第四章　群、环和域简介

命题 3.14 设 $\phi : R \longrightarrow S$ 是环同态. 则 $\mathrm{im}(\phi)$ 是子环.

证明. 因为 ϕ 是关于加法的群同态, 所以 $(\mathrm{im}(\phi), +, 0_S)$ 是 $(S, +, 0_S)$ 的子群(第四章第一讲命题 2.28). 设 $u, v \in \mathrm{im}(\phi)$. 则存在 $x, y \in R$ 使得 $u = \phi(x)$ 和 $v = \phi(y)$. 则

$$uv = \phi(x)\phi(y) = \phi(xy) \implies uv \in \mathrm{im}(\phi).$$

于是, S 中的乘法关于 $\mathrm{im}(\phi)$ 封闭. 因为 $\phi(1_R) = 1_S$, 所以 $1_S \in \mathrm{im}(\phi)$. 故 $(\mathrm{im}(\phi), \cdot, 1_S)$ 是含幺半群. 而 $\mathrm{im}(\phi)$ 中的分配律可由 S 中的分配律直接得出. □

3.3　零因子和可逆元

定义 3.15 设 a, b 是环 R 中的非零元素. 如果 $ab = 0$, 则称 a 是 R 的左零因子*(left zero-divisor)*, b 是 R 的右零因子*(right zero-divisor)*. 如果 $x \in R$ 满足 $x \neq 0$ 且 x 既非左零因子又非右零因子, 则称 x 是非零因子 *(non-zero-divisor)*. 当 R 交换时, 左右零因子统称为零因子.

例 3.16 整数环中没有零因子.

命题 3.17 在 $\mathbb{Z}_n$ 中, $\bar{a}$ 是零因子当且仅当 $1 < \gcd(n, a) < n$.

证明. 设 $g = \gcd(n, a)$. 则存在 $m \in \mathbb{Z}^+$ 使得 $n = mg$. 再设 $\ell = \mathrm{lcm}(n, a)$. 根据第一章第四讲定理 7.10,

$$\ell = ma \implies \bar{m}\bar{a} = \bar{\ell} = \bar{0}.$$

如果 $1 < g < n$, 则 $\bar{a} \neq \bar{0}$ 且 $\bar{m} \neq \bar{0}$ (因为 $0 < m < n$). 故 $\bar{a}$ 是零因子. 反之, $\bar{a} \neq \bar{0}$. 故 $g < n$. 又存在 $b \in \{1, 2, \ldots, n-1\}$ 使得 $\bar{b}\bar{a} = \bar{0}$. 即 ba 是 n 和 a 的公倍式. 于是, 存在 $c \in \mathbb{Z}^+$ 使得 $ba = c\ell$ (见第一章第四讲定理 7.10 的证明). 于是,

$$ba = c\ell = cma \implies b = cm \implies m < n \implies g > 1. \quad \square$$

例 3.18 剩余环 $\mathbb{Z}_6$ 中的所有零因子是 $\{\bar{2}, \bar{3}, \bar{4}\}$.

例 3.19 设 $A \in \mathrm{M}_n(\mathbb{R})$ 是非零矩阵. 证明 A 是左或右零因子当且仅当 $\mathrm{rank}(A) < n$.

证明. 设 A 是左零因子. 则存在非零 $B \in \mathrm{M}_n(\mathbb{R})$ 使得 $AB = O$. 根据 *Sylvester* 不等式,

$$0 = \mathrm{rank}(AB) \geq \mathrm{rank}(A) + \mathrm{rank}(B) - n \implies \mathrm{rank}(A) \leq n - \mathrm{rank}(B).$$

因为 $\mathrm{rank}(B) > 0$, 所以 $\mathrm{rank}(A) < n$.

反之, 设 $\mathrm{rank}(A) < n$. 则存在 $\mathbf{v} \in \mathbb{R}^n \setminus \{\mathbf{0}_n\}$ 使得 $A\mathbf{v} = \mathbf{0}_n$ *(第二章第三讲推论 4.2)*. 设

$$B = (\mathbf{v}, \underbrace{\mathbf{0}_n, \ldots, \mathbf{0}_n}_{n-1}).$$

则

$$AB = (A\mathbf{v}, A\mathbf{0}_n, \ldots, A\mathbf{0}_n) = O.$$

故 A 是左零因子.

事实上, $\mathrm{rank}(A^t)$ 也小于 n. 故 A^t 也是左零因子. 于是, 存在非零矩阵 $C \in \mathrm{M}_n(\mathbb{R})$ 使得 $A^tC = O$. 于是, $C^tA = O$. 我们得到 A 是左零因子当且仅当它是右零因子. 这是矩阵环的一个特殊性质.

