

$(\mathbb{Z}, +)$ —— 是一个循环群，由 1 生成

子群

↓

$$2 = 1+1$$

$$3 = 2+1 = 1+1+1$$

$$m \in \mathbb{Z}^+ \quad m = \underbrace{1+1+\dots+1}_{m \uparrow} = (m-1)+1 \quad \text{从整数用 0 截断再加 0.}$$

带余除法：设 $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}$, 则 $\exists q \in \mathbb{Z}$, $r \in \{0, 1, \dots, a-1\}$, s.t. $b = qa+r$. 并且满足上述条件的 (q, r) 是唯一的.

唯一性 设还有 $q' \in \mathbb{Z}$, $r' \in \{0, 1, \dots, a-1\}$, s.t. $b = q'a+r'$, 来证 $q=q'$, $r=r'$.

$$q'a+r'=qa+r$$

$$(q'-q)a = r-r' \quad |r-r'| = |q-q'|a$$

$$0 \leq r, r' \leq a-1 \quad |r-r'| \leq a-1 < a \quad |q-q'|a < a. \quad |q-q'| < 1.$$

$$\text{而 } q, q' \in \mathbb{Z}. \quad |q-q'| = 0. \Rightarrow |r-r'| = 0.$$

$$\therefore q'=q, r'=r.$$

命题 设 $A \subseteq \mathbb{Z}^+$, $A \neq \emptyset$, 且满足

$$(1) \forall a, b \in A, a+b \in A$$

对加、减法封闭

$$(2) \forall a, b \in A, a < b, b-a \in A$$

$$\text{则 } \exists c \in \mathbb{Z}^+, \text{s.t. } A = \{cq \mid q \in \mathbb{Z}^+\}$$

证: $\because A \neq \emptyset \therefore \exists c \in A$ 是 A 的最小数.

$$\text{下证 } A = \{cq \mid q \in \mathbb{Z}^+\}$$

先说右 $\subseteq A$. //c 的所有倍数在 A 中

$$c \in A, 2c = c+c \in A, 3c = 2c+c \in A.$$

$$\text{对 } g \in \mathbb{Z}^+, (g+1)c = \underbrace{gc}_{\in A} + \underbrace{c}_{\in A}$$

再说 $A \subseteq \mathbb{Z}$. $\forall b \in A$, $b \neq c$ 作带余除法 $b = qc + r$, $0 \leq r \leq c-1$, $q \in \mathbb{Z}$.
 $\therefore c$ 是 A 中最小数 $b > c \Rightarrow q \in \mathbb{Z}^+$, $q \in A$.

反证. 反设 $r \neq 0$. 由 $0 \leq r \leq c-1 \Rightarrow 1 \leq r \leq c-1$.

$r = b - qc \geq 1$, $b > qc$, $b \in A$, $qc \in A$. 由(1), $b - qc \in A$. $b \neq qc$.

但 c 是 r 的最小数, 而 $r \in A$, $r < c$.

$$\Rightarrow r = 0, b = qc, q \in \mathbb{Z}^+$$

$\therefore A = \text{右}$

#

例. 设 X 是一个 n 元有限集, $\sigma: X \rightarrow X$ 双射. $y \in X$

$$A = \{l | l \in \mathbb{Z}^+, \sigma^l(y) = y\} \quad f^i = f \circ f \circ \dots \circ f, f^0 = f$$

$$y, \underbrace{\sigma(y), \sigma^2(y), \dots, \sigma^n(y)}_{n+1 \text{ 个}} \in X, |X| = n.$$

$$\exists 0 \leq i < j \leq n, \text{ s.t. } \underline{\sigma^i(y)} = \sigma^j(y) = \underline{\sigma^i(\sigma^{j-i}(y))}$$

但 σ 是双射, σ^i 也是.

$$y = \sigma^{j-i}(y), 1 \leq j-i \leq n, j-i \in A.$$

设 $a, b \in A$, 来说明 $a+b \in A$; $a < b \Rightarrow b-a \in A$.

$$\sigma^a(y) = y, \sigma^b(y) = y.$$

$$\sigma^{a+b}(y) = \sigma^a(\sigma^b(y)) = \sigma^a(y) = y. \quad a+b \in A.$$

设 $a < b$, 来说明 $b-a \in A$, $\sigma^{b-a}(y) = \sigma^{b-a}(\sigma^a(y)) = \sigma^b(y) = y$.

