LINEAR GROUPS AND THEIR ACTIONS ON CERTAIN FIELDS

By

MUHAMMAD ASLAM

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

LINEAR GROUPS AND THEIR ACTIONS ON CERTAIN FIELDS

By

MUHAMMAD ASLAM

Supervised by
Prof. Qaiser Mushtaq

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

Dedicated to

My parents, wife and children

ACKNOWLEDGEMENT

All thanks and praises to Almighty God, the most Merciful and Compassionate, who gave me the courage and guidance to finish this work.

My deepest gratitude to my supervisor, **Professor Qaiser Mushtaq**, whose constant encouragement and guidance was certainly instrumental in the completion of this work.

I am grateful to my research fellows, Major M. Ashiq and Major Tariq Maqsood, for their sincere help and cooperation.

In the end, I would like to thank my parents for their continuous blessings. Their special prayers and unlimited love has been a constant source of guidance for me. I cannot forget to thank my wife, Aneela Aslam, whose moral support and encouragement enabled me to complete this task.

Muhammad Aslam

NOTATIONS

Most of the set theoretic and group theoretic notations used in this thesis are standard, and are available in [8], [9] and [26]. However, some special notations which have been used extensively in this thesis are presented in the following.

$G_{6,6}(2,Z) =< u,v : u^6 = v^6 = 1 >$

$G^*_{6,6}(2,Z) =< u,v,t : u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 >$

$\Delta(l,m,n) =< u,v : u^l = v^m = (uv)^n = 1 >$

$\Delta(6,6,k) =< u,v : u^6 = v^6 = (uv)^k = 1 >$

$\Delta^*(l,m,n) =< u,v,t : u^l = v^m = t^2 = (uv)^n = (ut)^2 = (vt)^2 = 1 >$

$\Delta^*(6,6,k) =< u,v,t : u^6 = v^6 = t^2 = (uv)^k = (ut)^2 = (vt)^2 = 1 >$

$\Delta(6,6,k;n) =< u,v,t : u^6 = v^6 = t^2 = (uv)^k = (uvu^{-1}v^{-1})^n = (ut)^2 = (vt)^2 = 1 >$

$G_a = Stab(a) = \{g\epsilon G : a^g = a\}$

If A is a square matrix then the trace of the matrix A is denoted by $Tr(A)$

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

CONTENTS

PREFACE

An extension of degree 2 of the field of rational numbers Q is called the quadratic field. Since $Q(\sqrt{n_1}) = Q(\sqrt{n_2})$ if and only if $n_1 = c^2 n_2$, where $c \in Q$, therefore any quadratic field has the form $Q(\sqrt{n})$, where n is a square-free integer that is uniquely determined by the field. In what follows, n will always be taken to be this integer. When $n > 0$, $Q(\sqrt{n})$ is called a real, and when $n < 0$ an imaginary, quadratic field.

It is worthwhile to consider linear-fractional transformations x,y satisfying the relations $x^2 = y^m = 1$, with a view to studying an action of the group $< x,y >$ on real quadratic fields. If $y : z \to \frac{az+b}{cz+d}$ is to act on all real quadratic fields then a, b, c, d must be rational numbers and can be taken to be integers, so that $\frac{(a+d)^2}{ad-bc}$ is rational. But if $y : z \to \frac{az+b}{cz+d}$ is of order m one must have $\frac{(a+d)^2}{ad-bc} = \omega^2+\omega^{-2}+2$, where ω is a primitive $m-th$ root of unity. Now $\omega^2 + \omega^{-2}$ is rational, for a primitive $m-th$ root ω, only if $m = 1,2,3,4$ or 6. So these are the only possible orders of y . The group $< x,y >$ is C_2 (cyclic group of order 2) when $m = 1$. When $m = 2$, it is an infinite dihedral group and does not give inspiring information while studying its action on the real quadratic irrational numbers. For $m = 3$, the group $< x,y >$ is the modular group $PSL(2,Z)$. A real quadratic irrational number $\alpha = \frac{a+\sqrt{n}}{c}$ is said to be totally positive if α and its algebraic conjugate $\overline{\alpha}$ are both positive and said to be totally negative if both α and $\overline{\alpha}$ are negative. A real quadratic irrational number $\alpha = \frac{a+\sqrt{n}}{c}$ is said to be ambiguous if both α and $\overline{\alpha}$ are of opposite signs.

It is known that the group $G_{2,6}(2,Z) = < x,y : x^2 = y^6 = 1 >$ is generated by the linear fractional transformations x and y, where $(z)x = \frac{-1}{3z}$ and $(z)y = \frac{-1}{3(z+1)}$ are defined on the set of integers.

If we let $u = y$, $v = xyx$ then u, v can be considered as the linear fractional transformations defined by $(z)u = \frac{-1}{3(z+1)}$ and $(z)v = \frac{3z-1}{3z}$. So the group $G_{6,6}(2,Z) = < u,v >$ is a subgroup of the group $G_{2,6}(2,Z)$. That is, $G_{6,6}(2,Z) = < u,v : u^6 = v^6 = 1 >$ is the group of linear fractional transformations of the form $z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d \in Z$ and $ad-bc = 1$ or 3.

The linear-fractional transformation $t{:}z \rightarrow \frac{1}{3z}$ inverts u and v, that is, $t^2 = (ut)^2 = (vt)^2 = 1$ and so extends the group $G_{6,6}(2,Z)$ to $G^*_{6,6}(2,Z)$. The extended group $G^*_{6,6}(2,Z)$ has presentation $< u,v,t : u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 >$.

Triangle groups are represented by $\triangle(l,m,n) = < x,y : x^l = y^m = (xy)^n = 1 >$, where l,m,n are positive integers greater than or equal to one. It is well-known that $\triangle(l,m,n)$ is isomorphic to a subgroup of $PSL(2,C)$.

Let q be a prime. 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 $G^*_{6,6}(2,q)$ is then the group of linear fractional transformations of the form $z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d\epsilon F_q$ and $ad-bc \neq 0$, while $G_{6,6}(2,q)$ 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 four chapters. The aim of chapter one is to provide background material for succeeding chapters.

In chapter two, we show that for a given totally positive (negative) real quadratic irrational number there exists an alternating sequence of totally positive and totally negative numbers which terminate at an ambiguous number. The ambiguous numbers form a closed path in the coset diagram of the orbit αG, where $\alpha \in Q(\sqrt{n})$ and this is the only closed path in the diagram. We also show that the action of $G_{6,6}(2,Z)$ on the rational projective line is transitive and the coset diagram of this action is connected. Finally, we show that $u^6 = v^6 = 1$ are the defining relations for the group $G_{6,6}(2,Z)$. At the end, we show that the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$ is intransitive.

In chapter three, we study action of the group $G_{6,6}(2,Z)$ on the imaginary quadratic field $Q(\sqrt{-n})$ by using coset diagrams. In this chapter we show that the subset $\{\frac{a+\sqrt{-n}}{c} : a, \frac{a^2+n}{c}, c \in Z, c \neq 0\}$ of $Q(\sqrt{-n})$ is invariant under the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{-n})$ and the fixed points of the non identity elements of $G_{6,6}(2,Z)$ exists only when it acts on $Q^*(\sqrt{-3}) = \{\frac{a+\sqrt{-3}}{3c} : a, \frac{a^2+3}{3c}, c \in Z, c \neq 0\}$. Also we show that the total number of orbits under the action of $G_{6,6}(2,Z)$ on the set $Q^*(\sqrt{-n}) = \{\frac{a+\sqrt{-n}}{3c} : a, \frac{a^2+n}{3c}, c \in Z, c \neq 0\}$, when $n \neq 3$, are $2d(k)$ for $n = 3k$, $k \in Z$ and $4[d(k+1) + d(k+2) - 2]$ for $n = 3k+2$, $k \in Z$, where $d(n)$ is the arithmetic function. At the end, we show that the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{-n})$ is intransitive.

In chapter four, we parameterize the conjugacy classes of non-degenerate homomorphisms which represent actions of $\triangle(6,6,k) = < u, v : u^6 = v^6 = (uv)^k = 1 >$ on the projective line over F_q, $PL(F_q)$, where $q \equiv \pm 1 (\mathrm{mod}\, k)$. Also, for various values of k, we find conditions for the existence of coset diagrams depicting the permutation actions of $\triangle(6,6,k)$ on $PL(F_q)$. The conditions are polynomials with integer coefficients and the diagrams are such that every

vertex in them is fixed by $(\overline{u}\,\overline{v})^k$. In this way , we get $\triangle(6,6,k)$ as permutation groups on $PL(F_q)$. Also, we parameterize actions of $G^*_{6,6}(2,Z)$ on $PL(F_q)$ by the elements of F_q. We prove that the conjugacy classes of non-degenerate homomorphisms σ are in one-to-one correspondence with the conjugacy classes of non-trivial elements of F_q, under a correspondence which assigns to the homomorphism σ the class containing $(uv)\sigma$. Of course, this will mean that we can actually parameterize the actions of $G^*_{6,6}(2,Z)$ on $PL(F_q)$ by the elements of F_q. We develop a useful mechanism by which we can construct a unique coset diagram for each conjugacy class of these non-degenerate homomorphisms which depict the actions of $G^*_{6,6}(2,Z)$ on $PL(F_q)$.

A paper containing results from chapter two has been published [M.Aslam and Q.Mushtaq, Closed paths in the coset diagrams for $< y,t : y^6 = t^6 = 1 >$ acting on real quadratic fields, Ars Comb., 71(2004) 267-288.]. Another paper containing some results from this chapter has been accepted in the International Journal of Mathematics, Game Theory and Algebra. A paper containing results from chapter three has been submitted in an international journal for publication. Two papers containing results from chapter four have also been submitted for publication in international journals.

CHAPTER ONE

PRELIMINARIES

In this chapter we have given an introduction of linear groups, quadratic fields, finite fields, projective lines over the finite and infinite fields, the modular group and triangle groups. We have described also coset diagrams and their brief history. We have given here only those definitions which are relevant to the research work embodied in this thesis.

1.1 Group Actions

Let G be a group and X be a non-empy set. By an action of G on X we mean a function $\mu : X \times G \to X$ such that for all x in X and g, h in G the following axioms are satisfied (see, [5]).

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

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

For example, if G is a group and $X = G$ then $x^g = g^{-1}xg$ for $x \in X$ and $g \in G$ defines an action of G on itself.

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

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

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

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.

1.2 Quadratic Fields

An extension of degree 2 of the field of rational numbers Q is called the quadratic field. Since $Q(\sqrt{n_1}) = Q(\sqrt{n_2})$ if and only if $n_1 = c^2 n_2$, where $c \in Q$, therefore any quadratic field has the form $Q(\sqrt{n})$, where n is a square-free integer, that is, uniquely determined by the field. In what follows, n will always to be a square free integer.

When $n > 0$, $Q(\sqrt{n})$ is called a real, and when $n < 0$ an imaginary, quadratic field ([9], [13] and [21]).

If $\alpha \in Q(\sqrt{n})$ then $\alpha = a + b\sqrt{n}$, where $a, b \in Q$. The algebraic conjugate of $\alpha = a + b\sqrt{n}$ is defined by $\bar{\alpha}= a - b\sqrt{n}$. The trace of α, denoted by $Tr(\alpha)$ is defined as $\alpha + \bar{\alpha}$ and the norm of α, denoted by $N(\alpha)$ is defined as $\alpha\ \bar{\alpha}$. An $\alpha \in Q(\sqrt{n})$ is called an integer of $Q(\sqrt{n})$ if $Tr(\alpha), N(\alpha) \in Z$. For example, if $\alpha = \frac{1+\sqrt{5}}{2}$ belongs to $Q(\sqrt{5})$ then $Tr(\alpha) = 1$ and $N(\alpha) = -1$, therefore α is an integer in $Q(\sqrt{5})$. The algebraic integers in an arbitrary quadratic field do not necessarily have unique factorizations. For example, the fields $Q(\sqrt{-5})$ and $Q(\sqrt{-6})$ are not uniquely factorizable, because $21 = 3.7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ and $6 = 2.3 = \sqrt{-6}\,.\,\sqrt{-6}$. All other quadratic fields $Q(\sqrt{n})$ with $|n| \leq 7$ are uniquely factorable.

As a fundamental basis of $Q(\sqrt{n})$, that is, a basis of the ring of integers of the field $Q(\sqrt{n})$ over the ring of rational integers Z, one can take $\{1, \frac{1+\sqrt{n}}{2}\}$ when $n \equiv 1 (\mathrm{mod}\, 4)$ and

$\{1, \sqrt{n}\}$ when $n \equiv 2, 3 (\bmod 4)$.

Imaginary quadratic fields are the only type (apart from Q) with a finite unit group. This group has order 4 for $Q(\sqrt{-1})$ (and generator $\sqrt{-1}$), order 6 for $Q(\sqrt{-3})$ (and generator $\frac{1+\sqrt{-3}}{2}$), and order 2 (and generator -1) for all other imaginary quadratic fields.

For real quadratic fields the unit group is isomorphic to the direct product $\{\pm 1\} \times \{\varepsilon\}$, where $\{\pm 1\}$ is the group of order 2 generated by -1 and $\{\varepsilon\}$ is the infinite cyclic group generated by a fundamental unit ε. For example, for $Q(\sqrt{2})$, $\varepsilon = 1 + \sqrt{2}$.

1.3 Finite Fields

Let F be a field. There is a unique ring homomorphism $\phi : Z \to F$, defined by $\phi(n) = 1 + 1 + \ldots + 1$, n times, for $n \geq 0$ and $\phi(-n) = -\phi(n)$. If ϕ is injective, it identifies Z with a subring of F; then F also contains the field of fractions Q of Z. In this case, we say that F is of characteristic zero. If ϕ is not injective, its kernel is an ideal pZ, where $p > 0$; then Z/pZ is an integral domain (infact, a field) from which it follows that p is a prime number. In this case, we say that F is of characteristic p. We write F_p for Z/pZ. The subfield Q or F_p, of F is the smallest subfield of F, it is called the prime subfield of F. For every prime number p there exist fields of characteristic p, e.g., F_p.

Fields which have finitely many elements play an important role in group theory also. The most familiar examples of such fields are the fields Z_p for prime p, but these are not all. A finite field is uniquely determined up to isomorphism by the number of elements it contains; that this, number must be a power of a prime; and that for every prime p and integer $r > 0$, there exists a field with p^r elements. The field with $q = p^r$ elements is written by $GF(q)$ or F_q.

The ring Z of integers induces a natural ring structure on $Z_n = Z/nZ$, the integer modulo n. If n, is a prime p, then Z_p is in fact a field under this structure. $(Z_n)^r = \{(a_o, a_1, \dots, a_{r-1})$: $a_i \in Z_n\}$, where n is a prime, is a field. It is obtained in the following way.

We identify the sequence $(a_0, a_1, \dots, a_{r-1})$ with the polynomial $a_0 + a_1 t + \dots + a_{r-1} t^{r-1}$ in the ring of polynomial $Z_p[t]$ and choose a polynomial $f(t)$ of degree r which is irreducible in $Z_p[t]$ (that is, $f(t)$ has no zeros in Z_p).

We define multiplication of two sequences by multiplying the corresponding polynomials in $Z_p[t]$ and then reducing modulo $f(t)$. It is always possible to choose $f(t)$ in such a way that the non-zero elements of the field are just the powers $t, t^2, \dots, t^{p^r-1}$, the last of these being the multiplicative identity 1. The field constructed in this way is called the Galois field with p^r elements and is denoted by F_{p^r}.

For example, F_{3^2}, is constructed by choosing an irreducible polynomial $f(t) = t^2 + 2t + 2$ over $Z_3 = \{0, 1, 2\}$. The elements of F_{3^2} may be listed as follows.

Elements of F_{3^2}	Elements of F_{3^2} modulo $f(t)$
0	0
t	t
t^2	$t+1$
t^3	$2t+1$
t^4	2
t^5	$2t$
t^6	$2t+2$
t^7	$t+2$
t^8	1

We summarize the relevant properties of the finite fields.

There is a finite field with n elements if and only if n is a prime power, $n = q = p^r$.

If F is a finite field with q elements, then F is isomorphic with a Galois field F_q; in particular, the structure of the field does not depend on the choice of irreducible polynomial $f(t)$.

The multiplicative group of F_{p^r} is a cyclic group of order $p^r - 1$. A generator of this group is called a primitive element in the field. The group of field automorphisms of F_{p^r} is a cyclic group of order r generated by the automorphism $x \mapsto x^p$.

Let K be a field of order q, the multiplicative group K^* of non-zero elements of K is a cyclic group of order $q-1$. The elements of K are roots of the polynomial $x^q - x$. For example, $K^* = F_7^* = \{1,2,3,4,5,6\} = \{(\alpha^7 =)1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$, where $\alpha = 3$ is the primitive element of K^*. $K^* = F_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = \langle \alpha : \alpha^{11} = 1 \rangle$ where the primitive element of K^* is $\alpha = 2$.

1.4 A Projective Line over the Finite Field

Let V be a vector space over a field F, $V^* = V - \{0\}$, and $x, y \in V^*$, then the statement 'for some $\lambda \in F^* = F - \{0\}$, $x = \lambda y$, defines an equivalence relation on V^*, and the set of equivalence classes is called the projective space $PG(V)$. We shall denote the class of $x \in V^*$ by $[x] \in PG(V)$, and define a subspace $[U]$ of $PG(V)$, to the image of a subspace U of V under the map $x \longrightarrow [x]$. For geometric reasons it is convenient to say that if U has dimension k then $[U]$ has (projective) dimension $k-1$; in particular if $V = V(n,q)$, we write $PG(V) = PG(n-1,q)$.

We take $V = V(2,q)$ for a vector space of dimension 2 over a finite field F_q. V has q^2 elements. The projective space over $V = V(2,q)$ is the $PG(1,q)$ (called the projective line $PL(F_q)$) has $q+1$ points. It may be represented by q symbols $[1,z]$, (where z runs through F_q) and the additional symbol $[0,1]$. We often think of $PG(1,q) = PL(F_q)$ as the set $F_q \cup \{\infty\}$, where ∞ is image of $[0,1]$ under the bijection $[x_{0,}x_1] \leftrightarrow \frac{x_1}{x_0}$. Thus $PL(F_q) = PG(1,q) = F_q \cup \{\infty\} = \{0,1,2,3,\ldots,q-1\} \cup \{\infty\}$.

1.5 Linear Groups

Linear groups are important from the point of view of their applications in Physics and other branches of sciences. They are easy to deal with in the sense that many of their properties can be discussed by ordinary computation. They have been found useful in giving counter examples to answer various group theoretical conjectures (see,e.g., [17]).

Let V be a vector space of dimension n over a field F. The set $Hom_F(V,V)$ of all linear transformations of V is then a linear associative algebra. It possesses both the vector space and ring structures. The identity mapping I of V is the multiplicative identity of $Hom_F(V,V)$. An element ϕ of $Hom_F(V,V)$ is called invertible if there is a mapping ψ in $Hom_F(V,V)$ such that $\phi\psi = \psi\phi = I$.

The set of all invertible elements of $Hom_F(V,V)$ forms a group. This group is denoted by $GL_n(V)$ and is called the general linear group of dimension (or degree) n. If V has dimension n then $Hom_F(V,V)$ is denoted by $GL_n(V)$ and is called the general linear group of degree (or dimension) n. Closely related with $Hom_F(V,V)$ is the set $M_n(F)$ of all $n \times n$ matrices with entries from F. Both $Hom_F(V,V)$ and $M_n(F)$ are isomorphic as linear associative algebras. In $M_n(F)$, the matrices which have non-zero determinant (that is, non-singular or invertible matrices) form a group under multiplication. This group is denoted by $GL(n,F)$ and is isomorphic to $GL_n(V)$. Consequently, $GL(n,F)$ also is called the general linear group of dimension n.

In general, if R is a ring with identity and $M_n(R)$ is the ring of all $n \times n$ matrices with entries from R then the units of $M_n(R)$, that is, the invertible matrices, form the general linear group $GL(n,R)$.

Among the subgroups of $GL(n,F)$ there are some which are very important and deserve special attention. One of these is the special linear group $SL(n,F)$ of dimension n.

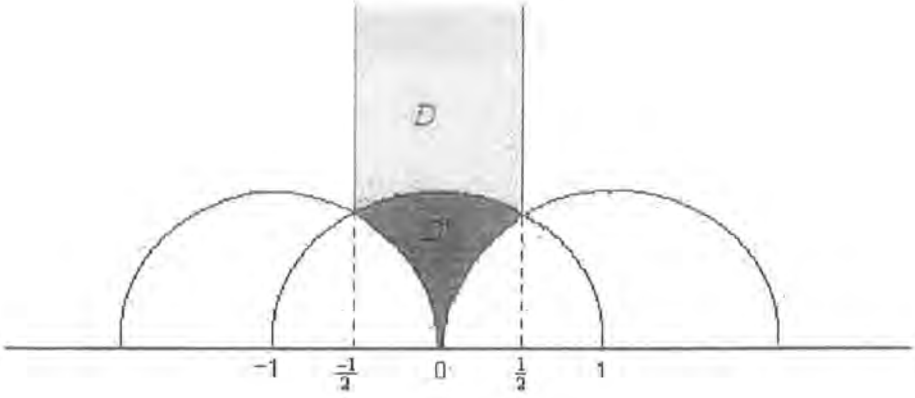
The significance of the special linear group $SL(2,Z) = \{[a_{ij}] : a_{ij} \in Z, i.j = 1,2, \det([a_{ij}]) = 1\}$ is related to the fact that in a 2-dimensional lattice bases $\{e_1,e_2\}$ and $\{f_1,f_2\}$ are related by the equations:

$$f_1 = ae_1 + ce_2$$
$$f_2 = be_1 + de_2$$

with $a,b,c,d \in Z$ 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, e_2. This guarantees that $ad - bc = 1$.

$SL(2,Z)$ act 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 the identity, so that we have an action of the group $SL(2,Z)/N$ where $N = \{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\}$. This quotient group is denoted by $PSL(2,Z)$ and is called the modular group. The modular group act on the upper half plane. A fundamental domain for it is given by the shaded region of the following modular region.



The upper half plane is a model of Lobachevsky plane and the motions in it preserve the orientation which are represented as transformations $z \to \frac{az+b}{cz+d}$ where $a,b,c,d \in R$ with $ad-bc = 1$. Thus the modular group $PSL(2,Z)$ is a discrete group of motions in the Lobachevsky plane. It is therefore possible to express the modular group as a group generated by two linear-fractional transformations $x : z \to \frac{-1}{z}$ and $y : z \to \frac{z-1}{z}$ such that $x^2 = y^3 = 1$ become its defining relations ([8]). It is well-known that $PSL(2,Z)$ is a free product of the cyclic group $< x >$ of order 2 and the cyclic group $< y >$ of order 3.

