THE NUMBER OF HOMOMORPHISMS FROM DIHEDRAL GROUPS IN TO SOME FINITE GROUPS

R. RAJKUMAR, M. GAYATHRI , T. ANITHA

Abstract: We derive general formulae for counting homomorphisms, monomorphisms and epimorphisms from dihedral groups into quaternion, quasi-dihedral and modular groups using only elementary group theory.

Keywords: finite groups, homomorphisms.

Introduction: Counting homomorphisms between two groups is a basic problem in group theory. In [2] Gallian and Buskirk obtained the number of homomorphisms between two given cyclic groups using only elementary group theory. Also using the elementary techniques, in [3] Gallian and Jungreis provided a method for counting homo-morphisms from $Z_m[i]$ into $Z_n[i]$ and $Z_m[\rho]$ into $Z_n[\rho]$, where $i^2+1=0$ and $\rho^2+\rho+1=0$. But in general counting homomorphisms between groups needs advanced tools of algebra; see, for instance [1, 5]. So in [4] Jeremiah Johnson, described a method of counting homomorphisms from a dihedral group D_n into another dihedral group D_m by using only elementary methods. Motivated by these, in this paper we not only count but also enumerate homomorphisms, monomorphisms and epimorphisms from a dihedral group into some finite groups, namely quaternion groups, quasi-dihedral groups and modular groups by using elementary techniques.

In this paper we use the following notations: for a positive integer $n>1$, D_n denotes the dihedral group generated by two generators x_n and y_n subject to the relations $x_n^n = e = y_n^2$ and $x_n y_n = y_n x_n^{-1}$; and for a positive integer $m>1$, Q_m denotes the quaternion group generated by two generators a_m and b_m subject to the relations $a_m^{2m} = e = b_m^4$ and $a_m b_m = b_m a_m^{-1}$ and for a positive integer $\alpha > 3$, QD_{2^α} denotes the quasi-dihedral group generated by two generators s_α and t_α subject to the relations $s_\alpha^{2^{\alpha-1}} = e = t_\alpha^2$ and $t_\alpha s_\alpha = s_\alpha^{2^{\alpha-2}-1} t_\alpha$; and for a positive integer $\beta > 2$, M_{p^β} denotes the modular group generated by two generators r_β and f_β subject to the relations $r_\beta^{p^{\beta-1}} = e = f_\beta^p$ and $f_\beta r_\beta = r_\beta^{p^{\beta-2}+1} f_\beta$.

1. *The number of homomorphisms from D_n into Q_m*

Theorem 1.1: *Let m be any positive integer and n be a positive odd integer. Then the number of group homomorphisms from D_n into Q_m is 2.*

Proof. Suppose that $\rho : D_n \to Q_m$ is a group homomorphism, where n is an odd positive integer and m is any positive integer. Then $|\rho(x_n)|$ must divide $|x_n| = n$, and $|\rho(y_n)|$ must divide $|y_n| = 2$. Since n is odd, $\rho(x_n)$ must be of the form a_m^α in Q_m, where $|a_m^\alpha|$ divides both n and $2m$, and $\rho(y_n)$ must be either e or a_m^m. But not all of these choices for $\rho(x_n)$ and $\rho(y_n)$ yield homomorphi-sms. So, let us check the homomorphism condition for other elements in D_n.

Suppose $\rho(x_n) = a_m^\alpha$, where $|a_m^\alpha|$ divides both n and $2m$, and $\rho(y_n) = e$. Then $\rho(x_n^k y_n) = a_m^{\alpha\, k(mod\, 2m)}$, $0 \le k < n$. The-refore, $|a_m^{\alpha\, k(mod\, 2m)}|$ must divide $|x_n^k y_n| = 2$. That is, $|a_m^{\alpha\, k(mod\, 2m)}|$ must be equal to either 1 or 2. Since n is odd, α must be equal to 0. That is, in this case we have only the trivial homomorphism.

