第四章　群、环和域简介

2　群

一个群 G 中有两个平凡的子群, 它们分别是该群本身和由单位元单独构成的子群. 当 G 有限时, $[G:G]=1$ 且 $[G,\{e\}]=\mathrm{card}(G)$.

例 2.30 *计算 $[S_n:A_n]$, 其中 $n>1$.*
解 设 σ 是 S_n 中的一个奇置换. 则 $L_\sigma(A_n)$ 中的元素都是奇置换. 设 τ 是 S_n 中任意奇置换. 则

$$\tau=\sigma(\sigma^{-1}\tau).$$

根据第一章第四讲引理 *6.23*, $\sigma^{-1}\tau\in A_n$. 故 $\tau\in L_\sigma(A_n)$. 故 $L_\sigma(A_n)$ 是所有奇置换构成的集合. 由此可知

$$S_n=A_n\cup L_\sigma(A_n)=L_e(A_n)\cup L_\sigma(A_n).$$

显然 $L_e(A_n)\cup L_\sigma(A_n)=\emptyset$. 我们得到 $[S_n:A_n]=2$.

例 2.31 *设 p 是素数. 群 G 中共有 p 个元素. 证明: G 没有非平凡子群.*

证明. 设 H 是 G 的子群. 根据第四章第一讲定理 2.29, $\mathrm{card}(H)|p$. 故 $\mathrm{card}(H)=1$ 或 $\mathrm{card}(H)=p$. 即 $H=\{e\}$ 或 $H=G$.

2.6 群的生成元

定义 2.32 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 2.33 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 $m\in\mathbb{Z}^+,x_1,\ldots,x_m\in S,e_1,\ldots,e_m\in\mathbb{Z}$,

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

例 2.34 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 $m\in\mathbb{Z}$ 使得 $\gcd(m,n)=1$. 下面我们证明 $\mathbb{Z}_n=\langle\bar{m}\rangle$. 由 *Bèzout* 关系可知, 存在 $u,v\in\mathbb{Z}$ 使得 $um+vn=1$. 则 $\bar{u}\bar{m}=\bar{1}$. 我们有 $u\bar{m}=\bar{1}$. 故 $\bar{1}\in\langle\bar{m}\rangle$. 故 $\mathbb{Z}_n=\langle\bar{m}\rangle$.

例 2.35 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 2.36 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 $\mathrm{ord}(g)$.

例 2.37 在 $(\mathbb{Z}_{10},+,\bar{0})$ 中计算 $\mathrm{ord}(\bar{3}),\mathrm{ord}(\bar{4}),\mathrm{ord}(\bar{5})$.
解 注意到 $m\bar{n}=\bar{0}$ 当且仅当 $\overline{mn}=\bar{0}$ 当且仅当 $10|mn$. 故 $\mathrm{ord}(\bar{n})$ 是最小的正整数 m 使得 $10|mn$, 即

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

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

命题 2.38 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, $g^m=e\implies k|m$.

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

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

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 2.39 *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 2.38 (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 $\mathrm{card}(\langle g \rangle) = k$. □

定义 2.40 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)*.

定理 2.41 设 $(G, \cdot, e)$ 是有限群. 则对于任意 $g \in G$, $\mathrm{ord}(g)|\mathrm{card}(G)$. 特别地, $g^{\mathrm{card}(G)} = e$.

证明. 设 $\mathrm{ord}(g) = k$. 根据命题 2.38 (i), $k < \infty$. 否则 $\langle g \rangle$ 是 G 的无限子群, 矛盾. 根据命题 2.38 (ii),

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

于是, $k = \mathrm{card}(\langle g \rangle)$. 由第四章第一讲定理 2.29, $k|\mathrm{card}(G)$. 再根据命题 2.38 (ii), $g^{\mathrm{card}(G)} = e$. □

例 2.42 设 p 是素数, G 是群且 $\mathrm{card}(G) = p$. 证明 G 是循环群.

2.7 循环群的结构

命题 2.43 设 $(G, \cdot, e)$ 是循环群且 $\mathrm{card}(G) > 1$.

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

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

证明. 设 $G = \langle g \rangle$.

