


# Sylow 定理及其应用

戚天成 

复旦大学 数学科学学院

2023 年 10 月 30 日

这份笔记的目的是记录 Sylow 定理的证明以及相关应用, 该定理以 P. L. Sylow(挪威, 1832-1918) 命名, 是由 Sylow 于 1872 年发表的. 首先让我们回顾一个  $p$ -群作用在有限集上的特性.

**Lemma 1.** 设群  $G$  是  $p$ -群,  $|G| = p^n, n > 0$ , 作用在有限集  $|X|$  上, 记它的不动点集为  $X_0 = \{x \in X | gx = x, \forall g \in G\}$ , 那么  $|X_0| \equiv |X| \pmod{p}$ . 特别地, 若考虑  $p$ -群在自身上的共轭作用, 立即得到  $p$ -群的中心非平凡.

*Proof.* 记  $x \in X$  所在的轨道为  $\mathcal{O}_x$ , 那么

$$|X| = \sum_{|\mathcal{O}_x|=1} |\mathcal{O}_x| + \sum_{|\mathcal{O}_x|>1} |\mathcal{O}_x|.$$

因为每个轨道的长度  $|\mathcal{O}_x|$  都整除  $|G| = p^n$ , 所以当  $|\mathcal{O}_x| \geq 2$  时  $p$  整除  $|\mathcal{O}_x|$ . 于是由  $X_0$  即所有长度为 1 的轨道之并知  $|X_0| \equiv |X| \pmod{p}$ .  $\square$

上述引理表明  $p$ -群作用在一个有限集上, 不动点集元素个数与整个集合元素个数模  $p$  同余. 下面我们使用上述事实证明 Cauchy 定理, 我们将利用 Cauchy 定理及其后面的引理证明 Sylow 定理.

**Cauchy's Theorem.** 给定素数  $p$  以及有限群  $G$ , 若素数  $p$  整除  $|G|$ , 那么  $G$  存在  $p$  阶元.

*Proof.* 作  $S = \{(a_1, a_2, \dots, a_p) \in G^p | a_1 a_2 \cdots a_p = 1_G\}$ , 那么  $|S| = |G|^{p-1}$ , 且  $S_p$  中轮换  $\sigma = (123 \cdots p)$  生成的子群  $\langle \sigma \rangle$  是  $p$  阶群且在  $S$  上有个天然群作用  $\langle \sigma \rangle \times S \rightarrow S, (\tau, (a_1, a_2, \dots, a_p)) \mapsto (a_{\tau(1)}, a_{\tau(2)}, \dots, a_{\tau(p)})$ , 易见该群作用的不动点集  $S_0 = \{(x, x, \dots, x) \in G^p | x^p = 1_G, x \in G\}$  且是非空的, 因为  $(1_G, 1_G, \dots, 1_G) \in S_0$ . 注意到  $|S_0| \equiv |S| \pmod{p}$ , 所以由  $p$  整除  $|S|$  可得  $p$  整除  $|S_0|$ . 故  $|S_0| \geq p$ , 特别地, 取  $a \neq 1_G \in G$  使得  $(a, a, \dots, a) \in S_0$ , 则  $a$  的阶为  $p$ .  $\square$

**Lemma 2.** 给定素数  $p$ , 设有限群  $G$  的子群  $H$  是  $p$ -群, 那么  $[N_G(H) : H] \equiv [G : H] \pmod{p}$ .

*Proof.* 记  $X$  是全体  $H$  在  $G$  中的左陪集构成的集合, 那么  $|X| = [G : H]$ . 将  $H$  通过左乘作用在  $X$  上, 那么  $gH \in X$  在不动点集  $X_0$  中的充要条件是  $hgH = gH, \forall h \in H$ , 因为  $G$  是有限群, 所以这等价于  $g \in N_G(H)$ . 于是  $|X_0| = [N_G(H) : H]$ . 由  $H$  是  $p$ -群可得  $[N_G(H) : H] = |X_0| \equiv |X| = [G : H] \pmod{p}$ .  $\square$

若有限群  $G$  的阶为  $p^r m$ ,  $p$  是素数,  $r, m$  是正整数且  $p$  不整除  $m$ , 则称阶为  $p^r$  的子群  $H$  为  $G$  的一个 Sylow  $p$ -子群. 我们把有限群  $G$  的全体 Sylow  $p$ -子群子群构成的集合记作  $\text{Syl}_p(G)$ .

