CHAPTER 6

Further Topics in Group Theory

6.1 p-GROUPS, NILPOTENT GROUPS, AND SOLVABLE GROUPS

Let p be a prime and let G be a finite group of order $p^a n$, where p does not divide n. Recall that a (finite) p-group is any group whose order is a power of p. Sylow's Theorem shows that p-groups abound as subgroups of G and in order to exploit this phenomenon to unravel the structure of finite groups it will be necessary to establish some basic properties of p-groups. In the next section we shall apply these results in many specific instances.

Before giving the results on p-groups we first recall a definition that has appeared in some earlier exercises.

Definition. A *maximal subgroup* of a group G is a proper subgroup M of G such that there are no subgroups H of G with $M < H < G$.

By order considerations every proper subgroup of a finite group is contained in some maximal subgroup. In contrast, infinite groups may or may not have maximal subgroups. For example, $p\mathbb{Z}$ is a maximal subgroup of $\mathbb{Z}$ whereas $\mathbb{Q}$ (under +) has no maximal subgroups (cf. Exercise 16 at the end of this section).

We now collect all the properties of p-groups we shall need into an omnibus theorem:

Theorem 1. Let p be a prime and let P be a group of order p^a, $a \geq 1$. Then

(1) The center of P is nontrivial: $Z(P) \neq 1$.

(2) If H is a nontrivial normal subgroup of P then H intersects the center nontrivially: $H \cap Z(P) \neq 1$. In particular, every normal subgroup of order p is contained in the center.

(3) If H is a normal subgroup of P then H contains a subgroup of order p^b that is normal in P for each divisor p^b of $|H|$. In particular, P has a normal subgroup of order p^b for every $b \in \{0, 1, \ldots, a\}$.

(4) If $H < P$ then $H < N_P(H)$ (i.e., every proper subgroup of P is a proper subgroup of its normalizer in P).

(5) Every maximal subgroup of P is of index p and is normal in P.

Proof: These results rely ultimately on the class equation and it may be useful for the reader to review Section 4.3.

Part 1 is Theorem 8 of Chapter 4 and is also the special case of part 2 when $H = P$. We therefore begin by proving (2); we shall not quote Theorem 8 of Chapter 4 although the argument that follows is only a slight generalization of the one in Chapter 4. Let H be a nontrivial normal subgroup of P. Recall that for each conjugacy class C of P, either $C \subseteq H$ or $C \cap H = \emptyset$ because H is normal (this easy fact was shown in a remark preceding Theorem 4.12). Pick representatives of the conjugacy classes of P:

$$a_1, a_2, \ldots, a_r$$

with $a_1, \ldots, a_k \in H$ and $a_{k+1}, \ldots, a_r \notin H$. Let C_i be the conjugacy class of a_i in P, for all i. Thus

$$C_i \subseteq H, \quad 1 \leq i \leq k \qquad \text{and} \qquad C_i \cap H = \emptyset, \quad k+1 \leq i \leq r.$$

By renumbering $a_1, \ldots, a_k$ if necessary we may assume $a_1, \ldots, a_s$ represent classes of size 1 (i.e., are in the center of P) and $a_{s+1}, \ldots, a_k$ represent classes of size > 1. Since H is the disjoint union of these we have

$$|H| = |H \cap Z(P)| + \sum_{i=s+1}^{k} \frac{|P|}{|C_P(a_i)|}.$$

Now p divides $|H|$ and p divides each term in the sum $\sum_{i=s+1}^{k} |P : C_P(a_i)|$ so p divides their difference: $|H \cap Z(P)|$. This proves $H \cap Z(P) \neq 1$. If $|H| = p$, since $H \cap Z(P) \neq 1$ we must have $H \leq Z(P)$. This completes the proof of (2).

