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 $\mathrm{ord}(\bar{k}) = n$. 即:

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

见上一讲推论 *2.38.*

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

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

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

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

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

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

证明. 设 $G = \langle g \rangle$.

(i) 考虑映射

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

则 $\phi(x+y) = g^{x+y} = g^x g^y = \phi(x)\phi(y)$. 故 ϕ 是同态. 下面证明 ϕ 是双射. 设 $\phi(x) = \phi(y)$. 则 $g^x = g^y$. 根据命题 2.38 (i), $x = y$. 故 ϕ 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 ϕ 是满射. 综上所述, ϕ 是同构.

(ii) 考虑映射

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

先验证 ϕ 是良定义的. 设 $\bar{k} = \bar{m}$. 则 $k = m + \ell n$, 其中 ℓ 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，ϕ 时良定义的.

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 ϕ 是同态.

最后验证 ϕ 是双射. 设 $\phi(\bar{x}) = \phi(\bar{y})$. 则 $g^x = g^y$. 故 $g^{x-y} = e$. 根据命题 2.38 (ii), $n|(x-y)$, 即 $\bar{x} = \bar{y}$. 由此可知, ϕ 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, ϕ 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 $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, s-1\}$. 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 $\mathrm{card}(G) = \infty$. 设 H 是 G 的子群且 $H \neq \{e\}$. 证明 $H \backsimeq G$.

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, $\mathrm{ord}(g^s) = \infty$. 否则, $\mathrm{ord}(g) < \infty \Longrightarrow \mathrm{card}(G) < \infty$, 矛

盾. 由命题 *2.51 (i)* 可知, $\mathrm{card}(H) = \infty$. 故 $H \backsimeq (\mathbb{Z}, +, 0)$. 于是, 命题 *2.51 (i)* 蕴含 $G \backsimeq H$. □

2.8 Cayley 定理

引理 2.55 设 $\phi : G \longrightarrow H$ 是群的单同态. 则 $G \backsimeq \mathrm{im}(\phi)$.

证明. 由第四章第一讲命题 2.28 可知, $\mathrm{im}(\phi)$ 是群. 而 $\phi : G \longrightarrow \mathrm{im}(\phi)$ 是双射. 故 $G \backsimeq \mathrm{im}(\phi)$. □

当 $\phi : G \longrightarrow H$ 是群的单同态时, 我们称 ϕ 把 G 嵌入到 H 中. 此时, G 同构于 H 的子群 $\mathrm{im}(\phi)$.

引理 2.56 设 $\phi : (G, \cdot, e) \longrightarrow (H, \cdot, \epsilon)$ 是群的同态. 则 ϕ 是嵌入当且仅当 $\phi(g) = \epsilon \Longrightarrow g = e$.

证明. 因为 ϕ 是同态, 所以 $\phi(e) = \epsilon$ (第四章第一讲命题 2.19 (i)). 故当 ϕ 是单射时, $\phi(g) = \epsilon \Longrightarrow g = e$. 反之, 设上述蕴含关系满足, 且 $g_1, g_2 \in G$ 满足 $\phi(g_1) = \phi(g_2)$. 则由第四章第一讲命题 2.19 (i),

$$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = \epsilon.$$

故 $g_1 g_2^{-1} = e$. 于是, $g_1 = g_2$, 即 ϕ 是单射. □

设 X 是非空. 令

$$T_X = \{f : X \longrightarrow X \mid f \text{ 是双射}\}.$$

则 $(T_X, \circ, \mathrm{id}_X)$ 称为 X 上的变换群.

定理 2.57 *(Cayley)* 设 $(G,\cdot,e)$ 是群. 则 G 可以被嵌入到变换群 T_G 中.

证明. 考虑映射:

$$\begin{array}{rccc}\phi: & G & \longrightarrow & T_G \\ & g & \mapsto & L_g\end{array},$$

其中 L_g 是第四章第一讲引理 2.11 中定义的左平移. 由该引理可知, ϕ 是良定义的映射. 注意到 $\phi(gh)=L_{gh}$. 对任意 $x\in G$, $L_{gh}(x)=(gh)x$. 而

$$L_g\circ L_h(x)=L_g(hx)=g(hx)=(gh)x=L_{gh}(x).$$

故 $L_{gh}=L_g\circ L_h$. 由此得出, $\phi(gh)=\phi(g)\circ\phi(h)$. 即 ϕ 是同态. 如果 $L_g=\mathrm{id}_G$, 则 $L_g(e)=\mathrm{id}_G(e)$, 即 $g=e$. 故 ϕ 是单射(引理 2.56). □

推论 2.58 设 G 是群且 n=card(G). 则 G 可嵌入到 S_n 中.

证明. 设 $G=\{g_1,\ldots,g_n\}$. 对 $f\in T_G$, 设 $f(g_i)=g_{k_i}$, $i=1,2,\ldots,n$. 则

$$\begin{pmatrix}1 & 2 & \cdots & n\\ k_1 & k_2 & \cdots & k_n\end{pmatrix}$$

是一个置换, 记为 σ_f. 则映射

$$\begin{array}{rccc}\phi: & T_G & \longrightarrow & S_n \\ & f & \mapsto & \sigma_f\end{array}.$$

双射. 再设 $w \in T_G$ 使得 $w(g_{k_i}) = g_{\ell_i}$, $i = 1, 2, \ldots, n$. 则 $w \circ f(g_i) = w(g_{k_i}) = g_{\ell_i}$. 另一方面, $\sigma_w \sigma_f(i) = \sigma_w(k_i) = \ell_i$. 于是,$\phi(w \circ f) = \sigma_w \sigma_f = \phi(w)\phi(f)$. 故 ϕ 是同构.

由定理 2.57 可知, G 可以通过单同态 $\psi : G \longrightarrow T_G$ 嵌入到 T_G 中. 于是, $\phi \circ \psi$ 把 G 嵌入到 S_n 中(第四章第一讲命题 2.19 (iii) 和第一章第二讲命题 4.8). □

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 $x,y\in R$,

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

(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

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

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

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

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

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

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)). 根据引理 2.56, 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 $\mathrm{rank}(A) < n$.

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.

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.

下面我们来讨论子环中的可逆元. 注意到 $\mathbb{Z}$ 是 $\mathbb{Q}$ 中的子环. 每个非零整数在 $\mathbb{Q}$ 中都可逆. 但非零整数在 $\mathbb{Z}$ 中的可逆元只有 ± 1.

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

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. □

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 $xy \in U$ (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 3.23 *(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 *(*第四章命题 *1.16)*. 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 3.24 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 3.25 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 $x \neq 0$

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

3.5 环的特征

定义 3.27 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 3.28 整数环的特征等于零, 而 $\mathrm{char}(\mathbb{Z}_n) = n$.

引理 3.29 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 3.30 *(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 3.29 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 3.31 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 3.32 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 3.33 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 $k, \ell \in \mathbb{Z}^+ \setminus \{1\}$. 则由广义分配律可知, $0 = m1 = (k\ell)1 = (k1)(\ell 1)$. 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, 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 *3.33*, 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. 由引理 2.56, 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. □

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 4.5 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 4.6 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 $S_8 = \langle (12), (12345678) \rangle$.

例 4.7 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

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

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

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

注解 4.8 第十一周习题 *6* 对一般的域不成立.