

§4. 群论基础

§4.1 循环群

$$(G, \cdot) = \text{群} \quad g \in G$$

$$g^m := \begin{cases} \underbrace{g \cdot g \cdots g}_m & m > 0 \\ 1 & m = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{-m} & m < 0 \end{cases}$$

$$(A, +) = \text{群} \quad a \in A$$

$$ma = \begin{cases} \underbrace{a + \cdots + a}_m & m > 0 \\ 0 & m = 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{-m} & m < 0 \end{cases}$$

例: (\mathbb{C}^*, \cdot) $\cdots g^{-2} g^{-1} 1, g, g^2, \cdots$

$(\mathbb{Z}, +)$ $\cdots -2d, -d, 0, d, 2d, \cdots$

$(\mathbb{Z}/6\mathbb{Z}, +)$ $\cdots \rightarrow \bar{0} \rightarrow \bar{3} \rightarrow \bar{0} \rightarrow \bar{3} \rightarrow \bar{0} \rightarrow \cdots$

$\cdots \rightarrow \bar{0} \rightarrow \bar{2} \rightarrow \bar{4} \rightarrow \bar{0} \rightarrow \cdots$

$\cdots \rightarrow \bar{0} \rightarrow \bar{5} \rightarrow \bar{4} \rightarrow \bar{3} \rightarrow \bar{2} \rightarrow \bar{1} \rightarrow \bar{0} \rightarrow \cdots$

$\cdots \rightarrow \bar{0} \rightarrow \bar{4} \rightarrow \bar{2} \rightarrow \bar{0} \rightarrow \cdots$

$(\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$ $\rightarrow \bar{1} \rightarrow \bar{1} \rightarrow \cdots$

$\rightarrow \bar{1} \rightarrow \bar{2} \rightarrow \bar{4} \rightarrow \bar{3} \rightarrow \bar{1} \rightarrow \cdots$

$\rightarrow \bar{1} \rightarrow \bar{3} \rightarrow \bar{4} \rightarrow \bar{2} \rightarrow \bar{1} \rightarrow \cdots$

$\rightarrow \bar{1} \rightarrow \bar{4} \rightarrow \bar{1} \rightarrow \cdots$

性质: 1) $\begin{cases} g^m \cdot g^n = g^{m+n} \\ g^{mn} = (g^m)^n \end{cases}$

即 $(\mathbb{Z}, +) \xrightarrow{\varphi} G$ 为群同态.
 $m \mapsto g^m$

2) $g^m = 1_G = g^n \Leftrightarrow g^{\gcd(m,n)} = 1_G$

$\ker \varphi$ 为 \mathbb{Z} 的理想

加法群呢?

性质: 设 (G, \cdot) 为群, $g \in G$. 则

$$\langle g \rangle := \{ g^k \mid k \in \mathbb{Z} \}$$

为 G 中包含 g 的最小子群. 称为由 g 生成的子群.

Pf: 1) $g^k \cdot (g^l)^{-1} = g^{k-l} \in \langle g \rangle \Rightarrow \langle g \rangle$ 为子群

2) $g \in \langle g \rangle$ 显然

3) 若 $g \in H \leq G$. 则 $g^k \in H \quad \forall (k > 0) \Rightarrow g^k = (g^{-k})^{-1} \in H \quad \forall k < 0$.

$\Rightarrow \langle g \rangle \subseteq H \Rightarrow \langle g \rangle$ 最小.

例: 在 \mathbb{Z} 中, $\langle d \rangle = \{ 0, \pm d, \pm 2d, \dots \}$ 为 \mathbb{Z} 的子群

在 $\mathbb{Z}/6\mathbb{Z}$ 中, $\langle \bar{2} \rangle = \langle \bar{4} \rangle = \{ \bar{0}, \bar{2}, \bar{4} \}$, $\langle \bar{3} \rangle = \{ \bar{0}, \bar{3} \}$

$\langle \bar{1} \rangle = \langle \bar{5} \rangle = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$

在 \mathbb{C} 中 $\langle \pi \rangle = \{ 0, \pm \pi, \pm 2\pi, \dots \} = \{ \dots -\pi, 0, \pi, 2\pi, \dots \}$