(i) 考虑映射

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

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

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

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 2.38 (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 2.44 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 2.45 设 $(G, \cdot, e)$ 是循环群且 $\operatorname{card}(G) = \infty$. 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, $\operatorname{ord}(g^s) = \infty$. 否则, $\operatorname{ord}(g) < \infty \Longrightarrow \operatorname{card}(G) < \infty$, 矛盾. 由命题 *2.43 (i)* 可知, $\operatorname{card}(H) = \infty$. 故 $H \simeq (\mathbb{Z}, +, 0)$. 于是, 命题 *2.43 (i)* 蕴含 $G \simeq H$. □

2.8 Cayley 定理

引理 2.46 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 2.47 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 2.48 *(Cayley)* 设 $(G, \cdot, \mathrm{id}_G)$ 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. 设 $g, h \in G$. 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 2.47). □

推论 2.49 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 2.48 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). □

2.9 置换群的生成元

引理 2.50 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 2.51 $S_n = \langle (12), (13), \ldots, (1n) \rangle$.

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 2.50 可知:

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

引理 2.52 $S_n = \langle (12), (23), \ldots, (n-1, n) \rangle$.

证明. 由引理 2.51 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

$$\begin{aligned} (1, k) &= (1, k-1)(k-1, k)(1, k-1) && \text{(引理 2.50)} \\ &\Rightarrow (1, k) \in \langle (12), (23), \ldots, (n-1, n) \rangle \quad \text{(归纳假设)}. \quad \square \end{aligned}$$

命题 2.53 $S_n = \langle (12), (12, \cdots, n) \rangle$.

证明. 根据引理 2.51, 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 2.50,

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

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.

例 3.2 设 $(R,+,0,\cdot,1)$ 是环. 则

(i) 对任意 $x\in R$, $0x=x0=0$;

(ii) 对任意 $x\in R$, $(-1)x=x(-1)=-x$;

(iii) 对任意 $x,y\in R$,

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

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

(ii) 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, $(-1)x = -x$.

(iii) 利用 *(ii)* 计算得

$$(-x)y = (-1 \cdot x)y = (-1)(xy) = -(xy)$$

和

$$x(-y) = x(y(-1)) = (xy)(-1) = -(xy).$$

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

例 3.3 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 3.4 $(\mathrm{M}_n(\mathbb{R}), +, O, \cdot, E)$ 是非交换环, 其中 $n > 1$.

定理 3.5 *(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 $y \in R$, $(x_1 + \cdots + x_n)y = x_1 y + \cdots + x_n y$.

设 $x = \sum_{i=1}^m x_i$. 则

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

推论 3.6 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 3.7 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 3.8 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 $x, y \in R$,

$\phi(x+y)=\phi(x)+\phi(y)$, $\phi(xy)=\phi(x)\phi(y)$, 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 2.47, ϕ 是环嵌入当且仅当

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

例 3.9 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 3.10 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 3.11 整数环是有理数环的子环.

设 $\mathrm{UT}_n(\mathbb{R}) := \{A \in \mathrm{M}_n(\mathbb{R}) \mid A \text{ 上三角}\}$. 则 $\mathrm{UT}_n(\mathbb{R})$ 是 $\mathrm{M}_n(\mathbb{R})$ 的子环. 验证如下. 因为两个上三角形矩阵之差仍是上三角的, 所以 $(\mathrm{UT}_n(\mathbb{R}), +, O)$ 是$(\mathrm{M}_n(\mathbb{R}), +, O)$ 的子群. 设 $A = (a_{i,k}), B = (b_{k,j}) \in \mathrm{UT}_n(\mathbb{R})$. 令 $C{=}(c_{i,j}){=}AB$. 则

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}.$$

因为当 $i > k$ 时 $a_{i,k} = 0$, 所以

$$c_{i,j} = \sum_{k=i}^{n} a_{i,k} b_{k,j}.$$

又因为 $k > j$ 时 $b_{k,j} = 0$, 所以当 $i > j$ 时, $c_{i,j} = 0$. 故 C 是上三角的. 于是, $\mathrm{UT}_n(\mathbb{R})$ 关于乘法封闭. 显然 $E \in \mathrm{UT}_n(\mathbb{R})$. 从而, $(\mathrm{UT}_n(\mathbb{R}), \cdot, E)$ 是含幺半群. 分配律自然满足. 验证完毕.