

**A
MEASURE OF COMMUTATIVITY
OF
THE QUATERNION GROUP**

A Dissertation
Submitted to the Gauhati University in partial
fulfilment of the requirements for the award
of the Degree of Master of Philosophy
in Mathematics



BY

GAYATREE DAS

DEPARTMENT OF MATHEMATICS

GAUHATI UNIVERSITY

MARCH, 1993

**A
MEASURE OF COMMUTATIVITY
OF
THE QUATERNION GROUP**

A Dissertation

**Submitted to the Gauhati University in partial
fulfilment of the requirements for the award
of the Degree of Master of Philosophy
in Mathematics**



BY

GAYATREE DAS

DEPARTMENT OF MATHEMATICS


GAUHATI UNIVERSITY

MARCH, 1993

This is to certify that the Dissertation entitled "A MEASURE OF COMMUTATIVITY OF THE QUATERNION GROUP", is the outcome of study and investigations carried out by Miss Gayatree Das and it has been done under my supervision and guidance in partial fulfilment of the M.Phil regulations of Gauhati University. Neither the dissertation nor any part thereof was previously submitted to this or any other University for any degree.

Miss Das fulfils the requirements of the regulations relating to the nature and prescribed period of course and research work for the award of Master of Philosophy of the Gauhati University.

Gauhati University
the 15th March 1993


Kuntala Patra
Lecturer
Mathematics Department
Gauhati University.

ACKNOWLEDGEMENTS

At the very beginning I express my sincere thanks to my supervisor Dr. Kuntala Patra, Lecturer, Department of Mathematics, Gauhati University, for extending her whole hearted cooperation in all respects for preparing this dissertation.

I am also grateful to Professor B.P. Chetiya, Department of Mathematics, Gauhati University for his constant help and encouragement throughout the preparation of this dissertation.

At the end, I express my sincere thanks to Mr. S.K. Das of the Department of Mathematics for typing this dissertation in a neat and presentable form.



Gayatree Das

"A MEASURE OF COMMUTATIVITY OF THE QUATERNION GROUP"

SYNOPSIS

The main purpose of this dissertation is to determine the Joseph measure of Quaternion group Q_n , $n \geq 2$. A pair (x,y) of elements of a group will be called a commuting pair if $xy = yx$. This was exactly the approach adopted by Joseph [Joseph, K.S.; 1969] in his doctoral thesis while defining the measure of commutativity of a finite non-commutative group. The Joseph measure of a finite non-commutative group G is

$$J(G) = \frac{\text{number of such commuting ordered pairs}}{|G|^2}$$

then $J(G)$ is the probability that a pair of element chosen at random in G , will commute with each other. Clearly $J(G) = 1$ if and only if G is abelian. In this dissertation we have defined the Joseph [Machale, P.D.; 1972] measure of a group G by

$$J(G) = \frac{K(G)}{|G|}, \text{ where } K(G) \text{ denotes the number of}$$

(ii)

conjugacy classes of G and $|G|$ is the order of the group G .

In Chapter 1 we have defined the "commutativity measure" of a finite group and given a theorem of determining the commutativity measure with the help of conjugacy classes of a group.

In Chapter 2 we have described the free groups and its presentations or abstract definitions.

In Chapter 3 we ^{have} defined the quaternion group and ~~given~~ a permutational representation of the group Q_n . As we know that [Armstrong, M.A.; 1987] the conjugate permutations have the same cycle structure, so a permutational representation of the group will help us in determining the conjugacy classes of the group.

In chapter 4 we have completely determined $J(Q_n)$ for every $n \in \mathbb{N}$ and finally obtained

$$J(Q_n) = \frac{n+3}{4n}$$

and from this we conclude that $J(Q_n) \in (\frac{1}{4}, 5/8]$ for $n \geq 2$.

Earlier in chapter 1, the problem of the dissertation is introduced and some preliminaries that are used as tools in the subsequent chapters.

A fairly exhaustive bibliography is added at the end of this dissertation.

CONTENTS

	<u>Page</u>
Acknowledgements	
Synopsis	i - ii
Chapter I Introduction	1 - 18
Chapter 2 Free groups and presentations	19 - 41
2.1 Free groups	19 - 29
2.2 Presentation of groups	29 - 41
Chapter 3 The Quaternion group and its presentation	42 - 55
3.1 The Quaternion group	42 - 47
3.2 Properties of Quaternion group and generalized quaternion group.	47 - 53(b)
3.3 Permutational representation of the Quaternion group	53(b) - 55
Chapter 4 Number of conjugacy classes and measure of Quaternion group	56 - 77
4.1 Listing of Conjugacy Classes	56 - 65
4.2 Determination of $J(Q_n)$	66 - 77
Bibliography	78 - 80

CHAPTER 1

INTRODUCTION

The purpose of this chapter is to explain the notion of the Joseph measure of commutativity of a finite group [Joseph K.S.; 1969] and to develop some machinery for use in the final chapter of the dissertation. Joseph observed that in an abelian or commutative group all the pairs of elements commute ; so the number of commuting pairs of elements in a non-commutative group may help us in defining a nice "measure" of the commutativity of the group. We present below Joseph's approach to define such a measure.

Let us examine the Cayley table of Q , the quaternion group of order 8, whose elements constitute the set—

$$\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$$

If $xy = yx$, where x, y belong to a group G , we call this situation a commutativity and place the number 1 in both of the boxes corresponding to xy and yx in the Cayley table for G . Similarly, if $xy \neq yx$ we place the number zero in both of these boxes. With this convention, Table 1 becomes :

Table 2

	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$	$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$	$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	1	1	1	1	1	1	1
$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	1	1	1	1	1	1	1	1
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	1	1	1	1	0	0	0	0
$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	1	1	1	1	0	0	0	0
$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$	1	1	0	0	1	1	0	0
$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$	1	1	0	0	1	1	0	0
$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$	1	1	0	0	0	0	1	1
$\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$	1	1	0	0	0	0	1	1

So we have a total of 40 commutativities out of a possible 64. Hence

$$\frac{40}{64} = 5/8$$

may perhaps be taken as a measure of commutativity of the group G .

Let us denote by $J(G)$ the fraction got by dividing the total number of commutativities in a finite group G by $|G|^2$, the square of the order of G . It is at once evident that $J(G) = 1$ if and only if G is commutative. Our object is to investigate the ratio $J(G)$ and to see if there are any restrictions on the values it may assume. The measure $J(G)$ will be referred to as the Joseph measure for the group G .

In other words $J(G)$ gives the probability that a pair of elements, chosen at random in G will commute with each other.

Some other information of a finite group also gives the idea about the tendency of a group of being commutative. For example, for a group G we can determine the centre $Z(G) = \{x \in G : xg = gx, \forall g \in G\}$ of the group. The more the number of elements in $Z(G)$ the greater will be the tendency of the group of being commutative. If $Z(G)$ equals G then G is commutative. If $Z(G)$ contains only one element

(the identity element) then the group will be totally non-commutative, that is $J(G)$ is least in such case.

The solubility of a group also gives the idea of the measure of commutativity of a finite group. A group G having a finite derived series

$$G = \delta_0(G) \triangleright \delta_1(G) \triangleright \delta_2(G) \triangleright \dots \triangleright \delta_n(G) = \{e\}$$

where $\delta_i(G)$ is the derived group of $\delta_{i-1}(G)$ is called a soluble or solvable group of length n .

The group G has a tendency of being commutative if the length n of the derived series is shorter. If $n = 2$ in the derived series of a solvable group, then the group G is known to be a metabelian group. So the next maximum value of $J(G)$ will be attained for metabelian groups.

By knowing the derived group of a group also we can form an idea about how much commutative can the group be.

A group G has a tendency of being commutative if it has a smaller derived group. But unfortunately there is no efficient method to compute the order of the centre or the length of the derived series of a group.

On the other hand there is a very efficient method given by Machalé [1972] for the determination of $J(G)$ of a

given finite group G . He proved a theorem for determining $J(G)$ with the help of conjugacy classes of a group. Before giving the main result due to Machale for determining $J(G)$ we need to recall a few facts from elementary group theory.

We begin with the definition of conjugate element and some well-known results of conjugacy classes. Most of the results of this chapter are contained in standard literature ([Hall; 1959], [Armstrong; 1987], [Scott; 1964], [Ledermann; 1961]).

Let x and y be any two elements of a group G , we say that x is conjugate to y if $gxg^{-1} = y$ for some $g \in G$.

The collection of all elements conjugate to a given element is called a conjugacy class, we claim that the distinct conjugacy classes form a partition of G . Let R be a subgroup of $G \times G$ consisting of pairs (x, y) for which x is conjugate to y . Each $x \in G$ is conjugate to itself as $exe^{-1} = x$, e is the identity element of G .

If x is conjugate to y , say $gxg^{-1} = y$, then y is conjugate to x as $g^{-1}yg = x$. Finally, if x is conjugate to y and y to z , say $g_1xg_1^{-1} = y$, $g_2yg_2^{-1} = z$, then x is conjugate to z because,

$$\begin{aligned} (g_2g_1) x (g_2g_1)^{-1} &= g_2(g_1xg_1^{-1}) g_2^{-1} \\ &= g_2yg_2^{-1} \\ &= z. \end{aligned}$$

Therefore R is an equivalence relation on R and its equivalence classes, the conjugacy classes mentioned above, partition G . These conjugacy classes will be worked out for quaternion groups in chapter 4.

Every class consists of elements conjugate to each other and the classes are mutually disjoint and the union of the classes is G . So if for a group there are K -distinct equivalence classes, then

$$G = [a_1] \cup [a_2] \cup \dots \cup [a_k], \quad \text{where}$$

$[a_i] \cap [a_j] = \emptyset$, $i \neq j$ and $[a_i]$ denotes the equivalence class containing the element a_i . If the number of elements in the equivalence class $[a_r]$ is h_r and the order of G is n , then we have

$n = h_1 + h_2 + h_3 + \dots + h_k$, which is called the class equation for G .

For a fixed element $g \in G$ the function from G to G given by

$$x \rightarrow gxg^{-1}$$

is an isomorphism called conjugation by g . (It is a bijection because it is invertible, its inverse being conjugation by g^{-1} ,

and it preserves the algebraic structure of G because

$$g(xy)g^{-1} = (gxg^{-1})(gyg^{-1})$$

for any two elements $x, y \in G$. Since an isomorphism preserves the order of an element we see that elements in the same conjugacy class must have the same order.

Let K be any complex (i.e. subset) of G . Then the set

$$\{x : x^{-1}Kx = K\}$$

is called the normalizer of the complex K and is denoted by $N(K)$. If K is a singleton set say $\{k\}$, then the normalizer is called the centralizer of the element k and is denoted by $N(k)$.

Both the normalizer and the centralizer are subgroups of G .

Lemma 1.1 $[G : N(K)]$ is equal to the number of the distinct conjugates of K in G .

Proof : Let $a, b \in G$

a is equivalent to b , denoted by $a \sim b$ if $a^{-1}Ka = b^{-1}Kb$.

Then ' \sim ' is an equivalence relation in G , because

$$(i) \quad a^{-1}Ka = a^{-1}Ka \Rightarrow a \sim a$$

$$(ii) \quad a \sim b \Rightarrow a^{-1}Ka = b^{-1}Kb$$

$$\Rightarrow b^{-1}Kb = a^{-1}Ka$$

$$\Rightarrow b \sim a$$

$$(iii) \quad a \sim b \Rightarrow a^{-1}Ka = b^{-1}Kb$$

$$\text{and } b \sim c \Rightarrow b^{-1}Kb = c^{-1}Kc;$$

Hence $a^{-1}Ka = c^{-1}Kc$, which implies that

$$a \sim c.$$

The number of equivalence classes is then equal to the number of distinct conjugates of K in G .

