CONSEQUENCES OF THE SYLOW THEOREMS

KEITH CONRAD

1. Statement of the Sylow theorems

We recall here the statement of the Sylow theorems.

Theorem 1.1 (Sylow I)**.** *A finite group G has a p-Sylow subgroup for every prime p and any p-subgroup of G lies in a p-Sylow subgroup of G.*

Theorem 1.2 (Sylow II)**.** *For each prime p, the p-Sylow subgroups of G are conjugate.*

Theorem 1.3 (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*

$$n_p | m \text{ and } n_p \equiv 1 \bmod p.$$

Theorem 1.4 (Sylow III*)**.** *Let n_p be the number of p-Sylow subgroups of G. Then $n_p = [G : \mathrm{N}(P)]$, where P is any p-Sylow subgroup and $\mathrm{N}(P)$ is its normalizer in G.*

The information in the Sylow theorems leads to basic 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 suggest a careful study of such groups [7].

We will not have too much use for Sylow III* in this handout. It is used in Theorems 2.3, 2.7, and A.4, and Corollary 5.4.

Corollary 1.5. *The condition $n_p = 1$ means a p-Sylow subgroup is a normal subgroup.*

Proof. All p-Sylows are conjugate by Sylow II, so $n_p = 1$ precisely when a p-Sylow of G is self-conjugate, *i.e.*, is a normal subgroup of G. □

Be sure you understand that reasoning. We will often 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 p. However, there are groups which have nontrivial normal subgroups but no nontrivial normal Sylow subgroups, such as S_4. (See Example 6.6.)

Corollary 1.6. *If p and q are different prime factors of $\#G$ and $n_p = 1$ and $n_q = 1$ then the elements of the p-Sylow subgroup commute with the elements of the q-Sylow subgroup.*

Proof. Let P be the p-Sylow subgroup and Q be the q-Sylow subgroup. Since P and Q have relatively primes sizes, $P \cap Q = \{e\}$ by Lagrange. The subgroups P and Q are normal in G since $n_p = 1$ and $n_q = 1$ by hypothesis. For $a \in P$ and $b \in Q$,

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in P \cap Q = \{e\},$$

so $ab = ba$. □

Note Corollary 1.6 is *not* saying the p-Sylow and q-Sylow subgroups of G are abelian, but rather that any element of either subgroup commutes with any element of the other subgroup if the two Sylow subgroups are the only subgroups of their size.

Corollary 1.7. *All the Sylow subgroups of a finite group are normal if and only if the group is isomorphic to the direct product of its Sylow subgroups.*

Proof. If a group is isomorphic to the direct product of its Sylow subgroups then all the Sylow subgroups are normal since a factor in a direct product is a normal subgroup of the direct product. Conversely, suppose G is finite and all of its Sylow subgroups are normal. Write the nontrivial Sylow subgroups as $P_1, P_2, \ldots, P_m$. Elements in P_i and P_j commute for $i \neq j$, so the map $P_1 \times \cdots \times P_m \to G$ given by

$$(x_1, \ldots, x_m) \mapsto x_1 \cdots x_m$$

is a homomorphism. It is injective since the order of a product of commuting elements with relatively prime orders is equal to the product of their orders. Our map is between two groups of equal size, so from injectivity we get that it is an isomorphism. □

2. Applications to specific groups

Theorem 2.1. *The groups A_5 and S_5 each have* 10 *subgroups of size* 3 *and* 6 *subgroups of size* 5.

Proof. Any element of odd order in a symmetric group is an even permutation, so the 3-Sylow and 5-Sylow subgroups of S_5 lie in A_5. Therefore it suffices to focus on A_5.

Since $\#A_5 = 60 = 2^2 \cdot 3 \cdot 5$, the 3-Sylow subgroups have size 3 and the 5-Sylows have size 5. Call the numbers n_3 and n_5. By Sylow III, $n_3|20$ and $n_3 \equiv 1 \bmod 3$, so $n_3 = 1$, 4, or 10. The number of 3-cycles (abc) in A_5 is 20, and these come in inverse pairs, giving us 10 subgroups of size 3. So $n_3 = 10$. Turning to the 5-Sylows, $n_5|12$ and $n_5 \equiv 1 \bmod 5$, so n_5 is 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 $n_5 = 6$. □

Theorem 2.2. *In the group* $\mathrm{Aff}(\mathbf{Z}/(5))$*, there are five* 2*-Sylow subgroups and the* 5*-Sylow subgroup is normal.*

Proof. This group has size 20, so the 2-Sylows have size 4 and the 5-Sylows have size 5.

By Sylow III, $n_2|5$, so $n_2 = 1$ or 5. The matrices $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generate different 2-Sylow subgroups, so $n_2 = 5$.

Now we turn to the 5-Sylow subgroups. By Sylow III, $n_5|4$ and $n_5 \equiv 1 \bmod 5$. The only choice is $n_5 = 1$, which means there is one 5-Sylow subgroup, so it must be normal. □

Let's explore $\mathrm{Aff}(\mathbf{Z}/(5))$ a little further. Since we know the number of 2-Sylow and 5-Sylow subgroups, we can search for all the Sylow subgroups and know when to stop. There are five 2-Sylow subgroups and the five matrices $\left(\begin{smallmatrix} 2 & j \\ 0 & 1 \end{smallmatrix}\right)$, where $j \in \mathbf{Z}/(5)$, generate different subgroups of size 4, so these are all of the 2-Sylow subgroups (and they are cyclic). The matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order 5 and therefore generates the unique 5-Sylow subgroup.

As an illustration of Sylow II in $\mathrm{Aff}(\mathbf{Z}/(5))$, any element of 2-power order is conjugate to an element of the subgroup $\langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \rangle$. For instance, $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order 4 and an explicit search reveals

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix}^{-1}.$$

The matrix $\left(\begin{smallmatrix} 4 & 4 \\ 0 & 1 \end{smallmatrix}\right)$ has order 2 and

$$\begin{pmatrix} 4 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}^{-1}.$$

Theorem 2.3. *For a prime p, any element of $\mathrm{GL}_2(\mathbf{Z}/(p))$ with order p is conjugate to a strictly upper-triangular matrix $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$. The number of p-Sylow subgroups is $p+1$.*

Proof. The size of $\mathrm{GL}_2(\mathbf{Z}/(p))$ is $(p^2-1)(p^2-p) = p(p-1)(p^2-1)$. Therefore a p-Sylow subgroup has size p. The matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order p, so it generates a p-Sylow subgroup $P = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle = \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}$ Since all p-Sylow subgroups are conjugate, any matrix with order p is conjugate to some power of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

The number of p-Sylow subgroups is $[\mathrm{GL}_2(\mathbf{Z}/(p)) : \mathrm{N}(P)]$ by Sylow III*. We'll compute $\mathrm{N}(P)$ and then find its index. For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to lie in $\mathrm{N}(P)$ means it conjugates $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ to some power $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - ac/\Delta & a^2/\Delta \\ -c^2/\Delta & 1 + ac/\Delta \end{pmatrix},$$

where $\Delta = ad - bc \neq 0$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{N}(P)$ precisely when $c = 0$. Therefore $\mathrm{N}(P) = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ in $\mathrm{GL}_2(\mathbf{Z}/(p))$. The size of $\mathrm{N}(P)$ is $(p-1)^2p$. Since $\mathrm{GL}_2(\mathbf{Z}/(p))$ has size $p(p-1)(p^2-1)$, the index of $\mathrm{N}(P)$ is $n_p = p+1$. □

Corollary 2.4. *The number of elements of order p in $\mathrm{GL}_2(\mathbf{Z}/(p))$ is p^2-1.*

Proof. Each p-Sylow subgroup has $p-1$ elements of order p. Different p-Sylow subgroups intersect trivially, so the number of elements of order p is $(p-1)n_p = p^2-1$. □

Theorem 2.5. *There is a unique p-Sylow subgroup of $\mathrm{Aff}(\mathbf{Z}/(p^2))$.*

Proof. The group has size $p^2\varphi(p^2) = p^3(p-1)$, so a p-Sylow subgroup has order p^3.

