Sylow Theorems

Let \( G \) be a finite group and \( p \) be a prime number. Write

\[ |G| = p^e m \quad \text{where} \quad (p,m)=1. \]

First Sylow Theorem: There is a subgroup of \( G \) of order \( p^e \).

Corollary: If \( p \mid |G| \) then \( G \) has an element of order \( p \).

Proof: Let \( H \leq G \) be a subgroup of order \( p^e \). Choose a non-identity element \( x \in H \), say with \( o(x) = p^k \), \( k > 1 \). Then

\[ (x^{p^k})^p = e \quad \text{and} \quad x^{p^{k-1}} \neq e. \]

Def: Let \( G, \ p, \ |G| = p^e m \) be as above.

A subgroup of \( G \) of order \( p^e \) is a Sylow \( p \)-subgroup of \( G \).
Second Sylow Theorem. Let $K \leq G$ be a subgroup whose order is divisible by $p$, and let $H$ be a Sylow $p$-subgroup of $G$. Then for some $x \in G$, $xHx^{-1} \cap K$ is a Sylow $p$-subgroup of $K$.

Corollary. Any two Sylow $p$-subgroups of $G$ are conjugate, i.e., if $H$, $H'$ are Sylow $p$-subgroups of $G$ then there exists $x \in G$ such that $xHx^{-1} = H'$.

Third Sylow Theorem. Notation as above.

Then the number of Sylow $p$-subgroups of $G$ divides $n$ and is congruent to $1$ modulo $p$. 
Application. Let $G$ be a group of order 15. Let $n_3$ be the number of Sylow 3-subgroups of $G$; then $n_3 \equiv 1 \pmod{3}$, so $n_3$ is one of $1, 4, 7, 10, ...$. But also $n_3$ divides 5, so we conclude $n_3 = 1$. Similarly one argues that the number $n_5$ of Sylow 5-subgroups is 1. Thus, by the Corollary to the 2nd Sylow Theorem, $G$ has normal subgroups $H_1, H_2$ of orders 3 and 5. Certainly $H_1 \cap H_2 = \{e\}$, and we find, by a homework problem, that the function

$$H_1 \times H_2 \to G$$

$$\phi(h_1, h_2) = h_1 h_2$$

is a group isomorphism. Since $H_1 \cong \mathbb{Z}/3\mathbb{Z}$ and $H_2 \cong \mathbb{Z}/5\mathbb{Z}$, we find $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. 
We'll want a couple of preliminaries:

**Lemma 1** Let $S$ be a subset of a finite group $G$. Then the order of $Stab(S) = \{g \in G \mid gS \subseteq S\}$ divides the order of $G$.

**Proof.** The stabilizer $Stab(S)$ is a subgroup of $G$ that preserves $S \subseteq G$, hence we get an action of $Stab(S)$ on $S$. So $S$ is a union of orbits of $Stab(S)$. These orbits are of the form $Stab(S)x$ for $x \in S$, i.e. cosets of $Stab(S)$. So $S$ is a union of right $Stab(S)$-cosets. \[\square\]

**Lemma 2** Suppose the group $G$ acts on a set $S$, $x \in S$, and $g \in G$. Then $gG \cdot x \cdot g^{-1} = G_{gx}$. 


Proof of First Sylow Theorem:

Let $p$ be a prime, $e \geq 1$ an integer, $G$ a finite group of order $p^e m$ where $(p, m) = 1$. Let $S$ be the set of all subsets of $G$ of order $p^e$. 

Claim: $|S| = (p^e m)^{p^e - 1}$ and is relatively prime to $p$.

Proof: The equation is standard. Note that

$$(p^e m)^{p^e - 1} = \frac{p^e m (p^e m - 1) \ldots (p^e m - p^e + 1)}{p^e (p^e - 1) \ldots 1}.$$

Also, $p$ divides $p^e m - 1$ exactly $k$ times

$\iff$ $p$ divides $l$ exactly $k$ times ($0 \leq l \leq p^e - 1$)

$\iff$ $p$ divides $p^e - l$ exactly $k$ times. So $|S|$ is prime to $p$. This proves the claim. □.
Let $G$ act on $S$ by left multiplication. Since $(p, |S|) = 1$, there is an orbit of order not divisible by $p$, say the orbit of a subset $S$ of $G$. Then $|\text{Stab}(S)|$ is a power of $p$ by Lemma 1 above, and $|G/\text{Stab}(S)|$ is the size of the orbit, hence prime to $p$. So $|\text{Stab}(S)| = p^e$, which must therefore make $\text{Stab}(S)$ a Sylow $p$-subgroup. This proves the First Sylow Thm. QED

Proof of Second Sylow Theorem. Let $H$ be a Sylow $p$-subgroup of $G$ and $K$ a subgroup of $G$ such that $p \mid |K|$. Let $K$ act on the set

$$G/H = \bigcup_{a \in G} aH$$

on the left. Since $(|G/H|, p) = 1$, there is a $K$-orbit of cardinality not divisible by $p$, call it $O = K \cdot aH$. The stabilizer of $aH$ in $G$ is $aHa^{-1}$, so in $K$ it is $KHa^{-1}$. 
We get a bijection

\[ G \cong K/K_{\text{Natta}^{-1}} \]

which has cardinality prime to \( p \). So \( K_{\text{Natta}^{-1}} \) must be a Sylow \( p \)-subgroup of \( K \). \( \square \)

Proof of Third Sylow Theorem.

By our Corollary from last time, the Sylow \( p \)-subgroups are all conjugate to a given one, call it \( H \). So

\[ \# \{ \text{Sylow } p\text{-subgroups} \} = [G : N_G(H)] \]

where

\[ N_G(H) = \{ g \in G \mid ghg^{-1} = H \} \]

Now certainly \( [G : N_G(H)] \mid [G : H] \)

since \( H \leq N_G(H) \). So we need to show that this number is congruent to 1 mod \( p \).
So, let’s break the set $T$ of Sylow $p$-subgroups into orbits under the action of the Sylow $p$-subgroup $H$ by conjugation. Every orbit is in bijection with a set of left cosets $H/K$ for some subgroup $K \leq H$, so every orbit has size $p^k$ for some $0 \leq k \leq e$. When can an orbit have size $p^0 = 1$? Iff it consists of a Sylow $p$-subgroup $L \leq G$ such that $H \leq N_G(L)$. Then $H$ and $L$ are both Sylow $p$-subgroups of $N_G(L)$, hence are conjugate in $N_G(L)$. Since $L$ is normal in $N_G(L)$, it follows that $H = L$.

So there is a unique such orbit, consisting just of $H$, and every other orbit has size divisible by $p$. This completes the proof. \[ \square \]