**Sylow's Theorem.** 设  $G$  是有限群,  $p$  是素数, 设在正整数  $n, m$  使得  $|G| = p^n m$ , 其中  $p$  不整除  $m$ , 则有:

- (1) 任给自然数  $0 \leq i \leq n$ ,  $G$  存在  $p^i$  阶子群, 特别地, Sylow  $p$ -子群存在, 即  $\text{Syl}_p(G) \neq \emptyset$ .
- (2) 任给  $G$  的一个 Sylow  $p$ -子群  $P$  以及  $p$ -子群  $H$ , 存在  $g \in G$  使得  $H \subseteq gPg^{-1}$ . 特别地, 任意两个 Sylow  $p$ -子群在群  $G$  中共轭.
- (3) 记  $n_p = |\text{Syl}_p(G)|$  为 Sylow  $p$ -子群的个数, 则  $n_p \equiv 1 \pmod{p}$  且  $n_p | m$ .

*Proof.* (1) 当  $i = 0$  时结论明显成立. 当  $i = 1$  时由 Cauchy 定理保证了存在  $p$  阶元, 该元素生成的循环群就是  $G$  的一个  $p$  阶子群. 假设  $G$  存在  $p^i$  阶子群  $H_i$ , 这里  $1 \leq i \leq n-1$ , 我们说明  $G$  存在  $p^{i+1}$  阶子群  $H_{i+1}$ . 因为  $H_i$  是  $p$ -群, 所以  $[N_G(H_i) : H_i] = [G : H_i] \pmod{p}$ , 而  $|H_i| = p^i, i \leq n-1$  表明  $p$  整除  $[G : H_i]$ , 所以  $p$  整除  $[N_G(H_i) : H_i]$ . 因此由 Cauchy 定理, 商群  $N_G(H_i)/H_i$  有  $p$  阶元, 进而有  $p$  阶子群  $K$ , 由子群对应定理知存在  $N_G(H_i)$  的子群  $H_{i+1}$  使得  $K = H_{i+1}/H_i$ , 故  $H_{i+1}$  是  $G$  的  $p^{i+1}$  阶子群. 于是结合  $i = 1$  的情形可知 (1) 成立.

(2) 由 (1) 知确实存在 Sylow  $p$ -子群  $P$ . 记  $S$  是全体  $P$  关于  $G$  的左陪集构成的集合, 那么  $p$ -群  $H$  可通过左乘作用在  $S$  上, 不动点集  $S_0$  为  $S_0 = \{gP \in S | g^{-1}Hg \subseteq P\}$ . 由  $|S| = m$  不被  $p$  整除以及  $|S| \equiv |S_0| \pmod{p}$  可知  $S_0$  非空, 所以存在  $g \in G$  使得  $g^{-1}Hg \subseteq P$ , 即  $H \subseteq gPg^{-1}$ , 故 (2) 成立.

(3) 将群  $G$  共轭作用在  $\text{Syl}_p(G)$  上, 由 (2) 知该群作用是传递的, 所以  $n_p$  作为轨道长度整除  $|G|$ . 更进一步, 对每个 Sylow  $p$ -子群  $P$ , 其稳定化子即  $N_G(P) \supseteq P$ , 故

$$n_p = \frac{|G|}{|N_P(G)|} \mid m.$$

下面固定一个 Sylow  $p$ -子群  $P$ , 将其共轭作用在  $\text{Syl}_p(G)$  上, 我们断言  $|\text{Syl}_p(G)_0| = 1$ , 一旦证明该断言, 则  $n_p \equiv 1 \pmod{p}$  成立. 易见  $P \in (\text{Syl}_p(G))_0$ , 对任给  $Q \in (\text{Syl}_p(G))_0$ , 有  $P \subseteq N_G(Q)$ . 因此  $Q, P$  都是正规化子  $N_G(Q)$  的两个 Sylow  $p$ -子群, 由 (2) 知它们在  $N_G(Q)$  中共轭, 故  $P = Q$ . 这就证明了断言.  $\square$

**Remark 3.** 如果  $G$  的 Sylow  $p$ -子群只有一个, 那么它必定是  $G$  的正规子群.

在给出 Sylow 定理的应用前我们引入一个基本的观察.

