few exercises deal with this important subgroup.

21. Prove that $\Phi(G)$ is a characteristic subgroup of G.

22. Prove that if $N \trianglelefteq G$ then $\Phi(N) \leq \Phi(G)$. Give an explicit example where this containment does not hold if N is not normal in G.

23. Compute $\Phi(S_3)$, $\Phi(A_4)$, $\Phi(S_4)$, $\Phi(A_5)$ and $\Phi(S_5)$.

24. Say an element x of G is a *nongenerator* if for every proper subgroup H of G, $\langle x, H \rangle$ is also a proper subgroup of G. Prove that $\Phi(G)$ is the set of nongenerators of G (here $|G| > 1$).

25. Let G be a finite group. Prove that $\Phi(G)$ is nilpotent. [Use Frattini's Argument to prove that every Sylow subgroup of $\Phi(G)$ is normal in G.]

26. Let p be a prime, let P be a finite p-group and let $\overline{P} = P/\Phi(P)$.
   (a) Prove that $\overline{P}$ is an elementary abelian p-group. [Show that $P' \leq \Phi(P)$ and that $x^p \in \Phi(P)$ for all $x \in P$.]
   (b) Prove that if N is any normal subgroup of P such that P/N is elementary abelian then $\Phi(P) \leq N$. State this (universal) property in terms of homomorphisms and commutative diagrams.
   (c) Let $\overline{P}$ be elementary abelian of order p^r (by (a)). Deduce from Exercise 24 that if $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_r}$ are any basis for the r-dimensional vector space $\overline{P}$ over $\mathbb{F}_p$ and if x_i is any element of the coset $\overline{x_i}$, then $P = \langle x_1, x_2, \ldots, x_r \rangle$. Show conversely that if $y_1, y_2, \ldots, y_s$ is any set of generators for P, then $s \geq r$ (you may assume that every minimal generating set for an r-dimensional vector space has r elements, i.e., every basis has r elements). Deduce *Burnside's Basis Theorem*: a set $y_1, \ldots, y_s$ is a minimal generating set for P if and only if $\overline{y_1}, \ldots, \overline{y_s}$ is a basis of $\overline{P} = P/\Phi(P)$. Deduce that any minimal generating set for P has r elements.
   (d) Prove that if $P/\Phi(P)$ is cyclic then P is cyclic. Deduce that if P/P' is cyclic then so is P.
   (e) Let σ be any automorphism of P of prime order q with $q \neq p$. Show that if σ fixes the coset $x\Phi(P)$ then σ fixes some element of this coset (note that since $\Phi(P)$ is characteristic in P every automorphism of P induces an automorphism of $P/\Phi(P)$). [Use the observation that σ acts a permutation of order 1 or q on the p^a elements in the coset $x\Phi(P)$.]
   (f) Use parts (e) and (c) to deduce that every nontrivial automorphism of P of order prime to p induces a nontrivial automorphism on $P/\Phi(P)$. Deduce that any group of automorphisms of P which has order prime to p is isomorphic to a subgroup of $\mathrm{Aut}(\overline{P}) = GL_r(\mathbb{F}_p)$.

27. Generalize part (d) of the preceding exercise as follows: let p be a prime, let P be a p-group and let $\overline{P} = P/\Phi(P)$ be elementary abelian of order p^r. Prove that P has exactly $\dfrac{p^r - 1}{p - 1}$ maximal subgroups. [Since every maximal subgroup of P contains $\Phi(P)$, the maximal subgroups of P are, by the Lattice Isomorphism Theorem, in bijective correspondence with the maximal subgroups of the elementary abelian group $\overline{P}$. It therefore suffices to show that the number of maximal subgroups of an elementary abelian p-group of order p^r is as stated above. One way of doing this is to use the result that an abelian group is isomorphic to its dual group (cf. Exercise 14 in Section 5.2) so the number of subgroups of *index* p equals the number of subgroups of *order* p.]

28. Prove that if p is a prime and $P = Z_p \times Z_{p^2}$ then $|\Phi(P)| = p$ and $P/\Phi(P) \cong Z_p \times Z_p$. Deduce that P has $p + 1$ maximal subgroups.

29. Prove that if p is a prime and P is a non-abelian group of order p^3 then $\Phi(P) = Z(P)$ and $P/\Phi(P) \cong Z_p \times Z_p$. Deduce that P has $p + 1$ maximal subgroups.

30. Let p be an odd prime, let $P_1 = Z_p \times Z_{p^2}$ and let P_2 be the non-abelian group of order p^3 which has an element of order p^2. Prove that P_1 and P_2 have the same lattice of subgroups.

31. For any group G a *minimal normal subgroup* is a normal subgroup M of G such that the only normal subgroups of G which are contained in M are 1 and M. Prove that every minimal normal subgroup of a finite solvable group is an elementary abelian p-group for some prime p. [If M is a minimal normal subgroup of G, consider its characteristic subgroups: M' and $\langle x^p \mid x \in M \rangle$.]

32. Prove that every maximal subgroup of a finite solvable group has prime power index. [Let H be a maximal subgroup of G and let M be a minimal normal subgroup of G — cf. the preceding exercise. Apply induction to G/M and consider separately the two cases: $M \leq H$ and $M \not\leq H$.]

