

# PARAMETRIZATION OF CERTAIN GROUP ACTIONS

DISS  
MAT  
491  
c-1



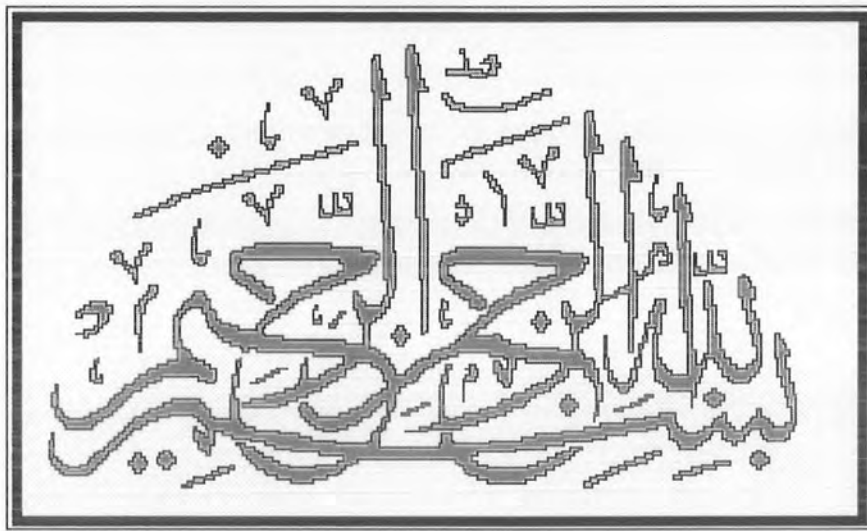
By

**MUHAMMAD ASHIQ**

**Department of Mathematics  
Quaid-i-Azam University  
Islamabad, Pakistan**

2004

*In the name of Allah  
the most beneficent, the most merciful*



# PARAMETRIZATION OF CERTAIN GROUP ACTIONS



By

**MUHAMMAD ASHIQ**

Supervised By

**PROF. QAISER MUSHTAQ**

**Department of Mathematics  
Quaid-i-Azam University  
Islamabad, Pakistan  
2004**

# PARAMETRIZATION OF CERTAIN GROUP ACTIONS



By

**MUHAMMAD ASHIQ**

A thesis submitted in partial fulfilment  
of the requirements for the degree of  
Doctor of Philosophy

**Department of Mathematics  
Quaid-i-Azam University  
Islamabad, Pakistan  
2004**

*Dedicated to*

*My parents & family*

## **ACKNOWLEDGEMENTS**

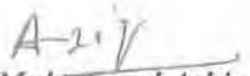
*In the name of **Almighty Allah**, the most Merciful and Compassionate, who enabled me to complete this thesis.*

*I wish to express my profound gratitude to my supervisor, **Professor Qaiser Mushtaq**, whose guidance and keen interest enabled me to accomplish this work. I would never have been able to do it up to the standard otherwise.*

*I am grateful to my research fellows, Major Tariq Maqsood and Professor Aslam Wasim, for their sincere help and cooperation.*

*I wish to express my heartfelt thanks and deep gratitude to my parents, brothers sisters for their encouragement and moral support during my studies. Their special prayers and unlimited love has been a constant source of guidance for me. I cannot forget to thank my wife, Azra Ashiq, who morally supported me in completing this task.*

*Finally, I would like to place on record my gratitude to the Pakistan Army for selecting me to do this Ph. D.*

  
**Muhammad Ashiq**

## NOTATIONS

Most of the set theoretic and group theoretic notations used in this thesis are standard, and are available in [7], [31] and [36]. However, some special notations which have been used extensively in this thesis are presented here.

$$G^{3,3}(2, Z) = \langle u, v : u^3 = v^3 = 1 \rangle.$$

$$G^{3,3}(2, Z) = \langle u, v, t : u^3 = v^3 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle.$$

$$G^{3,n}(2, Z) = \langle u_1, v_1 : u_1^3 = v_1^n = 1 \rangle.$$

$$G^{3,n}(2, Z) = \langle u_1, v_1, t : u_1^3 = v_1^n = t^2 = (u_1 t)^2 = (v_1 t)^2 = 1 \rangle.$$

$$\Delta(3, n, k) = \langle u_1, v_1 : u_1^3 = v_1^n = (u_1 v_1)^k = 1 \rangle.$$

$$\Delta^*(3, n, k) = \langle u_1, v_1, t : u_1^3 = v_1^n = t^2 = (u_1 t)^2 = (v_1 t)^2 = (u_1 v_1)^k = 1 \rangle.$$

$$\Delta(l, n, k) = \langle u_1, v_1 : u_1^l = v_1^n = (u_1 v_1)^k = 1 \rangle.$$

$$\Delta(3, 3, k) = \langle u, v : u^3 = v^3 = (uv)^k = 1 \rangle.$$

$$\Delta(3, 3, k; n_1) = \langle u, v : u^3 = v^3 = (uv)^k = (uvu^{-1}v^{-1})^{n_1} = t^2 = (ut)^2 = (vt)^2 = 1 \rangle.$$

By  $Q(\sqrt{n})$  we shall mean the real quadratic field and by  $Q(\sqrt{-n})$  the imaginary quadratic field. The projective line over the finite field  $F_q$  is denoted by

$$PL(F_q) = F_q \cup \{\infty\}.$$

# ABSTRACT

We have investigated properties of certain groups by looking at their actions on suitable spaces. These actions are studied by using a graphical technique now known as coset diagrams for the group  $G^{3,3}(2, Z)$ . We have used these diagrams to establish a relationship between real and imaginary quadratic irrational numbers and the elements of the group.

The aim of this research has been to study actions of the group generated by the linear-fractional transformations  $u: z \rightarrow \frac{z-1}{z}$  and  $v: z \rightarrow \frac{-1}{z+1}$ , which satisfy the relations  $u^3 = v^3 = 1$  on the projective line over the real, imaginary quadratic field and the finite field.

We have shown that the coset diagram for the actions of  $G^{3,3}(2, Z)$  on the rational projective line is connected and the action is transitive. Using this we have shown that  $u^3 = v^3 = 1$  are defining relations for the group.

We have found out that if  $\alpha$  is any real quadratic irrational number then the ambiguous numbers form a closed path in the coset diagram for the orbit  $\alpha G^{*3,3}(2, Z)$  and it is the only closed path contained in it.

Next we have parametrized the actions of the group  $G^{*3,3}(2, Z) = \langle u, v, t : u^3 = v^3 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle$  on the projective line over the finite field  $F_q$ . That is, each conjugacy class of actions of  $G^{*3,3}(2, Z)$  on  $PL(F_q)$  can be represented by a coset diagram  $D(\theta, q)$ , where  $\theta \in F_q$  and  $q$  is a prime power. In particular, we have associated each conjugacy class of actions of the infinite triangle groups  $\Delta(3,3,k)$  on  $PL(F_q)$  with a coset diagram  $D(\theta, q)$ .



# CONTENTS

<b>PREFACE</b>	01
<b>CHAPTER 1</b>	06
<b>DEFINITIONS AND BASIC CONCEPTS</b>	
1.1 Definitions	06
1.2 Coset Diagrams	09
1.3 The Group $G^{3,3}(2, Z) = \langle u, v : u^3 = v^3 = 1 \rangle$	15
1.4 Coset Diagrams for the Group $G^{3,3}(2, Z)$	19
1.5 Quadratic Fields	21
<b>CHAPTER 2</b>	24
<b>FINITE PRESENTATION OF <math>G^{3,3}(2, Z)</math></b>	
2.1 Introduction	24
2.2 Action of $G^{3,3}(2, Z)$ on the Rational Projective Line	24
<b>CHAPTER 3</b>	33
<b>ACTION OF <math>G^{3,3}(2, Z)</math> ON REAL AND IMAGINARY QUADRATIC FIELDS</b>	
3.1 Introduction	33
3.2 Coset Diagrams for the Group $G^{3,3}(2, Z)$	34
3.3 Existence of Ambiguous Numbers	38
3.4 Conclusion	42

3.5	Action of $G^{3,3}(2, Z)$ on an Imaginary Quadratic Field	43
3.6	Existence of Fixed Points in $Q^*(\sqrt{-n})$ and Orbits of $Q^*(\sqrt{-n})$	46

## CHAPTER 4 70

### PARAMETRIZATION OF ACTIONS OF $G^{*3,n}(2, Z)$

4.1	Introduction	70
4.2	Conjugacy Classes of the non degenerate Homomorphisms	72
4.3	Triangle Groups	83

## CHAPTER 5 90

### $\Delta(3,3, k)$ & PARAMETRIZATION OF ACTIONS OF $G^{*3,3}(2, Z)$

5.1	Introduction	90
5.2	Coset Diagrams for the Group $\Delta(3,3, k)$	92
5.3	Relation Between the non-degenerate Homomorphisms and the Parameters	93
5.4	Parametrization of the Actions	93
5.5	A Condition for the Existence of Certain Coset Diagrams	96
5.6	Conjugacy Classes Corresponding to $\theta = 3$	101
5.7	Conjugacy Classes of non-degenerate Homomorphism	104
5.8	Parameters for the Conjugacy Classes of $G^{3,3}(2, q)$	105
5.9	Parametrization of the Actions of $\Delta(3, 3, k; n_1)$	118

## REFERENCES 123

## PREFACE

The modular group  $PSL(2, Z)$  is generated by the linear fractional transformations  $x: z \rightarrow \frac{-1}{z}$  and  $y: z \rightarrow \frac{z-1}{z}$ , which satisfy the relations,  $x^2 = y^3 = 1$ . The importance of  $PSL(2, Z)$  stems from the fact that it is a discrete group of motions in the Lobachevsky plane.

Let  $v = xyx$  and  $u = y$ . Then  $(z)v = \frac{-1}{z+1}$  and  $u^3 = v^3 = 1$ . So the group generated by  $u$  and  $v$  is a proper subgroup of the modular group  $PSL(2, Z)$  and is isomorphic to the free product of the cyclic groups  $\langle u \rangle$  and  $\langle v \rangle$  of order 3. Since  $\langle u, v: u^3 = v^3 = 1 \rangle$  is a group of linear-fractional transformations of the form  $z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in Z$  and  $ad - bc = 1$ , we denote it by  $G^{3,3}(2, Z)$ . Specifically, the linear-fractional transformations of  $G^{3,3}(2, Z)$  are  $u: z \rightarrow \frac{z-1}{z}$  and  $v: z \rightarrow \frac{-1}{z+1}$  which satisfy the relations,  $u^3 = v^3 = 1$ .

As  $u$  and  $v$  have the same order, there is an automorphism interchanging  $u$  and  $v$  and this yields the split extension  $G^{*3,3}(2, Z)$ . The linear-fractional transformation  $t: z \rightarrow \frac{1}{z}$  inverts  $u$  and  $v$ , that is,  $t^2 = (ut)^2 = (vt)^2 = 1$  and so extends the group  $G^{3,3}(2, Z)$  to  $G^{*3,3}(2, Z)$ . The extended group  $G^{*3,3}(2, Z)$  is then  $\langle u, v, t: u^3 = v^3 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle$ .

Let  $q$  be a power of a prime  $p$ . Then by the projective line over the finite field  $F_q$ , we mean  $F_q \cup \{\infty\}$ , we denote it by  $PL(F_q)$ . The group  $G^{*1}(2, q)$  is then the group of linear-fractional transformations of the form  $z \rightarrow \frac{az + b}{cz + d}$ , where  $a, b, c, d \in F_q$  and  $ad - bc \neq 0$ , while  $G^{3,3}(2, q)$  is its subgroup consisting of all those linear-fractional transformations of the form  $z \rightarrow \frac{az + b}{cz + d}$ , where  $a, b, c, d \in F_q$  and  $ad - bc$  is a non-zero square in  $F_q$ .

This thesis comprises five chapters. The aim of chapter one is to provide background material for succeeding chapters.

In chapter two, we show that the coset diagram for the action of  $G^{3,3}(2, Z)$  on the rational projective line is connected and the action is transitive. Using the coset diagrams we show that  $u^3 = v^3 = 1$  are defining relations for the group.

In chapter three, we study action of the group  $G^{3,3}(2, Z)$  on  $Q(\sqrt{n})$  and  $Q(\sqrt{-n})$  by using coset diagrams.

Let  $n$  be a non-square positive integer and  $Q(\sqrt{n})$  be a real quadratic field. Consider a subset  $Q^+(\sqrt{n}) = \left\{ \frac{a + \sqrt{n}}{c} : a, c \in Z, c \neq 0, b = \frac{a^2 - n}{c} \in Z, (a, b, c) = 1 \right\}$  of  $Q(\sqrt{n})$ . For a fixed non-square positive integer  $n$ , if the real quadratic irrational number  $\alpha = \frac{a + \sqrt{n}}{c}$  and its algebraic conjugate  $\bar{\alpha} = \frac{a - \sqrt{n}}{c}$  have different signs, then such an  $\alpha$  is known as an ambiguous number. They

play an important role in classifying the orbits of  $G^{3,3}(2, Z)$  on  $Q(\sqrt{n})$ . We have classified all the ambiguous numbers in the orbit. If  $\alpha$  and  $\bar{\alpha}$  are both positive (negative),  $\alpha$  is called a totally positive (negative) number.

Here, we have explored some interesting group theoretic properties of this action vis-à-vis the orbit of  $\alpha$  in  $G^{3,3}(2, Z)$ . It is known that the set of ambiguous numbers is finite and that the ambiguous numbers in the coset diagram for the orbit  $\alpha G^{3,3}(2, Z)$  form a closed path and it is the only closed path contained in it.

The imaginary quadratic fields are defined by the set  $\{a + b\sqrt{-n} : a, b \in Q\}$  and denoted by  $Q(\sqrt{-n})$ , where  $n$  is a square-free positive integer.

In section two of chapter three, we prove that if  $\alpha = \frac{a + \sqrt{-n}}{c} \in Q^*(\sqrt{-n}) = \{\frac{a + \sqrt{-n}}{c} : a, \frac{a^2 + n}{c}, c \in Z, c \neq 0\}$  then  $n$  does not change its value in the orbit  $\alpha G^{3,3}(2, Z)$ . Also we show that the number of orbits of  $Q^*(\sqrt{-n})$  under the action of  $G^{3,3}(2, Z)$  is  $2[d(n) + 2d(n+1) - 4]$  and  $2[d(n) + 2d(n+1) - 6]$  accordingly  $n$  is even or odd, except for  $n=3$  for which there are exactly eight orbits. Also, the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{-n})$  is always intransitive.

In chapter four, we consider conjugacy classes, which arise from the actions of  $\Delta(3, n, k)$  on projective line over  $PL(F_q)$ . Also, we prove that a one-to-one correspondence can be established between the conjugacy classes of non-degenerate homomorphism  $\sigma : G^{3,3}(2, Z) \rightarrow G^{3,3}(2, q)$ , under the action of inner automorphisms of  $G^{3,3}(2, q)$ , and the non-trivial conjugacy classes of elements

of  $G^{*1,n}(2,q)$  such that the correspondence assigns to any non-degenerate homomorphism  $\sigma$  the class containing  $(uv)\sigma$ . In other words we have parametrized the actions of  $G^{*1,n}(2,Z)$  on  $PL(F_q)$ . Also we consider the conjugacy classes which arise from the actions of triangle groups  $\Delta(3, n, k)$  on the projective line over  $PL(F_q)$ .

In chapter five, we parametrize the conjugacy classes of non-degenerate homomorphism which represent actions of  $\Delta(3,3,k) = \langle u, v : u^3 = v^3 = (uv)^k = 1 \rangle$  on  $PL(F_q)$  where  $q \equiv \pm 1 \pmod{k}$ . Also, for various values of  $k$ , we find the conditions for the existence of coset diagrams depicting the permutation actions of  $\Delta(3, 3, k)$  on  $PL(F_q)$ . The conditions are polynomials with integer coefficients and the diagrams are such that every vertex in them is fixed by  $(\bar{u}\bar{v})^k$ . In this way, we get a homomorphic image of  $\Delta(3,3,k)$  as permutation groups on  $PL(F_q)$ . Also, we parametrize actions of  $G^{*3,3}(2,Z)$  on  $PL(F_q)$  by the elements of  $F_q$ . We prove that the conjugacy classes of non-degenerate homomorphism  $\sigma$  are in one-to-one correspondence with the conjugacy classes of non-trivial elements of  $G^{*3,3}(2,q)$ , under a correspondence which assigns to the homomorphism  $\sigma$  the class containing  $(uv)\sigma$ . Of course, this will mean that we can actually parametrize the actions of  $G^{*3,3}(2,q)$  on  $PL(F_q)$  by the elements of  $F_q$ . We develop a useful mechanism by which one can construct a unique coset diagram for each conjugacy class of these non-degenerate homomorphisms which depict the actions of  $G^{*3,3}(2,Z)$  on  $PL(F_q)$ .

A paper entitled *Finite Presentation of a Linear-Fractional Group* containing results from chapter two has been accepted in Algebra Colloquium. Another paper entitled *Action of a Two Generator Group on a Real Quadratic Field* containing some results of chapter three is accepted in Southeast Asian Bulletin of Mathematics. Some results of *Imaginary Quadratic Fields* from chapter three are presented in The Fourth European Congress of Mathematics 2004 in Sweden (Stockholm University). A paper entitled *Parametrization of  $G^*(2, Z)$  on  $PL(F_q)$*  has been published in the Proceedings of ICM - 2002 Satellite Conference in Algebra and Related Topics (Advances in Algebra, 2003, 264 – 270), held in Hong Kong from August 14 – 17, 2002. A talk entitled *Coset Diagrams for a Homomorphic Image of  $\Delta(3, 3, k)$*  containing results from chapter five was presented in the International Congress of Mathematicians – 2002 held in China (Beijing). The other four papers are submitted in well reputed international journals for publication.

## CHAPTER ONE

### DEFINITIONS AND BASIC CONCEPTS

The prime objective of this introductory chapter about definitions and basic concepts is to provide background to the material to be presented more formally in succeeding chapters. We have included only those definitions and descriptions, which are specifically relevant to the material embodied in this thesis. However, for comprehensive reference we suggest reference [29].

#### 1.1 DEFINITIONS

Let  $G$  be a group and  $X$  a set. By an action of  $G$  on  $X$  we mean a function  $\mu: X \times G \rightarrow X$  such that for all  $x$  in  $X$  and  $g, h$  in  $G$ , the following axioms are satisfied [31].

$$(i) \quad ((x, g)\mu, h)\mu = (x, gh)\mu$$

$$(ii) \quad (x, 1)\mu = x.1 = x, \text{ where } 1 \text{ denotes the identity in the group } G.$$

Let us take  $G$  to be any group. Let  $X = G$  and define  $x^g = g^{-1}xg$  for  $x \in X$  and  $g \in G$ . It follows easily from the above axioms that this defines an action of  $G$  on itself.



Let  $G$  be a group acting on the set  $X$  and if  $a \in X$ , we define the stabilizer of  $a$  by

$$G_a = \text{Stab}(a) = \{g \in G : a^g = a\}.$$

Let  $G$  be a group acting on the set  $X$ . Then  $a^G = aG = \{a^g = ag : g \in G\}$  is called an orbit of  $a$  in  $G$ . Also  $G$  acts on  $X$  transitively if  $X \neq \emptyset$  and for any  $a, b \in X$  there exists  $g \in G$  such that  $a^g = b$ .

The linear-fractional groups for different fields arose independently. In 1852, A. F. Möbius studied synthetically the field of complex numbers. The field of real numbers appeared in the work of Von Staudt in 1847 as the projective group on a line, with elements formed by a sequence of projections from one line to another in the real projective plane (see in [1] and [7]).

For the field  $Z_p$ , the linear-fractional group and its subgroup was studied by E. Galois in 1832. In 1893, the linear-fractional group was studied by E. H. Moore for arbitrary finite fields, who established the simplicity of the projective special linear group of divisor 2 for fields of order greater than 3. The homomorphism of general linear group of divisor 2 over a field  $F$  to the linear-fractional group is implied in the work of E. Galois in 1832 and J. A. Serret in 1866, and was used by A. Cayley in 1880 to determine properties of linear-fractional transformations (see in [30] and [36]).

Let  $F$  be a field and  $n$  a positive integer. We write  $M_n(F)$  for the set of all  $n \times n$  matrices with entries from  $F$ . Then  $GL(n, F) = \{A \in M_n(F) : A \text{ is invertible}\}$ , the set of all  $n \times n$  invertible matrices, with entries from  $F$  forms a group under the matrix multiplication. The group

$GL(n, F)$  is known as the  $n$ -dimensional general linear group over  $F$ . The  $n$ -dimensional special linear group  $SL(n, F)$  is defined to be the group of all  $n \times n$  matrices with entries from  $F$  and determinant 1, that is,  $SL(n, F) = \{A \in GL(n, F) : \det(A) = 1\}$ . The group  $SL(n, F)$  is a normal subgroup of  $GL(n, F)$ , due to the fact that the determinant map  $\det : GL(n, F) \rightarrow F^\times$ , where  $F^\times$  denotes the multiplicative group of non-zero elements of  $F$ , is a group epimorphism and has  $SL(n, F)$  as its kernel. Thus  $GL(n, F)/SL(n, F) \cong F^\times$ .

If  $F$  is a finite field and has  $q$  elements (where  $q$  is a prime power), then  $F$  can be denoted by  $F_q$ . In this case, the general linear group of dimension  $n$ , over the field  $F_q$  is  $GL(n, F_q)$ . Similarly we define  $SL(n, F_q)$ . Since all finite fields of the same order are isomorphic, therefore  $GL(n, F_q)$  and  $SL(n, F_q)$  are written as  $GL(n, q)$  and  $SL(n, q)$  respectively. These are finite groups and we can compute their orders as,  $|GL(n, q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$  and

$$|SL(n, q)| = \frac{|GL(n, q)|}{(q-1)}.$$

Let  $V$  be an  $n$ -dimensional vector space over a field  $F$ . Then an isomorphism of  $V$  into itself is called an automorphism of the vector space  $V$ . The general linear group  $GL(n, q)$  can be considered as the group of all automorphism of  $n$ -dimensional vector space over the field  $F_q$  of  $q$  elements. The special linear group  $SL(n, q)$  is its normal subgroup consisting of automorphism of determinant 1. For, the centre of either of these groups consists of the operations of the form  $x \rightarrow kx$  where  $k \in F_q$  and so the corresponding

projective groups namely,  $PGL(n, q)$  and  $PSL(n, q)$ , can be obtained by factoring out these centres.

Let  $X$  be any non-empty set. The set of all permutations defined on  $X$  is a group with composition of mappings as the binary operation defined in the group. Also, there is a one to one correspondence between actions of  $G$  on  $X$  and representations of  $G$  by permutations of  $X$ . Thus an action gives rise to a permutation representation and vice – versa.

Suppose that  $S$  is a permutation group acting on a set  $X$ . Let  $S$  be generated by  $x_1, x_2, \dots, x_k$ . Then the points of  $X$  are represented by the vertices of the diagram; and if  $l, m$  are points of  $X$  such that  $lx_i = m$ , we represent this fact by a directed edge ‘of colour  $i$ ’ joining  $l$  to  $m$  [6]. The resulting diagram will be connected, that is to say any two of its vertices can be joined by an unbroken sequence of edges, if and only if  $S$  is transitive on  $X$ . In the case of a connected diagram the points of  $X$  can be identified with cosets  $N_g$  where  $N$  is the stabilizer of some arbitrary point of  $X$  and  $g$  is an element of  $S$ .

## 1.2 COSET DIAGRAMS

Graphs have abundant applications in several branches of mathematics. They provide methods by which various algebraic and topological structures can be conceived. Graphical methods have been extensively used to study finitely generated groups. The graphs have proven themselves as an economical mathematical technique to authenticate certain important results (see, [5], [6], [10], [12], [13], [17], and [25]). For finite groups of small order the graphs can be used in lieu of Cayley table. They give the same information but in a much more effective way (see [6], and [20]).

The method of representing group actions by graphs has a long and rich history. The first paper in which graphs were used explicitly was by A. Cayley [6] in 1878. After A. Cayley, in 1893, Hurwitz used graphs to represent groups [8], and [13]. Then in 1896, H. Maschke [19] used Cayley's colour graphs to prove some important results on the representation of finite groups, especially on the rotation groups of the regular bodies in three and four-dimensional spaces.

The Cayley's graphs were rediscovered by Dehn, in 1910. For this reason, some authors call it as the Dehnzch Gruppenbild. But Cayley's priority is indisputable, as he described graphs much earlier [13].

Later, mathematicians like O. Schreier, J. H. C. Whitehead [35], H. S. M. Coxeter and W. O. J. Moser [13], W. Burnside [5], etc, contributed seminal papers containing graphical representations of groups.

In 1978, G. Higman propounded the idea of coset diagrams for the modular group. M. D. E. Conder [9], [10], and [11] and Q. Mushtaq [22 - 29] in their separate works have used these diagrams to solve certain "identification problems". In G. Higman's words, "Q. Mushtaq laid the foundation of the theory of coset diagrams for the modular group".

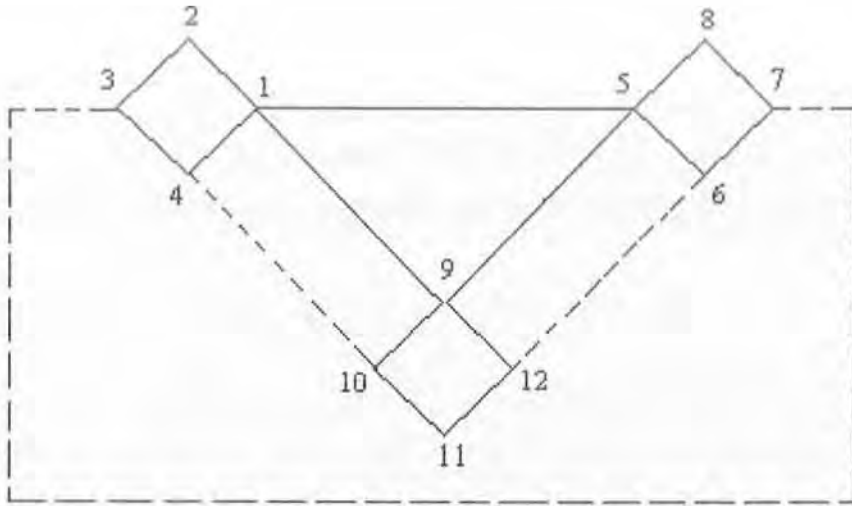
A. Cayley [6] used graphs to study certain groups in 1878. He represented the multiplication table of a group with given generators by graph, and proposed the use of colours to distinguish the edges of the graphs associated with different generators. The Cayley diagram for a given group is a graph whose vertices represent the elements of the group, which are the cosets of the trivial subgroup. O. Schreier generalized this notion by considering a graph whose vertices represent the cosets of any subgroup. In 1965, Coxeter and Moser [13] used both Cayley and Schreier diagrams to prove some results on finitely generated groups.