As usual $[a]$ denotes the equivalence class containing a .

It is to be observed that

$$[1] = N(K), [[1] = \{x \in G : x^{-1}Kx = 1^{-1}K1 = K\}]$$

Let $[x]$ be an equivalence class $\neq [1]$.

First we show that

$$[x] = [1]x.$$

$$\begin{aligned}
\text{Observe that } b \in [x] &\Leftrightarrow b^{-1}Kb = x^{-1}Kx \\
&\Leftrightarrow xb^{-1}Kbx^{-1} = K \\
&\Leftrightarrow (bx^{-1})^{-1}K(bx^{-1}) = K (=1^{-1}K1) \\
&\Leftrightarrow bx^{-1} \in [1] \\
&\Leftrightarrow b \in [1]x
\end{aligned}$$

Thus

$$[x] = [1]x = \{N(K)\}x$$

This shows that the number of distinct classes is equal to the number of distinct right cosets of $N(K)$, i.e. the index of $N(K)$ in G , i.e.

$$[G : N(K)]$$

So ultimately it follows that

$$[G : N(K)] = \text{The number of distinct conjugates of } K \text{ in } G.$$

This can be expressed also ^{in the} following form :

$$O(N(K)) = \frac{O(G)}{\text{The number of distinct conjugates of } K \text{ in } G}$$

(if G is finite)

Corollary 1.1.1 : If the complex K of the group G consists

of the single element a i.e. if $K = \{a\}$, then

$[G : N(a)] =$ number of elements of the conjugacy class $[a]$.

An element $a \in G$ is called self conjugate if and only if

$$a = x^{-1}ax \quad \forall x \in G \quad \text{or} \quad xa = ax \quad \forall x \in G.$$

Thus a self conjugate element is one which commutes with each element of the group.

The centre of a group G consists of all those elements which commute with every element of G . It is usually denoted by $Z(G)$ so that $Z(G) = \{x \in G : xg = gx, \forall g \in G\}$

Lemma 1.2. The centre is a subgroup of G and is made up of the conjugacy classes which contain just one element.

Proof : If $x, y \in Z(G)$ and $g \in G$, then

$$\begin{aligned} gxy^{-1} &= xgy^{-1} \quad [\text{because } x \in Z(G)] \\ &= x(yg^{-1})^{-1} \\ &= x(g^{-1}y)^{-1} \quad (\because y \in Z(G)) \\ &= xy^{-1}g \end{aligned}$$

Therefore, $xy^{-1} \in Z(G)$. Certainly $e \in Z(G)$, so the centre is a subgroup.

Since $xg = gx$ if and only if $gxg^{-1} = x$, we see that x lies in $Z(G)$ precisely when the conjugacy class of x is the singleton set $\{x\}$.

Lemma 1.3. If G is a non-commutative group then the factor group $G/Z(G)$ cannot be cyclic.

Proof : Assume that $Z(G) = Z$ and let G/Z be cyclic, generated by Zg .

Then

$$\begin{aligned} G &= Z \cup Zg \cup (Zg)^2 \cup \dots \cup (Zg)^k \cup \dots \\ &= Z \cup Zg \cup Zg^2 \cup \dots \cup (Zg)^k \cup \dots \end{aligned}$$

Typical elements of G may now be expressed as Z_1g^i and Z_2g^j , where Z_1 and $Z_2 \in Z$. These elements clearly commute.

Since,

$$(Z_1g^i)(Z_2g^j) = (Z_2g^j)(Z_1g^i) \quad [\because Z_1, Z_2 \in Z]$$

Contradicting the fact that G is non-commutative.

Hence $G/Z(G)$ cannot be cyclic.

Lemma 1.4 $G/Z(G)$ cannot have prime order for any group G .

Proof : We know that a group of prime order is cyclic. But from the lemma 4.3 $G/Z(G)$ cannot be cyclic, so it cannot have prime order for any group G .

Now we shall state and give the proof of the theorem due to Machale (1972).

Theorem 1.1 : Let the finite group G have $K(G)$ conjugacy classes. Then $J(G) = K(G)/|G|$.

Proof : Suppose the group G has n conjugacy classes, and they are $[a_1], [a_2], \dots, [a_n]$. Therefore

$$[a_1] \cup [a_2] \cup \dots \cup [a_n] = G$$

$$\text{i.e. } h_1 + h_2 + \dots + h_n = |G|$$

where h_r denotes the number of elements in the class $[a_r]$.

We recall that $\mathcal{C}(G)$ denote the total number of all the commuting pairs of element of G . For a fixed element a of G the number of commuting pairs of the form (a, x) , $x \in G$, is equal to the order of $N(a)$, i.e. $|N(a)|$. Thus the number of all commuting pairs of elements of G is equal to

$$\sum_{a \in G} |N(a)|$$

$$\text{i.e. } \mathcal{C}(G) = \sum_{a \in G} |N(a)| .$$

Now, by definition of $J(G)$ as given earlier, we have

$$\begin{aligned}
 J(G) &= \frac{C(G)}{|G|^2} = \sum_{a \in G} \frac{|N(a)|}{|G|^2} \\
 &= \frac{1}{|G|^2} \sum_{a \in G} |N(a)| \\
 &= \frac{1}{|G|^2} \sum_{a \in G} \frac{|G|}{|[a]|} \quad [\text{Using Cor. 1.1.1.}]
 \end{aligned}$$

Hence $|[a]|$ denotes the number of elements of the conjugacy class $[a]$.

$$\begin{aligned}
 \text{Now, } J(G) &= \frac{1}{|G|} \sum_{a \in G} \frac{1}{|[a]|} \\
 &= \frac{1}{|G|} \sum_{i=1}^n \frac{h_i}{h_i} \\
 &= \frac{1}{|G|} n \\
 &= \frac{K(G)}{|G|}
 \end{aligned}$$

Theorem 1.2 :

If G is a finite non-commutative group then

$$J(G) \leq 5/8.$$

Proof : Suppose $K(G)$ denotes the number of conjugacy classes of the finite group G . Now, to maximise $K(G)$ we must make $|Z(G)|$, the number of one-element classes, as large as possible. By lemma 1.4, $|G/Z(G)|$ cannot be 2 or 3 and hence $|G/Z(G)| \geq 4$ i.e. $|Z(G)| \leq \frac{3}{4} |G|$. This leaves $\frac{1}{4} |G|$ elements, which must be distributed among classes containing at least two elements each.

$$\text{Thus } K(G) \leq \frac{1}{4} |G| + \frac{1}{2} \cdot \frac{3}{4} |G| = \frac{5}{8} |G|$$

$$\text{so that } J(G) = \frac{K(G)}{|G|} \leq \frac{5}{8}$$

Theorem 1.3 [Gallagher; 1970]

If H is any subgroup of G , then

$$J(G) \leq J(H)$$

Proof : We may assume that $H \neq G$, since otherwise the result is obvious. Here we shall use the symbol $N_G(x)$ to denote the normaliser of x in G .

As in the proof of theorem 1.1,

$$K(G) = \frac{1}{|G|} \sum_{g \in G} |N_G(g)| \quad \text{and} \quad K(H) = \frac{1}{|H|} \sum_{g \in H} |N_H(g)|$$

we have,

$N_H(g) \subset N_G(g)$, since H is a subgroup of G and $H \neq G$.

$$\text{i.e. } \sum_{g \in H} |N_H(g)| < \sum_{g \in G} |N_G(g)|$$

$$\text{i.e. } \frac{1}{|H|} \sum_{g \in H} |N_H(g)| < \frac{|G|}{|H|} \frac{1}{|G|} \sum_{g \in G} |N_G(g)|$$

i.e. $K(H) < [G : H] K(G)$, where $[G : H]$ is the index of H in G . We now use twice the inequality

$|N_G(g)| \leq [G : H] |N_H(g)|$ to obtain

$$\sum_{g \in G} |N_G(g)| \leq [G : H] \sum_{g \in G} |N_H(g)|$$

$$= [G : H] \sum_{t \in H} |N_G(t)|$$

$$\leq [G : H]^2 \sum_{t \in H} |N_H(t)|$$

$$\text{i.e. } \sum_{g \in G} |N_G(g)| \leq \frac{|G|^2}{|H|^2} \sum_{t \in H} |N_H(t)|$$

$$\text{i.e. } \frac{1}{|G|} \sum_{g \in G} |N_G(g)| \leq \frac{|G|}{|H|} \cdot \frac{1}{|H|} \sum_{t \in H} |N_H(t)|$$

$$\text{i.e. } K(G) \leq [G : H] K(H)$$

$$\text{i.e. } \frac{K(G)}{|G|} \leq \frac{K(H)}{|H|}$$

which implies that $J(G) \leq J(H)$.

Now we shall list some 'forbidden values' of the function $J(G)$. We have already seen that $J(G) \notin (5/8, 1)$ for any finite group G . If $J(G) > \frac{1}{2}$, it can be shown that

$J(G) = \frac{1}{2} + \left(\frac{1}{2}\right)^{2s+1}$ for some positive integer s . The group

S_3 shows that it is possible to have $J(G) = \frac{1}{2}$. However, if $p (\neq 2)$ is the least prime number dividing $|G|$, it is not possible to have $J(G) = 1/p$. (Note however that if $G = A_4$, the tetrahedral group which is isomorphic to the group of all even permutations on four symbols, then $J(A_4) = \frac{1}{3}$).

Finally, we state the rather surprising fact that it is not possible to have $J(G) \in \left(\frac{7}{16}, \frac{1}{2}\right)$ for any finite group G .

Our main objective in this dissertation is to find the Joseph measure of the family of quaternion groups. The problem relating to two other classes of finite groups (i) the dihedral groups D_n ($n \geq 3$), (ii) the K -meta cyclic groups have been studied by Miss Anu Kalita (1989) and Mrs Niva Barman (1993) respectively.

As the notion of free groups play an important role in finding an abstract definition or presentation of groups, so in our next chapter we discuss free groups and presentation of groups. In chapter 3 we obtained a presentation of

quaternion group Q_n of order $4n$, $n \geq 2$ and used this presentation of Q_n to get a suitable permutational representation of it.

In the last chapter we shall determine the conjugacy classes of Q_n and used the theorem 1.1 to obtain the Joseph measure of Q_n for every $n \in \mathbb{N}$. Precisely speaking we shall show that $J(Q_n) = \frac{n+3}{4n}$ for all n . And it follows that $J(Q_n) = 5/8$ if and only if $n = 2$ i.e. Q_n attains the maximum value $5/8$ of $J(G)$ and no other member of this family (Q_n , $n \geq 3$; Q_n is commutative for $n = 1$) attains the maximum value. Also we shall show that $J(Q_n) \in (\frac{1}{4}, 5/8]$ for $n \geq 2$.

A fairly exhaustive bibliography is added at the end of the dissertation.

CHAPTER 2

FREE GROUPS AND PRESENTATIONS

The main purpose of this chapter is to discuss the notion of a presentation (or an abstract definition) of a group because our discussion in succeeding chapters will be on finding, and on employing a presentation of the quaternion group. But the notion of a presentation of a group is inseparably linked with the notion of free groups. We therefore begin with a carefull description of "free groups".

In § 2.1 of this chapter we give some elementary definitions, and discuss free groups and their properties. Having developed some elementary but important properties of free groups (such as their existence), We also give two theorems which will be basic tools for the latter chapters of our dissertation.

In § 2.2 we discuss the notion of a presentation of a group.

2.1. Free Groups :

Let X be a non-empty arbitrary set. For each $x \in X$

define a new symbol x^{-1} and make no distinction between x and x^1 .

An X-word is a finite ordered succession of symbols of the form :

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}, \quad \varepsilon_i = \pm 1, \quad x_i \in X$$

where repetitions are permissible.

The positive integer 'n' is called the length of the word.

