第五章　复数域和多项式

1　一元多项式

1.1　一元多项式环的构造

设 R 是交换环. 令

$$\widetilde{R} = \{(r_0, r_1, r_2, \ldots, r_n, \ldots) \,|\, r_n \in R, \text{有限多个非零}\}.$$

我们定义

$$\begin{array}{rccc} + : & \widetilde{R} \times \widetilde{R} & \longrightarrow & \widetilde{R} \\ & ((\ldots, r_n, \ldots),\ (\ldots, s_n, \ldots)) & \mapsto & (\ldots, r_n + s_n, \ldots) \end{array}.$$

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 $(\widetilde{R}, +, \tilde{0})$ 是交换群, 其中 $\tilde{0}$ 代表由 0 组成的无穷序列.

再定义

$$\begin{array}{rccc} \cdot : & \widetilde{R} \times \widetilde{R} & \longrightarrow & \widetilde{R} \\ & ((\ldots, r_n, \ldots),\ (\ldots, s_n, \ldots)) & \mapsto & (\ldots, \sum_{i+j=n} r_i s_j, \ldots) \\ & & & \qquad\qquad \uparrow_n \end{array}.$$

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

我们来验证 $(\widetilde{R},\cdot,\tilde{1})$ 是交换的含幺半群, 其中

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

交换性成立来自 R 是交换环和

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

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

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

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

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

则

$$q_n=\sum_{i+j=n}p_ic_j=\sum_{i+j=n}\left(\sum_{k+\ell=i}a_kb_\ell\right)c_j=\sum_{k+\ell+j=n}a_kb_\ell c_j.$$

类似地,

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

故 $q_n=v_n$. 由此可知结合律成立.

我们再来验证乘法单位

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

故 $(\widetilde{R},\cdot,\tilde{1})$ 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

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

故分配律成立. 我们证明了下述命题.

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

引理 1.2 *设 $(R,+,0,\cdot,1)$ 是交换环. 则*

$$\begin{array}{rccc} \phi: & R & \longrightarrow & \widetilde{R} \\ & r & \mapsto & (r,0,0,\ldots) \end{array}$$

是单的环同态.

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

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

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

和

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

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

于是, R 与 $\widetilde{R}$ 的子环 $\{(r,0,0,\ldots)\,|\,r\in R\}$ 同构. 我们可以把 $(r,0,0,\ldots)$ 简记为 r.

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

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

令

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

我们用数学归纳法来证明: 对任意 $n\in\mathbb{Z}^+$

$$x^n=(\underbrace{0,\ldots,0}_{n},1,0,0,\ldots). \tag{1}$$

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

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

归纳法完成.

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

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

故

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

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 $r_0, r_1, \ldots, r_n \in R$,

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

1.2 加法与乘法

定义 1.4 设 $p = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_0 \in R[x]$, 其中 p_n, p_{n-1}, $\ldots$, $p_0 \in R$. 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 $\mathrm{lc}(p)$. 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. □

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

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 $\mathrm{lc}(pq) = p_k q_\ell$. 当 $p = 0$ 或 $q = 0$ 时结论自然成立. □

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

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

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 $\mathrm{lc}(p)$ 和 $\mathrm{lc}(q)$ 都不等于 0. 因为 D 是整环, 所以 $\mathrm{lc}(p)\mathrm{lc}(q) \neq 0$. 根据命题 1.6, $\mathrm{lc}(pq) \neq 0$. 故 $pq \neq 0$. □

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, $\phi : R \longrightarrow S$ 是环同态, 且 $s \in S$. 则存在唯一的环同态 $\phi_s : R[x] \longrightarrow S$ 满足

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

证明. 定义:

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

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:

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

于是,

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

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 $r \in R$,

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

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. □

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 $\phi = \mathrm{id}_R$ 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 $\phi = \mathrm{id}_{\mathbb{Z}}$. 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 $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ 是商映射(环同态). 则

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

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, $\phi_{\bar{3}} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_5$ 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

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

推论 1.14 设 F 是域, $A \in \mathrm{M}_n(F)$. 则

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

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

证明. 根据第四章第三讲 § 3.5 节, $F[A]$ 是交换环. 注意到

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

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. □

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

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

推论 1.16 设 F 是域, $\phi \in \mathrm{Hom}(F^n, F^n)$. 则

$$\begin{array}{rccc} \rho_\phi : & F[x] & \longrightarrow & F[\phi] \\ & \sum_{i=0}^k p_i x^i & \mapsto & \sum_{i=0}^k p_i \phi^i \end{array}$$

