群论笔记 Chapter 3: Sylow 定理的详细证明与应用

整理自抽象代数笔记

2025 年 12 月 2 日

目录

本章导读

Sylow 定理 (西罗定理) 是有限群论中关于子群结构最深刻的定理之一，它构成了拉格朗日定理 (Lagrange's Theorem) 的某种“逆命题”。

- 拉格朗日定理告诉我们子群的阶整除群的阶，但反之不一定成立。
- Sylow 定理告诉我们，对于素数幂 p^n，如果它是群阶数的最大 p 因子，那么一定存在该阶数的子群，且这些子群具有极强的对称性（共轭）。

本文将利用**群作用 (Group Action)** 的观点，详细证明 Sylow 第一、第二、第三定理。

预备知识：群作用与不动点

在证明 Sylow 定理之前，我们需要一个关于 p-群作用的关键引理。

引理 0.1 (p-群作用的不动点引理). *设 G 是一个 p-群（即 $|G| = p^k$），X 是一个有限集合，G 作用在 X 上。记 X^G 为 G 作用下的不动点集合，即 $X^G = \{x \in X \mid g \cdot x = x, \forall g \in G\}$。则有：*

$$|X| \equiv |X^G| \pmod p$$

证明. 根据轨道-稳定子定理，集合 X 可以分解为若干个不相交轨道的并：$X = \bigcup_i \mathrm{Orb}(x_i)$。轨道的大小 $|\mathrm{Orb}(x_i)| = [G : \mathrm{Stab}(x_i)]$ 必须整除 $|G|$，因此轨道大小是 p 的幂。

- 如果 $x \in X^G$，则其轨道大小为 1。
- 如果 $x \notin X^G$，则其轨道大小为 p 的倍数（因为是 p 的幂且大于 1）。

因此：

$$|X| = \sum_{x \in X^G} 1 + \sum_{x \notin X^G} |\mathrm{Orb}(x)| = |X^G| + k \cdot p$$

即 $|X| \equiv |X^G| \pmod p$。 □

Sylow 第一定理：存在性

1 Sylow 第一定理 (Sylow I)

定义 1.1 (Sylow p-子群). *设 G 是有限群，其阶数为 $|G| = p^n m$，其中 p 是素数且 $\gcd(p, m) = 1$。若 G 的子群 P 的阶数为 p^n，则称 P 为 G 的一个* ***Sylow*** **p-子群。**

定理 1.2 (Sylow 第一定理). *设 G 是有限群，p 是素数。如果 p^n 是整除 $|G|$ 的 p 的最高次幂，那么 G 必包含一个阶为 p^n 的子群（即 Sylow p-子群存在）。*

1.1 证明思路：归纳法与类方程

我们对群的阶数 $|G|$ 进行归纳。

- **基础：**当 $|G| = 1$ 或 p 时，结论显然成立。
- **归纳假设：**假设对于所有阶数小于 $|G|$ 的群，定理成立。

考虑群 G 的类方程 (Class Equation)：

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)]$$

其中 $Z(G)$ 是中心，g_i 是非中心元素的代表元。

情形 1：p 整除 $|Z(G)|$

1. 根据柯西定理 (Cauchy's Theorem) 的阿贝尔群版本，由于 $Z(G)$ 是阿贝尔群且 $p \mid |Z(G)|$，必存在一个阶为 p 的正规子群 $N \leq Z(G)$。
2. 考虑商群 $\bar{G} = G/N$。其阶数为 $|\bar{G}| = p^n m/p = p^{n-1}m$。
3. 由归纳假设，$\bar{G}$ 包含一个阶为 p^{n-1} 的子群 $\bar{P}$。
4. 根据对应定理，存在 G 的子群 P 使得 $P/N = \bar{P}$。
5. $|P| = |\bar{P}| \cdot |N| = p^{n-1} \cdot p = p^n$。证毕。

情形 2：p 不整除 $|Z(G)|$

1. 回看类方程：$|G| = |Z(G)| + \sum [G : C_G(g_i)]$。
2. 由于 $p \mid |G|$ 且 $p \nmid |Z(G)|$，必然存在至少一个非中心元素 g_i，使得 $p \nmid [G : C_G(g_i)]$。

