

$(G, *)$  群  $|_G$  么元

$\emptyset \neq H$  是  $(G, *)$  的子群, 即  $\forall a, b \in H$ , 有  $a * b \in H, a^{-1} \in H$ .  $(H, *)$  成群

固定  $\#(G, *)$ , 子群  $H \leq G$ . 如下定义  $G$  上的二元关系  $\sim$

$\forall a, b \in G, a \sim b \Leftrightarrow a^{-1} * b \in H$

$(G, \sim) = (\mathbb{Z}, \sim)$ ,  $n \in \mathbb{Z}^+$ ,  $H = \{ng \mid g \in \mathbb{Z}\}$ ,  $\sim$  即为模  $n$  同余关系

事实

(1)  $(G, \sim)$  是等价关系

(2)  $\forall a, b \in G, a \sim b \Leftrightarrow \exists h \in H$  s.t.  $b = a * h$

(3) 若  $a^{-1} * b \in H$ , 则  $a^{-1} * b = h \in H$

$$a * h = a * (a^{-1} * b) = (a * a^{-1}) * b = b, h \in H.$$

反之, 若  $b = a * h, h \in H$ ,

$$a^{-1} * b = a^{-1} * (a * h) = (a^{-1} * a) * h = |_G * h = h \in H.$$

(1)  $\forall a, b, c \in G$ .

$$1^\circ a \sim a, a^{-1} * a = |_G \in H$$

$$2^\circ a \sim b \Rightarrow b \sim a \quad a^{-1} * b \in H.$$

$$(a^{-1} * b)^{-1} \in H$$

$$(a^{-1} * b)^{-1} = b^{-1} * (a^{-1})^{-1} = b^{-1} * a \in H. \quad b \sim a$$

$$3^\circ a \sim b, b \sim c. \quad a^{-1} * b \in H, b^{-1} * c \in H$$

$$(a^{-1} * b) * (b^{-1} * c) = a^{-1} * (b * b^{-1}) * c = a^{-1} * c \in H. \quad a \sim c$$

$\therefore \sim$  是等价关系.

$$|aH|=|H|$$

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

$$\text{若 } A = \{a\}, \{a\}B = aB = \{a*b \mid b \in B\}$$

$$(3) \text{ 设 } a \in G, \text{ 则 } \{b \mid b \in G, a \sim b\} = aH = \{a*h \mid h \in H\}$$

( $a$ 所在的等价类 =  $a$ 所在的关于  $H$  的右陪集)

由(2),  $a \sim b \Leftrightarrow \exists h \in H, \text{ s.t. } b = a * h$ .

$$G/H = \{\text{全体 } \sim \text{下的等价类}\}$$

$$= \{aH \mid a \in G\} \quad (G \text{ 关于 } H \text{ 的左陪集分解})$$

$$(xH \cap yH = \emptyset \Leftrightarrow xH = yH \Leftrightarrow x^{-1}y \in H.)$$

### Lagrange 定理

$$\text{设 } G \text{ 有限, 则 } |G| = |H| |G/H|$$

$$\text{等价地, 有 } \frac{|G|}{|H|} = |G/H|$$

$$\text{特别地, 有 } |H| \mid |G| \quad (\text{子群元素个数整除原大群 })$$

证:  $(G, \sim)$  是等价关系

$G/H$  中全体成员做成  $G$  的不变并分解

$$|G| = \sum_{A \in G/H} |A|$$

对任一  $a \in G$ , 断言  $|aH| = |H|$  (群运算有消去律,  $a * h_1 = a * h_2 \Leftrightarrow h_1 * h_2^{-1} \in H$ , 元素个数不变)

$$|G| = \sum_{A \in G/H} |A| = |G/H| |H| \quad \#$$

任给  $d \mid |G|$ ,  $(G, *)$  一定有  $d$  阶子群吗? 不一定

若有如比  $G$ , 称为 Lagrange 群.

最早反例: 存在 12 阶群, 无 6 阶子群

$$12 = 2^2 \times 3 \quad \text{有 } 2, 2^2, 3 \text{ 阶子群}$$

推论: 设  $G$  有限且  $|G|$  是素数, 则  $(G, *)$  的子群只有 2 个:  $\{e\}$  和  $G$ . (平凡的子群)

证: 设  $H$  是  $(G, *)$  的子群

由 Lagrange 定理,  $|H| \mid |G|$ , 但  $|G|$  是素数  
 $\therefore |H|=1$  或  $|H|=|G|$   
 $\downarrow$   
 $H \in H, H = \{e\}, \quad H=G \quad \#$

### ④ 证

反之, 若  $G$  的子群只有  $\{e\}$  和  $G$ , 则  $G$  有限且  $|G|$  是素数.

