ABSTRACT: The structure of groups plays an important role in the study of the nature of the groups. We examine some basic properties and structural characteristics of the dihedral group of degree $n$, where $n$ is a natural number, by group-theoretic approach. We begin the exploration by providing a foundational understanding of dihedral groups, elucidating their definitions and essential properties. Furthermore, we investigated the algebraic and geometric aspects of these groups, highlighting their role in describing symmetries of $n$-gons and other mathematical entities. Special attention is given to the distinctive features that differentiate dihedral groups from other algebraic structures. The analytic expressions for the order of subgroups are obtained and the commutativity investigated. The groups are all represented for further analysis and applications.

KEYWORDS: Algebraic Structure, Permutation Group, Dihedral Group, Subgroups, Isomorphism, Generators
INTRODUCTION

Background of the Study

A group is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property. Until the mid nineteenth century, the concept of a group was essentially that of a permutation group, and even though we now have a more abstract concept of a group, it is the simple result of Cayley’s theory that any group can be embedded into a permutation group (Cayley, 1844). Although it is often less beneficial to study groups within this framework, permutation groups are still quite important and not only appear in many other branches of mathematics (for example, combinatorics) but also form an active field of research today. Although group theory is a mathematical subject, it is indispensable to many areas of modern theoretical physics, from atomic physics to condensed matter physics, particle physics to string theory. In this work, we shall focus on a subset of symmetric group called the Dihedral group. In mathematics, a dihedral group is the group of symmetries of an n-sided regular polygon for n > 1, which includes rotations and reflections. Dihedral group is denoted as $D_n$. According to Conrad (2018 and 2018b) the order of the Dihedral group is $2n$ and every rotation in the dihedral group is conjugate to its inverse. Dihedral groups are among the simplest examples of finite groups, and they play an important role in group theory, geometry, and chemistry. Jaume et al, (2017) gave a new classification of the infinite dihedral groups, and they showed that a complete classification of all representations can be described by a system of numerical invariants for the dihedral group of rank 2. Müller (2013) proved that it is only dihedral group which does not admit any outer automorphisms among the various types of groups. A dihedral group is simply a group of rotations and reflections for a regular polygon, the dihedral group for n-polygon is denoted by $D_{2n}$, where the order of this group is the number of rotations and reflections for the vertices of n-polygon. That is by determining the symmetric axes (which depends on whether n is odd or even), and then find the reflections and rotations in term of each symmetric axis. The number of distinct rotations is n which is also the number of distinct reflections, so $|D_n| = 2n$, this is why we use the notation $D_{2n}$. In general, let $S = \{s_0,s_1,\cdot\cdot\cdot, s_{n-1}\}$ be the set of all reflection symmetries and $R = \{r_0,r_1,\cdot\cdot\cdot, r_{n-1}\}$ be the set of all rotational symmetries both are outcomes by permutating the vertices of n-polygon then, according to (Marlos and Vasudevan, 2015), we can give the following definition.

Definition. A dihedral group, $D_{2n}$, for the regular n-polygon is the set $S\cup R$ equipped with the composition operation $\circ$, given by the following relations:

\[
\begin{align*}
    r_i \circ r_j &= r_{(i+j) \mod n}, \\
    s_i \circ s_j &= s_{(i+j) \mod n}, \\
    r_i \circ r_j &= s_{(i-j) \mod n}, \\
    s_i \circ s_j &= r_{(i-j) \mod n},
\end{align*}
\]

where the composition of symmetries is also symmetric. Notice that $r_0 = e$ the counter clockwise rotations by $0^\circ$ is the identity element (David and Richard, 2014).

In this project work, we shall focus on the finite dihedral groups of degree n for n > 1, their application, their elements, their subgroups and their structures.
METHOD

The method we are using in this research is the theoretical method and here are some relevant theorems and proofs.

**Theorem** (Cameron, 1981)

The symmetric group on \( n \) letters, \( S_n \), is a group with \( n! \) elements, where the binary operation is the composition of maps.

**Proof:**

The identity of \( S_n \) is just the identity map that sends 1 to 1, 2 to 2, \( \ldots \), \( n \) to \( n \). If \( f : S_n \to S_n \) is a permutation, then \( f^{-1} \) exists, since \( f \) is one-to-one and onto; hence, every permutation has an inverse. Composition of maps is associative, which makes the group operation associative.

**Theorem** (Cayley, 1854)

Any finite group \( G \) is isomorphic to a subgroup of the symmetric group \( S_n \) of degree \( n \), where \( n = |G| \).

**Proof:**

Let \( G \) act on itself by right multiplication \( g^h = gh \) for all \( g, h \in G \). If \( g^h = g \) then \( gh = g \) and so \( h = 1 \), That is, the kernel of the action is \{1\}. The mapping \( f : G \to \text{sym}(G) \) define by \( f : g \to f_g \) where \( \alpha f_g = \alpha^g \) for any \( \alpha \in G \) is a homomorphism. Then \( G/\ker f \cong \text{im} f \), But \( \ker f = \{1\} \) and \( \text{im} f \leq \text{sym}(G) = S_n \), Accordingly \( G \leq S_n \). In general we have that if \( G \) acts on \( \Omega \) with \( k \) kernel of the action then \( G/k \leq \text{sym}(\Omega) \).

