

ACTIONS OF A SUBGROUP OF $PGL(2,C)$



By

Saima Anis

Supervised by

Prof. Qaiser Mushtaq

Department of Mathematics
Quaid-i-Azam University, Islamabad
2009

ACTIONS OF A SUBGROUP OF $PGL(2,C)$



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

By

Saima Anis

Department of Mathematics
Quaid-i-Azam University, Islamabad
2009

Certificate

ACTIONS OF A SUBGROUP OF $PGL(2,C)$

By

Saima Anis

A thesis submitted in the partial fulfillment of the requirement for the degree
of Doctor of Philosophy

We accept this thesis as conforming to the required standard.

1. 

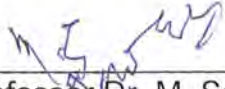
Professor Dr. Qaiser Mushtaq
(Supervisor)

2. 

Professor Dr. Muhammad Ayub
(Chairman)

3. 

Professor Dr. Muhammad Aslam
(External Examiner)

4. 

Professor Dr. M. Sarwar Kamran
(External Examiner)

Department of Mathematics
Quaid-i-Azam University, Islamabad
2009

With everlasting love
and dedication
to my mother
and
to the memory of my late father

Acknowledgements

Thanks to Almighty Allah, the most Merciful and Compassionate who enabled me to complete this thesis.

I am indebted to my supervisor, Professor Qaiser Mushtaq for his encouragement and invaluable discussions which enabled me to accomplish this work. I would never have been able to do it without his continual guidance.

I am grateful to my husband Dr. Madad Khan for his help and cooperation. I cannot forget to thank my friends who morally supported me in completing this task.

Finally, I wish to express my heartiest gratitude to my mother, sister and brothers for their prayers and moral support during my studies.

July 2009



Saima Anis

Notations

The symbols and notations that have been used in this thesis are by and large standard and are available in [16], [17] and [31]. However, some extensively used symbols in this thesis are given below for the sake of convenience.

$$\Gamma = \langle A, B, C, D : A^3 = B^2 = C^3 = D^2 = (AC)^2 = (AD)^2 = (BC)^2 = (BD)^2 = 1 \rangle.$$

$$G_1 = \langle A, C, D : A^3 = C^3 = D^2 = (AC)^2 = (AD)^2 = 1 \rangle.$$

$$G_2 = \langle B, C, D : B^2 = C^3 = D^2 = (BC)^2 = (BD)^2 = 1 \rangle.$$

$$M = \langle C, D : C^3 = D^2 = 1 \rangle.$$

$$\mathbb{Q}^*(ki) = \left\{ \frac{a + ki}{c} : a, c, d \in \mathbb{Z}, c > 0 \right\}, \text{ where } i = \sqrt{-1}, k \in \mathbb{Z} \text{ and } d = \frac{a^2 + k^2}{c}.$$

$$\mathbb{Q}(ki) = \left\{ \frac{a + ki}{c} : a, c, d \in \mathbb{Z}, c \neq 0 \right\}.$$

$$\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}, \text{ where } n \text{ is a square-free positive integer.}$$

$$\mathbb{Q}(\sqrt{-n}) = \{a + b\sqrt{-n} : a, b \in \mathbb{Q}\}.$$

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \{a_0 + a_1\sqrt{m} + a_2\sqrt{n} + a_3\sqrt{mn} : a_0, a_1, a_2, a_3 \in \mathbb{Q}\}, \text{ where } m \text{ and } n \text{ are two distinct square-free integers.}$$

$$\mathbb{Q}(i, \sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}(i)\}.$$

$$S_3 = \langle A, D : A^3 = D^2 = (AD)^2 = 1 \rangle \text{ is a symmetric group of degree 3.}$$

$$A_4 = \langle A, C : A^3 = C^3 = (AC)^2 = 1 \rangle \text{ is an alternating group of degree 4.}$$

$$D_2 = \langle B, D : B^2 = D^2 = (BD)^2 = 1 \rangle \text{ is a dihedral group of order 4.}$$

$$\mathbb{Z}_n \text{ is a cyclic group of order } n \text{ having binary operation addition mod } n.$$

Abstract

We have investigated properties of Picard group $\Gamma = \langle A, B, C, D : A^3 = B^2 = C^3 = D^2 = (AC)^2 = (AD)^2 = (BC)^2 = (BD)^2 = 1 \rangle$ by looking at its action on suitable spaces, where A, B, C and D are linear fractional transformations defined by $A(z) = \frac{1}{z-i}$, $B(z) = \frac{1}{z}$, $C(z) = \frac{1+z}{-z}$ and $D(z) = \frac{-1}{z}$. The aim of this research has been to study actions of Γ on the quadratic, biquadratic and finite fields by using diagrams.

We have found out that $\mathbb{Q}(i)$ is the smallest infinite and the only quadratic field on which Γ acts. The one point extension of $\mathbb{Q}(i)$ is $\mathbb{Q}(i, \sqrt{n})$, where n is a square-free positive integer, on which Γ acts. Among the biquadratic fields $\mathbb{Q}(i, \sqrt{n})$, the field $\mathbb{Q}(i, \sqrt{3})$ is the only one which contains all the fixed points of generators of Γ . So, action of Γ on $\mathbb{Q}(i, \sqrt{3})$ must be unique and interesting.

We have defined coset diagrams for the Picard group and have used them to study actions of Γ on the above fields. We have shown that the coset diagram for the action of Γ on $\mathbb{Q}(i)$ is connected and the action of Γ on $\mathbb{Q}(i)$ is transitive. We have shown also that action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is intransitive.

We have proved that if α is an ambiguous number in $\mathbb{Q}(i, \sqrt{3})$ then the ambiguous numbers form a closed path in the coset diagram for the orbit $\Gamma\alpha$ and it is the only closed path of ambiguous numbers contained in it.

Next we have investigated types of the closed path formed by ambiguous numbers and shown that there is only one type in the coset diagram for the action of Γ on

$\mathbb{Q}(i, \sqrt{3})$, that is, $(n_1, \dots, n_k, n_k, \dots, n_1)$ unlike in the case of coset diagrams for the action of the modular group on real quadratic irrational numbers. We have also found a condition under which the above closed path exists in the coset diagram for the action of Γ on $PL(F_p)$, where p is a Pythagorean prime.

Contents

Preface	1
Chapter one	
Definitions and Basic Concepts	6
Chapter two	
Action of Γ on Imaginary Quadratic Fields	32
Chapter three	
Action of Γ on Biquadratic Fields	56
Chapter four	
Closed paths of Ambiguous Numbers	94
Bibliography	118

Preface

A portion of infinite group theory, especially combinatorial group theory, is tied to subgroups of projective general linear group $PGL(2, \mathbb{C})$, where \mathbb{C} is the field of complex numbers. One of its subgroups is the projective special linear group $PSL(2, \mathbb{C})$. The survey article by W. Magnus [21] has given a broad overview of the use of $PSL(2, \mathbb{C})$ in combinatorial group theory. There are several methods to generate interesting subgroups of $PSL(2, \mathbb{C})$. One of the methods is to consider subgroups $PSL(2, A)$, where A is a ring of algebraic integers in \mathbb{C} . The foremost example is the modular group $M = PSL(2, \mathbb{Z})$, the group of linear fractional transformations with integer entries and determinant equal to one. In 1890's, L. Bianchi and others (see [20]) have initiated the study of Bianchi groups $\Gamma_d = PSL(2, O_d)$, as a natural extension of the study of the modular group, where d is a positive square-free integer and O_d is the ring of algebraic integers in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$. These groups have attracted a great deal of attention both for their intrinsic interest as discrete groups and for their applications in hyperbolic geometry, topology and number theory.

The group Γ_1 , that is, $PSL(2, O_1)$, where O_1 is the ring of Gaussian integers, has been studied independently. It was first introduced by E. Picard and has been named the Picard group [17]. We have denoted the Picard group by Γ for our convenience.

Picard group Γ is $PSL(2, \mathbb{Z}[i])$. The group Γ is an important subgroup of $PSL(2, \mathbb{C})$. It is an example of the fact that the discreteness on $\mathbb{C} \cup \{\infty\}$ does not imply the

discontinuity. Its action on $\mathbb{C} \cup \{\infty\}$ is not discontinuous, whereas its action on $H^3 = \{z + tj : z \in \mathbb{C}, t > 0\}$ is discontinuous [2].

The presentation for Γ is

$$\langle A, B, C, D : A^3 = B^2 = C^3 = D^2 = (AC)^2 = (AD)^2 = (BC)^2 = (BD)^2 = 1 \rangle,$$

where A, B, C and D are linear fractional transformations defined by $A(z) = \frac{1}{z-i}$, $B(z) = \frac{1}{z}$, $C(z) = \frac{1+z}{-z}$ and $D(z) = \frac{-1}{z}$. In form of matrices, these linear fractional transformations can be written as

$$A = \begin{bmatrix} 0 & i \\ i & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, C = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, \text{ and } D = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Now let

$$G_1 = \langle A, C, D : A^3 = C^3 = D^2 = (AC)^2 = (AD)^2 = 1 \rangle,$$

$$G_2 = \langle B, C, D : B^2 = C^3 = D^2 = (BC)^2 = (BD)^2 = 1 \rangle, \text{ and}$$

$$M = \langle C, D : C^3 = D^2 = 1 \rangle.$$

We can decompose Γ as a free product of G_1 and G_2 with M amalgamated, that is,

$$\Gamma = G_1 \underset{M}{*} G_2.$$

This thesis is comprised of four chapters. The aim of chapter one is to provide background material for succeeding work. We have given an introduction of quadratic fields, biquadratic fields, linear groups, Picard group and coset diagrams. We have

defined coset diagrams for the Picard group Γ , and have described the fragment of the coset diagram for the action of Γ on $\mathbb{Q}(i) \cup \{\infty\}$.

In chapter two, we have shown that Γ acts on infinite fields like $\mathbb{Q}(i)$ and $\mathbb{Q}(i, \sqrt{n})$, where n is a square-free positive integer. The smallest extension of \mathbb{Q} on which Γ acts is $\mathbb{Q}(i)$. We have shown that action of Γ on $\mathbb{Q}(i)$ is transitive but actions of its component groups G_1, G_2 and amalgamated group M are intransitive.

In chapter three, we have explored some interesting group theoretic properties of action of Γ on $\mathbb{Q}(i, \sqrt{3})$. Fixed points of a linear fractional transformation g are those x in \mathbb{C} which satisfy $g(x) = x$, if this is so, we say that g fixes x . The fixed points of generators A, B, C and D of Γ are $\frac{i \pm \sqrt{3}}{2}, \pm 1, \frac{-1 \pm \sqrt{3}i}{2}$ and $\pm i$ respectively. They all lie in a biquadratic field $\mathbb{Q}(i, \sqrt{3})$. So, it is interesting to study closed paths in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$. This is the reason why we have studied it independently from other biquadratic fields $\mathbb{Q}(i, \sqrt{n})$, where n is a positive square-free integer. The algebraic integers of $\mathbb{Q}(i, \sqrt{3})$ are $\frac{1}{2}((a + bi) + (c + di)\sqrt{3})$, where $a \equiv d \pmod{2}$, $b \equiv c \pmod{2}$ and $a, b, c, d \in \mathbb{Z}$ [36]. We have studied algebraic integers in $\mathbb{Q}(i, \sqrt{3})$ and used them to prove that the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is intransitive.

Coset diagrams for the orbit of Γ on biquadratic field $\mathbb{Q}(i, \sqrt{3})$ give some interesting information. The action of Γ on $\mathbb{Q}(i, \sqrt{3})$ shows that some elements of $\mathbb{Q}(i, \sqrt{3})$ of the form $\frac{a + b\sqrt{3}}{c}$ have a pattern; so they need to be classified. The conjugate of $\alpha = \frac{a + b\sqrt{3}}{c}$ is $\bar{\alpha} = \frac{a - b\sqrt{3}}{c}$. A real quadratic irrational number

$\alpha = \frac{a + b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$ is called totally positive (negative) if α and $\bar{\alpha}$ are both positive (negative). When α and $\bar{\alpha}$ have opposite signs, then they are called ambiguous numbers. We have noticed that ambiguous numbers in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ form a unique pattern, so they deserve special attention. We have shown that there is a finite number of ambiguous numbers in an orbit $\Gamma\alpha$, where α is an ambiguous number, and they form a closed path and it is the only closed path in the orbit $\Gamma\alpha$. In this way we have classified all the ambiguous numbers in the orbit.

The ring \mathbb{Z} of integers induces a natural ring structure on $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, the integers modulo n ; if n is prime p , then \mathbb{Z}_p is a field under this structure, also denoted as F_p . The projective line over finite field is denoted by $PL(F_p) = F_p \cup \{\infty\}$.

In chapter four, we have found certain types of closed paths formed by ambiguous numbers in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ and the linear fractional transformation which the closed path induces. Also a condition for a closed path to contain $\alpha = \frac{a + b\sqrt{3}}{c}$ with $\bar{\alpha}$, α with $\frac{1}{\alpha}$ and α with $\frac{1}{\bar{\alpha}}$ is established, where $a, b, c \in \mathbb{Z}$. We have found a condition under which a homomorphic image of the closed path of ambiguous numbers of the form $\frac{a + b\sqrt{3}}{c}$ exist in the coset diagram for the action of Γ on $PL(F_p)$. An element $\alpha = \frac{1}{2}((a + bi) + (c + di)\sqrt{3})$ in $\mathbb{Q}(i, \sqrt{3})$ corresponds to $\left(\frac{1}{2}(a + bm) + (c + dm)n\right) \bmod p$ in F_p , under the homomorphism from $\mathbb{Q}(i, \sqrt{3}) \cup \{\infty\}$ to $PL(F_p)$, where $m^2 \equiv -1 \pmod{p}$ and $n^2 \equiv 3 \pmod{p}$.

Four papers containing results from chapters two, three and four have been sub-

mitted for publication in international journals. Complete information about these is given as below.

1. Q. Mushtaq and S. Anis, Actions of Picard group.
2. Q. Mushtaq and S. Anis, Pattern in coset diagram for the Picard group when acting on biquadratic space $\mathbb{Q}(i, \sqrt{3}) \cup \{\infty\}$.
3. Q. Mushtaq and S. Anis, Ambiguous numbers in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$.
4. Q. Mushtaq and S. Anis, Closed paths of ambiguous numbers in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$.

Chapter 1

Definitions and Basic Concepts

The aim of this chapter is to introduce the concepts, background material, and objectives of this thesis. We have given a brief introduction of quadratic fields, bi-quadratic fields, linear groups and a Picard group. We have described coset diagrams, their brief history and examples. We have also defined coset diagrams for the Picard group. We have included here only those definitions which are relevant to the research work embodied in this thesis.

1.1 Definitions

Let G be a group and X be a non-empty set. By an action of G on X we mean a function $\mu : G \times X \rightarrow X$ such that for all x in X and g, h in G the following axioms are satisfied [3].

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

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

We can write x^g instead of $\mu(g, x)$. For example G acts on itself by conjugation, that is, $x^g = g^{-1}xg$ for each $x, g \in G$.

Let G be a group acting on a set X . Then $\{x^g : g \in G\}$ is called an orbit of x in G for $x \in X$, we denote it by Gx and X is called a G -set or a G -space. Also G acts on X transitively if $X \neq \phi$ and for any $x, y \in X$ there exists $g \in G$ such that $x^g = y$. If a G -space has one orbit, then the action of G on X is called transitive.

Let $A = \langle a_1, \dots : R_1, \dots \rangle$ and $B = \langle b_1, \dots : S_1, \dots \rangle$ be two groups with $H < A, K < B$ and $\phi : H \rightarrow K$ be an isomorphism. Then the free product of A and B , amalgamating H to K , is the group G with presentation

$$G = \langle a_1, \dots, b_1, \dots : R_1, \dots, S_1, \dots, H = \phi(H) \rangle,$$

that is, the group G has generators as the union of the generators of A and B and has relations as the union of the relations of A and B together with an additional set of relations giving the subgroup isomorphism. Identifying H with its isomorphic image, G is called the free product of A and B with H amalgamated, denoted as $G = A *_H B$. Here A and B are called the components of G . If $H = \{1\}$, then G is called the free product of A and B [17].

An integer a is called square-free if it can be written as a product of distinct primes $a = p_1 p_2 \dots p_r$.

A group G is called torsion-free if every element of G except the identity is of infinite order.

A Fuchsian group is a discontinuous subgroup of $PSL(2, \mathbb{C})$ which leaves invariant a disc.

1.2 Quadratic Fields

A quadratic field is of the form $\mathbb{Q}(\xi)$, where ξ is a zero of an irreducible quadratic polynomial over \mathbb{Q} . The elements of such a field are of the form $a_0 + a_1\xi$, where a_0 and a_1 are rational numbers. If ξ is of the form $(a + b\sqrt{m})/c$ where $a, b, c \neq 0$ are integers and m is a square-free integer, then $\mathbb{Q}(\xi) = \mathbb{Q}\left(\frac{a + b\sqrt{m}}{c}\right) = \mathbb{Q}(a + b\sqrt{m}) = \mathbb{Q}(b\sqrt{m}) = \mathbb{Q}(\sqrt{m})$. These fields have degree 2 over \mathbb{Q} , with basis $\{1, \sqrt{m}\}$. If m and n are two different square-free rational integers, then $\mathbb{Q}(\sqrt{m}) \neq \mathbb{Q}(\sqrt{n})$ because \sqrt{m} does not belong to $\mathbb{Q}(\sqrt{n})$.

A complex number ξ is called an algebraic number if it satisfies some polynomial equation $f(x) = 0$, where $f(x)$ is a polynomial over \mathbb{Q} . An algebraic number ξ is called an algebraic integer if it satisfies some monic polynomial equation $f(x) = x^n + b_1x^{n-1} + \cdots + b_n = 0$ with integral coefficients. The set of all algebraic numbers forms a field and the class of all algebraic integers forms a ring. The algebraic integers of rational numbers form \mathbb{Z} and algebraic integers of $\mathbb{Q}(i)$ form $\mathbb{Z}[i]$.

Theorem 1 *[[32], Theorem 9.20] Every quadratic field is of the form $\mathbb{Q}(\sqrt{m})$, where*

m is a square-free rational integer, positive or negative but not equal to 1. Numbers of the form $a + b\sqrt{m}$ with rational integers a and b are algebraic integers of $\mathbb{Q}(\sqrt{m})$. These are the only integers of $\mathbb{Q}(\sqrt{m})$ if $m \equiv 2$ or $3 \pmod{4}$. If $m \equiv 1 \pmod{4}$, the numbers $(a + b\sqrt{m})/2$, with odd rational integers a and b , are also algebraic integers of $\mathbb{Q}(\sqrt{m})$, and there are no further integers.

A quadratic field $\mathbb{Q}(\sqrt{m})$ is called imaginary if $m < 0$, and it is called real if $m > 1$. An element α in $\mathbb{Q}(\sqrt{m})$ is called unit, if it is a divisor of the integer 1. An imaginary quadratic field has only a finite number of units; in fact ± 1 are the only units in these fields except for the case $\mathbb{Q}(i)$ where the units are ± 1 and $\pm i$, and for the case $\mathbb{Q}(\sqrt{-3})$ where the units are ± 1 and $(\pm 1 \pm \sqrt{-3})/2$. On the other hand, as it is well known that every real quadratic field has infinitely many units.