Suppose $\rho(x_n) = a_m^\alpha$, where $|a_m^\alpha|$ divides both n and $2m$, and $\rho(y_n) = a_m^m$. Then $\rho(x_n^k y_n) = a_m^{\alpha\, k+m\, (mod\, 2m)}$, $0 \le k < n$. Th-erefore, $|a_m^{\alpha\, k+m\, (mod\, 2m)}|$ must divide $|x_n^k y_n| = 2$ Since n

is odd, α must be equal to 0. That is, in this case we have one homomorphism which is $\rho(x_n)=e$ and $\rho(y_n)=a_m^m$. So, in total there are 2 homo-morphisms.

Theorem 1.2: *Let m be any positive integer and n be an even positive integer. Then the number of group homomorphisms from D_n into Q_m is 4.*

Proof. First we consider the case when n is an even positive integer which is not divisible by 4. In this case $\rho(x_n)$ must be in the form a_m^α in Q_m, where $|a_m^\alpha|$ divides both n and $2m$, and $\rho(y_n)$ must be either e or a_m^m.

As in proof of Theorem 1.1, if $\rho(x_n)=a_m^\alpha$, where $|a_m^\alpha|$ divides both n and $2m$, and $\rho(y_n)=e$, the order of $a_m^{\alpha\, k(mod\, 2m)}$ must be equal to either 1 or 2. Therefore, we have two possible choices for α, one is 0 and the other is m. That is, in this case there are 2 homomorphisms; one is $\rho(x_n)=e$ and $\rho(y_n)=e$ which is trivial; and another one is $\rho(x_n)=a_m^m$ and $\rho(y_n)=e$. Similarly, if $\rho(y_n)=a_m^m$, we have two choices for $\rho(a_m)$ which are $\rho(a_m)=e$ and $\rho(a_m)=a_m^m$. Thus we have 4 homomorphisms.

Next, we consider the case when n is an even positive integer which is divisible by 4. In this case, $\rho(x_n)$ has an additional possibility that $\rho(x_n)$ can be of the form $a_m^k b_m$, $0\le k<2m$. Suppose $\rho(x_n)=a_m^k b_m$, $0\le k<2m$ and $\rho(y_n)=e$ is a homomor-phism, then $\rho(x_n y_n)=a_m^k b_m$. Therefore, $|a_m^k b_m|$ must divide $|x_n y_n|=2$. But this is not possible, since the order of $a_m^k b_m$ is 4 for every $0\le k<2m$. Similarly, if $\rho(x_n)=a_m^k b_m$, $0\le k<2m$ and $\rho(y_n)=a_m^m$ cannot be a homomorphism. So, in this case also we have 4 homomorphisms. This completes the proof.

Corollary 1.1: *Let m and n be any two positive integers. Then there is no monomorphism from D_n into Q_m; and there is no epimorphism from D_n onto Q_m.*

Proof . By Theorem 2.1, there exist two homomorphisms from D_n into Q_m, when n is odd; and by Theorem 2.2, there exixt 4 homomorphisms from D_n into Q_m, when n is even. By simple calculations, we can verify that these homomorphisms are neither one to one nor onto.

2 The number of homomorphisms from D_n into QD_{2^α}

Theorem 2.1: *Let n be positive even integer and $\alpha>3$ be positive integer. Then the number of homomorphisms from D_n into QD_{2^α} is $4+2^\alpha+2^{\alpha-2}\left(\sum_{k|\,\gcd(n,\,2^{\alpha-2})}\phi(k)\right)$.*

Proof. Suppose that $\rho: D_n \to QD_{2^\alpha}$ is a group homomorphism, where n is a positive even integer and $\alpha>3$ is positive integer. Then $|\rho(x_n)|$ divides $|x_n|=n$ and $|\rho(y_n)|$ divides $|y_n|=2$.

