3 \textit{p-groups}

A \textit{p-group} is a finite group \( P \) of order \( p^k \) where \( k \geq 0 \). Note that every subgroup of a \( p \)-group is a \( p \)-group. When we want to exclude the trivial case \( k = 0 \) we say that \( P \) is a \textit{nontrivial} \( p \)-group. One of the most important properties of \( p \)-groups is that they have nontrivial centers:

\textbf{Theorem 3.1.} Every nontrivial \( p \)-group has a nontrivial center \(( P \neq 1 \Rightarrow Z(P) \neq 1)\). Furthermore, every nontrivial normal subgroup \( N \) of \( P \) meets \( Z(P) \) nontrivially \(( 1 \neq N \leq P \Rightarrow N \cap Z(P) \neq 1)\).

\textit{Proof.} The second statement implies the first statement. So suppose that \( N \) is a nontrivial normal subgroup of \( P \). Then \( |N| \) is divisible by \( p \). The group \( P \) acts on the set \( N \) by conjugation:

\[ g \cdot x = gxg^{-1} \]

This action has a fixed point, namely \( x = 1 \). [\( x \) is a \textit{fixed point} if \( g \cdot x = x \) for all \( g \) in the group. When the action is conjugation this is the same as saying that \( x \) commutes with every element of the group, i.e., \( x \in Z(P) \cap N \).]

However, we know that the number of fixed points is congruent modulo \( p \) to \( |N| \) which is congruent to 0. Therefore there must be at least \( p \) fixed points so \( |Z(P) \cap N| \geq p \). \( \square \)

\textbf{Corollary 3.2.} Given a \( p \)-group \( P \) of order \( p^k \) there exists an increasing sequence of normal subgroups

\[ 1 \triangleleft N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_{k-1} \triangleleft P \]

so that \( |N_j| = p^j \) for all \( j \).

\textit{Proof.} If \( k = 1 \) there is nothing to prove so suppose that \( k \geq 2 \). By the theorem we know that the center of \( P \) is nontrivial. By Cauchy’s Theorem we know that \( Z(P) \) contains an element of order \( p \). Let \( N_1 \) be the cyclic subgroup of \( P \) generated by this central element. Then \( N_1 \triangleleft P \) and \( |N_1| = p \) so \( P/N_1 \) is a \( p \)-group of order \( p^{k-1} \). By induction \( P/N_1 \) has a normal series as above. The preimage in \( P \) of this normal series (together with \( N_1 \)) forms the desired normal series for \( P \). \( \square \)

\textbf{Corollary 3.3.} Every maximal proper subgroup of a \( p \)-group \( P \) is normal and has index \( p \).

\textit{Proof.} First of all note that if a proper subgroup \( M < P \) is maximal and normal then its index must be \( p \) since otherwise, by the corollary above, \( P/M \) has a subgroup of index \( p \) which corresponds to a subgroup \( Q \) of \( P \) so that \( M < Q < P \). Thus it suffices to show that every maximal proper subgroup of \( P \) is normal.

Take \( M < P \) maximal and let \( Z < P \) be a central subgroup of order \( p \). There are two cases.
1. If \( Z \subseteq M \) then \( M/Z < P/Z \) is maximal and thus normal by induction on \( |P| \). This implies \( M \lhd P \).

2. If \( Z \not\subseteq M \) then \( P = ZM = N(M) \) so \( M \lhd P \).

Given any group \( G \) its center \( Z(G) \) is an abelian normal subgroup of \( G \). For a \( p \)-group \( P \), \( Z(P) \) must be a product of cyclic \( p \)-groups. But what about \( P/Z(P) \)?

**Lemma 3.4.** For any group \( G \) the quotient \( G/Z(G) \) cannot be a nontrivial cyclic group. In particular \( |G : Z(G)| \) cannot be prime.

**Proof.** Suppose that \( G/Z(G) \) is a cyclic group generated by the element \( \bar{x} = xZ(G) \). Then the powers of \( x \) give a complete set of coset representative so every element of \( G \) can be written in the form \( g = x^nz \) where \( z \in Z(G) \). But then \( G \) is abelian and \( Z(G) = G \). \( \square \)

Combine this with Theorem 3.1 and we see that any group of order \( p^2 \) is abelian. [So it must be either \( \mathbb{Z}/p^2 \) or \( \mathbb{Z}/p \times \mathbb{Z}/p \).]

**Proposition 3.5.** Every nonabelian \( p \)-group has at least \( p^3 \) elements and the index of its center is at least \( p^2 \).

