African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)
www.abjournals.org

ANALYSIS ON PROPERTIES AND STRUCTURE OF DIHEDRAL GROUPS

Ben O. Johnson[1*], Adagba T. Titus[2] and Auta T. Jonathan[3]

[1-3]Department of Mathematics and Statistics, Federal University, Wukari, Taraba State, Nigeria.

[*]Corresponding Author's Email: benjohnsonnig@yahoo.com

Cite this article:

Ben O. J., Adagba T. T., Auta T. J. (2024), Analysıs on Propertıes and Structure of Dıhedral Groups. African Journal of Mathematics and Statistics Studies 7(2), 51-68. DOI: 10.52589/AJMSS-UCZXWKC0

Manuscript History

Received: 15 Jan 2024

Accepted: 12 Mar 2024

Published: 8 Apr 2024

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

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

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 symetric 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 $S = \{s_0, s_1, \cdots, s_{n-1}\}$ be the set of all reflection symmetries and $R = \{r_0, r_1, \cdots, r_{n-1}\}$ 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:

$r_i \circ r_j = r_{(i+j) \bmod n}$, $s_i \circ s_j = s_{(i+j) \bmod n}$, $r_i \circ r_j = s_{(i-j) \bmod n}$ and $s_i \circ s_j = r_{(i-j) \bmod n}$, where the composition of symmetries is also symmetric. Notice that $r_0 = e$ the counter clockwise rotations by 0° 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.

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68) www.abjournals.org

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, … , n to n. If $f: S_n \rightarrow S_n$ 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 $f: G \rightarrow sym(G)$ define by $f: g \rightarrow f_g$ where $\alpha f_g = \alpha^g$ for any $\alpha \in G$ is a homomorphism. Then $G/_{\ker f} \cong im\, f$, But $ker\, f = \{1\}$ and $im\, f \leq sym(G) = S_n$, Accordingly $G \leq S_n$, In general we have that if G acts on Ω with k kernel of the action then $G/_k \leq sym(\Omega)$,

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 $X_i g = x_i.\ i.j = 1.\dots.n$. Now let V be an n-dimensional vector space with basis $B = \{e_i.\dots.e_n\}$. For $g \in G$ define $\mathrm{p}(g)$ such that $e_i \mathrm{p}(g) = e_j$, So $\mathrm{p}(g)$ 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 σ, τ 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 σ 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 τ is a transposition, then for any odd permutation α we have $\beta := \alpha \circ \tau \in A_n$, and $\alpha = \beta \circ \tau$ (since $\tau^2 = id$). Hence the coset $A_n \circ \tau$ contains all odd permutations.

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)
www.abjournals.org

Since An 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 $A_n \circ \tau = S_n \backslash A_n$.

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

$A_3 = \{id, (1, 2, 3), (1, 3, 2)\} = <(1, 2, 3)> \cong Z_3$.

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

Proof: Let α and β be permutations on set S given by;

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

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

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

Case I: $x \epsilon A$

Then;

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

$= \alpha(x)[x \epsilon A \Rightarrow \beta(x) = x$ (β fixes every element of A)]

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

$= \beta\alpha(x)$.

Case II: $x \epsilon B$

Then;

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

$= \beta(x)[x \epsilon B \Rightarrow \alpha(x) = x$ (α fixes every element of B)]

$=\alpha(\beta(x))\{x \epsilon B \Rightarrow \beta(x) \epsilon B \Rightarrow \alpha(\beta(x)) = \beta(x)]$

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

Case III: $x \epsilon C$

Then;

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

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

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

Thus $\alpha\beta$ and $\beta\alpha$ agrees on every element of s, whence $\alpha\beta = \beta\alpha$.

Hence the two permutations α and β 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 $k \in \mathbb{N}$

$A^k(ai) = a^{k-1}(a(a_i))$

$=a^{k-1}(a_{i+1})$

$=a_{k-2}(a(a_{i+1}))$

$=ak-2(a_{i+2})$

$: = a_{1+k}$

(with the assumption that $a_k = a_{k \text{ (mod n)}}$ for all k).

