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 $|G|=[G:e]=p^k(k\in\mathbb{N})$, 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) $t\equiv n\pmod p$, 也即 $n\equiv t\pmod p$;

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

(3) G 的中心 $C(G)\neq\{e\}$. ♡

注 由(1)式知 $\{x\in X\mid g(x)=x,\forall g\in G\}$ 中的元素 x 的轨道都只包含其自身一个元素即 $O_x=\{x\},|O_x|=1$. 故 t 就是只包含一个元素的 X 的轨道的个数.

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

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

故

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

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

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

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, $n=p^lm,(m,p)=1$. 若 $k\in\mathbb{N},k\leqslant l$, 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 $i=j_ip^t$, 其中, $(j_i,p)=1$, 于是有 $t<k\leqslant l$, 而此时

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

$$p^k - i = p^t(p^{k-t} - j_i),$$

因而 $p^t||(n-i), p^t||(p^k-i)$. 又

$$\begin{aligned}
\mathrm{C}_n^{p^k} &= \frac{n}{p^k}\frac{n-1}{p^k-1}\cdots\frac{n-(p^k-1)}{p^k-(p^k-1)} = \frac{n}{p^k}\cdot\prod_{i=1}^{p^k-1}\frac{n-i}{p^k-i} \\
&= \frac{p^l m}{p^k}\cdot\prod_{i=1}^{p^k-1}\frac{p^t\left(p^{l-t}m-j_i\right)}{p^t\left(p^{k-t}-j_i\right)} = p^{l-k}\cdot m\prod_{i=1}^{p^k-1}\frac{p^{l-t}m-j_i}{p^{k-t}-j_i}.
\end{aligned}$$

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

□

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

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

显然 $|X| = \mathrm{C}_n^{p^k}$, 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. 于是由定理**????**知 X 有轨道分解

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

由引理 0.1知 $p^{l-k}||\mathrm{C}_n^{p^k}$, 即 $p^{l-k}|||X|$. 因而 $\exists A \in X$, 使 $p^{l-k} \mid |O_A|, p^{l-k+1} \nmid |O_A|$. 从而存在 t, 使 $(p,t) = 1$ 且 $|O_A| = p^{l-k}t$. 设 F_A 是 A 的迷向子群, 于是由推论**??**及 Lagrange 定理可得

$$\begin{aligned}
|O_A| = [G:F_A] = \frac{p^l m}{[F_A:e]} &= \frac{p^l m}{|F_A|} \Longrightarrow |O_A|\cdot|F_A| = p^l m \\
&\Longrightarrow p^{l-k}t\cdot|F_A| = p^l m \Longrightarrow |F_A|t = p^k.
\end{aligned}$$

又 $(p,t) = 1$, 故 $p^k \mid |F_A|$. 若 $p^{k+1} \mid |F_A|$, 则存在 c, 使 $|F_A| = p^{k+1}c$, 从而由上式知

$$p^l m = |O_A|\cdot|F_A| = p^{l-k}t\cdot p^{k+1}c = p^{l+1}tc \implies m = ptc,$$

这与 $(p,m) = 1$ 矛盾! 故 $p^{k+1} \nmid |F_A|$, 因此 $p^k \parallel |F_A|$.

另一方面, 对 $g \in F_A$ 有 $gA = A$, 即 $g(a) = ga \in A (\forall a \in A)$. 于是 $F_A \cdot a \subseteq A$, 故再由命题**??**知

$$|F_A \cdot a| = |F_A| \leqslant |A| = p^k.$$

由此知 $|F_A| = p^k$, 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.

命题 0.1

设 P 为群 G 的一个 Sylow p 子群, 则对 $\forall a \in P$, 都存在 $k \in \mathbb{N}$, 使得 $\operatorname{ord} a = p^k$. ♠

注 这个命题表明:Sylow p 子群的元素的阶都是 p 的方幂.

证明 设 $|P| = p^l$, 则由推论??知 $\operatorname{ord} a \mid |P|$, 故存在 $k \in \mathbb{N}$, 使得 $\operatorname{ord} a = p^k$.

□

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

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

由 Lagrange 定理知

$$[G:e] = [G:P][P:e] \iff |G| = |G/P|\,|P| \iff p^l m = |G/P|\,p^l \iff |G/P| = m.$$

又 $|H| = p^k$, $(p,m) = 1$, 故由定理 0.1(2)知 G/P 中含有元素 gP, 其轨道仅含 gP, 即 $hgP = gP(\forall h \in H)$, 故存在 p_1, p_2, 使 $hgp_1 = gp_2$, 从而 $h = gp_2p_1^{-1}g^{-1} \in gpg^{-1}$. 因此 $H \subseteq gPg^{-1}$.

