CHAPTER 4

The Sylow Theorems

p-Groups

The order of a group G has consequences for its structure. A rough rule of thumb is that the more complicated the prime factorization of $|G|$, the more complicated the group. In particular, the fewer the number of distinct prime factors in $|G|$, the more tractible it is. We now study the "local" case when only one prime divides $|G|$.

Definition. If p is a prime, then a ***p-group*** is a group in which every element has order a power of p.

Corollary 4.3 below gives a simple characterization of finite p-groups.

Lemma 4.1. *If G is a finite abelian group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Write $|G| = pm$, where $m \geq 1$. We proceed by induction on m after noting that the base step is clearly true. For the inductive step, choose $x \in G$ of order $t > 1$. If $p|t$, then Exercise 2.11 shows that $x^{t/p}$ has order p, and the lemma is proved. We may, therefore, assume that the order of x is not divisible by p. Since G is abelian, $\langle x \rangle$ is a normal subgroup of G, and $G/\langle x \rangle$ is an abelian group of order $|G|/t = pm/t$. Since $p \nmid t$, we must have $m/t < m$ an integer. By induction, $G/\langle x \rangle$ contains an element y^* of order p. But the natural map $v: G \to G/\langle x \rangle$ is a surjection, and so there is $y \in G$ with $v(y) = y^*$. By Exercise 2.14, the order of y is a multiple of p, and we have returned to the first case. ∎

We now remove the hypothesis that G is abelian.

Theorem 4.2 (Cauchy, 1845). *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Recall Theorem 3.2. If $x \in G$, then the number of conjugates of x is $[G : C_G(x)]$, where $C_G(x)$ is the centralizer of x in G. If $x \notin Z(G)$, then its conjugacy class has more than one element, and so $|C_G(x)| < |G|$. If $p \mid |C_G(x)|$ for such a noncentral x, we are done, by induction. Therefore, we may assume that $p \nmid |C_G(x)|$ for all noncentral x in G. Better, since $|G| = [G : C_G(x)]|C_G(x)|$, we may assume that $p \mid [G : C_G(x)]$ (using Euclid's lemma, which applies because p is prime).

Partition G into its conjugacy classes and count (recall that $Z(G)$ consists of all the elements of G whose conjugacy class has just one element):

$$(*) \qquad |G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

where one x_i is selected from each conjugacy class with more than one element. Since $|G|$ and all $[G : C_G(x_i)]$ are divisible by p, it follows that $|Z(G)|$ is divisible by p. But $Z(G)$ is abelian, and so it contains an element of order p, by the lemma. ▩

Definition. Equation $(*)$ above is called the ***class equation*** of the finite group G.

Here is a second proof of Cauchy's theorem, due to J.H. McKay, which avoids the class equation. Assume that p is a prime and that G is a finite group. Define

$$X = \{(a_1, \ldots, a_p) \in G \times \cdots \times G : a_1 a_2 \ldots a_p = 1\}.$$

Note that $|X| = |G|^{p-1}$, for having chosen the first $p - 1$ coordinates arbitrarily, we must set $a_p = (a_1 a_2 \ldots a_{p-1})^{-1}$. Now X is a $\mathbb{Z}_p$-set, where $g \in \mathbb{Z}_p$ acts by cyclically permuting the coordinates (since $a_i \ldots a_p a_1 \ldots a_{i-1}$ is a conjugate of $a_1 a_2 \ldots a_p$, the product of the permuted coordinates is also equal to 1). By Corollary 3.21, each orbit of X has either 1 or p elements. An orbit with just one element is a p-tuple having all its coordinates equal, say, $a_i = a$ for all i; in other words, such orbits correspond to elements $a \in G$ with $a^p = 1$. Clearly $(1, \ldots, 1)$ is such an orbit; were this the only such orbit, then we would have

$$|X| = |G|^{p-1} = 1 + kp$$

for some integer $k \geq 0$; that is, $|G|^{p-1} \equiv 1 \bmod p$. If p divides $|G|$, however, this is a contradiction, and so we conclude that G must have an element of order p. (As A. Mann remarked to me, if $|G|$ is not divisible by p, then we have proved Fermat's theorem.)

Corollary 4.3. *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Proof. If $|G| = p^m$, then Lagrange's theorem shows that G is a p-group. Conversely, assume that there is a prime $q \neq p$ which divides $|G|$. By Cauchy's theorem, G contains an element of order q, and this contradicts G being a p-group. ∎

Theorem 4.4. *If $G \neq 1$ is a finite p-group, then its center $Z(G) \neq 1$.*

Proof. Consider the class equation

$$|G| = |Z(G)| + \sum [G : C_G(x_i)].$$

Each $C_G(x_i)$ is a proper subgroup of G, for $x_i \notin Z(G)$. By Corollary 4.3, $[G : C_G(x_i)]$ is a power of p (since $|G|$ is). Thus, p divides each $[G : C_G(x_i)]$, and so p divides $|Z(G)|$. ∎

If G is a finite simple p-group, then $G = Z(G)$ and G is abelian; therefore, G must be cyclic of order p. Theorem 4.4 is false for infinite p-groups.

Corollary 4.5. *If p is a prime, then every group G of order p^2 is abelian.*

Proof. If G is not abelian, then $Z(G) < G$; since $1 \neq Z(G)$, we must have $|Z(G)| = p$. The quotient group $G/Z(G)$ is defined, since $Z(G) \lhd G$, and it is cyclic, because $|G/Z(G)| = p$; this contradicts Exercise 3.3. ∎

Theorem 4.6. *Let G be a finite p-group.*

(i) *If H is a proper subgroup of G, then $H < N_G(H)$.*
(ii) *Every maximal subgroup of G is normal and has index p.*

Proof. (i) If $H \lhd G$, then $N_G(H) = G$ and the theorem is true. If X is the set of all the conjugates of H, then we may assume that $|X| = [G : N_G(H)] \neq 1$. Now G acts on X by conjugation and, since G is a p-group, every orbit of X has size a power of p. As $\{H\}$ is an orbit of size 1, there must be at least $p - 1$ other orbits of size 1. Thus there is at least one conjugate $gHg^{-1} \neq H$ with $\{gHg^{-1}\}$ also an orbit of size 1. Now $agHg^{-1}a^{-1} = gHg^{-1}$ for all $a \in H$, and so $g^{-1}ag \in N_G(H)$ for all $a \in H$. But $gHg^{-1} \neq H$ gives at least one $a \in H$ with $g^{-1}ag \notin H$, and so $H < N_G(H)$.