It follows that$_a{}^k(a_i) = a_i$ if and only if k is a mutlipel 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 α 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 $1 \to 2 \to 1$, $3 \to 5 \to 6 \to 4 \to 3$, $7 \to 7$

One can easily verify that we can write α as follows;

$\alpha(12)(3564)(7)$

Thus we are able to express the given permutation α into product of cycles (disjoint). Can we express every permutation defined on a finite set into cycles or product or cycles? Indeed in

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)
www.abjournals.org

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 α 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 α be any permutation of any finite set S and $\alpha = a_1a_2\ldots a_n$ be decomposition of α into product of disjoint cycles, where a_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: Lets be any finite and α be any permutation on S. consider my element $x_1 \in S$, then $a_1 = x_1$, $a_2 = \alpha(x_1)$, $a_3 = a^2\ (x_1)\ldots$ are elements of S. Since S is finite and $\{a_1,a_2\ldots\} \subseteq S$, therefore we can choose the least positive integer m_1 such that $a_{m1+1}= a_1$. If $S = \{a_1,\ldots,a_{m1}\}$, then $\alpha = (a_1a_2\ldots a_{m1})$ and we are through.

Other we choose any element $x_2 \in s\backslash\{a_1\ldots,a_{m1}\}$ and as before we can show the existence of a least positive integer m_2 such that $b_{m2+1} = b_1$, 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

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

$\Rightarrow b = a^{j-1}(a) \in \{a_1,\ldots,a_{m1}\}$

Which contradicts the choice of b. hence $b_i \neq a_j$ for an i,j. Again. If

$S = \{a_1,\ldots,a_{m1},b_1,b_2,\ldots,b_{m2}\}$

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 α be any permutation of any finite set S and $\alpha = a_1a_2\ldots a_n$ be decomposition of α into product of disjoint cycles, where a_i is a cycle of length m_i.

Claim: $|a_1a_2\ldots a_n| = \text{l.c.m}\ (m_1,m_2,\ldots,m_n)$

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)

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., $|a_1a_2\ldots a_k| =$ l.c.m $(m_1,m_2\ldots,m_k)$. we need to show that $|a_1a_2\ldots a_ka_{k+1}| =$ l.c.m $(m_1,m_2,\ldots,m_k,m_{k+1}) = p$, l.c.m. $(m_1,m_2,\ldots,m_{k+1}) = q$ and $|a_1a_2\ldots a_ka_{k+1}| = r$.

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

$I_s = \{a_1a_2\ldots a_ka_{k+1})^r$

$=\{a^1a^2\ldots a^k)^r a^{k+1r}[\{ab\}^r = a^rb^r$ if a and b commutes]

$\Rightarrow \{a1a2\ldots ak)r = a_{k+1\text{-}5}^{-r}$.

Let ak+1 = $(a1a2\ldots a_{mk+1})$. 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$(1 \leq j \leq m_{k+1})$, $a_1a_2\ldots a_k$ fixes a_j and consequently $\{a_1a_2\ldots a_k\}^r$ $_{\text{fixes}}$ a_j. thus a_{k+1}^{-r} 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 $a_{k+1},^{-r}$ fixes every element of S which is not in a_{k+1}. Hence a_{k+1}^{-r} fixes every element in S and therefore.

$\{a_1a_2\ldots a_k\}^r = a_{k+1}^{-r} = I_s$.

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

$\{a_1a_2\ldots a_k\}^a = \{a_1\}^q\{a_2\}^q$

$= I_sI_s\ldots I_s = I_s[\,|a_i| = m_i$ divides q]

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

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.,

$A = a_1a_2\ldots a_k$

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 ϵ {1,2,…,k}, consider the cycle a_j. if $a_j = (r)$ for some r ϵ {1,2,…,n}, then we can write.

$a_j = (r) = (rt)\ (rt)$ for any t ϵ {1,2,…,n} – (5)

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

$a_j = (r_1r_p)\ (r_1r_{p-1})\ldots(r_1r_2)$

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68) www.abjournals.org

Since for any j ϵ {1,2,….,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 $I_n \in H$. 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 α (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, $E_H \neq \Phi$ and $O_H \neq \Phi$. Define $\Phi: E_H \longrightarrow O_H$ as follows;

$\Phi(\beta) = \alpha\beta \ \forall \beta \in E_H$

Claim: Φ is bijective.

Injective: Consider for $\beta_1 \beta_2 \in E_H$ such that;

$\Phi(\beta_1) = \Phi(\beta_2)$

$\Rightarrow \quad \alpha\beta_1 = \alpha\beta_1$

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

$\Rightarrow \quad a^{|a|}\beta_1 = a^{|a|}\beta_2$

$\Rightarrow \quad \beta_1 = \beta_2$

Thus Φ is injective.