若 c 是 A 中最小数, 则 $A = \{cq | q \in \mathbb{Z}^+\}$.

$y, \sigma(y), \sigma^2(y), \dots, \sigma^{c-1}(y)$ 两两不同.

σ 关于 y 的轮换

例. 设 X 是有限集. (a_1, a_2, \dots, a_n) 是 X 上的序列

$$(a_n, a_1, a_2, \dots, a_{n-1})$$

$$(a_{n-1}, a_n, a_1, \dots, a_{n-2})$$

...
↓
...
固定 (a_1, \dots, a_n)

$$(a_{n-k+1}, \dots, a_n, a_1, \dots, a_{n-k})$$

固定 (a_1, \dots, a_n)

$A = \{l \mid l \in \mathbb{Z}^+, (a_1, \dots, a_n) \text{ 在 } l \text{ 次操作后变回自身}\}$

$n \in A$. A 满足条件(1)(2).

$A = \{cq \mid q \in \mathbb{Z}^+\}$, c 是 A 的最小数, $c \mid n$.

$(a_1, a_2, \dots, a_n) = (a_1, \dots, a_c, a_1, \dots, a_c, a_1, \dots, a_c, \dots, a_1, \dots, a_c)$

由 $\frac{n}{c}$ 个 a_1, \dots, a_c 拼接而成.

#

$(1, 2, 3, 1, 2, 3) \quad c=3. \quad (1, 2, 1, 2, 1, 2) \quad c=2.$ 周期

$(1, 2, 3, 4, 5, 6) \quad c=6.$

\mathbb{Z} 上 +: 群.

\mathbb{Z} 上 +: 半群

好证 ←

也可用证明题的方法用
带余除法做.

定理 ($(\mathbb{Z}, +)$ 的子群)

(1) 设 $H \subseteq \mathbb{Z}$, $H \neq \emptyset$, 且 $\forall a, b \in H$, 总有 $a+b \in H, -a \in H$.

则 $\exists c \in \mathbb{N}$ s.t. $H = \{cq \mid q \in \mathbb{Z}\}$.

(2) 设 $c \in \mathbb{Z}$, $H = \{cq \mid q \in \mathbb{Z}\}$, 则 $\forall a, b \in H$, 总有 $a+b \in H, -a \in H$.

证明: (1) 先证 $0 \in H$

$\because H \neq \emptyset \therefore \exists x \in H \therefore -x \in H \therefore x+(-x)=0 \in H$.

记 $A = H \cap \mathbb{Z}^+$, 分两种情况讨论.

① 若 $A = \emptyset$, 则 $H = \{0\}$, 于是取 $c=0$ 即可.

② 设 $a < 0$, $a \in H \Rightarrow -a \in H \cap \mathbb{Z}^+$, 矛盾.

2° 若 $A \neq \emptyset$, 则 $\exists c \in \mathbb{Z}^+, s.t. A = \{cq \mid q \in \mathbb{Z}^+\}$. // 上述命题已证.

事实上, $H = \{cq \mid q \in \mathbb{Z}\}$

$\forall q \in \mathbb{Z}^+, cq \in H, -q \in H, 0 \in H$.

$\forall h \in H, h > 0 \Rightarrow h \in A \Rightarrow h \in \mathbb{N}$.

$h = 0 \Rightarrow h \in \mathbb{N}$

$h < 0 \Rightarrow -h \in H \cap \mathbb{Z}^+ = A$

$\Rightarrow -h \in \mathbb{N} \Rightarrow h \in \mathbb{N}$. #.

