

第四章 群、环和域简介

2 群

2.1 群的定义

定义 2.1 设 $*$ 是 S 上的二元运算. 如果 $*$ 满足结合律, 则称 $(S, *)$ 是半群(*semi-group*).

例 2.2 $(\mathbb{Z}^+, +)$ 是半群. 因为加法是交换的, 所以它是交换半群, 也称 *abelian semigroup*. 设

$$S = \{A \in M_n(\mathbb{R}) \mid \text{rank}(A) < n\}.$$

由秩不等式可知, $A, B \in S$ 蕴含 $AB \in S$, 即 S 关于乘法是封闭的. 而结合律自然成立. 故 (S, \cdot) 是半群.

定义 2.3 设 $(M, *)$ 是半群. 如果 M 中有关于 $*$ 的单位元 e , 则称 $(M, *, e)$ 是含幺半群(*monoid*).

例 2.4 $(\mathbb{N}, +, 0)$ 是一个含幺半群. 因为加法是交换的, 所以它是一个交换含幺半群, 也称 *abelian monoid*.

显然, $(M_n(\mathbb{R}), \cdot, E)$ 是含幺半群. 设 S 如上. 则 $(S, +, O)$ 不是含幺半群. 这是因为两个不满秩的矩阵之和可能是满秩的.

设 X 是非空集, $X^X = \{f : X \rightarrow X \mid f \text{ 是映射}\}$.
则 $(X^X, \circ, \text{id}_X)$ 是含幺半群.

命题 2.5 设 $(M, *, e)$ 是含幺半群, $x \in M$.

- (i) 如果 $y, z \in S$ 使得 $yx=xz=e$, 则 $y=z$. 从而 x 可逆.
- (ii) 如果 x 可逆, 则它的逆唯一.

证明. (i) 我们有 $y(xz) = ye = y$. 再根据结合律,

$$y(xz) = (yx)z = ez = z.$$

我们得到 $y = z$. (ii) 由 (i) 直接可得. \square

设 $x \in M$ 可逆. 它的逆记为 x^{-1} . 再由可逆元的定义可知 x^{-1} 也是可逆元且

$$(x^{-1})^{-1} = x.$$

命题 2.6 设 $(M, *, e)$ 是含幺半群. 如果 $x, y \in M$ 可逆, 则 $x * y$ 也可逆且其逆是 $y^{-1} * x^{-1}$.

证明. 设 $z = y^{-1} * x^{-1}$. 则

$$z * (x * y) = (y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = e.$$

类似地, $(x * y) * z = e$. \square

设 x_1, \dots, x_n 是 M 中的逆元. 反复利用命题 2.5 可得,
 $x_1 * \cdots * x_n$ 可逆且

$$(x_1 * \cdots * x_n)^{-1} = x_n^{-1} * \cdots * x_1^{-1}.$$

设 x 是上述含幺半群 M 中的可逆元. 则其逆记为
 x^{-1} . 设 $n \in \mathbb{Z}$. 令

$$x^n = \begin{cases} \underbrace{x * \cdots * x}_n, & n > 0, \\ e, & n = 0, \\ \underbrace{x^{-1} * \cdots * x^{-1}}_{-n}, & n < 0. \end{cases}$$

当 M 中的运算用“+”代表, 单位元用 0 代表时, x 的逆元
记为 $-x$. 令

$$nx = \begin{cases} \underbrace{x + \cdots + x}_n, & n > 0, \\ 0, & n = 0, \\ \underbrace{-x + \cdots + (-x)}_{-n}, & n < 0. \end{cases}$$

由广义结合律可得, 对于任意 $m, n \in \mathbb{Z}$

$$(x^m)(x^n) = x^{m+n}, \quad (x^m)^n = x^{mn}$$

或

$$mx + nx = (m+n)x, \quad m(nx) = (mn)x.$$

定义 2.7 设 $(G, *, e)$ 是一个含幺半群. 如果 G 中每个元素都可逆, 则称 G 是一个群(*group*). 换言之, 集合 G 和其上的二元运算 $*$ 构成群, 如果

(G1) 对任意 $x, y, z \in G$, $x * (y * z) = (x * y) * z$; (结合律)

(G2) 存在 $e \in G$ 使得对任意 $g \in G$, $g * e = e * g = g$; (单位元)

(G3) G 中每个元素都可逆. (逆元)

设 $(G, *, e)$ 是群. 如果对于任意 $x, y \in G$, $x * y = y * x$. 则称 G 是交换群或 abelian group.