Letting n_p be the number of p-Sylow subgroups, Sylow III says $n_p|(p-1)$ and $n_p \equiv 1 \bmod p$. Therefore $n_p = 1$.

As an alternate proof, we can locate a p-Sylow subgroup of $\mathrm{Aff}(\mathbf{Z}/(p^2))$ explicitly, namely the matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

where $a^p = 1$ in $(\mathbf{Z}/(p^2))^\times$. (There are p choices for a and p^2 choices for b.) This subgroup is the kernel of the homomorphism $\mathrm{Aff}(\mathbf{Z}/(p^2)) \to (\mathbf{Z}/(p^2))^\times$ given by $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mapsto a^p$, so it is a *normal* subgroup, and therefore is the unique p-Sylow subgroup by Sylow II. □

Note the unique p-Sylow subgroup of $\mathrm{Aff}(\mathbf{Z}/(p^2))$ is a nonabelian group of size p^3. It has an element of order p^2, namely $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and therefore is not isomorphic to $\mathrm{Heis}(\mathbf{Z}/(p))$ when $p \neq 2$, since every non-identity element of $\mathrm{Heis}(\mathbf{Z}/(p))$ has order p. (It can be shown that every nonabelian group of size p^3 for an odd prime p is isomorphic to $\mathrm{Heis}(\mathbf{Z}/(p))$ or to this p-Sylow subgroup of $\mathrm{Aff}(\mathbf{Z}/(p^2))$.)

Can we characterize $\mathrm{Heis}(\mathbf{Z}/(p))$ as the unique p-Sylow subgroup of some larger group? Yes.

Theorem 2.6. *For any prime p,* $\mathrm{Heis}(\mathbf{Z}/(p))$ *is the unique p-Sylow subgroup of the group of invertible upper-triangular matrices*

$$\begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix} \tag{2.1}$$

in $\mathrm{GL}_3(\mathbf{Z}/(p))$.

Proof. This matrix group, call it U, has size $(p-1)^3p^3$, so $\mathrm{Heis}(\mathbf{Z}/(p))$ is a p-Sylow subgroup of U. To show it is the only p-Sylow subgroup, the relations in Sylow III are *not* adequate. They tell us $n_p|(p-1)^3$ and $n_p \equiv 1 \bmod p$, but it does not follow from this that n_p must be 1. For instance, $(p-1)^2$ satisfies these two conditions in place of n_p.

To show $n_p = 1$, we will prove $\mathrm{Heis}(\mathbf{Z}/(p)) \lhd U$. Projecting a matrix in U onto its 3 diagonal entries is a function from U to the 3-fold direct product $(\mathbf{Z}/(p))^\times \times (\mathbf{Z}/(p))^\times \times (\mathbf{Z}/(p))^\times$. This is a homomorphism with kernel $\mathrm{Heis}(\mathbf{Z}/(p))$, so $\mathrm{Heis}(\mathbf{Z}/(p)) \lhd U$. $\square$

Theorem 2.7. *Let $\mathbf{F}$ be a finite field and $q = \#\mathbf{F}$. For any prime p dividing $q-1$, the number of p-Sylow subgroups of* $\mathrm{Aff}(\mathbf{F})$ *is q.*

Proof. The group $\mathrm{Aff}(\mathbf{F})$ has size $q(q-1)$ and contains $H = \{(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}) : a \in \mathbf{F}^\times\}$, which has size $q-1$. Let p^r be the highest power of p dividing $q-1$. Let P be the p-Sylow subgroup of H (it's unique since H is abelian). Then P is a p-Sylow subgroup of $\mathrm{Aff}(\mathbf{F})$ too and the number of p-Sylow subgroups of $\mathrm{Aff}(\mathbf{F})$ is $[\#\,\mathrm{Aff}(\mathbf{F}) : \mathrm{N}(P)]$ by Sylow III*, where $\mathrm{N}(P)$ is the normalizer of P in $\mathrm{Aff}(\mathbf{F})$.

We will show $\mathrm{N}(P) = H$. Since H is abelian, $P \lhd H$, so $H \subset \mathrm{N}(P)$. To get the reverse inclusion, suppose $(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix})$ is in $\mathrm{N}(P)$. Pick a non-identity element of P, say $(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix})$. Then $(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix})(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix})(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix})^{-1} = (\begin{smallmatrix} a & y(1-a) \\ 0 & 1 \end{smallmatrix})$. For this to be in P at least requires $y(1-a) = 0$, so $y = 0$ since $a \neq 1$. Thus $\mathrm{N}(P) \subset H$.

The number of p-Sylow subgroups of $\mathrm{Aff}(\mathbf{F})$ is $[\mathrm{Aff}(\mathbf{F}) : H] = q(q-1)/q-1 = q$. $\square$

Remark 2.8. From the theory of finite fields, every finite field has prime-power size and for every prime power there is a field of that size. (Warning: a field of size 9 is not constructed as $\mathbf{Z}/(9)$, since that is not a field. Fields of non-prime size can't be constructed as quotient rings of $\mathbf{Z}$. Another method is needed.) Therefore Theorem 2.7 shows any prime power $\equiv 1 \bmod p$ occurs as the number of p-Sylow subgroups of a finite group. For example, $81 \equiv 1 \bmod 5$ and there are 81 different 5-Sylow subgroups of $\mathrm{Aff}(\mathbf{F}_{81})$, where $\mathbf{F}_{81}$ is a field of size 81.

It is an interesting question to ask if the congruence condition $n \equiv 1 \bmod p$ from Sylow III is the only constraint on p-Sylow counts: for $n \in \mathbf{Z}^+$ with $n \equiv 1 \bmod p$ is there a finite group in which the number of p-Sylow subgroups is n? The answer is affirmative when $n = 1$ using $\mathbf{Z}/(p)$, so we only consider $n > 1$. When $p = 2$ the answer is affirmative using dihedral groups: when $n > 1$ is odd a 2-Sylow subgroup of D_n has order 2 and the elements of order 2 are precisely the n reflections, so the number of 2-Sylow subgroups of D_n is n. What if $p \neq 2$? Remark 2.8 shows any prime power $n \equiv 1 \bmod p$ is the number of p-Sylow subgroups of some finite group (explicitly). But for $p \neq 2$ there are $n \equiv 1 \bmod p$ which do not arise as a p-Sylow count. For example, there is no finite group G in which $n_3(G) = 22$ or $n_5(G) = 21$ or $n_p(G) = 1 + 3p$ for prime $p \geq 7$. This is proved in [2].

3. Characterizing Cyclic Groups

Here is a nice application of Sylow I.

Theorem 3.1. *If a finite group has at most one subgroup of any size, then it is a cyclic group.*

The converse is of course true and we saw it earlier in the course.

Proof. Our argument has two steps: use Sylow I to reduce the theorem to the prime power case, and then settle the prime power case.

Step 1: Let G be a group with a unique subgroup of each size. In particular, for each prime p we obtain by Sylow I that G has one p-Sylow subgroup. Each Sylow subgroup is normal since $n_p = 1$. Then, for different primes p and q dividing $\#G$, the elements of the p-Sylow and q-Sylow subgroups commute with each other by Corollary 1.6.