A coset diagram is a graph whose vertices are the (right) cosets of a subgroup of finite index in a finitely generated group. The vertices representing cosets  $g$  and  $h$  (say), are joined by an  $s_i$ -edge, of “colours  $i$ ” directed from vertex  $g$  to vertex  $h$ , whenever,  $gs_i = h$ .

$$g \rightarrow gs_i = h$$

It may well happen that  $gs_i = g$ , in which case the  $g$ -vertex is joined to itself by an  $s_i$ -loop.

Formally, a coset diagram, corresponding to a subgroup  $H$  of finite index in a finitely generated group  $G$ , is a directed edge whose vertices are the (right) cosets of  $H$  in  $G$  and whose edges are defined as follows: we take a specific set of generators for  $G$ , and for each generator  $x$  and each vertex  $H_g$ , for some  $g$  in  $G$ , draw an edge from  $H_g$  to  $H_g x$ . This is very similar to the notion of a Schreier coset diagram whose vertices represent the cosets of any given subgraph in a finitely generated group, and also to that of a Cayley graph whose vertices are the group elements themselves, with trivial stabilizer. These diagrams may be drawn for any finitely generated group acting on any arbitrary sets or spaces. For example, a transitive permutation representation (on 12 points) of the group  $G = \langle u, v, w : u^2 = v^3 = w^4 = 1 \rangle$  can be represented by the following diagram.



Here  $u$  acts as  $(4\ 10)(6\ 12)(3\ 7)$ ,  $v$  acts as  $(1\ 9\ 5)$ , and  $w$  acts as  $(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 10\ 11\ 12)$ .

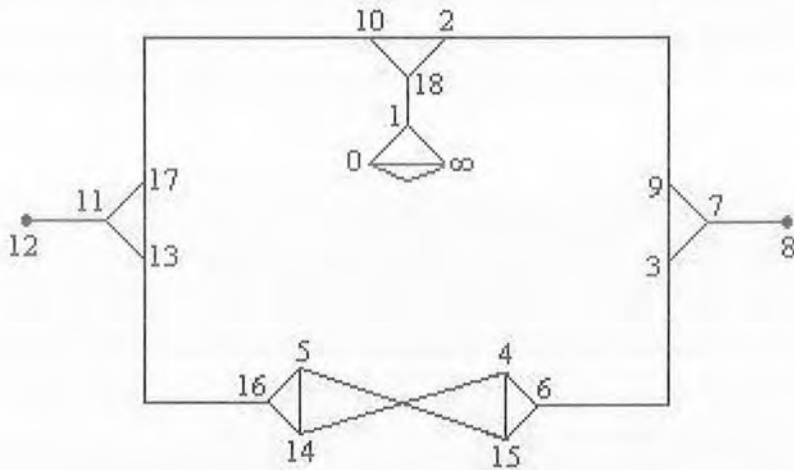
Then in 1978, G. Higman introduced the coset diagrams for the modular group  $PSL(2, Z)$ . Coset diagrams defined by G. Higman for the actions of  $PSL(2, Z)$  are special in a number of ways. First, they are defined for a particular group, namely  $PSL(2, Z)$ , which has a representation in terms of two generators  $x$  and  $y$ . Since there are only two generators, it is possible to avoid using colours as well as the orientation of edges associated with the involution  $x$ . For  $y$ , which has order 3, there is a need to distinguish  $y$  from  $y^2$ . The 3-cycles of  $y$  are therefore represented by small triangles, with the convention that  $y$  permutes their vertices counterclockwise, while the fixed points of  $x$  and  $y$ , if any, are denoted by heavy dots. Thus the geometry of the figure makes the distinction between  $x$ -edges and  $y$ -edges obvious.

For instance, consider the action of  $PGL(2, Z)$  on  $PL(F_{19})$ . We can calculate the permutation representations of  $x, y$  and  $t$  as  $(z)x = \frac{-1}{z}$ ,  $(z)y = \frac{z-1}{z}$  and  $(z)t = \frac{1}{z}$ , where  $z \in PL(F_{19})$ .

$$x = (0 \infty)(1 \ 18)(2 \ 9)(3 \ 6)(4 \ 14)(5 \ 15)(7 \ 8)(10 \ 17)(11 \ 12)(13 \ 16),$$

$$y = (0 \ \infty \ 1)(2 \ 10 \ 18)(3 \ 7 \ 9)(4 \ 15 \ 6)(5 \ 16 \ 14)(13 \ 17 \ 11)(8)(12), \text{ and}$$

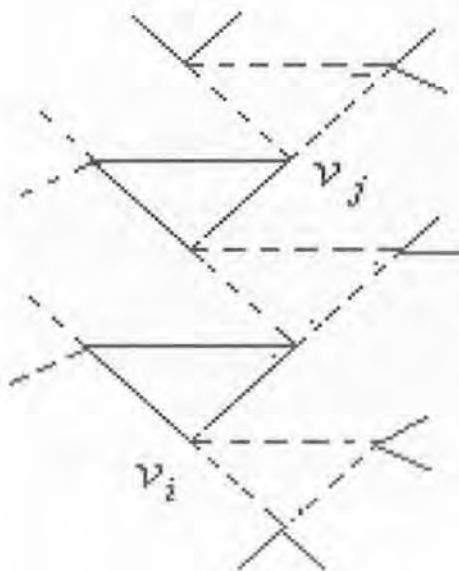
$$t = (0 \ \infty)(1)(2 \ 10)(3 \ 13)(4 \ 5)(6 \ 16)(7 \ 11)(8 \ 12)(9 \ 17)(14 \ 15)(18).$$



A coset diagram is a graph where the points of  $X$  are identified with the cosets  $N_g$ . If  $\pi = \{v_0, e_1, v_1, e_2, \dots, e_k, v_k\}$  is an alternating sequence of vertices and edges of a coset diagram, then  $\pi$  is a path in the diagram, joining  $v_0$  and  $v_k$ , if  $e_i$  joins  $v_{i-1}$  and  $v_i$  for each  $i$  and  $e_i \neq e_j$  ( $i \neq j$ ). A closed path is one



whose initial and terminal vertices coincide. A coset diagram is called connected if any two vertices in the diagram are joined by a path. For example, the path from vertex  $v_i$  to  $v_j$  ( $i \neq j$ ), in the following figure



corresponds to the word  $uv^{-1}u$ . Obviously the products of words appear as products of paths. A word is an element expressed as a product of the generators and their inverses.

Every connected coset diagram for a finitely generated group  $G$  on a set of  $n$  points corresponds to a transitive permutation representation of  $G$  on the set, which is in fact equivalent to the natural action of  $G$  on the cosets of some subgroup  $H$  of index  $n$ .



### 1.3 THE GROUP $G^{3,3}(2, Z) = \langle u, v : u^3 = v^3 = 1 \rangle$

The significance of the special linear group  $SL(2, Z)$  is related to the fact that in a two-dimensional lattice basis  $\{e_1, e_2\}$  and  $\{f_1, f_2\}$  are related by the equations:

$$\begin{aligned}f_1 &= ae_1 + ce_2 \\f_2 &= be_1 + de_2\end{aligned}$$

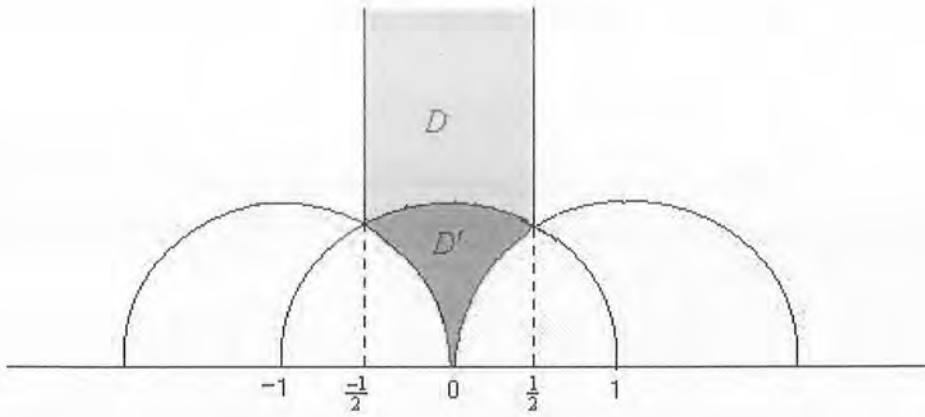
where  $a, b, c, d \in Z$  and  $ad - bc = \pm 1$ . It is also required that the direction of rotation from  $f_1$  to  $f_2$  is the same as that from  $e_1$  to  $e_2$ . This guarantees  $ad - bc = 1$ .

$SL(2, Z)$  acts on the upper half plane as,  $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  belongs to  $SL(2, Z)$

and  $(z)g = \frac{az + b}{cz + d}$ . Hence the matrix  $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$  acts as identity, so that, we have

an action of the group  $SL(2, Z)/N$  where  $N = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ . This

quotient group is denoted by  $PSL(2, Z)$  and is called the modular group. It acts on the upper half plane. The shaded region of the following modular region gives a fundamental domain for it.



The upper half plane is a model of Lobachevsky plane and the motions in it that preserve the orientation are given as transformations  $z \rightarrow \frac{az + b}{cz + d}$ , where  $a, b, c, d \in R$  and  $ad - bc = \pm 1$ . Thus the modular group  $PSL(2, Z)$  is a discrete group of motions in the Lobachevsky plane, where  $Z$  is the set of integers.

It is therefore possible to express the modular group as a group generated by two linear-fractional transformations  $x: z \rightarrow \frac{-1}{z}$  and  $y: z \rightarrow \frac{z-1}{z}$  such that  $x^2 = y^3 = 1$  becomes its defining relations. Therefore,  $PSL(2, Z)$  is a free product of the cyclic groups  $\langle x \rangle$  of order 2 and the cyclic group  $\langle y \rangle$  of order 3.

The linear-fractional transformation  $t: z \rightarrow \frac{1}{z}$  inverts  $x$  and  $y$ , that is,  $t^2 = (xt)^2 = (yt)^2 = 1$ , and so extends the group  $PSL(2, Z)$  to  $PGL(2, Z)$ . The extended modular group  $PGL(2, Z)$  is then generated by  $x$ ,  $y$ , and  $t$  and its defining relations are:

$$x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1$$

Let  $q$  be a power of a prime  $p$ . Then the group  $PGL(2, q)$  is the group of transformations  $z \rightarrow \frac{az + b}{cz + d}$ , where  $a, b, c, d \in F_q$  and  $ad - bc \neq 0$ , while the group  $PSL(2, q)$  is its subgroup of all those linear-fractional transformations  $z \rightarrow \frac{az + b}{cz + d}$ , where  $ad - bc$  is a non-zero square in  $F_q$ .

If  $PGL(2, Z)$  acts on  $PL(F_q)$ , then every element of  $PGL(2, q)$  gives a permutation on the points of  $PL(F_q)$ , and so  $PGL(2, q)$  is a subgroup of the symmetric group  $S_{q+1}$ . As the elements of  $PSL(2, q)$  give only even permutations, it is therefore a subgroup of the alternating group  $A_{q+1}$ .

The modular group  $PSL(2, Z)$  is the best known example of a large class of Fuchsian groups. Such groups are studied via their action on a metric space called hyperbolic 2-space. The study of modular groups via its action on some spaces has been extended in a number of directions. Of particular importance is, for example, the Bianchi groups. They are (low dimensional) groups which act as isometries on hyperbolic 3-space and generalize the Fuchsian groups in a natural way.

Let  $v = xyx$  and  $u = y$ . Then  $(z)v = \frac{-1}{z+1}$  and  $u^3 = v^3 = 1$ . So the group generated by  $u$  and  $v$  is a proper subgroup of the modular group  $PSL(2, Z)$  and is isomorphic to the free product of  $\langle u \rangle$  and  $\langle v \rangle$  of order 3. Since  $\langle u, v : u^3 = v^3 = 1 \rangle$  is a group of linear-fractional transformations of the form  $z \rightarrow \frac{az + b}{cz + d}$ , where  $a, b, c, d \in Z$  and  $ad - bc = 1$ , we denote it by  $G^{3,3}(2, Z)$ .

Specifically, the linear-fractional transformations of  $G^{3,3}(2, Z)$  are  $u: z \rightarrow \frac{z-1}{z}$

and  $v: z \rightarrow \frac{-1}{z+1}$  which satisfy the relations:

$$u^3 = v^3 = 1 \tag{1.3.1}$$

As  $u$  and  $v$  have the same order, there is an automorphism interchanging  $u$  and  $v$  and this yields the split extension  $G^{*3,3}(2, Z)$  of  $G^{3,3}(2, Z)$ . The linear-fractional transformation  $t: z \rightarrow \frac{1}{z}$  inverts  $u$  and  $v$ , that is,  $t^2 = (ut)^2 = (vt)^2 = 1$  and so extends the group  $G^{3,3}(2, Z)$  to  $G^{*3,3}(2, Z)$ . The extended group  $G^{*3,3}(2, Z)$  is then the group of transformations of the form  $z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in Z$  and  $ad - bc = \pm 1$  and its defining relations are of the form:

$$u^3 = v^3 = t^2 = (ut)^2 = (vt)^2 = 1 \tag{1.3.2}$$

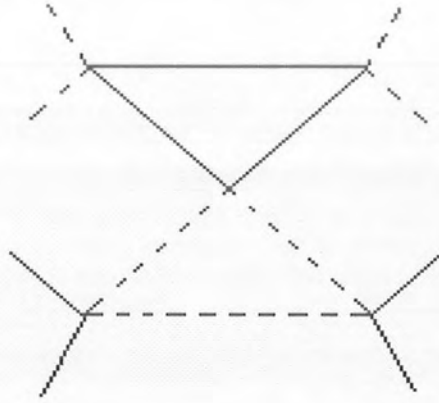
Let  $q$  be a power of a prime  $p$ . Then by the projective line over the finite field  $F_q$ , we mean  $F_q \cup \{\infty\}$ , we denote it by  $PL(F_q)$ . The group  $G^{*3,3}(2, q)$  is then the group of linear-fractional transformations of the form  $z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in F_q$  and  $ad - bc \neq 0$ , while  $G^{3,3}(2, q)$  is its subgroup consisting of all those linear-fractional transformations of the form  $z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in F_q$  and  $ad - bc$  is a non-zero square in  $F_q$ .

#### 1.4 COSET DIAGRAMS FOR THE GROUP $G^{*3,3}(2, Z)$

We use coset diagrams, described in section 1.2, for the group  $G^{*3,3}(2, Z)$  and study its action on  $PL(F_q)$ . The coset diagrams defined for the actions of  $G^{*3,3}(2, Z)$  are special in a number of ways. First, they are defined for a particular group, namely,  $G^{*3,3}(2, Z)$ , which has a presentation in terms of three generators  $t, u$  and  $v$ . Since there are only three generators, it is possible to avoid using colours as well as the orientation of edges associated with the involution  $t$ . For  $u$ , and  $v$  both have order 3, there is a need to distinguish  $u$  from  $u^2$  and  $v$  from  $v^2$ . The three cycles of the transformation  $u$  are denoted by three unbroken edges of a  $u$ -triangle permuted anti-clockwise by  $u$  and the three cycles of the transformation  $v$  are denoted by three broken edges of a  $v$ -triangle permuted anti-clockwise by  $v$ . The action of  $t$  is depicted by the symmetry about vertical axis because  $t^2 = (ut)^2 = (vt)^2 = 1$ . Fixed points of  $u$  and  $v$ , if they exist, are denoted by heavy dots.

A part of the coset diagram of the action of  $G^{*3,3}(2, Z)$  on  $PL(F_q)$  will look as follows:



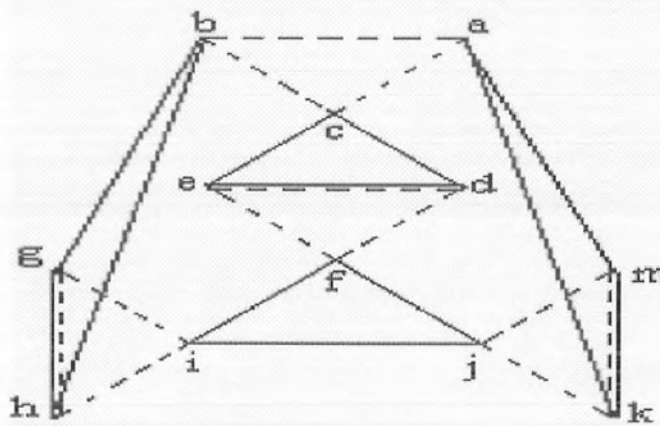


For example, the following diagram depicts a permutation representation of  $G^*(2, Z)$  on twelve points in which:

$$u = (c e d)(f i j)(b g h)(a k m),$$

$$v = (a b c)(d e f)(g h i)(m j k), \text{ and}$$

$$t = (a b)(d e)(j i)(m g)(k h)(c)(f).$$



## 1.5 QUADRATIC FIELDS

Now, we consider coset diagrams for the action of  $G^{3,3}(2, Z)$  on infinite spaces, namely,  $Q(\sqrt{n})$  and  $Q(\sqrt{-n})$ . In this case the coset diagrams are of infinite order, that is, the coset diagrams are with infinite number of vertices.

A number  $n$  is said to be square free if its prime decomposition contains no repeated factors. All primes are therefore trivially square free.

An algebraic integer of the form  $a + b\sqrt{n}$ , where  $n$  is square free, forms a quadratic field and is denoted by  $Q(\sqrt{n})$ . If  $n > 0$ , the field is called real quadratic field, and if  $n < 0$ , it is called an imaginary quadratic field. The integers in  $Q(\sqrt{1})$  are simply called the integers. The integers in  $Q(\sqrt{-1})$  are called Gaussian integers, and the integers in  $Q(\sqrt{-3})$  are called Eisenstein integers. The algebraic integers in an arbitrary quadratic field do not necessary have unique factorization. For example, the fields  $Q(\sqrt{-5})$  and  $Q(\sqrt{-6})$  are not uniquely factorable. All other quadratic fields  $Q(\sqrt{n})$  with  $n \leq 7$  are uniquely factorable.

An element  $\alpha = \frac{a + \sqrt{n}}{c}$  is called real quadratic irrational number where

$n$  is a non-square positive integer and  $a, \frac{a^2 - n}{c}, c$  are relatively prime integers.

An algebraic conjugate of  $\alpha = \frac{a + \sqrt{n}}{c}$  is the real quadratic irrational number

$\frac{a - \sqrt{n}}{c}$ , we denote it by  $\bar{\alpha}$ . Note that  $\alpha$  and  $\bar{\alpha}$  may have different signs. If this

is the case then the real quadratic irrational number  $\alpha$  is called an ambiguous

number. If  $\alpha$  and  $\bar{\alpha}$  both have the same sign positive (negative) then  $\alpha$  is called a totally positive (negative) number.

Let  $F$  be an extension field of degree 2 over the field  $Q$  of rational numbers. Then any element  $x \in F - Q$  is of degree two over  $Q$  and is a primitive element of  $F$  (that is,  $F = Q[x]$  and  $\{1, x\}$  is a base of  $F$  over  $Q$ ). Let  $F(x) = x^2 + bx + c$ , where  $b, c \in Q$ , be the minimal polynomial of such an element  $x \in F$ . Then  $2x = -b \pm \sqrt{b^2 - 4c}$  and so  $F = Q(\sqrt{b^2 - 4c})$ . Here, since  $b^2 - 4c$  is a rational number  $\frac{l}{m} = \frac{lm}{m^2}$  with  $l, m \in Z$ , we obtain  $F = Q(\sqrt{lm})$  with  $l, m \in Z$ . In fact, it is possible to write  $F = Q(\sqrt{n})$ , where  $n$  is a square free integer.

The imaginary quadratic fields are usually denoted by  $Q(\sqrt{-n})$ , where  $n$  is a square free positive integer. We shall denote the subset  $\{\frac{a + \sqrt{-n}}{c} : a, \frac{a^2 + n}{c}, c \in Z, c \neq 0\}$  by  $Q^*(\sqrt{-n})$ . The imaginary quadratic fields are very useful in different branches of mathematics, for example, in [21] the Bianchi groups are the groups  $PSL_2(O_n)$ , where  $O_n$  is the ring of integers of the imaginary quadratic number field  $Q(\sqrt{-n})$ . Interesting results are obtained by considering  $O_n$  as an Euclidean ring, that is, when  $n = 1, 2, 3, 7$  or  $11$ .

In [23], many properties of  $Q(\sqrt{n})$  have been discussed for modular group  $PSL(2, Z)$ . In chapter three, we will discuss some fundamental results of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{n})$  and  $Q^*(\sqrt{-n})$ .

Coset diagrams for the orbit of the group  $G^{3,3}(2, Z)$  acting on real and imaginary quadratic fields give some interesting information. For the modular



group, Q. Mushtaq [23] has shown that for a fixed value of  $n$  (a non square positive integer) there are only a finite number of ambiguous numbers  $\alpha$ , where  $\alpha$  and that part of the coset diagram containing these numbers form a single closed path and it is the only closed path in the orbit of  $\alpha$ .

## CHAPTER TWO

### FINITE PRESENTATION OF $G^{3,3}(2, Z)$

#### 2.1 INTRODUCTION

In this chapter we have shown that the coset diagram for the action of the group  $G^{3,3}(2, Z)$ , generated by the linear-fractional transformations  $u : z \rightarrow \frac{z-1}{z}$  and  $v : z \rightarrow \frac{-1}{z+1}$ , on the rational projective line is transitive and the coset diagram for the action is connected. Using the coset diagrams we have shown that  $u^3 = v^3 = 1$  are defining relations for the group.

#### 2.2 ACTION OF $G^{3,3}(2, Z)$ ON THE RATIONAL PROJECTIVE LINE

##### Lemma 2.2.1

If  $k \neq 1, 0, \infty$  then of the vertices  $k, ku$  and  $ku^2$  of a  $u$ -triangle (unbroken lines), in a coset diagram for the action of  $G^{3,3}(2, Z)$  on any subset of the real projective line, one vertex is negative and two are positive.

### Proof

Consider a coset diagram for the action of  $G^{3,3}(2, Z)$  on any subset of the real projective line. If  $k \neq 1, 0, \infty$  is one of the three vertices of the triangle in the coset diagram, since  $(z)u = \frac{z-1}{z}$ , then

- a. if  $z < 0$ , then  $(z)u > 1$ ,
- b. if  $z > 1$ , then  $0 < (z)u < 1$ , and
- c. if  $0 < z < 1$ , then  $(z)u < 0$ .

Thus, in particular, of the vertices  $k, ku$  and  $ku^2$ , one is negative and the other two are positive. Diagrammatically, it can be shown as:

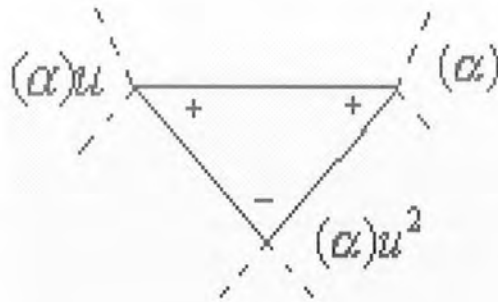


Fig-2.1

**Lemma 2.2.2**

If  $k \neq -1, 0, \infty$ , then of the vertices  $k, kv$  and  $kv^2$ , of a  $v$ - triangle (broken lines), in a coset diagram for the action of  $G^{3,3}(2, Z)$  on any subset of the real projective line, one vertex is positive and two are negative.

**Proof**

Consider a coset diagram for the action of  $G^{3,3}(2, Z)$  on any subset of the real projective line. If  $k \neq -1, 0, \infty$  is one of the three vertices of the triangle in

the coset diagram, since  $(z)v = \frac{-1}{z+1}$ , then

- a. if  $z < -1$ , then  $(z)v > 0$ ,
- b. if  $z > 0$ , then  $-1 < (z)v < 0$ , and
- c. if  $-1 < z < 0$ , then  $(z)v < -1$ .

Thus, one of the vertices  $k, kv$  and  $kv^2$  one is positive and the other two are negative. Diagrammatically, it can be shown as:

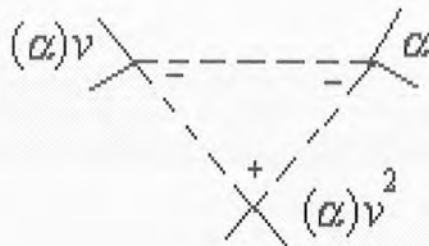


Fig-2.2

**Lemma 2.2.3**

Let  $k = \pm \frac{a}{b}$  where  $a, b$  are positive integers with no common factor. For  $k \neq 0, \infty$ , we define  $\|k\| = \max(|a|, |b|)$ , then

- a. if  $k$  is positive then,  $\|k\| < \|kv\|$  and  $\|k\| < \|kv^2\|$ , and
- b. if  $k$  is negative with  $b < 0$ , then  $\|k\| < \|ku\|$  and  $\|k\| < \|ku^2\|$ .

**Proof**

If  $k$  is positive, then  $(k)v = \frac{-b}{a+b}$  and  $(k)v^2 = \frac{-(a+b)}{a}$  and so  $\|k\| < \|kv\|$  and  $\|k\| < \|kv^2\|$ . Now if  $k$  is negative, then  $(k)u = \frac{a-b}{a}$  and  $(k)u^2 = \frac{-b}{a-b}$  and so  $\|k\| < \|ku\|$  and  $\|k\| < \|ku^2\|$ .

**Theorem 2.2.4**

The coset diagram for the action of  $G^{3,3}(2, Z)$  on the rational projective line is connected.

**Proof**

To prove this we need only to show that for any rational number  $k_0$  there is a path joining  $k_0$  to  $\infty$ .

Let  $k_0 = \frac{a}{b}$  be a positive rational number. Then  $(k_0)v^j = \frac{-b}{(a+b)}$  and  $\frac{-(a+b)}{a}$  for  $j=1$  or  $2$ . Then, by lemma 2.2.3,  $\|(k_0)v\| = (a+b)$  and  $\|(k_0)v^2\| = (a+b)$ , so,  $\|(k_0)v^j\| > \|k_0\|$  for  $j=1$  or  $2$  respectively. Similarly, if  $k_0 = \frac{a}{b}$  is a negative rational number with  $b < 0$ , then  $(k_0)u^i = \frac{a-b}{a}$  and  $\frac{-b}{a-b}$  for  $i=1$  or  $2$  respectively. That is,  $\|(k_0)u\| = (a-b)$  and  $\|(k_0)u^2\| = (a-b)$ . Hence  $\|(k_0)u^i\| > \|k_0\|$  for  $i=1$  or  $2$ .

