JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SOME PROPERTIES OF DIHEDRAL GROUP REPRESENTING AS A GROUP OF RESIDUE CLASSES

SUBHASH CHANDRA SINGH

Kunwar Singh Inter College, Civil line, District: Ballia, State : Uttar Pradesh, Country : India, Pin: 277001
Gmail : drsubhash4321@gmail.com

Abstract

The aim of this paper is to introduce a new representation of dihedral group D_n of degree n as a group of residue classes and study its properties. We find the (N,M)-th Commutativity degree $P_N^M(D_n)$ for all positive integers N, M and n. $P_N^M(D_n)$ is the probability of a random pair (*x*,*y*) of $D_n \times D_n$ so that $x^N y^M = y^M x^N$. Let $D_n^K = \{a^K | a \in D_n\}$ for a positive integer K. Further We find the relative (N,M)-th commutativity degree $P_N^M(D_n, D_n) = P(D_n^N, D_n^M)$ for all positive integers N, M and n. $P_N^M(D_n, D_n)$ is the probability that a random element of D_n^N commutes with a random element of D_n^M. Finally We find all subgroups, all normal subgroups, the center and the commutator subgroup of D_n.

1. Introduction

Conrad [4] defined dihedral group D_n as a result of reflection and rotation operations. All the properties of D_n are proven by geometry approach. In this paper, We represent D_n as a group of residue classes. Then it becomes very easy to study any property of D_n. Erodos and Turan [8], and, Gustofson [9] introduced the concept of the commutativity degree P(G). P(G) is the probability that a random element of G commutes with a random element of G. Sarmin and Mohamad [7] extended the concept of the commutativity degree P(G) as the N-th

Mathematics Subject classification (2010). 20F17, 20B35, 20B05,20K27.
Key words and Phrases. Dihedral group. Residue Classes, N-th commutativity degree, relative commutativity degree, Equivalence relation.

commutativity degree $P_N(G)$ for a positive integer N. $P_N(G)$ is the probability of a random pair (x, y) of G×G so that $x^N y = yx^N$. Ali and Sarmin [6], and, Azizi and Dostie [2] defined the same $P_N(G)$. In this paper, We extend the concept of the N-th commutativity degree $P_N(G)$ as the (N,M)-th commutativity degree $P_N^M(G)$ for positive integers N and M. $P_N^M(G)$ is the probability of a random pair (x, y) of G×G so that $x^N y^M = y^M x^N$. Sarmin and Mohamad [7], and, Ali and Sarmin [6] obtained $P_N(D_4)$ for all N. Abdul Hamid [5] obtained P(D_n), and, Azizi and Dostie [2] obtained $P_N(D_n)$, for all N and n. In this paper, We find $P_N^M(D_n)$ for all N, M and n. Erfanian and Rezaei [1] introduced the concept of the relative commutativity degree P(H, G) of a subgroup H of a finite group G. P(H,G) is the probability that a random element of H commutes with a random element of G. Let $G^N = \{a^N | a \in G\}$ for a positive integer N. Yahya et all [10] used same $P_N(G)$ defined by Sarmin and Mohamad [7]. They [10] expressed $P_N(G)$ by the equation $P_N(G) = |\{(x, y) \in G \times G | x^N y = yx^N\}|/(|G|^2)$. But to prove $P_N(D_n)$ they [10] did not use this equation. Their [10] proof for $P_N(D_n)$ can be obtained by using the equation $P_N(G) = |\{(x, y) \in G^N \times G | xy = yx\}|/(|G^N||G|)$ which is the relative commutativity degree $P(G^N, G)$. We define $P(G^N, G)$ as the relative N-th commutativity degree and denote it by $P_N(G, G)$. Yahya et all [10] obtained $P_N(D_n, D_n)$ for all N and for some dihedral groups D_n upto degree $n = 12$. In this paper We extend the concept of the relative N-th commutativity degree $P_N(G, G)$ as the relative $(N, M) - th$ commutativity degree $P_N^M(G, G) = P(G^N, G^M)$ for Positive integers N and M. $P_N^M(G, G)$ is the probability that a random element of G^N commutes with a random element of G^M. In this paper We find $P_N^M(D_n, D_n)$ for all N, M and n. Then $P_N^M(D_n)$ and $P_N^M(D_n, D_n)$ are improvements of $P_N(D_n)$ (or $P(D_n)$) and $P_N(D_n, D_n)$ (or $P(D_n)$) respectively. Finally we find all subgroups, all normal subgroups, the center and the commutator subgroup of D_n.

2. Preliminaries

Definition 2.1 [4,3]. Dihedral group D_n for $n \geq 3$ is defined as the rigid motions taking a regular n-gon back to itself, with operation being composition and obtained D_n as following :

(i) $D_n = \{1, x, x^2, \ldots\ldots, x^{n-1}, y, yx, yx^2, \ldots\ldots, yx^{n-1}\}$,

(ii) $y^2 = 1, x^n = 1 = x^0,\ xy = yx^{-1},\ x^i y = yx^{-i}$ and $|D_n| = 2n$.

Definition 2.2 [8]. The commutativity degree P(G) of a finite group G is defined by

$P(G) = |\{(x, y) \in G \times G | xy = yx\}| / (|G|^2)$.

Definition 2.3 [2,6,7]. The N-th commutativity degree $P_N(G)$ of a finite group G is defined by

$P_N(G) = |\{(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{G} \times \boldsymbol{G} | \boldsymbol{x}^N \boldsymbol{y} = \boldsymbol{y}\boldsymbol{x}^N\}| / (|\boldsymbol{G}|^2)$.

Definition 2.4 [1]. The relative commutativity degree P(H,G) of a subgroup H of a finite group G is defined by $P(H, G) = |\{(x, y) \in H \times G | xy = yx\}| / (|H||G|)$.

Definition 2.5 [10]. The N-th commutativity degree $P_N(G)$ in [10] can be replaced by the relative N-th commutativity degree $P_N(G, G) = P(G^N, G)$. $P_N(G, G)$ is the probability that a random element of G^N commutes with a random element of G given by

$P_N(G, G) = P(G^N, G) = |\{(x, y) \in G^N \times G | xy = yx\}| / (|G^N||G|)$.

Definition 2.6 [3]. A relation ~ on Z is called an equivalence relation on Z if

(i) $a \sim a\ \forall (for\ every) a \in Z$, $(ii)\ a \sim b \Rightarrow b \sim a$ and (iii) $a \sim b\ and\ b \sim c \Rightarrow a \sim c$.

Theorem 2.7 [3]. ***An equivalence relativon ~ on a set Z decomposes Z into disjoint equivalence classes and [a] = [b] if and only if a~b. Where [x] denotes the equivalence class by x ∈ Z.***

3. Representation Of Dihedral Group As A Group Of Residue Classes

Definition 3.1. Let Z be the set of integers and 2n be a positive integer. Let $a, b \in Z$. We define a relation ~ on Z by

$a \sim b \Leftrightarrow 2n\ divides\ (a - b) \Leftrightarrow a - b = 2nq$ for some $q \in Z$.

Then ~ is called the relation of congruent modulo 2n and We write $a \equiv b (mod\ 2n)$.

Lemma 3.2. ***The relation ~ of congruent modulo 2n is an equivalence relation on Z.***

Proof. Let $a, b, c \in Z$. We can write a – a = 2n(0). Then from definition 3.1, We get $a \sim a$. Let $a \sim b$. Then from definition 3.1, We get a – b = 2nq for some $q \in Z$, implies $b - a = 2n(-q)$, implies $b \sim a$. Let $a \sim b$ and $b \sim c$. Then from definition 3.1, We get $a - b = 2nq_1\ and\ b - c = 2nq_2$ for some $q_1, q_2 \in Z$, implies $a - b + b - c = 2nq_1 + 2nq_2$, implies $a - c = 2n(q_1 + q_2)$, implies $a \sim c$. It follows that ~ is an equivalence relation on Z.

Definition 3.3. Let $a \in z$ and $\sim$ be the relation of congruent modulo 2n. Let

$[a] = \{x \in z | x \sim a\}$.

Then [a] is called equivalence class by a. [a] is also called residue class modulo 2n by a. We can also denote residue class modulo 2n by $[a]_n$.

Lemma 3.4. The relation ~ of congruent modulo 2n On Z decomposes Z into disjoint residue classes.

Proof. The proof follows from lemma 3.2, definition 3.3 and the fact that an equivalence relation decomposes a set into disjoint equivalence classes.

Lemma 3.5. Let $a, b \in Z$. Let [a] and [b] be the residue classes modulo 2n. Then,

$[\boldsymbol{a}] = [\boldsymbol{b}] \Leftrightarrow \boldsymbol{2n}$ ***divides*** $(\boldsymbol{a} - \boldsymbol{b}) \Leftrightarrow \boldsymbol{a} - \boldsymbol{b} = \boldsymbol{2nq}$ ***for some*** $\boldsymbol{q} \in \boldsymbol{Z}$.

Proof. Let $a, b \in Z. Since\ the\ relation \sim$ of congruent modulo 2n is an equivalence relation so $[a] = [b] \Leftrightarrow$ a~b. Then the proof follows from definition 3.1.

Lemma 3.6. Let ~ be the relation of congruent modulo 2n on Z. Then,

(i) $a \in Z \Longrightarrow$ [a] = [r], for some $0 \le r < 2n$,

(ii) $0 \le r, s < 2n,\ r \ne s \Longrightarrow [r] \ne [s]$,

(iii) for all $k, a \in Z$, $[2kn + a] = [a] = [r] \in Z_{2n}$, for some $0 \le r < 2n$, and

(iv) for all k, [2kn] = [2n] = [0].

Proof.

(i) Let $a \in Z$. Then by division algorithm, We get $a = 2nq + r$ for some $q \in Z$ and $0 \le r < 2n$, implies $a - r = 2nq$. Then from lemma 3.5, We get [a] = [r].

(ii) Let $0 \le r, s < 2n, r \ne s$, implies $0 \le |r - s| < 2n$, implies 2n does not divide $r - s$. Then from lemma 3.5, We get $[r] \ne [s]$.

(iii) We can write $(2kn + a) - a = 2kn$. Then from lemma 3.5, We get [2kn + a] = [a]. Then proof follows from lemma 3.6 (i).

(iv) The proof follows from lemma 3.5.

Lemma 3.7. Let $\mathbf{Z_{2n}}$ denote the set of residue classes modulo 2n. Then,

$\boldsymbol{Z_{2n}} = \{[\boldsymbol{r}] | \boldsymbol{0} \le \boldsymbol{r} < 2\boldsymbol{n}\} = \{[\boldsymbol{2r}], [\boldsymbol{2r} + \boldsymbol{1}] | \boldsymbol{0} \le \boldsymbol{r} < n\}$ ***and*** $|\boldsymbol{Z_{2n}}| = \boldsymbol{2n}$.

