

Sylow 定理

B.Huppert (German)

«有限群论» Endliche Gruppen

$n \leq 11$. 都有所有因数阶的群

$n = 12$, A_4 无6阶子群

$n = p_1 p_2 \cdots p_s$, p_i 素

$n \in \mathbb{Z}^+$, $p^k \mid n$, $p^{k+1} \nmid n$.

④思考

$$24 = 2^3 \times 3$$

定义 (Sylow 子群)

设 G 是有限群, $|G| = n$, p 是素数. 设 $p^k \mid n$, $p^{k+1} \nmid n$. 看 $H \leq G$

(1) 若 $|H|$ 是 p 的幂次, 则称 H 是 G 的 p -子群 // $|H| = p^l$, $p^l \mid n$. $\Rightarrow l \leq k$

(2) 若 $|H| = p^k$, 则称 H 是 G 的 Sylow - p 子群 // k 最大

$$G \trianglelefteq G, g \in G, gag^{-1}$$

$$A \subseteq G, g \in G, \{g\} A \{g^{-1}\} = gAg^{-1} = \{gag^{-1} \mid a \in A\}$$

G 群, $g \in G$, 如下定义 $f: G \rightarrow G$, $\forall a \in G, f(a) = gag^{-1}$. f 是 G 的自身的群同构, 并且 f^{-1} 如下给出: $\forall a \in G, f^{-1}(a) = g^{-1}ag$ // 例证双射, 乘法

f 称为由 g 导出的 G 的内自同构.

定理 (Sylow 定理, 1872)

设 G 是有限群, $|G| = n$, p 是素数, 则:

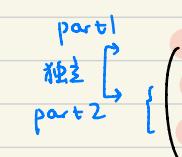
1. G 有 Sylow - p 子群, 进一步地, $|\{H \mid H \text{ 是 } G \text{ 的 Sylow - } p \text{ 子群}\}| \equiv 1 \pmod{p}$

2. 设 H 和 K 是 G 的两个 Sylow - p 子群, 则 $\exists g \in G$, s.t. $K = gHg^{-1}$.

3. 设 A 是 G 的 p -子群, 则 $\exists H$ 是 G 的 Sylow - p 子群, s.t. $A \leq H$.

4. 设 $p^k \mid n$, 则 $|\{A \mid A \leq G, |A|=p^k\}| \equiv 1 \pmod{p}$ // p 子群

$$C(n, p^k) = C_n^{p^k} \quad C(n, p^k) = \text{各等价类的元素个数之和}$$



第一部分的特例:

A 是 G 的 2-子群

自反: $a = a$. 对称: $a \sim b \Leftrightarrow b \sim a$

传递: $a \sim b, b \sim c \Rightarrow a \sim c$

$$a=b, b=c \Rightarrow a=c$$

$$a=b^{-1}, b=c \Rightarrow a=c^{-1}$$

$$a=b^{-1}, b=c^{-1} \Rightarrow a=(c^{-1})^{-1}=c.$$

命题. 设 G 是偶数阶群, 则 $|\{a \mid a \in G, a^2 = 1_G\}| \equiv 0 \pmod{2}$ 去掉 1_G 二阶元个数为奇,

$$\leftarrow \text{从而 } |\{a \mid a \in G, |a|=2\}| \equiv 1 \pmod{2} \quad // p=2, l=1, p^l=2 \quad \hookrightarrow \text{--对应二阶子群} \\ = \{1_G\} \cup \{G \text{ 中二阶元}\} \quad \{a, a^{-1}\}$$

证: 如下定义 G 上的等价关系 ~: $\forall a, b \in G, a \sim b \Leftrightarrow a = b \text{ 或 } a = b^{-1}$ // 自反, 对称, 传递

