We claim p divides $|X|$. In forming a p-tuple in X, we may let $g_1, g_2, \cdots, g_{p-1}$ be any elements of G, and g_p is then uniquely determined as $(g_1 g_2 \cdots g_{p-1})^{-1}$. Thus $|X| = |G|^{p-1}$ and since p divides $|G|$, we see that p divides $|X|$.

Let σ be the cycle $(1, 2, 3, \cdots, p)$ in S_p. We let σ act on X by

$$\sigma(g_1, g_2, \cdots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \cdots, g_{\sigma(p)}) = (g_2, g_3, \cdots, g_p, g_1).$$

Note that $(g_2, g_3, \cdots, g_p, g_1) \in X$, for $g_1(g_2 g_3 \cdots g_p) = e$ implies that $g_1 = (g_2 g_3 \cdots g_p)^{-1}$, so $(g_2 g_3 \cdots g_p) g_1 = e$ also. Thus σ acts on X, and we consider the subgroup $\langle \sigma \rangle$ of S_p to act on X by iteration in the natural way.

Now $|\langle \sigma \rangle| = p$, so we may apply Theorem 36.1, and we know that $|X| \equiv |X_{\langle \sigma \rangle}| \pmod{p}$. Since p divides $|X|$, it must be that p divides $|X_{\langle \sigma \rangle}|$ also. Let us examine $X_{\langle \sigma \rangle}$. Now $(g_1, g_2, \cdots, g_p)$ is left fixed by σ, and hence by $\langle \sigma \rangle$, if and only if $g_1 = g_2 = \cdots = g_p$. We know at least one element in $X_{\langle \sigma \rangle}$, namely $(e, e, \cdots, e)$. Since p divides $|X_{\langle \sigma \rangle}|$, there must be at least p elements in $X_{\langle \sigma \rangle}$. Hence there exists some element $a \in G$, $a \neq e$, such that $(a, a, \cdots, a) \in X_{\langle \sigma \rangle}$ and hence $a^p = e$, so a has order p. Of course, $\langle a \rangle$ is a subgroup of G of order p. ◆

36.4 Corollary Let G be a finite group. Then G is a p-group if and only if $|G|$ is a power of p.

Proof We leave the proof of this corollary to Exercise 14. ◆

The Sylow Theorems

Let G be a group, and let $\mathscr{S}$ be the collection of all subgroups of G. We make $\mathscr{S}$ into a G-set by letting G act on $\mathscr{S}$ by conjugation. That is, if $H \in \mathscr{S}$ so $H \leq G$ and $g \in G$, then g acting on H yields the conjugate subgroup gHg^{-1}. (To avoid confusion, we will never write this action as gH.) Now $G_H = \{g \in G \mid gHg^{-1} = H\}$ is easily seen to be a subgroup of G (Exercise 11), and H is a normal subgroup of G_H. Since G_H consists of *all* elements of G that leave H invariant under conjugation, G_H is the largest subgroup of G having H as a normal subgroup.

36.5 Definition The subgroup G_H just discussed is the **normalizer of H in G** and will be denoted $N[H]$ from now on. ■

In the proof of the lemma that follows, we will use the fact that if H is a *finite* subgroup of a group G, then $g \in N[H]$ if $ghg^{-1} \in H$ for all $h \in H$. To see this, note that if $gh_1g^{-1} = gh_2g^{-1}$, then $h_1 = h_2$ by cancellation in the group G. Thus the conjugation map $i_g : H \to H$ given by $i_g(h) = ghg^{-1}$ is one to one. Because $|H|$ is finite, i_g must then map H *onto* H, so $gHg^{-1} = H$ and $g \in N[H]$.

36.6 Lemma Let H be a p-subgroup of a finite group G. Then

$$(N[H] : H) \equiv (G : H) \pmod{p}.$$

■ Historical Note

The Sylow theorems are due to the Norwegian mathematician Peter Ludvig Mejdell Sylow (1832–1918), who published them in a brief paper in 1872. Sylow stated the theorems in terms of permutation groups (since the abstract definition of a group had not yet been given). Georg Frobenius re-proved the theorems for abstract groups in 1887, even though he noted that in fact every group can be considered as a permutation group (Cayley's theorem [Theorem 8.16]). Sylow himself immediately applied the theorems to the question of solving algebraic equations and showed that any equation whose Galois group has order a power of a prime p is solvable by radicals.

Sylow spent most of his professional life as a high school teacher in Halden, Norway, and was only appointed to a position at Christiana University in 1898. He devoted eight years of his life to the project of editing the mathematical works of his countryman Niels Henrik Abel.

Proof Let $\mathscr{S}$ be the set of left cosets of H in G, and let H act on $\mathscr{S}$ by left translation, so that $h(xH) = (hx)H$. Then $\mathscr{S}$ becomes an H-set. Note that $|\mathscr{S}| = (G : H)$.

Let us determine $\mathscr{S}_H$, that is, those left cosets that are fixed under action by all elements of H. Now $xH = h(xH)$ if and only if $H = x^{-1}hxH$, or if and only if $x^{-1}hx \in H$. Thus $xH = h(xH)$ for all $h \in H$ if and only if $x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H$ for all $h \in H$, or if and only if $x^{-1} \in N[H]$ (see the comment before the lemma), or if and only if $x \in N[H]$. Thus the left cosets in $\mathscr{S}_H$ are those contained in $N[H]$. The number of such cosets is $(N[H] : H)$, so $|\mathscr{S}_H| = (N[H] : H)$.

Since H is a p-group, it has order a power of p by Corollary 36.4. Theorem 36.1 then tells us that $|\mathscr{S}| \equiv |\mathscr{S}_H| \pmod{p}$, that is, that $(G : H) \equiv (N[H] : H) \pmod{p}$. ◆

36.7 Corollary Let H be a p-subgroup of a finite group G. If p divides $(G : H)$, then $N[H] \neq H$.

Proof It follows from Lemma 36.6 that p divides $(N[H] : H)$, which must then be different from 1. Thus $H \neq N[H]$. ◆

We are now ready for the first of the Sylow theorems, which asserts the existence of prime-power subgroups of G for any prime power dividing $|G|$.

36.8 Theorem **(First Sylow Theorem)** Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and where p does not divide m. Then

1. G contains a subgroup of order p^i for each i where $1 \leq i \leq n$,
2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.

Proof

1. We know G contains a subgroup of order p by Cauchy's theorem (Theorem 36.3). We use an induction argument and show that the existence of a subgroup of order p^i for $i < n$ implies the existence of a subgroup of order p^{i+1}. Let H be a subgroup of order p^i. Since $i < n$, we see p divides $(G : H)$. By Lemma 36.6, we then know p divides $(N[H] : H)$. Since H is a normal

subgroup of $N[H]$, we can form $N[H]/H$, and we see that p divides $|N[H]/H|$. By Cauchy's theorem, the factor group $N[H]/H$ has a subgroup K which is of order p. If $\gamma : N[H] \to N[H]/H$ is the canonical homomorphism, then $\gamma^{-1}[K] = \{x \in N[H] \mid \gamma(x) \in K\}$ is a subgroup of $N[H]$ and hence of G. This subgroup contains H and is of order p^{i+1}.

