(x) \mapsto f(s)$

例 1.11 设 $f = x^2 - 4 \in \mathbb{Z}[x]$. 计算 $f(15)$.

证明. 设 $\phi = \text{id}_{\mathbb{Z}}$. 则

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

或

$$\begin{aligned}f(15) &= \phi_{15}(f) = \phi_{15}((x-2)(x+2)) \\ &= \phi_{15}(x-2)\phi_{15}(x+2) \quad (\phi_{15} \text{ 是环同态}) \\ &= 13 \times 17 = 221.\end{aligned}$$

例 1.12 设 $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ 是商映射(环同态). 则

$$\begin{aligned}\phi: \mathbb{Z} &\longrightarrow \mathbb{Z}_n[x] \\ m &\mapsto \bar{m}.\end{aligned}$$

由定理 1.10 可知, ϕ_y 是环同态, 其中 $\phi_y|_{\mathbb{Z}} = \phi = \pi$ 且 $\phi_y(x) = x$.

例 1.13 设 $g = (179x - 286)(413x - 587)$. 计算 $g(\bar{3})$, 其中 $\bar{3} \in \mathbb{Z}_5$. 由定理 1.10 可知, $\phi_{\bar{3}} : \mathbb{Z}[x] \rightarrow \mathbb{Z}_5$ 是环同态, 其中 $\phi_{\bar{3}}|_{\mathbb{Z}}$ 是从 \mathbb{Z} 到 \mathbb{Z}_5 的商映射, 且 $\phi_{\bar{3}}(x) = \bar{3}$. 则

$$\begin{aligned} g(\bar{3}) &= \phi_{\bar{3}}(g) \quad (\text{符号的定义}) \\ &= \phi_{\bar{3}}((179x - 286)(413x - 587)) \\ &= \phi_{\bar{3}}(179x - 286)\phi_{\bar{3}}(413x - 587) \quad (\phi_{\bar{3}} \text{ 是环同态}) \\ &= (\overline{179\bar{3}} - \overline{286})(\overline{413\bar{3}} - \overline{587}) \quad (\phi_{\bar{3}} \text{ 的定义}) \\ &= (\bar{4}\bar{3} - \bar{1})(\bar{3}\bar{3} - \bar{2}) = \bar{2}. \end{aligned}$$

推论 1.14 设 F 是域, $A \in M_n(F)$. 则

$$\begin{aligned} \rho_A : F[x] &\longrightarrow F[A] \\ \sum_{i=0}^k p_i x^i &\mapsto \sum_{i=0}^k p_i A^i \end{aligned}$$

是环同态, 其中 $k \in \mathbb{N}$, $p_0, p_1, \dots, p_k \in F$.

证明. 根据第四章第二讲 § 3.5 节, $F[A]$ 是交换环. 注意到

$$\begin{aligned} \rho : F &\longrightarrow F[A] \\ \lambda &\mapsto \lambda E_n \end{aligned}$$

是环同态. 根据定理 1.10, ρ_A 是由 $\rho_A|_F = \rho$ 和 $\rho_A(x) = A$ 确定的环同态. \square

例 1.15 设 $f = x^2 - 4 \in \mathbb{R}[x]$, $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$. 计算 $f(A)$.

解. (法 1)

$$f(A) = A^2 - 4E = \begin{pmatrix} 4 & 4 \\ 0 & 4 \end{pmatrix} - 4E = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}.$$

(法 2) 因为 $f = (x - 2)(x + 2)$, 所以

$$f(A) = (A - 2E)(A + 2E) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}.$$

我们用多项式赋值的观点重新叙述一下求矩阵逆的多项式法.

引理 1.16 设 F 是域, $A \in M_n(F)$. 则存在非零多项式 $f \in F[t]$ 使得 $f(A) = O$.

