THE SYLOW THEOREMS

Remember: Here are a few definitions and other facts you might want to recall.

Definitions: Let X be a set and let G be a group.

$$Fixer_X(g) = X_g = \{x \in X \mid g(x) = x \text{ for } g \in G\}$$

$$Stabilizer_G(x) = G_x = \{g \in G \mid g(x) = x \text{ for } x \in X\}$$

$$Orbit_G(x) = \{y \in X \mid g(x) = y \text{ for some } g \in G \text{ and } x, y \in X\}$$

Definition: To the above we will add our definition of the center of X under G as $Center_G(X) = Z_G(X) = \{x \in X \mid g(x) = x \text{ for all } g \in G\}$. Notice that we define things this way because if G is acting on G by conjugation, then we get back the usual definition for the center of G. In other words, if $Center_G(G) = Z_G(G) = \{x \in G \mid g(x) = gxg^{-1} = x \text{ for all } g \in G\}$, then $x \in G$ is in this center if and only if $gxg^{-1} = x \Leftrightarrow gx = xg$ for all $g \in G$.

Fact: Recall that if G is a finite group that acts on a set X, and if $x \in X$, then the number of elements in the orbit of x is $|Orbit_G(x)| = [G : G_x] = \frac{|G|}{|G_x|} = \frac{|G|}{|Stabilizer_G(x)|}$. From this we derived Burnside's Counting Theorem, that the number of orbits created by G acting on X is $\frac{1}{|G|}\sum_{x \in X}|G_x| = \frac{1}{|G|}\sum_{x \in X}|Stabilizer_G(x)| = \frac{1}{|G|}\sum_{g \in G}|Fixer_X(g)|$. Also, recall the Class Equation, $|G| = |Z(G)| + \sum_{x \notin Z(G)} \frac{|G|}{|C_G(x)|}$ where in our summation only a single value x is chosen from each distinct conjugacy class that contains more than one element. The Class Equation is simply says that the number of elements in G is just the sum of the number of elements in each orbit where an orbit is produced by letting elements of G act upon G itself by means of conjugation. Clearly, the Class Equation is just a special case of a group G acting on a set X where in this case $X = G$ and the permutations are created by the operation of conjugation. We can now replace this special case by the following more general formula where we state that the number of elements in X is merely the sum of the number of elements in each orbit produced by permutations in G, or in other words, $|X| = |Z_G(X)| + \sum_{x \notin Z_G(X)} \frac{|G|}{|G_x|}$.

Theorem: Let G be a group such that $|G| = p^n$ and let X be a set that G acts on. Then $|X| - |Z_G(X)|$ is divisible by p.

Proof: Since $Stabilizer_G(x) = G_x = \{g \in G \mid g(x) = x \text{ for } x \in X\}$ is a subgroup of G, $|G_x|$ divides $|G|$, and since $|G| = p^n$, it follows that $|G_x| = p^k$ where $0 \le k \le n$. Now we will use our generalized Class Equation, $|X| = |Z_G(X)| + \sum_{x \notin Z_G(X)} \frac{|G|}{|G_x|}$ where in our summation only a single value x is chosen from each distinct conjugacy class that contains more than one element. In this case, we can conclude that $G_x \neq G$ since if it were, then we would have $x \in Z_G(X)$. Thus, we also now have that $|G_x| < |G|$, and, hence, $\frac{|G|}{|G_x|} = p^m$ where $0 < m < n$.

Therefore, p divides $\sum_x \frac{|G|}{|G_x|} = |X| - |Z_G(X)|$, and we're done.

□

Definition: If H is a subgroup of a group G, then the set of all $x \in G$ such that $xHx^{-1} = H$ is called the normalizer of H in G and is denoted by $N_G(H)$.

Theorem: If H is a p-subgroup of a finite group G for some prime p, then $\frac{|G|}{|H|}-\frac{|N_G(H)|}{|H|}$ is divisible by p.