Any subgroup of G has at most one subgroup of any size (otherwise G itself would have two subgroups of the same size). *Suppose* we knew the theorem for all groups with prime-power size. Then, for each prime p dividing $\#G$, the p-Sylow subgroup of G has to be cyclic. Choose a generator a_p of the p-Sylow subgroup of G. The order of a_p is the size of the p-Sylow subgroup of G. These a_p's commute as p varies, by the previous paragraph, and their orders are relatively prime, so the product of the a_p's has order equal to the product of the sizes of the Sylow subgroups of G. This product of sizes is $\#G$, so G is cyclic.

Step 2: We are now reduced to verifying our theorem for groups with prime-power size. The Sylow theorems will not be used further.

Let $\#G = p^k$ where p is prime, $k \geq 1$, and assume G has at most one subgroup of each size. To show G is cyclic, we argue by induction on k. If $k = 1$ then G has prime size so it is cyclic. We now suppose that $k \geq 2$ and the theorem is proved for all groups with p-power size less than p^k which have at most one subgroup of each size.

Since G is a nontrivial group with p-power size, it has a nontrivial center. Pick (by Cauchy) an element a of order p in the center of G. Then $\langle a \rangle$ is a subgroup of G with order p, so it is the unique such subgroup. Since *every* nontrivial subgroup of G contains a subgroup of size p by Cauchy, every nontrivial subgroup of G contains $\langle a \rangle$.

Since a lies in the center of G, $\langle a \rangle$ is a normal subgroup of G. We therefore can consider the group $G/\langle a \rangle$, whose size is p^{k-1}. Let's show $G/\langle a \rangle$ has at most one subgroup of any size. For any subgroup H of $G/\langle a \rangle$, let H' be the inverse image of H in G (all the elements of G which reduce to H). Then H' contains $\langle a \rangle$, has p times as many elements as H, and $H = H'/\langle a \rangle$. If K is a subgroup of $G/\langle a \rangle$ with the same size as H then $\#K' = \#H'$ (we define K' from K in the same way as H' is defined from H), so $H' = K'$ since G is assumed to have at most one subgroup of any size. Reducing back modulo $\langle a \rangle$, we get $H = H'/\langle a \rangle = K'/\langle a \rangle = K$ in $G/\langle a \rangle$.

By induction, $G/\langle a \rangle$ is a cyclic group:

$$G/\langle a \rangle = \langle \bar{b} \rangle.$$

Then every element of G has the form $b^i a^j$ for some i and j, and $b \neq e$ since $G/\langle a \rangle$ is nontrivial. Since $\langle b \rangle$ is a nontrivial subgroup of G, it must contain $\langle a \rangle$. Therefore $a \in \langle b \rangle$, so $b^i a^j$ is a power of b. This implies G is cyclic, which settles the theorem for groups of prime-power size. □

Remark 3.2. If every Sylow subgroup is cyclic, the group need not be cyclic. Try D_n with odd n. The finite groups whose Sylow subgroups are all cyclic can be classified. See [8,

p. 281]. If every Sylow subgroup is cyclic and there is just one p-Sylow subgroup for each prime p dividing $\#G$ then G is cyclic. This is the basic reasoning in the proof of Theorem 3.1.

Here is another application of Sylow I to prove a similar theorem.

Theorem 3.3. *Let G be a finite group such that, for each n dividing $\#G$, the equation $x^n = 1$ in G has at most n solutions. Then G is cyclic.*

Proof. We again argue in two steps: reduction to the prime power case using Sylow I and then the prime power case.

Step 1: Let p be a prime dividing $\#G$ and p^k be the largest power of p in $\#G$. Every $g \in G$ of p-power order in G has order dividing p^k (all orders divide $\#G$), so g is a solution to $x^{p^k} = 1$. Let P be a p-Sylow subgroup of G. It provides us with p^k solutions to this equation, so by assumption these are all the solutions. Therefore all elements of p-power order are in P, so P is the only p-Sylow subgroup.

The hypothesis on G passes to any of its subgroups, such as its Sylow subgroups. If we knew the theorem for groups of prime-power size then we get cyclicity of the Sylow subgroups, so G is cyclic by the same argument as in Step 1 of the proof of Theorem 3.1.

Step 2: We now verify the theorem for p-groups. The Sylow theorems are not going to be used. Let $\#G = p^k$, where $k \geq 2$. (The case $k = 1$ is trivial.) Assume $x^n = 1$ has at most n solutions in G whenever $n|p^k$. We want to show G is cyclic. If $N \lhd G$ and $\#(G/N) > p$ then G/N has a nontrivial normal subgroup of order p (such as a subgroup of order p in its center). Lifting this subgroup of G/N back to G gives a normal subgroup $H \lhd G$ with $N \subset H \subset G$ and $[H : N] = p$. We can repeat this with H in place of N, and so on, so a *maximal* proper normal subgroup of G has index p in G. Let M be such a subgroup, so $\#M = p^{k-1}$. The equation $x^{p^{k-1}} = 1$ has p^{k-1} solutions in M, so by hypothesis these are the only solutions to this equation in G. Therefore any element of $G - M$ does not have order dividing p^{k-1}, so its order must be p^k, which shows G is cyclic. □

4. Commutativity properties based on $\#G$

All groups of order p^2 are abelian. (See the handout on conjugation in a group.) Cauchy's theorem can be used to show all groups of order pq with primes $p < q$ and $q \not\equiv 1 \bmod p$ (*e.g.*, $pq = 15$) are abelian (and in fact cyclic). The Sylow theorems provide further tools to show all groups of a given size are abelian.

Theorem 4.1. *Any group of size 45 is abelian.*

Proof. Let G have size 45. In G, a 3-Sylow subgroup has size 9 and a 5-Sylow subgroup has size 5. Using Sylow III,

$$n_3|5, \quad n_3 \equiv 1 \bmod 3 \Longrightarrow n_3 = 1$$

and

$$n_5|9, \quad n_5 \equiv 1 \bmod 5 \Longrightarrow n_5 = 1.$$

Therefore G has normal 3-Sylow and 5-Sylow subgroups. Denote them by P and Q respectively, so $\#P = 9$ and $\#Q = 5$. Then P is abelian and Q is cyclic (thus abelian).

The set $PQ = \{ab : a \in P, b \in Q\}$ is a subgroup of G since P and Q are normal subgroups (we really only need one of them to be normal for PQ to be a subgroup). Since PQ contains P and Q as subgroups, Lagrange tells us $\#PQ$ is divisible by both 9 and 5. Therefore $45|\#PQ$, so $PQ = G$. Since P and Q are both abelian, we will know G is abelian once we show each element of P commutes with each element of Q. This commutativity is Corollary 1.6. □

Remark 4.2. The reader can check that the same argument shows any group of size p^2q with primes $p < q$ and $q \not\equiv 1 \bmod p$ is abelian. Examples include $99 = 2^2 \cdot 11$ and $175 = 5^2 \cdot 7$.

Theorem 4.3. *Let p and q be primes where $p < q$ and $q \not\equiv 1 \bmod p$. Then any group of size pq is cyclic.*

This was already proved in the handout on consequences of Cauchy's theorem. The proof we give here is in the same spirit, but it uses the Sylow theorems to handle more *efficiently* certain parts of the proof. Compare the two proofs.

Proof. Let $\#G = pq$, where $p < q$ and $q \not\equiv 1 \bmod p$. By Cauchy's theorem, G has an element a of order p and an element b of order q. Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

These subgroups have size p and q and are, respectively, p-Sylow and q-Sylow subgroups of G. Using the Sylow theorems, we will show P and Q are both normal subgroups of G. It then will follow from Corollary 1.6 that elements of P commute with elements of Q. Then, since a and b commute and they have relatively prime order, their product ab has order pq. As $\#G = pq$, G is cyclic.