A real quadratic irrational number α of the form $(a + b\sqrt{m})/c$ where $a, b, c \in \mathbb{Z}$ and its conjugate $\bar{\alpha} = (a - b\sqrt{m})/c$ may have different signs. If such is the case, then α is called an ambiguous number, for example, $(1 + \sqrt{3})/2$ is an ambiguous number. A real quadratic irrational number $\alpha = (a + b\sqrt{m})/c$, where $a, b, c \in \mathbb{Z}$, is called totally positive (negative) if α and $\bar{\alpha}$ are both positive (negative), for example, $(2 + \sqrt{3})/2$ is totally positive while $(-2 + \sqrt{3})/2$ is totally negative real quadratic number.

1.3 Biquadratic Fields

If m and n are two distinct square-free rational integers, then the field formed by adjoining \sqrt{m} and \sqrt{n} to \mathbb{Q} is denoted by $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ and is called a biquadratic field over \mathbb{Q} , where \sqrt{m} and \sqrt{n} are zeros of an irreducible quartic polynomial over \mathbb{Q} . The elements of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ are of the form $a_0 + a_1\sqrt{m} + a_2\sqrt{n} + a_3\sqrt{mn}$, where $a_0, a_1, a_2, a_3 \in \mathbb{Q}$. Any element of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ which satisfies a monic equation of degree ≥ 1 with rational integral coefficients is called an algebraic integer of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$. In [36], the explicit form of the algebraic integers, an integral basis and the discriminant of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is given. These fields have degree 4 over \mathbb{Q} . Some of the subfields of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ are $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{mn})$. The author supposed that l is the greatest common divisor of m and n , that is, $l = (m, n)$, so that $m = lm_1$, $n = ln_1$ and $(m_1, n_1) = 1$.

Theorem 2 [[36], Theorem 1] *Letting a, b, c, d denote rational integers, the algebraic integers of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ are given as follows:*

(i) *if $(m, n) \equiv (m_1, n_1) \equiv (1, 1) \pmod{4}$, then the algebraic integers are*

$$\frac{1}{4}(a + b\sqrt{m} + c\sqrt{n} + d\sqrt{m_1n_1}), \text{ where } a \equiv b \equiv c \equiv d \pmod{2}, a - b + c - d \equiv$$

$0 \pmod{4}$;

(ii) *if $(m, n) \equiv (1, 1)$, $(m_1, n_1) \equiv (3, 3) \pmod{4}$, then the algebraic integers are*

$$\frac{1}{4}(a + b\sqrt{m} + c\sqrt{n} + d\sqrt{m_1n_1}), \text{ where } a \equiv b \equiv c \equiv d \pmod{2}, a - b - c - d \equiv$$

$0 \pmod{4}$;

- (iii) if $(m, n) \equiv (1, 2) \pmod{4}$, then the algebraic integers are $\frac{1}{2}(a + b\sqrt{m} + c\sqrt{n} + d\sqrt{m_1n_1})$, where $a \equiv b, c \equiv d \pmod{2}$;
- (iv) if $(m, n) \equiv (2, 3) \pmod{4}$, then the algebraic integers are $\frac{1}{2}(a + b\sqrt{m} + c\sqrt{n} + d\sqrt{m_1n_1})$, where $a \equiv c \equiv 0, b \equiv d \pmod{2}$;
- (v) if $(m, n) \equiv (3, 3) \pmod{4}$, then the algebraic integers are $\frac{1}{2}(a + b\sqrt{m} + c\sqrt{n} + d\sqrt{m_1n_1})$, where $a \equiv d, b \equiv c \pmod{2}$.

Example 3 Let $m = 2$ and $n = -1$, then $\mathbb{Q}(\sqrt{2}, i)$ is a biquadratic field which has degree 4 over \mathbb{Q} . The monic polynomial $x^4 - x^2 - 2$ is irreducible in \mathbb{Q} , and $\sqrt{2}$ and i are zeros of this polynomial. The numbers of this field are $a_0 + a_1\sqrt{2} + a_2i + a_3\sqrt{2}i$, where $a_0, a_1, a_2, a_3 \in \mathbb{Q}$, and algebraic integers of the field are $a + b\sqrt{2} + ci + di\sqrt{2}$, where a and c are integers, b and d are either both integers or both halves of odd integers [18].

1.4 Linear Groups

The linear fractional groups for different fields arose independently. The linear fractional groups and its subgroup with square determinants for the field \mathbb{Z}_p were studied by E. Galois in 1832. The homomorphism of $GL(2, F)$ to the linear fractional group is implied in his work. In 1847, the linear fractional group for the field of real numbers appeared in the work of V. Staudt 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 [7].

In 1852, the linear fractional group for the field of complex numbers was studied synthetically by A. F. Möbius. After E. Galois, the homomorphism of $GL(2, F)$ to the linear fractional group is also implied in the work of J. A. Serret in 1866, and was used by A. Cayley in 1880 to determine properties of linear fractional transformations. In 1893, the linear fractional group for arbitrary finite fields was studied by E. H. Moore who established the simplicity of $PSL(2, F)$ for fields of order greater than 3 [7].

The class of non-singular 2×2 complex matrices is a general linear group with respect to the usual matrix multiplication and is denoted by $GL(2, \mathbb{C})$. Its subgroup, $SL(2, \mathbb{C})$, the special linear group, consists of those matrices with determinants 1. The set $Z = \{aI : a \in \mathbb{C}\}$, where I is 2×2 identity matrix, is a normal subgroup of $GL(2, \mathbb{C})$. The projective general linear group is defined by $PGL(2, \mathbb{C}) = GL(2, \mathbb{C})/Z$, and the projective special linear group is defined as $PSL(2, \mathbb{C}) = SL(2, \mathbb{C})/SL(2, \mathbb{C}) \cap Z$.

Any 2×2 complex matrix A in $GL(2, \mathbb{C})$ induces the Möbius transformation g_A of the extended complex plane onto itself by the formula $A \rightarrow g_A$, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $g_A(z) = \frac{az + b}{cz + d}$. The class \mathcal{M} of Möbius transformations is a group under the usual composition of functions. We denote the map $A \rightarrow g_A$ by Φ . An elementary computation shows that Φ is a homomorphism. The kernel K of Φ is $\{aI : a \neq 0\}$. In particular, \mathcal{M} is isomorphic to $GL(2, \mathbb{C})/K = PGL(2, \mathbb{C})$. The kernel of the

restriction of Φ to $SL(2, \mathbb{C})$ is $K \cap SL(2, \mathbb{C}) = \{I, -I\}$ and each g_A in \mathcal{M} is therefore the projection of exactly two matrices, say A and $-A$, in $SL(2, \mathbb{C})$. We deduce that \mathcal{M} is isomorphic to $SL(2, \mathbb{C}) / \{I, -I\} = PSL(2, \mathbb{C})$, see [2].

Thus the *projective general linear group* $PGL(2, \mathbb{C})$ is the group of linear fractional transformations $T(z) = \frac{az + b}{cz + d}$ with $ad - bc \neq 0$ and $a, b, c, d \in \mathbb{C}$ and the *projective special linear group* $PSL(2, \mathbb{C})$ is the group of linear fractional transformations $T(z) = \frac{az + b}{cz + d}$ with $ad - bc = 1$ and $a, b, c, d \in \mathbb{C}$, is a normal subgroup of $PGL(2, \mathbb{C})$.

The $GL(2, \mathbb{C})$ is both a group and a topological space, that is, a topological group with respect to the metric $\|X - Y\|$, where $\|X - Y\| = [|a - \alpha|^2 + |b - \beta|^2 + |c - \gamma|^2 + |d - \delta|^2]^{1/2}$ for $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $Y = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. A subgroup G of $GL(2, \mathbb{C})$ is discrete if and only if the subspace topology on G is the discrete topology. For instance, the Modular group, is the subgroup of $SL(2, \mathbb{C})$ consisting of all matrices A with a, b, c and d integers, is discrete. More generally, the Picard group, consisting of all matrices A in $SL(2, \mathbb{C})$ with a, b, c and d Gaussian integers, is discrete [2].

Let X be a topological space and G be a group of homeomorphisms of X onto itself. We say that G acts discontinuously on X if and only if for every compact subset K of X , $g(K) \cap K = \emptyset$, except for a finite number of g in G .

Let $H^3 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_3 > 0\}$ be the upper half space equipped with the hyperbolic metric $ds^2 = \frac{dx_1^2 + dx_2^2 + dx_3^2}{x_3^2}$ of constant curvature -1 . In terms of quaternions \mathbb{H} , $H^3 = \{z \in \mathbb{H} : z = x_1 + x_2i + x_3j, x_3 > 0\}$. The relationship between discreteness and discontinuity as applied to subgroups of \mathcal{M} is stated in the following

Theorem,

Theorem 4 [[2], Theorem 5.3.2] *A subgroup G of \mathcal{M} is discrete if and only if it acts discontinuously in H^3 .*

Of course, Theorem 4 shows that if G acts discontinuously in some non-empty open subset of $\mathbb{C} \cup \{\infty\}$, then G is discrete. The converse is false: it is possible for G to be discrete yet not act discontinuously in any open subset of $\mathbb{C} \cup \{\infty\}$. Picard group is an example of this fact. Although its action on $\mathbb{C} \cup \{\infty\}$ is not discontinuous, its action on H^3 is discontinuous [2].

1.5 Picard Group

Picard group Γ is $PSL(2, \mathbb{Z}[i])$ or $PSL(2, O_1)$, where O_1 is the ring of Gaussian integers. Specifically, it is the group of linear fractional transformations $T(z) = \frac{az + b}{cz + d}$ with $ad - bc = 1$ and $a, b, c, d \in \mathbb{Z}[i]$.

Γ belongs to the class of Bianchi groups $\Gamma_d = PSL(2, O_d)$, where d is a positive square-free integer and O_d is the ring of algebraic integers in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$. Bianchi groups are the subgroups of $PSL(2, \mathbb{C})$. These groups have attracted a great deal of attention both for their intrinsic interest as discrete groups and also for their applications in hyperbolic geometry, topology and number theory. The study of this class of groups was initiated in the 1890's by Bianchi and others [20] as a natural extension of the study of the modular group $PSL(2, \mathbb{Z})$. The

rings O_d are all discretely normed and for $d = 1, 2, 3, 7, 11$, O_d have a Euclidean algorithm. Thus they are similar to the ring of rational integers \mathbb{Z} .

The group Γ was first introduced by E. Picard and has been named the Picard group [17]. E. Picard derived both generators for Γ as well as fundamental domain in H^3 . R. Fricke and F. Klein have dealt with the importance of Γ in the study of binary quadratic forms with Gaussian integer coefficients. They also found a presentation for Γ based on a fundamental region. Let (X, d) be a metric space and let G be a non-trivial group of isometries of X . A subset R of X is said to be a fundamental region for the group G if the set R of X is open in X , the members of $\{gR : g \in G\}$ are mutually disjoint, and $X = \cup\{g\bar{R} : g \in G\}$. A fundamental domain is a connected fundamental region.

With respect to group specific properties, Γ has been the most studied of the Bianchi groups. Real interest in the Picard group and the Bianchi groups in general began about 1970 as a consequence of two results of J. P. Serre. His first result which is covered in detail in [17] is that the Bianchi groups do not satisfy the congruence subgroup property. This contrasts with the fact (proved by Serre) that for all number fields K other than \mathbb{Q} and imaginary quadratics, the group $SL(2, R)$ (where R is the ring of integers of K) does satisfy the congruence subgroup property. Secondly, one attempts to express Γ_d as a free product with amalgamation. It turns out that this is possible in all cases except Γ_3 . A method for finding presentation of $SL(2, O_d)$ in the Euclidean case was found by P. M. Cohn [11]. Using his method the following

presentation for Γ was derived in [17].

$$\Gamma = \langle a, l, t, u : a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (at)^3 = (ual)^3 = [t, u] = 1 \rangle,$$

where $a(z) = \frac{-1}{z}$, $t(z) = z + 1$, $u(z) = z + i$, and $l(z) = izi$.

In [17], this presentation is obtained by finding a fundamental domain for Γ . The translation subgroup is generated by $t : z \mapsto z + 1$ and $u : z \mapsto z + i$. This together with the transformation $l : z \mapsto -z$ is the stabilizer of ∞ . The fundamental domain for Γ is $\{z = x + yi + rj \in H^3 : |x| \leq \frac{1}{2}, 0 \leq y \leq \frac{1}{2} \text{ and } (x^2 + y^2 + r^2)^{\frac{1}{2}} \geq 1\}$. The fundamental domain of Picard group is shown in figure below.

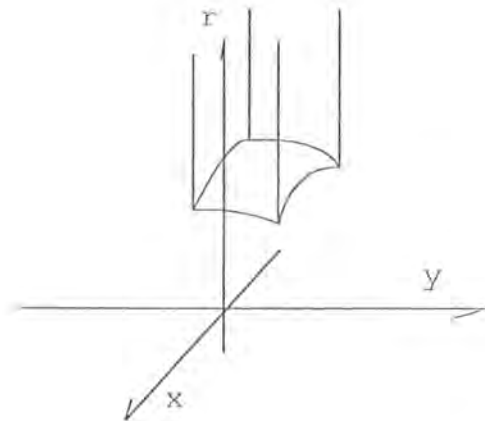


Figure 1

A convex polyhedron in a metric space X is a non-empty closed, convex subset of X with finitely many sides and a non-empty interior. A tessellation of X is a collection \mathcal{P} of convex polyhedra in X such that the interiors of the polyhedra in \mathcal{P} are mutually disjoint, and the union of the polyhedra in \mathcal{P} is equal to X . When

Γ acts on its fundamental domain, its transformed copies cover the entire space of H^3 without overlapping except at the boundaries, in other words the fundamental domain of Γ tessellates H^3 .

In [17], letting $A = lau^{-1}$, $B = al$, $C^{-1} = al$ and $D = a$ and applying Tietze transformations this presentation for Γ can be rewritten as

$$\langle A, B, C, D : A^3 = B^2 = C^3 = D^2 = (AC)^2 = (AD)^2 = (BC)^2 = (BD)^2 = 1 \rangle,$$

where A, B, C and D are linear fractional transformations defined by $A(z) = \frac{1}{z-i}$, $B(z) = \frac{1}{z}$, $C(z) = \frac{1+z}{-z}$ and $D(z) = \frac{-1}{z}$. This is a modification of a presentation derived by Sansone [34], using the original geometric method of L. Bianchi. With the usual convention for matrices, a faithful representation is given with

$$A = \begin{bmatrix} 0 & i \\ i & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, C = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, \text{ and } D = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

A. M. Brunner in [6], derived a 2-generator 5-relator presentation for Γ in 1992, that is,

$$\langle a, w, b : b = aw^2a^{-1}w^{-2}aw^2, (a^2waw^{-1})^2 = (awaw^{-1})^3 = (wb)^2 = (ab)^2 = b^2 = 1 \rangle,$$

where $a = AB$ and $w = DBC$.

It is worth mentioning that Γ contains the well known modular group M as a proper subgroup. The transformations C and D generate M and its finite presentation is $\langle C, D : C^3 = D^2 = 1 \rangle$.

Now let

$$G_1 = \langle A, C, D : A^3 = C^3 = D^2 = (AC)^2 = (AD)^2 = 1 \rangle,$$

$$G_2 = \langle B, C, D : B^2 = C^3 = D^2 = (BC)^2 = (BD)^2 = 1 \rangle.$$

The group Γ has decomposition as a free product of G_1 and G_2 with M amalgamated, that is,

$$\Gamma = G_1 *_M G_2.$$

Further, the subgroup G_1 has decomposition as $G_1 = G_{11} *_M G_{12}$, where

$$G_{11} = \langle A, C : A^3 = C^3 = (AC)^2 = 1 \rangle = A_4,$$

$$G_{12} = \langle A, D : A^3 = D^2 = (AD)^2 = 1 \rangle = S_3,$$

and $G_2 = G_{21} *_M G_{22}$, where

$$G_{21} = \langle B, C : B^2 = C^3 = (BC)^2 = 1 \rangle = S_3,$$

$$G_{22} = \langle B, D : B^2 = D^2 = (BD)^2 = 1 \rangle = D_2,$$

and as it is well known that S_3 is a symmetric group of degree 3, A_4 an alternating group of degree 4 and D_2 a dihedral group of order 4.

The amalgam decomposition of Γ can be written as

$$\Gamma = (A_4 *_M S_3) *_M (S_3 *_M D_2),$$

expressible also as a quadrangular product, where each vertex corresponds to a group G_v , each edge y corresponds to a group G_y and adjacent vertices are amalgamated via

relations along the edges. The group Γ is, then the group formed by the free product of G_v modulo the edge relations.

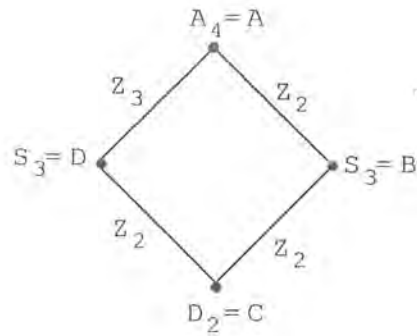


Figure 2

The fact that the components in the amalgam decomposition for Γ are finite, forces a free-like structure on the torsion-free subgroups. Although the torsion-free subgroups have the free-like structure there can be no free subgroups of finite index in Γ . It can be stated in the following theorem.

Theorem 5 *[17], Theorem 5.2.5] Γ contains no free subgroups of finite index. Every subgroup of finite index contains a free abelian subgroup of rank 2.*

Since finite subgroups of Γ must be conjugate to finite subgroups in the components, it follows that the possible finite subgroups of Γ are $\mathbb{Z}_2, \mathbb{Z}_3, D_2, S_3$ and A_4 . This argument proves the following theorem.

Theorem 6 *[17], Theorem 5.2.6] Suppose $G \subset \Gamma$ and G is torsion-free. If $|\Gamma : G| < \infty$ then $|\Gamma : G| = 12n$ for some n .*

In [5] A. M. Brunner, M. L. Frame, Y. W. Lee and N. J. Wielenberg have developed a theoretical method which explains how to completely classify, up to isomorphism, all torsion-free subgroups of Γ of a given finite index n . They have used the results of A. Karrass, A. Piecrowski, and D. Solitar on subgroups and have produced torsion-free subgroups. They carried out the computations for classifying up to isomorphism all torsion-free subgroups of Γ of indices 12 and 24. The summary of their result is as follows.

Theorem 7 [[17], Theorem 5.2.7] *Up to isomorphism there are two torsion-free subgroups of index 12 and seventeen torsion-free subgroups of index 24. Of these seventeen there is only one normal subgroup up to isomorphism.*

Modular group M plays a very important role to determine subgroups of Γ because of decomposition of Γ . M is a Fuchsian subgroup of Γ , and is not normal. The normal closure of M in Γ is $N(D, C) = M_1 *_M M_2$, where $M_1 \cong M_2 \cong S_3 *_Z A_4$. Further, the index of $N(D, C)$ in Γ is two [33]. In [16], it is proved that there are exactly three normal subgroups of index 2 in Γ . So $N(D, C)$ is one of these normal subgroups. In [15], and [16], some properties of the normal subgroups of Γ are determined and a complete classification of the normal subgroups for indices less than 60 is given. In [37], the normalizer of M in Γ , that is, a maximal subgroup of Γ in which M is normal, is obtained.

1.6 Coset Diagrams

A graph G is a finite non-empty set of objects called vertices (the singular is vertex) together with a (possibly empty) set of unordered pairs of distinct vertices of G called edges. The vertex set is denoted by $V(G)$, while the edge set is denoted by $E(G)$.

A coset diagram is a directed graph whose vertices are the (right) cosets of a subgroup of finite index in a finitely generated group. The vertices representing cosets g and h (say), are joined by an s_i -edge, of "colour i " directed from vertex g to vertex h , whenever $gs_i = h$, where s_i is generator of the group. It may well happen that $gs_i = g$, in which case the g -vertex is joined to itself by an s_i -loop.

