Counting Basis of Dihedral Groups

Vinod S[2,3,*], Biju. G.S.[1,3], Anil Kumar B.T[1,3] and N.Ganesh[1,3]

[1]Department of Mathematics, College of Engineering, Thiruvananthapuram, Kerala, INDIA

[2]Department of Mathematics, Government College for Women, Thiruvananthapuram, Kerala, INDIA

[3]Department of Collegiate Education, Kerala, INDIA

Abstract: Let G be a finite group. Any minimal generating subset of G is called a basis of G. The cardinality of any basis is called dimension of G. In this paper we characterize and compute the different basis of Dihedral groups. Also we compute the number different automorphisms of Dihedral groups .

Keywords: **Basis, Group, Dihedral group, Automorphism.**

1. Introduction

How many subgroups does a finite set have? The answer is 2^n, where n is the cardinality of the set. There are many interesting functions from the family of Dihedral groups to set of Natural numbers. For the Dihedral group D_n ,of order $2n$, Stephan.R.Cavior in [1] proved that the number of subgroups is $d(n) + \sigma(n)$, where $\sigma(n)$ is the sum of positive divisors of n. In [16],Vinod et al proved that $D_n$is associated to $d(n)$by the number of non-mixed subgroups also by non-mixed normal subgroups , associated to $\sigma(n)$ by its number of mixed subgroups, associated to $d(n) + n$ by its cyclic subgroups, associated to $(n + 3)/2$ if n odd and $(n + 6)/2$ if n even by its conjugacy classes etc. In this paper we find some nice relations between the family of Dihedral groups and the set of Natural numbers by finding the number of different basis and automorphisms of Dihedral groups.

2.Notations and Preliminary

A group G generated by two elements r and s with orders n and 2 such that $srs^{-1} = r^{-1}$is said to be the n[th] dihedral group and is denoted by D_n.The order of D_n is $2n$.Now we define this group geometrically. The distance preserving bijection on a metric space X is called a symmetry on X. The collection of all symmetries on a metric space X will form a group under composition of mapping called group of symmetries on X, denoted by $Sym(X)$. For $n \geq 3$, Let $P_n$denote the n-sided regular polygon in the plane. In [14], Keith Conrad proved that size of $Sym(P_n)$ is $2n$ and which is isomorphic toD_n. Most of the notations, definitions and results we mentioned here are standard and can be found in [7]or [11]For any given natural number$n$ we denote Z_n for the cyclic group of order n and DiC_n denote the dicyclic group of order 4n. We write the symbol $G \cong G'$, If the group G and the group G' are isomorphic. If H is a subgroup of the group G, then we denote it by $H \leq G$. The order of an element x in the group G is denoted by $o(x)$ and for any set X we denote $|X|$for the cardinality of the set X. If G is a group and $a_1, a_2, a_3, \ldots a_n$ are elements in G, the symbol $\langle a_1, a_2, a_3, \ldots, a_n \rangle$ represents for the subgroup generated by $a_1, a_2, a_3, \ldots a_n$.For any given natural number n denote:

$\varphi(n) =$ The number of non- negative integers lass than n and relatively prime to n

$d(n) =$ The number of positive divisors of n.

$\sigma(n)$ = The sum of positive divisors of n.

The greatest common divisor of m and n is denoted by(n, m)

Theorem 2.1: [14] Let$G$ be a group generated by a and b such that $a^n = e, b^2 = e$ and $bab^{-1} = a^{-1}$. If the size of G is $2n$ the G is isomorphic to D_n.

By theorem 2.1, we make an abstract definition for dihedral groups.

Definitin2.2: For $n \geq 3$, let $R_n = \{r_0, r_1, \dots, r_n\}$ and $S_n = \{s_0, s_1, \dots, s_n\}$. Define a binary operation on $G_n = R_n U S_n$by the following relations:

$$r_i \,.\, r_j = r_{i+jmod(n)} \qquad \mathrm{r_i}.\,\mathrm{s_j} = \mathrm{s_{i+jmod(n)}},$$

$$s_i \,.\, s_j = r_{i-jmod(n)} \qquad s_i \,.\, r_j = s_{i-jmod(n)} \;\; \forall\, 0 \leq i, j \leq n.$$

Then$(G_n, {}_0)$is a group of order $2n$ called nth Dihedral group.