3. 记 $H = C_G(g_i)$。由于 $g_i \notin Z(G)$，则 $H \subsetneq G$（真子群）。

4. 由于 $|G| = [G : H] \cdot |H| = p^n m$，且 p 不整除 $[G : H]$，这意味着 p^n 必须完全整除 $|H|$。即 H 的 p 部分与 G 相同。

5. 由归纳假设，H 包含一个阶为 p^n 的子群 P。

6. 由于 $P \leq H \leq G$，则 P 也是 G 的 Sylow p-子群。

$\square$

Sylow 第二定理：共轭性与包含性

2 Sylow 第二定理 (Sylow II)

Sylow 第二定理揭示了 Sylow p-子群之间的紧密联系：它们不仅存在，而且彼此“长得一样”（共轭）。

定理 2.1 (Sylow 第二定理). *设 G 是有限群。*

1. *G 的任意两个 Sylow p-子群都是***共轭***的。即若 $P_1, P_2 \in \mathrm{Syl}_p(G)$，则存在 $g \in G$，使得 $P_2 = gP_1g^{-1}$。*

2. *G 的任意一个 p-子群都包含在某个 Sylow p-子群中。*

2.1 证明：利用左陪集的作用

设 P 是 G 的一个 Sylow p-子群（由 Sylow I 知其存在）。设 Q 是 G 的**任意**一个 p-子群。

注意 (NOTE): 证明策略

我们让小群 Q 作用在大群的陪集空间 G/P 上，通过寻找不动点来锁定位置。

1. 考虑左陪集集合 $X = G/P = \{gP \mid g \in G\}$。

2. 集合大小 $|X| = [G : P] = \frac{p^n m}{p^n} = m$。注意 $\gcd(p, m) = 1$，即 p **不整除** $|X|$。

3. 让 p-子群 Q 通过左乘作用在 X 上：

$$q \cdot (gP) = (qg)P, \quad \forall q \in Q$$

4. 应用 p-**群作用的不动点引理**：

$$|X^Q| \equiv |X| \pmod p$$

由于 $p \nmid |X|$，必有 $|X^Q| \neq 0$。即**至少存在一个不动点**。

5. 设 gP 是 Q 作用下的一个不动点。这意味着：

$$\forall q \in Q, \quad qgP = gP$$

$$\implies g^{-1}qgP = P$$

$$\implies g^{-1}qg \in P$$

$$\implies q \in gPg^{-1}$$

6. 因此，对于任意 $q \in Q$，都有 $q \in gPg^{-1}$。即：

$$Q \subseteq gPg^{-1}$$

结论推导：

- **证明包含性：**上述逻辑直接证明了任意 p-子群 Q 都包含在 P 的某个共轭子群 gPg^{-1} 中（这也是一个 Sylow p-子群）。
- **证明共轭性：**如果 Q 本身也是一个 Sylow p-子群，则 $|Q| = |gPg^{-1}| = p^n$。由于 $Q \subseteq gPg^{-1}$ 且二者阶数相同（有限），故必有 $Q = gPg^{-1}$。证毕。

$\square$

Sylow 第三定理：计数

3 Sylow 第三定理 (Sylow III)

第三定理给出了 Sylow p-子群数量的限制条件，这在判断群的单性（Simplicity）时极为有力。

定理 3.1 (Sylow 第三定理)**.** *设 n_p 是 G 中 Sylow p-子群的个数。则：*

1. $n_p \equiv 1 \pmod p$
2. $n_p = [G : N_G(P)]$，*从而* $n_p \mid |G|$（*实际上* $n_p \mid m$）。

3.1 证明：共轭作用与不动点

令 $S = \mathrm{Syl}_p(G)$ 为 G 中所有 Sylow p-子群构成的集合。由 Sylow II 可知，G 通过共轭作用在 S 上是**传递**的 (Transitive)。

