第四章　群、环和域简介

2.5　群的生成元

定义 2.48 设 G 是群, S 是 G 中的非空子集. 由 S 生成的子群 是指

$$\langle S\rangle = \{x_1^{e_1}\cdots x_m^{e_m} \,|\, m\in\mathbb{Z}^+, x_1,\ldots,x_m\in S, e_1,\ldots,e_m\in\mathbb{Z}\}.$$

如果 $G=\langle S\rangle$, 则称 S 中的元素是 G 的一组生成元.

下面我们验证 $\langle S\rangle$ 是 G 的子群. 设 $x,y\in\langle S\rangle$. 则存在 $x_1,\ldots,x_m,y_1,\ldots,y_n\in S$, $k_1,\ldots,k_m,\ell_1,\ldots,\ell_n\in\mathbb{Z}$ 使得

$$x=x_1^{k_1}\cdots x_m^{k_m} \quad 和 \quad y=y_1^{\ell_1}\cdots y_n^{\ell_n}.$$

根据第四章第一讲命题 2.6,

$$xy^{-1}=x_1^{k_1}\cdots x_m^{k_m}y_n^{-\ell_n}\cdots y_1^{-\ell_1}\in\langle S\rangle.$$

由第四章第一讲命题 2.24, $\langle S\rangle$ 是子群.

注解 2.49 设 G 是群, S 是 G 中的非空子集. 再设 H 是 G 的子群且 $S\subset H$. 则对任意 $m\in\mathbb{Z}^+, x_1,\ldots,x_m\in S, e_1,\ldots,e_m\in\mathbb{Z}$,

$$x_1^{e_1}\cdots x_m^{e_m}\in H \Longrightarrow \langle S\rangle\subset H.$$

注解 2.50 如果群 G 中的运算是以加法表示的. 则

$$\langle S\rangle = \{e_1x_1+\cdots+e_mx_m \,|\, m\in\mathbb{Z}^+, e_1,\ldots,e_m\in\mathbb{Z}, x_1,\ldots,x_m\in S\}.$$

例 2.51 由第二章第六讲推论 *8.6* 可知, $\mathrm{GL}_n(\mathbb{R})$ 可由所有的初等矩阵生成. 根据第一章第三讲定理 *6.12*, S_n 可由所有循环生成. 第一章第四讲引理 *6.17* 蕴含 S_n 可由所有对换生成.

定义 2.52 设 $(G,\cdot,e)$ 是群, $g\in G$. 如果不存在 $n\in\mathbb{Z}^+$ 使得 $g^n=e$, 则称 g 是无限阶的, 否则称之为有限阶的. 如果 k 是最小的正整数满足 $g^k=e$, 则称 k 是 g 的阶, 记为 $\mathrm{ord}(g)$.

在置换群 $(S_n,\circ,e)$ 中元素的阶和计算方法在第一章关于置换的讲义中已经给出.

命题 2.53 设 $(G,\cdot,e)$ 是群 且 $g\in G$.

(i) 如果 $\mathrm{ord}(g)=\infty$, 则对任意 $i,j\in\mathbb{Z}$, $g^i=g^j$ 当且仅当 $i=j$;

(ii) 如果 $\mathrm{ord}(g)=k<\infty$, 则对任意 $i,j\in\mathbb{Z}$, $g^i=g^j$ 当且仅当 $k|(i-j)$; 特别地, $g^m=e\iff k|m$.

证明. (i) 设 $g^i=g^j$. 则 $g^{i-j}=e$. 因为 $\mathrm{ord}(g)=\infty$, 所以 $i=j$. 另一个方向是显然的.

