

Sylow 子群

定义 1 (p -群). 设 G 是有限群, p 是素数, 若 $|G| = p^k, k \in \mathbb{N}^+$, 则称 G 是一个 p -群.

引理 1. 设 p -群 G 作用在集合 X 上, 若 $|X| = n$, X 中的不动点个数为 t ($t \in \mathbb{N}$), 则

(1) $t \equiv n \pmod{p}$;

(2) 若 $(n, p) = 1$, 则不动点存在.

证明. (1) 设 $X = \bigsqcup_{i \in I} \text{Orb}(x_i)$. x_i 为不动点当且仅当 $|\text{Orb}(x_i)| = 1$, 于是

$$n = t + \sum_{|\text{Orb}(x_i)| \neq 1} |\text{Orb}(x_i)|.$$

而由轨道-稳定化子定理, $|\text{Orb}(x_i)|$ 能整除 $|G|$, 而 $|G| = p^k$ ($k \in \mathbb{N}^+$), 于是 p 能整除 $|\text{Orb}(x_i)|$. 故 $t \equiv n \pmod{p}$.

(2) 若 $(n, p) = 1$, 则 $n \nmid p$, 由 (1), 得 $t \nmid p$, 则 $t \neq 0$, 即存在不动点. \square

引理 2. 在正整数中, 设 p 是素数, $n = p^l m$, 若 $k \leq l$, 则 p^{l-k} 恰能整除 $C_n^{p^k}$.

证明. 由组合数公式,

$$C_n^{p^k} = \frac{n}{p^k} \prod_{i=1}^{p^k-1} \frac{n-i}{p^k-i},$$

而

$$\frac{n}{p^k} = p^{l-k} m \Rightarrow p^{l-k} \mid C_n^{p^k},$$

设 $1 \leq i \leq p^k - 1$ 表示为 $i = p^t j$, 其中 $(p, j) = 1$, $t < k \leq l$. 则

$$n - i = p^t (p^{l-t} m - j),$$

$$p^k - i = p^t (p^{k-t} - j),$$

于是 $p \nmid \prod_{i=1}^{p^k-1} \frac{n-i}{p^k-i}$, 故 p^{l-k} 恰能整除 $C_n^{p^k}$. \square

下面若无特殊说明, 默认 G 的阶为 $p^l m$, 其中 p 为素数, $(p, m) = 1$, $l \geq 1$.

定理 1 (Sylow 第一定理, 存在性). 若 $1 \leq k \leq l$, 则 G 存在 p^k 阶子群.

证明. 设 G 中所有 p^k 阶子集组成的集合为 \mathcal{X} . 则 $|\mathcal{X}| = C_n^{p^k}$, 这里 $n = p^l m$. 设 G 作用在 \mathcal{X} 上, 则有轨道分解

$$\mathcal{X} = \bigsqcup_{i \in I} \text{Orb}(A_i), \quad A_i \in \mathcal{X}.$$

于是

$$|\mathcal{X}| = \sum_{i \in I} |\text{Orb}(A_i)|.$$

由引理2, 存在 $A \in \mathcal{X}$, $p^{l-k+1} \nmid |\text{Orb}(A)|$. 由轨道-稳定化子定理,

$$p^{l-k+1} \nmid \frac{|G|}{|\text{Stab}(A)|} \Rightarrow p^{l-k+1} \nmid \frac{p^l m}{|\text{Stab}(A)|}.$$

设 $|\text{Stab}(A)| = p^a b$, 其中 $(a, b) = 1$. 则 $p^{l-a} < p^{l-k+1}$, 即 $a > k-1$, $a \geq k$. 于是 $p^k \mid |\text{Stab}(A)|$.