Note that the identity element in $(G_n, {}_0)$ $r_{0\,,}$ the inverse of $\mathrm{r_i}$ is $\mathrm{r_{n-i}}$ and the inverse of $\mathrm{s_i}$ is $\mathrm{s_i}$ for all $0 \leq \mathrm{i} \leq$ n. It is clear that ${r_1}^i = r_i$ and $r_j . s_0 = s_j \;\forall\, 0 \leq \mathrm{i,j} \leq \mathrm{n}$. Since $\mathrm{G_n}$is a group of order 2n and can be generated by $\mathrm{r_1}$and $\mathrm{s_0}$ such that:

$${\mathrm{r_1}}^{\mathrm{n}} = \mathrm{r_n} = \mathrm{r_0},\ {\mathrm{s_0}}^2 = \mathrm{r_0} \text{ and } \mathrm{s_0 r_1 s_0}^{-1} = \mathrm{s_0 r_1 s_0} = \mathrm{s_{-1} s_0} = \mathrm{r_{-1}} = \mathrm{r_{n-1}} = {\mathrm{r_1}}^{-1},$$

the group $\mathrm{G_n}$is isomorphic to $\mathrm{D_n} = \langle \mathrm{r_1}, \mathrm{s_0} \rangle$.

The elements of $\mathrm{R_n}$ are called rotations and that of $\mathrm{S_n}$ are called reflections.

A subgroup of $\mathrm{D_n}$which contain both rotations and reflections is called a mixed subgroups and other subgroups ie subgroups contain rotations only is called non-mixed subgroup.

Theorem2.3: [16] Every mixed subgroup of $\mathrm{D_n}$is dihedral.

Theorem2.4: [16] The number of non-mixed subgroups of $\mathrm{D_n}$is d(n) namely $\{\langle \mathrm{r_{n/d}} \rangle | \mathrm{d} \text{ is a divisor of n}\}$.

Theorem2.5: [16**]** If H is a mixed subgroup of $\mathrm{D_n}$then,

$|\mathrm{H}| = 2\mathrm{d}$, for some d and ddivide n and $\mathrm{H} \cong \mathrm{D_n} = \langle \mathrm{r_{\frac{n}{d}}}, \mathrm{s} \rangle$ for some s in H

Theorem2.6: [16] If d/n, the number of mixed subgroups of order 2d is n/d namely $\{\langle \mathrm{r_{n/d}}, \mathrm{s_i} \rangle | 0 \leq \mathrm{i} \leq \mathrm{n/d}\}$.

Theorem2.7: [14] If a and b are two elements in $\mathrm{D_n}$,then $\langle a, b \rangle = \{a^k b^m | 0 \leq k, m \leq n-1\}$

Definition 2.8: Let G be a finite Group. A subset A of G is said to be a basis of G if A generate G and $|B| \geq |A|$ for all generating set B of G.

By the above definition it is clear that all basis has same cardinality. This unique number is called the dimension of G and it is denoted by $d(G)$.

Definition2.9: The cardinality of any basis is of G called the dimension of G.

Example2.10: The Group $\mathrm{Z_n}$ can be generated by a single element namely {1}. Hence {1} is a basis of $\mathrm{Z_n}$ and the dimension of $\mathrm{Z_n}$is 1 ie $\mathrm{d(Z_n)} = 1$.

Theorem2.11: The group $\mathrm{Z_n}$ has $\varphi(n)$ basis namely $\{\{k\} | 0 \leq k < n, (k, n) = 1\}$

Example 2.12: The Kein-4-group $V = \{e, a, b, c\}$ cannot be generated by single element. But it can be generated by two elements, for example, $\{a, b\}$. Hence $\mathrm{d(V)} = 2$.

There are other bases for Klein-4-group V. $\{\{a, b\}, \{a, c\}, \{c, b\}\}$ are the different bases of V and the number of bases of Klein-4-group is 3. Also from the above, we have group $\mathrm{G_n} \cong \mathrm{D_n}$ and it is clear that

$d(D_n) = 2$ and $\{r_1, s_0\}$ is one of its basis. There are other bases for it. In this paper our first aim is to characterize this

3. Main results

A basis of D_n which contain both rotation and reflection is called a mixed basis and other basis is called non-mixed basis. By the definition 2.2 it is obvious that two rotations cannot generate D_n. Hence non-mixed basis of D_n are basis consisting of two reflections.

Theorem 3.1: The number of mixed basis for $D_n (n \geq 3)$ is $n\varphi(n)$.