在 \mathbb{C}^* 中 $\langle \pi \rangle = \{ 1, \pi^{\pm 1}, \pi^{\pm 2}, \dots \} = \{ \dots \frac{1}{\pi}, 1, \pi, \pi^2, \dots \}$

在 $(\mathbb{Z}/5\mathbb{Z})^\times$ 中 $\langle \bar{1} \rangle = \{ \bar{1} \}$

$\langle \bar{2} \rangle = \langle \bar{3} \rangle = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$

$\langle \bar{4} \rangle = \{ \bar{1}, \bar{4} \}$

定义: G 为群, $g \in G$, $S \subseteq G$ 称包含 S 的最小子群为由 S 生成的子群,

记为 $\langle S \rangle$. 若 $S = \{ x_1, \dots, x_n \}$, 则记 $\langle x_1, \dots, x_n \rangle := \langle S \rangle$.

例: 在 \mathbb{Z} 中, $\langle m_1, m_2, \dots, m_n \rangle = \langle \gcd(m_1, m_2, \dots, m_n) \rangle$. 特别地

-4-2-

$\langle m, n \rangle = \langle \gcd(m, n) \rangle$

定义: 设 $g \in G$. 若存在 $n \in \mathbb{N}_+$ 使得 $g^n = 1$, 则称满足 $g^n = 1$ 的最小的正整数 n 为 g 的阶 (order), 记作 $\text{ord}(g)$ 或 $o(g)$.
若上述 n 不存在, 则称 g 为阶为无限, 记作 $\text{ord}(g) = \infty$. (或 $o(g) = \infty$)

注: $o(g) = 1 \Leftrightarrow g = 1_G$

性质: 1). 若 $\text{ord}(g) = k < \infty$. 则 a) $g^n = 1 \Leftrightarrow n \equiv 0 \pmod k$ ($k | n$)
b) $g^i = g^j \Leftrightarrow i \equiv j \pmod k$ ($k | i - j$)
c) $\langle g \rangle = \{1, g, \dots, g^{k-1}\}$

2). 若 $\text{ord}(g) = \infty$. 则 $\forall i \neq j$, 均有 $g^i \neq g^j$.

3). $\text{ord}(g) = \# \langle g \rangle$

pf(a): $\forall n = kq + r$ $0 \leq r < k$

$$g^n = 1 \Leftrightarrow g^r = 1 \quad (0 \leq r < k) \xLeftrightarrow[\text{ord}(g)=k] r = 0 \Leftrightarrow k | n$$

$$(b): g^i = g^j \Leftrightarrow g^{i-j} = 1 \xLeftrightarrow[1) k | i-j$$

(c): 若 $H \ni g$ 为子群包含 g , 则 $\forall i \geq 1, g^i \in H$ & $e = g^0 \in H \Rightarrow \{1, g, \dots, g^{k-1}\} \subseteq H$

只需证明 $\{1, g, \dots, g^{k-1}\}$ 为子群. 由 2) 易知, 其关于乘法和取逆封闭.

(a) 反证: 若 $i \neq j$ 且 $g^i = g^j$. 不妨设 $j > i$. 则

$$g^{j-i} = 1 \Rightarrow \text{ord}(g) \neq \infty \quad \downarrow$$

(3) 由 (1) & (2) 可得.

定义: 设 G 为群.

1) 若 $S \subseteq G$ 满足 $G = \langle S \rangle$, 则称 G 由 S 生成 (finitely generated group)

2) 若存在有限子集 $S \subseteq G$ 使得 $G = \langle S \rangle$, 则称 G 为有限生成群

3) 若存在 $g \in G$ 使得 $G = \langle g \rangle$, 则称 G 为循环群 (Cyclic group)

称 g 为 G 的一个生成元 (generator)

例: 1) \mathbb{Z} 和 $\mathbb{Z}/n\mathbb{Z}$ 都是循环群

2) $(\mathbb{Z}/8\mathbb{Z})^\times$ 不是循环群, 但可由两个元素生成.

3) \mathbb{Q} 不是有限生成的.

同构意义下, 只有这两种循环群.

定理 (循环群结构定理): 设 G 为循环群

1) $\#G = n \Rightarrow G \cong \mathbb{Z}/n\mathbb{Z}$

2) $\#G = \infty \Rightarrow G \cong \mathbb{Z}$.

pf: 设 $G = \langle g \rangle$.

