2.5 Sylow Theorem

Theorem 1. (Cauchy Theorem)
Suppose $p \mid |G|$,where p is a prime.Then there exists $a \epsilon G$,with order p.

Proof.

Set$S = G^p = \{(g_1, g_2, ..., g_p) | g_i \epsilon G, g_1 g_2 ... g_p = e\}$

Note:$|S| = |G|^{p-1}$

Since $g_p = (g_1 g_2 ... g_{p-1})^{-1}$

Pick $\sigma = (1, 2, ..., p) \epsilon S_p$ and $H :=< \sigma >$

Let H acts on S by
$\sigma \cdot (g_1, g_2, ..., g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, ..., g_{\sigma(p)}) \epsilon S$

By class equation,

$$\begin{aligned} |G|^{p-1} &= |S| \\ &= \sum_i |\Theta_{s_i}| \\ &= \sum_i \frac{|H|}{|H_{s_i}|} \\ &= \sum_i \frac{p}{|H_{s_i}|} \end{aligned}$$

Since $p \mid |G|^{p-1}$, $p \mid \sum_i \frac{p}{H_{s_i}}$

Note:

$H_{(e,e,...e)} = H$

Hence,there exists s_j s.t.$\Theta_{s_j} \neq \Theta_{(e,e,...e)}$ and $H_{s_j} = H$

Assume,$s_j = (a_1, a_2, ..., a_p) \epsilon S$

Since $\sigma \epsilon H = H_{s_j}$,we have $\sigma \cdot s_j = s_j$

i.e.$(a_2, a_3, ..., a_p, a_1) = (a_1, a_2, ..., a_p)$

i.e.$a_1 = a_2 = ... = a_p = a$ for some $a \epsilon G$

Note:$a^p = e$ and $a \neq e$

Definition 1. *Suppose* $|G| < \infty$ *Let* $t \in \mathbb{N} \bigcup \{0\} s.t.$ $p^t \mid |G|$ *and* $p^{t+1} \nmid |G|$
Define $Sylp(G) := \{H < G||H| = p^t\}$ *is the set of p-Sylow subgroup.*

Theorem 2. (First Sylow Theorem)

$Sylp(G) \neq \emptyset$

Proof.

Induction on $|G|$

Let G acts on G by conjugation.

i.e. $S = G$, and $g \cdot s = g^{-1}sg$ for $g, s \in G$

Then (by class equation)

$$\begin{aligned} |S| &= |G| \\ &= \sum_i |\Theta_{s_i}| \\ &= \sum_{i,|\Theta_{s_i}|=1} 1 + \sum_{i,|\Theta_{s_i}|\neq 1} |\Theta_{s_i}| \end{aligned}$$

Note:

$|\Theta_{s_i}| = 1 \Leftrightarrow g^{-1}s_i g = s_i$, for all $g \in G \Leftrightarrow s_i \in Z(G)$,the order of G.

$$\text{Hence } |G| = |Z(G)| + \sum_{i,G_{s_i}\neq G} \frac{|G|}{|G_{s_i}|}$$

Case1:

$p \mid |Z(G)|$, by Cauchy Theorem , there exists $a \in Z(G)$ with $|a| = p$

Note:$< a > \lhd G$, By induction hypothesis , there exists $\overline{H} \in Sylp(\frac{G}{< a >})$

Set $H = \left\{g \in G | g < a > \ \in \overline{H}\right\}$

Then $H \in Sylp(G)$

Case2:

$p \nmid |Z(G)|$

Then $p \nmid \dfrac{|G|}{|G_{s_i}|}$ for some i

Hence , $Sylp(G_{s_i}) \subseteq Sylp(G)$, by induction.

Note:

By the some method in the proof of Sylow 1st Theorem

$|Z(G)| \neq 1$, if $|G| = p^n$(i.e. if $|G| = p^n \Rightarrow |Z(G)| \neq \ <e>$)

Theorem 3. (Second Sylow Theorem)

$H, H' \in Sylp(G) \Rightarrow H' = g^{-1}Hg$, for some $g \in G$

i.e. Any 2 p-Sylow subgroups are conjugate.

Proof.
Let H' acts on the left coset of H in G.

Then by class equation,
$\dfrac{|G|}{|h|} = \sum_{|\Theta_{s_i}|=1} 1 + \sum_{|\Theta_{s_i}|\neq 1} \dfrac{|H'|}{|H'_{s_i}|}$

Note:

$$\begin{aligned} |O_{s_i}| = 1 \quad &\Leftrightarrow \quad g \cdot s_i \text{ for all } g \in H' (\text{Say } s_i = g_i H) \\ &\Leftrightarrow \quad g g_i H = g_i H, \text{ for all } g \in H' \\ &\Leftrightarrow \quad g_i^{-1} g g_i \in H, \text{ for all } g \in H' \\ &\Leftrightarrow \quad g_i^{-1} H' g_i = H \end{aligned}$$

Note:

$p \nmid |\dfrac{|G|}{|H|}, p \mid \dfrac{|H'|}{|H'_{s_i}|}$ for all i with $|\Theta_{s_i}| \neq 1$

$$\text{Hence, } p \nmid \sum_{|\Theta_{s_i}|=1} 1$$

Then there exists s_i with $|\Theta_{s_i}| = 1$

i.e.$g_i^{-1}H'g_i = H$

Theorem 4. (Third Sylow Theorem)
(1) $|Sylp(G)|$ divides $|G|$
(2) $|Sylp(G)| \equiv 1(mod\ p)$

Proof.
(1)

Let G acts on $Sylp(G)$ by conjugations.

i.e.$S = Sylp(G)$, $g \cdot s_i = g^{-1}s_i g$ for $g \in G$

By there is a unique orbit , by 2nd Sylow Theorem.

Then$|Sylp(G)| = \dfrac{|G|}{|G_{s_i}|}$

Hence,$|Sylp(G)|$ divides $|G|$

(2)

Pick $P \in Sylp(G)$, by 1st Theorem

Let P acts on $Sylp(G)$ by conjugation.

Then by class equation:

$$|Sylp(G)| = \sum_{|\Theta_{s_i}|=1} 1 + \sum_{|\Theta_{s_i}|\neq 1} \frac{|P|}{|P_{s_i}|}$$

Note:

$$\begin{aligned} |O_{s_i}| = 1 \quad &\Leftrightarrow \quad g^{-1}s_i g = s_i \text{ , for all } g \in P \\ &\Leftrightarrow \quad P \subseteq N_G(s_i) \\ &\Leftrightarrow \quad p = s_i (if p = s_i \ \Leftrightarrow \ P \subseteq N_G(s_i)) \end{aligned}$$

Note:

$p, s_i \in Sylp(N_G(s_i))$, if $P \subseteq N_G(s_i)$

Hence,$p = g^{-1}s_i g = s_i$ for some $g \in N_G(s_i)$, by 2nd Sylow Theorem.

$$\text{Hence} \sum_{|\Theta_{s_i}|=1} 1 = 1$$

$$\text{Then } |Sylp(G)| = 1 + \sum_{P_{s_i} \neq P} \frac{|P|}{|P_{s_i}|} \equiv 1(modp)$$