The method of representing group actions by graphs has a long and rich history. The first paper in which graphs were used explicitly was by A. Cayley [10] in 1878. He represented the multiplication table of a group with given generators by graph, and proposed the use of colours to distinguish the edges of the graphs associated with different generators. The Cayley's diagram for a given group is a graph whose vertices represent the elements of the group, which are the cosets of the trivial subgroup and edges represent generators of the group. In 1893, A. Hurwitz [9, 14] used graphs to represent groups. Then in 1896, H. Maschke [22] used Cayley's colour graphs to prove some important results on the representation of finite groups, especially on the rotation groups of the regular bodies in three and four dimensional spaces.

The Cayley's graphs were rediscovered by M. Dehn, in 1910. For this reason, some

authors call it as the Dehnzch Gruppenbild. But Cayley's priority is indisputable, as he described graphs much earlier [14]. O. Schreier generalized this notion by considering a graph whose vertices represent the cosets of any subgroup.

Later, mathematicians like J. H. C. Whitehead [35], H. S. M. Coxeter and W. O. J. Moser [14], W. Burnside [8], etc., contributed seminal papers containing graphical representations of groups. In 1965, H. S. M. Coxeter and W. O. J. Moser [14] used both Cayley and Schreier diagrams to prove some results on finitely generated groups.

About 1978, G. Higman propounded the idea of coset diagrams for the modular group. M. D. E. Conder [12, 13] and Q. Mushtaq [1, 19, 23 – 31] in their separate works have used these diagrams to solve certain "identification problems". In G. Higman's words¹, "Q. Mushtaq laid the foundation of the theory of coset diagrams for the modular group". One of the examples on uses of coset diagrams is in [1].

In a coset diagram the vertices are identifiable with the right cosets in a permutation group G , of the stabilizer H of any point of the set Ω , so that an edge of colour i joins the set Hg to the set Hgx_i , for each element g of G . This is very similar to the notion of a Schreier coset diagram whose vertices represent the cosets of any given subgroup in a finitely generated group, and also to that of a Cayley's graph whose vertices are the group elements themselves, with trivial stabilizer. These diagrams may be drawn for any finitely generated group acting on any arbitrary sets or spaces.

G. Higman introduced the coset diagrams for the modular group $PSL(2, \mathbb{Z})$, which

¹In a private letter of Professor G. Higman to Dr. Farhana Shaheen, (available with Professor Q. Mushtaq).

has a representation in terms of two generators x and y and the way they can be connected together. 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 anticlockwise, while the fixed points of x and y , if any, are denoted by heavy dots. Thus the geometry of the figure makes the distinction obvious between x -edges and y -edges.

For instance, consider the action of $PGL(2, \mathbb{Z})$ on $PL(F_{13})$, defined by $x(z) = \frac{-1}{z}$, $y(z) = \frac{z-1}{z}$ and $t(z) = \frac{1}{z}$, where $z \in PL(F_{13})$. Here t represents the vertical symmetry. We can calculate the permutation representations of x , y and t as follows:

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

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

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

The coset diagram for the action of $PGL(2, \mathbb{Z})$ on $PL(F_{13})$ is shown in Figure 3.

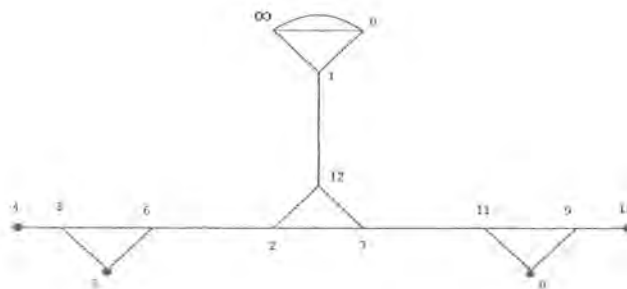


Figure 3

If $\pi = \{v_0, e_1, v_1, e_2, \dots, e_k, v_k\}$ is an alternating sequence of vertices and edges of a coset diagram, then π is a *path* in the diagram from v_0 to v_k , where e_i joins v_{i-1} and v_i for each i and $e_i \neq e_j (i \neq j)$. A *closed path* is one whose initial and terminal vertices coincide. A coset diagram is *connected* if any two vertices in the diagram are joined by a path. A *word* is an element of group expressed as a product of its generators and their inverses. A word in a group is a corresponding path in a coset diagram.

Every connected coset diagram for a finitely generated group G on a non-empty space corresponds to a transitive action of G on that space.

1.7 Coset Diagrams for the Picard Group

We have defined coset diagrams for the Picard group Γ . They need symbols for the generators as well as a method or pattern to join them. The group Γ consists of four generators, two of order 3 and two of order 2, so it is possible to avoid using colours. The generators A and C both have order 3, so the 3-cycles of A and C are represented by triangles. But to distinguish generator A from generator C , we have denoted the 3-cycles of the generator C by three unbroken edges of a triangle permuted anticlockwise. The 3-cycles of the generator A are denoted by three broken edges of a triangle permuted anticlockwise.

As generators B and D are involutions so we have represented them by edges and

orientation of edges can be avoided. To distinguish generator B from generator D , the 2-cycles of generator B have been represented by a bold edge and two vertices which are interchanged by D have been joined by an edge. Fixed points of A, B, C and D , if they exist, have been denoted by heavy dots.

The generators A and C together form a Cayley's diagram of $A_4 = \langle A, C : A^3 = C^3 = (AC)^2 = 1 \rangle$ as shown in the Figure 4.

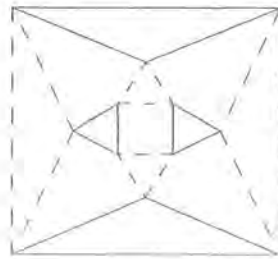


Figure 4

Two diagrams of A_4 have been joined by edges of generator D as shown in Figure 5.

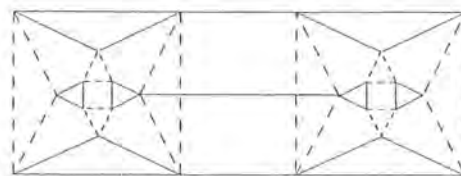


Figure 5

The edges have joined the 3 vertices of a triangle with broken edges of one diagram of A_4 to that of another diagram of A_4 . The generators A and D together have generated $S_3 = \langle A, D : A^3 = D^2 = (AD)^2 = 1 \rangle$, which is shown in the Figure 6 below.



Figure 6

A triangle having broken edges is common between the diagrams of A_4 and S_3 as shown in Figure 5. Algebraically, \mathbb{Z}_3 is an amalgam of A_4 and S_3 .

One diagram of A_4 can be joined to four other diagrams of A_4 by edges representing the generator D . By a fragment $A - C - D$, we mean the fragment of the coset diagram which consists of diagrams of A_4 and edges of D , that is, Figure 7, because this fragment of coset diagram is composed by the use of generators A, C , and D as shown in figure below.

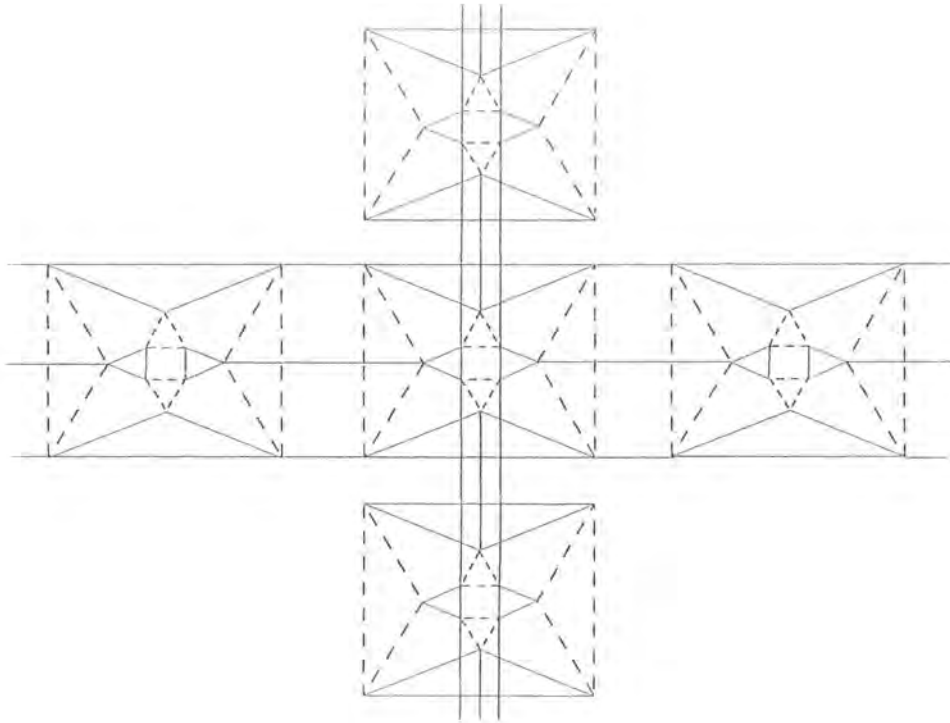


Figure 7

At a zero level we have one diagram of A_4 , and, then at the first level, we have joined 4 diagrams of A_4 by edges representing the generator D . At the second level we have joined $4 \times 3 = 12$ diagrams of A_4 and at the third level we have joined $4 \times 3^2 = 36$ diagrams of A_4 by edges. So at the l^{th} level we have joined $4 \times 3^{l-1}$ diagrams of A_4 by edges. If we denote the diagram of A_4 by a small square, then the diagram, up to the second level is given as follows.

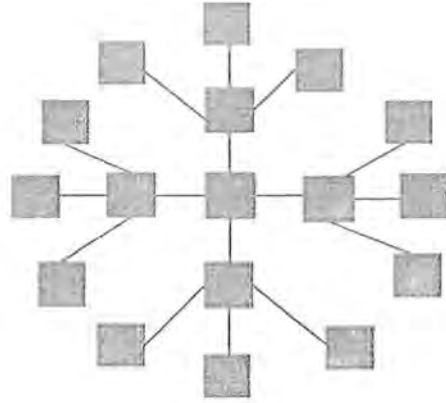


Figure 8

The two fragments $A - C - D$ have joined by bold edges representing the generator B as shown in Figure 9.

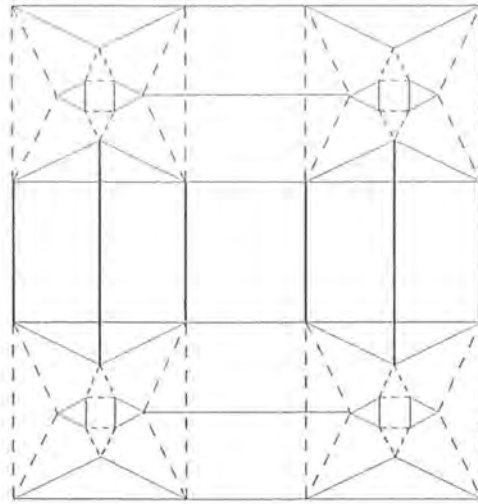


Figure 9

The bold edges have joined the 3 vertices of triangle with unbroken edges of one diagram of A_4 of one fragment $A - C - D$ to that of another fragment $A - C - D$. The

generators B and C together generate $S_3 = \langle B, C : B^2 = C^3 = (BC)^2 = 1 \rangle$, which is shown in Figure 10 below.

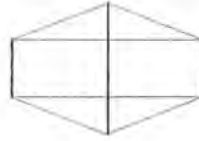


Figure 10

The transformations B and D in Figure 11, which is a fragment of Figure 9, have generated the group $D_2 = \langle B, D : B^2 = D^2 = (BD)^2 = 1 \rangle$. A bold edge is common between the diagrams of S_3 and D_2 as shown in Figure 12. Algebraically, \mathbb{Z}_2 is an amalgam of S_3 and D_2 .

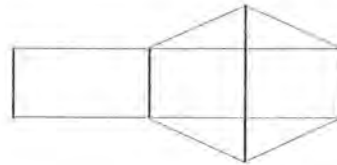
Figure 11: D_2 

Figure 12

The coset diagram for the action of Γ on $\mathbb{Q}(i)$ consists of one fragment $A - C - D$ at a zero level and then at the first level it has been joined with four other fragments $A - C - D$ by edges of the generator B . Further these 4 fragments $A - C - D$ have

been joined by 12 fragments $A - C - D$, that is, each fragment $A - C - D$ has been joined by 3 more fragments $A - C - D$ at second level of diagram and so on. This fragment of a coset diagram explains clearly the amalgam structure of Γ , that is, $\Gamma = (A_4 *_{\mathbb{Z}_3} S_3) *_{M} (S_3 *_{\mathbb{Z}_2} D_2)$. A general fragment of the coset diagram for the action of Γ on $\mathbb{Q}(i)$ will look as follows.

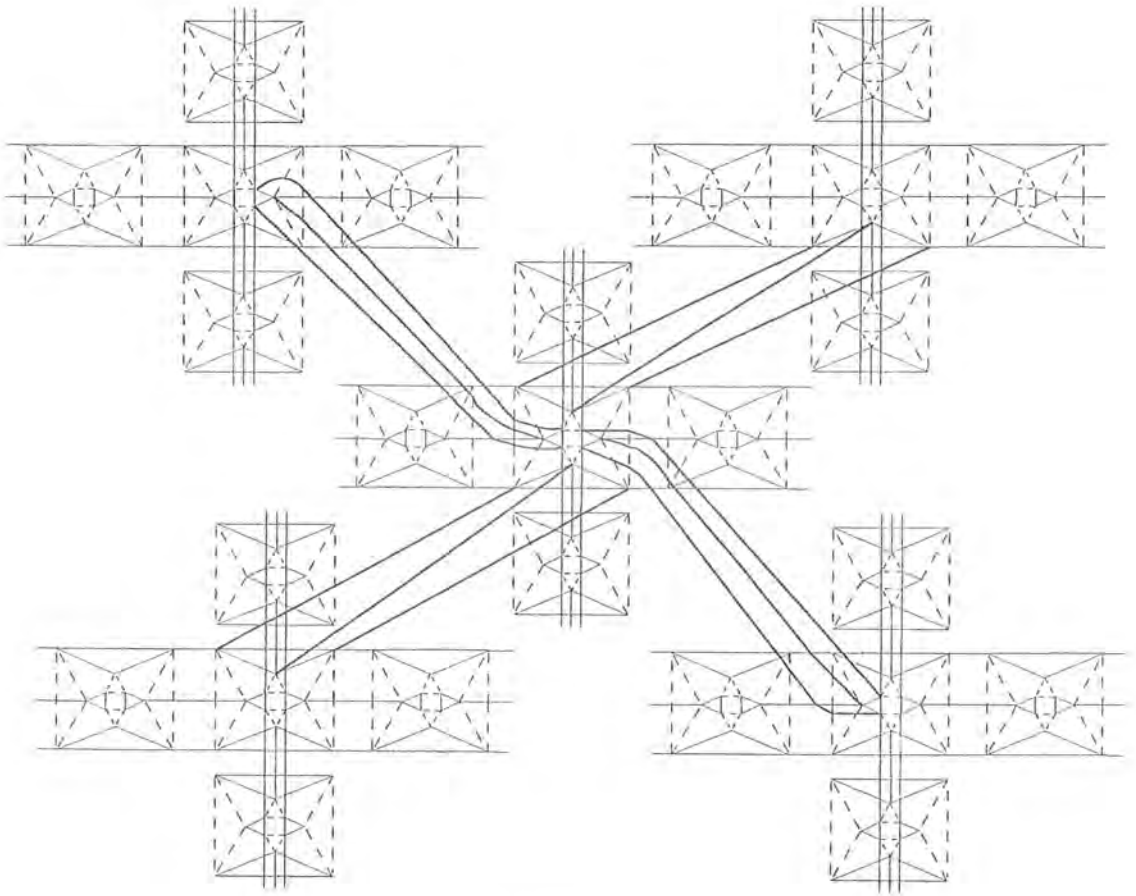


Figure 13

We have derived the coset diagrams for Γ by its action on $\mathbb{Q}(i)$ and $\mathbb{Q}(i, \sqrt{n})$,

and have obtained useful and interesting results related to Γ by using them. We have divided this coset diagram in to two layers, one containing α 's and the other containing $\frac{1}{\alpha}$'s. If a fragment $A - C - D$ is in layer 1, then the four fragments $A - C - D$ have joined it by bold edges are in layer 2. Similarly, the four fragments $A - C - D$ have further joined each with three fragments $A - C - D$, which are in layer 1, by bold edges. In this way, up to this level there are thirteen fragments $A - C - D$ in layer 1 and four fragments $A - C - D$ in layer 2. For instance, if $\alpha \in \mathbb{Q}(i, \sqrt{3})$ is in one layer, then its conjugate $\bar{\alpha}$ over $\mathbb{Q}(i)$ is in another layer.

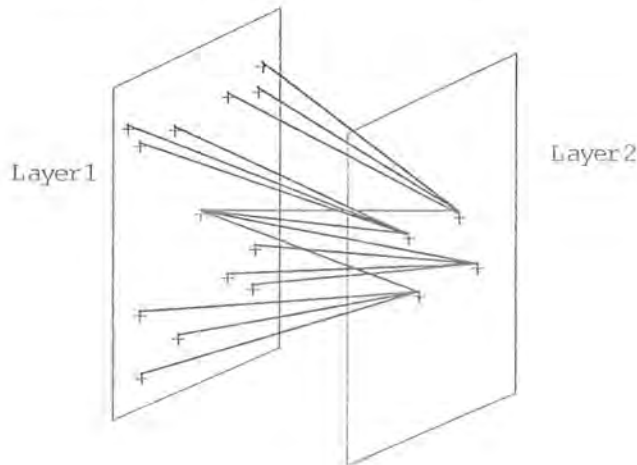


Figure 14

Chapter 2

Action of Γ on Imaginary

Quadratic Fields

In this chapter, we have studied an action of the Picard group $PSL(2, \mathbb{Z}[i])$, denoted by

$$\Gamma = \langle A, B, C, D : A^3 = B^2 = C^3 = D^2 = (AC)^2 = (AD)^2 = (BC)^2 = (BD)^2 = 1 \rangle$$

on $\mathbb{Q}(i) \cup \{\infty\}$ by using coset diagrams, where A, B, C and D are linear fractional transformations defined by $A(z) = \frac{1}{z-i}$, $B(z) = \frac{1}{z}$, $C(z) = \frac{1+z}{-z}$ and $D(z) = \frac{-1}{z}$.

It has been shown in [17] that Γ can be viewed as a free product of G_1 and G_2 with M amalgamated, that is,

$$\Gamma = G_1 *_M G_2,$$

where

$$G_1 = \langle A, C, D : A^3 = C^3 = D^2 = (AC)^2 = (AD)^2 = 1 \rangle,$$

$$G_2 = \langle B, C, D : B^2 = C^3 = D^2 = (BC)^2 = (BD)^2 = 1 \rangle,$$

and M is the modular group $\langle C, D : C^3 = D^2 = 1 \rangle$. Here G_1 and G_2 are called the components of Γ and M is called the amalgamated group. Further, $G_1 = S_3 \underset{\mathbb{Z}_3}{*} A_4$ and $G_2 = S_3 \underset{\mathbb{Z}_2}{*} D_2$, where S_3 is a symmetric group of degree 3, A_4 an alternating group of degree 4 and D_2 a dihedral group of order 4.

