

## A PROOF OF SYLOW'S THEOREMS

In this handout, we give proofs of the three Sylow theorems which are slightly different from the ones in the book. Recall the following lemma:

**Lemma.** *Let  $p$  be a prime number, and let  $G$  be a  $p$ -group (a finite group of order  $p^k$  for some  $k \geq 1$ ) acting on a finite set  $S$ . Then the number of fixed points of the action is congruent to  $|S|$  modulo  $p$ .*

We make the following definition: if  $G$  has order  $p^k m$  with  $p \nmid m$ , a *Sylow  $p$ -subgroup* of  $G$  is a subgroup of order  $p^k$ .

**Theorem** (Sylow's First Theorem). *If  $G$  is a finite group of order  $n = p^k m$  with  $p$  prime and  $p \nmid m$ , then  $G$  has a subgroup of order  $p^k$ . In other words, if  $\text{Syl}_p(G)$  denotes the set of Sylow  $p$ -subgroups of  $G$ , then  $\text{Syl}_p(G) \neq \emptyset$ .*

*Proof.* The proof is by induction on  $|G|$ , the base case  $|G| = 1$  being trivial. If there exists a proper subgroup  $H$  of  $G$  such that  $p \nmid [G : H]$ , then a Sylow  $p$ -subgroup of  $H$  is also a Sylow  $p$ -subgroup of  $G$  and we're finished by induction. So without loss of generality, we may assume that  $p \mid [G : H]$  whenever  $H < G$ . From the class equation, it follows that  $p \mid |Z_G|$ . By Cauchy's theorem, there exists a subgroup  $N \leq Z_G$  of order  $p$ , which is necessarily normal in  $G$ . Let  $\overline{G} = G/N$ , so  $|\overline{G}| = p^{k-1}m$ . By induction,  $\overline{G}$  has a subgroup  $\overline{P}$  of order  $p^{k-1}$ . Let  $P$  be the subgroup of  $G$  containing  $N$  which corresponds to  $\overline{P}$  by the first isomorphism theorem. Then

$$|P| = |P/N| \cdot |N| = p^{k-1} \cdot p = p^k,$$

so that  $P$  is a Sylow  $p$ -subgroup of  $G$  as desired.  $\square$

**Theorem** (Sylow's Second Theorem). *If  $G$  is a finite group and  $p$  is a prime number, then all Sylow  $p$ -subgroups of  $G$  are conjugate to one another.*

*Proof.* We show more precisely that if  $H$  is any subgroup of  $G$  of  $p$ -power order and  $P$  is any Sylow  $p$ -subgroup of  $G$ , then there exists  $x \in G$  such that  $H \leq xPx^{-1}$ . (This implies the theorem, since if  $H \in \text{Syl}_p(G)$  then

$|H| = |P| = |xPx^{-1}|$ , which implies that  $H = xPx^{-1}$ , so that  $H$  is conjugate to  $P$ .) Note that  $H$  acts on  $G/P$  (the set of left cosets of  $P$  in  $G$ ) by left multiplication. Let  $\text{Fix}$  denote the elements of  $G/P$  fixed by this action. Then  $|\text{Fix}| \equiv |G/P| \pmod{p}$  by the Lemma. Since  $p \nmid m = |G/P|$ ,  $|\text{Fix}| \neq 0$ , and thus  $\text{Fix} \neq \emptyset$ . Let  $xP$  be a left coset fixed by the action. Then

$$hxP = xP \forall h \in H \Rightarrow x^{-1}Hx \leq P,$$

so that  $H \leq xPx^{-1}$  as desired.  $\square$

**Theorem** (Sylow's Third Theorem). *If  $G$  is a finite group and  $p$  is a prime number, let  $n_p = |\text{Syl}_p(G)|$ . Then  $n_p \mid |G|$  and  $n_p \equiv 1 \pmod{p}$ .*

*Proof.* We consider the action of  $G$  on  $\text{Syl}_p(G)$  by conjugation. By the second Sylow theorem, this action is transitive, so there is just one orbit. Hence  $n_p$ , which is the size of this orbit, divides  $|G|$ .

To prove the congruence  $n_p \equiv 1 \pmod{p}$ , we fix a Sylow  $p$ -subgroup  $P \in \text{Syl}_p(G)$  and consider the action of  $P$  on  $\text{Syl}_p(G)$  by conjugation. Let  $\text{Fix}$  denote the set of fixed points of this action. Note that  $Q \in \text{Fix} \iff P \leq N_G(Q)$ , and in particular  $P \in \text{Fix}$ . If  $Q \in \text{Fix}$ , then  $P, Q \leq N_G(Q)$  are both Sylow  $p$ -subgroups of  $N_G(Q)$ , so they are conjugate in  $N_G(Q)$  (again by the second Sylow theorem). But  $Q$  is a normal subgroup of  $N_G(Q)$ , so  $P = Q$ . Thus  $\text{Fix} = \{P\}$ , and in particular  $|\text{Fix}| = 1$ . By the Lemma,  $n_p \equiv 1 \pmod{p}$  as desired.  $\square$

The more precise fact established in our proof of Sylow's Second Theorem yields the following useful result:

**Corollary.** *If  $G$  is a finite group and  $p$  is a prime number, then any subgroup of  $G$  of  $p$ -power order is contained in some Sylow  $p$ -subgroup.*

Since  $G$  acts transitively by conjugation on  $\text{Syl}_p(G)$ , and the stabilizer of  $P \in \text{Syl}_p(G)$  is  $N_G(P)$ , we deduce that  $n_p = [G : N_G(P)]$  for any  $P \in \text{Syl}_p(G)$ . Therefore:

**Corollary.** *If  $G$  is a finite group and  $p$  is a prime number, let  $n_p$  be the number of Sylow  $p$ -subgroups of  $G$ . Then the following are equivalent:*

1.  $n_p = 1$ .
2. Every Sylow  $p$ -subgroup of  $G$  is normal.
3. Some Sylow  $p$ -subgroup of  $G$  is normal.