If  $k_0$  is positive then one of  $(k_0)u^i$  for  $i=1$ , or  $2$  is negative. If we let this negative number to be  $k_1$  then  $\|k_0\| > \|k_1\|$ . As  $k_1$  is negative one of  $(k_1)v^j$ , where  $j=1, 2$  is positive. Let it be  $k_2$ , that is,  $k_2 = (k_1)v^j$  where  $j=1$  or  $2$ . This implies that  $\|k_1\| > \|k_2\|$ . If we continue in this way, we obtain a unique alternating sequence of positive and negative rational numbers  $k_0, k_1, k_2, \dots$  such that  $\|k_0\| > \|k_1\| > \|k_2\| \dots$



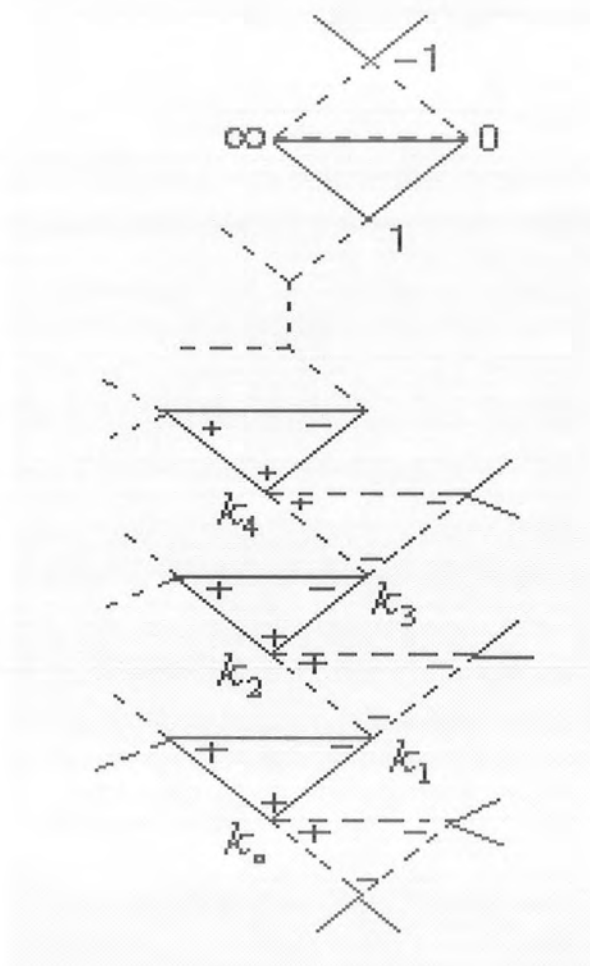


Fig-2.3

The decreasing sequence of positive integers must terminate, and it can terminate only because ultimately the directed path leads to a  $u$ -triangle (unbroken lines) with the vertices  $1, 0, \infty$  or  $v$ -triangle (broken lines) with the vertices  $-1, 0, \infty$ .

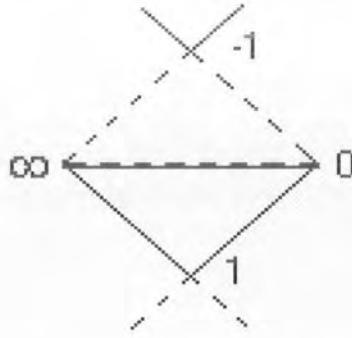


Fig-2.4

An alternating sequence of positive and negative rational numbers  $k_0, k_1, k_2, \dots$  such that  $\|k_0\| > \|k_1\| > \|k_2\| \dots$  shows that there is a directed graph joining  $k_0$  to  $\infty$ . This implies that every rational number occurs in the diagram and that diagram for the action of  $G^{3,3}(2, Z)$  on the rational projective line is connected.

**Theorem 2.2.5**

The action of  $G^{3,3}(2, Z)$  on the rational projective line is transitive.

**Proof**

We shall prove transitivity of the action by showing that if there is a path from a rational number  $p$  to a rational number  $q$  then there exists some  $g$  in  $G^{3,3}(2, Z)$  such that  $pg = q$ .

As we have shown in theorem 2.2.4 that there exists a path joining  $k_0$  to  $\infty$ , that is, there exists an element  $g_1 = u^{\epsilon_1} v^{\eta_1} u^{\epsilon_2} v^{\eta_2} \dots u^{\epsilon_i} v^{\eta_i}$  of  $G^{3,3}(2, Z)$  such



that  $\infty = pg_1 = p(u^{\varepsilon_1} v^{\eta_1} u^{\varepsilon_2} v^{\eta_2} \dots u^{\varepsilon_m} v^{\eta_m})$  where  $\varepsilon_i = 0, 1$  or  $2$  for  $i = 1, 2, \dots, m$  and  $\eta_j = 0, 1$  or  $2$ , where  $j = 1, 2, \dots, m$ . Similarly we can find another element  $g_2$  in  $G^{3,3}(2, Z)$  such that  $\infty = qg_2$ . Hence  $pg_1 = qg_2$  or  $pg_1 g_2^{-1} = q$ . That is, the action of  $G^{3,3}(2, Z)$  on the rational projective line is transitive.

In the following theorem, we shall show that  $u^3 = v^3 = 1$  are defining relations for  $G^{3,3}(2, Z)$ .

### Theorem 2.2.6

$u^3 = v^3 = 1$  are defining relations for  $G^{3,3}(2, Z)$ .

### Proof

Suppose  $u^3 = v^3 = 1$  are not defining relations of  $G^{3,3}(2, Z)$ . Then there is a relation of the form  $u^{\varepsilon_1} v^{\eta_1} u^{\varepsilon_2} v^{\eta_2} \dots u^{\varepsilon_m} v^{\eta_m} = 1$  where  $m \geq 1$ ,  $\varepsilon_i, \eta_j = 1$  or  $2$  and  $i, j = 1, 2, \dots, m$ . We know that neither  $u$  nor  $v$  can be 1.

The coset diagram (Fig-2.3) depicts that it does not contain any closed path. For if it contains a closed path and  $k_1, k_2, \dots, k_m$  are the vertices of the triangles in the diagram such that  $k_o > 0$ , then this leads to a contradiction  $\|k_o\| > \|k_1\| > \dots > \|k_m\| > \|k_o\|$ . So the coset diagram (Fig-2.3) does not contain any closed path.

This shows that there are points in the diagram whose 'distance' from the point  $\infty$  is arbitrarily large. Choose  $k > 0$ , so that the 'distance' from the point  $k_o$  to the point  $\infty$  is greater than  $m$ . Define  $k_i = ku^{\varepsilon_1} v^{\eta_1} u^{\varepsilon_2} v^{\eta_2} \dots u^{\varepsilon_i} v^{\eta_i}$  where

$i = 1, 2, \dots, m$ . Then  $\|k_0\| > \|k_1\| > \|k_2\| > \dots > \|k_m\|$  and in particular  $k_m \neq k_0$ . Thus  $u^{\varepsilon_1} v^{\eta_1} u^{\varepsilon_2} v^{\eta_2} \dots u^{\varepsilon_i} v^{\eta_i} \neq 1$  and so  $u^3 = v^3 = 1$  are defining relations for  $G^{3,3}(2, Z)$ .

This of course shows also that  $u^3 = v^3 = t^2 = (ut)^2 = (vt)^2 = 1$  are defining relations for  $G^{*3,3}(2, Z) = \langle u, v, t \rangle$ .

## CHAPTER THREE

### ACTION OF $G^{3,3}(2, Z)$ ON REAL AND IMAGINARY QUADRATIC FIELDS

#### 3.1 INTRODUCTION

In this chapter, we are interested in studying an action of the group  $G^{3,3}(2, Z) = \langle u, v : u^3 = v^3 = 1 \rangle$ , where  $u$  and  $v$  are linear-fractional transformations  $z \rightarrow \frac{z-1}{z}$  and  $z \rightarrow \frac{-1}{z+1}$  respectively on  $Q(\sqrt{n})$  and  $Q(\sqrt{-n})$  by using coset diagrams.

Let  $n$  be a non-square positive integer and  $Q(\sqrt{n})$  be a real quadratic field. Consider a subset  $Q^*(\sqrt{n}) = \left\{ \frac{a+\sqrt{n}}{c} : a, c \in Z, c \neq 0, b = \frac{a^2-n}{c} \in Z, (a, b, c) = 1 \right\}$  of  $Q(\sqrt{n})$ .

For a fixed non-square positive integer  $n$ , if the real quadratic irrational number  $\alpha = \frac{a+\sqrt{n}}{c}$  and its algebraic conjugate  $\bar{\alpha} = \frac{a-\sqrt{n}}{c}$  have different signs. Such an  $\alpha$  is known as an ambiguous number [23]. They play an important

role in classifying the orbits of  $G^{3,3}(2, Z)$  on  $Q(\sqrt{n})$ . In the action of  $G^{3,3}(2, Z)$  on  $Q(\sqrt{n})$ ,  $Stab_\alpha(G)$  are the only non-trivial stabilizers and in the orbit  $\alpha G^{3,3}(2, Z)$ ; there is only one (up to isomorphism). We have also classified all the ambiguous numbers in the orbit. If  $\alpha$  and  $\bar{\alpha}$  are both positive (negative),  $\alpha$  is called a totally positive (negative) number.

In this chapter, we explore some interesting group theoretic properties of this action vis-à-vis the orbit of  $\alpha$  in  $G^{3,3}(2, Z)$ . It is known that the set of ambiguous numbers is finite [23] and that the ambiguous numbers in the coset diagram for the orbit  $\alpha G^{3,3}(2, Z)$  form a closed path and it is the only closed path contained in it. We have classified all the ambiguous numbers in the orbit.

### 3.2 COSET DIAGRAMS FOR THE GROUP $G^{3,3}(2, Z)$

We use coset diagrams, as defined in chapter one, for the group  $G^{3,3}(2, Z)$  and study its action on the projective line over real and imaginary quadratic fields.

For the action of  $G^{3,3}(2, Z)$  on the projective line over a real quadratic field, we have the following observations:

- (i) If  $k \neq 1, 0, \infty$  then of the vertices  $k, ku$  and  $ku^2$  of a  $u$ -triangle, in a coset diagram for the action of  $G^{3,3}(2, Z)$  on any subset of the projective line, one vertex is negative and two are positive.



(ii) If  $k \neq -1, 0, \infty$  then of the vertices  $k, kv$  and  $kv^2$  of a  $v$ -triangle, in a coset diagram for the action of  $G^{3,3}(2, Z)$  on any subset of the projective line, one vertex is positive and two are negative.

(iii) Let  $k = \pm \frac{a}{b}$  where  $a, b$  are positive integers with no common factor.

For  $k \neq 0, \infty$  we define  $\|k\| = \max(|a|, |b|)$ .

(iv) Let  $\alpha$  be a totally positive quadratic number, then  $\alpha\bar{\alpha} = \frac{a^2 - n}{c^2} > 0$

implying that  $\frac{b}{c} > 0$ . Therefore, either  $b, c > 0$  or  $b, c < 0$ . If  $b, c > 0$ ,

then as  $\frac{a - \sqrt{n}}{c} > 0$  implies  $a - \sqrt{n} > 0$  or  $a > \sqrt{n}$  and so  $a > 0$ .

Now if  $b, c < 0$ , then as  $\frac{a + \sqrt{n}}{c} > 0$  implies  $a + \sqrt{n} < 0$  or  $a < -\sqrt{n}$

and so  $a < 0$ .

Thus  $\alpha$  is a totally positive quadratic number either  $a, b, c > 0$  or  $a, b, c < 0$ .

(v) Let  $\alpha$  be a totally negative quadratic number, then  $\alpha$  and  $\bar{\alpha}$  both are negative. Thus  $\alpha\bar{\alpha} = \frac{a^2 - n}{c^2} > 0$  implying that  $\frac{b}{c} > 0$ . Therefore,

either  $b, c > 0$  or  $b, c < 0$ . If  $b, c > 0$  then as  $\frac{a + \sqrt{n}}{c} < 0$  but  $c > 0$ .

Thus  $a + \sqrt{n} < 0$  or  $a < -\sqrt{n}$  and so  $a < 0$ . Now if  $b, c < 0$ , then as  $\frac{a - \sqrt{n}}{c} < 0$  but  $c < 0$ . Thus  $a - \sqrt{n} > 0$  or  $a > \sqrt{n}$  and so  $a > 0$ .

Thus  $\alpha$  is a totally negative quadratic number either  $a < 0$  and  $b, c > 0$  or  $a > 0$  and  $b, c < 0$ .

- (vi) Let  $\alpha$  be an ambiguous number, then  $\alpha$  and  $\bar{\alpha}$  both have opposite signs. Therefore,  $\alpha\bar{\alpha} = \frac{a^2 - n}{c} < 0$  implying that  $\frac{b}{c} < 0$  and so  $b$  and  $c$  have different signs and so  $bc < 0$ . Thus  $\alpha$  is an ambiguous number if  $bc < 0$ .

### Theorem 3.2.1

- (i) If  $\alpha$  is a totally negative quadratic number then  $(\alpha)u$  and  $(\alpha)u^2$  are both totally positive quadratic numbers.
- (ii) If  $\alpha$  is a totally positive quadratic number then  $(\alpha)v$  and  $(\alpha)v^2$  are both totally negative quadratic numbers.

### Proof

- (i) Let  $\alpha$  be a totally negative quadratic number. Then by observation (v), there are two possibilities either  $a < 0$  and  $b, c > 0$  or  $a > 0$  and  $b, c < 0$ .

Let  $a < 0$  and  $b, c > 0$ . We can easily tabulate the following information:

$\alpha$	$a$	$b$	$c$
$(\alpha)u$	$b - a$	$-2a + b + c$	$b$
$(\alpha)u^2$	$c - a$	$c$	$-2a + b + c$

From the above information we see that the new values of  $a, b$  and  $c$  for  $(\alpha)u$  and  $(\alpha)u^2$  are positive, therefore,  $(\alpha)u$  and  $(\alpha)u^2$  are totally positive quadratic numbers.

Now, let  $a > 0$  and  $b, c < 0$ . Then the new values of  $a, b$  and  $c$  for  $(\alpha)u$  and  $(\alpha)u^2$  are negative, therefore,  $(\alpha)u$  and  $(\alpha)u^2$  are totally positive quadratic numbers.

- (ii) Let  $\alpha$  be a totally positive quadratic number. Then by observation (iv), there are two possibilities either  $a, b, c > 0$  or  $a, b, c < 0$ .

Let  $a, b, c > 0$ . We can easily tabulate the following information:

$\alpha$	$a$	$b$	$c$
$(\alpha)v$	$-a-c$	$c$	$2a+b+c$
$(\alpha)v^2$	$-a-b$	$2a+b+c$	$b$

From the above information we see that the new value of  $a$  for  $(\alpha)v$  and  $(\alpha)v^2$  is negative and the new values of  $b$  and  $c$  for  $(\alpha)v$  and  $(\alpha)v^2$  are positive, therefore,  $(\alpha)v$  and  $(\alpha)v^2$  are totally negative quadratic numbers.

Now, let  $a, b, c < 0$ . Then the new value of  $a$  for  $(\alpha)v$  and  $(\alpha)v^2$  is positive and the new values of  $b$  and  $c$  for  $(\alpha)v$  and  $(\alpha)v^2$  are negative, therefore,  $(\alpha)v$  and  $(\alpha)v^2$  are totally negative quadratic numbers.

### 3.3 EXISTENCE OF AMBIGUOUS NUMBERS

The coset diagrams depicting an orbit of the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{n})$  do not contain a closed path unless there is an ambiguous number in the orbit. A closed path, if it exists, will evolve the element  $g = u^{\varepsilon_1} v^{\eta_1} u^{\varepsilon_2} v^{\eta_2} \dots u^{\varepsilon_n} v^{\eta_n}$  of  $G^{3,3}(2, Z)$ , where  $\varepsilon_1 = 0, 1$  or  $2$ , and  $\varepsilon_i = 1$  or  $2$ , for  $i = 2, 3, \dots, n$  and  $\eta_n = 0, 1$  or  $2$  and  $\eta_j = 1$  or  $2$ , where  $j = 1, 2, \dots, n-1$  fixing the element  $v_1$  of  $Q^*(\sqrt{n})$ .



Let  $\alpha \in Q^*(\sqrt{n})$  and  $\alpha G^{3,3}(2, Z)$  denote the orbit of  $\alpha$  in  $G^{3,3}(2, Z)$ . The existence of ambiguous numbers in  $\alpha G^{3,3}(2, Z)$  is related to the stabilizers of  $G^{3,3}(2, Z)$ . We describe the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{n})$  in the following theorems.

**Theorem 3.3.1**

- (i) If  $\alpha$  is an ambiguous number then one of  $(\alpha)u$  and  $(\alpha)u^2$  is ambiguous and the other is totally positive.
- (ii) If  $\alpha$  is an ambiguous number then one of  $(\alpha)v$  and  $(\alpha)v^2$  is ambiguous and the other is totally negative.

**Proof**

- (i) First we suppose that  $\alpha$  is a positive number. Then:

$\alpha$	$(\alpha)u$	$(\alpha)u^2$	$\bar{\alpha}$	$\overline{(\alpha)u}$	$\overline{(\alpha)u^2}$
+	-	+	-	+	+
+	+	-			

Similarly if  $\alpha$  is a negative number, then:

$\alpha$	$(\alpha)u$	$(\alpha)u^2$	$\bar{\alpha}$	$\overline{(\alpha)u}$	$\overline{(\alpha)u^2}$
-	+	+	+	-	+
			+	+	-

Therefore, from the above tables we can easily deduce that one of  $(\alpha)u$  and  $(\alpha)u^2$  is ambiguous and the other is totally positive.

(ii) First we suppose that  $\alpha$  is a positive number. Then:

$\alpha$	$(\alpha)v$	$(\alpha)v^2$	$\bar{\alpha}$	$\overline{(\alpha)v}$	$\overline{(\alpha)v^2}$
+	-	-	-	+	-
			-	-	+

Similarly if  $\alpha$  is a negative number, then:

$\alpha$	$(\alpha)v$	$(\alpha)v^2$	$\bar{\alpha}$	$\overline{(\alpha)v}$	$\overline{(\alpha)v^2}$
-	+	-	+	-	-
-	-	+			

Therefore from the above tables we can easily deduce that one of  $(\alpha)v$  and  $(\alpha)v^2$  is ambiguous and the other is totally negative.

### Theorem 3.3.2

The ambiguous numbers in the coset diagram for the orbit  $\alpha G^{3,3}(2, Z)$ , where  $\alpha = \frac{a + \sqrt{n}}{c} \in Q^*(\sqrt{n})$ , form a closed path and it is the only closed path contained in it.

### Proof

If  $k_0$  is an ambiguous number in  $\alpha G^{3,3}(2, Z)$ , then either  $(k_0)v^j$  is ambiguous or  $(k_0)u_i$  for  $i, j = 1$  or  $2$ . We may therefore assume that  $(k_0)v^j$  is an ambiguous number.

Due to theorem 3.3.1, each triangle representing three edges of  $v$  or  $u$  contains two ambiguous numbers, so within the  $k$ -th triangle, we successively apply  $u$  (or  $v$ ) to reach the next ambiguous number in the  $(k+1)$ th triangle.

Suppose the  $k$ -th triangle depicting the three cycles of the generator  $v$ , contains two ambiguous numbers, namely  $\alpha_1$  and  $\alpha_2$ . Then,  $\alpha_2^{(k-1)} = \alpha_1^{(k-1)}v^{\varepsilon_1}$ ,  $\alpha_2^k = \alpha_1^k u^{\varepsilon_2}$  and  $\alpha_2^{(k+1)} = \alpha_1^{(k+1)}v^{\varepsilon_3}$ , where  $\varepsilon_1, \varepsilon_2, \varepsilon_3 = 1$  or  $2$ . Also, since  $\alpha_2^{(k-1)} = \alpha_1^k$  and  $\alpha_2^k = \alpha_1^{(k+1)}$ , therefore,  $\alpha_1^{(k-1)}v^{\varepsilon_1}v^{\varepsilon_2}v^{\varepsilon_3} = \alpha_2^{(k+1)}$ . We can continue in this way and since by theorem 3 in [23] there are only a finite number

of ambiguous numbers, after a finite number of steps we reach the vertex (ambiguous number)  $\alpha_2^{(k+m)} = \alpha_1^{(k-1)}$ .

Hence the ambiguous numbers form a path in the coset diagram. The path is closed because there are only a finite number of ambiguous numbers in a coset diagram. Since only ambiguous numbers form a closed path and these are the only ambiguous numbers therefore they form a single closed path in the coset diagram of the orbit  $\alpha G^{3,3}(2, Z)$ .

### 3.4 CONCLUSION

We conclude this section with the following observations. If we are given a real quadratic irrational number  $\alpha$ , we can always find the closed path in the orbit  $\alpha G^{3,3}(2, Z)$ . If  $\alpha$  is totally negative then one of  $(\alpha)v^j$ , for  $j = 1$  or  $2$  is totally positive, and we can use theorem 5 [23] to find an ambiguous number in the same orbit. When we have an ambiguous number, the proof of theorem 3.3.2 shows how to construct the closed path. This means that if  $\alpha$  and  $\beta$  are two real quadratic irrational numbers, then we can test whether or not they belong to the same orbit. We can find closed paths in the orbits  $\alpha G^{3,3}(2, Z)$  and  $\beta G^{3,3}(2, Z)$  and see if they are same or not. Note that for a fixed value of  $n$ , a non-square positive integer, all possible ambiguous numbers do not lie in the same orbit.

### 3.5 ACTION OF $G^{3,3}(2, Z)$ ON IMAGINARY QUADRATIC FIELDS

The imaginary quadratic fields are defined by the set  $\{a + b\sqrt{-n} : a, b \in Q\}$  and denoted by  $Q(\sqrt{-n})$ , where  $n$  is a square-free positive integer. In this section, we have proved that if  $\alpha = \frac{a + \sqrt{-n}}{c} \in Q^*(\sqrt{-n}) = \{\frac{a + \sqrt{-n}}{c} : a, \frac{a^2 + n}{c}, c \in Z, c \neq 0\}$  then  $n$  does not change its value in the orbit  $\alpha G^{3,3}(2, Z)$ . Also we show that the number of orbits of  $Q^*(\sqrt{-n})$  under the action of  $G^{3,3}(2, Z)$  are  $2[d(n) + 2d(n+1) - 4]$  and  $2[d(n) + 2d(n+1) - 6]$  accordingly  $n$  is even or odd, except for  $n=3$  for which there are exactly eight orbits. Also, the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{-n})$  is always intransitive.

#### Theorem 3.5.1

If  $\alpha = \frac{a + \sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ , then  $n$  does not change its value in  $\alpha G^{3,3}(2, Z)$ .

#### Proof

Let  $\alpha = \frac{a + \sqrt{-n}}{c} \in Q^*(\sqrt{-n})$  and  $b = \frac{a^2 + n}{c}$ . Since  $(\alpha)u = \frac{\alpha - 1}{\alpha} = 1 - \frac{1}{\alpha} = 1 - \frac{c}{a + \sqrt{-n}} = \frac{b - a + \sqrt{-n}}{b}$ . Therefore, the new values of  $a$  and  $c$  for  $(\alpha)u$  are  $b - a$  and  $b$  respectively. The new value of  $b$  for  $(\alpha)u$  is

$$\frac{(b-a)^2 + n}{b} = -2a + b + c. \text{ Now } (\alpha)v = \frac{-1}{\alpha+1} = \frac{-c}{a+c+\sqrt{-n}} = \frac{-a-c+\sqrt{-n}}{b+c+2a}.$$

Therefore, the new values of  $a$  and  $c$  for  $(\alpha)v$  are  $-a-c$  and  $2a+b+c$

respectively. The new value of  $b$  for  $(\alpha)v$  is  $\frac{(-a-c)^2 + n}{2a+b+c} = c$ . Similarly, we can

calculate the new values of  $a, b$  and  $c$  for  $(\alpha)u^2$ ,  $(\alpha)v^2$ ,  $(\alpha)uv$ ,  $(\alpha)u^2v$ ,  $(\alpha)vu$ ,

$(\alpha)uv^2$ ,  $(\alpha)vu^2$  and  $(\alpha)v^2u$  as follows:

$\alpha$	$a$	$b$	$c$
$(\alpha)u$	$b - a$	$-2a + b + c$	$b$
$(\alpha)v$	$-a - c$	$c$	$2a + b + c$
$(\alpha)u^2$	$c - a$	$c$	$-2a + b + c$
$(\alpha)v^2$	$-a - b$	$2a + b + c$	$b$
$(\alpha)uv$	$a - 2b$	$b$	$-4a + 4b + c$
$(\alpha)u^2v$	$3a - b - 2c$	$-2a + b + c$	$-4a + b + 4c$
$(\alpha)vu$	$a + 2b$	$4a + b + 4c$	$c$
$(\alpha)uv^2$	$3a - 2b - c$	$-4a + 4b + c$	$-2a + b + c$
$(\alpha)vu^2$	$3a + b + 2c$	$2a + b + c$	$4a + b + 4c$
$(\alpha)v^2u$	$3a + 2b + c$	$4a + 4b + c$	$2a + b + c$



From the above information we see that all the elements of  $\alpha G^{3,3}(2, Z)$  are in  $Q^*(\sqrt{-n})$ . That is,  $n$  does not change its value in  $\alpha G^{3,3}(2, Z)$ .

As we know from [29] the real quadratic irrational numbers are fixed points of the elements of  $PSL(2, Z) = \langle x, y : x^2 = y^3 = 1 \rangle$  except for the group theoretic conjugates of  $x, y^{\pm 1}$  and  $(xy)^n$ . Now we want to see that when imaginary quadratic numbers are fixed points of the elements of  $G^{3,3}(2, Z)$ .

### 3.6 EXISTENCE OF FIXED POINTS IN $Q^*(\sqrt{-n})$ AND ORBITS OF $Q^*(\sqrt{-n})$

#### Remark 3.6.1

Let  $(z)u = z$ . This implies  $\frac{z-1}{z} = z$  gives  $z^2 - z + 1 = 0$ . Thus  $z = \frac{1 \pm \sqrt{-3}}{2} \in Q^*(\sqrt{-3})$ . Similarly,  $(z)v = z$  implies  $\frac{-1}{z+1} = z$ . So,  $z^2 + z + 1 = 0$  gives  $z = \frac{-1 \pm \sqrt{-3}}{2} \in Q^*(\sqrt{-3})$ .

#### Theorem 3.6.2

The fixed points under the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{-n})$  exist only if  $n = 3$ .



## Proof

Let  $g$  be a linear-fractional transformation in  $G^{3,3}(2, Z)$ . Therefore,  $(z)g$  can be taken as  $\frac{az+b}{cz+d}$ , where  $ad-bc=1$ . Let  $\frac{az+b}{cz+d}=z$  which gives us the quadratic equation  $cz^2+(d-a)z-b=0$ . It has the imaginary roots only if  $(d-a)^2+4bc<0$  or  $(d+a)^2-4(ad-bc)<0$  or  $(a+d)^2<4$ . That is,  $a+d=0, \pm 1$ .

If  $a+d=0$ , then  $g$  is an involution but there is not any involution in  $G^{3,3}(2, Z)$ . Now, if  $a+d=\pm 1$ , then as  $(\text{trace}(g))^2=\det(g)$ , order of  $g$  will be three and hence it is conjugate to the linear-fractional transformations  $u^{\pm 1}$  and  $v^{\pm 1}$ . Since the fixed points of the linear-fractional transformations  $u$  and  $v$  (by remark (3.6.1)) are  $\frac{1\pm\sqrt{-3}}{2}$  and  $\frac{-1\pm\sqrt{-3}}{2}$  respectively, therefore, the roots of the quadratic equation  $cz^2+(d-a)z-b=0$  belongs to the imaginary quadratic field  $Q^*(\sqrt{-3})$ . If two elements of  $G^{3,3}(2, Z)$  are conjugate, then their corresponding determinant are also equivalent.