Suppose n is even, but not a multiple of 4, it must be the case that $\rho(x_n)=s_\alpha^l t_\alpha$, $0\le l<2^{\alpha-1}$ and l is even or $\rho(x_n)=s_\alpha^l$, where $|s_\alpha^l|$ divides both $2^{\alpha-1}$ and n, and $\rho(y_n)$ is one of $e, s_\alpha^{2^{\alpha-2}}$ or $s_\alpha^m t_\alpha$, $0\le m<2^{\alpha-1}$ and m is even. But not all of these choices for $\rho(y_n)$ yield group homomorphisms, as can be seen when we consider where ρ sends the remaining elements in D_n of the form $x_n^j y_n$, $0\le j<n$.

If $\rho(y_n)=e$ and $\rho(x_n)=s_\alpha^l$, where $|s_\alpha^l|$ divides both $2^{\alpha-1}$ and n, then $\rho(x_n y_n)=s_\alpha^l$ and $|s_\alpha^l|$ divides $|x_n y_n|=2$. Therefore, $\rho(x_n)$ must be either e or $s_\alpha^{2^{\alpha-2}}$. If $\rho(y_n)=e$ and $\rho(x_n)=s_\alpha^l t_\alpha$, $0\le l<2^{\alpha-1}$ and l is even, then $\rho(x_n y_n)=s_\alpha^l t_\alpha$ and $|s_\alpha^l t_\alpha|=2$ which divides $|x_n y_n|=2$. Thus there are $2+2^{\alpha-2}$ homomorphisms send y_n to e.

Suppose $\rho(y_n)=s_\alpha^{2^{\alpha-2}}$ and $\rho(x_n)=s_\alpha^l t_\alpha$, $0\le l<2^{\alpha-1}$ and l is even, then $\rho(x_n^k y_n)=(s_\alpha^l t_\alpha)^k s_\alpha^{2^{\alpha-2}}$. If k is even, then $(s_\alpha^l t_\alpha)^k s_\alpha^{2^{\alpha-2}}=s_\alpha^{2^{\alpha-2}}$ and $|s_\alpha^{2^{\alpha-2}}|=2$ which divides $|x_n^k y_n|=2$. If k is odd, then $(s_\alpha^l t_\alpha)^k s_\alpha^{2^{\alpha-2}}=s_\alpha^{l-2^{\alpha-2}} t_\alpha$ and $|s_\alpha^{l-2^{\alpha-2}} t_\alpha|=2$

which divides $|x_n^k y_n|$. If $\rho(y_n) = s_\alpha^{2^{\alpha-2}}$ and $\rho(x_n) = s_\alpha^l$, then $\rho(x_n^k y_n) = s_\alpha^{kl+2^{\alpha-2}}$ and $|s_\alpha^{kl+2^{\alpha-2}}|$ divides $|x_n^k y_n| = 2$, it is possible when either $l = 0$ or $2^{\alpha-2}$. So there are $2 + 2^{\alpha-2}$ homomorphisms send y_n to $s_\alpha^{2^{\alpha-2}}$.

Suppose $\rho(y_n) = s_\alpha^m t_\alpha$, $0 \le m < 2^{\alpha-1}$ and m is even, and $\rho(x_n) = s_\alpha^l t_\alpha$, $0 \le l < 2^{\alpha-1}$ and l is even, then $\rho(x_n^k y_n) = (s_\alpha^l t_\alpha)^k (s_\alpha^m t_\alpha)$. If k is even, then $(s_\alpha^l t_\alpha)^k (s_\alpha^m t_\alpha) = s_\alpha^m t_\alpha$ and $|s_\alpha^m t_\alpha| = 2$ which divides $|x_n^k y_n| = 2$. If k is odd, then $(s_\alpha^l t_\alpha)^k (s_\alpha^m t_\alpha) = s_\alpha^{l+m2^{\alpha-2}-m}$ and $|s_\alpha^{l+m2^{\alpha-2}-m}|$ divides $|x_n^k y_n| = 2$, it is possible when either $l - m = 0$ or $l - m = 2^{\alpha-2}$. Thus for each l, we have two choices for m. Thus we have $2^{\alpha-1}$ homomorphisms.

