第四章　群、环和域简介

3　环

3.1　定义和基本性质

定义 3.1 五元组 $(R,+,0,\cdot,1)$, 其中 R 是集合, $0,1\in R$ 且 $0\neq 1$, $+,\cdot$ 是 R 上的二元运算, 称为(含幺)环*(ring)*, 如果

(i) $(R,+,0)$ 是交换群;

(ii) $(R,\cdot,1)$ 是含幺半群; 且

(iii) 对于任意 $x,y,z\in R$,

$$x(y+z)=xy+xz \qquad (x+y)z=xz+yz.$$

当 $(R,\cdot,1)$ 是交换的含幺半群时, R 称为交换环. 否则称之为非交换环.

注解 3.2 科斯特利金书中环不一定含有乘法单位元, 即 $(R,\cdot)$ 是半群即可. 在本讲义中，我们只考虑含幺环，并简称为环.

例 3.3 设 $(R,+,0,\cdot,1)$ 是环. 则

(i) 对任意 $x\in R$, $0x=x0=0$;

(ii) 对任意 $x, y \in R$,

$$(-x)y = x(-y) = -(xy) \quad \text{和} \quad (-x)(-y) = xy;$$

(iii) 对任意 $x \in R$, $(-1)x = x(-1) = -x$.

证明. *(i)* 注意到 $0x = (0+0)x = 0x + 0x$. 于是, $0x = 0$. 类似可得 $x0 = 0$.

(ii) 由 $x + (-x) = 0$ 和 *(i)* 可知, $(x + (-x))y = 0$. 依据分配律, $xy + (-x)y = 0$. 故 $(-x)y = -(xy)$. 同理可知, $x(-y) = -(xy)$. 进而,

$$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy.$$

(iii) 因为 $1 + (-1) = 0$, 所以 $x(1 + (-1)) = 0$. 即 $x1 + x(-1) = 0$, $x + x(-1) = 0$. 由群 $(R, +, 0)$ 中的加法逆的唯一性, $x(-1) = -x$. 同理, $(-1)x = -x$.

例 3.4 下列环是交换环: $(R, +, 0, \cdot, 1)$, 其中 R 是 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ 或 $\mathbb{C}$; 对任意大于 1 的整数 n, $(\mathbb{Z}_n, +, \bar{0}, \cdot, \bar{1})$.

我们来验证 $\mathbb{Z}_n$ 中的分配律. 设 $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$, 则

$$\bar{x}(\bar{y}+\bar{z}) = \bar{x}\overline{y+z} = \overline{x(y+z)} = \overline{xy+xz} = \overline{xy}+\overline{xz} = \bar{x}\bar{y}+\bar{x}\bar{z}.$$

设 $S = \{f \mid f : \mathbb{R} \longrightarrow \mathbb{R}\}$. 设 $f, g \in S$. 定义

$$f+g:\ \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \mapsto & f(x)+g(x)\end{array} \quad \text{和} \quad f\cdot g:\ \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \mapsto & f(x)g(x)\end{array}$$

则 $(S,+,0,\cdot,1)$ 是交换环, 其中 0 是把所有实数都映成零的函数, 1 是把有实数都映成一的函数.

例 3.5 $(\mathrm{M}_n(\mathbb{R}),+,O,\cdot,E)$ 是非交换环, 其中 $n>1$.

定理 3.6 *(广义分配律)* 设 $x_1,\ldots,x_m,y_1,\ldots,y_n$ 是环 R 中的元素. 则

$$\left(\sum_{i=1}^{m} x_i\right)\left(\sum_{j=1}^{n} y_j\right)=\sum_{i=1}^{m}\sum_{j=1}^{n} x_i y_j.$$

证明. 先证明: 对任意 $x\in R$, $x(y_1+\cdots y_n)=xy_1+\cdots+xy_n$. 对 n 归纳. 当 $n=1$ 时, 结论显然成立. 设 $n>1$ 且 $n-1$ 时结论成立. 则

$$\begin{aligned} x(y_1+\cdots+y_{n-1}+y_n) &= x((y_1+\cdots y_{n-1})+y_n) && \text{(加法结合律)}\\ &= x(y_1+\cdots y_{n-1})+xy_n && \text{(左分配律)}\\ &= xy_1+\cdots+xy_{n-1}+xy_n && \text{(归纳假设).} \end{aligned}$$

类似地可证对任意 $y\in R$, $(x_1+\cdots+x_n)y=x_1y+\cdots+x_ny$.