The linear-fractional transformation $t : z \to \frac{1}{z}$ 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 all transformations $z \to \frac{az+b}{cz+d}$ where a,b,c,d are in F_q and $ad-bc \neq 0$, while the group $PSL(2,q)$ is its subgroup consisting of all those linear-fractional transformations $z \to \frac{az+b}{cz+d}$ where $ad-bc$ is a non-zero square in F_q.

If $PGL(2,Z)$ act 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 linear-fractional groups for different fields arose independently. In 1852, A. F. Mobius studied 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 ([8]).

For the field Z_p, the linear-fractional group, and its subgroups were 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 the 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 ([26]).

1.6 The Group $G_{6,6}(2,Z)$

It is worthwhile to consider linear-fractional transformations x,y satisfying the relations $x^2 = y^m = 1$, with a view to studying an action of the group $< x,y >$ on real quadratic fields. If $y : z \to \frac{az+b}{cz+d}$ is to act on all real quadratic fields then a,b,c,d must be rational numbers and can be taken to be integers, so that $\frac{(a+d)^2}{ad-bc}$ is rational. But if $y : z \to \frac{az+b}{cz+d}$ is of order m one must have $\frac{(a+d)^2}{ad-bc} = \omega^2 + \omega^{-2} + 2$, where ω is a primitive $m-th$ root of unity. Now $\omega^2+\omega^{-2}$ is rational, for a primitive $m-th$ root ω, only if $m = 1,2,3,4$ or 6. So these are the only possible orders of y . The group $< x,y >$ is trivial when $m = 1$. When $m = 2$, it is an infinite dihedral group and does not give inspiring information while studying its action on the real quadratic irrational numbers. For $m = 3$, the group $< x,y >$ is the modular group $PSL(2,Z)$ and its action on real quadratic irrational numbers has been discussed in detail in [16] and [20].

It has been proved in [19] that the group $G_{2,6}(2,Z) = < x,y : x^2 = y^6 = 1 >$ is generated by the linear fractional transformations x and y, where $(z)x = \frac{-1}{3z}$ and $(z)y = \frac{-1}{3(z+1)}$ are defined on the set of integers.

1.7 Coset Diagrams

The method of representing group actions by graphs has a long and rich history. Graphs have applications in several branches of mathematics. They provide methods by which various algebraic and topological structures can be visualized. Graphical methods have been explicitly used to study the finitely generated groups. The graphs have proven themselves as an economical mathematical technique to prove certain important results (see [3],[4] and [7]). For finite groups of small order the graphs can be used instead of multiplication tables; they give the same information but in a much more efficient way (see [4],[22] and [24]). The first paper in which graphs were used explicitly was by A. Cayley [4] in 1878. After A. Cayley, Hurwitz [7] used graphs in1893 to represent groups. Then in 1896, H. Maschke used Cayley's 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 extensively used by Dehn, in 1910. Later, mathematicians like

O. Schreier, J. H. C. Whitehead [26], H. S. M. Coxeter and W. O. J. Moser [7], W. Burnside [3], et al., contributed seminal papers containing graphical representations of groups.

In 1978, G. Higman propounded the idea of coset diagrams for the modular group PSL(2,Z). M. D. E. Conder [5] and [6] 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 in 1983' [10].

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 [7] 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 v and u (say), are joined by an S_i –edge, of "colour i" directed from vertex v to vertex u, whenever $vS_i = u$.

$$v \to v\mathrm{S}_i = u$$

It may well happen that $vS_i = v$, in which case the v –vertex is joined to itself by an S_i –loop or a fixed point.

Formally, a coset diagram corresponding to a subgroup H of finite index in a finitely generated group G, is a directed edge, coloured graph, 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 Hg, for some g in G, draw an edge of colour E^x from Hg

to Hgx. This is very similar to the notion of a Schreier coset graph whose vertices represent the cosets of any given subgroup in a finitely-generated group, and also to that of a Caylay graph whose vertices are the group elements themselves, with trivial stabilizer. These diagrams may be drawn for any finitely generated groups depicting actions on any arbitrary sets or spaces.

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 that set, which is in fact equivalent to the natural action of G on the cosets of some subgroup H of index n. Coxeter and Moser [7] attribute these diagrams to Schreier. Steinberg [24] has proved that all finite simple groups of Lie type are two generators groups. It is also generally known that many, if not all, known finite simple groups are of Lie type. This means that all but a finite number of finite simple groups are two generator groups.

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.

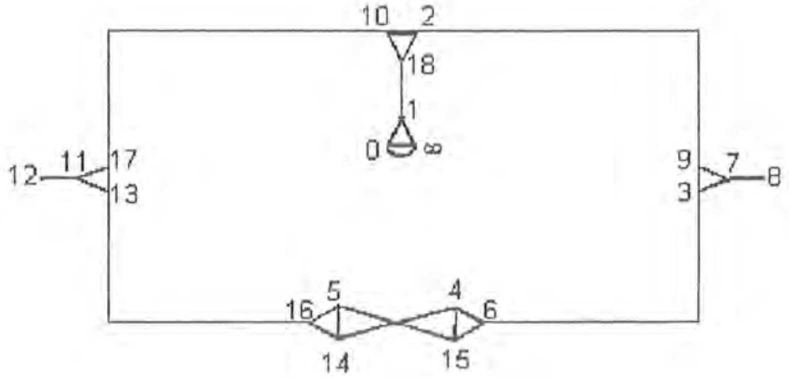
For instance, consider the action of $PGL(2,Z)$ on $PL(F_{19})$ defined by $x(z)=\frac{-1}{Z}$, $y(z)=\frac{Z-1}{Z}$, $t(z)=\frac{1}{Z}$ where $z \in \mathrm{PL}(\mathrm{F}_{19})$. We calculate the permutation representations of x, y

and *t* as follows:

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

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

$\overline{T}$: $(0\ \infty)(1)(2\ 10)(3\ 13)(4\ 5)(6\ 16)(7\ 11)(8\ 12)(9\ 17)(14\ 15)(18)$.



In 1983, Q. Mushtaq [15] studied the coset diagrams for the modular group extensively and proved that for each element θ of a finite field F_q, where q is a prime power, there exists a coset diagram for the natural permutation action of $PGL(2,Z)$ on $PL(F_q)$. The thesis contains also some partial answers concerning the 'Reconstruction Conjecture'. That is, the way a diagram is reproducible from certain types of fragments. If we have certain fragments of a coset diagram, we can find the conditions for the existence of those fragments in the respective coset diagram. The condition in fact is a polynomial in $Z[z]$. The modular group $PSL(2,Z)$ has many important homomorphic images. For many reasons connected with $PGL(2,q)$ actions on surfaces, it is important to know when $PGL(2,q)$ is an image of the extended modular group $PGL(2,Z)$. The solution to that has been given in [15].

Q. Mushtaq [17] in 1990 has parametrized the actions of $\Delta(2,3,7) = < x,y : x^2 = y^3 = (xy)^7 = 1 >$ on the projective lines over the finite fields F_q, with the help of coset diagrams. He also proved in this paper that for certain values of q, there is a natural homomorphism induced from $\Delta(2,3,7)$ and that there exist vertices on the vertical line of symmetry in the diagram depicting these actions.

In 1992, Q. Mushtaq [18] has shown that any homomorphism from $PGL(2,Z)$ into $PGL(2,q)$, except in the case where the order of the images of xy is 6 but the images of x and y do not commute in $PGL(2,q)$. He has also shown that every element in $PGL(2,q)$, not of order 1,2, or 6 is the image of xy under some non-degenerate homomorphism. He has parametrized the conjugacy classes of non-degenerate homomorphisms α with the non-trivial elements of F_q. Due to this parametrization, he has developed a useful mechanism by which one can construct a unique coset diagram for each conjugacy class, depicting the action of PGL(2,Z) on $PL(F_q)$.

Coset diagrams for the orbit of the modular group acting on real quadratic fields give some interesting information. By using these coset diagrams, Q. Mushtaq [16] has shown that for a fixed value of n, a non-square positive integer, there are only a finite number of real quadratic irrational numbers of the form $\theta = \frac{a+\sqrt{n}}{c}$, where θ and its algebraic conjugate $\bar{\theta}= \frac{a-\sqrt{n}}{c}$ have different signs, and that part of the coset diagram containing such numbers form a single circuit (closed path) and it is the only circuit in the orbit of θ.

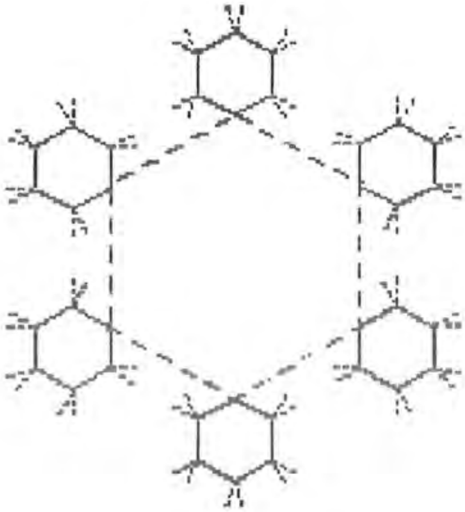
Let Ω denote the projective line over the real quadratic field and $PL(F_q)$ denote the projective line over the finite field F_q with q elements. Coset diagrams for the orbits of the modular group acting on Ω and $PL(F_q)$ give some interesting information. By using these diagrams in [20], he has determined a condition for the existence of an orbit of modular group on Ω containing a circuit of a given type. If such a circuit exists, he has found a condition under which the orbit contains a real quadratic irrational number α along with its algebraic conjugate $\bar{\alpha}$. As there are two projections from Ω to $PL(F_q)$, he has taken the care, when modular group acts on δ and determined necessary and sufficient conditions for the existence of two orbits of modular group: one containing α along with $\frac{1}{\alpha}$ and the other containing α together with $\frac{1}{\bar{\alpha}}$.

Coset diagrams may be used to provide diagramatic interpretations of several aspects of combinatorial group theory, such as the Reidemeister-Schreier procedure, as well as a proof of the Ree-Singerman theorem (on the cycle structures of generating-permutations for a transitive group). They can be used also as an equivalent to the Abelianized form of the Reidemeister-Schreier process. The same sort of method is also useful for the construction of infinite families of finite quotients of a given finitely-presented group. Use of coset diagrams to find torsion-free subgroups of certain finitely-presented groups has been instrumental in the construction of small volume hyperbolic 3-orbifolds and other hyperbolic 3-manifolds with interesting properties. They are also applied to the construction of arc-transitive graphs and maximal automorphism groups of Riemann surfaces [6].

1.8 Coset Diagrams for the Group $G^*_{6,6}(2,Z)$

The coset diagrams for the group $G^*_{6,6}(2,Z)$ are defined as follows. The six cycles of the transformation u are denoted by six unbroken edges of a hexagon (may be irregular) permuted anti-clockwise by u and the six cycles of the transformation v are denoted by six broken edges of a hexagon (may be irregular) permuted anti-clockwise by v . Fixed points of u and v, if they exist, are denoted by heavy dots. This graph can be interpreted as a coset diagram, with the vertices identified with the cosets of $Stab_{\alpha}(G_{6,6}(2,Z))$, the stabilizer of some vertex α of the graph, or as 1-skeleton of the cover of the fundamental complex of the presentation which corresponds to the subgroup $Stab_{v}(G_{6,6}(2,Z))$.

A general fragment of the coset diagram of the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$ will look as follows.



CHAPTER TWO

ACTION OF $G_{6,6}(2,Z)$ ON REAL QUADRATIC FIELDS

2.1 Introduction

In this chapter we have shown that the action of $G_{6,6}(2,Z)$ on the rational projective line $PL(Q)$ is transitive and the linear fractional transformations $u : z \to \frac{-1}{3(z+1)}$ and $v : z \to \frac{3z-1}{3z}$ generate $G_{6,6}(2,Z)$. Using the coset diagrams we have shown that $u^6 = v^6 = 1$ are defining relations for the group. We have shown that the set of ambiguous numbers is finite and that part of the coset diagram containing these numbers forms a single closed path and it is the only closed path in the orbit of α. We have also concluded that in the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$, $Stab_\alpha(G_{6,6}(2,Z))$ are the only non-trivial stabilizers and in the orbit $\alpha G_{6,6}(2,Z)$ there is only one (up to isomorphism) non-trivial stabilizer.

For a fixed non-square positive integer n, an element $\alpha = \frac{a+\sqrt{n}}{c}$ and its algebraic conjugate $\bar{\alpha}$= $\frac{a-\sqrt{n}}{c}$ may have different signs. If such is the case then we shall call such α an ambiguous number. If α and $\bar{\alpha}$ are both positive (negative), then we shall call α a totally positive (negative) number. Ambiguous numbers play an important role in the study of actions of the groups $G_{2,m}(2,Z) =< x,y : x^2 = y^m = 1 >$ for $m = 1,2,3,4$ or 6 on $Q(\sqrt{n})$.

In this chapter, we have considered the action of a subgroup of $G_{2,6}(2,Z) = < x,y : x^2 = y^6 = 1 >$, where $(z)x = \frac{-1}{3z}$ and $(z)y = \frac{-1}{3(z+1)}$ are linear fractional transformations, on the real quadratic irrational numbers.

If we let $v = xyx$, $u = y$ then v can be considered as the linear-fractional transformation defined by $(z)v = 1 - \frac{1}{3z}$ and $v^6 = 1$. Some number-theoretic properties of the ambiguous numbers belonging to the orbit of $G_{2,6}(2,Z)$ when acting on $Q^*(\sqrt{n}) = \{\frac{a+\sqrt{n}}{c} : a, c \in Z,$ $b = \frac{a^2-n}{c} \in Z$, $(a,b,c) = 1\}$ have been discussed in [19].

In this chapter, we have explored group-theoretic properties of this action vis-a-vis the orbit of α in $G_{6,6}(2,Z)$. We have shown that the set of ambiguous numbers in the orbit for the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$ is finite 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 α. We have shown here that in the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$, $Stab_\alpha(G_{6,6}(2,Z))$ are the only non-trivial stabilizers and in the orbit $\alpha G_{6,6}(2,Z)$ there is only one (up to isomorphism) non-trivial stabilizer.

We have used coset diagrams for the group $G_{6,6}(2,Z)$ and studied its action on the projective line over real quadratic fields. In [19], it has been observed that if $z \neq -1, \frac{-2}{3}, \frac{-1}{2}, \frac{-1}{3}, 0, \infty$ is one of the six vertices of a hexagon (with unbroken edges) in the coset diagram, then

(i) $z < -1$ implies that $(z)u > 0$,

(ii) $z > 0$ implies that $\frac{-1}{3} < (z)u < 0$,

(iii) $\frac{-1}{3} < z < 0$ implies that $\frac{-1}{2} < (z)u < \frac{-1}{3}$,

(iv) $\frac{-1}{2} < z < \frac{-1}{3}$ implies that $\frac{-2}{3} < (z)u < \frac{-1}{2}$,

(v) $\frac{-2}{3} < z < \frac{-1}{2}$ implies that $-1 < (z)u < \frac{-2}{3}$, and

(vi) $-1 < z < \frac{-2}{3}$ implies that $(z)u < -1$.

Also if $z \neq 1, \frac{2}{3}, \frac{1}{2}, \frac{1}{3}, 0, \infty$ is one of the six vertices of a hexagon (with broken edges) in the coset diagram, then

(i) $z < 0$ implies that $(z)v > 1$,

(ii) $z > 1$ implies that $\frac{2}{3} < (z)v < 1$,

(iii) $\frac{2}{3} < z < 1$ implies that $\frac{1}{2} < (z)v < \frac{2}{3}$,

(iv) $\frac{1}{2} < z < \frac{2}{3}$ implies that $\frac{1}{3} < (z)v < \frac{1}{2}$,

(v) $\frac{1}{3} < z < \frac{1}{2}$ implies that $0 < (z)v < \frac{1}{3}$, and

(vi) $0 < z < \frac{1}{3}$ implies that $(z)v < 0$.

We state here the following lemmas from [11] for later use.

Lemma 2.1.1 An $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ is a totally positive number if and only if one of the following is true.

(i) $a, b, c > 0$, where $b = \frac{a^2-n}{c}$

(ii) $a, b, c < 0$, where $b = \frac{a^2-n}{c}$

Lemma 2.1.2 An $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ is a totally negative number if and only if one of the following is true.

(i) $a < 0$ and $b > 0, c > 0$, where $b = \frac{a^2-n}{c}$

(ii) $a > 0$ and $b < 0, c < 0$, where $b = \frac{a^2-n}{c}$

Lemma 2.1.3 An $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ is an ambiguous number if and only if $bc < 0$, where $b = \frac{a^2-n}{c}$.

Lemma 2.1.4 If A is an invertible 2×2 matrix with entries from R(or F_q) such that A^2, A^3 are not scalar matrices then $A^6 = \lambda I$, $0 \neq \lambda \in R$ if and only if $\{Tr(A)\}^2 = 3\det(A)$.

Proof

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then $A^3 = \begin{bmatrix} a^3 + 2abc + bcd & a^2b + b^2c + bd^2 + abd \\ a^2c + bc^2 + cd^2 + acd & abc + 2bcd + d^3 \end{bmatrix}$.

If $A^6 = \lambda I$, then the trace of A^3 is equal to zero and so $a^3 + d^3 + 3abc + 3bcd = 0$. This implies that $(a+d)(a^2 + d^2 - ad + 3bc) = 0$ or $(a+d)[(a+d)^2 \quad -3(ad-bc)]$ or $(a+d)[\{Tr(A)\}^2 -3\det(A)] = 0$. But $a + d \neq 0$; hence $\{Tr(A)\}^2 = 3\det(A)$.

2.2 Existence of Ambiguous Numbers

Ambiguous numbers play an important role in the study of actions of the group $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$. We have proved here that $Stab_\alpha(G_{6,6}(2,Z))$ are the only non-trivial stabilizers in the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$ and that there is only one (up to isomorphism) non-trivial stabilizer in the orbit $\alpha G_{6,6}(2,Z)$.

Theorem 2.2.1 If $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ is a totally negative real quadratic irrational number then $(\alpha)v^i$ is totally positive for $i = 1,2,3,4$ or 5.

Proof

If $\alpha = \frac{a+\sqrt{n}}{c}$, where $b = \frac{a^2-n}{c}$, then $(\alpha)v = 1 - \frac{1}{3\alpha} = 1 - \frac{c}{3(a+\sqrt{n})} = \frac{(3a-c)+3\sqrt{n}}{3(a+\sqrt{n})} \times \frac{a-\sqrt{n}}{a-\sqrt{n}}$ $= \frac{-a+3b+\sqrt{n}}{3b}$. Hence the new values of a and c are $-a+3b$ and $3b$. Using these values, we then obtain the new value for b, that is, $\frac{(-a+3b)^2-n}{3b} = \frac{-6a+9b+c}{3}$. Similarly, the new values for a, b and c with respect to $(\alpha)v^i$ are:

α	a	b	c
$i=1$	$-a+3b$	$\frac{-6a+9b+c}{3}$	$3b$
$i=2$	$-5a+6b+c$	$-4a+4b+c$	$-6a+9b+c$
$i=3$	$-7a+6b+2c$	$\frac{-12a+9b+4c}{3}$	$3(-4a+4b+c)$
$i=4$	$-5a+3b+2c$	$-2a+b+c$	$-12a+9b+4c$
$i=5$	$-a+c$	$\frac{c}{3}$	$3(-2a+b+c)$

If α is a totally negative number then by Lemma 2.1.2 , either a, b, c satisfy (i) or (ii). If (i) is the case then from the above table the new a, b, c for $(\alpha)v^i$ are all positive. Hence by Lemma 2.1.1 $(\alpha)v^i$ are totally positive.

Similarly, if (ii) is the case then it is easy to see that the new values of a, b, c for $(\alpha)v^i$ are all negative. Then by Lemma 2.1.1 $(\alpha)v^i$ are totally positive.

Example 2.2.2 Let $\alpha = -2+\sqrt{3}$ then $a = -2, c = 1, n = 3$ and $b = \frac{a^2-n}{c} = 1$. Because a is negative and b, c are positive therefore α is a totally negative real quadratic irrational number. We can easily tabulate the following information.

α	-2	1	1
$(\alpha)v$	5	$\frac{22}{3}$	3
$(\alpha)v^2$	17	13	22
$(\alpha)v^3$	22	$\frac{37}{3}$	39
$(\alpha)v^4$	15	6	37
$(\alpha)v^5$	3	$\frac{1}{3}$	18

It is evident from the above information that the values of a, b and c for $(\alpha)v^i$, where $i = 1,2,3,4$ and 5, are positive. Therefore, $(\alpha)v^i$, for $i = 1,2,3,4$ and 5 are all totally positive.

Theorem 2.2.3 If $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ is a totally positive real quadratic irrational number then $(\alpha)u^j$ is totally negative for $j = 1,2,3,4$ or 5.

Proof

If $\alpha = \frac{a+\sqrt{n}}{c}$, where $b = \frac{a^2-n}{c}$, then $(\alpha)u = \frac{-1}{3(\alpha+1)} = \frac{-a-c+\sqrt{n}}{3(2a+b+c)}$. Hence the new values of a and c are respectively $-a-c$ and $3(2a+b+c)$. Using these values, we then obtain the new value for b, that is, $\frac{(-a-c)^2-n}{3(2a+b+c)} = \frac{c}{3}$. Similarly, the new values for a, b and c with respect to $(\alpha)v^j$ are:

α	a	b	c
$j = 1$	$-a-c$	$\frac{c}{3}$	$3(2a+b+c)$
$j = 2$	$-5a-3b-2c$	$2a+b+c$	$12a+9b+4c$
$j = 3$	$-7a-6b-2c$	$\frac{12a+9b+4c}{3}$	$3(4a+4b+c)$
$j = 4$	$-5a-6b-c$	$4a+4b+c$	$6a+9b+c$
$j = 5$	$-a-3b$	$\frac{6a+9b+c}{3}$	$3b$

If α is a totally positive number then by Lemma 2.1.1, a, b, c either satisfy (i) or (ii). If (i) is the case then from the above table the new a, b, c for $(\alpha)u^j$ are such that $a < 0$ and $b, c > 0$. Hence by Lemma 2.1.2 $(\alpha)u^j$ are totally negative for $j = 1,2,3,4,5$.

Similarly, if (ii) is the case then the new values of a, b, c for $(\alpha)u^j$, where $j = 1,2,3,4,5$ are such that $a > 0$ and $b, c < 0$. Then by Lemma 2.1.2 $(\alpha)u^j$ are totally negative.