### Definition 3.6.3

If  $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$  is such that  $ac < 0$  then  $\alpha$  is called a totally negative imaginary quadratic number and is called totally positive imaginary quadratic number if  $ac > 0$ .

As  $b = \frac{a^2 + n}{c}$ , therefore,  $bc$  is always positive. So,  $b$  and  $c$  have same sign. Hence an imaginary quadratic number  $\alpha = \frac{a + \sqrt{-n}}{c} \in Q^*(\sqrt{-n})$  is totally negative if either  $a < 0$  and  $b, c > 0$  or  $a > 0$  and  $b, c < 0$ . Similarly,  $\alpha = \frac{a + \sqrt{-n}}{c} \in Q^*(\sqrt{-n})$  is totally positive if either  $a, b, c > 0$  or  $a, b, c < 0$ .

### Theorem 3.6.4

- (i) If  $\alpha$  is a totally negative imaginary quadratic number then  $(\alpha)u$  and  $(\alpha)u^2$  are both totally positive imaginary quadratic numbers.
- (ii) If  $\alpha$  is a totally positive imaginary quadratic number then  $(\alpha)v$  and  $(\alpha)v^2$  are both totally negative imaginary quadratic numbers.

### Proof

- (i) Let  $\alpha = \frac{a + \sqrt{-n}}{c}$  be a totally negative imaginary quadratic number. Here are two possibilities either  $a < 0$  and  $b, c > 0$  or  $a > 0$  and  $b, c < 0$ .

Let  $a < 0$  and  $b, c > 0$ . We can easily tabulate the following information.

$\alpha$	$a$	$b$	$c$
$(\alpha)u$	$b - a$	$-2a + b + c$	$b$
$(\alpha)u^2$	$c - a$	$c$	$-2a + b + c$

From the above information, we see that the new values of  $a, b$  and  $c$  for  $(\alpha)u$  and  $(\alpha)u^2$  are positive, therefore,  $(\alpha)u$  and  $(\alpha)u^2$  are both totally positive imaginary quadratic numbers.

Now, let  $a > 0$  and  $b, c < 0$ . Then the new values of  $a, b$  and  $c$  for  $(\alpha)u$  and  $(\alpha)u^2$  are negative, therefore,  $(\alpha)u$  and  $(\alpha)u^2$  are both totally positive imaginary quadratic numbers.

- (ii) Let  $\alpha = \frac{a + \sqrt{-n}}{c}$  be a totally positive imaginary quadratic number. Here are two possibilities either,  $a, b, c > 0$  or  $a, b, c < 0$ .

Let  $a, b, c > 0$ . We can easily tabulate the following information.

$\alpha$	$a$	$b$	$c$
$(\alpha)v$	$-a - c$	$c$	$2a + b + c$
$(\alpha)v^2$	$-a - b$	$2a + b + c$	$b$

From the above information, we see that the new value of  $a$  for  $(\alpha)v$  and  $(\alpha)v^2$  is negative and the new values of  $b$  and  $c$  for  $(\alpha)v$  and  $(\alpha)v^2$  are positive, therefore,  $(\alpha)v$  and  $(\alpha)v^2$  are both totally negative imaginary quadratic numbers.

Now, let  $a, b, c < 0$ . Then the new value of  $a$  for  $(\alpha)v$  and  $(\alpha)v^2$  is positive and the new values of  $b$  and  $c$  for  $(\alpha)v$  and  $(\alpha)v^2$  are negative, therefore,  $(\alpha)v$  and  $(\alpha)v^2$  are both totally negative imaginary quadratic numbers.

The converse of the above theorem is not true. For example, there are triangles in which all three vertices are totally positive or all three vertices are totally negative.

**Theorem 3.6.5**

- (i) If  $\alpha = \frac{a + \sqrt{-n}}{c}$  where  $c > 0$  then the denominator of every element in  $\alpha G^{3,3}(2, Z)$  is also positive.
- (ii) If  $\alpha = \frac{a + \sqrt{-n}}{c}$  where  $c < 0$  then the denominator of every element in the orbit  $\alpha G^{3,3}(2, Z)$  is also negative.

### Proof

- (i) Since  $\alpha = \frac{a + \sqrt{-n}}{c}$  with  $c > 0$ , therefore,  $b$  is also positive. As  $b$  and  $c$  always have same sign. Using this fact, we can easily see from the information given in theorem 3.5.1 that every element in  $\alpha G^{3,3}(2, Z)$  has positive denominator.
- (ii) Since  $\alpha = \frac{a + \sqrt{-n}}{c}$  with  $c < 0$  therefore,  $b$  is also negative as  $b$  and  $c$  always have same sign. Using this fact we can easily see from the information given in theorem 3.5.1 that every element in  $\alpha G^{3,3}(2, Z)$  has negative denominator.

### Definition 3.6.6

For  $\alpha = \frac{a + \sqrt{-n}}{c} \in \mathcal{Q}^*(\sqrt{-n})$ , we define  $\|\alpha\| = |a|$ .

### Theorem 3.6.7

- (i) Let  $\alpha$  be a totally negative imaginary quadratic number. Then  $\|(\alpha)u\| > \|\alpha\|$  and  $\|(\alpha)u^2\| > \|\alpha\|$ , and

- (ii) Let  $\alpha$  be a totally positive imaginary quadratic number. Then  $\|(\alpha)v\| > \|\alpha\|$  and  $\|(\alpha)v^2\| > \|\alpha\|$ .

**Proof**

- (i) Let  $\alpha$  be a totally negative imaginary quadratic number. Then either,  $a < 0$  and  $b, c > 0$  or  $a > 0$  and  $b, c < 0$ . Let us take  $a < 0$  and  $b, c > 0$ . Then, by theorem 3.6.4(i),  $(\alpha)u$  and  $(\alpha)u^2$  both are totally positive imaginary quadratic numbers. Thus,  $\|(\alpha)u\| = |b - a| > |a| = \|\alpha\|$ , and  $\|(\alpha)u^2\| = |c - a| > |a| = \|\alpha\|$ . Similarly, we have the same result for  $a > 0$  and  $b, c < 0$ .

- (ii) Let  $\alpha$  be a totally positive imaginary quadratic number. Then either,  $a, b, c > 0$  or  $a, b, c < 0$ . Let us take  $a, b, c > 0$ . Now using the information given in theorem 3.5.1, we can easily see that  $\|(\alpha)v\| = |-a - c| = |a + c| > |a| = \|\alpha\|$ , and  $\|(\alpha)v^2\| = |-a - b| = |a + b| > |a| = \|\alpha\|$ . Similarly, we have the same result for  $a, b, c < 0$ .

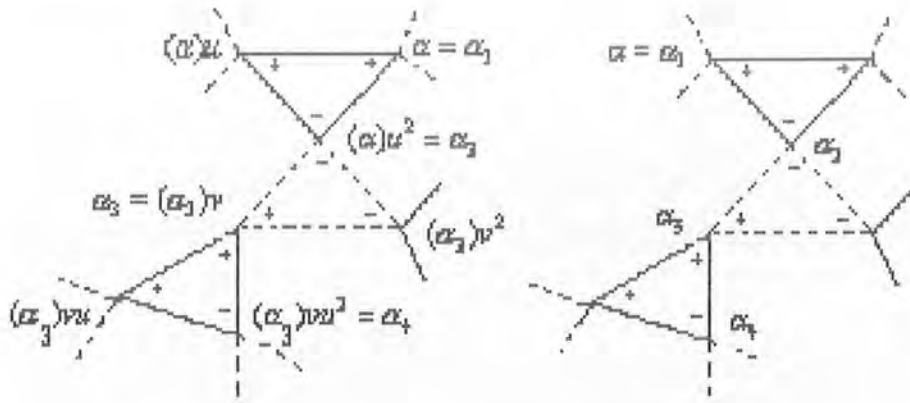
**Theorem 3.6.8**

Let  $\alpha$  be a totally positive or negative imaginary quadratic number. Then there exists a sequence  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_m$  such that  $\alpha_i$  is alternately totally negative and totally positive number for  $i = 1, 2, 3, \dots, m - 1$  and  $\|\alpha_m\| = 0$  or 1.

## Proof

Let  $\alpha = \alpha_1$  be a totally positive imaginary quadratic number, then, by theorem 3.6.4(i),  $(\alpha)u$  or  $(\alpha)u^2$  is totally negative imaginary quadratic number. If  $(\alpha)u$  is totally negative imaginary quadratic number, then put  $\alpha_2 = (\alpha)u$  and by theorem 3.6.7 (i),  $\|\alpha_1\| > \|\alpha_2\|$ . Now if  $(\alpha)u^2$  is totally negative imaginary quadratic number, then put  $\alpha_2 = (\alpha)u^2$ . In this case we have also  $\|\alpha_1\| > \|\alpha_2\|$ .

Now if  $(\alpha)u$  is totally negative imaginary quadratic number, then  $(\alpha)uv$  or  $(\alpha)uv^2$  is totally positive imaginary quadratic number. If  $(\alpha)uv$  is totally positive imaginary quadratic number, put  $(\alpha)uv = \alpha_3$  and so by theorem 3.6.7(ii),  $\|(\alpha)uv\| < \|(\alpha)u\| < \|\alpha\|$  or  $\|\alpha_3\| < \|\alpha_2\| < \|\alpha_1\|$  and continue in this way we obtain an alternate sequence  $\alpha_1, \alpha_2, \dots, \alpha_m$  of totally positive and totally negative numbers such that  $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \dots > \|\alpha_m\|$ . Since  $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \dots, \|\alpha_m\|$  is a decreasing sequence of non negative integers, therefore, it must terminate and that happens only when ultimately we reach at an imaginary quadratic number  $\alpha_m = \frac{a' + \sqrt{-n}}{c}$  such that  $\|\alpha_m\| = |a'| = 0$  or 1. It can be shown diagrammatically as:



### Theorem 3.6.9

There are exactly eight orbits of  $Q^*(\sqrt{-n})$  under the action of the group  $G^{3,3}(2, Z)$  for  $n = 3$ .

### Proof

As we have seen in theorem 3.6.8, we get a decreasing sequence of non negative integers  $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \dots, \|\alpha_m\|$  such that  $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \dots > \|\alpha_m\|$  which must terminate and that happens only when ultimately we reach at an imaginary quadratic number  $\alpha_m = \frac{a' + \sqrt{-3}}{c}$  such that  $\|\alpha_m\| = |a'| = 0$  or 1.

If  $\alpha_m = \frac{1 \pm \sqrt{-3}}{2}$  or  $\frac{-1 \pm \sqrt{-3}}{2}$  then because  $\frac{\pm 1 \pm \sqrt{-3}}{2}$  are the fixed points of  $u$  and  $v$ , therefore, we can not reach at an imaginary quadratic number whose norm is equal to zero. So in this case there are four orbits, namely,



$$\frac{1+\sqrt{-3}}{2}G^{3,3}(2,Z), \quad \frac{1-\sqrt{-3}}{2}G^{3,3}(2,Z), \quad \frac{-1+\sqrt{-3}}{2}G^{3,3}(2,Z) \quad \text{and}$$

$$\frac{-1-\sqrt{-3}}{2}G^{3,3}(2,Z) \text{ of } \mathcal{Q}^*(\sqrt{-3}).$$

Now, if we reach at an imaginary quadratic number  $\alpha_m = \frac{a' + \sqrt{-3}}{c}$  such that  $\|\alpha_m\| = |a'| = 0$ , then  $\alpha_m = \frac{\sqrt{-3}}{c}$ . Since  $\alpha_m = \frac{\sqrt{-3}}{c} \in \mathcal{Q}^*(\sqrt{-3})$ , therefore  $c = \pm 1, \pm 3$ . That is,  $\alpha_m = \frac{\sqrt{-3}}{1}, \frac{\sqrt{-3}}{-1}, \frac{\sqrt{-3}}{3}$  and  $\frac{\sqrt{-3}}{-3}$ .



Now, if  $\alpha = \frac{\sqrt{-3}}{1}$ , we can easily calculate the values of  $a, b$  and  $c$  as:

$\alpha$	0	3	1
$(\alpha)u$	3	4	3
$(\alpha)v$	-1	1	4
$(\alpha)u^2$	1	1	4
$(\alpha)v^2$	-3	4	3

Hence, from the above table,  $\sqrt{-3}, \frac{1+\sqrt{-3}}{4}$  and  $\frac{-1+\sqrt{-3}}{4}$  lie in  $\alpha G^{3,3}(2,Z)$ .

Similarly, if  $\alpha = \frac{\sqrt{-3}}{-1}$ , then  $-\sqrt{-3}, \frac{-1+\sqrt{-3}}{-4}$  and  $\frac{1+\sqrt{-3}}{-4}$  lie in  $\alpha G^{3,3}(2, Z)$ , if  $\alpha = \frac{\sqrt{-3}}{3}$ , then  $\frac{\sqrt{-3}}{3}, \frac{1+\sqrt{-3}}{1}$  and  $\frac{-1+\sqrt{-3}}{1}$  lie in  $\alpha G^{3,3}(2, Z)$ , and if  $\alpha = \frac{\sqrt{-3}}{-3}$ , then  $\frac{\sqrt{-3}}{-3}, \frac{1+\sqrt{-3}}{-1}$  and  $\frac{-1+\sqrt{-3}}{-1}$  lie in  $\alpha G^{3,3}(2, Z)$ .

Thus,  $\frac{\sqrt{-3}}{1}, \frac{\sqrt{-3}}{-1}, \frac{\sqrt{-3}}{3}$  and  $\frac{\sqrt{-3}}{-3}$  lie in four different orbits. Hence there are exactly eight orbits of  $Q^*(\sqrt{-3})$ .

**Remark 3.6.10**

(i) If  $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ , then  $Stab_\alpha(G)$  is non-trivial only if  $n=3$ .

Particularly, if  $\alpha = \frac{\pm 1 \pm \sqrt{-3}}{2}$  then  $Stab_\alpha(G) \cong C_3$ .

(ii) In  $Q^*(\sqrt{-3})$ , there are four elements of norm zero, namely,  $\frac{\sqrt{-3}}{1}, \frac{\sqrt{-3}}{-1}, \frac{\sqrt{-3}}{3}$  and  $\frac{\sqrt{-3}}{-3}$ .

(iii) In  $Q^*(\sqrt{-3})$ , there are twelve elements of norm one, namely,  $\frac{\pm 1 \pm \sqrt{-3}}{2}, \frac{\pm 1 \pm \sqrt{-3}}{4}$  and  $\frac{\pm 1 \pm \sqrt{-3}}{1}$ .

### Theorem 3.6.11

Let  $\alpha \in Q^*(\sqrt{-n})$ , where  $n \neq 3$ , then

- (i) if  $\alpha = \sqrt{-n}$ , then  $\sqrt{-n}$ ,  $\frac{1+\sqrt{-n}}{n+1}$  and  $\frac{-1+\sqrt{-n}}{n+1}$  lie in  $\alpha G^{3,3}(2, Z)$ ,
- (ii) if  $\alpha = \frac{\sqrt{-n}}{n}$ , then  $\frac{\sqrt{-n}}{n}$ ,  $\frac{1+\sqrt{-n}}{1}$  and  $\frac{1+\sqrt{-n}}{1}$  lie in  $\alpha G^{3,3}(2, Z)$ ,
- (iii) if  $\alpha = \frac{\sqrt{-n}}{2}$ , where  $n$  is even, then  $\alpha$  is the only element of norm zero in  $\alpha G^{3,3}(2, Z)$ ,
- (iv) if  $\alpha = \frac{\sqrt{-n}}{n_1}$ , where  $k_1 = \frac{n}{n_1}$  and  $n_1 \neq 1$  or  $n$ , then  $\alpha$  is the only element of norm zero in  $\alpha G^{3,3}(2, Z)$ , and
- (v) if  $\alpha = \frac{1+\sqrt{-n}}{c_1}$ , where  $1+n=c_1c_2$  and  $c_1 \neq 1$  or  $n+1$ , then  $\alpha$  is the only element of norm one in  $\alpha G^{3,3}(2, Z)$ .

**Proof**

(i) Let  $\alpha = \sqrt{-n}$ , then we can easily tabulate the following information.

$\alpha$	0	$n$	1
$(\alpha)u$	$n$	$n+1$	$n$
$(\alpha)v$	-1	1	$n+1$
$(\alpha)u^2$	1	1	$n+1$
$(\alpha)v^2$	$-n$	$n+1$	$n$

Hence, from the above table, we see that  $\sqrt{-n}$ ,  $\frac{1+\sqrt{-n}}{n+1}$  and  $\frac{-1+\sqrt{-n}}{n+1}$  lie in  $\alpha G^{3,3}(2, Z)$ .

(ii) if  $\alpha = \frac{\sqrt{-n}}{n}$ , then we can calculate the new values of  $a, b$  and  $c$  as:

$\alpha$	0	1	$n$
$(\alpha)u$	1	$n+1$	1
$(\alpha)v$	$-n$	$n$	$n+1$
$(\alpha)u^2$	$n$	$n$	$n+1$
$(\alpha)v^2$	$-1$	$n+1$	1

Hence, from the above table, we see that  $\frac{\sqrt{-n}}{n}$ ,  $\frac{1+\sqrt{-n}}{1}$  and  $\frac{-1+\sqrt{-n}}{1}$  lie in  $\alpha G^{3,3}(2, Z)$ .

- (iii) If  $\alpha = \frac{\sqrt{-n}}{2}$ , and  $l = \frac{n}{2}$ , then we can calculate the new values of  $a, b$  and  $c$  as:

$\alpha$	0	$l_1$	2
$(\alpha)u$	$l_1$	$l_1+2$	$l_1$
$(\alpha)v$	$-2$	2	$l_1+2$
$(\alpha)u^2$	2	2	$l_1+2$
$(\alpha)v^2$	$-l_1$	$l_1+2$	$l_1$

Hence, from the above table, we see that  $\alpha$  is the only element of norm zero in  $\alpha G^{3,3}(2, Z)$ .

(iv) Let  $\alpha = \frac{\sqrt{-n}}{n_1}$ , where  $k_1 = \frac{n}{n_1}$  and  $n_1 \neq 1$  or  $n$ , then

$\alpha$	0	$k_1$	$n_1$
$(\alpha)u$	$k_1$	$n_1 + k_1$	$k_1$
$(\alpha)v$	$-n_1$	$n_1$	$n_1 + k_1$
$(\alpha)u^2$	$n_1$	$n_1$	$n_1 + k_1$
$(\alpha)v^2$	$-k_1$	$n_1 + k_1$	$k_1$

Hence, from the above table, we see that  $\alpha$  is the only element of norm zero in  $\alpha G^{3,3}(2, Z)$ .

(v) Now if  $\alpha = \frac{1 + \sqrt{-n}}{c_1}$ , where  $1 + n = c_1 c_2$  and  $c_1 \neq 1$  or  $n + 1$ , then the new values of  $a, b$  and  $c$  can be calculated as:

$\alpha$	1	$c_2$	$c_1$
$(\alpha)u$	$c_2 - 1$	$-2 + c_1 + c_2$	$c_2$
$(\alpha)v$	$-1 - c_1$	$c_1$	$2 + c_1 + c_2$
$(\alpha)u^2$	$c_1 - 1$	$c_1$	$-2 + c_1 + c_2$
$(\alpha)v^2$	$-1 - c_2$	$2 + c_1 + c_2$	$c_2$

If  $c_1 = 2$ , then  $\|(\alpha)u^2\| = 1$  implies that  $(\alpha)u^2 = \frac{1 + \sqrt{-n}}{c_2}$ . If  $c_1 = -2$ , then  $\|(\alpha)v\| = 1$  implies that  $(\alpha)v = \frac{1 + \sqrt{-n}}{c_2}$ . That is,  $\frac{1 + \sqrt{-n}}{2}$  and  $\frac{1 + \sqrt{-n}}{\frac{n+1}{2}}$  lie in the same orbit, and  $\frac{1 + \sqrt{-n}}{-2}$  and  $\frac{1 + \sqrt{-n}}{-\frac{n+1}{2}}$  lie in the same orbit.

Now, if  $c_1 \neq 1, 2$  or  $\frac{n+1}{2}, n+1$ , that is,  $c_2 \neq n+1, \frac{n+1}{2}$  or 1. Then  $\frac{1 + \sqrt{-n}}{c_1}$  and  $\frac{-1 + \sqrt{-n}}{c_2}$  lie in  $\alpha G^{3,3}(2, Z)$ .

### Example 3.6.12

Let us find the orbits of  $Q^*(\sqrt{-14})$  by using the theorem 3.6.11.

(i)  $\sqrt{-14}$ ,  $\frac{1+\sqrt{-14}}{15}$  and  $\frac{-1+\sqrt{-14}}{15}$  lie in one orbit.

(ii)  $\frac{\sqrt{-14}}{-1}$ ,  $\frac{1+\sqrt{-14}}{-15}$  and  $\frac{-1+\sqrt{-14}}{-15}$  lie in one orbit.

(iii)  $\frac{\sqrt{-14}}{14}$ ,  $\frac{1+\sqrt{-14}}{1}$  and  $\frac{-1+\sqrt{-14}}{1}$  lie in one orbit.

(iv)  $\frac{\sqrt{-14}}{-14}$ ,  $\frac{1+\sqrt{-14}}{-1}$  and  $\frac{-1+\sqrt{-14}}{-1}$  lie in one orbit.

(v)  $\frac{\sqrt{-14}}{2}$  lies in one orbit.

(vi)  $\frac{\sqrt{-14}}{-2}$  lies in one orbit.

(vii)  $\frac{\sqrt{-14}}{7}$  lies in one orbit.

(viii)  $\frac{\sqrt{-14}}{-7}$  lies in one orbit.

(ix)  $\frac{1+\sqrt{-14}}{3}$  lies in one orbit.



(x)  $\frac{-1+\sqrt{-14}}{3}$  lies in one orbit.

(xi)  $\frac{1+\sqrt{-14}}{-3}$  lies in one orbit.

(xii)  $\frac{-1+\sqrt{-14}}{-3}$  lies in one orbit.

(xiii)  $\frac{1+\sqrt{-14}}{5}$  lies in one orbit.

(xiv)  $\frac{-1+\sqrt{-14}}{5}$  lies in one orbit.

(xv)  $\frac{1+\sqrt{-14}}{-5}$  lies in one orbit.

(xvi)  $\frac{-1+\sqrt{-14}}{-5}$  lies in one orbit.

So, there are sixteen orbits of  $Q^*(\sqrt{-n})$  for  $n = 14$ .

**Remark 3.6.13**

- (i) If  $\alpha = \frac{a + \sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ , then  $\alpha G^{3,3}(2, Z)$  does not contain the conjugates of the elements of  $\alpha G^{3,3}(2, Z)$ . Since  $\alpha = \frac{a + \sqrt{-n}}{c}$  and  $\bar{\alpha} = \frac{a - \sqrt{-n}}{c}$  lie in two different orbits. Therefore,  $\alpha G^{3,3}(2, Z)$  and  $\bar{\alpha} G^{3,3}(2, Z)$  are always disjoint.
- (ii) The elements of norm zero and one in  $Q^*(\sqrt{-n})$ , play a vital role to identify the orbits of  $Q^*(\sqrt{-n})$ .

**Definition 3.6.14**

If  $n$  is a positive integer then  $d(n)$  denotes the arithmetic function defined by the number of positive divisors of  $n$ .

**Theorem 3.6.15**

If  $n \neq 3$ , then the total number of orbits of  $Q^*(\sqrt{-n})$  under the action of  $G^{3,3}(2, Z)$  are:

(i)  $2[d(n) + 2d(n+1) - 6]$  if  $n$  is odd, and

(ii)  $2[d(n) + 2d(n+1) - 4]$  if  $n$  is even.

### Proof

First suppose that  $n$  is odd, then  $n+1$  is even. Let the divisors of  $n$  are  $\pm 1, \pm n_1, \pm n_2, \pm \dots \pm n$  and the divisors of  $n+1$  are  $\pm 1, \pm 2, \pm m_1, \pm m_2, \pm \dots \pm (\frac{n+1}{2}), \pm (n+1)$ . Then by theorem 3.6.11(i), there exist two orbits of  $Q^*(\sqrt{-n})$  corresponding to the divisors  $\pm 1$  of  $n$  and  $\pm (n+1)$  of  $n+1$ . By theorem 3.6.11(ii), there exists two orbits of  $Q^*(\sqrt{-n})$  corresponding to the divisors  $\pm n$  of  $n$  and  $\pm 1$  of  $n+1$ . By theorem 3.6.11(v), there exists two orbits of  $Q^*(\sqrt{-n})$  corresponding to the divisors  $\pm 2, \pm (\frac{n+1}{2})$  of  $n+1$ . Now we are left with  $2d(n) - 4$  divisors of  $n$  and  $4d(n+1) - 16$  divisors of  $n+1$ . Thus total orbits are  $2d(n) - 4 + 4d(n+1) - 16 + 8 = 2d(n) + 4d(n+1) - 12 = 2[d(n) + 2d(n+1) - 6]$ .

Now, if  $n$  is even, then the total orbits are  $[2(d(n) - 4) + [4d(n+1) - 8] + 4 = 2d(n) + 4d(n+1) - 8 = 2[d(n) + 2d(n+1) - 4]$ .

### Example 3.6.16

Now, by using above theorem, the orbits of  $Q^*(\sqrt{-14})$  and  $Q^*(\sqrt{-15})$  are:

(i) The orbits of  $Q^*(\sqrt{-14})$  are:

$$2[d(n) + 2d(n+1) - 4] = 2[d(14) + 2d(15) - 4] = 2[4 + 8 - 4] = 16.$$

(ii) The orbits of  $Q^*(\sqrt{-15})$  are:

$$2[d(n) + 2d(n+1) - 6] = 2[d(15) + 2d(16) - 6] = 2[4 + 10 - 6] = 16.$$

### Theorem 3.6.17

There are  $2d(n)$  elements of  $Q^*(\sqrt{-n})$  of norm zero.

### Proof

Let  $\alpha_m = \frac{a' + \sqrt{-n}}{c} \in Q^*(\sqrt{-n})$  such that  $\|\alpha_m\| = |a'| = 0$ , then  $\alpha_m = \frac{\sqrt{-n}}{c}$ .

Since  $\alpha_m = \frac{\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ , where  $b = \frac{a^2 + n}{c} = \frac{n}{c}$ , that is,  $c$  must be a divisor of

$n$ . Hence there are  $2d(n)$  elements of  $Q^*(\sqrt{-n})$  of norm zero.

### Theorem 3.6.18

There are  $4d(n+1)$  elements of  $Q^*(\sqrt{-n})$  of norm one.

**Proof**

Let  $\alpha_m = \frac{a' + \sqrt{-n}}{c} \in Q^*(\sqrt{-n})$  such that  $\|\alpha_m\| = |a'| = 1$ , then  $\alpha_m = \frac{\pm 1 + \sqrt{-n}}{c}$ , where  $b = \frac{a^2 + n}{c} = \frac{1+n}{c}$ , that is,  $c$  must be a divisor of  $n+1$ .

Hence there are  $4d(n+1)$  elements of  $Q^*(\sqrt{-n})$  of norm one.