可证: $a \in G$, a 所在 ~ 下的等价类: $\{b \mid b \in G, a \sim b\} = \{a, a^{-1}\}$

$$|\{a, a^{-1}\}| = 1 \Leftrightarrow a = a^{-1} \Leftrightarrow a^2 = 1_G$$

$$|\{a, a^{-1}\}| = 2 \Leftrightarrow a^2 \neq e.$$

记 T 为 G 在 \sim 下的全体类

$$\begin{aligned} |G| &= \sum_{A \in T} |A| = \left(\sum_{A \in T, |A|=1} |A| \right) + \left(\sum_{A \in T, |A|=2} |A| \right) = |\{A \in T \mid |A|=1\}| + 2|\{A \in T \mid |A|=2\}| \\ &= |\{a \mid a \in G, a^2=e\}| + 2|\{A \in T \mid |A|=2\}| \end{aligned}$$

$$\therefore |G| \equiv |\{a \mid a \in G, a^2=e\}| \pmod{2}$$

G 为偶数阶群

$$\text{但 } |G| \text{ 是偶数, } \therefore |\{a \mid a \in G, a^2=e\}| \equiv 0 \pmod{2}$$

方二: 记 A_1, A_2, \dots, A_m 是全体类, 其中 A_1, \dots, A_l 的元素个数为 l .

$$A_{l+1}, \dots, A_m \cdots \cdots 2.$$

$$\therefore |G| = |A_1| + |A_2| + \cdots + |A_m| = l + 2(m-l)$$

$$|G| \equiv l \pmod{2} \quad |G| \text{ 偶} \Rightarrow l \equiv 0 \pmod{2}$$

$$\text{又 } l = |\{a \in G \mid a^2=e\}|$$

第二部分: \cdots

G 是 n 阶群, $d \mid n$. 考察 G 中有无 d 阶子群

记 $T = \{A \mid A \subseteq G, |A|=d\}$. 在 T 上定义类 \sim : T 是 G 的 d 阶子集的集合

$A \sim B \Leftrightarrow \exists g \in G, s.t. B = gA = \{ga \mid a \in A\}$. → 思考: 定义类

对任 $-A \subseteq G, |A|=d$, A 所在的类为: $\{B \mid B \subseteq G, |B|=d, A \sim B\} = \{gA \mid g \in G\}$.

记 $[A] = \{gA \mid g \in G\}$. 则: $\underbrace{B \in T}_{(\text{集合})}$

(1) 若 $[A]$ 中含子群, 则有且仅有 1 个子群, 并且 $|[A]| = \frac{n}{d}$. 类中的元素个数

(2) 若 $[A]$ 中不含子群, 则 $|[A]| = \frac{n}{d}w$, 其中 $w \geq 2$, 且 $w \nmid d$ (w 与 d 互质)

或: 记 L_1, L_2, \dots, L_m 为全体类, 其中 L_1, \dots, L_k 含子群, L_{k+1}, \dots, L_m 不含子群.

从而 G 恰有 k 个 d 阶子群. 各一个

(Sylow 定理第一部分)

定理. G 是有限群, $p^l \mid |G|$, 则 G 的 p^l 阶子群个数 $\equiv 1 \pmod{p}$, 即

$$\left| \{A \mid A \leq G, |A|=p^l\} \right| \equiv 1 \pmod{p}$$

命题. 设 G 是 n 阶群, $d \mid n$, $d \geq 2$. G 的 d 阶子群个数为 k , 则:① 存在 d 的一些 ≥ 2 的因子 w_1, w_2, \dots, w_s ($s \geq 0, w_i \geq 2, w_i \mid d$)

$$\text{s.t. } C(n-1, d-1) = k + w_1 + w_2 + \dots + w_s$$

② 设 p 是素数, $d = p^l$, 则 $k \geq 1$ ③ 在 ② 的条件下, 还有 $k \equiv 1 \pmod{p}$ 先由 ① \Rightarrow ② ③在 ① 中代入 $d = p^l$, $C(n-1, p^l-1) = k + w_1 + w_2 + \dots + w_s$. $\forall 1 \leq i \leq s, w_i \mid p^l$, p 是素数. \uparrow p 的倍数

$$\therefore w_i = p^t (t \leq l) \quad \text{又 } w_i \geq 2, \quad \therefore t \neq 0. \quad p \nmid w_i \pmod{p} \neq 0$$