**The Permutation Representation** (grove, 1997, p.99)

Supposed \( G \) acts on the set \( X \) of \( n \)-elements such that for each \( g \in G \) we have a permutation of the form \( x_i g = x_i \), \( i, j = 1, \ldots, n \). Now let \( V \) be an \( n \)-dimensional vector space with basis \( B = \{e_i, \ldots, e_n\} \). For \( g \in G \) define \( p(g) \) such that \( e_i p(g) = e_j \). So \( p(g) \) permutes the basis elements of \( V \) in the same manner as \( g \) act on \( X \).

**The alternating group**

Lemma 3.4.1 Let \( n \geq 2 \). The set \( A_n \) of all even permutations of \{1,...,n\} is a subgroup of \( S_n \). Moreover, \( A_n \) has index 2 in \( S_n \). (In other words, there are precisely two right cosets of \( A_n \) in \( S_n \).)

**Proof:**

We use the subgroup test to show that \( A_n \) is a subgroup of \( S_n \). Certainly \( A_n \) is closed: if \( \sigma, \tau \) are composites of \( 2k, 2l \) transpositions respectively, then \( \sigma \circ \tau \) is a composite of \( 2(k + l) \) transpositions. The identity permutation is the composite of 0 transpositions. Finally, if \( \sigma \) is a composite \( \tau_1 \circ \cdots \circ \tau_{2k} \) of \( 2k \) transpositions, then so is \( \sigma^{-1} = \tau_{2k} \circ \cdots \circ \tau_1 \).

Thus \( A_n \) is a subgroup. If \( \tau \) is a transposition, then for any odd permutation \( \alpha \) we have \( \beta := \alpha \circ \tau \in A_n \), and \( \alpha = \beta \circ \tau \) (since \( \tau^2 = \text{id} \)). Hence the coset \( A_n \circ \tau \) contains all odd permutations.
Since $A_n$ contains all even permutations, $A_n \cup A_n \circ \tau = S_n$, so the only two right cosets of $A_n$ in $S_n$ are $A_n$ and $A_n \circ \tau = S_n \setminus A_n$.

Example. $S_3 = \{\text{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$.

$A_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\} = \langle(1, 2, 3)\rangle \cong \mathbb{Z}_3$.

The group $A_n$ is known as the alternating group of degree $n$. It has order $n!/2$, since it is a subgroup of index 2 in the group $S_n$ of order $n!$.

**Theorem (Disjoint Cycles Commute)**

If $\alpha = (a_1a_2a_3…a_m)$ and $\beta = (b_1b_2b_3…b_n)$ are two cycles having no entries in common, then $\alpha$ and $\beta$ commutes i.e., $\alpha \beta = \beta \alpha$.

**Proof:** Let $\alpha$ and $\beta$ be permutations on set $S$ given by:

$$S = \{a_1,a_2,a_3,…,a_m,b_1,b_2,b_3,…,b_n,c_1,c_2,c_3,…,c_k\}$$

Where $c_i$s are elements in $S$ which are left fixed by both $\alpha$ and $\beta$. Let $A = \{a_1,a_2,a_3,…,a_m\}$, $B = \{b_1,b_2,b_3,…,b_n\}$ and $C = \{c_1,c_2,c_3,…,c_k\}$. By definition, $\alpha$ fixes every element of $B \cup C$ and $\beta$ fixes every element of $A \cup C$. Also, $\alpha(x) \in A$ for all $x \in A$ and $\beta(y) \in B$ for all $y \in B$.

Now to show that $\alpha \beta = \beta \alpha$, consider any element $s \in S$. Then we have three possibilities:

**Case I:** $x \in A$

Then;

$$\alpha \beta(x) = \alpha(\beta(x))$$

$$= \alpha(x)[x \in A \Rightarrow \beta(x) = x \ (\beta \text{ fixes every element of } A)]$$

$$= \beta(\alpha(x))[x \in A \Rightarrow \alpha(x) \in A \Rightarrow \beta(\alpha(x)) = \alpha(x)]$$

$$= \beta \alpha(x).$$

**Case II:** $x \in B$

Then;

$$\beta \alpha(x) = \beta(\alpha(x))$$

$$= \beta(x)[x \in B \Rightarrow \alpha(x) = x \ (\alpha \text{ fixes every element of } B)]$$

$$= \alpha(\beta(x))[x \in B \Rightarrow \beta(x) \in B \Rightarrow \alpha(\beta(x)) = \beta(x)]$$

$$= \alpha(\beta(x).$$

**Case III:** $x \in C$

Then;

$$\alpha(x) = x = \beta(x) \text{ and hence we have;}$$
\(\alpha\beta(x) = \alpha(\beta(x)) = \alpha(x) = x = \beta(x) = \beta(\alpha(x)) = \beta\alpha(x)\)

Thus \(\alpha\beta\) and \(\beta\alpha\) agrees on every element of \(S\), whence \(\alpha\beta = \beta\alpha\).