设 $x=\sum_{i=1}^{m} x_i$. 则

$$\left(\sum_{i=1}^{m} x_i\right)\left(\sum_{j=1}^{n} y_j\right)=x\left(\sum_{j=1}^{n} y_j\right)=\sum_{j=1}^{n} xy_j=\sum_{i=1}^{m}\sum_{j=1}^{n} x_i y_j. \quad \square$$

推论 3.7 设 $m,n\in\mathbb{Z}$, $x,y\in R$. 则 $(mx)(ny)=(mn)(xy)$.

证明. 设整数环中的加法单位是 0, 而环 R 中的加法单位是 0_R, 乘法单位是 1_R.

如果 $m, n \in \mathbb{Z}^+$, 则由上述定理可得

$$(mx)(ny) = (mn)(xy).$$

如果 m, n 中有一个是 0, 则不妨设 $m = 0$. 由第四章第一讲第 7 页的符号约定可知, $mx = 0_R$. 故 $(mx)(ny) = 0_R$ 且 $(mn)(xy) = 0_R$. 结论成立.

如果 m, n 一正一负, 则不妨设 $n < 0$. 由第四章第一讲第 7 页的符号约定可知, $(mx)(ny) = (mx)((-n)(-y))$. 故

$$(mx)(ny) = (m(-n))(x(-y)) = (m(-n))(-xy) = (mn)(xy).$$

最后, 设 m, n 都是负的. 则

$$\begin{aligned}(mx)(ny) &= ((-m)(-x))((-n)(-y)) \\ &= ((-m)(-n))((-x)(-y)) \\ &= (mn)(xy). \quad \square\end{aligned}$$

注解 3.8 利用加法交换律, 上述推论还可以进一步的推广为

$$(mx)(ny) = (mn)(xy) = m(nxy) = n(m(xy)).$$

3.2 环同态和子环

定义 3.9 设 $(R, +, 0_R, \cdot, 1_R)$ 和 $(S, +, 0_S, \cdot, 1_S)$ 是两个环. 如果映射 $\phi : R \longrightarrow S$ 满足对任意 $x, y \in R$,

$$\phi(x+y) = \phi(x) + \phi(y),\ \phi(xy) = \phi(x)\phi(y),\ \text{和}\ \phi(1_R) = 1_S,$$

则称 ϕ 是环同态. 如果环同态 ϕ 是单射, 则称 ϕ 是环嵌入; 如果是双射, 则称环同构.

注意到从 R 到 S 的环同态 ϕ 一定是从 $(R, +, 0_R)$ 到 $(S, +, 0_S)$ 的群同态. 故 $\phi(0_R) = 0_S$ (见第四章第一讲命题 2.19 (i)). 根据第十三周练习4(3), ϕ 是环嵌入当且仅当

$$\phi(x) = 0_S \implies x = 0_R.$$

例 3.10 设 $n > 1$. 则商映射 $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ 是环同态. 验证如下: 对任意 $x, y \in \mathbb{Z}$,

$$\pi(x+y) = \overline{x+y} = \bar{x} + \bar{y} = \pi(x) + \pi(y)$$

和

$$\pi(xy) = \overline{xy} = \bar{x}\bar{y} = \pi(x)\pi(y)$$

且 $\pi(1) = \bar{1}$.

设 $C \in \mathrm{GL}_n(\mathbb{R})$. 定义:

$$\begin{array}{rccc} \psi_C : & \mathrm{M}_n(\mathbb{R}) & \longrightarrow & \mathrm{M}_n(\mathbb{R}) \\ & A & \mapsto & C^{-1}AC \end{array}$$

是环同构. 验证如下: 设 $A, B \in \mathrm{M}_n(\mathbb{R})$. 则

$$\psi_C(A+B) = C^{-1}(A+B)C = C^{-1}AC+C^{-1}BC = \psi_C(A)+\psi_C(B)$$

和

$$\psi(AB) = C^{-1}ABC = (C^{-1}AC)(C^{-1}BC) = \psi_C(A)\psi_C(B)$$

且 $\psi_C(E) = C^{-1}EC = E$.

定义 3.11 设 $(R, +, 0_R, \cdot, 1_R)$ 是环, $S \subset R$ 使得 $(S, +, 0_R, \cdot, 1_R)$ 也是环. 则称 S 是 R 的子环*(subring)*.

例 3.12 整数环是有理数环的子环.

例 3.13 设 $A \in \mathrm{M}_n(\mathbb{R})$ 且 $A \neq O$. 令

$$\mathbb{R}[A] := \{\sum_{i=0}^{k} \alpha_k A^k \mid k \in \mathbb{N}, \alpha_i \in \mathbb{R}\}.$$

验证 $\mathbb{R}[A]$ 是 $\mathrm{M}_n(\mathbb{R})$ 的子环且 $\mathbb{R}[A]$ 是交换环.