Lemma 2.2.4 If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is an ambiguous number then one of $(\alpha)v^i$, where $i = 1,2,3,4$ or 5, is ambiguous and the other four are totally positive.

Proof

It is obvious that if l, m, n, p, q, r are the vertices of a hexagon then $\overline{l}, \overline{m}, \overline{n}, \overline{p}, \overline{q}, \overline{r}$ are also vertices of a hexagon in a coset diagram for the action of the group $G_{6,6}(2, Z)$..

First we suppose that α is a negative number. Then the possibilities for $\overline{\alpha}$ to be positive or negative are as follows:

α	$(\alpha)v$	$(\alpha)v^2$	$(\alpha)v^3$	$(\alpha)v^4$	$(\alpha)v^5$	$\overline{\alpha}$	$\overline{(\alpha)v}$	$\overline{(\alpha)v^2}$	$\overline{(\alpha)v^3}$	$\overline{(\alpha)v^4}$	$\overline{(\alpha)v^5}$
$-$	$+$	$+$	$+$	$+$	$+$	$+$	$-$	$+$	$+$	$+$	$+$
						$+$	$+$	$-$	$+$	$+$	$+$
						$+$	$+$	$+$	$-$	$+$	$+$
						$+$	$+$	$+$	$+$	$-$	$+$
						$+$	$+$	$+$	$+$	$+$	$-$

Similarly, if α is a positive number then

α	$(\alpha)v$	$(\alpha)v^2$	$(\alpha)v^3$	$(\alpha)v^4$	$(\alpha)v^5$	$\overline{\alpha}$	$\overline{(\alpha)v}$	$\overline{(\alpha)v^2}$	$\overline{(\alpha)v^3}$	$\overline{(\alpha)v^4}$	$\overline{(\alpha)v^5}$
+	−	+	+	+	+	−	+	+	+	+	+
+	+	−	+	+	+						
+	+	+	−	+	+						
+	+	+	+	−	+						
+	+	+	+	+	−						

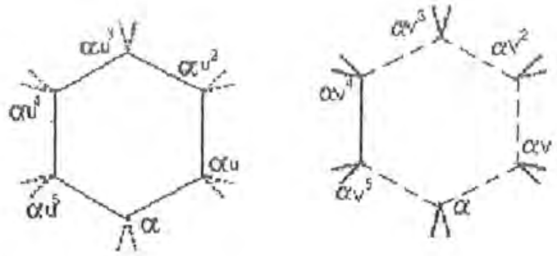
Therefore, from the above tables we can easily deduce that one of $(\alpha)v^i$, for $i = 1,2,3,4$ or 5 is ambiguous and the other four are totally positive.

Example 2.2.5 Let $\alpha = 1 + \sqrt{2}$ then $a = 1, c = 1, n = 2$ and $b = \frac{a^2-n}{c} = -1$. As $bc < 0$, therefore, α is an ambiguous real quadratic irrational number. We can easily tabulate the following information.

α	1	−1	1
$(\alpha)v$	−4	$\frac{-14}{3}$	−3
$(\alpha)v^2$	−10	−7	−14
$(\alpha)v^3$	−11	$\frac{-17}{3}$	−21
$(\alpha)v^4$	−6	−2	−17
$(\alpha)v^5$	0	$\frac{1}{3}$	−6

As it is evident from the above information, the values of a, b and c for $(\alpha)v^i$, where $i = 1,2,3$ and 4, are negative, therefore, $(\alpha)v^i$, for $i = 1,2,3$ and 4 are all totally positive. As for $(\alpha)v^5$, $bc < 0$, therefore, $(\alpha)v^5$ is an ambiguous real quadratic irrational number.

Diagrammatically, the six vertices representing the six cycles of u and v will be as follows.



Lemma 2.2.6 If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is an ambiguous number then one of $(\alpha)u^j$, for $j = 1,2,3,4$ or 5 , is ambiguous and the other four are totally negative numbers.

Proof

First, we suppose that α is a positive number. The possibilities for $\overline{\alpha}$ to be positive or negative are as follows:

α	$(\alpha)u$	$(\alpha)u^2$	$(\alpha)u^3$	$(\alpha)u^4$	$(\alpha)u^5$	$\overline{\alpha}$	$\overline{(\alpha)u}$	$\overline{(\alpha)u^2}$	$\overline{(\alpha)u^3}$	$\overline{(\alpha)u^4}$	$\overline{(\alpha)u^5}$
+	−	−	−	−	−	−	+	−	−	−	−
						−	−	+	−	−	−
						−	−	−	+	−	−
						−	−	−	−	+	−
						−	−	−	−	−	+

Similarly, if α is a negative number then:

α	$(\alpha)u$	$(\alpha)u^2$	$(\alpha)u^3$	$(\alpha)u^4$	$(\alpha)u^5$	$\overline{\alpha}$	$\overline{(\alpha)u}$	$\overline{(\alpha)u^2}$	$\overline{(\alpha)u^3}$	$\overline{(\alpha)u^4}$	$\overline{(\alpha)u^5}$
$-$	$+$	$-$	$-$	$-$	$-$	$+$	$-$	$-$	$-$	$-$	$-$
$-$	$-$	$+$	$-$	$-$	$-$						
$-$	$-$	$-$	$+$	$-$	$-$						
$-$	$-$	$-$	$-$	$+$	$-$						
$-$	$-$	$-$	$-$	$-$	$+$						

Therefore, from the above tables we can easily deduce that one of $(\alpha)v^j$, for $j = 1,2,3,4$ or 5 is ambiguous and the other four are totally positive.

We define the norm of $\alpha = \frac{a+\sqrt{n}}{c}$ by $\|\alpha\| = |a|$.

Theorem 2.2.7 If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is totally positive then

(i) $\|(\alpha)u^j\| > \|\alpha\|$, for $j = 1,2,3,4$ and 5.

(ii) $\|(\alpha)v^i\| < \|\alpha\|$ if $(\alpha)v^i$ is totally negative for $i = 1,2,3,4,$ or 5.

Proof

(i) If $\alpha = \frac{a+\sqrt{n}}{c}$, where $b = \frac{a^2-n}{c}$, then it is easy to caculate new values of a, b, c for $(\alpha)u^j$, where $j = 1,2,3,4$ and 5, as follows.

α	a	b	c
$j = 1$	$-a-c$	$\frac{c}{3}$	$3(2a+b+c)$
$j = 2$	$-5a-3b-2c$	$2a+b+c$	$12a+9b+4c$
$j = 3$	$-7a-6b-2c$	$\frac{12a+9b+4c}{3}$	$3(4a+4b+c)$
$j = 4$	$-5a-6b-c$	$4a+4b+c$	$6a+9b+c$
$j = 5$	$-a-3b$	$\frac{6a+9b+c}{3}$	$3b$

Since α is a totally positive number so either $a,b,c > 0$ or $a,b,c < 0$. If $a,b,c > 0$ (or $a,b,c < 0$), $\|(\alpha)u\| = |a+c|$, $\|(\alpha)u^2\| = |5a+3b+2c|$, $\|(\alpha)u^3\| = |7a+6b+2c|$, $\|(\alpha)u^4\| = |5a+6b+c|$ and $\|(\alpha)u^5\| = |a+3b|$. Thus, $\|(\alpha)u^j\| > \|\alpha\|$, for $j = 1,2,3,4$ and 5.

(ii) The new values of a,b,c for $(\alpha)v^i$, where $i = 1,2,3,4,$ or 5, are tabulated as follows.

α	a	b	c
$i=1$	$-a+3b$	$\frac{-6a+9b+c}{3}$	$3b$
$i=2$	$-5a+6b+c$	$-4a+4b+c$	$-6a+9b+c$
$i=3$	$-7a+6b+2c$	$\frac{-12a+9b+4c}{3}$	$3(-4a+4b+c)$
$i=4$	$-5a+3b+2c$	$-2a+b+c$	$-12a+9b+4c$
$i=5$	$-a+c$	$\frac{c}{3}$	$3(-2a+b+c)$

By Theorem 2.2.1, one of $(\alpha)v^i$, for $i = 1,2,3,4,$ or 5, is totally negative. Note also that since α is totally positive, there are only two possibilities, namely, either $a,b,c > 0$ or $a,b,c < 0$. We deal with these possibilities one by one.

We suppose that $(\alpha)v$ is totally negative. If $a,b,c > 0$ then from the above information, it is easy to see that $-a+3b < 0$. Hence $-a < -a+3b < a$ or $|-a+3c| < a$ or $\|(\alpha)v\| < \|\alpha\|$. Similarly, for $a,b,c < 0$, we note that $\|(\alpha)v\| < \|\alpha\|$.

Suppose that $(\alpha)v^2$ is totally negative, therefore,$(\alpha)v$ must be totally positive. If $a,b,c > 0$ then $-a+3b > 0$, $-6a+9b+c > 0$, $-5a+6b+c < 0$ and $-4a+4b+c > 0$. Since $-5a+6b+c = (-4a+4b+c)-a+2b$, therefore, $-a+2b < -5a+6b+c$ or $-a < -5a+6b+c < a$ or $|-5a+6b+c| < |a|$ or $\|(\alpha)v^2\| < \|\alpha\|$. Similarly, for $a,b,c < 0$, $\|(\alpha)v^2\| < \|\alpha\|$.

Now, suppose that $(\alpha)v^3$ is totally negative. Then $(\alpha)v$ and $(\alpha)v^2$ must be totally positive. If $a,b,c > 0$ then $-a+3b > 0$, $-6a+ 9b+c > 0$, $-5a+ 6b+c > 0$, $-4a+ 4b+c > 0$, $-7a+6b+ 2c < 0$ and $-12a+9b +4c > 0$. Since $-14a+12b +4c = (-12a+9b+4c)$ $-2a+3b$, therefore, $-2a < -14a+12b+4c$ or $-a < -7a +6b +2c$ or $-a < -7a+6b+2c < a$ or $|-7a+6b +2c| < |a|$ or $\|(\alpha)v^3\| < \|\alpha\|$. Similarly, for $a,b,c < 0$, we obtain $\|(\alpha)v^3\| < \|\alpha\|$.

Next, let $(\alpha)v^4$ be totally negative. Then $(\alpha)v$, $(\alpha)v^2$ and $(\alpha)v^3$ are totally positive. If $a,b,c > 0$ then . $-5a+3b +2c < 0$ and $-2a+b+c > 0$. Since $-5a+3b +2c = (-4a+2b +2c)$ $-a+b$, therefore $-a < -5a +3b+ 2c < a$ or $|-5a+3b +2c| < |a|$ or $\|(\alpha)v^4\| < \|\alpha\|$. Similarly, for $a,b,c < 0$ we get $\|(\alpha)v^4\| < \|\alpha\|$.

Finally, suppose that $(\alpha)v^5$ is totally negative. Therefore $(\alpha)v$, $(\alpha)v^2$, $(\alpha)v^3$ and $(\alpha)v^4$ are totally positive. If $a,b,c > 0$ then $-a+c < 0$, and so $-a < -a+ c < a$ or $|-a+c| < |a|$ or $\|(\alpha)v^5\| < \|\alpha\|$. Similarly, for $a,b,c < 0$ we have $\|(\alpha)v^5\| < \|\alpha\|$.

Example 2.2.8 Let $\alpha = 3+\sqrt{3}$ then $a = 3, c = 1, n = 3$ and $b = \frac{a^2-n}{c} = 6$ As a,b and c are positive therefore α is a totally positive real quadratic irrational number. We put this information in the following form.

α	3	6	1
$(\alpha)u$	-4	$\frac{1}{3}$	39
$(\alpha)u^2$	-35	13	94
$(\alpha)u^3$	-59	$\frac{94}{3}$	111
$(\alpha)u^4$	-52	37	73
$(\alpha)u^5$	-24	$\frac{73}{3}$	18
$(\alpha)v$	15	$\frac{37}{3}$	18
$(\alpha)v^2$	22	13	37
$(\alpha)v^3$	17	$\frac{22}{3}$	39
$(\alpha)v^4$	5	1	22
$(\alpha)v^5$	-2	$\frac{1}{3}$	3

It is clear from here that $(\alpha)u^j$, where $j = 1,2,3,4$ and 5, are totally negative numbers and $\|(\alpha)u^j\| > \|\alpha\|$ for $j = 1,2,3,4$ and 5. Also, $(\alpha)v^5$ is a totally negative number such that $\|(\alpha)v^5\| < \|\alpha\|$.

Theorem 2.2.9 If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is a totally negative number. Then

(i) $\|(\alpha)v^i\| > \|\alpha\|$, for $i = 1,2,3,4,$ or 5, and

(ii) $\|(\alpha)u^j\| < \|\alpha\|$ if $(\alpha)u^j$ is totally negative for $j = 1,2,3,4,$ and 5.

Proof

(i) If $\alpha = \frac{a+\sqrt{n}}{c}$, where $b = \frac{a^2-n}{c}$, then we can easily calculate new a,b,c for $(\alpha)v^i$ as follows.

α	a	b	c
$i = 1$	$-a + 3b$	$\frac{-6a+9b+c}{3}$	$3b$
$i = 2$	$-5a + 6b + c$	$-4a + 4b + c$	$-6a + 9b + c$
$i = 3$	$-7a + 6b + 2c$	$\frac{-12a+9b+4c}{3}$	$3(-4a + 4b + c)$
$i = 4$	$-5a + 3b + 2c$	$-2a + b + c$	$-12a + 9b + 4c$
$i = 5$	$-a + c$	$\frac{c}{3}$	$3(-2a + b + c)$

Since α is a totally negative number so $a > 0$, and $b < 0, c < 0$ or $a < 0$, and $b > 0, c > 0$. If $a > 0$, and $b < 0, c < 0$ (or $a < 0$, and $b > 0, c > 0$) then $\|(\alpha)v\| = |-a + 3b|$, $\|(\alpha)v^2\| = |-5a + 6b + c|$, $\|(\alpha)v^3\| = |-7a + 6b + 2c|$, $\|(\alpha)v^4\| = |-5a + 3b + 2c|$ and $\|(\alpha)v^5\|$ $= |-a + c|$. Hence, $\|(\alpha)v^i\| > \|\alpha\|$, for $i = 1, 2, 3, 4$ and 5.

(ii) Again, we can write information about $(\alpha)u^j$, as follows.

α	a	b	c
$j = 1$	$-a - c$	$\frac{c}{3}$	$3(2a + b + c)$
$j = 2$	$-5a - 3b - 2c$	$2a + b + c$	$12a + 9b + 4c$
$j = 3$	$-7a - 6b - 2c$	$\frac{12a+9b+4c}{3}$	$3(4a + 4b + c)$
$j = 4$	$-5a - 6b - c$	$4a + 4b + c$	$6a + 9b + c$
$j = 5$	$-a - 3b$	$\frac{6a+9b+c}{3}$	$3b$

Since in Theorem 2.2.3, we have seen that if α is totally positive then $(\alpha)u^j$, where $j = 1, 2, 3, 4$ and 5 are totally negative.

First, let us suppose that $(\alpha)u$ is totally positive. As α is totally negative, there are two possibilities, either $a < 0$, and $b > 0, c > 0$ or $a > 0$, and $b < 0$, $c < 0$. If $a < 0$, and $b > 0, c > 0$ then $-a - c > 0$. Hence $-a > -a - c > a$ or $|-a - c| < |a|$ or $\|(\alpha)u\| < \|\alpha\|$.

Similarly,$\|(\alpha)u\| < \|\alpha\|$ for $a > 0$, and $b < 0, c < 0$.

Now, suppose that $(\alpha)u^2$ is totally positive. Then $(\alpha)u$ must be totally negative.If $a < 0$, and $b > 0, c > 0$ then $2a + b + c > 0, -a - c < 0$, $-5a - 3b - 2c > o$ and $12a + 9b + 4c > 0$. Since, $-15a - 9b - 6c = (-12a - 9b - 4c)$ $-3a - 2c$, therefore $-15a - 9b - 6c < -3a$. Hence $a < -5a - 3b - 2c < -a$ or $|-5a - 3b - 2c| < |a|$ or $\|(\alpha)u^2\| < \|\alpha\|$. Similarly, $\|(\alpha)u^2\| < \|\alpha\|$ for $a > 0$, and $b < 0, c < 0$.

Let $(\alpha)u^3$ be totally positive. Then $(\alpha)u$ and $(\alpha)u^2$ are totally negative. If $a < 0$, and $b > 0$, $c > 0$ then $-a - c < 0$, $2a + b + c > 0$, $-5a - 3b -2c < 0$, $12a + 9b +4c > 0$, $-7a - 6b -2c > 0$ and $4a + 4b +c > 0$. Since $-14a - 12b - 4c = (-12a - 9b - 4c) - 2a - 3b < -2a$. Then $-7a - 6b -2c < -a$ or $a < -7a - 6b - 2c < -a$ or $\left|-7a - 6b - 2c\right| < |a|$ or $\|(\alpha)u^3\| < \|\alpha\|$ Similarly, $\|(\alpha)u^3\| < \|\alpha\|$ for $a > 0$, and $b < 0, c < 0$.

Next, suppose that $(\alpha)u^4$ is totally positive. Then $(\alpha)u, (\alpha)u^2$ and $(\alpha)u^3$ are totally negative. If $a < 0$, and $b > 0$, $c > 0$ then $-a - c < 0$, $2a + b +c > 0$, $-5a - 3b -2c < 0$, $12a + 9b +4c > 0$, $-7a - 6b -2c > 0$, $4a + 4b + c > 0$, $-5a - 6b -c > 0$ and $6a + 9b +c > 0$. Since$-10a - 12b - 2c = (-8a - 8b - 2c)$ $-2a - 4b$. Then $-10a - 12b - 2c < -2a$ or $a < -5a - 6b - c < -a$ or $|-5a - 6b - c| < |a|$ or $\|(\alpha)u^4\| < \|\alpha\|$ Similarly, $\|(\alpha)u^4\| < \|\alpha\|$ for $a > 0$, and $b < 0, c < 0$.

Finally, we suppose that $(\alpha)u^5$ is totally positive. If $a < 0$, and $b > 0$, $c > 0$ then $-a - 3b > 0$. This implies that $a < -a - 3b < -a$ or $|-a - 3b| < |a|$ or $\|(\alpha)u^5\| < \|\alpha\|$. Similarly, $\|(\alpha)u^5\| < \|\alpha\|$ for $a > 0$, and $b < 0, c < 0$.

Example 2.2.10 Let $\alpha = -3 + \sqrt{2}$ then $a = -3, c = 1, n = 2$ and $b = \frac{a^2-n}{c} = 7$. As a is negative and b, c are positive therefore α is a totally negative real quadratic irrational number. The information is tabulated as follows.

α	-3	7	1
$(\alpha)u$	2	$\frac{1}{3}$	6
$(\alpha)u^2$	-8	2	31
$(\alpha)u^3$	23	$\frac{31}{3}$	51
$(\alpha)u^4$	-28	17	46
$(\alpha)u^5$	-18	$\frac{46}{3}$	21
$(\alpha)v$	24	$\frac{82}{3}$	21
$(\alpha)v^2$	58	41	82
$(\alpha)v^3$	65	$\frac{103}{3}$	123
$(\alpha)v^4$	38	14	103
$(\alpha)v^5$	4	$\frac{1}{3}$	42

It is clear from this information that $(\alpha)v^i$, where $i = 1,2,3,4$ and 5 are totally positive numbers and $\|(\alpha)v^i\| > \|\alpha\|$, for $i = 1,2,3,4$ and 5. Also $(\alpha)u$ is a totally positive number such that $\|(\alpha)u\| < \|\alpha\|$.

Theorem 2.2.11 If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is a totally positive number, then there exists a sequence $\alpha(= \alpha_1), \alpha_2, \alpha_3, \ldots, \alpha_m$ such that α_i is alternately totally positive and totally negative number, for $i = 1,2,3,\ldots,m-1$ and α_m is an ambiguous number.

Proof

Since $\alpha = \alpha_1 = \frac{a+\sqrt{n}}{c}$ is a totally positive number so by Theorem 2.2.1 , one of $(\alpha)v^i$, for

$i = 1,2,3,4$ or 5, is totally negative. If $(\alpha)v^i$ is totally negative then by Theorem 2.2.7, $\|(\alpha)v^i\| < \|\alpha\|$. Also $(\alpha)v^i$ is totally negative, then, one of $(\alpha)v^iu^j$, for $j = 1,2,3,4$, and 5 is totally positive. If $(\alpha)v^iu^j$ is totally positive then by Theorem 2.2.9, $\|(\alpha)v^iu^j\| < \|(\alpha)v^i\| < \|\alpha\|$. If we let, $\alpha = \alpha_1$, $(\alpha)v^i = \alpha_2$and $(\alpha)v^iu^j = \alpha_3$ and continue in this way we obtain an alternate sequence $\alpha_1,\alpha_2,\alpha_3,\ldots,\alpha_m$ of totally positive and totally negative numbers such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| >\ldots> \|\alpha_m\|$. Since $\|\alpha_1\|,\|\alpha_2\|,\|\alpha_3\|, \ldots,\|\alpha_m\|$ is a decreasing sequence of non-negative integers so it must terminate. That is, after a finite number of steps we reach to α_m such that $\|\alpha_m\| < \sqrt{n}$. This means that, if $\alpha_m = \frac{a_1+\sqrt{n}}{c_1}$ then $\|\alpha_m\| = |a_1| < \sqrt{n}$. Thus $a_1^2 < \sqrt{n}$ or $a_1^2 - n < 0$ or $\frac{a_1^2-n}{c_1^2} < 0$ or $\alpha_m\overline{\alpha_m} < 0$. Hence α_m is an ambiguous number.

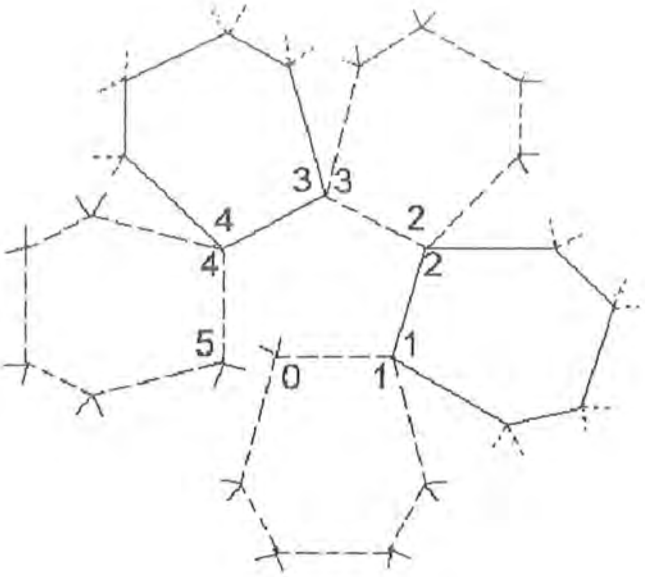
Example 2.2.12

If $\alpha = 6 + \sqrt{3}$ then $a = 6, c = 1, n = 3$ and $b = \frac{a^2-n}{c} = 33$. As a,b,c are positive, therefore α is a totally positive real quadratic irrational number, therefore:

$\alpha_0 = \alpha$	6	33	1	totally positive
$\alpha_1 = (\alpha_0)v^5$	-5	$\frac{1}{3}$	66	totally negative
$\alpha_2 = (\alpha_1)u^5$	4	13	1	totally positive
$\alpha_3 = (\alpha_2)v^5$	-3	$\frac{1}{3}$	18	totally negative
$\alpha_4 = (\alpha_3)u^5$	2	1	1	totally positive
$\alpha_5 = (\alpha_4)v^5$	-1	$\frac{1}{3}$	-6	ambiguous

We can see from the above information that $\alpha_0,\alpha_1,\alpha_2,\alpha_3,\alpha_4$and α_5 is an alternating sequence of totally positive and totally negative numbers and α_5 is an ambiguous number.