Proof: Let X be the set of left-cosets of H in G, and let H act on X by letting $h(xH)=(hx)H$ where $x\in G$ and $h\in H$. Then $Z_H(X)\subseteq X$ is the set of left-cosets of H in G such that $h(xH)=xH$ for all $h\in H$. Given such a left-coset we have that $h(xH)=xH \Leftrightarrow hxH=xH \Leftrightarrow x^{-1}hxH=H \Leftrightarrow x^{-1}hx\in H$ for all $h\in H$, and this in turn means that $x\in N_G(H)$, the normalizer of H in G. In other words, $x\in N_G(H)$ if and only if $x^{-1}hx\in H$ when $h\in H$ if and only if $x^{-1}hxH=H$ if and only if $hxH=xH$ if and only if $h(xH)=xH$ for all $h\in H$ if and only if $xH\in Z_H(X)$. Additionally, the number of such distinct left-cosets involving elements of $N_G(H)$ is $\left|\frac{N_G(H)}{H}\right|=\frac{|N_G(H)|}{|H|}=|Z_H(X)|$.

Also, since H is a p-group, $|H|=p^n$ for some $n\in\mathbb{N}$. Furthermore, our previous theorem tells us that p divides $|X|-|Z_H(X)|$. But in this case $|X|=$ the number of left-cosets of H in $G=\frac{|G|}{|H|}$ and $|Z_H(X)|=\frac{|N_G(H)|}{|H|}$. Therefore, p divides $\frac{|G|}{|H|}-\frac{|N_G(H)|}{|H|}$.

□

Corollary: If $|G|=p^nm$ where $n\geq 1$ and p is a prime that does not divide m, and if H is a subgroup of G such that $|H|=p^i$ for $1\leq i<n$, then $N_G(H)\neq H$ and p divides $|N_G(H)/H|$.

Proof: By our theorem, p divides $\frac{|G|}{|H|}-\frac{|N_G(H)|}{|H|}$. However, since $|G|=p^nm$ and $|H|=p^i$ for $1\leq i<n$, it immediately follows that p divides $\frac{|G|}{|H|}=p^{n-i}m$. Hence, p must also divide $\frac{|N_G(H)|}{|H|}$. However, this also means that $\frac{|N_G(H)|}{|H|}\neq 1$, and therefore, $N_G(H)\neq H$. □

The First Sylow Theorem: Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and p is a prime that does not divide m. then,

1. G contains a subgroup of order p for each I such that $1 \leq i \leq n$.

2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.

Proof: (1) We will proceed by induction on the power of p. First, by Cauchy's Theorem, we know that s subgroup of order p exists. Now suppose that for all i such that $1 \leq i < n$ that it is true that there exists a subgroup of order p^i. in particular, let H be a subgroup such that $|H| = p^i$. Now consider $N_G(H)$, the normalizer of H in G. By definition, $H \lhd N_G(H)$. Also, by the corollary to our previous proof, $N_G(H) \neq H$ and p divides $|N_G(H)/H|$. Hence, since $|N_G(H)/H|$ is divisible by p, it follows from Cauchy's Theorem that $N_G(H)/H$ has a subgroup K/H of order p where $K = \{x \in N_G(h) \mid xH \in K/H\}$ and K is a subgroup of $N_G(H)$. Hence, K is also a subgroup of G. Furthermore, since $p = |K/H| = \frac{|K|}{|H|} = \frac{|K|}{p^i}$, it now follows that $|K| = p^{i+1}$, and our induction argument is complete.

(2) For the second part of this theorem, note that $H \lhd N_G(H)$, $H \leq K$, and $K \leq N_G(H)$. Since every element of K is also an element of $N_G(H)$, it follows that if $k \in K$, then $kHk^{-1} = H$. Hence, $H \lhd K$, and since $|H| = p^i$ and $|K| = p^{i+1}$, we're done. □

Definition: If G is a finite group and $|G| = p^n m$ where $n \geq 1$ and p is a prime that does not divide m, then any subgroup of G of order p^n is called a Sylow p-subgroup.

The Second Sylow Theorem: If P_1 and P_2 are distinct Sylow p-subgroups of a fnite group G, then P_1 and P_2 are conjugate.

