

设 $(G, *)$, (H, Δ) $f: G \rightarrow H$, 称 f 是 $(G, *)$ 到 (H, Δ) 的同态是指
 $\forall a, b \in G$, $f(a * b) = f(a) \Delta f(b)$.

若同态 f 还是双射, 则称 f 是 $(G, *)$ 到 (H, Δ) 的同构

例. $G = \{1, -1\}$, $(G, -)$ $H = \{0, 1\}$, (H, \oplus) 横+加

$$\begin{aligned} f: G \rightarrow H \quad &f(1) = 0, \quad f(-1) = 1. \quad |x| = 1 \leftrightarrow 0 \oplus 0 = 0 \\ &|-1| = -1 \leftrightarrow 0 \oplus 1 = 1 \\ &(-1) * 1 = -1 \leftrightarrow 1 \oplus 0 = 1 \\ &(-1) * (-1) = 1 \leftrightarrow 1 \oplus 1 = 0 \end{aligned}$$

★ 命题. $\omega(G, *)$, (H, Δ) 是群, 元记为 $|_G$, $|_H$. $f: G \rightarrow H$ 同态, 则

$$(1) f(|_G|) = |_H$$

$$(2) \forall a \in G, f(a^{-1}) = f(a)^{-1}$$

$$(3) \forall a \in G, m \in \mathbb{Z}, \text{ 有 } f(a^m) = f(a)^m$$

$$\text{证: (1) } f(|_G|) = f(|_G * |_G|) = f(|_G) \Delta f(|_G|)$$

$$\text{由消去律 (等式两边乘 } f(|_G|)^{-1}) \quad f(|_G|) = |_H$$

$$(2) f(a * a^{-1}) = f(a) \Delta f(a^{-1})$$

$$f(|_G|) = |_H \quad \therefore f(a) \Delta f(a^{-1}) = |_H. \quad f(a^{-1}) = f(a)^{-1}.$$

$$(3) \forall a \in G, f(a^2) = f(a * a) = f(a) \Delta f(a) = f(a)^2$$

$$f(a^3) = f(a^2 * a) = f(a^2) \Delta f(a) = f(a)^2 \Delta f(a) = f(a)^3$$

$$\text{设 } k \in \mathbb{Z}^+, \text{ 有 } f(a^k) = f(a)^k$$

$$\text{① } f(a^{k+1}) = f(a^k) \Delta f(a) = f(a)^k \Delta f(a) = f(a)^{k+1}, \text{ 由归纳, } m \in \mathbb{Z}^+ \text{ 都对}$$

$$\text{② } \forall k \in \mathbb{Z}^+, f(a^{-k}) = f((a^k)^{-1}) = f(a^k)^{-1} = (f(a)^k)^{-1} = f(a)^{-k}$$

#

例. $M_{nn}(\mathbb{R}) \rightarrow \mathbb{R}$

矩阵 $A \mapsto \det(A)$

$\det: M_{nn}(\mathbb{R}) \rightarrow \mathbb{R}$

$\det(AB) = \det(A)\det(B)$, \det 是矩阵乘法 → 实数乘法的同态

$\det(A) \neq 0 \Leftrightarrow A$ 可逆, 即 $\exists B$, s.t. $AB = BA = I_n$.

\det 将 $n \times n$ 可逆矩阵 (乘法下) 到非 0 实数 (乘法下) 的群同态

例. $GL_n(\mathbb{R})$: 实数上 n 阶可逆阵全体 $\rightarrow GL_{n+1}(\mathbb{R})$

$f: GL_n(\mathbb{R}) \rightarrow GL_{n+1}(\mathbb{R})$

$$f(A) = \begin{pmatrix} A & 0 \\ 0 & \det(A)^{-1} \end{pmatrix}$$

$\det(f(A)) = \det(A)\det(A)^{-1} = 1$ ④ 验证矩阵乘法保持

Map

集合 X $M(X) = \{f \mid f: X \rightarrow X\}$ $(M(X), \circ)$ 么半群 // 映射。结合律 ✓ 么元恒映射

Symmetric \leftarrow $Sym(X) = \{f \mid f: X \rightarrow X \text{ 双射}\}$ $(Sym(X), \circ)$ 群 // 有逆映射

Left. 反象 a

$(G, *)$ 是半群, $a \in G$, 可以诱导 G 到 G 的一个映射 L_a . $\forall b \in G$, $L_a(b) = a * b$

凯莱定理 设 $(G, *)$ 是半群, 对任 $a \in G$, 定义 $L_a: G \rightarrow G$, 其中

$$\forall b \in G, L_a(b) = a * b.$$

定义 $f: G \rightarrow M(G)$: $\forall a \in G, f(a) = L_a$.