The above information is depicted in the following coset diagram in which $0,1,2,3,4$ and 5 represent $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ and α_5 respectively.



2.3 Existence of Closed Paths

The ambiguous numbers play an important role in studying the action of $G_{6,6}(2,Z)$ on $Q^*(\sqrt{n}) \cup \{\infty\}$. Let $\alpha \in Q^*(\sqrt{n})$ and $\alpha G_{6,6}(2,Z)$ denote an orbit of $Q^*(\sqrt{n})$. The existence of an ambiguous number in $\alpha G_{6,6}(2,Z)$ is related to the stabilizers of $G_{6,6}(2,Z)$. We describe the action of $G_{6,6}(2,Z)$ on $Q^*(\sqrt{n}) \cup \{\infty\}$ in the following way.

Theorem 2.3.1 The ambiguous numbers in the coset diagram for the orbit $\alpha G_{6,6}(2,Z)$, where $\alpha = \frac{a+\sqrt{n}}{3c} \in Q^*(\sqrt{n})$, form a closed path and it is the only closed path contained in it.

Proof

Let k_0 be an arbitrary ambiguous number in $\alpha G_{6,6}(2,Z)$. We pass on to another ambiguous number by successive applications of either u^j or v^i, for $i,j = 1,2,3,4$ or 5. Without loss of generality, we assume that $(k_0)u^j$ is another ambiguous number.

Since each hexagon, representing six edges of u or v, contains two ambiguous numbers (by virtue of Lemmas 2.2.4, 2.2.6) so at the second ambiguous number within the $k-th$ hexagon, we successively apply the second generator, namely u (or v) to reach the next ambiguous number in the $(k+1)-th$ hexagon.

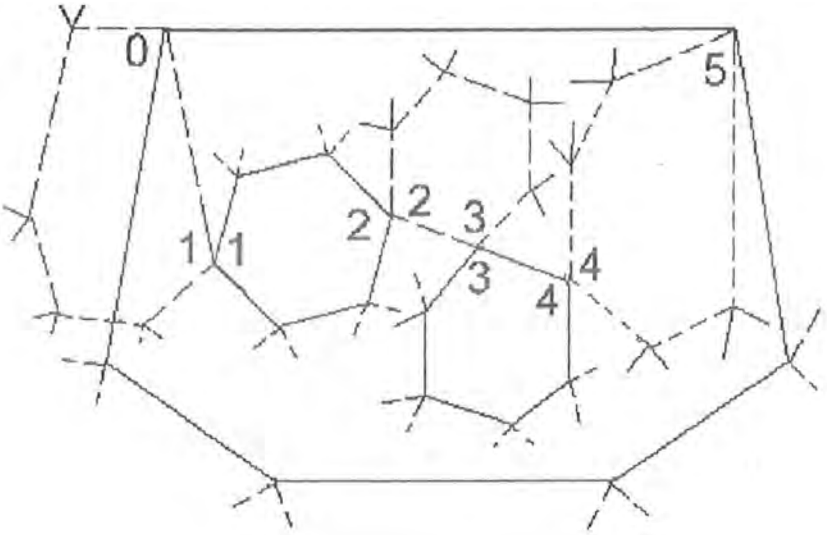
Suppose $k-th$ hexagon (depicting either the six cycles of the generator u (or v) contains two ambiguous numbers, namely α_1 and α_2. We assume that the $k-th$ hexagon is the one which depicts the six cycles of the generator v. Then $\alpha_2^{(k-1)} = \alpha_1^{(k-1)}u^{\varepsilon_1}, \alpha_2^{(k)} = \alpha_1^{(k)}u^{\varepsilon_2}$, and $\alpha_2^{(k+1)} = \alpha_1^{(k+1)}u^{\varepsilon_3}$, where $\varepsilon_1, \varepsilon_2, \varepsilon_3 = 1,2,3,4$ or 5 Also, since $\alpha_2^{(k-1)} = \alpha_1^{(k)}$ and $\alpha_2^{(k)} = \alpha_1^{(k+1)}$ so $\alpha_1^{(k-1)}u^{j_1}v^{j_2}u^{j_3} = \alpha_2^{(k+1)}$. We can continue in this way and since by Lemma 3 [16] there are only finite number of ambiguous numbers of the form $\alpha = \frac{a+\sqrt{n}}{3c}$ in $Q^*(\sqrt{n})$, after a finite number of steps we reach to 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 finite number of ambiguous numbers in the coset diagram. Since only the ambiguous numbers form a closed path and these are the only ambiguous numbers therefore all the ambiguous numbers form a single closed path in the coset diagram of the orbit $\alpha G_{6,6}(2,Z)$.

Example 2.3.2 Let $\alpha = \frac{2+\sqrt{7}}{3}$ then $a = 2, c = 3, n = 7$ and $b = \frac{a^2-n}{c} = -1$. As $bc < 0$ therefore α is an ambiguous number. We tabulate the information as follows.

$\alpha_0 = \alpha$	2	-1	3	ambiguous
$\alpha_1 = (\alpha_0)v^5$	1	1	-6	ambiguous
$\alpha_2 = (\alpha_1)u^3$	-1	-1	6	ambiguous
$\alpha_3 = (\alpha_2)v$	-2	1	-3	ambiguous
$\alpha_4 = (\alpha_3)u^5$	-1	-2	3	ambiguous
$\alpha_5 = (\alpha_4)v^3$	1	2	-3	ambiguous
$\alpha_0 = (\alpha_5)u$	2	-1	3	ambiguous

We can see from the above information that $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4$and α_5 form a closed path. The above information is depicted in the following coset diagram in which $0, 1, 2, 3, 4$ and 5 represent $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4$and α_5 respectively.



Theorem 2.3.3 The graph of the action of $G_{6,6}(2,Z)$ 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 ∞.

Let k_0 be a positive rational number, say, $\frac{a}{b}$. Then $(k_0)u^j = \frac{-b}{3(a+b)}, \frac{-(a+b)}{3a+2b}, \frac{-(3a+2b)}{3(2a+b)}, \frac{-(2a+b)}{3a+b}$ and $\frac{-(3a+b)}{3a}$, for $j = 1,2,3,4$ or 5. Suppose $\|k_0\| = \max\ (|a|,|b|)$. Then $\|(k_0)u\| = 3(a+b)$, $\|(k_0)u^2\| = 3a+2b$, $\|(k_0)u^3\| = 3(2a+b)$, $\|(k_0)u^4\| = 3a+b$ and $\|(k_0)u^5\| = 3a+b$. Therefore, $\|(k_0)u^j\| > \|k_0\|$ for $j = 1,2,3,4,$ and 5. Similarly, if k_0 is a negative rational number, $\frac{a}{b}$ with $b < 0$ then $(k_0)v^i = \frac{3a-b}{3a}, \frac{2a-b}{3a-b}, \frac{3a-2b}{3(2a-b)}, \frac{a-b}{3a-2b}$ and $\frac{-b}{3(a-b)}$, for $i = 1,2,3,4$ or 5. That is, $\|(k_0)v\| = 3a-b$, $\|(k_0)v^2\| = 3a-b$, $\|(k_0)v^3\| = 3(2a-b)$, $\|(k_0)v^4\| = 3a-2b$ and $\|(k_0)v^5\| = 3(a-b)$. Hence $\|(k_0)v^i\| > \|k_0\|$ for $i = 1,2,3,4$ or 5. If k_0 is positive then one of $(k_0)v^i$ is negative. If we let this negative number to be k_1 then $\|k_0\| > \|k_1\|$. As k_1 is negative, one of $(k_1)u^j$ is positive. Let it be k_2, that is, $k_2 = (k_1)u^j$ where j = 1,2,3,4 or 5. This implies that $\|k_1\| > \|k_2\|$. If we continue in this way, we get a unique alternating sequence of positive and negative rational numbers $k_0, k_1, k_3, \ldots$ such that $\|k_0\| > \|k_1\| > \|k_2\| > \ldots$. The decreasing sequence of positive integers must terminate after a finite number of steps. It will terminate only when ultimately we arrive at a hexagon with vertices $-1, \frac{-2}{3}, \frac{-1}{2}, \frac{-1}{3}, 0, \infty$ or $1, \frac{2}{3}, \frac{1}{2}, \frac{1}{3}, 0, \infty$. An alternating sequence of positive and negative rational numbers $k_0, k_1, k_2, \ldots$ such that $\|k_0\| > \|k_1\| > \|k_2\| > \ldots$ shows that there is a path joining k_0 to ∞. Hence every rational number occur in the coset diagram and that the diagram for the action of $G_{6,6}(2,Z)$ on the rational projective line is connected.

Theorem 2.3.4 The action of $G_{6,6}(2,Z)$ on the rational projective line is transitive.

Proof We shall prove transitivity of the action by showing that there is a path from a rational number p to a rational number q, that is, there exists some h in $G_{6,6}(2,Z)$ such that $ph = q$. As we have shown in Theorem 2.3.3 that there exists a path joining p to ∞, that is, there exists an element $g_1 = u^{\varepsilon_1}v^{\eta_1}\, u^{\varepsilon_2}v^{\eta_2}\ldots u^{\varepsilon_n}v^{\eta_n}$ of $G_{6,6}(2,Z)$ such that $\infty = pg_1 = p(u^{\varepsilon_1}v^{\eta_1}\, u^{\varepsilon_2}v^{\eta_2}\ldots u^{\varepsilon_n}v^{\eta_n})$ where $\varepsilon_1 = 0,1,2,\ 3,4$ or 5, $\varepsilon_i = 1,2,3,\ 4$ or 5 , for $i = 2,3,\ldots,n$ and $\eta_n = 0,1,2,$ $3,4$ or 5, $\eta_j = 1,2,3,4$ or 5, where $j = 2,3,\ldots,n-1$. Similarly we can find another element g_2 in $G_{6,6}(2,Z)$ such that $\infty = qg_2$ Hence $pg_1 = qg_2$ or $pg_1g_2^{-1} = q$. That is, the action of $G_{6,6}(2,Z)$ on the rational projective line is transitive.

Now we find a finite presentation of $G_{6,6}(2,Z)$.

Theorem 2.3.5 The linear fractional transformations $v : z \to \frac{3z-1}{3z}$ and $u : z \to \frac{-1}{3(z+1)}$ generate $G_{6,6}(2,Z)$ and $u^6 = v^6 = 1$ are defining relations for the group $G_{6,6}(2,Z)$.

Proof

Suppose that $u^6 = v^6 = 1$ are not defining relations of $G_{6,6}(2,Z)$. Then there is a relation of the form $u^{\eta_1}v^{\eta_2}\, u^{\eta_3}\, v^{\eta_4}\ldots u^{\eta_{n-1}}v^{\eta_n} = 1$ where $n \geq 1$, $\eta_i = 1,2,3,4$ or 5, $1 \leq i \leq n$. We note that neither u nor v can be 1. The coset diagram for the action of the group $G_{6,6}(2,Z)$ on the rational projective line $PL(Q)$ does not contain any circuit. Suppose a contradiction, that is, a closed path exists in the coset diagram. Let there be n hexagons, depicting u and v, in the closed path. Since a hexagon depicting u always contains one positive number (vertex) and a hexagon depicting v always contains one negative number (vertex), we label these alternate negative and positive vertices by $k_1, k_2, \ldots, k_n$. If we let $\|k\| = \max(|a|,|b|)$, where $k = \frac{a}{b}$ is a rational number, then $\|k_1\| \geq \|k_2\| \geq \ldots \geq \|k_n\| \geq \|k_1\|$ gives a contradiction. Thus the coset diagram does not contain any closed path. This shows that there are vertices in the coset diagram such that the path connecting them with ∞ is of arbitrary length. Choose $k > 0$, so that the path between k and ∞ is of length greater than n, that is there are more than n hexagons between k and ∞. Define $k_0 = k, k_i = ku^{\eta_1}v^{\eta_2}\ u^{\eta_3}\ v^{\eta_4} \ldots u^{\eta_{i-1}}v^{\eta_i}$ where $i = 1,2,3\ldots,n$. Then $\|k_0\| \geq \|k_1\| \geq \|k_2\| \geq \ldots \geq \|k_n\|$ and, in particular, $k_n \neq k_0$. Thus $u^{\eta_1}v^{\eta_2}u^{\eta_3}v^{\eta_4} \ldots u^{\eta_{n-1}}$ $v^{\eta_n} \neq 1$ and so $u^6 = v^6 = 1$ are defining relations for the group $G_{6,6}(2,Z)$.

2.4 Intransitive Action of $G_{6,6}(2,Z)$

In this section, we prove that the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n}) \cup \{\infty\}$ is intransitive.

Theorem 2.4.1 (i) If $\alpha = \frac{a+\sqrt{n}}{3c} \in Q^*(\sqrt{n})$ then every element in $\alpha G_{6,6}(2,Z)$ is of the form $\frac{a'+\sqrt{n}}{3c'}$ and $\alpha G_{6,6}(2,Z) \subseteq Q^*(\sqrt{n})$.

(ii) If $\alpha = \frac{a+\sqrt{n}}{3c+1} \in Q^*(\sqrt{n})$ then the elements in $\alpha G_{6,6}(2,Z)$ are either of the form $\frac{a'+\sqrt{n}}{3c'}$ or $\frac{a'+\sqrt{n}}{3c'+1}$, where the elements of the form $\frac{a'+\sqrt{n}}{3c'+1}$ belong to $Q^*(\sqrt{n})$ but the elements of the form $\frac{a'+\sqrt{n}}{3c'}$ belong to $Q(\sqrt{n})\backslash Q^*(\sqrt{n})$.

(iii) If $\alpha = \frac{a+\sqrt{n}}{3c+2} \in Q^*(\sqrt{n})$ then the elements in $\alpha G_{6,6}(2,Z)$ are either of the form $\frac{a'+\sqrt{n}}{3c'}$ or $\frac{a'+\sqrt{n}}{3c'+2}$, where the elements of the form $\frac{a'+\sqrt{n}}{3c'+2}$ belong to $Q^*(\sqrt{n})$ but the elements of the form $\frac{a'+\sqrt{n}}{3c'}$ belong to $Q(\sqrt{n})\backslash Q^*(\sqrt{n})$.

Proof

(i) If $\alpha = \frac{a+\sqrt{n}}{c}$, where $b = \frac{a^2-n}{c}$, then $(\alpha)v = 1 - \frac{1}{3\alpha} = 1 - \frac{c}{3(a+\sqrt{n})} = \frac{(3a-c)+3\sqrt{n}}{3(a+\sqrt{n})} \times \frac{a-\sqrt{n}}{a-\sqrt{n}}$ $= \frac{-a+3b+\sqrt{n}}{3b}$. Hence the new values of a and c are $-a+3b$ and $3b$ respectively. Using these values, we then obtain the new value for b. That is, $\frac{(-a+3b)^2-n}{3b} = \frac{-6a+9b+c}{3}$. Similarly, the new values for a, b and c with respect to $(\alpha)v^i$ are listed in the following table.

α	a	b	c
$i = 1$	$-a+3b$	$\frac{-6a+9b+c}{3}$	$3b$
$i = 2$	$-5a+6b+c$	$-4a+4b+c$	$-6a+9b+c$
$i = 3$	$-7a+6b+2c$	$\frac{-12a+9b+4c}{3}$	$3(-4a+4b+c)$
$i = 4$	$-5a+3b+2c$	$-2a+b+c$	$-12a+9b+4c$
$i = 5$	$-a+c$	$\frac{c}{3}$	$3(-2a+b+c)$

Similarly, we can calculate the new values of a, b, c for $(\alpha)u^j$, where $j = 1,2,3,4,$ and 5, as follows.

α	a	b	c
$j = 1$	$-a-c$	$\frac{c}{3}$	$3(2a+b+c)$
$j = 2$	$-5a-3b-2c$	$2a+b+c$	$12a+9b+4c$
$j = 3$	$-7a-6b-2c$	$\frac{12a+9b+4c}{3}$	$3(4a+4b+c)$
$j = 4$	$-5a-6b-c$	$4a+4b+c$	$6a+9b+c$
$j = 5$	$-a-3b$	$\frac{6a+9b+c}{3}$	$3b$

Every element in $G_{6,6}(2,Z)$ is of the form $u^{\varepsilon_1}v^{\eta_1}u^{\varepsilon_2}v^{\eta_2}\ldots u^{\varepsilon_n}v^{\eta_n}$, where $\varepsilon_1 = 0,1,2,3,4$ or 5, $\varepsilon_i = 1,2,3,4$ or 5 , for $i = 2,3,\ldots,n$ and $\eta_n = 0,1,2,3,4$ or 5, $\eta_j = 1,2,3,4$ or 5, where $j = 2,3,\ldots,n-1$. Now from the above tables we can easily see that if $\alpha = \frac{a+\sqrt{n}}{3c} \in Q^*(\sqrt{n})$

then every element in $\alpha G_{6,6}(2,Z)$ is of the form $\frac{a'+\sqrt{n}}{3c'}$ and $\alpha G_{6,6}(2,Z) \subseteq .Q^*(\sqrt{n})$.

(ii) From the preceding tables we can easily see that every element in $\alpha G_{6,6}(2,Z)$ where $\frac{a+\sqrt{n}}{3c+1}$, is either of the form $\frac{a'+\sqrt{n}}{3c'}$ or $\frac{a'+\sqrt{n}}{3c'+1}$, whence the elements of the form $\frac{a'+\sqrt{n}}{3c'+1}$ belong to $Q^*(\sqrt{n})$ but the elements of the form $\frac{a'+\sqrt{n}}{3c'}$ belong to $Q(\sqrt{n})\backslash Q^*(\sqrt{n})$.

(iii) From the preceding tables we can easily see that every element in $\alpha G_{6,6}(2,Z)$ for $\alpha = \frac{a+\sqrt{n}}{3c+2}$ is either of the form $\frac{a'+\sqrt{n}}{3c'}$ or $\frac{a'+\sqrt{n}}{3c'+2}$, whence the elements of the form $\frac{a'+\sqrt{n}}{3c'+2}$ belong to $Q^*(\sqrt{n})$ but the elements of the form $\frac{a'+\sqrt{n}}{3c'}$ belong to $Q(\sqrt{n})\backslash Q^*(\sqrt{n})$.

Theorem 2.4.2 The action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n}) \cup \{\infty\}$ is intransitive.

Proof

The non-square positive integer n can be of three types, namely, $n = 3m$, $n = 3m+1$, and $n = 3m+2$, where $m \in Z$. We consider the three cases one by one.

(i) Consider $n = 3m$. If we take $\alpha = \frac{\sqrt{n}}{3}$, then $a = 0, c = 3$ and $b = \frac{a^2-n}{c} = -m$. Hence $\alpha \in Q^*(\sqrt{n})$. Also if we take $\beta = \sqrt{n}$ then $\beta \in Q^*(\sqrt{n})$. Similarly if we take $\gamma = \frac{1+\sqrt{n}}{2}$ when m is odd and take $\gamma = \frac{\sqrt{n}}{2}$ when m is even. Hence $\gamma \in Q^*(\sqrt{n})$. Since according to Theorem 2.4.1, the elements of the form $\frac{a+\sqrt{n}}{3c}$, $\frac{a+\sqrt{n}}{3c+1}$ and $\frac{a+\sqrt{n}}{3c+2}$ lie in different orbits of $Q(\sqrt{n})$, so there are at least three orbits of $Q(\sqrt{n})$. Hence the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$ is intransitive.

(ii) Let $n = 3m+1$. If we take $\alpha = \frac{1+\sqrt{n}}{3}$, then $a = 1, c = 3$ and $b = \frac{a^2-n}{c} = -m$. Hence $\alpha \in Q^*(\sqrt{n})$. Also if we take $\beta = \sqrt{n}$ then $\beta \in Q^*(\sqrt{n})$. Similarly, if we take $\gamma = \frac{1+\sqrt{n}}{2}$

when m is even and take $\gamma = \frac{\sqrt{n}}{2}$ when m is odd then $\gamma \in Q^{*}(\sqrt{n})$. As the elements of the form $\frac{a+\sqrt{n}}{3c}$, $\frac{a+\sqrt{n}}{3c+1}$ and $\frac{a+\sqrt{n}}{3c+2}$ lie by virtue of Theorem 2.4.1, in different orbits of $Q(\sqrt{n})$, so there are at least three orbits of $Q(\sqrt{n})$. Hence the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$ is intransitive.

(iii) Suppose $n = 3m+2$. If we take $\alpha = \sqrt{n}$ then $\alpha \in Q^{*}(\sqrt{n})$. Also if we take $\beta = \frac{1+\sqrt{n}}{2}$ when m is odd and take $\beta = \frac{\sqrt{n}}{2}$ when m is even then $\beta \in Q^{*}(\sqrt{n})$. Thus, there are at least two orbits of $Q(\sqrt{n})$, and so the action of $G_{6,6}(2,Z)$ on $Q(\sqrt{n})$ is intransitive.

We conclude this chapter by highlighting the following points. If $n = 3m+2, m \in Z$ then there does not exist any real quadratic irrational number of the form $\alpha = \frac{a+\sqrt{n}}{3c}$ in $Q^{*}(\sqrt{n})$. So there does not exist any orbit containing elements of the form $\alpha = \frac{a+\sqrt{n}}{3c}$ in $Q^{*}(\sqrt{n})$ where $n = 3m+2$. If we are given a real quadratic irrational number α, we can find the closed path in the orbit $\alpha G_{6,6}(2,Z)$. If α is totally negative then one of $(\alpha)v^{j}$, for $j = 1,2,3,4$ or 5 is totally positive, and we can use Theorem 2.2.11 to find an ambiguous number in the same orbit. The existence of an ambiguous number assures the existence of a closed path. This means that if α and β are two real quadratic irrational numbers then we can find out whether or not they belong to the same orbit. We can then look for closed paths in the orbits $\alpha G_{6,6}(2,Z)$ and $\beta G_{6,6}(2,Z)$ and see if they are same or not. It is important to note that for a fixed value of a non-square positive integer n, all possible ambiguous numbers do not lie in the same orbit.

