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

$$S=\{A\in \mathrm{M}_n(\mathbb{R})|\mathrm{rank}(A)<n\}.$$

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, $(\mathrm{M}_n(\mathbb{R}),\cdot,E)$ 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, $X^X = \{f : X \longrightarrow X \mid f \text{ 是映射}\}$. 则$(X^X, \circ, \mathrm{id}_X)$ 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. □

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

$$\left(x^{-1}\right)^{-1} = x.$$

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, $(x * y) * z = e$. □

设 $x_1,\ldots,x_n$ 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 $\{1, 2, \ldots, n\}$ 上的恒同映射. 称 S_n 是 置换群.

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

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

$$\begin{aligned} L_g\colon G &\longrightarrow G \\ x &\mapsto g * x \end{aligned} \quad \text{和} \quad \begin{aligned} R_g\colon G &\longrightarrow G \\ x &\mapsto x * g. \end{aligned}$$

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, $L_{g^{-1}} \circ L_g = \mathrm{id}_G$. 同理, $L_g \circ L_{g^{-1}} = \mathrm{id}_G$. 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 $G = \{e, g_1, \ldots, g_{k-1}\}$ 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.

$$\begin{array}{c|ccccc}
* & e & g_1 & g_2 & \cdots & g_{k-1} \\
\hline
e & e & g_1 & g_2 & \cdots & g_{k-1} \\
g_1 & g_1 & g_1^2 & g_1g_2 & \cdots & g_1g_{k-1} \\
g_2 & g_2 & g_2g_1 & g_2^2 & \cdots & g_2g_{k-1} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
g_{k-1} & g_{k-1} & g_{k-1}g_1 & g_{k-1}g_2 & \cdots & g_{k-1}^2
\end{array}$$

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

$*$	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

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

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 $(H,\star,\epsilon)$ 是两个群. 则映射 $\phi: G\longrightarrow H$ 称为同态*(homomorphism)*, 如果对于任意 $x,y\in G$,

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

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

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

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 $(H,\star,\epsilon)$ 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 $(M,\diamond,\theta)$ 是群. 如果 $\phi: G\to H$ 和 $\psi: H\to M$ 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 $\phi : G \longrightarrow H$. 由命题 2.19 (ii) 可知, $\phi^{-1} : H \longrightarrow G$ 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 $\phi : G \longrightarrow H$ 和 $\psi : H \longrightarrow M$. 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 $\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow R^*$ 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 $\phi: S_3\longrightarrow\mathbb{Z}_6$ 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.

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 2.23 *(Cayley) 设 $(G, \cdot, e)$ 是群. 则 G 可以被嵌入到变换群 T_G 中, 即存在单同态 $\phi : G \to T_G$.*

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 $L_g = L_h$, 则 $L_g(e) = L_h(e)$, 即 $g = h$. 故 ϕ 是单射. □

推论 2.24 *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 2.23 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. □

2.4 子群

定义 2.25 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 2.26 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 $h_1, h_2 \in H$, $h_1h_2^{-1} \in H$.

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 $h_1h_2^{-1} \in H$. 反之, 设 $h_1 \in H$. 则 $e = h_1h_1^{-1} \in H$. 进而, $h_1^{-1} = eh_1^{-1} \in H$. 再设 $h_2 \in H$. 则 $h_2^{-1} \in H$. 故

$$h_1h_2 = h_1(h_2^{-1})^{-1} \in H.$$

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. □

例 2.27 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 2.28 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 2.29 设 $\mathrm{GL}_n(\mathbb{Q})=\{A\in\mathrm{GL}_n(\mathbb{R})\,|\,A$ 中元素都是有理数$\}$. 设 $A,B\in\mathrm{GL}_n(\mathbb{Q})$. 则由求逆的算法可知

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

根据命题 *2.26*, $\mathrm{GL}_n(\mathbb{Q})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的子群. 称之为有理数上的一般线性群.

设 $\mathrm{SL}_n(\mathbb{R})=\{A\in\mathrm{GL}_n(\mathbb{R})\,|\,\det(A)=1\}$. 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 *2.26*, $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的子群. 称之为实数上的特殊线性群*(special linear group)*.

设

$$\mathrm{SL}_n(\mathbb{Z})=\{A\in\mathrm{GL}_n(\mathbb{R})\,|\,A \text{ 中元素都是整数且 } \det(A)=1\}.$$

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

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

所以 $BA^{-1} \in \mathrm{SL}_n(\mathbb{Z})$. 再根据命题 *2.26*, $\mathrm{SL}_n(\mathbb{Z})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的子群. 称之为整数上的特殊线性群.

命题 2.30 设 G, H 是两个群, $\phi : G \longrightarrow H$ 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, $vu^{-1} \in \mathrm{im}(\phi)$. 再根据命题 2.26, $\mathrm{im}(\phi)$ 是 H 的子群. □

引理 2.31 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, G 同构于 H 的子群 $\mathrm{im}(\phi)$. 由 Cayley 定理可知, G 同构于 T_G 的一个子群. 特别地, 设 G 是 n 阶群. 则 G 同构于 S_n 的一个子群.

定理 2.32 *(Lagrange)* 设 G 是有限群, H 是 G 的子群. 则

$$\mathrm{card}(H)|\mathrm{card}(G).$$

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 $g_1, \ldots, g_k \in G$ 使得

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

下面我们证明子集 $L_{g_1}(H), \ldots, L_{g_k}(H)$ 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

$$x = g_i h_i \quad 和 \quad x = g_j h_j.$$

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 $L_{g_1}(H), \ldots, L_{g_k}(H)$ 两两互不相交. 由此得出

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

根据引理 2.11, 任何左平移都是单射. 于是,

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

再由 (1) 可得 $\mathrm{card}(G) = k\mathrm{card}(H)$. □

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

例 2.33 *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 $[S_n : A_n] = 2$ 和 $\mathrm{card}(A_n) = n!/2$.

例 2.34 *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 $H = G$.