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

证明. 根据第四章第三讲 § 3.5 节, $F[\phi]$ 是交换环. 注意到

$$\begin{array}{rccc} \rho : & F & \longrightarrow & F[\phi] \\ & \lambda & \mapsto & \lambda \mathrm{id}_{F^n} \end{array}$$

是环同态. 根据定理 1.10, ρ_ϕ 是由 $\rho_\phi|_F = \rho$ 和 $\rho_\phi(x) = \phi$ 确定的环同态. □

1.4 多项式的除法

引理 1.17 设 $f, g \in R[x]$ 且 $g \neq 0$. 再设 $\mathrm{lc}(g)$ 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

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

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

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

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 $\mathrm{lc}(g)$ 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. □

沿用引理 1.17 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 $\mathrm{quo}(f, g, x)$ 和 $\mathrm{rem}(f, g, x)$. 有时也可以省略未定元 x.

例 1.18 设 $f = x^3 + 3x + 1$ 和 $g = 2x^2 + 1$ 是 $\mathbb{Q}[x]$ 中的多项式. 计算 $\mathrm{rem}(f, g, x)$.

解. 直接计算得

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

因为 $\deg(h) < \deg(g)$, 所以

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

例 1.19 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 $\mathrm{quo}(f, g, x)$ 和 $\mathrm{rem}(f, g, x)$.

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

定理 1.20 *(余式定理)* 设 $a \in R$ 和 $f(x) \in R[x]$. 则

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

证明. 因为 $\mathrm{lc}(x - a) = 1$ 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 代换为 a 是环同态. 于是,

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

故 $f(a) = r$. □

定理 1.21 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 $\mathrm{lc}(g) \neq 0$. 因为 F 是域, 所以 $\mathrm{lc}(g)$ 可逆. 根据引理 1.17, 商和余式存在且唯一. □

1.5 多项式的根

定义 1.22 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 1.23 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 1.24 设 F 是域, 且 $f \in F[x]$ 且 $\deg(f) = n > 0$. 则 $\alpha \in F$ 是 f 的根当且仅当 $\mathrm{rem}(f, x-\alpha) = 0$;

证明. (i) 由余式定理可知,

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

2 整环中的最大公因子和最小公倍式

记号. 在本节中, 设 D 是整环. 则 $D^* = D \setminus \{0\}$ 和 U_D 是 D 中所有可逆元的集合. 由第四章第三讲命题 3.21, U_D 关于 D 中的乘法是交换群.

2.1 整除和相伴

定义 2.1 设 $a \in D^*$ 和 $b \in D$. 如果存在 $c \in D$ 使得

$$b = ca,$$

则称 a 是 b 的因子*(divisor)*, b 是 a 的倍式*(multiple)*. 此时, 我们称 a 在 D 中整除 b, 记为 $a|b$.

例 2.2 在 $\mathbb{Z}$ 中, $2|4$ 但 $2 \nmid 5$. 在 $\mathbb{Q}[x]$ 中, $(x+1)|(x^2-1)$ 但 $(x+1) \nmid (x^2+1)$. 在 $\mathbb{Z}_2[x]$ 中, $(x+\bar{1})|(x^2+\bar{1})$ *(Freshmen's dream)*.

命题 2.3 设 $a, b \in D^*$, $c, f, g \in D$. 则

(i) 如果 $a|b$ 和 $b|c$, 则 $a|c$;

(ii) 如果 $a|f$ 和 $a|g$, 则对任意 $u, v \in D$, $a|(uf+vg)$.

证明. (i) 设 $b = pa$ 和 $c = qb$, 其中 $p, q \in D^*$. 则 $c = (qp)a$. 于是, $a|c$. (ii) 与第一章第四讲引理 7.1 的证明类似. □

定义 2.4 设 $a, b \in D$. 如果存在 $u, v \in U_D$ 使得 $ua = vb$, 则称 a 和 b 在 D 上相伴, 记为 $a \approx b$.

下面验证 $\approx$ 是等价关系. 对任意 $a \in D$, $1a{=}1a \implies a{\approx}a$. 自反性成立. 设 $a \approx b$. 则存在 $u, v \in U$ 使得 $ua = vb$. 故 $vb = ua$. 于是, $b \approx a$. 对称性成立. 设 $a \approx b$ 和 $b \approx c$. 则存在 $s, t, u, v \in U$ 使得 $sa = tb$ 和 $ub = vc$. 于是

$$usa = utb = tvc.$$

因为 U_D 是群, 所以 $us, tv \in U_D$. 故 $a \approx c$. 传递性成立.