设 $(G, *)$ 是一个群, $H \subseteq G$. 称 H 是 G 的子群, 是指 H 满足:

(1) $H \neq \emptyset$

(2) $\forall a, b \in H, a * b \in H \quad \Leftrightarrow (H, *)$ 是群

(3) $\forall a \in H, a^{-1} \in H \quad (a * a^{-1} = a^{-1} * a = l_G)$

回忆: \mathbb{R}, \mathbb{R}^n 称 $U \subseteq \mathbb{R}^n$ 是一个 \mathbb{R}^n 的子空间, 若
线性空间

(1) $U \neq \emptyset$ (2) $\forall x, y \in U, x + y \in U$ (3) $\forall a \in \mathbb{R}, x \in U, ax \in U$

且满足

4条

事实. 若 H 是 $(G, *)$ 的子群, 则 $l_G \in H$. 并且 $(H, *)$ 是群.

证: $\because H \neq \emptyset \therefore \exists x \in H \therefore x^{-1} \in H \therefore x * x^{-1} \in H$. 即 $l_G \in H$.

$(H, *)$ 符合群的定义. ① * 在 H 上有定义, 由(2), 封闭

② 结合律: 由 G 继承

③ 元元: $l_G \in H$

④ 逆元: 由(3)

消去律: $a*b = a*c \Rightarrow b=c$
同时左乘 a^{-1} 消去

事实. 设 $H \subseteq G$, 且 $(H, *)$ 是群. 则 H 是 $(G, *)$ 的子群

证: (1) $H \neq \emptyset$, 至少有么元

(2) \checkmark $(H, *)$ 是群, 则 $*$ 有定义, 封闭

(3) 先说 $|_G \in H$

$\because (H, *)$ 是群 $\therefore \exists |_H \in H$, s.t. $\forall a \in H$, $a * |_H = a$.

$|_H * |_H = |_H$. 又 $|_H \in G$. $|_H * |_G = |_H$

$\therefore |_H * |_H = |_H * |_G$. 由 $(G, *)$ 的消去律

$\Rightarrow |_H = |_G \in H$.

$\forall a \in H$. $\because (H, *)$ 是群, $|_G \in H$ 是其么元. $\exists b \in H$, s.t. $a * b = |_G$.

另一方面, $a * a^{-1} = |_G$. $\therefore a * b = a * a^{-1}$.

由 $(G, *)$ 中的消去律, $b = a^{-1} \in H$. #.

回忆

\mathbb{R}^n U, V 是 \mathbb{R}^n 的子空间

$U \cap V$ 是子空间, $U+V$ 是子空间 $U+V = \{x+y \mid x \in U, y \in V\}$

$\dim(U \cup V) + \dim(U \cap V) = \dim(U) + \dim(V)$

子群不用再用群公理验证。
H继承了大群的二元运算。

- (G, *) 群 $H \subseteq G$ H 是 $(G, *)$ 的子群 $\Leftrightarrow (H, *)$ 是群
- 称 H 是 $(G, *)$ 的子群，若 H 是 ... 子群 $\Rightarrow \{e\} \in H$.
- (1) $H \neq \emptyset$
 - (2) $\forall a, b \in H, a * b \in H$.
 - (3) $\forall a \in H, a^{-1} \in H$.

回忆 \mathbb{R}^n . U, V 是子空间.

$$U \cap V$$

$$U + V = \{u + v \mid u \in U, v \in V\}$$

$$\dim(U \cap V) + \dim(U + V) = \dim U + \dim V$$

记 $\{H \subseteq G \mid H$ 是 G 的子群

子群的交

- (1) $A \subseteq G, B \subseteq G$, 则 $A \cap B \subseteq G$ $\{x \mid \forall i \in I, x \in A_i\}$
- (2) $(A_i \mid i \in I)$ 是 G 的一组子群. ($I \neq \emptyset$, 且 $\forall i \in I, A_i \subseteq G$) $\cap_{i \in I} A_i \subseteq G$.
证: (1) $\{g \in A, g \in B \Rightarrow \{g \in A \cap B\}$. $A \cap B \neq \emptyset$

$$\forall a, b \in A \cap B$$

$$a \in A, A \subseteq G. \quad a * b \in A$$

$$b \in B, B \subseteq G. \quad a * b \in B \quad \therefore \underline{a * b \in A \cap B}.$$