### 完全对称

右陪集  $Ha = \{h * a \mid h \in H\} \quad a \approx b \Leftrightarrow \exists h \in H, \text{s.t. } b = h * a \Leftrightarrow a * b^{-1} \in H$

$$\begin{aligned} 2^2 &= 2 \times 2 \\ 2^3 &= 2 \times 2 \times 2 \\ 2^2 &= \frac{1}{2^2} = \left(\frac{1}{2}\right)^2 \\ 2^{\frac{1}{2}} &= \sqrt{2} \\ 2^2 \times 2^3 &= 2^{2+3} = 2^5 \\ (2^2)^3 &= 2^{2 \times 3} = 2^6 \end{aligned}$$

元素的幂  
 $(G, *)$  是半群

$$a^2 = a * a$$

$$a^3 = a^2 * a = a * a \quad \text{if } n \in \mathbb{Z}^+$$

$$n \in \mathbb{Z}^+, a^n = \underbrace{a * a * \dots * a}_{n \uparrow} = a^{n-1} * a \quad (n \geq 2)$$

$$\forall a \in G, a^1 = a.$$

$$\forall k \in \mathbb{Z}^+, a^{k+n} = a^k * a^n$$

事实 设  $m, n \in \mathbb{Z}^+$ , 则  $a^m * a^n = a^{m+n}$

$$(a^m)^n = a^{mn}$$

归纳法 ✓ 直观上,  $\underbrace{a * \dots * a}_{m \uparrow} * \underbrace{a * \dots * a}_{n \uparrow} = a^{m+n}$

$$(a^m)^n = \underbrace{a^m * a^m * \dots * a^m}_{n \uparrow}$$

$$= \underbrace{a^{k-1} * a * \dots * a}_{m \uparrow} * \underbrace{a^{k-1} * a * \dots * a}_{m \uparrow} = a^{mn}$$

$\# mn \uparrow$ .

## 快速幂 (平方模乘)

算  $a^n$ , 需要做几次 \* 运算?

$a \cdot a = a^2 \quad a^3 = a^2 * a \quad a^4 = a^2 * a^2 \dots \quad a^{k+1} = a^k * a$ . 并到  $a^n$ , 用  $n-1$  次 \* 运算

$\log(n)$  级别的次数? 二进制:  $n = a_0 \cdot 2^0 + a_1 \cdot 2^1 + \dots + a_k \cdot 2^k$ ,  $a_i \in \{0, 1\}$ ,  $a_k = 1$

$\downarrow n$  的位数

$a^2 = a * a \quad 1$  次

$a^4 = a^2 * a^2 \quad + 1$  次

$a^8 = a^4 * a^4 \quad + 1$  次

- 一般地,  $a^{2^m} = a^{2^k} * a^{2^k} \quad + 1$  次

$m$  次运算, 得到  $(a, a^2, a^4, \dots, a^{2^k}) = (a^{2^t} \mid 0 \leq t \leq m)$

$n = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \dots + b_k \cdot 2^k$ ,  $b_k = 1$ ,  $b_i \in \{0, 1\}$

$= \sum_{i \in I} 2^i$ , 其中  $I = \{i \mid b_i = 1\}$

$a^n = a^{\sum_{i \in I} 2^i} = \prod_{i \in I} a^{2^i}$

先做  $k-1$  次  $a$  的平方运算, 得  $(a, a^2, \dots, a^{2^k})$ , 再算  $\prod_{i \in I} a^{2^i}$ , 需要  $|I|-1$  次运算

(注意  $k-1+|I|-1=k+|I|-2$  次的运算出  $a^n$ ).

$$\leq k + (k+1) - 2 = 2k-1, \quad k: \log_2 n$$

$(G, *)$  是么群, 证明 | $G$ |

$a^0 = |G|$  (人为定义)