由 ① 可知 $C(n-1, p^l-1) \equiv k \pmod{p}$ 又 $C(n-1, p^l-1) \neq 0 \Rightarrow k \geq 1$ $\because p$ 是素数, $p^l \mid n \Rightarrow C(n-1, p^l-1) \equiv 1 \pmod{p} \quad \therefore k \equiv 1 \pmod{p}$ eg. $p=2, 2 \mid n$

$$p^l=2 \quad C(n-1, 2-1) = n-1 \equiv 1 \pmod{2}$$

$$p^l=4 \quad C(n-1, 4-1) = \frac{(n-1)(n-2)(n-3)}{6}$$

$$4 \mid n, n=4m \quad \frac{(4m-1)(4m-2)(4m-3)}{6} \text{ 是奇数, } \equiv 1 \pmod{2}$$

① 的证明:

设 $T = \{A \mid A \leq G \text{ 且 } |A|=d\}$, 在 T 上定义等价关系 $\sim: A \sim B \Leftrightarrow \exists g \in G, \text{ s.t. } B = gA$. $\forall A \leq G, |A|=d$, A 所在的等价类为: $[A] = \{gA \mid g \in G\}$ 且 (i) 若 $[A]$ 中含 d 阶子群, 则仅含 1 个且 $|[A]| = \frac{n}{d} = \frac{|G|}{d}$.(ii) 若 $[A]$ 中不含 d 阶子群, 则 $|[A]| = \frac{n}{d} \cdot w$, 其中 $w \mid d, w \geq 2$.设 L_1, L_2, \dots, L_m 为 (T, \sim) 的全体等价类,自反性: $A = _0 A$ 对称性: $B = gA \Rightarrow A = g^{-1}B$.传递性: $B = g_1 A, C = g_2 B$

$$\Rightarrow C = (g_2 g_1) A$$

G 的. ($|G|=n$)

\checkmark 元素个数为 d 的子集. C_n^d

$$C_n^d = \frac{n(n-1)\dots(n-d+1)}{d!}$$

$$C_{n-1}^{d-1} = \frac{(n-1)\dots(n-k-d+1+1)}{(d-1)!}$$

G 的 d 阶子群恰有 k 个

由(i) 含 d 阶子群的支集类有 k 个, 不妨设为 L_1, \dots, L_k .

$$\text{由(ii)(ii)} |L_1| = |L_2| = \dots = |L_k| = \frac{n}{d}$$

$$\text{对 } \forall k+1 \leq j \leq m, |L_j| = \frac{n}{d} w_j (w_j \geq 1, w_j | d)$$

$$|T| = |L_1| + |L_2| + \dots + |L_m| = \frac{n}{d} \cdot k + \frac{n}{d} (w_{k+1} + \dots + w_m)$$

$$\checkmark |T| = C(n, d) = \frac{n}{d} C(n-1, d-1)$$

$$\text{可知 } C(n-1, d-1) = k + w_{k+1} + \dots + w_m.$$

eg. 12 阶循群的 Sylow-2 子群

$$12 = 2^2 \cdot 3 \quad p^1 = 2^2 = 4$$

$$G = \langle a \rangle \quad o(a) = 12$$

$H = \langle a^3 \rangle$, 由 a^3 导出的生成子群 // H: Sylow-p 子群 $|H|=4$.

$$\text{eg. } A_4 \quad H = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

$$H \triangleleft A_4, H \triangleleft S_4$$

\mathbb{R}^n . 数乘

$$\lambda(a_1, \dots, a_n) = (\lambda a_1, \dots, \lambda a_n)$$

$$\mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n$$

对 $\lambda, \mu \in \mathbb{R}, \alpha \in \mathbb{R}^n$,

$$\begin{cases} (\lambda \mu) \alpha = \lambda(\mu \alpha) \\ 1 \cdot \alpha = \alpha \end{cases}$$

群作用

定义(么半群在集合上的作用)

设 G 是么半群, X 是集合, $\rightarrow: G \times X \rightarrow X$ 的一个映射 ($\forall g \in G, x \in X, g \rightarrow x = \omega(g, x)$)

若 ① $\forall g, h \in G, x \in X, (gh) \rightarrow x = g \rightarrow (h \rightarrow x)$

② $\forall x \in X, 1_G \rightarrow x = x$.

