

第四章 群、环和域简介

1 二元运算

1.2 同余运算

设 n 是大于 1 的正整数. 在第一章第三讲我们定义了同余关系 \equiv_n (定义 5.8). 设 $\mathbb{Z}_n = \mathbb{Z} / \equiv_n$. 则

$$\mathbb{Z}_n = \{\bar{a} \mid a \in \mathbb{Z}\}.$$

对于 $\bar{a}, \bar{b} \in \mathbb{Z}_n$, $\bar{a} = \bar{b}$ 当且仅当 $a \equiv_n b$, 即 $n \mid (a - b)$.

定义 1.1 定义 \mathbb{Z}_n 上的加法:

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) &\longmapsto \overline{a + b}. \end{aligned}$$

验证良定义如下, 设 $a, b, x, y \in \mathbb{Z}$ 使得 $\bar{a} = \bar{x}$ 和 $\bar{b} = \bar{y}$. 则存在 $k, \ell \in \mathbb{Z}$ 使得 $a = x + kn$ 和 $b = y + \ell n$. 于是

$$a + b = (x + y) + (k + \ell)n.$$

故

$$\overline{a + b} = \overline{x + y}.$$

由此得出

$$\bar{a} + \bar{b} = \bar{x} + \bar{y}.$$

我们验证了 $+$ 是良定义的.

例 1.2 在 $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ 中, 我们有

$$\bar{1} + \bar{1} = \overline{1+1} = \bar{2} = \bar{0}.$$

定义 1.3 定义 \mathbb{Z}_n 上的乘法:

$$\begin{aligned} \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) &\longmapsto \overline{ab}. \end{aligned}$$

验证良定义如下, 设 $a, b, x, y \in \mathbb{Z}$ 使得 $\bar{a} = \bar{x}$ 和 $\bar{b} = \bar{y}$. 则存在 $k, \ell \in \mathbb{Z}$ 使得 $a = x + kn$ 和 $b = y + \ell n$. 于是

$$ab = xy + (ky + \ell x + k\ell n)n.$$

故

$$\overline{ab} = \overline{xy}.$$

由此得出

$$\bar{a}\bar{b} = \bar{x}\bar{y}.$$

我们验证了 \cdot 是良定义的.

例 1.4 在 $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ 中, 我们有

$$\bar{2}\bar{4} = \overline{2 \cdot 4} = \bar{8} = \bar{2} \quad \text{和} \quad \bar{2}\bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{0}.$$

1.3 单位元和逆元

定义 1.5 设 $*$ 是集合上的二元运算. 如果存在 $e \in S$ 使得对于任意的 $x \in S$, $x * e = e * x = x$. 则称 e 是关于 $*$ 的单位元.

整数关于加法的单位元是 0 , 在 \mathbb{Z}_n 中关于加法的单位是 $\bar{0}$, 在 $\mathbb{R}^{m \times n}$ 中关于加法的单位是 $O_{m \times n}$. 整数关于乘法的单位元是 1 , 在 \mathbb{Z}_n 中关于乘法的单位是 $\bar{1}$, 在 $M_n(\mathbb{R})$ 中关于乘法的单位是 E_n .

命题 1.6 设 $*$ 是集合上的二元运算. 设 $e, e' \in S$ 是单位元. 则 $e = e'$.

证明. 注意到 $ee' = e = e'$. \square .

定义 1.7 设 $*$ 是集合上的二元运算, $e \in S$ 是单位元. 设 $x \in S$. 如果存在 $y \in S$ 使得 $x * y = y * x = e$. 则称 x 是可逆元, y 是 x 的逆.

整数, \mathbb{Z}_n , $\mathbb{R}^{m \times n}$ 中每个元素关于加法都是可逆的. 整数关于乘法的可逆元是 ± 1 , 在 $M_n(\mathbb{R})$ 中关于乘法的可逆元是可逆矩阵.

例 1.8 设 X 是非空集合, 定义 X^X 是从 X 到它自身的所有映射的集合. 则复合 \circ 是 X^X 上的运算. 它的单位是恒同映射. 可逆元是双射.

命题 1.9 设 $\bar{a} \in \mathbb{Z}_n$. 则 \bar{a} 关于乘法可逆当且仅当 a 和 n 互素.