1° $\#G = \infty$: 定义 $\varphi: \mathbb{Z} \rightarrow G$, 则 φ 为群的满同态.
 $k \mapsto g^k$

$\text{ord}(g) = \infty \Rightarrow g^i \neq g^j \ (i \neq j) \Rightarrow \varphi$ 为单射 $\Rightarrow \varphi$ 为同构.

2° $\#G = n$.

$(g^i = g^j \Leftrightarrow i \equiv j \pmod{n}) \Rightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{\bar{\varphi}} G$ 良定义, 且既单又满 $\Rightarrow \bar{\varphi}$ 为同构
 $k \pmod{n} \mapsto g^k$

例: $\mathbb{Z}/6\mathbb{Z} = \langle 1 \rangle = \langle 5 \rangle \neq \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle \quad / \quad \mathbb{Z}/n\mathbb{Z} = \langle d \rangle \Leftrightarrow \gcd(d, n) = 1$

循环群的生成元及其自同构群:

定理: 设 $G = \langle g \rangle$ 则 $|G| = \text{ord}(g)$, 且

(1). $\#G = \infty \Rightarrow G$ 的生成元为 g 或 g^{-1} .

(2). $\#G = n < \infty \Rightarrow G$ 的生成元集合为 $\{g^k \mid 0 \leq k < n, (k, n) = 1\}$

(3). $\text{Aut}(G) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \#G = \infty \\ (\mathbb{Z}/n\mathbb{Z})^\times & \#G = n. \end{cases}$

$\hookrightarrow G$ 的自同构群, $\text{Aut}(G) := \{\varphi: G \rightarrow G \mid \varphi \text{ 为同构}\}.$

-4-4- $\forall \varphi \in \text{Aut}(G) \Rightarrow \varphi(g)$ 为生成元.

pf: (1) $G = \{g^n \mid n \in \mathbb{Z}\} = \{(g^{-1})^n \mid n \in \mathbb{Z}\} \Rightarrow g \text{ 和 } g^{-1} \text{ 都为 } G \text{ 的生成元.}$

反之, 若 g^a 为 G 的生成元, 则 $\exists b \in \mathbb{Z} \text{ s.t. } g = (g^a)^b = g^{ab}.$

$$\Rightarrow ab=1 \Rightarrow a=\pm 1 \Rightarrow g^a = g \text{ 或 } g^{-1}$$

(2) $\forall k \in \mathbb{Z} : (k, n)=1. \Rightarrow \exists s, t \text{ s.t. } ks + nt = 1.$

$$\Rightarrow \forall m \in \mathbb{Z}, g^m = g^{ksm} \cdot g^{ktn} = (g^k)^{sm} \in \langle g^k \rangle$$

$$\Rightarrow G = \langle g^k \rangle \Rightarrow g^k \text{ 为 } G \text{ 的生成元}$$

反之, 若 g^a 为 G 的生成元, 则 $\exists b \in \mathbb{Z} \text{ s.t. } g = (g^a)^b = g^{ab}$

$$\Rightarrow ab \equiv 1 \pmod{n} \Rightarrow a$$

若 g^a 为 G 的生成元, 则 $\exists b \in \mathbb{Z} \text{ s.t. } g = (g^a)^b = g^{ab}.$

$$\#G=n \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n)=1. \Rightarrow \checkmark$$

$$(3), G = \varphi(G) = \{ \varphi(g^n) \mid n \in \mathbb{Z} \} = \{ (\varphi(g))^n \mid n \in \mathbb{Z} \} = \langle \varphi(g) \rangle$$

$\Rightarrow \varphi(g)$ 为 G 的生成元. 而 φ 由 $\varphi(g)$ 唯一决定, 因此

可构造如下映射

$$1^\circ \#G=\infty \quad \psi: \text{Aut } G \rightarrow \{\pm 1\} = \mathbb{Z}^\times$$

$$\psi(\varphi) = \begin{cases} 1 & \varphi(g)=g \\ -1 & \varphi(g)=g^{-1} \end{cases}$$

$$2^\circ \#G=n. \quad \psi: \text{Aut } G \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\varphi(g)=g^a \Rightarrow \psi(\varphi)=a \pmod{n}$$

通过验证可得 ψ 为群同态. 且既单又满 (即为同构)

