Sylow’s Theorem I: If $p^n$ divides the order of $G$ with $p$ a prime, then $G$ has a subgroup of order $p^n$.

Corollary: Cauchy’s Theorem: Suppose $p$ divides the order of $G$. Then $G$ has an element of order $p$.

Definition: Suppose $p^n$ divides the order of $G$, but $p^{n+1}$ does not. Then a subgroup of $G$ of order $p^n$ is called a Sylow $p$-subgroup of $G$.

Recall: In the following notes, let $H, K$ be finite subgroups of a group $G$, and define $HK := \{hk | h \in H, k \in K\}$.

1. $|HK| = \frac{|H||K|}{|H \cap K|}$

2. $HK$ is a subgroup of $G$ if $HK = KH$

3. If $H$ or $K$ is normal, then $HK$ is normal.

4. If $H \subseteq N_G(K)$, then $HK$ is a subgroup.

Definition: Suppose $X$ is a $G$-set, $x \in X$ is called a fixed point of $G$ if $G_x = G$, or equivalently, $Gx = \{x\}$.

Notation: Suppose $p$ divides the order of $G$. Then $\text{Syl}_p(G) := \{\text{all Sylow } p\text{-subgroups}\}$ and $n_p := |\text{Syl}_p(G)|$.

Remark: If $H$ is a subgroup of order $n$ and $x \in G$ then $xHx^{-1}$ is also a subgroup of order $n$, and $xHx^{-1}$ is called a conjugate of $H$. Therefore, any conjugate of a Sylow $p$-subgroup is a Sylow $p$-subgroup. In addition, the number of conjugates of a subgroup $H$ is $[G : N_G(H)]$.

Lemma 1: Let $H$ be a $p$-subgroup of $G$ and $P \in \text{Syl}_p(G)$ and suppose $H \subseteq N_G(H)$. Then $H \subseteq P$.

Proof: By one of the remarks, $HP$ is a subgroup of $G$, and then

$$|HP| = \frac{|H||P|}{|H \cap P|} = |P| \cdot \left(\frac{|H|}{|H \cap P|}\right)$$

$$= |P| \cdot p^\alpha = p^{n+\alpha}$$

Therefore, $\alpha = 0$, since $P \subseteq HP$ but $P$ is a sylow $p$-subgroup. So, this implies $H = H \cap P \subseteq P$.

Lemma 2: Let $X$ be a $G$-set and suppose $G$ is a $p$-group. Let $n$ be the number of fixed points of $G$. Then $|X| \equiv n \pmod p$.

Proof:

$$|X| = \sum |Gx|$$
\[ = n + \sum |Gx| \]

And since \(|Gx|\) divides \(|G|\), we know that

\[ = n + \sum p^{\alpha_i} \]

For some \(\alpha_i > 0\). Now modding out by \(p\), we get

\[ |X| \equiv n \pmod{p}. \]

**Sylow’s Second Theorem:** Suppose for the following that \(p\) divides the order of \(G\). Then

1. Any \(p\)-subgroup is contained in a Sylow \(p\)-subgroup.
2. All Sylow \(p\)-subgroups are conjugate.
3. \(n_p = [G : N_G(P)]\) for any \(P \in \text{Syl}_p(G)\), and in particular \(n_p\) divides \(|G|/|P| = \frac{|G|}{p^n}\).
4. \(n_p \equiv 1 \pmod{p}\).

**Proof:**

1. Let \(P \in \text{Syl}_p(G)\) and let \(X = \{xPx^{-1} | x \in G\}\). Then \(|X| = [G : N_G(P)]\). Now let \(H\) be any \(p\)-subgroup of \(G\), and let \(H\) act on \(X\) by conjugation (i.e. if \(Q \in X\) then \(h \cdot Q = hQh^{-1}\). Note that \(p \nmid |X|\), since \(P \subseteq N_G(X)\). By lemma 2, we have \(|X| \equiv \text{fixed points of } H \pmod{p}\). Since \(|X| \not\equiv 0 \pmod{p}\), \(\exists\) a fixed point of \(H\) in \(X\), say \(Q\). So, we know \(hQh^{-1} = Q \forall h \in H\). But \(Q \in X \subseteq \text{Syl}_p(G)\). The above implies that \(H \subseteq N_G(Q)\) and by lemma 1, we have \(H \subseteq Q\).

2. Let \(P' \in \text{Syl}_p(G)\). By replacing \(H\) by \(P'\) in the previous argument, we get \(P' \subseteq Q = xPx^{-1}\) (since \(xPx^{-1}\) has the same order of \(Q\)). Hence any two Sylow \(p\)-subgroups are conjugates, and thus \(X = \text{Syl}_p(G)\).


4. Choose \(P \in \text{Syl}_p(G)\) and \(X = \{xPx^{-1} | x \in G\} = \text{Syl}_p(G)\). Let \(P\) act on \(X\) by conjugation. By the same argument as in 1, there exists a fixed point of \(P\) in \(X\), say \(Q\). This means that \(yQy^{-1} = Q \forall y \in P\), thus \(P \subseteq N_G(Q)\) which implies \(P \subseteq Q\) which also implies \(P = Q\). Hence, there is only one fixed point of \(P\) in \(X\). By lemma 2, \(n_p = |X| \equiv \text{number of fixed points} = 1 \pmod{p}\).

**Corollary:** Let \(P \in \text{Syl}_p(G)\). Then \(P < G \iff P\) is the unique sylow \(p\)-subgroup of \(G\).