Math 594. Some consequences of the Sylow theorems

The Sylow theorems concern subgroups with prime power size, especially with maximal prime power size.

When $\#G = p^k m$ and p^k is as large as possible (that is, p doesn't divide m), we call any subgroup of G with size p^k a *p-Sylow subgroup.* (When p doesn't divide $\#G$, $p^k = 1$ and the trivial subgroup is the p-Sylow subgroup.) A subgroup that is a p-Sylow subgroup for some p is called a *Sylow subgroup.* For example, the Sylow subgroups of S_5 (whose size is $120 = 2^3 \cdot 3 \cdot 5$) are the subgroups with size 1, 8, 3, or 5.

Theorem 0.1 (Sylow I). *If $p^d | \#G$, then G has a subgroup of size p^d. In particular, G has a p-Sylow subgroup for every prime p.*

Theorem 0.2 (Sylow II). *For each prime p, any p-subgroup of G lies in a p-Sylow subgroup, and the p-Sylow subgroups of G are conjugate.*

Theorem 0.3 (Sylow III). *Let n_p be the number of p-Sylow subgroups of G. Write $\#G = p^k m$, where p doesn't divide m. Then*

$$n_p | m, \quad n_p \equiv 1 \bmod p.$$

Theorem 0.4 (Sylow III*). *Let n_p be the number of p-Sylow subgroups of G. Then $n_p = [G : H]$ for some subgroup H.*

The information in the Sylow theorems leads to many structure theorems about finite groups, some of which we treat below. Because of the Sylow theorems, groups of prime power size take on a heightened significance, and these theorems might motivate a mathematician to undertake a special study of groups with prime power size.

For each prime p, the p-Sylow subgroups in G are conjugate by Sylow II, and therefore $n_p = 1$ precisely when a p-Sylow subgroup is a normal subgroup. *Be sure you understand that reasoning.* We will constantly shift back and forth between the condition $n_p = 1$ (if it holds) and the condition that G has a normal p-Sylow subgroup. In particular, the Sylow theorems are a tool for proving a group has a nontrivial normal subgroup because we can try to show $n_p = 1$ for some prime p dividing $\#G$.

The last theorem above, which we call Sylow III*, is not traditionally stated as part of the Sylow theorems, although it does follow from the proof of Sylow III. Sylow III* gives a condition on the number n_p which is somewhat less useful in basic applications than the conditions on n_p in Sylow III. We will not have a use for Sylow III* until the final application of this handout where we use it to give a proof of simplicity of A_5 which avoids mucking around with 3-cycles and instead is of more "structural" type.

We first apply the Sylow theorems to some concrete groups.

Corollary 0.5. *The group A_5 has 6 subgroups of size 5.*

Proof. Since $\#A_5 = 60 = 2^2 \cdot 3 \cdot 5$, the 5-Sylow subgroups have size 5. By Sylow III, $n_5 | 12$ and $n_5 \equiv 1 \bmod 5$. The only choices are $n_5 = 1$ or 6. Since A_5 has at least two subgroups of size 5 (the subgroups generated by (12345) and by (21345) are different), $n_5 > 1$ and therefore $n_5 = 6$. ■

The next few corollaries show that knowledge of the size of G can sometimes force G to have a unique p-Sylow subgroup for some p, which is thus a normal subgroup.

We start with a lemma which, while not a consequence of the Sylow theorems, will be used in conjunction with the Sylow theorems.

Lemma 0.6. *If G has k subgroups of size p, it has $k(p-1)$ elements of order p.*

Proof. In a subgroup of size p, all nonidentity elements have order p. Conversely, any element of order p generates a subgroup of size p. By Lagrange, distinct subgroups of size p must intersect trivially, so their nonidentity elements are disjoint from each other. Therefore each subgroup of size p has its own $p - 1$ elements of order p, not shared by any other subgroup of size p. The number of elements of order p is therefore $k(p - 1)$. ■

Corollary 0.7. *If $\#G = 6$, then G has a normal 3-Sylow subgroup.*

Proof. Since we already know groups of size 6 are either cyclic of size 6 (if abelian) or isomorphic to S_3 (if nonabelian), we could prove this by checking the conclusion holds on such explicitly known groups.