- 例: (1) $\mathbb{Z}/n\mathbb{Z}$ 的生成元 $\{1 \leq a < n \mid (a, n) = 1\}$
 (2) μ_n 的生成元 $\{\zeta_n^a \mid 1 \leq a < n, (a, n) = 1\}$
 (3) $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 为循环群 $\Leftrightarrow \gcd(m, n) = 1$.

pf: (3), \Leftarrow : CRT. \Rightarrow : 设 (g_1, g_2) 为生成元, 则
 $mn = \text{ord}(g_1, g_2) \mid \text{lcm}(\text{ord}(g_1), \text{ord}(g_2)) \mid \text{lcm}(m, n) \leq mn \Rightarrow \gcd(m, n) = 1$.

循环群的子群分类:

- 定理: 1) $\forall d \in \mathbb{N} = \mathbb{Z}_{\geq 0} \Rightarrow \langle d \rangle = \{0, \pm d, \pm 2d, \dots\}$ 为 \mathbb{Z} 的循环子群.
 2) \mathbb{Z} 的所有子群均为(1)中的形式.
 3) $\langle a_1, a_2, \dots, a_n \rangle = \langle \gcd(a_1, a_2, \dots, a_n) \rangle \subseteq \mathbb{Z}$.

pf 1) \checkmark

2) 设 H 为 $(\mathbb{Z}, +)$ 的子群. 则 H 为 $(\mathbb{Z}, +, \cdot)$ 的理想.

$$\begin{cases} \cdot h_1 + h_2 \in H & (\forall h_1, h_2 \in H \vee) \\ \cdot nh = \underbrace{h + \dots + h}_n \in H & (nh = \underbrace{(-h) + \dots + (-h)}_{-n} \in H) \end{cases}$$

$$\Rightarrow H = (d) = \{0, \pm d, \pm 2d, \dots\} = \langle d \rangle \subseteq \mathbb{Z}.$$

$\mathbb{Z}/6\mathbb{Z}$ 的子群有 $\langle \bar{0} \rangle, \langle \bar{1} \rangle, \langle \bar{2} \rangle, \langle \bar{3} \rangle$.

定理: 1) $\forall d \mid m (d > 0)$. 则

$$\langle \bar{d} \rangle = \{\bar{0}, \bar{d}, \dots, (\frac{m}{d}-1)\bar{d}\}$$

为 $\mathbb{Z}/m\mathbb{Z}$ 的 $\frac{m}{d}$ 阶循环子群

2) $\mathbb{Z}/m\mathbb{Z}$ 的所有子群均为(1)中的形式.

3) $\langle \bar{a}_1, \dots, \bar{a}_n \rangle = \langle \overline{\gcd(a_1, a_2, \dots, a_n, m)} \rangle \subseteq \mathbb{Z}/m\mathbb{Z}$. 特别地,

$$\langle \bar{a} \rangle = \langle \overline{\gcd(a, m)} \rangle.$$

pf: 1) $\text{ord}(\bar{a}) = \frac{m}{d} \Rightarrow \checkmark$

2) 设 $H \leq \mathbb{Z}/m\mathbb{Z}$. 设 $I_H := \{x \in \mathbb{Z} \mid \bar{x} \in H\}$ 则

-4-6- I_H 为 \mathbb{Z} 的子群 ($\forall \bar{x}, \bar{y} \in I_H \quad \overline{x-y} = \bar{x} - \bar{y} \in H \Rightarrow x-y \in I_H$)

$$\Rightarrow I_H = \langle d \rangle \subseteq \mathbb{Z}, \quad (\text{WMA } d \geq 0)$$

$$\text{由于 } \overline{m} = \overline{0} \in H \Rightarrow m \in I_H \Rightarrow d|m$$

$$\Rightarrow H = \{ \overline{x} \mid x \in I_H \} = \{ \overline{dk} \mid k \in \mathbb{Z} \} = \langle \overline{d} \rangle.$$

3) " \leq " \checkmark

$$\text{"} \geq \text{" 贝祖} \Rightarrow \gcd(a_1, \dots, a_n, m) = a_1 x_1 + \dots + a_n x_n + m y$$

$\Rightarrow \checkmark$

推论: $G = m$ 阶循环群. 设 x 为 G 的生成元. $\forall d|m$, 记

$$H_d = \{ 1, x^{\frac{m}{d}}, x^{\frac{2m}{d}}, \dots, x^{\frac{(d-1)m}{d}} \}$$

则 (1) H_d 为 G 的 d 阶循环子群.