步骤 1：证明 $n_p = [G : N_G(P)]$

- 取固定 $P \in S$。S 是 P 在 G 共轭作用下的轨道。
- 根据轨道-稳定子定理：

$$n_p = |S| = |\mathrm{Orb}(P)| = [G : \mathrm{Stab}(P)] = [G : N_G(P)]$$

- 这直接说明了 n_p 是 $|G|$ 的因子。

步骤 2：证明 $n_p \equiv 1 \pmod p$

- 既然 S 是 G 的作用集合，我们限制由子群 P（它是 p-群）作用在 S 上（通过共轭）。
- 应用不动点引理：$|S| \equiv |S^P| \pmod p$。
- 显然 P 自身是一个不动点，因为 $xPx^{-1} = P, \forall x \in P$。所以 $P \in S^P$。
- **关键问题：**是否还有其他不动点？
- 假设 $Q \in S$ 是 P 作用下的不动点，即 $\forall x \in P, xQx^{-1} = Q$。这意味着 $P \subseteq N_G(Q)$。
- 考察群 $N_G(Q)$。P 和 Q 都是 $N_G(Q)$ 的子群。
  - Q 是 $N_G(Q)$ 的 Sylow p-子群（显然）。

- P 是 p-子群，根据 Sylow II，它包含在 $N_G(Q)$ 的某个 Sylow p-子群中。
- 但注意 $Q \trianglelefteq N_G(Q)$（正规化子的定义），所以 Q 是 $N_G(Q)$ 中**唯一**的 Sylow p-子群。
- 因此，必须有 $P \subseteq Q$。

- 由于 $|P| = |Q| = p^n$，故 $P = Q$。
- 这说明 $S^P = \{P\}$，即不动点只有一个。
- 结论：$n_p = |S| \equiv 1 \pmod p$。

□

直观理解：应用示例

证明 $|G| = 15$ 的群必定是循环群。

- $|G| = 3 \times 5$。
- $n_3 \mid 5$ 且 $n_3 \equiv 1 \pmod 3 \implies n_3 = 1$。记为 $P_3 \trianglelefteq G$。
- $n_5 \mid 3$ 且 $n_5 \equiv 1 \pmod 5 \implies n_5 = 1$。记为 $P_5 \trianglelefteq G$。
- 因为正规且阶互素，$P_3 \cap P_5 = \{e\}$ 且 $xy = yx$。
- $G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$。

例题：pq 阶群的可解性

例 3.2 (pq 阶群的可解性). **命题：** *设 $|G| = pq$，其中 p 和 q 是素数，且 $p < q$。证明 G 是可解群。*

证明： 要证明 G 可解，我们需要构造一个正规列 $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G$，使得每个商群 G_{i+1}/G_i 都是阿贝尔群。

1. **寻找正规子群：** *根据 Sylow 第三定理，考察 Sylow q-子群的个数 n_q：*

$$n_q \equiv 1 \pmod q \quad \text{且} \quad n_q \mid p$$

由于 p 是素数，其因子只有 1 和 p。又因为 $p < q$，显然 $p \not\equiv 1 \pmod q$。因此，唯一的可能性是 $n_q = 1$。

*这意味着 G 存在**唯一**的 Sylow q-子群，记为 Q。由 Sylow 第二定理的推论可知，唯一的 Sylow 子群必是正规子群，即 $Q \trianglelefteq G$。*

2. **构造正规列**：我们构造如下群列：

$$\{e\} \trianglelefteq Q \trianglelefteq G$$

3. **验证商群性质**：

   - 因子群 $Q/\{e\} \cong Q$：其阶数为 q（素数）。素数阶群必为循环群，因此是阿贝尔群。
   - 因子群 G/Q：其阶数为 $|G|/|Q| = pq/q = p$（素数）。素数阶群必为循环群，因此也是阿贝尔群。