2. We repeat the construction in part 1 and note that $H < \gamma^{-1}[K] \leq N[H]$ where $|\gamma^{-1}[K]| = p^{i+1}$. Since H is normal in $N[H]$, it is of course normal in the possibly smaller group $\gamma^{-1}[K]$. ◆

36.9 Definition A **Sylow p-subgroup** P of a group G is a maximal p-subgroup of G, that is, a p-subgroup contained in no larger p-subgroup. ■

Let G be a finite group, where $|G| = p^n m$ as in Theorem 36.8. The theorem shows that the Sylow p-subgroups of G are precisely those subgroups of order p^n. If P is a Sylow p-subgroup, every conjugate gPg^{-1} of P is also a Sylow p-subgroup. The second Sylow theorem states that every Sylow p-subgroup can be obtained from P in this fashion; that is, any two Sylow p-subgroups are conjugate.

36.10 Theorem **(Second Sylow Theorem)** Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G.

Proof Here we will let one of the subgroups act on left cosets of the other, and use Theorem 36.1. Let $\mathscr{S}$ be the collection of left cosets of P_1, and let P_2 act on $\mathscr{S}$ by $y(xP_1) = (yx)P_1$ for $y \in P_2$. Then $\mathscr{S}$ is a P_2-set. By Theorem 36.1, $|\mathscr{S}_{P_2}| \equiv |\mathscr{S}| \pmod{p}$, and $|\mathscr{S}| = (G : P_1)$ is not divisible by p, so $|\mathscr{S}_{P_2}| \neq 0$. Let $xP_1 \in \mathscr{S}_{P_2}$. Then $yxP_1 = xP_1$ for all $y \in P_2$, so $x^{-1}yxP_1 = P_1$ for all $y \in P_2$. Thus $x^{-1}yx \in P_1$ for all $y \in P_2$, so $x^{-1}P_2x \leq P_1$. Since $|P_1| = |P_2|$, we must have $P_1 = x^{-1}P_2x$, so P_1 and P_2 are indeed conjugate subgroups. ◆

The final Sylow theorem gives information on the number of Sylow p-subgroups. A few illustrations are given after the theorem, and many more are given in the next section.

36.11 Theorem **(Third Sylow Theorem)** If G is a finite group and p divides $|G|$, then the number of Sylow p-subgroups is congruent to 1 modulo p and divides $|G|$.

Proof Let P be one Sylow p-subgroup of G. Let $\mathscr{S}$ be the set of all Sylow p-subgroups and let P act on $\mathscr{S}$ by conjugation, so that $x \in P$ carries $T \in \mathscr{S}$ into xTx^{-1}. By Theorem 36.1, $|\mathscr{S}| \equiv |\mathscr{S}_P| \pmod{p}$. Let us find $\mathscr{S}_P$. If $T \in \mathscr{S}_P$, then $xTx^{-1} = T$ for all $x \in P$. Thus $P \leq N[T]$. Of course $T \leq N[T]$ also. Since P and T are both Sylow p-subgroups of G, they are also Sylow p-subgroups of $N[T]$. But then they are conjugate in $N[T]$ by Theorem 36.10. Since T is a normal subgroup of $N[T]$, it is its only conjugate in $N[T]$. Thus $T = P$. Then $\mathscr{S}_P = \{P\}$. Since $|\mathscr{S}| \equiv |\mathscr{S}_P| = 1 \pmod{p}$, we see the number of Sylow p-subgroups is congruent to 1 modulo p.

Now let G act on $\mathscr{S}$ by conjugation. Since all Sylow p-subgroups are conjugate, there is only one orbit in $\mathscr{S}$ under G. If $P \in \mathscr{S}$, then $|\mathscr{S}| = |\text{orbit of } P| = (G : G_P)$ by Theorem 16.16. (G_P is, in fact, the normalizer of P.) But $(G : G_P)$ is a divisor of $|G|$, so the number of Sylow p-subgroups divides $|G|$. ◆

Also, it follows from Theorem 24.1 that if x and y are in the same conjugacy class, then $|C(x)| = |C(y)|$ (see Exercise 53). If, for example, $\text{cl}(a) = \{a_1, a_2, \ldots, a_t\}$, then

$$|C(a_1)| + |C(a_2)| + \cdots + |C(a_t)| = t|C(a)| = |G{:}C(a)|\,|C(a)| = |G| = n.$$

So, by choosing one representative from each conjugacy class, say, x_1, $x_2, \ldots, x_m$, we have

$$|K| = \sum_{x \in G} |C(x)| = \sum_{i=1}^{m} |G{:}C(x_i)||C(x_i)| = m \cdot n.$$

Thus, the answer to our question is $mn/n^2 = m/n$, where m is the number of conjugacy classes in G and n is the number of elements of G.

Obviously, when G is non-Abelian, $\Pr(G)$ is less than 1. But how much less than 1? Clearly, the more conjugacy classes there are, the larger $\Pr(G)$ is. Consequently, $\Pr(G)$ is large when the sizes of the conjugacy classes are small. Noting that $|\text{cl}(a)| = 1$ if and only if $a \in Z(G)$, we obtain the maximum number of conjugacy classes when $|Z(G)|$ is as large as possible and all other conjugacy classes have exactly two elements in each. Since G is non-Abelian, it follows from Theorem 9.3 that $|G/Z(G)| \geq 4$ and, therefore, $|Z(G)| \leq |G|/4$. Thus, in the extreme case, we would have $|Z(G)| = |G|/4$, and the remaining $(3/4)|G|$ elements would be distributed in conjugacy classes with two elements each. So, in a non-Abelian group, the number of conjugacy classes is no more than $|G|/4 + (1/2)(3/4)|G|$, and $\Pr(G)$ is less than or equal to 5/8. The dihedral group D_4 is an example of a group that has probability equal to 5/8.

The Sylow Theorems

Now to the Sylow theorems. Recall that the converse of Lagrange's Theorem is false; that is, if G is a group of order m and n divides m, G need *not* have a subgroup of order n. Our next theorem is a partial converse of Lagrange's Theorem. It, as well as Theorem 24.2, was first proved by the Norwegian mathematician Ludwig Sylow (1832–1918). Sylow's Theorem and Lagrange's Theorem are the two most important results in finite group theory. The first gives a sufficient condition for the existence of subgroups, and the second gives a necessary condition.

Theorem 24.3 Existence of Subgroups of Prime-Power Order (Sylow's First Theorem, 1872)

Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

PROOF We proceed by induction on $|G|$. If $|G| = 1$, Theorem 24.3 is trivially true. Now assume that the statement is true for all groups of order less than $|G|$. If G has a proper subgroup H such that p^k divides $|H|$, then, by our inductive assumption, H has a subgroup of order p^k and we are done. Thus, we may henceforth assume that p^k does not divide the order of any proper subgroup of G. Next, consider the class equation for G in the form

$$|G| = |Z(G)| + \Sigma |G:C(a)|,$$

where we sum over a representative of each conjugacy class $\text{cl}(a)$, where $a \notin Z(G)$. Since p^k divides $|G| = |G:C(a)|\,|C(a)|$ and p^k does not divide $|C(a)|$, we know that p must divide $|G:C(a)|$ for all $a \notin Z(G)$. It then follows from the class equation that p divides $|Z(G)|$. The Fundamental Theorem of Finite Abelian Groups (Theorem 11.1), or Theorem 9.5, then guarantees that $Z(G)$ contains an element of order p, say x. Since x is in the center of G, $\langle x \rangle$ is a normal subgroup of G, and we may form the factor group $G/\langle x \rangle$. Now observe that p^{k-1} divides $|G/\langle x \rangle|$. Thus, by the induction hypothesis, $G/\langle x \rangle$ has a subgroup of order p^{k-1} and, by Exercise 49 in Chapter 10, this subgroup has the form $H/\langle x \rangle$, where H is a subgroup of G. Finally, note that $|H/\langle x \rangle| = p^{k-1}$ and $|\langle x \rangle| = p$ imply that $|H| = p^k$, and this completes the proof. ∎

Let's be sure we understand exactly what Sylow's First Theorem means. Say we have a group G of order $2^3 \cdot 3^2 \cdot 5^4 \cdot 7$. Then Sylow's First Theorem says that G must have at least one subgroup of each of the following orders: 2, 4, 8, 3, 9, 5, 25, 125, 625, and 7. On the other hand, Sylow's First Theorem tells us nothing about the possible existence of subgroups of order 6, 10, 15, 30, or any other divisor of $|G|$ that has two or more distinct prime factors. Because certain subgroups guaranteed by Sylow's First Theorem play a central role in the theory of finite groups, they are given a special name.