$a^{m+n} = a^m * a^n \quad \left. \right)$  扩展  $m, n \neq 0$  情况

$(a^m)^n = a^{mn} \quad \forall m, n \in \mathbb{N}$

$(G, *)$  是群

$$a \in G, m \in \mathbb{N}. a^{-m} = \underline{(a^{-1})^m} = (a^m)^{-1}$$

④ 驗

用  $(x * y)^{-1} = y^{-1} * x^{-1}$  與  $m$  有關

$$a^{m+n} = a^m * a^n$$

$$(a^m)^n = a^{mn}, \text{ 對 } m, n \in \mathbb{Z}$$

$(G, *)$  群 元元  $|_G$

设  $\{H_i \mid i \in I\}$  是一组子群，则  $\bigcap_{i \in I} H_i$  是子群

设  $S \subseteq G$ ，总有唯一的子群  $H$  满足

$\parallel H: S$  生成的子群

1)  $S \subseteq H$  (2)  $\forall K$  是子群， $S \subseteq K \Rightarrow H \subseteq K$ .  $H = \langle S \rangle$

$$\langle S \rangle = \{a^{c_1} * a^{c_2} * \dots * a^{c_n} \mid n \in \mathbb{N}, \text{ 每 } a \in S, \text{ 每 } c_i = \pm 1\}$$

$$\begin{aligned} a \in G, a^0 &= 1_G, a^1 = a, \forall m \in \mathbb{Z}^+, a^{m+1} = a^m * a, \forall m \in \mathbb{N}, a^{-m} = (a^1)^m = (a^m)^{-1}, \\ a^{m+n} &= a^m * a^n, (a^m)^n = a^{mn}, \forall m, n \in \mathbb{Z}. \end{aligned}$$

-1元素生成的子群

$$\text{设 } a \in G, \{a\} \quad \langle \{a\} \rangle = \{a\} \quad \langle a \rangle = \{a^j \mid j \in \mathbb{Z}\}$$

1° 单独验证右边是子群.  $\forall i, j \in \mathbb{Z}$ .  $a^i * a^j = a^{i+j} \in \langle a \rangle$

$$(a^i)^{-1} = a^{-i} \in \langle a \rangle.$$

$$\therefore \langle a \rangle \leq G.$$

2° 设  $H$  是子群，且  $a \in H$ .

$\forall m \in \mathbb{N}$ . 规定  $a^0 = a * a \in H$ ,  $a^1 = a^0 * a \in H$ , ...  $a^{m+1} = a^m * a \in H$

$$a^{-m} = (\underbrace{a^m}_{\in H})^{-1} \in H \quad \therefore \langle a \rangle \leq H \quad \therefore \langle a \rangle \text{ 是 } a \text{ 在其中的最小子群}$$

考虑：是否有可能  $i \neq j$ ，但  $a^i = a^j$ ，或者只要  $i \neq j$ ，就有  $a^i \neq a^j$ ? 都可能

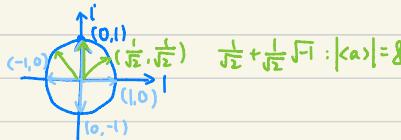
例.  $(\mathbb{C} - \{0\}, \times)$  群.  $(\mathbb{C}^*, \times)$  元元:

$$\forall a \in \mathbb{C}, a \neq 0, \langle a \rangle = \{a^j \mid j \in \mathbb{Z}\}$$

$$1^\circ a = -1, \langle -1 \rangle = \{-1, 1\}$$

$$3^\circ a = 2, \langle 2 \rangle = \{2^i \mid i \in \mathbb{Z}\}$$

$$2^\circ a = \sqrt{-1}, \langle \sqrt{-1} \rangle = \{\sqrt{-1}, -1, -\sqrt{-1}, 1\}$$



考虑有结合律但无交换律的例子：①

② 双射下的复合

$$(\mathbb{C}, \times) \text{ 中: } o(A_1) = 2, \quad o(\sqrt{-1}) = 4$$

$$o\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right) = 8.$$

$GL_2(\mathbb{R}) = \{A \mid A \text{ 是 } 2 \text{ 阶可逆实方阵}\}$

$$A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$A_1^2 = I_2 \quad A_2^j = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \quad \forall j \in \mathbb{Z}.$$

$$\langle A_1 \rangle = \{A_1, I_2\} \quad \langle A_2 \rangle = \left\{ \left( \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \mid j \in \mathbb{Z} \right) \right\} \text{ 无限个.}$$

### 元素的阶

设  $a \in G$ ,

(1) 若  $\exists n \in \mathbb{Z}^+$ , s.t.  $a^n = I_G$ , 则称  $a$  是  $(G, \cdot)$  中的有限阶元, 并记:

$$o(a) = \min \{m \mid m \in \mathbb{Z}^+, a^m = I_G\} \Rightarrow a \text{ 在 } (G, \cdot) \text{ 中的阶.}$$

