MAT 347
A proof of Sylow's Theorems
October 22, 2019

Given a finite group G and a subgroup $H \leq G$, we say that H is a *p-subgroup* if $|H| = p^k$ for some k, and H is a *Sylow p-subgroup* if $|H|$ is the highest power of p dividing G. The goal for today is to prove Sylow's Theorem:

Theorem Let G be a group of order $p^\alpha m$, where p is a prime not dividing m. Let n_p denote the number of Sylow p-subgroups of G.

1. G has a Sylow p-subgroup ($n_p > 0$).
2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$. In particular, all Sylow p-subgroups are conjugate.
3. $n_p \equiv 1 \pmod p$, and $n_p = |G : N_G(P)| \,\big|\, m$ for any Sylow p-subgroup P of G.

Part 1

1. Prove that $\binom{p^\alpha m}{p^\alpha} \equiv m \pmod p$.

   Hint: What is $(1+x)^p$ when you reduce the cofficients modulo p? What about $(1+x)^{p^2} = ((1+x)^p)^p$? $(1+x)^{p^\alpha}$? And finally, $(1+x)^{p^\alpha m} = \left((1+x)^{p^\alpha}\right)^m$?

2. Let S denote the collection of all subsets of G with cardinality p^α. G acts on S by left multiplication. Prove that there exists an orbit $\mathcal{O}$ of this action such that $p \nmid |\mathcal{O}|$.

   Hint: What does the quantity in Question 1 count?

3. Given $X \in \mathcal{O}$, prove that $p^\alpha \,\big|\, |\text{Stab}(X)|$. (Here, $\mathcal{O}$ is as in Question 2.)

4. With X as above, let $x \in X$. What is the relationship between the sets $\text{Stab}(X)x$ and X? Use this to prove $|\text{Stab}(X)| \leq p^\alpha$, and conclude that $\text{Stab}(X)$ is a Sylow p-subgroup.

Lemma

5. Let H be a p-group ($|H| = p^n$ for some n) acting on a set T, and let $\text{Fix}(H) = \{t \in T : \forall h \in H, h \cdot t = t\}$ denote the set of elements of T which are fixed by the action. Prove that $|\text{Fix}(H)| \equiv |T| \pmod p$.

Part 2

6. Let P be a Sylow p-subgroup, and Q any p-subgroup of G. Then Q acts on G/P (the set of left cosets) by left multiplication. Prove that there exists a coset of P which is fixed by this action.

   Hint: Use the lemma.

7. Take $g \in G$ so that gP is fixed by the action of Q. Prove that $Q \leq gPg^{-1}$.

Part 3

8. Use the Second Sylow Theorem to prove that $n_p = |G : N_G(P)|$. Deduce that n_p divides m.

   Hint: What group action does $N_G(P)$ have anything to do with?

9. Given a Sylow p-subgroup P, P acts on the set of all Sylow p-subgroups by conjugation. Show that there is a fixed point P'. For *any* fixed point P' deduce that $P \leq N_G(P')$ and $P' \lhd N_G(P')$.

10. Show that $P' = P$, and conclude that $n_p \equiv 1 \pmod p$.

    Hint: Apply the Second Sylow Theorem to $N_G(P')$ and remember the lemma.

Fun problem: Generalising your proof to Question 1, show that $\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\cdots \pmod p$, where $n = n_0 + pn_1 + \cdots$ and $k = k_0 + pk_1 + \cdots$ are the base p expansions of the integers n, k (meaning $n_i, k_i \in \{0, 1, \ldots, p-1\}$). For example, $\binom{100}{50} \equiv \binom{2}{1}\binom{0}{0}\binom{2}{1} \equiv 4 \pmod 7$.