0.1 Sylow 子群

定义 0.1 (p 群)

设 p 是素数. 若群 G 的阶是 p 的方幂, 即 $|G| = [G : e] = p^k(k \in \mathbf{N})$, e 为 G 的幺元, 则称 G 是一个 ***p* 群**.

定理 0.1

设 p 群 G 作用在集合 X 上, $|X| = n, t = |\{x \in X \mid g(x) = x, \forall g \in G\}|$, 则有下列结论:

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

(2) 当 $(n, p) = 1$ 时, $t \geqslant 1$, 即 $\exists x \in X$, 使 $g(x) = x(\forall g \in G)$;

(3) G 的中心 $C(G) \neq \{e\}$.

证明

(1) 由定理????及 $|X| = n$, 可设 X 的轨道分解为

$$X = O_{x_1} \bigcup O_{x_2} \bigcup \cdots \bigcup O_{x_m},$$

其中 $O_{x_1}, O_{x_2}, \cdots, O_{x_m}(m \leqslant n)$ 为 X 中所有不同的轨道. 注意到

$$x \in \{x \in X \mid g(x) = x, \forall g \in G\} \Longleftrightarrow g(x) = x(\forall g \in G)$$
$$\Longleftrightarrow O_x = \{g(x) \in X \mid g \in G\} = \{x\} \Longleftrightarrow |O_x| = 1,$$

从而对 $\forall x, y \in \{x \in X \mid g(x) = x, \forall g \in G\}$ 且 $x \neq y$, 有 $O_x = \{x\} \neq \{y\} = O_y$. 因此 $x, y \in \{x_1, x_2, \cdots, x_m\}$. 故 $\{x \in X \mid g(x) = x, \forall g \in G\} \subseteq \{x_1, x_2, \cdots, x_m\}$. 于是

$$n = \left|O_{x_1}\right| + \cdots + \left|O_{x_m}\right| = \sum_{|O_{x_i}|=1} |O_{x_i}| + \sum_{|O_{x_i}|\neq 1} |O_{x_i}|$$
$$= \sum_{x_i \in \{x \in X \mid g(x)=x, \forall g \in G\}} 1 + \sum_{|O_{x_i}|\neq 1} |O_{x_i}| = t + \sum_{|O_{x_i}|\neq 1} |O_{x_i}|.$$

由推论??知 $|O_{x_i}| \mid |G|$. 由 G 为 p 群, $|O_{x_i}| > 1$, 故 $p \mid |O_{x_i}|$, 因而结论 (1) 成立.

(2) $(n, p) = 1$, 由结论 (1) 知 $t \neq 0$, 故结论 (2) 成立.

(3) 考虑 G 在 G 上的伴随作用. 由定理????知

$$C(G) = \{x \in G \mid \mathrm{ad}x\,(g) = \mathrm{id}_G\,(g) = g, \forall g \in G\}.$$

自然 $e \in C(G)$, 故 $|C(G)| \geqslant 1$. 又 $p \mid |G|$, 由结论 (1)(取 $X = C(G)$) 知 $|G| \equiv |C(G)| \pmod p$, 故 $|C(G)| > 1$, 即 $C(G) \neq \{e\}$.

□

引理 0.1

设 p 是素数, $n = p^l m, (m, p) = 1$. 若 $k \in \mathbf{N}, k \leqslant l$, 则

$$p^{l-k} || \mathrm{C}_n^{p^k},$$

其中 $||$ 表示恰能整除, 即 $p^{l-k} \mid \mathrm{C}_n^{p^k}$ 但 $p^{l-k+1} \nmid \mathrm{C}_n^{p^k}$, $\mathrm{C}_n^{p^k}$ 是组合数.