By Sylow III, $n_p | q$ and $n_p \equiv 1 \bmod p$. The only choices are $n_p = 1$ or q. Since $q \not\equiv 1 \bmod p$ (by hypothesis) we must have $n_p = 1$, so P is the only p-Sylow subgroup and is thus normal in G.

By Sylow III, $n_q | p$ and $n_q \equiv 1 \bmod q$. The only choices are $n_q = 1$ or p. Since $1 < p < q$, the congruence condition on n_q implies $n_q = 1$. Therefore Q is the only q-Sylow subgroup and is thus normal in G. (Compare this to the proof in the handout on consequences of Cauchy's theorem that G has only one subgroup of size q.) □

5. Normalizers of Sylow subgroups

The normalizers of Sylow subgroups occur in Sylow III: the number of p-Sylow subgroups is the index of the normalizer of a p-Sylow subgroup. We record here some additional properties of Sylow normalizers.

Recall we write $\mathrm{Syl}_p(G)$ for the set of p-Sylow subgroups of G. It will be convenient sometimes to denote the normalizer of a subgroup $K \subset G$ as $\mathrm{N}_G(K)$ rather than as $\mathrm{N}(K)$ to stress the overlying group in which the normalizer is being computed.

Theorem 5.1. *Let $P \in \mathrm{Syl}_p(G)$. Then P is the unique p-Sylow subgroup of $\mathrm{N}(P)$ and $\mathrm{N}(P)$ is the largest subgroup of G with this property.*

Proof. Since $P \in \mathrm{Syl}_p(\mathrm{N}(P))$, Sylow II for $\mathrm{N}(P)$ says any p-Sylow subgroup of $\mathrm{N}(P)$ is gPg^{-1} for some $g \in \mathrm{N}(P)$. By the definition of $\mathrm{N}(P)$, $gPg^{-1} = P$. So P is the unique p-Sylow subgroup of $\mathrm{N}(P)$. (This kind of argument was used in the proof of Sylow III to show $n_p \equiv 1 \bmod p$.)

Now suppose $P \subset H \subset G$ and the only p-Sylow subgroup of H is P. For $h \in H$, hPh^{-1} is a p-Sylow subgroup of H, so $hPh^{-1} = P$. Thus $h \in \mathrm{N}(P)$, so $H \subset \mathrm{N}(P)$. □

Theorem 5.2. *Let $N \lhd G$ and $P \in \mathrm{Syl}_p(N)$.*

1. *[Frattini argument] If $N \lhd G$ and $P \in \mathrm{Syl}_p(N)$ then $G = N \cdot \mathrm{N}_G(P)$.*
2. *If $P \lhd N$ then $P \lhd G$.*

Note P is a Sylow subgroup of N, not necessarily of G.

Proof. Pick $g \in G$. Since $P \subset N$ and $N \lhd G$, $gPg^{-1} \subset N$. Then by Sylow II for the group N, there is an $n \in N$ such that $gPg^{-1} = nPn^{-1}$, so $n^{-1}gPg^{-1}n = P$. That means $n^{-1}g \in \mathrm{N}_G(P)$, so $g \in n\,\mathrm{N}_G(P)$. Thus $G = N \cdot \mathrm{N}_G(P)$.

If $P \lhd N$ then $N \subset \mathrm{N}_G(P)$, so $N \cdot \mathrm{N}_G(P) = \mathrm{N}_G(P)$. Thus $G = \mathrm{N}_G(P)$, so $P \lhd G$. □

The Frattini argument is very useful in finite group theory (*e.g.*, in the study of nilpotent groups). We will apply the second part of Theorem 5.2 several times in the next section.

Normality is not usually transitive: if $N_1 \lhd N_2$ and $N_2 \lhd G$, it need not follow that $N_1 \lhd G$. (This is illustrated by $\langle s \rangle \lhd \langle r^2, s \rangle \lhd D_4$.) Theorem 5.2 gives a setting where something like this is true: a normal *Sylow* subgroup of a normal subgroup is a normal subgroup.

Example 5.3. Let $G = \mathrm{GL}_2(\mathbf{Z}/(3))$ and $N = \mathrm{SL}_2(\mathbf{Z}/(3))$. There is a unique 2-Sylow subgroup of N, so it is normal in N, and thus normal in G. Thus the 2-Sylow subgroup of N lies in every 2-Sylow subgroup of G (but is not itself a 2-Sylow subgroup of G).

Corollary 5.4. *Let $P \in \mathrm{Syl}_p(G)$. If $\mathrm{N}_G(P) \subset H \subset G$ then $\mathrm{N}_G(H) = H$ and $[G : H] \equiv 1 \bmod p$. In particular, $\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P)$.*

Proof. Since P is a Sylow subgroup of G and $P \subset \mathrm{N}_G(P) \subset H$, P is a Sylow subgroup of H. Then, since $H \lhd \mathrm{N}_G(H)$, Theorem 5.2 (with $\mathrm{N}_G(H)$ in place of G) implies $\mathrm{N}_G(H) = H\,\mathrm{N}_{\mathrm{N}_G(H)}(P) \subset H\,\mathrm{N}_G(P) \subset H$. The reverse inclusion is obvious, so $\mathrm{N}_G(H) = H$.

Since $\mathrm{N}_G(P) \subset H$, the normalizer of P in H is also $\mathrm{N}_G(P)$ (that is, $\mathrm{N}_H(P) = \mathrm{N}_G(P)$). By Sylow III and III* applied to H and to G, we have

$$n_p(G) = [G : \mathrm{N}_G(P)] \equiv 1 \bmod p,$$
$$n_p(H) = [H : \mathrm{N}_H(P)] = [H : \mathrm{N}_G(H)] \equiv 1 \bmod p.$$

Thus their ratio, which is $[G : H]$, is $\equiv 1 \bmod p$. □

6. Non-trivial normal subgroups

The consequences of the Sylow theorems in this section are cases where the size of G forces G to have a nontrivial normal subgroup (usually, but not always, a normal Sylow subgroup). This topic is a popular source of exercises in algebra textbooks, in part because it can be used to determine all groups of various sizes up to isomorphism. For instance, near the end of this section we will find all the groups of size 105.

Theorem 6.1. *If $\#G = 20$ or 100 then G has a normal 5-Sylow subgroup.*

Proof. By Sylow III, $n_5 | 4$ and $n_5 \equiv 1 \bmod 5$. Thus $n_5 = 1$. □

This proof is identical to part of the proof of Theorem 2.2, which was concerned with a specific group of size 20.

Theorem 6.2. *If $\#G = pq$, where $p < q$ are distinct primes, then G has a normal q-Sylow subgroup.*

Proof. Read the proof of Theorem 4.3, where it is shown that $n_q = 1$. This part of the proof did not use the congruence condition $q \not\equiv 1 \bmod p$ from that theorem, so $n_q = 1$ whether or not that congruence condition holds. □

The following lemma does not involve the Sylow theorems, but will be used in conjunction with the Sylow theorems to prove more theorems about the existence of normal subgroups.

Lemma 6.3. *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 $k(p-1)$. $\square$

Theorem 6.4. *If $\#G = 12$ then G has a normal 2-Sylow or 3-Sylow subgroup.*

Proof. By Sylow III, $n_2|3$, 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 6.3 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 thus fills up the remaining elements. Therefore $n_2 = 1$.

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

In Theorem 6.4, it need not happen that both n_2 and n_3 equal 1 when $\#G = 12$. For example, A_4 has $n_2 = 1$ and $n_3 = 4$, while D_6 has $n_2 = 3$ and $n_3 = 1$.