Hence the two permutations \(\alpha\) and \(\beta\) commutes.

In the next theorem we give order of a cycle which we will be using later to find the order of a given permutation.

**Theorem (Order of a cycle)**

A cycle of length \(n\) has order \(n\).

**Proof:** Let \(\alpha = (a_1a_2\ldots a_n)\) be a cycle of length \(n\) defined on set \(S\). For any \(i\) \((1 \leq i \leq n)\) and any \(k \in \mathbb{N}\)

\[
A^k(ai) = a^{k-1}(a(ai)) \\
= a^{k-1}(ai+1) \\
= a_{k-2}(a(ai+1)) \\
= a_{k-2}(ai+2) \\
\vdots = a_{i+k}
\]

(with the assumption that \(a_k = a_k \mod n\) for all \(k\)).

It follows that \(a^k(ai) = ai\) if and only if \(k\) is a multilipel of \(n\), hence \(n\) is the smallest positive integer such that \(a^n\) fixes every member of \(A = \{a_1,\ldots,a_n\}\). also, since \(\alpha\) fixes every element of \(S – A\), therefore \(a^n\) fixes every element of \(S – A\). Thus \(n\) is the smallest positive integer such that \(a^n\) fixes every element of \(s\) i.e., \(a^n = I_s\). consequently, \(|\alpha| = n\) and the theorem follows.

Now having defined a cycle, given the formula for the order of a cycle and introduced multiplication between two cycles, the next natural question that comes to our mind is how to apply these? In other words, if we have been given a permutation in array form, how we can represent it in the cycle form? Is it always possible to do so? We will have answer to these questions shortly.

Before answering these questions let us consider a permutation given in array form.

\[
\alpha = \begin{bmatrix} 
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 1 & 5 & 3 & 6 & 4 & 7 
\end{bmatrix}
\]

Observe that here \(1 \rightarrow 2 \rightarrow 1, 3 \rightarrow 5 \rightarrow 6 \rightarrow 4 \rightarrow 3, \ 7 \rightarrow 7\)

One can easily verify that we can write \(\alpha\) as follows;

\[
\alpha(12)(3564)(7)
\]

Thus we are able to express the given permutation \(\alpha\) into product of cycles (disjoint). Can we express every permutation defined on a finite set into cycles or product of cycles? Indeed in
the next theorem we prove that every permutation is either a cycle or is expressible as a product of disjoint cycles. The technique used in the proving the theorem is implicit in the way we decomposed the permutation $\alpha$ is above example.

**Theorem (Order of a Permutation on a finite set)**

The order of a permutation defined on a finite set is the least common multiple of the lengths of the cycles in a decomposition of permutation into product of disjoint cycles.

**Proof:** Let $\alpha$ be any permutation of any finite set $S$ and $\alpha = \alpha_1\alpha_2\ldots\alpha_n$ be decomposition of $\alpha$ into product of disjoint cycles, where $\alpha_i$ is a cycle of length $m_i$.

**Theorem (Product of Disjoint Cycles)**

Any permutation on a finite set is either a cycle or is expressible as a product of disjoint cycles.

**Proof:** Let $S$ be any finite and $\alpha$ be any permutation on $S$. Consider my element $x_1 \in S$, then $a_1 = x_1$, $a_2 = \alpha(x_1)$, $a_3 = a^2(x_1)$... are elements of $S$. Since $S$ is finite and $\{a_1,a_2,...\} \subseteq S$, therefore we can choose the least positive integer $m_1$ such that $a_{m_1+1} = a_1$. If $S = \{a_1,\ldots,a_{m_1}\}$, then $\alpha = (a_1a_2\ldots a_{m_1})$ and we are through.

Other we choose any element $x_2 \in S\backslash\{a_1,\ldots,a_{m_1}\}$ and as before we can show the existence of a least positive integer $m_2$ such that $b_{m_2+1} = b_1$, where $b_i = a^{i-1}(x_2)$. Further $b_i \neq a_j$ for any $i, j$. For if, $b_i = a_j$ for some $i, j$, then

$a^{i-1}(b) = a^{i-1}(a)$

$\Rightarrow b = a^{i-1}(a) \in \{a_1,\ldots,a_{m_1}\}$

Which contradicts the choice of $b$. Hence $b_i \neq a_j$ for an $i,j$. Again. If $S = \{a_1,\ldots,a_{m_1},b_1,b_2,\ldots,b_{m_2}\}$

Where they cycles are disjoint. Hence the theorem.