A word is said to be a reduced word, if it is of the form :

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}, \quad \text{in which } x_i^{\varepsilon_i} \neq x_{i+1}^{-\varepsilon_{i+1}},$$

$$1 \leq i \leq n-1.$$

Thus a word is a reduced word if it does not contain any pair of the form xx^{-1} or $x^{-1}x$.

A word having no symbols in it is called an empty word or a null-word. An empty word is usually denoted by the symbol 1. Obviously an empty word is a reduced word.

$$\text{Let } u = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m}, \quad \varepsilon_i = \pm 1, \quad x_i \in X.$$

$$v = y_1^{\eta_1} y_2^{\eta_2} \dots y_n^{\eta_n}, \quad \eta_i = \pm 1, y_i \in X$$

be two X-words. The product uv is defined as the X-word given by

$$uv = x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} y_1^{\eta_1} \dots y_n^{\eta_n}$$

The X-words u and v are said to be identical if $m = n$, $x_i = y_i$, $\varepsilon_i = \eta_i$ for $i = 1, 2, 3, \dots, m$. If they are not identical then they are said to be different. Also u and v are said to be equivalent and denoted by $u \sim v$ if v can be obtained from u by inserting or deleting a finite number of X-words of the form xx^{-1} or $x^{-1}x$.

The equivalence between X-words defines an equivalence relation on the set of all X-words. The equivalence class containing the X-word u is denoted as usual by the symbol $[u]$. It can be seen that equivalence class contains one and only one reduced word. The product of two equivalence classes $[u]$ and $[v]$ of X-words is defined to be the class $[uv]$.

The product of two equivalence classes of X-words is well defined, and the set of all equivalence classes with this binary operation forms a group.

The proof of the above result is as follows :

First we show that if $[u'] = [u]$

and $[v'] = [v]$, then $[u'v'] = [uv]$

$$[u'] = [u] \Rightarrow u' \sim u \Rightarrow [u'v] = [uv]$$

because $u'v$ and uv are equivalent if u' and u are equivalent. Similarly

$$[v'] = [v] \Rightarrow v' \sim v \Rightarrow [u'v'] = [u'v]$$

Thus $[u'v'] = [uv]$.

Next we verify the group axioms.

1) Closure : It is obvious.

2) Associativity :

$$\begin{aligned} [u] ([v][w]) &= [u] [vw] \\ &= [u (vw)] \\ &= [(uv)w] \\ &= [uv] [w] \\ &= ([u][v]) [w] . \end{aligned}$$

3) Identity :

Let $[1]$ be the class containing the empty word. Then

$$[1][u] = [lu] = [u],$$

$$[u][1] = [ul] = [u].$$

therefore $[1]$ is an identity element.

4) Inverses :

Let $u = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$, $\epsilon_i = \pm 1$, be any X -word. Then

$$u x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1} \sim 1,$$

$$x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1} u \sim 1$$

and so

$$[u x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1}] = [1]$$

$$[x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1} u] = [1]$$

so that $[x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1}]$ is an inverse of $[u]$.

Let X be a non-empty set, the group of all equivalence

classes of X-words under multiplication of equivalence classes is called the free-group on the set X. Now the free-group on X may be considered as the group of the reduced X-words under multiplication defined as follows :

$$\text{If } u = x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m}, v = y_1^{\eta_1} \dots y_n^{\eta_n}, \varepsilon_i \eta_i = \pm 1$$

are two reduced X-words, then their product uv is taken as the reduced X-word obtained by deleting in

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m} y_1^{\eta_1} \dots y_n^{\eta_n}$$

the pairs of symbols of the form

$$xx^{-1} \quad \text{and} \quad x^{-1}x$$

Let F be the free-group on a set X . Since every element of X is a reduced X-word, the set X may be considered as a subset of F . This leads us to the following observation:

In the free-group F on a subset X every element can be expressed in a unique manner in the form :

$$x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}, x_i \in X, \varepsilon_i = \pm 1,$$

where $x_1^{\varepsilon_1} \neq x_{i+1}^{-\varepsilon_{i+1}}$ for $1 \leq i \leq k-1$, i.e. every element ($\neq 1$) of it can be expressed uniquely in the form

$$x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}, \quad x_i \in X, \quad \varepsilon_i = \pm 1,$$

where $x_1^{\varepsilon_i} \neq x_{i+1}^{-\varepsilon_{i+1}}$ for $1 \leq i \leq k-1$.

i.e. every element ($\neq 1$) of it can be expressed uniquely in the form :

$$x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}, \quad x_i \in X \text{ where}$$

$$x_i \neq x_{i+1}, \quad 1 \leq i \leq m-1,$$

and the n_i 's are non-zero integers.

Let G be any group and X a subset of G such that G is isomorphic to the free group $F(X)$ on the set X . In such a case also we say that G is a free group. Then the set X is said to be a set of free-generators for G and sometimes G is said to be freely generated by the set X . The following are the differences between free generators for a group and ordinary generators for an arbitrary group.

An element of a free group is expressible in a unique manner as a product of powers of its free generators, but for an arbitrary group the expression for an element as a product of powers of its generators need not be unique. Because of this there is no relations among the elements of a free group, but for an arbitrary group there may exist some relations among its elements.

It is easily seen that if there is a one-one correspondence between two sets X and X' , i.e. if there is a one-one and onto mapping $X \rightarrow X'$, $x_i \leftrightarrow x'_i$, then the free groups $F(X)$ and $F(X')$ are isomorphic to each other.

Theorem 2.1.1.

Every group is isomorphic to a factor group of a free group (i.e. A group is always a homomorphic image of a free group.)

Proof : Let G be an arbitrary group with a set of generators S . Let X be a set i.e. it corresponds with S such that

$$x_i \leftrightarrow s_i, \quad x_i \in X, \quad s_i \in S.$$

Let $F(X)$ be the free group on the set X . Let us define a mapping

$\phi : F(X) \rightarrow G$ such that

$$x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k} \rightarrow s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}, \quad \varepsilon_i = \pm 1$$

Since every element of G is an image of some element of $F(X)$, hence the mapping ϕ is onto. Also it is a homomorphism :

$$\text{Let } \phi(x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}) = s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}, \quad \varepsilon_i = \pm 1$$

$$\text{and } \phi(y_1^{\eta_1} \dots y_l^{\eta_l}) = t_1^{\eta_1} \dots t_l^{\eta_l}, \quad \eta_i = \pm 1$$

and $t_i \in S$. Then

$$\begin{aligned} & \phi(x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k} y_1^{\eta_1} \dots y_l^{\eta_l}) \\ &= s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k} t_1^{\eta_1} \dots t_l^{\eta_l} \\ &= \phi(x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}) \phi(y_1^{\eta_1} \dots y_l^{\eta_l}) \end{aligned}$$

Therefore ϕ is an epimorphism from the free group $F(X)$ onto G . Then by the fundamental theorem of homomorphism it follows that

$G \cong F(X)/K$, where K is the kernel of ϕ i.e.

$K = \ker \phi$.

From the above theorem we have

$$F(X)/K \cong G, \quad K = \ker \phi.$$

Moreover $x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$ is a reduced word (element)

of K . So in G there corresponds a relation

$$s_1^{n_1} \dots s_k^{n_k} = 1 \quad (x_i \leftrightarrow s_i)$$

between the elements of S .

Suppose that the kernel K is generated by a subset N . A system of relations that corresponds to the words in N is called a system of defining relations of G . A group G is completely determined by its defining relations. Since the set N completely determines the normal subgroup K of the free group $F(X)$ and therefore $F(X)/K$.

Since every group is a factor group of a free group, every group can be given by a system of defining relations connecting the elements of a set of generators.

Theorem 2.1.2 : (Von Dyck's theorem)

If a group G is given by a system of defining relations,

~~and~~*

and if a group G' is given by these defining relations and some further relations in the same symbols then the group G' is a homomorphic image of the group G .

Proof : We know that the free groups on two equivalent sets (i.e. sets having a one-one correspondence between them) are isomorphic to each other, and that two isomorphic free groups may be considered as the same free group (with the underlying isomorphism between them). Since G and G' have equivalent sets of generators, the groups G and G' can be represented as factor groups of the same free group F (by theorem 2.1.1.). Then $G \cong F/K$, and $G' \cong F/K'$, where K and K' are the kernels of the corresponding epimorphisms from F to G and from F to G' . By the condition on the defining relations of G and G' we have $K \subseteq K'$.

Since K and K' are normal in F , K is normal in K' .
By the first isomorphism theorem

$$G' \cong F/K' \cong (F/K) / (K'/K) \cong G/N,$$

where $N = K'/K$.

Thus G' is a factor group of G . This implies that G' is a homomorphic image of G . Hence the proof.

2.2. Presentation of Groups :

A set of generators together with a system of defining

relations for a group is called a presentation of the group. A presentation that consists of a finite set of generators and a finite system of defining relations is called a finite presentation. Otherwise, a presentation is said to be infinite.

Thus a presentation for a finite group G is an ordered pair $\langle X, R \rangle$ where X is a set of generators for G and R is a set of defining relations for G .

Finding a presentation for a group is not an easy task nor does there exist a single method which is generally applicable to all group. Now-a-days the computer is also used in many cases for finding presentations. We explain below a mechanical method for finding presentations, which is suitable for computer programming. [Coxeter and Moser; 1965, pp 12-16]. Throughout this section E is used to denote the identity of a group and capital letters are used to denote elements of a group.

The principle of the method is as follows. Let us suppose that the relations

$$g_k(S_1, S_2, \dots, S_m) = E \quad (k = 1, 2, \dots, S) \quad (2.21)$$

are proposed as an abstract definition for a given group G of order g . In practice, these equations are obtained by taking a set of generators of G and observing some of the relations satisfied by them. It is natural to select relations

of a simple form, such as those which express the orders of generators or of simple combinations of them. The number of relations to select is a matter for experiment, and the "method of cosets" is the way to test the success of the experiment. If the group G' defined by (2.21), is not itself isomorphic to G , it possesses a normal subgroup G_1 such that the factor group G'/G_1 is isomorphic to G . In all cases the order of G' is at least g . If we can verify that the order of G' is at most g , it will follow that G' is isomorphic to G . To test whether this is or is not the case, we pick out a subset T_1, T_2, \dots, T_n of elements of G' such that the relations (2.21) imply the relations

$$h_1 (T_1, T_2, \dots, T_n) = E \quad (l = 1, 2, \dots, t) \quad (2.22)$$

which are already known to be an abstract definition for a group H of order $h \leq g$. Conceivably the relations (2.21) imply other relations between the T 's independent of (2.21), in which case the subgroup H of G' generated by the T 's will not be H' but some factor group H'/H_1 . In all cases the order of H is at most h . We now consider the sets of elements $H.R.$ obtained by multiplying the elements of H on the right by the various elements of G' . Two such sets either coincide or have no common member, and every element

of G' belongs to at least one such coset. There will be at least g/h different cosets (otherwise the order of G' would be less than $h \cdot g/h = g$). If we can show that there are in fact exactly g/h distinct cosets, then the order of G' will be at most $h \cdot g/h = g$ and it follows that G and G' are isomorphic.

Let us expand each g_k of (2.21) into a product of the generators and their inverses, eg., $(S_1^3 S_2^{-2})^2$ will be expressed as

$$S_1 S_1 S_1 S_2^{-1} S_2^{-1} S_1 S_1 S_1 S_2^{-1} S_2^{-1} .$$

Such an expression, involving c factors S_i^{+1} , serves as the heading for a table of cosets having $C + 1$ columns¹). Each factor occurs between two adjacent columns (as on page 35). We denote the cosets (in an order to be defined soon) by the numerals 1, 2, 3, ... If two such numerals, α and β , occur side by side in the pair of columns headed by S_i^{+1} , we understand that $\alpha \cdot S_i^{+1} = \beta$. Thus, if α is given, we can insert $\beta = \alpha \cdot S_i^{+1}$, but if β is given, we can insert $\alpha = \beta \cdot S_i^{+1}$. The first and last columns of each table are identical.