**Lemma 4.** 若有限群  $G$  的阶为  $2m$ , 其中  $m$  是奇数, 则  $G$  存在指数为 2 的子群.

*Proof.* 将群  $G$  左乘作用在  $G$  上可得群同态  $\rho : G \rightarrow S(G), g \mapsto \rho_g$ . 易见对每个  $g \neq 1_G$ , 有  $\rho_g(c) \neq c, \forall c \in G$ . 设  $f : G = \{g_1, g_2, \dots, g_{2m}\} \rightarrow \{1, 2, \dots, 2m\}, g_k \mapsto k$  为双射, 则  $\gamma : S(G) \rightarrow S_{2m}, \sigma \mapsto f\sigma f^{-1}$  是群同构, 所以  $\psi = \gamma\rho : G \rightarrow S_{2m}$  是单群同态. 由 Cauchy 定理,  $G$  中有 2 阶元  $a$ , 那么  $\psi(a)$  是  $S_{2m}$  中 2 阶元, 故是一些不相交对换的乘积. 因为  $\rho_a$  改变  $G$  中任何元素, 所以  $\psi(a)$  改变集合  $\{1, 2, \dots, 2m\}$  中任何元素, 因此它是  $m$  个不相交对换的乘积, 是奇置换. 从而  $A_{2m} \text{Im}\psi = S_{2m}$ , 进而知  $A_{2m} \cap \text{Im}\psi$  是  $\text{Im}\psi$  指数为 2 的子群, 因此由  $\psi$  是单群同态易知  $G$  有指数为 2 的子群.  $\square$

**Application 5.** 给定有限群  $G$ , 设  $p, q$  是素数.

- (1)(阶为两素数乘积的群不是单群) 如果  $|G| = pq$ , 那么  $G$  不是单群.
  - (2)(阶为一素数平方与素数乘积的群不是单群) 如果  $|G| = p^2q$ , 那么  $G$  不是单群.
- 特别地, 阶为

4, 6, 8, 9, 10, 12, 14, 15, 18, 20, 21, 22, 25, 26, 27, 28, 33, 34, 35, 38, 39, 44, 45, 46, 49, 50, 51, 52, 55, 57, 58

的群不是单群.

*Proof.* (1) 当  $p = q$  时,  $G$  是交换群, 由 Cauchy 定理知  $G$  有  $p$  阶子群, 是非平凡正规子群, 所以  $G$  不是单群. 当  $p > q$  时, 由 Sylow 第三定理, Sylow  $p$ -子群的个数  $n_p$  满足  $n_p | q$  且  $n_p \equiv 1 \pmod{p}$ . 因此  $n_p = 1$ , 即  $G$  有唯一的 Sylow  $p$ -子群, 它是  $G$  的非平凡正规子群, 故  $G$  不是单群. 当  $p < q$  时, 同理可知  $G$  有唯一的 Sylow  $q$ -子群, 它是  $G$  的非平凡正规子群, 故  $G$  不是单群. 于是 (1) 得证.

(2) 若  $p = q$ , 那么  $|G| = p^3$ . 如果  $G$  是交换群, 那么由 Cauchy 定理可知  $G$  有  $p$  阶非平凡正规子群. 如果  $G$  不是交换群, 因为  $p$ -群的中心非平凡, 所以  $Z(G)$  是  $G$  的非平凡正规子群, 于是  $G$  不是单群. 下设  $p \neq q$ , 如果  $p > q$ , 那么 Sylow  $p$ -子群的个数  $n_p$  满足  $n_p | q$  且  $n_p \equiv 1 \pmod{p}$ , 这迫使  $n_p = 1$ , 即  $G$  有唯一的 Sylow  $p$ -子群, 它是  $G$  的非平凡正规子群, 故  $G$  不是单群. 最后我们讨论  $p < q$  的情形.