If $\rho(y_n) = s_\alpha^m t_\alpha$, $0 \le m < 2^{\alpha-1}$ and m is even and $\rho(x_n) = s_\alpha^l$, where $|s_\alpha^l|$ divides both $2^{\alpha-1}$ and n, then $\rho(x_n^k y_n) = s_\alpha^{lk+m} t_\alpha$ and $|s_\alpha^{lk+m} t_\alpha|$ divides $|x_n^k y_n| = 2$, it is possible when l is even. Then $|s_\alpha^l| \ne 2^{\alpha-1}$. Then there are $2^{\alpha-2}\left(\sum_{k|\gcd(n,2^{\alpha-2})} \phi(k)\right)$ homomorphisms exist. In total, we get the number of homomorphisms as mentioned in the result.

Suppose n is even and a multiple of 4, we have in addition to the choices for $\rho(x_n)$ that occur when n is not a multiple of 4, the possibility of mapping x_n to those elements in QD_{2^α} of the form $s_\alpha^l t_\alpha$, $0 \le l < 2^{\alpha-1}$ and l is odd. So we have to check whether these additional maps are homomorphisms or not. Suppose $\rho(y_n) = e$ and $\rho(x_n) = s_\alpha^l t_\alpha$, $0 \le l < 2^{\alpha-1}$ and l is odd, then $\rho(x_n y_n) = s_\alpha^l t_\alpha$ and $|s_\alpha^l t_\alpha| = 4$ does not divide $|x_n y_n|$.

Suppose $\rho(y_n) = s_\alpha^{2^{\alpha-2}}$ and $\rho(x_n) = s_\alpha^l t_\alpha$, $0 \le l < 2^{\alpha-1}$ and l is odd, then $\rho(x_n^k y_n) = s_\alpha^{l+2^{\alpha-2}}$ or $s_\alpha^{l2^{\alpha-2}+l+2^{\alpha-2}}$, and these two elements have order 4 which does not divide $|x_n^k y_n| = 2$.

Suppose $\rho(y_n) = s_\alpha^m t_\alpha$, $0 \le m < 2^{\alpha-1}$, m is even and $\rho(x_n) = s_\alpha^l t_\alpha$, $0 \le l < 2^{\alpha-1}$, l is odd, then $\rho(x_n^k y_n) = s_\alpha^{l+m\,2^{\alpha-2}-m}$ or $s_\alpha^{l2^{\alpha-2}+l+m2^{\alpha-2}-m}$, and the order of this element divides $|x_n^k y_n|$, which is possible only when $l - m = 0$ or $l - m = 2^{\alpha-2}$. But this is not possible, since m is even. Thus it turns out that the number of homomorphisms of this case is the same as the case when n is not a multiple of 4. This completes the proof.

Theorem 2.2: *Let n be positive odd integer and $\alpha > 3$. Then the number of group homomorphisms from D_n into QD_{2^α} is $2 + 2^{\alpha-2}$.*

Proof. Suppose that $\rho : D_n \to QD_{2^\alpha}$ is a group homomorphism, where n is a positive odd integer and $\alpha > 3$ is a positive integer. Then $|\rho(x_n)|$ divides $|x_n| = n$, which is odd and $|\rho(y_n)|$ divides $|y_n| = 2$. This is possible only when $\rho(x_n)$ is e and $\rho(y_n)$ is one of $e, s_\alpha^{2^{\alpha-2}}$ or $s_\alpha^m t_\alpha$, $0 \le m < 2^{\alpha-1}$ and m is even.