$$a \in A, A \subseteq G. \quad a^{-1} \in A$$

$$a \in B, B \subseteq G. \quad a^{-1} \in B \quad \therefore \underline{a^{-1} \in A \cap B}. \text{ 同理, } b^{-1} \in A \cap B.$$

$$(2) \text{ 1. } \forall i \in I, A_i \subseteq G \Rightarrow \{e\} \in A_i. \quad \therefore \{e\} \in \cap_{i \in I} A_i.$$

$$\text{2. } \exists a, b \in \cap_{i \in I} A_i. \quad \forall i \in I, A_i \subseteq G. \quad a, b \in A_i, a * b \in A_i, a^{-1} \in A_i, b^{-1} \in A_i \cap B.$$

$$\therefore a * b \in \cap_{i \in I} A_i, a^{-1} \in \cap_{i \in I} A_i, b^{-1} \in \cap_{i \in I} A_i$$

回忆 \mathbb{R}^n . 包含的最小空间
 $x \in \mathbb{R}^n, \{x\}$ 生成的子空间为
 $\{ax \mid a \in \mathbb{R}\}$ // 直线
 $x, y \in \mathbb{R}^n, \{x, y\} \dots$
 $\{ax + by \mid a, b \in \mathbb{R}\}$ // 平面
 包含 x, y 的 min 空间

$A \leq G, B \leq G, A \cup B$? 类似于子空间的和?
 任取 $S \subseteq G$. 考虑由 S 生成的子群, 称 $H \leq G$ 是 S 在 $(G, *)$ 中生成的子群, 是指
 (1) $H \leq G, S \subseteq H$
 (2) $\forall k \leq G, S \subseteq k$ 有 $H \subseteq k$ // H 是(1)中最小的
 命题: 设 $S \subseteq G$, 则 S 在 $(G, *)$ 中生成的子群存在且唯一, 常记作 $\langle S \rangle$.
 证: 唯一性. 设 H_1, H_2 都是 S 在 $(G, *)$ 中生成的子群.
 由(2), $H_1 \leq H_2, H_2 \leq H_1 \therefore H_1 = H_2$.
 考虑 $T = \{H \mid H \leq G, S \subseteq H\}$
 ★ 断言: $T \neq \emptyset$, 且 $\bigcap_{H \in T} H$ 就是 S 在 $(G, *)$ 中生成的子群
 $G \leq G, S \subseteq G \Rightarrow G \in T$.
 $\bigcap_{H \in T} H \leq G$ ($\forall H \in T, H \leq G$, 且子群对 \cap 封闭)
 $S \subseteq \bigcap_{H \in T} H$ ($\forall H \in T, S \subseteq H$)
 $\forall k \leq G, S \subseteq k \quad k \in T \quad \bigcap_{H \in T} H \subseteq k \quad \#$

$S \subseteq G$, 则 $\langle S \rangle = \{a_1^{c_1} * a_2^{c_2} * \dots * a_n^{c_n} \mid \forall i \in \{1, 2, \dots, n\}, c_i \in \mathbb{Z}\}$
 e.g. $S = \{a, b\} \quad a * \dots * a * b * \dots * b, \quad a * b * a * b \dots$ (不是交换律)

$(G, *)$ 设 $a, b, c \in G$.

- (1) $(a * b)^{-1} = b^{-1} * a^{-1}$
- (2) $(a^{-1})^{-1} = a$
- (3) $a * b = c \iff b = a^{-1} * c \iff a = c * b^{-1}$.

证: (1) $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * |_G * a^{-1} = a * a^{-1} = |_G$.
 $\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

$(b^{-1} * a^{-1})$ 同理验证.

定义 + 消去律

$$(1) a * a^{-1} = a^{-1} * a = \text{Id}, \quad (a^{-1})^{-1} * (a^{-1}) = a^{-1} * (a^{-1})^{-1} = \text{Id}.$$

$$a * a^{-1} = (a^{-1})^{-1} * a^{-1}. \Rightarrow a = (a^{-1})^{-1}$$

$$(2) a * b = c, \quad a^{-1} * c = a^{-1} * (a * b) = (a^{-1} * a) * b = \text{Id} * b = b.$$

$$c * b^{-1} = (a * b) * b^{-1} = a * (b * b^{-1}) = a * \text{Id} = a.$$

G 有限, $B \subseteq G$, $|B| \mid |G|$

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

$A = \{a\}, B \subseteq G$. $\{a\}B = aB = \{a * b \mid b \in B\}$. B 的一个左陪集.