Recall that the real quadratic field is defined by the set $\{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$ and denoted by $\mathbb{Q}(\sqrt{n})$ and imaginary quadratic field is $\mathbb{Q}(\sqrt{-n}) = \{a + b\sqrt{-n} : a, b \in \mathbb{Q}\}$, where n is square-free positive integer. The biquadratic field $\mathbb{Q}(i, \sqrt{n})$ is defined as $\{a + b\sqrt{n} : a, b \in \mathbb{Q}(i)\}$.

2.1 The Picard Group Action

Modular group and the extended modular group have been studied extensively, and the Picard group is the extension of these groups. In [23] Q. Mushtaq has studied coset diagrams for the modular group. Here, we have defined coset diagrams for the Picard group Γ and have used them to investigate various properties of the group vis-à-vis quadratic and biquadratic fields. The natural action of Γ on different fields gives interesting information. It is natural to study the action of Γ on $\mathbb{Z}[i]$, since Γ consists of linear fractional transformations $T(z) = \frac{az + b}{cz + d}$ with $ad - bc = 1$ and

$a, b, c, d \in \mathbb{Z}[i]$. But Γ does not act on $\mathbb{Z}[i]$. The question has arisen, whether Γ acts on the imaginary quadratic field $\mathbb{Q}(i)$? We have found that among the quadratic fields, Γ acts only on $\mathbb{Q}(i)$. We have proved that action of Γ on $\mathbb{Q}(i) \cup \{\infty\}$ is transitive but actions of its component groups G_1, G_2 and amalgamated group M are intransitive. But all the fixed points of the generators of Γ do not lie in $\mathbb{Q}(i)$, so we need extension of $\mathbb{Q}(i)$. The one point extension of $\mathbb{Q}(i)$ is $\mathbb{Q}(i, \sqrt{n})$, where n is a square-free positive integer. We have proved that Γ acts on $\mathbb{Q}(i, \sqrt{n}) \cup \{\infty\}$.

Proposition 8 Γ does not act on $\mathbb{Z}[i]$.

Proof. Let $a + bi \in \mathbb{Z}[i]$, where $a, b \in \mathbb{Z}$. Then $B(a + bi) = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$. Since $\frac{a - bi}{a^2 + b^2} \notin \mathbb{Z}[i]$ for all $a, b \in \mathbb{Z}$, therefore Γ does not act on $\mathbb{Z}[i]$. ■

Proposition 9 Γ does not act on $\mathbb{Q}(\sqrt{n})$, where $n > 1$ is a square-free integer.

Proof. Let $a + b\sqrt{n} \in \mathbb{Q}(\sqrt{n})$, where $a, b \in \mathbb{Q}$ and $n > 1$ is a square-free integer.

Then

$$\begin{aligned} A(a + b\sqrt{n}) &= \frac{1}{a + b\sqrt{n} - i} \\ &= \frac{a + b\sqrt{n} + i}{a^2 - b^2n + 2ab\sqrt{n} + 1} \\ &= \frac{(a + b\sqrt{n} + i)(a^2 - b^2n + 1 - 2ab\sqrt{n})}{(a^2 - b^2n + 1)^2 - (2ab\sqrt{n})^2}. \end{aligned}$$

Since $i \notin \mathbb{Q}(\sqrt{n})$, therefore $A(a + b\sqrt{n}) \notin \mathbb{Q}(\sqrt{n})$. Thus Γ does not act on $\mathbb{Q}(\sqrt{n})$. ■

Proposition 10 Γ acts on $\mathbb{Q}(i)$.

Proof. Let $\alpha = a + bi \in \mathbb{Q}(i)$, where $a, b \in \mathbb{Q}$. Then

$$\begin{aligned} A(\alpha) &= \frac{1}{\alpha - i} = \frac{a - (b-1)i}{a^2 + b^2 + 1 - 2b} \in \mathbb{Q}(i). \\ B(\alpha) &= \frac{1}{\alpha} = \frac{a - bi}{a^2 + b^2} \in \mathbb{Q}(i). \\ C(\alpha) &= \frac{1 + \alpha}{-\alpha} = \frac{-a - a^2 - b^2 + bi}{a^2 + b^2} \in \mathbb{Q}(i). \\ D(\alpha) &= \frac{-1}{\alpha} = \frac{-a + bi}{a^2 + b^2} \in \mathbb{Q}(i). \end{aligned}$$

We can define a mapping $\mu : \Gamma \times \mathbb{Q}(i) \rightarrow \mathbb{Q}(i)$ by $\mu(g, \alpha) = g(\alpha)$, where $g \in \Gamma$ and $\alpha \in \mathbb{Q}(i)$. Obviously $g(\alpha) \in \mathbb{Q}(i)$, because g can be written as $A^{l_1} B^{m_1} C^{n_1} D^{o_1} \dots A^{l_k} B^{m_k} C^{n_k} D^{o_k}$, where $l_j, n_j = 0, 1, 2$ and $m_j, o_j = 0, 1$, and the generators A, B, C , and D give elements of $\mathbb{Q}(i)$ when applied on it, as proved above. We know that $\mu(1, \alpha) = 1(\alpha) = \alpha$, where 1 is the identity element of Γ . Also $\mu(g, \mu(h, \alpha)) = g(h(\alpha)) = \mu(gh, \alpha)$ by composition of linear fractional transformations. Thus Γ acts on $\mathbb{Q}(i)$. ■

Proposition 11 Γ does not act on $\mathbb{Q}(\sqrt{-n})$, where $n > 1$ is a square-free integer.

Proof. Let $a + b\sqrt{-n} \in \mathbb{Q}(\sqrt{-n})$, where $a, b \in \mathbb{Q}$ and $n > 1$ is a square-free integer. Then

$$\begin{aligned} A(a + b\sqrt{-n}) &= \frac{1}{a + b\sqrt{-n} - i} \\ &= \frac{a + b\sqrt{-n} + i}{a^2 - b^2n + 2ab\sqrt{-n} + 1} \\ &= \frac{(a + b\sqrt{-n} + i)(a^2 - b^2n + 1 - 2ab\sqrt{-n})}{(a^2 - b^2n + 1)^2 + 4a^2b^2n}. \end{aligned}$$

Since $i \notin \mathbb{Q}(\sqrt{-n})$, this means that $A(a + b\sqrt{-n}) \notin \mathbb{Q}(\sqrt{-n})$. Thus Γ does not act on $\mathbb{Q}(\sqrt{-n})$ naturally. ■

Proposition 12 Γ acts on $\mathbb{Q}(i, \sqrt{n})$, where n is a square-free positive integer.

Proof. Let $\alpha = a + bi + c\sqrt{n} + d\sqrt{ni} \in \mathbb{Q}(i, \sqrt{n})$, where $a, b, c, d \in \mathbb{Q}$ and n is a square-free positive integer. The generators of Γ are A, B, C and D defined as $A : z \mapsto \frac{1}{z-i}$, $B : z \mapsto \frac{1}{z}$, $C : z \mapsto \frac{1+z}{-z}$ and $D : z \mapsto \frac{-1}{z}$. Now the applications of generators of Γ on α yield $A(\alpha) = \frac{1}{\alpha-i} = \frac{c}{a+bi+c\sqrt{n}+d\sqrt{ni}-i}$

$$= \frac{(a+bi-i-c\sqrt{n}-d\sqrt{ni})(a^2-b^2-c^2n+d^2n-1+2b-2abi+2ncdi+2ai)}{(a^2-b^2-c^2n+d^2n-1+2b)^2+(2ab-2ncd-2a)^2}.$$

This implies that $A(\alpha) \in \mathbb{Q}(i, \sqrt{n})$. Also

$$\begin{aligned} B(\alpha) &= \frac{1}{\alpha} = \frac{1}{a+bi+c\sqrt{n}+d\sqrt{ni}} \in \mathbb{Q}(i, \sqrt{n}). \\ D(\alpha) &= \frac{-1}{\alpha} = \frac{-1}{a+bi+c\sqrt{n}+d\sqrt{ni}} \in \mathbb{Q}(i, \sqrt{n}). \\ C(\alpha) &= \frac{1+\alpha}{-\alpha} = \frac{1+a+bi+c\sqrt{n}+d\sqrt{ni}}{-a-bi-c\sqrt{n}-d\sqrt{ni}} \in \mathbb{Q}(i, \sqrt{n}). \end{aligned}$$

The element g of Γ can be written as $A^{l_1}B^{m_1}C^{n_1}D^{o_1} \dots A^{l_k}B^{m_k}C^{n_k}D^{o_k}$, where $l_j, n_j = 0, 1, 2$ and $m_j, o_j = 0, 1$. This means that $g(\alpha) \in \mathbb{Q}(i, \sqrt{n})$. We can define a mapping $\mu : \Gamma \times \mathbb{Q}(i, \sqrt{n}) \rightarrow \mathbb{Q}(i, \sqrt{n})$ by $\mu(g, \alpha) = g(\alpha)$ for all $\alpha \in \mathbb{Q}(i, \sqrt{n})$. We know that $\mu(1, \alpha) = 1(\alpha) = \alpha$, where 1 is the identity element of Γ . Also $\mu(g, \mu(h, \alpha)) = g(\mu(h, \alpha)) = \mu(gh, \alpha)$ by composition of linear fractional transformations of Γ . This ensures that μ is an action of Γ on $\mathbb{Q}(i, \sqrt{n})$. ■

Thus, above results imply that Γ acts on those infinite fields which contain i because Γ consists of linear fractional transformations $T(z) = \frac{az + b}{cz + d}$ with $ad - bc = 1$ and $a, b, c, d \in \mathbb{Z}[i]$. Among the quadratic fields, $\mathbb{Q}(i)$ is the only imaginary quadratic field on which Γ acts.

An action of the Picard group on projective line over imaginary quadratic field $\mathbb{Q}(i)$ is better understood by studying actions of the component groups G_1, G_2 and the amalgamated group M of Γ on $\mathbb{Q}(i)$. We have used a graphical technique called coset diagrams propounded by G. Higman in 1978 to study these actions. In 1983 Q. Mushtaq has defined coset diagrams for the modular group [23] and later on used them extensively, for example, in [19], [24]-[31].

A coset diagram for action of the modular group $M = \langle C, D : C^3 = D^2 = 1 \rangle$ on $\mathbb{Q}(i) \cup \{\infty\}$ depicts a permutation representation of the modular group: the 3-cycles of the generator C are denoted by three unbroken edges of a triangle permuted anti-clockwise and two vertices which are interchanged by D are joined by an edge. For instance, the following portion of a diagram depicts the action of M on $\mathbb{Q}(i) \cup \{\infty\}$.

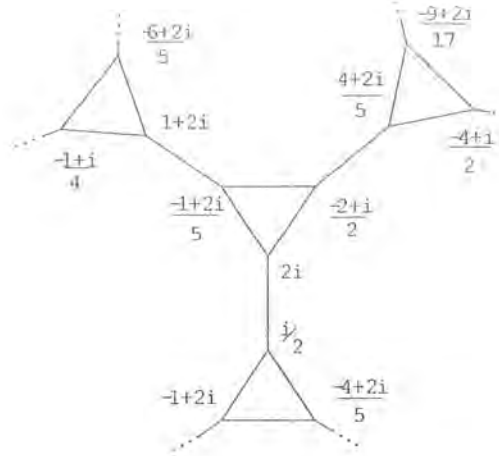


Figure 15

Let k be an integer. Consider a subset $\mathbb{Q}^*(ki) = \left\{ \frac{a+ki}{c} : a, c, d \in \mathbb{Z}, c > 0, d = \frac{a^2+k^2}{c} \in \mathbb{Z} \right\}$ of $\mathbb{Q}(i)$. If $k=0$, $\mathbb{Q}^*(ki)$ reduces to the field of rational numbers, which has been an object of study in [19].

A totally positive imaginary quadratic number $\alpha = \frac{a+ki}{c} \in \mathbb{Q}^*(ki)$, has $a, c, d > 0$ and totally negative imaginary quadratic number has $a < 0$ and $c, d > 0$.

To ensure that $\mathbb{Q}(i) = \bigcup_{k \in \mathbb{Z}} \mathbb{Q}^*(ki)$ or in other words every element of $\mathbb{Q}(i)$ lies in one of the sets $\mathbb{Q}^*(ki)$, where $k \in \mathbb{Z}$, we have the following result.

Proposition 13 *Every element of $\mathbb{Q}(i)$ can be written as $\frac{a+bi}{c}$, where c divides a^2+b^2 for all $a, b, c \in \mathbb{Z}$.*

Proof. Let $\alpha = \frac{\acute{a}+\acute{b}i}{\acute{c}} \in \mathbb{Q}(i)$ such that \acute{c} does not divide $\acute{a}^2+\acute{b}^2$. By multiplying and dividing α with \acute{c} , we get $\alpha = \frac{\acute{c}(\acute{a}+\acute{b}i)}{\acute{c}^2}$. Let $a = \acute{c}\acute{a}$, $b = \acute{c}\acute{b}$ and $c = \acute{c}^2$. Now

$\alpha = \frac{a+bi}{c}$, here $a^2 + b^2 = c^2 (a'^2 + b'^2)$. So c divides $a^2 + b^2$ and the quotient is $a'^2 + b'^2$. Thus we can write every element of $\mathbb{Q}(i)$ in the form $\frac{a+bi}{c}$, where c divides $a^2 + b^2$ for all $a, b, c \in \mathbb{Z}$. ■

To know how these totally positive and totally negative imaginary quadratic numbers belong to $\mathbb{Q}^*(ki)$, we have proved the following results.

Proposition 14 *If $\alpha = \frac{a+ki}{c} \in \mathbb{Q}^*(ki)$ is a totally positive imaginary quadratic number, then $D(\alpha)$ is totally negative and vice versa.*

Proof. Let $\alpha = \frac{a+ki}{c}$ be a totally positive imaginary quadratic number, that is, $a, c, d > 0$, where $d = \frac{a^2 + k^2}{c}$.

When $a, c, d > 0$, the generator D of Γ gives $D(\alpha) = D\left(\frac{a+ki}{c}\right) = \frac{-a+ki}{d}$. Here $a_1 = -a < 0$, $c_1 = d > 0$, and $d_1 = c > 0$. This implies that $D\left(\frac{a+ki}{c}\right)$ is totally negative.

Similarly by taking α to be totally negative, one can show that $D(\alpha)$ is totally positive. ■

Proposition 15 *If $\alpha = \frac{a+ki}{c} \in \mathbb{Q}^*(ki)$ is a totally positive imaginary quadratic number, then $C(\alpha)$ and $C^2(\alpha)$ are totally negative.*

Proof. Let $\alpha = \frac{a+ki}{c}$ be a totally positive imaginary quadratic number, that is, $a, c, d > 0$. Then $C(\alpha) = C\left(\frac{a+ki}{c}\right) = \frac{-a-d+ki}{d}$ and $C^2(\alpha) = \frac{-a-c+ki}{c+d+2a}$.

We can tabulate the information as follows.

α	a	c	d
$C(\alpha)$	$-a-d$	d	$c+d+2a$
$C^2(\alpha)$	$-a-c$	$c+d+2a$	c

We have seen that if $a, c, d > 0$, then the new values of a, c, d for $C(\alpha)$ and $C^2(\alpha)$ are as follows: $a < 0$ and $c, d > 0$. Therefore $C(\alpha)$ and $C^2(\alpha)$ are totally negative imaginary quadratic numbers. ■

Remark 16 *In a triangle of the coset diagram for the action of M on $\mathbb{Q}(i)$, there is only one totally positive and two totally negative imaginary quadratic numbers.*



Figure 16

Example 17 Let $\alpha = \frac{3+4i}{5}$. Here $a = 3, c = 5$ and $d = 5$. Since a, c and d are positive integers, therefore α is a totally positive imaginary quadratic number. We have $C(\alpha) = \frac{-8+4i}{5}$, where $a_1 = -8, c_1 = 5$ and $d_1 = 16$. Since $a_1 < 0$ and $c_1, d_1 > 0$, therefore $C(\alpha)$ is a totally negative imaginary quadratic number. The image of transformation C^2 , that is, $C^2(\alpha) = \frac{-8+4i}{16}$, where $a_2 = -8, c_2 = 16$ and $d_2 = 5$. Since $a_2 < 0$ and $c_2, d_2 > 0$, this implies that $C^2(\alpha)$ is also totally negative imaginary quadratic number. The generator D has an image $D(\alpha) = \frac{-3+4i}{5}$. This

shows that $D(\alpha)$ is totally negative imaginary quadratic number because $a_3 = -3$, $c_3 = 5$ and $d_3 = 5$.

In order to find a unique path between any two elements of $\mathbb{Q}^*(ki)$ in the coset diagram for the action of M on $\mathbb{Q}^*(ki)$, we have to define norm in $\mathbb{Q}^*(ki)$. The norm of $\alpha = \frac{a+ki}{c} \in \mathbb{Q}^*(ki)$ is defined as $\|\alpha\| = |a|$. This norm yields ordering in elements of $\mathbb{Q}^*(ki)$.

Proposition 18 *If $\alpha = \frac{a+ki}{c} \in \mathbb{Q}^*(ki)$, then $\|D(\alpha)\| = \|\alpha\|$.*

Proof. If $\alpha = \frac{a+ki}{c} \in \mathbb{Q}^*(ki)$ where $a, c \in \mathbb{Z}$ and k is a constant integer, then $D(\alpha) = \frac{-a+ki}{d}$. So $\|\alpha\| = |a|$ and $\|D(\alpha)\| = |-a|$. Three possibilities, namely (i) $a > 0$, (ii) $a < 0$ and (iii) $a = 0$ arise here.

(i) When $a > 0$, then norm of $D(\alpha)$ is $\|D(\alpha)\|$ which is equal to $|-a| = a$, but the norm of α , that is, $\|\alpha\| = |a| = a$,

(ii) when $a < 0$, then norm of $D(\alpha)$ is $\|D(\alpha)\|$ which is equal to $|-a| = -a$. But the norm of α , that is, $\|\alpha\| = |a| = -a$, and

(iii) when $a = 0$, then norm of $D(\alpha)$ is $\|D(\alpha)\|$, that is, $|0| = 0$. But the norm of α , that is, $\|\alpha\| = |0| = 0$. Hence in all the three cases the norm of $D(\alpha)$ and the norm of α are equal, that is, $\|D(\alpha)\| = \|\alpha\|$. ■

Proposition 19 *If $\alpha \in \mathbb{Q}^*(ki)$ is a totally positive imaginary quadratic number, then $\|\alpha\| < \|C(\alpha)\|$ and $\|\alpha\| < \|C^2(\alpha)\|$, where $\|\alpha\| = |a|$.*

Proof. Let $\alpha = \frac{a + ki}{c}$ be a totally positive imaginary quadratic number, that is, $a, c, d > 0$, where $d = \frac{a^2 + k^2}{c}$. Then $\|C(\alpha)\| = |-a - d| = |-(a + d)| = a + d$, and $\|C^2(\alpha)\| = |-a - c| = |-(a + c)| = a + c$. Also $\|\alpha\| = |a| = a$. Now $a + d > 0$ and $a + c > 0$, because $c, d > 0$ for totally positive imaginary quadratic numbers. This implies that $\|\alpha\| < \|C(\alpha)\|$ and $\|\alpha\| < \|C^2(\alpha)\|$. ■

Theorem 20 *The coset diagram for the action of M on $\mathbb{Q}^*(i)$ is connected.*

Proof. To prove this we need only to show that for any quadratic number α in $\mathbb{Q}^*(i)$, there is a path joining α to i . Since one of α and $D(\alpha)$ is totally positive by Proposition 14, therefore without loss of generality, we can assume that $\alpha = \frac{a + i}{c}$ is totally positive.