The coset 1 is defined as the subgroup H , and this information is put into every table. Thus, the information

that we have to begin with is

$$1. T_j = 1 \quad (j = 1, 2, \dots, n) .$$

Before proceeding we make sure that the number 1 appears in every table in every essentially different position. The coset 2 is defined as the set $1.R$ where R is a suitably chosen element of G' not belonging to H . This is done by inserting in one of the tables the number 2 in some (suitable) unoccupied place which is preceded or followed by the number 1. We now (and at all times) fill up as much as possible of all the tables before defining the next coset, in this case 3, and make sure that 2 appears in every essentially different place in every table before proceeding. When some new information is won, as happens when a row becomes complete, it is immediately put into the tables. When all the tables are completed, the process is at an end. If the number of cosets does not exceed g/h , our experiment has been successful : G and G' are not merely homomorphic but isomorphic.

Examples :

As an example of the enumeration method, consider the alternating group A_5 , of order 60, generated by the permutations

$$S = (2 \ 5 \ 4), \quad U = (1 \ 2 \ 3 \ 4 \ 5).$$

Since $SU = (1\ 2)(3\ 4)$, these generators satisfy the relations

$$S^3 = U^5 = (SU)^2 = E, \quad \dots \quad (2.23)$$

which we propose as an abstract definition for A_5 . In order to show that the group G' defined by (2.23) is of order 60, we take for H the subgroup of order 5 generated by U . The tables with $1.U = 1$ inserted are

S	S	S	U	U	U	U	U	S	U	S	U
1		1	1	1	1	1	1	1		1	1

Note that the symbol 1 (meaning H) appears in each table in every essentially different position. We define the coset $2 = 1.S$, and insert this into the tables to obtain

S	S	S	U	U	U	U	U	S	U	S	U
1	2		1	1	1	1	1	1	2	1	1
			2					2			2

Note that in the second and third tables we have placed a 2 in a new row so that the tables contain 2 in every essentially different position. Define $3 = 2.S$. The first table

yields $3.S = 1$; then the third table yields $2.U = 3$. The table become

S	S	S		U	U	U	U	U		S	U	S	U	
1	2	3	1	1	1	1	1	1	1	1	2	3	1	1
				2	3				2	2	3			2

Continuing in this manner, we define, in order,

$4 = 3.U, 5 = 4.S, 6 = 5.S, 7 = 4.U, 8 = 7.S,$

$9 = 8.S, 10 = 9.U, 11 = 10.S, 12 = 11.S.$

when the coset 12 has been defined the tables become

S	S	S		U	U	U	U	U		S	U	S	U	
1	2	3	4	1	1	1	1	1	1	1	2	3	1	1
4	5	6	4	2	3	4	7	5	2	2	3	4	5	2
7	8	9	7	6	9	10	11	8	6	6	4	7	8	6
10	11	12	10	12	12	12	12	12	12	9	7	5	6	9
										10	11	8	9	10
										12	10	11	12	12

The tables have "closed up" and hence the order of G' is at most 60, as desired.

and make sure that the four tables all have the same first column and all have the same last column. The tables for this group, with $\{E\}$ as the subgroup, are :

R	R	S	S	T	T	R	S	T				
1	2	5	3	5	1	4	5	1	2	4	5	
2	5	7	2	4	7	2	6	7	2	5	6	7
3	8	6	3	5	6	3	2	6	3	8	2	6
4	3	8	4	7	8	4	5	8	4	3	5	8
5	7	1	5	6	1	5	8	1	5	7	8	1
6	4	3	6	1	3	6	7	3	6	4	7	3
7	1	2	7	8	2	7	3	2	7	1	3	2
8	6	4	8	2	4	8	1	4	8	6	1	4

Hence the cosets have been defined as follows :

$$1.R = 2, 1.S = 3, 1.T = 4, 2.R = 5, 2.T = 6, 5.R = 7, 3.R = 8.$$

The table close up after the coset 8 has been entered, and hence the group defined by (2.23) is of order 8.

We close this chapter with a list of presentations for some familiar groups of small order (Coxeter and Moser; 1965) :

Table 1. : Some non-abelian groups of order less than 32.

Order	Description	Abstract definition
6	K-metacyclic	$S^3 = T^2 = (ST)^2 = E$
8	Dihedral	$S^4 = T^2 = (ST)^2 = E$
8	Quaternion	$S^2 = T^2 = (ST)^2$
10	ZS-metacyclic	$S^5 = T^2 = (ST)^2 = E$
12	Dihedral	$S^6 = T^2 = (ST)^2 = E$
12	Tetrahedral	$S^3 = T^2 = (ST)^3 = E$
12	ZS-metacyclic	$S^3 = T^2 = (ST)^2$
14	ZS-metacyclic	$S^7 = T^2 = (ST)^2 = E$
16	Dihedral	$S^8 = T^2 = (ST)^2 = E$
16	Dicyclic	$S^4 = T^2 = (ST)^2$
18	ZS-metacyclic	$S^9 = T^2 = (ST)^2 = E$
18	Z-metacyclic	$S^3 = T^6 = E, T^{-1}ST = S^{-1}$
20	Dihedral	$S^{10} = T^2 = (ST)^2 = E$
20	K-metacyclic	$S^5 = T^4 = E, T^{-1}ST = S^2$
20	ZS-metacyclic	$S^5 = T^2 = (ST)^2$
21	ZS-metacyclic	$T^3 = E, T^{-1}ST = S^2$
22	ZS-metacyclic	$S^{11} = T^2 = (ST)^2 = E$
24	Dihedral	$S^{12} = T^2 = (ST)^2 = E$
24	Octahedral	$S^4 = T^2 = (ST)^3 = E$
24	Binary tetrahedral	$R^3 = S^3 = (RS)^2$
24	ZS-metacyclic	$S^2 = T^2 = (ST)^3$

Contd... Table 1

Order	Description	Abstract Definition
24	Dicyclic	$S^6 = T^2 = (ST)^2$
26	ZS-metacyclic	$S^{13} = T^2 = (ST)^2 = E.$
28	Dihedral	$S^{14} = T^2 = (ST)^2 = E$
28	ZS-metacyclic	$S^7 = T^2 = (ST)^2$
30	ZS-metacyclic	$T^2 = E, TST = S^4$
30	ZS-metacyclic	$T^2 = E, TST = S^{-4}$
30	ZS-metacyclic	$S^{15} = T^2 = (ST)^2 = E.$

Table 2 : Alternating and Symmetric groups of degree less than 7.

Group	Abstract Definition	Generators
A_3	$S^3 = E$	$S = (1\ 2\ 3)$
S_3	$R^2 = S^3 = (RS)^2 = E$	$R = (1\ 2), S = (1\ 2\ 3)$
A_4	$R^2 = S^3 = (RS)^3 = E$	$R = (1\ 2)(3\ 4),$ $S = (2\ 3\ 4)$
S_4	$R^2 = S^3 = T^4 = RST = E$	$R = (3\ 4), S = (1\ 2\ 3)$ $T = (4\ 3\ 2\ 1)$
A_5	$R^2 = S^3 = (RS)^5 = E$	$R = (1\ 2)(4\ 5),$ $S = (1\ 3\ 4)$
S_5	$R^5 = S^4 = (RS)^2 = (R^2S^2)^3 = E$	$R = (5\ 4\ 3\ 2\ 1)$ $S = (1\ 2\ 3\ 4)$
A_6	$A^3 = B^4 = (AB)^5 = (A^{-1}B^{-1}AB)^2 = E$	$A = (1\ 3\ 5)(2\ 4\ 6)$ $B = (1\ 4)(2\ 6\ 3\ 5)$
S_6	$A^2 = B^6 = (AB^{-1}AB)^3$ $= (AB^{-1}AB^2)^4 = (AB)^5$ $= (AB^{-2}AB^2)^2 = E$	$A = (1\ 2),$ $B = (1\ 2\ 3\ 4\ 5\ 6)$

Table 3 : The groups $PSL(2,p)$ for $2 \leq p \leq 30$

p	Order $p(p^2-1)/2$	Generators (mod p)	Abstract definition
3	12	$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$S^3 = T^2 = (ST)^3 = E$
5	60	$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$S^5 = T^2 = (ST)^3 = E$
7	168	$R = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, S = \begin{pmatrix} 2 & 0 \\ 1 & -3 \end{pmatrix}$	$R^3 = S^3 = (RS)^4$ $= (R^{-1}S)^4 = E$
11	660	$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$S^{11} = T^2 = (ST)^3$ $= (S^4TS^6T)^2 = E$
13	1092	$S = \begin{pmatrix} 5 & 4 \\ -6 & -2 \end{pmatrix}, T = \begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix}$	$S^7 = T^2 = (ST)^6$ $= (S^2T)^3 = E$
17	2448	$S = \begin{pmatrix} 5 & 8 \\ 5 & -2 \end{pmatrix}, T = \begin{pmatrix} -4 & 0 \\ -9 & 4 \end{pmatrix}$	$S^9 = T^2 = (ST)^4$ $= (S^2T)^3 = E$
19	3420	$S = \begin{pmatrix} 4 & 0 \\ 0 & 5 \end{pmatrix}, T = \begin{pmatrix} 4 & 4 \\ -9 & -4 \end{pmatrix}$	$S^9 = T^2 = (ST)^5$ $= (S^{-1}TST)^2 = E$
23	6072	$S = \begin{pmatrix} 3 & 0 \\ 0 & 8 \end{pmatrix}, T = \begin{pmatrix} 9 & 9 \\ -4 & -9 \end{pmatrix}$	$S^{11} = T^2 = (ST)^3$ $= (S^{-1}TST)^4 = E$
29	12180	$P = \begin{pmatrix} -7 & 12 \\ 11 & 10 \end{pmatrix}$ $Q = \begin{pmatrix} 4 & -8 \\ 9 & 4 \end{pmatrix}$	$P^7 = (P^2Q)^3 = (P^3Q)^2$ $= (PQ^8)^2 = E$

CHAPTER 3

THE QUATERNION GROUP AND ITS PRESENTATION

This chapter is of a preparatory nature to obtain the results of the final chapter, being devoted mainly to definitions and basic properties of the quaternion groups, including derivation of a presentation for such a group.

In §3.1 we define a generalized quaternion group and find a presentation for it. This is followed by §3.2 in which we give some basic properties of the quaternion groups. In §3.3 we give a permutational representation of the generalized quaternion group which will help us in determining the conjugacy classes of the quaternion group in chapter 4.

3.1. The Quaternion group

In 1896, Adolf Hurwitz published a highly interesting paper "Über die Zahlentheorie der quaternionen" (Nachrichten der Gesellschaft der Wissensch, Göttingen 1896, p 313-340), in which he developed a factorization theory of "integer quaternions" and applied it to the problem of representing integers as sums of four squares. In 1919 Hurwitz elaborated his ideas with full

proofs in a very nice booklet entitled "vorlesungen über die Zahlentheorie der quaternionen" [Waerden B.L.vander; 1985].

In 1621, in his edition of the Arithmetica of Diophantos, C.G.Bachet noted that apparently every integer is either a square or a sum of 2 or 3 or 4 squares. Later authors called this assertion "Bachet's theorem". Bachet verified it for all integers up to 325. If zero terms are allowed, we may say that every integer N is a sum of four square :

$$N = s^2 + x^2 + y^2 + z^2$$

The first proof of this assertion was given by Joseph - Louis Lagrange in 1772 (Oeuvres 3, p. 189-201). One year later, Leonard Euler presented a simpler proof (Opera omnia, pars prima, Vol. 3 p. 218-239).