Proof: Let $s_j (0 \leq j \leq n-1)$ be a reflection in D_n. Then for any $0 \leq i \leq n-1$,

$$\begin{aligned}\langle r_i, s_j \rangle &\cong \{r_i^m s_j^t \mid 0 \leq m, t \leq n-1\} \quad \text{;by theorem 2.7}\\ &= \{r_i^m s_j, r_i^m r_0 \mid 0 \leq m, \leq n-1\} \quad \text{; since } s_j^t = s_j \text{ or } r_0\\ &= \{r_i^m s_j, r_i^m \mid 0 \leq m \leq n-1\}\\ &= \{r_i^m s_j \mid 0 \leq m \leq n-1\} \cup \{r_i^m \mid 0 \leq m \leq n-1\}\\ &= \langle r_i \rangle s_j \cup \langle r_i \rangle = D_n \text{ iff } 0 \leq i \leq n-1 \text{ and } (i, n) = 1.\end{aligned}$$

Hence corresponding to each reflection s_j $(0 \leq j \leq n-1)$there are $\varphi(n)$mixed bases are there namely $\{\{s_j, r_i\} \mid 0 \leq i \leq n-1 \text{ and } (i, n) = 1\}$.So the number of mixed basis for $D_n (n \geq 3)$ is $n\varphi(n)$.

Theorem3.2: The number of non-mixed basis for $D_n (n \geq 3)$ is $\frac{n\varphi(n)}{2}$.

Proof: Since the dimension of D_n is 2, any basis of D_n contain exactly two elements. The subgroup generated by two rotations always lies in R_n and hence cannot form a basis. Therefore any non- mixed basis of D_n contain exactly two reflections. : Let $s_j (0 \leq j \leq n-1)$ be a reflection in D_n. Then for any $0 \leq i \leq n-1$,

$$\begin{aligned}\langle s_i, s_j \rangle &= \langle r_{i-j} s_j, s_j \rangle \quad \text{; by definition 2.2}\\ &= \langle r_{i-j}, s_j \rangle \cong D_n \text{ iff } i - j \equiv k \bmod n \text{ and } (k, n) = 1\end{aligned}$$

Hence corresponding to each reflection s_j $(0 \leq j \leq n-1)$ there are $\varphi(n)$ non-mixed basis for D_n namely $\{\{s_{i+j}, s_j\} \mid 0 \leq i \leq n-1 \text{ and } (i, n) = 1\}$. If $\{s_i, s_j\}$ is a mixed basis corresponding to the reflection s_i then it is also a basis corresponding to the reflection s_j. Hence the number of non-mixed basis for $D_n (n \geq 3)$ is $\frac{n\varphi(n)}{2}$.

Theorem3.3: The number of different basis for $D_n (n \geq 3)$ is $\frac{3}{2} n\varphi(n)$.

Proof: The collection of all different bases of $D_n (n \geq 3)$is the union of all mixed and non-mixed bases .Hence the different bases of $D_n (n \geq 3)$ is $\frac{n\varphi(n)}{2} + n\varphi(n) = \frac{3}{2} n\varphi(n)$.

Theorem3.4: The number of automorphism on $D_n (n \geq 3)$ is $n\varphi(n)$.

Proof: Let $\phi: D_n \to D_n$ be an automorphism**.** Since $\{s_0, r_1\}$ is a basis for D_n and ϕ is an automorphism, ϕ preserve basis and order $\phi(\{s_0, r_1\})$ is a basis for D_n , $o(s_0) = o(\phi(s_0))$ and $o(r_1) = o(\phi(r_1))$.Since $o(s_0) = 2$ and $o(r_1) = n$,we have $o(\phi(s_0)) = 2$ and $o(\phi(r_1)) = n$. Since $n \geq 3$, $\phi(r_1)$ is a rotation of order n and hence $\phi(r_1) = r_k$ for some $0 \leq k \leq n-1$ and $(k, n) = 1$. If $\phi(s_0)$ is a rotation

then $\phi(\{s_0, r_1\})$ is a subset of R_n and hence it cannot be a basis. This gives $\phi(s_0)$ is a reflection and hence $\phi(s_0)$ has n possibilities namely $\{s_j | 0 \le j \le n-1\}$. Suppose $\phi(r_1) = r_k$; $0 \le k \le n-1$ and $(k,n) = 1$ and $\phi(s_0) = s_j$ .Then $\phi(r_i) = \phi(r_1{}^i) = [\phi(r_1)]^i = (r_k)^i = r_{ki(modn)}$

and $\phi(s_i) = \phi(r_i s_0) = \phi(r_i)\phi(s_0) = r_{ki}.s_j = s_{ki+j(modn)}$.

Thus every automorphism ϕ: $D_n \to D_n$ has the form $r_i \to r_{ki(modn)}$ and $s_i \to s_{ki+j(modn)}$ for some $0 \le k, j \le n-1$ and $(k,n) = 1$.