We earlier mentioned that expressing permutations into cycles have many advantages. One of such advantages is that we can easily calculate the order of a given permutation by looking at its cycle decomposition. This indeed is an enormous advantage, as it really gives us a lot of depth into the study of permutations.

**Theorem (Order of a Permutation on a finite set)**

The order of a permutation defined on a finite set is the least common multiple of the lengths of the cycles in a decomposition of permutation into product of disjoint cycles.

**Proof:** Let $\alpha$ be any permutation of any finite set $S$ and $\alpha = \alpha_1\alpha_2\ldots\alpha_n$ be decomposition of $\alpha$ into product of disjoint cycles, where $\alpha_i$ is a cycle of length $m_i$.

Claim: $\mid \alpha_1\alpha_2\ldots\alpha_n \mid = l.c.m (m_1,m_2,\ldots,m_n)$
We shall prove the claim using induction on \( n \). For \( n = 1 \), \( \alpha = \alpha_1 \) and hence by Theorem 5.3, \( |a_1| = m_1 \). Suppose the claim holds for \( n = k \) i.e., \( |a_1a_2...a_k| = \text{l.c.m.}(m_1, m_2, ..., m_k) \). We need to show that \( |a_1a_2...a_ka_{k+1}| = \text{l.c.m.}(m_1, m_2, ..., m_k, m_{k+1}) = p \), \( \text{l.c.m.}(m_1, m_2, ..., m_{k+1}) = q \) and \( |a_1a_2...a_ka_{k+1}| = r \).

Now since \( a_{k+1} \) commutes with each \( a_i (1 \leq i \leq k) \), therefore \( a_{k+1} \) commutes with \( a_1a_2...a_k \). Thus

\[
I_s = \{a_1a_2...a_ka_{k+1}\}^r
\]

\[
= \{a^1a^2...a^ka^{k+1}\}[\{ab\}^r = a^b \text{ if } a \text{ and } b \text{ commutes}]
\]

\[
\Rightarrow \{a_1a_2...a_k\}r = a_{k+1}^{-r}.
\]

Let \( a_{k+1} = (a_1a_2...a_{mk+1}) \). Then for each \( i (1 \leq i \leq k) \) and each \( j (1 \leq j \leq m_{k+1}) \), \( a_i \) fixes \( a_j \) Hence for each \( j (1 \leq j \leq m_{k+1}) \), \( a_1a_2...a_k \) fixes \( a_j \) and consequently \( \{a_1a_2...a_k\}^r \text{ fixes } a_j \), thus \( a_{k+1}^{-r} \text{ fixes } a_j \) for each \( j (1 \leq j \leq m_{k+1}) \). Also, since \( a_{k+1} \) fixes every element of \( S \) which is not in \( a_{k+1}^{-r} \text{ fixes every element of } S \) which is not in \( a_{k+1} \). Hence \( a_{k+1}^{-r} \text{ fixes every element in } S \) and therefore.

\[
\{a_1a_2...a_k\}^r = a_{k+1}^{-r} = I_s.
\]

It follows that \( |a_1a_2...a_k| \text{ divides } r \) and \( |a_{k+1}| \text{ divides } r \text{ i.e., } p \mid r \text{ and } m_{k+1} \mid r \), which further implies that \( q \mid r \). Now consider.

\[
\{a_1a_2...a_k\}^q = \{a_1\}^q\{a_2\}^q
\]

\[
= I_{I_s}...I_s = I_s[\{a_1\} = m_1 \text{ divides } q]
\]

Thus \( |a_1a_2...a_ka_{k+1}| = r \text{ divides } q \) and therefore it follows that \( q = r \). Hence by induction our claim holds i.e., \( |a_1a_2...a_n| = \text{l.c.m.}(m_1, m_2, ..., m_n) \).

**Theorem (Permutation as product of 2-cycles Cannon et al. (2001))**

Every permutation is \( S_n (n \geq 2) \) is expressible as a product of 2-cycles.

**Proof:** Let \( a \) be any permutation in \( S_n \). Then by theorem 5.4, \( a \) is expressible as a product of disjoint cycles i.e.,

\[
A = a_1a_2...a_k
\]

Thus to express \( a \) as a product of 2-cycles it is enough to show that each \( a_i \) is expressible as a product of 2-cycles. Now for any \( j \in \{1,2,...,k\} \), consider the cycle \( a_j \) if \( a_j = (r) \) for some \( r \in \{1,2,...,n\} \), then we can write.

\[
a_j = (r) = (rt) (rt) \text{ for any } t \in \{1,2,...,n\} - (5)
\]

and we are through in this case. Therefore let \( a_j = (r_1r_2...r_p) \) \( (p \leq 2) \), then it can be easily verified that;

\[
a_j = (r_1r_p) (r_1r_{p-1})... (r_1r_2)
\]
Since for any \( j \in \{1, 2, \ldots, k\} \), the cycle \( a_j \) is expressible as a product of 2-cycles, therefore permutation \( a \) is expressible as a product of 2-cycles. Hence the theorem.