Proof: Let $X =$ the set of left cosets of P_1 in G and let P_2 act on X as follows: If $xP_1 \in X$ and $y \in P_2$, then $y(xP_1) = (yx)P_1$. Also, let $Z_{P_2}(X) = \{xP_1 \in X \mid \text{for every } y \in P_2,\ y(xP_1) = (yx)P_1 = xP_1\}$. Then by previous proof, $|X| - |Z_{P_2}(X)|$ is divisible by p. Also, since $|X| = \frac{|G|}{|P_1|}$ is not divisible by p (since P_1 is a Sylow p-subgroup), it follows that $|Z_{P_2}(X)| \neq 0$. Hence, $yxP_1 = xP_1$ for all $y \in P_2 \Leftrightarrow x^{-1}yxP_1 = P_1 \Leftrightarrow x^{-1}yx \in P_1 \Leftrightarrow x^{-1}P_2 x \leq P_1$. However, since $|P_1| = |P_2|$, we can conclude that $x^{-1}P_2 x = P_1$, and P_1 and P_2 are conjugate. □

The Third Sylow Theorem: If G is a finite group and a prime p divides G, then the number of Sylow p-subgroups minus one is also divisible by p. Additionally, the number of Sylow p-subgroups is also a divisor of $|G|$.

Proof: Let P be a Sylow p-subgroup and let X be the set of all Sylow p-subgroups in G, and let P act on X by conjugation. Then by previous proof, $|X| - |Z_P(X)|$ is divisible by p. If $T \in Z_P(X)$, then $xTx^{-1} = T$ for all $x \in P$. Hence, $P \leq N_G(T)$. Also, $T \leq N_G(T)$. Furthermore, since P and T are both Sylow p-subgroups of G, they are also Sylow p-subgroups of $N_G(T)$, and since T and P are conjugate with $T \lhd N_G(T)$, it follows that $T = P$. Thus, $Z_P(X) = \{T\} = \{P\}$, and $|Z_P(X)| = 1$. Hence, p divides $|X| - |Z_P(X)| = |X| - 1$.

Now let G act on X by conjugation. Then since all the Sylow p-subgroups are conjugate, G produces only one orbit on X. Thus, if $P \in X$, then $|X| = |\text{orbit of } P| = \frac{|G|}{|G_P|} = \frac{|G|}{|Stabilizer_G(P)|}$. Since we can rewrite this as $|Stabilizer_G(P)| = \frac{|G|}{|X|}$, it follows that the number of Sylow p-subgroups is a divisor of $|G|$. □

Corollary: If G is a finite group such that $|G| = p^n m$ where p is a prime that does not divide m, then the number of Sylow p-subgroups is a divisor of m.

Proof: Let k be the number of Sylow p-subgroups. Then k divides $|G| = p^n m$. Additionally, p divides $k-1$. If $k = p^i q$ for $1 \le i \le n$ and q a divisor of m, then we have a problem since p does not evenly divide $p^i q - 1$. Therefore, $k = q$ where q is a divisor of m.

□

Corollary: If G is a finite group such that $|G| = p^n m$ where p is a prime that does not divide m and if P is a Sylow p-subgroup, then the number of Sylow p-subgroups is equal to $[G : N_G(P)] = \dfrac{|G|}{|N_G(P)|}$.

Proof: Let's consider the left cosets of $N_G(P)$ in G. If $x \in N_G(P)$, then $xPx^{-1} = P$. Furthermore, if $y \cdot N_G(P) = z \cdot N_G(P)$, then $z^{-1}y \cdot N_G(P) = N_G(P)$. But this means that $z^{-1}y \in N_G(P)$ and, hence, $(z^{-1}y)P(z^{-1}y)^{-1} = P \Leftrightarrow (z^{-1}y)P(y^{-1}z) = P \Leftrightarrow yPy^{-1} = zPz^{-1}$. In other words, two elements belong to the same left coset of $N_G(P)$ if and only if they generate the same conjugate subgroup of P. Thus, the number of conjugate subgroups of P is equal to the number of left cosets of $N_G(P)$ in G, and this, in turn, is equal to $[G : N_G(P)] = \dfrac{|G|}{|N_G(P)|}$.

□

Corollary: If G is a finite abelian group and $|G| = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ for primes $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$, then $G = S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}$ where each $S_{p_i^{n_i}}$ is a Sylow p_i-subgroup.

Proof: We know that each $S_{p_i^{n_i}}$ is normal in G, that $\left|S_{p_i^{n_i}}\right| = p_i^{n_i}$, that $S_{p_i^{n_i}} \cap S_{p_j^{n_j}} = e$ when $i \neq j$, and that $\left|S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}\right| = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$. Therefore, it must follow that $G = S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}$.

□