SHORT PROOFS OF THE SYLOW THEOREMS

PAUL POLLACK

Definition 1. *Let G be a group and H and K subgroups. By an* H-K double coset *we mean a subset of G of the form $HaK := \{hak : h \in H, k \in K\}$.*

One checks that two double cosets HaK and $Ha'K$ are either identical or disjoint; thus the double cosets partition G.

Definition 2. *If H is a subgroup of G and $a \in G$, we use the notation H^a to mean the conjugate subgroup $a^{-1}Ha$.*

Lemma 1 (Double Coset Counting Formula)**.** *Let H, K be finite subgroups of a group G, and let $a \in G$. Then $|HaK| = |H||K|/|H^a \cap K|$.*

Proof. Consider the obvious surjective map $H \times K \to HaK$. The preimage of any element h_1ak_1 consists of those (h_2, k_2) with $h_2ak_2 = h_1ak_1$, i.e., $a^{-1}h_1^{-1}h_2a = k_1k_2^{-1}$. Both sides of this equation lie in $H^a \cap K$, and given any $e \in H^a \cap K$, there exists a unique pair $(h_2, k_2) \in H \times K$ for which

$$a^{-1}h_1^{-1}h_2a = k_1k_2^{-1} = e.$$

It follows that the preimage of the (arbitrary) element h_1ak_1 has size precisely $|H^a \cap K|$, which gives the result. □

Definition 3. *Let p be a prime. A subgroup H of a finite group G is a p-*Sylow subgroup of G *if $|H| = p^k$, where p^k is the highest power of p dividing $|G|$.*

Theorem 1. *Suppose G is a finite group with a p-Sylow subgroup P. Let H be a subgroup of G. Then there exists an $a \in G$ with $P^a \cap H$ a p-Sylow subgroup of H.*

Proof. We can write G as the disjoint union of $P - H$ double cosets. Then taking the sum over a complete set of representatives, we have

$$|G| = \sum_a |PaH| = \sum_a \frac{|P||H|}{|P^a \cap H|},$$

whence

$$|G|/|P| = \sum_a \frac{|H|}{|P^a \cap H|}. \tag{1}$$

The left hand side is not divisible by p, so some term in the right hand sum is not divisible by p. Any a corresponding to such a term works in the theorem. □

Corollary 1 (Second Sylow Theorem)**.** *Let G be a finite group, and let P_1 and P_2 be two p-Sylow subgroups. Then there exists $a \in G$ with $P_1^a = P_2$.*

Proof. Take $P = P_1$ and $H = P_2$ in the theorem to see there exists $a \in G$ with P_1^a a p-Sylow subgroup of P_2. But P_2 is the only p-Sylow subgroup of P_2. □

Theorem 2 (First Sylow Theorem)**.** *Let G be a finite group. Then there exists a p-Sylow subgroup of G.*

Proof. By the preceding theorem, it suffices to embed G in a group possessing a p-Sylow subgroup. If $n = |G|$, then G emebds in S_n by Cayley's theorem; S_n in turn embeds in $\mathrm{GL}_n(\mathbf{F}_p)$. It thus suffices to produce a p-Sylow subgroup of $\mathrm{GL}_n(\mathbf{F}_p)$.

We claim the group of upper triangular matrices with 1's along the diagonal is such a p-Sylow subgroup. The size of this group is $p^1p^2 \dots p^{n-1} = p^{n(n-1)/2}$. But this is the highest power of p dividing the order of $\mathrm{GL}_n(\mathbf{F}_p)$, since said order is

$$(p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) = p^{n(n-1)/2} \prod_{i=1}^{n-1} (p^i - 1). \qquad \square$$

Our next corollary is sometimes included as part of the first Sylow theorem.

Corollary 2. *Let G be a finite group and let H be a p-subgroup of G (i.e., one whose order is a power of p). Then H is contained in a p-Sylow subgroup of G.*

Proof. Let P be a p-Sylow subgroup of G (which we can do by Theorem 2). By Theorem 1, there exists $g \in G$ with $P^g \cap H$ a p-Sylow subgroup of H; this forces $P^g \cap H = H$. So we may take P^g as the p-Sylow subgroup. □

Theorem 3 (Third Sylow Theorem)**.** *Let G be a finite group and let p be a prime. The number n_p of p-Sylow subgroups of G is the index of the normalizer $N_G(P)$ in G. Moreover, this number n_p satisfies $n_p \equiv 1 \pmod{p}$.*

Proof. Let P be a fixed p-Sylow subgroup (which exists by Theorem 2).

That $n_p = [G : N_G(P)]$ follows from the orbit-stabilizer theorem: if G acts on its subgroups by conjugation, then the orbit of P is all of the p-Sylow subgroups (by Theorem 1). The size of this orbit is the size of G divided by the size of the stabilizer of P under this action, which is just $N_G(P)$.

To see $n_p \equiv 1 \pmod{p}$, we once again appeal to double coset counting. This time we consider the double cosets of P and P. As before, we have (cf. (1))

$$|G|/|P| = \sum_a \frac{|P|}{|P^a \cap P|},$$

the sum being over any complete set A of representatives of the double cosets. The terms in the right hand sum are all divisible by p except for those where $P^a = P$, i.e., for those where $a \in N_G(P)$. Thus

$$|G|/|P| \equiv \#\{a \in A : a \in N_G(P)\} \pmod{p}.$$

It is straightforward to check that for any a,

$$a \in N_G(P) \iff \text{the double coset } PaP \text{ is contained in } N_G(P).$$

Consequently, the right hand side of our congruence is just the number of double cosets of P contained in $N_G(P)$, which is the same as the number of double cosets of P as a subgroup of its normalizer $N_G(P)$.

Each such double coset PaP has size

$$|P|^2/|P^a \cap P| = |P|^2/|P| = |P|,$$

since $a \in N_G(P)$. Since the double cosets partition $N_G(P)$, there are exactly $|N_G(P)|/|P|$ of them. Substituting this into our previous congruence shows

$$|G|/|P| \equiv |N_G(P)|/|P| \pmod{p},$$

whence

$$|G| \equiv |N_G(P)| \pmod{p|P|},$$

and

$$n_p = |G|/|N_G(P)| \equiv 1 \pmod{p\frac{|P|}{\gcd(|N_G(P)|, |P|)}}.$$

Since p divides the final modulus, the result follows. □

NOTE: These arguments are not mine, and I am not sure of their ultimate origin. The arguments for the first two were told to me secondhand by someone who had learned them in John Conway's undergraduate algebra class. The third argument was conjured by Davesh Maulik during a brainstorming/generals-studying session.