For instance, if we take $n = 7$, then $(1+\sqrt{7})u^{5}v^{5}u^{5}\ v^{3}u^{5}v^{5}u^{5}v^{5}u^{3}v^{5} = (1+\sqrt{7})$ and $(1-\sqrt{7})u^{5}v^{5}u^{5}v^{3}u^{5}\ v^{5}u^{5}v^{5}u^{3}v^{5} = (1-\sqrt{7})$. If we let $\alpha = (1+\sqrt{7})$ and $\beta = (1-\sqrt{7})$ then $\alpha G_{6,6}(2,Z) \cap \beta G_{6,6}(2,Z)$ is empty. That is, α and β do not lie in the same orbit.

CHAPTER THREE

ACTION OF $G_{6,6}(2,Z)$ ON IMAGINARY QUADRATIC FIELDS

3.1 Introduction

In this chapter, we have studied an action of the group $G_{6,6}(2,Z)$ on the imaginary quadratic fields $Q(\sqrt{-n})$, where n is a square free positive integer. Using the coset diagrams we have shown that the action of $G_{6,6}(2,Z)$ on $Q^{*}(\sqrt{-n}) = \{\frac{a+\sqrt{-n}}{3c} : a, \frac{a^2+n}{3c}, c \in Z, c \neq 0\}$ is always intransitive.

Let F be an extension field of degree two over the field Q of rational numbers. If n is a negative square free integer then $Q(\sqrt{n})$ is called an imaginary quadratic field and the elements of $Q(\sqrt{n})$ are of the form $a + b\sqrt{n}$ with $a, b \in Q$. The imaginary quadratic fields are usually denoted by $Q(\sqrt{-n})$. Imaginary quadratic fields are the only type (apart from Q) with a finite unit group. This group has order 4 for $Q(\sqrt{-1})$ (and generator $\sqrt{-1}$), order 6 for $Q(\sqrt{-3})$ (and generator $(1 + \sqrt{-3})/2$), and order 2 (and generator -1) for all other imaginary quadratic fields. We shall denote the subset $\{\frac{a+\sqrt{-n}}{3c} : a, \frac{a^2+n}{3c}, c \in Z, c \neq 0\}$ by $Q^{*}(\sqrt{-n})$.

Theorem 3.1.1 If $\alpha = \frac{a+\sqrt{-n}}{3k} \in Q^{*}(\sqrt{-n})$, then n does not change its value in the orbit $\alpha G_{6,6}(2,Z)$, that is $\alpha G_{6,6}(2,Z) \subseteq Q^{*}(\sqrt{-n})$.

Proof

If $\alpha = \frac{a+\sqrt{-n}}{c}$, where $c = 3k$ and $d = \frac{a^2+n}{c}$, then the new values of a, c, d for $(\alpha)u^j$, where $j = 1,2,3,4$ and 5 are as follows.

α	a	d	c
$(\alpha)u$	$-a-3k$	k	$3(2a+d+3k)$
$(\alpha)u^2$	$-5a-3d-6k$	$2a+d+3k$	$3(4a+3d+4k)$
$(\alpha)u^3$	$-7a-6d-6k$	$4a+3d+4k$	$3(4a+4d+3k)$
$(\alpha)u^4$	$-5a-6d-3k$	$4a+4d+3k$	$3(2a+3d+k)$
$(\alpha)u^5$	$-a-3d$	$2a+3d+k$	$3d$

Similarly, $(\alpha)v = 1 - \frac{1}{3\alpha} = 1 - \frac{c}{3(a+\sqrt{-n})} = \frac{(3a-c)+3\sqrt{-n}}{3(a+\sqrt{-n})} \times \frac{a-\sqrt{-n}}{a-\sqrt{-n}} = \frac{-a+3d+\sqrt{-n}}{3d}$. Hence the new values of a and c for $(\alpha)v$ are $-a+3d$ and $3d$ respectively. Using these values, we then obtain the new value for d, that is, $\frac{(-a+3d)^2+n}{3d} = \frac{-6a+9d+c}{3}$. Similarly, the new values for a, d and c with respect to $(\alpha)v^i$, for $i = 1,2,3,4$ and 5 are:

α	a	d	c
$(\alpha)v$	$-a+3d$	$-2a+3d+k$	$3d$
$(\alpha)v^2$	$-5a+6d+3k$	$-4a+4d+3k$	$3(-2a+3d+k)$
$(\alpha)v^3$	$-7a+6d+6k$	$-4a+3d+4k$	$3(-4a+4d+3k)$
$(\alpha)v^4$	$-5a+3d+6k$	$-2a+d+3k$	$3(-4a+3d+4k)$
$(\alpha)v^5$	$-a+3k$	k	$3(-2a+d+3k)$
$(\alpha)uv$	$a+6k$	$4a+d+12k$	$3k$
$(\alpha)vu$	$a-6d$	d	$3(-4a+12d+k)$

From the above information we see that every element in $\alpha G_{6,6}(2,Z)$ is of the form $\frac{a+\sqrt{-n}}{3c}$. Hence the non-square positive integer n does not change its value in the orbits $\alpha G_{6,6}(2,Z)$ and $\alpha G_{6,6}(2,Z) \subseteq Q^*(\sqrt{-n})$.

3.2 Existence of Fixed Points in $Q^*(\sqrt{-n})$

Theorem 3.2.1 The fixed points under the action of $G_{6,6}(2,Z)$ on $Q^*(\sqrt{-n})$ exist only if $n = 3$.

Proof

Let g be a non-identity linear fractional transformation in $G_{6,6}(2,Z)$. Then $(z)g$ can be taken as $\frac{az+b}{cz+d}$ where $ad-bc = 1$ or 3. If $\frac{az+b}{cz+d} = z$, we get the quadratic equation $cz^2 + (d-a)z - b = 0$. It has the imaginary roots only if $(d-a)^2 + 4bc < 0$ or $(d+a)^2 - 4(ad-bc) < 0$.

If $ad - bc = 1$ then $(a+d)^2 < 4$, and so $a+d = 0, \pm 1$.

If $a+d = 0$ then g is an involution and hence conjugate to the linear fractional transformations v^3 or u^3.

If $a+d = \pm 1$ then because $(Tr(g))^2 = \det(g)$, the order of g will be three and hence conjugate to the linear fractional transformations $v^{\pm 2}$ or $u^{\pm 2}$.

Next, we consider the case when $ad-bc = 3$. Since $(a+d)^2 < 12$, therefore, $a+d = 0, \pm 1, \pm 2, \pm 3$.

If $a+d = 0$ then g is an involution and hence conjugate to the linear fractional transformations v^3 or u^3.

If $a+d = \pm 1, \pm 2$ then the order of g must be infinite and so g is conjugate to $(uv)^m$, where m is a positive integer..

If $a+d = \pm 3$ then as $(Tr(g))^2 = 3\det(g)$, therefore, order of g will be six and hence it is conjugate to the linear fractional transformations $v^{\pm 1}$ or $u^{\pm 1}$. Hence the fixed points of g are imaginary provided it is conjugate to the linear fractional transformations $v^{\pm 1}, v^{\pm 2}, v^3, u^{\pm 1}, u^{\pm 2}$ or u^3. Since the fixed points of u and v are $\frac{-3\pm\sqrt{-3}}{6}$ and $\frac{3\pm\sqrt{-3}}{6}$ respectively and the conjugates of v and u have the same discriminant, therefore, the imaginary fixed points of the elements of $G_{6,6}(2,Z)$ are contained in $Q^*(\sqrt{-3})$.

3.3 Orbits of $Q^*(\sqrt{-3})$

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

Note that cd is always positive because $d = \frac{a^2+n}{c}$ and so c and d will have the 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 $c,d > 0$ or $a > 0$ and $c,d < 0$. Similarly, $\alpha = \frac{a+\sqrt{-n}}{c} \in Q(\sqrt{-n})$ is totally positive if either $a,c,d > 0$ or $a,c,d < 0$.

Theorem 3.3.1 If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q(\sqrt{-n})$ is a totally negative imaginary quadratic number then $(\alpha)v^i$ is totally positive for $i = 1,2,3,4$ or 5.

Proof

If $\alpha = \frac{a+\sqrt{-n}}{c}$, $d = \frac{a^2+n}{c}$, then $(\alpha)v = 1 - \frac{1}{3\alpha} = 1 - \frac{c}{3(a+\sqrt{-n})} = \frac{(3a-c)+3\sqrt{-n}}{3(a+\sqrt{-n})} \times \frac{a-\sqrt{-n}}{a-\sqrt{-n}} = \frac{-a+3d+\sqrt{-n}}{3d}$. Hence the new values of a and c for $(\alpha)v$ are $-a+3d$ and $3d$ respectively. Using these values, we then obtain the new value for d. That is, $\frac{(-a+3d)^2+n}{3d} = \frac{-6a+9d+c}{3}$. Similarly, the new values for a, d and c with respect to $(\alpha)v^i$ are:

α	a	d	c
$i = 1$	$-a+3d$	$\frac{-6a+9d+c}{3}$	$3d$
$i = 2$	$-5a+6d+c$	$-4a+4d+c$	$-6a+9d+c$
$i = 3$	$-7a+6d+2c$	$\frac{-12a+9d+4c}{3}$	$3(-4a+4d+c)$
$i = 4$	$-5a+3d+2c$	$-2a+d+c$	$-12a+9d+4c$
$i = 5$	$-a+c$	$\frac{c}{3}$	$3(-2a+d+c)$

If α is a totally negative number then either $a < 0$ and $c, d > 0$ or $a > 0$ and $c, d < 0$.

If $a < 0$ and $c, d > 0$ then from the preceding table the new a, d, c for $(\alpha)v^i$ are all positive, and hence $(\alpha)v^i$ are totally positive for $i = 1,2,3,4$ or 5.

Similarly, if $a > 0$ and $c, d < 0$ then the new values of a, d, c for $(\alpha)v^i$ are all negative, and hence $(\alpha)v^i$ for $i = 1,2,3,4$ or 5 are totally positive.

Note that there are hexagons (with unbroken sides) in which all six vertices are totally positive or five are totally positive and the sixth is neither totally positive nor totally negative.

Theorem 3.3.2 If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q(\sqrt{-n})$ is a totally positive imaginary quadratic number then $(\alpha)u^j$ is totally negative for $j = 1,2,3,4$ or 5.

Proof

Since $(z)u = \frac{-1}{3(z+1)}$, therefore, $(\alpha)u = \frac{-1}{3(\alpha+1)} = \frac{-a-c+\sqrt{-n}}{3(2a+d+c)} = \frac{a_1+\sqrt{-n}}{c_1}$ where, $a_1 = -a-c$, $c_1 = 3(2a+d+c)$ and $d_1 = \frac{a_1^2+n}{c_1} = \frac{c}{3}$.

Similarly, the values of a, d, c for $(\alpha)u^j$ can be tabulated in the following fashion.

α	a	d	c
$j = 1$	$-a - c$	$\frac{c}{3}$	$3(2a + d + c)$
$j = 2$	$-5a - 3d - 2c$	$2a + d + c$	$12a + 9d + 4c$
$j = 3$	$-7a - 6d - 2c$	$\frac{12a+9d+4c}{3}$	$3(4a + 4d + c)$
$j = 4$	$-5a - 6d - c$	$4a + 4d + c$	$6a + 9d + c$
$j = 5$	$-a - 3d$	$\frac{6a+9d+c}{3}$	$3d$

Since α is totally positive, either $a, d, c > 0$ or $a, d, c < 0$.

If $a,d,c > 0$, then from the preceding table we see that $(\alpha)u^j$ is totally negative for $j = 1,2,3,4$ or 5 and on the other hand if $a,d,c < 0$ then $(\alpha)u^j$ is totally negative for $j = 1,2,3,4$ or 5.

Note that there are hexagons (with broken sides) in which all six vertices are totally negative or five are totally negative and the sixth is neither totally positive nor totally negative

Let the norm of $\alpha = \frac{a+\sqrt{-n}}{c}$ be defined as $\|\alpha\| = |a|$.

Theorem 3.3.3 If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q(\sqrt{-n})$ is totally positive imaginary quadratic number then $\|(\alpha)u^j\| > \|\alpha\|$, for $j = 1,2,3,4$ and 5.

Proof

If $\alpha = \frac{a+\sqrt{-n}}{c}$, where $d = \frac{a^2+n}{c}$, then we can easily calculate new values of a, c, d for $(\alpha)u^j$, where $j = 1,2,3,4$ and 5 as follows.

α	a	d	c
$j=1$	$-a-c$	$\frac{c}{3}$	$3(2a+d+c)$
$j=2$	$-5a-3d-2c$	$2a+d+c$	$12a+9d+4c$
$j=3$	$-7a-6d-2c$	$\frac{12a+9d+4c}{3}$	$3(4a+4d+c)$
$j=4$	$-5a-6d-c$	$4a+4d+c$	$6a+9d+c$
$j=5$	$-a-3d$	$\frac{6a+9d+c}{3}$	$3d$

Since α is a totally positive number, therefore, either $a,c,d > 0$ or $a,c,d < 0$.

If $a,c,d > 0$ (or $a,c,d < 0$), then $\|(\alpha)u\| = |a+c|$, $\|(\alpha)u^2\| = |5a+3d+2c|$, $\|(\alpha)u^3\| = |7a+6d+2c|$, $\|(\alpha)u^4\| = |5a+6d+c|$ and $\|(\alpha)u^5\| = |a+3d|$. Thus, $\|(\alpha)u^j\| > \|\alpha\|$, for $j = 1,2,3,4$ and 5.

Theorem 3.3.4 If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q(\sqrt{-n})$ is totally negative imaginary quadratic number, then $\|(\alpha)v^i\| > \|\alpha\|$, for $i = 1,2,3,4$ or 5.

Proof

If $\alpha = \frac{a+\sqrt{-n}}{c}$, where $d = \frac{a^2+n}{c}$, then the new values for a,c,d for $(\alpha)v^i$ are as follows.

α	a	d	c
$i=1$	$-a+3d$	$\frac{-6a+9d+c}{3}$	$3d$
$i=2$	$-5a+6d+c$	$-4a+4d+c$	$-6a+9d+c$
$i=3$	$-7a+6d+2c$	$\frac{-12a+9d+4c}{3}$	$3(-4a+4d+c)$
$i=4$	$-5a+3d+2c$	$-2a+d+c$	$-12a+9d+4c$
$i=5$	$-a+c$	$\frac{c}{3}$	$3(-2a+d+c)$

Since α is a totally negative number so either $a > 0$, and $d < 0, c < 0$ or $a < 0$, and $d > 0, c > 0$.

If $a > 0$ and $d < 0, c < 0$ (or $a < 0$ and $d > 0, c > 0$) then $\|(\alpha)v\| = |-a+3d|$, $\|(\alpha)v^2\| = |-5a+6d+c|$, $\|(\alpha)v^3\| = |-7a+6d+2c|$, $\|(\alpha)v^4\| = |-5a+3d+2c|$ and $\|(\alpha)v^5\| = |-a+c|$. Hence, $\|(\alpha)v^i\| > \|\alpha\|$, for $i = 1,2,3,4$ and 5.

Theorem 3.3.5 (i) If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q(\sqrt{-n})$, where $c > 0$ then the denominator of every element in $\alpha G_{6,6}(2,Z)$ is also positive.

(ii) If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q(\sqrt{-n})$, where $c < 0$ then the denominator of every element in $\alpha G_{6,6}(2,Z)$ is also negative.

Proof

We can tabulate the following information.

α	a	d	c
$(\alpha)u$	$-a-c$	$\frac{c}{3}$	$3(2a+d+c)$
$(\alpha)u^2$	$-5a-3d-2c$	$2a+d+c$	$12a+9d+4c$
$(\alpha)u^3$	$-7a-6d-2c$	$\frac{12a+9d+4c}{3}$	$3(4a+4d+c)$
$(\alpha)u^4$	$-5a-6d-c$	$4a+4d+c$	$6a+9d+c$
$(\alpha)u^5$	$-a-3d$	$\frac{6a+9d+c}{3}$	$3d$
$(\alpha)v$	$-a+3d$	$\frac{-6a+9d+c}{3}$	$3d$
$(\alpha)v^2$	$-5a+6d+c$	$-4a+4d+c$	$-6a+9d+c$
$(\alpha)v^3$	$-7a+6d+2c$	$\frac{-12a+9d+4c}{3}$	$3(-4a+4d+c)$
$(\alpha)v^4$	$-5a+3d+2c$	$-2a+d+c$	$-12a+9d+4c$
$(\alpha)v^5$	$-a+c$	$\frac{c}{3}$	$3(-2a+d+c)$
$(\alpha)uv$	$a+2c$	$4a+d+4c$	c
$(\alpha)vu$	$a-6d$	d	$-12a+36d+c$

(i) Since $\alpha = \frac{a+\sqrt{-n}}{c}$ with $c > 0$, therefore d is also positive because d and c have the same sign. Using this fact, we can easily see from the above table that every element in $\alpha G_{6,6}(2,Z)$ has positive denominator.

(ii) Since $\alpha = \frac{a+\sqrt{-n}}{c}$ with $c < 0$, therefore d is also negative because d and c have the same sign. Using this fact, we can easily see from the above table that every element in $\alpha G_{6,6}(2,Z)$ has negative denominator.

Theorem 3.3.6 If $\alpha = \frac{a+\sqrt{-3}}{3c} \in Q^*(\sqrt{-3})$ is a totally positive imaginary quadratic number, then there exists a sequence $\alpha(=\alpha_1),\alpha_2,\alpha_3,\ldots,\alpha_m$ such that α_i is alternately totally positive and totally negative, for $i = 1,2,3,\ldots,m-1$ and $\|\alpha_m\| = 0$ or 3.

Proof

Since $\alpha = \frac{a+\sqrt{-3}}{3c}$ is a totally positive imaginary quadratic number, therefore by Theorem 3.3.2, one of $(\alpha)v^i$, for $i = 1,2,3,4$ or 5, is totally negative. If $(\alpha)v^i$ is totally negative then by Theorem 3.3.4, $\|(\alpha)v^i\| < \|\alpha\|$. Also since $(\alpha)v^i$ is totally negative, then, one of $(\alpha)v^iu^j$, for $j = 1,2,3,4,$ and 5 is totally positive. If $(\alpha)v^iu^j$ is totally positive then by Theorem 3.3.3, $\|(\alpha)v^iu^j\| < \|(\alpha)v^i\| < \|\alpha\|$. If we let, $\alpha = \alpha_1$, $(\alpha)v^i = \alpha_2, (\alpha)v^iu^j = \alpha_3$ and continue in this way we obtain an alternate sequence $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m$ of totally positive and totally negative numbers such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$. Since $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ is a decreasing sequence of non-negative integers, therefore it must terminate. After a finite number of steps, the sequence terminates at α_m such that $\|\alpha_m\| = 0$ or 3. If $\alpha_m = \frac{-3\pm\sqrt{-3}}{6}$ or $\frac{3\pm\sqrt{-3}}{6}$ and since $\frac{-3\pm\sqrt{-3}}{6}$ and $\frac{3\pm\sqrt{-3}}{6}$ are the fixed points of u and v respectively, it does not end at an imaginary quadratic number whose norm is equal to zero, because otherwise we reach at $\alpha_m = \frac{\sqrt{-3}}{\pm 3}$ such that $\|\alpha_m\| = 0$.

Theorem 3.3.7 There are exactly six orbits of $Q^*(\sqrt{-3})$ under the action of $G_{6,6}(2,Z)$.

Proof

As we have seen in Theorem 3.3.6, we can obtain a decreasing sequence of non-negative integers $\|\alpha_0\|, \|\alpha_1\|, \|\alpha_2\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_0\| > \|\alpha_1\| > \|\alpha_2\| > \ldots > \|\alpha_m\|$ 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 3. If $\alpha_m = \frac{-3\pm\sqrt{-3}}{6}$ or $\frac{3\pm\sqrt{-3}}{6}$ and because $\frac{-3\pm\sqrt{-3}}{6}$ and $\frac{3\pm\sqrt{-3}}{6}$ are the fixed points of v and u respectively, therefore we cannot reach at an imaginary quadratic number whose norm is equal to zero. Therefore, in this case, there are four orbits of $Q^*(\sqrt{-3})$. That is, $\frac{-3+\sqrt{-3}}{6}G_{6,6}(2,Z)$, $\frac{-3-\sqrt{-3}}{6}G_{6,6}(2,Z)$, $\frac{3+\sqrt{-3}}{6}G_{6,6}(2,Z)$ and $\frac{3-\sqrt{-3}}{6}G_{6,6}(2,Z)$. Also, there are only two elements $\frac{\sqrt{-3}}{3}$ and $\frac{\sqrt{-3}}{-3}$ in $Q^*(\sqrt{-3})$ whose norm is equal to zero. Since $\frac{\sqrt{-3}}{3}$ and $\frac{\sqrt{-3}}{-3}$ lie in two different orbits other than $\frac{-3+\sqrt{-3}}{6}G_{6,6}(2,Z)$, $\frac{-3-\sqrt{-3}}{6}G_{6,6}(2,Z)$, $\frac{3+\sqrt{-3}}{6}G_{6,6}(2,Z)$ and $\frac{3-\sqrt{-3}}{6}G_{6,6}(2,Z)$, hence there are exactly six orbits of $Q^*(\sqrt{-3})$ under the action of $G_{6,6}(2,Z)$.

3.4 Orbits of $Q^*(\sqrt{-n})$

Now we look at the orbits of $Q^*(\sqrt{-n})$, when $n \neq 3$.

Remark 3.4.1

(i) If $n = 3k$, where $k \in Z$, then there does not exist any element of norm 1 or 2 in $Q^*(\sqrt{-n})$.

(ii) If $n = 3k+1$, where $k \in Z$, then $Q^*(\sqrt{-n})$ is empty.

(iii) If $n = 3k+2$, where $k \in Z$, then $Q^*(\sqrt{-n})$ contains elements of norm 1 and of norm 2, but not of norm zero.

Theorem 3.4.2 If $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*(\sqrt{-n})$, where $n \neq 3$, is a totally positive imaginary quadratic number, then there exists a sequence $\alpha(=\alpha_1), \alpha_2, \alpha_3, \ldots, \alpha_m$ such that α_i is alternately totally positive and totally negative, for $i = 1,2,3,\ldots,m-1$ and $\|\alpha_m\| = 0, 1$ or 2.

