Sylow 定理

群作用的应用

livi

2026 年 1 月 20 日

1. 群作用工具准备
2. sylow 定理

设 G 是群，Ω 是一个集合，如果 $f: G \times \Omega \to \Omega, (g,x) \mapsto g \cdot x$ 满足

$$e_G \cdot x = x, \quad \forall x \in \Omega$$
$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x), \quad \forall g_1, g_2 \in G$$

则称 f 是 G 在 Ω 上的一个作用, 以后简记 $g \cdot x = gx$. 从同态角度来看，G 在 Ω 上作用全体与 $\mathrm{Hom}(G, S_\Omega)$ 有一一对应关系.
设 G 在 Ω 上有个作用，则对任意 $x \in \Omega$，称

$$Gx = \{gx \mid g \in G\}$$

是 x 的轨道. 称

$$G_x = \{g \in G \mid gx = x\} < G$$

是 x 的稳定子群.

在 Gx 中，有

$$g_1 x = g_2 x \iff g_2^{-1} g_1 \in G_x \iff g_1 G_x = g_2 G_x$$

于是 $|G_x| = [G : G_x] = \dfrac{|G|}{|G_x|}$(当 G 是有限群时). 如果 $|Gx| = 1$，即 $G_x = G$，则称 x 为 G 的不动点.
对任意 $x, y \in \Omega$，有简单的事实：$Gx = Gy$ 或者 $Gx \cap Gy = \varnothing$，于是有

$$\Omega = \bigcup_{x \in \Omega} Gx = \bigcup_{x \in R} Gx$$

其中 R 表示一个代表系，即对任意 $x, y \in R$，有 $Gx \cap Gy = \varnothing$，最终我们得到

$$|\Omega| = \sum_{x \in R} |Gx| = \sum_{x \in R} \frac{|G|}{|G_x|} = |X_0| + \sum_{x \in R \setminus X_0} \frac{G}{|G_x|} \tag{1}$$

其中 X_0 是 G 的不动点集.

1. 群作用工具准备
2. sylow 定理

Cauchy

引理 1

设 G 是有限群，p 是 $|G|$ 的一个素因子，则 G 中有 p 阶元.

证明.

考虑集合

$$X = \{(a_1, \cdots, a_p) \mid a_i \in G, a_1 \cdots a_p = e\}$$

则 $|X| = |G|^{p-1}$. 设 $\sigma = (12 \cdots p)$，则 $|\langle\sigma\rangle| = p$，考虑 $\langle\sigma\rangle$ 在 X 中的作用为

$$\sigma(a_1, \cdots, a_p) = (a_{\sigma(1)}, \cdots, a_{\sigma(p)}) = (a_2, \cdots, a_n, a_1) \in X$$

则该作用下每个轨道元素个数只能是 p 或 1，若记 X_0 是 $\langle\sigma\rangle$ 的不动点集，则由(1)有，p 整除 $|G|^{p-1} - |X_0|$, 于是 $p \mid |X_0|$，且 $|X_0| \neq 0$（因为 $(e, \cdots, e) \in X_0$），所以存在 $a \neq e$，使得 $a^p = e$，这意味着 a 的阶为 p. □

定理 2 (sylow1)

设 G 是有限群，$p^k \mid |G|$，则 G 中有 p^k 阶群.

证明.

对群 G 的阶进行归纳，假设结论对阶数小于 $|G|$ 的群成立. 考虑 G 到自身的共轭作用，则该作用下 G 的不动点集为 $C(G)$, 由 (1)就有

$$|G| = |C(G)| + \sum_{g \in R, g \notin C(G)} [G : C(g)]$$

- 若 $p||C(G)|$，由 [引理，1]，$|C(G)|$ 中有 p 阶元 a，且 $\langle a \rangle \lhd G$，于是可以考虑商群 $G/\langle a \rangle$ ，那么由归纳假设 $G/\langle a \rangle$ 中有 p^{k-1} 阶群 $H/\langle a \rangle$，则 $|H| = |H : \langle a \rangle| \cdot |\langle a \rangle| = p^k$，即 H 是 G 的 p^k 阶群.
- 若 $p \nmid |C(G)|$，则存在 $g \notin C(G)$，使得 $p \nmid [G : C(g)]$，于是 $p^k \mid C(g)$. 由于 $|C(g) < |G|$，则由归纳假设 $C(g)$ 中有 p^k 阶子群 H, 其自然也是 G 的 p^k 阶子群.

$\square$

设 $|G| = p^k m$，其中 $(p, m) = 1$，则 [定理，2] 说明了 G 中 p^k 阶群的存在性，我们称 G 中的 p^k 阶群为 G 的 sylow-p 群.

定理 3 (sylow2)

设 G 是有限群，且 $|G| = p^k m, (p, m) = 1$，则 G 的 *sylow-p* 群相互共轭.

证明.

设 H 是 G 的一个 sylow-p 群. 对任意 G 的 sylow-p 群 K，考虑 K 在 G/H 上的左诱导作用：$k(gH) := (kg)H$. 记 X_0 为 K 的不动点集，则 $(|K|, |G/H|) = 1$，且由(1)有

$$|G/H| \equiv |X_0| \pmod{p}$$

于是 $|X_0| \neq 0$，即 K 有不动点 gH：满足对任意 $k \in K$，有 $kgH = gH$，即 $g^{-1}kg \in H$，即 $k \in gHg^{-1}$，从而 $K \subset gHg^{-1}$，比较两边元素个数就有 $K = gHg^{-1}$. $\square$

由 [定理，3]，$S = \left\{ gHg^{-1} \mid g \in G \right\}$ 即是 G 所有 Sylow-p 群，且

$$g_1 H g_1^{-1} = g_2 H g_2^{-1} \iff g_2^{-1} g_1 \in N_G(H) \iff g_1 N_G(H) = g_2 N_G(H)$$

即 $|S| = [G : N_G(H)] \mid m$，是 G 所有不同的 Sylow-p 群个数.

定理 4 (sylow3)

设 G 是有限群，$|G| = p^k m, (p, m) = 1$，记 n_p 是 G 的 *sylow-p* 群个数，则 $n_p \equiv 1 \pmod p$.

证明.

设 H 是 G 的一个 sylow-p 群，考虑 H 在 $S=\{gHg^{-1} \mid g\in G\}$ 上的共轭作用：

$$h(gHg^{-1}) := hgH(hg)^{-1}.$$

设 gHg^{-1} 是 H 一个不动点，则对任意 $h\in H$，有

$$(hg)H(hg)^{-1} = gHg^{-1}$$

即 $g^{-1}Hg\subset N_G(H)$，也就是说 $g^{-1}Hg$ 也是 $N_G(H)$ 的 Sylow-p 群，但注意 $N_G(H)$ 的 sylow-p 群的个数为 $[N_G(H):N_G(H)]=1$，且 H 就是 $N_G(H)$ 的一个 sylow-p 群，于是就有 $g^{-1}Hg=H$，那么

$$gHg^{-1} = g(g^{-1}Hg)g^{-1} = H.$$

则 H 的不动点只有一个，由(1)就有 $n_p\equiv 1 \pmod{p}$. □