**Theorem 3.6.19**

The action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{-n})$  is intransitive.



**Proof**

If  $n$  is even, then the minimum value of  $n$  in  $Q^*(\sqrt{-n})$  is 2. So, by theorem 3.6.15, the total orbits are  $2[d(n) + 2d(n+1) - 4] = 2[2 + 2(2) - 4] = 4$ . So, the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{-n})$  must be intransitive.

Now, if  $n$  is odd, then the minimum value of  $n$  in  $Q^*(\sqrt{-n})$  is five, when  $n \neq 3$ . So, by theorem 3.6.15, the total orbits are  $2[d(n) + 2d(n+1) - 6] = 2[2 + 2(4) - 6] = 8$ . So, the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{-n})$  must be intransitive.

According to theorem 3.6.9, there are exactly eight orbits of  $Q^*(\sqrt{-n})$  when  $n=3$  under the action of the group  $G^{3,3}(2, Z)$ .

Thus, the action of  $G^{3,3}(2, Z)$  on  $Q^*(\sqrt{-n})$  is intransitive.

So, far, we have considered action of  $G^{3,3}(2, Z)$  on  $Q(\sqrt{n})$  and  $Q(\sqrt{-n})$ . In this case, coset diagrams were infinite, that is, the number of vertices are infinite. Now in chapters four and five, we consider coset diagrams for the action of  $G^{3,3}(2, Z)$  on  $PL(F_q)$ . Here we get coset diagrams of finite order, that is, coset diagrams with finite number of vertices.

We are going to consider actions of  $G^{3,3}(2, Z)$  on  $PL(F_q)$ . But first notice that there is a projection of  $PL(Q)$  onto  $PL(F_q)$ . Here, if  $l = \frac{m}{n}$  is a rational number in the lowest terms, then  $l$  maps on  $\frac{\bar{m}}{\bar{n}}$ , where bars indicating, taking residues modulo prime  $p$ , unless  $\bar{n} = 0$ , when  $l$  maps on  $\infty$ . If  $g : z \rightarrow \frac{az + b}{cz + d}$  is any element of the group  $G^{3,3}(2, Z)$ , or indeed any element of  $GL(2, Q)$  whose determinant is a unit modulo  $p$ , then  $g$  can be taken to act on  $PL(F_q)$  by  $z \rightarrow \frac{\bar{a}z + \bar{b}}{\bar{c}z + \bar{d}}$  and this projection commutes with the action of  $G^{3,3}(2, Z)$ . Thus the coset diagram for the action of  $G^{3,3}(2, Z)$  on  $PL(F_q)$  can be obtained from the coset diagram for the action of  $G^{3,3}(2, Z)$  on  $PL(Q)$  by identifying appropriate points. The projection also commutes with  $t : z \rightarrow \frac{1}{z}$ , so that the diagram for the action of  $G^{3,3}(2, Z)$  admits an axis of symmetry such that reflection in this axis expresses the action  $t$ .

Next notice that for appropriate  $\theta$ ,  $p$ , the coset diagram for the action of  $G^{3,3}(2, Z)$  on  $PL(F_q)$  will also be an image under a projection of the diagram for the orbit  $\sigma G^{3,3}(2, Z)$ . In fact, if the positive square free integer  $n$  is a quadratic residue modulo  $p$  (and  $p$  does not divide  $2n$ ) then in the integer ring  $R$  of the field  $Q(\sqrt{n})$ ,  $p$  factorizes as the product of two distinct primes  $p_1$  and  $p_2$ , and  $\frac{R}{p_i}$  ( $i = 1, \text{ or } 2$ ) is naturally isomorphic to  $z \rightarrow \frac{Z}{qZ} = F_q$ . Thus, we can construct two distinct projection from  $PL(Q\sqrt{n})$  to  $PL(F_q)$  using the primes  $p_1$  and  $p_2$  in the same way that we used the prime  $p$  previously ( $R$  is not necessarily a principle integral domain); so we cannot talk about writing an element  $r$  in  $Q(\sqrt{n})$  as a fraction  $\frac{a}{b}$  in lowest terms; but  $R$  is a Dedekind domain so that if  $p_i$  is a prime ideal of  $R$ , any element  $l$  of  $R$  can be written as  $\frac{a}{b}$  when  $p_i$  does not divide both  $a$  and  $b$ . This all that is necessary to construct the projection.

## CHAPTER FOUR

### PARAMETRIZATION OF ACTIONS OF $G^{*3,n}(2, Z)$

#### 4.1 INTRODUCTION

In this chapter, we have considered conjugacy classes, which arise from the actions of  $\Delta(3, n, k) = \langle u_1, v_1 : u_1^3 = v_1^n = (u_1 v_1)^k = 1 \rangle$  on projective line over  $PL(F_q)$ . Also, we have proved that a one-to-one correspondence can be established between the conjugacy classes of non-degenerate homomorphisms  $\sigma : G^{*3,n}(2, Z) \rightarrow G^{*3,n}(2, q)$ , under the action of inner automorphisms of  $G^{*3,n}(2, q)$ , and the non-trivial conjugacy classes of elements of  $G^{*3,n}(2, q)$  such that the correspondence assigns to any non-degenerate homomorphism  $\sigma$  the class containing  $(u_1 v_1)\sigma$ . Of course this means that we can in fact parametrize the actions of  $G^{*3,n}(2, Z)$  on  $PL(F_q)$ . Also we have considered the conjugacy classes which arise from the actions of  $\Delta(3, n, k)$  on the projective line over  $PL(F_q)$ .

In the last section, we find a condition in the form of a polynomial with integer coefficients for the existence of actions of  $\langle u_1, v_1, t : u_1^3 = v_1^n = t^2 = (u_1 v_1)^2 = (v_1 t)^2 = 1 \rangle$  on  $PL(F_q)$ , which yield



$\Delta(3, n, k)$  as groups of permutations defined on  $PL(F_q)$ , where  $q$  is a prime congruent to  $\pm 1$  modulus  $k$ .

Let  $G^{3,n}(2, Z)$  be the group of linear-fractional transformations of the form  $z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in Z$  and  $ad - bc = 1$ , generated by  $u_1, v_1$  satisfying the relations:

$$u_1^3 = v_1^n = 1 \quad (4.1.1)$$

The linear-fractional transformation  $t : z \rightarrow \frac{1}{z}$  inverts both  $u_1$  and  $v_1$ , that is,  $t^2 = (u_1 t)^2 = (v_1 t)^2 = 1$  and so extends the group  $G^{3,n}(2, Z)$  to  $G^{*3,n}(2, Z)$ . The extended group  $G^{*3,n}(2, Z)$  is then the group of transformations of the form:

$$z \rightarrow \frac{az+b}{cz+d} \quad (4.1.2)$$

where  $a, b, c, d \in Z$  and  $ad - bc = \pm 1$  and its defining relations are of the form

$$u_1^3 = v_1^n = t^2 = (u_1 t)^2 = (v_1 t)^2 = 1 > \quad (4.1.3)$$

The group  $G^{*3,n}(2, q)$  is then the group of linear-fractional transformations of the form  $z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in F_q$  and  $ad - bc \neq 0$ , while  $G^{3,n}(2, q)$  is its subgroup consisting of all those linear-fractional transformations of the form  $z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in F_q$  and  $ad - bc$  is a non-zero square in  $F_q$ .

The group  $\Delta(3, n, k)$  is the triangle group with presentation  $\langle u_1, v_1 : u_1^3 = v_1^n = (u_1 v_1)^k = 1 \rangle$ . By adjoining an involution  $t$ , which inverts both  $u_1$  and  $v_1$ , the groups  $\Delta(3, n, k)$  can be extended to the triangle groups  $\Delta^*(3, n, k) = \langle u_1, v_1, t : u_1^3 = v_1^n = (u_1 v_1)^k = t^2 = (u_1 t)^2 = (v_1 t)^2 = 1 \rangle$ . The triangle group  $\Delta(3, n, k)$  is of index 2 in  $\Delta^*(3, n, k)$  and so is normal in  $\Delta^*(3, n, k)$ . The group  $\Delta^*(2, n, k)$  has Coxeter group  $G^{k,l,m} = \langle x, y, t : x^2 = y^k = (xy)^l = t^2 = (xt)^2 = (yt)^2 = (xyt)^m = 1 \rangle$  as its factor group [13].

## 4.2 CONJUGACY CLASSES OF THE NON-DEGENERATE HOMOMORPHISMS

The homomorphism  $\sigma : G^{*3,n}(2, Z) \rightarrow G^{*3,n}(2, q)$  amounts to choosing  $\bar{u}_1 = u_1\sigma, \bar{v}_1 = v_1\sigma$  and  $\bar{t} = t\sigma$  in  $G^{*3,n}(2, q)$ , such that

$$\bar{u}_1^3 = \bar{v}_1^n = \bar{t}^2 = (u_1 t)^2 = (v_1 t)^2 = 1 \quad (4.2.1)$$

We call  $\sigma$  to be non-degenerate homomorphism with the condition that the orders of  $u_1$  and  $v_1$  are the same as orders of  $(u_1)\sigma$  and  $(v_1)\sigma$  respectively, we mean neither of the generators  $u_1, v_1$  of  $G^{*3,n}(2, Z)$  lies in the kernel of  $\sigma$ , so that their images  $\bar{u}_1$  and  $\bar{v}_1$  are of orders 3 and  $n$  respectively. Both  $G^{3,n}(2, Z)$  and  $G^{*3,n}(2, Z)$  have index 2 in their automorphism groups. Let  $\delta$  be the automorphism on  $G^*(2, Z)$  defined by  $u_1\delta = tu_1t, v_1\delta = v_1$ , and  $t\delta = t$ . The homomorphism  $\sigma' = \delta\sigma$  is called the dual homomorphism of  $\sigma$ . This, of course, means that if  $\sigma$  maps  $u_1, v_1, t$  to  $\bar{u}_1, \bar{v}_1, \bar{t}$ , then  $\sigma'$  maps  $u_1, v_1, t$  to  $\bar{t}\bar{u}_1\bar{t}, \bar{v}_1, \bar{t}$

respectively. Since the elements  $u_1, v_1, t$  as well as  $\bar{t}\bar{u}_1\bar{t}, \bar{v}_1, \bar{t}$  satisfy the relations (4.2.1), therefore the solutions of these relations occur in dual pairs. Of course, if  $\sigma$  is conjugate to  $\tau$  then  $\sigma'$  is conjugate to  $\tau'$ . The parameter of  $\sigma$ , or of the conjugacy class containing  $\sigma$ , is the parameter of  $\bar{u}_1 \bar{v}_1$ .

We define a pair  $\bar{u}_1, \bar{v}_1$ , satisfying the relations  $\bar{u}_1^3 = \bar{v}_1^n = 1$ , in  $G^{3,n}(2, q)$  to be invertible if there exists  $\bar{t}$  in  $G^{3,n}(2, q)$  such that  $\bar{t}^2 = 1$ ,  $\bar{t}\bar{u}_1\bar{t} = \bar{u}_1^{-1}$  and  $\bar{t}\bar{v}_1\bar{t} = \bar{v}_1^{-1}$ .

We need the following easy but useful result for later use.

**Lemma 4.2.1**

A non-singular  $2 \times 2$  matrix  $M$  with entries in  $F_q$ , where  $q$  is not a power of 2, represent, an involution in  $G^{3,n}(2, q)$  if and only if the  $trace(M)$  is zero.

**Lemma 4.2.2**

If  $\bar{u}_1, \bar{v}_1$  are the elements of  $G^{3,n}(2, q)$  such that  $\bar{u}_1$  is of order 3 and  $\bar{v}_1$  is of order  $n$  and let  $U_1$  and  $V_1$  are matrices representing  $\bar{u}_1$  and  $\bar{v}_1$ , respectively. If  $r$  and  $m_1$  are the traces of  $U_1 V_1$  and  $V_1$  respectively, and the determinant of  $U_1 V_1$  to be equal to one, then either  $r^2 + rm_1 + m_1^2 = 3$  or the pair  $(\bar{u}_1, \bar{v}_1)$  is invertible.

**Proof**

Let  $\bar{u}_1$  and  $\bar{v}_1$  be the elements of  $G^{s^3n}(2, Z)$ , satisfying the relations  $\bar{u}_1^3 = \bar{v}_1^n = 1$  and  $\bar{u}_1$  and  $\bar{v}_1$  be represented by the matrices  $U_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  and  $V_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$  are the elements of  $GL(2, q)$ . Then, since  $\bar{u}_1^3 = 1$ , and  $U_1^3$  is a scalar matrix, and hence the determinant of  $U_1$  is a square in  $F_q$ . Thus, replacing  $U_1$  by a suitable scalar multiple, we assume that  $\det(U_1) = 1$ .

Since, for any matrix  $M$ ,  $M^3 = \lambda I$  if and only if  $(\text{trace}(M))^2 = \det(M)$ , so we may assume that  $\text{trace}(U_1) = a + d = -1$  and  $\det(U_1) = 1$ . Thus,  $U_1 = \begin{bmatrix} a & b \\ c & -a-1 \end{bmatrix}$ . Since  $\bar{u}_1^3 = 1$  implies that the  $\text{trace}(U_1) = -1$ , every element of  $GL(2, q)$  of trace equal to  $-1$  has upto scalar multiplication, a conjugate of the form  $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ . We can therefore assume that  $U_1$  has the form  $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ .

Also, since  $\bar{v}_1^n = 1$ ,  $V_1^n$  is a scalar matrix and hence the determinant of  $V_1$  is a square in  $F_q$ . Thus replacing  $V_1$  by a suitable scalar multiple, we assume the determinant of  $V_1$  equal to 1 so that we have  $\det(V_1^n) = 1$ . We observe that  $\det(V_1^n) = 1$  or  $\det(V_1^n) = -1$  depending upon the value of the integer  $n$  being odd or even. Since  $m_1$  be the trace of  $V_1$ . So, the characteristic equation of  $V_1$  is

$$V_1^2 - m_1 V_1 + I = 0 \quad (4.2.2)$$

Thus  $m_1 = e + h$  and therefore,  $V_1 = \begin{bmatrix} e & f \\ g & m_1 - e \end{bmatrix}$  giving

$\det(V_1) = e(m_1 - e) - fg = 1$ , so that

$$1 + fg + e^2 - em_1 = 0 \quad (4.2.3)$$

Now suppose that there exists an invertible element  $\bar{t}$  in  $G^{*3,n}(2, q)$  satisfying

$$\bar{t}^{-2} = (\bar{u}_1 \bar{t})^2 = (\bar{v}_1 \bar{t})^2 = 1 \quad (4.2.4)$$

Let a matrix representing  $\bar{t}$  be  $T = \begin{bmatrix} l & m \\ n & j \end{bmatrix}$ . Then, since  $\bar{t}$  is an involution, by lemma 4.2.1,  $j = -l$  yields  $T = \begin{bmatrix} l & m \\ n & -l \end{bmatrix}$ .

Let  $U_1 T$  be a matrix representing  $\bar{u}_1 \bar{t}$  of  $G^{*3,n}(2, q)$ .  $U_1 T = \begin{bmatrix} -n & l \\ l - n & m + l \end{bmatrix}$ , which again by lemma 4.2.1, and  $(\bar{u}_1 \bar{t})^2 = 1$ , implies that

$$m + l = n \quad (4.2.5)$$

Similarly, choosing  $V_1 T$  to be a matrix representing the element  $\bar{v}_1 \bar{t}$  of  $G^{*3,n}(2, q)$ , we obtain

$$V_1 T = \begin{bmatrix} el + fn & em - fl \\ gl + n(m_1 - e) & mg - l(m_1 - e) \end{bmatrix}$$

Since  $\bar{v}_1\bar{t}$  is also an involution, therefore, by the arguments given above, we have  $mg - l(m_1 - e) = -(el + fn)$ , which together with equation (4.2.5) yields  $2le + fn + ng - lm_1 - gl = 0$ . That is,

$$l(2e - g - m_1) + n(f + g) = 0 \quad (4.2.6)$$

Now for  $T$  to be a non-singular matrix, we should have  $\det(T) \neq 0$ , that is:

$$nl - l^2 - n^2 \neq 0 \quad (4.2.7)$$

Thus the necessary and sufficient conditions for the existence of  $\bar{t}$  in  $G^{*3,n}(2, q)$  are the equations (4.2.5), (4.2.6) and (4.2.7). Hence  $\bar{t}$  exists in  $G^{*3,n}(2, q)$  unless  $nl - l^2 - n^2 = 0$ .

If both  $2e - g - m_1$  and  $f + g$  are equal to zero, then the existence of  $\bar{t}$  is trivial. If not, then  $\frac{l}{n} = \frac{-(f + g)}{(2e - g - m_1)}$ , and so equation (4.2.6) is equivalent to

$(2e - g - m_1)(m - 2e - f) \neq 0$ . Thus, there exist,  $\bar{t}$  in  $G^{*3,n}(2, q)$  such that  $\bar{t}^{-2} = (\bar{u}_1\bar{t})^2 = (\bar{v}_1\bar{t})^2 = 1$  unless  $(f + g)^2 = (2e - g - m_1)((m - 2e - f))$ .

Simplification gives

$$(f - g)(f - g + 2e - m_1) = 4 + fg - m_1^2 \quad (4.2.8)$$

Now  $U_1V_1 = \begin{bmatrix} -g & -(m_1 - e) \\ (e - g) & f - m_1 + e \end{bmatrix}$  implies that the

$\text{trace}(U_1V_1) = f - g - m_1 + e$ . Let  $\text{trace}(U_1V_1) = r$ . Using equation (4.2.3) and substituting the value of  $r$  in equation (4.2.8), we obtain:

$$r^2 + rm_1 + m_1^2 = 3 \quad (4.2.9)$$

### Lemma 4.2.3

Any non-trivial element  $\bar{g}$ , whose order is not equal to 2 and whose dual is also not of order 2, of  $G^{*3,n}(2, q)$  is the image of  $uv$  under some non-degenerate homomorphism of  $G^{*3,n}(2, Z)$  into  $G^{*3,n}(2, q)$ .

### Proof

Using lemma 4.2.2, we show that every non-trivial element of  $G^{*3,n}(2, q)$  is a product of an element of order 3 and an element of order  $n$ . So we find elements  $\bar{u}_1, \bar{v}_1$  and  $\bar{t}$  of  $G^{*3,n}(2, q)$  satisfying the relations (4.2.1). Let  $\bar{u}_1, \bar{v}_1$  and

$\bar{t}$  be represented by the matrices  $U_1 = \begin{bmatrix} a & kc \\ c & -a-1 \end{bmatrix}$ ,  $V_1 = \begin{bmatrix} e & kf \\ f & m_1 - e \end{bmatrix}$  and

$T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ , where  $a, c, e, f, k$  are elements of  $F_q$ , with  $k \neq 0$ , so that

$$1 + a + a^2 + kc^2 = 0 \quad (4.2.10)$$

Also, assuming the determinant of  $V_1$  to be equal to 1, we have

$$1 + kf^2 + e^2 - em_1 = 0 \quad (4.2.11)$$

We take  $\bar{u}_1\bar{v}_1$  in a given conjugacy class. A matrix representing  $\bar{u}_1\bar{v}_1$  is given by

$$U_1V_1 = \begin{bmatrix} ae + kcf & akf + ck(m_1 - e) \\ ce - af - f & kcf - a(m_1 - e) - m_1 + e \end{bmatrix}.$$

Its trace, which we denote by  $r$ , is given by

$$r = \text{trace}(U_1V_1) = a(2e - m_1) + 2kfc + (e - m_1) \quad (4.2.12)$$

Also,  $\det(U_1V_1) = \det(U_1)\det(V_1) = 1$ , as determinant of  $U_1$  and  $V_1$  is assumed to be 1. Also

$$U_1V_1T = \begin{bmatrix} akf + km_1 - kce & ake - k^2cf \\ kcf - am_1 + ae - m_1 + e & -kce + akf + kf \end{bmatrix}$$

So,  $\text{trace}(U_1V_1T) = k(2af - 2ce + f + cm_1)$ . Let  $\text{trace}(U_1V_1T) = ks$ , so that,

$$s = 2af - c(2e - m_1) + f \quad (4.2.13)$$

Hence, we have

$$r^2 + ks^2 + m_1^2 - r - 3 = 0 \quad (4.2.14)$$

Since  $\bar{g} = \bar{u}_1\bar{v}_1$  (or its dual  $\bar{u}_1\bar{v}_1\bar{t}$ ) are not of order 2, the class to which we want them to belong do not consist of involutions, so that  $(\bar{u}_1\bar{v}_1)^2 \neq 1$  and  $(\bar{u}_1\bar{v}_1\bar{t})^2 \neq 1$ . Thus the traces of the matrices  $U_1V_1$  and  $U_1V_1T$  are not equal to zero, by lemma 4.2.1. Hence  $r \neq 0$ , and  $s \neq 0$ , so that we have  $\theta = r^2 \neq 0$ ; and it



is sufficient to show that we can choose  $a, c, e, f, k$  in  $F_q$ , so that  $r^2$  is indeed equal to  $\theta$ , and we choose it arbitrarily in  $F_q$  to satisfy the conditions, and we then choose  $r$  to satisfy  $\theta = r^2$ . From equation (4.2.14), we have  $ks^2 = 3 - m_1^2 - r^2 + r$ . If  $r^2 - r \neq 3 - m_1^2$ , we select  $k$  according to the above argument.

Any quadratic polynomial  $\lambda z^2 + \mu z + \nu$ , with coefficients in  $F_q$  takes at least  $\frac{q+1}{2}$  distinct values, as  $z$  runs through  $F_q$ ; since the equation  $\lambda z^2 + \mu z + \nu = k$  has at most two roots for fixed  $k$ ; and there are  $q$  elements in  $F_q$ , and  $q$  is odd. In particular,  $e^2 - em_1$  and  $-kf^2 - 1$  each take at least  $\frac{q+1}{2}$  distinct values as  $e$  and  $f$  run through  $F_q$ . Hence we can find  $e$  and  $f$  so that  $e^2 - em_1 = -kf^2 - 1$ .

Finally by substituting the values of  $r, s, e, f, k$  in equations (4.2.13) and (4.2.14) we can find the values of  $a$  and  $c$ . Now these two equations are linear equations for  $a$  and  $c$  with determinant  $-(2e - m_1)^2 - 4kf^2 = 4 - m_1^2$ , which is non-zero, so that we can find,  $a$  and  $c$  satisfying equation (4.3.10).

#### Lemma 4.2.4

Any two non-degenerate homomorphisms  $\sigma, \tau$  of  $G^{*3,n}(2, Z)$  into  $G^{*3,n}(2, q)$  are conjugate if  $(u_1 v_1)\sigma = (u_1 v_1)\tau$ .

**Proof**

Let  $\sigma : G^{*3,n}(2,Z) \rightarrow G^{*3,n}(2,q)$  be the non-degenerate homomorphism such that  $\bar{u}_1\bar{v}_1$  has parameter  $\theta$  constructed as in the proof of lemma 4.2.3. We also suppose that the non-degenerate homomorphism has the same parameter  $\theta$ .

First, since there are just two classes of elements of order 2 in  $G^{*3,n}(2,Z)$ , one in  $G^{*3,n}(2,q)$  and the other not, we can pass to a conjugate of  $\tau$  in which  $t\tau$  is represented by  $\begin{bmatrix} 0 & -k' \\ 1 & 0 \end{bmatrix}$  for some  $k' \neq 0$  in  $F_q$ . Then because  $u_1\tau$  and  $tu_1t\tau$  are both of order 3,  $u_1\tau$  must be represented by a matrix  $\begin{bmatrix} a' & k'c' \\ c' & -a'-1 \end{bmatrix}$  and because  $v_1\tau$  is of order  $n$  and  $v_1t\tau$  is of order 2,  $v_1\tau$  must be represented by a matrix  $\begin{bmatrix} e' & k'f' \\ f' & m_1 - e' \end{bmatrix}$ , with  $a', c', e', f', k'$ , satisfying the equations (4.2.3), (4.2.6) and (4.2.7). Then  $\theta = r'^2 = r^2$ , and  $(3 - m_1^2) - \theta + r = k's'^2$ . Hence  $\theta \neq 0$ ,  $(3 - m_1^2) - \theta + r \neq 0$ ; so it follows that  $k'/k$  is a square in  $F_q$ .

Now  $v_1\sigma$  and  $v_1\tau$  are both of order  $n$  and so are conjugate in  $G^{*3,n}(2,q)$ . So we can pass to a conjugate of  $\tau$  with  $v_1\sigma = v_1\tau$ . Then  $t\sigma$  and  $t\tau$  are involutions which invert  $v_1\sigma$ , and so belong to  $N(\langle v_1\sigma \rangle)$ , there are two classes of such involutions, one in  $G^{*3,n}(2,q)$  and the other not. Because  $t\sigma$  is  $\begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$  and  $t\tau$  is conjugate to  $\begin{bmatrix} 0 & -k' \\ 1 & 0 \end{bmatrix}$  and  $k'/k$  is a square,  $t\sigma$  and  $t\tau$  either both belong to  $G^{*3,n}(2,q)$  or neither. Hence they are conjugate in  $N(\langle v_1\sigma \rangle)$ .

That is, passing to a new conjugate, we can assume  $v_1\sigma = v_1\tau$ ,  $t\sigma = t\tau$ . This means that in the notations above, we can assume  $k' = k$ ,  $f' = f$  and  $e' = e$ . We can also, by multiplying the matrix representing  $u_1\tau$  by a scalar, assume,  $r = r'$  and  $s = s'$ . Then the equations (4.2.10), (4.2.11), (4.2.12) and (4.2.13) with  $a, c, e, f, k$  and then with  $a', c', e', f', k'$  and ensure that  $a = a', c = c'$ . That is,  $\sigma = \tau$ .

We now put together the lemmas (4.2.3) and (4.2.4) to obtain the following.

**Theorem 4.2.5**

The conjugacy classes of non-degenerate homomorphisms of  $G^{*3,n}(2, Z)$  into  $G^{*3,n}(2, q)$  are in one to one correspondence with the non-trivial conjugacy classes of elements of  $G^{*3,n}(2, q)$  under a correspondence which assigns to any non-degenerate homomorphism  $\sigma$  the class containing  $(u_1 v_1)\sigma$ .

**Proof**

Let  $\sigma$  be a non-degenerate homomorphism of  $G^{*3,n}(2, Z)$  into  $G^{*3,n}(2, q)$  such that it maps  $u_1, v_1$  to  $\bar{u}_1, \bar{v}_1$ . Let  $\theta$  be the parameter of the class represented by  $\bar{u}_1 \bar{v}_1$ . Now  $\sigma$  is determined by  $u_1, v_1$  and each  $\theta$  gives us this pair  $u_1, v_1$ , so that  $\sigma$  is associated with  $\theta$ . We shall call the parameter  $\theta$  of the class containing  $u_1, v_1$ , the parameter of the non-degenerate homomorphism of  $G^{*3,n}(2, Z)$  into  $G^{*3,n}(2, q)$ .