则: (1) $\forall u, v \in G$, 有 $L_{u+v} = L_u \circ L_v$. 故 f 是 $(G, *)$ 到 $(M(G), \circ)$ 的同态

(2) 设 $(G, *)$ 是么半群, 么元为 I_G . 则 $f(I_G) = L_{I_G} = id_G$ ($G \rightarrow G$ 的恒双映射)

且 f 是单射

\downarrow identical

(3) 设 $(G, *)$ 是群, 则 $\forall a \in G, L_a: G \rightarrow G$ 是双射, 故 f 是 $(G, *)$ 到 $(\text{Sym}(G), \circ)$ 的群同态.

(1) 设 $u, v \in G, \forall b \in G, L_{u \circ v}(b) = (u * v) * b$

$$(L_u \circ L_v)(b) = L_u(L_v(b)) = L_u(v * b) = u * (v * b)$$

由结合律相等.

$$L_{uv} : L_{uv}$$

(2) $L_G = \text{id}_G, \forall b \in G, L_{I_G}(b) = I_G * b = b \therefore L_G = \text{id}_G$

设 $u, v \in G, f(u) = f(v) \therefore L_u = L_v, L_u(I_G) = L_v(I_G) \therefore u = v$

(3) 设 $a \in G$, 来证 $L_a: G \rightarrow G$ 是双射.

单射. 设 $u, v \in G, L_a(u) = L_a(v) \therefore a * u = v * a$.

向消去律 (左乘 a^{-1}) $\Rightarrow u = v$.

满射. $\forall b \in G, L_a(a^{-1} * b) = a * (a^{-1} * b) = (a * a^{-1}) * b = I_G * b = b$.
[构造]

$$|G| = n, |\text{Sym}(G)| = n!$$

定义. 设 $(G, *)$ 是群, H 是 $(G, *)$ 的子群. 若 $\forall g \in G, \forall a \in H, g * a * g^{-1} \in H$

则称 H 是 $(G, *)$ 的正规子群, 记作 $H \triangleleft G$

(若 $(G, *)$ 交换 $(a * b = b * a)$ $g * a * g^{-1} = a * (g * g^{-1}) = a * I_G = a \in H$)

例. $GL_n(\mathbb{R}) \quad SL_n(\mathbb{R}) = \{A \mid A \in GL_n(\mathbb{R}), \det(A) = 1\}, \quad I_n \in SL_n(\mathbb{R}), \rightarrow \neq \emptyset$

$A, B \in SL_n(\mathbb{R}), \det(A) = \det(B) = 1, \det(AB) = \det(A)\det(B) = 1$.

$\det(A^{-1}) = \det(A)^{-1} = 1$. // 证明 $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

$\forall A \in SL_n(\mathbb{R}), C \in GL_n(\mathbb{R}), \text{看 } CAC^{-1}$

$$\det(CAC^{-1}) = \det(C) \det(A) \det(C^{-1}) = \det(C) \cdot 1 \cdot \det(C^{-1}) = 1$$

$$SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$$

$\{l_G\} \trianglelefteq G \quad G \trianglelefteq G$ 单群：除了 $\{l_G\}$ 和 G 之外，无其它正规子群
 $g * l_G * g^{-1} = g * g^{-1} = l_G$

命题 设 $(G, *)$, (H, Δ) 是群, $f: G \rightarrow H$ 是同态, 记 $\ker(f) = \{a \mid a \in G, f(a) = l_H\}$

则 $\ker(f) \trianglelefteq G$.

证: $\because f(l_G) = l_H, \quad \ker(f) \neq \emptyset$

设 $a, b \in \ker(f) \quad f(a) = f(b) = l_H$

$$f(a * b) = f(a) \Delta f(b) = l_H \Delta l_H = l_H$$

$$f(a^{-1}) = f(a)^{-1} = l_H^{-1} = l_H$$

$$a * b \in \ker(f) \quad a^{-1} \in \ker(f) \quad // \quad \ker(f) \leq G.$$

设 $g \in G, a \in \ker(f)$ 且 $g * a * g^{-1}$

$$f(g * a * g^{-1}) = f(g) * f(a) * f(g^{-1}) = f(g) * l_H * f(g^{-1}) = f(g) * f(g)^{-1} = l_H$$

$$g * a * g^{-1} \in \ker(f)$$

#

$g * a * g^{-1}$: a 关于 g 的共轭元素

相似矩阵 PAP^{-1} 相似于上三角矩阵 $P \begin{pmatrix} a & b \\ c & d \end{pmatrix} P^{-1} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$

陪集 命题 设 $(G, *)$ 群, H 是 $(G, *)$ 的子群, 定义 G 上关系~

$$a \sim b \Leftrightarrow \exists h \in H, \text{s.t. } b = a * h \Leftrightarrow a^{-1} * b \in H.$$

(G, \sim) 等价

若 $a \sim b, c \sim d$, 是否一定有 $a * c \sim b * d$?

