第四章　群、环和域简介

4.2　分式域

设 D 是整环, $D^* = D \setminus \{0\}$. 在集合 $D \times D^*$ 上定义二元关系如下. 设 $(a,b),(c,d) \in D \times D^*$. 如果 $ad = bc$, 则 $(a,b) \sim (c,d)$.

我们来验证 $\sim$ 是等价关系. 对任意 $(a,b) \in D \times D^*$, $ab = ba \implies (a,b) \sim (a,b)$. 自反性成立. 设 $(a,b) \sim (c,d)$. 则 $ad = bc \Longrightarrow cb = da \Longrightarrow (c,d) \sim (a,b)$. 对称性成立. 设 $(a,b) \sim (c,d)$ 和 $(c,d) \sim (e,f)$. 则

$$ad = cb, cf = ed \implies adcf = cbed \implies cd(af - eb) = 0.$$

如果 $c \neq 0$, 则 $af = eb$ (D 是整环). 如果 $c = 0$, 则 $ad = 0$ 和 $ef = 0$. 故 $a = e = 0$. 于是 $af = 0 = be$. 综上所述 $(a,b) \sim (e,f)$. 传递律成立.

记商集 $(D \times D^*) / \sim$ 为 $\mathrm{Fr}(D)$, 并把 (a,b) 关于 $\sim$ 的等价类记为 a/b. 则 $a/b = c/d$ 当且仅当 $ad = cb$. 注意到等价关系 $\sim$ 的定义和等价类的记号直接蕴含约分法则: 对于任意 $x \in D, y, z \in D^*$

$$\frac{x}{y} = \frac{zx}{zy}.$$

下面我们在 $\mathrm{Fr}(D)$ 上定义加法如下:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}.$$

现在验证加法是良定义的. 设 $a/b{=}a'/b'$ 和 $c/d{=}c'/d'$. 则

$$ab'=a'b,\quad cd'=c'd. \tag{1}$$

由加法的定义可知

$$\frac{a'}{b'}+\frac{c'}{d'}=\frac{a'd'+b'c'}{b'd'}.$$

验证加法的良定义意味着证明:

$$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'},$$

即

$$b'd'(ad+bc)=bd(a'd'+b'c'). \tag{2}$$

我们从上式的左侧出发

$$\begin{aligned} b'd'(ad+bc) &= ab'dd'+bb'cd' \\ &= a'bdd'+b'bc'd \quad (\text{根据 (1)}) \\ &= bd(a'd'+b'c'). \end{aligned}$$

由此可知, (2) 成立. 故加法是良定义的.

下面验证 $(\mathrm{Fr}(D),+,0/1)$ 是交换群. 由加法的定义可知, $+$ 是交换的. 根据定义直接计算得

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{adf+bcf+ebd}{bdf}$$

和

$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{cf+de}{df}=\frac{adf+bcf+bde}{bdf}.$$

于是, 结合律成立.

直接计算得对任意 $a/b\in \mathrm{Fr}(D)$,

$$\frac{a}{b}+\frac{0}{1}=\frac{a}{b}.$$

进而

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ba}{b^2}=\frac{0}{b^2}=\frac{0}{1}.$$

于是, $(\mathrm{Fr}(D),+,0/1)$ 是交换群.

定义 $\mathrm{Fr}(D)$ 的乘法如下: 对任意 $a/b,c/d\in \mathrm{Fr}(D)$,

$$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}.$$

利用引入乘法的符号验证良定义如下: 因为

$$\frac{a'}{b'}\frac{c'}{d'}=\frac{a'c'}{b'd'}.$$

所以

$$\frac{a}{b}\frac{c}{d}=\frac{a'}{b'}\frac{c'}{d'}\iff\frac{ac}{bd}=\frac{a'c'}{b'd'}\iff acb'd'=a'c'bd.$$

根据 (1), 最后一个等式显然成立.