则称 \rightarrow 是么半群 G 在 X 上的一个作用. G 的幂集

群在其子集上的左乘作用: $G, X \rightarrow 2^X = \{A | A \subseteq G\}$

定义 $g \rightarrow A \triangleq gA \quad G \times 2^G \rightarrow 2^G$ (此时 $X = 2^G$)

验证: $1_G \rightarrow A = 1_G \cdot A = A. \quad (\{1_G \cdot a | a \in A\})$

$(gh) \rightarrow A = (gh)A = \{(gh)a | a \in A\}$.

$g \rightarrow (h \rightarrow A) = h \rightarrow (g \cdot hA) = \{g \cdot (ha) | a \in A\}$.

$G = GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, \text{ 且 } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ 可逆} \right\}$ $x = \mathbb{R}^2$ 例向量 $\therefore A \alpha = A \beta$ $\text{设 } \alpha, \beta \in X, \alpha, \beta \neq 0$ $\text{则 } \exists A \in G, \text{ s.t. } \beta = A\alpha$ $\text{eg. } \alpha = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \beta = \begin{pmatrix} c \\ d \end{pmatrix} \neq 0$ $\text{令 } A = \begin{pmatrix} c & * \\ d & * \end{pmatrix}$ $A\alpha = \begin{pmatrix} c & * \\ d & * \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = \beta$	<p>X 集合, $G = Sym(X)$. $\sigma \rightarrow x = \sigma(x)$</p> <p>验证: $id \rightarrow x = id(x) = x$</p> <p>$(\sigma \circ \tau) \rightarrow x = (\sigma \circ \tau)(x)$</p> <p>$\sigma \rightarrow (\tau \rightarrow x) = \sigma(\tau(x))$</p> <p>共轭作用 $\stackrel{G}{\sim}$</p> <p>$G \times G, g \rightarrow x = gxg^{-1} \quad G \times G \rightarrow G$</p> <p>验证: $l_g \rightarrow x = l_g x l_g^{-1} = x$</p> <p>$gh \rightarrow x = (gh)x(gh)^{-1}$</p> <p>$g \rightarrow (h \rightarrow x) = g \cdot (h \cdot h^{-1})g^{-1} = (gh)x(gh)^{-1}$</p> <p>群在其子集上的共轭作用 $G: X = 2^G \quad g \rightarrow A = gag^{-1} = \{gag^{-1} \mid a \in A\}$.</p> <p>$H \leq G, H \triangleleft G$, 则 $\forall g \in G, ghg^{-1} = h \Leftrightarrow \forall g \in G, g \rightarrow h = h$.</p> <p>作用是传递的</p> <p>$G$ 是群, \sim 作用在 X 上, 在 X 上定义等价关系 $\sim: x \sim y \Leftrightarrow \exists g \in G, \text{ s.t. } y = g \rightarrow x$.</p> <p>验证等价性:</p> <p>自反: $x = l_g \rightarrow x$</p> <p>对称: $x \sim y \quad y = g \rightarrow x, g \in G \quad (y = g \rightarrow x \Leftrightarrow x = g^{-1} \rightarrow y)$</p> <p>$g^{-1} \rightarrow y = g^{-1} \rightarrow (g \rightarrow x) = (g^{-1}g) \rightarrow x = x$.</p> <p>传递: $x \sim y, y \sim z$</p> <p>$y = g \rightarrow x, z = h \rightarrow y, z = h \rightarrow g \rightarrow x = (hg) \rightarrow x \quad \therefore x \sim z$.</p>
---	---