Surjective: Let y ϵ O_H be any arbitrary element. Since inverse of an odd permutation is odd, therefore α^{-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 Φ. It follows that Φ is surjective.

Thus Φ 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

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)
www.abjournals.org

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) $e, r, r^2, ..., r^{n-1}$ are all distinct and $r^n = e$ so $o(r) = n$:

(2) $o(s) = 2$.

(3) $s \neq r^i$ for any i.

(4) $r^i f \neq r^j f$ for all $0 \leq i; j \leq n - 1$ with $i \neq j$:

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

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^{-1} 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+2} and r sends v_{n-i+2} to v_{n-i+3} whereas r^{-1} sends v_i to v_{i-1} and f sends v_{i-1} to $v_{n-(i-1)+2} = v_{n-i+}$. 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 $f(rf) = f(fr^{-1}) = (ff^{-1})r^{-1} = r^{n-1}$ 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

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)

Theorem (Order of Dihedral Group)

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

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

Obviously <ρ> captures all the pure rotations of a regular n-gon. Now let μ be any rotation, then the rest of the elements can that be found by composing each <ρ> with μ to get the list of elements:

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

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

RESULT AND DİSCUSSİON

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

The Group *D₃*

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

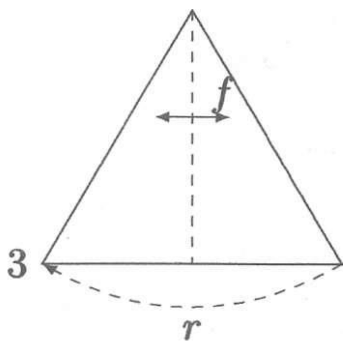


Figure 1. A Trangle with vertexes label 1, 2, 3.

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° (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*** *o 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*** o (*ror*) 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*.

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

For convenience of notation, we omit the composition symbols, writing, for instance, ***fr*** for ***f*** o ***r***, ***r*** o ***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** (ie reflection over the line connecting 3 and the midpoint of 1-2).

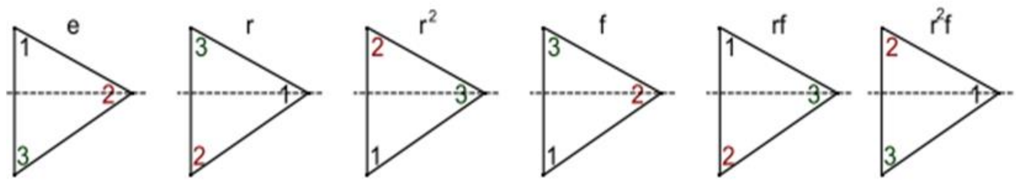


Figure 2. A labeled triangle after individual elements of D_3 have been applied

Declaring that **f** ° = r° = 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 = fr²** 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 $f^s r^t$ for some **s,t** € N. Finally, let $R_2(s)$ and $R_3(t)$ be the remainders when you divide **s** by 2 and **t** by 3; then $f^s r^t = f^{R2(s)} r^{R3(t)}$ € D_3. So (D_3, o) is a binary structure.

Next, function composition is always associative, and the function *e* clearly acts as identity element in D_3. Finally, let $x = f^i r^j$ € D_3. Then $y = r^{3-j} f^{2-i}$ 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.

×	e	r	r^2	f	rf	r^2f
e	e	r	r^2	f	rf	r^2f
r	r	r^2	e	rf	r^2f	f

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

r^2	r^2	e	r	r^2f	f	rf
f	f	r^2f	rf	e	r^2	r
rf	rf	f	r^2f	r	e	r^2
r^2f	r^2f	rf	f	r^2	r	e

Table 1. Calay'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.

element	e	r	r^2	f	rf	r^2f
order	1	3	3	2	2	2

2. List of elements of each order in D_3

order	1	2	3
# elements	1	3	2

3. The inverses of the elements of D_3

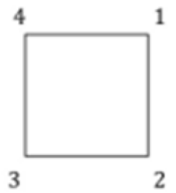
element	e	r	$r2$	f	rf	$r2f$
inverse	e	$r2$	r	f	rf	$r2f$

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)

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◦ (or π^2 radians). We call that rotation r. We can also rotate by 180◦ (or π radians) and 270◦ (or 3/2 π radians).