在验证 $(\mathrm{Fr}(D),\cdot,1/1)$ 是含幺半群. 利用上面的符号, 直接计算得

$$\left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f}=\frac{ace}{bdf}=\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right).$$

故结合律成立. 进而,

$$\frac{a}{b}\frac{1}{1} = \frac{a}{b} = \frac{1}{1}\frac{a}{b}.$$

事实上, D 中乘法的交换性蕴含 $(\mathrm{Fr}(D), \cdot, 1/1)$ 是交换的含幺半群. 我们再来看分配律:

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\frac{cf + de}{df} = \frac{acf + ade}{bdf}$$

和

$$\frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{acbf + aebd}{bdbf}.$$

因为

$$\frac{acf + ade}{bdf} = \frac{acbf + aebd}{bdbf},$$

所以分配律成立. 故 $(\mathrm{Fr}(D), +, 0/1, \cdot, 1/1)$ 是交换环.

注意到

$$\frac{a}{b} \neq \frac{0}{1} \iff a \neq 0.$$

当 $a \neq 0$ 时,

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}.$$

于是, a/b 可逆. 我们得到 $(\mathrm{Fr}(D), +, 0/1, \cdot, 1/1)$ 是域. 称之为 D 的分式域.

命题 4.5 设 D 是整环. 则

$$\begin{array}{rccc} \phi: & D & \longrightarrow & \mathrm{Fr}(D) \\ & x & \mapsto & \frac{x}{1} \end{array}$$

是环的单同态.

证明. 由 $\mathrm{Fr}(D)$ 中的运算可知, 对任意 $x, y \in D$,

$$\phi(x+y) = \phi(x) + \phi(y) \quad \text{和} \quad \phi(xy) = \phi(x)\phi(y).$$

由 ϕ 的定义可知, $\phi(1) = 1/1$. 于是, ϕ 是环同态. 设 $\phi(x) = 0/1$. 则 $x/1 = 0/1$. 于是, $x = 0$. 由第四章第二讲引理 2.46, ϕ 是单射. □

上述命题指出

$$D \cong \mathrm{im}(\phi) = \left\{ \frac{x}{1} | x \in D \right\}.$$

故我们可以把 D 和 $\mathrm{im}(\phi)$ 看成一样的. 特别地, 把 $x/1$ 简记为 x. 于是, D 可以看成 $\mathrm{Fr}(D)$ 的子集.

4.3 域的特征

定义 4.6 设 $(F, +, 0, \cdot, 1)$ 是域. 如果加法群 $(F, +, 0)$ 中 1 的阶有限, 则 $\mathrm{ord}(1)$ 称为 F 的特征. 否则, F 的特征定义为零. 域 F 的特征记为 $\mathrm{char}(F)$.

命题 4.7 设 F 是域. 则 F 的特征或是零或是素数.

证明. 设 $m = \mathrm{char}(F) > 0$ 且 $m = k\ell$, 其中 $k, \ell \in \mathbb{Z}^+ \setminus \{1\}$. 则由广义分配律可知, $0 = m1 = (k\ell)1 = (k1)(\ell 1)$. 因为 F 是整环, 所以 $k1 = 0$ 或 $\ell 1 = 0$. 故 $\mathrm{char}(F) < m$, 矛盾. □

命题 4.8 设 F 是特征为 $p > 0$ 的域. 则对任意 $x \in F$ 和整数 m, $(mp)x = 0$.

证明. 由定义可知

$$(mp)x = \underbrace{mx + \cdots + mx}_{p} = \underbrace{(1 + \cdots + 1)}_{p}(mx) = 0(mx) = 0. \quad \square$$

例 4.9 $\mathbb{Q}$ 和 $\mathbb{R}$ 的特征等于零. 对于素数 p, $\mathrm{char}(\mathbb{Z}_p) = p$.

命题 4.10 *(Freshmen's dream)* 设域 F 的特征是素数 p. 则对任意 $x, y \in F$, $(x+y)^p = x^p + y^p$.