证明. 设 $B=\sum_{i=0}^{k} \alpha_i A^i$ 和 $C=\sum_{j=0}^{\ell} \beta_j A^j$, 其中 $\alpha_i, \beta \in \mathbb{R}$.

(i) 验证 $(\mathbb{R}[A], +, O)$ 是 $(\mathrm{M}_n(\mathbb{R}), +, O)$ 的子群. 因为 $B-C$ 仍是 A 的非负幂次在 $\mathbb{R}$ 上的线性组合, 所以 $B-C \in \mathbb{R}[A]$. 由子群判别法, 验证完毕.

(ii) 验证 $\mathbb{R}[A]$ 关于乘法封闭, 根据广义分配律,

$$BC = \sum_{i=1}^{k}\sum_{j=1}^{\ell} \alpha_i A^i \beta_j A^j.$$

在根据矩阵运算的规律,

$$BC = \sum_{i=1}^{k} \sum_{j=1}^{\ell} \alpha_i \beta_j A^{i+j}. \tag{1}$$

故 $BC \in \mathbb{R}[A]$. 验证完毕.

因为 $E = A^0$, 所以 $E \in \mathbb{R}[A]$. 故 $\mathbb{R}[A]$ 是子环.

由 (1) 的推导过程可知 $CB = \sum_{i=1}^{k} \sum_{j=1}^{\ell} \alpha_i \beta_j A^{i+j}$. 故 $BC = CB$. 我们得到 $\mathbb{R}[A]$ 是交换环.

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.

定义 3.16 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 3.17 整数环中没有零因子, 它的可逆元是 ± 1.

命题 3.18 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 $\ell=\operatorname{lcm}(n,a)$. 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, 设 $\bar{a}$ 是零因子. 则 $\bar{a}$ 关于乘法不可逆. 故 $g\neq 1$ (第四章命题 1.16). 又因为 $\bar{a}\neq 0$. 故 $g\neq n$. □.

在 $\mathbb{Z}_n$ 中非零元或者是零因子或者是可逆元.

例 3.19 剩余环 $\mathbb{Z}_6$ 中的零因子是 $\bar{2},\bar{3},\bar{4}$, 可逆元是 $\bar{1}$ 和 $\bar{5}$.

例 3.20 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 $\operatorname{rank}(A)<n$.

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,

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

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.

矩阵环 $\mathrm{M}_n(\mathbb{R})$ 中的非零矩阵或者是零因子或者是可逆元.

例 3.21 设 $B \in \mathbb{R}[A]$ 且非零. 证明 B 可逆当且仅当 $\mathrm{rank}(B) = n$.

证明. 设 m 是最小的正整数使得

$$\alpha_0 E + \alpha_1 B + \cdots + \alpha_m B^m = O,$$

其中 $\alpha_i \in \mathbb{R}$. 由第二章命题 *9.4 (矩阵求逆的多项式法)*, B 满秩, 则 $B^{-1} \in \mathbb{R}[B]$. 因为 $B \in \mathbb{R}[A]$, 所以 $\mathbb{R}[B] \subset \mathbb{R}[A]$. 故 $B^{-1} \in \mathbb{R}[A]$. 另一个方向是显然的. □

思考题: 确定 $\mathbb{R}[A]$ 中的零因子.

命题 3.22 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 $xy \in U$ (穿衣脱衣规则). 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. □

命题 3.23 设 p 素数. 则 $\mathbb{Z}_p$ 中的非零元都可逆.

证明. 设 $\bar{a} \in \mathbb{Z}_p \setminus \{\bar{0}\}$. 则 $p \nmid a$. 因为 p 是素数, 所以 $\gcd(p, a) = 1$. 根据本章命题 1.16, $\bar{a}$ 在 $\mathbb{Z}_p$ 中可逆. □

3.4 消去律

命题 3.24 设 R 是环, $a, b \in R$ 都非零, $x, y \in R$. 则

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

(ii) (右消去律) 若 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 3.25 设 D 是交换环. 如果 D 中没有零因子, 则称 D 是整环*(domain)*.

推论 3.26 设 D 是整环. 则对于任意 $x, y, z \in D$ 且 $x \neq 0$

$$xy = xz \Longrightarrow y = z.$$

4 域

4.1 域的定义和基本性质

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, 且 $\mathbb{Q}$ 是 $\mathbb{R}$ 的子域. 设 p 是素数. 则 $\mathbb{Z}_p$ 是域 *(命题 3.23)*.

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.

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 是单射.