A purely algebraic proof was given by Hurwitz by means of his number theory of integer quaternions. Hurwitz defines :

A quaternion

$$q = s + ix + jy + kz$$

with rational coefficients s, x, y, z is called integer, if the coefficients are either all integers or all of the form

$\frac{n+1}{2}$. The four units $1, i, j, k$ satisfy $i^2 = j^2 = -1,$

$ij = -ji = k$. In other words : integer quaternions are the

linear combinations of $\rho = \frac{1}{2} (1 + i + j + k)$, i, j, k .

Quaternions with complex coefficients are called by Hamilton biquaternions. [W.R. Hamilton : Lectures on quaternions (1853), art. 669]. The algebra of these biquaternions is isomorphic to a full matrix ring over the complex number field, for quaternions $a + ib + jc + kd$ with complex coefficients a, b, c, d can be represented by matrices

$$\begin{pmatrix} a + bi & -c + di \\ c + di & a - bi \end{pmatrix}$$

We can define a quaternion group as a subgroup of the group $GL(2, \mathbb{C})$ generated by all 2×2 matrices over the complex field. For this let us give a brief description of the $GL(2, \mathbb{C})$.

The set of all $n \times n$ matrices with real numbers as entries forms a group under matrix multiplication. Each matrix A in this group determines an invertible linear transformation

$$f_A : \mathbb{R}^n \rightarrow \mathbb{R}^n \quad \text{defined by}$$

$$f_A(x) = x_A^t \quad \text{for all vectors}$$

$x = (x_1, \dots, x_n) \in \mathbb{R}^n$, where t stands for transpose.

Since

$$f_{AB}(x) = x (AB)^t = xB^t A^t = f_A (f_B(x))$$

we see that the product matrix AB determines the composite linear transformation $f_A f_B$. Conversely, if

$f : R^n \rightarrow R^n$ is an invertible linear transformation, and if A is the matrix which represents it with respect to the standard basis in both copies R^n , then A is invertible and $f = f_A$. For these reasons the group is called the general linear group, GL_n . If we wish to emphasise that the entries all have real entries, then we write $GL_n(R)$. Changing R to C gives the corresponding group $GL_n(C)$ of $n \times n$ invertible complex matrices.

Matrix multiplication is not commutative for $n \geq 2$, so we have a family of infinite non-abelian groups

$$GL_2(C), GL_3(C), \dots$$

Definition : A quaternion group is a subgroup Q of $GL_2(C)$ generated by the matrices :

$$\xi = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \eta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

where $i^2 = -1$ [Johnson]. Now we have $|\xi| = 4$ and $\eta \notin \langle \xi \rangle$, so that $|Q| \geq 8$. Furthermore, we have $\eta^2 = \xi^2$ and $\eta^{-1} \xi \eta = \xi^{-1}$, so we hopefully put

$$G = \langle a, b \mid a^4 = e, a^2 = b^2 = (ab)^2, b^{-1}ab = a^{-1} \rangle \quad (1)$$

and use the substitution test to obtain the epimorphism :

$$\begin{aligned} \theta : G &\rightarrow Q \\ a &\rightarrow \xi \\ b &\rightarrow \eta \end{aligned}$$

To show that θ is an isomorphism, we merely have to prove that $|G| \leq 8$.

To do this, it will be sufficient to show that any element of G is equal to a member of the set

$$u = \{a^i b^j \mid 0 \leq i \leq 3, 0 \leq j \leq 1\}$$

It follows from the relations in (1) that u is closed under post multiplication by $a^{\pm 1}$ and $b^{\pm 1}$.

For example,

$$(a^i b) a = a^i b^2 b^{-1} a b b^{-1} = a^i a^2 a^{-1} b^{-1} = a^{i-1} b.$$

Thus $uw \subseteq u$ for any word w in $\{a^{\pm 1}, b^{\pm 1}\}$.

Since these words cover G (by San) and $e \in u$, we have

$$G = eG \subseteq uG \subseteq u, \text{ as required.}$$

The group generated by (1) satisfies all the requirements for our proposed group of order 8 (above) and we have just shown it is isomorphic to the concrete Q - called the quaternions.

For n an integer ≥ 2 , we define the generalized quaternion group Q_n to be the subgroup of $GL(2, \mathbb{C})$ generated by the matrices

$$\xi = \begin{pmatrix} w & 0 \\ 0 & \bar{w} \end{pmatrix}, \quad \eta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

where $w = e^{i\pi/n} \in \mathbb{C}$.

Theorem 3.1.1 [Johnson]

The generalized quaternion group Q_n is of order $4n$ has the presentation :

$$\langle a, b \mid a^{2n} = e, a^n = b^2 = (ab)^2, b^{-1}ab = a^{-1} \rangle \quad (2)$$

Proof : Letting G be the group presented by (2), we see that

$a^n = b^2$ commutes with b , and so

$$a^n = (a^n)^b = (a^b)^n = a^{-n}, \text{ that is}$$

$$a^{2n} = e \text{ in } G.$$

Thus the quaternion group Q is just Q_4 . We proceed as the above example, and observe that mapping a, b to ξ, η respectively yields a homomorphism from G to Q_n . That $|Q_n| \geq 4n$ follows from the fact that a is a primitive $2n^{\text{th}}$ root of

unity and $\eta \notin \langle \xi \rangle$.

Finally the proof that $|G| \leq 4n$ differs from the above only in the choice of

$$u = \{a^i b^j \mid 0 \leq i \leq 2n-1, 0 \leq j \leq 1\}$$

3.2. Properties of Quaternion group and generalized quaternion group :

In this section we shall give some interesting properties and results of the family of quaternion groups .

We have defined quaternion group as group of order 8 with generators a and b which has the following defining relations

$$a^4 = 1(e), \quad a^2 = b^2 = (ab)^2, \quad b^{-1}ab = a^{-1}$$

Its eight elements are

$$1, a, a^2, a^3 \\ b, ab, a^2b, a^3b$$

If instead we write

$$1, i, -1, -i \\ j, k, -j, -k$$

and set $-(-1) = 1$, $-(-i) = i$, $-(-j) = j$, $-(-k) = k$ then we have the following calculation rules :

$$1.x = x.1 = x, \quad -1.x = x.(-1) = -x, \quad (-1)^2 = 1,$$

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i,$$

$$ki = -ik = j$$

Theorem 3.2.1. The Quaternion group has exactly 24 automorphism [Zassenhaus].

Proof : If A' is of order 4 and B' is of order 4 and if A' , B' generate the whole quaternion group then

$$A'^2 = B'^2 = (A'B')^2 = A^2$$

Therefore all the calculational rules which are valid for power products of A and B also remain valid for the corresponding power product of A' and B' .

Since A' , B' generate the whole group, $\langle A' \rangle$ is a normal subgroup of index 2 and every element can be written uniquely in the form :

$$A'^{\nu} B'^{\mu} \quad (0 \leq \nu < 4, \quad 0 \leq \mu < 2)$$

Therefore the mapping

$$A^{\nu} B^{\mu} \rightarrow A'^{\nu} B'^{\mu}$$

is an automorphism of the group. The number of all automorphisms is equal to the number of pairs A', B' . It follows by simple enumeration that the quaternion group has exactly 24 automorphisms.

The automorphism group of the quaternion group is isomorphic to S_4 , the symmetric group on four letters. Next we shall give below some of the findings regarding the general quaternion groups Q_n and also try to prove some of them.

i) The order of Q_n is $4n$.

ii) The only commutative group is Q_1 i.e. Q_n , $n \geq 2$

is non-commutative.

iii) The centre of any quaternion group has order 2.

It contains the elements e and $a^n = b^2$.

iv) The order of an element of the form $a^i b$, $0 < i \leq 2n$ is 4.

v) Q_n contains D_n , the dihedral group as its subgroup.

vi) The commutator subgroup of Q_n is a cyclic group generated by a^2 and is of order n and hence a quaternion group has a derived series of length 2 i.e.

$$Q_n \trianglelefteq Q'_n \trianglelefteq Q''_n = \{e\}.$$

So a quaternion group is a metabelian group. The proof of (iv), (v) and (vi) are given below :

Proof :

$$(iv) \text{ Let } |a^i b| = m, 1 \leq i \leq 2n$$

$$\text{Therefore } (a^i b)^m = 1$$

$$\begin{aligned} \text{Now } (a^i b)^2 &= (a^i b)(a^i b) \\ &= a^i b^2 (b^{-1} a^i b) \\ &= a^i a^n a^{-i} (\dots b^2 = a^n, b^{-1} a b = a^{-1}) \\ &= a^n \end{aligned}$$

$$\begin{aligned} (a^i b)^3 &= (a^i b)(a^i b)(a^i b) \\ &= a^n a^i b \\ &= a^{n+i} b \end{aligned}$$

$$\begin{aligned} (a^i b)^4 &= (a^i b)(a^i b)(a^i b)(a^i b) \\ &= a^n \cdot a^n \\ &= a^{2n} = 1 \end{aligned}$$

$$\begin{aligned}
 \text{Therefore } (a^i b)^m &= \underbrace{(a^i b)(a^i b) \dots (a^i b)(a^i b)}_{m \text{ - times}} \\
 &= \{(a^i b)(a^i b)\} \dots \{(a^i b)(a^i b)\} \\
 &= \underbrace{a^n \dots a^n}_{m/2 \text{ - times}}, \text{ if } m \text{ is even} \\
 &= (a^n)^{m/2}, \text{ if } m \text{ is even} \\
 &= a^{nm/2}, \text{ if } m \text{ is even}
 \end{aligned}$$

ie., $(a^i b)^m = a^{mn/2}, \text{ if } m \text{ is even}$

Similarly $(a^i b)^m = a^{\frac{m-1}{2} n+i} b, \text{ if } m \text{ is odd.}$

Therefore

$$(a^i b)^m = 1 \text{ implies}$$

either $a^{\frac{nm}{2}} = 1$ if m is even

or $a^{\frac{m-1}{2} n+i} b = 1$ if m is odd.

In the second case i.e. when m is odd, we have

$$b = a^{-i - \frac{m-1}{2} n}$$

which is not true as Q_n is non-cyclic. So m can not be odd.

Therefore we must have m even

and $a^{\frac{nm}{2}} = 1$

i.e. $\frac{nm}{2} \equiv 0 \pmod{2n}$

or $\frac{nm}{2} = 2ns \quad s \geq 1$

or $m = 4s$

Since the least value is taken as the order, so $m = 4$ is the order of an element of the form $a^i b$, $0 < i \leq 2n$

(v) We know that there exists a homomorphism (natural homomorphism) :

$$\phi : Q_n \rightarrow Q_n / Z(Q_n) \quad [= Q_n / Z]$$

where $Z(Q_n)$ is the centre of Q_n .

Let us define this homomorphism by

$$a \rightarrow aZ = x \quad (\text{say})$$

$$b \rightarrow bZ = y \quad (\text{say})$$

$$\text{Now } \phi(a^n) = a^n Z = Z \quad (\text{since } a^n \in Z)$$

$$\text{Therefore, } x^n = e.$$

53(d)

$$\phi(b^2) = (bZ)^2 = b^2Z = Z \quad (\text{Since } a^n = b^2 \in Z)$$

Therefore $y^2 = e$

$$\phi(ab)^2 = (ab)^2Z = Z \quad (\text{Since } (ab)^2 = a^n \in Z)$$

Therefore $(xy)^2 = e.$

By Von Dyck's theorem (theorem 2.1.2) Q_n/Z is generated by x, y such that

$$x^n = y^2 = (xy)^2 = 1, \quad yx = x^{-1}y$$

$$|Q_n/Z| = 2n$$

Now the dihedral group D_n has the same presentation as that of Q_n/Z and the order of D_n is also $2n$. So there exists an isomorphism from

$$Q_n/Z \rightarrow D_n \text{ as such}$$

$$Q_n/Z \cong D_n .$$

Hence the quaternion group Q_n contains D_n as its subgroup.