Let $\alpha = \alpha_0$ be a totally positive imaginary quadratic number. Then, by Proposition 14, $D(\alpha_0)$ is totally negative. There is just one totally positive number (vertex) say α_1 , in the triangle containing $D(\alpha_0)$. We have either of the fragments of the coset diagram.

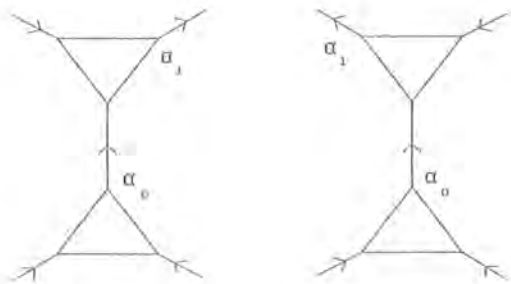


Figure 17

By using Propositions 18 and 19, we get $\|\alpha_0\| > \|\alpha_1\|$. If we now consider α_1 , then $D(\alpha_1)$ will be totally negative, whereas one of $CD(\alpha_1)$ and $C^2D(\alpha_1)$ will be totally positive. Let it be α_2 . This implies that $\|\alpha_1\| > \|\alpha_2\|$.

If we continue this way and follow the arrowheads, which show direction of unique path towards i , from $\alpha = \alpha_0$ in Figure 18, we get a sequence of totally positive imaginary quadratic numbers such that $\|\alpha_0\| > \|\alpha_1\| > \|\alpha_2\| \dots$

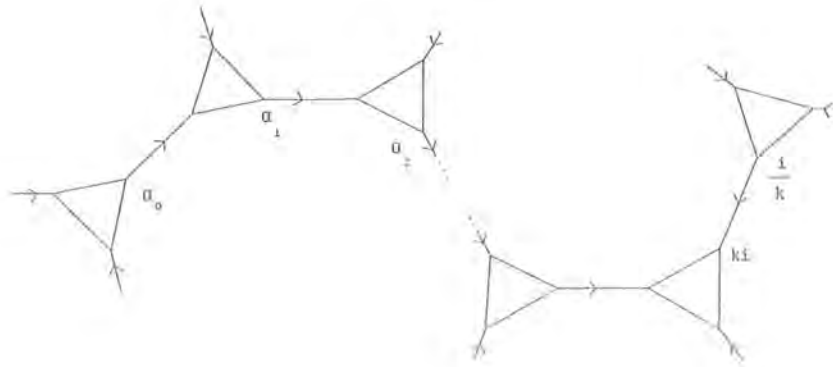


Figure 18

The decreasing sequence of non-negative integers must terminate and it will terminate at the triangle, which does not contain any totally positive quadratic number, that is, the triangle containing i , whose norm is zero. So we reach to a triangle containing i as a vertex.

A sequence of totally positive imaginary quadratic numbers $\alpha_0, \alpha_1, \alpha_2, \dots$ such that $\|\alpha_0\| > \|\alpha_1\| > \|\alpha_2\| \dots$, shows that there is a path joining $\alpha = \alpha_0$ to i , and the coset diagram for the action of M on $\mathbb{Q}^*(i)$ is connected. ■

Theorem 21 *The action of M on $\mathbb{Q}^*(i) \cup \{\infty\}$ is transitive.*

Proof. Let $\alpha, \beta \in \mathbb{Q}^*(i)$ and $g \in M$. If $g(\alpha) = \beta$, then $D^2 = 1$ implies that $gDD(\alpha) = \beta$ and since one of α and $D(\alpha)$ is totally positive, we can assume without loss of generality that α is totally positive. Let $\alpha = \alpha_0$ and $\beta = \alpha_j$, for some j . Then from the fragment of the coset diagram (Figure 17), we note that each α_{j+1} is either $CD(\alpha_j)$ or $C^2D(\alpha_j)$. This implies that $\beta = C^{\varepsilon_j}DC^{\varepsilon_{j-1}}D \dots C^{\varepsilon_1}D(\alpha)$, where each $\varepsilon_j = 1$ or 2 . If $g = C^{\varepsilon_j}DC^{\varepsilon_{j-1}}D \dots C^{\varepsilon_1}D$, then $\beta = g(\alpha)$. Hence the action of M on $\mathbb{Q}^*(i)$ is transitive. ■

Theorem 22 *The action of M on $\mathbb{Q}(i) \cup \{\infty\}$ is intransitive.*

Proof. We can write $\mathbb{Q}(i) \cup \{\infty\} = \mathbb{Q}^*(i) \cup \{\mathbb{Q}(i) \setminus \mathbb{Q}^*(i)\}$. By Theorem 18, the action of M on $\mathbb{Q}^*(i)$ is transitive, so $\mathbb{Q}^*(i)$ is one of the orbits of $\mathbb{Q}(i)$. Thus the action of M on $\mathbb{Q}(i) \cup \{\infty\}$ is intransitive because $\mathbb{Q}(i) \cup \{\infty\}$ has more than one orbit. ■

Recall that an algebraic integer in $\mathbb{Q}(i)$ is a root of some monic polynomial equation with integral coefficients. The algebraic integers in $\mathbb{Q}(i)$ form $\mathbb{Z}[i]$. Action of M on $\mathbb{Q}(i) \cup \{\infty\}$ has more than one orbit and in one orbit, the value of imaginary part of algebraic integers does not change.

Theorem 23 *If C and D are generators of M , then $(CD)^{\pm n}(a + bi) = (a \mp n) + bi$, where $a + bi$ is an algebraic integer in $\mathbb{Q}(i)$.*

Proof. We know that algebraic integers in $\mathbb{Q}(i)$ are of the form $a + bi$, where $a, b \in \mathbb{Z}$. To prove the result, we have used mathematical induction on $n \in \mathbb{Z}^+$.

For $n = 1$, we have $CD(a + bi) = a + bi - 1 = (a - 1) + bi$. Let it be true for $n = k$, that is, $(CD)^k(a + bi) = (a - k) + bi$. Then

$$\begin{aligned} (CD)^{k+1}(a + bi) &= (CD)(CD)^k(a + bi) \\ &= CD((a - k) + bi) \\ &= a - k - 1 + bi \\ &= a - (k + 1) + bi. \end{aligned}$$

Thus the result is true for all $n \in \mathbb{Z}^+$, that is, $(CD)^n(a + bi) = (a - n) + bi$. By following the same steps one can prove that $(CD)^{-n}(a + bi) = (a + n) + bi$. ■

We have denoted the orbit of ki when M is acting on $\mathbb{Q}(i)$ by $M(ki)$, where $ki \in \mathbb{Q}(i)$.

Proposition 24 *The algebraic integers in $M(ki)$ are of the form $\{a + ki : a \in \mathbb{Z}\}$, $k \in \mathbb{Z}$.*

Proof. We know that algebraic integers in $\mathbb{Q}(i)$ are of the form $a + bi$, where $a, b \in \mathbb{Z}$. Let $m + ki$ be an arbitrary algebraic integer from $\mathbb{Q}(i)$, where $m, k \in \mathbb{Z}$. By varying the value of $n \in \mathbb{Z}^+$ in Theorem 23, we get algebraic integers of the form $a + ki$, where $a \in \mathbb{Z}$. Hence, by applying elements of M on ki , we get elements of $\mathbb{Q}(i)$ of the form $\frac{a + ki}{c}$ such that $a + ki$ are algebraic integers. ■

A prime number p is called Pythagorean if it can be written as a sum of two squares, that is, $x^2 + y^2$, where $x, y \in \mathbb{Z}$. Pythagorean primes are of the form $4k + 1$ or $4k + 2$, where $k \geq 0$. In such primes $-1 \equiv x^2 \pmod{p}$.

Proposition 25 *If $m \in F_p$, then there exists an algebraic integer in $\mathbb{Q}(i)$, congruent to m , by the formula $m = x + k\sqrt{p-1}$, where $x \in \mathbb{Z}$, k is a constant integer and p is a Pythagorean prime number.*

Proof. Let $m \in F_p$ and M act on $\mathbb{Q}(i)$. We know that algebraic integers in $\mathbb{Q}(i)$ are of the form $a + bi$, where $i = \sqrt{-1} = \sqrt{p-1}$ in F_p . Let the orbit in which we are looking for an algebraic integer is $M(ki)$, then the algebraic integer $x + ki$ takes the form $x + k\sqrt{p-1}$, where $x \in \mathbb{Z}$. If $m \in F_p$ is known, then x can be found by $x = m - k\sqrt{p-1}$. Here $\sqrt{p-1}$ must belong to \mathbb{Z} , that is, $p-1$ is a square in F_p . In other words p is a Pythagorean prime. ■

The following Proposition states nature of the path formed by the algebraic integers in the coset diagram for the action of M on $\mathbb{Q}^*(ki)$.

Theorem 26 *There does not exist a closed path of algebraic integers in the coset diagram for the action of M on $\mathbb{Q}^*(ki)$.*

Proof. It is shown in Theorem 23 that the transformation CD maps an algebraic integer to another algebraic integer, that is, $CD(a + ki) = (a - 1) + ki$ or $CD(\alpha) = \alpha - 1$, where α is an algebraic integer. Let $\alpha_0, \alpha_1, \dots, \alpha_{m-1}$ be distinct algebraic integers and they form a closed path, $\alpha_0, \alpha_1, \dots, \alpha_{m-1}, \alpha_0$. This implies that $(CD)^m(\alpha_0) = \alpha_0$,

that is, $\alpha_0 - m = \alpha_0$. This implies that $m = 0$, that is, $1(\alpha_0) = \alpha_0$, where 1 is the identity of M . Thus there does not exist a word W other than identity such that $W(\alpha_0) = \alpha_0$. Hence there does not exist any closed path of algebraic integers in the coset diagram for the action of M on $\mathbb{Q}^*(ki)$. ■

2.1.1 The Extended Modular Group

The extended modular group G_2 has the finite presentation

$$\langle B, C, D : B^2 = C^3 = D^2 = (BC)^2 = (BD)^2 = 1 \rangle.$$

It can decompose as a free product of S_3 and D_2 with \mathbb{Z}_2 amalgamated, that is, $G_2 = (S_3 *_{\mathbb{Z}_2} D_2)$, where $S_3 = \langle B, C : B^2 = C^3 = (BC)^2 = 1 \rangle$, $D_2 = \langle B, D : B^2 = D^2 = (BD)^2 = 1 \rangle$ and $\mathbb{Z}_2 = \langle B : B^2 = 1 \rangle$. Let

$$\acute{\mathbb{Q}}(ki) = \left\{ \frac{a + ki}{c} : a, c, d \in \mathbb{Z}, c \neq 0 \right\} \subset \mathbb{Q}(i),$$

where $k \geq 0$ be a constant integer and $d = \frac{a^2 + k^2}{c}$. That is, $\acute{\mathbb{Q}}(ki) = \mathbb{Q}^*(ki) \cup \mathbb{Q}^*(-ki)$. A totally positive imaginary quadratic number $\alpha = \frac{a + ki}{c} \in \acute{\mathbb{Q}}(ki)$ has $a, c, d > 0$ or $a, c, d < 0$ and a totally negative imaginary quadratic number has $a > 0$ and $c, d < 0$ or $a < 0$ and $c, d > 0$.

The generator B in G_2 (represented by a bold edge) has joined two fragments of the Figure 15, to form a fragment of coset diagram for the action of G_2 on $\acute{\mathbb{Q}}(ki)$ as shown in Figure 19. In this figure one can clearly see the Cayley's diagram of S_3, D_2 and the amalgam \mathbb{Z}_2 .

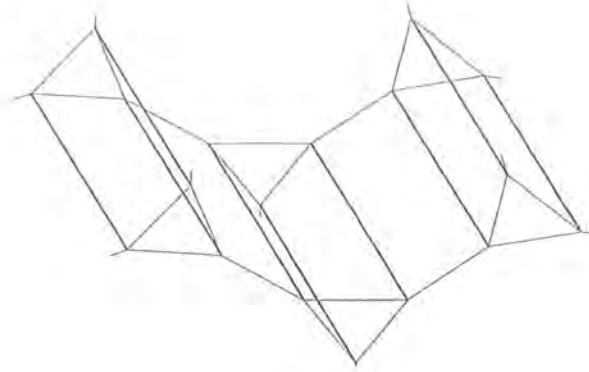


Figure 19

Proposition 27 If $\alpha = \frac{a+ki}{c} \in \mathcal{Q}(ki)$ is a totally positive (or totally negative) imaginary quadratic number, then so is $B(\alpha)$.

Proof. Let $\alpha = \frac{a+ki}{c}$ be a totally positive imaginary quadratic number, that is, either $a, c, d > 0$ or $a, c, d < 0$, where $d = \frac{a^2+k^2}{c}$.

When $a, c, d > 0$, $B(\alpha) = B\left(\frac{a+ki}{c}\right) = \frac{-a+ki}{-d}$. Here $a_1 = -a < 0$, $c_1 = -d < 0$, and $d_1 = -c < 0$, shows that $B\left(\frac{a+ki}{c}\right)$ is also totally positive.

When $a, c, d < 0$, $a_1 = -a > 0$, $c_1 = -d > 0$, and $d_1 = -c > 0$, then $B\left(\frac{a+ki}{c}\right)$ is totally positive. Similarly, if α is a totally negative, then so is $B(\alpha)$. ■

Proposition 28 If $\alpha = \frac{a+ki}{c} \in \mathcal{Q}(ki)$, then $\|B(\alpha)\| = \|\alpha\|$ where $\|\alpha\| = |a|$.

Proof. Let $\alpha = \frac{a+ki}{c} \in \mathcal{Q}(ki)$. Then $B(\alpha) = \frac{-a+ki}{-d}$, and $\|\alpha\| = |a|$ and $\|B(\alpha)\| = |-a|$. Three possibilities $a > 0$, $a < 0$ and $a = 0$ arise here. So, if $a > 0$, then the norm of $B(\alpha)$ is $\|B(\alpha)\|$ which is equal to $|-a| = a$, but $\|\alpha\| = |a| = a$. If

$a < 0$, then the norm of $B(\alpha)$ is $|-a| = -a$, but in this case the norm of α is $|a|$, which is equal to $-a$. In the case when $a = 0$, the norm of $B(\alpha)$ is $\|B(\alpha)\| = |0| = 0 = |0| = \|\alpha\|$. Thus in all the three cases the norm of $B(\alpha)$ is equal to the norm of α . ■

Theorem 29 *The coset diagram for the action of G_2 on $\hat{\mathbb{Q}}(i)$ is connected.*

Proof. To prove this we need only to show that for any quadratic number α in $\hat{\mathbb{Q}}(i)$, there is a path joining α to i . It is straight forward that for $d = \frac{a^2 + 1}{c}$,

$$\begin{aligned} \hat{\mathbb{Q}}(i) &= \left\{ \frac{a+i}{c} : a, c, d \in \mathbb{Z}, c \neq 0 \right\} \\ &= \left\{ \frac{a+i}{c} : a, c, d \in \mathbb{Z}, c > 0 \right\} \cup \left\{ \frac{a+i}{c} : a, c, d \in \mathbb{Z}, c < 0 \right\} \\ &= \left\{ \frac{a+i}{c} : a, c, d \in \mathbb{Z}, c > 0 \right\} \cup \left\{ \frac{a-i}{c} : a, c, d \in \mathbb{Z}, c > 0 \right\} \\ &= \mathbb{Q}^*(i) \cup \mathbb{Q}^*(-i). \end{aligned}$$

Since $M \leq G_2$, and by Theorem 20, the coset diagram for the action of M on $\mathbb{Q}^*(i)$ is connected, therefore the coset diagram for the action of G_2 on $\mathbb{Q}^*(i)$ is also connected. An analogous proof of Theorem 20 can be used to prove that the coset diagram for the action of G_2 on $\mathbb{Q}^*(-ki)$ is connected. Since $DB(i) = -i$, this shows that there is a path which joins the coset diagram for the action of G_2 on $\mathbb{Q}^*(i)$ with the coset diagram for the action of G_2 on $\mathbb{Q}^*(-i)$. Thus there is a path for an imaginary quadratic number α in $\hat{\mathbb{Q}}(i)$ to i . Hence the coset diagram for the action of G_2 on $\hat{\mathbb{Q}}(i)$ is connected. ■

Theorem 30 *The action of G_2 on $\hat{\mathbb{Q}}(i)$ is transitive.*

Proof. It has been proved in Theorem 21 that the action of M on $\mathbb{Q}^*(ki)$ is transitive. Similarly, it can be proved that the action of M on $\mathbb{Q}^*(-i)$ is transitive. Since $M \leq G_2$, thus the actions of G_2 on $\mathbb{Q}^*(i)$ and $\mathbb{Q}^*(-i)$ are also transitive. As $\mathbb{Q}(i) = \mathbb{Q}^*(i) \cup \mathbb{Q}^*(-i)$, we let $\alpha = \frac{a-i}{c} \in \mathbb{Q}^*(-i)$ and $\beta \in \mathbb{Q}^*(i)$. Since $B(\alpha) = \frac{a+i}{d} \in \mathbb{Q}^*(i)$ and action of G_2 on $\mathbb{Q}^*(i)$ is transitive, there exist some element $C^{\epsilon_j}DC^{\epsilon_{j-1}}D\dots C^{\epsilon_1}D \in G_2$ such that $C^{\epsilon_j}DC^{\epsilon_{j-1}}D\dots C^{\epsilon_1}DB(\alpha) = \beta$. Let $g = C^{\epsilon_j}DC^{\epsilon_{j-1}}D\dots C^{\epsilon_1}DB$. Then $g(\alpha) = \beta$ implies that the action of G_2 on $\mathbb{Q}(i)$ is transitive. ■

Corollary 31 *The action of G_2 on $\mathbb{Q}(i) \cup \{\infty\}$ is intransitive.*

Proof. Let the action of G_2 on $\mathbb{Q}(i) \cup \{\infty\}$ be transitive. Consider $3i$ and $\frac{1+3i}{2} \in \mathbb{Q}(i)$. There does not exist any $g \in G_2$ such that $g(3i) = \frac{1+3i}{2}$. Hence the action of G_2 on $\mathbb{Q}(i) \cup \{\infty\}$ is intransitive. ■

2.1.2 The Group G_1

The component group G_1 of Γ has finite presentation

$$G_1 = \langle A, C, D : A^3 = C^3 = D^2 = (AC)^2 = (AD)^2 = 1 \rangle,$$

which can be decomposed as a free product of A_4 and S_3 with \mathbb{Z}_3 amalgamated, that is, $G_1 = (A_4 *_Z S_3)$, where $A_4 = \langle A, C : A^3 = C^3 = (AC)^2 = 1 \rangle$, $S_3 = \langle A, D : A^3 = D^2 = (AD)^2 = 1 \rangle$ and $\mathbb{Z}_3 = \langle A : A^3 = 1 \rangle$. The generators C, D are represented graphically in the same way as in the case of the modular group, however, the 3-cycles

of generator A are denoted by three broken edges of a triangle permuted anticlockwise by A as shown in Figure 20 which is a fragment of a coset diagram for the action of G_1 on $\mathbb{Q}(i)$. One Cayley's diagram of A_4 has contained four triangles with broken edges. So, one diagram of A_4 can be connected to four other diagrams of A_4 by edges representing the generator D . The connection between two diagrams of A_4 is actually the diagram of S_3 , a component of G_1 . One can see in Figure 20 that a triangle having broken edges is common between the Cayley's diagram of A_4 and S_3 , which is actually $\mathbb{Z}_3 = \langle A \rangle$. We will denote the coset diagram for the action of G_1 on $\mathbb{Q}(i)$ by a fragment $A - C - D$ because this fragment of the coset diagram is composed by the use of generators A, C and D .