4. **结论**：由于该正规列的所有商群均为阿贝尔群，根据定义，G 是一个可解群。

注意 *(NOTE)*: *Burnside* 引理的推广

这个例子其实是著名的 ***Burnside*** p^aq^b **定理** 的一个特例。*Burnside* 证明了所有阶数为 p^aq^b 的群都是可解群。虽然 pq 阶的情形用 *Sylow* 定理就能轻松解决，但通用的 p^aq^b 证明需要用到表示论（*Character Theory*）。

本章导读

有限单群分类是数学史上的宏伟工程。本节我们探讨一个基础但重要的问题：**最小的"复杂"群在哪里？**

- 我们将证明阶数小于 60 的群（除了素数阶群）都不可能是单群。
- 我们将利用共轭类方程证明 A_5（阶数为 60）是单群，这是数学中第一个非阿贝尔单群。

注：当我们讨论"非单群"时，如果群是阿贝尔群，则只要它不是素数阶，它就不是单群。本节重点在于排除**非阿贝尔**的情形。

Part 1: 为什么 60 阶以下的群不是非阿贝尔单群？

要证明 $|G| < 60$ 的群（非素数阶）都有非平凡正规子群，我们可以利用 Sylow 定理进行逐个击破。

4 各类阶数的排除法

4.1 1. p^k 阶群 (素数幂)

结论：若 $|G| = p^k$ $(k > 1)$，则 G 不是单群。**理由：** p-群的中心 $Z(G)$ 是非平凡的（类方程结论）。

- 如果 $Z(G) \neq G$，则 $Z(G)$ 是正规子群。
- 如果 $Z(G) = G$，则 G 是阿贝尔群。此时若 $k > 1$，则存在阶为 p 的子群，也是正规的。

排除阶数： 4, 8, 9, 16, 25, 27, 32, 49 等。

4.2 2. pq 阶群与 pqr 阶群

我们之前已经证明 $|G| = pq$ 的群是可解的（必定存在正规 Sylow 子群）。对于 $|G| = pqr$（三个素数乘积），Burnside 证明了它们也是可解的。**排除阶数：**6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58。

4.3 3. $2m$ 阶群 (其中 m 为奇数)

定理 4.1. *设 G 是有限群，若 $|G| = 2m$ 且 m 是奇数，则 G 必有一个指数为 2 的正规子群（阶数为 m）。*

定理 4.2. *设 G 是一个有限群，其阶数为 $|G| = 2m$，其中 m 是***奇数***。则 G 必包含一个阶数为 m 的正规子群（即指数为 2 的正规子群）。特别地，G 不是单群。*

4.3.1 详细证明过程

我们利用 **Cayley 定理**和 **正则表示 (Regular Representation)** 将群元素视为置换，通过分析置换的奇偶性来构造正规子群。

Step 1: 寻找 2 阶元素
根据 **柯西定理 (Cauchy's Theorem)**，因为 $2 \mid |G|$，所以在群 G 中必然存在一个阶为 2 的元素 t。即存在 $t \in G$ 使得 $t \neq e$ 且 $t^2 = e$。

Step 2: 构造左正则表示
考虑 Cayley 定理给出的左正则表示。我们要把 G 看作是其自身集合上的置换群。定义映射 $\lambda_t : G \to G$，规则为左乘 t：

$$\lambda_t(x) = tx, \quad \forall x \in G$$

显然 λ_t 是集合 G 上的一个双射（置换），即 $\lambda_t \in S_{|G|} = S_{2m}$。

Step 3: 分析 λ_t 的轮换分解
我们需要知道置换 λ_t 长什么样。

- 对于任意 $x \in G$，λ_t 将 x 映射为 tx。
- 再作用一次：$\lambda_t(tx) = t(tx) = t^2x = ex = x$。

这意味着 λ_t 中的循环都是长度为 2 的 **对换 (Transposition)**，形式为 (x, tx)。**有没有不动点？** 假设 x 是不动点，即 $tx = x$。两边右乘 x^{-1} 得 $t = e$，矛盾。因此，λ_t 没有不动点。

