

## 第四章 群、环和域简介

### 2.7 循环群的结构

**定义 2.48** 设  $G$  是群,  $g \in G$ . 则  $\langle g \rangle$  称为  $G$  中由  $g$  生成的循环子群. 如果存在  $g \in G$  使得  $G = \langle g \rangle$ , 则称  $G$  是循环群 (*cyclic group*).

**例 2.49** 整数的加法群  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ . 关于  $n$  的剩余类的加法群  $\mathbb{Z}_n = \langle \bar{1} \rangle$ . 设  $\bar{k} \in \mathbb{Z}_n$ . 则  $\mathbb{Z}_n = \langle \bar{k} \rangle$  当且仅当  $\text{ord}(\bar{k}) = n$ . 即:

$$n = \frac{n}{\gcd(n, k)} \iff \gcd(n, k) = 1.$$

见上一讲推论 2.42.

**例 2.50** 设  $p$  是素数,  $G$  是群且  $\text{card}(G) = p$ . 证明  $G$  是循环群.

证明. 设  $g \in G$  且  $g \neq e$ . 则  $\text{card}(\langle g \rangle)$  大于 1. 由 *Lagrange* 定理和  $p$  是素数可知,

$$\text{card}(\langle g \rangle) = p \implies \langle g \rangle = G. \quad \square$$

**命题 2.51** 设  $(G, \cdot, e)$  是循环群且  $\text{card}(G) > 1$ .

(i) 如果  $\text{card}(G) = \infty$ , 则  $G \simeq (\mathbb{Z}, +, 0)$ ;

(ii) 如果  $\text{card}(G) = n$ , 则  $G \simeq (\mathbb{Z}_n, +, \bar{0})$ .

证明. 设  $G = \langle g \rangle$ .

(i) 考虑映射

$$\begin{aligned}\phi: \mathbb{Z} &\longrightarrow G \\ m &\mapsto g^m.\end{aligned}$$

则  $\phi(x+y) = g^{x+y} = g^x g^y = \phi(x)\phi(y)$ . 故  $\phi$  是同态. 下面证明  $\phi$  是双射. 设  $\phi(x) = \phi(y)$ . 则  $g^x = g^y$ . 根据命题 2.38 (i),  $x = y$ . 故  $\phi$  是单射. 设  $h$  是  $G$  中任意元素. 则存在  $k \in \mathbb{Z}$  使得  $h = g^k$ . 于是,  $\phi(k) = h$ . 故  $\phi$  是满射. 综上所述,  $\phi$  是同构.

(ii) 考虑映射

$$\begin{aligned}\phi: \mathbb{Z}_n &\longrightarrow G \\ \bar{m} &\mapsto g^m.\end{aligned}$$

先验证  $\phi$  是良定义的. 设  $\bar{k} = \bar{m}$ . 则  $k = m + \ell n$ , 其中  $\ell$  是某个整数. 我们有

$$\phi(\bar{k}) = g^k = g^{m+\ell n} = g^m (g^n)^\ell = g^m = \phi(\bar{m}).$$

于是,  $\phi$  是良定义的.

设  $\bar{x}, \bar{y} \in \mathbb{Z}_n$ . 则

$$\phi(\bar{x} + \bar{y}) = \phi(\overline{x+y}) = g^{x+y} = g^x g^y = \phi(\bar{x})\phi(\bar{y}).$$

故  $\phi$  是同态.

最后验证  $\phi$  是双射. 设  $\phi(\bar{x}) = \phi(\bar{y})$ . 则  $g^x = g^y$ . 故  $g^{x-y} = e$ . 根据命题 2.41 (ii),  $n|(x-y)$ , 即  $\bar{x} = \bar{y}$ . 由此可知,  $\phi$  是单射. 对任意  $h \in G$ , 存在  $k \in \mathbb{Z}$  使得  $h = g^k$ . 于是,  $\phi(\bar{k}) = h$ . 我们得到,  $\phi$  是满射.

**例 2.52** 设  $p$  是素数, 群  $G$  含有  $p$  个元素. 根据 2.50,  $G$  和  $(\mathbb{Z}_p, +, 0)$  同构.

**例 2.53** 设  $(G, \cdot, e)$  是循环群. 证明:  $G$  的子群也循环.

证明. 设  $G = \langle g \rangle$ ,  $H$  是  $G$  的子群且  $H \neq \{e\}$ . 因为  $H$  是子群, 所以存在正整数  $m$  使得  $g^m \in H$ . 设  $s$  是最小的正整数使得  $g^s \in H$ . 则  $\langle g^s \rangle \subset H$ . 反之, 设  $h \in H$ . 则存在  $k \in \mathbb{Z}$  使得  $h = g^k$ . 由整数带余除法,  $k = qs + r$ , 其中  $q \in \mathbb{Z}$ ,  $r \in \{0, 1, \dots, s-1\}$ . 故

$$h = g^k = g^{qs+r} = (g^s)^q g^r \implies g^r = h(g^s)^{-q} \in H.$$

由  $s$  的极小性可知,  $r = 0$ . 故  $h \in \langle g^s \rangle$ . 我们得到,  $H \subset \langle g^s \rangle$ . 从而,  $H = \langle g^s \rangle$ .

**例 2.54** 设  $(G, \cdot, e)$  是循环群且  $\text{card}(G) = \infty$ . 设  $H$  是  $G$  的子群且  $H \neq \{e\}$ . 证明  $H \simeq G$ .

