International Journal of Mathematics And its Applications
Volume 3, Issue 3–A (2015), 23–30.
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

The Number of Homomorphisms From Quaternion Group into Some Finite Groups

Research Article

R.Rajkumar[1]*, M.Gayathri [1] and T.Anitha [1]

1 Department of Mathematics, The Gandhigram Rural Institute–Deemed University, Gandhigram, Tamil Nadu, India.

Abstract: We derive general formulae for counting the number of homomorphisms from quaternion group into each of quaternion group, dihedral group, quasi-dihedral group and modular group by using only elementary group theory.

MSC: 20K30.

Keywords: Finite groups, homomorphisms.

1. Introduction

Finding the number of homomorphisms between two groups is a basic problem in abstract algebra. In [2] Gallian and Buskirk give the enumeration of homomorphisms between two specified cyclic groups by using only elementary group theory. Also using the elementary techniques, in [3] Gallian and Jungreis provided a method for counting homomorphisms from $\mathbb{Z}_m[i]$ into $\mathbb{Z}_n[i]$ and $\mathbb{Z}_m[\rho]$ into $\mathbb{Z}_n[\rho]$, 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 enumerating homomorphisms from a dihedral group D_n into another dihedral group D_m by using only elementary methods. Motivated by these, in [6] authors give the enumeration of homomorphisms, monomorphisms and epimorphisms from a dihedral group into some finite groups, namely quaternion, quasi-dihedral and modular groups by using elementary techniques. In this paper, we consider the problem of enumerating the homomorphisms, monomorphisms and epimorphisms from a quaternion group into each of dihedral, quaternion, quasi-dihedral and modular groups by using elementary methods.

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 $f_\beta r_\beta = r_\beta^{p^{\beta-2}+1} f_\beta$.

* E-mail: rrajmaths@yahoo.co.in

2. The Number of Group Homomorphisms from Q_m into Q_n

Theorem 2.1. *Let m and n be positive odd integers. Then the number of group homomorphisms from Q_m into Q_n is $2+2n(1+\phi(2m))$, if m divides n; $2+2n$, if m does not divide n.*

Proof. Suppose that $\rho : Q_m \to Q_n$ is a group homomorphism, where m and n are positive odd integers. We consider all of the places that ρ could send the generators a_m and b_m of Q_m which yield group homomorphisms. Since $|\rho(b_m)|$ divides $|b_m| = 4$, $\rho(b_m)$ is one of e, a_n^n or $a_n^\beta b_n$, $0 \leq \beta < 2n$. As m is odd, it must be the case that $\rho(a_m) = a_n^\alpha$, where a_n^α is an element of Q_n whose order divides both $2m$ and $2n$. Since $\rho(a_m^l b_m)^2 = \rho(a_m^m)$, $|\rho(a_m^l b_m)|$ divides 2, for every l, $0 \leq l < 2m$ iff $|\rho(a_m)|$ divides m.

If $\rho(b_m) = e$ and $\rho(a_m) = a_n^\alpha$, where $|\rho(a_m^m)|$ divides both m and $2n$, then $\rho(a_m^k b_m) = a_n^{k\alpha}$ and $|a_n^{k\alpha}|$ divides $|a_m^k b_m|$ only when $\alpha = 0$. Therefore, if $\rho(b_m) = e$, then $\rho(a_m)$ must be e. Thus we have trivial homomorphism in this case.

If $\rho(b_m) = a_n^n$ and $\rho(a_m) = a_n^\alpha$, where $|\rho(a_m^m)|$ divides both m and $2n$ then $\rho(a_m^k b_m) = a_n^{k\alpha+n}$ and $|a_n^{k\alpha+n}|$ divides $|a_m^k b_m|$ only when $\alpha = 0$. Therefore, if $\rho(b_m) = a_n^n$, then $\rho(a_m)$ must be e. Thus we have one homomorphism in this case.

Suppose $\rho(b_m) = a_n^\beta b_n, 0 \leq \beta < 2n$ and $\rho(a_m) = a_n^\alpha$, where $|a_n^\alpha|$ divides both $2m$ and $2n$ and does not divide m, then $\rho(a_m^k b_m) = a_n^{k\alpha+\beta \ (mod\ 2n)} b_n$ and $|a_n^{k\alpha+\beta \ (mod\ 2n)} b_n| = 4$ divides $|a_m^k b_m| = 4$. So, $|\rho(a_m)| = 2$ or $2m$. Therefore, we have $2n(1+\phi(2m))$ homomorphisms, if m divides n; $2n$ homomorphisms, if m does not divide n. Hence we get the result. □

Theorem 2.2. *Let m be a positive odd integer and n a positive even integer. Then the number of group homomorphisms from Q_m into Q_n is $4+2n(1+\phi(2m))$, if m divides n; $4+2n$, if m does not divide n.*

Proof. Suppose that $\rho : Q_m \to Q_n$ is a group homomorphism, where m is a positive odd integer and n is an even integer. Then $|\rho(a_m)|$ divides $|a_m| = 2m$ and $|\rho(b_m)|$ divides $|b_m| = 4$. Therefore, $\rho(a_m)$ must be of the form a_n^α, where $|a_m^\alpha|$ divides both $2m$ and $2n$, and $\rho(b_m)$ must be one of e, $a_n^{\frac{n}{2}}$, a_n^n, $a_n^{\frac{3n}{2}}$ or $a_n^\beta b_n$, $0 \leq \beta < 2n$. Also $|\rho(a_m^l b_m)|$ divides 2, for every l, $0 \leq l < 2m$ iff $|\rho(a_m)|$ divides m.

As in the proof of the Theorem 2.1, if $\rho(a_m) = a_n^\alpha$, where $|a_m^\alpha|$ divides both $2m$ and $2n$ and does not divide m, and $\rho(b_m) = a_n^\beta b_n$, $0 \leq \beta < 2n$ is a homomorphism. Thus we have $2n(1+\phi(2m))$ homomorphisms, if m divides n; $2n$ homomorphisms, if m does not divide n.