证明. 设存在 $\bar{b} \in \mathbb{Z}_n$ 使得 $\bar{a}\bar{b} = \bar{1}$. 则

$$ab \equiv_n 1.$$

故存在 $k \in \mathbb{Z}$ 使得 $ab - 1 = kn$ 即 $ab + kn = 1$. 由第一章第四讲定理 7.8, a, n 互素.

反之, 设 a, n 互素. 同样的定理蕴含存在 $u, v \in \mathbb{Z}$ 使得 $ua + vn = 1$. 故 $\bar{u}\bar{a} = \bar{1}$. 进而 $\bar{u}\bar{a} = \bar{a}\bar{u} = \bar{1}$. \square .

例 1.10 计算 \mathbb{Z}_{15} 中的所有关于乘法的可逆元.

解. 由上述命题可知, 可逆元是 $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}$.

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 $(\mathbb{Z}^+, +)$ 是一个半群. 因为加法是交换的, 所以它是一个交换半群, 也称 *abelian semigroup*. 设

$$S = \{A \in M_n(\mathbb{R}) \mid \det(A) > 1\}.$$

由行列式乘法定理, 矩阵乘法是 S 上的二元运算, 即 S 关于乘法是封闭的. 则 (S, \cdot) 是一个半群.

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

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

$$T = \{A \in M_n(\mathbb{R}) \mid \det(A) \geq 1\}.$$

由行列式乘法定理, 矩阵乘法是 T 上的二元运算, 即 T 关于乘法是封闭的. 则 (T, \cdot, E) 是一个含么半群. 此外, $(M_n(\mathbb{R}), \cdot, E)$ 也是含么半群.

设 X 是非空集,

$$X^X = \{f : X \longrightarrow X \mid f \text{ 是映射}\}.$$

则 $(X^X, \circ, \text{id}_X)$ 和 $(M_n(\mathbb{R}), \cdot, E)$ 都是含么半群.

命题 2.5 设 $(M, *, e)$ 是含么半群. 如果 $x \in M$ 可逆, 则它的逆唯一.

证明. 设 $y, z \in M$ 是 x 的逆. 则 $yx = xz = e$. 故

$$y(xz) = ye = y.$$

再根据结合律,

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

我们得到 $y = z$. \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, $x_1 * \dots * x_n$ 可逆且

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

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

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

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 $(G, *, e)$ 是一个含么半群. 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 $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A \text{ 可逆}\}$. 则 $(GL_n(\mathbb{R}), \cdot, E_n)$ 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 $(T_X, \circ, \text{id}_X)$ 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

$$L_g : G \longrightarrow G \quad \text{和} \quad R_g : G \longrightarrow G$$

$$x \mapsto g * x \quad \quad \quad x \mapsto x * g.$$

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

$$\begin{array}{c|c} * & e \\ \hline e & e \end{array}$$

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

例 2.13 设 $G = \{e, a\}$. 则

$$\begin{array}{c|cc} * & e & a \\ \hline e & e & a \\ a & a & e \end{array}$$

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

$$\begin{array}{c|ccc} * & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array}$$

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

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

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 $\phi :$

$G \longrightarrow H$ 称为同态 (*homomorphism*), 如果对于任意 $x, y \in G$,

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

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 $(H, *, \epsilon)$ 是两个群.

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

(ii) 如果 $\phi : G \rightarrow H$ 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.

例 2.22 证明 S_3 和 $(\mathbb{Z}_6, +, \bar{0})$ 不同构.

证明. 假设 $\phi : S_3 \rightarrow \mathbb{Z}_6$ 是同构. 设 $\phi((12)) = \bar{a}$ 和 $\phi((23)) = \bar{b}$. 则

$$\phi((12)(23)) = \phi((12)) + \phi((23)) = \bar{a} + \bar{b}$$

和

$$\phi((23)(12)) = \phi((23)) + \phi((12)) = \bar{b} + \bar{a} = \bar{a} + \bar{b}.$$

于是, $\phi((12)(23)) = \phi((23)(12))$. 因为 ϕ 是单射, 所以 $(12)(23) = (23)(12)$. 但

$$(12)(23) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{和} \quad (23)(12) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

矛盾.