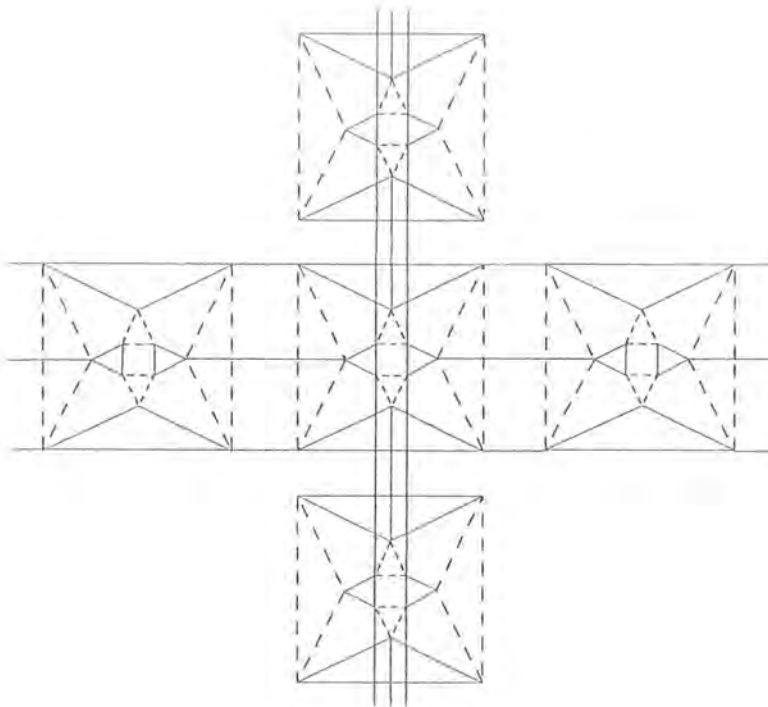


Figure 20

Theorem 32 Under the action of G_1 on $\mathbb{Q}(i)$,

- (i) the generator C does not have any fixed point,
- (ii) the generator A has no fixed point, and
- (iii) the fixed points of the generator D are i and $-i$.

Proof. (i) If $z \in \mathbb{Q}(i)$ is a fixed point of C , then $C(z) = z$. Therefore $\frac{1+z}{-z} = z$ implies that $1+z = -z^2$, that is, $z^2 + z + 1 = 0$. Whence $z = \frac{-1 \pm \sqrt{-3}}{2} \notin \mathbb{Q}(i)$.

(ii) If $z \in \mathbb{Q}(i)$ is a fixed point of A , then $A(z) = z$. Therefore $\frac{1}{z-i} = z$ implies that $z(z-i) = 1$, that is, $z^2 - iz - 1 = 0$. This implies that $z = \frac{i \pm \sqrt{3}}{2} \notin \mathbb{Q}(i)$.

(iii) If $z \in \mathbb{Q}(i)$ is a fixed point of D , then $D(z) = z$. Therefore $\frac{-1}{z} = z$, this implies that $z^2 = -1$ or $z = \pm i \in \mathbb{Q}(i)$. ■

Theorem 33 The action of G_1 on $\mathbb{Q}(i) \cup \{\infty\}$ has infinite number of orbits.

Proof. Let $\alpha = ki$, where $k \in \mathbb{Z}$ and the orbit of ki by the action of G_1 on $\mathbb{Q}(i)$ be $G_1(ki)$. By Theorem 23, the transformations $(CD)^{\pm n}$ yield a sequence $\{a + ki : a \in \mathbb{Z}\}$, where k is a constant integer. Application of CA on ki and $(CD)^{\pm n}$ on $CA(ki)$ yield another sequence $\{a + (1-k)i : a \in \mathbb{Z}\}$. Further, applications of DA on these sequences evolve the same two sequences. The transformations CA and DA change the imaginary part of an element in $\mathbb{Q}(i)$ but since both have order two, that is why, they cannot yield another sequence whose imaginary part is

different from the above two sequences. Therefore in one orbit of $\mathbb{Q}(i)$ containing ki , there are only two sequences of algebraic integers, that is, $\{a + ki : a \in \mathbb{Z}\}$ and $\{a + (1 - k)i : a \in \mathbb{Z}\}$ for constant $k \in \mathbb{Z}$.

By varying k one can get different orbits. Since \mathbb{Z} is infinite, therefore there are infinite orbits of $\mathbb{Q}(i) \cup \{\infty\}$. ■

There are exactly two sequences of algebraic integers in one orbit of $\mathbb{Q}(i) \cup \{\infty\}$ for the action of G_1 and they are of the form $\{a + ki : a \in \mathbb{Z}\}$ and

$\{a + (1 - k)i : a \in \mathbb{Z}\}$, where k is a constant integer.

2.1.3 The Picard Group

The coset diagram for the action of the Picard group on $\mathbb{Q}(i)$ has the basic fragment $A - C - D$. In this coset diagram, one fragment $A - C - D$ is linked with other four fragments $A - C - D$ by the bold edges. A general fragment of a coset diagram for the action of Γ on $\mathbb{Q}(i)$ is shown in Figure 21. This fragment, the details of which are described in chapter 1, shows clearly the amalgam decomposition of Γ , that is,

$$\Gamma = (A_4 \underset{\mathbb{Z}_3}{*} S_3) \underset{M}{*} (S_3 \underset{\mathbb{Z}_2}{*} D_2).$$

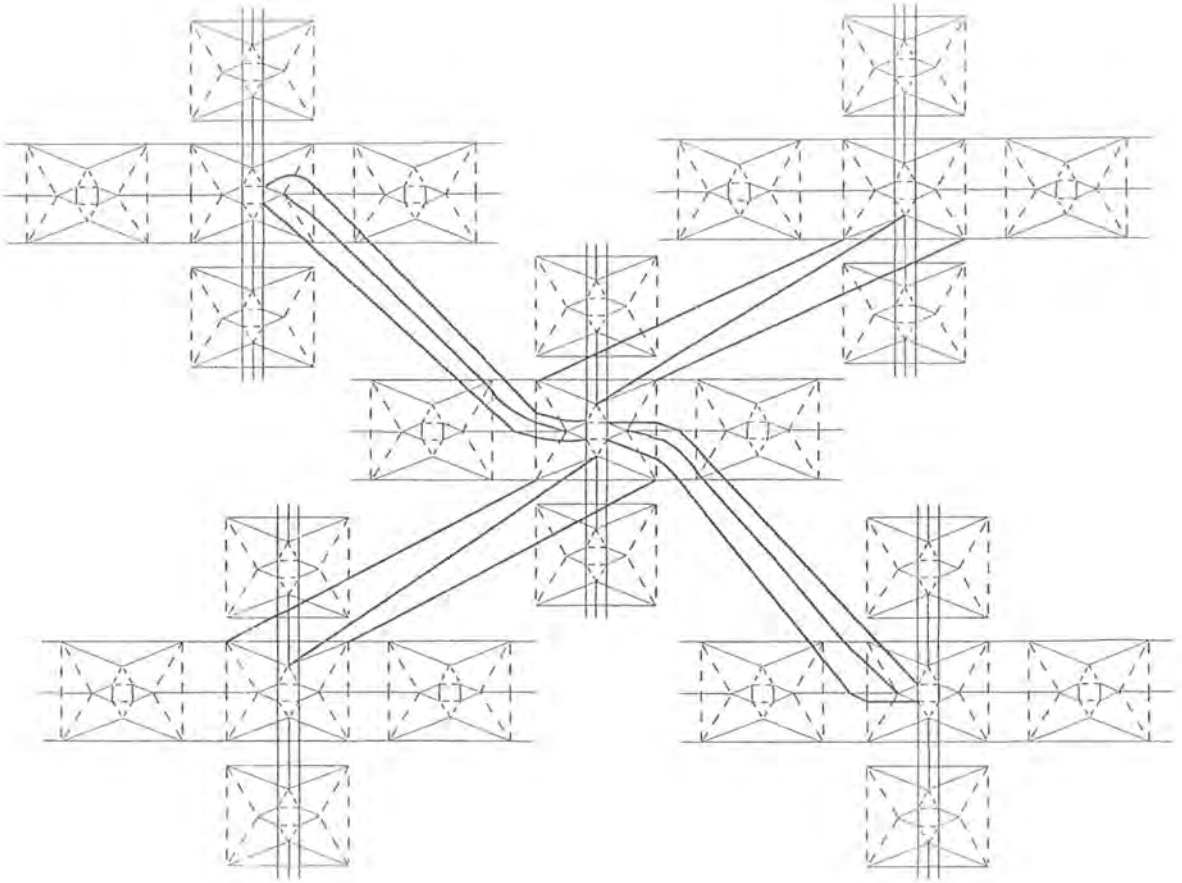


Figure 21

Theorem 34 *The action of Γ on $\mathbb{Q}(i) \cup \{\infty\}$ is transitive.*

Proof. In the proof of Theorem 33, it is shown that there are 2 sequences of algebraic integers, that is, $\{a + ki : a \in \mathbb{Z}\}$ and $\{a + (1 - k)i : a \in \mathbb{Z}\}$ for $k \in \mathbb{Z}$. Therefore it suffices to show that for any $l, m \in \mathbb{Z}$ there exists $g \in \Gamma$ such that $g(li) = mi$.

If $ki \in \mathbb{Q}(ki)$, then $BA(ki) = (k-1)i$ and $(BA)^n(ki) = (k-n)i$. Also $A^2B(ki) = (k+1)i$ and $(A^2B)^n(ki) = (k+n)i$ where $n \in \mathbb{Z}^+$. This implies that $(BA)^n$ and $(A^2B)^n$ connect together all $k \in \mathbb{Z}^+$. Thus the action of Γ on $\mathbb{Q}(i) \cup \{\infty\}$ is transitive.

We can also prove this theorem as follows. Let $a_0 + a_1i = \frac{b_0 + b_1i}{c_0 + c_1i} = \frac{\alpha}{\gamma}$, where $\alpha, \gamma \in \mathbb{Z}[i]$ and $(\alpha, \gamma) = 1$. By Euclidean algorithm in $\mathbb{Z}[i]$, there exists $\beta, \delta \in \mathbb{Z}[i]$ such that $\alpha\delta - \beta\gamma = 1$. So there exists $g \in \Gamma$ such that $g(z) = \frac{\alpha z + \beta}{\gamma z + \delta}$ and $\alpha\delta - \beta\gamma = 1$, where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[i]$. Since $g(\infty) = \frac{\alpha}{\gamma} = a_0 + a_1i \in \mathbb{Z}[i]$, this means ∞ is mapped to every element of $\mathbb{Z}[i]$. Hence the action of Γ on $\mathbb{Q}(i) \cup \{\infty\}$ is transitive. ■

We conclude that the action of component groups G_1, G_2 and amalgamated group M of Γ have intransitive action on $\mathbb{Q}(i) \cup \{\infty\}$, whereas action of Γ on $\mathbb{Q}(i) \cup \{\infty\}$ is transitive. That is, there is only one orbit obtained by action of Γ on $\mathbb{Q}(i) \cup \{\infty\}$, also this is the only imaginary quadratic number field on which Γ acts.

Chapter 3

Action of Γ on Biquadratic Fields

As described in chapter 1, the field formed by adjoining \sqrt{m} and \sqrt{n} to \mathbb{Q} , where m and n are square-free integers, is denoted by $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ and is called biquadratic field over \mathbb{Q} . The elements of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ are of the form $a_0 + a_1\sqrt{m} + a_2\sqrt{n} + a_3\sqrt{mn}$, where a_0, a_1, a_2 and $a_3 \in \mathbb{Q}$.

We have shown that Γ acts on $\mathbb{Q}(i, \sqrt{n})$, where $n > 1$ is a square-free integer. The fixed points of generators A, B, C and D of Γ are $\frac{i \pm \sqrt{3}}{2}, \pm 1, \frac{-1 \pm \sqrt{3}i}{2}$ and $\pm i$ respectively. They all lie in a biquadratic field $\mathbb{Q}(i, \sqrt{3})$, where i and $\sqrt{3}$ are zeros of an irreducible polynomial $(t^2 - 3)(t^2 + 1)$ over \mathbb{Q} . The action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is different from $\mathbb{Q}(i, \sqrt{n})$, where $n > 1$ is a square-free integer and deserves special account because $\mathbb{Q}(i, \sqrt{3})$ contains all the fixed points of the generators of Γ . So the closed paths in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ must be significantly different from the coset diagrams for the action of Γ on $\mathbb{Q}(i, \sqrt{n})$ when $n \neq 3$.

The elements of $\mathbb{Q}(i, \sqrt{3})$ are of the form $u + v\sqrt{3}$, where $u, v \in \mathbb{Q}(i)$. They can be written as $\alpha = \frac{(a + bi) + (c + di)\sqrt{3}}{e}$, where $a, b, c, d, e \in \mathbb{Z}$. The conjugates of α over \mathbb{Q} are $\alpha_1 = \frac{(a + bi) - (c + di)\sqrt{3}}{e}$, $\alpha_2 = \frac{(a - bi) + (c - di)\sqrt{3}}{e}$ and $\alpha_3 = \frac{(a - bi) - (c - di)\sqrt{3}}{e}$. The conjugate of α over $\mathbb{Q}(i)$ is α_1 and the conjugate of α over $\mathbb{Q}(\sqrt{3})$ is α_2 . The action of Γ on $\mathbb{Q}(i, \sqrt{3})$ shows that certain elements of $\mathbb{Q}(i, \sqrt{3})$ of the form $\frac{a + b\sqrt{3}}{c}$ behave special under this action. Thus they deserve a classification. As there are two conjugates of $\alpha = \frac{a + b\sqrt{3}}{c}$ over \mathbb{Q} , namely, α and $\frac{a - b\sqrt{3}}{c}$, and the conjugate of α is again α over $\mathbb{Q}(\sqrt{3})$, so we have considered conjugate of α over $\mathbb{Q}(i)$, that is, $\frac{a - b\sqrt{3}}{c}$. A real quadratic irrational number $\alpha = \frac{a + b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$, where $a, b, c \in \mathbb{Z}$, is called totally positive (negative) if α and $\bar{\alpha}$ are both positive (negative). When α and $\bar{\alpha}$ have opposite signs, then they are called ambiguous numbers [25]. They play an important role in classifying the orbits of $\mathbb{Q}(i, \sqrt{3})$ when Γ acts on it.

In this chapter, we have explored some group theoretic properties of the action of Γ on $\mathbb{Q}(i, \sqrt{3})$. We have shown that there is a finite number of ambiguous numbers in the orbit $\Gamma\alpha$, where α is ambiguous, and that they form a closed path and it is the only closed path in the orbit $\Gamma\alpha$. We have classified all the ambiguous numbers in the orbit. We need Propositions 36 to 39 to obtain one ambiguous number from the other.

Note that the fixed points of B and D lie in $\mathbb{Q}(i)$ and consequently in $\mathbb{Q}(i, \sqrt{n})$, where $n > 1$ is a square-free integer. Whereas the fixed points of A and C lie only in $\mathbb{Q}(i, \sqrt{3})$.

Proposition 35 *If $\alpha = \frac{a + b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$ is a totally positive real quadratic irrational number, then $C(\alpha)$ and $C^2(\alpha)$ are totally negative.*

Proof. Let α be a totally positive quadratic number. Then there are two possibilities either $a, d, c > 0$ or $a, d, c < 0$, where $d = \frac{a^2 - 3b^2}{c}$. When $a, d, c > 0$, then

$$C(\alpha) = C\left(\frac{a + b\sqrt{3}}{c}\right) = \frac{-a - d + b\sqrt{3}}{d}.$$

Here $a_1 = -a - d < 0$, $c_1 = d > 0$, and $d_1 = 2a + c + d > 0$. This shows that $C(\alpha)$ is totally negative. Also

$$C^2(\alpha) = \frac{-1}{1 + \alpha} = \frac{-a - c + b\sqrt{3}}{2a + c + d}.$$

Here $a_2 = -a - c < 0$, $c_2 = 2a + c + d > 0$, and $d_2 = \frac{a_2^2 - 3b^2}{c_2} = \frac{a^2 + c^2 + 2ac - 3b^2}{2a + c + d} = \frac{c(2a + c + d)}{2a + c + d} = c > 0$. This shows that $C^2(\alpha)$ is totally negative. Similarly, it can be proved that when $a, d, c < 0$, then $C(\alpha)$ and $C^2(\alpha)$ are totally negative. ■

If a number α is ambiguous, then $\alpha\bar{\alpha} = \frac{a^2 - 3b^2}{c^2} < 0$, that is, $a^2 - 3b^2 < 0$. Thus, in other words α is an ambiguous when $dc < 0$, where $d = \frac{a^2 - 3b^2}{c}$.

Lemma 36 *Transformations B and D map an ambiguous number to an ambiguous number.*

Proof. Let $\alpha = \frac{a + b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$ be an ambiguous number, where $a, b, c \in \mathbb{Z}$. This implies that $\alpha\bar{\alpha} < 0$, that is, $\frac{a^2 - 3b^2}{c^2} < 0$ which further implies that $a^2 - 3b^2 < 0$.

Now

$$B(\alpha) = \frac{1}{\alpha} = \frac{a - b\sqrt{3}}{d}, \text{ and}$$

$$D(\alpha) = \frac{-1}{\alpha} = \frac{a - b\sqrt{3}}{-d},$$

$$\text{imply that } (B(\alpha))(\overline{B(\alpha)}) = \frac{a^2 - 3b^2}{d^2} = D(\alpha)(\overline{D(\alpha)}).$$

Here $\frac{a^2 - 3b^2}{d^2} < 0$, since $a^2 - 3b^2 < 0$ and $d^2 > 0$. This shows that $B(\alpha)$ and $D(\alpha)$ are ambiguous numbers. ■

Lemma 37 *If α is not ambiguous, then so are $D(\alpha)$ and $B(\alpha)$.*

Proof. Suppose $\alpha = \frac{a + b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$ is not ambiguous number, where $a, b, c \in \mathbb{Z}$. This means that $\alpha\bar{\alpha} \geq 0$, that is, $\frac{a^2 - 3b^2}{c^2} \geq 0$ which further implies that $a^2 - 3b^2 \geq 0$ because $c^2 \neq 0$. Since $B(\alpha) = \frac{1}{\alpha} = \frac{a - b\sqrt{3}}{d}$, and $D(\alpha) = \frac{-1}{\alpha} = \frac{-a + b\sqrt{3}}{d}$, so $(B(\alpha))(\overline{B(\alpha)}) = \frac{a^2 - 3b^2}{d^2} = D(\alpha)(\overline{D(\alpha)})$. Here $\frac{a^2 - 3b^2}{d^2} \geq 0$, because $a^2 - 3b^2 \geq 0$ and $d^2 > 0$. This shows that $B(\alpha)$ and $D(\alpha)$ are not ambiguous numbers.

■

Proposition 38 *If α is an ambiguous number, then $A(\alpha)$ and $A^2(\alpha)$ are not ambiguous.*

Proof. Let $\alpha = \frac{a + b\sqrt{3}}{c}$ be an ambiguous number. This means that $\alpha\bar{\alpha} < 0$, that is, $\frac{a^2 - 3b^2}{c^2} < 0$. This implies that $a^2 - 3b^2 < 0$. After rationalization of $A(\alpha) = \frac{1}{\alpha - i} = \frac{c}{a + b\sqrt{3} - ci}$, the imaginary part is $(a^2c^2 + c^4 + 3b^2c^2 - 2abc^2\sqrt{3})$. This

means that $A(\alpha)$ will be ambiguous if and only if $(a^2c^2 + c^4 + 3b^2c^2 - 2abc^2\sqrt{3})i = 0$. Since $i \neq 0$, it implies that $a^2c^2 + c^4 + 3b^2c^2 - 2abc^2\sqrt{3} = 0$. Left hand will be zero only if $c = 0$. But c cannot be zero because otherwise $\alpha = \infty$ will be not ambiguous.