事实. 若 $a, c, d \in G, c \sim d$, 则 $a * c \sim a * d$

$\forall c \sim d \quad \exists h \in H, \text{s.t. } d = c * h$

$$a * d = a * (c * h) = (a * c) * h, h \in H.$$

$$\therefore a * c \sim a * d$$

事實 下面2條件等價

(1) $H \triangleleft G$

(2) $\forall a, b, c, d \in G, a \sim b, c \sim d, \text{ 有 } ac \sim bd.$

証: (1) \Rightarrow (2) $\because a \sim b \quad \exists u \in H, \text{s.t. } b = a * u$

$c \sim d \quad \exists v \in H, \text{s.t. } d = c * v$

$$b * d = a * u * c * v = a * (c * c^{-1}) * u * c * v$$

$$= (a * c) * (c^{-1} * u * c) * v$$

$\because u \in H, H \triangleleft G \quad \therefore c^{-1} * u * c \in H, \forall v \in H. \quad \therefore (c^{-1} * u * c) * v \in H.$

$\therefore a * c \sim b * d.$

(tbc)

(共轭元)

称H是G的正规子群，是指H是G的子群，并且 $\forall g \in G, \forall a \in H, g * a * g^{-1} \in H$

记作 $H \triangleleft G$

事实. $H \triangleleft G \Leftrightarrow \forall g \in G, \forall a \in H, g^{-1} * a * g \in H$

$\Rightarrow \forall g \in G, a \in H.$

$$\because g^{-1} \in G, H \triangleleft G \quad \therefore g^{-1} * a * (g^{-1})^{-1} \in H$$

$$\text{但 } (g^{-1})^{-1} = g. \quad \therefore g^{-1} * a * g \in H$$

$\Leftarrow \forall g \in G, a \in H.$

$$\text{对 } g^{-1} \in G, \text{ 有 } (g^{-1})^{-1} * a * g^{-1} \in H$$

$$\text{但 } (g^{-1})^{-1} = g \quad \therefore g * a * g^{-1} \in H$$

$\Rightarrow H \triangleleft G$

设H是G的子群，在G上定义二元关系 $\sim : a \sim b \Leftrightarrow a^{-1} * b \in H \Leftrightarrow \exists h \in H, \text{ s.t. } b = a * h$
 (G, \sim) 等价关系。

$$\forall a \in G, \{b \mid b \in G, a \sim b\} = aH = \{a * h \mid h \in H\}$$

$$\text{特别地, } \{b \mid b \in G, a \sim b\} = H$$

$$\text{若 } a, c, d \in G, c \sim d, \text{ 则 } a * c \sim b * d \quad (\exists h \in H, \text{ s.t. } d = c * h, a * d = (a * c) * h)$$

若 $c \sim d$, 是否有 $c * a \sim d * a$? 不一定

$$d = c * h, h \in H. \quad d * a = c * h * a, \text{ 不能证明}$$

事实. 下面2个论证等价

(1) $H \triangleleft G$

(2) $\forall a, b, c, d \in G. \quad a \sim b, c \sim d, \text{ 则 } a * c \sim b * d$

(1) \Rightarrow (2) $\because a \sim b, c \sim d$

$$\therefore \exists u, v \in H, \text{ s.t. } b = a * u, d = c * v$$

$$a \equiv b \pmod{n}, c \equiv d \pmod{n}$$

$$\text{则 } a + c \equiv b + d \pmod{n}$$

插入公元，找 H 中元素

$$b*d = a*c*u*c*v = a*c*c^{-1}*u*c*v = (a*c)*(c^{-1}*u*c)*v$$

$\because u \in H, H \trianglelefteq G \quad \therefore c^{-1} * u * c \in H. \quad \therefore (c^{-1} * u * c) * v \in H$

$\therefore a*c \sim b*d$

(2) \Rightarrow (1) 取 $g \in G, a \in H$.

$$\therefore l_g \sim a \quad \text{if } \{b \mid b \in G, l_g \sim b\} = H. H \text{ 是 } l_g \text{ 的左阶类}$$