特别地, 若 H 也是 G 的一个 Sylow p 子群, 则 $|H| = p^l$, 再由命题??知 $|H| = p^l = |P| = |gPg^{-1}|$. 又由之前证明知 $H \subseteq gPg^{-1}$, 从而 $H = gPg^{-1}$. 由定理??知 H, P 相互共轭.

□

推论 0.1

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, 则

(1) 群 G 中 Sylow p 子群的集合是 $X = \{gPg^{-1} | g \in G\}$, 即 P 的共轭子群构成的集合.

(2) $G \times X$ 到 X 的映射

$$f(g, P_1) = g(P_1) = gP_1g^{-1}, \quad \forall g \in G, P_1 \in X.$$

是群 G 在 X 上的作用. 并且 G 在 X 上的作用 f 是可递的.

证明

(1) 任取 $g \in G$, 对 $\forall p_1, p_2 \in P$, 有 $(gp_1g^{-1})(gp_2g^{-1})^{-1} = gp_1p_2^{-1}g^{-1} \in gPg^{-1}$, 因此 gPg^{-1} 是 G 的子群. 又由命题??知 $|P| = |gPg^{-1}| = p^l$, 故 gPg^{-1} 也是 G 的 Sylow p 子群.

又若 P_1 是 G 的另一 Sylow p 子群. 由Sylow 第二定理知 $\exists g_1 \in G$, 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.

(2) 根据群作用的定义容易验证 f 是群 G 在 X 上的一个作用. 对 $\forall P_1, P_2 \in \{X\}$, 由Sylow 第二定理知 P_1, P_2 共轭, 即存在 $g \in G$, 使

$$P_1 = gP_2g^{-1} = g(P_1) = f(g, P_1).$$

故 G 在 X 上的作用 f 是可递的.

□

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 k 也是 G 中任意一个 Sylow p 子群的共轭子群的个数. 并且有

(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 设 P 是 G 的一 Sylow p 子群. 则由推论 0.1(1)知 $X = \{gPg^{-1} | g \in G\}$ 是 G 中 Sylow p 子群的集合. 从而 k 也是 G 中任意一个 Sylow p 子群的共轭子群的个数.

(1) 若 $|X| = 1$, 即 $gPg^{-1} = P(\forall g \in G)$, 故由正规子群定义知 $P \lhd G$. 反之, 若 $P \lhd G$, 则 $gPg^{-1} = P(\forall g \in G)$, 故 $|X| = 1$. 这样就证明了结论 (1).

(2) 由推论 0.1(1)知 $X=\{gPg^{-1}|g\in G\}$ 是 G 中 Sylow p 子群的集合. 现设 $|X|=k$, 由推论 0.1(2)知 $G\times X$ 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. 设 F_P 为 P 的迷向子群, 即

$$F_P=\{g\in G,|gPg^{-1}=P\}.$$

显然, $P\lhd F_P$, 故由 Lagrange 定理知 $|P|\mid|F_P|$, 即 $p^l\mid|F_P|$, 因而存在 t, 使得

$$|F_P|=p^lt. \tag{2}$$

于是由 Lagrange 定理知

$$|G|=[G:F_P]|F_P|\iff p^lm=[G:F_P]p^lt\iff m=[G:F_P]t\Longrightarrow[G:F_P]\mid m,\ t\mid m. \tag{3}$$

又注意到 G 在 X 上的作用下 P 的轨道为 $O_P=X$, 故由推论**??**知

$$k=|X|=[G:F_P].$$

因此再结合(3)式得 $k\mid m$.

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 X 上的作用下 P 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Sylow 第二定理, $\exists h\in G$, 使得 $P_1=hPh^{-1}$, 因而

$$g(hPh^{-1})g^{-1}=hPh^{-1}(\forall g\in P)\iff(h^{-1}gh)P(h^{-1}gh)^{-1}=P(\forall g\in P).$$

故 $h^{-1}gh\in F_P(\forall g\in P)$, 从而 $hPh^{-1}\subseteq F_P$. 因此 $h^{-1}Ph,P$ 均为 F_P 的子群. 由(3)式知 $t\mid m$, 又因为 $(p,m)=1$, 所以 $(p,t)=1$. 而由(2)知 $|F_p|=p^lt,|P|=p^l$, 再由命题**??**知 $|h^{-1}Ph|=|P|=p^l$, 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. 注意到

$$P'\in\{P'\in X\mid g(P')=gP'g^{-1}=P',\forall g\in P\}\iff O_{P'}=\{g(P')=gP'g^{-1}=P'\mid g\in P\}=\{P'\},$$

故

$$\{P'\in X\mid g(P')=gP'g^{-1}=P',\forall g\in P\}=\{P'\in X\mid O_{P'}=\{P'\}\}=\{P\}.$$

即 $|\{P'\in X\mid g(P')=gP'g^{-1}=P',\forall g\in P\}|=1$. 故由定理 0.1(1)知 $k\equiv1\pmod p$.

