In this series of exercises we will classify all groups of order $2p$, where $p$ is an odd prime.

1. Assume $G$ is a group of order $2p$, where $p$ is an odd prime. If $a \in G$, show that $a$ must have order 1, 2, $p$, or $2p$.

   \textit{Proof.} Let $a \in G$. By Lagrange, the order of $a$ divides the order of the group. Therefore $|a| | 2p$. Since the divisors of $2p$ are 1, 2, $p$, and $2p$, then $a$ must have order 1, 2, $p$, or $2p$. \hfill \square

2. Suppose that $G$ has an element of order $2p$. Prove that $G$ isomorphic to $\mathbb{Z}_{2p}$.

   \textit{Proof.} If $a$ has order $2p$, then $G = \langle a \rangle$. Therefore $G$ is cyclic of order $2p$ so it is isomorphic to $\mathbb{Z}_{2p}$. \hfill \square

\textbf{From now on, suppose $G$ is not cyclic:}


   \textit{Proof.} Let 1 be the identity of $G$. Since $G$ is not cyclic and $G$ has no element of order $p$, if $a \in G$ and $a$ is not the identity, then the order of $a$ is 2. But this is true for all non-identity elements of $G$. This implies that $G$ is abelian (we proved this in a homework exercise from Chapter 3). Since $|G| = 2p$ and $p$ is an odd prime, then $|G| \geq 6$. So it must have at least 5 non-identity elements. Let $a$ and $b$ be two distinct non-identity elements of $G$. Then $a$ and $b$ have order 2. Now $ab \in G$. $ab \neq a$ because $(ab = a) \rightarrow (b = 1)$ by the left-cancellation law. $ab \neq b$ because $(ab = b) \rightarrow (a = 1)$ by the right-cancellation law. We know $a^2 = 1$, therefore if $ab = 1$, then $ab = a^2$ so $b = a$ by the left-cancellation law. Since $b \neq a$, then $ab \neq 1$. Therefore 1, $a$, $b$, $ab$ are all distinct elements. Consider the set $\{1, a, b, ab\}$. Note that $a \cdot b = ab \in G$, $a \cdot (ab) = a^2b = b \in G$ and $b \cdot (ab) = b(ab) = b(ba) = b^2a = a \in G$. For the last one we used that $G$ is abelian. So the operation is closed in $\{1, a, b, ab\}$, every element has inverses (the inverse of each element is itself) and it contains the identity. Therefore $\{1, a, b, ab\}$ is a subgroup of $G$. But then by Lagrange, that means that $4|(2p)$, so $2|p$, so $p$ is even. But $p$ is odd. Therefore we’ve reached a contradiction. Hence, there must be an element of order $> 2$. Since $G$ is not cyclic and it doesn’t have elements of order $2p$, there must be an element of order $p$. \hfill \square

4. Let $z$ be an element of order $p$. Let $P = \langle z \rangle$. Show that if $g \notin P$, then $g$ has order 2.
5. Let \( P \in G \) such that \( g \notin P \). Since \(|P| = p\), then there are two cosets of \( P \) in \( G \). Since \( g \notin P \), then \( gP \neq P \), therefore one coset is \( P \) and the other is \( gP \). We know \( P \cup gP = G \). So we have:

\[
P = \{1, z, z^2, z^3, \ldots, z^{p-1}\},
\]
\[
gP = \{g, gz, gz^2, gz^3, \ldots, gz^{p-1}\}.
\]

Now, \( P \) has index 2 in \( G \), therefore if \( a \notin P \) and \( b \notin P \), then \( ab \in P \). Hence if \( a \notin P \), then \( a^2 \in P \). Since \( g \) is not the identity and \( G \) is not cyclic, then the order of \( g \) is either 2 or \( p \). For the sake of contradiction suppose the order is not 2. Then the order of \( g \) is \( p \). We know \( g^2 \in P \) so there exists an integer \( k \) such that \( g^2 = z^k \). But \( g^2 \neq 1 \) (since we’re assuming that \( g \) does not have order 2) so \( 1 \leq k \leq p - 1 \). But \( \langle z^k \rangle = \langle z \rangle \) for any \( 1 \leq k \leq p - 1 \) because \( k \) is relatively prime to \( p \). Therefore \( \langle g^2 \rangle = P \). But because \( p \) is odd and \( g^2 \neq 1 \), then \( \langle g^2 \rangle = \langle g \rangle \). Therefore if \( g \) has order \( p \), then \( g \) must be an element of \( P \). But \( g \) is not an element of \( P \). Therefore \( g \) has order 2.