(ii) If H is a maximal subgroup of G, then $H < N_G(H)$ implies that $N_G(H) = G$; that is, $H \lhd G$. By Exercise 2.58, $[G : H] = p$. ∎

Lemma 4.7. *If G is a finite p-group and r_1 is the number of subgroups of G having order p, then $r_1 \equiv 1 \bmod p$.*

Proof. Let us first count the number of elements of order p. Since $Z(G)$ is

Central Series and Nilpotent Groups

The Sylow theorems show that knowledge of p-groups gives information about arbitrary finite groups. Moreover, p-groups have a rich supply of normal subgroups, and this suggests that normal series might be a powerful tool in their study. It turns out that the same methods giving theorems about p-groups also apply to a larger class, the *nilpotent groups*, which may be regarded as generalized p-groups.

Definition. If $H, K \leq G$, then

$$[H, K] = \langle [h, k]: h \in H \text{ and } k \in K \rangle,$$

where $[h, k]$ is the commutator $hkh^{-1}k^{-1}$.

An example was given, in Exercise 2.43, showing that the *set* of all commutators need not be a subgroup; in order that $[H, K]$ be a subgroup, therefore, we must take the subgroup generated by the indicated commutators. It is obvious that $[H, K] = [K, H]$, for $[h, k]^{-1} = [k, h]$. The commutator subgroup G' is equal to $[G, G]$ and, more generally, the higher commutator subgroup $G^{(i+1)}$ is equal to $[G^{(i)}, G^{(i)}]$.

We say that a subgroup K ***normalizes*** H if $K \leq N_G(H)$; it is easy to see that K normalizes H if and only if $[H, K] \leq H$.

Definition. If $H \leq G$, the ***centralizer*** of H in G is

$$C_G(H) = \{x \in G: x \text{ commutes with every } h \in H\};$$

that is, $C_G(H) = \{x \in G: [x, h] = 1 \text{ for all } h \in H\}$.

We say that a subgroup K ***centralizes*** H if $K \leq C_G(H)$; it is easy to see that K centralizes H if and only if $[H, K] = 1$.

If $x, y \in G$ and $[x, y] \in K$, where $K \lhd G$, then x and y "commute mod K"; that is, $xKyK = yKxK$ in G/K.

Lemma 5.30.

(i) *If $K \lhd G$ and $K \leq H \leq G$, then $[H, G] \leq K$ if and only if $H/K \leq Z(G/K)$.*
(ii) *If $H, K \leq G$ and $f: G \to L$ is a homomorphism, then $f([H, K]) = [f(H), f(K)]$.*

Proof. (i) If $h \in H$ and $g \in G$, then $hKgK = gKhK$ if and only if $[h, g]K = K$ if and only if $[h, g] \in K$.

(ii) Both sides are generated by all $f([h, k]) = [f(h), f(k)]$. ∎

Definition. Define characteristic subgroups $\gamma_i(G)$ of G by induction:

$$\gamma_1(G) = G; \qquad \gamma_{i+1}(G) = [\gamma_i(G), G].$$

Notice that $\gamma_2(G) = [\gamma_1(G), G] = [G, G] = G' = G^{(1)}$. It is easy to check that $\gamma_{i+1}(G) \leq \gamma_i(G)$. Moreover, Lemma 5.30(i) shows that $[\gamma_i(G), G] = \gamma_{i+1}(G)$ gives $\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$.

Definition. The ***lower central series*** (or *descending central series*) of G is the series

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots$$

(this need not be a normal series because it may not reach 1).

There is another series of interest.

Definition. The ***higher centers*** $\zeta^i(G)$ are the characteristic subgroups of G defined by induction:

$$\zeta^0(G) = 1; \qquad \zeta^{i+1}(G)/\zeta^i(G) = Z(G/\zeta^i(G));$$

that is, if $v_i\colon G \to G/\zeta^i(G)$ is the natural map, then $\zeta^{i+1}(G)$ is the inverse image of the center.

Of course, $\zeta^1(G) = Z(G)$.

Definition. The ***upper central series*** (or *ascending central series*) of G is

$$1 = \zeta^0(G) \leq \zeta^1(G) \leq \zeta^2(G) \leq \cdots.$$

When no confusion can occur, we may abbreviate $\zeta^1(G)$ by ζ^i and $\gamma_i(G)$ by γ_i.

Theorem 5.31. *If G is a group, then there is an integer c with $\zeta^c(G) = G$ if and only if $\gamma_{c+1}(G) = 1$. Moreover, in this case,*

$$\gamma_{i+1}(G) \leq \zeta^{c-i}(G) \qquad \textit{for all } i.$$

Proof. Assume that $\zeta^c = G$, and let us prove that the inclusion holds by induction on i. If $i = 0$, then $\gamma_1 = G = \zeta^c$. If $\gamma_{i+1} \leq \zeta^{c-i}$, then

$$\gamma_{i+2} = [\gamma_{i+1}, G] \leq [\zeta^{c-i}, G] \leq \zeta^{c-i-1},$$

the last inclusion following from Lemma 5.30. We have shown that the inclusion always holds; in particular, if $i = c$, then $\gamma_{c+1} \leq \zeta^0 = 1$.