33. Let π be any set of primes. A subgroup H of a finite group is called a *Hall π-subgroup* of G if the only primes dividing $|H|$ are in the set π and $|H|$ is relatively prime to $|G : H|$. (Note that if $\pi = \{p\}$, Hall π-subgroups are the same as Sylow p-subgroups. Hall subgroups were introduced in Exercise 10 of Section 3.3). Prove the following generalization of Sylow's Theorem for solvable groups: if G is a finite solvable group then for every set π of primes, G has a Hall π-subgroup and any two Hall π-subgroups (for the same set π) are conjugate in G. [Fix π and proceed by induction on $|G|$, proving both existence and conjugacy at once. Let M be a minimal normal subgroup of G, so M is a p-group for some prime p. If $p \in \pi$, apply induction to G/M. If $p \notin \pi$, reduce to the case $|G| = p^\alpha n$, where $p^\alpha = |M|$ and n is the order of a Hall π-subgroup of G. In this case let N/M be a minimal normal subgroup of G/M, so N/M is a q-group for some prime $q \neq p$. Let $Q \in Syl_q(N)$. If $Q \trianglelefteq G$ argue as before with Q in place of M. If Q is not normal in G, use Frattini's Argument to show $N_G(Q)$ is a Hall π-subgroup of G and establish conjugacy in this case too.]

The following result shows how to produce normal p-subgroups of some groups on which the elements of order prime to p act faithfully by conjugation. Exercise 26(f) then applies to restrict these actions and give some information about the structure of the group.

34. Let p be a prime dividing the order of the finite solvable group G. Assume G has no nontrivial normal subgroups of order prime to p. Let P be the largest normal p-subgroup of G (cf. Exercise 37, Section 4.5). Note that Exercise 31 above shows that $P \neq 1$. Prove that $C_G(P) \leq P$, i.e., $C_G(P) = Z(P)$. [Let $N = C_G(P)$ and use the preceding exercise to show $N = Z(P) \times H$ for some Hall π-subgroup H of N — here π is the set of all prime divisors of $|N|$ except for p. Show $H \trianglelefteq G$ to obtain the desired conclusion: $H = 1$.]

35. Prove that if G is a finite group in which every proper subgroup is nilpotent, then G is solvable. [Show that a minimal counterexample is simple. Let M and N be distinct maximal subgroups chosen with $|M \cap N|$ as large as possible and apply Part 2 of Theorem 3 to show that $M \cap N = 1$. Now apply the methods of Exercise 53 in Section 4.5.]

36. Let p be a prime, let V be a nonzero finite dimensional vector space over the field of p elements and let φ be an element of $GL(V)$ of order a power of p (i.e., V is a nontrivial elementary abelian p-group and φ is an automorphism of V of p-power order). Prove that there is some nonzero element $v \in V$ such that $\varphi(v) = v$, i.e., φ has a nonzero fixed point on V.

37. Let V be a finite dimensional vector space over the field of 2 elements and let φ be an element of $GL(V)$ of order 2. (i.e., V is a nontrivial elementary abelian 2-group and φ is an

automorphism of V of order 2). Prove that the map $v \mapsto v + \varphi(v)$ is a homomorphism from V to itself. Show that every element in the image of this map is fixed by φ. Deduce that the subspace of elements of V which are fixed by φ has dimension $\geq \frac{1}{2}$(dimension V). (Note that if G is the semidirect product of V with $\langle \varphi \rangle$, where $V \trianglelefteq G$ and φ acts by conjugation on V by sending each $v \in V$ to $\varphi(v)$, then the fixed points of φ on V are $C_V(\varphi)$ and the above map is simply the commutator map: $v \mapsto [v, \varphi]$. In this terminology the problem is to show that $|C_V(\varphi)|^2 \geq |V|$.)

38. Use the preceding exercise to prove that if P is a 2-group which has a cyclic center and M is a subgroup of index 2 in P, then the center of M has rank ≤ 2. [The group G/M of order 2 acts by conjugation on the $\mathbb{F}_2$ vector space: $\{z \in Z(M) \mid z^2 = 1\}$ and the fixed points of this action are in the center of P.]

6.2 APPLICATIONS IN GROUPS OF MEDIUM ORDER

The purpose of this section is to work through a number of examples which illustrate many of the techniques we have developed. These examples use Sylow's Theorems extensively and demonstrate how they are applied in the study of finite groups. Motivated by the Hölder Program we address primarily the problem of showing that for certain n every group of order n has a proper, nontrivial normal subgroup (i.e., there are no simple groups of order n). In most cases we shall stop once this has been accomplished. However readers should be aware that in the process of achieving this result we shall already have determined a great deal of information about arbitrary groups of given order n for the n that we consider. This information could be built upon to classify groups of these orders (but in general this requires techniques beyond the simple use of semidirect products to construct groups).

Since for p a prime we have already proved that there are no simple p-groups (other than the cyclic group of order p, Z_p) and since the structure of p-groups can be very complicated (recall the table in Section 5.3), we shall not study the structure of p-groups explicitly. Rather, the theory of p-groups developed in the preceding section will be applied to subgroups of groups of non-prime-power order.

Finally, for certain n (e.g., 60, 168, 360, 504,...) there do exist simple groups of order n so, of course, we cannot force every group of these orders to be nonsimple. As in Section 4.5 we can, in certain cases, prove there is a unique simple group of order n and unravel some of its internal structure (Sylow numbers, etc.). We shall study simple groups of order 168 as an additional test case. Thus the Sylow Theorems will be applied in a number of different contexts to show how groups of a given order may be manipulated.

We shall end this section with some comments on the existence problem for groups, particularly for finite simple groups.

For $n < 10000$ there are 60 odd, non-prime-power numbers for which the congruence conditions of Sylow's Theorems do *not* force at least one of the Sylow subgroups to be normal i.e., n_p can be > 1 for all primes $p \mid n$ (recall that n_p denotes the number of Sylow p-subgroups). For example, no numbers of the form pq, where p and q are distinct primes occur in our list by results of Section 4.5. In contrast, for even numbers < 500 there are already 46 candidates for orders of simple groups (the congruence