Groups of prime-power order

**Definition** Let $p$ be a prime. A finite group $G$ is a $p$-group if $|G|$ is a power of $p$.

For example, $D_8$ is a 2-group.

Lagrange’s Theorem shows that if $G$ is a $p$-group and $g$ is an element of $G$ then the order of $g$ is a power of $p$.

**Theorem** If $G$ is a non-trivial finite $p$-group for some prime $p$ then $Z(G) \neq \{1_G\}$.

**Proof** Let $|G| = p^n$ for some $n \geq 1$. Every conjugacy class in $G$ has size dividing $p^n$, so has size $p^r$ for some $r \leq n$. Suppose that there are $m_r$ conjugacy classes of size $p^r$ for $r = 0, 1, \ldots, n$. Then

$$m_0 1 + m_1 p + m_2 p^2 + \cdots + m_r p^r + \cdots + m_n p^n = p^n,$$

so $p$ divides $m_0$. But $\{x\}$ is a whole conjugacy class of size 1 if and only if $x \in Z(G)$, so $m_0 = |Z(G)|$: therefore $m_0 \neq 0$, because $\{1_G\} \leq Z(G)$. So $|Z(G)|$ is a non-zero multiple of $p$, and therefore $|Z(G)| \geq p$. □

(Compare this with the proof of Cauchy’s Theorem.)

**Corollary** If $G$ is a finite group of order $p^n$, where $p$ is prime, then there are subgroups

$$\{1_G\} = G_0 < G_1 < \cdots < G_n = G$$

such that $|G_i| = p^i$ and $G_i \leq G$ for $i = 0, \ldots, n$.

**Proof** The proof is by induction on $n$. The statement is true when $n = 1$, for then $G_0 = \{1_G\}$ and $G_1 = G$. 

1
Now take \( n \geq 2 \), and assume that the statement is true for \( n - 1 \). The theorem says that \( Z(G) \neq \{1_G\} \), so \( p \) divides \( |Z(G)| \). By Cauchy’s Theorem, \( Z(G) \) has an element \( z \) of order \( p \). Put \( G_1 = \langle z \rangle \). Then \( G_1 \leq G \), because \( G_1 \leq Z(G) \). Also, \( |G_1| = p \).

Put \( H = G/G_1 \). Then \( |H| = p^n/p = p^{n-1} \), so by the inductive hypothesis \( H \) has subgroups

\[
\{1_H\} = H_0 < H_1 < \cdots < H_{n-1} = H
\]

with \( |H_i| = p^i \) and \( H_i \leq H \) for \( i = 0, \ldots, n - 1 \). By the Correspondence Theorem, there is a subgroup \( G_{i+1} \) of \( G \) containing \( G_1 \) such that \( G_{i+1}/G_1 = H_i \) and \( G_{i+1} \leq G \) for \( i = 0, \ldots, n - 1 \). Moreover, \( |G_{i+1}| = |G_1| \times |H_i| = p^{i+1} \) for \( i = 0, \ldots, n - 1 \). Finally, the Correspondence Theorem shows that \( G_i \leq G_{i+1} \) for \( i = 0, \ldots, n - 1 \). \( \square \)

\begin{center}
\begin{tikzpicture}
  \node (G) at (0,0) {$G$};
  \node (H) at (2,0) {$H$};
  \node (G1) at (0,-1) {$G_1$};
  \node (G2) at (1,-1) {$G_2$};
  \node (H1) at (1,1) {$H_1$};
  \node (H0) at (1,-2) {$H_0 = \{1_H\}$};
  \node (1H) at (0,-4) {$\{1_G\}$};
  \draw (G) -- (H); \draw (G1) -- (G2); \draw (G1) -- (1H); \draw (G2) -- (H1); \draw (H0) -- (1H); \draw (H0) -- (H1);
\end{tikzpicture}
\end{center}

**Theorem** If \( G \) is Abelian then \( Z(G) = G \); otherwise, \( G/Z(G) \) is not cyclic.

**Proof** Part of the coursework.
**Small $p$-groups**

Let $p$ be a prime. If $|G| = p$ then $G$ is cyclic, because Lagrange’s Theorem shows that every element of $G$ other than the identity has order $p$.

If $|G| = p^2$ then $|Z(G)|$ is 1 or $p$ or $p^2$. We have just proved that $|Z(G)| \neq 1$. If $|Z(G)| = p$ then $|G/Z(G)| = p$ so $G/Z(G)$ is cyclic, contradicting the above theorem: hence $|Z(G)| \neq p$. Therefore $Z(G) = G$ and so $G$ is Abelian.

If $G$ has an element of order $p^2$ then it is cyclic. Otherwise, all non-identity elements have order $p$. Let $a$ be an element of order $p$, and put $A = \langle a \rangle$. Choose any element $b$ in $G \setminus A$. Then $b$ also has order $p$. Put $B = \langle b \rangle$. Now $A \cap B \leq B$; and $A \cap B$ cannot be $B$, because $b \notin A$, so $A \cap B = \{1_G\}$. Moreover, $xy = yx$ for all $x$ in $A$ and all $y$ in $B$, because $G$ is Abelian. Therefore $G$ contains the internal direct product $\langle a \rangle \times \langle b \rangle$. Because of the uniqueness of the expression of an element of an internal direct product,

$$\langle a \rangle \times \langle b \rangle = \{a^nb^m : 0 \leq n \leq p-1, 0 \leq m \leq p-1\},$$

and these $p^2$ products are all distinct. Therefore $G = \langle a \rangle \times \langle b \rangle$.

**Challenge!**

Find all groups of order 8.

**Infinite $p$-groups**

What could an infinite $p$-group be? Here is an example of an infinite group in which every element has order a power of the prime 2. We work inside the infinite Abelian group $(\mathbb{C} \setminus \{0\}, \times)$. Put

$$G = \{e^{2\pi i m/2^n} : n \in \mathbb{Z}, n \geq 0, m \in \mathbb{Z}\}.$$ 

Then $G$ contains elements of order $2^n$ for all non-negative integers $n$. 

3