定义 3.20 设 R 是环. 则含幺半群 $(R, \cdot, 1)$ 中的可逆元称为环 R 中的可逆元.

例 3.21 整数环中的可逆元是 ± 1.

由第四章第一讲命题 1.9 可知, 在 $\mathbb{Z}_n$ 中, $\bar{a}$ 可逆当且仅当 $\gcd(n, a) = 1$. 再根据命题 3.17, $\mathbb{Z}_n$ 中所有非零因子都可逆. 由上例可知, 这一结论对 $\mathrm{M}_n(\mathbb{R})$ 也成立, 但对整数环不成立.

例 3.22 计算 $\bar{8}, \overline{11}$ 在 $\mathbb{Z}_{15}$ 中的逆.

解. 利用扩展的 *Euclid* 算法, 我们得到

$$2 \times 8 - 15 = 1 \quad \text{和} \quad 11 \times 11 - 8 \times 15 = 1.$$

故 $\bar{8}^{-1} = \bar{2}$ 且 $\overline{11}^{-1} = \overline{11}$.

例 3.23 设 $A \in \mathrm{M}_n(\mathbb{R})$. 确定 $\mathbb{R}[A]$ 中的可逆元.

解. 设 $B \in \mathbb{R}[A]$. 如果 B 是 $\mathbb{R}[A]$ 中的可逆元, 则它是 $\mathrm{M}_n(\mathbb{R})$ 中的可逆元. 故 $\mathrm{rank}(B) = n$. 下面我们来考察 B^{-1} 是否在 $\mathbb{R}[A]$ 中. 根据第二章第六讲命题 *9.4*, $B^{-1} \in \mathbb{R}[B] \subset \mathbb{R}[A]$. 故 $B^{-1} \in \mathbb{R}[A]$. 由此可知, B 可逆当且仅当 $\mathrm{rank}(B) = n$. 即 $\mathbb{R}[A]$ 中的可逆元就是 $\mathbb{R}[A]$ 中的可逆矩阵. □

命题 3.24 设 U_R 是环 R 中所有可逆元的集合. 则 $(U, \cdot, 1)$ 是群.

证明. 设 $x, y \in U$. 则 $xy \in U$ (第四章第一讲命题 2.6). 故环中的乘法是 U 上的二元运算. 乘法显然满足结合律, 且 $1 \in U$. 由可逆元的定义可知, $x \in U \implies x^{-1} \in U$. 故 U 是群. □

例 3.25 *(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. 在环 $\mathbb{Z}_p$ 中, 任何非零元素都是可逆的 *(*第四章第一讲命题 *1.9)*. 于是, $\mathbb{Z}_p$ 中所有可逆元构成的群 $U_{\mathbb{Z}_p}$ 共有 $p-1$ 个元素且 $\bar{m} \in U_{\mathbb{Z}_p}$. 根据第四章第一讲定理 *2.40*, $\bar{m}^{p-1} = \bar{1}$. 故 $m^{p-1} \equiv 1 \mod p$.

3.4 消去律

命题 3.26 设 R 是环, $a, b \in R$ 都非零, $x, y \in R$. 则

(i) *(左消去律)* 如果 a 不是左零因子且 $ax = ay$, 则 $x = y$;

(ii) *(右消去律)* 如果 b 不是右零因子且 $xb = yb$, 则 $x = y$.

证明. (i) 根据分配律

$$ax = ay \implies a(x - y) = 0.$$

因为 a 不是左零因子, 所以 $x - y = 0$. 于是, $x = y$.

(ii) 类似. □

定义 3.27 设 D 是交换环. 如果 D 中没有零因子, 则称 D 是整环*(domain)*.

推论 3.28 设 D 是整环. 则在 D 中消去律成立.

3.5 环的特征

定义 3.29 设 $(R, +, 0, \cdot, 1)$ 是环. 如果加法群 $(R, +, 0)$ 中 1 的阶有限, 则 $\mathrm{ord}(1)$ 称为 R 的特征. 否则, R 的特征定义为零. 环 R 的特征记为 $\mathrm{char}(R)$.

例 3.30 整数环的特征等于零, 而 $\mathrm{char}(\mathbb{Z}_n) = n$.

引理 3.31 设环 R 的特征等于 $n > 0$, $m \in \mathbb{Z}$ 满足 $n|m$. 则对于任意 $r \in R$, $mr = 0$.