Now  $U_1T = \begin{bmatrix} ck & -ak \\ -a-1 & -ck \end{bmatrix}$  implies that  $\det(U_1T) = -k(a^2 + a + kc^2) = k$

(by equation (4.2.10)), Also

$$(U_1T)V_1 = \begin{bmatrix} cke - akf & ck^2c - ak(m_1 - e) \\ -ae - e - ckf & -akf - ck(m_1 - e) - kf \end{bmatrix}$$

implies that  $\text{trac}((U_1T)V_1) = 2cke - 2akf - ck m_1 - kf = -k(2af - 2cke + kf + ck m_1) = -ks$ . If  $\bar{u}_1, \bar{v}_1, \bar{t}$  satisfy the relations (4.2.1), then so do  $\bar{t}\bar{u}_1\bar{t}, \bar{v}_1, \bar{t}$ . So that the solutions of relation (4.2.1) occur in dual pairs. Hence replacing the solutions in lemma 4.2.3 by  $\bar{t}\bar{u}_1\bar{t}, \bar{v}_1, \bar{t}$ , we interchange  $r$  by  $-ks$  (where  $r = \text{trace}(U_1V_1)$ ), to get the new parameter  $ks^2$ . We then find the relationship between the parameters of dual non-degenerate homomorphisms.

#### Corollary 4.2.6

If  $\sigma : G^{*3,n}(2, Z) \rightarrow G^{*3,n}(2, q)$  is a non-degenerate homomorphism,  $\sigma'$  is its dual and  $\theta, \phi$  are their respective parameters then  $\theta + \phi = 3 - m_1^2 + r$ .

#### Proof

Let  $\sigma : G^{*3,n}(2, Z) \rightarrow G^{*3,n}(2, q)$  be a non-degenerate homomorphism satisfying the relations  $u_1\sigma = \bar{u}_1, v_1\sigma = \bar{v}_1$  and  $t\sigma = \bar{t}$ . Let  $\sigma'$  be the dual of  $\sigma$ .

As in lemma 4.2.3, we choose the matrices  $U_1 = \begin{bmatrix} a & ck \\ k & -a-1 \end{bmatrix}$ ,  $V_1 = \begin{bmatrix} e & kf \\ f & m_1 - e \end{bmatrix}$

and  $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ , representing  $\bar{u}_1, \bar{v}_1$  and  $\bar{t}$ , respectively, of  $G^{*3,n}(2, q)$ . Now by

lemma 4.2.1, we have  $\text{trace}(U_1V_1) = 0$  if and only if  $(\bar{u}_1\bar{v}_1)^2 = 1$ . Also, we have  $\{\text{trace}(U_1V_1T)\}/k = s = 0$  if and only if  $(\bar{u}_1\bar{v}_1\bar{t})^2 = 1$ .

Now  $\det(U_1V_1) = 1$ , thus giving the parameter of  $\bar{u}_1\bar{v}_1$  equal to  $r^2 = \theta$ , say. Also since  $\text{trace}(U_1V_1T) = ks$  and  $\det(U_1V_1T) = k$  (since  $\det(U_1) = 1, \det(V_1) = 1$  and  $\det(T) = k$ ), we obtain the parameter of  $\bar{u}_1\bar{v}_1\bar{t}$  equal to  $ks^2$ , which we will denote by  $\phi$ . Thus  $\theta + \phi = r^2 + ks^2$ . Substituting the values from equation (4.3.14), we thus obtain  $\theta + \phi = 3 - m_1^2 + r$ . Hence if  $\theta$  is the parameter of the non-degenerate homomorphism  $\sigma$ , then  $\phi = 3 - m_1^2 + r - \theta$  is the parameter of the dual  $\sigma'$  of  $\sigma$ .

### 4.3 TRIANGLE GROUPS

In this section we discuss the triangle groups  $\Delta(3, n, k) = \langle u_1, v_1 : u_1^3 = v_1^n = (u_1v_1)^k = 1 \rangle$ , where  $3 \leq n \leq k$ . We shall find a condition in the form of a polynomial with integer coefficients for the existence of actions of  $G^{*3,n}(2, Z) = \langle u_1, v_1, t : u_1^3 = v_1^n = t^2 = (u_1t)^2 = (v_1t)^2 = 1 \rangle$  on  $PL(F_q)$ , which yield  $\Delta(3, n, k)$  as groups of permutations defined on  $PL(F_q)$ , where  $q$  is a prime congruent to  $\pm 1$  modulus  $k$ .

For positive integers  $l, n$  and  $k$ , the triangle groups [2, 16]  $\Delta(l, n, k)$  are the groups with abstract presentation  $\langle u_1, v_1 : u_1^l = v_1^n = (u_1v_1)^k = 1 \rangle$ . When  $\frac{1}{l} + \frac{1}{n} + \frac{1}{k} > 1$ , this group is finite, and is one of the finite spherical groups (either cyclic or dihedral, or isomorphic to  $A_4, S_4$  or  $A_5$ ) in particular the 2-sphere can be tessellated using a triangle whose interior angles are  $\frac{\pi}{l}, \frac{\pi}{n}$  and  $\frac{\pi}{k}$ . When

$\frac{1}{l} + \frac{1}{n} + \frac{1}{k} = 1$ , the group is infinite but soluble and the Euclidean plane can be tessellated using a triangle with angles  $\frac{\pi}{l}$ ,  $\frac{\pi}{n}$  and  $\frac{\pi}{k}$ . Finally, if  $\frac{1}{l} + \frac{1}{n} + \frac{1}{k} < 1$ , then the triangle group  $\Delta(3, n, k)$  is infinite but insoluble and the hyperbolic plane can be tessellated using a hyperbolic triangle with angles  $\frac{\pi}{l}$ ,  $\frac{\pi}{n}$  and  $\frac{\pi}{k}$ .

The triangle groups have long received special attention. They have been subjects of extensive study primarily by Brahana [3], Miller [20] and Sinkov [32].

In [27], it has been mentioned that in the finite case the triplet  $(l, n, k)$  can have the values  $(4, 3, 1)$ ,  $(4, 3, 2)$ ,  $(4, 3, 3)$ ,  $(4, 3, 4)$  and  $(4, 3, 5)$ , that is, when  $\frac{1}{l} + \frac{1}{n} + \frac{1}{k} > 1$ , and  $(2, 3, k)$  where  $k \geq 6$ . Therefore the triplet attains the values  $(2, 3, k)$  where  $k < 6$  in the finite case and  $k \geq 6$  in the infinite case.

It has been described in [25] that  $\Delta(2, 3, k)$  is trivial,  $S_3$ ,  $A_4$ ,  $S_5$  and  $A_5$  if  $k = 1, 2, 3, 4$  and  $5$  respectively. The group  $\Delta(2, 3, k)$  when  $k = 6$ , deserves special treatment. It is an extension by the cyclic group  $C_6$ , of a free Abelian group of rank 2, and in particular is soluble. This group has been studied extensively in [20] and [22].

When  $k = 7$ , the group  $\Delta(2, 3, k)$  has been investigated extensively because of the fact that Hurwitz groups are non-trivial quotients of these groups. A detailed account of these groups is available in [25], [33] and [34].

Eviritt [14] and [15] has shown that the triangle group  $\Delta(2, q, r)$  is a homomorphic image of  $\Delta(p, q, r)$  for  $p$  even and possesses Higman-property,

that is, each of  $\Delta(p, q, r)$  for  $\frac{1}{l} + \frac{1}{n} + \frac{1}{k} < 1$  contains among its homomorphic images all but finitely many of the alternating or symmetric groups. He has further proved that:

- a.  $\Delta(3, 3, r)$  has Higman-property for all  $r \geq 4$ .
- b.  $\Delta(3, 5, r)$  has Higman-property for all  $r \geq 40$ .
- c.  $\Delta(3, q, r)$  possesses Higman-property for all  $q \geq 7$  prime and  $r \geq 4q$ .

Actions of the extended modular group on  $PL(F_q)$  have been parametrized by Mushtaq in [26]. In [25], Mushtaq has parametrized actions of  $\Delta(2, 3, 7)$  on  $PL(F_q)$ . It has shown that if  $\theta$  is a root of the equation  $\theta^3 - 5\theta^2 + 6\theta - 1 = 0$  in  $F_q$ , where  $q$  satisfies the conditions of Macbeath [18], then corresponding to  $\theta$  there exists a pair  $(\bar{x}, \bar{y})$  such that  $\bar{x}^2 = \bar{y}^3 = (\bar{x}\bar{y})^7 = 1$ .

In [22] and [25], conditions in form of equations are found whose roots in  $F_q$ , for suitable prime numbers  $q$ , guarantee only those actions of  $PGL(2, Z)$  on  $PL(F_q)$  which evolve  $\Delta^*(2, 3, 6)$  and  $\Delta^*(2, 3, 7)$ .

Now we have devised a method by which we can obtain  $\Delta^*(3, n, k)$  through the actions of  $G^{*3,n}(2, Z)$  on  $PL(F_q)$  by using the parametrization technique as developed in lemma 4.2.3. We will see in the following that the method evolves polynomials  $f(\theta) \in Z[z]$  such that for each root of  $f(\theta) = 0$  in  $F_q$ , for suitable  $q$ , there exists a triplet of linear-fractional transformations

$(\bar{u}_1, \bar{v}_1, \bar{l})$  such that they satisfy the relations  $\bar{u}_1^3 = \bar{v}_1^n = \bar{l}^2 = (\bar{u}_1\bar{l})^2 = (\bar{v}_1\bar{l})^2 = 1$  and generate the group  $\Delta^*(3, n, k)$ .

**Theorem 4.3.1**

If  $k$  is a prime number and  $q \equiv \pm 1 \pmod{k}$  then there exists a polynomial  $f \in Z[z]$  such that corresponding to each zero  $\theta$  of  $f$  there exists a pair  $\bar{u}, \bar{v}$  of elements of  $G^{*3,n}(2, q)$  such that  $\bar{u}^3 = \bar{v}^n = (\bar{u}\bar{v})^k = 1$ .

**Proof**

We suppose that the matrix  $M$  is a product of two non-singular  $2 \times 2$  matrices  $U_1$  and  $V_1$  corresponding to  $\bar{u}_1$  and  $\bar{v}_1$  of  $G^{*3,n}(2, q)$ . Then, the characteristic equation of  $U_1V_1$  is

$$(U_1V_1)^2 - rU_1V_1 + \Delta I = 0 \tag{4.3.1}$$

Here, the determinant of  $M = \Delta$  and the trace of  $M = r$ . Equation (4.3.1) implies that,

$$(U_1V_1)^2 = rU_1V_1 - \Delta I \tag{4.3.2}$$

Multiplying equation (4.3.2) by  $U_1V_1$  on both sides. We obtain,

$$(U_1V_1)^3 = r(U_1V_1)^2 - (U_1V_1)\Delta I \tag{4.3.3}$$

Substituting the value of  $(U_1V_1)^2$  from equation (4.3.2) in equation (4.3.3), we get



$$(U_1V_1)^3 = (r^2 - \Delta)U_1V_1 - r\Delta I \quad (4.3.4)$$

On recursion, equation (4.3.4) yields

$$(U_1V_1)^k = \left\{ \binom{k-1}{0} r^{k-1} - \binom{k-2}{1} r^{k-3} \Delta + \dots \right\} U_1V_1 - \left\{ \binom{k-2}{0} r^{k-2} - \binom{k-3}{1} r^{k-4} \Delta + \dots \right\} \Delta I \quad (4.3.5)$$

Furthermore, if we let,

$$f(r) = \binom{k-1}{0} r^{k-1} - \binom{k-2}{1} r^{k-3} + \dots \quad (4.3.6)$$

We can then substitute  $\theta$  for  $r^2$  in  $f(r)$  and obtain a polynomial, say  $f$ , in  $\theta$ .

Note that  $U_1V_1$  has order  $k$  if  $(U_1V_1)^k$  is a scalar multiple of the identity matrix. This happens if  $f(\theta) = 0$ . Since  $k$  is prime and  $q \equiv \pm 1 \pmod{k}$ , there will be  $\frac{k-1}{2}$  zeros of  $f(\theta) = 0$  and each zero  $\theta_i$  of  $f(\theta) = 0$  will yield a pair of linear-fractional-transformations  $\bar{u}, \bar{v}$  of elements of  $G^{3,n}(2, q)$  such that  $\bar{u}_1^3 = \bar{v}_1^n = (\bar{u}_1\bar{v}_1)^k = 1$ .

When  $k$  is not a prime, we have the same conditions as given theorem 5.5.4 and theorem 5.5.5.

We conclude here by mentioning that we have dealt with the actions of  $G^{*3,n}(2, q)$  on  $PL(F_q)$  which yield triangle groups  $\Delta(3, n, k)$  where  $q$  is congruent to  $\pm 1$  modulus  $k$  and  $3 \leq n \leq k$ . In the case where  $q$  is incongruent to  $\pm 1$  modulus  $k$ , the group  $G^{3,n}(2, q)$  does not contain any element of order  $k$ , so its action is not faithful.

In the following, we list conditions in form of equations  $f(\theta) = 0$  for the existence of triangle groups  $\Delta(3, n, k)$  where  $1 \leq k \leq 20$ .

<u>Triangle group</u>	<u>Minimal equation satisfied by <math>\theta</math></u>
$\Delta(3, n, 1)$	$\theta - 4 = 0$
$\Delta(3, n, 2)$	$\theta = 0$
$\Delta(3, n, 3)$	$\theta - 1 = 0$
$\Delta(3, n, 4)$	$\theta - 2 = 0$
$\Delta(3, n, 5)$	$\theta^2 - 3\theta + 1 = 0$
$\Delta(3, n, 6)$	$\theta - 3 = 0$
$\Delta(3, n, 7)$	$\theta^3 - 5\theta^2 + 6\theta - 1 = 0$
$\Delta(3, n, 8)$	$\theta^2 - 4\theta + 2 = 0$
$\Delta(3, n, 9)$	$\theta^3 - 6\theta^2 + 9\theta - 1 = 0$
$\Delta(3, n, 10)$	$\theta^2 - 5\theta + 5 = 0$
$\Delta(3, n, 11)$	$\theta^5 - 9\theta^4 + 28\theta^3 - 35\theta^2 + 15\theta - 1 = 0$
$\Delta(3, n, 12)$	$\theta^2 - 4\theta + 1 = 0$
$\Delta(3, n, 13)$	$\theta^6 - 11\theta^5 + 45\theta^4 - 84\theta^3 + 70\theta^2 - 21\theta + 1 = 0$
$\Delta(3, n, 14)$	$\theta^6 - 120\theta^5 + 55\theta^4 - 120\theta^3 + 126\theta^2 - 56\theta + 7 = 0$
$\Delta(3, n, 15)$	$\theta^7 - 13\theta^6 + 66\theta^5 - 165\theta^4 + 210\theta^3 - 126\theta^2 + 28\theta - 1 = 0$

<u>Triangle group</u>	Minimal equation satisfied by $\theta$
$\Delta(3, n, 16)$	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 106\theta^2 - 40\theta + 4 = 0$
$\Delta(3, n, 17)$	$\theta^8 - 15\theta^7 + 91\theta^6 - 286\theta^5 + 495\theta^4 - 462\theta^3 + 210\theta^2 - 36\theta + 1 = 0$
$\Delta(3, n, 18)$	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 105\theta^2 - 36\theta + 3 = 0$
$\Delta(3, n, 19)$	$\theta^9 - 17\theta^8 + 120\theta^7 - 455\theta^6 + 100\theta^5 - 1287\theta^4 + 924\theta^3 - 330\theta^2 + 45\theta - 1 = 0$
$\Delta(3, n, 20)$	$\theta^8 - 17\theta^7 + 104\theta^6 - 352\theta^5 + 661\theta^4 - 680\theta^3 + 356\theta^2 - 80\theta + 5 = 0$

## CHAPTER FIVE

# $\Delta(3,3,k)$ AND PARAMETRIZATION OF ACTIONS OF $G^{*3,3}(2,Z)$



### 5.1 INTRODUCTION

In this chapter, we want to deal with  $\Delta(3,3,k) = \langle u, v : u^3 = v^3 = (uv)^k = 1 \rangle$ ,  $k \neq 3$ , we need a triangle with angles  $\frac{\pi}{3}, \frac{\pi}{3}, \frac{\pi}{k}$ . Since  $\frac{\pi}{3} + \frac{\pi}{3} + \frac{\pi}{k} \neq \pi$  we cannot do this in the plane. Thus we can replace the plane by the sphere if  $k < 3$  or by a hyperplane if  $k > 3$ . If  $k < 3$ , the group is finite, because there are only a finite number of triangles.

Also, we parameterize the conjugacy classes of non-degenerate homomorphism which represent actions of  $\Delta(3,3,k) = \langle u, v : u^3 = v^3 = (uv)^k = 1 \rangle$  on  $PL(F_q)$  where  $q \equiv \pm 1 \pmod{k}$ . Also, for various values of  $k$ , we shall find the conditions for the existence of coset diagrams depicting the permutation actions of  $\Delta(3,3,k)$  on  $PL(F_q)$ . The conditions are polynomials with integer coefficients and the diagrams are such that every vertex in them is fixed by  $(\overline{uv})^k$ . In this way, we get a homomorphic image of  $\Delta(3,3,k)$  as permutation groups on  $PL(F_q)$ .

In second section of this chapter, we have shown that any non-degenerate homomorphism from  $G^{3,3}(2, Z)$  into  $G^{3,3}(2, q)$  can be extended to a homomorphism  $G^{*3,3}(2, Z)$  into  $G^{*3,3}(2, q)$ . It has been shown also that every element in  $G^{3,3}(2, q)$ , not of order 1 or 3 is the image of  $uv$  under some non-degenerate homomorphism. We have parameterized the conjugacy classes of non-degenerate homomorphism  $\sigma$  with the non-trivial elements of  $F_q$ .

The group  $\Delta(3,3,k)$  is the triangle group with presentation  $\langle u, v : u^3 = v^3 = (uv)^k = 1 \rangle$ . Let  $q$  be a prime power and  $F_q$  denote the finite field of order  $q$ . A one-to-one correspondence can be established between the conjugacy classes of non-degenerate homomorphisms  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$ , under the action of inner automorphisms of  $G^{*3,3}(2, q)$ , and the non-trivial conjugacy classes of elements of  $G^{*3,3}(2, q)$  such that the correspondence assigns to any non-degenerate homomorphisms  $\sigma$  the class containing  $(uv)\sigma$ . In this chapter we have considered the conjugacy classes which arise from the action of  $\Delta(3,3,k)$  on the projective line over  $F_q$ .

It is well known in [13] that  $\Delta(3,3,k)$  is finite precisely when  $k = 1, 2$ :  $\Delta(3,3,k)$  is respectively  $C_3$  and the alternating group  $A_4$ , being isomorphic to the group of rotations of the regular tetrahedron. The group  $\Delta(3,3,k)$  is infinite for  $k \geq 3$ .

In [11], it has been mentioned that  $\Delta(3,3,k)$  for  $k = 3$  is soluble, its commutator subgroup is a free abelian group on two generators, and the associated factor commutator group is cyclic of order  $k$ . It has been described in [15] that  $\Delta(3,3,k)$  possesses Higman property that an infinite triangle group

contains among its homomorphic images of all but finitely many of the  $A_n$  or  $S_n$  groups for  $k \geq 4$ .

**5.2 COSET DIAGRAMS FOR THE TRIANGLE GROUP  $\Delta(3,3,k)$**

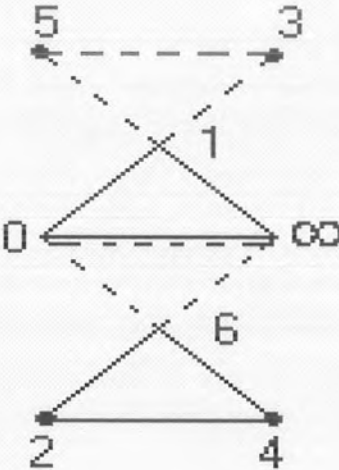
We use coset diagrams as defined in chapter one for the group  $G^{*3,3}(2,Z)$  and study its action on  $PL(F_q)$ . For example, the following diagram depicts a permutation representation of the  $G^{*3,3}(2,Z)$  on  $PL(F_7)$  in which:

$u$  acts as  $(1\ 0\ \infty)(2\ 4\ 6)(3)(5)$ ,

$v$  acts as  $(0\ 6\ \infty)(1\ 3\ 5)(2)(4)$ , and

$t$  acts as  $(0\ \infty)(2\ 4)(3\ 5)(1)(6)$ ,

represent the group  $\Delta(3,3,7)$ . The coset diagram is as under:



### 5.3 RELATION BETWEEN THE NON-DEGENERATE HOMOMORPHISMS AND THE PARAMETERS

A homomorphism  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  is called a non-degenerate homomorphism, with the orders of  $u$  and  $v$  are the same as the orders of  $(u)\sigma$  and  $(v)\sigma$ , if neither of the generators  $u, v$  lies in the kernel of  $\sigma$ . The group  $G^{*3,3}(2, q)$  has a natural permutation representation on  $PL(F_q)$  and therefore any non-degenerate homomorphisms  $\sigma$  and  $\tau$  are called conjugate if  $\tau = \sigma\rho$  for some inner automorphism  $\rho$  of  $G^{*3,3}(2, q)$ . We denote  $u\sigma, v\sigma$  and  $t\sigma$  respectively by  $\bar{u}, \bar{v}$  and  $\bar{t}$ .

We now give the method by which, for any  $\theta$  in  $F_q$ , we can find a non-trivial conjugacy class of pairs  $(\bar{u}, \bar{v})$  and corresponding to this class we can construct a coset diagram depicting the action.

### 5.4 PARAMETRIZATION OF THE ACTIONS

Let  $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  be an element of  $GL(2, q)$  which yields the element  $\bar{u}$  of  $G^{*3,3}(2, q)$ . Then, since  $\bar{u}^3 = 1, U^3$  is a scalar matrix, and hence the determinant of  $U$  is a square in  $F_q$ . Thus, replacing  $U$  by a suitable scalar multiple, we assume that the determinant of  $U$  is equal to one.

Since, for any matrix  $M, M^3 = \lambda I$  if and only if  $(\text{trace}(M))^2 = \det(M)$ . So, we may assume that  $\text{trace}(U) = a + d = -1$  and  $\det(U) = 1$ . Thus

$$U = \begin{bmatrix} a & b \\ c & -a-1 \end{bmatrix}. \quad \text{Similarly, } V = \begin{bmatrix} e & f \\ g & -e-1 \end{bmatrix}. \quad \text{Since } \bar{u}^3 = 1$$

implies that the  $\text{trace}(\bar{u}) = -1$ , every element of  $GL(2, q)$  of trace equal to  $-1$  has upto scalar multiplication, a conjugate of the form  $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ . We can therefore assume that  $U$  has the form  $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ .

Now let a matrix corresponding to  $\bar{t}$ , be represented by  $T = \begin{bmatrix} l & m \\ n & j \end{bmatrix}$ . Since  $\bar{t}^2 = 1$ , the trace of  $T$  is zero. So, upto scalar multiplication, we can assume that the matrix representing  $\bar{t}$  has the form  $\begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ . Because  $(\bar{u}\bar{t})^2 = (\bar{v}\bar{t})^2 = 1$ , the trace of  $\bar{u}\bar{t}$  and  $\bar{v}\bar{t}$  is zero and so  $b = kc$  and  $f = gk$ .

Thus we can take the matrices corresponding to generators  $\bar{u}$ ,  $\bar{v}$  and  $\bar{t}$  of  $G^{*3,3}(2, q)$  as:

$$U = \begin{bmatrix} a & kc \\ c & -a-1 \end{bmatrix}, \quad V = \begin{bmatrix} e & gk \\ g & -e-1 \end{bmatrix}, \quad \text{and} \quad T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix} \quad \text{respectively,}$$

where  $a, c, e, g, k \in F_q$ . Then,

$$1 + a + a^2 + kc^2 = 0 \tag{5.4.1}$$

and

$$1 + e + e^2 + kg^2 = 0 \tag{5.4.2}$$

because the determinants of  $U$  and  $V$  are one.



This certainly evolves elements satisfying the relations  $U^3 = V^3 = \lambda I$ , where  $\lambda$  is a scalar and  $I$  is the identity matrix. The non-degenerate homomorphism  $\sigma$  is determined by  $\bar{u}, \bar{v}$  because one-to-one correspondence assigns to  $\sigma$  the class containing  $\bar{u}\bar{v}$ . So we only have to check on the conjugacy class of  $\bar{u}\bar{v}$ . The matrix

$$UV = \begin{bmatrix} ae + gkc & agk - kce - kc \\ ec - ag - g & gkc + ae + a + e + 1 \end{bmatrix} \text{ has the trace}$$

$$r = a(2e + 1) + 2kgc + (e + 1) \quad (5.4.3)$$

Also

$$UVT = \begin{bmatrix} agk - gk^2c & -kae - kce - kc \\ gkc + ae + a + e + 1 & -kce + gka + kg \end{bmatrix}.$$

If  $\text{trace}(UVT) = ks$ , then

$$s = 2ag - c(2e + 1) + g \quad (5.4.4)$$

So the relationship between (5.4.3) and (5.4.4) is

$$r^2 + ks^2 - r - 2 = 0 \quad (5.4.5)$$

We set

$$\theta = r^2 \quad (5.4.6)$$

Now for each conjugacy class of pairs  $(\bar{u}, \bar{v})$  we can draw a coset diagram.

By  $D(\theta, q)$ , we shall mean a coset diagram associated with the conjugacy class of non-degenerate homomorphisms  $\sigma$  from  $G^{*3,3}(2, Z)$  into  $G^{*3,3}(2, q)$  corresponding to  $\theta \in F_q$ .

## 5.5 A CONDITION FOR THE EXISTENCE OF CERTAIN COSET DIAGRAMS

As we have mentioned earlier, in this chapter we shall concentrate on the group  $\Delta(3,3,k)$ , where  $k > 2$ . We shall also discuss in particular the special case when  $\theta = 3$ . We shall use the coset diagrams to determine the group  $\Delta(3,3,k)$ . In order to do so, we shall find a condition for the existence of a coset diagram in which every vertex is fixed by  $(\bar{u}\bar{v})^k$ .

For each  $\theta$  in  $F_q$ , there exists a non-trivial conjugacy class of pairs  $\bar{u}, \bar{v}$  of elements of  $G^{*3,3}(2, q)$ , where both  $\bar{u}$  and  $\bar{v}$  are of orders 3. Each pair  $\bar{u}, \bar{v}$  determines the non-degenerate homomorphism  $\sigma$  from  $G^{*3,3}(2, Z)$  to  $G^{*3,3}(2, q)$ . Once we have obtained  $\bar{u}, \bar{v}$  we can draw a coset diagram depicting the permutation action of  $(\bar{u}\bar{v})$  on  $PL(F_q)$ . Here we are interested in coset diagrams in which every vertex is fixed by  $(\bar{u}\bar{v})^k$ . Finally we will concentrate on a particular case, that is, when  $\theta = 3$ . Such diagrams exist for certain  $\theta$  in  $F_q$  and these  $\theta$ 's are special in the sense that they satisfy certain polynomial equations. That is, for the solution  $\theta$ 's of polynomial  $f(\theta)$ , obtained from the relation  $(\bar{u}\bar{v})^k = 1$ . we get certain diagrams in which every vertex is fixed by  $(\bar{u}\bar{v})^k$  depending upon the value of  $k$ . We shall consider the cases for all  $k > 2$ , as the case is trivial when  $k = 1$  and for  $k = 2$ ,  $\theta$  has only one root, that is, 0. The

following theorem gives a method for finding a condition for the existence of a coset diagram in which every vertex is fixed by  $(\bar{u}\bar{v})^k$ . That is, it will give a condition for the existence of a coset diagram for the homomorphic image of  $\Delta(3,3,k)$  on  $PL(F_q)$ .