This shows that $A(\alpha)$ is not ambiguous.

Also, $A^2(\alpha) = \frac{1+i\alpha}{\alpha} = \frac{a-b\sqrt{3}+di}{d}$ will be ambiguous when imaginary part becomes zero, that is, $d = 0$. But d cannot be zero because otherwise $A^2(\alpha)$ will become ∞ . This shows that $A^2(\alpha)$ is not ambiguous. ■

Proposition 39 *If $\alpha = \frac{a+b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$ is an ambiguous number, then one of $C(\alpha)$ and $C^2(\alpha)$ is ambiguous and the other is totally negative.*

Proof. Suppose that α is a positive ambiguous number. Then by Proposition 35, the information can be tabulated as follows.

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

Similarly, if α is a negative ambiguous number, then the information about $C(\alpha)$, $C^2(\alpha)$, $\bar{\alpha}$, $\overline{C(\alpha)}$ and $\overline{C^2(\alpha)}$ can be tabulated as follows.

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

Therefore, from the above tables it can easily be deduced that one of $C(\alpha)$ and $C^2(\alpha)$ is ambiguous and the other is totally negative. ■

Example 40 Let $\alpha = 1 + 2\sqrt{3}$. Here $a = 1, c = 1$ and $d = -11$. As $dc < 0$ this implies that α is an ambiguous number. Thus $C(\alpha) = \frac{10 + 2\sqrt{3}}{-11}$, where $a_1 = 10, c_1 = -11$ and $d_1 = -8$. As $d_1c_1 > 0$, this shows that $C(\alpha)$ is not ambiguous. Also $a_1 > 0$ and $c_1d_1 < 0$. This shows that $C(\alpha)$ is a totally negative number. Then $C^2(\alpha) = \frac{-2 + 2\sqrt{3}}{-8}$, where $a_2 = -2, c_2 = -8$ and $d_2 = 1$. The inequality $d_2c_2 < 0$, implies that $C^2(\alpha)$ is an ambiguous number. Thus $B(\alpha) = \frac{1 - 2\sqrt{3}}{-11}$, where $c_3 = -11$ and $d_3 = 1$ so that $d_3c_3 < 0$. This shows that $B(\alpha)$ is an ambiguous number. Also $D(\alpha) = \frac{1 - 2\sqrt{3}}{11}$, where $c_4 = 11$ and $d_4 = -1$ so that $d_4c_4 < 0$. This shows that $D(\alpha)$ is an ambiguous number.

Proposition 41 If $\alpha = \frac{a + b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$ such that $d = \frac{a^2 - 3b^2}{c}$ is an integer, then the following hold:

- (i) d of $C(\alpha)$ and $C^2(\alpha)$ are integers,
- (ii) d of $B(\alpha)$ is an integer,
- (iii) d of $D(\alpha)$ is an integer.

Proof. (i) Let $\alpha = \frac{a + b\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$ such that $d = \frac{a^2 - 3b^2}{c} \in \mathbb{Z}$. Then $C(\alpha) = \frac{-a - d + b\sqrt{3}}{d}$, where $d_1 = 2a + c + d \in \mathbb{Z}$, and $C^2(\alpha) = \frac{-a - c + b\sqrt{3}}{2a + c + d}$, where $d_2 = c \in \mathbb{Z}$.

- (ii) Since $B(\alpha) = \frac{a - b\sqrt{3}}{d}$, the value of d of $B(\alpha)$ is $\frac{a^2 - 3b^2}{d} = c \in \mathbb{Z}$.

(iii) Also $D(\alpha) = \frac{a - b\sqrt{3}}{-d}$ implies that d of $D(\alpha)$ is $\frac{a^2 - 3b^2}{-d} = -c \in \mathbb{Z}$. ■

Remark 42 *The value of b is invariant for the elements of the form $\alpha = \frac{a + b\sqrt{3}}{c}$ in $\Gamma\alpha$, where $\alpha \in \mathbb{Q}(i, \sqrt{3})$.*

A closed path whose all vertices are ambiguous numbers is called the closed path of ambiguous numbers. Lemma 43, Theorem 44 and Theorem 46 show that there are finite number of ambiguous numbers in one orbit and they form a single closed path in the orbit. In this single closed path the value of b in $\frac{a + b\sqrt{3}}{c}$ remain invariant.

Lemma 43 *Ambiguous numbers in $\Gamma\alpha$ are finite.*

Proof. Let $\alpha = \frac{a + b\sqrt{3}}{c}$. It will be ambiguous when $\frac{a^2 - 3b^2}{c^2} < 0$ or $a^2 - 3b^2 < 0$ or $a^2 < 3b^2$. This shows that the values of a are finite which satisfy the condition $a^2 < 3b^2$ for constant value of b . By Remark 42, the value of b remain invariant for the numbers of the form $\frac{a + b\sqrt{3}}{c}$ in $\Gamma\alpha$, where $a, b, c \in \mathbb{Z}$. By Proposition 41, d is integer, this implies that c divides $(a^2 - 3b^2)$, so values of c are also finite. As values of a and c are finite and value of b is fixed in an orbit so ambiguous numbers of the form $\frac{a + b\sqrt{3}}{c}$ are also finite in an orbit. ■

Theorem 44 *In a coset diagram for $\Gamma\alpha$, where α is an ambiguous number, the ambiguous numbers form a closed path.*

Proof. If k_0 is an ambiguous number in $\Gamma\alpha$, then by Proposition 39, either $C(k_0)$ is ambiguous or $C^2(k_0)$. If $C(k_0)$ is ambiguous, then by Proposition 36, $BC(k_0)$ is

ambiguous. Each triangle with unbroken edges in the coset diagram for Γ contains two ambiguous numbers, so within the k^{th} triangle, the generators D or B are used to reach the next ambiguous number in the $(k+1)^{\text{th}}$ triangle and in m^{th} triangle respectively, as shown in Figure 22. Suppose the k^{th} triangle, contains two ambiguous numbers, namely α_1 and α_2 . Then $\alpha_1^k = D(\alpha_2^{k-1})$, $\alpha_1^{k+1} = D(\alpha_2^k)$,

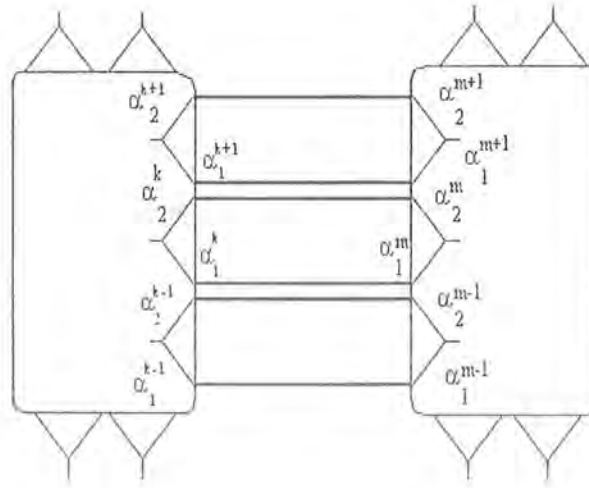


Figure 22

Also in m^{th} triangle $\alpha_1^m = D(\alpha_2^{m-1})$. As $(BD)^2 = 1$, this implies that $\alpha_2^{k-1} = B(\alpha_2^{m-1})$ and $\alpha_1^m = B(\alpha_1^k)$. We can continue in this way as shown in Figure 22 and since by Lemma 43, there are only a finite number of ambiguous numbers, therefore after a finite number of steps we reach the vertex, $\alpha_1^{k+n} = \alpha_1^{k-1}$. Hence ambiguous numbers form a closed path in the coset diagram. ■

Remark 45 The 3^{rd} vertex of the triangle whose two vertices are in the closed path

of ambiguous numbers of the form $\frac{a + b\sqrt{3}}{c}$, is not ambiguous and it has the form $\frac{a + b\sqrt{3}}{c}$.

Theorem 46 *If α is an ambiguous number, then in $\Gamma\alpha$ there is only one closed path of ambiguous numbers.*

Proof. In a diagram of A_4 there are four triangles with unbroken edges. So the diagram of A_4 in which $\alpha = \alpha_0$ is a vertex of one of the triangles with unbroken edges contains three more triangles with unbroken edges. According to Proposition 39, if α_0 is an ambiguous number, then one of $C(\alpha_0)$ and $C^2(\alpha_0)$ is also an ambiguous number. Let us denote this ambiguous number by α_1 . Then by Lemma 36, these two ambiguous numbers are joined with other ambiguous numbers by generators B and D . Therefore suppose $B(\alpha_0) = \alpha_2$, $B(\alpha_1) = \alpha_3$ and $D(\alpha_0) = \alpha_4$, $D(\alpha_1) = \alpha_5$.

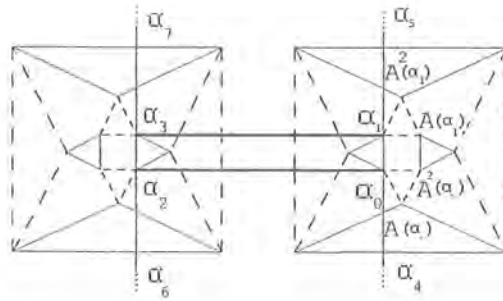


Figure 23

As the vertices of other three triangles with unbroken edges are also vertices of triangles with broken edges, according to Proposition 38, $A(\alpha_j)$ and $A^2(\alpha_j)$ are not

ambiguous numbers but they contain i , where $j = 0, 1$. By applying transformations C and C^2 on them, one gets not ambiguous numbers having i . So this diagram for A_4 contains only one triangle having two ambiguous numbers. If we expand this diagram and apply generators B and D on numbers which are not ambiguous, then by Lemma 37, no further ambiguous numbers are found. Since these numbers which are not ambiguous contain i , so by applying transformations C and C^2 on them, one gets numbers which are not ambiguous but contain i . According to Lemma 36 and Proposition 39, the generators B, C and D map α_0 and α_1 to other ambiguous numbers, namely, $\alpha_2, \alpha_3, \alpha_4, \dots, \alpha_n$, since they are finite according to Lemma 43. By Theorem 44 they form a closed path. As one cannot find any further ambiguous numbers from the numbers which are not ambiguous, this means that there is only one closed path of ambiguous numbers in $\Gamma\alpha_0$. ■

There are exactly two ambiguous numbers of the form $\frac{a + b\sqrt{3}}{c}$, where b remains invariant, in one diagram of A_4 . With respect to the form $\frac{a + b\sqrt{3}}{c}$, where b is constant, there may be more than one closed paths of ambiguous numbers but they lie in different orbits because one orbit contains only one closed path. For instance, with respect to the form $\frac{a + 4\sqrt{3}}{c}$, there are two closed paths of ambiguous numbers, one containing $\frac{4\sqrt{3}}{3}$ and the other containing $4\sqrt{3}$, as shown in figures below. But these two closed paths lie in different orbits.

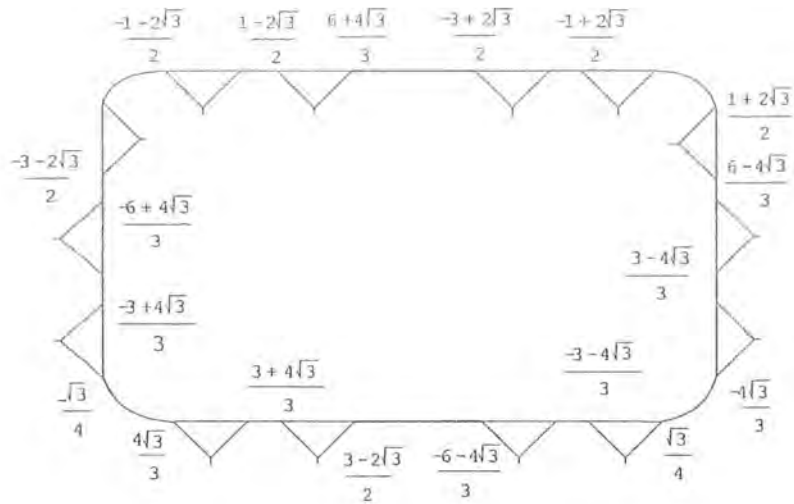


Figure 24

The closed path containing $4\sqrt{3}$ is shown in Figure 25.

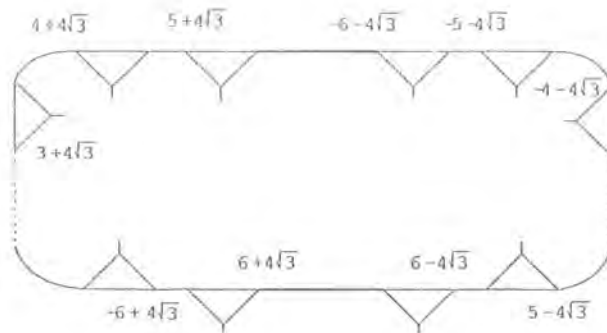


Figure 25

Theorem 47 If α is an ambiguous number of the form $\frac{a+k\sqrt{3}}{c} \in \mathbb{Q}(i, \sqrt{3})$, where $a, c \in \mathbb{Z}$ and k is a constant integer, then

(i) $a^2 < 3k^2$,

(ii) c is a divisor of $a^2 - 3k^2$.

Proof. (i) Let $\alpha = \frac{a + k\sqrt{3}}{c}$ be an ambiguous number. This means that $\alpha\bar{\alpha} < 0$ that is $\frac{a^2 - 3k^2}{c^2} < 0$. Since $c^2 > 0$, this implies that $a^2 - 3k^2 < 0$, which further implies that $a^2 < 3k^2$.

(ii) The ambiguous number in the closed path containing $k\sqrt{3}$ are of the form $\frac{a + k\sqrt{3}}{c}$. We know that d of $k\sqrt{3}$ is $-3k^2$. By Proposition 41, d of other ambiguous numbers in the closed path containing $k\sqrt{3}$ are also integer. We have $d = \frac{a^2 - 3k^2}{c}$, it will be integer if and only if c divides $a^2 - 3k^2$. This shows that c is the divisor of $a^2 - 3k^2$. ■

We denote the greatest common divisor of a, b and c by (a, b, c) , where $a, b, c \in \mathbb{Z}$.

If a divides b , then we denote it by $a \mid b$.

Proposition 48 Let $m \neq k$ is a factor of $k \in \mathbb{Z}^+$ and $(a, k, c) \neq 1$. If $\alpha = \frac{\acute{a} + m\sqrt{3}}{\acute{c}}$ such that $(\acute{a}, m, \acute{c}) = 1$ and $\acute{c} \mid \acute{a}^2 - 3m^2$, then ambiguous numbers of the form $\frac{a + m\sqrt{3}}{c}$ do not exist in the closed path of ambiguous numbers of the form $\frac{a + k\sqrt{3}}{c}$.

Proof. Let $m \neq k$ be a factor of k . Let $\alpha = \frac{a + k\sqrt{3}}{c}$ be an ambiguous number such that $(a, k, c) \neq 1$. This means that α can be written as $\frac{\acute{a} + m\sqrt{3}}{\acute{c}}$ such that $(\acute{a}, m, \acute{c}) = 1$. For $q \in \mathbb{Z}$ we have $\acute{a}q = a, \acute{c}q = c$ and $mq = k$. Since α is ambiguous number, this means that $\acute{a}^2 < 3m^2$ and $\acute{c} \mid \acute{a}^2 - 3m^2$. This means that α is an ambiguous number of the form $\frac{\acute{a} + m\sqrt{3}}{\acute{c}}$ and by Theorem 44, it forms a closed path of ambiguous numbers. By Remark 42, they are of the form $\frac{\acute{a} + m\sqrt{3}}{\acute{c}}$. By Theorem

46, it is the only closed path of ambiguous numbers of the form $\frac{\acute{a} + m\sqrt{3}}{\acute{c}}$ in an orbit. So if $m \neq k$, then in the closed path all ambiguous numbers will be of the form $\frac{a + m\sqrt{3}}{c}$. Hence the ambiguous numbers of forms $\frac{a + k\sqrt{3}}{c}$ and $\frac{a + m\sqrt{3}}{c}$ lie in different closed paths. ■

Remark 49 By Proposition 48, one can check whether an element of the form $\frac{a + k\sqrt{3}}{c}$, where $(a, k, c) \neq 1$, belongs to the closed path of ambiguous numbers of form $\frac{a + k\sqrt{3}}{c}$ or of the form $\frac{a + m\sqrt{3}}{c}$, where $m \neq k$ is a factor of k . Let $\alpha = \frac{a + k\sqrt{3}}{c}$ such that $(a, k, c) \neq 1$, then α can be written as $\frac{\acute{a} + m\sqrt{3}}{\acute{c}}$ such that $(\acute{a}, m, \acute{c}) = 1$, where m is a factor of k . If $\acute{c} \mid \acute{a}^2 - 3m^2$, then α is of the form $\frac{a + m\sqrt{3}}{c}$, otherwise $\frac{a + k\sqrt{3}}{c}$, in this case c should divide $a^2 - 3k^2$. In other words if $\alpha = \frac{a + k\sqrt{3}}{c}$ is in its simplest form and $c \mid a^2 - 3k^2$, then α occurs in the closed path of the form $\frac{a + k\sqrt{3}}{c}$.

Example 50 For $k = 2$. The prime decomposition of k is obviously $2 = 2 \times 1$. Therefore ambiguous numbers of the form $\frac{a + \sqrt{3}}{c}$ already exist in a closed path containing $\sqrt{3}$. So they will not exist in the closed path containing $2\sqrt{3}$. By using Theorem 47 and Proposition 48, it can be shown easily that the closed path containing $2\sqrt{3}$ has 32 ambiguous numbers. For $\alpha = \frac{a + 2\sqrt{3}}{c}$ to be ambiguous, $a^2 < 12$ which implies that $a = 0, \pm 1, \pm 2, \pm 3$. Let $d = \frac{a^2 - 12}{c}$. When $a = 0$, then $d = \frac{-12}{c}$ will be integer if and only if $c = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. When $a = 0$ and $c = 2$, then $\alpha = \frac{2\sqrt{3}}{2} = \sqrt{3}$. Since $\sqrt{3}$ already exist in the closed path of ambiguous numbers of the form $\frac{a + \sqrt{3}}{c}$, we discard $c = \pm 2$ and its cofactor ± 6 . Also when $c = 6$, then $\alpha = \frac{2\sqrt{3}}{6} = \frac{\sqrt{3}}{3}$ and 3

divides 3. This shows that α belongs to the closed path of the form $\frac{a + \sqrt{3}}{c}$, therefore we also discard the cofactor 6. Eventually, we have eight values of c , this means we have eight values of α .

When $a = \pm 1$, then $d = \frac{1 - 12}{c} = \frac{-11}{c}$, $d \in \mathbb{Z}$ if and only if $c = \pm 1, \pm 11$. So we have four values of c . When $a = 2$, $d = \frac{4 - 12}{c} = \frac{-8}{c}$, $d \in \mathbb{Z}$ if and only if $c = \pm 1, \pm 2, \pm 4, \pm 8$. When $a = \pm 2$ and $c = \pm 2$, $\alpha = \frac{\pm 2 \pm 2\sqrt{3}}{2} = \pm 1 \pm \sqrt{3}$ is of the form $\frac{a + \sqrt{3}}{c}$. So we discard 2 and 4 (its cofactor). When $a = \pm 3$, then $d = \frac{9 - 12}{c} = \frac{-3}{c}$ implies that $c = \pm 1, \pm 3$. Here we have twelve values of c for $a = \pm 1, \pm 2, \pm 3$. This means that there are 24 values of α because of the positive and negative values of a . Thus the total ambiguous numbers of the form $\frac{a + 2\sqrt{3}}{c}$ in an orbit of the coset diagram obtained by action of Γ on $\mathbb{Q}(i, \sqrt{3})$ are $24 + 8 = 32$.