Theorem 6.5. *If $\#G = 24$ then G has a normal subgroup of size 4 or 8.*

Proof. Let P be a 2-Sylow subgroup, so $\#P = 8$. Consider the left multiplication action $\ell\colon G \to \mathrm{Sym}(G/P) \cong S_3$. Set K to be the kernel of ℓ. Then

- $K \subset P$, so $\#K|8$,
- G/K embeds into S_3, so $[G : K]|6$. That is, $4|\#K$.

This tells us $\#K = 4$ or 8. Since K is the kernel of ℓ, $K \lhd G$. $\square$

Example 6.6. Let $G = S_4$. The number of 2-Sylow subgroups is 3, so S_4 does not have a normal subgroup of size 8 (Corollary 1.5). Theorem 6.5 then says S_4 must have a normal subgroup of size 4. Indeed, one is

$$\{(1), (12)(34), (13)(24), (14)(23)\}.$$

There are other subgroups of size 4, such as $\langle(1234)\rangle$, but they are not normal.

Example 6.7. Let $G = \mathrm{SL}_2(\mathbf{Z}/(3))$. This group has size 24 and a normal 2-Sylow subgroup.

Theorem 6.8. *If $\#G = 30$ then G has normal 3-Sylow and 5-Sylow subgroups: $n_3 = 1$ and $n_5 = 1$.*

Proof. Pick $g \in G$ of order 2. Since $\#G = 30$, left multiplication $\ell_g\colon G \to G$ is a product of 15 transpositions, so its sign is -1. Therefore the composite $\mathrm{sgn} \circ \ell\colon G \to \{\pm 1\}$ is onto, so the kernel is a (normal) subgroup of G with size 15. Call it N. Then N is cyclic (Theorem 4.3). Its 3-Sylow and 5-Sylow subgroups are normal in N (since N is abelian), so they are also normal in G by Theorem 5.2. $\square$

Remark 6.9. Up to isomorphism there are four groups of order 30: $\mathbf{Z}/(30)$, D_{15}, $\mathbf{Z}/(3) \times D_5$, and $\mathbf{Z}/(5) \times D_6$.

Theorem 6.10. *Every group of size 105 has normal 5-Sylow and 7-Sylow subgroups. In other words, every group of size 105 has unique subgroups of size 5 and 7.*

Proof. We will first prove $n_5 = 1$ or $n_7 = 1$. Then we will refine this to $n_5 = 1$ and $n_7 = 1$.

By Sylow III,

$$n_3|35, \ n_3 \equiv 1 \bmod 3 \Longrightarrow n_3 = 1 \text{ or } 7,$$

$$n_5|21,\ n_5 \equiv 1 \bmod 5 \Longrightarrow n_5 = 1 \text{ or } 21,$$
$$n_7|15,\ n_7 \equiv 1 \bmod 7 \Longrightarrow n_7 = 1 \text{ or } 15.$$

Could $n_5 > 1$ and $n_7 > 1$? If so, then $n_5 = 21$ and $n_7 = 15$. Using Lemma 6.3, the number of elements with order 5 is $21 \cdot 4 = 84$ and the number of elements with order 7 is $15 \cdot 6 = 90$. Since $84 + 90 > \#G$, we have a contradiction, so $n_5 = 1$ or $n_7 = 1$. In either case we will show G has a subgroup with order 35.

Suppose $n_5 = 1$ and let N_5 be the (normal) 5-Sylow subgroup of G. Then $N_5 \lhd G$, so G/N_5 is a group of size 21. The pullback (*i.e.*, inverse image) of the 7-Sylow of G/N_5 under the natural homomorphism $G \to G/N_5$ is a subgroup of G with size $7 \cdot 5 = 35$.

Now suppose $n_7 = 1$ and let N_7 be the (normal) 7-Sylow subgroup of G. The group G/N_7 has size 15. Under the natural map $G \to G/N_7$, the pullback of a 5-Sylow of G/N_7 is a subgroup of G with order $5 \cdot 7 = 35$.

We have proved, whether $n_5 = 1$ or $n_7 = 1$, that G has a subgroup of order 35. Such a subgroup has index $105/35 = 3$ in G. This is the smallest prime factor of G, so the subgroup is normal in G. (See the handout on group actions.) Denote it as N. Any group of size 35 is cyclic, by Theorem 4.3, so N is cyclic. In particular, any Sylow subgroup of N is a normal subgroup of N, so Theorem 5.2 tells us any Sylow subgroup of N is also a normal subgroup of G. A 5-Sylow or 7-Sylow of N is also a 5-Sylow or 7-Sylow of G, and therefore their normality in G implies $n_5 = 1$ and $n_7 = 1$. □

Theorem 6.11. *Any group of size* 105 *is isomorphic to* $\mathbf{Z}/(5) \times H$*, where* $\#H = 21$.

Proof. Let $\#G = 105$. By Theorem 6.10 we have $n_5 = n_7 = 1$. Let N_5 and N_7 denote the 5-Sylow and 7-Sylow subgroups of G. Let P be a 3-Sylow subgroup of G. Then the product set $H = PN_7$ is a subgroup of G with size 21. Since $N_5 \lhd G$, HN_5 is a subgroup of G with size 105, so $G = HN_5$. It remains to show $G \cong H \times N_5$, that is, elements of H commute with elements of N_5.

Consider the conjugation action of H on N_5 (this makes sense since $N_5 \lhd G$). It gives a homomorphism $H \to \mathrm{Aut}(N_5) \cong (\mathbf{Z}/(5))^\times$. Since H has size 21, this homomorphism is trivial, elements of H fix elements of N_5 by conjugation. Thus elements of H commute with elements of N_5. □

Corollary 6.12. *Up to isomorphism there are two groups of size* 105.

Proof. From the handout on applications of Cauchy's theorem, there are two groups of size 21 up to isomorphism. One is abelian (the cyclic group) and one is not. Using these for H in Theorem 6.11 gives two groups of size 105, one being abelian (in fact cyclic) and the other being non-abelian. □

Theorem 6.13. *If* $\#G = p^2q^2$*, where* $p < q$ *are distinct primes, then* G *has a normal* q*-Sylow subgroup unless* $\#G = 36$*, in which case* G *has either a normal* 2*-Sylow or* 3*-Sylow subgroup.*

The size 36 is a genuine exception: here $q = 3$ and $\mathbf{Z}/(3) \times A_4$ has $n_3 = 4$.

Proof. Without loss of generality, $p < q$. By the Sylow theorems, $n_q|p^2$ and $n_q \equiv 1 \bmod q$, so $n_q = 1$ or p^2. If $n_q = 1$ then the q-Sylow subgroup is normal. Now suppose $n_q = p^2$. Then $p^2 \equiv 1 \bmod q$, so $p \equiv \pm 1 \bmod q$. Since $p < q$, the congruence forces $p = q - 1$. As consecutive primes, $p = 2$ and $q = 3$, which shows for $\#G \neq 36$ that $n_q = 1$. (The reader who doesn't care too much about this theorem can skip the rest of the proof, which analyzes the remaining case $\#G = 36$.)

For the rest of the proof, let $\#G = 36$. Then $n_3 = 1$ or 4. We will show that if $n_3 = 4$ then $n_2 = 1$. Assume $n_3 = 4$ and $n_2 > 1$. Since $n_2 > 1$, G has no subgroup of size 18 (it would have index 2 and therefore be normal, so a 3-Sylow subgroup would be normal in G by Theorem 5.2, which contradicts $n_3 > 1$). Since $n_2 > 1$, G is non-abelian. Our goal is to get a contradiction. We will try to count elements of different orders in G and find the total comes out to more than 36 elements. That will be our contradiction.