Proof. The proof follows from lemma 3.6 (i, ii).

Definition 3.8. **Let $[r],[s] \in Z_{2n}$. We define an operation '.' On Z_{2n} by**

(i) $[r].[s] = [r+s]$, *if s is even, and*

(ii) $[r].[s] = [-r+s] = [2n-r+s]$, *if s is odd.*

Lemma 3.9. The binary operation '.' on Z_{2n} defined by definition 3.8 (i, ii) is well defined.

Proof. Let $a_1, a_2, b_1, b_2 \in Z$. Let $[a_1] = [a_2]$ and $[b_1] = [b_2]$. Then from lemma 3.5, We get $a_1 - a_2 = 2nq_1$, and $b_1 - b_2 = 2nq_2$ for some $q_1, q_2 \in Z$, implies $(a_1 + b_1) - (a_2 + b_2) = 2n(q_1 + q_2)$ and $(-a_1 + b_1) - (-a_2 + b_2) = 2n(q_2 - q_1)$, b_1 and b_2 both are even or both are odd, implies $[a_1 + b_1] = [a_2 + b_2]$ and $[-a_1 + b_1] = [-a_2 + b_2]$, b_1 and b_2 both are even or both are odd. Then from definition 3.8 (i,ii), We get $[a_1].[b_1] = [a_2].[b_2]$. From lemma 3.6(iii), We get $[-r+s] = [2n-r+s]$.

Lemma 3.10. Z_{2n} is closed under '.', that is $[r],[s] \in Z_{2n} \Rightarrow [r].[s] \in Z_{2n}$, $\forall [r],[s] \in Z_{2n}$.

Proof . The proof follows from lemma 3.6 (i, iii) and definition 3.8 (i, ii).

Lemma 3.11. Z_{2n} is associative under '.'. That is $[r].([s].[t]) = ([r].[s]).[t], \forall [r],[s],[t] \in Z_{2n}$.

Proof. Let s be even and t be even. Then from definition 3.8 (i), We get $[r].([s].[t]) = [r].([s+t]) = [r+s+t] = [r+s].[t] = ([r].[s]).[t]$.

Let s be even and t be odd. Then from definition 3.8 (ii), We get $[r].([s].[t]) = [r].[-s+t] = [-r-s+t] = [r+s].[t] = ([r].[s]).[t]$.

Let s be odd and t be even. Then from definition 3.8 (i, ii), We get $[r].([s].[t]) = [r].[s+t] = [-r+s+t] = [-r+s].[t] = ([r].[s]).[t]$.

Let s be odd and t be odd. Then from definition 3.8 (i, ii), We get $[r].([s].[t]) = [r].[-s+t] = [r-s+t] = [-r+s].[t] = ([r].[s]).[t]$.

Lemma 3.12. [0] is identity of Z_{2n} under '.'. That is $[r].[0] = [0].[r] = [r], \forall [r] \in Z_{2n}$.

Proof. Let $[r] \in Z_{2n}$. if r is even, then from definition 3.8(i), We get $[r].[0] = [r+0] = [r] = [0+r] = [0].[r]$. If r is odd, then from definition 3.8 (i, ii), We get $[r].[0] = [r+0] = [r] = [-0+r] = [0].[r]$.

Lemma 3.13. Let $[r] \in Z_{2n}$. Then inverse of [r] under '.' is given by

(i) $[r]^{-1} = [-r] = [2n-r]$, if r is even, and

(ii) $[r]^{-1} = [r]$, if r is odd.

Proof. Let [r] ∈ Z_{2n}. If r is even, then from definition 3.8 (i), We get $[r].[-r] = [r-r] = [0] = [-r+r] = [-r].[r]$, implies $[r]^{-1} = [-r]$. If r is odd, then from definition 3.8(ii), We get $[r].[r] = [-r+r] = [0]$, implies $[r]^{-1} = [r]$. Also from lemma 3.6(iii), We get $[-r] = [2n-r]$.

Lemma 3.14. ***Z_{2n} is not commutative for $n \geq 3$ under ∵***

Proof. Let $[1],[2] \in Z_{2n}$. Then from definition 3.8 (i, ii), We get $[1].[2] = [1+2] = [3]$ and $[2].[1] = [-2+1] = [-1] = [2n-1]$, by lemma 3.6 (iii). If $n \geq 3$, then $2n-1 \neq 3$ and $0 \leq 2n-1, 3 < 2n$. Then from lemma 3.6(ii), We get $[3] \neq [2n-1]$. Then it follows that $[1].[2] \neq [2].[1]$.

Theorem 3.15. ***The set Z_{2n} of residue classes modulo 2n forms a group of order 2n under ∵ Further Z_{2n} is non-abelian for $n \geq 3$.***

Proof. The proof follows from lemma 3.7, definition 3.8 and lemma (3.9, 3.10, 3.11, 3.12, 3.13, 3.14).

Theorem 3.16. The dihedral group D_n of degree n has a new representation as a group of residue classes modulo 2n given by

$\boldsymbol{D_n = Z_{2n} = \{[r] | 0 \leq r < 2n\} = \{[2r],[2r+1] | 0 \leq r < n\}}$ ***under ∵ defined by definition 3.8 (i, ii).***

Proof. Let D_n be dihedral group of degree n defined by definition 2.1 [3,4]. We define a mapping $f: Z_{2n} \to D_n$ from Z_{2n} into D_n by $f([2r]) = x^r$ and $f([2r+1]) = yx^r$, where r = 0,1,2 ..., (n-1). Let $[l],[m] \in Z_{2n}$.

Let $l = 2r$ and $m = 2t+1$. Then from definition 2.1 (i, ii), definition 3.8 (ii) and definition of f, We get $f([l].[m]) = f([2r].[2t+1]) = f([-2r+2t+1]) = f([2(-r+t)+1]) = yx^{-r+t} = yx^t x^{-r} = x^r yx^t = f([2r])f([2t+1]) = f([l])f([m])$.

Let $l = 2r$ and $m = 2t$. Then from definition 3.8 (i) and definition of f, We get $f([l].[m]) = f([2r].[2t]) = f([2r+2t]) = f([2(r+t)]) = x^{r+t} = x^r x^t = f([2r])f([2t]) = f([l])f([m])$.

Let $l = 2r+1$ and $m = 2t$. Then from definition 3.8 (i) and definition of f, We get $f([l].[m]) = f([2r+1].[2t]) = f([2r+1+2t]) = f([2(r+t)+1]) = yx^{r+t} = yx^r x^t$

$= f([2r+1])f([2t]) = f([l])f([m])$.

Let $l = 2r + 1$ and $m = 2t + 1$. Then from definition 2.1 (ii), definition 3.8 (ii) and definition of f, We get $f([l].[m]) = f([2r + 1].[2t + 1]) = f([-2r + 2t]) = ([2(-r + t)]) = x^{-r+t} = x^{-r}x^t = x^{-r}.1.x^t = x^{-r}y^2x^t = x^{-r}yyx^t = yx^ryx^t = f([2r + 1])f([2t + 1]) = f([l])f([m])$.

It follows that f is a homomorphism. From definition 2.1(i,ii), lemma 3.7 and definition of f, it follows that f is one-one and onto. Hence We get $Z_{2n} \cong D_n$. Then the proof follows from lemma 3.7 and theorem 3.15.

Definition 3.17. *Let D_n be dihedral group of degree n given by theorem 3.16. Then $[r] \in D_n$ will be called even or odd element of D_n according as r is even or odd.*

Lemma 3.18. Let E and O be defined by

(i) $E = \{[2r] | 0 \le r < n\}$, *and*

(ii) $O = \{[2r + 1] | 0 \le r < n\}$.

Then E and O are sets of even and odd elements of D_n and

(iii) $D_n = E \cup O, E \cap O = \emptyset = null$,

(iv) $|E| = n,\ |O| = n$ *and* $|D_n| = 2n$.

Proof. The proof follows from theorem 3.16.

Lemma 3.19. Let D_n be dihedral group of degree n and $[s], [2r], [2r + 1], [l] \in D_n$. Then,

(i) $K[2r] = [K(2r)]$, for any positive integer K,

(ii) $L[2r + 1] = [0]$, if L is even,

(iii) $L[2r + 1] = [2r + 1]$, *if L is Odd*, and

(iv) $[s] = [l] \Leftrightarrow [s - l] = [0]$,

where N[r] denote the N-th power of $[r] \in D_n$. That is $N[r] = [r]^N$.

Proof. (i) From definition 3.8 (i), We get, $1[2r] = [2r], 2[2r] = [2r].[2r] = [2r + 2r] = [2(2r)], 3[(2r)] = 2[2r].[2r] = [2(2r)].[2r] = [2(2r) + 2r] = [3(2r)]$. Continuing, We get, $K[2r] = [K(2r)]$.

(ii) Let L be even. Then L = 2q for some $q \in Z$. Then from definition 3.8 (ii) and lemma 3.19(i), We get, $L[2r + 1] = 2q[2r + 1] = q([2r + 1].[2r + 1]) = q[-2r - 1 + 2r + 1] = q[0] = [q(0)] = [0]$.

(iii) Let L be odd. Then L = 2q+1 for some $q \in Z$.

Then from lemma 3.19(ii) and definition 3.8 (ii), We get, $L[2r + 1] = (2q + 1)[2r + 1] = 2q[2r + 1].[2r + 1] = [0].[2r + 1] = [-0 + 2r + 1] = [2r + 1]$.

(iv) Using lemma 3.5 and lemma 3.6 (iv), We get,

$[s] = [l] \Leftrightarrow s - l = 2nq \Leftrightarrow [s - l] = [2nq] = [0]$.

4. The (N,M)-th Commutativity Degree Of Dihedral Groups

Definition 4.1. We define the (N,M)-th commutativity degree $P_N^M(G)$ of a finite group G by

$$\boldsymbol{P_N^M(G) = |\{(x,y) \in G \times G | x^N y^M = y^M x^N\}| / (|G|^2)},$$

for positive integers N and M.

Definition 4.2. The (N, M)-th commutativity set $C_N^M(A \times B)$ of A×B subset of $D_n \times D_n$ is defined by

$$\boldsymbol{C_N^M(A \times B) = \{([r],[s]) \in A \times B | N[r].M[s] = M[s].N[r]\}},$$

where We define L[r]=$[r]^L$ for any integer L.