Next we prove (3) by induction on a. If $a \leq 1$ or $H = 1$, the result is trivial. Assume therefore that $a > 1$ and $H \neq 1$. By part 2, $H \cap Z(P) \neq 1$ so by Cauchy's Theorem $H \cap Z(P)$ contains a (normal) subgroup Z of order p. Use bar notation to denote passage to the quotient group P/Z. This quotient has order p^{a-1} and $\overline{H} \trianglelefteq \overline{P}$. By induction, for every nonnegative integer b such that p^b divides $|\overline{H}|$ there is a subgroup $\overline{K}$ of $\overline{H}$ of order p^b that is normal in $\overline{P}$. If K is the complete preimage of $\overline{K}$ in P then $|K| = p^{b+1}$. The set of all subgroups of H obtained by this process together with the identity subgroup provides a subgroup of H that is normal in P for each divisor of $|H|$. The second assertion of part 3 is the special case $H = P$. This establishes part 3.

We prove (4) also by induction on $|P|$. If P is abelian then all subgroups of P are normal in P and the result is trivial. We may therefore assume $|P| > p$ (in fact, $|P| > p^2$ by Corollary 4.9). Let H be a proper subgroup of P. Since all elements of $Z(P)$ commute with all elements of P, $Z(P)$ normalizes every subgroup of P. By part 1 we have that $Z(P) \neq 1$. If $Z(P)$ is not contained in H, then H is properly contained in $\langle H, Z(P) \rangle$ and the latter subgroup is contained in $N_P(H)$ so (4) holds. We may therefore assume $Z(P) \leq H$. Use bar notation to denote passage to the quotient $P/Z(P)$. Since $\overline{P}$ has smaller order than P by (1), by induction $\overline{H}$ is properly contained in $N_{\overline{P}}(\overline{H})$. It follows directly from the Lattice Isomorphism Theorem that $N_P(H)$ is the complete preimage in P of $N_{\overline{P}}(\overline{H})$, hence we obtain proper containment of H in its normalizer in this case as well. This completes the induction.

To prove (5) let M be a maximal subgroup of P. By definition, $M < P$ so by part 4, $M < N_P(M)$. By definition of maximality we must therefore have $N_P(M) = P$, i.e., $M \trianglelefteq P$. The Lattice Isomorphism Theorem shows that P/M is a p-group with no proper nontrivial subgroups because M is a maximal subgroup. By part 3, however,

P/M has subgroups of every order dividing $|P/M|$. The only possibility is $|P/M| = p$. This proves (5) and completes the proof of the theorem.

Definition.

(1) For any (finite or infinite) group G define the following subgroups inductively:

$$Z_0(G) = 1, \qquad Z_1(G) = Z(G)$$

and $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

(i.e., $Z_{i+1}(G)$ is the complete preimage in G of the center of $G/Z_i(G)$ under the natural projection). The chain of subgroups

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

is called the *upper central series of* G. (The use of the term "upper" indicates that $Z_i(G) \leq Z_{i+1}(G)$.)

(2) A group G is called *nilpotent* if $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest such c is called the *nilpotence class* of G.

One of the exercises at the end of this section shows that $Z_i(G)$ is a characteristic (hence normal) subgroup of G for all i. We use this fact freely from now on.

Remarks:

(1) If G is abelian then G is nilpotent (of class 1, provided $|G| > 1$), since in this case $G = Z(G) = Z_1(G)$. One should think of nilpotent groups as lying between abelian and solvable groups in the hierarchy of structure (recall that solvable groups were introduced in Section 3.4; we shall discuss solvable groups further at the end of this section):

cyclic groups $\subset$ *abelian groups* $\subset$ *nilpotent groups* $\subset$ *solvable groups* $\subset$ *all groups*

(all of the above containments are proper, as we shall verify shortly).

(2) For any finite group there must, by order considerations, be an integer n such that

$$Z_n(G) = Z_{n+1}(G) = Z_{n+2}(G) = \cdots.$$

For example, $Z_n(S_3) = 1$ for all $n \in \mathbb{Z}^+$. Once two terms in the upper central series are the same, the chain stabilizes at that point (i.e., all terms thereafter are equal to these two). For example, if $G = Z_2 \times S_3$,

$$Z(G) = Z_1(G) = Z_2(G) = Z_n(G) \quad \text{has order 2 for all } n.$$

By definition, $Z_n(G)$ is a proper subgroup of G for all n for non-nilpotent groups.