**Theorem 5.5.1**

Let  $U$  and  $V$  be two non-singular  $2 \times 2$  matrices corresponding to the generators  $\bar{u}$  and  $\bar{v}$  of  $G^{*3,3}(2,q)$ . Let  $\det(UV) = 1$  and its trace be  $r$ . Then for a positive integer  $k$

$$(UV)^k = \left\{ \binom{k-1}{0} r^{k-1} - \binom{k-2}{1} r^{k-3} + \dots \right\} UV - \left\{ \binom{k-2}{0} r^{k-2} - \binom{k-3}{1} r^{k-4} + \dots \right\} I \quad (5.5.1)$$

**Proof**

Since  $\det(UV) = 1$  and trace of  $UV$  is  $r$ , therefore the characteristic equation of  $UV$  is

$$(UV)^2 - rUV + I = 0 \quad (5.5.2)$$

On recursion, equation (5.5.2) yield

$$(UV)^k = \left\{ \binom{k-1}{0} r^{k-1} - \binom{k-2}{1} r^{k-3} + \dots \right\} UV - \left\{ \binom{k-2}{0} r^{k-2} - \binom{k-3}{1} r^{k-4} + \dots \right\} I \quad (5.5.3)$$

**Corollary 5.5.2**

Let  $k$  be any positive integer greater than 2. Then,

- (i) if  $k = 2n + 1$  and  $n > 0$ , then

$$(UV)^{2n+1} = \left\{ \binom{2n}{0} r^{2n} - \binom{2n-1}{1} r^{2n-2} + \dots \right\} UV - \left\{ \binom{2n-1}{0} r^{2n-1} - \binom{2n-2}{1} r^{2n-3} + \dots \right\} I \quad (5.5.4)$$

(ii) if  $k = 2n$  for all positive integers  $n$ , then

$$(UV)^{2n} = \left\{ \binom{2n-1}{0} r^{2n-1} - \binom{2n-2}{1} r^{2n-3} + \dots \right\} UV - \left\{ \binom{2n-2}{0} r^{2n-2} - \binom{2n-3}{1} r^{2n-4} + \dots \right\} I \quad (5.5.5)$$

### Theorem 5.5.3

If  $k$  is a prime integer and  $q \equiv \pm 1 \pmod{k}$  then there exists a polynomial  $g$  in  $Z[z]$  such that corresponding to each zero  $\theta$  of  $g$  the diagram  $D(\theta, q)$  depicts an action of  $\Delta(3,3,k)$  on  $PL(F_q)$ .

### Proof

If  $\theta$  and  $q$  are known we can determine (by using equations (5.4.1) to (5.4.6))  $\bar{u}$ ,  $\bar{v}$  and  $\bar{t}$ ; and thus can draw a coset diagram corresponding to the conjugacy class of non-degenerate homomorphisms representing the natural action of  $G^{s,3}(2, Z)$  on  $PL(F_q)$ .

Furthermore, by equation (5.5.3), if we take,

$$f(r) = \binom{k-1}{0} r^{k-1} - \binom{k-2}{1} r^{k-3} + \dots \quad (5.5.6)$$

We can substitute  $\theta$  for  $r^2$  in  $f(r)$  and obtain a minimal polynomial, say  $g$  in  $\theta$ .

Now  $(UV)$  has order  $k$  if and only if  $(UV)^k$  is a scalar multiple of the identity matrix  $I$ . This happens if and only if  $g(\theta) = 0$ . Since  $k$  is prime and

$q \equiv \pm 1 \pmod{k}$ , there will be  $\frac{k-1}{2}$  zeros of  $g(\theta) = 0$  and each zero  $\theta_i$  of  $g(\theta) = 0$  will yield a coset diagram in which every vertex is fixed by  $(\bar{u}\bar{v})^k$ , where  $\bar{u}\bar{v} \neq 1$ . Since no non-trivial linear-fractional transformation fixes more than two vertices in  $D(\theta, q)$ , we have  $(\bar{u}\bar{v})^k = 1$ . Thus, for each zero  $\theta_i$  of  $g(\theta) = 0$ , there will exist a coset diagram  $D(\theta, q)$  depicting the action of  $\Delta(3,3,k)$  on  $PL(F_q)$ .

When  $k$  is not a prime, we have two cases to deal with, namely,

- (i) when  $k$  is odd, and
- (ii) when  $k$  is even.

In the following we deal with them separately.

**Theorem 5.5.4**

If  $k$  is a positive odd integer (which is not a prime) and  $q \equiv \pm 1 \pmod{k}$  then  $g(\theta) = 0$  splits in  $F_q$  into equations  $g_{k/d}(\theta) = 0$  and  $g(\theta) = 0$  where  $d$  is the least prime divisor of  $k$ , and

- (i) if  $\theta_i$  is zero of  $g_{k/d}(\theta) = 0$  then  $D(\theta_i, q)$  depicts an action of  $\Delta(3,3,k/d)$  on  $PL(F_q)$ , and
- (ii) if  $\phi_j$  is zero of  $g_k(\theta) = 0$  then  $D(\phi_j, q)$  depicts an action of  $\Delta(3,3,k)$  on  $PL(F_q)$ .



**Proof**

The proof is similar to theorem 5.5.3 except that in equation (5.5.6) we substitute  $k/d$  for  $k$ , where  $d$  is the least prime divisor of  $k$ . Note that  $g(\theta) = g_{k/d}(\theta)g_k(\theta)$ .

**Theorem 5.5.5**

If  $k > 2$  is an even integer and a positive integer  $d$  divides  $k$ , where  $d < k$  and  $q \equiv \pm 1 \pmod{k}$ , then  $g(\theta) = \theta(\prod_{d|k} g_{k/d}(\theta))$  and corresponding to each  $\theta_i$ , where  $g_k(\theta_i) = 0$ , there exists  $D(\theta_i, q)$  depicting an action of  $\Delta(3,3,k/d)$  on  $PL(F_q)$ .

**Proof**

Since  $k > 2$  is an even integer, then  $g(\theta)$  will split in  $F_q$  into factors namely,  $g_{k/2}(\theta)$  and  $g_k(\theta)$ , where  $g_{k/2}(\theta)$  is obtained from equation (5.5.6) by taking  $k/2$  instead of  $k$  and  $g_k(\theta) = g(\theta)/g_{k/2}(\theta)$ .

If  $k/2$  is prime, we proceed as in theorem 5.5.3 and if  $k/2$  is odd, we proceed as in theorem 5.5.4. If  $k/2$  is even, the polynomial  $g_{k/2}(\theta)$  splits into factors,  $g_{k/4}(\theta)$  and  $g_n(\theta)$  where  $g_{k/4}(\theta)$  is obtained from equation (5.5.6) by replacing  $k$  by  $k/4$ . Here  $g_n(\theta) = g_{k/2}(\theta)/g_{k/4}(\theta)$ . We continue in this way (keeping in mind when  $k/2$  is prime, odd or even) until we get no more factors. In this way, we get  $g(\theta) = \theta(\prod_{d|k} g_{k/d}(\theta))$ . If  $\theta_i$  is zero of  $g_{k/d}(\theta) = 0$ , then every vertex of  $D(\theta_i, q)$  will be fixed by  $(\overline{uv})^{k/d}$  where  $d < k$  and  $\overline{uv} \neq 1$ . Again by the fact that no non-trivial linear-fractional transformation fixes more than two

vertices in  $D(\theta, q)$ , we get  $(\overline{uv})^{k/d} = 1$ . So, the diagram  $D(\theta, q)$  will depict an action of  $\Delta(3,3, k/d)$  on  $PL(F_q)$ .

## 5.6 CONJUGACY CLASS CORRESPONDING TO $\theta = 3$

Considering the case for  $\theta = 3$ , we observe that this is the only parameter, which gives the coset diagrams  $D(3, p)$  for the actions of  $\Delta(3,3, k)$  on  $PL(F_q)$ . Thus, we have proved the following theorem.

### Theorem 5.6.1

For any coset diagram  $D(\theta, p)$ , where  $p = 12n \pm 1$  for a positive integer  $n$ ,  $\theta = 3$  if and only if  $\overline{uv}$  has order 6.

### Proof

Put  $k = 6$  in equation (5.5.6), then  $f(r) = r^5 - 4r^3 + 3r$ . As  $\theta = r^2$ , we can substitute  $\theta$  for  $r^2$  in  $f(r)$  and obtain a polynomial in  $\theta$ . Now  $(UV)^6$  is a multiple of  $I$  if  $f(r) = 0$ . That is,  $r(r^4 - 4r^2 + 3) = 0$ . Substituting  $r^2 = \theta$ , we get  $r(\theta^2 - 4\theta + 3) = 0$ . If we take  $r = 0$  then  $\theta$  being equal to  $r^2$  will be zero and so the class of non-degenerate homomorphisms  $\alpha$  will contain involutions. That is, in this case we will get  $(\overline{uv})^2 = 1$ , which gives us a group known as the tetrahedral group of order 12 [13]. Since we are taking  $k$  to be different from 2 therefore  $r \neq 0$ .

$$\text{Hence } f(\theta) = \theta^2 - 4\theta + 3 = (\theta - 1)(\theta - 3) = 0.$$

Again  $\theta = 1$  evolves a conjugacy class of non-degenerate homomorphism  $\sigma : \Delta(3,3,3) \rightarrow G^*(2, q)$ . This implies that  $\theta = 3$  if and only if  $(\bar{u}\bar{v})^6 = 1$ .

As an illustration, we now give an example for  $\theta = 3$ .

### Example 5.6.2

The coset diagram  $D(3,13)$  is a homomorphic image of an action of  $\Delta(3,3,6)$  on  $PL(F_{13})$ .

### Proof

By equation (5.4.6),  $\theta = r^2$  and so  $r^2 = 3 \equiv 16$  implies that  $r = \pm 4$ . Let us take  $r = 4$ . Now substitute the value of  $r$  in (5.4.5) and suppose that  $k = 1$ . We get  $s^2 = 3 \equiv 16$  implying that  $s = \pm 4$ . Let us choose  $s = 4$ . If we suppose  $e = 0$  in equation (5.4.2) we have  $f^2 = -1 \equiv 25$ , that is,  $f = \pm 5$ . Suppose  $f = 5$  and substitute the value of  $r, s, d, k$  and  $f$  in equations (5.4.3) and (5.4.4) to obtain  $3 = a + 10c$  and  $-1 = 10a - c$ . Solving these equations for  $a$  and  $c$  we get  $a = -2$  and  $c = 7$ . Thus  $U = \begin{bmatrix} -2 & 7 \\ 7 & 1 \end{bmatrix}$ ,  $V = \begin{bmatrix} 0 & 5 \\ 5 & -1 \end{bmatrix}$ , and  $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ . So, our projective images will be  $\bar{u} : z \rightarrow \frac{-2z+7}{7z+1}$ ,  $\bar{v} : z \rightarrow \frac{5}{5z-1}$ ,  $\bar{t} : z \rightarrow \frac{-1}{z}$  respectively, where  $z \in PL(F_{13})$ .

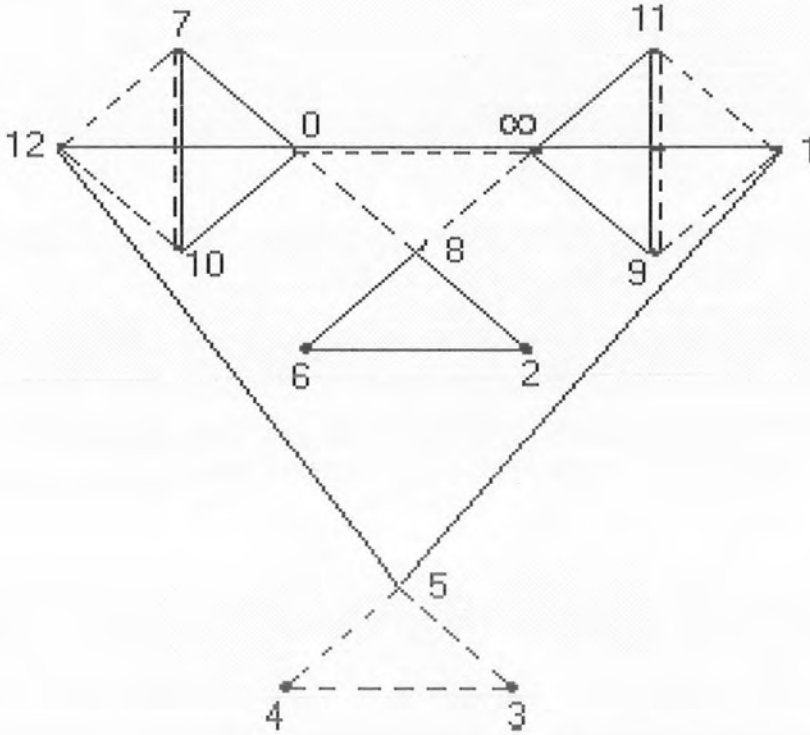
The linear-fractional transformation  $\bar{u}, \bar{v}$  and  $\bar{t}$  act respectively as:

$$(0 \ 7 \ 10)(1 \ 12 \ 5)(2 \ 8 \ 6)(9 \ 11 \ \infty)(3)(4),$$

$$(0 \ 8 \ \infty)(1 \ 11 \ 9)(3 \ 5 \ 4)(7 \ 12 \ 10)(2)(6), \text{ and}$$



$(0 \infty)(1 \ 12)(2 \ 6)(3 \ 4)(7 \ 11)(9 \ 10)(5)(8)$  yielding the coset diagram  $D(3,13)$ :



We note that each vertex of the diagram is fixed by  $(\overline{uv})^6$ . As no non-trivial linear-fractional transformation can fix more than two vertices therefore  $(\overline{uv})^6 = 1$ . Thus; the above coset diagram  $D(3,13)$  is a homomorphic image of  $\Delta(3,3,6)$ .

#### 4.7 CONJUGACY CLASSES OF THE NON-DEGENERATE HOMOMORPHISM

In this section, we have parametrized the actions of  $G^{*3,3}(2, Z)$  on  $PL(F_q)$ , except for a few uninteresting ones, by the elements of  $F_q$ . It is also proved that the conjugacy classes of non-degenerate homomorphism  $\sigma$  are in one-to-one correspondence with the conjugacy classes of non-trivial elements of  $G^{*3,3}(2, q)$ , under a correspondence which assigns to the homomorphism  $\sigma$  the class containing  $(uv)\sigma$ . Of course, this will mean that we can actually parametrize the actions of  $G^{*3,3}(2, q)$  on  $PL(F_q)$ , except for a few uninteresting ones, by the elements of  $F_q$ . We have developed a useful mechanism by which one can construct a unique coset diagram, attributed to Graham Higman [26], for each conjugacy class of these non-degenerate homomorphism which depict the actions of  $G^{*3,3}(2, Z)$  on  $PL(F_q)$ .

The transformations  $u : z \rightarrow \frac{z-1}{z}$ ,  $v : z \rightarrow \frac{-1}{z+1}$  and  $t : z \rightarrow \frac{1}{z}$  generate  $G^{*3,3}(2, Z)$ , subject to defining relations (1.3.2). Thus to choose a homomorphism  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  amounts to choosing  $\bar{u} = u\sigma$ ,  $\bar{v} = v\sigma$  and  $\bar{t} = t\sigma$ , in  $G^{*3,3}(2, q)$  such that

$$\bar{u}^3 = \bar{v}^3 = \bar{t}^2 = (\bar{u}\bar{t})^2 = (\bar{v}\bar{t})^2 = 1 \quad (5.7.1)$$

Both  $G^{3,3}(2, Z)$  and  $G^{*3,3}(2, Z)$  have index 2 in their automorphism groups. Let  $\delta$  be the automorphism on  $G^{*3,3}(2, Z)$  defined by  $u\delta = tut$ ,  $v\delta = v$ , and  $t\delta = t$ . The homomorphism  $\sigma' = \delta\sigma$  is called the dual homomorphism of  $\sigma$ .

This, of course, means that if  $\sigma$  maps  $u, v, t$  to  $\bar{u}, \bar{v}, \bar{t}$ , then  $\sigma'$  maps  $u, v, t$  to  $\bar{t}\bar{u}\bar{t}, \bar{v}, \bar{t}$  respectively. Since the elements  $\bar{u}, \bar{v}, \bar{t}$  as well as  $\bar{t}\bar{u}\bar{t}, \bar{v}, \bar{t}$  satisfy the relations (5.7.1), therefore the solutions of these relations occur in dual pairs. Of course, if  $\sigma$  is conjugate to  $\tau$  then  $\sigma'$  is conjugate to  $\tau'$ . The parameter of  $\sigma$ , or of the conjugacy class containing  $\sigma$ , is the parameter of  $\bar{u}\bar{v}$ .

Thus for each  $\theta$ , which is a square in  $F_q$ , there exists a unique coset diagram. It is unique for  $\theta$  in  $F_q$  in the sense that the diagram is the same except for the labels for any element in the conjugacy class that, it represents; only the vertices vary. Hence if we know  $\theta$ , we can find some homomorphism  $\sigma$  and hence, we can draw a coset diagram.

We define a pair  $\bar{u}, \bar{v}$ , satisfying the relations  $\bar{u}^3 = \bar{v}^3 = 1$ , in  $G^{3,3}(2, q)$  to be invertible if there exists  $\bar{t}$  in  $G^{*3,3}(2, q)$  such that  $\bar{t}^2 = 1, \bar{t}\bar{u}\bar{t} = \bar{u}^{-1}$  and  $\bar{t}\bar{v}\bar{t} = \bar{v}^{-1}$ .

## 5.8 PARAMETERS FOR THE CONJUGACY CLASSES OF $G^{*3,3}(2, q)$

If the natural mapping  $GL(2, q) \rightarrow G^{*3,3}(2, q)$  maps a matrix  $M$  to the element  $g$  of  $G^{*3,3}(2, q)$  then  $\theta = \frac{(tr(M))^2}{\det(M)}$  is an invariant of the conjugacy class of  $g$ . We refer to it as the parameter of  $g$  or of the conjugacy class. Of course, every element in  $F_q$  is the parameter of some conjugacy class in  $G^{*3,3}(2, q)$ . For instance, the class represented by a matrix with characteristic polynomial  $z^2 - \theta z + \theta \neq 0$  if  $\theta \neq 0$  or  $z^2 - 1$  if  $\theta = 0$ .

If  $q$  is an odd and  $g$  is not an involution, then  $g$  belongs to  $G^{3,3}(2, q)$  if and only if  $\theta$  is a square in  $F_q$ . On the other hand,  $g: z \rightarrow \frac{az+b}{cz+d}$ , where  $a, b, c, d \in F_q$ , has a fixed point in the natural representation of  $G^{3,3}(2, q)$  on  $PL(F_q)$  if and only if the discriminant,  $a^2 + d^2 - 2ad + 4bc$ , of the quadratic equation  $k^2c + k(d-a) - b = 0$  is a square in  $F_q$ . Since we have the determinant  $ad - bc$  is 1 and the trace  $a + d$  is  $r$ , then the discriminant is  $(\theta - 4)$ . Thus,  $g$  has fixed point in the natural representation of  $G^{3,3}(2, q)$  on  $PL(F_q)$  if and only if  $(\theta - 4)$  is a square in  $F_q$ .

With the help of equation 5.5.6, we can construct the following table.

<u><math>k</math></u>	<b>Equation satisfied by <math>\theta</math></b>
1	$\theta = 4$
2	$\theta = 0$
3	$\theta - 1 = 0$
4	$\theta - 2 = 0$
5	$\theta^2 - 3\theta + 1 = 0$
6	$\theta - 3 = 0$
7	$\theta^3 - 5\theta^2 + 6\theta - 1 = 0$
8	$\theta^2 - 4\theta + 2 = 0$
9	$\theta^3 - 6\theta^2 + 9\theta - 1 = 0$

10	$\theta^2 - 5\theta + 5 = 0$
11	$\theta^5 - 9\theta^4 + 28\theta^3 - 35\theta^2 + 15\theta - 1 = 0$
12	$\theta^2 - 4\theta + 1 = 0$
13	$\theta^6 - 11\theta^5 + 45\theta^4 - 84\theta^3 + 70\theta^2 - 21\theta + 1 = 0$
14	$\theta^6 - 120\theta^5 + 55\theta^4 - 120\theta^3 + 126\theta^2 - 56\theta + 7 = 0$
15	$\theta^7 - 13\theta^6 + 66\theta^5 - 165\theta^4 + 210\theta^3 - 126\theta^2 + 28\theta - 1 = 0$
16	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 106\theta^2 - 40\theta + 4 = 0$
17	$\theta^8 - 15\theta^7 + 91\theta^6 - 286\theta^5 + 495\theta^4 - 462\theta^3 + 210\theta^2 - 36\theta + 1 = 0$
18	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 105\theta^2 - 36\theta + 3 = 0$
19	$\theta^9 - 17\theta^8 + 120\theta^7 - 455\theta^6 + 1001\theta^5 - 1287\theta^4 + 9242\theta^3 - 330\theta^2 + 45\theta - 1 = 0$
20	$\theta^8 - 17\theta^7 + 104\theta^6 - 352\theta^5 + 661\theta^4 - 680\theta^3 + 356\theta^2 - 80\theta + 5 = 0$

**Lemma 5.8.1**

If  $\bar{t}$  inverts both  $\bar{u}$  and  $\bar{v}$  of  $G^{*3,3}(2, q)$ , then  $\overline{uv}$  is of order 3 or 1.

**Proof**

From section 5.4, we have  $U = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, V = \begin{bmatrix} e & gk \\ g & -e-1 \end{bmatrix}$  and

$$T = \begin{bmatrix} l & m \\ n & -l \end{bmatrix}, \text{ where}$$

$$kg^2 + e^2 + e + 1 = 0 \quad (5.8.1)$$

Let  $\text{trace}(UV) = r = gk - g + e + 1$  implies  $gk - g = r - e - 1$ . We note that the  $\det(UV)$  is  $-g^2k - e^2 - e = -(g^2k + e^2 + e) = 1$ . Because,  $\bar{i}^2 = (\overline{ui})^2 = (\overline{vi})^2 = 1$ , then by lemma 4.2.1,  $m = n - l$  and so

$$(2e - g + 1)l + (gk + g)n = 0 \quad (5.8.2)$$

Now for  $T$  to be a non-singular matrix, we should have  $\det(T) \neq 0$ , that is:

$$nl - l^2 - n^2 \neq 0 \quad (5.8.3)$$

Thus the necessary and sufficient conditions for the existence of  $\bar{i}$  in  $G^{*3,3}(2, q)$  are the equations (5.8.2) and (5.8.3). Hence  $\bar{i}$  exists in  $G^{*3,3}(2, q)$  unless  $nl - l^2 - n^2 = 0$ . Of course, if both  $2e - g + 1$  and  $gk + g$  are equal to zero, then the existence of  $\bar{i}$  is trivial. If not, then  $\frac{l}{n} = \frac{-(gk + g)}{(2e - g + 1)}$ , and so equation

(5.8.3) is equivalent to  $(gk + g)^2 + (2e - g + 1)^2 + (2e - g + 1)(gk + g) \neq 0$ . Thus, there exist,  $\bar{i}$  in  $G^{*3,3}(2, q)$  such that  $\bar{i}^2 = (\overline{ui})^2 = (\overline{vi})^2 = 1$  unless  $(gk + g)^2 + (2e - g + 1)(gk + g) = -(2e - g + 1)^2$ . But if  $(gk + g)^2 + (2e - g + 1)(gk + g) = -(2e - g + 1)^2$ , then,  $g^2k^2 + g^2 + 2g^2k + 2egk + 2eg - g^2k - g^2 + gk + g = -(4e^2 + g^2 + 1 + 4e - 2g - 4eg) = -[4e^2 + 4e + 1 + g^2 - 2g - 4eg] = -\{4g^2k - 3 + g^2 - 2g - 4eg\}$ . Simplification gives:

$$(gk - g)^2 + (gk - g) + 2e(gk - g) - g^2k = 3 \quad (5.8.4)$$



Since  $gk - g = r - e - 1$ , equation (5.8.4) can be further simplified as:

$$r^2 - r - 2 = 0 \tag{5.8.5}$$

Equation (5.8.5) implies that  $r^2 - 2 = r$ . Squaring both sides of this equation we obtain  $r^4 + 4 - 4r^2 = r^2$ . Now substitute  $r^2 = \theta$  to obtain  $\theta^2 - 5\theta + 4 = 0$  which gives  $\theta = 1, 4$ .

Now,  $\theta = 1$  implies that the order of  $\overline{uv}$  is 3 and  $\theta = 4$  implies that the order of  $\overline{uv}$  is 1.

Next, we shall find a relationship between the parameters of the dual homomorphism. We first prove the following.

**Lemma 5.8.2**

Any non-trivial element  $\overline{g}$  of  $G^{*3,3}(2, q)$  whose order is not equal to 1 or 3 is the image of  $uv$  under some non-degenerate homomorphism  $\sigma$  of  $G^{*3,3}(2, Z)$  into  $G^{*3,3}(2, q)$ .

**Proof**

Using lemma 5.8.1, we show that every non-trivial element of  $G^{*3,3}(2, q)$  is a product of two elements of order 3. So we find elements  $\overline{u}, \overline{v}$  and  $\overline{t}$ , satisfying the relations (5.7.1) with  $\overline{uv}$  in a given conjugacy class.

The class to which we want  $\overline{uv}$  do not consist of involutions because  $\overline{g} = \overline{uv}$  is not of order 2. Thus the traces of the matrices  $UV$  and  $UVT$  are not

equal to zero, by lemma 4.2.1. Hence  $r \neq 0$ , and  $s \neq 0$ , so that we have  $\theta = r^2 \neq 0$ ; and it is sufficient to show that we can choose  $a, c, e, k$  in  $F_q$  so that  $r^2$  is indeed equal to  $\theta$ . The solution of  $\theta$  is therefore arbitrarily in  $F_q$ . We can choose  $r$  to satisfy  $r^2 = \theta$ . Equation (5.4.5) yields  $ks^2 = 2 + r - r^2$ . If  $r^2 \neq 2 + r$  we select  $k$  as above.

Any quadratic polynomial  $\lambda z^2 + \mu z + \nu$ , with coefficients in  $F_q$  takes at least  $\frac{q+1}{2}$  distinct values, as  $z$  runs through  $F_q$ ; since the equation  $\lambda z^2 + \mu z + \nu = k$  has at most two roots for fixed  $k$ ; and there are  $q$  elements in  $F_q$ , where  $q$  is odd. In particular,  $e^2 + e$  and  $-kg^2 - 1$  each take at least  $\frac{q+1}{2}$  distinct values as  $e$  and  $f$  run through  $F_q$ . Hence we can find  $e$  and  $f$  so that  $e^2 + e = -kg^2 - 1$  (equation 5.4.2).