Lemma 4.3. Let D_n be dihedral group of degree n. Then,

$$\boldsymbol{P_N^M(D_n) = \left[|C_N^M(E \times E)| + |C_N^M(E \times O)| + |C_N^M(O \times E)| + |C_N^M(O \times O)|\right] / (4n^2)}.$$

Proof. From definition (4.1, 4.2), for $G = D_n$ and $|D_n| = 2n$, We get,

$$\boldsymbol{P_N^M(D_n) = |\{([r],[s]) \in D_n \times D_n | N[r].M[s] = M[s].N[r]\}| / (4n^2)}, \textit{ and}$$

$$\boldsymbol{C_N^M(D_n \times D_n) = \{([r],[s]) \in D_n \times D_n | N[r].M[s] = M[s].N[r]\}}.$$

Then, We get, $P_N^M(D_n) = |C_N^M(D_n \times D_n)| / (4n^2)$. From lemma 3.18(iii, iv), We get $D_n \times D_n = (E \times E) \cup (E \times O) \cup (O \times E) \cup (O \times O)$, where any two of $E \times E$, $E \times O$, $O \times E$ and $O \times O$ are disjoint. Then using definition 4.2, We get, $|C_N^M(D_n \times D_n)| = |C_N^M(E \times E)| + |C_N^M(E \times O)| + |C_N^M(O \times E)| + |C_N^M(O \times O)|$. Then We get lemma 4.3.

Lemma 4.4. Let D_n be dihedral group of degree n. Then ,

(i) $P_N^1(D_n) = P_N(D_n)$, and

(ii) $P_1^1(D_n) = P(D_n)$.

Proof . The proof follows from definition (2.2, 2.3, 4.1) for G = D_n.

Lemma 4.5. $|C_K^L(A \times B)| = |C_L^K(B \times A)|$, ***for any L and K.***

Proof. From definition 4.2, We get, $C_K^L(A \times B) = \{([r],[s]) \in A \times B | K[r].L[s] = L[s].K[r]\}$ and $C_L^K(B \times A) = \{([s],[r]) \in B \times A | L[s].K[r] = K[r].L[s]\}$. Then it follows that $([r],[s]) \in C_K^L(A \times B) \Leftrightarrow ([s],[r]) \in C_L^K(B \times A)$, implies $|C_K^L(A \times B)| = |C_L^K(B \times A)|$.

Lemma 4.6. Let D_n be dihedral group of degree n. Then,

(i) $|C_K^L(E \times O)| = |C_L^K(O \times E)| = |C_K^1(E \times O)| = |C_1^K(O \times E)|$, if L is odd and K is any integer,

(ii) $|C_K^L(O\times O)| = |C_L^K(O\times O)| = |C_1^1(O\times O)|$, if L and K both are odd,

(iii) $|C_K^L(E\times O)| = |C_L^K(O\times E)| = |C_K^L(O\times O)| = |C_L^K(O\times O)| = n^2$, if L is even and K is any integer, and

(iv) $|C_K^L(E\times E)| = n^2$, if L and K are any positive integer.

Proof.

(i) From definition 4.2, We get, $C_K^L(E\times O) = \{([r],[s]) \in E\times O | K[r].L[s] = L[s].K[r]\}$ and $C_K^1(E\times O) = \{([r],[s]) \in E\times O | K[r].[s] = [s].K[r]\}$. Let L be odd. Then from lemma 3.19 (iii), We get, $L[s] = [s]$. Then it follows that $C_K^L(E\times O) = C_K^1(E\times O)$, implies $|C_K^L(E\times O)| = |C_K^1(E\times O)|$. Then using lemma 4.5, We get lemma 4.6 (i).

(ii) From definition 4.2, We get $C_K^L(O\times O) = \{([r],[s]) \in O\times O | K[r].L[s] = L[s].K[r]\}$ and $C_K^1(O\times O) = \{([r],[s]) \in O\times O | [r].[s] = [s].[r]\}$. If L and K both are odd, then from lemma 3.19 (iii), We get L[s] = [s] and K[r] = [r]. Then it follows that

$C_K^L(O\times O) = C_1^1(O\times O), implies\ |C_K^L(O\times O)| = |C_1^1(O\times O)|$. Then, using lemma 4.5, We get lemma 4.6 (ii).

(iii) From definition 4.2, We get $C_K^L(E\times O) = \{([r],[s]) \in E\times O | K[r].L[s] = L[s].K[r]\}$ and $C_K^L(O\times O) = \{([r],[s]) \in O\times O | K[r].L[s] = L[s].K[r]\}$. If L is even, then from Lemma 3.19 (ii) , We get $L[s] = [0]$. Then from lemma 3.12, We get $K[r].L[s] = L[s].K[r]$, $\forall\ [r] \in D_n, \forall\ [s] \in O$. Then it follows that,

$C_K^L(E\times O) = E\times O, C_K^L(O\times O) = O\times O.$

Then from lemma 3.18 (iv), We get $|C_K^L(E\times O)| = |E||O| = n.n = n^2$ and $|C_K^L(O\times O)| = |O||O| = n.n = n^2$. Then from lemma 4.5, We get lemma 4.6 (iii).

(iv) From definition 4.2, We get $C_K^L(E\times E) = \{([r],[s]) \in E\times E | K[r].L[s] = L[s].K[r]\}$. Since [r] and [s] are even, so from 3.19 (i), it follows that K[r] and L[s] are even. From definition 3.8(i), We get $K[r].L[s] = [Kr].[Ls] = [Kr + Ls] = [Ls + Kr] = [Ls].[Kr]$

$= L[s].K[r], \forall\ [r],[s] \in E$. Then It follows that $|C_K^L(E\times E)| = |E\times E| = |E|.|E| = n^2$ using lemma 3.18 (iv).

Lemma 4.7. If K is any positive integer and $[2t] \in D_n$***, then*** $K[2t] = [0]$ ***has p = (n, K) number of solutions as*** $[2t] = [2vc]$, $0 \le v < p, c = n / p$.

Proof. Let p = greatest common divisor of n and K = (n, K). Then n = pc, K = pd, (d, c) = 1. Let [2t] ∈ D_n and $K[2t] = [0]$. Let $0 \le 2t < 2n$. Then, from lemma 3.19(i), We get [2Kt] = [0]. Then from lemma 3.5, We get $K(2t) = 2rn$, for some r, $0 \le 2t < 2n$, implies $t = rn/K, K\backslash rn (K\ divides\ rn), 0 \le 2rn/K < 2n$, implies, $t = rpc\ /pd,\ pd\backslash rpc,\ 0 \le 2rpc/pd < 2pc,\ c = n/p,\ p = (n, K), (d, c) = 1,\ implies\ t = rc/d,\ d\backslash r, 0 \le r/d < p, c = n/p,\ p = (n, K),\ implies\ t = vdc/d, r = vd, 0 \le vd/d < p, c = n/p, p = (n, K), implies\ t = vc, 0 \le v < p, c = n/p, p = (n, K),\ implies\ [2t] = [2vc], 0 \le v < p, c = n/p, t = vc, p = (n, K). Now\ 0 \le v < p, c = n/p, implies\ 0 \le 2vc < 2pc, 0 \le v < p, c = n/p, implies\ 0 \le 2vc < 2n\ for\ 0 \le v < p.$ Then from lemma 3.6 (ii), it follows that [2t] = [2vc], for v = 0,1,2…, (p-1), are p = (n, K) different elements of D_n. Let t be any integer. Then by division algorithm We get $2t = 2nq + 2l, 0 \le 2l < 2n$. Then from lemma 3.6(iii), We get $[2t] = [2nq + 2l] = [2l], 0 \le 2l \le 2n$, implies $K[2t] = K[2l]$ and $K[2t] = [0] \Leftrightarrow K[2l] = [0], 0 \le 2l < n$. Then by previous case We get the theorem.

Lemma 4.8. ***Let K be any integer. Then*** $|C_K^1(E \times O)| = |C_1^K(O \times E)| = (n, 2K)n$.

Proof. **From definition 4.2, We get** $C_K^1(E \times O) = \{([2t], [2r+1]) \in E \times O | K[2t].[2r+1] = [2r+1].K[2t]\}$. Then from definition 3.8 (i,ii) and lemma 3.19 (i, iv), We get $C_K^1(E \times O) = \{([2t], [2r+1]) \in E \times O | 2K[2t] = [0]\}$. Then from lemma 3.18(iv) and lemma 4.7, We get $C_K^1(E \times O) = \{([2vc], [2r+1]) | 0 \le v < p,\ 0 \le r < n,\ p = (n, 2K), c = n/p\}$, implies $|C_K^1(E \times O)| = pn = (n, 2K)n$. From lemma 4.5, We get $|C_1^K(O \times E)| = |C_K^1(E \times O)| = (n, 2K)n$.

Lemma 4.9. $|\mathbf{C_1^1(O \times O)}| = (\mathbf{n}, \mathbf{2})\mathbf{n}$.

Proof. From definition 4.2, We get $C_1^1(O \times O) = \{([2t+1], [2r+1]) \in O \times O | [2t+1].[2r+1] = [2r+1].[2t+1]\}$. Then from definition 3.8 (ii) and lemma 3.19 (iv), We get $C_1^1(O \times O) = \{([2t+1], [2r+1]) \in O \times O | 2[2(t-r)] = [0]\}$. Then from lemma 3.18 (iv), lemma 3.19(iv) and lemma 4.7, We get $C_1^1(O \times O) = \{([2t+1], [2r+1]) | [2t - 2r] = [2vc],\ 0 \le v < p, 0 \le r < n,\ c = n/p,\ p = (n, 2)\}$ = $\{([2vc + 2r + 1], [2r+1]) | 0 \le v < p,\ 0 \le r < n, c = n/p, p = (n, 2)\}$,

implies $|C_1^1(O \times O)| = \mathrm{pn} = (\mathrm{n}, 2)\mathrm{n}$.

Theorem 4.10. If N and M both are odd positive integers, then,

$P_N^M(D_n) = [n + (n, 2N) + (n, 2M) + (n, 2)]/[4n]$.

Proof. Let N and M both be odd. Then from lemma 4.6 (i, ii, iv), lemma 4.8 and lemma 4.9, We get $|C_N^M(E\times O)| = |C_N^1(E\times O)| = (n,2N)n$, $|C_N^M(O\times E)| = |C_1^M(O\times E)| = (n,2M)n$, $|C_N^M(O\times O)| = |C_1^1(O\times O)| = (n,2)n$ and $|C_N^M(E\times E)| = n^2$. Then from lemma 4.3, We get $P_N^M(D_n) = [n^2 + (n,2N)n + (n,2M)n + (n,2)n]/[4n^2]$=$[n + (n,2N) + (n,2M) + (n,2)]/[4n]$.

Theorem 4.11. If N is even and M is odd, then,

$P_N^M(D_n) = [3n + (n,2N)]/[4n]$.

Proof. Let N be even and M be odd. Then from lemma 4.6 (i,ii,iii) and lemma 4.8, We get,

$|C_N^M(E\times O)| = |C_N^1(E\times O)| = (n,2N)n, |C_N^M(O\times E)| = n^2, |C_N^M(O\times O)| = n^2$

and $|C_N^M(E\times E)| = n^2$. Then from lemma 4.3, We get $P_N^M(D_n) = [n^2 + (n,2N)n + n^2 + n^2]/[4n^2] = [3n + (n,2N)]/(4n)$.