**Theorem** Let \( H \) be a sub-group of the symmetric group \( S_n \). then either every permutation in \( H \) is an even permutation or exactly half of the permutations in \( H \) are even.

**Proof:** Let \( H \leq S_n \), then \( I \in H \). Thus \( H \) contains at least one even permutation. Now if every permutation in \( H \) is an even permutation. Then we are done. Therefore let \( H \) contains an odd permutation \( \alpha \) (say).

Now let \( E_H \) be the set of all even permutations in \( H \) and \( O_H \) be the set of all odd permutations in \( H \). Clearly, \( E_H \neq \emptyset \) and \( O_H \neq \emptyset \). Define \( \Phi : E_H \mapsto O_H \) as follows;

\[ \Phi(\beta) = \alpha \beta \quad \forall \beta \in E_H \]

**Claim:** \( \Phi \) is bijective.

**Injective:** Consider for \( \beta_1, \beta_2 \in E_H \) such that;

\[ \Phi(\beta_1) = \Phi(\beta_2) \]

\[ \Rightarrow \quad \alpha \beta_1 = \alpha \beta_2 \]

\[ \Rightarrow \quad a^{|a|^{-1}} \alpha \beta_1 = a^{|a|^{-1}} \alpha \beta_2 \quad \text{[Multiplying both sides by } a^{|a|^{-1}} \text{]} \]

\[ \Rightarrow \quad a^{|a|} \beta_1 = a^{|a|} \beta_2 \]

\[ \Rightarrow \quad \beta_1 = \beta_2 \]

Thus \( \Phi \) is injective.

**Surjective:** Let \( y \in O_H \) be any arbitrary element. Since inverse of an odd permutation is odd, therefore \( \alpha^{-1} \) is an odd permutation and consequently, \( \alpha^{-1}y \in E_H \). Now.

\[ \Phi(\alpha^{-1}y) = \alpha \alpha^{-1}y = y. \]

Since \( y \) is an arbitrary element in \( O_H \), therefore every element in \( O_H \) has a pre-image under \( \Phi \). It follows that \( \Phi \) is surjective.

Thus \( \Phi \) is bijective map, which further implies that \( |E_H| = |O_H| \). Hence the theorem.

**Corollary** For \( n \geq 2 \), the order of the group \( A_n \) is \( n!/2 \) i.e.,

\[ |A_n| = \frac{n!}{2} \]

**Proof:** Since \( S_n \) is a subgroup of itself and it contains odd permutations, therefore by Theorem 2.7, exactly half of the permutation in \( S_n \) are even. Hence

\[ |A_n| = \frac{|S_n|}{2} = \frac{n!}{2} \]
Definition: The dihedral group of order $2n$ is the group formed by the symmetries of a regular $n$-gon. We denote this group as $D_n$ (although the occasional book will write this as $D_{2n}$).

Theorem: Label the vertices of $D_n$ starting with $v_1$ and working clockwise to $v_2$, $v_3$, etc. Let $r$ be rotation of the $n$-gon by $2\pi/n$ radians and let $f$ be reflection across the line connecting $v_1$ to the center of the object.

1. $e, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = e$ so $o(r) = n$;
2. $o(s) = 2$.
3. $s \neq r^i$ for any $i$.
4. $rf \neq fr$ for all $0 \leq i; j \leq n - l$ with $i \neq j$.

From this we can conclude that $D_n = \{e, r, r^2, \ldots, r^{n-1}, f, rf, r^2f, \ldots, r^{n-1}s\}$.

Proof:

1. Consider where $v_1$ gets mapped under each symmetry. The symmetry $r$ sends $v_1$ to $v_2$, while $r^2$ sends $v_1$ to $v_3$ and $r^i$ sends $v_1$ to $v_{i+1}$ and $i + 1 \neq j + 1$ when $i \neq j$ if $0 \leq i; j < n$.
2. Simply consider what applying $f$ twice to each vertex will do to it.
3. The symmetry $f$ fixes $v_1$ yet the only $r^i$ which does this is $r^n = e$ but $f$ is not the identity since it sends $v_2$ to $v_n$.
4. Since $r^i \neq r^j$ by (1), reflecting each by $f$ will not produce the same symmetry.

Definition: Since every element of $D_n$ is a product of $f$ and $r$, we say that those two elements generate the group. In general we say that a subset $S$ of a group $G$ generates the group if every element of the group may be written as a product of elements in $S$.

Theorem: Let $r, f \in D_n$ be as defined above.

1. $rf = fr^{-1}$.
2. $r^i f = fr^i$ for all $0 \leq i \leq n$.

Proof:

For (1) consider where $rf$ sends $v_1$. The symmetry $f$ sends it to $v_1$, followed by the symmetry $r$ which sends $v_1$ to $v_2$. Conversely, for $fr^{-1}$ we first apply $r^{-1}$ to $v_1$ which goes to $v_n$ and then $f$ sends $v_n$ to $v_2$.