证明. 设  $G = \langle g \rangle$ . 由上例可知存在  $s \in \mathbb{Z}^+$  使得  $H = \langle g^s \rangle$ . 于是,  $\text{ord}(g^s) = \infty$ . 否则,  $\text{ord}(g) < \infty \implies \text{card}(G) < \infty$ , 矛

盾. 由命题 2.51 (i) 可知,  $\text{card}(H) = \infty$ . 故  $H \simeq (\mathbb{Z}, +, 0)$ . 于是, 命题 2.51 (i) 蕴含  $G \simeq H$ .  $\square$

## 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  $x, y, z \in R$ ,

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

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

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

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

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

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**  $(M_n(\mathbb{R}), +, O, \cdot, E)$  是非交换环, 其中  $n > 1$ .

**定理 3.6** (广义分配律) 设  $x_1, \dots, x_m, y_1, \dots, y_n$  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  $x \in R$ ,  $x(y_1 + \dots + y_n) = xy_1 + \dots + xy_n$ .

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

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

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

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  $\phi: R \rightarrow S$  满足对任意  $x, y \in R$ ,

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

则称  $\phi$  是环同态. 如果环同态  $\phi$  是单射, 则称  $\phi$  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  $\phi$  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),  $\phi$  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  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n$  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  $C \in \text{GL}_n(\mathbb{R})$ . 定义:

$$\begin{aligned} \psi_C: M_n(\mathbb{R}) &\longrightarrow M_n(\mathbb{R}) \\ A &\longmapsto C^{-1}AC \end{aligned}$$



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

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

和

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

$$\text{且 } \psi_C(E) = C^{-1}EC = E.$$

**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  $A \in M_n(\mathbb{R})$  且  $A \neq O$ . 令

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

验证  $\mathbb{R}[A]$  是  $M_n(\mathbb{R})$  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  $\alpha_i, \beta_j \in \mathbb{R}$ .

(i) 验证  $(\mathbb{R}[A], +, O)$  是  $(M_n(\mathbb{R}), +, O)$  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,

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

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  $\phi: R \rightarrow S$  是环同态. 则  $\text{im}(\phi)$  是子环.

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

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

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

### 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  $\pm 1$ .

**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  $l = \text{lcm}(n, a)$ . 根据第一章第四讲定理 7.10,

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

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  $\bar{a} \neq \bar{0}$ . 故  $g \neq n$ .  $\square$ .

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  $A \in M_n(\mathbb{R})$  是非零矩阵. 证明  $A$  是左或右零因子当且仅当  $\text{rank}(A) < n$ .

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

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

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

反之, 设  $\text{rank}(A) < n$ . 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

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

则

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

故  $A$  是左零因子.

事实上,  $\text{rank}(A^t)$  也小于  $n$ . 故  $A^t$  也是左零因子. 于是, 存在非零矩阵  $C \in M_n(\mathbb{R})$  使得  $A^t C = O$ . 于是,  $C^t A = O$ . 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  $M_n(\mathbb{R})$  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  $\text{rank}(B) = n$ .

证明. 设  $m$  是最小的正整数使得

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

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.  $\square$

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.  $\square$

**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.  $\square$

**例 3.24** (*Fermat* 小定理) 设  $p$  是素数,  $m \in \mathbb{Z} \setminus \{0\}$  且  $p \nmid m$ . 则  $m^{p-1} \equiv 1 \pmod{p}$ .

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  $m^{p-1} \equiv 1 \pmod{p}$ .

## 3.4 消去律

**命题 3.25** 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.  $\square$

**定义 3.26** 设  $D$  是交换环. 如果  $D$  中没有零因子, 则称  $D$  是整环 (*domain*).

**推论 3.27** 设  $D$  是整环. 则对于任意  $x, y, z \in D$  且  $x \neq 0$

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

## 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  $\phi$  是单射.

证明. 注意到  $\phi$  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.  $\square$

## 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  $\text{ord}(1)$  称为  $F$  的特征. 否则,  $F$  的特征定义为零. 域  $F$  的特征记为  $\text{char}(F)$ .

**命题 4.6** 设  $F$  是域. 则  $F$  的特征或是零或是素数.

证明. 设  $m = \text{char}(F) > 0$  且  $m = kl$ , 其中  $k, l \in \mathbb{Z}^+ \setminus \{1\}$ . 则由广义分配律可知,  $0 = m1 = (kl)1 = (k1)(l1)$ . 因为  $F$  是整环, 所以  $k1 = 0$  或  $l1 = 0$ . 故  $\text{char}(F) < m$ , 矛盾.  $\square$

**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  $p$ ,  $\text{char}(\mathbb{Z}_p) = p$ .

**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,  $p \mid \binom{p}{k}$ . 根据引理 4.7,  $\binom{p}{k} x^{p-k} y^k = 0$ ,  $k = 1, 2, \dots, p-1$ . 故  $(x + y)^p = x^p + y^p$ .  $\square$

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

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

设  $\text{char}(F) = p$ . 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  $\text{char}(K) = p$ .  $\square$



### 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,  $A \in M_n(F)$ .

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

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

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

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 4.11** 设

$$A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ \bar{1} & \bar{4} & \bar{2} \end{pmatrix} \in M_3(\mathbb{Z}_5).$$

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,  $\text{rank}(A) = 2 \implies \dim(V_A) = 1$ . 由方程  $\bar{2}x_2 + \bar{4}x_3 = \bar{0}$ , 得到  $x_2 = -\bar{3}\bar{4}x_3 = -\bar{12}x_3 = \bar{3}x_3$ . 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 4.12** 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 4.13** 设  $A \in M_n(\mathbb{R})$ . 证明  $\text{rank}(A) = \text{rank}(A^t A)$ .

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

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

则

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

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,

$$y_1^2 + \dots + y_n^2 = 0.$$

因为  $y_1, \dots, y_n \in \mathbb{R}$ , 所以  $y_1 = \dots = y_n = 0$ . 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,  $\text{rank}(A) = \text{rank}(B)$ .  $\square$

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

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