证明. 根据交换环上的二项式定理

$$(x+y)^p = x^p + \left(\sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k \right) + y^p.$$

根据第一章例 7.17, $p | \binom{p}{k}$. 根据引理 4.8, $\binom{p}{k} x^{p-k} y^k = 0$, $k = 1, 2, \ldots, p-1$. 故 $(x+y)^p = x^p + y^p$. $\square$

命题 4.11 *(Fermat 小定理)* 设 p 是素数, $m \in \mathbb{Z} \setminus \{0\}$ 且 $p \nmid m$. 则 $m^{p-1} \equiv 1 \mod p$.

证明. 由上述命题可知, $\mathbb{Z}_p$ 中所有可逆元构成的群 $U_{\mathbb{Z}_p}$ 共有 $p-1$ 个元素且 $\bar{m} \in U_{\mathbb{Z}_p}$. 根据本章定理 2.44, $\bar{m}^{p-1} = \bar{1}$. 故 $m^{p-1} \equiv 1 \mod p$. $\square$

例 4.12 设 p 是素数, $\bar{k} \in \mathbb{Z}_p$. 证明: $\bar{k}^p = \bar{k}$.
证明. 如果 $\bar{k} \neq \bar{0}$. 则 $p \nmid k$. 故 $\bar{k}^{p-1} = \bar{1}$ *(Fermat 小定理)*. 于是, $\bar{k}^p = \bar{k}$. 如果 $\bar{k} = \bar{0}$, 则等式显然成立. $\square$

4.4 域上的线性代数

第一、二和三章中关于线性代数的结论(除了用到 $2 \neq 0$ 的)对任何域 F 和坐标空间 F^n 都成立. 两个需要重新考察的地方如下. 设 F 是特征等于 2 的域, $A \in \mathrm{M}_n(F)$.

(i) 如果 A 是斜对称的, 则 A 在对角线上的元素是否等于零? 当 n 是奇数时, $\det(A)$ 是否等于零?

(ii) 设 A 中有两行(列)相同. 它的行列式是否等于零?

设 $A = (a_{i,j})_{n\times n}$.

(i) 如果 A 是斜对称的, 则 $A^t = -A$. 即 $a_{i,j} = -a_{i,j}$. 因为 $\mathrm{char}(F) = 2$, 所以 $1 = -1$. 于是, $a_{i,j} = a_{j,i}$. 故 A 斜对称和对称是等价的. 例如

$$B = \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

既是对称的又是斜对称的. 但 $\det(B) = \bar{1} \neq \bar{0}$. 另一方面, 对于特征不等于 2 的域上奇数阶斜对称矩阵的行列式等于零.

(ii) 见第十一周讲义例 2.9.

于是, 除了奇数阶斜对称矩阵行列式等于零以外, 关于线性方程组、矩阵、线性空间、向量、线性映射和行列式的所有结果适用于所有的域上的任何方阵.

例 4.13 设

$$A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ \bar{1} & \bar{4} & \bar{2} \end{pmatrix} \in \mathrm{M}_3(\mathbb{Z}_5).$$

计算以 A 为系数矩阵的齐次线性方程组的解空间 V_A 的一组基.

解. 利用 *Gauss* 消去法计算

$$A \longrightarrow \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ \bar{0} & \bar{2} & \bar{4} \end{pmatrix} \longrightarrow \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix}.$$

于是, $\mathrm{rank}(A) = 2 \Longrightarrow \dim(V_A) = 1$. 由方程 $\bar{2}x_2 + \bar{4}x_3 = \bar{0}$, 得到 $x_2 = -\bar{3}\,\bar{4}x_3 = -\overline{12}x_3 = \bar{3}x_3$. 进而

$$x_1 = -\bar{6}x_3 - \bar{3}x_3 = -\bar{9}x_3 = x_3.$$

于是 V_A 的一组基是 $(\bar{1}, \bar{3}, \bar{1})^t$. 故

$$V_A = \left\{ \lambda \begin{pmatrix} \bar{1} \\ \bar{3} \\ \bar{1} \end{pmatrix} \mid \lambda \in \mathbb{Z}_5 \right\}.$$

例 4.14 三维坐标空间 $\mathbb{Z}_2^3$ 关于加法是一个交换群. 它的标准基记为 $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$. 如果群 $(\mathbb{Z}_2^3, +, \mathbf{0})$ 可以由两个元素 $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^3$ 生成. 则 $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ 在 $\mathbf{u}, \mathbf{v}$ 生成的子空间中. 于是, $\dim(\mathbb{Z}_2^3) \leq 2$. 矛盾.