Suppose $\rho(b_m) = a_n^k$, where k is either 0 or n and $\rho(a_m) = a_n^\alpha$, where $|a_m^\alpha|$ divides both m and $2n$. Then as in the proof of the Theorem 2.1, ρ is a homomorphism only when $\alpha = 0$. Thus we have two such homomorphisms. Suppose $\rho(b_m) = a_n^k$, where k is either $\frac{n}{2}$ or $\frac{3n}{2}$ and $\rho(a_m) = a_n^\alpha$, where $|a_m^\alpha|$ divides both $2m$ and $2n$ and does not divide m. Then $\rho(a_m)$ must be equal to a_n^n. Thus we have 2 homomorphisms in this case. Hence the result. □

Theorem 2.3. *Let m be a positive even integer and n a positive odd integer. Then the number of group homomorphisms from Q_m into Q_n is 4.*

Proof. Suppose that $\rho : Q_m \to Q_n$ is a group homomorphism, where m is a positive even integer and n is an odd integer. When m is even, $\rho(a_m)$ is either a_n^α, where $|a_n^\alpha|$ divides both $2m$ and $2n$ or $a_n^\beta b_n$, $0 \leq \beta < 2n$; and $\rho(b_m)$ is one of e, a_n^n or $a_n^\gamma b_n, 0 \leq \gamma < 2n$.

Suppose $\rho(a_m) = a_n^\alpha$, where $|a_n^\alpha|$ divides both m and $2n$, and $\rho(b_m) = a_n^k$, $k = 0$ or n, then $\rho(a_m b_m) = a_n^{\alpha+k}$. The ρ is a homomorphism when $\alpha = 0$ or n. Thus we have 4 such homomorphisms.

Next, suppose $\rho(b_m) = a_n^\gamma b_n, 0 \leq \gamma < 2n$ and $\rho(a_m) = a_n^\alpha$, then ρ is well defined only when $|a_n^\alpha|$ divides both $2m$ and $2n$ and does not divide m. But since m is even and n is odd, m does not divide n. Thus we have no such homomorphisms.

Next, suppose $\rho(a_m) = a_n^\beta b_n, 0 \le \beta < 2n$ and $\rho(b_m) = e$. But this is not well defined since $\rho(b_m^2) \neq \rho(a_m b_m)^2$. Suppose $\rho(a_m) = a_n^\beta b_n, 0 \le \beta < 2n$ and $\rho(b_m) = a_n^\gamma b_n, 0 \le \gamma < 2n$, then ρ is well defined only when $m \equiv 2 \ (mod\ 4)$. Then $\rho(a_m b_m) = a_n^{\beta-\gamma}$. Suppose ρ is a homomorphism, $|a_n^{\beta-\gamma}|$ divides $|a_m b_m| = 4$ but does not divide 2. But since n is odd, there is no such element in Q_n. Hence we get the result. ☐

Theorem 2.4. *Let m and n be positive even integers. Then the number of group homomorphisms from Q_m into Q_n is* $4 + 8n + 2n\left(\sum_{k|\gcd(2m,2n),\ k\nmid m} \phi(k)\right)$*, if $m \equiv 2\ (mod\ 4)$; $4 + 2n\left(\sum_{k|\gcd(2m,2n),\ k\nmid m} \phi(k)\right)$, if $m \equiv 0\ (mod\ 4)$.*

Proof. Let us assume that $\rho : Q_m \to Q_n$ be a group homomorphism, where m and n are positive even integers. As in the proof of Theorem 2.3, when m is even, the possible choices for $\rho(a_m)$ are a_n^α, where $|a_n^\alpha|$ divides both $2m$ and $2n$ and $a_n^\beta b_n, 0 \le \beta < 2n$.

Next, let us consider the choices for $\rho(b_m)$. Since $|\rho(b_m)|$ divides $|b_m| = 4$, the value of $|\rho(b_m)|$ must be one of $1, 2$ or 4. Therefore, $\rho(b_m)$ is one of $e, a_n^n, a_n^{\frac{n}{2}}, a_n^{\frac{3n}{2}}$ or $a_n^\gamma b_n, 0 \le \gamma < 2n$. Next, we check the homomorphism condition for all possible combinations of $\rho(a_m)$ and $\rho(b_m)$.

Suppose $\rho(a_m) = a_n^\alpha$, where $|a_n^\alpha|$ divides both $2m$ and $2n$ and does not divide m, $\rho(b_m) = a_n^\gamma b_n, 0 \le \gamma < 2n$, then ρ is a homomorphism. Thus in this case we have $2n\left(\sum_{k|\gcd(2m,2n),\ k\nmid m} \phi(k)\right)$ homomorphisms.

Suppose $\rho(b_m) = a_n^k$, where k either 0 or n, and $\rho(a_m) = a_n^\alpha$, where $|a_n^\alpha|$ divides both m and $2n$. Then $\rho(a_m^l b_m) = a_n^{l\alpha+k}$. Then ρ is well defined only when $|\rho(a_m^l b_m)|$ divides 2. Therefore, α has 2 choices that are 0 or n. Thus in this case we have 4 homomorphisms.

Suppose $\rho(b_m) = a_n^k$, where $k = \frac{n}{2}$ or $\frac{3n}{2}$, and $\rho(a_m) = a_n^\alpha$, where $|a_n^\alpha|$ divides both $2m$ and $2n$ and does not divide m. Then α has 2 choices that are $\frac{n}{2}$ and $\frac{3n}{2}$ when $m \equiv 2\ (mod\ 4)$; no choices when $m \equiv 0\ (mod\ 4)$. But since $\rho(a_m b_m) = a_n^{\alpha+k}$, $|a_n^\alpha|$ divides m also. Thus there is no homomorphisms in both cases.