(2) 若  $\forall n \in \mathbb{Z}^+$ , 均有  $a^n \neq I_G$ , 则称  $a$  是  $(G, \cdot)$  中的无限阶元,  $o(a) = +\infty$

事实 若  $a \in G$  是无限阶元, 则  $\forall i, j \in \mathbb{Z}$ ,  $a^i = a^j \Rightarrow i = j$ .  $\mathbb{Z} \setminus \{0\}$

证:  $\forall n \in \mathbb{Z}^+$ ,  $a^n = I_G$ .  $\therefore (a^n)^{-1} = I_G$ ,  $\text{If } a^{-n} \neq I_G$ .  $\forall h \in \mathbb{Z}^+ \cup \mathbb{Z}^-$ ,  $a^h \neq I_G$

$$\text{设 } i, j \in \mathbb{Z}, a^i = a^j, \text{ 则 } a^{i-j} = a^i * a^{-j} = a^{-j+i} = a^{j-i}$$

$$= (a^i)^{-1} \quad \text{I.G.} \quad \therefore a^{j-i} = I_G \quad \therefore j-i=0, i=j.$$

设  $a \in G$  是有限阶元, 记  $o(a) = m \in \mathbb{Z}^+$ , 则

$$(1) \forall j \in \mathbb{Z}, a^j = I_G \Leftrightarrow m \mid j$$

$$(2) \forall i, j \in \mathbb{Z}, a^i = a^j \Leftrightarrow m \mid (j-i) \Leftrightarrow (i \equiv j \pmod m)$$

$$(3) \langle a \rangle = \{a^j \mid j \in \{0, 1, \dots, m-1\}\}, \# \langle a \rangle = m = o(a).$$

特别地,  $\forall i, j \in \{0, 1, \dots, m-1\}$ ,  $a^i = a^j \Rightarrow i = j$ .

$$(1) \Leftrightarrow \text{若 } m \mid j, \text{ 即 } j = ml, l \in \mathbb{Z}. \quad a^j = a^{ml} = (a^m)^l = I_G^l = I_G = (a^m)^l$$

$$\Rightarrow \text{设 } j = qr + r, q \in \mathbb{Z}, 0 \leq r \leq m-1$$

$$|_G = \alpha^j = \alpha^{qm+r} = \alpha^{qm} * \alpha^r = (\alpha^m)^q * \alpha^r = |_G^q * \alpha^r = \alpha^r.$$

$$\alpha^r = |_G, \quad m = o(\alpha) = \min\{n | n \in \mathbb{Z}^+, \alpha^n = |_G\}.$$

$$0 \leq r \leq m-1, \quad r \in \mathbb{Z}^+.$$

$$\therefore r=0, \quad j=qm, \quad m|j.$$

④

方证:  $H = \{i \mid i \in \mathbb{Z}, \alpha^i = |_G\}$ , 证明  $H$  是  $(\mathbb{Z}, +)$  的子群, 且  $H = \{mq \mid q \in \mathbb{Z}\}$

$$(2) \alpha^i = \alpha^j \Leftrightarrow (\alpha^i)^{-1} * \alpha^i = (\alpha^j)^{-1} * \alpha^j$$

$$\Leftrightarrow |_G = \alpha^{-i} * \alpha^i = \alpha^{(i-j)} = \alpha^{j-i}$$

$$\Leftrightarrow |_G = \alpha^{j-i} \Leftrightarrow m|(j-i)$$

$$(3) \text{ 设 } j \in \mathbb{Z}, \quad j = qm+r, \quad q \in \mathbb{Z}, \quad 0 \leq r \leq m-1 \quad \left[ \begin{array}{c} |\alpha^0, \alpha^1, \dots, \alpha^{m-1}| \\ \hline \end{array} \right]$$

$$m|(j-r) \quad \therefore \alpha^r = \alpha^j. \quad // \text{说明 } \alpha^r \text{ 落在 } \langle \alpha \rangle \text{ 中.}$$

$$\text{设 } i, j \in \{0, 1, \dots, m-1\} \quad \alpha^i = \alpha^j \Leftrightarrow i \equiv j \pmod{m} \Rightarrow i = j$$

$$// i \equiv j \pmod{m} \Leftrightarrow m|(j-i) \quad |j-i| \leq m-1. \quad \text{故 } j-i=0, \quad i=j$$

#.