根据第四章第二讲推论 *2.48*, $(\mathbb{Z}_2^3, +, \mathbf{0})$ 同构于 S_8 的子群. 但 $S_8 = \langle (12), (12345678) \rangle$.

例 4.15 设 $A \in \mathrm{M}_n(\mathbb{R})$. 证明 $\mathrm{rank}(A) = \mathrm{rank}(A^tA)$.

证明. 设 $B = A^tA$, 以 A 和 B 为系数矩阵的齐次线性方程组的解空间分别记为 V_A 和 V_B. 设 $\mathbf{v} \in V_A$. 则

$$B\mathbf{v} = A^tA\mathbf{v} = A^t(A\mathbf{v}) = A^t\mathbf{0} = \mathbf{0}.$$

于是, $V_A \subset V_B$. 反之, 设 $\mathbf{w} \in V_B$ 和 $\mathbf{y} = A\mathbf{w}$. 令

$$\mathbf{y} = (y_1, \ldots, y_n)^t.$$

则

$$\mathbf{w}^tA^tA\mathbf{w} = (A\mathbf{w})^t(A\mathbf{w}) = \mathbf{y}^t\mathbf{y} = (y_1, \ldots, y_n)\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = y_1^2 + \cdots + y_n^2.$$

另一方面, $\mathbf{w}^tA^tA\mathbf{w} = \mathbf{w}^tB\mathbf{w} = \mathbf{w}^t\mathbf{0} = 0$. 于是,

$$y_1^2 + \cdots + y_n^2 = \mathbf{0}.$$

因为 $y_1, \ldots, y_n \in \mathbb{R}$, 所以 $y_1 = \cdots = y_n = 0$. 由此得出 $A\mathbf{w} = \mathbf{0}$. 我们得到 $\mathbf{w} \in V_B$. 故 $V_A = V_B$. 特别有 $\dim(V_A) = \dim(V_B)$. 根据对偶定理, $\mathrm{rank}(A) = \mathrm{rank}(B)$. □

注意到上例中的结论并不是对任意域都成立的. 例如在 $\mathbb{Z}_5$ 上, 令

$$A = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{2} \end{pmatrix}.$$

则

$$A^t A = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{1} & \bar{2} \end{pmatrix} \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{2} \end{pmatrix} = O.$$

第五章　多项式和复数域

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. □

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 $n\in\mathbb{Z}^+$

$$x^n=(\underbrace{0,\ldots,0}_{n},1,0,0,\ldots). \tag{3}$$

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 (3) 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 加法与乘法的性质

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 $pq \neq 0$. □

1.3 赋值定理

本节说明如何把多项式看成“函数”.

定理 1.9 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,

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

最后, $\phi_s(1_R) = \phi_s(1_Rx^0) = \phi(1_R)s^0 = 1_Ss^0 = 1_S$. 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

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

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 1.10 设 $f = x^2 - 4 \in \mathbb{Q}[x]$. 计算 $f(15)$.
解. 设 $\phi = \mathrm{id}_{\mathbb{Z}}$. 则 $f(15) = 15^2 - 4 = 221$. 或

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

设 $\phi = \pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ 是商映射(环同态). 令 $\bar{k} \in \mathbb{Z}_n$. 由定理 1.9 可知, 我们有赋值同态 $\phi_{\bar{k}} : \mathbb{Z}[x] \to \mathbb{Z}_n$.

例 1.11 设 $g = (179x - 286)(413x - 587)$. 计算 $g(\bar{3})$, 其中 $\bar{3} \in \mathbb{Z}_5$. 由定理 *1.9* 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 1.12 设 F 是域, $A \in \mathrm{M}_n(F)$ 且 $A \neq O$. 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 1.9, ρ_A 是由 $\rho_A|_F = \rho$ 和 $\rho_A(x) = A$ 确定的环同态. □

例 1.13 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

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