Assume that $\gamma_{c+1} = 1$, and let us prove that $\gamma_{c+1-j} \leq \zeta^j$ by induction on j (this is the same inclusion as in the statement: set $j = c - i$). If $j = 0$, then $\gamma_{c+1} = 1 = \zeta^0$. If $\gamma_{c+1-j} \leq \zeta^j$, then the third isomorphism theorem gives a surjective homomorphism $G/\gamma_{c+1-j} \to G/\zeta^j$. Now $[\gamma_{c-j}, G] = \gamma_{c+1-j}$, so that Lemma 5.30 gives $\gamma_{c-j}/\gamma_{c+1-j} \leq Z(G/\gamma_{c+1-j})$. By Exercise 3.10 [if $A \leq Z(G)$

and $f: G \to H$ is surjective, then $f(A) \leq Z(H)$], we have

$$\gamma_{c-j}\zeta^j/\zeta^j \leq Z(G/\zeta^j) = \zeta^{j+1}/\zeta^j.$$

Therefore, $\gamma_{c-j} \leq \gamma_{c-j}\zeta^j \leq \zeta^{j+1}$, as desired. We have shown that the inclusion always holds; in particular, if $j = c$, then $G = \gamma_1 \leq \zeta^c$. ▩

The following result reflects another relationship between these two series.

Theorem 5.32 (Schur). *If G is a group with $G/Z(G)$ finite, then G' is also finite.*

***Proof* (Ornstein).** Let $g_1, \ldots, g_n$ be representatives of the cosets of $Z(G)$ in G; that is, each $x \in G$ has the form $x = g_i z$ for some i and some $z \in Z(G)$. For all $x, y \in G$, $[x, y] = [g_i z, g_j z'] = [g_i, g_j]$. Hence, every commutator has the form $[g_i, g_j]$ for some i, j, so that G' has a finite number ($< n^2$) of generators.

Each element $g' \in G'$ can be written as a word $c_1 \cdots c_t$, where each c_i is a commutator (no exponents are needed, for $[x, y]^{-1} = [y, x]$). It suffices to prove that if a factorization of g' is chosen so that $t = t(g')$ is minimal, then $t(g') < n^3$ for all $g' \in G'$.

We prove first, by induction on $r \geq 1$, that if $a, b \in G$, then $[a, b]^r = (aba^{-1}b^{-1})^r = (ab)^r(a^{-1}b^{-1})^r u$, where u is a product of $r - 1$ commutators. This is obvious when $r = 1$. Note, for the inductive step, that if $x, y \in G$, then $xy = yxx^{-1}y^{-1}xy = yx[x^{-1}, y^{-1}]$; that is, $xy = yxc$ for some commutator c. Thus, if $r > 1$, then

$$\begin{aligned}(aba^{-1}b^{-1})^{r+1} &= aba^{-1}b^{-1}(aba^{-1}b^{-1})^r \\ &= ab[a^{-1}b^{-1}]\{(ab)^r(a^{-1}b^{-1})^r\}u \\ &= ab\{(ab)^r(a^{-1}b^{-1})^r\}[a^{-1}b^{-1}]cu\end{aligned}$$

for some commutator c, as desired.

Since $yx = x^{-1}(xy)x$, we have $(yx)^n = x^{-1}(xy)^n x = (xy)^n$, because $[G : Z(G)] = n$ implies $(ab)^n \in Z(G)$. Therefore, $(a^{-1}b^{-1})^n = ((ba)^{-1})^n = ((ba)^n)^{-1} = ((ab)^n)^{-1}$. It follows that

(*) $[a, b]^n$ is a product of $n - 1$ commutators.

Now $xyx = (xyx^{-1})x^2$, so that two x's can be brought together at the expense of replacing y by a conjugate of y. Take an expression of an element $g' \in G'$ as a product of commutators $c_1 \ldots c_t$, where t is minimal. If $t \geq n^3$, then there is some commutator c occurring m times, where $m > n$ (for there are fewer than n^2 distinct commutators). By our remark above, all such factors can be brought together to c^m at the harmless expense of replacing commutators by conjugates (which are still commutators); that is, the number of commutator factors in the expression is unchanged. By (*), the length of the minimal expression for g' is shortened, and this is a contradiction. Therefore, $t < n^3$, and so G' is finite. ▩

Definition. A group G is ***nilpotent***[4] if there is an integer c such that $\gamma_{c+1}(G) = 1$; the least such c is called the ***class*** of the nilpotent group G.

Theorem 5.31 shows, for nilpotent groups, that the lower and upper central series are normal series of the same length.

A group is nilpotent of class 1 if and only if it is abelian. By Theorem 5.31, a nilpotent group G of class 2 is described by $\gamma_2(G) = G' \leq Z(G) = \zeta^1(G)$. Every nonabelian group of order p^3 is nilpotent of class 2, by Exercise 4.7.

Theorem 5.33. *Every finite p-group is nilpotent.*

Proof. Recall Theorem 4.4. Every finite p-group has a nontrivial center. If, for some i, we have $\zeta^i(G) < G$, then $Z(G/\zeta^i(G)) \neq 1$ and so $\zeta^i(G) < \zeta^{i+1}(G)$. Since G is finite, there must be an integer i with $\zeta^i(G) = G$; that is, G is nilpotent. ▩

This theorem is false without the finiteness hypothesis, for there exist infinite p-groups that are not nilpotent (see Exercise 5.45 below); indeed, there is an example of McLain (1954) of an infinite p-group G with $Z(G) = 1$, with $G' = G$ (so that G is not even solvable), and with no characteristic subgroups other than G and 1.

Theorem 5.34.

(i) *Every nilpotent group G is solvable.*
(ii) *If* $G \neq 1$ *is nilpotent, then* $Z(G) \neq 1$.
(iii) S_3 *is a solvable group that is not nilpotent.* ▩

Proof. (i) An easy induction shows that $G^{(i)} \leq \gamma_i(G)$ for all i. It follows that if $\gamma_{c+1}(G) = 1$, then $G^{(c+1)} = 1$; that is, if G is nilpotent (of class $\leq c$), then G is solvable (with derived length $\leq c + 1$).

(ii) Assume that $G \neq 1$ is nilpotent of class c, so that $\gamma_{c+1}(G) = 1$ and $\gamma_c(G) \neq 1$. By Theorem 5.31, $1 \neq \gamma_c(G) \leq \zeta^1(G) = Z(G)$.