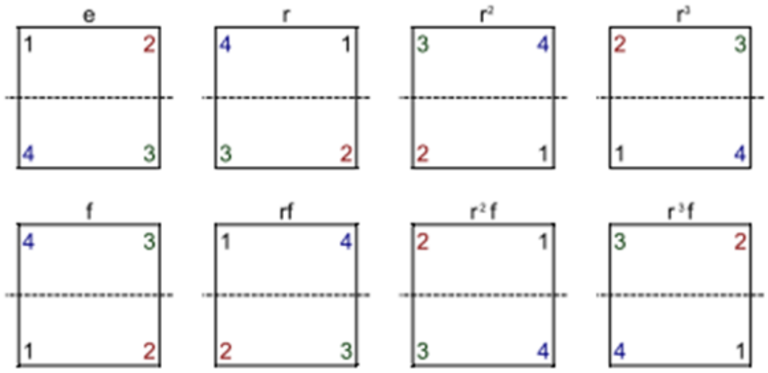


Figure 4. A labeled square after individual elements of D_4 have been applied

×	e	r	r^2	r^3	f	rf	r^2f	r^3f
e	e	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	e	rf	r^2f	r^3f	f
r^2	r^2	r^3	e	r	r^2f	r^3f	f	rf
r^3	r^3	e	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	e	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	e	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	e	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	e

Table 2. Calay's table for D_4

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

From the table the following are clearly seen.

1. The orders of the elements of D_4:

element	e	r	r^2	r^3	f	rf	r^2f	r^3f
order	1	4	2	4	2	2	2	2

2. The number of elements of each order in D_4

order	1	2	3	4
elts	1	5	0	2

3. The inverses of the elements of D_4:

elt	e	r	r^2	r^3	f	rf	r^2f	r^3f
inverse	e	r^3	r^2	r	f	rf	r^2f	r^3f

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

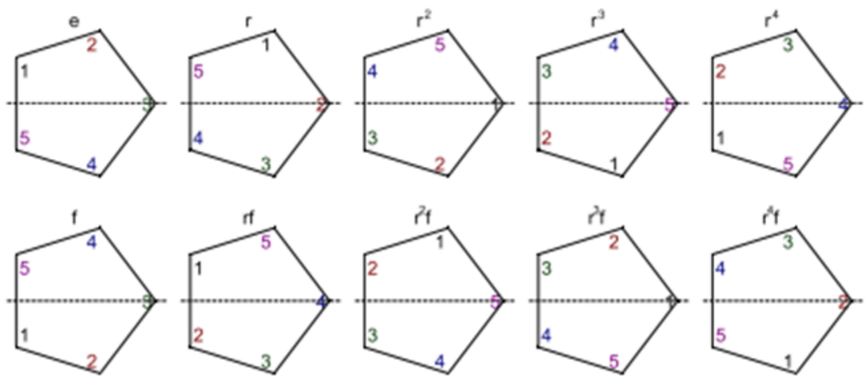


Figure 6. A labeled pentagon after individual elements of D_5 have been applied

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

×	e	r	r^2	r^3	r^4	f	rf	r^2f	r^3f	r^4f
e	e	r	r^2	r^3	r^4	f	rf	r^2f	r^3f	r^4f
r	r	r^2	r^3	r^4	e	rf	r^2f	r^3f	r^4f	f
r^2	r^2	r^3	r^4	e	r	r^2f	r^3f	r^4f	f	rf
r^3	r^3	r^4	e	r	r^2	r^3f	r^4f	f	rf	r^2f
r^4	r^4	e	r	r^2	r^3	r^4f	f	rf	r^2f	r^3f
f	f	r^4f	r^3f	r^2f	rf	e	r^4	r^3	r^2	r
rf	rf	f	r^4f	r^3f	r^2f	r	e	r^4	r^3	r^2
r^2f	r^2f	rf	f	r^4f	r^3f	r^2	r	e	r^4	r^3
r^3f	r^3f	r^2f	rf	f	r^4f	r^3	r^2	r	e	r^2
r^4f	r^4f	r^3f	r^2f	rf	f	r^4	r^3	r^2	r	e

Table 3. Calay's table for D_5

From the table the following are clearly seen.

1. The orders of the elements of D_5:

element	e	r	r^2	r^3	r^4	f	rf	r^2f	r^3f	r^4f
order	1	5	5	5	5	2	2	2	2	2

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

order	1	2	3	4	5
elts	1	5	0	0	4

3. The inverses of the elements of D_5:

elt	e	r	r^2	r^3	r^4	f	rf	r^2f	r^3f	r^4f
inverse	e	r^4	r^3	r^2	r	f	rf	r^2f	r^3f	r^4f

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 $\mathbf{D_3}$ can be uniquely identified with a unique element of S_3. For instance, $\boldsymbol{f}$ corresponds to the permutation (23) in S_3, while $\boldsymbol{fr}$ corresponds to the permutation (13). It turns out that $D_3 \cong \boldsymbol{S_3}$**,** via the following correspondence.