结论： 由于 $|G| = 2m$，且没有不动点，所有元素都两两配对。λ_t 恰好由 $\frac{2m}{2} = m$ 个不相交的对换组成：

$$\lambda_t = (x_1, tx_1)(x_2, tx_2) \cdots (x_m, tx_m)$$

Step 4: 奇置换的判定
回顾置换的奇偶性定义：

- 一个置换如果能分解为偶数个对换之积，则为偶置换（符号为 1）。
- 一个置换如果能分解为奇数个对换之积，则为奇置换（符号为 -1）。

在 Step 3 中我们得出 λ_t 是 m 个对换的乘积。**关键条件：** 题目给定 m **是奇数**。因此，λ_t 是一个**奇置换**。

Step 5: 构造同态并寻找核
考虑 G 到置换群 S_{2m} 的左正则同态 $\rho : G \to S_{2m}$，再复合上符号同态 $\mathrm{sgn} : S_{2m} \to \{1, -1\}$。定义复合映射 $\Phi : G \to \{1, -1\}$ 为：

$$\Phi(g) = \mathrm{sgn}(\lambda_g)$$

这是一个群同态。

- 因为 $\Phi(t) = \mathrm{sgn}(\lambda_t) = -1$（由 Step 4 知它是奇置换），所以这个同态是**满射**。

- 像集是 $\{1, -1\}$，同构于 $\mathbb{Z}_2$。

令 $N = \ker \Phi$。根据群同态基本定理：

$$G/N \cong \{1, -1\}$$

这意味着 $|G|/|N| = 2$，即 $|N| = |G|/2 = m$。

Step 6: 结论
N 是同态的核，因此 N 是 G 的**正规子群**。因为 $|N| = m \neq 1$ 且 $|N| \neq |G|$（因为 $m \geq 1$ 且 $t \notin N$），所以 N 是非平凡正规子群。故 G 不是单群。

直观理解：直观理解

想象你在给群里的元素排队。左乘 t 相当于把所有人两两交换位置。因为总共有 m 对人，且 m 是奇数，如果你数一下交换的次数，是奇数次。这种“奇数次交换”的性质在群的乘法下是能够保持的，这暗示了群内部有一个更小的结构（偶置换构成的子群）把群分成了两半。

理由 (Cayley 定理推广)： G 作用在自身上等价于嵌入 S_{2m}。根据正则表示，阶为 2 的元素对应 m 个对换的乘积。因为 m 是奇数，这是一个奇置换。包含奇置换的群必包含指数为 2 的交错群子群。**排除阶数：** 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58。

4.4 4. 困难关卡：排除 30, 36, 48, 56

剩下的几个合数阶需要 Sylow 定理的精细操作。

例 4.3 (排除 $|G| = 30$)**.** $30 = 2 \cdot 3 \cdot 5$。

- $n_5 \equiv 1 \pmod 5$ 且 $n_5 \mid 6 \implies n_5 \in \{1, 6\}$。
- $n_3 \equiv 1 \pmod 3$ 且 $n_3 \mid 10 \implies n_3 \in \{1, 10\}$。

假设 G 是单群，则 $n_5 = 6, n_3 = 10$。

- *阶为 5 的元素个数：$6 \times (5-1) = 24$。*
- *阶为 3 的元素个数：$10 \times (3-1) = 20$。*
- *总元素：$24 + 20 = 44 > 30$。矛盾！*

故必有 $n_5 = 1$ 或 $n_3 = 1$，即存在正规子群。

例 4.4 (排除 $|G| = 56$). $56 = 2^3 \cdot 7$。

- $n_7 \equiv 1 \pmod 7$ 且 $n_7 \mid 8 \implies n_7 \in \{1, 8\}$。

假设 G 是单群，则 $n_7 = 8$。

- 阶为 *7* 的元素个数：$8 \times 6 = 48$。
- 剩下的元素个数：$56 - 48 = 8$。

这剩下的 *8* 个元素必须组成唯一的 *Sylow 2*-子群（因为 *Sylow 2*-子群阶数就是 *8*）。既然是唯一的，它就是正规子群。矛盾。

例 4.5 (排除 $|G| = 48$). $48 = 2^4 \cdot 3$。

- $n_2 \equiv 1 \pmod 2$ 且 $n_2 \mid 3 \implies n_2 \in \{1, 3\}$。

假设 G 是单群，则 $n_2 = 3$。令 G 作用在 *Sylow 2*-子群的集合 $S = \{P_1, P_2, P_3\}$ 上。这诱导了一个同态 $\phi : G \to S_3$。