例 2.8 以下是交换群的若干例子: $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}^*, \cdot, 1)$; 其中 $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$; $(\mathbb{Z}_n, +, \bar{0})$, 其中 $n > 1$. 在线性代数中: $(\mathbb{R}^n, +, \mathbf{0})$ 和 $(\mathbb{R}^{m \times n}, +, O_{m \times n})$.

例 2.9 设 $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) \mid A \text{ 可逆}\}$. 则 $(\mathrm{GL}_n(\mathbb{R}), \cdot, E_n)$ 是(非交换)群, 称为一般线性群 (*general linear group*).

设 X 是非空集.

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

则 $(T_X, \circ, \mathrm{id}_X)$ 是群. 特别地, (S_n, \circ, e) 是群, 其中 e 是 $\{1, 2, \dots, n\}$ 上的恒同映射. 称 S_n 是置换群.

当 $\text{card}(G) < \infty$ 时, 群 G 称为有限群. 注意到 $\text{card}(\mathbb{Z}_n) = n$ 和 $\text{card}(S_n) = n!$.

命题 2.10 (群中的消去律) 设 G 是群, $x, y, g \in G$. 如果 $gx = gy$ 或 $xg = yg$, 则 $x = y$.

证明. 设 $gx = gy$. 则

$$g^{-1}(gx) = g^{-1}(gy) \implies (g^{-1}g)x = (g^{-1}g)y.$$

于是, $x = y$. \square

2.2 群的乘法表

引理 2.11 设 $(G, *, e)$ 是群, $g \in G$. 定义

$$\begin{array}{ccc} L_g : G & \longrightarrow & G \\ & & \text{和} \\ x & \mapsto & g * x \end{array} \quad \begin{array}{ccc} R_g : G & \longrightarrow & G \\ & & \\ x & \mapsto & x * g. \end{array}$$

则 L_g 和 R_g 都是双射且 $L_g^{-1} = L_{g^{-1}}$ 和 $R_g^{-1} = R_{g^{-1}}$.

证明. 设 $x \in G$. 则

$$L_{g^{-1}} \circ L_g(x) = g^{-1}(gx) = (g^{-1}g)x = x.$$

于是, $L_{g^{-1}} \circ L_g = \text{id}_G$. 同理, $L_g \circ L_{g^{-1}} = \text{id}_G$. 故 L_g 可逆且其逆是 $L_{g^{-1}}$. 对 R_g 的结论可以类似地证明. \square

设 $G = \{e, g_1, \dots, g_{k-1}\}$ 是一个 k 阶群. 我们可以通过如下乘法表来理解这个群的结构.

*	e	g_1	g_2	\cdots	g_{k-1}
e	e	g_1	g_2	\cdots	g_{k-1}
g_1	g_1	g_1^2	g_1g_2	\cdots	g_1g_{k-1}
g_2	g_2	g_2g_1	g_2^2	\cdots	g_2g_{k-1}
\vdots	\vdots	\vdots	\vdots	\ddots	\vdots
g_{k-1}	g_{k-1}	$g_{k-1}g_1$	$g_{k-1}g_2$	\cdots	g_{k-1}^2

注意到以 g_i 为标识的行是 L_{g_i} 的像, 以 g_j 为标识的列是 R_{g_j} 的像. 根据引理 2.11, 每行(列)中的元素两两不同.

例 2.12 设 $G = \{e\}$. 则

*	e
e	e

实例: $(\{0\}, +, 0)$, $(\{1\}, \times, 1)$, $(\{E_n\}, \cdot, E_n)$.