(ii) 设 $g^i=g^j$. 则 $g^{i-j}=e$. 由带余除法可知, 存在 $q\in\mathbb{Z},r\in\{0,1,\ldots,k-1\}$ 使得 $i-j=qk+r$. 故

$$e=g^{i-j}=g^{qk+r}=(g^k)^qg^r=g^r.$$

根据阶的定义, 我们有 $r = 0$. 故 $k|(i-j)$. 反之, 我们有 $i - j = hk$, 其中 h 是某个整数. 则

$$g^{i-j} = g^{hk} = e \implies g^i = g^j.$$

取 $i = m$ 和 $j = 0$. 我们得到 $g^m = e$ 当且仅当 $k|m$. □

推论 2.54 *设 G 是群, $g \in G$ 且 $m = \mathrm{ord}(g) < \infty$. 再设 $k \in \mathbb{Z}^+$. 则*

$$\mathrm{ord}(g^k) = \frac{m}{\gcd(m,k)} = \frac{\mathrm{lcm}(m,k)}{k}.$$

证明. 设 $q = m/\gcd(m,k)$. 根据第二章第一讲命题 7.11, $kq = \mathrm{lcm}(k,m)$. 根据命题 2.53 (ii),

$$e = g^{kq} = (g^k)^q.$$

同样的命题蕴含 $\mathrm{ord}(g^k)|q$. 另一方面, $g^{k\mathrm{ord}(g^k)} = e$ 蕴含 $m|k\mathrm{ord}(g^k)$. 于是, $k\mathrm{ord}(g^k)$ 是 m 和 k 的公倍数. 故 $kq|k\mathrm{ord}(g^k)$. 从而, $q|\mathrm{ord}(g^k)$. 我们得到 $q = \mathrm{ord}(g^k)$. □

例 2.55 *在 $(\mathbb{Z}_{10}, +, \bar{0})$ 中计算 $\mathrm{ord}(\bar{3}), \mathrm{ord}(\bar{4}), \mathrm{ord}(\bar{5})$.*

解 根据推论 2.54, 对任意 $\bar{s} \in \mathbb{Z}_{10}$,

$$\mathrm{ord}(\bar{s}) = \frac{\mathrm{lcm}(10,s)}{|s|}.$$

由此得出 $\mathrm{ord}(\bar{3}) = 10$, $\mathrm{ord}(\bar{4}) = 5$ 和 $\mathrm{ord}(\bar{5}) = 2$.

推论 2.56 设 G 是群, $g \in G$ 且 $\mathrm{ord}(g) < \infty$. 则

$$\mathrm{card}(\langle g \rangle) = \mathrm{ord}(g).$$

证明. 设 $\mathrm{ord}(g) = k$. 我们来证明:

$$\langle g \rangle = \{e, g, \ldots, g^{k-1}\}, \tag{1}$$

其中 $e, g, \ldots, g^{k-1}$ 两个不同.

显然, $\{e, g, \ldots, g^{k-1}\} \subset \langle g \rangle$. 反之, 设 $m \in \mathbb{Z}$. 则存在 $q \in \mathbb{Z}$ 和 $r \in \{0, 1, \ldots, k-1\}$ 使得

$$m = qk + r.$$

故 $g^m = g^{qk+r} = (g^k)^q g^r = g^r \in \{e, g, \ldots, g^{k-1}\}$. 由此得出, $\langle g \rangle \subset \{e, g, \ldots, g^{k-1}\}$. 故 (1) 成立.

设 $0 \le i \le j \le k-1$ 且 $g^i = g^j$. 由命题 2.53 (ii) 可知, $k|(j-i)$. 又因为 $j - i \in \{0, 1, \ldots, k-1\}$, 所以 $j = i$. 于是, $e, g, \ldots, g^{k-1}$ 两个不同. 故 $\mathrm{card}(\langle g \rangle) = k$. □

定理 2.57 设 G 是有限群, $g \in G$. 则 $g^{\mathrm{card}(G)} = e$, 即 $\mathrm{ord}(g)|\mathrm{card}(G)$.

证明. 由 Lagrange 定理, $\mathrm{card}(G) = [G : \langle g \rangle]\mathrm{card}(\langle g \rangle)$. 根据上述推论 $\mathrm{card}(G) = [G : \langle g \rangle]\mathrm{ord}(g)$. □

2.6 置换群的生成元(选读)

引理 2.58 设 $(i_1,\ldots,i_k)\in S_n$. 则对任意 $\sigma\in S_n$,

$$\sigma(i_1,\ldots,i_k)\sigma^{-1}=(\sigma(i_1),\ldots,\sigma(i_k)).$$

证明. 只要证 $\sigma(i_1,\ldots,i_k)=(\sigma(i_1),\ldots,\sigma(i_k))\sigma$.