Theorem 4.12. If N is odd and M is even, then,

$P_N^M(D_n) = [3n + (n,2M)]/[4n]$.

Proof. Let N be odd and M be even. Then from lemma 4.6 (i, iii, iv) and lemma 4.8, We get

$|C_N^M(E\times O)| = n^2, |C_N^M(O\times E)| = |C_1^M(O\times E)| = (n,2M)n, |C_N^M(O\times O)| = n^2 \ and$

$|C_N^M(E\times E)| = n^2$. Then from lemma 4.3, We get

$P_N^M(D_n) = [n^2 + n^2 + (n,2M)n + n^2]/[4n^2] = [3n + (n,2M)]/[4n]$.

Theorem 4.13. If N and M both are even, then, $P_N^M(D_n) = 1$.

Proof. Let N and M both be even. Then from lemma 4.6 (iii, iv), We get $|C_N^M(E\times O)| = n^2$, $|C_N^M(O\times E)| = n^2$, $|C_N^M(O\times O)| = n^2$ and $|C_N^M(E\times E)| = n^2$. Then from lemma 4.3 We get $P_N^M(D_n) = [n^2 + n^2 + n^2 + n^2]/[4n^2]$ =1.

Theorem 4.14. The N-th commutativity degree of dihedral group of degree n is given by

(i) $P_N^1(D_n) = P_N(D_n)$ = $[n + (n,2N) + 2(n,2)]/[4n]$, if N is odd and

(ii) $P_N^1(D_n) = P_N(D_n)$ = $[3n + (n,2N)]/[4n]$, if N is even.

Proof. The proof follows from lemma 4.4(i), theorem 4.10 and theorem 4.11, for M = 1.

Theorem 4.15. Let D_n be dihedral group of degree n. Then,

$P_1^1(D_n) = P(D_n)$ = $[n + 3(n,2)]/[4n]$.

Proof. The proof follows from lemma 4.4(ii) and theorem 4.14 (i) for N = 1.

Theorem 4.16[2]. Let D_n be dihedral group of degree n, where $n \geq 3, d = g.c.d.(n, N)$ and

$r = n/d$. Then,

(i) $P_N(D_n) = 1/4 + 1/(2n) + 1/(4r)$, n is odd, N is odd,

(ii) $P_N(D_n) = 1/4 + 2[1/(2n) + 1/(4r)]$, n is even, N is odd,

(iii) $P_N(D_n) = 3/4 + 1/(2r)$, r is even, N is even,

(iv) $P_N(D_n) = 3/4 + 1/(4r)$, r *is odd*, N *is even.*

Proof. Let d = g.c.d.(n, N) and $r = n/d = n/(n, N)$. Then $(n, N) = n/r$. Le N be odd. If n is odd, then (n, 2) = 1 and $(n, 2N) = (n, N) = n/r$. If n is even, then $(n, 2) = 2$ and $(n, 2N) = 2(n, N) = 2n/r$. Let N be even. If $r = n/d = n/(n, N)$ is even, then $(n, 2N) = 2(n, N) = 2n/r$. If r is odd, then, $(n, 2N) = (n, N) = n/r$. Then proof follows from theorem 4.14 by putting the values of $(n, 2)$ *and* $(n, 2N)$.

Theorem 4.17 [1]. Let D_n be dihedral group of degree n. Then, (i) $P(D_n) = (n + 3)/(4n)$, if n is odd and (ii) $P(D_n) = (n + 6)/(4n)$, if n is even.

Proof. Let n be odd, then $(n, 2) = 1$. Let n be even, then $(n, 2) = 2$. Then the proof follows from theorem 4.15 by putting the values of (n, 2).

Theorem 4.18 [6,7]. Let D_4 be dihedral group of degree 4. Then,

(i) $P_N(D_4) = 5/8$, if N is odd and

(ii) $P_N(D_4) = 1$, if N is even.

Proof. Let n = 4. Then (n, 2) = (4, 2) = 2. If N is odd, then (n, 2N) = (4, 2N) = 2. If N is even, then (n, 2N) = (4, 2N) = 4. Then from theorem 4.14 (i, ii), We get $P_N(D_4) = 5/8$, if N is odd and $P_N(D_4) = 1$, if N is even.

5. The Relative (N,M)-th Commutativity Degree Of Dihedral Groups

Definition 5.1. *The relative (N,M)-th commutativity degree*

$P_N^M(G, G)$ of a finite group G is defined by

$P_N^M(G, G) = P(G^N, G^M) = |\{(x, y) \in G^N \times G^M | xy = yx\}|/(|G^N||G^M|)$, for positive integers N and M. Then $P_N^M(G, G)$ is the probability that a random element of G^N commutes with a random element of G^M.

Definition. 5.2. The commutativity set $C(A \times B)$ of $(A \times B)$ subset of $D_n \times D_n$ is defined by

$\boldsymbol{C(A \times B) = \{([r], [s]) \in A \times B | [r].[s] = [s].[r]\}}$.

Lemma 5.3. The relative (N,M)-th commutativity degree of dihedral group D_n is given by

$P_N^M(D_n, D_n) = |C(ND_n \times MD_n)|/(|ND_n||MD_n|)$, where We define $KA = A^K$, the set of distinct elements of K-th power of elements of A, for any subset A of D_n.

Proof. From definition 5.1, for G $= D_n$, We get $P_N^M(D_n) = |\{([r],[s]) \in ND_n \times MD_n | [r].[s] = [s].[r]\}| / (|ND_n||MD_n|)$.

From definition 5.2, for A = ND_n and B = MD_n , We get $C(ND_n \times MD_n) = \{([r],[s]) \in ND_n \times MD_n | [r].[s] = [s].[r]\}$. Then We get lemma 5.3.

Lemma 5.4. If D_n is dihedral group of degree n. Then,

(i) $P_N^1(D_n, D_n) = P_N(D_n, D_n)$, and

(ii) $P_1^1(D_n, D_n) = P_1^1(D_n) = P(D_n)$.

Proof. The proof follows from definition (2.2, 2.5, 4.1, 5.1) for G = D_n.

Lemma 5.5. Let E and O be the sets of even and odd elements of D_n *respectively. If K is any positive integer and* $KE = \{K[2t] | [2t] \in E\}$, *Then,*

(i) $|KE| = n/(n,K)$, and

(ii) $|C(KE \times O)| = |C(O \times KE)| = [(n,2K)n]/(n,K)$.

Proof. Let [2r],[2t]$\in E$. We define a relation ~ on E by $[2r] \sim [2t] \Leftrightarrow K[2r] = K[2t]$. Then it is easy to see that ~ is an equivalence relation on E and decomposes E into disjoint equivalence classes. Let $[\overline{2r}]$ be the class containing [2r]. Then $[\overline{2r}] = \{[2t] \in E | K[2t] = K[2r]\}$. Then from lemma 3.19 (i, iv), We get $[\overline{2r}] = \{[2t] \in E | K[2(t-r)] = [0]\}$. Then from lemma 4.7, We get $|[\overline{2r}]| = (n,K)$. Let there be l distinct classes. Then, $l(n,K) = |E|$. Then from lemma 3.18 (iv), We get $l(n,K) = n$, implies $l = n/(n,K)$. If $[2t],[2s] \in [\overline{2r}]$, then $K[2t] = K[2s]$ and so one element of KE will be obtained from all the elements of one class. Then it follows that $|KE| = l = n/(n,K)$, Which is lemma 5.5(i).

Let $P = \{[2t] \in E | K[2t].[2r+1] = [2r+1].K[2t]$, for some $[2r+1] \in O\}$. Then using definition 3.8 (i, ii) and lemma 3.19 (i, ii), We get $P = \{[2t] \in E | 2K[2t] = [0]\}$. Then from lemma 4.7, We get $P = \{[2vc] | 0 \leq v < p, p = (n,2K), c = n/p\}$ and $|P| = (n,2K)$, implies P is independent of [2r+1], implies, $K[2t].[2r+1] = [2r+1].K[2t]$, $\forall [2t] \in P, \forall [2r+1] \in O$. Then it follows that every element of KE obtained from P will commute with all n odd elements of O. Let $[2t] \in P$ and $[2s] \in [\overline{2t}]$. Then, $K[2t].[2r+1] = [2r+1].K[2t], \forall [2r+1] \in O, and\ K[2s] = K[2t]$, implies, $K[2s].[2r+1] = [2r+1].K[2s], \forall [2r+1] \in O$, implies $[2s] \in P$. Then it follows that P is union of some q equivalence classes. Then it follows that $q.(n,K) = |P| = (n,2K)$, implies, $q = (n,2K)/(n,K)$. Also it follows that q elements of KE will be obtained from elements of P and these q elements of KE will commute with all n odd elements of O. Then from definition of P and definition 5.2, We get,

$|C(KE \times O)| = |\{([r],[s]) \in KE \times O| \ \ [r].[s] = [s].[r]\}| = qn = \{(n,2K)/\,(n,K)\}.n = \{(n,2K)n\}/(n,K)$. From definition 5.2, We get $C(KE \times O) = \{([r],[s]) \in KE \times O|[r].[s] = [s].[r]\}$ and $C(O \times KE) = \{([s],[r]) \in O \times KE|[s].[r] = [r].[s]\}$.

Then, $([r],[s]) \in (KE \times O) \Leftrightarrow [r].[s] = [s].[r] \Leftrightarrow [s].[r] = [r].[s] \Leftrightarrow ([s],[r]) \in C(O \times KE)$.

Then it follows that $|C(O \times KE)| = |C(KE \times O)| = \{(n,2K)n\}/(n,K)$, which is lemma 5.5 (ii).

Lemma 5.6. Let E and O be the sets of even and odd elements of D_n respectively. Then,

(i) $|C(KE \times LE)| = (n^2)/\{(n,K)(n,L)\}$, for any positive integers K and L, and

(ii) $|C(O \times O)| = (n,2)n$.

Proof .

(i) From definition 5.2, We get $C(KE \times LE) = \{([r],[s]) \in KE \times LE|[r].[s] = [s].[r]\}$.

From lemma 3.19 (i) it follows that elements of KE and LE are always even for any K and L. From definition 3.8(i), it follows that any two even elements will always commute. Then it follows that $|C(KE \times LE)| = |KE||LE|$.

Then from lemma 5.5(i), We get, $|C(KE \times LE)| = \{n/\,(n\,,K)\}.\{n/\,(n,L)\} = (n^2)/\{(n,K)(n,L)\}$.

(ii) From definition (4.2, 5.2), We get

$C_1^1(O \times O) = C(O \times O) = \{([r],[s]) \in O \times O|[r].[s] = [s].[r]\}$. Then, using lemma 4.9 We get,

$|C(O \times O)| = |C_1^1(O \times O)| = (n,2)n$.

Lemma 5.7. Let E and O be the sets of even and odd elements of D_n respectively.