2.4 子群

定义 2.23 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 2.24 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 2.25 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 2.26 设 A_n 是 S_n 中所有的偶置换的集合. 因为偶置换的逆也是偶置换, 而偶置换之积也是偶置换, 所以上述命题蕴含 A_n 是 S_n 的子群. 我们称 A_n 是交错群 (*alternating group*)

例 2.27 设 $GL_n(\mathbb{Q}) = \{A \in GL_n(\mathbb{R}) \mid A \text{ 中元素都是有理数}\}$. 设 $A, B \in GL_n(\mathbb{Q})$. 则由求逆的算法可知

$$B^{-1} \in GL_n(\mathbb{Q}) \implies AB^{-1} \in GL_n(\mathbb{Q}).$$

根据命题 2.24, $GL_n(\mathbb{Q})$ 是 $GL_n(\mathbb{R})$ 的子群. 称之为有理数上的一般线性群.

设 $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$. 设 $A, B \in SL_n(\mathbb{R})$. 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 $BA^{-1} \in SL_n(\mathbb{R})$. 再根据命题 2.24, $SL_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$ 的子群. 称之为实数上的特殊线性群 (*special linear group*).

设

$SL_n(\mathbb{Z}) = \{A \in GL_n(\mathbb{R}) \mid A \text{ 中元素都是整数且 } \det(A) = 1\}$.

设 $A, B \in SL_n(\mathbb{Z})$. 由前一段推理可知 $|BA^{-1}| = 1$. 因为

$$A^{-1} = \frac{1}{|A|}A^\vee = A^\vee,$$

所以 $BA^{-1} \in SL_n(\mathbb{Z})$. 再根据命题 2.24, $SL_n(\mathbb{Z})$ 是 $GL_n(\mathbb{R})$ 的子群. 称之为整数上的特殊线性群.

命题 2.28 设 G, H 是两个群, $\phi: G \rightarrow H$ 是群同态. 则 $\text{im}(\phi)$ 是 H 的子群.

证明. 设 $u, v \in \text{im}(\phi)$. 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 2.24, $\text{im}(\phi)$ 是 H 的子群. \square

定理 2.29 (Lagrange) 设 G 是有限群, H 是 G 的子群. 则

$$\text{card}(H) \mid \text{card}(G).$$

证明. 对任意 $g \in G$, 设 L_g 是引理 2.11 定义的左平移映射. 因为 $e \in H$ 且 $L_g(e) = g$, 所以 $g \in L_g(H)$. 故

$$G = \bigcup_{g \in G} L_g(H).$$

因为 G 有限, 所以存在最小正整数 k 和 $g_1, \dots, g_k \in G$ 使得

$$G = \bigcup_{i=1}^k L_{g_i}(H).$$

下面我们证明子集 $L_{g_1}(H), \dots, L_{g_k}(H)$ 两两互不相交.

假设 $x \in L_{g_i}(H) \cap L_{g_j}(H)$. 则存在 $h_i, h_j \in H$ 使得

$$x = g_i h_i \quad \text{和} \quad x = g_j h_j.$$

于是, $g_i = g_j h_j h_i^{-1}$. 设 y 是 L_{g_i} 中的任意元素. 则存在 $h \in H$ 使得 $y = g_i h$. 故 $y = g_j h_j h_i^{-1} h$. 因为 H 是子群, 所以 $h_j h_i^{-1} h \in H$. 由此可知, $y \in L_{g_j}(H)$. 故 $L_{g_i}(H) \subset L_{g_j}(H)$. 同理, $L_{g_j}(H) \subset L_{g_i}(H)$. 故 $L_{g_j}(H) = L_{g_i}(H)$. 由 k 的极小

性可知, $i = j$. 故子集 $L_{g_1}(H), \dots, L_{g_k}(H)$ 两两互不相交. 由此得出

$$\text{card}(G) = \sum_{i=1}^k \text{card}(L_{g_i}(H)). \quad (1)$$

根据引理 2.11, 任何左平移都是单射. 于是,

$$\text{card}(L_g(H)) = \text{card}(H).$$

再由 (1) 可得 $\text{card}(G) = k\text{card}(H)$. \square

上述证明中的正整数 k 称为子群 H 关于 G 的指标(index), 记为 $[G : H]$.