Proof

Since $\alpha = \frac{a+\sqrt{-n}}{3c}$ is a totally positive imaginary quadratic number, therefore by Theorem 3.3.1, one of $(\alpha)v^i$, for $i = 1,2,3,4$ or 5, is totally negative. If $(\alpha)v^i$ is totally negative then by

Theorem 3.3.3, $\|(\alpha)v^i\| < \|\alpha\|$. Also since $(\alpha)v^i$ is totally negative, then one of $(\alpha)v^i u^j$, for $j = 1,2,3,4,$ and 5 is totally positive. If $(\alpha)v^i u^j$ is totally positive then by Theorem 3.3.4, $\|(\alpha)v^i u^j\| < \|(\alpha)v^i\| < \|\alpha\|$. If we let ,$\alpha = \alpha_1$, $(\alpha)v^i = \alpha_2$, $(\alpha)v^i u^j = \alpha_3$ and continue in this way we obtain an alternate sequence $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m$ of totally positive and totally negative numbers such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$. Since $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ is a decreasing sequence of non-negative integers, therefore, it must terminate.

For the square-free positive integer n there are three possibilities, namely $3k, 3k+1$ and $3k+2$ where $k \in Z$.

If $n = 3k$ then there does not exist any element of norm 1 or of norm 2 in $Q^*(\sqrt{-n})$, but elements $(\frac{\sqrt{-n}}{3c})$ of norm zero exist in $Q^*(\sqrt{-n})$. Hence in this case, after a finite number of steps we reach to α_m such that $\|\alpha_m\| = 0$.

If $n = 3k+1$ then there does not exist any element of the form $\frac{a+\sqrt{-n}}{3c}$ such that $\frac{a^2+n}{3c} \in Z$. Hence in this case, $Q^*(\sqrt{-n})$ becomes the empty set.

If $n = 3k+2$ then there does not exist any element $(\frac{\sqrt{-n}}{3c})$ of norm zero in $Q^*(\sqrt{-n})$, but elements of norm 1 and of norm 2 exist in $Q^*(\sqrt{-n})$. Hence in this case, after a finite number of steps we reach to α_m such that $\|\alpha_m\| = 1$ or 2.

Theorem 3.4.3 Let $\alpha \in Q^*(\sqrt{-n})$, where $n \neq 3$.

(i) If $\alpha = \frac{\pm 1+\sqrt{-n}}{\pm 3}$, where $n = 3k+2, k \in Z$, then $\frac{\pm 2+\sqrt{-n}}{\pm 3(k+2)} \in \alpha G_{6,6}(2,Z)$.

(ii) If $\alpha = \frac{\pm 2+\sqrt{-n}}{\pm 3}$, where $n = 3k+2, k \in Z$, then $\frac{\pm 1+\sqrt{-n}}{\pm 3(k+1)} \in \alpha G_{6,6}(2,Z)$.

(iii) If $\alpha = \frac{\pm 1+\sqrt{-n}}{3k_1}$, where $n = 3k+2, k \in Z$ and $\frac{k+1}{k_1} = k_2 \in Z$ and $k_1, k_2 \neq \pm 1$, then there does not exist any element of norm 1 (other than α) or of norm 2 in $\alpha G_{6,6}(2,Z)$.

(iv) If $\alpha = \frac{\pm 2+\sqrt{-n}}{3k_1}$, where $n = 3k+2, k \in Z$ and $\frac{k+2}{k_1} = k_2 \in Z$ and $k_1, k_2 \neq \pm 1$ then there does not exist any element of norm 1 or of norm 2 (other than α) in $\alpha G_{6,6}(2,Z)$.

Proof

(i) Let $\alpha = \frac{1+\sqrt{-n}}{3}$, where $n = 3k+2, k \in Z$. Then:

α	1	$k+1$	3
$(\alpha)u$	-4	1	$3(k+6)$
$(\alpha)u^2$	$-3k-14$	$k+6$	$9k+33$
$(\alpha)u^3$	$-6k-19$	$3k+11$	$3(4k+11)$
$(\alpha)u^4$	$-6k-14$	$4k+11$	$9k+18$
$(\alpha)u^5$	$-3k-4$	$3k+6$	$3(k+1)$
$(\alpha)v$	$3k+2$	$3k+2$	$3(k+1)$
$(\alpha)v^2$	$6k+4$	$4k+3$	$3(3k+2)$
$(\alpha)v^3$	$6k+5$	$3k+3$	$3(4k+3)$
$(\alpha)v^4$	$3k+4$	$k+2$	$3(3k+3)$
$(\alpha)v^5$	2	1	$3(k+2)$

From the preceding table we see that $\frac{2+\sqrt{-n}}{3(k+2)} \in \alpha G_{6,6}(2,Z)$.

Similarly, let $n = 3k+2$, when $k \in Z$. If $\alpha = \frac{-1+\sqrt{-n}}{3}$, $\beta = \frac{1+\sqrt{-n}}{-3}$, $\gamma = \frac{-1+\sqrt{-n}}{-3}$, then $\frac{-2+\sqrt{-n}}{3(k+2)} \in \alpha G_{6,6}(2,Z)$, $\frac{2+\sqrt{-n}}{-3(k+2)} \in \beta G_{6,6}(2,Z)$ and $\frac{-2+\sqrt{-n}}{-3(k+2)} \in \gamma G_{6,6}(2,Z)$.

(ii) Let $\alpha = \frac{2+\sqrt{-n}}{3}$, where $n = 3k+2, k \in Z$. We can easily tabulate the following information.

α	2	$k+2$	3
$(\alpha)u$	-5	1	$3(k+9)$
$(\alpha)u^2$	$-3k-22$	$k+9$	$9k+54$
$(\alpha)u^3$	$-6k-32$	$3k+18$	$3(4k+19)$
$(\alpha)u^4$	$-6k-25$	$4k+19$	$9k+24$
$(\alpha)u^5$	$-3k-8$	$3k+8$	$3(k+2)$
$(\alpha)v$	$3k+4$	$3k+3$	$3(k+2)$
$(\alpha)v^2$	$6k+5$	$4k+3$	$3(3k+3)$
$(\alpha)v^3$	$6k+4$	$9k+6$	$3(4k+3)$
$(\alpha)v^4$	$3k+2$	$k+1$	$3(9k+6)$
$(\alpha)v^5$	1	1	$3(k+1)$

From the preceding table we note that $\frac{1+\sqrt{-n}}{3(k+1)} \in \alpha G_{6,6}(2,Z)$. Similarly, it is clear that if $\alpha = \frac{-2+\sqrt{-n}}{3}$, $\beta = \frac{2+\sqrt{-n}}{-3}$ and $\gamma = \frac{-2+\sqrt{-n}}{-3}$, where $n = 3k+2$, $k \in Z$, then $\frac{-1+\sqrt{-n}}{3(k+1)} \in \alpha G_{6,6}(2,Z)$, $\frac{-1+\sqrt{-n}}{-3(k+2)} \in \beta G_{6,6}(2,Z)$ and $\frac{-1+\sqrt{-n}}{-3(k+2)} \in \gamma G_{6,6}(2,Z)$.

(iii) Let $\alpha = \frac{1+\sqrt{-n}}{3k_1}$, where $n = 3k+2, k \in Z$ and $\frac{k+1}{k_1} = k_2 \in Z$.and $k_1, k_2 \neq \pm 1$. Then the information is tabulated in the following way.

α	1	k_2	$3k_1$
$(\alpha)u$	$-1-3k_1$	k_1	$3(2+3k_1+k_2)$
$(\alpha)u^2$	$-5-6k_1-3k_2$	$2+3k_1+k_2$	$12+12k_1+9k_2$
$(\alpha)u^3$	$-7-6k_1-6k_2$	$4+4k_1+3k_2$	$3(4+3k_1+4k_2)$
$(\alpha)u^4$	$-5-3k_1-6k_2$	$4+3k_1+4k_2$	$6+3k_1+9k_2$
$(\alpha)u^5$	$-1-3k_2$	$2+k_1+3k_2$	$3k_2$
$(\alpha)v$	$-1+3k_2$	$-2+k_1+3k_2$	$3k_2$
$(\alpha)v^2$	$-5+3k_1+6k_2$	$-4+3k_1+4k_2$	$-6+3k_1+9k_2$
$(\alpha)v^3$	$-7+6k_1+6k_2$	$-4+4k_1+3k_2$	$3(-4+3k_1+4k_2)$
$(\alpha)v^4$	$-5+6k_1+3k_2$	$-2+3k_1+k_2$	$-12+12k_1+9k_2$
$(\alpha)v^5$	$-1+3k_1$	k_1	$3(-2+3k_1+k_2)$

From the preceding table we note that there does not exist any element of norm 1 (other than α) or of norm 2 in $\alpha G_{6,6}(2,Z)$. Similarly, if $\alpha = \frac{-1+\sqrt{-n}}{3k_1}$, where $\frac{k+1}{k_1} = k_2 \in Z$.and $k_1, k_2 \neq \pm 1$ then there does not exist any element of norm 1 (other than α) or of norm 2 in $\alpha G_{6,6}(2,Z)$.

(iv) Let $\alpha = \frac{2+\sqrt{-n}}{3k_1}$, where $n = 3k+2, k \in Z$ and $\frac{k+2}{k_1} = k_2 \in Z$ and $k_1, k_2 \neq \pm 1$. We mention the obtained information in the following table.

α	2	k_2	$3k_1$
$(\alpha)u$	$-2-3k_1$	k_1	$3(4+3k_1+k_2)$
$(\alpha)u^2$	$-10-6k_1-3k_2$	$4+3k_1+k_2$	$24+12k_1+9k_2$
$(\alpha)u^3$	$-14-6k_1-6k_2$	$8+4k_1+3k_2$	$3(8+3k_1+4k_2)$
$(\alpha)u^4$	$-10-3k_1-6k_2$	$8+3k_1+4k_2$	$12+3k_1+9k_2$
$(\alpha)u^5$	$-2-3k_2$	$4+k_1+3k_2$	$3k_2$
$(\alpha)v$	$-2+3k_2$	$-4+k_1+3k_2$	$3k_2$
$(\alpha)v^2$	$-10+3k_1+6k_2$	$-8+3k_1+4k_2$	$-12+3k_1+9k_2$
$(\alpha)v^3$	$-14+6k_1+6k_2$	$-8+4k_1+3k_2$	$3(-8+3k_1+4k_2)$
$(\alpha)v^4$	$-10+6k_1+3k_2$	$-4+3k_1+k_2$	$-24+12k_1+9k_2$
$(\alpha)v^5$	$-2+3k_1$	k_1	$3(-4+3k_1+k_2)$

From the preceding table we note that there does not exist any element of norm 2 (other than α) or of norm 1 in $\alpha G_{6,6}(2,Z)$. Similarly, if $\alpha = \frac{-2+\sqrt{-n}}{3k_1}$, where $\frac{k+2}{k_1} = k_2 \in Z$ and $k_1, k_2 \neq \pm 1$ then there does not exist any element of norm 2 (other than α) or of norm 1 in $\alpha G_{6,6}(2,Z)$.

If n is a positive integer then $d(n)$ is the arithmetic function defined by the number of positive divisors of n. For example, $d(1) = 1, d(2) = 2, d(3) = 2, d(4) = 3, d(5) = 2$ and $d(6) = 4$.

Theorem 3.4.4

(i) If $n = 3k$ where $k \in Z$ and $n \neq 3$ then the total number of orbits of $Q^*(\sqrt{-n})$ under the action of $G_{6,6}(2,Z)$ is $2d(k)$.

(ii) If $n = 3k+2$ where $k \in Z$ then the total number of orbits of $Q^*(\sqrt{-n})$ under the action of $G_{6,6}(2,Z)$ is equal to $4[d(k+1)+d(k+2)-2]$.

Proof

(i) As we have seen in Theorem 3.3.6, if $n = 3k$ where $k \in Z$ and $n \neq 3$ then there exists a alternate sequence $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m$ of totally positive and totally negative numbers such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ and $\|\alpha_m\| = 0$. This means that α_m is of the form $\frac{\sqrt{-n}}{3c}$. As $\frac{\sqrt{-n}}{3c} \in Q^*(\sqrt{-n})$, therefore, $\frac{n}{3c} = \frac{k}{c} \in Z$ and hence c divides k. This shows that the total number of orbits of $Q^*(\sqrt{-n})$ under the action of $G_{6,6}(2,Z)$, for $n = 3k$ is equal to $2d(k)$.

(ii) By Theorem 3.4.2, if $n = 3k + 2$ where $k \in Z$ then there exists a alternate sequence $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m$ of totally positive and totally negative numbers such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ and $\|\alpha_m\| = 1$ or 2. This means that α_m is of the form $\frac{\pm 1 + \sqrt{-n}}{3c}$ or $\frac{\pm 2 + \sqrt{-n}}{3c}$. By virtue of Theorem 3.4.3 (i) and (ii), corresponding to the divisors $\pm 1, \pm(k+1)$ of $k+1$ and $\pm 1, \pm(k+2)$ of $k+2$ there exist eight orbits of $Q^*(\sqrt{-n})$. Here we are left with $2d(k+1) - 4$ divisors of $k+1$ and $2d(k+2) - 4$ divisors of $k+2$. By Theorem 3.4.3 (iii) and (iv), there are $4d(k+1) - 8$ and $4d(k+2) - 8$ more orbits. Hence the total number of orbits of $Q^*(\sqrt{-n})$ are $8 + 4d(k+1) - 8 + 4d(k+2) - 8 = 4[d(k+1) + d(k+2) - 2]$.

Example 3.4.5 (i) When $n = 6$ and $6 = 3(2)$, we get $k = 2$ and so corresponding to the four divisors of 2, namely $\pm 1, \pm 2$, there are exactly 4 orbits of $Q^*(\sqrt{-6})$, namely, $\frac{\sqrt{-6}}{3}G_{6,6}(2,Z)$, $\frac{\sqrt{-6}}{-3}G_{6,6}(2,Z)$, $\frac{\sqrt{-6}}{6}G_{6,6}(2,Z)$ and $\frac{\sqrt{-6}}{-6}G_{6,6}(2,Z)$. Also, we can verify that $2d(k) = 2d(2) = 2(2) = 4$.

(ii) When $n = 11$ and $11 = 3(3) + 2$, we get $k = 3$ and so corresponding to the six divisors of 4, namely $\pm 1, \pm 2, \pm 4$ and four divisors of 5, namely $\pm 1, \pm 5$. Therefore the possible orbits of $Q^*(\sqrt{-11})$ are $\frac{1+\sqrt{-11}}{3}G_{6,6}(2,Z)$, $\frac{-1+\sqrt{-11}}{3}G_{6,6}(2,Z)$, $\frac{1+\sqrt{-11}}{-3}G_{6,6}(2,Z)$, $\frac{-1+\sqrt{-11}}{-3}G_{6,6}(2,Z)$,

$\frac{1+\sqrt{-11}}{6}G_{6,6}(2,Z)$, $\frac{-1+\sqrt{-11}}{6}G_{6,6}(2,Z)$, $\frac{1+\sqrt{-11}}{-6}G_{6,6}(2,Z)$, $\frac{-1+\sqrt{-11}}{-6}G_{6,6}(2,Z)$, $\frac{1+\sqrt{-11}}{12}G_{6,6}(2,Z)$, $\frac{-1+\sqrt{-11}}{12}G_{6,6}(2,Z)$, $\frac{1+\sqrt{-11}}{-12}G_{6,6}(2,Z)$, $\frac{-1+\sqrt{-11}}{-12}G_{6,6}(2,Z)$, $\frac{2+\sqrt{-11}}{5}G_{6,6}(2,Z)$, $\frac{-2+\sqrt{-11}}{5}G_{6,6}(2,Z)$, $\frac{2+\sqrt{-11}}{-5}G_{6,6}(2,Z)$, $\frac{-2+\sqrt{-11}}{-5}G_{6,6}(2,Z)$, $\frac{2+\sqrt{-11}}{15}G_{6,6}(2,Z)$, $\frac{-2+\sqrt{-11}}{15}G_{6,6}(2,Z)$, $\frac{2+\sqrt{-11}}{-15}G_{6,6}(2,Z)$ and $\frac{-2+\sqrt{-11}}{-15}G_{6,6}(2,Z)$. But $\frac{1+\sqrt{-11}}{3}$, $\frac{2+\sqrt{-11}}{15}$ lie in the same orbit, $\frac{-1+\sqrt{-11}}{3}$, $\frac{-2+\sqrt{-11}}{15}$ lie in the same orbit, $\frac{1+\sqrt{-11}}{-3}$, $\frac{2+\sqrt{-11}}{-15}$ lie in the same orbit, $\frac{-1+\sqrt{-11}}{-3}$, $\frac{-2+\sqrt{-11}}{-15}$ lie in the same orbit, $\frac{2+\sqrt{-11}}{3}$, $\frac{1+\sqrt{-11}}{12}$ lie in the same orbit, $\frac{-2+\sqrt{-11}}{3}$, $\frac{-1+\sqrt{-11}}{12}$ lie in the same orbit, $\frac{2+\sqrt{-11}}{-3}$, $\frac{1+\sqrt{-11}}{-12}$ lie in the same orbit and $\frac{-2+\sqrt{-11}}{-3}$, $\frac{-1+\sqrt{-11}}{-12}$ lie in the same orbit. Hence there are 12 orbits of $Q^*(\sqrt{-11})$. Now, we can verify that $4[d(k+1)+d(k+2)-2] = 4[d(4)+d(5)-2] = 4[3+2-2] = 12$.

Theorem 3.4.6 The action of $G_{6,6}(2,Z)$ on $Q^*(\sqrt{-n})$ is intransitive.

Proof

Since by Theorem 3.3.7, there exist six orbits of $Q^*(\sqrt{-3})$ and the minimum value of $4[d(k+1)+d(k+2)-2]$ is 8, therefore there exist at least six orbits of $Q^*(\sqrt{-n})$ and so the action of $G_{6,6}(2,Z)$ on $Q^*(\sqrt{-n})$ is intransitive.

So far, we have considered action of $G_{6,6}(2,Z)$ 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 chapter four, we consider coset diagrams for the action of $G_{6,6}(2,Z)$ on $PL(F_q)$. In this case we get coset diagrams of finite order, that is, coset diagrams with finite number of vertices.

We shall consider actions of $G_{6,6}(2,Z)$ 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 $\frac{\overline{m}}{\overline{n}}$ where bars indicate residues modulo prime q, unless $\overline{n} = 0$, when l is mapped on ∞. If $g : z \to \frac{az+b}{cz+d}$ is any element of the group $G_{6,6}(2, Z)$ or indeed any element of $GL(2, Q)$ whose determinant is a unit modulo p then g is let to act on $PL(F_q)$ by $z \to \frac{\overline{a}z+\overline{b}}{\overline{c}z+\overline{d}}$. This projection commutes with the action of $G_{6,6}(2, Z)$. Thus the coset diagram for the action of $G_{6,6}(2, Z)$ on $PL(F_q)$ can be obtained from the coset diagram for the action of $G_{6,6}(2, Z)$ on $PL(Q)$ by identifying appropriate points. The projection also commutes with $t : z \to \frac{1}{3z}$, so that the diagram for the action of $G_{6,6}(2, Z)$ admits an axis of symmetry which is the action of t.

We shall point out that for appropriate θ and q, the coset diagram for the action of $G_{6,6}(2, Z)$ on $PL(F_q)$ will also be an image under a projection of the diagram for the orbit $\sigma G_{6,6}(2, Z)$. In fact, if the positive square free integer n is a quadratic residue modulo q (and q does not divide $2n$) then in the integer ring R of the field $Q(\sqrt{n})$, q factorizes as the product of two distinct primes q_1 and q_2, and $R/q_i(i = 1$, or $2)$ is naturally isomorphic to $z \to Z/qZ = F_q$. Thus, we can construct two distinct projections from $PL(Q(\sqrt{n}))$ to $PL(F_q)$ using the primes q_1 and q_2 in the same way that we used the prime q previously (R is not necessarily a principal 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 q_i is a prime ideal of R, any element l of R can be written as $\frac{a}{b}$ when q_i does not divide both a and b. This is all that is necessary to construct the projection.

CHAPTER FOUR

$\Delta(6,6,\mathrm{k})$ & PARAMETRIZATION OF ACTIONS OF $\mathrm{G}^{*}_{6,6}(2,\mathrm{Z})$

4.1 Introduction

In this chapter, we parameterize the conjugacy classes of non-degenerate homomorphisms which represent actions of $\Delta(6,6,k)$ on $PL(F_q)$ where $q \equiv \pm 1(\bmod k)$. Also, for various values of k we shall find the conditions for the existence of coset diagrams depicting the permutation actions of $\Delta(6,6,k)$ on $PL(F_q)$. The conditions are polynomials with integer coefficients and the diagrams are such that every vertex in them is fixed by $(\overline{u}\,\overline{v})^k$. In this way, we get $\Delta(6,6,k)$ as permutation groups on $PL(F_q)$.

In second section of this chapter, we show that any non-degenerate homomorphism from $G_{6,6}(2,Z)$ into $G_{6,6}(2,q)$ can be extended to a homomorphism $G^{*}_{6,6}(2,Z)$ into $G^{*}_{6,6}(2,q)$. We show also that every element in $G_{6,6}(2,q)$, not of order 1 or 3 is the image of uv under some non-degenerate homomorphism. We parameterize the conjugacy classes of non-degenerate homomorphism σ with the non-trivial elements of F_q.

Let q be a prime power and F_q denote the finite field of order q. A one-to-one correspondence is established between the conjugacy classes of non-degenerate homomorphisms $\sigma : G^{*}_{6,6}(2,Z) \rightarrow G^{*}_{6,6}(2,q)$, under the action of inner automorphisms of $G^{*}_{6,6}(2,q)$, and the non-trivial conjugacy classes of elements of $G^{*}_{6,6}(2,q)$ such that the correspondence assigns to any non-degenerate homomorphisms σ the class containing $(uv)\sigma$.

It is known [19] that the group $G_{2,6}(2,Z) = < x,y : x^2 = y^6 = 1 >$ is generated by the linear fractional transformations x and y, where $(z)x = \frac{-1}{3z}$ and $(z)y = \frac{-1}{3(z+1)}$ are defined on the set of integers.