If $\rho(x_n) = e$ and $\rho(y_n) = s_\alpha^{2^{\alpha-2}}$, then $\rho(x_n^k y_n) = s_\alpha^{2^{\alpha-2}}$ and $|s_\alpha^{2^{\alpha-2}}| = 2$ divides $|x_n^k y_n|$. If $\rho(x_n) = e$ and $\rho(y_n) = s_\alpha^m t_\alpha$, $0 \le m < 2^{\alpha-1}$ and m is even, then $\rho(x_n^k y_n) = s_\alpha^m t_\alpha$ and $|s_\alpha^m t_\alpha| = 2$ divides $|x_n^k y_n|$. So, there are $2^{\alpha-2} + 1$ homomorphisms exist such that $\rho(x_n) = e$ and $\rho(y_n) = s_\alpha^{2^{\alpha-2}}$ or $s_\alpha^m t_\alpha$, $0 \le m < 2^{\alpha-1}$ and m is even. Including the trivial homomorphism we get the result.

Corollary 2.1: *Let n be any positive integer and $\alpha > 3$. Then the number of monomorphisms from D_n into QD_{2^α} is $2^{\alpha-2}\phi(n)$, if n divides $2^{\alpha-2}$; o otherwise. There is no epimorphism from D_n onto QD_{2^α}.*

Proof . Suppose n does not divide $2^{\alpha-1}$, then there is no element in QD_{2^α} has order n. Thus there is no monomorphism from D_n into QD_{2^α}. So, assume that n divides $2^{\alpha-1}$; that is, n is even. Suppose that $\rho : D_n \to QD_{2^\alpha}$ is a monomorphism. Then by Theorem 3.1,

$\rho(x_n) = s_\alpha^l$, where $|s_\alpha^l| = n \neq 2^{\alpha-1}$, and $\rho(y_n) = s_\alpha^m t_\alpha$, $0 \leq m < 2^{\alpha-1}$ and m is even, are homomorphisms that preserves the order of x_n and y_n. Then $\rho(x_n^r y_n) = s_\alpha^{lr+m} t_\alpha$. Since $|s_\alpha^l| \neq 2^{\alpha-1}$, l is even. Thus $|s_\alpha^{lr+m} t_\alpha| = 2$. Therefore, we have $2^{\alpha-2}\phi(n)$ monomorphisms when n divides $2^{\alpha-2}$. We can verify that none of the homomorphisms obtained in Theorem 3.1 are onto. Hence the result.

3 The number of homomorphisms from D_n into M_{p^α}

Theorem 3.1: *Let $p \neq 2$ be a prime, n be a positive integer and $\alpha > 2$. Then the only homomorphism from D_n into M_{p^α} is trivial.*

Proof. Suppose $\rho : D_n \to M_{p^\alpha}$ is a group homomorphism, where $p \neq 2$. Then $|\rho(x_n)|$ divides $|x_n| = n$ and $|\rho(y_n)|$ divides $|y_n| = 2$. Then $\rho(y_n)$ must be e and $\rho(x_n) = r_\alpha^k$, where $|r_\alpha^k|$ divides both n and $p^{\alpha-1}$. Then $\rho(x_n^l y_n) = r_\alpha^{lk}$. Then $|r_\alpha^{lk}|$ must divide $|x_n^l y_n| = 2$. This is possible only when $k = 0$. Thus we have only the trivial homomorphism.

Theorem 3.2: *Let n be a positive odd integer and $\alpha > 2$. Then there are 4 homomorphisms exist from D_n into M_{2^α}.*

Proof. Suppose $\rho : D_n \to M_{2^\alpha}$ is a group homomorphism. Then $|\rho(x_n)|$ divides $|x_n| = n$ and $|\rho(y_n)|$ divides $|y_n| = 2$. Since n is odd, $\rho(x_n)$ must be e, and $\rho(y_n) = r_\alpha^{m_1 2^{\alpha-2}} f_\alpha^{m_2}$, $m_1, m_2 = 0,1$. Then $\rho(x_n^k y_n) = r_\alpha^{m_1 2^{\alpha-2}} f_\alpha^{m_2}$. Thus $|\rho(x_n^k y_n)|$ divides $|x_n^k y_n| = 2$. Hence we get the result.