设 $j\in\{i_1,\ldots,i_k\}$. 则

$$\sigma(i_1,\ldots,i_k)(j)=\begin{cases}\sigma(i_{s+1}), & j=i_s, s<k\\ \sigma(i_1), & j=i_k\end{cases}.$$

而

$$(\sigma(i_1),\ldots,\sigma(i_k))\sigma(j)=\begin{cases}\sigma(i_{s+1}), & j=i_s, s<k\\ \sigma(i_1), & j=i_k\end{cases}.$$

对于 $j\notin\{i_1,\ldots,i_k\}$,

$$\sigma(i_1,\ldots,i_k)(j)=\sigma(j)\quad\text{和}\quad(\sigma(i_1),\ldots,\sigma(i_k))=\sigma(j).$$

故 $\sigma(i_1,\ldots,i_k)=(\sigma(i_1),\ldots,\sigma(i_k))\sigma$. □

引理 2.59 $S_n=\langle(12),(13),\ldots,(1n)\rangle$.

证明. 根据第一章第四讲引理 6.17, 只要证明任意对换在 $\langle(12),(13),\ldots,(1n)\rangle$ 中即可. 设 $i,j\in\{1,2,\ldots,n\}$ 且 $i\neq j$ 和 $i\neq 1$. 由引理 2.58 可知:

$$(i,j)=(1,i)(1,j)(1,i)\in\langle(12),(13),\ldots,(1n)\rangle.\quad\square$$

引理 2.60 $S_n = \langle (12), (23), \ldots, (n-1, n) \rangle$.

证明. 由引理 2.59 可知, 我们只要证明

$$(1, k) \in \langle (12), (23), \ldots, (n-1, n) \rangle,$$

$k = 2, 3, \ldots, n$. 对 k 归纳. 当 $k = 2$ 时, 结论显然成立. 设 $k > 2$ 且 $(1, k-1) \in \langle (12), (23), \ldots, (n-1, n) \rangle$. 注意到

$$(1, k) = (1, k-1)(k-1, k)(1, k-1) \qquad \text{(引理 2.58)}$$
$$\Rightarrow (1, k) \in \langle (12), (23), \ldots, (n-1, n) \rangle \text{ (归纳假设).} \quad \square$$

命题 2.61 $S_n = \langle (12), (12, \cdots, n) \rangle$.

证明. 根据引理 2.59, 我们证明 $(k-1, k) \in \langle (12), (12, \cdots, n) \rangle$ 即可, 其中 $k = 2, 3, \ldots, n$. 当 $k = 2$ 时结论显然成立. 设 $k > 2$ 且 $(k-2, k-1) \in \langle (12), (12, \cdots, n) \rangle$. 根据引理 2.58,

$$(k-1, k) = (12 \cdots n)(k-2, k-1)(12 \cdots n)^{-1} \in \langle (12), (12, \cdots, n) \rangle. \quad \square$$

命题 2.62 当 $n \geq 3$ 时, 偶置换群*(交错群)*

$$A_n = \langle (123), (124), \ldots, (12n) \rangle.$$

证明. 由偶置换的定义可知, A_n 由两个对换之积生成. 可直接验证对任意 $a, b, c, d \in \{1, 2, \ldots, n\}$, 两两不同,

$$(abc)(abd) = (ac)(bd).$$

故 A_n 可以由长度为 3 的循环生成. 于是, 我们只需证明长度为 3 的循环可以由 $(123), (124), \ldots, (12n)$ 生成. 根据引理 2.58, 对 $k, m \in \{3, 4, \ldots, n\}$, $k \neq m$.

$$(12k)(12m)(12k)^{-1} = (2km) \Longrightarrow (2km) \in \langle (123), (124), \ldots, (12n) \rangle.$$

再取 $\ell \in \{1, 3, 4, \ldots, n\}$ 且 $\ell \neq k$, $\ell \neq m$. 根据引理 2.58,

$$(2km)(2k\ell)(2km)^{-1} = (k\ell m).$$

于是, 所有长度为 3 的循环都在 $\langle (123), (124), \ldots, (12n) \rangle$ 中. 故命题成立. □

命题 2.63 设 $\sigma = (12\ldots, n)$ 和 $k \in \mathbb{Z}^+$. 则

(i) $\operatorname{ord}(\sigma^k) = \frac{n}{\gcd(n,k)}$.