首先  $G$  的 Sylow  $q$ -子群个数  $n_q$  满足  $n_q | p^2$  且  $n_q \equiv 1 \pmod{q}$ . 那么  $n_q$  只可能是 1 或  $p^2$ . 如果  $n_q = 1$ , 那么  $G$  唯一的 Sylow  $q$ -子群给出了  $G$  的一个非平凡正规子群, 故  $G$  不是单群. 下面考虑  $n_q = p^2$  的情形, 我们断言  $G$  有唯一的 Sylow  $p$ -子群. 因为任意两个 Sylow  $q$ -子群的交只可能是  $\{1_G\}$ , 所以全体 Sylow  $q$ -子群之并所得集合  $A$  有  $p^2(q-1) + 1$  个元素. 任取  $G$  的一个 Sylow  $p$ -子群  $P$ , 它与任何 Sylow  $q$ -子群的交也是  $\{1_G\}$ , 所以  $P \subseteq (G - A) \cup \{1_G\}$ . 注意到  $(G - A) \cup \{1_G\}$  恰好  $p^2$  个元素, 所以  $P = (G - A) \cup \{1_G\}$ , 这说明  $G$  有唯一的 Sylow  $p$ -子群, 断言得证. 由此该 Sylow  $p$ -子群是  $G$  的一个非平凡正规子群, 故  $G$  不是单群.  $\square$

**Application 6.** 设有限群  $G$  阶为 24, 则  $G$  不是单群.

*Proof.* 由 Sylow 第三定理, 全体 Sylow 2-子群构成的集合  $\text{Syl}_2(G)$  元素个数  $n_2 = 1$  或 3. 如果  $n_2 = 1$ , 那么  $G$  有唯一的 Sylow 2-子群, 不是单群. 下设  $n_2 = 3$ , 将  $G$  共轭作用到  $\text{Syl}_2(G)$  上, 该群作用是传递的, 并诱导群同态  $\rho: G \rightarrow \text{Sym}(\text{Syl}_2(G))$ , 易见  $\text{Im} \rho$  至少有两个元素, 这表明  $\text{Ker} \rho$  是  $G$  的真子群. 再由  $G/\text{Ker} \rho \cong \text{Im} \rho$  可得  $|\text{Ker} \rho| \geq 4$ , 所以  $\text{Ker} \rho$  是  $G$  的一个非平凡正规子群.  $\square$

**Application 7.** 60 阶非交换单群总同构于  $A_5$ .

*Proof.* 设  $G$  是 60 阶非交换单群, 则  $G$  的 Sylow 2-子群个数  $n_2 | 15$  且  $n_2$  是奇数, 于是知  $n_2 = 1, 3, 5, 15$ . 由于  $G$  是单群, 所以  $n_2 \neq 1$ . 假设  $n_2 = 3$ , 则将  $G$  共轭作用到  $\text{Syl}_2(G)$  上, 那么该作用导出群同态  $\varphi: G \rightarrow \text{Sym}(\text{Syl}_2(G))$ . 因为该群作用是传递的, 所以  $\text{Ker} \varphi$  是  $G$  的真子群, 由  $G/\text{Ker} \varphi \cong \text{Im} \varphi$  易得  $\text{Ker} \varphi$  至少有 10 个元素, 所以  $\text{Ker} \varphi$  是  $G$  的一个非平凡正规子群, 矛盾. 故  $n_2 \neq 3$ . 最后讨论  $n_2 = 5$  与  $n_2 = 15$  的情形.

我们用反证法说明  $n_2 \neq 15$ . 如果  $n_2 = 15$ , 那么  $G$  存在两个 Sylow 2-子群的交不是平凡的, 因为如果  $G$  的任意两个 Sylow 2-子群交是平凡的, 注意到  $G$  的 Sylow 5-子群有 6 个且 Sylow 5-子群与 Sylow 2-子群一共含有  $6(5-1) + 15(4-1) + 1 = 24 + 45 + 1 = 70$  个元素, 这与  $G$  仅含有 60 个元素矛盾. 设  $S, T$  是  $G$  的 Sylow 2-子群满足  $S \cap T \neq \{1_G\}$ , 那么  $K = S \cap T$  是 2 阶群. 注意到 4 阶群总交换, 所以  $S, T \subseteq C_G(K)$ , 这表明  $C_G(K)$  至少 6 个元素. 事实上  $C_G(K)$  必定是  $G$  的真子群, 否则  $K \subseteq Z(G)$  以及  $G$  非交换得到  $Z(G)$  是  $G$  的非平凡正规子群, 与  $G$  是单群矛盾. 我们断言  $|C_G(K)| \leq 12$ , 若不然, 则  $[G : C_G(K)] < 5$ , 于是  $|G| > [G : C_G(K)]!$ , 这与  $G$  是单群矛盾. 再结合  $4 | |C_G(K)|$  以及  $|C_G(K)| | 60$  可得  $|C_G(K)| = 12$ . 将  $G$  通过左乘作用到  $C_G(K)$  所有左陪集构成的集合  $Y$  上, 那么  $|Y| = 5$  且有单群同态  $\gamma: G \rightarrow S_5$ , 于是知  $G$  与  $S_5$  的一个指数为 2 的子群同构. 但  $S_5$  指数为 2 的正规子群只有  $A_5$ , 所以  $G \cong A_5$ . 这表明  $A_5$  也有 15 个 Sylow 2-子群. 将  $A_5$  共轭作用在  $\text{Syl}_2(A_5)$  上, 因为这个群作用是传递的, 所以对任何  $A_5$  的 Sylow 2-子群  $H$ ,