Similarly $f$ sends $v_2$ to $v_n$ and $r$ sends $v_n$ to $v_1$ while $r^i$ sends $v_2$ to $v_1$ and $f$ preserves $v_1$.

In general, if $2 < i \leq n$ then $f$ sends $v_i$ to $v_{n+i}$ and $r$ sends $v_{n+i}$ to $v_{n+i+1}$ whereas $r^i$ sends $v_i$ to $v_{i+1}$ and $f$ sends $v_{i+1}$ to $v_{n+i+1} = v_{n+i+2}$. So $rf$ and $fr^{-1}$ send every vertex to the same vertex.

Notice that (1) tells us that $D_n$ is not abelian if $n \geq 3$. The Theorem above is very useful for computations. For example if we want to know what $f(rf)$ is in the group, we can rewrite $rf$ as $fr^{-1}$ and get $f(rf) = f(fr^{-1}) = (fr^{-1})r^{-1} = r^{n-1}$ since $f$ has order 2 and $r \cdot r^{n-1} = r^n = e$. 

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0
Theorem (Order of Dihedral Group)

The Order of $D_{2n}$ is precisely $2n$

Proof: Let $\rho$ be a rotation that generate a sub-group of order $n$ in $D_{2n}$.

Obviously $\langle \rho \rangle$ captures all the pure rotations of a regular n-gon. Now let $\mu$ be any rotation, then the rest of the elements can that be found by composing each $\langle \rho \rangle$ with $\mu$ to get the list of elements:

$$D_{2n} = \{1, \rho, \ldots, \rho^{n-1}, \mu, \mu \rho, \ldots, \mu \rho^n\}.$$ 

Thus the order of $D_{2n}$ is $2n$.

RESULT AND DISCUSSION

Dihedral groups are groups of symmetries of regular n-gons. We start with an example using structural approach.

The Group $D_3$

Consider a regular triangle $T$, with vertices labeled 1, 2, and 3. We show $T$ below, also using dotted lines to indicate a vertical line of symmetry of $T$ and a rotation of $T$.

1

![Figure 1. A Triangle with vertexes label 1, 2, 3.](image)

Note that if we reflect $T$ over the vertical dotted line (indicated in the picture by $f$), $T$ maps onto itself, with 1 mapping to 1, and 2 and 3 mapping to each other. Similarly, if we rotate $T$ clockwise by $120^\circ$ (indicated in the picture by $r$), $T$ again maps onto itself, this time with 1 mapping to 2, 2 mapping to 3, and 3 mapping to 1. Both of these maps are called symmetries of $T$; $f$ is a reflection or flip and $r$ is a rotation.

Of course, these are not the only symmetries of $T$. If we compose two symmetries of $T$, we obtain a symmetry of $T$: for instance, if we apply the map $f \circ r$ to $T$ (meaning first do $r$, then do $f$) we obtain reflection over the line connecting 2 to the midpoint of line segment 1-3. Similarly, if we apply the map $f \circ (r o r)$ to $T$ (first do $r$ twice, then do $f$) we obtain reflection over the line connecting 3 to the midpoint of line segment 1-2. In fact, every symmetry of $T$ can be obtained by composing applications of $f$ and applications of $r$. 
For convenience of notation, we omit the composition symbols, writing, for instance, \( fr \) for \( f \circ r \), \( r \circ r \) as \( r^2 \), etc. It turns out there are exactly six symmetries of \( T \), namely:

1. the map \( e \) from \( T \) to \( T \) sending every element to itself;
2. \( f \) (i.e., reflection over the line connecting 1 and the midpoint of 2-3);
3. \( r \) (that is, clockwise rotation by 120°);
4. \( r^2 \) (that is, clockwise rotation by 240°);
5. \( fr \) (i.e., reflection over the line connecting 2 and the midpoint of 1-3); and
6. \( fr^2 \) (i.e., reflection over the line connecting 3 and the midpoint of 1-2).

![Figure 2. A labeled triangle after individual elements of \( D_3 \) have been applied](image)

Declaring that \( f^o = r^o = e \), the set
\[ D_3 = \{e, f, r, r^2, fr, fr^2\} = \{f^i r^j : i = 0,1, j = 0,1,2\} \]
is the collection of all symmetries of \( T \).

**Remark:** Notice that \( rf = fr^2 \) and that \( f^2 = r^3 = e \).

Theorem 4.3. \( D_3 \) is a group under composition:

**Proof.**

First, as noted above, \( rf = fr^2 \). So any map of the form \( f^i r^j f^k r^l \) (i, k = 0,1, j,l = 0,1,2) can be written in the form \( f^i r^j \) for some \( s,t \in \mathbb{N} \). Finally, let \( R_2(s) \) and \( R_3(t) \) be the remainders when you divide \( s \) by 2 and \( t \) by 3; then \( f^i r^j = f^{R_2(s)} r^{R_3(t)} \in D_3 \). So \( (D_3, \circ) \) is a binary structure.