例 2.13 设 $G = \{e, a\}$. 则

*	e	a
e	e	a
a	a	e

实例: $(\mathbb{Z}_2, +, \bar{0})$, $(\{1, -1\}, \times, 1)$, $(\{E_n, -E_n\}, \cdot, E_n)$.

例 2.14 设 $G = \{e, a, b\}$. 则

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

实例: $(\mathbb{Z}_3, +, \bar{0})$. 设集合 G 由以下三个矩阵:

$$E_2, \quad A = \begin{pmatrix} \cos\left(\frac{2\pi}{3}\right) & -\sin\left(\frac{2\pi}{3}\right) \\ \sin\left(\frac{2\pi}{3}\right) & \cos\left(\frac{2\pi}{3}\right) \end{pmatrix}, \quad B = \begin{pmatrix} \cos\left(\frac{4\pi}{3}\right) & -\sin\left(\frac{4\pi}{3}\right) \\ \sin\left(\frac{4\pi}{3}\right) & \cos\left(\frac{4\pi}{3}\right) \end{pmatrix}.$$

注意到

$$\begin{aligned} & \begin{pmatrix} \cos(\theta_1) & -\sin(\theta_1) \\ \sin(\theta_1) & \cos(\theta_1) \end{pmatrix} \begin{pmatrix} \cos(\theta_2) & -\sin(\theta_2) \\ \sin(\theta_2) & \cos(\theta_2) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta_1 + \theta_2) & -\sin(\theta_1 + \theta_2) \\ \sin(\theta_1 + \theta_2) & \cos(\theta_1 + \theta_2) \end{pmatrix}. \end{aligned}$$

于是, $A^2 = B$, $B^2 = A$ 和 $AB = BA = E_2$. 故 (G, \cdot, E_2) 是 3 阶子群. 群 G 代表把平面上的向量逆时针旋转 0° , 120° 和 240° (见第二章第三讲例 5.10).

例 2.15 设 $G = \{e, a, b, c\}$. 则

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

实例: $(\mathbb{Z}_4, +, \bar{0})$. 设集合 G 由以下四个矩阵:

$$E_2, \quad A = \begin{pmatrix} \cos\left(\frac{\pi}{2}\right) & -\sin\left(\frac{\pi}{2}\right) \\ \sin\left(\frac{\pi}{2}\right) & \cos\left(\frac{\pi}{2}\right) \end{pmatrix}, \quad B = \begin{pmatrix} \cos(\pi) & -\sin(\pi) \\ \sin(\pi) & \cos(\pi) \end{pmatrix}$$

和

$$C = \begin{pmatrix} \cos\left(\frac{3\pi}{2}\right) & -\sin\left(\frac{3\pi}{2}\right) \\ \sin\left(\frac{3\pi}{2}\right) & \cos\left(\frac{3\pi}{2}\right) \end{pmatrix}$$

组成. 群 (G, \cdot, E_2) 代表把平面上的向量逆时针旋转 0° , 90° , 180° 和 270° . (见第二章第三讲例 5.10).

四阶群还可以有另一张乘法表如下.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

实例 1: $\mathbb{Z}_2 \times \mathbb{Z}_2$, 其上的运算是坐标分别相加. 则 $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$ 是上述乘法表给出的 4 阶群. 设集合 H 由下列四个矩阵

$$E_2, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \text{ 和 } \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

组成. 群 (G, \cdot, E_2) 中的元素分别代表把平面上的恒同变换, 关于 x 轴, y 轴和原点的反射.

以后我们将证明 5 阶群的乘法表只有一个. 注意到 S_3 是 6 阶群, 它是非交换的.

2.3 同态与同构

定义 2.16 设 $(G, *, e)$ 和 (H, \star, ϵ) 是两个群. 则映射 $\phi : G \rightarrow H$ 称为同态(*homomorphism*), 如果对于任意 $x, y \in G$,

$$\phi(x * y) = \phi(x) \star \phi(y).$$

当同态 ϕ 是双射时, ϕ 称为同构(*isomorphism*). 此时我们称群 G 和 H 是同构的(*isomorphic*), 记为 $G \simeq H$.