Let $KE = \{K[2t]|[2t] \in E\}$ *and* $LO = \{L[2r+1]|[2r+1] \in O\}$. *Then,*

(i) $[0] \in KE$, for any integer K,

(ii) LO = O, if L is odd integer,

(iii) LO = {[0]}, if L is even integer,

(iv) $KE \cap O = \emptyset = null$, for any integer K, and

(v) $|KE \cup O| = \{n/(n,K)\} + n$, for any integer K.

Proof.

(i) From lemma 3.18(i), We get $[0] \in E. Then\ using\ lemma\ 3.19(i),\ We\ get\ K[0] = K[2(0)] = [K\ (2(0))] = [0] \in KE.$

(ii) Let L be odd and $[2r+1] \in O$. Then from lemma 3.19(iii), We get $L[2r+1] = [2r+1]$. Then $LO = \{L[2r+1] | [2r+1] \in O\} = \{[2r+1] | [2r+1] \in O\} = O$

(iii) Let L be even and $[2r+1] \in O$. Then from lemma 3.19(ii), We get $L[2r+1] = [0]$. Then $LO = \{L[2r+1] | [2r+1] \in O\} = \{[0] | [2r+1] \in O\} = \{[0]\}$.

(iv) From lemma 3.19(i), it follows that elements of $KE = \{K[2t] | [2t] \in E\} = \{[2Kt] | [2t] \in E\}$ are even. But elements of O are odd. Therefore $KE \cap O = \emptyset = null$.

(v) From (iv), We get $KE \cap O = \emptyset$ so We get $|KE \cup O| = |KE| + |O|$. Then from 3.18(iv) and lemma 5.5(i), We get $|KE \cup O| = \{n/(n,K)\} + \text{n}$.

Theorem 5.8. Let N and M both be odd. Then,

$$P_N^M(D_n, D_n) = [n + (n,2N)(n,M) + (n,2M)(n,N) + (n,2)(n,N)(n,M)]/[n\{1+(n,N)\}\{1+(n,M)\}].$$

Proof . Let N and M both be odd. Then using lemma 3.18(iii) and lemma 5.7(ii), We get $ND_n = NE \cup NO = NE \cup O$ and $MD_n = ME \cup MO = ME \cup O$. Then using lemma 5.7 (v), We get $|ND_n| = \{n/(n,N)\} + n$ and $|MD_n| = \{n/(n,M)\} + n$. From lemma 5.7(iv), it follows that any two of $NE \times ME, NE \times O, O \times ME\ and\ O \times O$ are disjoint. Then using definition 5.2, We get $|C(ND_n \times MD_n)| = |C\{(NE \cup O) \times (ME \cup O)\}| = |C(NE \times ME)| + |C(NE \times O)| + |C(O \times ME)| + |C(O \times O)|$. Then using lemma 5.5 (ii) and lemma 5.6(i, ii), We get $|C(ND_n \times MD_n)| = (\text{n}^2)/\{(\text{n},\text{N})(\text{n},\text{M})\} + \{(\text{n},2\text{N})\text{n}\}/(\text{n},\text{N}) + \{(n,2M)n\}/(n,M) + (n,2)n$. Then using lemma 5.3 We get $P_N^M(D_n, D_n) = |C(ND_n \times MD_n)|/(|ND_n||MD_n|)$

$= [(n^2)/\{(\text{n, N}) (\text{n, M})\} + \{(\text{n, 2N}) \text{n}\}/ (\text{n, N}) + \{(\text{n, 2M}) \text{n}\}/(\text{n, M}) + (\text{n, 2}) \text{n}]/ [\{\text{n}/(\text{n, N})+\text{n}\}\{(\text{n}/(\text{n, M})+\text{n}\}]$

$= [n + (n,2N)(n,M) + (n,2M)(n,N) + (n,2)(n,N)(n,M)] / [n\{1+(n,N)\}\{1+(n,M)\}].$

Theroem 5.9. Let N be even and M be odd. Then,

$P_N^M(D_n, D_n) = [n + (n,2N)(n,M)]/ [n\{1+(n,M)\}].$

Proof. Let N be even and M be odd. Then using lemma 3.18(iii) and lemma 5.7(i, ii, iii), We get

$$ND_n = NE \cup NO = NE \cup \{[0]\} = NE\ and\ MD_n = ME \cup MO = ME \cup O.$$

Then using lemma 5.5(i) and lemma 5.7(v), We get $|ND_n| = |NE| = n/(n, N)$ and $|MD_n| = |ME \cup O| = n/(n, M) + n$. From lemma 5.7(iv), it follows that NE×ME and NE×O are disjoint. Then using definition 5.2, We get $|C(ND_n \times MD_n)| = |C\{NE \times (ME \cup O)\}|$

$= |C\{(NE \times ME) \cup (NE \times O)\}| = |C(NE \times ME)| + |C(NE \times O)|$.

Then using lemma 5.5(ii) and lemma 5.6(i), We get

$|C(ND_n \times MD_n)| = (n^2)/\{(n, N)(n, M)\} + \{(n, 2N)n\}/(n, N)$.

Then using lemma 5.3, We get $P_N^M(D_n, D_n) = |C(ND_n \times MD_n)|/(|ND_n||MD_n|) =$

$[(n^2)/\{(n, N)(n, M)\} + \{(n, 2N)n\}/(n, N)]/[\{n/(n, N)\}\{n/(n, M) + n\}] =$

$[n + (n, 2N)(n, M)] / [n\{1 + (n, M)\}]$.

Theorem 5.10. Let N be odd and M be even. Then,

$P_N^M(D_n, D_n) = [n + (n, 2M)(n, N)]/[n\{1 + (n, N)\}]$.

Proof. Let N be odd and M be even. Then from lemma 3.18(iii) and lemma 5.7 (i, ii, iii), We get $ND_n = NE \cup NO = NE \cup O$ and $MD_n = ME \cup MO = ME \cup \{[0]\} = ME$. Then from lemma 5.5(i) and lemma 5.7(v) We get $|ND_n| = |NE \cup O| = \{n/(n, N)\} + n$ and $|MD_n| = |ME| = n/(n, M)$. From lemma 5.7(iv), it follows that $NE \times ME$ and $O \times ME$ are disjoint. Then using definition 5.2, We get $|C(ND_n \times MD_n)| = |C\{(NE \cup O) \times ME\}| = |C\{(NE \times ME) \cup (O \times ME)\}|$

$=|C(NE \times ME)| + |C(O \times ME)|$. Then using lemma 5.5 (ii) and lemma 5.6(i), , We get $|C(ND_n \times MD_n)| = (n^2)/\{(n, N)(n, M)\} + \{(n, 2M)n\} / (n, M)$.

Then using lemma 5.3, We get $P_N^M(D_n, D_n) = |C(ND_n \times MD_n)|/(|ND_n||MD_n|) =$

$[(n^2)/\{(n, N)(n, M)\} + \{(n, 2M)n\}/(n, M)]/[\{n/(n, N) + n)\}\{n/(n, M)\}]$

$= [n + (n, 2M)(n, N)] / [n\{1 + (n, N)\}]$.

Theorem 5.11. Let N and M both be even. Then, $\boldsymbol{P_N^M(D_n, D_n) = 1}$.

Proof. Let N and M both be even. Then from lemma 3.18(iii) and lemma 5.7(i, iii), We get $ND_n = NE \cup NO = NE \cup \{[0]\} = NE$ and $MD_n = ME \cup MO = ME \cup \{[0]\} = ME \cup \{[0]\} = ME$. Then using lemma 5.6(i), We get $|C(ND_n \times MD_n)| = |C(NE \times ME)| = (n^2)/\{(n, N)(n, M)\}$.

Using lemma 5.5(i), We get $|(ND_n)| = |NE| = n/(n, N)$ and $|(MD_n)| = |(ME)| = n/(n, M)$. Then using lemma 5.3, We get $P_N^M(D_n, D_n) = |C(ND_n \times MD_n)|/(|ND||MD_n|) = [(n^2)/\{(n, N)(n, M)\}] / [\{n/(n, N)\}\{n/(n, M)\}] = 1$.

Theorem 5.12. The relative N-th commutativity degree of dihedral group of degree n is given by

(i) $P_N^1(D_n, D_n) = P_N(D_n, D_n) = [n + (n, 2N) + 2(n, 2)(n, N)]/[2n\{1 + (n, N)\}]$, if N is odd, and

(ii) $P_N^1(D_n, D_n) = P_N(D_n, D_n) = [n + (n, 2N)]/[2n]$, if N is even.

Proof. If M =1, then (n, M) =1 and (n, 2M) = (n, 2). Then proof follows from Theorem (5.8, 5.9).

Theorem 5.13 [10]. Let D_3 be dihedral group of degree 3, then for K, N∈ Z^+, where K=0,1,2..., the relative N-th commutativity degree of D_3, $P_N(D_3, D_3)$ is given as follows,

(i) $P_N(D_3, D_3) = 1/2;\ N = 1 + 2K,$

(ii) $P_N(D_3, D_3) = 2/3;\ N = 2 + 6K, N = 4 + 6K,$

(iii) $P_N(D_3, D_3) = 1;\ N = 6 + 6K.$

Proof. Let n = 3. $If\ N = 1 + 2K,\ then\ (3, 2N) = (3, N)\ and\ (3, 2) = 1$. Then from theorem 5.12(i) , we get $P_N(D_3, D_3) = [3 + (3, 2N) + 2(3, 2)(3, N)]/[2(3)\{1 + (3, N)\}] = [3 + (3, N) + 2(3, N)]/ [2(3)\{1 + (3, N)\}] = [3\{1 + (3, N)\}] / [2(3)\{1 + (3, N)\}] = 1/2.$ $If\ N = 2 + 6K, 4 + 6k$, then, $(n, 2N) = (3,2N) = 1$. Then from theorem 5.12 (ii), We get $P_N(D_3, D_3)$= $[3 + 1]/[2(3)] = 2/3.$ $If\ N = 6 + 6K, then\ (n, 2N) = (3, 2N) = 3$. Then, from theorem 5.12 (ii), We get $P_N(D_3, D_3) = [3 + 3]/[2(3)] = 1$.

Remark. In [10], $P_N(D_3, D_3)$ has been denoted by $P_N(D_3)$. We can obtain all the theorems of [10] from theorem 5.12 (i,ii).

Theorem 5.14. Let D_4 be dihedral group of degree 4. Then,

(i) $P_N(D_4, D_4) = P_N(D_4) = 5/8$, If N is odd and

(ii) $P_N(D_4, D_4) = P_N(D_4) = 1$ if N is even.

Proof. Let n = 4. If N is odd, then (n, 2N) = 2, (n, N) = 1 and (n, 2) = 2. Then from theorem 5.12(i) and theorem 4.14(i), We get $P_N(D_4, D_4)$ =$P_N(D_4)$ = 10/16 = 5/8. If N is even, then (n, 2N) = 4. Then from theorem 5.12 (ii) and theorem 4.14(ii), We get $P_N(D_4, D_4) = P_N(D_4) = 8/8 = 1$.

