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 $\boldsymbol{p}$**-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 $X=\bigsqcup\limits_{i\in I}\mathrm{Orb}(x_i)$. x_i 为不动点当且仅当 $|\mathrm{Orb}(x_i)|=1$，于是

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

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

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

证明. 由组合数公式，

$$\mathrm{C}_n^{p^k}=\frac{n}{p^k}\prod_{i=1}^{p^k-1}\frac{n-i}{p^k-i},$$

而

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

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

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

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

于是 $p\nmid\prod\limits_{i=1}^{p^k-1}\dfrac{n-i}{p^k-i}$，故 p^{l-k} 恰能整除 $\mathrm{C}_n^{p^k}$. □

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

定理 1 (Sylow 第一定理，存在性)**.** 若 $1\leqslant k\leqslant l$，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 $|\mathcal{X}|=\mathrm{C}_n^{p^k}$，这里 $n=p^l m$. 设 G 作用在 $\mathcal{X}$ 上，则有轨道分解

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

于是

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

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

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

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

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

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 $H=gPg^{-1}$. □

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 $P\lhd G$;

(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 $P'\subset\left\{gPg^{-1}\mid g\in G\right\}$，同时有 $P\subset\left\{gP'g^{-1}\mid g\in G\right\}$. 若 $k=1$，则 $P=gPg^{-1}$，对任意 $g\in G$ 成立，于是 $P\lhd G$. 反之，若 $P\lhd G$，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 $P_1 \lhd N_G(P_1)$，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 $P \in \mathcal{X}$，

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

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 $k \mid m$. □

下面介绍 Sylow 定理的若干应用.

定义 3 (单群). 没有非平凡正规子群的群称为**单群**。

例 1. 72 阶群不是单群.

证明. 首先，$72 = 2^3 \times 3^2$，设有限群 G 的阶 $|G| = 72$，设 G 的 Sylow 2-子群的个数为 k_1，Sylow 3-子群的个数为 k_2. 由 Sylow 第三定理，k_1 可能为 $1, 3, 9$，k_2 可能为 $1, 4$.

当 $k_1 = 1$ 时，由 Sylow 第三定理 (1)，这个 8 阶的 Sylow 2-子群是 G 的正规子群. 当 $k_2 = 1$ 时，这个 9 阶的 Sylow 3 子群也是 G 的正规子群. 它们都不是平凡的.

当 $k_2 = 4$ 时，设 $X = \{P_1, P_2, P_3, P_4\}$，其中 P_i 是互不相同的 Sylow 3-子群. 设 G 作用在 X 上的作用为共轭作用. 即

$$g \cdot P_i = gP_ig^{-1},\ \forall g \in G,$$

则这个作用决定了一个同态 $\varphi : G \to S_X$.

而 $\ker\varphi \lhd G$，假设 $\ker\varphi = G$，则对任意 $g \in G$，

$$g \cdot P_i = \mathrm{id}(P_i) = P_i,$$

则 Sylow 子群之间不能互相共轭，这与 Sylow 第二定理矛盾.

假设 $\ker\varphi = \{e\}$，则由同态基本定理，

$$G/\ker\varphi \cong \varphi(G),$$

于是

$$|G/\ker\varphi| = |G/e| = |G| = |\varphi(G)| < |S_4| = 24,$$

而 $|G| = 72$，矛盾.

于是 $\ker\varphi$ 是 G 的非平凡正规子群，故 72 阶群不是单群. □

例 2. 56 阶群不是单群.

证明. 首先，$56 = 2^3 \times 7$，设有限群 G 的阶 $|G| = 56$，设 G 的 Sylow 2-子群的个数为 k_1，Sylow 7-子群的个数为 k_2. 由 Sylow 第三定理，k_1 可能为 $1, 7$，k_2 可能为 $1, 8$.

当 $k_1 = 1$ 时，由 Sylow 第三定理 (1)，这个 8 阶的 Sylow 2-子群是 G 的正规子群. 当 $k_2 = 1$ 时，这个 7 阶的 Sylow 7-子群也是 G 的正规子群. 它们都不是平凡的.

当 $k_1 = 7$ 且 $k_2 = 8$ 时，由于素数阶群必为循环群，于是这 8 个 Sylow 7-子群中，除幺元外的 6 个元素都是 7 阶的，且各不相同. 于是一共含有 $|G|$ 中的 $1 + 6 \times 8 = 49$ 个元素. 对任意的一个 Sylow 2-子群，除幺元外含有 7 个元素，且与 Sylow 7-子群中的元素不同. 这就有 $49 + 7 = 56$ 个元素. 而这 7 个 Sylow 2-子群元素不是完全一致的，于是 Sylow 7 子群和 Sylow 8 子群中不重复的元素个数就超过了 56，这与 $|G| = 56$ 矛盾！于是 $k_1 = 1$ 或 $k_2 = 1$，则由上述可知 56 阶群不是单群. □

例 3. 设 $|G| = p^l m$，$(p, m) = 1$，$p > m \neq 1$，则 G 是单群.

证明. 设 G 的 Sylow p-子群的个数为 k，由 Sylow 第三定理，k 的取值只能为 1. 而 $m > 1$，于是 G 的 Sylow p-子群是 G 的 p^l 阶真正规子群. □

注. *k 的取值只能为 1，因为当 k 取 $1 + p$ 时，$1 + p > m$ 于是不能整除. 那么其他取值更不能取到了.*