Suppose $\rho(a_m) = a_n^\beta b_n, 0 \le \beta < 2n$ and $\rho(b_m) = e$ or a_n^n. As in the proof of Theorem 2.3, this ρ is not well defined. Suppose $\rho(a_m) = a_n^\beta b_n, 0 \le \beta < 2n$ and $\rho(b_m) = a_n^{\frac{n}{2}}$ or $a_n^{\frac{3n}{2}}$, then ρ is well defined only when $m \equiv 2\ (mod\ 4)$ and ρ is a homomorphism. Thus we have $4n$ such homomorphisms, if $m \equiv 2\ (mod\ 4)$.

Now, suppose $\rho(a_m) = a_n^\beta b_n,\ 0 \le \beta < 2n$ and $\rho(b_m) = a_n^\gamma b_n,\ 0 \le \gamma < 2n$ is a homomorphism. Then $\rho(a_m b_m) = a_n^{\beta-\gamma}$ and ρ is a well defined only when $m \equiv 2\ (mod\ 4)$. If ρ is a homomorphism, then $|a_n^{\beta-\gamma}|$ divides $|a_m b_m| = 4$ and does not divide 2. Therefore, $\beta - \gamma$ must be either $\frac{n}{2}$ or $\frac{3n}{2}$. Therefore, for each β, $0 \le \beta < 2n$, there are 2 choices for γ. So in this case, we have $4n$ homomorphisms, if $m \equiv 2\ (mod\ 4)$. Hence we get the result. ☐

Corollary 2.1. *Let m and n be any two positive integers. Then the number of monomorphisms from Q_m into Q_n is $2n\ \phi(2m)$, if $m \neq 2$ divides n; $12n$, if $m = 2$ divides n; 0, otherwise. Also the number of automorphisms on Q_n is $2n\ \phi(2n)$, if $n \neq 2$; 24, if $n = 2$.*

Proof. Suppose m does not divide n, then there is no element in Q_n having order $2m$. Thus there is no monomorphism from Q_m into Q_n. So, assume that m divides n and $m \neq 2$. First we consider the case that both m and n are odd. Then by the Theorem 2.1, $\rho(a_m) = a_n^\alpha$, where $|a_n^\alpha| = 2m$ and $\rho(b_m) = a_n^\gamma b_n,\ 0 \le \gamma < 2n$ is a homomorphism which preserves the order of a_m and b_m. Then $\rho(a_m^k b_m) = a_n^{k\alpha+\gamma} b_n$. Therefore, this ρ is a monomorphism. And we can verify that the additional homomorphisms obtained in other cases are not monomorphisms. Thus we have $2n\ \phi(2m)$ monomorphisms, if $m \neq 2$.

Suppose $m = 2$ and m divides n. Suppose $\rho : Q_2 \to Q_n$ is a monomorphism. If $\rho(a_2)$ is either $a_n^{\frac{n}{2}}$ or $a_n^{\frac{3n}{2}}$ and $\rho(b_2) = a_n^\gamma b_n,\ 0 \le \gamma < 2n$, then we have $4n$ such monomorphisms. Similarly if, $\rho(a_2) = a_n^\beta b_n,\ 0 \le \beta < 2n$ and $\rho(b_2)$ is either $a_n^{\frac{n}{2}}$ or $a_n^{\frac{3n}{2}}$, then we have another $4n$ monomorphisms.

Suppose $\rho(a_2) = a_n^{\beta} b_n,\ 0 \leq \beta < 2n$ and $\rho(b_2) = a_n^{\gamma} b_n,\ 0 \leq \gamma < 2n$, then $\rho(a_n^k b_n)$ is one of $a_n^{\gamma} b_n,\ a_n^{\beta-\gamma},\ a_n^{n+\gamma} b_n$ or $a_n^{n+\beta-\gamma}$. Then $|\rho(a_n^k b_n)| = 4$ only when $\beta - \gamma = \frac{n}{2}$ or $\frac{3n}{2}$. Thus for each β, we have 2 choices for γ. Thus we have $4n$ monomorphisms in this case. Hence totally we have $12n$ monomorphisms in this case. Hence the result. □

Corollary 2.2. *Let m and n be any two positive integers. Then the number of epimorphisms from Q_m onto Q_n is $2n\ \phi(2n)$, if $n \neq 2$ divides m; 24, if $n = 2$ and $m \equiv 2\ (mod\ 4)$; 8, if $n = 2$ and $m \equiv 0\ (mod\ 4)$; 0, otherwise.*

Proof. Suppose $\rho : Q_m \to Q_n$ is a homomorphism, then $|\rho(x)|$ divides $|x|$, for every $x \in Q_n$. Suppose n does not divide n, then a_n has no pre image in Q_m. So, assume that $n \neq 2$ divides m. First consider the the case that both m and n are odd. Then by the Theorem 2.1, $\rho(a_m) = a_n^{\alpha}$, where $|a_n^{\alpha}| = 2n$ and $\rho(b_m) = a_n^{\gamma} b_n,\ 0 \leq \gamma < 2n$ is a homomorphism in which $\rho(a_m)$ and $\rho(b_m)$ generate the group D_n. Therefore, this ρ is a epimorphism. And we can verify that the additional homomorphisms obtained in other cases are not epimorphisms. Thus we have $2n\ \phi(2n)$ monomorphisms, if $n \neq 2$.

Suppose $n = 2$ divides m. Suppose $\rho : Q_m \to Q_2$ is a homomorphism. Then consider the homomorphisms $\rho(a_m)$ is one of $a_2,\ a_2^3$ or $a_2^{\beta} b_2,\ 0 \leq \beta < 4$ and $\rho(b_m)$ is one of $a_2,\ a_2^3$ or $a_2^{\gamma} b_2,\ 0 \leq \gamma < 4$ obtained in the Theorem 2.4.

