17 Proofs of Sylow's theorem parts 2 and 3 (11/01)

Lemma 17.1. *Let G be a finite group, p a prime number, $P \subseteq G$ a p-Sylow subgroup, and $Q \subseteq G$ a sub-p-group. Then, $P \cap Q = N_G(P) \cap Q$.*

Theorem 17.2 (Sylow parts 2 and 3)**.** *Let G be a finite group and fix a prime p. Fix a p-Sylow subgroup P of G.*

(2) *If Q is any p-subgroup of G, then $Q \subseteq gPg^{-1}$ for some $g \in G$. Thus, any two p-Sylow subgroups of G are conjugate.*

(3) *Let n_p be the number of p-Sylow subgroups of G. Then,*

$$n_p = [G : N_G(P)] \equiv 1 \mod p.$$

Proof. Let $X = \{P = P_1, \ldots, P_k\}$ be the set of conjugates of P in G. This set is non-empty by because it contains P and it is finite because G has only finitely many subgroups. Let $\mathrm{Syl}_p(G)$ be the set of p-Sylow subgroups of G. We want, among other things, to show that $X = \mathrm{Syl}_p(G)$ and to show that G acts transitively on $\mathrm{Syl}_p(G)$ under conjugation. Let $Q \subseteq G$ be a p-subgroup of G. Then, Q acts on X by conjugation. While G acts transitively on X (by definition), we do not know that about Q. So, let $X = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \cdots \sqcup \mathcal{O}_r$ be the partition of X into disjoint orbits for the conjugation action of Q. Let $P_{\mathcal{O}_i} \in \mathcal{O}_i$ be a representative. This means that $P_{\mathcal{O}_i} \in X$ (so that is conjugate to P via an element of G) and its orbit under the conjugation action of Q is $\mathcal{O}_i$. Of course,

$$|\mathcal{O}_i| = [Q : N_Q(P_{\mathcal{O}_i})] = [Q : P_{\mathcal{O}_i} \cap Q],$$

where $N_Q(P_{\mathcal{O}_i})$ is defined to be $N_G(P_{\mathcal{O}_i}) \cap Q$ and where we use Lemma 17.1 for the second equality.

The paragraph above works for any p-group Q. Then, the orbit of X containing P_1 under conjugation by P_1 is just $\{P_1\}$. Call this orbit $\mathcal{O}_1$. If $\mathcal{O}_i$ is another orbit, so $2 \leqslant i \leqslant r$, then $P_{\mathcal{O}_i} \cap P_1$ is a proper subset of P_1, since otherwise they would be equal subgroups. Thus, $|\mathcal{O}_i| = [P_1 : P_{\mathcal{O}_i} \cap P_1]$ is a power of p. So,

$$|X| = \sum_{i=1}^{r} |\mathcal{O}_1| = 1 + pN$$

for some N. Therefore,

$$k \equiv 1 \mod p.$$

Now, let Q be an arbitrary non-trivial sub-p-group of G. Assume that Q is not contained in any p-Sylow subgroup of G and in particular in no member of X. Then, $P_i \cap Q$ is a proper subgroup of Q for all $i = 1, \ldots, k$. Therefore, in the orbit decomposition, $p \mid |Q : N_Q(P_{\mathcal{O}_i})|$ for all $1 \leqslant i \leqslant r$. But, by the class formula for actions, this implies that $p \mid |X| \equiv 1 \mod p$, which is a contradiction. This proves that Q is contained in a member of X. As this applies also to other p-Sylow subgroups of G, we see that in fact X is a complete list of the p-Sylow subgroups and that every p-Sylow subgroup of G is conjugate to P. This proves (2).

It also proves that $n_p = k \equiv 1 \mod p$. Now, using orbit decomposition again, since the action of G on $\mathrm{Syl}_p(G)$ is transitive, we find that $n_p = \frac{|G|}{|N_G(P)|} = [G : N_G(P)]$. This completes the proof. □

Corollary 17.3. *Any two p-Sylow subgroups of a finite group are isomorphic as groups.*

Proof. By Theorem 17.2, it is enough to show that conjugate subgroups are isomorphic. Let G be a group, let $P, Q \subseteq G$ be subgroups, and let $g \in G$. If $gPg^{-1} = Q$, then $P \cong Q$. Let $c \colon P \to Q$ be defined by $c(h) = ghg^{-1}$. This is a group homomorphism because $c(hk) = ghkg^{-1} = ghg^{-1}ghg^{-1} = c(h)c(k)$. It is injective because if $c(h) = e$, it follows that $ghg^{-1} = e$ or $h = g^{-1}g = e$. It is surjective because given $k \in Q$ the element $g^{-1}kg$ is in P and $c(g^{-1}kg) = k$. □

Warning 17.4. We are *not* saying that any two p-Sylow subgroups are equal as subgroups, i.e. that they have the same elements. We are saying that they are isomorphic as abstract groups.

Corollary 17.5. *If G is a finite group and p is a prime and G has a normal p-Sylow subgroup P, then P is the only p-Sylow subgroup. Conversely, if P is the only p-Sylow subgroup in G, then it is normal.*

Proof. If P is normal, then $N_G(P) = P$ so $n_p = 1$. Conversely, if $n_p = 1$, then $[G : N_G(P)] = 1$, so $N_G(P) = G$ and P is normal in G. □

Example 17.6 (Groups of order pq)**.** Let $p < q$ be distinct prime numbers. Let G be a group of order pq. I claim that G has a normal subgroup of order q. Note that this is precisely what happens for S_3 which has a normal subgroup of order 3. Suppose that $p < q$. If Q is not normal, then $N_G(Q) = Q$ and $1 \neq n_q = p \equiv 1 \mod q$, which is impossible and gives a contradiction.

Example 17.7 (From Dummit–Foote)**.** Prove that a group G of order 200 has a normal 5-Sylow subgroup. (Note there are 52 such groups!) We have that $200 = 8 * 25 = 2^3 * 5^2$. We have $n_5 \equiv 1 \mod 5$ and is equal to one of $1, 2, 4, 8$. It must be 1, so there is one 5-Sylow subgroup, which is necessarily normal.

17.1 Exercises

Exercise 17.1. Prove that a group of order $2 \leqslant |G| \leqslant 20$ is either of prime order or has a nontrivial normal subgroup.

n

Exercise 17.2. Prove that a group of order 99 has a normal 11-Sylow subgroup.