If we let $u = y, v = xyx$ then v can be considered as the linear fractional transformation defined by $(z)v = \frac{3z-1}{3z}$. So the group $G_{6,6}(2,Z) = < u,v >$ is a proper subgroup of the group $G_{2,6}(2,Z)$. Thus $G_{6,6}(2,Z) = < u,v : u^6 = v^6 = 1 >$ is the group of linear fractional transformations of the form $z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d \in Z$ and $ad-bc = 1$ or 3. Specifically, the linear fractional transformations of $G_{6,6}(2,Z)$ are $u : z \rightarrow \frac{-1}{3(z+1)}$ and $v : z \rightarrow \frac{3z-1}{3z}$ which satisfy the relations

$$u^6 = v^6 = 1 \qquad 4.1.1$$

The linear fractional transformation $t{:}z \rightarrow \frac{1}{3z}$ inverts u and v, that is, $t^2 = (ut)^2 = (vt)^2 = 1$ and so extends the group $G_{6,6}(2,Z)$ to $G^*_{6,6}(2,Z)$. The extended group $G^*_{6,6}(2,Z)$ is then the group of linear fractional transformations of the form $z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d \in Z$ and $ad-bc = 1$ or ± 3 and its finite presentation is given by

$$G^*_{6,6}(2,Z) = < u,v,t : u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 > \qquad 4.1.2$$

Let $PL(F_q)$ denote the projective line over the Galois field F_q, where q is a prime number. The points of $PL(F_q)$ are the elements of F_q together with the additional point ∞. The group $G^*_{6,6}(2,q)$ 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 $G_{6,6}(2,q)$ is its subgroup consisting of linear fractional transformations of the form $z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d \in F_q$ and $ad-bc$ is a non-zero square in

F_q.

For positive integers l, m and n, the triangle groups $\Delta(l,m,n)$ are the groups with abstract presentation $< u,v : u^l = v^m = (uv)^n = 1 >$. When $\frac{1}{l}+\frac{1}{m}+\frac{1}{n} > 1$, 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 tesselated using a triangle whose interior angles are $\frac{\pi}{l}$, $\frac{\pi}{m}$ and $\frac{\pi}{n}$. When $\frac{1}{l}+\frac{1}{m}+\frac{1}{n} = 1$, the group is infinite but soluble and the Euclidean plane can be tesselated using a triangle with angles $\frac{\pi}{l}$, $\frac{\pi}{m}$ and $\frac{\pi}{n}$. Finally, if $\frac{1}{l}+\frac{1}{m}+\frac{1}{n} < 1$, then the triangle group $\Delta(l,m,n)$ is infinite but insoluble and the hyperbolic plane can be tesselated using a hyperbolic triangle with angles $\frac{\pi}{l}$, $\frac{\pi}{m}$ and $\frac{\pi}{n}$.

The triangle groups have long received special attention. They have been subjects of extensive study primarily by Brahana [3], Miller [19] and Sinkov [27]. It is known that by adjoining an involution t, which inverts both u and v, the groups $\Delta(6,6,n)$ can be extended to the triangle groups $\Delta^*(6,6,n) = < u,v,t : u^6 = v^6 = (uv)^n = t^2 = (ut)^2 = (vt)^2 = 1 >$. The triangle group $\Delta(6,6,n)$ is of index 2 in $\Delta^*(6,6,n)$ and so is normal in $\Delta^*(6,6,n)$. By [9], the group $\Delta^*(2,m,n)$ has Coxeter group $G^{k,l,m} =< x,y,t : x^2 = y^k = (xy)^l = t^2 = (xt)^2 = (yt)^2 = (xyt)^m = 1 >$ as its factor group.

In this chapter we have discussed the triangle groups $\Delta(6,6,n)$ where $2 \leq n$. The group $\Delta(6,6,n)$ is infinite except for $n = 1$. In this case it is the cyclic group of order 6, that is, C_6.

4.2 Parameters for the Conjugacy Classes of $G^*_{6,6}(2,Z)$

The transformations $u : z \to \frac{-1}{3(z+1)}$, $v : z \to 1 - \frac{1}{3z}$ and $t : z \to \frac{1}{3z}$ generate $G^*_{6,6}(2,Z)$, subject to defining relations (4.1.2). Thus to choose a homomorphism

$\sigma : G^*_{6,6}(2,Z) \to G^*_{6,6}(2,q)$ amounts to choosing $\overline{u} = u\sigma$, $\overline{v} = v\sigma$ and $\overline{t} = t\sigma$, in $G^*_{6,6}(2,q)$ such that $\overline{u}^6 = \overline{v}^6 = \overline{t}^2 = (\overline{u}\,\overline{t})^2 = (\overline{v}\,\overline{t})^2 = 1$.

If the natural mapping $GL(2,q) \to G^*_{6,6}(2,q)$ maps a matrix M to the element g of $G^*_{6,6}(2,q)$ then $\theta = (tr(M))^2/\det(M)$ 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 $G^*_{6,6}(2,q)$. For instance, the class represented by a matrix with characteristic polynomial $z^2 - \theta z + \theta$ if $\theta \neq 0$ or $z^2 - 1$ if $\theta = 0$.

It is an easy fact that if U and V are two non-singular 2×2 matrices corresponding to the generators $\overline{u}$ and $\overline{v}$ of $G^*_{6,6}(2,Z)$ with $\det(UV) = 1$ and trace r, then of course UV will satisfy its characteristic equation

$$(UV)^2 - rUV + I = 0 \qquad 4.2.1$$

$$(UV)^2 = rUV - I \qquad 4.2.2$$

Multiplying equation (4.2.2) by UV on both sides. We obtain,

$$(UV)^3 = r(UV)^2 - (UV)I \qquad 4.2.3$$

Substituting the value of $(UV)^2$ from equation (4.2.2) in equation (4.2.3), we get

$$(UV)^3 = (r^2 - 1)UV - rI \qquad 4.2.4$$

On recursion, equation (4.2.4) yields

$$\begin{aligned}(UV)^k = &\{\binom{k-1}{0}r^{k-1} - \binom{k-2}{1}r^{k-3} + \ldots\}UV \\ &- \{\binom{k-2}{0}r^{k-2} - \binom{k-3}{1}r^{k-4} + \ldots\}I\end{aligned}$$

Furthermore, if we let

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

and substitute $r^2 = \theta$ in the polynomial $f(r)$ if k is odd and $r = \sqrt{\theta}$ otherwise, we obtain a polynomial $f(\theta)$.

A divisor d of a positive integer k is called a proper divisor if $1 < d < k$. Let $g_k(\theta) = f_k(\theta)$, if k is a prime number. For example, $g_2(\theta) = f_2(\theta) = \sqrt{\theta}$, $g_3(\theta) = f_3(\theta) = \theta - 1$, $g_5(\theta) = f_5(\theta) = \theta^2 - 3\theta + 1$ and so on. If $d_1, d_2, \ldots, d_n$ are the proper divisors of a positive integer k, then one can find a polynomial $g_k(\theta) = \frac{f_k(\theta)}{g_{d_1}(\theta) \cdot g_{d_2}(\theta) \cdots g_{d_n}(\theta)}$. The degree of the minimal polynomial $g_k(\theta)$ is thus given by, $\deg(g_k(\theta)) = \deg(f_k(\theta)) - \sum_{i=1}^{n} \deg(g_{d_i}(\theta))$, where $\deg(f_k(\theta)) = \frac{k}{2}$, if k is even and $\deg(f_k(\theta)) = \frac{k-1}{2}$ if k is odd. If k is a prime then $\deg(g_k(\theta)) = \frac{k-1}{2}$, on the other hand if $k = p^n$, where p is a prime, then $\deg(g_k(\theta)) = \frac{p^n - p^{n-1}}{2}$.

Now $\deg(g_4(\theta)) = \frac{2^2-2}{2} = 1$, $g_4(\theta) = \frac{f_4(\theta)}{g_2(\theta)} = \frac{\theta(\theta-2)}{\theta} = \theta - 2$

$\deg(g_6(\theta)) = \deg(f_6(\theta)) - \deg(g_2(\theta)) - \deg(g_3(\theta)) = 3 - 1 - 1 = 1$ and $g_6(\theta) = \frac{f_6(\theta)}{g_2(\theta) . g_3(\theta)}$ $= \frac{\theta(\theta^2-4\theta+3)}{\theta(\theta-1)} = \theta - 3$

$\deg(g_8(\theta)) = \frac{2^3-2^2}{2} = 2$ and $g_8(\theta) = \frac{f_8(\theta)}{g_2(\theta) . g_4(\theta)} = \frac{\theta(\theta^3-6\theta^2+10\theta-4)}{\theta(\theta-2)} = \theta^2 - 4\theta + 2$

$\deg(g_9(\theta)) = \frac{3^2-3}{2} = 3.$

We conclude here by mentioning that the actions of $G^*_{6,6}(2, Z)$ on $PL(F_q)$ which yield triangle groups $\Delta^*(6, 6, k)$ where q is congruent to $\pm 1 (\mathrm{mod}\, k)$. In the case where q is incongruent to $\pm 1 (\mathrm{mod}\, k)$, the group $G_{6,6}(2, Z)$ does not contain any element of order k. Thus its action is not faithful.

In the following, we list conditions in form of equations $f(\theta) = 0$ for the existence of triangle groups $\Delta(6,6,k)$ for $1 \leq k \leq 20$.

Triangle Group	**Minimal Equation satisfied by θ**
$\Delta(6,6,1)$	$\theta - 4 = 0$
$\Delta(6,6,2)$	$\theta = 0$
$\Delta(6,6,3)$	$\theta - 1 = 0$
$\Delta(6,6,4)$	$\theta - 2 = 0$
$\Delta(6,6,5)$	$\theta^2 - 3\theta + 1 = 0$
$\Delta(6,6,6)$	$\theta - 3 = 0$
$\Delta(6,6,7)$	$\theta^3 - 5\theta^2 + 6\theta - 1 = 0$
$\Delta(6,6,8)$	$\theta^2 - 4\theta + 2 = 0$
$\Delta(6,6,9)$	$\theta^3 - 6\theta^2 + 9\theta - 1 = 0$
$\Delta(6,6,10)$	$\theta^2 - 5\theta + 5 = 0$
$\Delta(6,6,11)$	$\theta^5 - 9\theta^4 + 28\theta^3 - 35\theta^2 + 15\theta - 1 = 0$
$\Delta(6,6,12)$	$\theta^2 - 4\theta + 1 = 0$
$\Delta(6,6,13)$	$\theta^6 - 11\theta^5 + 45\theta^4 - 84\theta^3 + 70\theta^2 - 21\theta + 1 = 0$
$\Delta(6,6,14)$	$\theta^3 - 7\theta^2 + 14\theta - 7 = 0$
$\Delta(6,6,15)$	$\theta^4 - 9\theta^3 + 26\theta^2 - 24\theta + 1 = 0$

$\Delta(6,6,16)$ $\quad \theta^4 - 8\theta^3 + 20\theta^2 - 16\theta + 2 = 0$

$\Delta(6,6,17)$ $\quad \theta^8 - 15\theta^7 + 19\theta^6 - 286\theta^5 + 495\theta^4 - 462\theta^3 + 210\theta^2$

$\quad - 36\theta + 1 = 0$

$\Delta(6,6,18)$ $\quad \theta^3 - 6\theta^2 + 9\theta - 3 = 0$

$\Delta(6,6,19)$ $\quad \theta^9 - 17\theta^8 + 120\theta^7 - 455\theta^6 + 1001\theta^5 - 1287\theta^4$

$\quad + 924\theta^3 - 330\theta^2 + 45\theta - 1 = 0$

$\Delta(6,6,20)$ $\quad \theta^4 - 8\theta^3 + 19\theta^2 - 12\theta + 1 = 0$

4.3 Parametrization of the Actions of $\Delta(6,6,\mathrm{k})$

Let $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $GL(2,q)$ which yields the element $\overline{u}$ of $G^*_{6,6}(2,q)$. Then, since $\overline{u}^6 = 1$, therefore, U^6 is a scalar matrix, and hence the $\det(U)$ is a square in F_q, where $q = \pm 1 (\mathrm{mod}\, 12)$. Thus, replacing U by a suitable scalar multiple, we assume that $\det(U) = 1$.

Since, for any matrix M, $M^6 = \lambda I$, where λ is a non-zero real number, if and only if $(Tr(M))^2 = 3\det(M)$. So, we may assume that $Tr(U) = a + d = \sqrt{3}$ and $\det(U) = 1$. Thus $U = \begin{bmatrix} a & b \\ c & -a+\sqrt{3} \end{bmatrix}$. Similarly, $V = \begin{bmatrix} e & f \\ g & -e+\sqrt{3} \end{bmatrix}$.

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

$b = kc$.

Thus we can consider $U = \begin{bmatrix} a & kc \\ c & -a+\sqrt{3} \end{bmatrix}$, $V = \begin{bmatrix} e & kf \\ f & -e+\sqrt{3} \end{bmatrix}$ and $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$,

as matrices corresponding to generators $\overline{u}$, $\overline{v}$ and $\overline{t}$ of $G^*_{6,6}(2,q)$, where $a, c, e, f, k \in F_q$.

Then,

$$1 + a^2 + kc^2 - \sqrt{3}\,a = 0 \tag{4.3.1}$$

and

$$1 + e^2 + kf^2 - \sqrt{3}\,e = 0 \tag{4.3.2}$$

because the determinants of U and V are 1.

This certainly evolves elements satisfying the relations $U^6 = V^6 = \lambda I$, where λ is a non-zero scalar and I is the identity matrix.

$$UV = \begin{bmatrix} a & kc \\ c & -a+\sqrt{3} \end{bmatrix}\begin{bmatrix} e & kf \\ f & -e+\sqrt{3} \end{bmatrix} = \begin{bmatrix} ae + kcf & akf - kce + \sqrt{3}\,kc \\ ce - af + \sqrt{3}f & ae + kcf + 3 - a\sqrt{3} - e\sqrt{3} \end{bmatrix}$$

The matrix UV has the trace

$$r = 2(ae + kcf) + 3 - \sqrt{3}\,(a + e) \tag{4.3.3}$$

If $Tr(UVT) = ks$, then

$$s = 2af - c(2e - \sqrt{3}\,) - \sqrt{3}f \tag{4.3.4}$$

So the relationship between (4.3.3) and (4.3.4) is

$$r^2 + ks^2 = 4a^2e^2 + 4k^2c^2f^2 + 8acefk + 9 + 3a^2 + 3e^2 + 6ae + 12ae + 12kcf$$

$$-4\sqrt{3}\,a^2e - 4\sqrt{3}\,akcf \text{-} 4\sqrt{3}\,ae^2 - 4\sqrt{3}\,kcef - 6\sqrt{3}\,a - 6\sqrt{3}\,e + 4ka^2f^2 + 3kf^2$$

$$-4\sqrt{3}\,akf^2 + 3kc^2 + 4kc^2e^2 - 4\sqrt{3}\,kec^2 + 4\sqrt{3}\,akcf - 8kacef - 6kcf + 4\sqrt{3}\,kcef$$

$$= 4e^2(a^2 + kc^2) + 4kf^2(a^2 + kc^2) + 3(e^2 + kf^2) + 3(a^2 + kc^2) - 4\sqrt{3}\,a(e^2 + kf^2)$$

$$-4\sqrt{3}\,e(a^2 + kc^2) + 9 + 18ae + 6kcf - 6\sqrt{3}\,a - 6\sqrt{3}\,e$$

$$= 4(a^2 + kc^2)(e^2 + kf^2) + (e^2 + kf^2)(3 - 4\sqrt{3}\,a) + (a^2 + kc^2)(3 - 4\sqrt{3}\,e) + 9$$

$$+18ae + 6kcf - 6\sqrt{3}\,a - 6\sqrt{3}\,e$$

$$= 4(3ae - \sqrt{3}\,a - \sqrt{3}\,e + 1) + (3\sqrt{3}\,e - 12ae - 3 + 4\sqrt{3}\,a) + (3\sqrt{3}\,a - 12ae - 3$$

$$+4\sqrt{3}\,e) + 9 + 18ae + 6kcf - 6\sqrt{3}\,a - 6\sqrt{3}\,e$$

$$= 7 - 3\sqrt{3}\,a - 3\sqrt{3}\,e + 6ae + 6kcf$$

$$= 7 - 3\sqrt{3}\,(a + e) + 6(ae + kcf)$$

$$= 7 + 3[2(ae + kcf) - \sqrt{3}\,(a + e)]$$

$$= 7 + 3(r - 3)$$

$$r^2 + ks^2 = 3r - 2 \qquad 4.3.5$$

We set

$$\theta = r^2 \qquad 4.3.6$$

Example 4.3.1 In this example we consider an action of $G^*_{6,6}(2,Z)$ on $PL(F_{13})$. Suppose that $\theta = 3$, then by (4.3.6), $\theta = r^2$ and so $r^2 = 3 \equiv 16(\text{mod}\,13)$ implies that $r = \pm 4$. We consider $r = 4$. Substituting the value of r in (4.3.5) and supposing that $k = 2$, we get

$s^2 = -3 \equiv 49$. This implies that $s = \pm 7$. We choose $s = 7$. If we suppose $a = 1$ in equation (4.3.1), we obtain $c^2 = 1$, that is, $c = \pm 1$. If we suppose $c = 1$ and substitute the values of r, s, a, k and c in equations (4.3.3) and (4.3.4), we obtain $5 = 4f - 2e$ and $-3 = 2f + 2e$. Solving these equations for e and f, we obtain $e = f = -4$. Thus $U = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$, $V = \begin{bmatrix} -4 & -8 \\ -4 & 8 \end{bmatrix}$ and $T = \begin{bmatrix} 0 & -2 \\ 1 & 0 \end{bmatrix}$. So, $\overline{u}$, $\overline{v}$ and $\overline{t}$ will be $\overline{u} : z \to \frac{z+2}{z+3}$, $\overline{v} : z \to \frac{z+2}{z-2}$, and $\overline{t} : z \to \frac{-2}{z}$ respectively.

If we now consider the action of $\overline{u}$, $\overline{v}$ and $\overline{t}$ on $PL(F_{13})$, we obtain

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

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

$\overline{t} : (0\ \infty)(1\ 11)(2\ 12)(3\ 8)(4\ 6)(5\ 10)(7\ 9)$.

We can easily verify that every element of $PL(F_{13})$ is fixed by$(\overline{u}\,\overline{v})^6$.

4.4 Parametrization of the Actions of $\Delta(6, 6, k; n)$

Let $\Delta(6,6,k;n)$ denote the generalized triangule group $< u, v, t : u^6 = v^6 = (uv)^k = (uvu^{-1}v^{-1})^n = t^2 = (ut)^2 = (vt)^2 = 1 >$. Clearly, $\Delta(6,6,k;n)$ is a factor group of $\Delta(6,6,k)$.

As we have seen in the previous section $U = \begin{bmatrix} a & kc \\ c & -a+\sqrt{3} \end{bmatrix}$, $V = \begin{bmatrix} e & kf \\ f & -e+\sqrt{3} \end{bmatrix}$, this gives

$U^{-1} = \begin{bmatrix} -a+\sqrt{3} & -kc \\ -c & a \end{bmatrix}$, $V^{-1} = \begin{bmatrix} -e+\sqrt{3} & -kf \\ -f & e \end{bmatrix}$. Let l be the trace of $UVU^{-1}V^{-1}$ then after using (4.3.1) to (4.3.5), we get $r^2 - ks^2 = 2l + 3r - 6$ 4.4.1

Thus $r^2 + ks^2 = 3r - 2$, implies that

$$r^2 = l + 3r - 4 \qquad 4.4.2$$

Since $\det(UVU^{-1}V^{-1}) = 1$ and its trace is equal to l, therefore the characteristic equation of $UVU^{-1}V^{-1}$ is

$$(UVU^{-1}V^{-1})^2 - l(UVU^{-1}V^{-1}) + I = 0 \qquad 4.4.3$$

or

$$(UVU^{-1}V^{-1})^2 = l(UVU^{-1}V^{-1}) - I \qquad 4.4.4$$

Multiplying equation (4.4.4) by $UVU^{-1}V^{-1}$ on both sides. We obtain,

$$(UVU^{-1}V^{-1})^3 = l(UVU^{-1}V^{-1})^2 - (UVU^{-1}V^{-1})I \qquad 4.4.5$$

Substituting the value of $(UVU^{-1}V^{-1})^2$ from equation (4.4.4) in equation (4.4.5), we get

$$(UVU^{-1}V^{-1})^3 = (l^2 - 1)UVU^{-1}V^{-1} - lI \qquad 4.4.6$$

On recursion, equation (4.4.6) yields

$$\begin{aligned}(UVU^{-1}V^{-1})^n = {} & \{\binom{n-1}{0}l^{n-1} - \binom{n-2}{1}l^{n-3} + \ldots\}UVU^{-1}V^{-1} \\ & - \{\binom{n-2}{0}l^{n-2} - \binom{n-3}{1}l^{n-4} + \ldots\}I\end{aligned}$$

Furthermore, if we let

$$f(l) = \binom{n-1}{0}l^{n-1} - \binom{n-2}{1}l^{n-3} + \ldots$$

Let $f_k(l)$ denote the polynomial obtained by putting $n = k$ in $f(l)$. If $d_1, d_2, \ldots, d_n$ are the proper divisors of a positive integer k, then one can find a polynomial $g_k(l) = \frac{f_k(l)}{g_{d_1}(l) \cdot g_{d_2}(l) \cdots g_{d_n}(l)}$, where $g_k(l) = f_k(l)$ if k is a prime number. The degree of the minimal polynomial $g_k(l)$ is thus given by, $\deg(g_k(l)) = \deg(f_k(l)) - \sum_{n=1}^{k} \deg(f_{d_n}(l))$, where $\deg(f_k(l)) = k - 1$. If k is prime, then $\deg(f_k(l)) = k - 1$. On the other hand if $k = p^n$, where p is prime, then $\deg(f_k(l)) = p^n - p^{n-1}$. For various values of n, we obtain the minimal equations satisfied by l. We list them as follows.

n	**Minimal Equation satisfied by l**
1	$l - 2 = 0$
2	$l = 0$
3	$l^2 - 1 = 0$
4	$l^2 - 2 = 0$
5	$l^4 - 3\,l^2 + 1 = 0$
6	$l^2 - 3 = 0$
7	$l^6 - 5l^4 + 6\,l^2 - 1 = 0$
8	$l^4 - 4\,l^2 + 2 = 0$
9	$l^6 - 6l^4 + 9\,l^2 - 1 = 0$
10	$l^4 - 5\,l^2 + 5 = 0$
11	$l^{10} - 9l^8 + 28l^6 - 35l^4 + 15l^2 - 1 = 0$
12	$l^4 - 4l^2 + 1 = 0$

13	$l^{12} - 11l^{10} + 45l^{8} - 84l^{6} + 70l^{4} - 21l^{2} + 1 = 0$
14	$l^{6} - 7l^{4} + 14l^{2} - 7 = 0$
15	$l^{8} - 9l^{6} + 26l^{4} - 24l^{2} + 1 = 0$
16	$l^{8} - 8l^{6} + 20l^{4} - 16l^{2} + 2 = 0$
17	$l^{16} - 15l^{14} + 19l^{12} - 286l^{10} + 495l^{8} - 462l^{6} + 210l^{4}$ $- 36l^{2} + 1 = 0$
18	$l^{6} - 6l^{4} + 9l^{2} - 3 = 0$
19	$l^{18} - 17l^{16} + 120l^{14} - 455l^{12} + 1001l^{10} - 1287l^{8} + 924l^{6}$ $- 330l^{4} + 45l^{2} - 1 = 0$
20	$l^{8} - 8l^{6} + 19l^{4} - 12l^{2} + 1 = 0.$

Example 4.4.1 Here we consider an action of $G^{*}_{6,6}(2,Z)$ on $PL(F_{13})$. Suppose that $l = 1$, since $r^2 = l + 3r - 4$ then we have $r = \frac{3\pm\sqrt{-3}}{2} \equiv 5, 11(\mathrm{mod}\,13)$. Let us take r = 5. Substituting the value of r in (4.3.5) and supposing that $k = -1$, we get $s^2 = 25$. This implies that $s = \pm 5$. We choose $s = 5$. If we suppose $a = 2$ in equation (4.3.1) we have $c^2 = 36$, that is, $c = \pm 6$. Suppose $c = 6$ and substitute the values of r, s, a, k and c in equations (4.3.3) and (4.3.4), to obtain $f = -3$ and $e = -6$. Thus $U = \begin{bmatrix} 1 & -3 \\ 3 & 1 \end{bmatrix}$, $V = \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix}$. So, $\overline{u}$ and $\overline{v}$ will be $\overline{u} : z \to \frac{z-3}{3z+1}$ and $\overline{v} : z \to \frac{2z-1}{z+1}$ respectively.