Suppose $\rho(a_m)$ is either a_2 or a_2^3 and $\rho(b_m) = a_2^{\gamma} b_2,\ 0 \leq \gamma < 4$, then this homomorphism is a epimorphism since $\rho(a_m)$ and $\rho(b_m)$ generate the group Q_2. Similarly, if $\rho(a_m) = a_2^{\beta} b_2,\ 0 \leq \beta < 4$ and $\rho(b_m)$ is either a_2 or a_2^3 is a epimorphism but this is well defined only when $m \equiv 2\ (mod\ 4)$. Thus we have 16 epimorphisms, if $m \equiv 2\ (mod\ 4)$; 8 epimorphisms, if $m \equiv 0\ (mod\ 4)$.

Suppose $\rho(a_m) = a_2^{\beta} b_2,\ 0 \leq \beta < 4$ and $\rho(b_m) = a_2^{\gamma} b_2,\ 0 \leq \gamma < 4$, then $\rho(a_m)$ and $\rho(b_m)$ generate the group Q_2 only if $\beta - \gamma = \frac{n}{2}$ or $\frac{3n}{2}$ but this is well defined only when $m \equiv 2\ (mod\ 4)$. Thus for each β, we have 2 choices for γ. Thus we have 8 monomorphisms, if $m \equiv 2\ (mod\ 4)$. □

3. The Number of Homomorphisms from Q_m into D_n

Theorem 3.1. *Let m be a positive integer and n a positive odd integer. Then the number of group homomorphisms from Q_m into D_n is $1 + 2n + n\left(\sum_{k|\ \gcd(m,n)} \phi(k)\right)$, if m is even; $1 + n\left(\sum_{k|\ \gcd(m,n)} \phi(k)\right)$, if m is odd.*

Proof. Suppose that $\rho : Q_m \to D_n$ is a group homomorphism, where n is odd positive integer and m is any positive integer. Then $|\rho(b_m)|$ must divide $|b_m| = 4$. Then $\rho(b_m)$ must be either e or $x_n^{\gamma} y_n,\ 0 \leq \gamma < n$. Since $\rho(a_m^l b_m)^2 = \rho(a_m^m)$, $|\rho(a_m^l b_m)|$ divides 2 iff $|\rho(a_m)|$ divides m, for some $l,\ 0 \leq l < 2m$. Thus $\rho(a_m)$ must be either $x_n^{\alpha} y_n,\ 0 \leq \alpha < n$ or x_n^{β} whose order divides both m and n.

If $\rho(b_m) = e$, then $\rho(a_m b_m) = \rho(a_m)$ and $|\rho(a_m)|$ divides $|a_m b_m| = 4$ and m. Thus $\rho(a_m)$ must be either e or $x_n^{\alpha} y_n,\ 0 \leq \alpha < n$, if m is even; $\rho(a_m) = e$ if m is odd. Thus we have $n + 1$ homomorphisms, if m is even; only trivial homomorphism, if m is odd.

Suppose $\rho(b_m) = x_n^{\gamma} y_n,\ 0 \leq \gamma < n$ and $\rho(a_m) = x_n^{\beta}$, where $|x_n^{\beta}|$ divides both m and n, then $\rho(a_m^k b_m) = x_n^{k\beta+\gamma\ (mod\ n)} y_n$ and $|x_n^{k\beta+\gamma\ (mod\ n)} y_n|$ divides $|a_m^k b_m|$. Therefore, for each β such that $|x_n^{\beta}|$ divides both n and m, and for each $\gamma,\ 0 \leq \gamma < n$, $\rho(a_m) = x_n^{\beta}$ and $\rho(b_m) = x_n^{\gamma} y_n$ is a homomorphism. Thus we have $n\left(\sum_{k|\ \gcd(m,n)} \phi(k)\right)$ homomorphisms.

Suppose $\rho(a_m) = x_n^{\alpha} y_n,\ 0 \leq \alpha < n$ and $\rho(b_m) = x_n^{\gamma} y_n,\ 0 \leq \gamma < n$, then ρ is well defined only when m is even and ρ is a homomorphism only when $\alpha = \gamma$. For, if k is even, $\rho(a_m^k b_m) = x_n^{\gamma} y_n$ and $|x_n^{\gamma} y_n|$ divides $|a_m^k b_m|$; and if k is odd, then $\rho(a_m^k b_m) = x_n^{\alpha-\gamma}$. Then $|x_n^{\alpha-\gamma}|$ must divide $|a_m^k b_m| = 4$. As n is odd, this condition is satisfied only when $|x_n^{\alpha-\gamma}|$ is 1. That is α must be equal to γ. Thus we have n such homomorphisms, if m is even. Hence we obtain the result. □

Theorem 3.2. *Let m be a positive integer and n a positive even integer such that $n \equiv 2 \ (mod\ 4)$. Then the number of group homomorphisms from Q_m into D_n is $3+3n+n\left(\sum\limits_{k|\gcd(m,n)} \phi(k)\right)$, if m is even; $2+n\left(\sum\limits_{k|\gcd(m,n)} \phi(k)\right)$, if m is odd.*