例 2.5 在 $\mathbb{Z}$ 中, $U_{\mathbb{Z}} = \{1, -1\}$. 故 $a \approx b \iff a = \pm b$. 设 F 是域. 则 $U_{F[x]} = F^*$. 故在 $F[x]$ 中,

$$f \approx g \iff \exists\ \alpha, \beta \in F^*,\ \alpha f = \beta g.$$

特别地, 当 $f \neq 0$ 时, $f \approx \mathrm{lc}(f)^{-1} f$. 这里, $\mathrm{lc}(f)^{-1} f$ 是首项系数等于 *1* 的多项式, 简称首一多项式*(monic polynomial)* 而 $\mathrm{lc}(f)^{-1} f$ 称为 f 的首一部分.

例 2.6 设 $f, g \in F[x]^*$. 证明*:* $f \approx g$ 当且仅当 f 和 g 的首一部分相同.

证明. 设 $f \approx g$. 则存在 $u, v \in F^*$ 使得 $uf = vg$. 则

$$\begin{aligned} f = u^{-1}vg &\implies \mathrm{lc}(f) = u^{-1}v\mathrm{lc}(g) \\ &\implies \mathrm{lc}(f)^{-1} f = (u^{-1}v)^{-1}\mathrm{lc}(g)^{-1}(u^{-1}v)g = \mathrm{lc}(g)^{-1} g. \end{aligned}$$

故 f 和 g 的首一部分相同.

反之, 我们有 $\mathrm{lc}(f)^{-1}f = \mathrm{lc}(g)^{-1}g$. 故 $f \approx g$. □

命题 2.7 设 $a, b \in D^*$. 则 $a \approx b$ 当且仅当 $a|b$ 和 $b|a$ 同时成立.

证明. 设 $a \approx b$. 则存在 $u, v \in U_D$ 使得 $ua = vb$. 则 $a = u^{-1}vb$. 故 $b|a$. 同理, $a|b$.

反之, 设 $b|a$ 和 $a|b$. 则存在 $c, d \in D^*$ 使得 $a = cb$ 和 $b = da$. 则 $a = cda$. 由整环中的消去律(第四章第三讲推论 3.23)可知, $cd = 1$. 故 $c, d \in U_D$, 即 $a \approx b$. □

2.2 最大公因子和最小公倍式

定义 2.8 设 $a, b_1, \ldots, b_n \in D^*$. 如果 a 是每个 $b_1, \ldots, b_n$ 的因子, 则称 a 是 $b_1, \ldots, b_n$ 的一个公因子. 再设 g 是 $b_1, \ldots, b_n$ 的一个公因子. 如果对于 $b_1, \ldots, b_n$ 的任意公因子 a, 我们有 $a|g$. 则称 g 是 $b_1, \ldots, b_n$ 的一个最大公因子.

设 $c, d_1, \ldots, d_n \in D^*$. 如果 c 是每个 $d_1, \ldots, d_n$ 的倍式, 则称 c 是 $d_1, \ldots, d_n$ 的一个公倍式. 再设 ℓ 是 $d_1, \ldots, d_n$ 的一个公倍式. 如果对于 $d_1, \ldots, d_n$ 的任意公倍式 c, 我们有 $\ell|c$. 则称 ℓ 是 $d_1, \ldots, d_n$ 的一个最小公倍式.

命题 2.9 设 $b_1, \ldots, b_n \in D^*$.

(i) 设 g 是 $b_1, \ldots, b_n$ 的最大公因子. 则 $h \in D^*$ 也是 $b_1, \ldots, b_n$ 的最大公因子当且仅当 $h \approx g$.

(ii) 设 ℓ 是 $b_1, \ldots, b_n$ 的最小公倍式, 则 $h \in D^*$ 也是 $b_1, \ldots, b_n$ 的最小公倍式当且仅当 $h \approx \ell$.

证明. (i) 设 h 也是 $b_1, \ldots, b_n$ 的最大公因子. 则 $g|h$ 且 $h|g$. 则命题 2.7 蕴含 $g \approx h$.

反之, 设 $h \approx g$. 则命题 2.7 蕴含 $h|g$ 和 $g|h$. 因为 $g|b_i$, 所以 $h|b_i$ (命题 2.3 (i)). 故 h 是 $b_1, \ldots, b_n$ 的公因子. 再设 d 是 $b_1, \ldots, b_n$ 的公因子. 则 $d|g$. 于是, $d|h$. 故 h 是 $b_1, \ldots, b_n$ 的最大公因子.