(iii) The group $G = S_3$ is solvable and $Z(S_3) = 1$. ▩

Theorem 5.35. *Every subgroup H of a nilpotent group G is nilpotent. Moreover, if G is nilpotent of class c, then H is nilpotent of class* $\leq c$.

Proof. It is easily proved by induction that $H \leq G$ implies $\gamma_i(H) \leq \gamma_i(G)$ for all i. Therefore, $\gamma_{c+1}(G) = 1$ forces $\gamma_{c+1}(H) = 1$. ▩

[4] There is an analogue of the descending central series for Lie algebras, and *Engel's theorem* says that if the descending central series of a Lie algebra L reaches 0, then L is isomorphic to a Lie algebra whose elements are nilpotent matrices. This is the reason such Lie algebras are called nilpotent, and the term for groups is taken from Lie algebras.

Theorem 5.36. *If G is nilpotent of class c and $H \lhd G$, then G/H is nilpotent of class $\leq c$.*

Proof. If $f\colon G \to L$ is a surjective homomorphism, then Lemma 5.30 gives $\gamma_i(L) \leq f(\gamma_i(G))$ for all i. Therefore, $\gamma_{c+1}(G) = 1$ forces $\gamma_{c+1}(L) = 1$. The theorem follows by taking f to be the natural map. ∎

We have proved the analogues for nilpotent groups of Theorems 5.15 and 5.16; is the analogue of Theorem 5.17 true? If $H \lhd G$ and both H and G/H are nilpotent, then is G nilpotent? The answer is "no": we have already seen that S_3 is not nilpotent, but both $A_3 \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$ are abelian, hence nilpotent. A positive result of this type is due to P. Hall. If $H \lhd G$, then we know that $H' \lhd G$; Hall proved that if both H and G/H' are nilpotent, then G is nilpotent (a much simpler positive result is in Exercise 5.38 below). The analogue of Corollary 5.18 is true, however.

Theorem 5.37. *If H and K are nilpotent, then their direct product $H \times K$ is nilpotent.*

Proof. An easy induction shows that $\gamma_i(H \times K) \leq \gamma_i(H) \times \gamma_i(K)$ for all i. If $M = \max\{c, d\}$, where $\gamma_{c+1}(H) = 1 = \gamma_{d+1}(K)$, then $\gamma_{M+1}(H \times K) = 1$ and $H \times K$ is nilpotent. ∎

Theorem 5.38. *If G is nilpotent, then it satisfies the **normalizer condition**: if $H < G$, then $H < N_G(H)$.*

Proof. There exists an integer i with $\gamma_{i+1}(G) \leq H$ and $\gamma_i(G) \not\leq H$ (this is true for any descending series of subgroups starting at G and ending at 1). Now $[\gamma_i, H] \leq [\gamma_i, G] = \gamma_{i+1} \leq H$, so that γ_i normalizes H; that is, $\gamma_i \leq N_G(H)$. Therefore, H is a proper subgroup of $N_G(H)$. ∎

The converse is also true; it is Exercise 5.37 below.

Theorem 5.39. *A finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups.*

Proof. If G is the direct product of its Sylow subgroups, then it is nilpotent, by Theorems 5.32 and 5.36.

For the converse, let P be a Sylow p-subgroup of G for some prime p. By Exercise 4.11, $N_G(P)$ is equal to its own normalizer. On the other hand, if $N_G(P) < G$, then Theorem 5.38 shows that $N_G(P)$ is a proper subgroup of its own normalizer. Therefore, $N_G(P) = G$ and $P \lhd G$. The result now follows from Exercise 4.12. ∎

Of course, in any group, every subgroup of prime index is a maximal

subgroup. The converse is false in general (S_4 has a maximal subgroup of index 4, as the reader should check), but it is true for nilpotent groups.

Theorem 5.40. *If G is a nilpotent group, then every maximal subgroup H is normal and has prime index.*

Proof. By Theorem 5.38, $H < N_G(H)$; since H is maximal, $N_G(H) = G$, and so $H \lhd G$. Exercise 2.58 now shows that G/H has prime order. ▩

Theorem 5.41. *Let G be a nilpotent group.*

(i) *If H is a nontrivial normal subgroup, then $H \cap Z(G) \neq 1$.*
(ii) *If A is a maximal abelian normal subgroup of G, then $A = C_G(A)$.*

Proof. (i) Since $\zeta^0(G) = 1$ and $G = \zeta^c(G)$ for some c, there is an integer i for which $H \cap \zeta^i(G) \neq 1$; let m be the minimal such i. Now $[H \cap \zeta^m(G), G] \leq H \cap [\zeta^m(G), G] \leq H \cap \zeta^{m-1}(G) = 1$, because $H \lhd G$, and this says that $1 \neq H \cap \zeta^m(G) \leq H \cap Z(G)$.

(ii) Since A is abelian, $A \leq C_G(A)$. For the reverse inclusion, assume that $g \in C_G(A)$ and $g \notin A$. It is easy to see, for any subgroup H (of any group G) and for all $g \in G$, that $gC_G(H)g^{-1} = C_G(g^{-1}Hg)$. Since $A \lhd G$, it follows that $gC_G(A)g^{-1} = C_G(A)$ for all $g \in G$, and so $C_G(A) \lhd G$. Therefore, $C_G(A)/A$ is a nontrivial normal subgroup of the nilpotent group G/A; by (i), there is $Ax \in (C_G(A)/A) \cap Z(G/A)$. The correspondence theorem gives $\langle A, x \rangle$ a normal abelian subgroup of G strictly containing A, and this contradicts the maximality of A. ▩

EXERCISES

5.35. If G is nilpotent of class 2 and if $a \in G$, then the function $G \to G$, defined by $x \mapsto [a, x]$, is a homomorphism. Conclude, in this case, that $C_G(a) \lhd G$.

5.36. If G is nilpotent of class c, then $G/Z(G)$ is nilpotent of class $c - 1$.

5.37. Show that the following conditions on a finite group G are equivalent:
(i) G is nilpotent;
(ii) G satisfies the normalizer condition;
(iii) Every maximal subgroup of G is normal.