(ii) σ^k 是 $\gcd(n, k)$ 个互不相交的长度为 $n/\gcd(n, k)$ 循环之积.

证明. 设 $q = n/\gcd(n, k)$.

(i) 根据第一章第四讲引理 6.9, $\operatorname{ord}(\sigma) = n$. 由推论 2.54, $q = \operatorname{ord}(\sigma^k)$.

(ii) 断言: 设 $\ell \in \mathbb{Z}^+$. 如果存在 $i \in \{1, 2, \ldots, n\}$ 使得 $\sigma^\ell(i) = i$, 则 $\sigma^\ell = e$, 其中 e 代表恒同置换(映射).
断言的证明. 设 j 是 $\{1, 2, \ldots, n\}$ 中任意元素. 因为 σ 是长度为 n 的循环, 所以存在 $s \in \mathbb{N}$ 使得 $\sigma^s(i) = j$. 则

$$\sigma^{s+\ell}(i) = \sigma^s(\sigma^\ell(i)) = \sigma^s(i) = j.$$

另一方面,

$$\sigma^{s+\ell}(i) = \sigma^{\ell}(\sigma^{s}(i)) = \sigma^{\ell}(j).$$

故 $\sigma^{\ell}(j) = j$. 从而得到 $\sigma^{\ell} = e$. 断言成立.

设 $\sigma^{k} = \sigma_1 \cdots \sigma_m$, 其中 $\sigma_1, \ldots, \sigma_m$ 是两两互不相交的循环(见第一章第四讲命题 6.14). 再设 $\ell_i = \mathrm{ord}(\sigma_i)$, $i = 1, 2, \ldots, m$. 则

$$\sigma^{k\ell_1} = \sigma_1^{\ell_1}\sigma_2^{\ell_1} \cdots \sigma_m^{\ell_1}, \quad \text{其中 } \sigma^{\ell_1} = e. \tag{2}$$

设 $i \in \{1, 2, \ldots, n\}$ 使得 $\sigma_1(i) \neq i$. 因为 σ_1 与 $\sigma_2, \ldots, \sigma_m$ 都不相交, 所以

$$i = \sigma_2(i) = \cdots = \sigma_m(i).$$

从而,

$$i = \sigma_2^{\ell_1}(i) = \cdots = \sigma_m^{\ell_1}(i).$$

故 (2) 蕴含 $\sigma^{k\ell_1}(i) = i$. 由断言可知 $\sigma^{k\ell_1} = e$. 根据第一章第三讲命题 6.6, $q|\ell_1$. 另一方面, 因为 $\sigma^{kq} = e$ 和 σ_1 与 $\sigma_2, \ldots, \sigma_m$ 都不相交, 所以 $\sigma_1^{q} = e$. 故 $\ell_1|q$. 我们得到 $\ell_1 = q$. 同理 $\ell_2 = \cdots = \ell_m = q$. 因为 $\sigma_1, \ldots, \sigma_m$ 都是循环, 由第一章引理 6.9. 每个 σ_i 的长度都是 q. 进而 $m = n/q = \gcd(n, k)$. □

2.7 循环群的结构

定义 2.64 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 2.65 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 *2.42.*

例 2.66 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 2.67 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

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

则 $\phi(x+y) = g^{x+y} = g^x g^y = \phi(x)\phi(y)$. 故 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

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

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 2.41 (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 2.68 设 p 是素数, 群 G 含有 p 个元素. 根据 *2.66*, G 和 $(\mathbb{Z}_p, +, 0)$ 同构.

例 2.69 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 2.70 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 *2.67 (i)* 可知, $\mathrm{card}(H) = \infty$. 故 $H \backsimeq (\mathbb{Z}, +, 0)$. 于是, 命题 *2.67 (i)* 蕴含 $G \backsimeq H$. □

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

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

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

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

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

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

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

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,

$$BC = \sum_{i=1}^{k} \sum_{j=1}^{\ell} \alpha_i \beta_j A^{i+j}. \tag{3}$$

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 (3) 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. □

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

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. □

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 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. □