例 2.17 设 π 是从 \mathbb{Z} 到 \mathbb{Z}_n 的商映射(第一章第三讲定义 5.14). 则 π 是从 $(\mathbb{Z}, +, 0)$ 到 $(\mathbb{Z}_n, +, \bar{0})$ 的同态. 验证如下: 设 $x, y \in \mathbb{Z}$. 则

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

例 2.18 证明: $(\mathbb{Z}_2, +, \bar{0})$ 与 $(\{1, -1\}, \cdot, 1)$ 同构.

证明. 设

$$\begin{aligned} \phi : \mathbb{Z}_2 &\longrightarrow \{-1, 1\} \\ \bar{0} &\mapsto 1 \\ \bar{1} &\mapsto -1 \end{aligned}$$

则

$$\phi(\bar{0} + \bar{0}) = 1 = 1 \cdot 1 = \phi(\bar{0}) \cdot \phi(\bar{0}),$$

$$\phi(\bar{0} + \bar{1}) = \phi(\bar{1}) = -1 = 1 \cdot (-1) = \phi(\bar{0}) \cdot \phi(\bar{1}).$$

类似地, $\phi(\bar{1} + \bar{0}) = \phi(\bar{1}) \cdot \phi(\bar{0})$. 最后

$$\phi(\bar{1} + \bar{1}) = \phi(\bar{0}) = 1 = (-1) \cdot (-1) = \phi(\bar{1}) \cdot \phi(\bar{1}).$$

命题 2.19 设 $(G, *, e)$ 和 (H, \star, ϵ) 是两个群.

(i) 如果 $\phi : G \longrightarrow H$ 是同态, 则对任意的 $x \in G$, $\phi(e) = \epsilon$ 和 $\phi(x^{-1}) = \phi(x)^{-1}$.

(ii) 如果 $\phi : G \longrightarrow H$ 是同构, 则 ϕ^{-1} 也是同构.

(iii) 再设 (M, \diamond, θ) 是群. 如果 $\phi : G \rightarrow H$ 和 $\psi : H \rightarrow M$ 是同态(构). 则 $\psi \circ \phi$ 也是同态(构).

证明. (i) 注意到 $\phi(e) = \phi(e * e) = \phi(e) \star \phi(e)$. 等式两侧同时乘以 $\phi(e)^{-1}$ 得 $\epsilon = \phi(e)$. 进而,

$$\epsilon = \phi(e) = \phi(x^{-1} * x) = \phi(x^{-1}) \star \phi(x).$$

等式右侧同时乘以 $\phi(x)^{-1}$ 得 $\phi(x^{-1}) = \phi(x)^{-1}$.

(ii) 设 $u, v \in H$ 和 $x = \phi^{-1}(u), y = \phi^{-1}(v)$. 则

$$\phi(x * y) = \phi(x) \star \phi(y) = u \star v.$$

故

$$\phi^{-1}(u \star v) = x * y = \phi^{-1}(u) \star \phi^{-1}(v).$$

于是, ϕ^{-1} 是同构.

(iii) 设 $x, y \in G$.

$$\psi \circ \phi(x * y) = \psi(\phi(x * y)) = \psi(\phi(x) \star \phi(y)) = (\psi \circ \phi(x)) \diamond (\psi \circ \phi(y)).$$

故 $\psi \circ \phi$ 是同态. 当 ϕ 和 ψ 是双射时, 它们的复合也是双射(第一章第二讲命题 4.8 (iii)). 故此时 $\psi \circ \phi$ 是同构. \square

设 \mathcal{G} 是所有群的集合. 下面我们验证同构关系 \cong 是 \mathcal{G} 上的等价关系. 对任意 $G \in \mathcal{G}$, id_G 是从 G 到 G 的同构. 故 $G \cong G$. 自反性成立. 再设 $H \in \mathcal{G}$ 且 $G \cong H$. 则存在同构 $\phi : G \rightarrow H$. 由命题 2.19 (ii) 可知, $\phi^{-1} : H \rightarrow G$ 是同构. 故 $H \cong G$. 对称性成立. 再设 $M \in \mathcal{G}$ 且 $G \cong H$ 和 $H \cong M$. 则存在群同构 $\phi : G \rightarrow H$ 和 $\psi : H \rightarrow M$. 由命题 2.19 (ii) 可知, $\psi \circ \phi$ 是从 G 到 M 的同构. 故 $G \cong M$. 传递性成立.