6. The Subgroups Of Dihedral Group

Definition 6.1. Let d be a positive integer such that $d\backslash n$ and $k = n/d$ or $kd = n$. Let O be the set of odd elements of D_n and $[2t + 1], [2i + 1] \in O$. We define a relation ~ on O by $[2t + 1]\sim [2i + 1] \Leftrightarrow 2d$ divides $(2t + 1 - 2i - 1) \Leftrightarrow 2t + 1 = 2rd + 2i + 1$, for some $r \in Z$.

Theorem 6.2. ***The relation $\sim$ defined by definition 6.1 is an equivalence relation on O. If $C_d[2i+1]$ is the equivalence class by $[2i+1] \in O$, then,***

(i) $C_d[2i+1] = \{[2rd+2i+1] | r \in Z\} = \{[2rd+2i+1] | 0 \le r < k\}$,

(ii) $|C_d[2i+1]| = k$, and

(iii) there are d distinct classes for $0 \le i < d$.

Proof. It is obvious that $\sim$ is an equivalence relation on O.Then ~ decomposes O into disjoint equivalence classes.

(i) Let $C_d[2i+1]$ be the equivalence class by $[2i+1] \in O$. Then $C_d[2i+1] = \{[2t+1] \in O | [2t+1] \sim [2i+1]\}$. Let $[2t+1] \in C_d[2i+1]$, implies $[2t+1] \sim [2i+1]$. Then from definition 6.1, We get $2t+1 = 2rd+2i+1$, for some $r \in Z$, implies $[2t+1] = [2rd+2i+1]$, for some $r \in Z$. Let $r \in Z$. Then $2d$ divides $(2rd+2i+1-2i-1)$. Then from definition 6.1, We get $[2rd+2i+1] \sim [2i+1]$, implies $[2rd+2i+1] \in C_d[2i+1]$. Then it follows that $C_d[2i+1] = \{[2rd+2i+1] | r \in Z\}$. Let $0 \le r_1, r_2 < k, r_1 \ne r_2$, implies, $0 \le 2r_1 d, 2r_2 d < 2kd, 2r_1 d \ne 2r_2 d$. Since $kd = n$, it follows that $0 \le 2r_1 d, 2r_2 d < 2n, 2r_1 d \ne 2r_2 d$. Then from lemma 3.6(ii), We get $[2r_1 d] \ne [2r_2 d]$. Then from lemma 3.19 (iv), We get $[2r_1 d+2i+1] \ne [2r_2 d+2i+1]$. Let $r \in Z$. Then by division algorithm We can write $r = qk + r_1, 0 \le r_1 < k$, implies $2rd+2i+1 = 2qkd+2r_1 d+2i+1 = 2nq+2r_1 d+2i+1$. Then from lemma 3.6 (iii), We get, $[2rd+2i+1] = [2nq+2r_1 d+2i+1] = [2r_1 d+2i+1], 0 \le r_1 < k$. Then it follows that $C_d[2i+1] = \{[2rd+2i+1] | r \in Z\} = \{[2rd+2i+1] | 0 \le r < k\}$ and $|C_d[2i+1]| = k$.

(ii) It follows from proof of(i).

(iii) Let there be l distinct classes. From (ii) it follows that each class has k elements. Then, We get $lk = |O|$. Then from lemma 3.18 (iv), We get $lk = n$, implies $l = n/k = d$. *Let* $[2t+1] \in O$. By division algorithm We can write $t = qd + i,\ 0 \le i < d$, implies $2t+1 = 2qd+2i+1, 0 \le i < d$. Then from definition 6.1, We get $[2t+1] \sim [2i+1], 0 \le i < d$, implies $C_d[2t+1] = C_d[2i+1]$, $0 \le i < d$. Then (iii) follows.

Theorem 6.3. The set of even elements of a subgroup H of D_n is a subgroup of H.

Proof. Let H be a subgroup of D_n . Let T be the set of even elements of H. Then $[0] \in H$, implies $[0] \in T$. Let $[2r], [2t] \in T$. implies $[2r], [2t] \in H$ implies, $[2r].[2t] \in H$. From definition 3.8(i), We get $[2r].[2t] =$

$[2r+2t] = [2(r+t)]$ which is even element. Then it follows that $[2r].[2t] \in T$. Hence T is closed and finite. Therefore T is a subgroup of H.

Theorem 6.4. Let $[2r+1], [2r] \in D_n$. Then,

(i) $O([2r+1])$ = order of $[2r+1] = 2$, and

(ii) $O([2r]) = n/(n,r)$, $r \geq 1$.

Proof. (i) From definition 3.8(ii), We get, $1[2r+1] = [2r+1], 2[2r+1] = [2r+1].[2r+1] = [-2r-1+2r+1] = [0]$, implies $O([2r+1]) = 2$.

(ii) Let $O([2r]) = m$. Then m is the least positive integer such that $m[2r] = [0]$, implies $[2mr] = [0]$ by lemma 3.19(i). Then from definition 3.1, We get $2mr = 2nq$ for some $q \in Z$, implies $m = (nq)/r$ where q is the least positive integer such that r divides nq. Let $p = (n,r)$. Then We can write $n = pl$ and $r = pa$ where l and a are relatively prime. Then $m = (lq)/a$ where q is the least positive integer such that a divides lq. Then it follows that $q = a$. Then $m = l = n/p = n/(n,r)$.

Theorem 6.5. Let $[2c] \in D_n$, $1 \leq c$ and $H = \{r[2c] | r \in Z\}$. Let $k = n/(n,c)$ or $k\,(n,c) = n$. Then H is cyclic subgroup of order k and index $2(n,c)$ given by $H = \{r[2(n,c)] = [2r(n,c)] | r \in Z\} = \{r[2(n,c)] = [2r(n,c)] | 0 \leq r < k\}$, where $2(n,c)$ is the least positive even integer such that $[2(n,c)] \in H$.

Proof. Let $[2c] \in D_n$, $1 \leq$ c and $H = \{r[2c] | r \in Z\}$. Then it is obvious that H is a cyclic subgroup generated by $[2c]$. From theorem 6.4(ii), We get $O([2c]) = n/(n,c)$. Let $k = n/(n,c)$ or $k(n,c) = n$. Then from theorem 6.4 (ii), We get $O([2(n,c)] = n/(n,(n,c)) = n/(n,c)$. Let $c = (n,c)a$. Then a and k are relatively prime. Then by Euclid division algorithm, there exists integers x and y such that $ax + ky = 1$, implies, $ax = 1 - ky$. Let $r = k + x$. Then from lemma 3.19(i), We get $r[2c] = [2rc] = [2(k+x)c] = [2(k+x)(n,c)a] = [2k(n,c)a + 2x(n,c)a] = [2na + 2(n,c)(1-ky)] = [2na + 2(n,c) - 2(n,c)ky] = [2na + 2(n,c) - 2ny] = [2n(a-y) + 2(n,c)] = [2(n,c)]$, by lemma 3.6(iii). Then it follows that $[2(n,c)] \in H$. Since $O([2c]) = O([2(n,c)]) = k$, We get that $H = \{r[2(n,c)] | r \in Z\} = \{r[2(n,c)] | 0 \leq r < k\}$, $|H| = k$, index $H = 2n/k = 2(n,c)$. Since $k(n,c) = n$, it follows that $2(n,c)$ is the least positive even integer such that $[2(n,c)] \in H$. From lemma 3.19(i), We get $r[2(n,c)] = [2r(n,c)]$.

Theorem 6.6. Let H be a subgroup of D_n. Let H contain even elements only and $2d$ be the least positive even integer such that $[2d] \in H$. Then $d \backslash n$. Let $k = n/d$ or $kd = n$. Then H is a cyclic subgroup of index $2d$ and order k given by

$H = \{r[2d] = [2rd] | r \in Z\} = \{r[2d] = [2rd] | 0 \leq r < k\}$.

Proof. Let $[2t] \in H$. Then by division algorithm We can write $t = rd + i,\ 0 \le i < d$, implies, $2t - 2rd = 2i,\ 0 \le i < d$. Now $[2t], [2d] \in H$, implies $[2t],\ r[2d] \in H$, implies $[2t], [2rd] \in H$, by lemma 3.19(i). Then $[2t].[2rd]^{-1} \in H$. Then from lemma 3.13(i) and definition 3.8 (i), We get $[2t].[2rd]^{-1} = [2t].[-2rd] = [2t - 2rd] \in H$, implies $[2i] \in H$. Since $2d$ is the least positive even integer such that $[2d] \in H$ and $[2i] \in H$ such that $0 \le 2i < 2d$, it follows that $2i = 0$. Then $[2t] = [2rd] = r[2d]$. Since H is subgroup, so $r[2d] \in H \forall r \in Z$. Therefore, $H = \{r[2d] | r \in Z\}$. Let $k = n/(n,d)$ or $k(n,d) = n$. Then from theorem 6.5 it follows that H is a cyclic subgroup of index 2(n, d) and order k given by $H = \{r[2(n,d)] = [2r(n,d)] | r \in Z\}$ $=\{r[2(n,d)] = [2r(n,d)] | 0 \le r < k\}$. where $2(n,d)$ is the least positive even integer such that $[2(n,d)] \in H$.

Therefore $2(n,d) = 2d$, implies $(n,d) = d$, Then it follows that $kd = n$ and $d \backslash n$.

Note. If $H = \{[0]\}$, then $2n$ is the least positive even integer such that $[2n] \in H$.

Theorem 6.7. *Let H be a subgroup of D_n and let H contain both even and odd dements.*

Let 2d be the least positive even integer such that [2d] ∈ H. Then d\n. Let k = n/d or kd = n . Then H is a dihedral subgroup of index d and order 2k given by $H = \{r[2d]\} | r \in Z\} \cup C_d[2l + 1] = \{[2rd], [2rd + 2l + 1] | r \in Z\} = \{[2rd], [2rd + 2l + 1] | 0 \le r < k\}$.

Where $[2l + 1]$ is any odd element of H. In particular there exists $[2i + 1] \in H$ such that $0 \le i < d$ and $H = \{[2rd], [2rd + 2i + 1] | 0 \le i < k\}$.

Proof. Let H be a subgroup of D_n and let H contain both even and odd elements. Let T be the set of even elements of H. Then from theorem 6.3 it follows that T is a subgroup of H. Then T is also a subgroup of D_n. Let $2d$ be the least positive even integer such that $[2d] \in T$. Then from theorem 6.6 it follows that $d \backslash n$. Let $k = n/d$ or $kd = n$. Then from theorem 6.6 it follows that T is a cyclic subgroup of index $2d$ and order k and $T = \{r[2d] | r \in Z\} = \{[2rd] | 0 \le r < k\}$.

