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 $|G|$.

17.4 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 14.20). 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 17.2, 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 $\gamma^{-1}[K]$. ◆

17.5 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 17.4. 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.

17.6 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 14.19. Let $\mathscr{L}$ be the collection of left cosets of P_1, and let P_2 act on $\mathscr{L}$ by $y(xP_1) = (yx)P_1$ for $y \in P_2$. Then $\mathscr{L}$ is a P_2-set. By Theorem 14.19, $|\mathscr{L}_{P_2}| \equiv |\mathscr{L}| \pmod p$, and $|\mathscr{L}| = (G : P_1)$ is not divisible by p, so $|\mathscr{L}_{P_2}| \neq 0$. Let $xP_1 \in \mathscr{L}_{P_2}$. 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.

17.7 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 14.19, $|\mathscr{S}| \equiv |\mathscr{S}_P| \pmod p$. 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 17.6. 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 14.17. (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 $|G|$. ◆

Theorem 17.7 is really a bit better than it sounds. Let $|G| = p^n m$ where the prime number p does not divide m and suppose that G contains k Sylow p-subgroups. Then Theorem 17.7 says that k is equivalent to 1 modulo p and k divides $|G|$. Since $\gcd(k, p) = 1$, k must divide m.

Applications of the Sylow Theorems

17.8 Example The Sylow 2-subgroups of D_3 have order 2. Three Sylow 2-subgroups are

$$\{\iota, \mu\}, \quad \{\iota, \mu\rho\}, \quad \{\iota, \mu\rho^2\}$$

Notice that Theorem 17.7 says that the number k of Sylow 2-subgroups must be odd and k must divide 6. However, by the observation above, k must divide 3. So in fact, the three subgroups listed are all three of the subgroups of D_3 having order 2. ▲

17.9 Lemma Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$. ◆

Proof We start by showing that $hk = kh$ for $k \in K$ and $h \in H$. Consider the commutator $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Since H and K are normal subgroups of G, the two groupings with parentheses show that $hkh^{-1}k^{-1}$ is in both K and H. Since $K \cap H = \{e\}$, we see that $hkh^{-1}k^{-1} = e$, so $hk = kh$.

Let $\phi : H \times K \to G$ be defined by $\phi(h, k) = hk$. Then

$$\begin{aligned}\phi((h,k)(h',k')) &= \phi(hh', kk') = hh'kk' \\ &= hkh'k' = \phi(h,k)\phi(h',k'),\end{aligned}$$

so ϕ is a homomorphism.

If $\phi(h, k) = e$, then $hk = e$, so $h = k^{-1}$, and both h and k are in $H \cap K$. Thus $h = k = e$, so $\text{Ker}(\phi) = \{(e, e)\}$ and ϕ is one-to-one.

By Lemma 16.4, we know that $HK = H \vee K$, and $H \vee K = G$ by hypothesis. Thus ϕ is onto G, and $H \times K \simeq G$. ◆

We turn now to a discussion of whether there exist simple groups of certain orders. We have seen that every group of prime order is simple. We also asserted that A_n is simple for $n \geq 5$ and that A_5 is the smallest simple group that is not of prime order. There was a famous conjecture of Burnside that every finite simple group of nonprime order must be of even order. It was a triumph when this was proved by Thompson and Feit [21].

17.10 Theorem If p and q are distinct primes with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence G is not simple. If q is not congruent to 1 modulo p, then G is abelian and cyclic.

Proof Theorems 17.4 and 17.7 tell us that G has a Sylow q-subgroup and that the number of such subgroups is congruent to 1 modulo q and divides pq, and therefore must divide p. Since $p < q$, the only possibility is the number 1. Thus there is only one Sylow

q-subgroup Q of G. This group Q must be normal in G, for under an inner automorphism it would be carried into a group of the same order, hence itself. Thus G is not simple.

Likewise, there is a Sylow p-subgroup P of G, and the number of these divides pq and is congruent to 1 modulo p. This number must be either 1 or q. If q is not congruent to 1 modulo p, then the number must be 1 and P is normal in G. Let us assume that $q \not\equiv 1 \pmod{p}$. Since every element in Q other than e is of order q and every element in P other than e is of order p, we have $Q \cap P = \{e\}$. Also $Q \vee P$ must be a subgroup of G properly containing Q and of order dividing pq. Hence $Q \vee P = G$ and by Lemma 17.9 is isomorphic to $Q \times P$ or $\mathbb{Z}_q \times \mathbb{Z}_p$. Thus G is abelian and cyclic. ◆

17.11 Example Recall that if p is a prime number, then up to isomorphism there is only one group of order p and it is cyclic. Theorem 17.10 shows that there are many nonprime numbers n such that every group of order n is cyclic. Since 5 is not equivalent to 1 modulo 3, by Theorem 17.10, every group of order 15 is cyclic. Exercise 33 shows that 15 is the smallest composite number with this property. ▲

We need another lemma for some of the counting arguments that follow.

17.12 Lemma If H and K are finite subgroups of a group G, then

$$|HK| = \frac{(|H|)(|K|)}{|H \cap K|}.$$

Proof Let

$$h_1(H \cap K), h_2(H \cap K), h_3(H \cap K), \ldots, h_r(H \cap K)$$

be the left cosets of $H \cap K$ in H with each coset listed exactly once. We let

$$S = \{h_1, h_2, h_3, \ldots, h_r\},$$

which includes exactly one element from each left coset of $H \cap K$ in H. So

$$|S| = \frac{|H|}{|H \cap K|}.$$

Let $f : S \times K \to HK$ be defined by $f(h_i, k) = h_i k$. We show that f is one-to-one and onto.

Suppose that $hk \in HK$. Then $h \in H$ is in some left coset of $H \cap K$, so $h \in h_i(H \cap K)$ for some $h_i \in S$. We have that $h = h_i x$ for some $x \in H \cap K$. Let $k_1 = xk$. Then $(h_i, k_1) \in S \times K$ and

$$f(h_i, k_1) = h_i k_1 = h_i x k = hk.$$

Thus f is onto.

We now show that f is one-to-one. Suppose that $f(h_i, k) = f(h_j, k_1)$. So $h_i k = h_j k_1$. Then $h_j^{-1} h_i = k_1 k^{-1} \in H \cap K$. But this implies that h_i and h_j are in the same left coset of $H \cap K$, so $h_i = h_j$. By cancellation, $k = k_1$ and f is one-to-one.

Since there is a one-to-one and onto function $f : S \times K \to HK$, we have

$$\begin{aligned} |HK| &= |S||K| \\ &= \frac{|H|}{|H \cap K|} \cdot |K| \\ &= \frac{(|H|)(|K|)}{|H \cap K|}. \end{aligned}$$

◆