- $|G| = 48$，而 $|S_3| = 6$。
- 根据同态基本定理，$|\ker \phi| \geq 48/6 = 8$。
- $\ker \phi$ 是 G 的正规子群。矛盾。

Part 2: 60 阶群 A_5 是单群

现在我们来到群论的一个里程碑：证明 A_5 是单群。注意：并非所有 60 阶群都是单群（例如 $\mathbb{Z}_{60}$），我们要证明的是 A_5 这个特定的群是单群。

5 A_5 的结构与单性证明

5.1 1. A_5 的元素分类

A_5 是 S_5 中所有偶置换构成的群，$|A_5| = 60$。我们要分析它的**共轭类**。注意：在 S_5 中共轭的元素在 A_5 中未必共轭（如果用来共轭的元素是奇置换）。

类型	置换形状	计算公式	数量
单位元	(1)	1	1
3-轮换	(abc)	$\frac{5\times4\times3}{3}$	20
双对换	$(ab)(cd)$	$\frac{1}{2}\binom{5}{2}\binom{3}{2}$	15
5-轮换	$(abcde)$	$\frac{5!}{5}=24$	**12 + 12**

注意 (NOTE): 5-轮换的分裂

在 S_5 中，所有 24 个 5-轮换都在同一个共轭类。但在 A_5 中，它们分裂成了两个大小为 12 的共轭类。**原因：** 5-轮换 $\sigma=(12345)$ 的中心化子 $C_{S_5}(\sigma)=\langle\sigma\rangle$，大小为 5。这 5 个元素都是偶置换。这意味着没有奇置换能与 σ 交换。根据群论判定准则，该共轭类在 A_5 中分裂为两半。

最终 A_5 的共轭类大小为：

$$1,\quad 15,\quad 20,\quad 12,\quad 12$$

5.2 2. 证明单性 (Simplicity)

定理 5.1. *A_5 是单群。*

证明. 利用反证法和正规子群的性质。

证明步骤：性质回顾

正规子群 N 必须是若干个完整共轭类的并集。而且 N 必须包含单位元类 $\{1\}$。即 $|N|=1+\sum$(某些类的大小)。同时，根据拉格朗日定理，$|N|$ 必须整除 $|G|=60$。

证明步骤：组合尝试

类的大小集合为 $C=\{15,20,12,12\}$。我们需要选取若干个数字，加上 1，使得和为 60 的因子。60 的因子有：1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60。
让我们尝试所有可能的组合：

- 最小的非单位元类是 12。$1+12=13$ (不是因子)。
- $1+15=16$ (不是因子)。
- $1+20=21$ (不是因子)。
- $1+12+12=25$ (因子只有 1, 5, 25... 不是 60 的因子)。

- $1 + 12 + 15 = 28$ (不是因子)。
- $1 + 12 + 20 = 33$ (不是因子)。
- $1 + 15 + 20 = 36$ (不是因子)。
- $1 + 12 + 12 + 15 = 40$ (不是因子)。
- $1 + 12 + 12 + 20 = 45$ (不是因子)。
- $1 + 15 + 20 + 12 = 48$ (不是因子)。

显然，没有任何一种组合（除了只取 1 或全取）能使得总和整除 60。

证明步骤：结论

由于找不到合适的共轭类组合来构成正规子群 N（除了 $\{1\}$ 和 G），因此 A_5 没有任何非平凡正规子群。A_5 **是单群。**

$\square$

直观理解：历史地位

A_5 是**最小的非阿贝尔单群**。这一事实导致了五次方程没有根式解（Galois 理论）。因为 S_5 的可解性取决于 A_5 的性质，而 A_5 是单群且非阿贝尔，打断了可解正规列。