Let $[2l + 1\ ]$ be any odd element of H . Then from theorem 6.2, We get $C_d[2l + 1] = \{[2rd + 2l + 1] | r \in Z\} = \{[2rd + 2l + 1] | 0 \le r < k\}$ and $|C_d[2l + 1]| = k$. Let $[2t + 1] \in H$. Then $[2l + 1].[2t + 1] \in H$. Then from definition 3.8(ii),We get $[-2l + 2t] \in H$, implies $[2t - 2l] \in T$, implies $[2t - 2l] = [2rd]$ for some $r \in Z$. Then from lemma 3.19(iv), We get $[2t + 1] = [2rd + 2l + 1]$, implies $[2t + 1] \in C_d[2l + 1]$. Now $[2d], [2l + 1] \in H$, implies $[2l + 1].r[2d] \in H\ \forall\ r \in Z$. Then from lemma 3.19(i) and definition 3.8(i), We get $[2rd + 2l + 1] \in H\ \forall\ r \in Z$. Then it follows that $H = T \cup C_d[2l + 1] =$

$\{[2rd]|r \in Z\} \cup C_d[2l+1] = \{[2rd], [2rd+2l+1]|r \in Z\} = \{[2rd],[2rd+2l+1]|0 \le r < k\}$ and $|H| = k + k = 2k$. By division algorithm, We can write $l = rd + i, 0 \le i < d$, implies $2l + 1 = 2rd + 2i + 1$. Then from definition 6.1, We get $[2l+1] \sim [2i+1]$, implies $C_d[2l+1] = C_d[2i+1]$. Then it follows that $H = \{[2rd],[2rd+2i+1]|0 \le r < k\}, [2i+1] \in H, 0 \le i < d$. Let D_k be dihedral group of degree k. Let $[s] \in D_k$. Then $[s]$ will be denoted by $[s]_k$. Therefore, $D_k = \{[2r]_k, [2r+1]_k|0 \le r < k\}$. We define a mapping $f: D_k \to H$ by $f([2r]_k) = [2rd]$ and $f([2r+1]_k) = [2rd+2i+1]$. Then using definition 3.8 (i, ii) and definition of f We get the following:

(i) $f([2r]_k.[2t]_k) = f([2r+2t]_k) = [(2r+2t)d]$

$= [2rd+2td] = [2rd].[2td] = f([2r]_k)f([2t]_k)$,

(ii) $f([2r]_k.[2t+1]_k) = f([-2r+2t+1]_k) = f([2(-r+t)+1]_k)$

$= [2(-r+t)d+2i+1] = [-2rd+2td+2i+1] = [2rd].[2td+2i+1]$

$= f([2r]_k)f([2t+1]_k)$,

(iii) $f([2r+1]_k.[2t]_k) = f([2r+1+2t]_k) = f([2(r+t)+1]_k) = [2(r+t)d+2i+1] = [2rd + 2td + 2i + 1] = [2rd+2i+1].[2td] = f([2r+1]_k)f([2t]_k)$,

(iv) $f([2r+1]_k.[2t+1]_k) = f([-2r+2t]_k) = f([2(-r+t)]_k)$

$= [2(-r+t)d] = [-2rd-2i-1+2td+2i+1]$

$= [2rd+2i+1].[2td+2i+1] = f([2r+1]_k)f([2t+1]_k)$.

Then it follows that f is homomorphism. Also it is obvious that f is one-one and onto. Then it follows that $D_k \cong H$ and hence H is a dihedral subgroup.

Theorem 6.8. Every subgroup of D_n is cyclic or dihedral. A complete listing of all subgroups of D_n is as follows:

(i) For each d such that $d \backslash n$ and $k = n/d$ or $kd = n$ there exists exactly one cyclic subgroup of index $2d$ and order k given by

$C_k^n = \{r[2d]|r \in Z\} = \{[2rd]|0 \le r < k\}$,

where $2d$ is the least positive even integer such that $[2d] \in C_k^n$.

(ii) For each d such that $d \backslash n$ and $k = n/d$ there are exactly d dihedral subgroups of index d and order $2k$ given by

$D_k^n = \{r[2d]|r \in Z\} \cup C_d[2i+1]$

$= \{[2rd], [2rd + 2i + 1] | r \in Z\}$

$= \{[2rd], [2rd + 2i + 1] | 0 \le r < k\},$

where $2d$ is the least positive even integer such that $[2d] \in D_k^n$ and $[2i + 1]$ is any odd element of O or D_n. But only d subgroups will be obtained for $0 \le i < d$.

Proof . Let H be a subgroup of D_n. Since $[0] \in H$ and $[0]$ is even element, so there are only two cases. Either H contains only even elements or H contains even and odd elements both. Then from theorem 6.6 and theorem 6.7 it follows that H is either cyclic or dihedral and H will be obtained from (i) and (ii) for some d such that $d\backslash n$.So all subgroups of D_n will be obtained from (i) and (ii) for different values of d such that $d\backslash n$.

(i) Let $d\backslash n$ and $k = n/d$ or $kd = n$. Let $C_k^n = \{r[2d] | r \in Z\}$. Since $d\backslash n$, implies $(n, d) = d$ and $n/(n, d) = n/d = k$. Then from theorem 6.5, We get (i).

(ii) Let $d\backslash n$ and $k = n/d$ or $kd = n$. Let $T = \{r[2d] | r \in Z\}$. Then form(i) it follows that T $=\{r[2d] = [2rd] | 0 \le r < k\}$, $|T| = k$ and 2d is the least positive even integer such that $[2d] \in T$. Let $[2i + 1] \in O$. Then from theorem 6.2, We get $C_d[2i + 1] = \{[2rd + 2i + 1] | r \in Z\} = \{[2rd + 2i + 1] | 0 \le r < k\}$ and $|C_d[2i + 1]| = k$. Let $D_k^n = T \cup C_d[2i + 1] = \{[2rd], [2rd + 2i + 1] | 0 \le r < k\} = \{[2rd], [2rd + 2i + 1] | r \in Z\}$. Then $|D_k^n| = |T| + |C_d[2i + 1]| = k + k = 2k$.

Let $[2rd], [2td] \in D_k^n$. Then from definition 3.8 (i). We get $[2rd].[2td] = [2rd + 2td] = [2(r + t)d] \in D_k^n$. *Let* $[2rd], [2td + 2i + 1] \in D_k^n$. Then form definition 3.8 (i, ii), We get $[2rd].[2td + 2i + 1] = [2(t - r)d + 2i + 1] \in D_k^n$ and $[2td + 2i + 1].[2rd] = [2(t + r)d + 2i + 1] \in D_k^n$. Let $[2rd + 2i + 1], [2td + 2i + 1] \in D_k^n$. Then from definition 3.8 (ii), We get $[2rd + 2i + 1].[2td + 2i + 1] = [2(t - r)d] \in D_k^n$. It follows that D_k^n is closed and finite subset of D_n. So D_k^n is a subgroup of index d and order $2k$. From theorem 6.7 it follows that D_k^n is dihedral. From theorem 6.2, it follows that there are d distinct classes $C_d[2i + 1]$ for $0 \le i < d$. So, We get d distinct dihedral subgroups.

Theorem 6.9. A complete listing of all normal subgroups of D_n is as follows:

(i) For each d such that $d\backslash n$ and $k = n/d$ or $kd = n$ there exists exactly one cyclic normal subgroup of index $2d$ and order k given by

$C_k^n = \{r[2d] | r \in Z\} = \{[2rd] | 0 \le r < k\}$, *where* 2d is the least positive even integer such that $[2d] \in C_k^n$.

(ii) If n is odd there exists exactly one dihedral normal subgroup namely D_n itself.

(iii) If n is even there exists exactly three dihedral normal subgroups given by

(a) $D_n = \{[2r], [2r+1] | 0 \le r < n\}$, of order $2n$,

(b) $D_{n/2}^n = \{[4r], [4r+1] | r \in Z\} = \{[4r], [4r+1] | 0 \le r < n/2\}$, of order n, and

(c) $D_{n/2}^n = \{[4r], [4r+3] | r \in Z\} = \{[4r], [4r+3] | 0 \le r < n/2\}$, of order n.

Proof. All subgroups of D_n are given by theorem 6.8(i,ii). Let $d \backslash n$ and $k = n/d$ or $kd = n$. Then from theorem 6.8(i), We get $C_k^n = \{r[2d] | r \in Z\} = \{[2rd] | 0 \le r < k\}$. Let $[2rd] \in C_k^n$ and $[2t] \in D_n$. Then using definition 3.8(i) and lemma 3.13(i), We get $[2t].[2rd].[2t]^{-1} = [2t + 2rd - 2t] = [2rd] \in C_k^n$. Let $[2t+1] \in D_n$ and $[2rd] \in C_k^n$. Then using definition 3.8 (ii) and lemma 3.13 (ii), We get $[2t+1].[2rd].[2t+1]^{-1} = [-2t - 1 - 2rd + 2t + 1] = [-2rd] = [2(-r)d] \in C_k^n$. Then it follows that C_k^n is normal subgroup of D_n and We get(i). From theorem 6.8(ii), We get $D_k^n = \{[2rd], [2rd + 2i + 1] | r \in Z\} = \{[2rd], [2rd + 2i + 1] | 0 \le r < k\} = \{[2rd] | r \in Z\} \cup C_d[2i + 1], 0 \le i < d$ and $|D_k^n| =$ 2k. Let $[2t], [2t+1] \in D_n$ and $[2rd], [2rd + 2i + 1] \in D_k^n$. Then using definition 3.8(i,ii) and lemma 3.13(i,ii), We get $[2t].[2rd].[2t]^{-1} = [2t + 2rd - 2t] = [2rd] \in D_k^n$, $[2t+1].[2rd].[2t+1]^{-1} = [-2t - 1 - 2rd + 2t + 1] = [2(-r)d] \in D_k^n$, $[2t].[2rd + 2i + 1].[2t]^{-1} = [-2t + 2rd + 2i + 1 - 2t] = [-4t + 2rd + 2i + 1]$ and $[2t+1].[2rd + 2i + 1].[2t+1]^{-1} = [4t - 2i + 1 - 2rd]$. D_k^n will be normal subgroup if and only if $[-4t + 2rd + 2i + 1], [4t - 2i + 1 - 2rd] \in C_d[2i+1]$ for every $0 \le t < n$ for every r$\in Z$.Then from theorem 6.1, We get that D_k^n is normal subgroup if and only if $2d \backslash (-4t + 2rd + 2i + 1 - 2i - 1)$ and $2d \backslash (4t - 2i + 1 - 2rd - 2i - 1)$ for every $0 \le t < n$ and for every $r \in Z$, if and only if $2d \backslash 4(-t)$ and $2d \backslash 4(t - i)$ for every $0 \le t < n$, if and only if $d \backslash 2$. If n is odd, then $d \backslash n$ and $d \backslash 2$, implies $d = 1$. Then $0 \le i < d$, implies $0 \le i < 1$, implies i = 0. Then $k = n/d = n/1 = n$ and $D_k^n = D_n^n = \{[2r], [2r+1] | 0 \le r < n\} = D_n$ and We get(ii). If n is even, then $d \backslash n$ and $d \backslash 2$, implies $d = 1, 2$. For $d = 1$, We get $D_k^n = D_n^n = \{[2r], [2r+1] | 0 \le r < n\} = D_n$ which is (iii)(a). If $d = 2$, Then $k = n/2$ and $0 \le i < d$, implies $0 \le i < 2$, implies $i = 0,1$. For $i = 0$,

We get $D_k^n = D_{n/2}^n = \{[4r], [4r+1] | 0 \le r < n/2\}$

which is (iii)(b). For $i = 1$, We get $D_k^n = D_{n/2}^n = \{[4r],[4r+3] | 0 \leq r < n/2\}$ which is (iii)(c).