Instead, using Sylow III, we have $n_3|2$ and $n_3 \equiv 1 \bmod 3$. Thus $n_3 = 1$, so the 3-Sylow subgroup is normal. ■

Corollary 0.8. *If $\#G = 12$, then G has a normal 2-Sylow or 3-Sylow subgroup.*

Proof. By Sylow III, $n_2|3$ and $n_2 \equiv 1 \bmod 2$, so $n_2 = 1$ or 3. Also $n_3|4$ and $n_3 \equiv 1 \bmod 3$, so $n_3 = 1$ or 4.

We want to show $n_2 = 1$ or $n_3 = 1$.

Assume $n_3 \neq 1$, so $n_3 = 4$. Since the 3-Sylows have size 3, Lemma 0.6 says G has $n_3 \cdot 2 = 8$ elements of order 3. The number of remaining elements is $12 - 8 = 4$. A 2-Sylow subgroup has size 4, and is a subset of this complementary 4 element set, and thus fills it up. Therefore $n_2 = 1$.

Since $n_3 \neq 1$ implies $n_2 = 1$, either n_2 or $n_3 = 1$. ■

That we were unable to show both n_2 and n_3 equal 1 is not an accident. Only one of the choices needs to arise, depending on the group with size 12. For example, A_4 has $n_2 = 1$ but $n_3 \neq 1$, while the mod 6 $ax + b$ group has $n_3 = 1$ but $n_2 \neq 1$.

Corollary 0.9. *If $\#G = 30$, then G has a normal 3-Sylow subgroup and a normal 5-Sylow subgroup.*

Proof. By Sylow III,

$$n_3|10, n_3 \equiv 1 \bmod 3 \Longrightarrow n_3 = 1 \text{ or } 10.$$

and

$$n_5|6, n_5 \equiv 1 \bmod 5 \Longrightarrow n_5 = 1 \text{ or } 6.$$

The 3-Sylows have size 3 and the 5-Sylows have size 5. If $n_3 = 10$ and $n_5 = 6$, then Lemma 0.6 says G has $n_3 \cdot 2 = 20$ elements of order 3 and $n_5 \cdot 4 = 24$ elements of order 5. This adds up to $20 + 24 = 44$ elements, which exceeds $\#G = 30$. Thus $n_3 = 1$ or $n_5 = 1$. We ultimately want to show both numbers equal 1.

Let P be a 3-Sylow subgroup and Q be a 5-Sylow subgroup. By the previous paragraph, at least one of these subgroups is a normal subgroup of G, so their product set PQ is a subgroup of G. Easily $\#PQ \leq 15$. Since P and Q are subgroups of PQ, Lagrange's theorem implies $\#PQ$ is divisible by 3 and 5, and thus by 15. Therefore $\#PQ = 15$, so PQ is a cyclic group (using structure theorem for pq-groups from class).

Since $[G : PQ] = 2$, $PQ \lhd G$. For any $g \in G$, gPg^{-1} and gQg^{-1} are subgroups of $g(PQ)g^{-1} = PQ$. Since PQ is cyclic, it has only one subgroup of each size, and in particular we must have

$$gPg^{-1} = P, \quad gQg^{-1} = Q.$$

As this holds for all $g \in G$, we see P and Q are normal subgroups of G. Thus $n_3 = 1$ and $n_5 = 1$. ■

Recall that normality is not usually transitive: if $N_1 \lhd N_2$ and $N_2 \lhd G$, it need not follow that $N_1 \lhd G$ (the counterexample from class is $G = D_4$). While it is false that a normal subgroup of a normal subgroup is a normal subgroup, it turns out that a normal Sylow subgroup of a normal subgroup is a normal subgroup, as follows.