(2). G 的任意子群均为这一形式.

pf: (1) $\text{ord}(x^{\frac{m}{d}}) = d \Rightarrow H_d = \langle x^{\frac{m}{d}} \rangle$ 为 d 阶循环子群

(2) $\forall H \leq G$. 则

$$m \in I_H := \{ i \in \mathbb{Z} \mid x^i \in H \} \leq \mathbb{Z}$$

因此 $I_H = \langle \frac{m}{d} \rangle, (d|m)$. 从而

$$H = \{ x^i \mid i \in I_H \} = \langle x^{\frac{m}{d}} \rangle = \{ 1, x^{\frac{m}{d}}, \dots, x^{\frac{(d-1)m}{d}} \}$$

推论: $n = \sum_{d|n} \varphi(d)$

$$H_d^\circ := \{ h \in H_d \mid H_d = \langle h \rangle \}$$

$$\forall g \in G \Rightarrow \exists d|n \text{ s.t. } H_d = \langle g \rangle \Rightarrow g \in H_d^\circ$$

$$\Rightarrow G = \bigsqcup_{d|n} H_d^\circ$$

$$\Rightarrow n = \sum_{d|n} |H_d^\circ| = \sum_{d|n} \varphi(d).$$

经典的对数函数 $\log_a(\cdot): (\mathbb{R}_+, \cdot) \rightarrow (\mathbb{R}, +)$ 为群同构, 定义为指数函数 $(\mathbb{R}, +) \xrightarrow{\cong} (\mathbb{R}_+, \cdot) \quad r \mapsto a^r$ 的逆函数.

类似地, 我们可定义离散对数:

定义: 设 $G = \langle g \rangle$ n 阶循环群. 记 $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} G$ 的逆映射为 $k \mapsto g^k$

$$\log_g: (G, \cdot) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +) \quad a = g^k \mapsto k \quad (\text{discrete logarithm})$$

则 \log_g 为循环群之间的同构. 称 $k = \log_g a$ 为 a 关于 g 的离散对数

问题: $G = \langle g \rangle$, $\forall a \in G$, 如何求 a 关于 g 的离散对数?

命题: $G = \langle g \rangle$ n 阶循环. $\forall a \in G$, $\forall k \in \mathbb{Z}$ 则 $x^k = a$ 有解 $\Leftrightarrow d = (k, n) \mid \log_g a \Rightarrow$ 有 d 个解.

$$\text{Pf: } \{x \in G \mid x^k = a\} \xleftrightarrow{|\cdot|} \{y \in \mathbb{Z}/n\mathbb{Z} \mid ky \equiv \log_g a \pmod{n}\}$$

$$x^k = a \text{ 有解} \Leftrightarrow ky \equiv \log_g a \pmod{n} \text{ 有解}$$

$$\Leftrightarrow d = (k, n) \mid \log_g a$$

若 $d \mid \log_g a$, 则

$$ky \equiv \log_g a \pmod{n} \Rightarrow y \equiv \frac{\log_g a}{d} \cdot c \pmod{\frac{n}{d}} \quad c \equiv \left(\frac{k}{d}\right)^{-1} \pmod{\left(\frac{n}{d}\right)}$$

$$\Rightarrow y \equiv \frac{c}{d} \log_g a + \frac{n}{d} \cdot i \pmod{n}$$

$$(0 \leq i < d).$$

§4.2 拉格朗日定理

$$\mathbb{Z} = \bigcup_{a=0}^{m-1} a + m\mathbb{Z} \quad m\mathbb{Z} \leq \mathbb{Z}$$

$$H < G$$

定义: $\forall a \in G$,

$$aH = \{ ah \mid h \in H \} \quad H \text{ 的左陪集 (left coset)}$$

$$Ha = \{ ha \mid h \in H \} \quad H \text{ 的右陪集 (right coset)}$$

引理: 1) $aH = bH \Leftrightarrow aH \cap bH \neq \emptyset \Leftrightarrow b^{-1}a \in H$