$\| A \subseteq G, B \subseteq G$ 不能保证 $AB \subseteq G$. 无交换律 $(a_1 * b_1) * (a_2 * b_2)$

有限,

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

$$|AB| / |A \cap B| = |A| / |B|$$

$$\dim(U+V) + \dim(A \cap B) = \dim U + \dim V$$

命题. 设 $A \subseteq G, B \subseteq G$, 则下面三个条件等价.

$$(1) AB = \{a * b \mid a \in A, b \in B\} \subseteq G. \quad \text{用子群 def 验证}$$

④ 验证

$$(2) \forall b \in B, \exists a \in A, \text{ 有 } b * a \in AB \quad (\text{即 } BA \subseteq AB)$$

$$(3) AB = BA$$

④ 用 def 验

设 $A \subseteq G, B \subseteq G$, 则 $A \cup B \subseteq G \Leftrightarrow A \subseteq B$ 或 $B \subseteq A$. $\| \cup$ -一般不封闭, 产生了新的

同余

$n \in \mathbb{Z}^+$, 对 $a, b \in \mathbb{Z}$, 若 $n \mid (b-a)$, 则称 a 和 b 模 n 同余, 记作: $a \equiv b \pmod{n}$

等价关系 $\left\{ \begin{array}{l} (1) a \equiv a \pmod{n} \quad \text{自反} \\ (2) a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n} \quad \text{对称} \\ (3) a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n} \quad \text{传递} \end{array} \right.$

⑤ 验 (1)~(4)

(5) ①

$$(1) a \equiv a \pmod{n}$$

$$(2) a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$$

$$(3) a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$$

$$(4) a \equiv b \pmod{n} \Leftrightarrow a \% n = b \% n.$$

$$(5) a \equiv b \pmod{n}, c \equiv d \pmod{n}, \text{ 则 } a \pm c \equiv b \pm d \pmod{n}, ac \equiv bd \pmod{n}$$

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (b-a)$$

$$\Leftrightarrow \exists q \in \mathbb{Z}, \text{ s.t. } b-a = qn$$

$$\Leftrightarrow \exists q \in \mathbb{Z}, \text{ s.t. } b = qn+a$$

$$\begin{aligned}
 (5) \quad a \equiv b \pmod{n} &\quad \therefore \exists g_1 \in \mathbb{Z}, \text{ s.t. } b = g_1 n + a \\
 \therefore c \equiv d \pmod{n} &\quad \therefore \exists g_2 \in \mathbb{Z}, \text{ s.t. } d = g_2 n + c. \\
 bd = (g_1 n + a)(g_2 n + c) &= g_1 g_2 n^2 + (g_1 c + g_2 a)n + ac \\
 &= n(g_1 g_2 n + g_1 c + g_2 a) + ac \\
 \therefore bd &\equiv ac \pmod{n}
 \end{aligned}$$

$(\mathbb{Z}, +)$ 的子群

$$H \leq (\mathbb{Z}, +) \quad \exists c \in \mathbb{N}, \text{ s.t. } H = \{cq \mid q \in \mathbb{Z}\}$$

$$n \in \mathbb{Z}^+, H = \{nq \mid q \in \mathbb{Z}\} \quad (\text{此时才有意义})$$

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (b-a) \Leftrightarrow b-a \in H$$

$$a \equiv 0 \pmod{n} \Leftrightarrow n \mid a \Leftrightarrow a \in H.$$

$(G, *)$ 群, $H \leq G$, 如下定义 G 上的二元关系 \equiv (在 \pmod{H})

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

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

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

(1) \sim 是 G 上的等价关系

$$(2) a \sim b \Rightarrow x * a \sim x * b \quad (\forall x \in G)$$

$$(3) a \in G, \{b \mid b \in G, a \sim b\} = \{axh \mid h \in H\} = \{a\}H = aH$$