Proof. Suppose that $\rho : Q_m \to D_n$ is a group homomorphism, where $n \equiv 2 \ (mod\ 4)$ and m is any positive integer. When $n \equiv 2 \ (mod\ 4)$, there is no change for the choices for $\rho(a_m)$. But we have additional choice for $\rho(b_m)$ which is $\rho(b_m) = x_n^{\frac{n}{2}}$. Suppose $\rho(b_m) = x_n^{\frac{n}{2}}$ and $\rho(a_m) = x_n^{\beta}$ whose order divides both m and n is a homomorphism. Then $\rho(a_m b_m) = x_n^{(\beta+\frac{n}{2}) \ (mod\ n)}$ and $|x_n^{(\beta+\frac{n}{2}) \ (mod\ n)}|$ must divide 2 since $\rho(b_m^2) = e$. This is possible when either $\beta = 0$ or $\beta = \frac{n}{2}$, if m is even; $\beta = 0$ if m is odd. Thus we have 2 additional homomorphisms, if m is even; 1 homomorphism, if m is odd.
If $\rho(b_m) = x_n^{\frac{n}{2}}$ and $\rho(a_m) = x_n^{\alpha} y_n$, $0 \leq \alpha < n$, then ρ is well defined only when m is even. Then $\rho(a_m^k b_m) = x_n^{\alpha} y_n$ or $x_n^{\alpha+n} y_n$. Thus ρ is a homomorphism, if m is even. Thus we have n such homomorphisms, if m is even.
Suppose $\rho(b_m) = e$, then as in the Theorem 3.1, there are $n+1$ such homomorphisms, if m is even; 1 homomorphisms, if m is odd. Suppose $\rho(a_m) = x_n^{\beta}$, $|x_n^{\beta}|$ divides both m and n, and $\rho(b_m) = x_n^{\gamma} y_n$, $0 \leq \gamma < n$, then there are $n\left(\sum\limits_{k|\gcd(m,n)} \phi(k)\right)$ such homomorphisms. But if $\rho(a_m) = x_n^{\alpha} y_n$, $0 \leq \alpha < n$ and $\rho(b_m) = x_n^{\gamma} y_n$, $0 \leq \gamma < n$, then ρ is well defined only when m is even and ρ is a homomorphism when either $\alpha = \beta$. Thus we have n such homomorphisms, if m is even. Hence we get the result. □

Theorem 3.3. *Let m be a positive integer and n a positive even integer such that $n \equiv 0 \ (mod\ 4)$. Then the number of group homomorphisms from Q_m into D_n is $1+n\left(\sum\limits_{k|\gcd(m,n)} \phi(k)\right)$, if m is odd; and $2+4n+n\left(\sum\limits_{k|\gcd(m,n)} \phi(k)\right)$, if m is even.*

Proof. Suppose that $\rho : Q_m \to D_n$ is a group homomorphism, where $n \equiv 0 \ (mod\ 4)$ and m is any positive integer. Then $\rho(a_m)$ must be either $x_n^{\alpha} y_n$, $0 \leq \alpha < n$ or x_n^{β} whose order divides both $2m$ and n, and $\rho(b_m)$ must be one of e, $x_n^{\frac{n}{4}}$, $x_n^{\frac{n}{2}}$, $x_n^{\frac{3n}{4}}$ or $x_n^{\gamma} y_n$, $0 \leq \gamma < n$.
If $\rho(b_m) = e$ or $x_n^{\frac{n}{2}}$, and $\rho(a_m) = x_n^{\beta}$, where $|x_n^{\beta}|$ divides both m and n. If m is odd, β must be 0; and if m is even, β is either e or $\frac{n}{2}$. Thus we have 2 homomorphisms, when m is even; 1 homomorphism, when m is odd; 4 homomorphisms, when m is even. Suppose $\rho(b_m) = x_n^{\frac{n}{4}}$ or $x_n^{\frac{3n}{4}}$, $\rho(a_m) = x_n^{\beta}$, where $|x_n^{\beta}|$ divides both $2m$ and n and does not divide m, then ρ is not well defined since $\rho(a_m b_m)^2 = e$, for some l, but $\rho(b_m^2) = e$.
If $\rho(b_m) = x_n^{\gamma} y_n$, $0 \leq \gamma < n$ and $\rho(a_m) = x_n^{\beta}$, where $|x_n^{\beta}|$ divides both n and m, then there are $n\left(\sum\limits_{k|\gcd(m,n)} \phi(k)\right)$ homomorphisms. If $\rho(b_m) = e$ or $x_n^{\frac{n}{2}}$, and $\rho(a_m) = x_n^{\alpha} y_n$, $0 \leq \alpha < n$, then ρ is well defined only when m is even and ρ is a homomorphism. Thus we have $2n$ homomorphisms, if m is even. And if $\rho(b_m) = x_n^{\frac{n}{4}}$ or $x_n^{\frac{3n}{4}}$, and $\rho(a_m) = x_n^{\alpha} y_n$, $0 \leq \alpha < n$, then ρ is not well defined since $\rho(b_m^2) \neq \rho(a_m b_m)^2$.
As in the proof of the Theorem 3.2, $\rho(a_m) = x_n^{\alpha} y_n$, $0 \leq \alpha < n$ and $\rho(b_m) = x_n^{\gamma} y_n$, $0 \leq \gamma < n$, then ρ is well defined only when m is even and ρ is a homomorphism when $\alpha - \gamma$ is one of 0 or $\frac{n}{2}$. Thus we have $2n$ such homomorphisms. Hence we get the result. □

Corollary 3.1. *Let m and n be any two positive integers. Then there is no monomorphism from Q_m into D_n; and the number of epimorphism from Q_m onto D_n is $n\ \phi(n)$, if n divides m; 0, otherwise.*

Proof. The group Q_m contains $m+2$ elements having order 4, but the group D_n contains atmost 2 elements having order 4. Thus there is no monomorphism from Q_m into D_n.
The homomorphism $\rho(a_m) = x_n^{\beta}$, where $|x_n^{\beta}| = n$ and $\rho(b_m) = x_n^{\gamma} y_n$, $0 \leq \gamma < n$ are epimorphisms from Q_m onto D_n since $\rho(a_m)$ and $\rho(b_m)$ generate the group D_n. But this is possible only when n divides m. Hence we get the result. □

4. The Number of Homomorphisms from Q_m into QD_{2^α}

Theorem 4.1. *Suppose m is an odd positive integer and $\alpha > 3$ is any integer. Then the number of homomorphisms from Q_m into QD_{2^α} is $4 + 2^{\alpha-1}$.*

Proof. Suppose that $\rho : Q_m \to QD_{2^\alpha}$ is a group homomorphism, then $|\rho(a_m)|$ divides $|a_m| = 2m$ and $|\rho(b_m)|$ divides $|b_m| = 4$. Therefore, $\rho(a_m)$ is one of e, $s_\alpha^{2^{\alpha-2}}$ or $s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and k_1 is even; and $\rho(b_m) = s_\alpha^t$, where $|s_\alpha^t|$ divides 4 or $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$. Also, $|\rho(a_m^l b_m)|$ divides 2, for some l, $0 \le l < 2m$ iff $|\rho(a_m)|$ divides m.