证明. 设 $m = kn$. 根据广义分配律, 我们有:

$$mr = (kn)r = kn(r \cdot 1) = (kr) \cdot (n1) = (kr) \cdot 0 = 0. \quad \square$$

命题 3.32 *(Freshmen's dream)* 设交换环 R 的特征是素数 p. 则对任意 $x, y \in R$,

$$(x + y)^p = x^p + y^p.$$

证明. 根据交换环上的二项式定理

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

根据第二章第一讲例 7.17(第一章最后一节), $p|\binom{p}{k}$. 由引理 3.31 可知,

$$\binom{p}{k} x^{p-k} y^k = 0, \quad k = 1, 2, \ldots, p-1.$$

故 $(x + y)^p = x^p + y^p$. $\square$

例 3.33 设 p 是素数. 对任意 $x, y \in \mathbb{Z}_p$, $(x+y)^p = x^p + y^p$. 这是因为 $\mathrm{char}(\mathbb{Z}_p) = p$.

命题 3.34 设 $(R,+,0_R,\cdot,1_R)$ 和 $(S,+,0_S,\cdot,1_S)$ 是两个环, $\phi: R \longrightarrow S$ 是环同态. 则

(i) $\mathrm{char}(R)=0$ 或 $\mathrm{char}(R) \geq \mathrm{char}(S) > 0$;

(ii) 当 ϕ 是单同态时, $\mathrm{char}(R)=\mathrm{char}(S)$.

证明. 设 $\mathrm{char}(R)=k$ 和 $\mathrm{char}(S)=m$.

(i) 设 $k>0$. 则 $k1_R=0_R$. 再设 $m=0$ 或 $m>k$. 则

$$\begin{aligned} 0_S &= \phi(k1_R) \quad (\because\ k1_R=0_R) \\ &= \phi(\underbrace{1_R+\cdots+1_R}_{k}) = \underbrace{\phi(1_R)+\cdots+\phi(1_R)}_{k} = \underbrace{1_S+\cdots+1_S}_{k} \\ &= k1_S \neq 0_S \quad (\because\ 0<k<m). \end{aligned}$$

矛盾. 故当 $k>0$ 时, $m\neq 0$ 且 $k \geq m$.

(ii) 先设 $m=0$. 由 (i) 可知, $k=0$.

再设 $m>0$. 直接计算得

$$\begin{aligned} \phi(m1_R) &= \phi(\underbrace{1_R+\cdots+1_R}_{m}) \\ &= \underbrace{\phi(1_R)+\cdots+\phi(1_R)}_{m} \\ &= \underbrace{1_S+\cdots+1_S}_{m} = m1_S = 0_S. \end{aligned}$$

如果 $k>m$. 则 $m1_R \neq 0$. 故 ϕ 不是单射. 矛盾. 由此和 (i) 可知, $k=m$. □

命题 3.35 设 D 是整环. 则 D 的特征或是零或是素数.

证明. 设 $m = \mathrm{char}(D)$ 且 $m = k\ell$, 其中 $k, \ell \in \mathbb{Z}^+ \setminus \{1\}$. 则

$$0 = m1 = (k\ell)1 = (k1)(\ell 1) \quad (\because \text{广义分配律}).$$

因为 D 是整环, 所以 $k1{=}0$ 或 $\ell 1{=}0$. 故 $\mathrm{char}(D){<}m$, 矛盾. □

4 域

4.1 域的定义和分式域

定义 4.1 设 F 是交换环. 如果 F 中任何非零元都可逆, 则称 F 是域*(field)*.

类似地, 我们可以定义子域的概念.

例 4.2 有理数环 $\mathbb{Q}$ 和实数环 $\mathbb{R}$ 是域, 它们的特征等于零, 且 $\mathbb{Q}$ 是 $\mathbb{R}$ 的子域.

设 p 是素数. 则 $\mathbb{Z}_p$ 是域. 验证如下: 设 $\bar{a} \in \mathbb{Z}_p \setminus \{\bar{0}\}$. 则 $p \nmid a$. 因为 p 是素数, 所以 $\gcd(p, a) = 1$. 根据第四章第一讲命题 *1.9*, $\bar{a}$ 在 $\mathbb{Z}_p$ 中可逆. 验证完毕.

注意到 $\mathbb{Z}_p$ 的特征是 p.

注解 4.3 设 F 是域. 则 F 是整环. 验证如下:

设 $a, b \in F \setminus \{0\}$. 如果 $ab = 0$, 则 $a^{-1}(ab) = 0$. 于是, $b = 0$. 矛盾. 验证完毕.

根据命题 *3.35*, F 的特征或者是零或者是素数.

命题 4.4 设 F 和 K 是域, $\phi : (F, +, 0_F, \cdot, 1_F) \longrightarrow (K, +, 0_K, \cdot, 1_K)$ 是环同态. 则 ϕ 是嵌入.