由于 $\text{Stab}(A) < G$, 对任意 $g \in \text{Stab}(A)$, $a \in A$, 定义群 $\text{Stab}(A)$ 对集合 A 的作用 $g \cdot a = ga$. 由于 $\text{Stab}(A) = \{g \in G \mid g \cdot a = a, \forall a \in A\}$, 于是 $ga \in A$. 则 $\text{Stab}(A) \cdot a \subset A$. 而 $\text{Stab}(A)$ 到 $\text{Stab}(A) \cdot a$ 之间是双射, 于是 $|\text{Stab}(A)| = |\text{Stab}(A) \cdot a| \leq |A| = p^k$. 即 $\text{Stab}(A)$ 是一个 p^k 阶子群. \square

定义 2 (Sylow p -子群). 设 G 的阶是 $p^l m$, 其中 p 是素数, 则 G 的 p^l 阶子群称为 G 的 Sylow p -子群.

定理 2 (Sylow 第二定理, 共轭性). 设 P 是 G 的一个 Sylow p -子群, H 是 P 的一个 p^k 阶子群, 则 H 包含于 P 的共轭子群中. 特别地, Sylow p -子群之间互相共轭.

证明. 设 G 作用在 G/P 上, $g \cdot gP = ggP$, 称为左平移作用. 将这个作用限制在 H 上, 则 $h \cdot gP = hgP$. 由于 $|G/P| = m$, $(m, p) = 1$, 由引理1(2), 存在 $gP \in G/P$ 满足 $hgP = gP$. 于是 $hg \in gP$, 即 $h \in gPg^{-1}$, H 包含于 P 的共轭子群中. 特别地, 当 $|H| = p^l$, 则 P 也包含在 H 的共轭子群中, 于是 $H = gPg^{-1}$. \square

定理 3 (Sylow 第三定理, 计数定理). 设 G 的 Sylow p -子群的个数为 k , 则

(1) 当且仅当 $k = 1$ 时, 这个 Sylow p -子群 $P \triangleleft G$;

(2) $k \equiv 1 \pmod{p}$ 且 $k \mid m$.

证明. (1) 设 P 是群 G 的一个 Sylow p -子群. 若 P' 是另外一个 Sylow p -子群, 则由 Sylow 第二定理, 有 $P' \subset \{gPg^{-1} \mid g \in G\}$, 同时有 $P \subset \{gP'g^{-1} \mid g \in G\}$. 若 $k = 1$, 则 $P = gPg^{-1}$, 对任意 $g \in G$ 成立, 于是 $P \triangleleft G$. 反之, 若 $P \triangleleft G$, 则 $P = gPg^{-1}$, 得 $k = 1$.

(2) 设 \mathcal{X} 是群 G 的所有 Sylow p -子群的集合, 群 $P \in \mathcal{X}$ 作用在集合 \mathcal{X} 上的作用为共轭作用. 对任意 $g \in P$,

$$g \cdot P = gPg^{-1} = P,$$

因此 P 是该作用下的一个不动点. 假设 P_1 也是一个不动点, 则对任意 $g \in P$,

$$gP_1g^{-1} = P_1,$$

因此 $g \in N_G(P_1)$, $P \subset N_G(P_1)$. 而 $|P| = p^l$, 于是设 $|N_G(P_1)| = p^l m_1$, 其中 $m_1 \mid m$. 于是 P, P_1 都是 $N_G(P_1)$ 的 Sylow p -子群, 而 $P_1 \triangleleft N_G(P_1)$, 由 (1), 得 $k = 1$, 即 $P = P_1$, 该作用下只有一个不动点. 由引理1(1), 有 $k \equiv 1 \pmod{p}$.

设群 G 在集合 \mathcal{X} 上的作用为共轭作用. 则由 Sylow 第二定理, 对任意 $P_1, P_2 \in \mathcal{X}$, 存在 $g \in G$, 使得

$$P_1 = g \cdot P_2 = gP_2g^{-1},$$

于是 \mathcal{X} 是可传递的. 对任意 $P \in \mathcal{X}$,

$$k = |\mathcal{X}| = |\text{Orb}(P)| = \frac{|G|}{|\text{Stab}(P)|},$$

于是 $k \mid |G|$, 即 $k \mid p^l m$. 而由于 $k \equiv 1 \pmod{p}$, 于是 $(k, p) = 1$, 则 $k \mid m$. □