Next, function composition is always associative, and the function \( e \) clearly acts as identity element in \( D_3 \). Finally, let \( x = f^i r^j \in D_3 \). Then \( y = r^k f^l \) is in \( D_3 \) with \( xy = yx = e \). So \( D_3 \) is a group. The Cayley table for the group \( D_3 \) is as follows.

<table>
<thead>
<tr>
<th>( \times )</th>
<th>( e )</th>
<th>( r )</th>
<th>( r^2 )</th>
<th>( f )</th>
<th>( rf )</th>
<th>( r^2 f )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( e )</td>
<td>( e )</td>
<td>( r )</td>
<td>( r^2 )</td>
<td>( f )</td>
<td>( rf )</td>
<td>( r^2 f )</td>
</tr>
<tr>
<td>( r )</td>
<td>( r )</td>
<td>( r^2 )</td>
<td>( e )</td>
<td>( rf )</td>
<td>( r^2 f )</td>
<td>( f )</td>
</tr>
</tbody>
</table>
Table 1. Cayley’s table for $D_3$

From the table the following are clearly seen.

1. The orders of the elements of $D_3$ are as below.

<table>
<thead>
<tr>
<th>element</th>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>order</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

2. List of elements of each order in $D_3$

<table>
<thead>
<tr>
<th>order</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td># elements</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

3. The inverses of the elements of $D_3$

<table>
<thead>
<tr>
<th>element</th>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>inverse</td>
<td>$e$</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
</tr>
</tbody>
</table>
3.3. The Group $D_4$
Let’s start by considering the square. Label it with vertices 1, 2, 3, and 4.

Notice that one plane symmetry is simply rotating the figure clockwise by $90^\circ$ (or $\pi/2$ radians). We call that rotation $r$. We can also rotate by $180^\circ$ (or $\pi$ radians) and $270^\circ$ (or $3/2 \pi$ radians).

![Figure 4. A labeled square after individual elements of $D_4$ have been applied](image)

<table>
<thead>
<tr>
<th>$\times$</th>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$r^3$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
<th>$r^3f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$r^3$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
</tr>
<tr>
<td>$r$</td>
<td>$r$</td>
<td>$e$</td>
<td>$r^3$</td>
<td>$r^2$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
<td>$f$</td>
</tr>
<tr>
<td>$r^2$</td>
<td>$r^2$</td>
<td>$r^3$</td>
<td>$e$</td>
<td>$r$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
<td>$f$</td>
<td>$rf$</td>
</tr>
<tr>
<td>$r^3$</td>
<td>$r^3$</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$e$</td>
<td>$r^3f$</td>
<td>$r^2f$</td>
<td>$f$</td>
<td>$rf$</td>
</tr>
<tr>
<td>$f$</td>
<td>$f$</td>
<td>$r^3f$</td>
<td>$r^2f$</td>
<td>$rf$</td>
<td>$e$</td>
<td>$r^3$</td>
<td>$r^2$</td>
<td>$r$</td>
</tr>
<tr>
<td>$rf$</td>
<td>$rf$</td>
<td>$f$</td>
<td>$r^3f$</td>
<td>$r^2f$</td>
<td>$r$</td>
<td>$e$</td>
<td>$r^3$</td>
<td>$r^2$</td>
</tr>
<tr>
<td>$r^2f$</td>
<td>$r^2f$</td>
<td>$rf$</td>
<td>$f$</td>
<td>$r^3f$</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$e$</td>
<td>$r^3$</td>
</tr>
<tr>
<td>$r^3f$</td>
<td>$r^3f$</td>
<td>$r^2f$</td>
<td>$rf$</td>
<td>$f$</td>
<td>$r^3$</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

Table 2. Calay’s table for $D_4$
From the table the following are clearly seen.

1. The orders of the elements of $D_4$:

<table>
<thead>
<tr>
<th>element</th>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$r^3$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
<th>$r^3f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>order</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

2. The number of elements of each order in $D_4$:

<table>
<thead>
<tr>
<th>order</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>elts</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

3. The inverses of the elements of $D_4$:

<table>
<thead>
<tr>
<th>elt</th>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$r^3$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
<th>$r^3f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>inverse</td>
<td>$e$</td>
<td>$r^3$</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
</tr>
</tbody>
</table>

3.4. The Group $D_5$

Let’s consider a pentagon with its corners numbered 1, 2, 3, 4 and 5.