Suppose $\rho(b_m) = s_\alpha^t$, where $t = 2^{\alpha-3}$ or $3\ 2^{\alpha-3}$ and $\rho(a_m) = s_\alpha^k$, then ρ is well defined only when k is $2^{\alpha-2}$. Then $\rho(a_m^l b_m) = s_\alpha^{lk+t}$. Then $|s_\alpha^{lk+t}|$ divides $|a_m^l b_m| = 4$. Therefore, ρ is a homomorphism. Thus we have 2 homomorphisms. Suppose $\rho(b_m) = s_\alpha^t$, where $t = 0$ or $2^{\alpha-2}$, and $\rho(a_m) = s_\alpha^k$, then k must be 0 since $|\rho(a_m)|$ must divide m which is odd. Thus we have 2 homomorphisms in this case.

Suppose $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is odd, and $\rho(a_m) = s_\alpha^k$, then ρ is well defined only when $k =$ is $2^{\alpha-2}$. Then $\rho(a_m^l b_m) = s_\alpha^{lk+k_2}t_\alpha$. Therefore, $|\rho(a_m^l b_m)|$ divides $|a_m^l b_m| = 4$, for every $0 \le l < 2m$. Thus we have $2^{\alpha-2}$ homomorphisms in this case. Suppose $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is even and $\rho(a_m) = s_\alpha^k$, then k must be equal to 0 since $|\rho(a_m)|$ must divide m which is odd. Thus we have $2^{\alpha-2}$ homomorphisms in this case.

Suppose $\rho(b_m) = s_\alpha^t$, where $|s_\alpha^t|$ divides 4, and $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and k_1 is even. But $\rho(a_m^2 b_m)^2 = s_\alpha^{2t} \ne \rho(a_m^m)$. Therefore, this ρ is not well defined. Suppose $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and k_1 is even. Then $\rho(a_m b_m)^2 = s_\alpha^{2(k_1-k_2)} \ne \rho(a_m^m)$. Therefore, this ρ is not well defined. Hence we get the result. □

Theorem 4.2. *Suppose m is an even positive integer and $\alpha > 3$ is any integer. Then the number of homomorphisms from Q_m into QD_{2^α} is $k + 4 + 2^{\alpha-2}\left(\sum_{k|\gcd(m,2^{\alpha-1})}\phi(k)\right) + 2^{\alpha-2}\left(\sum_{k|\gcd(2m,2^{\alpha-2})}\phi(k)\right)$, where k is $3\ 2^\alpha$, if $m \equiv 2\ (mod\ 4)$; $2^{\alpha+2}$, if $m \equiv 0\ (mod\ 4)$.*

Proof. Suppose that $\rho : Q_m \to QD_{2^\alpha}$ is a group homomorphism. Then $\rho(a_m) = s_\alpha^n$, where $|s_\alpha^n|$ divides both $2m$ and $2^{\alpha-1}$ or $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$; and $\rho(b_m) = s_\alpha^t$, where $|s_\alpha^t|$ divides 4 or $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$. Also, $|\rho(a_m^l b_m)|$ divides 2, for some l, $0 \le l < 2m$ iff $|\rho(a_m)|$ divides m.

Suppose $\rho(b_m) = s_\alpha^t$, where $t = 0$ or $2^{\alpha-2}$, and $\rho(a_m) = s_\alpha^n$, where $|s_\alpha^n|$ divides both m and $2^{\alpha-1}$. Then $\rho(a_m^l b_m) = s_\alpha^{ln+t}$. Since ρ is a homomorphism, $|s_\alpha^{ln+t}|$ must divide 2. This is possible when n is one of 0, $2^{\alpha-2}$. Thus we have 4 such homomorphisms. Suppose $\rho(b_m) = s_\alpha^t$, where $t = 2^{\alpha-3}$ or $3\ 2^{\alpha-3}$, and $\rho(a_m) = s_\alpha^n$, where $|s_\alpha^n|$ divides both $2m$ and $2^{\alpha-1}$ but does not divide m. Then $\rho(a_m^l b_m) = s_\alpha^{ln+t}$. Since ρ is a homomorphism, $|s_\alpha^{ln+t}|$ must divide 4 but not 2, which is not possible.

Suppose $\rho(a_m) = s_\alpha^n$, where $|s_\alpha^n|$ divides both $2m$ and $2^{\alpha-1}$ but does not divide m, and $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is odd. Then $\rho(a_m^l b_m) = s_\alpha^{ln+k_2}t_\alpha$. Therefore, $|\rho(a_m^l b_m)|$ divides $|a_m^l b_m| = 4$, for every $0 \le l < 2m$. Then ρ is well defined only when n is even. Therefore, $|s_\alpha^n|$ must divide $2^{\alpha-2}$ also. Thus we have $2^{\alpha-2}\left(\sum_{k|\gcd(2m,2^{\alpha-2})}\phi(k)\right)$ homomorphisms.