(vi) Any commutator of Q_n is of the form $[a^i b, a^j b]$

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

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

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

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

$$= b^{-1} a^{2j-2i} b$$

$$= a^{2i-2j}$$

$$= a^{2(i-j)}$$

$$= \text{even powers of } a \text{ for all } i \text{ and } j, j < i$$

which shows that the commutator subgroup of Q_n is generated by a^2 .

3.3. Permutational representation of the quaternion group.

In this section we shall give a presentation of the quaternion group as a subgroup of S_{4n} . Though it can be represented by permutation group of lesser degree, but for our computational convenience we give the following presentation.

Let Q_n be a quaternion group of order $4n$, having a presentation

$$a^{2n} = e, a^n = b^2 = (ab)^2, b^{-1} ab = a^{-1}$$

where a and b are two permutations. Let $G = \langle x, y \rangle$ be a

group with generators

$$x = (1 \ 2 \ 3 \ \dots \ 2n) (2n+1 \ 2n+2 \ \dots \ 4n)$$

$$y = (1 \ 4n-1 \ n+1 \ 3n-1) (2 \ 4n-2 \ n+2 \ 3n-2)$$

$$\dots\dots (n \ 3n \ 2n \ 4n) .$$

Now we claim that the group G contains the following distinct elements :

$$x^{2n} = e, \ x, \ x^2, \ \dots \ x^{2n-2}, \ x^{2n-1},$$

$$y = x^{2n}y, \ xy, \ x^2y, \ \dots \ x^{2n-2}y, \ x^{2n-1}y.$$

we shall show that the above elements are distinct.

It is obvious that the elements of the type

$x^i, 1 \leq i \leq 2n$ are $2n$ distinct elements of G and the elements of the type $x^jy, 0 \leq j < 2n$ are also distinct.

We are left to show that any element of the type

$x^i, 0 \leq i < 2n$ is not equal to any element of the type $x^jy, 0 \leq j < 2n$.

If possible let,

$$x^i = x^jy, \ 0 \leq i < 2n, \ 0 \leq j < 2n, \ i \neq j$$

i.e. $x^{i-j} = y$

which is impossible as the group is non cyclic. So all the $4n$ elements listed above are the $4n$ distinct elements of G .

Now we shall show that the group G is isomorphic to the Quaternion group Q_n of order $4n$.

Let us define a mapping

$$\phi : Q_n \rightarrow G$$

such that $\phi(a) = x$ and $\phi(b) = y$

Since G and Q_n have equivalent set of generators, therefore Q_n is a homomorphic image of G [using Von Dyck's theorem (theorem 2.1.2)] that is ϕ is an epimorphism. Also ϕ is one-to one, because the order of G is equal to the order of Q_n . Hence ϕ is an isomorphism.

CHAPTER 4

NUMBER OF CONJUGACY CLASSES AND MEASURE OF QUATERNION GROUP

In Chapter 1 we defined the Joseph measure of commutativity for a finite group and also gave a theorem for determining the Joseph measure for a finite group with the help of conjugacy classes of the group. In Chapter 3 we defined a quaternion group and gave a permutational representation of the group. As we know that [M.A.Armstrong; 1987] the conjugate permutations have the same cycle structure, so a permutational representation of the group will help us in determining the conjugacy classes of the group.

In this chapter we are going to list the conjugacy classes of Q_n for some small values of n . This result definitely helps us to guess the conjugacy classes of Q_n for a fixed n and depending on that 'guess' we shall generalise a result about the number of conjugacy classes of Q_n for every $n \in \mathbb{N}$. We shall finish this chapter by determining the measure of the quaternion group Q_n .

4.1. Listing of conjugacy classes :

In this section we list the conjugacy classes of Q_n

for some small values of n .

i) when $n = 2$

Element no. 1) $(1)(2)(3)(4)(5)(6)(7)(8) = a^4 = e$

Element no. 2) $(1\ 7\ 3\ 5)(2\ 6\ 4\ 8) = a^4b = b$

Element no. 3) $(1\ 2\ 3\ 4)(5\ 6\ 7\ 8) = a$

Element no. 4) $(1\ 3)(2\ 4)(5\ 7)(6\ 8) = a^2$

Element no. 5) $(1\ 4\ 3\ 2)(5\ 8\ 7\ 6) = a^3$

Element no. 6) $(1\ 6\ 3\ 8)(2\ 5\ 4\ 7) = ab$

Element no. 7) $(1\ 5\ 3\ 7)(2\ 8\ 4\ 6) = a^2b$

Element no. 8) $(1\ 8\ 3\ 6)(2\ 7\ 4\ 5) = a^3b$

The conjugacy classes :

Class no. 1)	1	} Conjugacy classes for power of $b = 0$
Class no. 2)	3,5	
Class no. 3)	4	
Class no. 4)	6,8	} Conjugacy classes for power of $b = 1$
Class no. 5)	2,7	

ii) when n = 3

Element no. 1)	$(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12) = a^6 = e$
Element no. 2)	$(1\ 11\ 4\ 8)(2\ 10\ 5\ 7)(3\ 9\ 6\ 12) = a^6 b = b$
Element no. 3)	$(1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9\ 10\ 11\ 12) = a$
Element no. 4)	$(1\ 3\ 5)(2\ 4\ 6)(7\ 9\ 11)(8\ 10\ 12) = a^2$
Element no. 5)	$(1\ 4)(2\ 5)(3\ 6)(7\ 10)(8\ 11)(9\ 12) = a^3$
Element no. 6)	$(1\ 5\ 3)(2\ 6\ 4)(7\ 11\ 9)(8\ 12\ 10) = a^4$
Element no. 7)	$(1\ 6\ 5\ 4\ 3\ 2)(7\ 12\ 11\ 10\ 9\ 8) = a^5$
Element no. 8)	$(1\ 10\ 4\ 7)(2\ 9\ 5\ 12)(3\ 8\ 6\ 11) = ab$
Element no. 9)	$(1\ 9\ 4\ 12)(2\ 8\ 5\ 11)(3\ 7\ 6\ 10) = a^2 b$
Element no. 10)	$(1\ 8\ 4\ 11)(2\ 7\ 5\ 10)(3\ 12\ 6\ 9) = a^3 b$
Element no. 11)	$(1\ 7\ 4\ 10)(2\ 12\ 5\ 9)(3\ 11\ 6\ 8) = a^4 b$
Element no. 12)	$(1\ 12\ 4\ 9)(2\ 11\ 5\ 8)(3\ 10\ 6\ 7) = a^5 b$

Conjugacy classes :

Class no. 1)	1	} Conjugacy classes for power of b = 0
Class no. 2)	3, 7	
Class no. 3)	4, 6	
Class no. 4)	5	
Class no. 5)	8, 12, 10	} Conjugacy classes for power of b = 1
Class no. 6)	2, 11, 9	

iii) when $n = 4$

- Element no. 1) (1) (2) (3) (4) (5) (6) (7) (8) (9) (10)
(11) (12) (13) (14) (15) (16) = $a^8 = e$
- Element no. 2) (1 15 5 11) (2 14 6 10) (3 13 7 9)
(4 12 8 16) = $a^8 b = b$.
- Element no. 3) (1 2 3 4 5 6 7 8) (9 10 11 12 13 14 15 16) = a
- Element no. 4) (1 3 5 7)(2 4 6 8)(9 11 13 15) (10 12 14 16)
= a^2
- Element no. 5) (1 4 7 2 5 8 3 6)(9 12 15 10 13 16 11 14)
= a^3
- Element no. 6) (1 5)(3 7)(2 6)(4 8)(9 13)(11 15)(10 14)
(12 16) = a^4
- Element no. 7) (1 6 3 8 5 2 7)(9 14 11 16 13 10 15 12) = a^5
- Element no. 8) (1 7 5 3)(2 8 6 4)(9 15 13 11)(10 16 14 12) = a^6
- Element no. 9) (1 8 7 6 5 4 3 2)(9 16 15 14 13 12 11 10) = a^7
- Element no. 10) (1 14 5 10)(2 13 6 9)(3 12 7 16)(4 11 8 15) = ab
- Element no. 11) (1 13 5 9)(2 12 6 16)(3 11 7 15)(4 10 8 14) = $a^2 b$
- Element no. 12) (1 12 5 16)(2 11 6 15)(3 10 7 14)(4 9 8 13) = $a^3 b$

Element no. 13) $(1\ 11\ 5\ 15)(2\ 10\ 6\ 14)(3\ 9\ 7\ 13)(4\ 16\ 8\ 12) = a^4 b$

Element no. 14) $(1\ 10\ 5\ 14)(2\ 9\ 6\ 13)(3\ 16\ 7\ 12)(4\ 15\ 8\ 11) = a^5 b$

Element no. 15) $(1\ 9\ 5\ 13)(2\ 16\ 6\ 12)(3\ 15\ 7\ 11)(4\ 14\ 8\ 10) = a^6 b$

Element no. 16) $(1\ 16\ 5\ 12)(2\ 15\ 6\ 11)(3\ 14\ 7\ 10)(4\ 13\ 8\ 9) = a^7 b$

Conjugacy classes :

Class no. 1)	1	}	Conjugacy classes for power of $b = 0$
Class no. 2)	3, 9		
Class no. 3)	4, 8		
Class no. 4)	5, 7		
Class no. 5)	6		
Class no. 6)	10, 16, 14, 12	}	Conjugacy classes for power of $b = 1$
Class no. 7)	2, 11, 13, 15		

iv) when $n = 5$

Element no. 1) $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)$
 $(11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20)$
 $= a^{10} = e$

Element no. 2) $(1\ 15\ 6\ 20)(2\ 14\ 7\ 19)(3\ 13\ 8\ 18)(4\ 12\ 9\ 17)$
 $(5\ 11\ 10\ 16) = a^{10} b = b$

- Element no. 3) (1 2 3 4 5 6 7 8 9 10)(11 12 13 14 15 16
17 18 19 20) = a
- Element no. 4) (1 3 5 7 9)(2 4 6 8 10)(11 13 15 17 19)
(12 14 16 18 20) = a²
- Element no. 5) (1 4 7 10 3 6 9 2 5 8)(11 14 17 20 13 16
19 12 15 18) = a³
- Element no. 6) (1 5 9 3 7)(2 6 10 4 8)(11 15 19 13 17)
(12 16 20 14 18) = a⁴
- Element no. 7) (1 6)(2 7)(3 8)(4 9)(5 10)(11 16)(12 17)
(13 18)(14 19)(15 20) = a⁵
- Element no. 8) (1 7 3 9 5)(4 10 6 2 8)(11 17 13 19 15)(
(14 20 16 12 18) = a⁶
- Element no. 9) (1 8 5 2 9 6 3 10 7 4)(11 18 15 12 19
16 13 20 17 14) = a⁷
- Element no. 10) (1 9 7 5 3)(2 10 8 6 4)(11 19 17 15 13)
12 20 18 16 14) = a⁸
- Element no. 11) (1 10 9 8 7 6 5 4 3 2)(11 20 19 18 17
16 15 14 13 12) = a⁹
- Element no. 12) (1 14 6 19)(2 13 7 18)(3 12 8 17)
(4 11 9 16)(5 20 10 15) = ab

$$\text{Element no. 13)} \quad (1 \ 13 \ 6 \ 18)(2 \ 12 \ 7 \ 17)(3 \ 11 \ 8 \ 16) \\ (4 \ 20 \ 9 \ 15)(5 \ 19 \ 10 \ 14) = a^2 b$$