5.38. If $H \leq Z(G)$ and if G/H is nilpotent, then G is nilpotent.

Definition. A normal series

$$G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$$

with each $G_i \lhd G$ and $G_i/G_{i+1} \leq Z(G/G_{i+1})$ is called a ***central series.***

5.39. (i) If G is nilpotent, then both the upper and lower central series of G are central series.

(ii) Prove that a group G is nilpotent if and only if it has a central series $G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$. Moreover, if G is nilpotent of class c, then $\gamma_{i+1}(G) \leq G_{i+1} \leq \zeta^{c-i}(G)$ for all i.

5.40. If G is a nilpotent group and H is a minimal normal subgroup of G, then $H \leq Z(G)$.

5.41. The dihedral group D_{2n} is nilpotent if and only if n is a power of 2.

5.42. Let G be a finite nilpotent group of order n. If $m|n$, then G has a subgroup of order m.

5.43. (i) If H and K are normal nilpotent subgroups of a finite group G, then HK is a normal nilpotent subgroup.
(ii) Every finite group G has a unique maximal normal nilpotent subgroup $\mathscr{F}(G)$ (which is called the ***Fitting subgroup*** of G).
(iii) Show that $\mathscr{F}(G)$ char G when G is finite.

5.44. (i) Show $\gamma_i(\mathrm{UT}(n, \mathbb{Z}_p))$ consists of all upper triangular matrices with 1's on the main diagonal and 0's on the $i-1$ superdiagonals just above the main diagonal (*Hint.* If A is unitriangular, consider powers of $A - E$, where E is the identity matrix.)
(ii) The group $\mathrm{UT}(n, \mathbb{Z}_p)$ of all $n \times n$ unitriangular matrices over $\mathbb{Z}_p$ is a p-group that is nilpotent of class $n-1$.

5.45. For each $n \geq 1$, let G_n be a finite p-group of class n. Define H to be the group of all sequences $(g_1, g_2, \ldots)$, with $g_n \in G_n$ for all n and with $g_n = 1$ for all large n; that is, $g_n \neq 1$ for only a finite number of g_n. Show that H is an infinite p-group which is not nilpotent.

5.46. If $x, y \in G$, denote yxy^{-1} by x^y. If $x, y, z \in G$, prove

$$[x, yz] = [x, y][x, z]^y \qquad \text{and} \qquad [xy, z] = [y, z]^x[x, z].$$

(Recall that $[x, y] = xyx^{-1}y^{-1}$.)

5.47 **(Jacobi identity).** If $x, y, z \in G$, denote $[x, [y, z]]$ by $[x, y, z]$. Prove that $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$.

5.48. (i) Let H, K, L be subgroups of G, and let $[H, K, L] = \langle [h, k, l]: h \in H, k \in K, l \in L \rangle$. Show that if $[H, K, L] = 1 = [K, L, H]$, then $[L, H, K] = 1$.
(ii) **(Three subgroups lemma).** If $N \lhd G$ and $[H, K, L][K, L, H] \leq N$, then $[L, H, K] \leq N$.
(iii) If H, K, and L are all normal subgroups of G, then $[L, H, K] \leq [H, K, L][K, L, H]$. (*Hint.* Set $N = [H, K, L][K, L, H]$.)

5.49. If G is a group with $G = G'$, then $G/Z(G)$ is centerless. (*Hint.* Use the three subgroups lemma with $H = \zeta^2(G)$ and $K = L = G$.)

5.50. Prove that $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$ for all i, j. (*Hint.* Use the three subgroups lemma.)

5.51. If $H \lhd G$ and $H \cap G' = 1$, then $H \leq Z(G)$ (and so H is abelian).

p-Groups

There are many ***commutator identities*** that are quite useful even though they are quite elementary.

Lemma 5.42. *Let $x, y \in G$ and assume that both x and y commute with $[x, y]$. Then:*

(i) $[x, y]^n = [x^n, y] = [x, y^n]$ *for all* $n \in \mathbb{Z}$; *and*
(ii) $(xy)^n = [y, x]^{n(n-1)/2} x^n y^n$ *for all* $n \geq 0$.

Proof. (i) We first prove (i) for nonnegative n by induction on $n \geq 0$; of course, it is true when $n = 0$. For the inductive step, note that

$$\begin{aligned}
[x, y]^n [x, y] &= x[x, y]^n y x^{-1} y^{-1}, \quad \text{by hypothesis} \\
&= x[x^n, y] y x^{-1} y^{-1}, \quad \text{by induction} \\
&= x(x^n y x^{-n} y^{-1}) y x^{-1} y^{-1} \\
&= [x^{n+1}, y].
\end{aligned}$$

Now $x[x, y] = [x, y]x$, by hypothesis, so that $xyx^{-1}y^{-1} = yx^{-1}y^{-1}x$; that is, $[x, y]^{-1} = [y, x^{-1}]^{-1} = [x^{-1}, y]$. Therefore, if $n \geq 0$, then $[x, y]^{-n} = [x^{-1}, y]^n = [x^{-n}, y]$, as desired.

(ii) The second identity is also proved by induction on $n \geq 0$.

$$\begin{aligned}
(xy)^n (xy) &= [y, x]^{n(n-1)/2} x^n y^n xy \\
&= [y, x]^{n(n-1)/2} x^{n+1} [x^{-1}, y^n] y^{n+1} \\
&= [y, x]^{n(n-1)/2} x^{n+1} [y, x]^n y^{n+1} \\
&= [y, x]^{n(n-1)/2} [y, x]^n x^{n+1} y^{n+1} \\
&= [y, x]^{(n+1)n/2} x^{n+1} y^{n+1}. \quad \blacksquare
\end{aligned}$$

Theorem 5.43. *If G is a p-group having a unique subgroup of order p and more than one cyclic subgroup of index p, then $G \cong \mathbb{Q}$, the quaternions.*