Suppose $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is even and $\rho(a_m) = s_\alpha^n$, where $|s_\alpha^n|$ divides both m and $2^{\alpha-1}$. Thus we have $2^{\alpha-2}\left(\sum_{k|\gcd(m,2^{\alpha-1})}\phi(k)\right)$ homomorphisms.

Suppose $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and $\rho(b_m) = s_\alpha^t$, where $|s_\alpha^t| = 4$. Then $\rho(a_m^l b_m)$ is one of s_α^t, $s_\alpha^{k_1-t}t_\alpha$, $s_\alpha^{k_1 2^{\alpha-2}+t}$ or $s_\alpha^{k_1 2^{\alpha-2}+k_1-t}t_\alpha$. Then k_1 must be odd when $m \equiv 2\ (mod\ 4)$. Thus we have $2 \times 2^{\alpha-2} = 2^{\alpha-1}$ homomorphisms when $m \equiv 2\ (mod\ 4)$; 2^α homomorphisms when $m \equiv 0\ (mod\ 4)$.

Suppose $\rho(b_m) = s_\alpha^t$, where $|s_\alpha^t| = 1$ or 2 and $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$, then k_1 must be even when $m \equiv 2\ (mod\ 4)$. Thus we have $2 \times 2^{\alpha-2} = 2^{\alpha-1}$ homomorphisms when $m \equiv 2\ (mod\ 4)$; 2^α homomorphisms when $m \equiv 0\ (mod\ 4)$.

Suppose $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$. Then $\rho(a_m^l b_m)$ is one of $s_\alpha^{k_2}t_\alpha$, $s_\alpha^{k_1-k_2}$, $s_\alpha^{k_1 2^{\alpha-2}+k_2}t_\alpha$ or $s_\alpha^{k_1 2^{\alpha-2}+k_1-k_2}$. Then ρ is a homomorphism only when $k_1 - k_2$ is one of 0, $2^{\alpha-2}$, $2^{\alpha-3}$ or $3\ 2^{\alpha-3}$. Thus we have $4 \times 2^{\alpha-1} = 2^{\alpha+1}$ homomorphisms. Hence we get the result. □

Corollary 4.1. *Let $\alpha > 3$ and m be any two positive integers. Then the number of monomorphisms from Q_m into QD_{2^α} is $2^{\alpha-2}\phi(2m)$, if $2m$ divides $2^{\alpha-2}$ and $m \neq 2$; $3\ 2^{\alpha-1}$, if $m = 2$; and 0, otherwise.*

Proof. Suppose $2m$ does not divide $2^{\alpha-1}$, then there is no monomorphism from Q_m into QD_{2^α} since there is no element in QD_{2^α} having order $2m$. So, assume that $2m$ divides $2^{\alpha-2}$ and $m \neq 2$. Then $\rho(a_m) = s_\alpha^n$, where $|s_\alpha^n| = 2m$ and $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is odd are homomorphisms that preserve the order of a_m and b_m. Then $\rho(a_m^l b_m) = s_\alpha^{ln+k_2}t_\alpha$. Then $|\rho(a_m^l b_m)| = |a_m^l b_m|$ only when n is even. Therefore, $2m$ cannot equal to $2^{\alpha-1}$. Thus we have $2^{\alpha-2}\phi(2m)$ monomorphisms from Q_m into QD_{2^α}, if $2m$ divides $2^{\alpha-2}$ and $m \neq 2$.
Suppose that $\rho : Q_2 \to QD_2^\alpha$ is a monomorphism. Then $\rho(a_m)$ is one of $s_\alpha^{2^{\alpha-3}}$, $s_\alpha^{3\ 2^{\alpha-3}}$ or $s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and k_1 is odd; and $\rho(b_m)$ is one of $s_\alpha^{2^{\alpha-3}}$, $s_\alpha^{3\ 2^{\alpha-3}}$ or $s_\alpha^{k_1}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is odd.
Suppose $\rho(a_m) = s_\alpha^{2^{\alpha-3}}$ or $s_\alpha^{3\ 2^{\alpha-3}}$ and $\rho(b_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is odd is a monomorphism. Thus we have $2^{\alpha-1}$ monomorphisms. Similarly if $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and k_1 is odd, and $\rho(b_m) = s_\alpha^{2^{\alpha-3}}$ or $s_\alpha^{3\ 2^{\alpha-3}}$ is a monomorphism. Thus we have another $2^{\alpha-1}$ monomorphisms.
Suppose $\rho(a_m) = s_\alpha^{k_1}t_\alpha$, $0 \le k_1 < 2^{\alpha-1}$ and k_1 is odd and $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ and k_2 is odd. Then $\rho(a_m^l b_m)$ is one of $s_\alpha^{k_1}t_\alpha$, $s_\alpha^{k_1+k_2 2^{\alpha-2}-k_2}$, $s_\alpha^{k_1 2^{\alpha-2}+k_2}t_\alpha$ or $s_\alpha^{k_1 2^{\alpha-2}+k_1-k_2}$. Then $|\rho(a_m^l b_m)| = 4$ only when $k_1 - k_2$ is either $2^{\alpha-3}$ or $3\ 2^{\alpha-3}$. Thus we have $2^{\alpha-1}$ monomorphisms. Hence we get the result. □

Corollary 4.2. *Let $\alpha > 3$ and m be any two positive integers. Then the number of epimorphisms from Q_m onto QD_{2^α} is $2^{2\alpha-3}$, if $2^{\alpha-1}$ divides m; 0, if $2^{\alpha-1}$ does not divide m.*