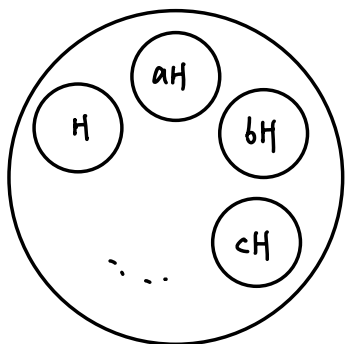
2) $Ha = Hb \Leftrightarrow Ha \cap Hb \neq \emptyset \Leftrightarrow ab^{-1} \in H$

pf: ① \Rightarrow ②: \checkmark

$$\text{②} \Rightarrow \text{③}: ah_1 = bh_2 \Rightarrow b^{-1}a = h_2h_1^{-1} \in H$$

$$\begin{aligned} \text{③} \Rightarrow \text{①}: b^{-1}a \in H &\Rightarrow b^{-1}aH = H \\ &\Rightarrow aH = b \cdot (b^{-1}a)H = bH \end{aligned}$$

注: aH 为右陪集, $\Leftrightarrow aH = Ha \Leftrightarrow aHa^{-1} = H \Leftrightarrow aha^{-1} \in H \forall h \Leftrightarrow a \in N_G(H)$.



$$\forall g \in G \Rightarrow g \in gH$$

$$\text{引理} \Rightarrow G = \bigsqcup_{i \in I} a_i H$$

\uparrow G 的一个分拆

定义: $H < G, \forall s \in G$,

1) 若 $G = \bigsqcup_{s \in S} sH$, 则称 S 为子群 H 的左陪集代表元系 (left coset representatives)

2) 若 $G = \bigsqcup_{s \in S} Hs$, 则称 S 为子群 H 的右陪集代表元系 (right coset representatives)

例如: $\{0, 1, \dots, m-1\}$ 为 $m\mathbb{Z}$ 在 \mathbb{Z} 中的陪集代表元系

引理: 若 $S \subseteq G$ 为 H 的 **左(右)**陪集代表元系, 则

$$S^{-1} := \{ s^{-1} \mid s \in S \}$$

为 H 的 **右(左)**陪集代表元系

Pf: 左 \Rightarrow 右:

方法-: 设 $G = \bigsqcup_{s \in S} sH$. 则

$$\forall g \in G, \exists s_g \in S \text{ 及 } h_g \in H \text{ s.t. } g^{-1} = s_g h_g$$

$$\Rightarrow g = h_g^{-1} \cdot s_g^{-1} \Rightarrow G = \bigcup_{s \in S} H s^{-1}$$

$$\forall s_1, s_2 \in S, \quad s_1 \neq s_2 \Rightarrow s_1 H \cap s_2 H = \emptyset$$

$$\Rightarrow s_1^{-1} s_2 \notin H$$

$$\Rightarrow H s_1^{-1} \cap H s_2^{-1} = \emptyset$$

$$\Rightarrow G = \bigsqcup_{s \in S} H s^{-1} = \bigsqcup_{t \in S^{-1}} H t$$

方法= (使用集合操作):

$$(aH)^{-1} = \{ (ah)^{-1} \mid h \in H \} = \{ h^{-1} a^{-1} \mid h \in H \}$$

$$= \{ h' a^{-1} \mid h' \in H \} = H a^{-1}$$

$$G = G^{-1} = \left(\bigsqcup_{s \in S} sH \right)^{-1} = \bigsqcup_{s \in S} (sH)^{-1} = \bigsqcup_{s \in S} H s^{-1} = \bigsqcup_{t \in S^{-1}} H t.$$

定义: $H < G$. 称 H 在 G 中的左(右)陪集总个数为 G 关于 H 的**指数** (index)

记为 $(G:H)$ 或 $[G:H]$. 若有无穷多个陪集, 则记为 $(G:H) = \infty$.

定理 (群论中的拉格朗日定理): $\#G = \#H \cdot (G:H)$

pf: $G = \bigsqcup_{i \in I} a_i H \quad (G:H := \#I)$

$\cdot \left(H \xrightarrow{a_i} a_i H \right) \Rightarrow \#(a_i H) = \#H$

\cdot 若 $\#G = \infty$,

则 $\#H = \infty$ 或 $\#I = \infty$ (否则右边为有限集)

因此 $\#G = \#H \cdot (G:H)$

\cdot 若 $\#G < \infty$, 则

$$\begin{aligned} \#G &= \sum_{i \in I} \#a_i H = \sum_{i \in I} (\#H) = \#H \cdot \#I \\ &= \#H \cdot (G:H). \end{aligned}$$

推论: $\#G < \infty$.