Definition Sylow *p*-Subgroup
Let G be a finite group and let p be a prime divisor of $|G|$. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a *Sylow p-subgroup of G*.

So, returning to our group G of order $2^3 \cdot 3^2 \cdot 5^4 \cdot 7$, we call any subgroup of order 8 a Sylow 2-subgroup of G, any subgroup of order 625 a Sylow 5-subgroup of G, and so on. Notice that a Sylow p-subgroup of G is a subgroup whose order is the largest power of p consistent with Lagrange's Theorem.

Since any subgroup of order p is cyclic, we have the following generalization of Theorem 9.5, first proved by Cauchy in 1845. His proof ran nine pages!

Corollary Cauchy's Theorem

Let G be a finite group and let p be a prime that divides the order of G. Then G has an element of order p.

Sylow's First Theorem is so fundamental to finite group theory that many different proofs of it have been published over the years [our proof is essentially the one given by Georg Frobenius (1849–1917) in 1895]. Likewise, there are scores of generalizations of Sylow's Theorem.

Observe that the corollary to the Fundamental Theorem of Finite Abelian Groups and Sylow's First Theorem show that the converse of Lagrange's Theorem is true for all finite Abelian groups and all finite groups of prime-power order.

There are two more Sylow theorems that are extremely valuable tools in finite group theory. But first we introduce a new term.

Definition Conjugate Subgroups
Let H and K be subgroups of a group G. We say that H and K are *conjugate* in G if there is an element g in G such that $H = gKg^{-1}$.

Recall from Chapter 7 that if G is a finite group of permutations on a set S and $i \in S$, then $\text{orb}_G(i) = \{\phi(i) \mid \phi \in G\}$ and $|\text{orb}_G(i)|$ divides $|G|$.

Theorem 24.4 Sylow's Second Theorem

If H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is contained in some Sylow p-subgroup of G.

PROOF Let K be a Sylow p-subgroup of G and let $C = \{K_1, K_2, \ldots, K_n\}$ with $K = K_1$ be the set of all conjugates of K in G. Since conjugation is an automorphism, each element of C is a Sylow p-subgroup of G. Let S_C denote the group of all permutations of C. For each $g \in G$, define $\phi_g: C \to C$ by $\phi_g(K_i) = gK_ig^{-1}$. It is easy to show that each $\phi_g \in S_C$.

Now define a mapping $T: G \to S_C$ by $T(g) = \phi_g$. Since $\phi_{gh}(K_i) = (gh)K_i(gh)^{-1} = g(hK_ih^{-1})g^{-1} = g\phi_h(K_i)g^{-1} = \phi_g(\phi_h(K_i)) = (\phi_g\phi_h)(K_i)$, we have $\phi_{gh} = \phi_g\phi_h$, and therefore T is a homomorphism from G to S_C.

Next consider $T(H)$, the image of H under T. Since $|H|$ is a power of p, so is $|T(H)|$ (see property 6 of Theorem 10.2). Thus, by the Orbit-Stabilizer Theorem (Theorem 7.3), for each i, $|\text{orb}_{T(H)}(K_i)|$ divides $|T(H)|$, so that $|\text{orb}_{T(H)}(K_i)|$ is a power of p. Now we ask: Under what condition does $|\text{orb}_{T(H)}(K_i)| = 1$? Well, $|\text{orb}_{T(H)}(K_i)| = 1$ means that $\phi_g(K_i) = gK_ig^{-1} = K_i$ for all $g \in H$; that is, $|\text{orb}_{T(H)}(K_i)| = 1$ if and only if $H \leq N(K_i)$. But the only elements of $N(K_i)$ that have orders that are powers of p are those of K_i (see Exercise 9). Thus, $|\text{orb}_{T(H)}(K_i)| = 1$ if and only if $H \leq K_i$.

So, to complete the proof, all we need to do is show that for some i, $|\text{orb}_{T(H)}(K_i)| = 1$. Analogous to Theorem 24.1, we have $|C| = |G{:}N(K)|$ (see Exercise 21). And since $|G{:}K| = |G{:}N(K)||N(K){:}K|$ is not divisible by p, neither is $|C|$. Because the orbits partition C, $|C|$ is the sum of powers of p. If no orbit has size 1, then p divides each summand and, therefore, p divides $|C|$, which is a contradiction. Thus, there is an orbit of size 1, and the proof is complete. ∎

Theorem 24.5 Sylow's Third Theorem

Let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G is equal to 1 modulo p and divides m. Furthermore, any two Sylow p-subgroups of G are conjugate.

PROOF Let K be any Sylow p-subgroup of G and let $C = \{K_1, K_2, \ldots, K_n\}$ with $K = K_1$ be the set of all conjugates of K in G. We first prove that $n \bmod p = 1$.

Let S_C and T be as in the proof of Theorem 24.4. This time we consider $T(K)$, the image of K under T. As before, we have $|\text{orb}_{T(K)}(K_i)|$ is a power of p for each i and $|\text{orb}_{T(K)}(K_i)| = 1$ if and only if $K \leq K_i$. Thus, $|\text{orb}_{T(K)}(K_1)| = 1$ and $|\text{orb}_{T(K)}(K_i)|$ is a power of p greater than 1 for all $i \neq 1$. Since the orbits partition C, it follows that, modulo p, $n = |C| = 1$.

Next we show that every Sylow p-subgroup of G belongs to C. To do this, suppose that H is a Sylow p-subgroup of G that is not in C. Let S_C and T be as in the proof of Theorem 24.4, and this time consider $T(H)$. As in the previous paragraph, $|C|$ is the sum of the orbits' sizes under the action of $T(H)$. However, no orbit has size 1, since H is not in C. Thus, $|C|$ is a sum of terms each divisible by p, so that, modulo p, $n = |C| = 0$. This contradiction proves that H belongs to C, and that n is the number of Sylow p-subgroups of G.

Finally, that n divides $|G|$ follows directly from the fact that $n = |G{:}N(K)|$ (see Exercise 21). ∎

order p or pq; in the latter case, c^q has order p by Theorem 7.8. In either case, G contains an element of order p. Therefore, the theorem is true for abelian groups of order n and, hence, by induction for all finite abelian groups. ◆

Proofs of the Sylow Theorems

We now have all the tools needed to prove the Sylow Theorems.

Proof of the First Sylow Theorem 8.13 The proof is by induction on the order of G. If $|G| = 1$, then p^0 is the only prime power that divides $|G|$, and G itself is a subgroup of order p^0. Suppose $|G| > 1$ and assume inductively that the theorem is true for all groups of order less than $|G|$. Combining the second and third forms of the class equation of G shows that

$$|G| = |Z(G)| + [G:C(a_1)] + [G:C(a_2)] + \cdots + [G:C(a_r)],$$

where for each i, $[G:C(a_i)] > 1$. Furthermore, $|Z(G)| \geq 1$ (since $e \in Z(G)$), and $|C(a_i)| < |G|$ (otherwise, $[G:C(a_i)] = 1$).