证明 当 $1 \leqslant i \leqslant p^k - 1$ 时,i 都有分解 $i = j_i p^t$, 其中, $(j_i, p) = 1$, 于是有 $t < k \leqslant l$, 而此时

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

因而 $p^t || (n - i)$, $p^t || (p^k - i)$. 又

$$\mathrm{C}_n^{p^k} = \frac{n}{p^k} \frac{n-1}{p^k-1} \cdots \frac{n-(p^k-1)}{p^k-(p^k-1)} = \frac{n}{p^k} \cdot \prod_{i=1}^{p^k-1} \frac{n-i}{p^k-i}$$

$$= \frac{p^l m}{p^k} \cdot \prod_{i=1}^{p^k-1} \frac{p^t\left(p^{l-t}m - j_i\right)}{p^t\left(p^{k-t} - j_i\right)} = p^{l-k} \cdot m \prod_{i=1}^{p^k-1} \frac{p^{l-t}m - j_i}{p^{k-t} - j_i}.$$

注意到 $(m \prod_{i=1}^{p^k-1} \frac{p^{l-t}m - j_i}{p^{k-t} - j_i}, p) = 1$, 故由此知 $p^{l-k} \| C_n^{p^k}$.

□

定理 0.2 (Sylow 第一定理)

设 G 是一个阶为 $p^l m$ 的群, 其中, p 为素数, $l \geqslant 1, (p, m) = 1$, 则对任何 $1 \leqslant k \leqslant l$, G 中一定有 p^k 阶子群.

♡

证明 令 X 是 G 中所有含 p^k 个元素的子集的集合, 即

$$X = \{A | A \subseteq G, |A| = p^k\}.$$

显然 $|X| = C_n^{p^k}$, 其中, $n = p^l m$.

$G \times X$ 到 X 上的映射

$$f(g, A) = gA = \{ga | a \in A\}$$

定义了 G 在 X 上的作用. 于是 X 有轨道分解

$$X = \bigcup O_A, \quad |X| = \sum |O_A|.$$

由引理 0.1知 $p^{l-k} \| C_n^{p^k}$, 因而 $\exists A \in X$, 使 $p^{l-k+1} \nmid |O_A|$. 设 F_A 是 A 的迷向子群, 于是

$$|O_A| = [G : F_A] = \frac{p^l m}{[F_A : e]} = \frac{p^l m}{|F_A|},$$

因而 $p^k \| [F_A : e]$.

另一方面, 对 $\forall a \in A, g \in F_A$ 有 $g(a) = ga \in A$. 于是 $F_A \cdot a \subseteq A$, 故 $|F_A \cdot a| = |F_A| \leqslant |A| = p^k$. 由此知 $[F_A : e] = p^k$, 即 F_A 是一个 p^k 阶子群.

□

定义 0.2 (Sylow p 子群)

设群 G 的阶为 $p^l m$, p 为素数且 $(p, m) = 1$, 则 G 的 p^l 阶子群称为 G 的 **Sylow p 子群**.

♣

注 Sylow 第一定理肯定了 Sylow p 子群的存在性, 故上述定义是良定义的.

定理 0.3 (Sylow 第二定理)

设群 G 的阶为 $p^l m$, p 为素数, $(p, m) = 1$. 又 P 是 G 的一个 Sylow p 子群, H 是 G 的一个 p^k 阶子群, 则 $\exists g \in G$, 使 $H \subseteq gPg^{-1}$.

特别地, G 的 Sylow p 子群是相互共轭的.

♡

证明 将 G 在 G/P 上的左平移作用限制在 H 上, 于是得到 H 在 G/P 上的左平移作用

$$h(gP) = hgP, \quad \forall h \in H, g \in G.$$

因 $|H| = p^k$, $|G/P| = m$, $(p, m) = 1$, 故由定理 4.3.1 的结论 (2) 知 G/P 中含有元素 gP, 其轨道仅含 gP, 即 $hgP = gP(\forall h \in H)$, 故 $hg \in gP$, $H \subseteq gPg^{-1}$.

特别地, 若 $|H| = p^l$, 则 $H = gPg^{-1}$.