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

African Journal of Mathematics and Statistics Studies
ISSN: 2689-5323
Volume 7, Issue 2, 2024 (pp. 51-68)
www.abjournals.org

$$\begin{aligned} e &\rightarrow e \\ f &\rightarrow (23) \\ r &\rightarrow (123) \\ r^2 &\rightarrow (132) \\ fr &\rightarrow (13) \\ fr^2 &\rightarrow (12) \end{aligned}$$

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, $r^i f = fr^{-i}$ (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 $r^1 f = fr^{-1}$. Now suppose $r^{i-1} f = fr^{-1(i-1)}$ for some $i \geq 2$. Then

$r^i f = r(r^{i-1}f) = r(fr^{-(i-1)}) = (rf)r^{-i+1} = (fr^{-1})\, r^{-i+1} = fr^{-i}$.

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

$$(fr^i)^2 = (fr^i)\,(fr^i) = f(r^i f)r^i = f(fr^{-i})r^i = f^2 r^\circ = e.$$

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

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

$D_n = \{ \boldsymbol{f^{I} r^{j}} : \mathbf{i} = 0,1, \mathbf{j} = 0,1,..., n\text{-}1\}$

with the relations

$rf = fr^{n-1}$ **and** $f^{2} = r^{n} = e$.

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., $\boldsymbol{r\, f = f\, r^{n-1} \neq f\, r}$**)** and has order 2n.

CONCLUSİON

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

Conrad, *K.* (2018). *Dihedral Groups, Retrieved from:* http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/dihedral. pdf.

Conrad, *K.* (2018b). *Dihedral Groups II Retrieved from:* http://www.math.uconn.edu/ *kconrad/blurbs/grouptheory/dihedral2. pdf.*

David S. D. and Richard M. F. (2014). *Abstract Algebra, 3-rd Edition, John Wiley and Sons, Pp 176.*

Deng, G. D. and Fan, Y. (2015). Permutation-like Matrix Groups with a Maximal Cycle of Power of Odd Prime Length. Linear Algebra Applications. Volume 480, Number 1.

Dixon, J. D. and Mortimer, B. (1996). *Permutation Groups.* Volume 163 of *Graduate Texts in Mathematics,* Springer, New York, NY, USA, 1996.

Elsenhans, A. S. (2016). Improved Methods for the Construction of Relative Invariants for Permutation Groups, *Journal of Symbolic Computing*. Volume 79, Issue 3. Pp. 211.

Gandi, T. I. and Hamma, S. (2018). Investigating simple and regular Dihedral groups of an even Degree regular polygon using the concept of p- groups. *Frontiers of knowledge, International Journal of pure and applied sciences*. ISSBN: 2635-3393| Vol. 1

Halasi, Z. (2012). On the Base Size for the Symmetric Group Acting on Subsets, *Studia Science Mathematics Hungar*. Volume 49, Number 3. pp. 492–500.

Jaume A., Carles B. and Laia S. (2017). *Rank Two Integral Representations of the Infinite Dihedral Group, Communications in Algebra, Volume 3 Issue5, Pp 39-51.*

Article DOI: 10.52589/AJMSS-UCZXWKC0
DOI URL: https://doi.org/10.52589/AJMSS-UCZXWKC0

Khukhro, E.I. and Mazurov, V.D. (2014). The Kourovka Notebook: Unsolved Problems in Group Theory, Eighteen Edition. *Institute of Mathematics, Novosibirsk*, (2)3.

Li, C.H. and Praeger, C. E. (2012). On Finite Permutation Groups with a Transitive Cyclic Subgroup. *Journal of Algebra*. Volume (349)1: 117.

Marlos V. and Vasudevan L. (2015). *Dihedral Representations and Statistical Geometric Optics II: Elementary optical instruments, Journal of Modern Optics, Volume 54, No. 4, 473-485.*

Müller, P. M. (2013). Permutation Groups With a Cyclic Two-Orbits Subgroup and Monodromy Groups of Laurent Polynomials. *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze, Serie 5, Volume 12, Number 2*, pp. 369-438.