Corollary 0.10. *Let $P \lhd N$ and $N \lhd G$, where P is a Sylow subgroup of N. Then $P \lhd G$.*

Proof. For any $g \in G$, from $P \subset N$ we have

$$gPg^{-1} \subset gNg^{-1} = N,$$

where the equation follows from normality of N in G. Since P is a Sylow subgroup of N, so is gPg^{-1} (it has the same size as P). However, since $P \lhd N$, it is the only Sylow subgroup of N with its size, by Sylow II. Therefore $gPg^{-1} = P$. As this holds for all $g \in G$, $P \lhd G$. ■

The rest of this handout is devoted to the topic of simple groups. We call a group *simple* when its only normal subgroups are the trivial subgroup and the whole group. For example, the groups of prime size are simple, for the crude reason that they have no subgroups at all besides the whole group and the trivial subgroup. One special property of simple groups is that a homomorphism on a simple group is either an embedding or sends all points to the identity. Indeed, the kernel of a homomorphism is a normal subgroup, so a homomorphism on a simple group is either one-to-one (if the kernel is trivial) or sends all points to the identity (if the kernel is the whole group).

We have seen how to use the Sylow theorems to prove a group is *not* simple. For example, groups of size 12 or 30 are not simple, by Corollaries 0.8 and 0.9. Meanwhile, in class we saw that p-groups and groups of size pq are solvable (it is a non-trivial theorem of Burnside that groups of size $p^a q^b$ are solvable, but his proof used representation theory; a purly group-theoretic proof was only found many decades later by Thompson).

So far we have used the Sylow theorems to prove groups with a certain size have a nontrivial normal subgroup, and therefore are not simple. Now we use the Sylow theorems to prove a certain kind of group *is* simple.

Theorem 0.11. *If* $\#G = 60$ *and* $n_5 > 1$*, then* G *is a simple group.*

For example, since $\#A_5 = (1/2)5! = 60$ and A_5 has more than one 5-Sylow subgroup (cf. Corollary 0.5), A_5 is a simple group. That is, A_5 has no normal subgroups besides A_5 and the trivial subgroup. It can be shown that A_n is a simple group for any $n \geq 5$, but we do not discuss that proof here.

Proof. The proof will use many of our previous corollaries of the Sylow theorems.

Assume G is *not* simple, so there is $N \lhd G$ with $1 < \#N < 60$. We will get a contradiction.

First we show $\#N$ is not divisible by 5. Assume $5 | \#N$, so N contains a 5-Sylow subgroup, which is also a 5-Sylow subgroup of G since $60 = 5 \cdot 12$. Because $N \lhd G$, Sylow II shows all the 5-Sylow subgroups of G lie in N.

Let n_5 be the number of 5-Sylows in G (which we know are all subgroups of N). Since $n_5 | 12$ and $n_5 \equiv 1 \bmod 5$, $n_5 = 1$ or 6. Because $n_5 > 1$, $n_5 = 6$. Therefore N contains *six* different subgroups of size 5. By Lemma 0.6,

$$\#N > n_5 \cdot 4 + 1 = 25.$$

Since $\#N$ is a proper factor of 60, $\#N = 30$. But then, by Corollary 0.9, N has only one 5-Sylow subgroup. This is a contradiction, so $\#N$ is not divisible by 5. This means $\#N$ can be 2, 3, 4, 6, or 12.

If $\#N$ equals 6, then by Corollary 0.7 N contains a normal subgroup of size 3. If $\#N$ equals 12, then by Corollary 0.8 N contains a normal subgroup of size 3 or 4. In either case, such a subgroup is a Sylow subgroup of N and therefore is a normal subgroup of G by Corollary 0.10. Because such a normal subgroup of G has size 3 or 4, which is one of the other possibilies under consideration for $\#N$, we are reduced to eliminating the possibility that $\#N = 2, 3,$ or 4.

If $\#N$ equals 2, 3, or 4, let $\overline{G} = G/N$, so $\overline{G}$ is a group with size 30, 20, or 15. But a group of size 15 is cyclic and thus has a normal 5-Sylow subgroup. It is easy to see by the Sylow theorems that a group of size 20 has a normal 5-Sylow subgroup. By Corollary 0.9, a group of size 30 has a normal 5-Sylow subgroup. Therefore in all cases $\overline{G}$ contains a normal 5-Sylow subgroup, say $\overline{P}$, with $\#\overline{P} = 5$.

Consider the projection $\pi\colon G \to \overline{G}$. Set $H = \pi^{-1}(\overline{P})$. Since $\overline{P} \lhd \overline{G}$, $H \lhd G$. Moreover, $H \neq G$. Thus H is a proper normal subgroup of G. Since π sends H onto $\overline{P}$, $\#H$ is divisible by 5. But we showed earlier that G contains no proper normal subgroups of size divisible by 5.