Finally by substituting the values of  $r, s, k, e, g$  in equations (5.4.3) and (5.4.4) we obtain the values of  $a$  and  $c$ . These equations are linear equations for  $a$  and  $c$  with determinant  $-(2e+1)^2 - 4kg^2 = 3$ . It is non-zero, so that we can find  $a$  and  $c$  satisfying equation (5.4.1).

It is clear from (5.4.5) and (5.4.6) that  $\theta = 0$  when  $r = 0$  and  $\theta = 1$  or  $4$  when  $s = 0$ . The possibility that  $\theta = 0$  gives rise to the situation where  $\overline{uv}$  is of order 2. Similarly, the possibility  $\theta = 1$  leads to the situation where  $\overline{uv}$  is of order 3, and similarly  $\theta = 4$  yields  $\overline{uv}$  is of order 1.



**Lemma 5.8.3**

Any two non-degenerate homomorphism  $\sigma, \tau$  of  $G^{*3,3}(2, Z)$  into  $G^{*3,3}(2, q)$  are conjugate if  $(uv)\sigma = (uv)\tau$ .

**Proof**

Let  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  be the non-degenerate homomorphism such that  $\overline{uv}$  has parameter  $\theta$  constructed as in the proof of lemma 5.8.2 . We also suppose that the non-degenerate homomorphism  $\tau : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  has the same parameter  $\theta$ .

First, since there are just two classes of elements of order 2 in  $G^{*3,3}(2, Z)$ , one in  $G^{*3,3}(2, Z)$  and the other not, we can pass to a conjugate of  $\tau$  in which  $t\tau$  is represented by  $\begin{bmatrix} 0 & -k' \\ 1 & 0 \end{bmatrix}$  for some  $k' \neq 0$  in  $F_q$ . Then because  $u\tau$  and  $v\tau$  are both of order 3,  $u\tau$  must be represented by a matrix  $\begin{bmatrix} a' & k'c' \\ c' & -a'-1 \end{bmatrix}$  and  $v\tau$  must be represented by a matrix  $\begin{bmatrix} e' & k'g' \\ g' & -e'-1 \end{bmatrix}$ , with  $a', c', e', g', k'$  satisfying the equations (5.4.1), (5.4.2) and (5.4.3). Then  $\theta = r'^2 = r^2$  and  $(2+r)-\theta = k's'^2 = ks^2$ . Here since  $\theta$  and  $(2+r)-\theta$  are non-zero, so it follows that  $\frac{k'}{k}$  is a square in  $F_q$ .

Now  $v\sigma$  and  $v\tau$  are both of orders 3 and so are conjugate in  $G^{*3,3}(2, q)$ . So we can pass to a conjugate of  $\tau$  with  $v\sigma = v\tau$ . As  $t\sigma$  and  $t\tau$  are involutions

which invert  $v\sigma$ , and so belong to  $N(\langle v\sigma \rangle)$  there are two classes of such involutions, one in  $G^*(2, q)$  and the other not. Because  $t\sigma$  is  $\begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$  and  $t\tau$  is conjugate to  $\begin{bmatrix} 0 & -k' \\ 1 & 0 \end{bmatrix}$  and  $\frac{k'}{k}$  is a square,  $t\sigma$  and  $t\tau$  either both belong to  $G^{*3,3}(2, q)$  or neither. Hence they are conjugate in  $N(\langle v\sigma \rangle)$ . That is, passing to a new conjugate we can assume  $v\sigma = v\tau$ ,  $t\sigma = t\tau$ . This means that in the notations above, we can assume  $k' = k, g = g'$  and  $e = e'$ . We can also, by multiplying the matrix representing  $u\tau$  by a scalar, assume  $r = r'$  and  $s = s'$ . Then the equations (5.4.1), (5.4.2), (5.4.3) and (5.4.4) with  $a, c, e, k, g$  and then with  $a', c', e', g', k'$  and ensure that  $a = a'$  and  $c = c'$ . That is  $\sigma = \tau$ .

#### Theorem 5.8.4

The conjugacy classes of non-degenerate homomorphism of  $G^{*3,3}(2, Z)$  into  $G^{*3,3}(2, q)$  are in one-to-one correspondence with the non-trivial conjugacy classes of elements of  $G^{*3,3}(2, q)$  under a correspondence which assigns to any non-degenerate homomorphism  $\sigma$  the class containing  $(uv)\sigma$ .

#### Proof

Let  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  be a non-degenerate homomorphism such that it maps  $u, v$  to  $\bar{u}, \bar{v}$ . Let  $\theta$  be the parameter of the class represented by  $\bar{u}\bar{v}$ . Now  $\sigma$  is determined by  $\bar{u}, \bar{v}$  and each  $\theta$  evolves a pair  $\bar{u}, \bar{v}$  so that  $\sigma$  is associated with  $\theta$ . We shall call the parameter  $\theta$  of the class containing  $\bar{u}\bar{v}$ , the

parameter of the non-degenerate homomorphism of  $G^{*3,3}(2, Z)$  into  $G^{*3,3}(2, q)$ .

Now

$$UT = \begin{bmatrix} ck & -ak \\ -a-1 & -ck \end{bmatrix}$$

implies that  $\det(UT) = -k(a^2 + a + kc^2) = k$  (equation 5.4.1). Also,

$$(UT)V = \begin{bmatrix} kec - akc & k^2gc + ak(e+1) \\ -ae - e - kgc & -akc - kg + ck(e+1) \end{bmatrix}$$

implies that  $\text{trac}((UT)V) = 2kec - 2akc - kg + kc = -1(2akc - 2kec + kg - kc) = -ks$ . If  $\bar{u}, \bar{v}, \bar{t}$  satisfy the relations (5.7.1), then so do  $\bar{t}\bar{u}, \bar{v}, \bar{t}$ . So that the solution of relation (5.7.1) occur in dual pairs. Hence replacing the solutions in lemma 5.8.2

by  $\bar{t}\bar{u}, \bar{v}, \bar{t}$ , we have  $\theta = \frac{[\text{tr}((UT)V)]^2}{\det(UT)} = \frac{k^2s^2}{k} = ks^2$ . We then find a relationship

between the parameters of the dual non-degenerate homomorphism.

There is an interesting relationship between the parameters of the dual non-degenerate homomorphism.

### Corollary 5.8.5

If  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  is a non-degenerate homomorphism,  $\sigma'$  is its dual and  $\theta, \phi$  are their respective parameters then  $\theta + \phi = r + 2$ .

**Proof**

Let  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  be a non-degenerate homomorphism satisfying the relations  $u\sigma = \bar{u}, v\sigma = \bar{v}$  and  $t\sigma = \bar{t}$ . Let  $\sigma'$  be the dual of  $\sigma$ . As in section 5.4, we choose the matrices  $U = \begin{bmatrix} a & ck \\ a & -a-1 \end{bmatrix}, V = \begin{bmatrix} e & gk \\ g & -e-1 \end{bmatrix}$  and  $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ , representing  $\bar{u}, \bar{v}, \bar{t}$ , respectively such that they satisfy the equations from (5.4.1) to (5.4.5). Now by lemma 4.2.1, we have  $trace(UV) = 0$  if and only if  $(\bar{uv})^2 = 1$ . Also, we have  $\frac{trace(UVT)}{k} = s = 0$  if and only if  $(\bar{uvt})^2 = 1$ . Now  $\det(UV) = 1$ , thus giving the parameter of  $\bar{uv}$  equal to  $r^2 = \theta$ , say. Also since  $trave(UVT) = ks$  and  $\det(UVT) = k$  (since  $\det(U) = 1, \det(V) = 1$  and  $\det(T) = k$ ), we obtain the parameter of  $\bar{uvt}$  equal to  $ks^2$ , which we denote by  $\phi$ . Thus  $\theta + \phi = r^2 + ks^2$ . Substituting the values from equation (5.4.5), we thus obtain  $\theta + \phi = r + 2$ . Hence if  $\theta$  is the parameter of the non-degenerate homomorphism  $\sigma$ , then  $\phi = r + 2 - \theta$  is the parameter of the dual  $\sigma'$  of  $\sigma$ .

Theorem 5.8.4, of course, means that we can actually parametrize the non-degenerate homomorphism of  $G^{*3,3}(2, Z)$  into  $G^{*3,3}(2, q)$  except for a few uninteresting ones, by the elements of  $F_q$ . Since  $G^{*3,3}(2, q)$  has a natural permutation representation on  $PL(F_q)$ , any homomorphism  $\sigma : G^{*3,3}(2, Z) \rightarrow G^{*3,3}(2, q)$  gives rise to an action of  $G^{*3,3}(2, Z)$  on  $PL(F_q)$ . This action is represented by a coset diagram  $D(\theta, q)$ . We can draw a coset diagram representing a conjugacy class of non-degenerate homomorphism corresponding

to each parameter  $\theta$ , which is a square in  $F_q$ , by determining  $\bar{u}, \bar{v}$  with the help of theorem 5.8.4.

### Example 5.8.6

Let us consider an action of  $G^{*3,3}(2, Z)$  on  $PL(F_{11})$  and draw a coset diagram for this action. Suppose  $\theta = 5$ , then by equation (5.4.6),  $\theta = r^2$  and so  $r^2 = 5 \equiv 16 \pmod{11}$  implies that  $r = \pm 4$ . Let us take  $r = 4$ . Substituting the value of  $r$  in (5.4.5) and supposing that  $k = 1$ , we get  $s^2 = -10 \equiv 1$ . This implies that  $s = \pm 1$ . Let us choose  $s = 1$ . If we suppose  $e = 3$  in equation (5.4.2) we have  $g^2 = -13 \equiv 9$ , that is,  $g = \pm 3$ . Suppose  $g = 3$  and substitute the values of  $r, s, e, k$  and  $g$  in equations (5.4.3) and (5.4.4) to obtain  $0 = 7a + 6c$  and  $-2 = 6a - 7c$ . Solving these equations for  $a$  and  $c$ , we obtain  $a = 4$  and  $c = -1$ .

Thus  $U = \begin{bmatrix} 4 & -1 \\ -1 & -5 \end{bmatrix}$ ,  $V = \begin{bmatrix} 3 & 3 \\ 3 & -4 \end{bmatrix}$  and  $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ . So, our  $\bar{u}, \bar{v}$  and  $\bar{t}$  will be

$$\bar{u}: z \rightarrow \frac{4z-1}{-z-5}, \bar{v}: z \rightarrow \frac{3z+3}{3z-4} \text{ and } \bar{t}: z \rightarrow \frac{-1}{z} \text{ respectively.}$$

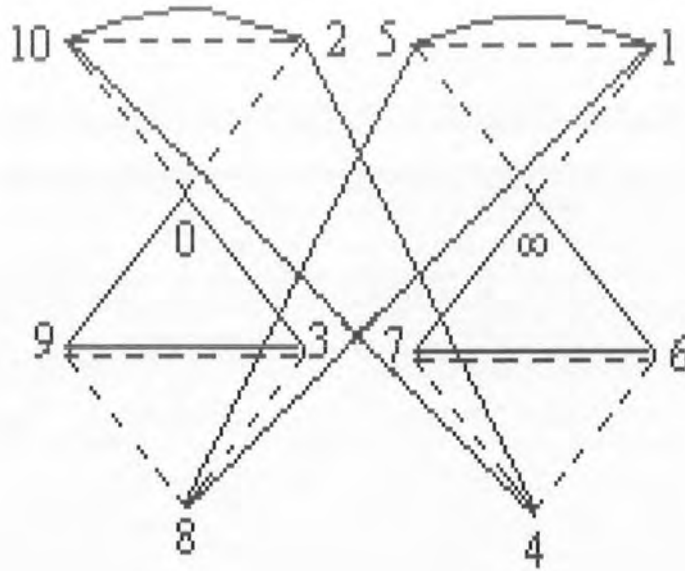
If we now consider the action of  $\bar{u}, \bar{v}$  and  $\bar{t}$ , we obtain

$$\bar{u} = (0 \ 9 \ 3)(\infty \ 7 \ 6)(1 \ 5 \ 8)(2 \ 10 \ 4),$$

$$\bar{v} = (0 \ 2 \ 10)(\infty \ 1 \ 5)(3 \ 9 \ 8)(4 \ 6 \ 7), \text{ and}$$

$$\bar{t} = (0 \ \infty)(1 \ 10)(2 \ 5)(3 \ 7)(4 \ 8)(6 \ 9).$$

The coset diagram for this action will be



**Example 5.8.7**

Let us again consider an action of  $G^{3,3}(2, Z)$  on  $PL(F_{11})$  and draw a coset diagram for the non-degenerate homomorphism  $\sigma'$ . As in example 5.8.6,  $\theta = 5$  implies that  $r = 4$ . Since for the dual homomorphism, we have  $\theta + \phi = r + 2$  which gives  $\phi = 1$ . By Corollary 5.8.5,  $ks^2 = \phi$ . Let us take  $k = 1$ . Then  $s^2 = 1$  implies that  $s = \pm 1$ . Let us choose  $s = 1$ . Solving equations (5.8.3) and (5.4.4),

we have  $r = 4, e = 2, a = -4$  and  $c = -3$ . Thus  $U = \begin{bmatrix} -4 & -3 \\ -3 & 3 \end{bmatrix}, V = \begin{bmatrix} 2 & 2 \\ 2 & -3 \end{bmatrix}$

and  $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$  respectively. So, our  $\bar{u}, \bar{v}$  and  $\bar{t}$  will be  $\bar{u} : z \rightarrow \frac{4z+3}{3z-3},$

$\bar{v} : z \rightarrow \frac{2z+2}{2z-3}$  and  $\bar{t} : z \rightarrow \frac{-1}{z}$  respectively, giving the action

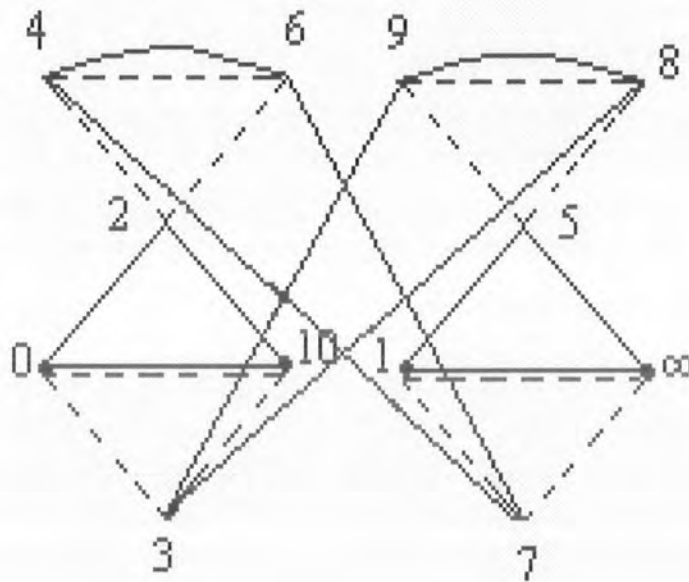


$$\bar{u} = (0 \ 10 \ 2)(1 \ \infty \ 5)(3 \ 8 \ 9)(4 \ 7 \ 6),$$

$$\bar{v} = (0 \ 3 \ 10)(1 \ 7 \ \infty)(2 \ 6 \ 4)(5 \ 8 \ 9), \text{ and}$$

$$\bar{t} = (0 \ \infty)(1 \ 10)(2 \ 5)(3 \ 7)(4 \ 8)(6 \ 9).$$

The coset diagram for this action will be:



Thus, both the actions in above examples for the non-degenerate homomorphism and its dual have the same coset diagram except the labeling of the vertices is different.

## 5.9 PARAMETRIZATION OF THE ACTIONS OF $\Delta(3, 3, k; n_1)$

Let  $\Delta(3, 3, k; n_1)$  denotes the triangular group  $\langle u, v, t : u^3 = v^3 = (uv)^k = w^n = t^2 = (ut)^2 = (vt)^2 = 1 \rangle$ , where  $w = (uvu^{-1}v^{-1})$ .

As we have,  $U = \begin{bmatrix} a & kc \\ c & -a-1 \end{bmatrix}$  and  $V = \begin{bmatrix} e & kg \\ g & -e-1 \end{bmatrix}$ . So,

$U^{-1} = \begin{bmatrix} -a-1 & -kc \\ -c & a \end{bmatrix}$  and  $V^{-1} = \begin{bmatrix} -e-1 & -kg \\ -g & e \end{bmatrix}$ . Thus,

$$UV = \begin{bmatrix} ae + kgc & akg - kce - kc \\ ec - ag - g & kgc + ac + a + e + 1 \end{bmatrix}$$

$$\text{and } U^{-1}V^{-1} = \begin{bmatrix} ae + a + c + kgc + 1 & akg + kg - kec \\ ec + c - ag & kgc + ae \end{bmatrix}.$$

From the equation (5.4.3), the trace of  $UV$  is,

$$r = 2ae + 2kgc + a + e + 1 \quad (5.9.1)$$

Also,

$$UVU^{-1}V^{-1} = \begin{bmatrix} (ae + kgc)(ae + a + c + kgc + 1) & (ae + kgc)(akg + kg - kec) \\ + (akg - kce - kc)(ec + c - ag) & + (akg - kec - kc)(kgc + ae) \\ (ec - ag - g)(ae + a + e + kgc + 1) & (ec - ag - g)(akg + kg - kec) \\ + (kgc + ac + a + e + 1)(ec + c - ag) & + (kgc + ac + a + e + 1)(kgc + ae) \end{bmatrix}.$$

Let  $l$  be the trace of  $W = UVU^{-1}V^{-1}$ , then  $l = 2(ae + kg)(kgc + ae + a + e + 1) + (c + ce - ag)(akg - kce - kc) + (ce - ag - g)(akg - kce + kg)$

By equation (5.9.1), we have



$$l = 2\left(\frac{r-a-e-1}{2}\right)\left(\frac{r-a-e-1}{2} + a+e+1\right) + k\left(c - \frac{s+c-g}{2}\right)\left(\frac{s-c-g}{2}\right) + k\left(-g - \frac{s+c-g}{2}\right)\left(\frac{s+c-g}{2} + g\right)$$

Simplification gives,

$$4l = 2r^2 - 2r - 2ks^2 + 4 \quad (5.9.2)$$

By equation (5.4.5), we have

$$l = 2 - ks^2 \quad (5.9.3)$$

or

$$l = r^2 - r \quad (5.9.4)$$

Since  $\det(W) = 1$  and  $\text{trace}(W) = l$ , therefore the characteristic equation of  $W$  is:

$$W^2 - lW + I = 0 \quad (5.9.5)$$

or

$$W^2 = lW - I \quad (5.9.6)$$

Multiplying equation (5.9.6) by  $W$  to obtain

$$W^3 = lW^2 - WI \quad (5.9.7)$$

Substituting the value of  $W^2$  from equation (5.9.6) in equation (5.9.7), we get

$$W^3 = (l^2 - 1)W - lI \quad (5.9.8)$$

On recursion, equation (5.9.8) yields

$$W^{n_1} = \left\{ \binom{n_1-1}{0} l^{n_1-1} - \binom{n_1-2}{1} l^{n_1-3} + \dots \right\} W - \left\{ \binom{n_1-2}{0} l^{n_1-2} - \binom{n_1-3}{1} l^{n_1-4} + \dots \right\} l \quad (5.9.9)$$

Furthermore, if we let

$$f(l) = \binom{n_1-1}{0} l^{n_1-1} - \binom{n_1-2}{1} l^{n_1-3} + \dots \quad (5.9.10)$$

One can find a minimal polynomial for positive integer  $n_1$  by the equation:

$$g_{n_1}(\theta) = \frac{f_{n_1}(\theta)}{g_{d_1}(\theta)g_{d_2}(\theta)\dots g_{d_m}(\theta)} \quad (5.9.11)$$

where  $d_1, d_2, \dots, d_m$ , are the divisors of  $n$  such that  $1 < d_i < k, i = 1, 2, \dots, m$  and  $f_{n_1}(\theta)$  is obtained by the equation (5.9.10).

The degree of the minimal polynomial is obtained as:

$$\deg[g_{n_1}(\theta)] = \deg[f_{n_1}(\theta)] - \sum \deg[g_{d_i}(\theta)] \quad (5.9.12)$$

where  $\deg[f_{n_1}(\theta)] = \begin{cases} n_1 - 1, & \text{if } n_1 \text{ is odd} \\ \frac{n_1}{2}, & \text{if } n_1 \text{ is even} \end{cases}$ . Also,  $\deg[g_{p^k}(\theta)] = \frac{p^k}{2} - \frac{p^{k-1}}{2}$ ,

where  $p$  is a prime. Thus, one can construct the following table:

$n_1$	Minimal equation satisfied by $l$
1	$l = 2$
2	$l = 0$
3	$l^2 - 1 = 0$
4	$l^2 - 2 = 0$
5	$l^4 - 3l^2 + 1 = 0$
6	$l^2 - 3 = 0$
7	$l^6 - 5l^4 + 6l^2 - 1 = 0$
8	$l^4 - 4l^2 + 2 = 0$
9	$l^6 - 6l^4 + 9l - 1 = 0$
10	$l^4 - 5l^2 + 5 = 0$

and so on.

### Example 5.9.1

Let us consider an action of  $G^{*3,3}(2, Z)$  on  $PL(F_{11})$  and draw a coset diagram for this action. Suppose  $l=1$ , then by equation (5.9.3), and supposing that  $k=1$ , we get  $s^2=1$ . This implies that  $s=\pm 1$ . Let us choose  $s=1$ . If we suppose  $e=2$  in equation (5.4.2) we have  $g^2=-7\equiv 4$ , that is,  $g=\pm 2$ . Suppose  $g=2$  and substituting the values of  $k$  and  $s$  in equation (5.4.5) to obtain  $r=4$ . Putting the values of  $r, s, e, k$  and  $g$  in equations (5.4.3) and (5.4.4) to obtain  $5a+4c=1$  and  $4a-5c=-1$ . Solving these equations for  $a$  and  $c$ , we obtain  $a=-4$  and  $c=-3$ . Thus  $U=\begin{bmatrix} -4 & -3 \\ -3 & 3 \end{bmatrix}$ ,  $V=\begin{bmatrix} 2 & 2 \\ 2 & -3 \end{bmatrix}$  and  $T=\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$  respectively. So, our  $\bar{u}, \bar{v}$  and  $\bar{t}$  will be  $\bar{u}: z \rightarrow \frac{4z+3}{3z-3}$ ,  $\bar{v}: z \rightarrow \frac{2z+2}{2z-3}$  and  $\bar{t}: z \rightarrow \frac{-1}{z}$  respectively, giving the action;

$$\bar{u} = (0 \ 10 \ 2)(1 \ \infty \ 5)(3 \ 8 \ 9)(4 \ 7 \ 6),$$

$$\bar{v} = (0 \ 3 \ 10)(1 \ 7 \ \infty)(2 \ 6 \ 4)(5 \ 8 \ 9), \text{ and}$$

$$\bar{t} = (0 \ \infty)(1 \ 10)(2 \ 5)(3 \ 7)(4 \ 8)(6 \ 9).$$

The coset diagram for this action is same as in example 5.8.7, in which every vertex of the diagram is fixed by  $(\bar{u}\bar{v}\bar{u}^{-1}\bar{v}^{-1})^3$  and  $(\bar{u}\bar{v})^5$ .

## REFERENCES

- [1] J. L. Alperin and R. B. Bel, *Groups and representations*, New York, Springer-Verlag, 1995.
- [2] G. Baumslag, J. W. Morgan and P. B. Shalen, *Generalized triangle groups*, *Math. Proc. Camb. Phil. Soc.*, 102, 1987, 25-31.
- [3] H. R. Brahana, *On the groups generated by two operators of orders two and three whose product is of order 8*, *Amer. Jour. Math.*, 53(1931), 891-901.
- [4] R. Bowen and C. Series, *Markov maps associated with Fuchsian groups*, *Publ. Math. IHES*, 50(1979), 153-170.
- [5] W. Burnside, *Theory of groups of finite order*, Dover Publications, Inc. New York (2<sup>nd</sup> ed.), 1995.
- [6] A. Caley, *The theory of groups, graphical representations*, *Amer. Jour. Math.*, 1(1878b), 174-176.
- [7] L. E. Dickson, *Linear groups: with exposition of the Galois field theory*, Dover Pub. Inc. N. York, 1958.
- [8] C. M. Campbell, M. D. E. Conder and E. F. Robertson, *Defining-relations for Hurwitz Groups*, *Glasgow Math. Jour.*, 36(1994), 363-370.
- [9] M. D. E. Conder, *Some results on quotients of triangle groups*, *Bull. Austral. Math. Soc.*, 29(1984), 73-90.

- [10] M. D. E. Conder, Generators for alternating and symmetric groups, Jour. London Math. Soc., 2(1980),75-86.
- [11] M. D. E. Conder, Some results on quotients of triangle groups, Bull. Austral. Math. Soc., 29(1984), 73-90.
- [12] H. S. M. Coxeter, The abstract group  $G^{m,n,p}$ , Trans. Amer. Math. Soc., 45(1939), 73-150.
- [13] H. S. M. Coxeter, and W. O. J Moser, Generators and relations for discrete groups, Springer-verlag, 1980.
- [14] B. Everitt, Permutation representations of the  $(2, 4, r)$  triangle groups, Bull. Austral. Math. Soc., 49(1994), 499-511.
- [15] B. Everitt, Alternating quotients of the  $(3,q,r)$  triangle groups, Comm. Algebra, 25, 6(1997), 1817-1832.
- [16] B. Fine and G. Rosenberger, A note on generalized triangle groups, Abh. Math. Sem. Univ. Hamburg, 56(1986), 233-244.
- [17] H. Hilton, An introduction to the theory of groups of finite orders, Oxford, Clarendon Press, 1908.
- [18] A.M.Macbeath, Generators of linear-fractional groups, Number Theory, Proc. Symp. in Pure Math., 12(AMS,1969),14-32.
- [19] H. Maschke, The representation of finite groups, especially of the rotation groups of the regular bodies in three and four dimensional spaces, Amer. Jour. Math. 18(1896), 156 – 194.

- [29] Q. Mushtaq, On word structure of the modular group over finite and real quadratic fields, *Discrete Mathematics*, 178(1998), 155-164.
- [30] D. J. S. Robinson, *A course in the theory of groups*, 2<sup>nd</sup> ed., New York, Springer-Verlag, 1995.
- [31] J. S. Rose, *A Course on group theory*, Cambridge University Press, Cambridge, 1978.
- [32] A. Sinkov, The number of abstract definitions of  $LF(2,p)$  as a quotient group of  $(2,3,n)$ , *Jour. Algebra*, 12(1969), 525-532.
- [33] W. W. Stothers, Subgroups of the modular group, *Proc. Camb. Phil. Soc.*, 75(1974), 139-153.
- [34] W. W. Stothers, Subgroups of the  $(2,3,7)$ -triangle group, *Manuscripta Math.*, 20(1977), 323-334.
- [35] J. H. C. Whitehead, On certain sets of elements in a free group, *Proc. London Math. Soc.*, Ser. 2, 41(1936), 48-56.
- [36] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.