An example of a nonabelian 2-group of order \( 2^3 = 8 \) is the **Dihedral group** \( D_8 \) which is define to be a group having 8 elements:

\[
D_8 = \{1, s, s^2, s^3, t, ts, ts^2, ts^3\}
\]

where \( t^2 = 1 = s^4 \) and \( tst = s^{-1} = s^3 \). A permutation representation of this group is given by: \( s = (1234), t = (14)(23) \). A geometric representation of \( D_8 \) is given by taking the symmetries of a square. A matrix representation is given by

\[
s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\]

The center is \( D_8 \) is \( Z(D_8) = \langle s^2 \rangle = \{1, s^2\} \). (Prove it!) Note that the square of every element of \( D_8 \) is either \( s^2 \) or 1. This example can be generalized.

For any prime \( p \) let \( P \) be the group of order \( p^3 \) whose elements are given by \( a^ib^j \) where \( 0 \leq i < p^2 \) and \( 0 \leq j < p \) subject to the relations \( a^{p^2} = 1, b^p = 1 \) and \( bab^{-1} = a^{p+1} \). In other words, the multiplication rule in \( P \) is given by:

\[
(a^ib^j)(a^kb^\ell) = a^{i+k+jp}b^{j+\ell}
\]

Then the center of \( P \) is generated by \( a^p \).

There are exactly two nonisomorphic nonabelian groups of order \( p^3 \). Alperin-Bell prove this in the case of odd primes\(^1\) and Rotman proves this

---

\(^1\)For an odd prime \( p \) the second nonabelian group of order \( p^3 \) has the property that every nontrivial element has order \( p \) [AB, Prop 8.11]. We will discuss this example later.
for $p = 2$. For $p = 2$ the other group is the group of **quaternions**. This is defined to be the group $Q$ generated by $a, b$ subject to the relations $a^4 = 1$, $b^2 = a^2$ and $bab^{-1} = a^{-1} = a^3$. If we let $c = ab$ we get a familiar list of identities:

$$ab = c, \ bc = a, \ ca = b, \ ba = c^{-1}, \ ac = b^{-1}, \ cb = a^{-1}$$

These are six of the elements of $Q$. They all have order 4. The other two are $1$ and $a^2 = b^2 = c^2$ which has order 2.

**Theorem 3.6.** Every nonabelian group of order 8 is isomorphic to either $D_8$ or $Q$.

**Proof.** Let $P$ be a nonabelian group of order 8. We know that $P$ contains an element of order 4. [Otherwise all nontrivial elements of $P$ have order 2, making $P$ abelian.] Call that element $a$ and let $A = \langle a \rangle = \{1, a, a^2, a^3\}$ be the subgroup generated by $a$. Then $A$ is normal since it has index 2. Let $b$ be any element of $P - A$. Then $\phi_b(a) = bab^{-1} = a^3$. [Since $\phi_b$ is an automorphism, it take elements of order 4 to elements of order 4 and $a^2$ has order 2. Also $bab^{-1} \neq a$ since this would make $P$ abelian.]

Since $b^2 \in A$ there are two cases. Either $b^2 = 1$ or $b^2 = a^2$. [$b^2$ cannot be $a$ or $a^3$ since that would make $P$ cyclic and thus abelian.] In the first case, $P$ is isomorphic to $D_8$ with $a, b$ mapping to $s, t$. It the second case $P$ is isomorphic to $Q$ with $a, b$ mapping to elements of $Q$ with the same name. \(\square\)

**Elementary abelian $p$-groups**

A $p$-group is called **elementary abelian** if it is abelian and every nontrivial element has order $p$.\(^2\) This is the same as saying that $P$ is a $\mathbb{Z}/p$-module.\(^3\) Since $\mathbb{Z}/p$ is a fields, $P$ is a vector space over $\mathbb{Z}/p$. Thus we get the following.

**Theorem 3.7.** Suppose that $P$ is an elementary abelian group of order $p^n$. Then

1. $P \cong (\mathbb{Z}/p)^n = \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$
2. Every minimal generating set for $P$ has $n$ elements.

**Exercise 1:** If $P$ is a nonabelian group of order $p^3$ then show that $P/Z(P)$ is elementary abelian of order $p^2$.

**Exercise 2:** Let $\Phi(P)$ be the intersection of all maximal subgroups of a $p$-group $P$. [$\Phi(P)$ is called the **Frattini subgroup** $P$.] Show that $P/\Phi(P)$ is elementary abelian.

---

\(^2\)If $p = 2$ the second statement implies the first, i.e., if every nontrivial element has order 2 the group is abelian. For odd $p$ this is not true. [See the previous footnote.]

\(^3\)A $\mathbb{Z}/n$-module is an abelian group in which every element has order dividing $n$. 

3