证明. 注意到 ϕ 是从 $(F, +, 0_F)$ 到 $(K, +, 0_K)$ 的群同态. 由第四章第二讲引理 2.46, 我们只要证明

$$\phi(x) = 0_K \implies x = 0_F.$$

假设 $x \in F \setminus \{0_F\}$ 使得 $\phi(x) = 0_K$. 则

$$\phi(x^{-1}x) = \phi(x^{-1})\phi(x) = 0_K.$$

另一方面,

$$\phi(x^{-1}x) = \phi(1_F) = 1_K.$$

我们有 $0_K = 1_K$, 矛盾. □

例 4.5 设 $(F, +, 0_F, \cdot, 1_F)$ 是域.

(i) 如果 $\mathrm{char}(F) = 0$, 则

$$\begin{array}{rccc} \phi_0 : & \mathbb{Q} & \longrightarrow & F \\ & \frac{m}{n} & \mapsto & (m1_F)(n1_F)^{-1}, \end{array}$$

其中 $m, n \in \mathbb{Z}$ 且 $n \neq 0$, 是同态.

(ii) 如果 $\mathrm{char}(F) = p > 0$, 则

$$\begin{array}{rccc} \phi_p : & \mathbb{Z}_p & \longrightarrow & F \\ & \bar{a} & \mapsto & a1_F, \end{array}$$

其中 $a \in \mathbb{Z}$, 是同态.

证明. *(i)* 断言: 设 $n, \ell \in \mathbb{Z}^+$. 则 $((n\ell)1_F))^{-1} = (n1_F)^{-1}(\ell 1_F)^{-1}$. 断言的证明. 根据上一讲推论 *3.7*, $(n\ell)1_F$=$(n1_F)(\ell 1_F)$. 故

$$((n\ell)1_F)^{-1} = ((n1_F)(\ell 1_F))^{-1} = (n1_F)^{-1}(\ell 1_F)^{-1}.$$

断言成立.

验证 ϕ_0 是良定义的. 设 $m/n = a/b$, 其中 $a, b \in \mathbb{Z}$ 且 $b \neq 0$. 我们需要验证

$$(m1_F)(n1_F)^{-1} = (a1_F)(b1_F)^{-1}. \tag{1}$$

该等式等价于 $(b1_F)(m1_F) = (a1_F)(n1_F)$. 再根据广义分配律, 它等价于 $bm(1_F1_F) = an(1_F1_F)$, 即 $(bm)1_F = (an)1_F$. 因为 $bm = an$, 所以 (1) 成立. 良定义成立.

对任意 $m/n, k/\ell \in \mathbb{Q})$,

$$\phi_0\left(\frac{m}{n} + \frac{k}{\ell}\right) = \phi_0\left(\frac{m\ell + kn}{k\ell}\right) = ((m\ell + kn)1_F)((n\ell)1_F)^{-1}$$

且

$$\phi_0\left(\frac{m}{n}\right) + \phi_0\left(\frac{k}{\ell}\right) = (m1_F)(n1_F)^{-1} + (k1_F)(\ell 1_F)^{-1}.$$

于是, 要验证

$$\phi_0\left(\frac{m}{n}+\frac{k}{\ell}\right)=\phi_0\left(\frac{m}{n}\right)+\phi_0\left(\frac{k}{\ell}\right). \tag{2}$$

只要验证

$$((m\ell+kn)1_F)((n\ell)1_F)^{-1}=(m1_F)(n1_F)^{-1}+(k1_F)(\ell 1_F)^{-1}.$$

利用断言和分配律可知左侧等于右侧.

要验证

$$\phi_0\left(\frac{m}{n}\frac{k}{\ell}\right)=\phi_0\left(\frac{m}{n}\right)\phi_0\left(\frac{k}{\ell}\right). \tag{3}$$

只要验证 $(mk)1_F((n\ell)1_F)^{-1}=(m1_F)(n1_F)^{-1}(k1_F)(\ell 1_F)^{-1}$. 而该等式由断言可直接导出.

进一步 $\phi_0(1)=\phi_0(1/1)=1_F1_F^{-1}=1_F$. 综上所述 ϕ_0 是同态.