□

定理 0.4 (Sylow 第三定理)

设群 G 的阶为 $p^l m$, p 为素数, $(p, m) = 1$. 又设 G 中 Sylow p 子群的个数为 k, 则有

(1) 当且仅当 $k = 1$ 时, G 的 Sylow p 子群 $P \lhd G$;

(2) $k|m, k \equiv 1 \pmod p$.

证明

(1) 设 P 是 G 的一 Sylow p 子群. 显然 $\forall g \in G, gPg^{-1}$ 也是 G 的 Sylow p 子群. 又若 P_1 是 G 的另一 Sylow p 子群. 由定理 4.3.3 知 $\exists g_1 \in G$, 使得 $g_1Pg_1^{-1} = P_1$, 因而 $X = \{gPg^{-1}|g \in G\}$ 是 G 中 Sylow p 子群的集合.
若 $|X| = 1$, 即 $gPg^{-1} = P(\forall g \in G)$, 故 $P \lhd G$. 反之, 若 $P \lhd G$, 则 $gPg^{-1} = P$, 故 $|X| = 1$. 这样就证明了结论 (1).

(2) 现设 $|X| = k$, 则 $G \times X$ 到 X 的映射
$$f(g, P_1) = gP_1g^{-1}, \quad \forall g \in G, P_1 \in X$$
定义了 G 在 X 上的作用, 由定理 4.3.3 知这个作用可递. 设 F_P 为 P 的迷向子群, 即
$$F_P = \{g \in G, |gPg^{-1} = P\} = N_G(P).$$
显然, $P \lhd F_P$, 故 $p^l||F_P|$, 因而
$$k = |X| = [G : F_P], \quad [G : F_P]|m.$$
将上面 G 在 X 上的作用限制为 P 在 X 上的作用, 显然 $P \in X$, P 在 P 作用下的轨道 $O'_P = \{P\}$. 若另有 $P_1 \in X$, 在 P 作用下的轨道 $O'_{P_1} = \{P_1\}$, 即有 $gP_1g^{-1} = P_1(\forall g \in P)$. 由定理 4.3.3, $\exists h \in G$, 使得 $P_1 = hPh^{-1}$, 因而 $g(hPh^{-1})g^{-1} = hPh^{-1}$, 故 $h^{-1}gh \in F_P$. 故 $h^{-1}Ph, P$ 均为 F_P 的 Sylow p 子群, 又 $P \lhd F_P$, 故由结论 (1) 知 $h^{-1}Ph = P$, 故 $P = P_1$. 这就说明包含一个元素的 X 的轨道仅有一个. 由定理 4.3.1 的结论 (1) 知 $k \equiv 1 \pmod p$.

□

Sylow 定理在群论中有许多应用, 其一就是判断某些有限群不是单群 (一个群如果没有非平凡的正规子群就称为**单群**).

例题 0.1 设群 G 的阶为 72, 则 G 不是单群.

解 $72 = 2^3 \cdot 3^2$. 设 G 中 Sylow 3 子群的个数为 k, 于是由定理 4.3.4 知有 t, 使得 $k = 3t + 1$, $k|8$, 因而 $t = 0$ 或 $t = 1$.

若 $t = 0$, 则 $k = 1$. 此时 Sylow 3 子群为 G 的正规子群, 故 G 不是单群.

若 $t = 1$, 则 $k = 4$. 设 $X = \{P_1, P_2, P_3, P_4\}$ 为 G 的 Sylow 3 子群的集合, G 在 X 上的作用可递, 由定理 4.2.1 知有 G 到 $S_X = S_4$ 中的同态 σ. 于是 $G/\ker\sigma$ 与 S_4 的一个子群同构, 而由 $|S_4| = 24 < 72$ 知 $\ker\sigma \neq \{e\}$. 又由 G 在 X 上作用可递知 $\ker\sigma \neq G$, 故 $\ker\sigma$ 是 G 的非平凡正规子群, 因而 G 不是单群.

□