Theorem 3.3: *Let n be a positive even integer and $\alpha > 3$. Then there are 16 homomorphisms exist from D_n into M_{2^α}.*

Proof. Suppose $\rho : D_n \to M_{2^\alpha}$ is a group homomorphism. Then $\rho(x_n) = r_\alpha^{k_1} f_\alpha^{m_1}$, where $|r_\alpha^{k_1}|$ divides both n and $2^{\alpha-1}$ and $m_1 = 0,1$, and $\rho(y_n) = r_\alpha^{k_2} f_\alpha^{m_2}$, where $|r_\alpha^{k_2}|$ divides 2 and $m_2 = 0,1$. Then $\rho(x_n y_n) = r_\alpha^{k_1+k_2+m_1 k_2 2^{\alpha-2}} f_\alpha^{m_1+m_2}$. Then ρ is a homomorphism only when $|r_\alpha^{k_1+k_2}|$ divides 2. This is possible only when $k_1 = 0$ or $2^{\alpha-2}$. Since $\rho(x_n)$ has 4 choices and $\rho(y_n)$ has 4 choices, we have 16 homomorphisms totally.

Corollary 3.1: *Let n be a positive integer and $\alpha > 2$. Then there is no monomorphism from D_n into M_{p^α}; and no epimorphisms from D_n onto M_{p^α}.*

Proof. If $p \neq 2$, by Theorem 3.1, the trivial homomorphism is the only homomorphism from D_n into M_{p^α}, which is neither $1-1$ nor onto. So assume that $p = 2$. D_n contains $n+1$ elements having order 2 but M_{2^α} contains only 2 elements having order 2. Thus there is no monomorphism from D_n into M_{2^α}. Also we can check that homomorphisms obtained in Theorems 3.2 and 3.3 are not onto.

References

1. Bate, The number of homomorphisms from finite groups to classical groups, *J. Algebra* 308 (2007) 612-628.
2. *Sangeetha Raghu,* A Study on Multiobjective Fully Fuzzy Linear Programming Problems; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 2 (2013), Pg 357-363
2. Gallian and J. Van Buskirk, The number of homomorphisms from Z_m into Z_n, *Amer. Math. Monthly* 91 (1984) 196-197.2.Gallian and J. Van Buskirk, The number of homomorphisms from Z_m

into Z_n, *Amer. Math. Monthly* 91 (1984) 196-197.

3. V. Chandrasekar ,R.Vijayaraj ,S. Dhanasekar, Oscillation theorems for Second Kind Advanced; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 3 Issue 1 (2014), Pg 208-213
4. J.A.Gallian and D. S. Jungreis, Homomorphisms from $Z_m[i]$ into $Z_n[i]$ and $Z_m[\rho]$ into $Z_n[\rho]$, where $i^2+1=0$ and $\rho^2+\rho+1=0$, *Amer. Math. Monthly* 95 (1988) 247-249.
5. Jeremiah Johnson, The number of group homomorphisms from D_m into D_n, *The College Mathematics Journal*, 44 (2013) 190-192.*Algebra* 308 (2007) 612-628.
6. *Partha Ghosh, Wasefer Zaman,* Improving Search and Retrieval of Reusable Learning ; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 2 (2013), Pg 465-473
7. D.Matei and A. Suciu, Counting homomorphisms onto finite solvable groups, *J. Algebra* 286 (2005) 161-186.

* * *

R. Rajkumar, Assistant professor,
Department of Mathematics, Gandhigram Rural Institute-Deemed University,
Gandhigram -624302, Tamilnadu. Email:rrajmaths@yahoo.co.in
M. Gayathri, Research Scholar,
Department of Mathematics, Gandhigram Rural Institute-Deemed University,
Gandhigram -624302, Tamilnadu. Email:mgayathri.maths@gmail.com
T. Anitha, Research Scholar,
Department of Mathematics, Gandhigram Rural Institute-Deemed University,
Gandhigram -624302, Tamilnadu. Email:rrajmaths@yahoo.co.in