p-GROUPS AND SYLOW'S THEOREMS

MIKE ZABROCKI

A friend showed me his notes on Sylow's theorems and his presentation he had a way of showing the theorems as a direct application of groups acting on sets. I've stripped down his proofs to the minimal details below, fill in the details (at least by doing the exercises, but it is best to rewrite the whole thing filling in the whole sentences).

Proposition 1. *Let G be a p-group acting on a (finite) set E, then*

$$|E| \equiv |Fix_G(E)| \ (mod\ p)$$

Proof. Break E into orbits $E = \mathtt{ORBIT}_G(x_1) \cup \mathtt{ORBIT}_G(x_2) \cup \cdots \cup \mathtt{ORBIT}_G(x_n)$ then

$$|E| = \sum_{i=1}^{n} |\mathtt{ORBIT}_G(x_i)| = \sum_{i=1}^{n} \frac{|G|}{|\mathtt{STAB}_G(x_i)|} \tag{1}$$

But since $\mathtt{STAB}_G(x_i)$ is a sub-group of G, each of $\frac{|G|}{|\mathtt{STAB}_G(x_i)|}$ is some p^{b_i} with $b_i \geq 0$. Note $Fix_G(E) = \{x_i : 1 \leq i \leq n, b_i = 0\}$, therefore

$$|E| = |Fix_G(E)| + \sum_{\substack{i=1 \\ x_i \notin Fix_G(E)}}^{n} |\mathtt{ORBIT}_G(x_i)| \equiv |Fix_G(E)| \ (mod\ p)$$

□

Corollary 2. *If p prime, and m an integer such that p does not divide m*

$$\binom{p^n m}{p^n} \equiv m \ (mod\ p)$$

Proof. Take G be $\mathbb{Z}_{p^n m}$ and H be a subgroup of order p^n.[1] Let X be the set of subsets $S \subseteq G$ such that $|S| = p^n$. Note that $|X| = \binom{p^n m}{p^n}$ and let H act on the elements of X by left multiplication. The set $Fix_H(X)$ are the left cosets of H.[2] Since we know that there are m left cosets of H, the corollary follows from Proposition 1. □

We already showed:

Theorem 3. *The center of a p-group G is non-trivial.*

[1] **Exercise**: Show there is a subgroup of order p^n

[2] **Exercise**: $S \in Fix_H(X)$ if and only if S is a left coset of H

Proof. Let G act on itself by conjugation, then $Fix_G(G) = Z(G)$.[3] By Proposition 1,

$$0 = |G| \equiv |Fix_G(G)| \equiv |Z(G)| \ (mod\ p)$$

so p divides $|Z(G)|$. □

Theorem 4. *(1^{st} Sylow theorem) Sylow p sub-groups always exist.*

Proof. Assume that G is a group of order $p^n m$ where $gcd(p, m) = 1$. Let X be the set of subsets of G of order p^n and let G act on X by left multiplication. As in (1), let x_i be the representatives of the orbits. Since $|X| = \binom{p^n m}{p^n}$, then $|X| \equiv m \ (mod\ p)$ so p does not divide $|X|$ so there exists at least one x_i such that p does not divide $|G|/|\mathtt{STAB}_G(x_i)|$ and hence p^n divides $|\mathtt{STAB}_G(x_i)|$. Now take a $y \in x_i$, $|\mathtt{STAB}_G(x_i)| = |\{zy : z \in \mathtt{STAB}_G(x_i)\}| \leq |x_i| = p^n$.[4] So $|\mathtt{STAB}_G(x_i)|$ is both less than and greater than or equal to p^n and so is a group of order p^n. □

Theorem 5. *(2^{nd} Sylow theorem) All Sylow p-subgroups are conjugate to each other.*

Proof. Let T and S be two subgroups of order p^n. Act T on the left cosets of G/S by left multiplication, then since T is a p-group,

$$|G/S| \equiv |Fix_T(G/S)| \ (mod\ p).$$

Since p does not divide $|G/S|$, $Fix_T(G/S)$ is non-empty and contains an element gS. Since $T \subseteq gSg^{-1}$,[5] then $T = gSg^{-1}$. □

Theorem 6. *(3^{rd} Sylow Theorem) Let n_p be the number of Sylow subgroups, then n_p divides the order of G.*

Proof. Let G act on the Sylow subgroups by conjugation. We know there is one orbit, so take one of them, S, and $n_p = |\mathtt{ORBIT}_G(S)| = |G|/|\mathtt{STAB}_G(S)|$ so n_p divides $|G|$. □

Theorem 7. *(4^{th} Sylow Thoerem) $n_p \equiv 1 \ (mod\ p)$*

Proof. Fix an $S \in Syl_p(G)$ and act on all the Sylow subgroups of G (denoted $Syl_p(G)$) by conjugation. By Proposition 1,

$$n_p = |Syl_p(G)| \equiv |Fix_S(Syl_p(G))| \ (mod\ p)$$

and it turns out that $|Fix_S(Syl_p(G))| = 1$. Take a $P \in Fix_S(Syl_p(G))$, then $S \subseteq N_G(P)$.[6] Since S and P are both Sylow p subgroups of $N_G(P)$, then by the 1^{st} Sylow theorem, $S = gPg^{-1}$ with $g \in N_G(P)$ and hence $S = gPg^{-1} = P$. □

[3] **Exercise**: Show that under this action $Fix_G(G) = Z(G)$

[4] **Exercise:** Explain why $|\mathtt{STAB}_G(x_i)| = |\{zy : z \in \mathtt{STAB}_G(x_i)\}|$

[5] **Exercise**: Show that if $gS \in Fix_T(G/S)$, then $T \subseteq gSg^{-1}$

[6] **Exercise**: Show if $P \in Fix_S(Syl_p(G))$, then $S \subseteq N_G(P)$.