$\therefore g * l_g \sim g * a.$ 由 $g * g^{-1} \sim e$ \rightarrow 由条件

$$\therefore g * g^{-1} \sim g * a * g^{-1} \text{ if } g^{-1} \therefore l_g \sim g * a * g^{-1}$$

$$\therefore g * a * g^{-1} \in H$$

$a \% n = a$ 除 n 的余数

$a = qn+r, q \in \mathbb{Z}, 0 \leq r < n-1$.

$$r = a \% n$$

$$a \equiv a \% (mod \ n)$$

$$x \equiv y \pmod{n}$$

$$0 \leq x, y \leq n-1$$

$$n | (y-x) \quad n | (y-x)$$

$$|y-x| \leq n-1. \quad \therefore y-x=0, y=x$$

$$n \in \mathbb{Z}^+ \quad \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\} \quad (\mathbb{Z}_n, +) \text{ 是群} \quad a \oplus b = (a+b) \% n$$

运算封闭性：余数在 $0 \sim n-1$ 之间

$$\text{结合律} \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$$

$$(a \oplus b) \oplus c \equiv (a \oplus b) + c \pmod{n}$$

$$a \oplus b \equiv a + b \pmod{n}$$

$$(a \oplus b) + c \equiv (a + b) + c \pmod{n}$$

$$\text{左} = (a \oplus b) \oplus c \equiv a + b + c \pmod{n} \quad // \text{由可结合性+}$$

$$\text{右} \quad b \oplus c \equiv b + c \pmod{n}$$

$$a + (b + c) \equiv a + b + c \pmod{n}$$

$$\text{右} = a \oplus (b \oplus c) \equiv a \oplus b \oplus c \pmod{n}$$

$$\therefore \text{左} \equiv \text{右} \pmod{n} \quad \therefore \text{左} = \text{右}$$

幺元：0. $\forall a \in \mathbb{Z}_n, a \oplus 0 = (a+0) \% n = a \% n = a. \quad 0 \oplus a = a$

逆元：0 的逆元是 0. ($0 \oplus 0 = 0$)

$$\text{设 } 1 \leq a \leq n-1 \quad n-a. \quad 1 \leq n-a \leq n-1$$

$$a \oplus (n-a) = (a+(n-a)) \% n = n \% n = 0.$$

交换律 $a \oplus b = (a+b) \% n = (b+a) \% n = b \oplus a$

$$a_1 \oplus a_2 \oplus \cdots \oplus a_m \equiv a_1 + a_2 + \cdots + a_m \pmod{n}$$

$$= (a_1 + a_2 + \cdots + a_m) \% n$$

$$\begin{aligned} x \equiv y \pmod{n} &\Leftrightarrow \\ y - x \in \{nq \mid q \in \mathbb{Z}\} \end{aligned}$$

类比

$$(G, *) , H \triangleleft G , (G, \sim) \quad a \sim b \Leftrightarrow a^{-1} * b \in H \Leftrightarrow \exists h \in H, \text{s.t. } b = a * h$$

$$G \leftrightarrow \mathbb{Z}, \quad H \leftrightarrow \{nq \mid q \in \mathbb{Z}\} \quad T \leftrightarrow [0, 1, \dots, n-1] = \mathbb{Z}_n$$

$$(1) \quad a, b \in \mathbb{Z}_n, \quad a \equiv b \pmod{n} \Rightarrow a = b. \quad \leftrightarrow \rightarrow + \quad \sim \leftrightarrow \equiv \pmod{n}$$

$$(2) \quad \forall k \in \mathbb{Z}, \quad \exists r \in \mathbb{Z}_n \text{ s.t. } k \equiv r \pmod{n} \quad (r = k \% n)$$

对 (G, \sim) , 取定 $T \subseteq G$ 满足 // 每个等价类里取一个, T不唯一

$$(1) \quad \forall a, b \in T, \quad a \sim b \Rightarrow a = b \quad \text{完全等价类, 通过 } \sim \text{ 定义}$$

$$(2) \quad \forall g \in G, \quad \exists a \in T, \text{s.t. } g \sim a$$

在 T 上定义二元运算 (T, \oplus) 存在(2). 唯一(1)

$$\forall a, b \in T \quad a * b \in G, \quad \text{由(1)(2), } \exists ! c \in T, \text{s.t. } a * b \sim c \quad (a \oplus b = a * b)$$

定义 $a \oplus b = c$.

$$\oplus \text{ 是 } T \text{ 上的二元运算} \quad (\forall a, b \in \mathbb{Z}_n : a * b \quad a \oplus b = (a * b) \% n)$$

(T, \oplus) 是群

结合律. $a, b, c \in T$ 要证 $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

$$a \oplus b \sim a * b$$

$$(a \oplus b) * c \sim (a * b) * c$$

$$(a \oplus b) \oplus c \sim (a \oplus b) * c$$

$$\text{故: } \therefore (a \oplus b) \oplus c \sim a * b * c$$

$$a \oplus (b \oplus c) \sim a * (b \oplus c)$$

$$b \oplus c \sim b * c \quad \therefore a * (b \oplus c) \sim a * (b * c)$$

$$\therefore a \oplus (b \oplus c) \sim a * b * c.$$

左~右, 都ET \therefore 左=右.