(ii) 设 h 也是 $b_1, \ldots, b_n$ 的最小公倍式. 则 $\ell|h$ 且 $h|\ell$. 则命题 2.7 蕴含 $h \approx \ell$. 反之, 设 $h \approx \ell$. 则命题 2.7 蕴含 $h|\ell$ 和 $\ell|h$. 因为 $b_i|\ell$, 所以 $b_i|h$ (命题 2.3 (i)). 故 h 是 $b_1, \ldots, b_n$ 的公倍式. 再设 q 是 $b_1, \ldots, b_n$ 的公倍式. 则 $\ell|q$. 于是, $h|q$. 故 h 是 $b_1, \ldots, b_n$ 的最小公倍式. □

如果 $b_1, \ldots, b_n \in D^*$ 的最大公因子存在, 则它们的最大公因子记为 $\gcd(b_1, \ldots, b_n)$. 该记号在相伴的意义下是唯一的. 类似地, 如果 $b_1, \ldots, b_n \in D^*$ 的最小公倍式存在, 则它们的最小公倍式记为 $\mathrm{lcm}(b_1, \ldots, b_n)$. 该记号在相伴的意义下也是唯一的.

由第一章第四讲可知 $\mathbb{Z}$ 中的有限个非零元的最大公因子和最小公倍式都存在. 它们的最大公因子和最小公倍

式通常是指正的整数.

下面的推论说明多个元素的最大公因子和最小公倍式的计算可以化成两个元素的情形.

推论 2.10 设 D 中任意有限多个非零元都有最大公因子(最小公倍式). 设 $b_1, \ldots, b_n \in D^*$, 其中 $n > 2$. 则

$$\gcd(b_1, \ldots, b_n) = \gcd(b_1, \gcd(b_2, \ldots, b_n))$$

$$(\operatorname{lcm}(b_1, \ldots, b_n) = \operatorname{lcm}(b_1, \operatorname{lcm}(b_2, \ldots, b_n))).$$

证明. 设 $g = \gcd(b_1, \ldots, b_n)$ 和 $h = \gcd(b_1, \gcd(b_2, \ldots, b_n))$. 则 g 是 $b_2, \ldots, b_n$ 的公因子. 故 $g | \gcd(b_2, \ldots, b_n)$. 于是, g 是 g_1 和 $\gcd(b_2, \ldots, b_n)$ 的公因子. 由此得出 $g|h$. 类似地, $h|b_i$, $i = 1, 2, \ldots, n$. 故 $h|g$. 根据命题 2.7, $g \approx h$. 于是, $h = \gcd(b_1, \ldots, b_n)$ (命题 2.9).

关于最小公倍式的结论类似可证. □

2.3 一元多项式的最大公因子和最小公倍式

本节中 F 代表域.

命题 2.11 设 $f_1, \ldots, f_n \in F[x]$ 不全为零. 则 $f_1, \ldots, f_n$ 的最大公因子存在. 设 g 是 $f_1, \ldots, f_n$ 最大公因子. 则存在 $a_1, \ldots, a_n \in F[x]$ 使得

$$a_1 f_1 + \cdots + a_n f_n = g. \tag{3}$$

证明. 设 $I = \{u_1 f_1 + \cdots u_n f_n \,|\, u_1, \ldots, u_n \in F[x]\}$. 令 g 是 I 中次数最小的非零多项式. 则存在 $a_1, \ldots, a_n \in F[x]$ 使得 (3) 成立. 我们只要证明 g 是 $f_1, \ldots, f_n$ 的最大公因子.

对任意 $i \in \{1, 2, \ldots, n\}$, 设 $r_i = \mathrm{rem}(f_i, g, x)$. 则

$$f_i = q_i g + r_i,$$

其中 $q_i \in F[x]$. 由 (3) 可知,

$$r_i = f_i - q_i a_1 f_1 - \cdots - q_i a_n f_n \in I.$$

于是, $r_i \in I$. 因为 $\deg(r_i) < \deg(g)$, 所以 $r_i = 0$. 故 $g | f_i$, $i = 1, 2, \ldots, n$. 我们证明了 g 是 $f_1, \ldots, f_n$ 的公因子.

再设 a 是 $f_1, \ldots, f_n$ 的公因子. 由命题 2.3 和 (3) 可知, $a | g$. 于是, g 是 $f_1, \ldots, f_n$ 的最大公因子. □