Since all choices for $\#N$ have been eliminated, there is no such N. Thus G is simple. ∎

The next result, which concludes our applications of the Sylow theorems, shows that A_5 is the only simple group of size 60, up to isomorphism.

Theorem 0.12. *Every simple group of size* 60 *is isomorphic to* A_5.

Proof. To prove a group is isomorphic to A_5, we want to make the group act on a set of 5 objects and then show this action is given only by the even permutations of the 5 objects.

We will seek an action on cosets. Let G be a simple group of size 60. *Suppose* G has a subgroup H with $[G : H] = 5$, so the left multiplication action of G on the coset space G/H gives a homomorphism

$$\varphi \colon G \to \operatorname{Perm}(G/H) \cong S_5.$$

The kernel of φ is a normal subgroup of G, and therefore is trivial or is G, since G is *simple*. If $g \in G$ is in the kernel of φ, then $gH = H$, so $g \in H$. In particular, the kernel of φ is a subgroup of H and therefore the kernel can't be G. The kernel of φ must be trivial, so φ is an embedding of G into S_5; G is isomorphic to its image $\varphi(G)$. In particular, $\varphi(G)$ is a simple group of size 60. Let's prove this image is A_5.

If $\varphi(G) \not\subset A_5$, then $\varphi(G)$ contains an odd permutation. That means the sign homomorphism

$$\operatorname{sgn} \colon \varphi(G) \to \{\pm 1\}$$

is surjective, so its kernel is a normal subgroup of $\varphi(G)$ with index 2. However, $\varphi(G)$ doesn't have such normal subgroups since it is isomorphic to the simple group G and therefore is itself simple. We conclude that all elements of $\varphi(G)$ have sign 1, so $\varphi(G) \subset A_5$. Both groups have size 60, so $\varphi(G) = A_5$.

We have shown that *if* G has a subgroup H with index 5, then the action of G on G/H gives an isomorphism of G with A_5. Now we prove G has a subgroup with index 5.

Step 1: For any proper subgroup $H \subset G$, $[G : H] \geq 5$.

Let $t = [G : H]$. The left multiplication action of G on G/H gives a homomorphism $G \to \operatorname{Perm}(G/H) \cong S_t$. Since H is a proper subgroup and G is simple, this homomorphism has trivial kernel. (The reason follows as before, when we were only concerned with index 5 subgroups: the kernel is a subgroup of H and therefore is a proper normal subgroup of G, which must be trivial since G is simple.) Therefore we have an embedding of G into S_t, so $60 | t!$. This can happen only when $t \geq 5$.

Step 2: G has a subgroup with index 5.

We use Sylow III for the primes 2, 3, and 5. They tell us that

$$n_2 \in \{1, 3, 5, 15\}, \quad n_3 \in \{1, 4, 10\}, \quad n_5 \in \{1, 6\}.$$

Since G is simple, $n_2, n_3, n_5 > 1$. Moreover, because Sylow III* says each n_p is the index of a subgroup of G, Step 1 tells us $n_2, n_3, n_5 \geq 5$. Therefore

$$n_2 \in \{5, 15\}, \quad n_3 = 10, \quad n_5 = 6.$$

We would love to show $n_2 = 5$, since Sylow III* then says there is a subgroup of G with index 5, and that would lead to an isomorphism of G with A_5 for reasons explained already.

To show $n_2 = 5$, we eliminate the possibility that $n_2 = 15$. By Lemma 0.6, G has $n_3 \cdot 2 = 20$ elements of order 3 and $n_5 \cdot 4 = 24$ elements of order 5. This is a total of 44 elements, which leaves at most $60 - 44 = 16$ elements that can lie in the 2-Sylow subgroups of G. Each 2-Sylow subgroup of G has size 4, so if $n_2 = 15$ then we'd have 15 different groups of size 4 squeezed into a 16 element subset of G. It is left to the reader to show this is impossible. (Warning: unlike groups of prime size, groups of size 4 can overlap nontrivially, but at most in a subgroup of size 2.) Therefore $n_2 \neq 15$, so $n_2 = 5$ and we have proved G has a subgroup with index 5 (thanks to Sylow III*). ∎