1) $H < G \Rightarrow \#H \mid \#G$.

2) $\forall x \in G \Rightarrow \text{ord}(x) \mid \#G \Rightarrow x^{\#G} = 1$.

推论 (欧拉定理) & (费马小定理)

pf: $\#(\mathbb{Z}/n\mathbb{Z})^\times =: \varphi(n)$

推论: $p = \text{素数}$. 则

1) p 阶群均同构于 $(\mathbb{Z}/p\mathbb{Z}, +)$

2) p 阶域均同构于 $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$

pf: $\forall g \in G \setminus \{1\} \Rightarrow \# \langle g \rangle \mid \#G = \text{素数} \Rightarrow \# \langle g \rangle = \#G \Rightarrow \langle g \rangle = G \Rightarrow \forall$

§4.3 正规子群与商群.

引理: $H \leq G$. $\forall a \in G$. 则 $Ha = aH \Leftrightarrow aHa^{-1} = H$

$$\text{Pf: } Ha = aH \Leftrightarrow \begin{cases} Ha \subseteq aH \Leftrightarrow (Ha)a^{-1} \subseteq (aH)a^{-1} \Leftrightarrow H \subseteq aHa^{-1} \\ aH \subseteq Ha \Leftrightarrow (aH)a^{-1} \subseteq (Ha)a^{-1} \Leftrightarrow aHa^{-1} \subseteq H \end{cases} \\ \Rightarrow aHa^{-1} = H.$$

定义: 设 $H \leq G$. 1) $\forall x, g \in G$. 称 gxg^{-1} 为 x 的共轭元

2) 若任意 H 中元素的共轭元均在 H 中 (i.e. $gHg^{-1} = \{ghg^{-1} | h \in H\} \subseteq H$).
则称 H 为 G 的正规子群. 记作 $H \triangleleft G$.

e.g.: 交换群的子群均正规.

推广: $H < G$. 则 $H \triangleleft G \Leftrightarrow gH = Hg (\forall g \in G)$

$$\text{Pf: } H \triangleleft G \Leftrightarrow \forall h \in H, \forall g \in G. ghg^{-1} \in H.$$

回顾: 设 $\varphi: G \rightarrow G'$ 为群同态, $\ker \varphi := \{g \in G | \varphi(g) = 1_{G'}\}$ 为 G 的子群.

推广: 设 $\varphi: G \rightarrow G'$ 为群同态. 则 $\ker \varphi$ 为正规子群.

实际上反过来也是对的. 一个子群为正规的当且仅当其为群同态的核.

为了证明这一点, 我们需要引入商群:

定理*: 设 N 为 G 的正规子群. 记 $G/N := \{gN | g \in G\}$ 定义 G/N 上的二元运算 $(gN) \cdot (g_2N) = (g_1g_2)N$.

则上述运算是良定义的, 且 $(G/N, \cdot)$ 构成群, 称为 G 关于 N 的商群.

推广: 设 $N \triangleleft G$. 则 $\varphi: G \rightarrow G/N, g \mapsto gN$ 为群的满同态, 且 $\ker \varphi = N$.

定理* (群同态基本定理) 设 $\varphi: G \rightarrow G'$ 为群同态, 则

$$\text{Im } \varphi \cong G / \ker \varphi.$$

§ 等价关系

生活中常见的关系：朋友，父子，老乡，

例：考察某家族的全体男性 $X = \{A, B, C, D, E, F, G\}$ ，及所有的父子
 $(A, B), (A, C), (A, D), (B, E), (B, F), (C, G)$