Suppose there is an index j such that p does *not* divide $[G:C(a_j)]$. Then by Theorem 1.8 p^k must divide $|C(a_j)|$ because p^k divides $|G|$ by hypothesis and $|G| = |C(a_j)| \cdot [G:C(a_j)]$ by Lagrange's Theorem. Since the subgroup $C(a_j)$ has order less than $|G|$, the induction hypothesis implies that $C(a_j)$, and, hence, G has a subgroup of order p^k.

On the other hand, if p divides $[G:C(a_i)]$ for every i, then since p divides $|G|$, p must also divide $|G| - [G:C(a_1)] - \cdots - [G:C(a_r)] = |Z(G)|$. Since $Z(G)$ is abelian, $Z(G)$ contains an element c of order p by Lemma 8.22. Let N be the cyclic subgroup generated by c. Then N has order p and is normal in G (Exercise 8). Consequently, the order of the quotient group G/N, namely $|G|/p$, is less than $|G|$ and divisible by p^{k-1}. By the induction hypothesis G/N has a subgroup T of order p^{k-1}. There is a subgroup H of G such that $N \subseteq H$ and $T = H/N$ by Theorem 7.44. Lagrange's Theorem shows that

$$|H| = |N| \cdot |H/N| = |N| \cdot |T| = pp^{k-1} = p^k.$$

So G has a subgroup of order p^k in this case, too. ◆

The basic tools needed to prove the last two Sylow Theorems are very similar to those used above, except that we will now deal with conjugate subgroups rather than conjugate elements. More precisely, let H be a fixed subgroup of a group G and let A and B be any subgroups of G. We say that A is ***H*-conjugate** to B if there exists an $x \in H$ such that

$$B = x^{-1}Ax = \{x^{-1}ax \mid a \in A\}.$$

In the special case when H is the group G itself, we simply say that A is **conjugate** to B.

THEOREM 8.23 *Let H be a subgroup of a group G. Then H-conjugacy is an equivalence relation on the set of all subgroups of G.*

Proof Copy the proof of Theorem 8.19, using subgroups A, B, C in place of elements a, b, c. ◆

Let A be a subgroup of a group G. The **normalizer** of A is the set $N(A)$ defined by

$$N(A) = \{g \in G \mid g^{-1}Ag = A\}.$$

THEOREM 8.24 *If A is a subgroup of a group G, then $N(A)$ is a subgroup of G and A is a normal subgroup of $N(A)$.*

Proof Exercise 7 shows that $A \subseteq N(A)$ and that $g \in N(A)$ if and only if $Ag = gA$. Using this fact, the proof of Theorem 8.20 can be readily adapted to prove that $N(A)$ is a subgroup. The definition of $N(A)$ shows that A is normal in $N(A)$. ◆

THEOREM 8.25 *Let H and A be subgroups of a finite group G. The number of distinct H-conjugates of A (that is, the number of elements in the equivalence class of A under H-conjugacy) is $[H:H \cap N(A)]$ and, therefore, divides $|H|$.*

Proof The proof of Theorem 8.21 carries over to the present situation if you replace G by H, a by A, and C by $H \cap N(A)$. ◆

LEMMA 8.26 *Let Q be a Sylow p-subgroup of a finite group G. If $x \in G$ has order a power of p and $x^{-1}Qx = Q$, then $x \in Q$.*

Proof Since Q is normal in $N(Q)$ by Theorem 8.24, the quotient group $N(Q)/Q$ is defined. By hypothesis, $x \in N(Q)$. Since $|x|$ is some power of p, the coset Qx in $N(Q)/Q$ also has order a power of p. Now Qx generates a cyclic subgroup T of $N(Q)/Q$ whose order is a power of p. By Theorem 7.44, $T = H/Q$, where H is a subgroup of G that contains Q. Since the orders of the groups Q and T are each powers of p and $|H| = |Q| \cdot |T|$ by Lagrange's Theorem, $|H|$ must be a power of p. But $Q \subseteq H$, and $|Q|$ is the largest power of p that divides $|G|$ by the definition of a Sylow p-subgroup. Therefore, $Q = H$, and, hence, $T = H/Q$ is the identity subgroup. So the generator Qx of T must be the identity coset Qe. The equality $Qx = Qe$ implies that $x \in Q$. ◆

Proof of the Second Sylow Theorem 8.15 Since K is a Sylow p-subgroup, K has order p^n, where $|G| = p^n m$ and $p \not| m$. Let $K = K_1, K_2, \ldots, K_t$ be the distinct conjugates of K in G. By Theorem 8.25 (with $H = G$ and $K = A$), $t = [G:N(K)]$. Note that p *does not divide* t [reason: $p^n m = |G| = |N(K)| \cdot [G:N(K)] =$

$|N(K)| \cdot t$ and p^n divides $|N(K)|$ because K is a subgroup of $N(K)$]. We must prove that the Sylow p-subgroup P is conjugate to K, that is, that P is one of the K_i. To do so we use the relation of P-conjugacy.

Since each K_i is a conjugate of K_1 and conjugacy is transitive, every conjugate of K_i in G is also a conjugate of K_1. In other words, every conjugate of K_i is some K_j. Consequently, the equivalence class of K_i under P-conjugacy contains only various K_j. So the set $S = \{K_1, K_2, \ldots, K_t\}$ of all conjugates of K is a union of distinct equivalence classes under P-conjugacy. The number of subgroups in each of these equivalence classes is a power of p because by Theorem 8.25 the number of subgroups that are P-conjugate to K_i is $[P:P \cap N(K_i)]$, which is a divisor of $|P| = p^n$ by Lagrange's Theorem. Therefore, t (the number of subgroups in the set S) is the sum of various powers of p (each being the number of subgroups in one of the distinct equivalence classes whose union is S). Since p doesn't divide t, at least one of these powers of p must be $p^0 = 1$. Thus some K_i is in an equivalence class by itself, meaning that $x^{-1}K_ix = K_i$ for every $x \in P$. Lemma 8.26 (with $Q = K_i$) implies that $x \in K_i$ for every such x, so that $P \subseteq K_i$. Since both P and K_i are Sylow p-subgroups, they have the same order. Hence, $P = K_i$. ◆

Proof of the Third Sylow Theorem 8.17 Let $S = \{K_1, \ldots, K_t\}$ be the set of all Sylow p-subgroups of G. By the Second Sylow Theorem, they are all conjugates of K_1. Let P be one of the K_i and consider the relation of P-conjugacy. The only P-conjugate of P is P itself by closure. The proof of the Second Sylow Theorem shows that the only equivalence class consisting of a single subgroup is the class consisting of P itself. The proof also shows that S is the union of distinct equivalence classes and that the number of subgroups in each class is a power of p. Just one of these classes contains P, so the number of subgroups in each of the others is a *positive* power of p. Hence, the number t of Sylow p-subgroups is the sum of 1 and various positive powers of p and, therefore, can be written in the form $1 + kp$ for some integer k. ◆

EXERCISES

NOTE: *Unless stated otherwise, G is a finite group and p is a prime.*

A. **1.** List the distinct conjugacy classes of the given group.

(a) D_4 **(b)** S_4 **(c)** A_4

2. If $a \in G$, then show by example that $C(a)$ may not be abelian. [*Hint:* If $a = (12)$ in S_5, then (34) and (345) are in $C(a)$.]

3. If H is a subgroup of G and $a \in H$, show by example that the conjugacy class of a in H may not be the same as the conjugacy class of a in G.