证明. 把 $M_n(F)$ 中的元素看成 F 上的坐标空间 F^{n^2} 中的向量. 则 $E = A^0, A, \dots, A^{n^2}$ 在 F 上线性相关. 故存在 $\alpha_0, \alpha_1, \dots, \alpha_{n^2} \in F$, 不全为零, 使得

$$\alpha_0 E + \alpha_1 A + \dots + \alpha_{n^2} A^{n^2} = O.$$

设 $f = \alpha_0 + \alpha_1 t + \dots + \alpha_{n^2} t^{n^2}$. 则 $f \in F[t] \setminus \{0\}$. 上述线性关系蕴含 $f(A) = O$. \square

命题 1.17 设 F 是域, $A \in M_n(F)$. 则 A 是可逆矩阵当且仅当存在多项式 $f \in F[t]$ 满足 f 关于 x^0 的系数非零且 $f(A) = O$.

证明. 设 $f(t) = f_m t^m + \cdots + f_1 t + f_0$, 其中 $f_m, \dots, f_1, f_0 \in F$. 如果 $f(A) = O$ 且 $f_0 \neq 0$. 则

$$\begin{aligned} A(f_m A^{m-1} + \cdots + f_1 E) + f_0 E &= O \\ \implies A \underbrace{(-f_0^{-1}(f_m A^{m-1} + \cdots + f_1 E))}_B &= E. \end{aligned}$$

故 $B = A^{-1}$.

反之, 设 A 可逆. 令 $g(t) = g_k t^k + g_{k-1} t^{k-1} + \cdots + g_0$ 是 $F[t]$ 中使得 $g(A) = O$ 的次数最低的非零多项式. 如果 $g_0 = 0$, 则

$$g(A) = O \implies A(g_k A^{k-1} + g_{k-1} A^{k-2} + \cdots + g_1 E) = O.$$

令 $h(t) = g_k t^{k-1} + g_{k-1} t^{k-2} + \cdots + g_1$. 则 $h \neq 0$ 且 $\deg(h) = k - 1$. 由 k 的极小性可知, $h(A) \neq O$. 但 $g(A) = O$ 蕴含 $Ah(A) = O$. 因为 A 可逆, $h(A) = O$. 矛盾. \square

注解 1.18 由上述证明的矩阵 B 可知, 如果 A 可逆, 则 $A^{-1} \in F[A]$.

最后, 我们描述域上的摄动法.

记号. 设 F 是域, $A(t) \in M_n(F[t])$, 即 $A(t) = (a_{i,j}(t))_{n \times n}$, 其中 $a_{i,j}(t) \in F[t]$. 设 $\alpha \in F$. 令

$$A(\alpha) = (a_{i,j}(\alpha))_{n \times n}.$$

命题 1.19 设 F 是域, $A(t), B(t) \in M_n(F[t])$, $\alpha \in F$. 则

$$(A(t)+B(t))(\alpha) = A(\alpha)+B(\alpha), \quad (A(t)B(t))(\alpha) = A(\alpha)B(\alpha)$$

和

$$\det(A(t))(\alpha) = \det(A(\alpha)).$$

证明. 由多项式带入值式环同态直接可得. \square

例 1.20 设 $A, B \in M_n(F)$. 证明: $(AB)^\vee = B^\vee A^\vee$.

证明. 设 A 和 B 可逆. 则

$$A^\vee = \det(A)A^{-1} \quad \text{和} \quad B^\vee = \det(B)B^{-1}.$$

于是

$$B^\vee A^\vee = \det(A) \det(B) B^{-1} A^{-1} = \det(A) \det(B) (AB)^{-1} = (AB)^\vee.$$

当 A 或 B 中至少由一个不可逆时, 令 $M(t) = tE + A$ 和 $N(t) = tE + B$. 则 $\det(M)$ 和 $\det(N)$ 都是次数为 n 的多项式. 故它们是 $M_n(F(t))$ 中的矩阵. 由上一段的结论可知 $(M(t)N(t))^\vee = N(t)^\vee M(t)^\vee$. 注意到多项式矩阵的伴随矩阵仍是多项式矩阵. 根据命题 1.19,

$$(M(0)N(0))^\vee = N(0)^\vee M(0)^\vee.$$

因为 $A = M(0)$ 和 $B = N(0)$, 所以 $(AB)^\vee = B^\vee A^\vee$. \square

1.4 多项式的除法

引理 1.21 设 $f, g \in R[x]$ 且 $g \neq 0$. 再设 $\text{lc}(g)$ 可逆. 则存在唯一的多项式 $q, r \in R[x]$ 满足

$$f = qg + r \quad \text{和} \quad \deg(r) < \deg(g).$$

证明. (存在性) 当 $\deg(f) < \deg(g)$ 时, 令 $q = 0$ 和 $r = f$ 即可. 否则, 设

$$f = f_{n+k}x^{n+k} + f_{n+k-1}x^{n+k-1} + \cdots + f_0, \quad g = g_nx^n + g_{n-1}x^{n-1} + \cdots + g_0,$$

其中 $k \geq 0$, $f_i, g_j \in R$ 且 g_n 可逆.