$$\text{Element no. 14)} \quad (1 \ 12 \ 6 \ 17)(2 \ 11 \ 7 \ 16)(3 \ 20 \ 8 \ 15) \\ (4 \ 19 \ 9 \ 14)(5 \ 18 \ 10 \ 13) = a^3 b$$

$$\text{Element no. 15)} \quad (1 \ 11 \ 6 \ 16)(2 \ 20 \ 7 \ 15)(3 \ 19 \ 8 \ 14) \\ (4 \ 18 \ 9 \ 13)(5 \ 17 \ 10 \ 12) = a^4 b$$

$$\text{Element no. 16)} \quad (1 \ 20 \ 6 \ 15)(2 \ 19 \ 7 \ 14)(3 \ 18 \ 8 \ 13) \\ (4 \ 17 \ 9 \ 12)(5 \ 16 \ 10 \ 11) = a^5 b$$

$$\text{Element no. 17)} \quad (1 \ 19 \ 6 \ 14)(2 \ 18 \ 7 \ 13)(3 \ 17 \ 8 \ 12) \\ (4 \ 16 \ 9 \ 11)(5 \ 15 \ 10 \ 20) = a^6 b$$

$$\text{Element no. 18)} \quad (1 \ 18 \ 6 \ 13)(2 \ 17 \ 7 \ 12)(3 \ 16 \ 8 \ 11) \\ (4 \ 15 \ 9 \ 20)(5 \ 14 \ 10 \ 19) = a^7 b$$

$$\text{Element no. 19)} \quad (1 \ 17 \ 6 \ 12)(2 \ 16 \ 7 \ 11)(3 \ 15 \ 8 \ 20) \\ (4 \ 14 \ 9 \ 19)(5 \ 13 \ 10 \ 18) = a^8 b$$

$$\text{Element no. 20)} \quad (1 \ 16 \ 6 \ 11)(2 \ 15 \ 7 \ 20)(3 \ 14 \ 8 \ 19) \\ (4 \ 13 \ 9 \ 18)(5 \ 12 \ 10 \ 17) = a^9 b$$

Conjugacy classes:

Class no. 1) 1

Class no. 2) 3, 11

Class no. 3) 4, 10

Class no. 4) 5, 9

Class no. 5) 6, 8

Class no. 6) 7

} Conjugacy classes
for power of $b = 0$

Class no. 7) 12, 20, 18, 16, 14	} Conjugacy classes for
Class no. 8) 2, 19, 17, 15, 13	

v) when $n = 6$:

Element no. 1) (1) (2) (3) (4) (5) (6) (7) (8) (9) (10)
 (11) (12) (13) (14) (15) (16) (17) (18)
 (19) (20) (21) (22) (23) (24) = $a^{12} = e$.

Element no. 2) (1 23 7 17)(2 22 8 16)(3 21 9 15)
 (4 20 10 14)(5 19 11 13)(6 18 12 24) = $a^{12}b$

Element no. 3) (1 2 3 4 5 6 7 8 9 10 11 12)
 (13 14 15 16 17 18 19 20 21 22 23 24) = a

Element no. 4) (1 3 5 7 9 11)(2 4 6 8 10 12)
 (13 15 17 19 21 23)(14 16 18 20 22 24) = a^2

Element no. 5) (1 4 7 10)(2 5 8 11)(3 6 9 12)(13 16 19 22)
 (14 17 20 23)(15 18 21 24) = a^3

Element no. 6) (1 5 9)(2 6 10)(3 7 11)(4 8 12)(13 17 21)
 (14 18 22)(15 19 23)(16 20 24) = a^4

Element no. 7) (1 6 11 4 9 2 7 12 5 10 3 8)
 (13 18 23 16 21 14 19 24 17 22 15 20) = a^5

Element no. 8) (1 7)(4 10)(2 8)(5 11)(3 9)(6 12)(13 19)
 (16 22)(14 20)(17 23)(15 21)(18 24) = a^6

- Element no. 9) (1 8 3 10 5 12 7 2 9 4 11 6)
(13 20 15 22 17 24 19 14 21 16 23 18) = a^7
- Element no. 10) (1 9 5)(2 10 6)(3 11 7)(4 12 8)(13 21 17)
(14 22 18)(15 23 19)(16 24 20) = a^8
- Element no. 11) (1 10 7 4)(2 11 8 5)(3 12 9 6)(13 22 19 16)
(14 23 20 17)(15 24 21 18) = a^9
- Element no. 12) (1 11 9 7 5 3)(2 12 10 8 6 4)(13 23 21 19
17 15)(14 24 22 20 18 16) = a^{10}
- Element no. 13) (1 12 11 10 9 8 7 6 5 4 3 2)
(13 24 23 22 21 20 19 18 17 16 15 14) = a^{11}
- Element no. 14) (1 22 7 16)(2 21 8 15)(3 20 9 14)
(4 19 10 13)(5 18 11 24)(6 17 12 23) = ab
- Element no. 15) (1 21 7 15)(2 20 8 14)(3 19 9 13)
(4 18 10 24)(5 17 11 23)(6 16 12 22) = a^2b
- Element no. 16) (1 20 7 14)(2 19 8 13)(3 18 9 24)
(4 17 10 23)(5 16 11 22)(6 15 12 21) = a^3b
- Element no. 17) (1 19 7 13)(2 18 8 24)(3 17 9 23)
(4 16 10 22)(5 15 11 21)(6 14 12 20) = a^4b
- Element no. 18) (1 18 7 24)(2 17 8 23)(3 16 9 22)
(4 15 10 21)(5 14 11 20)(6 13 12 19) = a^5b

- Element no. 19) $(1\ 17\ 7\ 23)(2\ 16\ 8\ 22)(3\ 15\ 9\ 21)$
 $(4\ 14\ 10\ 20)(5\ 13\ 11\ 19)(6\ 12\ 18) = a^6_b$
- Element no. 20) $(1\ 16\ 7\ 22)(2\ 15\ 8\ 21)(3\ 14\ 9\ 20)$
 $(4\ 13\ 10\ 19)(5\ 24\ 11\ 18)(6\ 23\ 12\ 17) = a^7_b$
- Element no. 21) $(1\ 15\ 7\ 21)(2\ 14\ 8\ 20)(3\ 13\ 9\ 19)(4\ 24\ 10\ 18)$
 $(5\ 23\ 11\ 17)(6\ 22\ 12\ 16) = a^8_b$
- Element no. 22) $(1\ 14\ 7\ 20)(2\ 13\ 8\ 19)(3\ 24\ 9\ 18)$
 $(4\ 23\ 10\ 17)(5\ 22\ 11\ 16)(6\ 21\ 12\ 15) = a^9_b$
- Element no. 23) $(1\ 13\ 7\ 19)(2\ 24\ 8\ 18)(3\ 23\ 9\ 17)$
 $(4\ 22\ 10\ 16)(5\ 21\ 11\ 15)(6\ 20\ 12\ 14) = a^{10}_b$
- Element no. 24) $(1\ 24\ 7\ 18)(2\ 23\ 8\ 17)(3\ 22\ 9\ 16)$
 $(4\ 21\ 10\ 15)(5\ 20\ 11\ 14)(6\ 19\ 12\ 13) = a^{11}_b$

The conjugacy classes:

Class no. 1)	1	} Conjugacy classes for power of $b = 0$
Class no. 2)	3, 13	
Class no. 3)	4, 12	
Class no. 4)	5, 11	
Class no. 5)	6, 10	
Class no. 6)	7, 9	
Class no. 7)	8	
Class no. 8)	14, 24, 22, 20, 18 16	} Conjugacy classes for power of $b = 1$
Class no. 9)	2, 23, 21, 19, 17, 15	

4.2. Determination of $J(Q_n)$:

From the above patterns [In§4.1] of the conjugacy classes we can "guess" the conjugacy classes of the generalized quaternion group Q_n of order $4n$.

Let us recall that the quaternion group Q_n has the permutational representation $\langle a, b : a^{2n} = e, a^n = b^2 = (ab)^2, b^{-1}ab = a^{-1} \rangle$

where $a = (1\ 2\ 3\ \dots\ 2n)\ (2n+1\ 2n+2\ \dots\ n+2\ 3n-2)$
 $\dots\ (n\ 3n\ 2n\ 4n)$

and the distinct elements of the group Q_n are the following:

$a^{2n} = e, a, a^2, a^3, \dots, a^{2n-2}, a^{2n-1}; a^{2n} b = b,$
 $ab, a^2b, a^3b, \dots, a^{2n-2}b, a^{2n-1}b.$

The probable conjugacy classes of Q_n are :

Class no. 1)	$a^{2n} = e$
Class no. 2)	a, a^{2n-1}
Class no. 3)	a^2, a^{2n-2}
Class no. 4)	a^3, a^{2n-3}
Class no. 5)	a^4, a^{2n-4}
Class no. 6)	a^5, a^{2n-5}
...	...
...	...
...	...

Class no. n)	a^{n-1}, a^{n+1}
Class no. $n+1$)	a^n
Class no. $n+2$)	$ab, a^3b, a^5b, \dots, a^{2n-1}b$.
Class no. $n+3$)	$b, a^2b, a^4b, a^6b, a^8b, \dots, a^{2n-2}b$.

If $K(Q_n)$ denotes the number of conjugacy classes of Q_n , then

$$K(Q_n) = n + 3, \text{ for all values of } n \in \mathbb{N}.$$

We now proceed to give a logical proof in support of the validity of our conjecture.

I. $a^{2n} = e$, the identity of the group Q_n . So $a^{2n} = e \in Z(Q_n)$, the centre of Q_n . Therefore the conjugacy class of a^{2n} i.e. $[a^{2n}]$ consists of single element a^{2n} , [Since the conjugacy class containing the element $a \in G$ i.e. $[a]$ consists of a single element if and only if $a \in Z(G)$, the centre of G].

Thus class no. (1) is obtained.

Let us consider the element a^n of Q_n .

Let a^j , $1 \leq j \leq 2n$, be an element of Q_n . Then $a^n \cdot a^j = a^{n+j} = a^j \cdot a^n$ which shows that a^n commutes with all the elements of the form a^j , $1 \leq j \leq 2n$.

Again consider an element of Q_n of the form $a^i b$,

$1 \leq i \leq 2n$; then

$$\begin{aligned}
 a^n(a^i b) &= a^{n+i} b \\
 &= ba^{-(i+n)} && \text{(Since } ab = ba^{-1}\text{)} \\
 &= ba^{-i} a^{-n} \\
 &= ba^{-i} a^n && \text{(Since } a^{2n} = e \text{ i.e. } a^n = a^{-n}\text{)} \\
 &= (a^i b) a^n && \text{(Since } ab = ba^{-1}\text{)}
 \end{aligned}$$

Thus we have

$$\alpha a^n = a^n \alpha, \quad \text{for all } \alpha \in Q_n$$

$$\text{i.e. } a^n = \alpha^{-1} a^n \alpha, \quad \text{for all } \alpha \in Q_n$$

$$\text{i.e. } a^n \in Z(Q_n)$$

This implies that a^n alone constitutes a conjugacy class.

Thus the class no. $n+1$ is obtained.

II. Consider the elements of Q_n of the form a^i ,

$1 \leq i \leq n$ and $n < i \leq 2n$. We want to find the conjugacy

classes of these elements. For this let us compute the

normaliser of a^i where $1 \leq i \leq n$ and $n < i \leq 2n$:

Let a^j ; $1 \leq j \leq 2n$ be an element of Q_n .