(c) Using this and the result for Problem 9(b), prove that in A_5 there is no normal subgroup N other than (e) and A_5.

11. Using Theorem 2.11.2 as a tool, prove that if $o(G) = p^n$, p a prime number, then G has a subgroup of order p^α for all $0 \leq \alpha \leq n$.

12. If $o(G) = p^n$, p a prime number, prove that there exist subgroups N_i, $i = 0, 1, \ldots, r$ (for some r) such that $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_r = (e)$ where N_i is a normal subgroup of N_{i-1} and where N_{i-1}/N_i is abelian.

13. If $o(G) = p^n$, p a prime number, and $H \neq G$ is a subgroup of G, show that there exists an $x \in G$, $x \notin H$ such that $x^{-1}Hx = H$.

14. Prove that any subgroup of order p^{n-1} in a group G of order p^n, p a prime number, is normal in G.

*15. If $o(G) = p^n$, p a prime number, and if $N \neq (e)$ is a normal subgroup of G, prove that $N \cap Z \neq (e)$, where Z is the center of G.

16. If G is a group, Z its center, and if G/Z is cyclic, prove that G must be abelian.

17. Prove that any group of order 15 is cyclic.

18. Prove that a group of order 28 has a normal subgroup of order 7.

19. Prove that if a group G of order 28 has a normal subgroup of order 4, then G is abelian.

2.12 Sylow's Theorem

Lagrange's theorem tells us that the order of a subgroup of a finite group is a divisor of the order of that group. The converse, however, is false. There are very few theorems which assert the existence of subgroups of prescribed order in arbitrary finite groups. The most basic, and widely used, is a classic theorem due to the Norwegian mathematician Sylow.

We present here three proofs of this result of Sylow. The first is a very elegant and elementary argument due to Wielandt. It appeared in the journal *Archiv der Matematik*, Vol. 10 (1959), pages 401–402. The basic elements in Wielandt's proof are number-theoretic and combinatorial. It has the advantage, aside from its elegance and simplicity, of producing the subgroup we are seeking. The second proof is based on an exploitation of induction in an interplay with the class equation. It is one of the standard classical proofs, and is a nice illustration of combining many of the ideals developed so far in the text to derive this very important cornerstone due to Sylow. The third proof is of a completely different philosophy. The basic idea there is to show that if a larger group than the one we are considering satisfies the conclusion of Sylow's theorem, then our group also must.

This forces us to prove Sylow's theorem for a special family of groups—the symmetric groups. By invoking Cayley's theorem (Theorem 2.9.1) we are then able to deduce Sylow's theorem for all finite groups. Apart from this strange approach—to prove something for a given group, first prove it for a much larger one—this third proof has its own advantages. Exploiting the ideas used, we easily derive the so-called second and third parts of Sylow's theorem.

One might wonder: why give three proofs of the same result when, clearly, one suffices? The answer is simple. Sylow's theorem is *that* important that it merits this multifront approach. Add to this the completely diverse nature of the three proofs and the nice application each gives of different things that we have learned, the justification for the whole affair becomes persuasive (at least to the author). Be that as it may, we state Sylow's theorem and get on with Wielandt's proof.

THEOREM 2.12.1 (SYLOW) *If p is a prime number and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.*

Before entering the first proof of the theorem we digress slightly to a brief number-theoretic and combinatorial discussion.

The number of ways of picking a subset of k elements from a set of n elements can easily be shown to be

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

If $n = p^\alpha m$ where p is a prime number, and if $p^r \mid m$ but $p^{r+1} \nmid m$, consider

$$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!}$$

$$= \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - i)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)\cdots(p^\alpha - i)\cdots(p^\alpha - p^\alpha + 1)}.$$

The question is, What power of p divides $\binom{p^\alpha m}{p^\alpha}$? Looking at this number, written out as we have written it out, one can see that except for the term m in the numerator, the power of p dividing $(p^\alpha m - i)$ is the same as that dividing $p^\alpha - i$, so all powers of p cancel out except the power which divides m. Thus

$$p^r \mid \binom{p^\alpha m}{p^\alpha} \quad \text{but} \quad p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}.$$

First Proof of the Theorem. Let $\mathscr{M}$ be the set of all subsets of G which have p^α elements. Thus $\mathscr{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements. Given $M_1, M_2 \in \mathscr{M}$ (M is a subset of G having p^α elements, and likewise so is M_2) define $M_1 \sim M_2$ if there exists an element $g \in G$ such that $M_1 = M_2 g$. It is immediate to verify that this defines an equivalence relation on $\mathscr{M}$. We claim that there is at least one equivalence class of elements in $\mathscr{M}$ such that the number of elements in this class is not a multiple of p^{r+1}, for if p^{r+1} is a divisor of the size of each equivalence class, then p^{r+1} would be a divisor of the number of elements in $\mathscr{M}$. Since $\mathscr{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements and $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$, this cannot be the case. Let $\{M_1, \ldots, M_n\}$ be such an equivalence class in $\mathscr{M}$ where $p^{r+1} \nmid n$. By our very definition of equivalence in $\mathscr{M}$, if $g \in G$, for each $i = 1, \ldots, n$, $M_i g = M_j$ for some j, $1 \leq j \leq n$. We let $H = \{g \in G \mid M_1 g = M_1\}$. Clearly H is a subgroup of G, for if $a, b \in H$, then $M_1 a = M_1$, $M_1 b = M_1$ whence $M_1 ab = (M_1 a)b = M_1 b = M_1$. We shall be vitally concerned with $o(H)$. We claim that $no(H) = o(G)$; we leave the proof to the reader, but suggest the argument used in the counting principle in Section 2.11. Now $no(H) = o(G) = p^\alpha m$; since $p^{r+1} \nmid n$ and $p^{\alpha+r} \mid p^\alpha m = no(H)$, it must follow that $p^\alpha \mid o(H)$, and so $o(H) \geq p^\alpha$. However, if $m_1 \in M_1$, then for all $h \in H$, $m_1 h \in M_1$. Thus M_1 has at least $o(H)$ distinct elements. However, M_1 was a subset of G containing p^α elements. Thus $p^\alpha \geq o(H)$. Combined with $o(H) \geq p^\alpha$ we have that $o(H) = p^\alpha$. *But then we have exhibited a subgroup of G having exactly p^α elements, namely H.* This proves the theorem; it actually has done more—it has constructed the required subgroup before our very eyes!

What is usually known as Sylow's theorem is a special case of Theorem 2.12.1, namely that

COROLLARY *If $p^m \mid o(G)$, $p^{m+1} \nmid o(G)$, then G has a subgroup of order p^m.*

A subgroup of G of order p^m, where $p^m \mid o(G)$ but $p^{m+1} \nmid o(G)$, is called a *p-Sylow subgroup of G*. The corollary above asserts that a finite group has p-Sylow subgroups for every prime p dividing its order. Of course the conjugate of a p-Sylow subgroup is a p-Sylow subgroup. In a short while we shall see how any two p-Sylow subgroups of G—for the same prime p—are related. We shall also get some information on how many p-Sylow subgroups there are in G for a given prime p. Before passing to this, we want to give two other proofs of Sylow's theorem.

We begin with a remark. As we observed just prior to the corollary, the corollary is a special case of the theorem. However, we claim that the

think of equivalent subsets, as different cosets of symmetry subgroup for subsets— thus all occur in multiples of m. If exactly m equivalent, then subsets are subgroup and its cosets. Each multiple of m must divide p^α thus equiv classes of size mp^α some j. $\binom{mp^\alpha}{p^\alpha}/mn$ not divisible by p, so at least one class is m elements and has subgroup of order p^α and its $m-1$ cosets.