Proof. If A is a subgroup of G of index p, then $A \lhd G$, by Theorem 5.40. Thus, if $x \in G$, then $Ax \in G/A$, a group of order p, and so $x^p \in A$. Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be distinct subgroups of index p, and let $D = A \cap B$; note that $D \lhd G$, for it is the intersection of normal subgroups. Our initial remarks show that the subset

$$G^p = \{x^p : x \in G\}$$

is contained in D. Since A and B are distinct maximal subgroups, it follows that $AB = G$, and so the product formula gives $[G : D] = p^2$. Hence, G/D is abelian and $G' \leq D$, by Theorem 2.23. As $G = AB$, each $x \in G$ is a product of a power of a and a power of b; but every element of D is simultaneously a

power of a and a power of b, and so it commutes with each $x \in G$; that is, $D \leq Z(G)$. We have seen that

$$G' \leq D \leq Z(G),$$

so that the hypothesis of Lemma 5.42(i) holds. Hence, for every $x, y \in G$, $[y, x]^p = [y^p, x]$. But $y^p \in D \leq Z(G)$, and so $[y, x]^p = 1$. Now Lemma 5.42(ii) gives $(xy)^p = [y, x]^{p(p-1)/2} x^p y^p$. If p is odd, then $p | p(p-1)/2$, and $(xy)^p = x^p y^p$. By Exercise 2.55, if $G[p] = \{x \in G: x^p = 1\}$ and $G^p = \{x^p: x \in G\}$ (as defined above), then both these subsets are subgroups and $[G : G[p]] = |G^p|$. Thus,

$$|G[p]| = [G : G^p] = [G : D][D : G^p] \geq p^2,$$

and $G[p]$ contains a subgroup E of order p^2; but E must be elementary abelian, so that $G[p]$, hence G, contains more than one subgroup of order p. We conclude that $p = 2$.

When $p = 2$, we have $D = \langle a^2 \rangle = G^2 \leq Z(G)$, $[G : D] = 4$, and since $[y, x]^2 = 1$ for all $x, y \in G$,

$$(xy)^4 = [y, x]^6 x^4 y^4 = x^4 y^4.$$

Hence $|G[2]| = [G : G^4] = [G : D][D : G^4] = 8$, because $D = \langle a^2 \rangle$ and $G^4 = \langle a^4 \rangle$. If $G[2]$ had only one cyclic subgroup of order 4, then it would contain more than one involution (for every element of $G[2]$ has order either 1, 2, or 4); there are thus two cyclic subgroups $\langle u \rangle$ and $\langle v \rangle$ of order 4 in $G[2]$. If $a^4 \neq 1$, we may take $\langle u \rangle \leq \langle a^2 \rangle \leq Z(G)$, and so $\langle u \rangle \langle v \rangle$ is an abelian subgroup of G. But $\langle u \rangle \langle v \rangle$ contains at least two involutions: either $u^2 \neq v^2$ or $u^2 \neq uv^{-1}$; this contradiction shows that $a^4 = 1$. It follows that $|D| = 2$ and $|G| = 8$. By Exercise 4.34, $G \cong \mathbb{Q}$ or $G \cong \mathbb{Z}_8$; but only $\mathbb{Q}$ has more than one subgroup of index 2. ∎

We do an exercise in congruences before giving the next theorem.

Theorem 5.44. *Let $U(\mathbb{Z}_{2^m})$ be the multiplicative group*

$$U(\mathbb{Z}_{2^m}) = \{[a] \in \mathbb{Z}_{2^m}: a \text{ is odd}\}.$$

If $m \geq 3$, then

$$U(\mathbb{Z}_{2^m}) = \langle [-1], [5] \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}.$$

Remark. $U(\mathbb{Z}_{2^m})$ is the group of units in the ring $\mathbb{Z}_{2^m}$.

Proof. By Exercise 2.23, $|U(\mathbb{Z}_{2^m})| = \varphi(2^m) = 2^{m-1}$. Induction and the binomial theorem show that

$$5^{2^{m-3}} = (1 + 4)^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m.$$

Since $U(\mathbb{Z}_{2^m})$ is a 2-group, $[5]$ has order 2^s, for some $s \geq m - 2$ (because $1 + 2^{m-1} \not\equiv 1 \bmod 2^m$). Of course, $[-1]$ has order 2. We claim that $\langle [5] \rangle \cap \langle [-1] \rangle = 1$. If not, then $[5^t] = [-1]$ for some t; that is,

$5^t \equiv -1 \bmod 2^m$. Since $m \geq 3$, this congruence implies $5^t \equiv -1 \bmod 4$; but $5 \equiv 1 \bmod 4$ implies $5^t \equiv 1 \bmod 4$, a contradiction. It follows that these two cyclic subgroups generate their direct product, which is a subgroup of order at least $2 \times 2^s \geq 2 \times 2^{m-2} = 2^{m-1} = \varphi(2^m)$. This subgroup is thus all of $U(\mathbb{Z}_{2^m})$. ∎

Corollary 5.45. *Let G be a group containing elements x and y such that x has order 2^m (where $m \geq 3$), $y^2 = x^{2^r}$, and $yxy^{-1} = x^t$. Then*

$$t = \pm 1 \qquad \text{or} \qquad t = \pm 1 + 2^{m-1}.$$

In the latter two cases, G contains at least two involutions.

Proof. Since $y^2 = x^{2^r}$ commutes with x, we have

$$x = y^2 x y^{-2} = y x^t y^{-1} = x^{t^2},$$

so that $t^2 \equiv 1 \bmod 2^m$, and the congruence class $[t]$ is an element of order 2 in $U(\mathbb{Z}_{2^m})$. If $m \geq 3$, the lemma exhibits the only four such elements, and this gives the first statement.

One involution in G is $x^{2^{m-1}}$. Suppose $t = 1 + 2^{m-1}$. For any integer k,

$$(x^k y)^2 = x^k (y x^k y^{-1}) y^2 = x^{k+kt+2^r} = x^{2s},$$

where $s = k(1 + 2^{m-2}) + 2^{r-1}$. Since $m \geq 3$, $1 + 2^{m-2}$ is odd, and we can solve the congruence

$$s = k(1 + 2^{m-2}) + 2^{r-1} \equiv 0 \mod 2^{m-1}.$$

For this choice of k, we have $(x^k y)^2 = x^{2s} = x^{2^m} = 1$, so that $x^k y$ is a second involution (lest $y \in \langle x \rangle$).