Let Q be a 3-Sylow in G, so $[G : Q] = 4$. Left multiplication of G on G/Q gives a homomorphism $G \to \mathrm{Sym}(G/Q) \cong S_4$. Since $\#G > \#S_4$, the kernel K is nontrivial. Since $K \subset Q$, either $\#K = 3$ or $K = Q$. Since $Q \ntriangleleft G$, Q does not equal K, so $\#K = 3$.

Since $K \lhd G$, we can make G act on K by conjugations. This is a homomorphism $G \to \mathrm{Aut}(K) \cong \mathbf{Z}/(2)$. If this homomorphism is onto (that is, some element of G conjugates on K in a nontrivial way) then the kernel is a subgroup of G with size 18, which G does not have. So the conjugation action of G on K is trivial, which means every element of G commutes with the elements of K, so $K \subset Z(G)$. Then $3|\#Z(G)$, so the size of $Z(G)$ is one of the numbers in $\{3, 6, 9, 12, 18, 36\}$. Since G is non-abelian and a group is abelian when the quotient by its center is cyclic, $\#Z(G)$ can't be 12, 18, or 36. Since $n_3 > 1$ there is no normal subgroup of size 9, so $\#Z(G) \neq 9$. If $\#Z(G) = 6$ then the product set $Z(G)Q$ is a subgroup of size 18, a contradiction. So we must have $\#Z(G) = 3$, which means $Z(G) = K$.

Now we start counting elements with various orders. The center is a 3-subgroup of G, so by the conjugacy of 3-Sylow subgroups every 3-Sylow subgroup contains K. Any two different 3-Sylow subgroups have K as their intersection, so we can count the total number of elements of 3-power order: $\#K + n_3 \cdot (9 - 3) = 27$.

Let $g \in G$ have order 2. Then the product set $K\langle g\rangle$ is abelian of size 6, so $K\langle g\rangle$ is cyclic. A cyclic group has a unique element of order 2, which must be g. Therefore when g and g' are different elements of order 2 in G, the groups $K\langle g\rangle$ and $K\langle g'\rangle$ have K has their intersection. So each element of order 2 provides us with 2 new elements of order 6. Let n be the number of elements of order 2 in G, so there are at least $2n$ elements of order 6, giving at least $3n$ elements in total with order 2 or 6. Since we already found 27 elements with 3-power order (including the identity), $3n \leq 36 - 27$, or $n \leq 3$. We can get an inequality on n in the other direction: $n \geq 2$. Indeed, no element of order 2 lies in $Z(G) = K$, so some conjugate of an element of order 2 is a second element of order 2. So $n = 3$.

Since $\#\{g \in G : g^2 = e\}$ is even (by McKay's proof of Cauchy's theorem) and this number is $1+n$, n is odd, so $n = 3$. Therefore G has 3 elements of order 2, so at least $3n = 9$ elements of order 2 or 6. Adding this to 27 from before gives $9 + 27 = 36 = \#G$, so each element of G has 3-power order or order 2 or 6. In particular, the 2-Sylow subgroup of G is isomorphic to $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ (no elements of order 4 in G). Then different 2-Sylow subgroups meet at most in a group of order 2, which gives us 5 elements of order 2 from both subgroups. We saw before that there are only 3 elements of order 2. This is a contradiction. □

7. Sylow numbers of subgroups and quotient groups

How do the numbers $n_p(G)$ behave when we pass to subgroups and quotient groups? Do you feel that the numbers should not get larger?

Theorem 7.1. *Let H be a subgroup of G. For any $P \in \mathrm{Syl}_p(G)$, there is a conjugate gPg^{-1} such that $gPg^{-1} \cap H \in \mathrm{Syl}_p(H)$.*

Proof. We give two proofs. The first will use the Sylow theorems for H (and G). The second, somewhat longer, will not use the Sylow theorems for H.

For our first proof, note $P \cap H$ is a p-subgroup of H, so by the Sylow theorems for H there is a p-Sylow of H, say Q, containing $P \cap H$. As Q lies in a p-Sylow of G, $Q \subset gPg^{-1}$ for some $g \in G$. Therefore $Q \subset gPg^{-1} \cap H$. This intersection is a p-subgroup of H, so it has to equal Q.

For our second proof, note that for any $g \in G$ the intersection $gPg^{-1} \cap H$ is a p-subgroup of H. For it to be a p-Sylow subgroup of H (our goal) we need the index $[H : gPg^{-1} \cap H]$ not to be divisible by p. Consider the left multiplication action of H (not G!) on G/P. The set G/P has size $[G : P]$, which is not divisible by p. Therefore some left coset gP has an H-orbit with size not divisible by p. We are going to show the H-orbit of gP has size $[H : gPg^{-1} \cap H]$, so $gPg^{-1} \cap H$ is a p-Sylow subgroup of H.

To count the size of the H-orbit of gP we compute Stab_{gP}:

$$\begin{aligned} \mathrm{Stab}_{\{gP\}} &= \{h \in H : hgP = gP\} \\ &= \{h \in H : g^{-1}hg \in P\} \\ &= \{h : h \in gPg^{-1}\} \\ &= gPg^{-1} \cap H. \end{aligned}$$

By the orbit-stabilizer formula, the size of the H-orbit of gP is $[H : \mathrm{Stab}_{\{gP\}}] = [H : gPg^{-1} \cap H]$. $\square$

Example 7.2. Let $G = D_6 = \langle r, s\rangle$, of size 12. Let $H = \langle r^2, s\rangle$, of size 6. A 2-Sylow subgroup of H has size 2. One 2-Sylow subgroup of G is $P = \langle r^3, rs\rangle$. While $P \cap H$ is trivial, $rPr^{-1} \cap H = \{1, s\}$ is a 2-Sylow in H.

Example 7.3. For a prime p, let $G = \mathrm{GL}_2(\mathbf{Z}/(p))$ and $H = \{(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix})\}$. One p-Sylow subgroup of G is $P = \{(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix})\}$, which meets H trivially. However, since $(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix})(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})^{-1} = (\begin{smallmatrix} 1 & 0 \\ -x & 1 \end{smallmatrix})$, $(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})P(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})^{-1}$ is a p-Sylow subgroup of H.

Remark 7.4. Since the second proof of Theorem 7.1 did not use the Sylow theorems for H, it means that the existence of Sylow subgroups of a group implies the existence of Sylow subgroups of any subgroup. In particular, we can show a finite group has a p-Sylow subgroup by embedding it in a larger group where it might be easier to write down a p-Sylow subgroup.

For example, every finite group can be embedded in a symmetric group (Cayley's theorem). To be precise, the left multiplication action of G on G gives an embedding of G into $\mathrm{Sym}(G) \cong S_n$, where $n = \#G$. Therefore if one can construct, for any prime p, a p-Sylow subgroup of each symmetric group we obtain the existence of a p-Sylow subgroup of every finite group. Exercises 15 and 16 in [4, p. 84] give a construction of Sylow subgroups of symmetric groups using wreath products. A construction of a p-Sylow subgroup of the symmetric groups S_{p^k} actually suffices, since S_n embeds into S_{p^k} for $p^k \geq n$; the construction in this special case can be found in the discussion of the Sylow theorems in [3, pp. 95–97].

Corollary 7.5. *Let $N \lhd G$. For any p-Sylow P of G, $P \cap N$ is a p-Sylow of N and all p-Sylows of N arise in this way. In particular, $n_p(N) \leq n_p(G)$.*

Proof. By Theorem 7.1, there is a g such that $gPg^{-1} \cap N$ is a p-Sylow in N. Since N is a normal subgroup of G,

$$gPg^{-1} \cap N = gPg^{-1} \cap gNg^{-1} = g(P \cap N)g^{-1}.$$

Therefore $P \cap N$ is a p-Sylow subgroup of $g^{-1}Ng = N$.