3rd part is same as $1 \equiv \binom{mp^\alpha}{p^\alpha}/m \pmod p$ which must be true since iff

cancel m, all common p factors, then shift m denominator to left side, reduce showing identity.

theorem is easily derivable from the corollary. That is, if we know that G possesses a subgroup of order p^m, where $p^m \mid o(G)$ but $p^{m+1} \nmid o(G)$, then we know that G has a subgroup of order p^α for any α such that $p^\alpha \mid o(G)$. This follows from the result of Problem 11, Section 2.11. This result states that any group of order p^m, p a prime, has subgroups of order p^α for any $0 \leq \alpha \leq m$. Thus to prove Theorem 2.12.1—as we shall proceed to do, again, in two more ways—it is enough for us to prove the existence of p-Sylow subgroups of G, for every prime p dividing the order of G.

Second Proof of Sylow's Theorem. We prove, by induction on the order of the group G, that for every prime p dividing the order of G, G has a p-Sylow subgroup.

If the order of the group is 2, the only relevant prime is 2 and the group certainly has a subgroup of order 2, namely itself.

So we suppose the result to be correct for all groups of order less than $o(G)$. From this we want to show that the result is valid for G. Suppose, then, that $p^m \mid o(G)$, $p^{m+1} \nmid o(G)$, where p is a prime, $m \geq 1$. If $p^m \mid o(H)$ for any subgroup H of G, where $H \neq G$, then by the induction hypothesis, H would have a subgroup T of order p^m. However, since T is a subgroup of H, and H is a subgroup of G, T too is a subgroup of G. But then T would be the sought-after subgroup of order p^m.

We therefore may assume that $p^m \nmid o(H)$ for ~~any subgroup~~ H of G, where $H \neq G$. We restrict our attention to a limited set of such subgroups. Recall that if $a \in G$ then $N(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G; moreover, if $a \notin Z$, the center of G, then $N(a) \neq G$. Recall, too, that the class equation of G states that

$$o(G) = \sum \frac{o(G)}{o(N(a))},$$

where this sum runs over one element a from each conjugate class. We separate this sum into two pieces: those a which lie in Z, and those which don't. This gives

$$o(G) = z + \sum_{a \notin Z} \frac{o(G)}{o(N(a))},$$

where $z = o(Z)$. Now invoke the reduction we have made, namely, that $p^m \nmid o(H)$ for any subgroup $H \neq G$ of G, to those subgroups $N(a)$ for $a \notin Z$. Since in this case, $p^m \mid o(G)$ and $p^m \nmid o(N(a))$, we must have that

$$p \left| \frac{o(G)}{o(N(a))} \right.$$

Restating this result,

$$p \left| \frac{o(G)}{o(N(a))} \right.$$

for every $a \in G$ where $a \notin Z$. Look at the class equation with this information in hand. Since $p^m \mid o(G)$, we have that $p \mid o(G)$; also

logic doesn't seem screwed up if read "either $p^\alpha \mid N(a)$ some $a \in G$, or this construction gets subgroup"

$$p \left| \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \right..$$

Thus the class equation gives us that $p \mid z$. Since $p \mid z = o(Z)$, by Cauchy's theorem (Theorem 2.11.3), Z has an element $b \neq e$ of order p. Let $B = (b)$, the subgroup of G generated by b. B is of order p; moreover, *since* $b \in Z$, B *must be normal* in G. Hence we can form the quotient group $\bar{G} = G/B$. We look at $\bar{G}$. First of all, its order is $o(G)/o(B) = o(G)/p$, hence is certainly less than $o(G)$. Secondly, we have $p^{m-1} \mid o(\bar{G})$, but $p^m \nmid o(\bar{G})$. Thus, by the induction hypothesis, $\bar{G}$ has a subgroup $\bar{P}$ of order p^{m-1}. Let $P = \{x \in G \mid xB \in \bar{P}\}$; by Lemma 2.7.5, P is a subgroup of G. Moreover, $\bar{P} \approx P/B$ (Prove!); thus

$$p^{m-1} = o(\bar{P}) = \frac{o(P)}{o(B)} = \frac{o(P)}{p}.$$

This results in $o(P) = p^m$. Therefore P is the required p-Sylow subgroup of G. This completes the induction and so proves the theorem.

With this we have finished the second proof of Sylow's theorem. Note that this second proof can easily be adapted to prove that if $p^\alpha \mid o(G)$, then G has a subgroup of order p^α directly, without first passing to the existence of a p-Sylow subgroup. (This is Problem 1 of the problems at the end of this section.)

We now proceed to the third proof of Sylow's theorem.

Third Proof of Sylow's Theorem. Before going into the details of the proof proper, we outline its basic strategy. We will first show that the symmetric groups S_{p^r}, p a prime, all have p-Sylow subgroups. The next step will be to show that if G is contained in M and M has a p-Sylow subgroup, then G has a p-Sylow subgroup. Finally we will show, via Cayley's theorem, that we can use S_{p^k}, for large enough k, as our M. With this we will have all the pieces, and the theorem will drop out.

be prepared to give overview

In carrying out this program in detail, we will have to know how large a p-Sylow subgroup of S_{p^r} should be. This will necessitate knowing what power of p divides $(p^r)!$. This will be easy. To produce the p-Sylow subgroup of S_{p^r} will be harder. To carry out another vital step in this rough sketch, it will be necessary to introduce a new equivalence relation in groups, and the corresponding equivalence classes known as *double cosets*. This will have several payoffs, not only in pushing through the proof of Sylow's theorem, but also in getting us the second and third parts of the full Sylow theorem.

So we get down to our first task, that of finding what power of a prime p exactly divides $(p^k)!$. Actually, it is quite easy to do this for $n!$ for any integer n (see Problem 2). But, for our purposes, it will be clearer and will suffice to do it only for $(p^k)!$.

Let $n(k)$ be defined by $p^{n(k)} \mid (p^k)!$ but $p^{n(k)+1} \nmid (p^k)!$.

LEMMA 2.12.1 $n(k) = 1 + p + \cdots + p^{k-1}$.

Proof. If $k = 1$ then, since $p! = 1 \cdot 2 \cdots (p-1) \cdot p$, it is clear that $p \mid p!$ but $p^2 \nmid p!$. Hence $n(1) = 1$, as it should be.

What terms in the expansion of $(p^k)!$ can contribute to powers of p dividing $(p^k)!$? Clearly, only the multiples of p; that is, $p, 2p, \ldots, p^{k-1}p$. In other words $n(k)$ must be the power of p which divides $p(2p)(3p)\cdots(p^{k-1}p) = p^{p^{k-1}}(p^{k-1})!$. But then $n(k) = p^{k-1} + n(k-1)$. Similarly, $n(k-1) = n(k-2) + p^{k-2}$, and so on. Write these out as

$$\begin{aligned} n(k) - n(k-1) &= p^{k-1}, \\ n(k-1) - n(k-2) &= p^{k-2}, \\ &\vdots \\ n(2) - n(1) &= p, \\ n(1) &= 1. \end{aligned}$$

Adding these up, with the cross-cancellation that we get, we obtain $n(k) = 1 + p + p^2 + \cdots + p^{k-1}$. This is what was claimed in the lemma, so we are done.

We are now ready to show that S_{p^k} has a p-Sylow subgroup; that is, we shall show (in fact, produce) a subgroup of order $p^{n(k)}$ in S_{p^k}.

LEMMA 2.12.2 *S_{p^k} has a p-Sylow subgroup.*

Proof. We go by induction on k. If $k = 1$, then the element $(1\ 2\ \ldots\ p)$, in S_p is of order p, so generated a subgroup of order p. Since $n(1) = 1$, the result certainly checks out for $k = 1$.