Conversely assume $\phi_{k,j}$: $D_n \to D_n$ be a map given by $r_i \to r_{ki(modn)}$ and $s_i \to s_{ki+j(modn)}$ for some $0 \le k, j \le n-1$ and $(k,n) = 1$.Now we will prove $\phi_{k,j}$ is an automorphism on D_n.

For this let $0 \le i, t \le n-1$; then

$\phi_{k,j}(r_i r_t) = \phi(r_{i+t}) = r_{[i+t]k(modn)} = r_{ik(modn)}.r_{tk(modn)} = \phi(r_i)\phi(r_t)$,

$\phi_{k,j}(s_i s_t) = \phi_{k,j}(r_{i-t}) = r_{[i-t]k(modn)} = s_{ik+j(modn)}.s_{tk+j(modn)} = \phi_{k,j}(s_i)\phi_{k,j}(s_t)$,

$\phi_{k,j}(r_i s_t) = \phi_{k,j}(s_{i+t}) = r_{[(i+t)k+j](modn)} = r_{ik(modn)}.s_{tk+j(modn)} = \phi_{k,j}(r_i)\,\phi_{k,j}(s_t)$,

and $\phi_{k,j}(s_t r_i) = \phi_{k,j}(s_{t-i}) = r_{[(t-i)k+j](modn)} = s_{tk+j(modn)}r_{ik(modn)} = \phi_{k,j}(s_t)\phi_{k,j}(r_i)$.

Hence $\phi_{k,j}$: $D_n \to D_n$ preserve the group structure. Since by $r_1 \to r_k$ and $s_0 \to s_j$, where $0 \le k, j \le n-1$ and $(k,n) = 1$, we have $\phi_{k,j}(\{s_0, r_1\})$ is a basis for $D_n$and hence $\phi_{k,j}$: $D_n \to D_n$ is a bijection also. Therefore $\phi_{k,j}$ is an automorphism and number of automorphisms on $D_n(n \ge 3)$ is $n\varphi(n)$ namely $\{\phi_{k,j} | 0 \le k, j \le n-1$ and $(k,n) = 1\}$.

4. Conclusion

In this paper we proved that the of mixed and non-mixed basis for $D_n(n \ge 3)$ is $\boldsymbol{n\varphi(n)}$ and $\frac{\boldsymbol{n\varphi(n)}}{\boldsymbol{2}}$ respectively. Also we compute that the number of different bases for $D_n(n \ge 3)$ is $\frac{\boldsymbol{3}}{\boldsymbol{2}}\boldsymbol{n\varphi(n)}$ and the number of automorphisms on $D_n(n \ge 3)$ is $\boldsymbol{n\varphi(n)}$

Referrences

[1] S.R.Cavior, "The subgroups of the dihedral group",Math.Mag48(1975). 107.

[2] Grigore Calugareanu, "The total number of subgroups of a finite abelian group", Scientiae Mathemati Japonicae 60,No 1,(2004),157-167

[3] Benson Farb and Dan Margalit, "Aprimer on mapping classgroups" ,Princeton University press, 2012.

[4] G.A.Miller, "Subgroups of the groups whose order can below thirty", Proceedings of the National Accademy of sciences of the United States of America 26(8)(1940),500-502.

[5] Marius Tarnauceanu, "An arithmetic method of counting the subgroups of a finite abelian group", Bull.Math.Sov.sci.math,Roumanie 53(101)no 4,(2010)373-386

[6] Tom M. Apostol, 1974, Mathematical Analysis 2nd Edition, Addition-Wesley Publishing Company.

[7] Gallian, J.A,1994, Contemporary Abstract Algebra,3rd Edition, D.C.Heath and Company

[8] Alex Cameron, "Counting ring homomorphisms", IIME Journal, Volume13, No. 2, 65-67

[9] M. Misaghian, "Factor Rings and their decompositions in the Eisenstein integers Ring Z[ω]", American Journal of Mathematics 5 No. 1 (2013): 58−68

[10] Mohmmad saleh and Hassan Yousef, The American Mathematical Monthly, 105(1998)259-260.

[11] David S. Dummit and Richard M.Foote, Abstract Algebra,Wiley, 3rdEdition,2003.

[12] William C. Calhous, The American mathematical monthly,vol.94,No 1,pp54-59

[13] Conrad Keith, Dihedral Groups, Retrieved from: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral.pdf

[14] Conrad Keith, Dihedral Groups II, Retrieved from: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral2.pdf

[15] H.Zassenhaus, Theory of groups, Chelsea, Newyork,1949

[16] Vinod.S, et al "On mixed subgroups of dihedral groups"IJRAR Volume 7(2),2020