容易看出 X 上的父子关系可由 $X \times X$ 的子集

$$\{(A, B), (A, C), (A, D), (B, E), (B, F), (C, G)\}$$

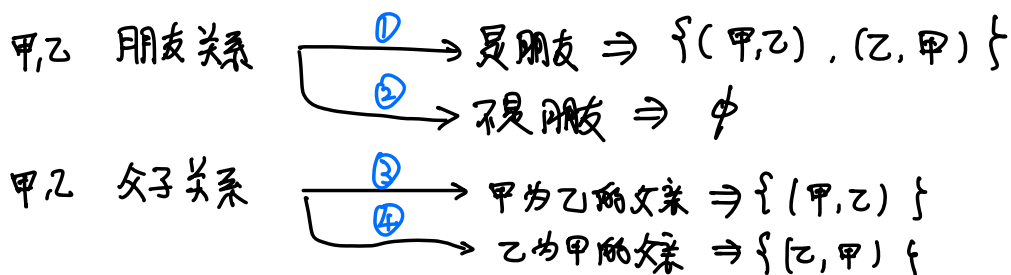
完全确定。因此我们可以用这个子集描述家族 X 中的父子关系。

其它关系也可以类似地描述。

于是我们可以用如下方式，从数学层面（集合论）角度来严格定义“关系”：

定义：设 X 为集合。称 $X \times X$ 的一个子集 R 为 X 上的一个关系。
我们也将 $(x, y) \in R$ 写成 xRy 。

例：两个元素之间共有 16 种可能的关系。



例：(同余) $a \equiv b \pmod{m}$ 。

在数学中有一些关系是特别受关注的：

定义：设 $R \subseteq X \times X$ 为 X 上的一个关系。称 R 为 X 上的等价关系，若 R 满足

1) (自反性) $(x, x) \in R \quad (\forall x \in X)$

2) (对称性) $(x, y) \in R \Rightarrow (y, x) \in R \quad (\forall x, y \in X)$

3) (传递性) $(x, y), (y, z) \in R \Rightarrow (x, z) \in R \quad (\forall x, y, z \in X)$

此时，若 $(x, y) \in R$ ，则称 x 等价于 y 。反之称 x 不等价于 y 。

e.g. 老乡, 同余,

老乡 \mapsto 按省(市,县)将人划分.

同余 \mapsto 按余数将整数划分.

对于等价关系, 我们有如下通俗理解:

定理: 给定 X 上的一个等价关系 等价于 给定 X 上的一个拆分.

pf: \cdot 设 R 为 X 上的一个关系, $\forall x \in X$, 记

$$[x] := \{y \in X \mid (x, y) \in R\} \subseteq X$$

\uparrow 称为 x 所在的 **等价类**

等价类有如下基本性质

$$\cdot [x] \cap [y] \neq \emptyset \Leftrightarrow [x] = [y]$$

$$\cdot X = \bigcup_{x \in X} [x]$$

因此 X 可写成一些等价类的无交并, 即给出 X 的一个拆分.

\cdot 设 $X = \bigsqcup_{i \in I} X_i$ 为一个拆分, 定义关系

$$R = \bigcup_{i \in I} X_i \times X_i \subseteq X \times X$$

即 $(x, y) \in R \Leftrightarrow x, y$ 落入同一个拆分子集中. □

由 X 出发的映射也可给出 X 上的等价关系:

命题: 1) 设 $\varphi: X \rightarrow Y$ 为映射, 定义

$$R := \{(x, y) \mid \varphi(x) = \varphi(y)\}$$

以及

$$X_y := \{x \in X \mid \varphi(x) = y\}$$

则 R 为 X 上的等价关系, 这一关系与拆分 $X = \bigsqcup_{y \in Y} X_y$ 对应.

2) 反之, 任意等价关系 R 都可通过 1) 中方式给出

证: $\begin{cases} \text{自反性: } \varphi(x) = \varphi(x) \\ \text{对称性: } \varphi(x) = \varphi(y) \Rightarrow \varphi(y) = \varphi(x) \\ \text{传递性: } \varphi(x) = \varphi(y) = \varphi(z) \Rightarrow \varphi(x) = \varphi(z) \end{cases}$

$$\varphi: X \longrightarrow \{[x]_R \mid x \in X\}$$

$$x \longmapsto [x]_R$$

$$\bullet \forall a \in X \Rightarrow [a] = \{x \in X \mid \varphi(x) = \varphi(a)\} = X_{\varphi(a)}$$

$$\Rightarrow \checkmark$$

总而言之: $\{\text{从 } X \text{ 出发的映射}\} \rightarrow \{X \text{ 上等价关系}\} \xleftrightarrow{1:1} \{X \text{ 上的拆分}\}$