Suppose that the result is correct for $k-1$; we want to show that it then must follow for k. Divide the integers $1, 2, \ldots, p^k$ into p clumps, each with p^{k-1} elements as follows:

$$\{1, 2, \ldots, p^{k-1}\}, \{p^{k-1}+1, p^{k-1}+2, \ldots, 2p^{k-1}\}, \ldots, \{(p-1)p^{k-1}+1, \ldots, p^k\}.$$

The permutation σ defined by $\sigma = (1, p^{k-1}+1, 2p^{k-1}+1, \ldots, (p-1)p^{k-1}+1)\cdots(j, p^{k-1}+j, 2p^{k-1}+j, \ldots, (p-1)p^{k-1}+1+j)\cdots(p^{k-1}, 2p^{k-1}, \ldots, (p-1)p^{k-1}, p^k)$ has the following properties:

1. $\sigma^p = e$.

2. If τ is a permutation that leaves all i fixed for $i > p^{k-1}$ (hence, affects only $1, 2, \ldots, p^{k-1}$), then $\sigma^{-1}\tau\sigma$ moves only elements in $\{p^{k-1}+1, p^{k-1}+2, \ldots, 2p^{k-1}\}$, and more generally, $\sigma^{-j}\tau\sigma^j$ moves only elements in $\{jp^{k-1}+1, jp^{k-1}+2, \ldots, (j+1)p^{k-1}\}$.

Consider $A = \{\tau \in S_{p^k} \mid \tau(i) = i \text{ if } i > p^{k-1}\}$. A is a subgroup of S_{p^k} and elements in A can carry out any permutation on $1, 2, \ldots, p^{k-1}$. From this it follows easily that $A \approx S_{p^{k-1}}$. By induction, A has a subgroup P_1 of order $p^{n(k-1)}$.

Let $T = P_1(\sigma^{-1}P_1\sigma)(\sigma^{-2}P_1\sigma^2)\cdots(\sigma^{-(p-1)}P_1\sigma^{p-1}) = P_1P_2\cdots P_{n-1}$, where $P_i = \sigma^{-i}P_1\sigma^i$. Each P_i is isomorphic to P_1 so has order $p^{n(k-1)}$. Also elements in distinct P_i's influence nonoverlapping sets of integers, *hence commute*. Thus T is a subgroup of S_{p^k}. What is its order? Since $P_i \cap P_j = (e)$ if $0 \leq i \neq j \leq p-1$, we see that $o(T) = o(P_1)^p = p^{pn(k-1)}$. We are not quite there yet. T is not the p-Sylow subgroup we seek!

Since $\sigma^p = e$ and $\sigma^{-i}P_1\sigma^i = P_i$ we have $\sigma^{-1}T\sigma = T$. Let $P = \{\sigma^j t \mid t \in T, 0 \leq j \leq p-1\}$. Since $\sigma \notin T$ and $\sigma^{-1}T\sigma = T$ we have two things: firstly, T is a subgroup of S_{p^k} and, furthermore, $o(P) = p \cdot o(T) = p \cdot p^{n(k-1)p} = p^{n(k-1)p+1}$. Now we are finally there! P is the sought-after p-Sylow subgroup of S_{p^k}.

Why? Well, what is its order? It is $p^{n(k-1)p+1}$. But $n(k-1) = 1 + p + \cdots + p^{k-2}$, hence $pn(k-1) + 1 = 1 + p + \cdots + p^{k-1} = n(k)$. Since now $o(P) = p^{n(k)}$, P is indeed a p-Sylow subgroup of S_{p^k}.

Note something about the proof. Not only does it prove the lemma, it actually allows us to construct the p-Sylow subgroup inductively. We follow the procedure of the proof to construct a 2-Sylow subgroup in S_4.

Divide 1, 2, 3, 4 into $\{1, 2\}$ and $\{3, 4\}$. Let $P_1 = ((1\,2))$ and $\sigma = (1\,3)(2\,4)$. Then $P_2 = \sigma^{-1}P_1\sigma = (3\,4)$. Our 2-Sylow subgroup is then the group generated by $(1\,3)(2\,4)$ and

$$T = P_1P_2 = \{(1\,2), (3\,4), (1\,2)(3\,4), e\}.$$

In order to carry out the program of the third proof that we outlined, we now introduce a new equivalence relation in groups (see Problem 39, Section 2.5).

DEFINITION Let G be a group, A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$.

We leave to the reader the verification—it is easy—of

LEMMA 2.12.3 *The relation defined above is an equivalence relation on G. The equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$.*

We call the set AxB a *double coset* of A, B in G.

If A, B are finite subgroups of G, how many elements are there in the double coset AxB? To begin with, the mapping $T:AxB \to AxBx^{-1}$ given by $(axb)T = axbx^{-1}$ is one-to-one and onto (verify). Thus $o(AxB) = o(AxBx^{-1})$. Since xBx^{-1} is a subgroup of G, of order $o(B)$, by Theorem 2.5.1,

$$o(AxB) = o(AxBx^{-1}) = \frac{o(A)o(xBx^{-1})}{o(A \cap xBx^{-1})} = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

We summarize this in

LEMMA 2.12.4 *If A, B are finite subgroups of G then*

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

We now come to the gut step in this third proof of Sylow's theorem.

LEMMA 2.12.5 *Let G be a finite group and suppose that G is a subgroup of the finite group M. Suppose further that M has a p-Sylow subgroup Q. Then G has a p-Sylow subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in M$.*

Proof. Before starting the details of the proof, we translate the hypotheses somewhat. Suppose that $p^m \mid o(M)$, $p^{m+1} \nmid o(M)$, Q is a subgroup of M of order p^m. Let $o(G) = p^n t$ where $p \nmid t$. We want to produce a subgroup P in G of order p^n.

Consider the double coset decomposition of M given by G and Q; $M = \bigcup GxQ$. By Lemma 2.12.4,

$$o(GxQ) = \frac{o(G)o(Q)}{o(G \cap xQx^{-1})} = \frac{p^n t p^m}{o(G \cap xQx^{-1})}.$$

Since $G \cap xQx^{-1}$ is a subgroup of xQx^{-1}, its order is p^{m_x}. We claim that $m_x = n$ for some $x \in M$. If not, then

$$o(GxQ) = \frac{p^n t p^m}{p^{m_x}} = t p^{m+n-m_x},$$

so is divisible by p^{m+1}. Now, since $M = \bigcup GxQ$, and this is disjoint union, $o(M) = \sum o(GxQ)$, the sum running over one element from each double coset. But $p^{m+1} \mid o(GxQ)$; hence $p^{m+1} \mid o(M)$. This contradicts $p^{m+1} \nmid o(M)$. Thus $m_x = n$ for some $x \in M$. But then $o(G \cap xQx^{-1}) = p^n$. Since $G \cap xQx^{-1} = P$ is a subgroup of G and has order p^n, the lemma is proved.

We now can easily prove Sylow's theorem. By Cayley's theorem (Theorem 2.9.1) we can isomorphically embed our finite group G in S_n, the symmetric group of degree n. Pick k so that $n < p^k$; then we can isomorphically embed S_n in S_{p^k} (by acting on $1, 2, \ldots, n$ only in the set

$1, 2, \ldots, n, \ldots, p^k$), hence G is isomorphically embedded in S_{p^k}. By Lemma 2.12.2, S_{p^k} has a p-Sylow subgroup. Hence, by Lemma 2.12.5, G must have a p-Sylow subgroup. This finishes the third proof of Sylow's theorem.