证明. 注意到 ϕ 是从 $(F,+,0_F)$ 到 $(K,+,0_K)$ 的群同态. 根据第十三次习题 4, 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, $\phi(x^{-1}x)=\phi(1_F)=1_K$. 故 $0_K=1_K$, 矛盾. □

4.2 域的特征

定义 4.5 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 4.6 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, $0=m1=(k\ell)1=(k1)(\ell1)$. 因为 F 是整环, 所以 $k1=0$ 或 $\ell1=0$. 故 $\mathrm{char}(F)<m$, 矛盾. □

命题 4.7 设 F 是域. 则 F 是素数 p. 则对任意 $x\in F$ 和整数 m, $(mp)x=0$.

证明. 由定义可知

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

例 4.8 $\mathbb{Q}$ 和 $\mathbb{R}$ 的特征等于零. 对于素数 p, $\mathrm{char}(\mathbb{Z}_p) = p$.

命题 4.9 *(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 4.7, $\binom{p}{k} x^{p-k} y^k = 0$, $k = 1, 2, \ldots, p-1$. 故 $(x+y)^p = x^p + y^p$. □

命题 4.10 设 $(F, +, 0_F, \cdot, 1_F)$ 和 $(K, +, 0_K, \cdot, 1_K)$ 是两个域, $\phi : F \longrightarrow K$ 是环同态. 则 $\mathrm{char}(F) = \mathrm{char}(K)$.

证明. 设 $\mathrm{char}(F) = 0$, $n \in \mathbb{Z}^+$. 则 $\phi(n1_F) = n1_K$. 因为 ϕ 是单射(命题 4.4) 且 $\phi(0_F) = 0_K$, 所以 $n1_K \neq 0_K$. 故 $\mathrm{char}(K) = 0$.

设 $\mathrm{char}(F) = p$. 则 $\phi(0_F) = \phi(p1_F) = p1_K = 0_K$. 故 1_K 在 $(K, +, 0_K)$ 中的阶整除 p. 因为 p 是素数, 所以该阶等于 p, 即 $\mathrm{char}(K) = p$. □

例 4.11 设 p 是素数, $m \in \mathbb{Z}$ 满足 $\gcd(m, p) = 1$. 证明: $m^{p-1} \equiv 1 \mod p$.

证明. 考虑环同态:

$$\begin{array}{rccc} \phi_p & \mathbb{Z} & \to & \mathbb{Z}_p \\ & x & \mapsto & \bar{x} \end{array}$$

则 $m^{p-1} \equiv 1 \mod p$ 当且仅当 $\overline{m}^{p-1} = \bar{1}$.

下面我们在 $\mathbb{Z}_p$ 中证明 $\overline{m}^{p-1} = \bar{1}$.

设 $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{}\}$. 因为 $\gcd(m, p = 1$, 所以 $\overline{m} \in \mathbb{Z}_p^*$. 设 $L_{\overline{m}}$ 是群 $\mathbb{Z}_p^*, \cdot, \bar{1})$ 上的左平移. 故

$$\{\bar{1}, \bar{2}, \ldots, \overline{p-1}\} = \{\overline{m} \cdot \bar{1}, \overline{m} \cdot \bar{2}, \ldots, \overline{m} \cdot \overline{p-1}\}.$$

把这些元素相乘得

$$\prod_{i=1}^{p-1} \bar{i} = \prod_{i=1}^{p-1} \overline{m} \cdot \bar{i} = \overline{m}^{p-1} \cdot \prod_{i=1}^{p-1} \bar{i}.$$

故 $\overline{m}^{p-1} = \bar{1}$. □

4.3 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) 答案是仍然等于零. 证明见第十一讲例 2.9.

例 4.12 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 4.13 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

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

4.4 分式域

例 4.14 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

$$(m1_F)(n1_F)^{-1} = (a1_F)(b1_F)^{-1}. \tag{2}$$

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 (2) 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

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

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

$$\phi_0\left(\frac{m}{n}\frac{k}{\ell}\right)=\phi_0\left(\frac{m}{n}\right)\phi_0\left(\frac{k}{\ell}\right). \tag{4}$$

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 4.15 *(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 $(a,b)\in D\times D^*$, $ab=ba\Longrightarrow (a,b)\sim(a,b)$. 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

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

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

$$ab'=a'b,\quad cd'=c'd. \tag{5}$$

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

$$b'd'(ad+bc)=bd(a'd'+b'c'). \tag{6}$$

我们从上式的左侧出发

$$\begin{aligned} b'd'(ad+bc) &= ab'dd'+bb'cd' \\ &= a'bdd'+b'bc'd \quad (\text{根据 (5)}) \\ &= bd(a'd'+b'c'). \end{aligned}$$

由此可知, (6) 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 (5), 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 4.16 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.