\[\Box\]

6. Let \( P \) be a subgroup of \( G \) with order \( p \) and \( y \in G \) have order 2. Show that \( yP = Py \).

**Proof.** Since the \([G : P] = 2\), then by exercise 18 in chapter 6 (from Homework 5), \( yP = Py \). The key of the proof is that if \( y \in P \), then \( yP = P = Py \) and if \( y \notin P \) then \( yP \neq P \) so it is the second coset. Similarly \( Py \neq P \) so \( Py \) is the second coset. So \( Py = yP \).

\[\Box\]

From now on, let \( z \in G \) be an element of order \( p \) and \( y \in G \) be an element of order 2.

7. Let \( P = \langle z \rangle \) is a subgroup of order \( p \) generated by \( z \). If \( y \) is an element of order 2, then \( yz = z^{p-1}y = z^{-1}y \).

**Proof.** First, let’s note that \( y \notin P \). Indeed every non-identity element in \( P \) has order \( p \) and the identity has order 1. Therefore \( y \notin P \). Now, since \( yP = Py \) and \( yz \in yP \), then \( yz \in Py \), therefore there exists an integer \( k \) such that \( yz = z^k y \) and \( 1 \leq k \leq p \) (because an element of \( P \) is an element of the form \( z^k \) with \( 1 \leq k \leq p \)). Suppose \( k = p \), then \( yz = z^py = y \). Therefore \( z = 1 \), but \( z \) has order \( p \), so it is not 1. Therefore \( k \neq p \). Therefore \( 1 \leq k < p \).

To finish, we need only show that \( k \neq 1 \). Suppose \( k = 1 \), then \( yz = zy \). Since \( yz \notin P \), then \( yz \) has order 2, then \( (yz)^2 = 1 \). But

\[
(yz)^2 = (zy)(yz) = zy^2z = z^2.
\]

So \( z^2 = 1 \), but that contradicts that \( z \) has order \( p \). Therefore \( yz \neq zy \), so \( k \neq 1 \).

A similar idea will prove that \( k = p - 1 \). Suppose \( yz = z^{k}y \). We know \( (yz)^2 = 1 \) on the one hand but

\[
(yz)^2 = (z^k y)(yz) = z^k(y^2)z = z^{k+1}.
\]

Therefore \( z^{k+1} = 1 \). But \( z \) has order \( p \), therefore \( k + 1 \equiv 0 \mod p \). Since \( 1 < k \geq p - 1 \), then \( k = p - 1 \).

\[\Box\]

8. Show that we can list the elements of \( G \) as \( \{y^iz^j \mid 0 \leq i \leq 1, 0 \leq j \leq p - 1\} \).

\[\Box\]
Proof. Let \( x \in G \). Then either \( x \in P \) or \( x \in yP \). If \( x \in P \), then \( x = z^k = y^0 z^k \) for some integer \( k \) such that \( 0 \leq k \leq p - 1 \). If \( x \in yP \), then \( x = yz^k = y^1 z^k \) for some integer \( k \) such that \( 0 \leq k \leq p - 1 \). But that is exactly what we want to prove.

\[ \square \]

9. Prove that \( G \) is isomorphic to the dihedral group \( D_p \).

Proof. We know \( G = \{1, z, z^2, z^3, \ldots, z^{p-1}, y, yz, yz^2, \ldots, yz^{p-1}\} \). We know that \( z^p = 1 \) and that \( y^2 = 1 \). We also know that \( yz = z^{-1}y \). Now \( D_p = \{1, r, r^2, \ldots, r^{p-1}, s, sr, sr^2, \ldots, s r^{p-1}\} \) satisfying that \( r^p = 1, s^2 = 1 \) and \( sr = r^{-1}s \). \( G \) and \( D_p \) look identical (and satisfy the same equations) if one changes the variable \( z \rightarrow r \) and \( y \rightarrow s \). \( y \) is the reflection and \( z \) is the rotation in other words. The three important equations of the dihedral group are satisfied and the elements of each set clearly match one to one. Therefore \( G \cong D_p \).

\[ \square \]