This third proof has given us quite a bit more. From it we have the machinery to get the other parts of Sylow's theorem.

THEOREM 2.12.2 (SECOND PART OF SYLOW'S THEOREM) *If G is a finite group, p a prime and $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$, then any two subgroups of G of order p^n are conjugate.*

Proof. Let A, B be subgroups of G, each of order p^n. We want to show that $A = gBg^{-1}$ for some $g \in G$.

Decompose G into double cosets of A and B; $G = \bigcup AxB$. Now, by Lemma 2.12.4,

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

If $A \neq xBx^{-1}$ for every $x \in G$ then $o(A \cap xBx^{-1}) = p^m$ where $m < n$. Thus

$$o(AxB) = \frac{o(A)o(B)}{p^m} = \frac{p^{2n}}{p^m} = p^{2n-m}$$

and $2n - m \geq n + 1$. Since $p^{n+1} \mid o(AxB)$ for every x and since $o(G) = \sum o(AxB)$, we would get the contradiction $p^{n+1} \mid o(G)$. Thus $A = gBg^{-1}$ for some $g \in G$. This is the assertion of the theorem.

Knowing that for a given prime p all p-Sylow subgroups of G are conjugate allows us to count up precisely how many such p-Sylow subgroups there are in G. The argument is exactly as that given in proving Theorem 2.11.1. In some earlier problems (see, in particular, Problem 16, Section 2.5) we discussed the normalizer $N(H)$, of a subgroup, defined by $N(H) = \{x \in G \mid xHx^{-1} = H\}$. Then, as in the proof of Theorem 2.11.1, we have that *the number of distinct conjugates, xHx^{-1}, of H in G is the index of $N(H)$ in G.* Since all p-Sylow subgroups are conjugate we have

LEMMA 2.12.6 *The number of p-Sylow subgroups in G equals $o(G)/o(N(P))$, where P is any p-Sylow subgroup of G. In particular, this number is a divisor of $o(G)$.*

However, much more can be said about the number of p-Sylow subgroups there are, for a given prime p, in G. We go into this now. The technique will involve double cosets again.

THEOREM 2.12.3 (THIRD PART OF SYLOW'S THEOREM) *The number of p-Sylow subgroups in G, for a given prime, is of the form $1 + kp$.*

Proof. Let P be a p-Sylow subgroup of G. We decompose G into double cosets of P and P. Thus $G = \bigcup PxP$. We now ask: How many elements are there in PxP? By Lemma 2.12.4 we know the answer:

$$o(PxP) = \frac{o(P)^2}{o(P \cap xPx^{-1})}.$$

Thus, if $P \cap xPx^{-1} \neq P$ then $p^{n+1} \mid o(PxP)$, where $p^n = o(P)$. Paraphrasing this: if $x \notin N(P)$ then $p^{n+1} \mid o(PxP)$. Also, if $x \in N(P)$, then $PxP = P(Px) = P^2x = Px$, so $o(PxP) = p^n$ in this case.

Now

$$o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP),$$

where each sum runs over one element from each double coset. However, if $x \in N(P)$, since $PxP = Px$, the first sum is merely $\sum_{x \in N(P)} o(Px)$ over the *distinct cosets* of P in $N(P)$. Thus this first sum is just $o(N(P))$. What about the second sum? We saw that each of its constituent terms is divisible by p^{n+1}, hence

$$p^{n+1} \Big| \sum_{x \notin N(P)} o(PxP).$$

We can thus write this second sum as

$$\sum_{x \notin N(P)} o(PxP) = p^{n+1}u.$$

Therefore $o(G) = o(N(P)) + p^{n+1}u$, so

$$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}u}{o(N(P))}.$$

Now $o(N(P)) \mid o(G)$ since $N(P)$ is a subgroup of G, hence $p^{n+1}u/o(N(P))$ is an integer. Also, since $p^{n+1} \nmid o(G)$, p^{n+1} can't divide $o(N(P))$. But then $p^{n+1}u/o(N(P))$ *must be divisible by* p, so we can write $p^{n+1}u/o(N(P))$ as kp, where k is an integer. Feeding this information back into our equation above, we have

$$\frac{o(G)}{o(N(P))} = 1 + kp.$$

Recalling that $o(G)/o(N(P))$ is the number of p-Sylow subgroups in G, we have the theorem.

In Problems 20–24 in the Supplementary Problems at the end of this chapter, there is outlined another approach to proving the second and third parts of Sylow's theorem.

We close this section by demonstrating how the various parts of Sylow's theorem can be used to gain a great deal of information about finite groups.

Let G be a group of order $11^2 \cdot 13^2$. We want to determine how many 11-Sylow subgroups and how many 13-Sylow subgroups there are in G. The number of 11-Sylow subgroups, by Theorem 2.12.13, is of the form $1 + 11k$. By Lemma 2.12.5, this must divide $11^2 \cdot 13^2$; being prime to 11, it must divide 13^2. Can 13^2 have a factor of the form $1 + 11k$? Clearly no, other than 1 itself. Thus $1 + 11k = 1$, and so there must be only one 11-Sylow subgroup in G. Since all 11-Sylow subgroups are conjugate (Theorem 2.12.2) we conclude that the 11-Sylow subgroup is *normal* in G.

What about the 13-Sylow subgroups? Their number is of the form $1 + 13k$ and must divide $11^2 \cdot 13^2$, hence must divide 11^2. Here, too, we conclude that there can be only one 13-Sylow subgroup in G, and it must be normal.

We now know that G has a normal subgroup A of order 11^2 and a normal subgroup B of order 13^2. By the corollary to Theorem 2.11.2, any group of order p^2 is abelian; hence A and B are both abelian. Since $A \cap B = (e)$, we easily get $AB = G$. Finally, if $a \in A$, $b \in B$, then $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in A$ since A is normal, and $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B$ since B is normal. Thus $aba^{-1}b^{-1} \in A \cap B = (e)$. This gives us $aba^{-1}b^{-1} = e$, and so $ab = ba$ for $a \in A$, $b \in B$. This, together with $AB = G$, A, B abelian, allows us to conclude that G *is abelian*. Hence any group of order $11^2 \cdot 13^2$ must be abelian.

We give one other illustration of the use of the various parts of Sylow's theorem. Let G be a group of order 72; $o(G) = 2^3 3^2$. How many 3-Sylow subgroups can there be in G? If this number is t, then, according to Theorem 2.12.3, $t = 1 + 3k$. According to Lemma 2.12.5, $t \mid 72$, and since t is prime to 3, we must have $t \mid 8$. The only factors of 8 of the form $1 + 3k$ are 1 and 4; hence $t = 1$ or $t = 4$ are the only possibilities. In other words G has either one 3-Sylow subgroup or 4 such.

If G has only one 3-Sylow subgroup, since all 3-Sylow subgroups are conjugate, this 3-Sylow subgroup must be normal in G. In this case G would certainly contain a nontrivial normal subgroup. On the other hand if the number of 3-Sylow subgroups of G is 4, by Lemma 2.12.5 the index of N in G is 4, where N is the normalizer of a 3-Sylow subgroup. But $72 \nmid 4! = (i(N))!$. By Lemma 2.9.1 N must contain a nontrivial normal subgroup of G (of order at least 3). Thus here again we can conclude that G contains a nontrivial normal subgroup. The upshot of the discussion is that any group of order 72 must have a nontrivial normal subgroup, hence cannot be simple.

Problems

1. Adapt the second proof given of Sylow's theorem to prove directly that if p is a prime and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.