Theorem 6.10. Let $Z(D_n)$ denote the center of $D_n(n \geq 3)$. Then,

(i) $Z(D_n) = \{[0]\}$, if n is odd, and

(ii) $Z(D_n) = \{[0],[n]\}$, if n is even.

Proof. Let $[2t+1] \in D_n$. Let $[2t+1].[2] = [2].[2t+1]$.

Then using definition 3.8 (i, ii), lemma 3.19(iv) and definition 3.1, We get $[2t+3] = [2t-1]$, implies, $[4] = [0]$, implies $2n\backslash 4$, implies, $n = 1,2$. So it follows that $[2t+1] \notin Z(D_n)$ if $n \geq 3$. Let $[2t],[2r] \in D_n$. Then from definition 3.8(i),We get $[2t].[2r] = [2t+2r] = [2r].[2t]$. Let $[2r+1] \in D_n$ and $[2t].[2r+1] = [2r+1].[2t]$. Then using definition 3.8(i,ii) and lemma 3.19(i,iv), We get $[2r+1-2t] = [2t+2r+1]$, implies $[4t] = [0]$, implies $2[2t] = [0]$. Then using lemma 4.7, We get $[2t] = [2vc],\ 0 \leq v < p,\ p = (n,2)$ and $c = n/p$. If n is odd, then $p = (n,2) = 1$. Then $[2t] = [0]$. Then We get (i). If n is even, then $p = (n,2) = 2$. Then $[2t] = [2vc], 0 \leq v < 2, c = n/2$, implies $[2t] = [0],[n]$. Then We get (ii).

Theorem 6.11. The commutator subgroup of D_n is given by $D_n' = \{r[2(n,2)] | r \in Z\} = \{[2r(n,2)] | 0 \leq r < n/(n,2)\}$.

Proof. Let $[2t],[2t+1],[2r],[2r+1] \in D_n$. Then using definition 3.8(i,ii) and lemma 3.13(i,ii), We get $[2t].[2r].[2t]^{-1}.[2r]^{-1} = [0], [2t].[2r+1].[2t]^{-1}.[2r+1]^{-1}$

$= [0],[2r+1].[2t].[2r+1]^{-1}.[2t]^{-1} = [-4t]$ and $[2t+1].[2r+1].[2t+1]^{-1}.[2r+1]^{-1} = [4(r-t)]$. Since $[2t],[2r] \in D_n$, $\forall t,r \in Z$. So, if H is the set of all commutators of D_n, then $H = \{[0],[-4t],[4(r-t)] | r,t \in Z\}$. Then it follows that $H = \{r[4] | r \in Z\} = \{r[2(2)] | r \in Z\}$. Then from theorem 6.5, it follows that H is a cyclic subgroup of index $2(n,2)$ and order $n/(n,2)$ given by

$H = \{r[2(n,2)] | r \in Z\}$=$\{[2r(n,2)] | 0 \leq r < n/(n,2)\}$.

Since the commutator subgroup D_n is the subgroup generated by the commutators. Therefore $D_n' = H$.

Theorem 6.12. Let k be a positive integer and H $= \{[\mathbf{2t}] \in D_n | \mathbf{k}[\mathbf{2t}] = [\mathbf{0}]\}$. Then H is a cyclic subgroup of order (n,k) and index $(2n)/(n,k)$ given by

$H = \{r[2c] | r \in Z,\ c = n/(n,k)\} = \{[2rc] | 0 \leq r < (n,k),\ c = n/(n,k)\}$.

Proof. Let $H = \{[2t] \in D_n | k[2t] = [0]\}$. Then using lemma 4.7, We get

$H = \{[2rc] = r[2c] | 0 \leq r < (n,k), c = n/(n,k)\}$. Since $c(n,k) = n$, So from theorem 6.8 (i), it follows that H is a cyclic subgroup of index $2c = (2n)/(n,k)$ and order (n,k).

Theorem 6.13. Let k be a positive integer . Let kE

$=\{k[2t] | [2t] \in E\}$ and $E_k = \{[2t] \in E | k[2t].[2r+1] = [2r+1].k[2t], \forall [2r+1] \in O\}$. Then,

(i) kE is a cyclic subgroup of E given by

$kE = \{r[2(n,k)] | r \in Z\} = \{[2r(n,k)] | 0 \le r < n/(n,k)\}$,

$|kE| = n/(n,k)$,

(ii) E_k is a cyclic subgroup of E given by

$E_k = \{r[2c] | 0 \le r < (n,2k),\ c = n/(n,2k)\}$,

$|E_k| = (n,2k)$,

(iii) kE_k is a cyclic subgroup of kE given by

$kE_k = \{r[2kc] | 0 \le r < (n,2k)/(n,k),\ c = n(n,k)/(n,2k)\}$,

$|kE_k| = (n,2k)/(n,k)$,

(iv) $|C_k^1(E \times O)| = |C_1^k(O \times E)| = |E_k \times O| = |E_k||O| = (n,2k)n$, and

(v) $|C(kE \times O)| = |C(O \times kE)| = |(kE_k \times O)| = |kE_k||O| = (n,2k)n/(n,k)$.

Proof. Let E be the set of even elements of D_n.

Then from lemma 3.18(i) and lemma 3.19 (i), We get $E = \{[2r] | 0 \le r < n\} = \{r[2] | r \in Z\}$ and $|E| = n$. From theorem 6.5, it follows that E is a cyclic subgroup of D_n. Let k be a positive integer and $kE = \{k[2t] | [2t] \in E\}$. Then using theorem 3.19 (i), We get $kE = \{t[2k] | [2t] \in E \text{ or } t \in Z\}$ and $kE \subseteq E$. Then from theorem 6.5, it follows that kE is a cyclic subgroup and

$kE = \{t[2(n,k)] | t \in Z\} = \{[2t(n,k)] | 0 \le t < n/(n,k)\}$, $|kE| = n/(n,k)$ which is (i).

Let $E_k = \{[2t] \in E | k[2t].[2r+1] = [2r+1].k[2t]\ \forall [2r+1] \in O\}$. Then using definition 3.8(i,ii) and lemma 3.19 (i, iv), We get $E_k = \{[2t] \in E | 2k[2t] = [0]\}$. Then using theorem 6.12, it follows that E_k is a cyclic subgroup of E and $E_k = \{r[2c] | 0 \le r < (n,2k),\ c = n/(n,2k)\}$, $|E_k| = (n,2k)$ which is (ii). Then using lemma 3.19(i), We get

$kE_k = \{k[2rc] | 0 \le r < (n,2k),\ c = n/(n,2k)\} = \{r[2kc] | 0 \le r < (n,2k) \text{ or } r \in Z,\ c = n/(n,2k)\}$.

Then clearly $kE_k \subseteq kE$. Now $(n,kc) = (n, kn/(n,2k)) = (n(n,2k)/(n,2k),\ kn/(n,2k))$ $= \{n/(n,2k)\}((n,2k),k) = \{n/(n,2k)\}(n,k) = n(n,k)/(n,2k)$, implies, $n/(n,kc) = (n,2k)/(n,k)$. Then from theorem 6.5, it follows that kE_k is a cyclic subgroup of kE and $kE_k = \{r[2n(n,k)/(n,2k)] | 0 \le r < (n,2k)/(n,k)\}$,

$|kE_k| = (n, 2k)/\ (n, k)$ which is (iii). Using definition 4.2, lemma 4.5, (ii), $|O| = n$ and definition of E_k , We get (iv). Using definition 5.2, (iii), definition of kE, definition of kE_k and $|O| = n,$ We get (v).

Conclusion

Dihedral group D_n of degree n has a new representation as a group of residue classes. This new representation will help us to study any property of dihedral groups. The (N, M)-th commutativity degree $P_N^M(D_n)$ and the relative (N, M)-th commutativity degree $P_N^M(D_n, D_n)$ for all N, M and n have been obtained. Also all subgroups, all normal subgroups, the center and commutator subgroup have been obtained.

Acknowledgement

Dr. Subhash Chandra Singh

K.S. Inter College, District : Ballia,

State : Uttar Pradesh,

Country : India, PIN: 277001

Gmail: drsubhash4321@gmail.com

References

[1] A. Erfanian, R. Rezaei and P. Lescot, On the relative commutativity degree of subgroup of a finite group, Communications in Algebra ® 35(2007), 4183-4197.

[2] B.Azizi and H.Dostie, Certain numerical results in non-associative structures, Mathematical sciences (2019) 13:27-32. https/doi.org/10.1007/540096-018-0274-0.

[3] D.S.Dummit and R.M. Foote, Abstract Algebra, John Wiley, N.Y. 2003.

[4] K.Conrad, Dihedral groups, course Hero, Access 27 January 2020. Available online at : https://www.coursehero.com/file/87268627/dihedral 2pdf/.

[5] M.Abdul Hamid, The probability that two elements commute in dihedral groups, "Under graduate Project Report, Universiti Teknology Malaysia(2010)."

[6] M.M. Ali and N.H. Sarmin, On some problems in group theory of probabilistic nature, Menemui Matematic (Discovering Mathematics) 32(2), 35-41(2010), ISS N 2231-7023.

[7] N.H. Sarmin and M.S. Mohammad, "The probability that two elements commute in some 2-generator 2-group of nilpotency class 2, " Technical Report of Department of Mathematics, Universiti Teknology Malaysia LT/M Bil. 3/2006.

[8] P. Erodos and P.Turan, On some problem of statistical group theory, Acta Math. Acad. Sci. Hungaricae 19, 413-435 (1968).

[9] W.H. Gustofson, what is the probability that two group elements commute? Amer, Math. Montholy 80, 1031-1304 (1973).

[10] Z. Yahya, N.M.M. Ali, N.H. Sarmin and F.N.A.Manaf, The n^{th} commutativity degree of some dihedral groups, Menemui Matematic (Discovering Mathematics) 34, 7-14(2012). DOI : 10.1063/1.4801214.