![Figure 5. A labeled pentagon](image)

Figure 6. A labeled pentagon after individual elements of $D_5$ have been applied
Table 3. Calay's table for $D_5$

<table>
<thead>
<tr>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$r^3$</th>
<th>$r^4$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
<th>$r^3f$</th>
<th>$r^4f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$r^3$</td>
<td>$r^4$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
<td>$r^4f$</td>
</tr>
<tr>
<td>$r^2$</td>
<td>$r^3$</td>
<td>$r^4$</td>
<td>$e$</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$r^3$</td>
<td>$r^4f$</td>
<td>$f$</td>
<td>$rf$</td>
</tr>
<tr>
<td>$r^3$</td>
<td>$r^4$</td>
<td>$e$</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$r^3$</td>
<td>$r^4f$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
</tr>
<tr>
<td>$r^4$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
<td>$r^4$</td>
<td>$e$</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$r^3$</td>
</tr>
<tr>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
<td>$r^4f$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
<td>$r^4f$</td>
</tr>
</tbody>
</table>

From the table the following are clearly seen.

1. The orders of the elements of $D_5$:

<table>
<thead>
<tr>
<th>element</th>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$r^3$</th>
<th>$r^4$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
<th>$r^3f$</th>
<th>$r^4f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>order</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

2. The number of elements of each order in $D_5$:

<table>
<thead>
<tr>
<th>order</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>elts</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

3. The inverses of the elements of $D_5$:

<table>
<thead>
<tr>
<th>elt</th>
<th>$e$</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$r^3$</th>
<th>$r^4$</th>
<th>$f$</th>
<th>$rf$</th>
<th>$r^2f$</th>
<th>$r^3f$</th>
<th>$r^4f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>inverse</td>
<td>$e$</td>
<td>$r^4$</td>
<td>$r^3$</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$f$</td>
<td>$rf$</td>
<td>$r^2f$</td>
<td>$r^3f$</td>
<td>$r^4f$</td>
</tr>
</tbody>
</table>

**Isomorphism of Dihedral group to the Symmetric group**

Let us look at $D_3$ another way. Note that each map in $D_3$ can be uniquely described by how it permutes the vertices 1,2,3 of $T$: that is, each map in $D_3$ can be uniquely identified with a unique element of $S_3$. For instance, $f$ corresponds to the permutation (23) in $S_3$, while $fr$ corresponds to the permutation (13). It turns out that $D_3 \cong S_3$, via the following correspondence.
The group $D_3$ is an example of class of groups called *dihedral groups*.

**Result:** Each $D_n$ is isomorphic to a subgroup of $S_n$.

Proof.

We described above how $D_3$ is isomorphic to a subgroup (namely, the improper subgroup) of $S_3$. One can show that each $D_n$ is isomorphic to a subgroup of $S_n$ by similarly labeling the vertices of the regular n-gon 1, 2, ..., $n$ and determining how these vertices are permuted by each element of $D_n$.

While $D_3$ is actually isomorphic to $S_3$ itself, for $n > 3$ we have that $D_n$ is not isomorphic to $S_n$ but is rather isomorphic to a *proper subgroup* of $S_n$. When $n > 3$ you can see that $D_n$ cannot be isomorphic to $S_n$ since $|D_n| = 2n < n! = |S_n|$ for $n > 3$.

It is important to be able to do computations with specific elements of dihedral groups. We have the following theorem.

**Result:** The following relations hold in $D_n$, for every $n$:

1. For every $i$, $r^i f = f r^{-i}$ (in particular, $rf = fr^{-1} = fr^{n-1}$);

2. $o(fr^i) = 2$ for every $i$ (in particular, $f^2 = e$);

3. $o(r) = o(r^{-1}) = n$;

Proof.

1. We use induction on the exponent of $r$.

We already know that $r^i f = fr^{-i}$. Now suppose $r^i f = fr^{-i(i-1)}$ for some $i \geq 2$. Then $r^f = r(r^i f) = r(fr^{i(i-1)}) = (rf)r^{-i-1} = (fr^{-1})r^{-i+1} = fr^i$.

2. For every $i$, $fr^i \neq e$, but

$$(fr^i)^2 = (fr^i)(fr^i) = f(ri) = f(fr^i)r^i = f^2 = e.$$
Theorem: Let \( n \) be an integer greater than or equal to 3. Then, again using the convention that \( f^\circ = r^\circ = e \), \( D_n \) can be uniquely described as
\[
D_n = \{ f^i r^j : i = 0,1, j = 0,1,..., n-1 \}
\]
with the relations
\[
rf = fr^{n-1} \quad \text{and} \quad f^2 = r^n = e.
\]
The dihedral group \( D_n \) is a nonabelian group of order 2n.

Proof.
The proof that \( D_n \) is a group parallels the proof, above, that \( D_3 \) is a group. It is clear that \( D_n \) is nonabelian (e.g., \( rf = fr^{n-1} \neq fr \)) and has order 2n.

CONCLUSION
In group theory, the study of dihedral groups have a wide application in Mathematics and other field of studies. In this work we have constructed dihedral groups by products permutations. We used the concept of group theory which includes Lagrange’s theory to carry out our analysis. We used examples to validate our results.

REFERENCES
Cayley A. (1844). On the Theory of Groups as Depending on the Symbolic Equation \( \theta^n = 1 \). Philosophical Magazine. 7 (42): 40–47