Let Q be a p-Sylow subgroup of N. Pick a p-Sylow of G, say P, which contains Q. Then $Q \subset P \cap N$, and $P \cap N$ is a p-Sylow of N, so $Q = P \cap N$. □

There is an extension of Corollary 7.5 to certain non-normal subgroups. Suppose $H \lhd K \lhd G$ (perhaps H is not normal in G). If P is a Sylow subgroup of G then $P \cap K$ is a Sylow subgroup of K, so $(P \cap K) \cap H = P \cap H$ is a Sylow subgroup of H. It is left to the reader to show every Sylow subgroup of H arises in this way. This can be extended to any subgroup which is at the bottom of a chain of subgroups increasing up to G with each one normal in the next. Such subgroups are called subnormal. (For example, in D_4 the subgroup $\langle s \rangle$ satisfies $\langle s \rangle \lhd \langle s, r^2 \rangle \lhd D_4$, so $\langle s \rangle$ is subnormal in D_4 but not normal in D_4.) The condition on a subgroup $H \subset G$ that $P \cap H$ is a Sylow subgroup of H for any Sylow subgroup P of G is actually equivalent to H being subnormal. This was the Kegel–Wielandt conjecture, and its proof [6] depends on the classification of finite simple groups.

We now show the inequality at the very end of Corollary 7.5 is true for all subgroups of a finite group.

Theorem 7.6. *Let G be a finite group and H be a subgroup. Choose a prime p. Distinct p-Sylow subgroups of H do not lie in a common p-Sylow subgroup of G. In particular, $n_p(H) \leq n_p(G)$.*

Proof. Let Q and Q' be distinct p-Sylow subgroups of H. If they lie in a common p-Sylow subgroup of G then the group $\langle Q, Q' \rangle$ is a p-group and it lies in H. However its size is too large, since it is a p-subgroup of H which properly contains the p-Sylow subgroup Q.

If we associate to each p-Sylow subgroup of H a p-Sylow subgroup of G it lies inside of (there is no canonical way to do this if we have choices available) then this correspondence from $\mathrm{Syl}_p(H)$ to $\mathrm{Syl}_p(G)$ is one-to-one, so $n_p(H) \leq n_p(G)$. □

Theorem 7.7. *Let $N \lhd G$. For any p-Sylow P of G, PN/N is a p-Sylow of G/N and all p-Sylows of G/N arise in this way. In particular, $n_p(G/N) \leq n_p(G)$.*

Proof. First, we will show for every p-Sylow P of G that PN/N is a p-Sylow of G/N. The group PN/N is a p-group (either because every element has p-power order or because $PN/N \cong P/(P \cap N)$). Using the inclusions

$$G \supset PN \supset N, \quad G \supset PN \supset P,$$

the first one shows $[G/N : PN/N] = [G : PN]$ and the second one shows $[G : PN] \not\equiv 0 \bmod p$. Therefore PN/N is a p-Sylow of G/N.

Now we show every p-Sylow of G/N has the form PN/N for some p-Sylow P of G. Let $Q \in \mathrm{Syl}_p(G/N)$ and write $Q = H/N$ for some subgroup $H \subset G$ containing N. Then $[G : H] = [G/N : Q] \not\equiv 0 \bmod p$. Choose $P \in \mathrm{Syl}_p(H)$, so $P \in \mathrm{Syl}_p(G)$ too by the previous congruence. Then PN/N is a subgroup of Q. It is also a p-Sylow subgroup of G/N by the previous paragraph, so $Q = PN/N$. □

Corollary 7.5 and Theorem 7.7 tell us the maps $\mathrm{Syl}_p(G) \to \mathrm{Syl}_p(N)$ and $\mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G/N)$ given by $P \mapsto P \cap N$ and $P \mapsto PN/N$ are surjective. By comparison, although $\#\,\mathrm{Syl}_p(G) \geq \#\,\mathrm{Syl}_p(H)$ for any subgroup H, there are no natural maps between $\mathrm{Syl}_p(G)$ and $\mathrm{Syl}_p(H)$ when H is non-normal in G. (The function $\mathrm{Syl}_p(H) \to \mathrm{Syl}_p(G)$ in the proof of Theorem 7.6 is not natural in any way.)

The inequality $n_p(H) \leq n_p(G)$ can't generally be refined to divisibility. For example, $n_3(A_4) = 4$ and $n_3(A_5) = 10$. As an exercise, decide if $n_p(N) | n_p(G)$ or $n_p(G/N) | n_p(G)$ when $N \lhd G$.

Corollary 7.8. *If a group has a unique p-Sylow subgroup for some prime p then any subgroup and quotient group have a unique p-Sylow subgroup.*

Proof. By Theorems 7.6 and 7.7, an upper bound on the number of p-Sylow subgroups in any subgroup or quotient group of the group is 1, and there is at least one p-Sylow subgroup in any subgroup and quotient group of the group by the Sylow theorems. □

Theorem 7.7 gives another proof of Corollary 7.5: since PN/N is a p-Sylow subgroup of G/N, its size $[PN : N] = [P : P \cap N]$ is the highest power of p in $[G : N]$. Since $\#P$ is the highest power of p in $\#G$, we conclude that $\#(P \cap N)$ is the highest power of p in $\#N$, so $P \cap N$ is a p-Sylow subgroup of N.

The proof of the next theorem is a nice application of the preservation of the Sylow property when intersecting with a normal subgroup (Corollary 7.5).

Theorem 7.9. *Write $\#G = 2^n m$, where m is not divisible by 2. If G has a cyclic 2-Sylow subgroup then G has a normal subgroup of size m.*

Proof. Every 2-Sylow subgroup of G is cyclic (they are isomorphic to each other), so each 2-subgroup of G is cyclic since each one lies in a 2-Sylow subgroup.

We prove our theorem by induction on n.

First we show G has a subgroup of index 2 (necessarily normal). Consider the action of G on G by left multiplication. This is a homomorphism $\ell\colon G \to \mathrm{Sym}(G)$. There is an element of order 2^n in G. Left multiplication by this on G is a permutation consisting of m disjoint 2^n-cycles. Since m is odd, this permutation is odd. Thus the composite map $\mathrm{sgn} \circ \ell \to \{\pm 1\}$ is onto. Its kernel is a normal subgroup of index 2. Let N be this kernel, so $\#N = 2^{n-1}m$.

If $n = 1$ we are done; N is a normal subgroup of G with size m. (This part repeats the case when $2m = 30$ from the proof of Theorem 6.8.) Suppose $n \geq 2$. The intersection $H \cap N$ is a 2-Sylow subgroup of N (Corollary 7.5) so it must be cyclic. Therefore, by induction, N has a normal subgroup $M \lhd N$ of size m. We will show $M \lhd G$, which will end the proof. Note M is the unique subgroup of N with order m: if M' is another one then (since $M \lhd N$) the set $MM' \subset N$ is a subgroup with odd order (its size divides $\#M\#M'$) but its order exceeds m. That's too big. For any $g \in G$, $gMg^{-1} \subset gNg^{-1} = N$, so $gMg^{-1} = M$ by the uniqueness of M as a subgroup of N with its size. □

Remark 7.10. Theorem 7.9 is also true if $\#G$ is odd and 2 is replaced by the smallest prime factor of $\#G$. The proof in this case is different. See [9, p. 138].

Corollary 7.11. *If $\#G = 2m$ where m is odd then G contains a normal subgroup of size m and all elements of order 2 in G are conjugate to each other.*

Proof. A 2-Sylow subgroup of G has size 2, which must be cyclic. Therefore, by Theorem 7.9 (the base case $n = 1$), there is a normal subgroup of size m.