定义. 循环群 Cyclic Group

若  $\exists a \in G$ , st.  $G = \langle a \rangle$ , 则称  $(G, *)$  是循环群. // 判断循环群: 看

同态, 同构

设  $(G, *)$  和  $(H, \Delta)$ , 其中  $*$  和  $\Delta$  分别是  $G$  和  $H$  上的二元运算,  $f: G \rightarrow H$

若  $\forall a, b \in G$ , 有  $f(a * b) = f(a) \Delta f(b)$ , 则称  $f$  是  $(G, *)$  到  $(H, \Delta)$  的同态.

若  $f: G \rightarrow H$  还是双射, 则称  $f$  是  $(G, *)$  到  $(H, \Delta)$  的同构.

例.  $((1, -1), *)$  (模 2 加) 同构

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

$f: \{0, 1\} \rightarrow \{\pm 1\}, \quad f(0) = 1, \quad f(1) = -1. \quad f$  是  $(\{0, 1\}, \oplus)$  到  $((1, -1), *)$  的同构.

$$f(0 \oplus 0) = f(0) = f(0) * f(0) \quad 1 = 1 * 1$$

$$f(0 \oplus 1) = f(1) = f(0) * f(1) \quad -1 = 1 * (-1)$$

$$f(1 \oplus 1) = f(0) = f(1) * f(1) \quad 1 = (-1) * (-1)$$

例.  $(\mathbb{R}, +), (\mathbb{R}^+, \times)$

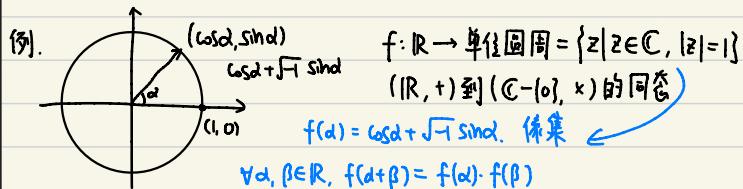
$$f: \mathbb{R} \rightarrow \mathbb{R}^+, f(x) = 2^x \text{ 双射易证.}$$

$f$  是  $(\mathbb{R}, +)$  到  $(\mathbb{R}^+, \times)$  的同构.

$$\forall x, y \in \mathbb{R}, f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$$

$\log_2: \mathbb{R}^+ \rightarrow \mathbb{R}$  是  $(\mathbb{R}^+, \times)$  到  $(\mathbb{R}, +)$  的同构, 且  $\log_2 = f^{-1}$ .

$$\log_2(ab) = \log_2 a + \log_2 b$$



$$\forall \alpha, \beta \in \mathbb{R}, f(\alpha + \beta) = f(\alpha) \cdot f(\beta)$$

$$\cos(\alpha + \beta) + \sqrt{-1} \sin(\alpha + \beta) = \underline{\cos \alpha \cos \beta - \sin \alpha \sin \beta} + \sqrt{-1} (\sin \alpha \cos \beta + \cos \alpha \sin \beta)$$

$$= \cos \alpha (\cos \beta + \sqrt{-1} \sin \beta) + \sqrt{-1} \sin \alpha (\cos \beta + \sqrt{-1} \sin \beta) = \bar{z} = f(\alpha) \cdot f(\beta)$$

$f: [0, 2\pi] \rightarrow \text{单位圆周的--对应}$

例.  $f: \mathbb{C} \rightarrow M_{2 \times 2}(\mathbb{R}) \quad f(a + \sqrt{-1} b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \rightarrow$  单射.

$$\forall \alpha, \beta \in \mathbb{C}, f(\alpha + \beta) = f(\alpha) + f(\beta) \quad \text{④ 验} \quad \text{但不是双射}$$

$$f(\alpha \beta) = f(\alpha) f(\beta) \quad // 同时成立 2 种运算$$

$$\alpha = a + \sqrt{-1} b, \beta = c + \sqrt{-1} d,$$

$$\alpha \beta = ac - bd + \sqrt{-1}(ad + bc)$$

$$f(\alpha) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, f(\beta) = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}, f(\alpha) f(\beta) = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix}$$

$$f(\alpha \beta) = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix} \quad \equiv$$

$$f(\alpha \beta) = \alpha f(\beta), \forall \alpha \in \mathbb{R}, \beta \in \mathbb{C}, \text{ 线性映射}$$