(3) For infinite groups G it may happen that all $Z_i(G)$ are proper subgroups of G (so G is not nilpotent) but

$$G = \bigcup_{i=0}^{\infty} Z_i(G).$$

Groups for which this hold are called *hypernilpotent* — they enjoy some (but not all) of the properties of nilpotent groups. While we shall be dealing mainly with finite nilpotent groups, results that do not involve the notion of order, Sylow subgroups etc. also hold for infinite groups. Even for infinite groups one of the main techniques for dealing with nilpotent groups is induction on the nilpotence class.

Proposition 2. Let p be a prime and let P be a group of order p^a. Then P is nilpotent of nilpotence class at most $a - 1$.

Proof: For each $i \geq 0$, $P/Z_i(P)$ is a p-group, so

$$\text{if } |P/Z_i(P)| > 1 \text{ then } Z(P/Z_i(P)) \neq 1$$

by Theorem 1(1). Thus if $Z_i(P) \neq G$ then $|Z_{i+1}(P)| \geq p|Z_i(P)|$ and so $|Z_{i+1}(P)| \geq p^{i+1}$. In particular, $|Z_a(P)| \geq p^a$, so $P = Z_a(P)$. Thus P is nilpotent of class $\leq a$. The only way P could be of nilpotence class exactly equal to a would be if $|Z_i(P)| = p^i$ for all i. In this case, however, $Z_{a-2}(P)$ would have index p^2 in P, so $P/Z_{a-2}(P)$ would be abelian (by Corollary 4.9). But then $P/Z_{a-2}(P)$ would equal its center and so $Z_{a-1}(P)$ would equal P, a contradiction. This proves that the class of P is $\leq a - 1$.

Example

Both D_8 and Q_8 are nilpotent of class 2. More generally, D_{2^n} is nilpotent of class $n - 1$. This can be proved inductively by showing that $|Z(D_{2^n})| = 2$ and $D_{2^n}/Z(D_{2^n}) \cong D_{2^{n-1}}$ for $n \geq 3$ (the details are left as an exercise). If n is not a power of 2, D_{2n} is not nilpotent (cf. Exercise 10).

We now give some equivalent (and often more workable) characterizations of nilpotence for *finite* groups:

Theorem 3. Let G be a finite group, let $p_1, p_2, \ldots, p_s$ be the distinct primes dividing its order and let $P_i \in Syl_{p_i}(G)$, $1 \leq i \leq s$. Then the following are equivalent:

(1) G is nilpotent

(2) if $H < G$ then $H < N_G(H)$, i.e., every proper subgroup of G is a proper subgroup of its normalizer in G

(3) $P_i \trianglelefteq G$ for $1 \leq i \leq s$, i.e., every Sylow subgroup is normal in G

(4) $G \cong P_1 \times P_2 \times \cdots \times P_s$.

Proof: The proof that (1) implies (2) is the same argument as for p-groups — the only fact we needed was if G is nilpotent then so is $G/Z(G)$ — so the details are omitted (cf. the exercises).

To show that (2) implies (3) let $P = P_i$ for some i and let $N = N_G(P)$. Since $P \trianglelefteq N$, Corollary 4.20 gives that P is characteristic in N. Since P char $N \trianglelefteq N_G(N)$ we get that $P \trianglelefteq N_G(N)$. This means $N_G(N) \leq N$ and hence $N_G(N) = N$. By (2) we must therefore have $N = G$, which gives (3).

Next we prove (3) implies (4). For any t, $1 \leq t \leq s$ we show inductively that

$$P_1 P_2 \cdots P_t \cong P_1 \times P_2 \times \cdots \times P_t.$$