Since the 2-Sylow subgroups of G have size 2, any two elements of order 2 generate conjugate subgroups by Sylow II, and therefore the elements themselves are conjugate. □

Example 7.12. A group of size 70 has a normal subgroup of size 35.

Example 7.13. For odd m, all reflections in D_m are conjugate and there is a normal subgroup of size m. Of course this is something we already know by explicit calculation in dihedral groups, but Corollary 7.11 puts this situation into a larger context.

Appendix A. Simple groups of order 60

We call a group *simple* when it is nontrivial and its only normal subgroups are the trivial subgroup and the whole group. For example, a group of prime size is simple for the crude reason that it has no subgroups at all besides the trivial subgroup and the whole group. An abelian group of non-prime size is not simple, since it always has a proper nontrivial subgroup, which is necessarily normal. Thus any simple group other than a group of prime size is nonabelian.

Simple groups can be characterized in terms of group homomorphisms, as follows.

Theorem A.1. *A nontrivial group G is simple if and only if any nontrivial group homomorphism out of G is an embedding.*

Proof. Suppose G is simple. Let $f\colon G \to H$ be a homomorphism, with $f(g) \neq e$ for some g. Then the kernel of f is a proper normal subgroup of G. Since G is simple, its only proper normal subgroup is trivial, so the kernel of f is trivial, which means f is an embedding. Conversely, suppose all nontrivial homomorphisms out of G are embeddings. If $N \lhd G$ and $N \neq G$ then the reduction map $G \to G/N$ is a homomorphism with kernel N. The image is not just the identity, so by hypothesis this is an embedding. Therefore the kernel N is trivial, so G is simple. □

Theorem A.2. *The group A_5 is simple.*

Proof. We want to show the only normal subgroups of A_5 are (1) and A_5.

There are 5 conjugacy classes in A_5, with representatives and sizes as indicated in the following table.

Rep.	(1)	(12345)	(21345)	(12)(34)	(123)
Size	1	12	12	15	20

If A_5 has a normal subgroup N then N is a union of conjugacy classes – including (1) – whose total size divides 60. However, no sum of the above numbers which includes 1 is a factor of 60 except for 1 and 60. Therefore N is trivial or A_5. □

The proof of Theorem A.2 required knowledge of the conjugacy classes in A_5. We now prove A_5 is simple using much less information: its size and that it has more than one 5-Sylow subgroup. (*cf.* Theorem 2.1). The result will apply to any group with the same two properties. Our discussion is based on [1, pp. 145–146].

Theorem A.3. *If $\#G = 60$ and $n_5 > 1$ then G is a simple group.*

Proof. Assume G is not simple, so there is $N \lhd G$ with $1 < \#N < 60$. That means

$$\#N \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}.$$

We will get a contradiction. Our argument will use many of the previous consequences we drew from the Sylow theorems (to groups of size 12, 15, 20, and 30).

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 $n_5 > 1$ by hypothesis, $n_5 = 6$. Therefore N contains six different subgroups of size 5. Counting elements of N with orders 1 or 5, Lemma 6.3 says

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

Since $\#N$ is a proper factor of 60, $\#N = 30$. But then, by Theorem 6.8, N has only one 5-Sylow subgroup. This is a contradiction of $n_5 = 6$, so $\#N$ is not divisible by 5. This means

$$\#N \in \{2, 3, 4, 6, 12\}.$$

If $\#N$ equals 6 then Theorem 6.2 says N contains a normal 3-Sylow subgroup. If $\#N$ equals 12 then Theorem 6.4 says N contains a normal 2-Sylow or 3-Sylow subgroup. A normal Sylow subgroup of N is a normal subgroup of G by Theorem 5.2. Because such a normal subgroup of G has size 3 or 4, which is one of the possibilities already 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. By Theorem 4.3, a group of size 15 is cyclic and thus has a normal 5-Sylow subgroup. By Theorem 6.1, a group of size 20 has a normal 5-Sylow subgroup. By Theorem 6.8, 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 $\overline{P} \lhd \overline{G}$, $H \lhd G$. Since $H \neq G$, 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. $\square$

The next result shows that A_5 is the only *simple* group of size 60, up to isomorphism. (In total, there are 13 groups of size 60 up to isomorphism.) The proof will use Sylow III*.

Theorem A.4. *Every simple group of size* 60 *is isomorphic to* A_5*.*

Proof. Let G be a simple group of size 60. To prove G is isomorphic to A_5, we will make G act on a set of 5 objects and then show this action is given by the even permutations of the 5 objects.

We seek an action on cosets. *Suppose* G has a subgroup H with $[G : H] = 5$ (*i.e.*, $\#H = 12$), so the left multiplication action of G on the coset space G/H gives a homomorphism

$$\varphi\colon G \to \mathrm{Sym}(G/H) \cong S_5.$$

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. Thus the kernel of φ is 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

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

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 simple. (Remember, φ gives an isomorphism of G with $\varphi(G)$.) 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 left multiplication action of G on the coset space G/H gives an isomorphism of G with A_5. The rest of the proof is devoted to showing G has a subgroup with index 5.

Step 1: For any proper subgroup $H \subset G$, $[G : H] \geq 5$. Thus $\#H \leq 12$.

Let $t = [G : H]$. The left multiplication action of G on G/H gives a homomorphism $G \to \mathrm{Sym}(G/H) \cong S_t$. 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, the nontrivial Sylow subgroups are not normal, so n_2, n_3, and n_5 all exceed 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

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

If $n_2 = 5$ then Sylow III* says there is a subgroup of G with index 5 and we're done. What should we do now: show the only other possibility, that $n_2 = 15$, leads to a contradiction? Instead we will show that if $n_2 = 15$ then there is a second way to show G has a subgroup with index 5.

Assume $n_2 = 15$. By Lemma 6.3, 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 (and thus is abelian), so if $n_2 = 15$ then we have 15 different subgroups of size 4 squeezed into a 16-element subset of G. These 2-Sylow subgroups can't all pairwise intersect trivially (otherwise there would be $3 \cdot 15 = 45$ non-identity elements among them). Pick two different 2-Sylows, say P and Q, which intersect nontrivially. Let $I = P \cap Q$. Both P and Q are abelian (they have size 4), so I is normal in each. Therefore the normalizer of I in G contains both P and Q, so it has size properly divisible by 4. The normalizer of I is not all of G since G has no proper nontrivial normal subgroups. Since proper subgroups of G have size 1, 2, 3, 4, 6, or 12, the normalizer of I has size 12 and thus $[G : I] = 5$. $\square$

Since $n_2(A_5) = 5$, we know after the proof that the assumption $n_2 = 15$ in the last paragraph does not actually occur.

References

[1] D. Dummit and R. Foote, "Abstract Algebra," 3rd ed., Wiley, 2004.
[2] M. Hall, On the Number of Sylow Subgroups in a Finite Group, *J. Algebra* **7** (1961), 363–371.
[3] I. Herstein, "Topics in Algebra," 2nd ed., Wiley, 1975.
[4] N. Jacobson, "Basic Algebra I," 2nd ed., W. H. Freeman & Co., New York, 1985
[5] M. I. Kargapolov and Y. I. Merzlyakov, "Fundamentals of the theory of groups," Springer–Verlag, New York, 1979.
[6] P. B. Kleidman, A proof of the Kegel–Wielandt conjecture on subnormal subgroups, *Ann. of Math.* **133** (1991), 369–428.
[7] C. Leedham-Green, "The Structure of Groups of Prime Power Order," Oxford Univ. Press, Oxford, 2002.
[8] D. J. S. Robinson, "A Course in the Theory of Groups," Springer-Verlag, New York, 1982.
[9] W. R. Scott, "Group Theory," Dover, New York, 1987.