The action of $\overline{u}$ and $\overline{v}$ on $PL(F_{13})$ yields the following permutations

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

$\overline{v}$: (0 12 ∞ 2 1 7)(3 11 5 8 6 9)(4)(10)

and they are such that every element of $PL(F_{13})$ is fixed by $(\overline{u}\,\overline{v}\,\overline{u}^{-1}\overline{v}^{-1})^3$ and $(\overline{u}\,\overline{v})^7$.

In this section, we have parametrized actions of $G^*_{6,6}(2,Z)$ on $PL(F_q)$, except for a few uninteresting ones, by the elements of F_q. We have shown that any homomorphism from $G_{6,6}(2,Z)$ into $G_{6,6}(2,q)$ can be extended to a homomorphism from $G^*_{6,6}(2,Z)$ into $G^*_{6,6}(2,q)$. We have shown also that every element in $G_{6,6}(2,q)$, not of order 1, or 3 is the image of uv under some non-degenerate homomorphism from $G^*_{6,6}(2,Z)$ into $G^*_{6,6}(2,q)$. We have proved that the conjugacy classes of non-degenerate homomorphisms σ are in one-to-one correspondence with the conjugacy classes of non-trivial elements of $G^*_{6,6}(2,q)$, under a correspondence which assigns to the homomorphism σ the class containing $(uv)\sigma$. Of course, in this way we have actually parametrized the actions of $G^*_{6,6}(2,q)$ on $PL(F_q)$, except for a few uninteresting ones, by the elements of F_q. We have developed a useful mechanism by which a unique coset diagram can be constructed [18], for each conjugacy class of these non-degenerate homomorphism which depict the actions of $G^*_{6,6}(2,Z)$ on $PL(F_q)$.

4.5 Conjugacy Classes of the Non-degenerate Homomorphisms

The transformations $u : z \to \frac{-1}{3(z+1)}$, $v : z \to 1 - \frac{1}{3z}$ and $t : z \to \frac{1}{3z}$ generate $G^*_{6,6}(2,Z)$, subject to defining relations (4.1.2). Thus to choose a homomorphism $\sigma : G^*_{6,6}(2,Z) \to G^*_{6,6}(2,Z)$ amounts to choosing $\overline{u} = u\sigma, \overline{v} = v\sigma$ and $\overline{t} = t\sigma$, in $G^*_{6,6}(2,Z)$ such that $\overline{u}^6 = \overline{v}^6 = \overline{t}^2 = (\overline{u}\,\overline{t})^2 = (\overline{v}\,\overline{t})^2 = 1$.

The homomorphism σ is called non-degenerate if neither of the generators u, v of

$G^*_{6,6}(2,Z)$ lies in the kernel of σ, that is, the images $\overline{u}$ and $\overline{v}$ are of orders 6. Two homomorphisms σ_1 and σ_2 from $G^*_{6,6}(2,Z)$ to $G^*_{6,6}(2,Z)$ are called conjugate if there exists an inner automorphism ρ of $G^*_{6,6}(2,Z)$ such that $\sigma_2 = \rho\sigma_1$. Both $G_{6,6}(2,Z)$ and $G^*_{6,6}(2,Z)$ have index 2 in their automorphism groups. Let δ be the automorphism on $G^*_{6,6}(2,Z)$ defined by $u\delta = tut, v\delta = v$, and $t\delta = t$.

The homomorphism $\sigma' = \delta\sigma$ is called the dual homomorphism of σ. This, of course, means that if σ maps u, v, t to $\overline{u}, \overline{v}, \overline{t}$, then σ' maps u, v, t to $\overline{t}\,\overline{u}\,\overline{t}$, $\overline{v}$, $\overline{t}$ respectively. Since the elements $\overline{u}, \overline{v}, \overline{t}$ as well as $\overline{t}\,\overline{u}\,\overline{t}, \overline{v}, \overline{t}$ satisfy the relations (4.1.1), therefore the solutions of these relations occur in dual pairs. Of course, if σ_1 is conjugate to σ_2 then σ'_1 is conjugate to σ'_2. The parameter of σ, or of the conjugacy class containing σ, is the parameter of $\overline{u}\,\overline{v}$.

Thus for each θ, which is a square in F_q, there exists a unique coset diagram. It is unique for θ in F_q in the sense that the diagram is the same except for the labels in the conjugacy class that it represents. Hence for some θ, we can find a pair $\overline{u}, \overline{v}$, for a homomorphism σ, and consequently a coset diagram.

A pair $\overline{u}, \overline{v}$, satisfying the relations $\overline{u}^6 = \overline{v}^6 = 1$, in $G_{6,6}(2,q)$ is called invertible if there exists $\overline{t}$ in $G^*_{6,6}(2,Z)$ is such that $\overline{t}^2 = 1$, $\overline{t}\,\overline{u}\,\overline{t} = \overline{u}^{-1}$ and $\overline{t}\,\overline{v}\,\overline{t} = \overline{v}^{-1}$.

By $D(\theta,q)$ we shall mean a coset diagram associated with the conjugacy class of non-degenerate homomorphisms α of $G^*_{6,6}(2,Z)$ into $G^*_{6,6}(2,q)$ corresponding to $\theta \in F_q$. For each conjugacy class of pairs $(\overline{u}, \overline{v})$ we can draw a coset diagram $D(\theta,q)$.

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

Lemma 4.5.1 A non-singular 2×2 matrix M with entries in F_q, where q is not a power of 2, represents, an involution in $G^*_{6,6}(2,q)$ if and only if the $Tr(M)$ is zero.

Lemma 4.5.2 If $\overline{u}, \overline{v}$ are elements of $G^*_{6,6}(2,q)$ and $\overline{u}\,\overline{v} \neq 1$, then either $\overline{u}\,\overline{v}$ is of order 3 or $\overline{t}$ inverts both $\overline{u}$ and $\overline{v}$.

Proof

Let U be an element of $GL(2,q)$ which yields the element $\bar{u}$ of $G^*_{6,6}(2,q)$. Since $(\bar{u})^6 = 1$, therefore we can assume that U has the form $\begin{bmatrix} 0 & -1 \\ 1 & -\sqrt{3} \end{bmatrix}$.

Let $V = \begin{bmatrix} a & b \\ c & -a+\sqrt{3} \end{bmatrix}$ and $T = \begin{bmatrix} l & m \\ n & -l \end{bmatrix}$ where $1 + a^2 + bc - \sqrt{3}\,a = 0$

Now suppose that there exists a transformation $\overline{t}$ in $G^*_{6,6}(2,Z)$ such that $\overline{t}^2 = (\overline{u}\,\overline{t})^2 = (\overline{v}\,\overline{t})^2 = 1$. Let r be the trace of UV. Then $r = 3 + b - c - \sqrt{3}\,a$. Now $UT = \begin{bmatrix} 0 & -1 \\ 1 & -\sqrt{3} \end{bmatrix}\begin{bmatrix} l & m \\ n & -l \end{bmatrix} = \begin{bmatrix} -n & l \\ l-\sqrt{3}\,n & m-\sqrt{3}\,l \end{bmatrix}$ give us $-n + m - \sqrt{3}\,l = 0$ or

$$m = n + \sqrt{3}\,l \qquad 4.5.1$$

Also $VT = \begin{bmatrix} a & b \\ c & -a+\sqrt{3} \end{bmatrix}\begin{bmatrix} l & m \\ n & -l \end{bmatrix} = \begin{bmatrix} al+bn & am-bl \\ cl-an+\sqrt{3}\,n & cm+al-\sqrt{3}\,l \end{bmatrix}$ yields

$2al + bn + cm - \sqrt{3}\,l = 0$ or $2al + bn + c(n + \sqrt{3}\,l) - \sqrt{3}\,l = 0$ or $2al + \ bn + cn \ + \sqrt{3}\,cl)$ $- \sqrt{3}\,l = 0$. Hence

$$(2a + \sqrt{3}\,c - \sqrt{3}\,)l + (b + c)n = 0 \qquad 4.5.2$$

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

$-l^2 - mn \neq 0$ or $l^2 + mn \neq 0$ or $l^2 + n(n + \sqrt{3}\, l) \neq 0$ or $l^2 + n^2 + \sqrt{3}\, nl \neq 0$ or $(\frac{l}{n})^2 + 1 + \sqrt{3}\,(\frac{l}{n}) \neq 0$ 4.5.3

Thus the necessary and sufficient conditions for the existence of $\overline{t}$ in $G^*_{6,6}(2,q)$ are the equations (4.5.2), and (4.5.3). Hence $\overline{t}$ exists in $G^*_{6,6}(2,q)$ unless $(\frac{l}{n})^2{+}1 + \sqrt{3}\,(\frac{l}{n}) = 0$. Of course, if both $2a + \sqrt{3}\, c - \sqrt{3}$ and $b + c$ are equal to zero, then the existence of $\overline{t}$ is trivial. If not, then $\frac{l}{n} = \frac{-(b+c)}{2a+\sqrt{3}\, c-\sqrt{3}}$, and so equation (4.5.3) is equivalent to $(b+c)^2 + (2a + \sqrt{3}\, c - \sqrt{3}\,)^2 + (2a + \sqrt{3}\, c - \sqrt{3}\,)(b + c) \neq 0$. Thus there exists $\overline{t}$ in $G^*_{6,6}(2,q)$ such that $\overline{t}^2 = (\overline{u}\,\overline{t})^2 = (\overline{v}\,\overline{t})^2 = 1$ unless $(b + c)^2 + (2a + \sqrt{3}\, c - \sqrt{3}\,)^2 = \sqrt{3}\,(2a + \sqrt{3}\, c - \sqrt{3}\,)(b + c)$. This yields $(b - c)^2 + 4bc + 4a^2 + 3c^2 + 3 + 4\sqrt{3}\, ac - 4\sqrt{3}\, a - 6c = \sqrt{3}\,(2ab + \sqrt{3}\, bc - \sqrt{3}\, b + 2ac + \sqrt{3}\, c^2 - \sqrt{3}\, c)$.

After simplification we get $r^2 - 3r + 2 = 0$. So, $r^2 = 3r - 2$ and after squaring both sides, we get $\theta^2 - 5\theta + 4 = 0$. This implies that $\theta = 1$ or $\theta = 4$.

By the table in Section 2 , $\theta = 1$ implies that the order of $\overline{u}\,\overline{v}$ is 3 and $\theta = 4$ gives the order of $\overline{u}\,\overline{v}$ is 1, so neglecting it because $(\overline{u}\,\overline{v}) \neq 1$, the parameter of $\overline{u}\,\overline{v}$ is 1 and the order of $\overline{u}\,\overline{v}$ is 3.

In our subsequent work we shall find a relationship between the parameters of the dual homomorphisms. We first need to prove the following.

Lemma 4.5.3 Any non trivial element $\overline{g}$ of $G^*_{6,6}(2,q)$ whose order is not equal to 2 and whose dual is also not of order 2, is the image of uv under some non-degenerate homomorphism σ of $G^*_{6,6}(2,Z)$ into $G^*_{6,6}(2,q)$.

Proof

Using lemma 4.5.2, we show that every non-trivial element of $G^{*}_{6,6}(2,q)$ is a product of two elements of order 3. So we find elements $\overline{u}, \overline{v}$ and, $\overline{t}$ of $G^{*}_{6,6}(2,q)$ satisfying the relations (4.1.2) with $\overline{u}\,\overline{v}$ in a given conjugacy class. Since $\overline{g} = \overline{u}.\overline{v}$ (or its dual $\overline{u}.\overline{v}.\overline{t}$) are not of order 2, the class to which we want $\overline{u}.\overline{v}$ to belong does not consist of involutions, so that $(\overline{u}.\overline{v})^2 \neq 1$ and $(\overline{u}.\overline{v}.\overline{t})^2 \neq 1$. Thus the traces of the matrices UV and UVT are not equal to zero, by Lemma 4.5.1. 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, f in F_q so that r^2 is indeed equal to θ. The solution of θ is therefore arbitrarily in F_q. We can choose r to satisfy $\theta = r^2$. Equation (4.3.5), yields $ks^2 = -2 + 3r - r^2$. If $r^2 \neq -2 + 3r$, we select k as above.

Any quadratic polynomial $\lambda z^2 + \mu z + v$, with coefficients in F_q takes at least $(q+1)/2$ distinct values, as z runs through F_q. Since the equation $\lambda z^2 + \mu z + v = k$ has at most two roots for fixed k and there are q elements in F_q, where q is odd throughout in this chapter. In particular, $a^2 - \sqrt{3}\,a$ and $-kc^2 - 1$ each taking at least $(q+1)/2$ distinct values as a and c run through F_q. Similarly, $e^2 - \sqrt{3}\,e$ and $-kf^2 - 1$ each takes at least $(q+1)/2$ distinct values as e and f run through F_q. Hence we can find a and c so that $a^2 - \sqrt{3}\,a = -kc^2 - 1$ and e, f so that $e^2 - \sqrt{3}\,e = -kf^2 - 1$.

Finally, by substituting the values of r, s, a, c, e, f, k in equations (4.3.3) and (4.3.4) we obtain the values of e and f. These equations are linear equations for e and f with determinant $(2a - \sqrt{3})^2 + 4kc^2 = 4a^2 + 3 - 4\sqrt{3}\,4kc^2 = 4(a^2 + kc^2 - \sqrt{3}\,a) + 3 = -4 + 3 = -1$. It is non-zero, so that we can find e and f satisfying equation (4.3.2). It is obvious from (4.3.5) and (4.3.6) that $\theta = 0$ when $r = 0$ and $\theta = 1$ or 4 when $s = 0$. By the table in the Section 2, the possibility that $\theta = 0$ gives rise to the situation where $\overline{u}.\overline{v}$ is of order 2. Similarly, the possibility $\theta = 1$ leads to the situation where $\overline{u}.\overline{v}$ is of order 3 and $\theta = 4$ yields $\overline{u}.\overline{v}$ of order 1.

Theorem 4.5.4 The conjugacy classes of non-degenerate homomorphisms of $G^*_{6,6}(2,Z)$ into $G^*_{6,6}(2,q)$ are in one-to-one correspondence with the non-trivial conjugacy classes of elements of $G^*_{6,6}(2,q)$ under a correspondence which assigns to any non-degenerate homomorphism σ the class containing $(uv)\sigma$.

Proof

Let $\sigma : G^*_{6,6}(2,Z) \rightarrow G^*_{6,6}(2,q)$ be a non-degenerate homomorphism such that it maps u, v to $\overline{u}, \overline{v}$. Let θ be the parameter of the class represented by $\overline{u}\ \overline{v}$. Now α is determined by $\overline{u}, \overline{v}$ and each θ evolves a pair $\overline{u}, \overline{v}$, so that σ is associated with θ. We shall call the parameter θ of the class containing $\overline{u}\ \overline{v}$, the parameter of the non-degenerate homomorphism of $G^*_{6,6}(2,Z)$ into $G^*_{6,6}(2,q)$. Now $UT = \begin{bmatrix} ck & -ak \\ -a+\sqrt{3} & -ck \end{bmatrix}$ implies that $\det(UT) = -k(a^2 + a + kc^2) = k$ (equation 4.1). Also, $(UT)V = \begin{bmatrix} kec - akf & k^2fc + ak(e - \sqrt{3}) \\ -ae + e\sqrt{3} - kfc & -akf + kf\sqrt{3} + ck(e - \sqrt{3}) \end{bmatrix}$ implies that $Tr((UT)V) = 2kec - 2akf + \sqrt{3}\,kf - \sqrt{3}\,kc = -k(-2ce + 2af - \sqrt{3}f + \sqrt{3}\,c) = -ks$. If $\overline{u}, \overline{v}, \overline{t}$ satisfy the relations (4.1.2), then so do $\overline{t}\,\overline{u}\,\overline{t}, \overline{v}, \overline{t}$. So that the solution of relations (4.1.2) occur in dual pairs. Hence replacing the solutions in Lemma 4.5.3 by $\overline{t}\,\overline{u}\,\overline{t}, \overline{v}, \overline{t}$, we have $\theta = \frac{[Tr((UT)V]^{2}}{\det(UT)} = \frac{k^2s^2}{k} = ks^2$. We then find a relationship between the parameters of the dual non-degenerate homomorphisms.

There is an interesting relationship between the parameters of the dual non-degenerate homomorphisms. We discuss this as follows.

Corollary 4.5.5

If $\sigma : G^*_{6,6}(2,Z) \rightarrow G^*_{6,6}(2,q)$ is a non-degenerate homomorphism, σ' is its dual and θ, ϕ are their respective parameters then $\theta + \phi = 3r - 2$.

Proof

Let $\sigma : G^*_{6,6}(2,Z) \rightarrow G^*_{6,6}(2,q)$ be a non-degenerate homomorphism satisfying the relations $u\sigma = \overline{u}$, $v\sigma = \overline{v}$ and $t\sigma = \overline{t}$. Let σ' be the dual of σ. As previouly in this Section , we choose the matrices $U = \begin{bmatrix} a & ck \\ c & -a+\sqrt{3} \end{bmatrix}$, $V = \begin{bmatrix} e & fk \\ f & -e+\sqrt{3} \end{bmatrix}$ and $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$, representing $\overline{u}, \overline{v}$ and $\overline{t}$, respectively such that they satisfy the equations from (4.3.1) to (4.3.5). Now by Lemma 4.5.1, we have $Tr(UV) = 0$ if and only if $(\overline{u}\,\overline{v})^2 = 1$. Also, we have $\{Tr(UVT)\}/k = s = 0$ if and only if $(\overline{u}\,\overline{v}\,\overline{t})^2 = 1$. Then $\det(UV) = 1$, thus giving the parameter of $\overline{u}\ \overline{v}$ equal to $r^2 = \theta$. Also since $Tr(UVT) = ks$ and $\det(UVT) = k$ (since $\det(U) = 1$, $\det(V) = 1$ and $\det(T) = k$), we obtain the parameter of $\overline{u}\,\overline{v}\,\overline{t}$ equal to ks^2, which we denote by ϕ. Thus $\theta + \phi = r^2 + ks^2$. Substituting the values from equation (4.3.5), we therefore obtain $\theta + \phi = 3r - 2$. Hence if θ is the parameter of the non-degenerate homomorphism σ, then $\phi = 3r - 2 - \theta$ is the parameter of the dual σ' of σ.

Theorem 4.5.4, of course, means that we can actually parametrize the non-degenerate homomorphisms of $G^*_{6,6}(2,Z)$ to $G^*_{6,6}(2,q)$ except for a few uninteresting ones, by the elements of F_q. Since $G^*_{6,6}(2,q)$ has a natural permutation representation on $PL(F_q)$, any homomorphism $\sigma : G^*_{6,6}(2,Z) \rightarrow G^*_{6,6}(2,q)$ gives rise to an action of $G^*_{6,6}(2,Z)$ 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 homomorphisms corresponding to each parameter θ, which is a square in F_q, by determining $\overline{u}$, $\overline{v}$ with the help of Theorem 4. 5. 4.

BIBLIOGRAPHY

[1] G. Baumslag, J.W. Morgan and P.B. Shalen, Generalized triangle groups, Math. Proc. Camb. Phil. Soc., 102(1987), 25 – 31.

[2] 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.

[3] W. Burnside, Theory of groups of finite order, 2nd. ed., Dover Pub. Inc., New York, 1955.

[4] A. Cayley, The theory of groups: graphical representations, Amer. J. Math., 1(1878), 174 – 176.

[5] M.D.E. Conder, Generators for alternating and symmetric groups, J. London Math. Soc., (2),22(1980), 75 – 86.

[6] M.D.E. Conder, Schreier coset graphs and their applications, RIMS Kokyuroku, 794(1992), 169 – 175.

[7] H.S.M. Coxeter and W.O.J. Moser, Generators and relations for discrete groups, 4th ed., Springer Verlag, Berlin, 1980.

[8] L. E. Dickson, Linear groups: with exposition of the Galois field theory, Dover Pub. Inc., New. York, 1958.

[9] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 4th. ed.,

$PGL(2,q)$, Comm. Algebra, 20, 4(1992), 1023 – 1040.

[19] Q. Mushtaq and M. Aslam, Group generated by two elements of orders 2 and 6 acting on R and $Q(\sqrt{n})$, Disc. Math., 79(1998)145 – 154.

[20] Q. Mushtaq, On word structure of the modular group over finite and real quadratic fields, Disc. Math., 178(1998), 155 – 164.

[21] I.Samuel, Algebraic theory of numbers, 1st. ed. Hermann Publisher in Arts and Science, Paris, France,1970

[22] 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.

[23] R. Steinberg, Finite reflection groups, Trans. Amer. Math. Soc., 91(1959), 493 – 504.

[24] W.W. Stothers, Subgroups of (2,3,7) triangle groups, Manuscripta Math., 20(1977), 323 – 334.

[25] J.H.C. Whitehead, On certain sets of elements in a free group, Proc. London Math. Soc., 2, 41(1936), 48 – 56.

[26] H. Wielandt, Finite permutation groups, Academic Press, New York, 1964.