我们对 k 归纳. 当 $k = 0$ 时, 计算

$$\begin{aligned} f - f_n g_n^{-1} g &= (f_n - f_n g_n^{-1} g_n) x^n + (f_{n-1} - f_n g_n^{-1} g_{n-1}) x^{n-1} + \cdots + f_0 - f_n g_n^{-1} g_0 \\ &= \underbrace{(f_{n-1} - f_n g_n^{-1} g_{n-1}) x^{n-1} + \cdots + f_0 - f_n g_n^{-1} g_0}_r \end{aligned}$$

再令 $q = f_n g_n^{-1}$. 则 $f = qg + r$ 且 $\deg(r) < n$ 即可.

设 $k > 0$ 且存在性对小于 k 的值都成立. 计算

$$\begin{aligned} f - f_{n+k} g_n^{-1} x^k g &= (f_{n+k} - f_{n+k} g_n^{-1} g_n) x^{n+k} + (f_{n+k-1} - f_{n+k-1} g_n^{-1} g_{n-1}) x^{n+k-1} + \\ &\quad \cdots + (f_k - f_{n+k} g_n^{-1} g_0) x^k + f_{k-1} x^{k-1} + \cdots + f_0 \\ &= \underbrace{(f_{n+k-1} - f_{n+k-1} g_n^{-1} g_{n-1}) x^{n+k-1} + \cdots + (f_k - f_{n+k} g_n^{-1} g_0) x^k + f_{k-1} x^{k-1} + \cdots + f_0}_h. \end{aligned}$$

则 $\deg(h) < n + k$. 由归纳假设或证明中第一段的结论可得, 存在 $\tilde{q}, r \in R[x]$ 满足

$$h = \tilde{q}g + r \quad \text{和} \quad \deg(r) < n.$$

则

$$f = \underbrace{(f_n g_n^{-1} x^{n-k} + \tilde{q})}_q g + r.$$

存在性成立.

(唯一性) 再设 $q', r' \in R[x]$ 满足

$$f = q'g + r' \quad \text{和} \quad \deg(r') < \deg(g).$$

则

$$(q - q')g = r' - r. \tag{2}$$

因为 $\deg(r) < \deg(g)$ 且 $\deg(r') < \deg(g)$, 所以

$$\deg(r' - r) < \deg(g)$$

(命题 1.5). 因为 $\text{lc}(g)$ 可逆, 所以

$$\deg((q - q')g) = \deg(q - q') + \deg(g)$$

(命题 1.6). 由此可知, (2) 蕴含 $q = q'$. 进而, $r = r'$. 唯一性成立. \square

沿用引理 1.21 的符号, 我们称 q 是被除式 f 关于除式 g 的商, r 是余式. 记为 $\text{quo}(f, g, x)$ 和 $\text{rem}(f, g, x)$. 有时也可以省略未定元 x .

例 1.22 设 $f = x^3 + 3x + 1$ 和 $g = 2x^2 + 1$ 是 $\mathbb{Q}[x]$ 中的多项式. 计算 $\text{rem}(f, g, x)$.

解. 直接计算得

$$h := f - \frac{1}{2}xg = \frac{5}{2}x + \frac{1}{2}.$$

因为 $\deg(h) < \deg(g)$, 所以

$$\text{rem}(f, g, x) = \frac{5}{2}x + \frac{1}{2} \quad \text{和} \quad \text{quo}(f, g, x) = \frac{1}{2}x.$$

例 1.23 设 $f = \bar{3}x^3 + \bar{2}x^2 + \bar{1}$ 和 $g = \bar{2}x^2 + \bar{4}$ 是 $\mathbb{Z}_5[x]$ 中的多项式. 计算 $\text{quo}(f, g, x)$ 和 $\text{rem}(f, g, x)$.