群论基本问题. 对群按同构分类, 即找出 \mathcal{G}/\cong 中所有的等价类, 并在每一类中找出一个典型的代表元.

当 \mathcal{G} 是所有有限群的集合时, 目前分类工作已经基本完成.

当不引起混淆时, 我们把群 G 中两元素 x, y 的运算结果记为 xy 或 $x + y$.

例 2.20 设 $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. 则 \mathbb{R}^* 关于乘法构成群. 则 $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ 是群同态. 这是行列式乘积定理的直接推论. 该同态是从非交换群到交换群的同态.

例 2.21 证明 $(\mathbb{Z}_4, +, \bar{0})$ 和 $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$ 不同构.

证明. 假设 ϕ 是从 \mathbb{Z}_4 到 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 的同构. 根据命题 2.19 (i), $\phi(\bar{0}) = (\bar{0}, \bar{0})$. 因为 ϕ 是单射, 所以 $\phi(\bar{1}) \neq (\bar{0}, \bar{0})$.

设 $\phi(\bar{1}) = (\bar{1}, \bar{0})$. 则

$$\phi(\bar{1} + \bar{1}) = \phi(\bar{1}) + \phi(\bar{1}) = (\bar{1}, \bar{0}) + (\bar{1}, \bar{0}) = (\bar{1} + \bar{1}, \bar{0} + \bar{0}) = (\bar{0}, \bar{0}).$$

故 $\phi(\bar{2}) = (\bar{0}, \bar{0})$. 再因为 ϕ 是单射, 所以 $\bar{2} = \bar{0}$ 在 \mathbb{Z}_4 中成立. 矛盾. 因为在 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中

$$(\bar{0}, \bar{1}) + (\bar{0}, \bar{1}) = (\bar{1}, \bar{1}) + (\bar{1}, \bar{1}) = (\bar{0}, \bar{0}),$$

所以我们可以类似地证明 $\phi(\bar{1})$ 既不等于 $(\bar{0}, \bar{1})$ 也不等于 $(\bar{1}, \bar{1})$. 故同构 ϕ 不存在.

2.4 子群

定义 2.22 设 (G, \cdot, e) 是群, $H \subset G$ 且 (H, \cdot, e) 也是群. 则称 H 是 G 的子群(*subgroup*).

命题 2.23 设 (G, \cdot, e) 是群, H 是 G 的非空子集. 则 H 是 G 的子群当且仅当对任意 $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.

证明. 设 H 是 G 的子群, $h_1, h_2 \in H$. 则 $h_2^{-1} \in H$. 因为 \cdot 也是 H 上的二元运算, 所以 $h_1 h_2^{-1} \in H$. 反之, 设 $h_1 \in H$.

则 $e = h_1 h_1^{-1} \in H$. 进而, $h_1^{-1} = e h_1^{-1} \in H$. 再设 $h_2 \in H$. 则 $h_2^{-1} \in H$. 故

$$h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H.$$

于是, \cdot 是 H 上的二元运算. 因为 \cdot 在 G 上满足结合律, 所以它在 H 上也满足结合律. \square

例 2.24 设 S 是所有偶数的集合. 因为偶数之差仍是偶数, 所以上述命题蕴含 $(S, +, 0)$ 是 $(\mathbb{Z}, +, 0)$ 的子群.

例 2.25 设 $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}$. 设 $A, B \in \mathrm{SL}_n(\mathbb{R})$. 因为 $A^{-1}A = E$, 所以行列式乘积定理蕴含 $|A^{-1}| |A| = E$. 故 $|A^{-1}| = 1$. 由此得出,

$$|BA^{-1}| = |B| |A^{-1}| = 1.$$

故 $BA^{-1} \in \mathrm{SL}_n(\mathbb{R})$. 再根据命题 2.23, $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的子群. 称之为实数上的特殊线性群(*special linear group*).