有  $|N_{A_5}(H)| = 4 = |H|$ , 所以  $N_{A_5}(H) = H$ . 取  $H = \{(1), (12)(34), (14)(23), (13)(24)\}$  是  $A_5$  的一个 Sylow 2-子群, 那么  $(123) \in N_{A_5}(H) - H$ , 这与  $N_{A_5}(H) = H$  矛盾.

根据前面的讨论知  $n_2 = 5$ , 将群  $G$  共轭作用在  $\text{Syl}_2(G)$  上, 由  $G$  是单群可导出单群同态  $\rho: G \rightarrow S_5$ , 于是知  $G$  同构于  $S_5$  的一个指数为 2 的子群, 即  $A_5$ , 故  $G \cong A_5$ .  $\square$

**Application 8.** 180 阶群不可能是单群.

*Proof.* 假设群  $G$  是 180 阶单群, 那么  $G$  的 Sylow 3-子群个数  $n_3$  只可能是 4 或 10. 假设  $n_3 = 4$ , 将  $G$  共轭作用到  $\text{Syl}_3(G)$  上可得群同态  $\rho: G \rightarrow \text{Sym}(\text{Syl}_3(G))$ , 因为该作用是传递的, 且  $G$  是单群, 所以  $\rho$  是单射, 从而  $180 = |G| \leq 4! = 24$ , 矛盾. 所以  $n_3 = 10$ . 我们断言  $G$  的任何两个 Sylow 3-子群之交是平凡群, 若不然, 则存在 Sylow 3-子群  $S, T$  使得  $K = S \cap T$  是 3 阶群. 因为 9 阶群必交换, 所以  $S, T \subseteq C_G(K)$ . 由  $S, T \subseteq C_G(K)$  可得  $|C_G(K)| \geq 15$ . 由  $G$  是单群易证  $C_G(K)$  是真子群, 于是可知  $|C_G(K)| \leq 30$ , 若不然, 则  $[G : C_G(K)] < 6$ , 进而  $|G| = 180 > 5! \geq [G : C_G(K)]!$ , 这与  $G$  是单群矛盾. 因此, 由  $15 \leq |C_G(K)| \leq 30$  并结合  $9 \mid |C_G(K)|, |C_G(K)| \mid 180$  可知  $|C_G(K)| = 18$ . 于是知  $C_G(K)$  的 Sylow 3-子群只有一个, 这与  $S, T$  都是它的 Sylow 3-子群矛盾. 因此, 我们得到  $G$  的任何两个 Sylow 3-子群之交是平凡群. 下证  $G$  的 Sylow 5-子群个数  $n_5 = 6$ . 首先由 Sylow 第三定理容易得到  $n_5 = 1, 6, 36$ . 而  $G$  是单群, 这迫使  $n_5$  只可能是 6 或 36. 下面用反证法说明  $n_5 \neq 36$ . 假设  $n_5 = 36$ , 由任意两个 Sylow 3-子群之交平凡可知全体 Sylow 3-子群与 Sylow 5-子群之并有  $10(9-1) + 36(5-1) + 1 = 225 > 180$ , 这与  $|G| = 180$  矛盾. 由此我们得到  $n_3 = 10, n_5 = 6$ . 将  $G$  共轭作用在集合  $\text{Syl}_5(G)$  上, 可得单群同态  $\alpha: G \rightarrow S_6$ . 我们断言  $\alpha(G) \subseteq A_6$ , 否则,  $\alpha(G)A_6 = S_6$  易得  $G$  有指数为 2 的子群  $\alpha^{-1}(\text{Im}\alpha \cap A_6)$ , 这与  $G$  是单群矛盾. 故  $A_6$  有指数为 2 的子群  $\text{Im}\alpha$ , 这和  $A_6$  是单群矛盾.  $\square$