Proof. If $2^{\alpha-1}$ does not divide m, none of the homomorphisms obtained in the Theorem 4.2, is onto. But if $2^{\alpha-1}$ divides m, the homomorphisms $\rho(a_m) = s_\alpha^{k_1}$, where k_1 is odd, and $\rho(b_m) = s_\alpha^{k_2}t_\alpha$, $0 \le k_2 < 2^{\alpha-1}$ is onto since $\rho(a_m)$ and $\rho(b_m)$ generate the group QD_{2^α}. Thus we have $2^{\alpha-1}\phi(2^{\alpha-1}) = 2^{2\alpha-3}$ epimorphisms, if $2^{\alpha-1}$ does not divide m. □

5. The Number of Homomorphisms from Q_m into M_{p^α}

Theorem 5.1. *Let $p \neq 2$ be a prime, m be a positive integer and $\alpha > 2$. Then there is only the trivial homomorphism from Q_m into M_{p^α}.*

Proof. Suppose $\rho : Q_m \to M_{p^\alpha}$ is a group homomorphism, where $p \neq 2$. Then $|\rho(a_m)|$ divides $|a_m| = 2m$ and $|\rho(b_m)|$ divides $|b_m| = 4$. Then $\rho(b_m)$ must be e and $\rho(a_m) = r_\alpha^k$, where $|r_\alpha^k|$ divides both $2m$ and $p^{\alpha-1}$. Then $\rho(a_m^l b_m) = r_\alpha^{lk}$. Then $|r_\alpha^{lk}|$ must divide $|a_m^l b_m| = 4$. This is possible only when $k = 0$. Thus we have only the trivial homomorphism. □

Theorem 5.2. *Let m be a positive integer and $\alpha > 3$. If m is odd, then the number of homomorphisms from Q_m to M_{2^α} is 4 homomorphisms, if m is odd; 32 homomorphisms, if m is even.*

Proof. Suppose $\rho : Q_m \to M_{2^\alpha}$ is a group homomorphism. Then $|\rho(a_m)|$ divides $|a_m| = 2m$ and $|\rho(b_m)|$ divides $|b_m| = 4$. Then $\rho(a_m) = r_\alpha^{k_1}f_\alpha^{m_1}$, where $|r_\alpha^{k_1}|$ divides both $2m$ and $2^{\alpha-1}$ and $m_1 = 0, 1$ and $\rho(b_m) = r_\alpha^{k_2}f_\alpha^{m_2}$, where $|r_\alpha^{k_2}|$ divides 4 and $m_2 = 0, 1$. Then $\rho(a_m b_m) = r_\alpha^{k_1+k_2+m_1 k_2 2^{\alpha-2}}f_\alpha^{m_1+m_2}$. Then ρ is a homomorphism only when $|r_\alpha^{k_1+k_2}|$ divides 4. Then $k_1 + k_2$ is one of 0, $2^{\alpha-2}$, $2^{\alpha-3}$ or $3\ 2^{\alpha-3}$. If $k_2 = 0$ or $2^{\alpha-2}$, then $\rho(b_m^2) = e$. Then $|\rho(a_m)|$ must divide m. Thus $\rho(a_m)$ must be e, if m is odd; k_1 is either 0 or $2^{\alpha-2}$, if $m \equiv 2\ (mod\ 4)$; k_1 is one of 0 or $2^{\alpha-2}$, $2^{\alpha-3}$ or $3\ 2^{\alpha-3}$ if $m \equiv 2\ (mod\ 4)$. Therefore, we have 2 homomorphisms, if m is odd; 16 homomorphisms, if $m \equiv 2\ (mod\ 4)$; 32 homomorphisms, if $m \equiv 0\ (mod\ 4)$.

If $k_2 = 2^{\alpha-3}$ or $2^{\alpha-3}$, then $\rho(b_m^2) = r_\alpha^{2^{\alpha-2}}$. Then $|\rho(a_m)|$ must not divide m. Thus, $\rho(a_m)$ is $r_\alpha^{2^{\alpha-2}}$, if m is odd; k_1 either $2^{\alpha-3}$ or $3\ 2^{\alpha-3}$, if $m \equiv 2\ (mod\ 4)$; there is no such choice, if $m \equiv 0\ (mod\ 4)$. Therefore in this case, we have 2 homomorphisms, if m is odd; 16 homomorphisms, if $m \equiv 2\ (mod\ 4)$; 0 homomorphisms, if $m \equiv 0\ (mod\ 4)$. □

Corollary 5.1. *Suppose $\alpha > 3$ and $\beta > 2$ are two positive integers. Then there is no monomorphism from QD_{2^α} into M_{2^β}; no epimorphisms from Q_m onto M_{2^β}.*

Proof. The group QD_{2^α} contains $1+2^{\alpha-2}$ elements having order 2. But M_{2^α} have only two elements of order 2. Therefore there is monomorphism from QD_{2^α} into M_{2^α}. Also we can verify that none of the homomorphisms obtained in the Theorem 5.2 are epimorphism. □

References

[1] M.Bate, *The number of homomorphisms from finite groups to classical groups*, J. Algebra, 308(2007), 612-628

[2] J.A.Gallian and J.Van Buskirk, *The number of homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$*, Amer. Math. Monthly, 91(1984), 196-197.

[3] J.A.Gallian and D.S.Jungreis, *Homomorphisms from $\mathbb{Z}_m[i]$ into $\mathbb{Z}_n[i]$ and $\mathbb{Z}_m[\rho]$ into $\mathbb{Z}_n[\rho]$, where $i^2+1=0$ and* $\rho^2+\rho+1=0$, Amer. Math. Monthly, 95(1988), 247-249.

[4] Jeremiah Johnson, *The number of group homomorphisms from D_m into D_n*, The College Mathematics Journal, 44(2013), 190-192.

[5] D.Matei and A.Suciu, *Counting homomorphisms onto finite solvable groups*, J. Algebra, 286 (2005), 161-186.

[6] R.Rajkumar, M.Gayathri and T.Anitha, *The number of homomorphisms from dihedral groups in to some finite groups*, Mathematical Sciences International Research Journal, 4(2015), 161-165.