□

定义 0.3 (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.

注 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.

解 $72=2^3\cdot3^2$. 设 G 中 Sylow 3 子群的个数为 k, 于是由Sylow 第三定理知有 t, 使得 $k=3t+1$, $k|8$, 因而 $t=0$ 或 $t=1$.

若 $t=0$, 则 $k=1$. 此时再由Sylow 第三定理知 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, 由推论 0.1(2)知有 G 在 X 上的作用

$$g(P_1)=gP_1g^{-1},\quad\forall g\in G,P_1\in X.$$

并且这个 G 在 X 上的作用是可递的. 由定理**??**知有 G 到 $S_X=S_4$ 中的同态 σ 满足

$$\sigma(g)=\sigma_g,\forall g\in G,$$

其中 $\sigma_g:X\to X,P\longmapsto g(P)=gPg^{-1}$. 于是由群的同态基本定理知 $\ker\sigma\lhd G$ 且 $G/\ker\sigma$ 与 S_4 的一个子群 $\sigma(G)$

同构, 而 $|S_4| = 24 < 72$, 于是

$$[G : \ker\sigma] = |\sigma(G)| \leqslant |S_4| = 24 < 72 = |G|.$$

再利用 Lagrange 定理可得

$$|G| = [G : \ker\sigma]|\ker\sigma| \implies |\ker\sigma| = \frac{|G|}{[G : \ker\sigma]} \geqslant \frac{72}{24} > 1.$$

因此 $\ker\sigma \neq \{e\}$.

注意到

$$\ker\sigma = \{g \in G \mid \sigma(g) = \mathrm{id}_G\} = \{g \in G \mid gPg^{-1} = P, \forall P \in X\},$$

又由 G 在 X 上的作用可递知对 $P_1, P_2 \in X$, 存在 $g_1 \in G$, 使 $P_2 = g(P_1) = g_1P_1g_1^{-1}$. 若 $\ker\sigma = G$, 则 $g_1 \in \ker\sigma$, 从而

$$P_2 = g_1P_1g_1^{-1} = P_1,$$

这与 $P_1 \neq P_2$ 矛盾! 因此 $\ker\sigma \neq G$. 故 $\ker\sigma$ 是 G 的非平凡正规子群, 因而 G 不是单群.

□

命题 0.2

设 p, q 都是素数, $p < q$, $p \nmid (q-1)$. 证明 pq 阶群一定是循环群.

证明 设 P, Q 分别为 pq 阶群 G 的 p, q 阶子群. 于是由Sylow 第三定理 (2), 可设 P, Q 共轭子群的个数分别为 $sp+1, tq+1 (s, t \in \mathbb{N})$. 由推论 0.1(1)知,$P$ 的共轭子群都是 G 的 Sylow p 子群,Q 的共轭子群都是 G 的 Sylow p 子群. 因此

$$sp + 1 = q, \quad tq + 1 = p.$$

由 $p < q$, 于是 $t = 0$, 因而 Q 是 G 的唯一的 q 阶子群. 若 $s \neq 0$, 则 $sp + 1 = q$, 这与 $p \nmid (q-1)$ 矛盾. 于是 $s = 0$, 因而 P 是 G 的唯一的 p 阶子群.

因为 p, q 都是素数且 $p < q$, 所以 $|P \cup Q| \leqslant p+q < pq = |G|$, 因此 $G \neq Q \cup P$. 对 $\forall a \in G \setminus (P \cup Q)$, 则 $\langle a \rangle \neq P, Q$, 从而由 P, Q 分别是 G 的唯一 p, q 阶子群知 $\langle a \rangle$ 的阶既不是 p 也不是 q. 又由 Lagrange 定理知 $|\langle a \rangle| =| pq$, 于是 $|\langle a \rangle| = pq$, 因此 $G = \langle a \rangle$ 为循环群.

□