Suppose that $t = -1 + 2^{m-1}$. As above, for any integer k, $(x^k y)^2 = x^{k+kt+2^r} = x^{k2^{m-1}+2^r}$. Rewrite the exponent

$$k2^{m-1} + 2^r = 2^r(k2^{m-r-1} - 1),$$

and choose k so that $k2^{m-r-1} \equiv 1 \bmod 2^{m-r}$; that is, there is an integer l with $k2^{m-r-1} - 1 = l2^{m-r}$. For this choice of k, we have

$$(x^k y)^2 = x^{2^r(k2^{m-r-1}-1)} = x^{l2^m} = 1,$$

and so G contains a second involution. ∎

Theorem 5.46. *A finite p-group G having a unique subgroup of order p is either cyclic or generalized quaternion.*

Proof. The proof is by induction on n, where $|G| = p^n$; of course, the theorem is true when $n = 0$.

Assume first that p is odd. If $n > 0$, then G has a subgroup H of index p, by Exercise 4.2, and H is cyclic, by induction. There can be no other subgroup of index p, lest G be the quaternions (Theorem 5.43), which is a 2-group. Therefore, H is the unique maximal subgroup of G, and so it contains every

proper subgroup of G. But if G is not cyclic, then $\langle x\rangle$ is a proper subgroup of G for every $x \in G$, and so $G \leq H$, which is absurd.

Assume now that G is a 2-group. If G is abelian, then Theorem 2.19 shows that G is cyclic; therefore, we may assume that G is not abelian. Let A be a maximal normal abelian subgroup of G. Since A has a unique involution, A is cyclic, by Theorem 2.19, say, $A = \langle a\rangle$. We claim that A has index 2. Assume, on the contrary, that $|G/A| \geq 4$. If G/A does not have exponent 2, then there is $Ab \in G/A$ with $b^2 \notin A$. Consider $H = \langle a, b^2\rangle < \langle a, b\rangle \leq G$. If H is abelian, then b^2 centralizes A, contradicting Theorem 5.41(ii). As H is not abelian, it must be generalized quaternion, by induction. We may thus assume that $b^2ab^{-2} = a^{-1}$. Now $\langle a\rangle \lhd G$ gives $bab^{-1} = a^i$ for some i, so that

$$a^{-1} = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^ib^{-1} = a^{i^2},$$

and $i^2 \equiv -1 \bmod 2^e$, where 2^e is the order of a. Note that $e \geq 2$, for A properly contains $Z(G)$. But there is no such congruence: if $e \geq 3$, then Theorem 5.44 shows that this congruence never holds; if $e = 2$, then -1 is not a square mod 4. It follows that G/A must have exponent 2. Since $|G/A| \geq 4$, G/A contains a copy of V. Therefore, there are elements c and d with $c, d, c^{-1}d \notin A$ and with $\langle a, c\rangle$, $\langle a, d\rangle$, and $\langle a, c^{-1}d\rangle$ proper subgroups of G. Now none of these can be abelian, lest c, d, or $c^{-1}d$ centralize A, so that all three are generalized quaternion. But there are equations $cac^{-1} = a^{-1} = dad^{-1}$, giving $c^{-1}d \in C_G(A)$, a contradiction. We conclude that $A = \langle a\rangle$ must have index 2 in G.

Choose $b \in G$ with $b^2 \in \langle a\rangle$. Replacing a by another generator of A if necessary, we may assume, by Exercise 2.20, that there is some $r \leq n - 2$ with

$$b^2 = a^{2^r}.$$

Now $bab^{-1} = a^t$ for some t, because $\langle a\rangle \lhd G$. Since G has only one involution, Corollary 5.45 gives $t = \pm 1$. But $t = 1$ says that a and b commute, so that G is abelian, hence cyclic. Therefore, we may assume that $t = -1$ and $G = \langle a, b\rangle$, where

$$a^{2^{n-1}} = 1, \qquad bab^{-1} = a^{-1}, \qquad b^2 = a^{2^r}.$$

To complete the proof, we need only show that $r = n - 2$. This follows from Theorem 5.44: since $t = -1$, we have $2^r \equiv -2^r \bmod 2^{n-1}$, so that $2^{r+1} \equiv 0 \bmod 2^{n-1}$, and $r = n - 2$. ∎

It is not unusual that the prime 2 behaves differently than odd primes.

Definition. If G is a group, the its ***Frattini subgroup*** $\Phi(G)$ is defined as the intersection of all the maximal subgroups of G.

If G is finite, then G always has maximal subgroups; if G is infinite, it may have no maximal subgroups. For example, let $G = \mathbb{Q}$, the additive group of rationals. Since G is abelian, a maximal subgroup H of G would be normal,

and so G/H would be a simple abelian group; hence G/H would be finite and of prime order. But it is easy to see that $\mathbb{Q}$ has no subgroups of finite index (it has no finite homomorphic images).

If an (infinite) group G has no maximal subgroups, one defines $\Phi(G) = G$.

It is clear that $\Phi(G)$ char G, and so $\Phi(G) \lhd G$.

Definition. An element $x \in G$ is called a ***nongenerator*** if it can be omitted from any generating set: if $G = \langle x, Y \rangle$, then $G = \langle Y \rangle$.