命题 2.26 设 G, H 是两个群, $\phi: G \rightarrow H$ 是群同态. 则 $\mathrm{im}(\phi)$ 是 H 的子群.

证明. 设 $u, v \in \mathrm{im}(\phi)$. 则存在 $x, y \in G$ 使得 $\phi(x) = u$ 和 $\phi(y) = v$. 根据命题 2.19 (i), $\phi(x^{-1}) = u^{-1}$. 故

$$\phi(yx^{-1}) = \phi(y)\phi(x^{-1}) = vu^{-1}.$$

由此可知, $vu^{-1} \in \text{im}(\phi)$. 再根据命题 2.23, $\text{im}(\phi)$ 是 H 的子群. \square

引理 2.27 设 $\phi: G \rightarrow H$ 是群的单同态. 则 $G \simeq \text{im}(\phi)$.

证明. 由第四章第一讲命题 2.28 可知, $\text{im}(\phi)$ 是群. 而 $\phi: G \rightarrow \text{im}(\phi)$ 是双射. 故 $G \simeq \text{im}(\phi)$. \square

2.5 群的生成元

定义 2.28 设 G 是群, S 是 G 中的非空子集. 由 S 生成的子群是指

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

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 $x_1, \dots, x_m, y_1, \dots, y_n \in S$, $k_1, \dots, k_m, \ell_1, \dots, \ell_n \in \mathbb{Z}$ 使得

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

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 2.29 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 $m \in \mathbb{Z}^+, x_1, \dots, x_m \in S, e_1, \dots, e_m \in \mathbb{Z}$,

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

注解 2.30 如果群 G 中的运算是以加法表示的. 则

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

例 2.31 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 2.32 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 2.33 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 $\text{ord}(g) = k < \infty$, 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 $\text{ord}(g) = \infty$, 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 $q \in \mathbb{Z}, r \in \{0, 1, \dots, k-1\}$ 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 $k|m$. \square

推论 2.34 设 G 是群, $g \in G$ 且 $m = \text{ord}(g) < \infty$. 再设 $k \in \mathbb{Z}^+$. 则

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

证明. 设 $q = m/\gcd(m, k)$. 根据第二章第一讲命题 7.11, $kq = \text{lcm}(k, m)$. 根据命题 2.33 (ii),

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

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

例 2.35 在 $(\mathbb{Z}_{10}, +, \bar{0})$ 中计算 $\text{ord}(\bar{3}), \text{ord}(\bar{4}), \text{ord}(\bar{5})$.

解 根据推论 2.34, 对任意 $\bar{s} \in \mathbb{Z}_{10}$,

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

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

推论 2.36 设 G 是群, $g \in G$ 且 $\text{ord}(g) < \infty$. 则

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

证明. 设 $\text{ord}(g) = k$. 我们来证明:

$$\langle g \rangle = \{e, g, \dots, g^{k-1}\}, \quad (1)$$

其中 e, g, \dots, g^{k-1} 两个不同.

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

$$m = qk + r.$$

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

设 $0 \leq i \leq j \leq k-1$ 且 $g^i = g^j$. 由命题 2.33 (ii) 可知, $k|(j-i)$. 又因为 $j-i \in \{0, 1, \dots, k-1\}$, 所以 $j = i$. 于是, e, g, \dots, g^{k-1} 两个不同. 故 $\text{card}(\langle g \rangle) = k$. \square

2.6 循环群的结构

定义 2.37 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 2.38 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 2.39 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 2.40 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 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 2.41 设 p 是素数, 群 G 含有 p 个元素. 根据 2.39, G 和 $(\mathbb{Z}_p, +, 0)$ 同构.

例 2.42 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 2.43 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, $\text{ord}(g^s) < \infty \implies \text{card}(G) < \infty$, 矛盾. 由命题 2.40 (i) 可知, $\text{card}(H) = \infty$. 故 $H \simeq (\mathbb{Z}, +, 0)$. 于是, 命题 2.40 (i) 蕴含 $G \simeq H$. \square