(ii) 首先验证 ϕ_p 是良定义的. 设 $\bar{a}=\bar{b}$. 则 $a=b+kp$, 其中 k 是某个整数. 故

$$\phi_p(\bar{a})=(b+kp)1_F=b1_F+k(p1_F)=b1_F=\phi_p(\bar{b}).$$

设 $\bar{x},\bar{y}\in\mathbb{Z}_p$. 则

$$\phi_p(\bar{x}+\bar{y})=\phi_p(\overline{x+y})=(x+y)1_F=x1_F+y1_F=\phi_p(\bar{x})+\phi_p(\bar{y})$$

且

$$\phi_p(\bar{x}\bar{y})=\phi_p(\overline{xy})=(xy)1_F=(x1_F)(y1_F)=\phi_p(\bar{x})\phi_p(\bar{y}).$$

再由 $\phi_p(\bar{1})=1(1_F)=1_F$ 可知, ϕ_p 是同态.

例 4.6 *(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 $ad = bc \implies cb = da \implies (c,d) \sim (a,b)$. 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

$$ab' = a'b, \quad cd' = c'd. \tag{4}$$

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

$$b'd'(ad+bc)=bd(a'd'+b'c'). \tag{5}$$

我们从上式的左侧出发

$$\begin{aligned} b'd'(ad+bc) &= ab'dd'+bb'cd' \\ &= a'bdd'+b'bc'd \quad (\text{根据 } (4)) \\ &= bd(a'd'+b'c'). \end{aligned}$$

由此可知, (5) 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 (4), 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

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

于是

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

由此得出分配律成立. 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 4.7 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 $x, y \in D$,

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

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.

4.2 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) 不妨设 A 的第一行和第二行相同. 由行列式的公式定义

$$\det(A) = \sum_{\sigma \in S_n} \epsilon_\sigma a_{1,\sigma(1)} a_{2,\sigma(2)} a_{3,\sigma(3)} \cdots a_{n,\sigma(n)}.$$

因为 $\mathrm{char}(F) = 2$, 所以 $1_F = -1_F$. 故

$$\epsilon_\sigma a_{1,\sigma(1)} a_{2,\sigma(2)} a_{3,\sigma(3)} \cdots a_{n,\sigma(n)} = a_{1,\sigma(1)} a_{2,\sigma(2)} a_{3,\sigma(3)} \cdots a_{n,\sigma(n)}.$$

$$\begin{aligned} \det(A) &= \sum_{\sigma \in S_n, \sigma(1) < \sigma(2)} (a_{1,\sigma(1)} a_{2,\sigma(2)} + a_{1,\sigma(2)} a_{2,\sigma(1)}) a_{3,\sigma(3)} \cdots a_{n,\sigma(n)} \\ &= \sum_{\sigma \in S_n, \sigma(1) < \sigma(2)} (2a_{1,\sigma(1)} a_{2,\sigma(2)}) a_{3,\sigma(3)} \cdots a_{n,\sigma(n)} \quad (\vec{A}_1 = \vec{A}_2) \\ &= 0 \quad (\mathrm{char}(F) = 2). \end{aligned}$$

于是, 除了奇数阶斜对称矩阵行列式等于零以外, 关于行列式的所有结果适用于所有的域上的任何方阵.

例 4.8 设

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

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 4.9 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. 则存在整数环上的矩阵

$$M = \begin{pmatrix} m_{1,1} & m_{1,2} & m_{1,3} \\ m_{2,1} & m_{2,2} & m_{2,3} \end{pmatrix} \quad \text{使得} \quad (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3) = (\mathbf{u}, \mathbf{v})M.$$

于是

$$E_3 = (\mathbf{u}, \mathbf{v}) \begin{pmatrix} \bar{m}_{1,1} & \bar{m}_{1,2} & \bar{m}_{1,3} \\ \bar{m}_{2,1} & \bar{m}_{2,2} & \bar{m}_{2,3} \end{pmatrix}.$$

但这与 $\mathrm{rank}(E_3) = 3$ 矛盾. 故群 $(\mathbb{Z}_2^3, +, \mathbf{0})$ 至少有三个元素生成. 事实上, $\mathbb{Z}_2^3 = \langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \rangle$.

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 $S_8 = \langle (12), (12345678) \rangle$ *(见第四章第二讲命题 2.52)*

例 4.10 设 $A \in \mathrm{M}_n(\mathbb{R})$. 证明 $\mathrm{rank}(A) = \mathrm{rank}(A^t A)$.

证明. 设 $B = A^t A$, 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

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

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

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

另一方面, $\mathbf{w}^t A^t A\mathbf{w} = \mathbf{w}^t B\mathbf{w} = \mathbf{w}^t\mathbf{0} = 0$. 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 $\mathbf{w} \in V_B$. 我们证明了 $V_A = V_B$. 特别有 $\dim(V_A) = \dim(V_B)$. 根据对偶定理,

$$\operatorname{rank}(A) = n - \dim(V_A) = n - \dim(V_B) = \operatorname{rank}(B). \quad \square$$

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

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