Theorem 5.47. *For every group G, the Frattini subgroup $\Phi(G)$ is the set of all nongenerators.*

Proof. Let x be a nongenerator of G, and let M be a maximal subgroup of G. If $x \notin M$, then $G = \langle x, M \rangle = M$, a contradiction. Therefore $x \in M$, for all M, and so $x \in \Phi(G)$. Conversely, if $z \in \Phi(G)$, assume that $G = \langle z, Y \rangle$. If $\langle Y \rangle \neq G$, then there exists a maximal subgroup M with $\langle Y \rangle \leq M$. But $z \in M$, and so $G = \langle z, Y \rangle \leq M$, a contradiction. Therefore, z is a nongenerator. ∎

Theorem 5.48. *Let G be a finite group.*

(i) **(Frattini, 1885).** *$\Phi(G)$ is nilpotent.*
(ii) *If G is a finite p-group, then $\Phi(G) = G'G^p$, where G^p is the subgroup of G generated by all pth powers.*
(iii) *If G is a finite p-group, then $G/\Phi(G)$ is a vector space over $\mathbb{Z}_p$.*

Proof. (i) Let P be a Sylow p-subgroup of $\Phi(G)$ for some p. Since $\Phi(G) \lhd G$, the Frattini argument (!) gives $G = \Phi(G)N_G(P)$. But $\Phi(G)$ consists of nongenerators, and so $G = N_G(P)$; that is, $P \lhd G$ and hence $P \lhd \Phi(G)$. Therefore, $\Phi(G)$ is the direct product of its Sylow subgroups; by Theorem 5.39, $\Phi(G)$ is nilpotent.

(ii) If M is a maximal subgroup of G, where G is now a p-group, then Theorem 5.40 gives $M \lhd G$ and $[G : M] = p$. Thus, G/M is abelian, so that $G' \leq M$; moreover, G' has exponent p, so that $x^p \in M$ for all $x \in G$. Therefore, $G'G^p \leq \Phi(G)$.

For the reverse inclusion, observe that $G/G'G^p$ is an abelian group of exponent p, hence is elementary abelian, and hence is a vector space over $\mathbb{Z}_p$. Clearly $\Phi(G/G'G^p) = 1$. If $H \lhd G$ and $H \leq \Phi(G)$, then it is easy to check that $\Phi(G)$ is the inverse image (under the natural map) of $\Phi(G/H)$ (for maximal subgroups correspond). It follows that $\Phi(G) = G'G^p$.

(iii) Since $G'G^p = \Phi(G)$, the quotient group $G/\Phi(G)$ is an abelian group of exponent p; that is, it is a vector space over $\mathbb{Z}_p$. ∎

Theorem 5.49 (Gaschütz, 1953). *For every (possibly infinite) group G, one has $G' \cap Z(G) \leq \Phi(G)$.*

Proof. Denote $G' \cap Z(G)$ by D. If $D \not\leq \Phi(G)$, there is a maximal subgroup M of G with $D \not\leq M$. Therefore, $G = MD$, so that each $g \in G$ has a factorization

$g = md$ with $m \in M$ and $d \in D$. Since $d \in Z(G)$, $gMg^{-1} = mdMd^{-1}m^{-1} = mMm^{-1} = M$, and so $M \lhd G$. By Exercise 2.58, G/M has prime order, hence is abelian. Therefore, $G' \leq M$. But $D \leq G' \leq M$, contradicting $D \nleq M$. ▩

Definition. A ***minimal generating set*** of a group G is a generating set X such that no proper subset of X is a generating set of G.

There is a competing definition in a finite group: a generating set of smallest cardinality. Notice that these two notions can be distinct. For example, let $G = \langle a \rangle \times \langle b \rangle$, where a has order 2 and b has order 3. Now $\{a, b\}$ is a minimal generating set, for it generates G and no proper subset of it generates. On the other hand, G is cyclic (of order 6) with generator ab, and so $\{ab\}$ is a minimal generating set of smaller cardinality. In a finite p-group, however, there is no such problem.

Theorem 5.50 (Burnside Basis Theorem, 1912). *If G is a finite p-group, then any two minimal generating sets have the same cardinality, namely,* dim $G/\Phi(G)$. *Moreover, every $x \notin \Phi(G)$ belongs to some minimal generating set of G.*

Proof. If $\{x_1, \ldots, x_n\}$ is a minimal generating set, then the family of cosets $\{\bar{x}_1, \ldots, \bar{x}_n\}$ spans $G/\Phi(G)$ (where $\bar{x}$ denotes the coset $x\Phi(G)$). If this family is dependent, then one of them, say $\bar{x}_1$, lies in $\langle \bar{x}_2, \ldots, \bar{x}_n \rangle$. There is thus $y \in \langle x_2, \ldots, x_n \rangle \leq G$ with $x_1 y^{-1} \in \Phi(G)$. Clearly, $\{x_1 y^{-1}, x_2, \ldots, x_n\}$ generates G, so that $G = \langle x_2, \ldots, x_n \rangle$, by Theorem 5.47, and this contradicts minimality. Therefore, $n =$ dim $G/\Phi(G)$, and all minimal generating sets have the same cardinality.

If $x \notin \Phi(G)$, then $\bar{x} \neq 0$ in the vector space $G/\Phi(G)$, and so it is part of a basis $\{\bar{x}, \bar{x}_2, \ldots, \bar{x}_n\}$. If x_i represents the coset $\bar{x}_i$, for $i \geq 2$, then $G = \langle \Phi(G), x, x_2, \ldots, x_n \rangle = \langle x, x_2, \ldots, x_n \rangle$. Moreover, $\{x, x_2, \ldots, x_n\}$ is a minimal generating set, for the cosets of a proper subset do not generate $G/\Phi(G)$. ▩

EXERCISES

5.52. Every subgroup of $\mathbf{Q}_n$ is either cyclic or generalized quaternion.

5.53 **(Wielandt).** A finite group G is nilpotent if and only if $G' \leq \Phi(G)$.

5.54. If G is a finite p-group, then G is cyclic if and only if $G/\Phi(G)$ is cyclic.

Definition. A finite p-group G is ***extra-special*** if $Z(G)$ is cyclic and $\Phi(G) = Z(G) = G'$.

5.55. If G is extra-special, then $G/Z(G)$ is an elementary abelian group.

5.56. Every nonabelian group of order p^3 is extra-special.

5.57. (i) If m is a power of 2, what is the class of nilpotency of D_{2n}?
(ii) What is the class of nilpotency of $\mathbf{Q}_n$? (*Hint.* Exercise 4.42.)