解. 注意到 $\bar{2}^{-1} = \bar{3}$. 于是

$$h_1 := f - \bar{3} \cdot \bar{3}xg = f - \bar{4}xg = \bar{2}x^2 - x + \bar{1} = \bar{2}x^2 + \bar{4}x + \bar{1}.$$

$$h_2 := h_1 - g = \bar{4}x - \bar{3} = \bar{4}x + \bar{2}.$$

于是,

$$f - \bar{4}xg - g = \bar{4}x + \bar{2} \implies f = (\bar{4}x + 1)g + (\bar{4}x + \bar{2}).$$

我们得到 $\text{quo}(f, g, x) = \bar{4}x + 1$ 和 $\text{rem}(f, g, x) = \bar{4}x + \bar{2}$.

定理 1.24 (余式定理) 设 $a \in R$ 和 $f(x) \in R[x]$. 则

$$f(a) = \text{rem}(f, x - a, x).$$

证明. 因为 $\text{lc}(x - a) = 1$ 是可逆的且 $\deg(x - a) = 1$, 所以存在 $q \in R[x]$ 和 $r \in R$ 使得

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

注意到把 x 替换为 a 是环同态. 于是,

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

故 $f(a) = r$. \square

定理 1.25 设 F 是域, $f, g \in F[x]$ 且 $g \neq 0$. 则存在唯一的多项式 $q, r \in F[x]$ 满足

$$f = qg + r \quad \text{和} \quad \deg(r) < \deg(g).$$

证明. 因为 $g \neq 0$, 所以 $\text{lc}(g) \neq 0$. 因为 F 是域, 所以 $\text{lc}(g)$ 可逆. 根据引理 1.21, 商和余式存在且唯一. \square

1.5 多项式的根

定义 1.26 设 F 和 K 是域, 且 F 是 K 的子域. 设 $f \in F[x]$ 且 $\alpha \in K$. 如果 $f(\alpha) = 0$, 则称 α 是 f 在 K 中的一个根 (root), 即 α 是方程 $f(x) = 0$ 在 K 中的一个解.

例 1.27 多项式 $x^2 - 2 \in \mathbb{Q}[x]$ 在 \mathbb{R} 中有根 $\pm\sqrt{2}$, 但它在 \mathbb{Q} 中无根.

命题 1.28 设 F 是域, 且 $f \in F[x]$ 且 $\deg(f) = n > 0$. 则

(i) $\alpha \in F$ 是 f 的根当且仅当 $\text{rem}(f, x - \alpha, x) = 0$;

(ii) f 在 F 中至多有 n 个互不相同的根.

证明. (i) 由余式定理可知,

$$f(\alpha) = 0 \iff \text{rem}(f, x - \alpha, x) = 0.$$

(ii) 对 n 归纳. 当 $n = 1$ 时, $f = f_1x + f_0$, $f_1, f_0 \in F$ 且 $f_1 \neq 0$. 于是, f 由唯一的根 $-f_0f_1^{-1}$. 结论成立. 设结论对 $F[x]$ 次数等于 $n - 1$ 次的多项式成立, 其中 $n > 0$. 如果 f 在 F 中没有根, 则结论显然成立. 假设 $\alpha \in F$ 是 f 的一个根. 根据 (i), $f(x) = g(x)(x - \alpha)$, 其中 $g \in F[x]$ 且 $\deg(g) = n - 1$. 由归纳假设 g 在 F 中至多有 $n - 1$ 个不同的根, 故 f 在 F 中至多有 n 个不同的根. \square

推论 1.29 设 F, K 是域且 F 是 K 的子域. 设 $f \in F[x]$ 且 $\deg(f) = n > 0$. 则

(i) $\alpha \in K$ 是 f 的根当且仅当 $\text{rem}(f, x - \alpha, x) = 0$;

(ii) f 在 K 中至多有 n 个互不相同的根.

证明. 因为 $F \subset K$, 所以 $F[x] \subset K[x]$. 故推论可由上述命题直接得到(把系数域 F 换为 K). \square