Observing

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$$

which implies that,

$$N(a^i) \supseteq \{ a, a^2, a^3, \dots, a^{2n} = e \}$$

we claim that, $N(a^i) = \{ a, a^2, \dots, a^{2n} = e \}$

On the contrary, if an element of the form $a^j b$;

$1 \leq j \leq 2n$ of Q_n belongs to $N(a^i)$ then we must have

$$(a^i)(a^j b) = (a^j b) a^i$$

$$\text{i.e. } a^{i+j} b = b a^{-j} a^i \quad (\text{since } b^{-1} a b = a^{-1})$$

$$\text{i.e. } a b = b a^{-1})$$

$$\text{i.e. } a^{i+j} b = b a^{-j+i}$$

$$\text{i.e. } a^{i+j} b = a^{-i+j} b \quad (\text{Since } a b = b a^{-1})$$

$$\text{i.e. } a^{i+j} = a^{-i+j}$$

$$\text{i.e. } a^i = a^{-i}$$

$$\text{i.e. } a^{2i} = 1 = a^{2n}$$

$$\text{i.e. } 2i = 2n$$

$$\text{i.e. } i = n$$

which is a contradiction to the fact that $1 \leq i \leq n$ and $n < i < 2n$.

$$\text{Therefore } N(a^i) = \{a, a^2, \dots, a^{2n-1}, a^{2n} = e\}$$

Then using Corollary 1.1.1 of chapter 1, we find that number of elements of the conjugacy class $[a^i]$ i.e.

$$|[a^i]| = \frac{|G_n|}{|N(a^i)|} = \frac{4n}{2n} = 2.$$

Thus it is found that the conjugacy class containing a^i , $1 \leq i \leq n$, $n < i < 2n$ contains only two elements. Hence the number of conjugacy classes with only two elements is equal to $\frac{2n-2}{2} = n-1$ and these are obtained in the following way :

$$\text{Since } b^{-1} a b = a^{-1}$$

$$\text{i.e. } b^{-1} a b = a^{2n-1} \quad (\text{Since } a^{2n} = 1)$$

$$\text{i.e. } a \sim a^{2n-1}$$

Here it is to be noted that if two elements x and y are conjugate to each other then we write $x \sim y$.

$$\text{Again } b^{-1} a^2 b = a^{-2}$$

$$= a^{2n-2} \quad (\text{Since } a^{2n} = 1)$$

$$\text{i.e. } a^2 \sim a^{2n-2}$$

Similarly we have,

$$\begin{aligned}
 a^3 &\sim a^{2n-3} \\
 a^4 &\sim a^{2n-4} \\
 &\dots \quad \dots \\
 &\dots \quad \dots \\
 a^{n-1} &\sim a^{2n-(n-1)} \text{ i.e. } a^{n-1} \sim a^{n+1}
 \end{aligned}$$

Thus we have the conjugacy classes which are listed above.

III. Consider the elements of Q_n of the form $a^i b$ where $1 \leq i \leq 2n$. For this we observe that the normaliser of the elements of the form $a^i b$, $1 \leq i \leq 2n$:

Let us consider an element of Q_n of the form $a^i b$, $1 \leq i \leq 2n$.

Suppose $a^j \in N(a^i b)$ where $1 \leq j \leq 2n$.

$$\text{Then } (a^j)(a^i b) = (a^i b)(a^j)$$

$$\text{i.e. } a^{j+i} b = (b a^{-i}) a^j \quad (\text{Since } b^{-1} a b = a^{-1} \text{ i.e. } a b = b a^{-1})$$

$$\text{i.e. } a^{i+j} b = b a^{-i+j}$$

$$\text{i.e. } a^{i+j} b = a^{i-j} b$$

$$\text{i.e. } a^j = a^{-j}$$

$$\text{i.e. } a^{2j} = 1 = a^{2n} \quad (\text{Since } a^{2n}=1)$$

$$\text{i.e. } j = n \quad \text{or} \quad j = 2n \quad (\text{Since } 1 \leq j \leq 2n)$$

$$\text{Hence } \{a^{2n}, a^n\} \subseteq N(a^i b)$$

Suppose that an element of the form $a^j b$ belongs to $N(a^i b)$ where $1 \leq j \leq 2n$, $j \neq i$. Then

$$(a^i b)(a^j b) = (a^j b)(a^i b)$$

$$\text{i.e. } a^i (b a^j) b = a^j (b a^i) b$$

$$\text{i.e. } a^i a^{-j} b \cdot b = a^j a^{-i} b \cdot b \quad \left. \begin{array}{l} (b^{-1} a b = a^{-1}) \\ \text{i.e. } ab = ba^{-1} \end{array} \right\}$$

$$\text{i.e. } a^{i-j} = a^{j-i}$$

$$\text{i.e. } a^{2(j-i)} = 1 = a^{2n} \quad (\because a^{2n}=1)$$

$$\text{i.e. } 2(j-i) = 2n$$

$$\text{i.e. } j - i = n$$

$$\text{i.e. } j = i+n$$

Therefore $\{a^i b, a^j b\} \subseteq N(a^i b)$ where $j = i+n$.

Finally we get

$$N(a^i b) = \{a^{2n}=e, a^n, a^i b, a^{i+n} b\}$$

We determine the number of elements in the conjugacy class $[a^i b]$ by similar procedure as that of earlier cases. Number of elements of the conjugacy classes $[a^i b]$ [by using the Corollary 1.1.1]

$$\text{i.e. } |[a^i b]| = \frac{|Q_n|}{|N(a^i b)|} = \frac{4n}{4} = n$$

Thus the conjugacy class of $a^i b$ contains n elements.

Now we find the conjugacy classes of $a^i b$, $1 \leq i \leq 2n$ in the following way :

Case (i): Let us consider two elements of Q_n of the form $a^i b$ and $a^j b$ where $1 \leq i, j \leq 2n$ and $i \leq j$.

Suppose i and j both are even and $j - i = 2$.

$a^i b$ and $a^j b$ are conjugate to each other because there is an element $a^{i+1} b \in Q_n$ such that,

$$\begin{aligned} & (a^{i+1} b)^{-1} (a^i b) (a^{i+1} b) \\ &= b^{-1} a^{-i-1} (a^i b) (a^{i+1} b) \\ &= b^{-1} (a^{-1} b) (a^{i+1} b) \\ &= b^{-1} (ba) (a^{i+1} b) \quad (\because ab = ba^{-1}) \end{aligned}$$

$$= a \cdot a^{i+1}b$$

$$= a^{i+2}b$$

$$= a^j b$$

Therefore $a^i b \sim a^j b$

Thus we have,

$$a^2 b \sim a^4 b \sim a^6 b \sim a^8 b \sim \dots \sim a^{2n-2} b \sim b.$$

Case II : Suppose i and j both are odd and $j - i = 2$.

Consider two elements of Q_n of the form $a^i b$ and $a^j b$ where $1 \leq i, j \leq 2n$ and $i \leq j$.

By the similar argument as in Case (i) it can be shown that $a^i b \sim a^j b$. Therefore

$$a^i b \sim a^j b$$

Thus we have

$$ab \sim a^3 b \sim a^5 b \sim \dots \sim a^{2n-1} b.$$

We have,

$$N(a^i b) = \{a^{2n} = e, a^n, a^i b, a^{i+n} b\}$$

$$\text{Therefore } N(ab) = \{e, a^n, ab, a^{1+n} b\}$$

$$\text{and } N(a^2 b) = \{e, a^n, a^2 b, a^{2+n} b\} .$$

Hence by the similar procedure as that of earlier cases the number of elements of the conjugacy classes $[ab]$ is

$$|[ab]| = \frac{|Qn|}{|N(ab)|} = \frac{4n}{4} = n$$

and the number of elements of the conjugacy class $[a^2b]$ is

$$|[a^2b]| = \frac{|Qn|}{|N(a^2b)|} = \frac{4n}{4} = n$$

Therefore the conjugacy class of ab contains n - elements and they are

$$ab \sim a^3b \sim a^5b \sim \dots \sim a^{2n-1}b .$$

Also the conjugacy class of a^2b contains n -elements and they are

$$a^2b \sim a^4b \sim a^6b \sim \dots \sim a^{2n-2}b \sim b .$$

Hence $a^i b$ and $a^j b$ do not belong to the same conjugacy class when i is odd and j is even. Thus the total number of conjugacy classes will be :

$$\begin{aligned} & \frac{2n-2}{2} + 2+? \\ & = n + 3 . \end{aligned}$$

Now $J(Q_n)$ is obtained by using theorem 1.1 of Chapter 1 and we have the following :

Theorem 4.2.1.

$$J(Q_n) = \frac{n+3}{4n} \quad , \text{ for all } n \in \mathbb{N}$$

Remarks : If $n = 2$ then $J(Q_n) = \frac{5}{8}$.

Conversely, let $J(Q_n) = \frac{5}{8}$

$$\text{i.e. } \frac{n+3}{4n} = \frac{5}{8}$$

$$\text{i.e. } 8n + 24 = 20n$$

$$\text{i.e. } 12n = 24$$

$$\text{i.e. } n = 2$$

Therefore we have $J(Q_n) = \frac{5}{8}$ if and only if $n = 2$. That is Q_2 attains the maximum value $\frac{5}{8}$ of $J(Q_n)$ and no other member of this family (i.e. Q_n for $n \geq 1$; Q_n is commutative for $n = 1$) attains the maximum value.

$J(Q_n)$ is a monotonically decreasing sequence for $n \geq 2$ and

$$\lim_{n \rightarrow \infty} J(Q_n) = \lim_{n \rightarrow \infty} \frac{n+3}{4n}$$

$$= \lim_{n \rightarrow \infty} \frac{1+3/n}{4}$$

$$= \frac{1+0}{4}$$

$$= 1/4$$

Hence we can conclude that the values of $J(Q_n)$ lie on the semiclosed interval $(\frac{1}{4}, \frac{5}{8}]$ for $n \geq 2$ i.e.

$$J(Q_n) \in (\frac{1}{4}, \frac{5}{8}] \text{ for } n \geq 2 .$$

BIBLIOGRAPHY

1. Armstrong, M.A. (1987) : Groups and symmetry.
Springer-Verlag,
New York Berlin Heidelberg.
London Paris Tokyo.
2. Barman, Niva (1993) : A study of the commutativity
behaviour of the K-metacyclic
group;
M-Phil thesis, Gauhati Univer-
sity.
3. Coxeter, H.S.M. and Moser, W.O.J. (1965) : Generators and relations for
discrete groups, Berlin,
Second edition.
4. Dornhoff, Lorry (1971) : Group representation theory,
Marcel Dekker Inc. New York.
5. Gallagher, P.X. (1970) : 'The number of conjugacy classes
in a finite group', Math, Z.
118, pp 175-179.
6. Hall, M. (1959) : The theory of Groups; Macmillan
and Co. London.

7. Herstein, I.N. (1975) : Topics in Algebra, Second Edition, Vikas Publishing House, Pvt. Ltd.
8. Joseph. K.S.(1969) : Commutativity in non-abelian groups, Ph.D. thesis; University of California, Los Angeles.
9. Johnson, D.L.(1980) : Topics in the theory of group representations, Cambridge University Press.
10. Kalita Anu (1988) : Determination of the Joseph measure of commutativity for some families of non-commutative finite groups; M.Phil thesis Gauhati University.
11. Ledermann, W.(1961) : Introduction to the theory of finite groups, Olyver and Boyd Series.
12. Machale, Desmond (1974): "How commutative can a non-commutative group be?" Mathematical Gazette, 58, pp 199-202.
13. Machale, P.D.(1972) : Finite groups with automorphism inverting many elements; Ph.D. thesis, University of Kelle.

14. Schenkman Eugene(1965) : Group Theory, (an East-West edition) Affiliated East-west press Pvt. Ltd., New Delhi.
15. Scott, W.R.(1964) : Group theory; Prentice Hall, Inc. New Jersey.
16. Waerden B.L.van der(1985) : A history of Algebra, Springer verlag Berlin Heidelberg New York Tokyo.
17. Zassenhaus, Hans J.(1958): The theory of groups, Chelsea Publishing Company, New York.