么元. 由(1)(2), $\exists! w \in T$, s.t. $|_G \sim w$

$$\forall a \in T, |_G \sim w, a *_G \sim a * w, a \sim a * w$$

$$\text{但 } a \in T \quad \therefore a \oplus w = a$$

$$\text{又: } w * a \sim |_G * a = a, a \in T. \quad \therefore w \oplus a = a.$$

逆元. $\forall a \in T$, $\exists a^{-1}$, $\exists! b \in T$, s.t. $b \sim a^{-1}$, $a \oplus b = b \oplus a = w$.

$$\because b \sim a^{-1} : a * b \sim a * a^{-1} = |_G \quad a * b \sim w. \quad \therefore a \oplus b = w.$$

$$\text{同理, } b \oplus a = w \quad \#.$$

群 $(G, *)$, $H \triangleleft G$, 定义 (G, \sim) , $a \sim b \Leftrightarrow a^{-1} * b \in H \Leftrightarrow \exists h \in H$, s.t. $b = a * h$.

取定 $T \subseteq G$, 满足

$$(1) \forall a, b \in T, a \sim b \Rightarrow a = b$$

$$\text{且 } \forall g \in G, \exists! a \in T, \text{s.t. } g \sim a$$

$$(2) \forall g \in G, \exists a \in T, \text{s.t. } g \sim a$$

在 T 上定义二元运算 \oplus

$$\forall a, b \in T, \exists! c \in T, \text{s.t. } a * b \sim c. \quad \text{令 } a \oplus b = c. \quad (a \oplus b \sim a * b)$$

则 (T, \oplus) 是群.

么元: $\exists! w \in T$, s.t. $|_G \sim w$

并且 $f: G \rightarrow T$, $(\forall a \in G, f(a) \in T, f(a) \sim a)$ 是 $(G, *)$ 到 (T, \oplus) 的同态, 且 $\text{ker}(f) = H$.

$$f: G \rightarrow T$$

$$\forall g \in G: \exists! a \in T, \text{s.t. } g \sim a. \quad \text{令 } f(g) = a. \quad \frac{(f(g) \sim g)}{a}$$

对任一二元关系, 不一定群
找到完全代表类后即可映射

II 知道同态，考虑核

$a \sim b, c \sim d, \text{且 } ac \sim bd$ 由 $H \triangleleft G$

f 是 $(G, *)$ 到 (T, \otimes) 的同态，并且 $\ker(f) = H = \{g \mid g \in G, f(g) = 1_T\}$

证：设 $u, v \in G$, 要证 $f(u * v) = f(u) \otimes f(v)$

由 f 的定义, $f(u * v) \sim u * v$. $f(u) \sim u, f(v) \sim v$.

$$\leftarrow f(u) * f(v) \sim u * v \rightarrow f(u * v) \sim f(u) * f(v) \quad \text{ET}$$

$f(u * v) \sim f(u) * f(v)$ 由 def

$$\Rightarrow f(u * v) = f(u) * f(v)$$

来证 $\ker(f) = H$.

$$\forall g \in G, g \in \ker(f) \Leftrightarrow f(g) = 1_T = w.$$

$\Leftrightarrow g \sim w$ (f 的定义)

$\Leftrightarrow g \sim 1_G$ ($w \sim 1_G$) 上证了 w

$\Leftrightarrow g \in H$ (\sim 的定义) $1_G \sim g$, $\text{即 } 1_G * g = g \in H$.

另一种叙述：

$(G, *)$, $H \triangleleft G$

$A, B \subseteq G, AB = \{a * b \mid a \in A, b \in B\} \subseteq G$.

$(AB)C = A(BC) = \{a * b * c \mid a \in A, b \in B, c \in C\} \subseteq G$

$G/H = \{aH \mid a \in G\}, aH = \{a * h \mid h \in H\}$

$(G/H, \otimes) \rightsquigarrow$ 子集之间的乘法

幺元： H 逆元： aH 的逆元为 $a^{-1}H$.

$f: G \rightarrow G/H \quad \forall a \in G, f(a) = aH. f$ 是同态, $\ker(f) = H$.

每个元素是 G 的子集