A fragment of the coset diagram obtained by action of Γ on $\mathbb{Q}(i, \sqrt{3})$ containing closed path of ambiguous numbers of form $\frac{a + 2\sqrt{3}}{c}$, is shown below. In Figure 26, there are two layers of fragment $A - C - D$. These two layers are connected by bold edges. The distinction between two layers are the conjugates, that is, if $\alpha = \frac{a + 2\sqrt{3}}{c}$ occurs in one layer, then $\bar{\alpha} = \frac{a - 2\sqrt{3}}{c}$ occurs in the second layer. Thus there is a mapping, say S , from one layer to the other, defined by $S : \alpha \mapsto \bar{\alpha}$. It can be noted here that in each diagram of A_A , there are exactly two ambiguous numbers.

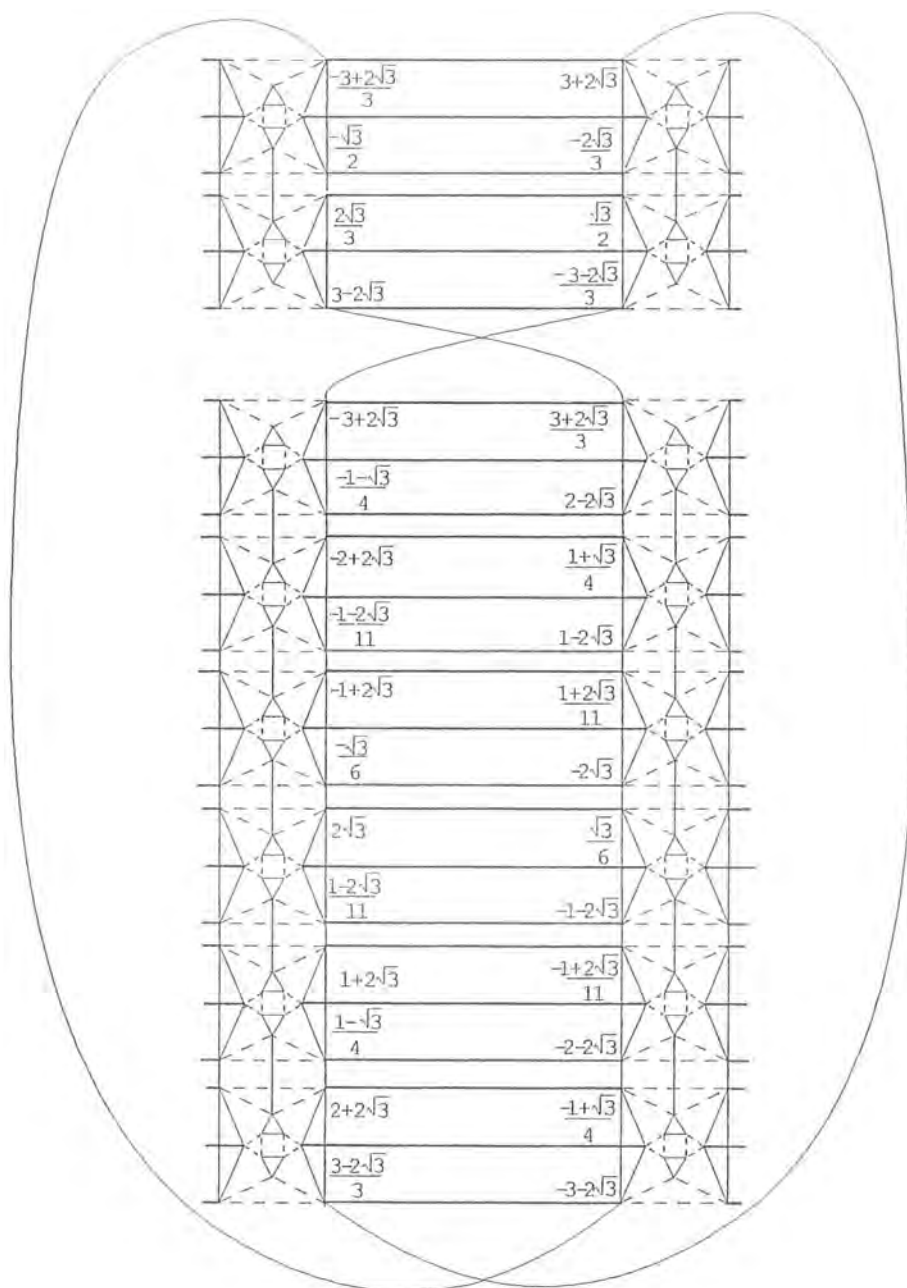


Figure 26

In the next diagram we have shown only the closed path of ambiguous numbers of the form $\frac{a + 2\sqrt{3}}{c}$ out of the fragment of Figure 26. In Figure 27, we apply repeatedly the

generators C, C^2 and D to obtain the ambiguous numbers in the path from $\frac{-3 - 2\sqrt{3}}{3}$ to $-3 + 2\sqrt{3}$ in one layer. The ambiguous numbers in the path from $\frac{3 + 2\sqrt{3}}{3}$ to $3 - 2\sqrt{3}$ are in second layer. These two layers are connected by bold edges. For instance, $-3 + 2\sqrt{3}$ and $\frac{3 + 2\sqrt{3}}{3}$ are connected by a bold edge as shown below.

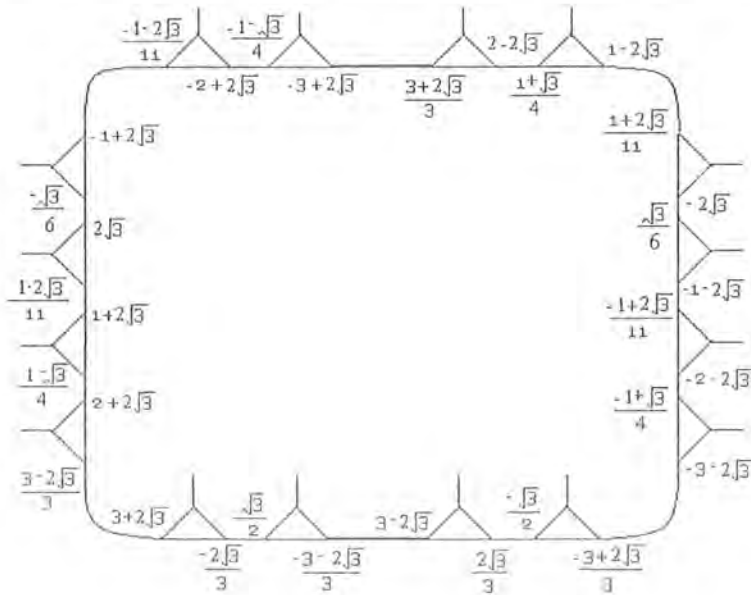


Figure 27

By choosing $a = 0$ and $c = 2$, we get $\alpha = \sqrt{3}$ which already exists in the closed path of ambiguous numbers of the form $\frac{a + \sqrt{3}}{c}$, as shown in Figure 28. This fragment also consists of two layers of fragment $A - C - D$, which are connected by bold edges. The distinction between two layers is because of the occurrence of α in one layer and its conjugate in the second layer.

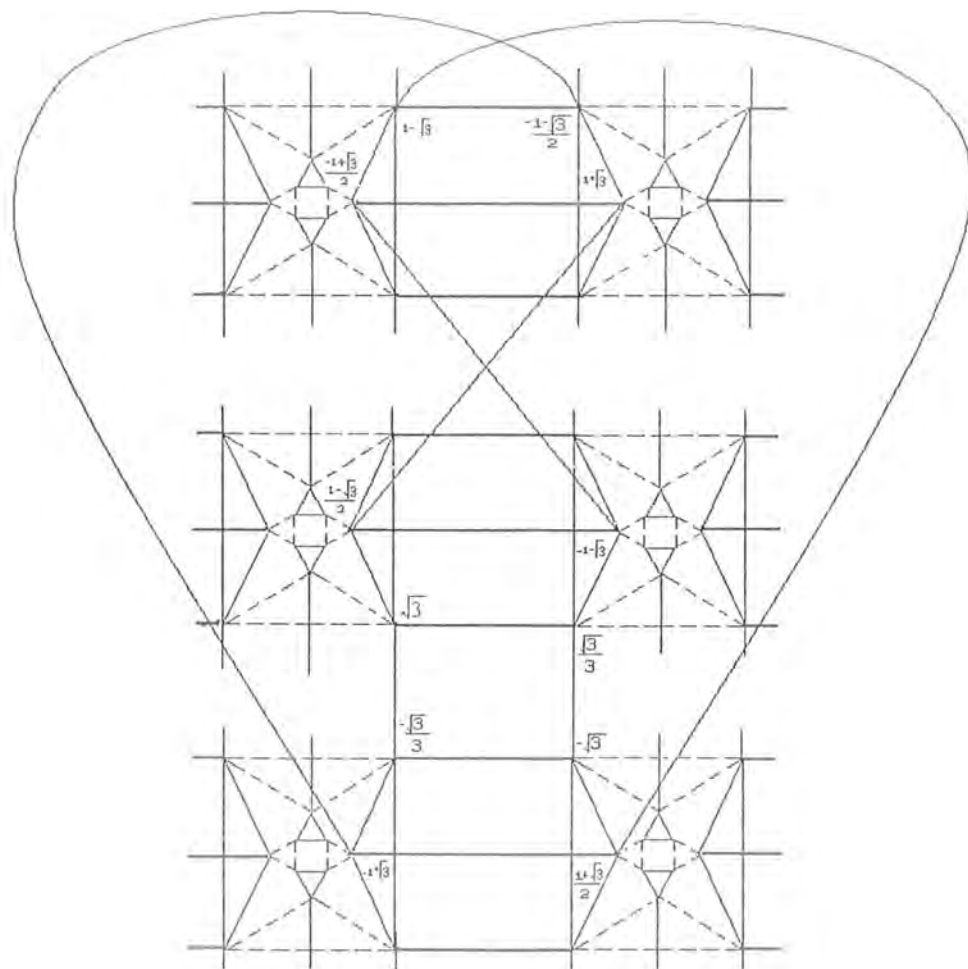


Figure 28

The closed path of ambiguous numbers $\frac{a + \sqrt{3}}{c}$ in Figure 28 can be seen clearly in Figure 29.

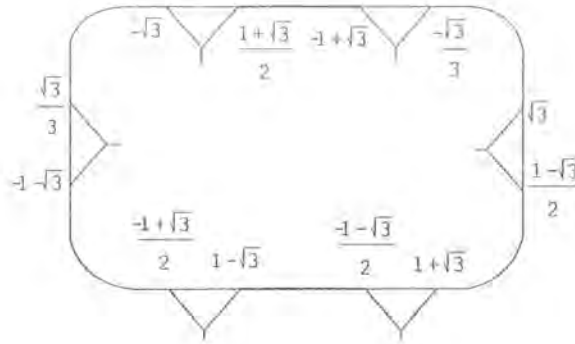


Figure 29

By Theorem 2, the algebraic integers of $\mathbb{Q}(i, \sqrt{3})$ are $\frac{1}{2}((a + bi) + (c + di)\sqrt{3})$, where $a \equiv d \pmod{2}$, $b \equiv c \pmod{2}$ and $a, b, c, d \in \mathbb{Z}$. In other words either a and d are both even or both odd. Also b and c are either both even or both odd.

Proposition 51 All ambiguous numbers of the form $\frac{a + k\sqrt{3}}{c}$ whose denominator is one are algebraic integers, where $(a, k, c) = 1$.

Proof. The ambiguous numbers in $\mathbb{Q}(i, \sqrt{3})$ are of the form $\frac{a + k\sqrt{3}}{c}$, where $a, c, k \in \mathbb{Z}$, or they can be written as $\frac{(a + 0i) + (k + 0i)\sqrt{3}}{c}$.

Obviously the coefficients of i and $i\sqrt{3}$ are even in $\alpha = \frac{(a + 0i) + (k + 0i)\sqrt{3}}{c}$. Now α will be algebraic integer when a and k are even and $c = 2$. Since a and k are even, the denominator becomes 1 after simplification. So α will be algebraic when α is of the form $a + k\sqrt{3}$, where $a, k \in \mathbb{Z}$. ■

Proposition 52 *The orbits which contain ambiguous numbers of the form $\frac{a + k\sqrt{3}}{c}$ also contain algebraic integers of the form $l + mi \pm k\sqrt{3}$ in $\mathbb{Q}(i, \sqrt{3})$, where $l, m \in \mathbb{Z}$, k is a constant positive integer.*

Proof. It has been proved in Proposition 51, that α is algebraic as well as ambiguous if it is of the form $a + k\sqrt{3}$, where $a \in \mathbb{Z}$, $a^2 < 3k^2$ and k is a constant positive integer. By applying $(CD)^n$ on α we get the series $l + k\sqrt{3}$, where $n, l \in \mathbb{Z}$. Further, applying $(A^2B)^n$ on α , we get the series $l + mi \pm k\sqrt{3}$, where $l, m \in \mathbb{Z}$ and k is a constant positive integer. ■

Proposition 53 (i) *If $\alpha = (a + bi) + (c + di)\sqrt{3}$, where $a, b, c, d \in \mathbb{Z}$, then $\Gamma\alpha$ have all the algebraic integers of the form $(l + mi) \pm (c \pm di)\sqrt{3}$, where $l, m \in \mathbb{Z}$ and c, d are constant positive integers.*

(ii) *If $\alpha = \frac{1}{2}\{(a + bi) + (c + di)\sqrt{3}\}$, where a, b, c, d are odd integers, then all the algebraic integers in $\Gamma\alpha$ are of the form $\frac{1}{2}\{(l + mi) \pm (c \pm di)\sqrt{3}\}$, where l, m are odd integers and c, d are constant odd positive integers.*

(iii) *If $\alpha = \frac{1}{2}\{(a + bi) + (c + di)\sqrt{3}\}$, where a and d are even (odd) integers and b, c are odd (even) integers, then $\Gamma\alpha$ have all the algebraic integers of the form $\frac{1}{2}\{(l + mi) \pm (c \pm di)\sqrt{3}\}$, where l is even (odd) integer and m is odd (even) integer.*

Proof. (i) By applying transformations $(CD)^n$ and $(A^2B)^n$ on $\alpha = (a + bi) + (c + di)\sqrt{3}$, we get the series $(l + mi) \pm (c \pm di)\sqrt{3}$, where $n, l, m \in \mathbb{Z}$ and c, d are

constant integers. The values of c or d can not be changed because Γ consists of only those linear fractional transformations whose coefficients are from $\mathbb{Z}[i]$. Hence values of c and d are constant.

(ii) If α is of the form $\frac{1}{2}\{(a+bi)+(c+di)\sqrt{3}\}$, where a, b, c, d are odd integers, then by applying transformations $(CD)^n$ and $(A^2B)^n$, where $n \in \mathbb{Z}$, on α , we get the series $\frac{1}{2}\{(l+mi) \pm (c \pm di)\sqrt{3}\}$, where l, m are odd integers and c, d are constant odd integers.

(iii) Let $\alpha = \frac{1}{2}\{(a+bi)+(c+di)\sqrt{3}\}$, where a, d are even(odd) integers and b, c are odd(even) integers. By applying transformations $(CD)^n$ and $(A^2B)^n$, $n \in \mathbb{Z}$ on α , we get the series $\frac{1}{2}\{(l+mi) \pm (c \pm di)\sqrt{3}\}$, where l is even(odd), m is odd(even), c is constant odd(even) and d is constant even(odd) integers. ■

Corollary 54 *If α is an algebraic integer in $\mathbb{Q}(i, \sqrt{3})$, then $\Gamma\alpha$ contains all its conjugates over \mathbb{Q} .*

Proof. Let $\alpha = \frac{1}{2}\{(a+bi)+(c+di)\sqrt{3}\}$, where $a \equiv d \pmod{2}$, $b \equiv c \pmod{2}$. By applying transformations $(CD)^n$, $(DC^2)^n$, $(A^2B)^n$ and $(BA)^n$ on α , where $n \in \mathbb{Z}^+$, we get algebraic integers $\frac{1}{2}\{(l+mi) \pm (c \pm di)\sqrt{3}\}$, where $l, m \in \mathbb{Z}$ and $l \equiv d \pmod{2}$ and $m \equiv c \pmod{2}$, which contain $\frac{1}{2}\{(a-bi)+(c-di)\sqrt{3}\}$, $\frac{1}{2}\{(a+bi)-(c-di)\sqrt{3}\}$ and $\frac{1}{2}\{(a-bi)-(c+di)\sqrt{3}\}$. ■

Proposition 55 *There are infinite number of orbits containing integers of $\mathbb{Q}(i, \sqrt{3})$.*

Proof. If $\alpha = \frac{1}{2}\{(a+bi)+(c+di)\sqrt{3}\}$, where $a \equiv d \pmod{2}$, $b \equiv c \pmod{2}$,

then by Proposition 53, $\Gamma\alpha$ contains algebraic integers of the form $\frac{1}{2}\{(l + mi) \pm (c \pm di)\sqrt{3}\}$, where $l \equiv d \pmod{2}$, $m \equiv c \pmod{2}$ and c, d are constant integers.

Thus by varying values of c and d where $c, d \in \mathbb{Z}$, we can get infinite number of orbits containing algebraic integers of $\mathbb{Q}(i, \sqrt{3})$. Also from Proposition 53, $(a + bi) + (c + di)\sqrt{3}$, where $a, b, c, d \in \mathbb{Z}$, $\frac{1}{2}\{(a + bi) + (c + di)\sqrt{3}\}$, where a, b, c, d are odd integers, and $\frac{1}{2}\{(a + bi) + (c + di)\sqrt{3}\}$, where a and d are even (odd) integers and b, c are odd(even) integers, belong to different orbits. ■

Theorem 56 *Action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is intransitive.*

Proof. In Theorem 34, it has been proved that action of Γ on $\mathbb{Q}(i)$ is transitive. So there are at least two orbits by the action of Γ on $\mathbb{Q}(i, \sqrt{3})$. One orbit is $\mathbb{Q}(i)$ and the other is $\mathbb{Q}(i, \sqrt{3}) \setminus \mathbb{Q}(i)$. This shows that action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is intransitive. ■

Theorem 57 *Action of Γ on $\mathbb{Q}(i, \sqrt{n})$ is intransitive, where $n > 1$ is a square-free integer.*

Proof. In Theorem 34, it has been proved that action of Γ on $\mathbb{Q}(i)$ is transitive. So one orbit is $\mathbb{Q}(i)$ and other is $\mathbb{Q}(i, \sqrt{n}) \setminus \mathbb{Q}(i)$, where $n > 1$ is a square-free integer. This shows that action of Γ on $\mathbb{Q}(i, \sqrt{n})$ is intransitive. ■

Proposition 58 *The fixed points of a linear fractional transformation $T(z) = \frac{az + b}{cz + d}$ where $a, b, c, d \in \mathbb{Z}[i]$, are algebraic integers when $\frac{d - a}{c}$ and $\frac{b}{c} \in \mathbb{Z}$.*

Proof. Let $k \in \mathbb{C}$ be a fixed point of a linear fractional transformation $T \in \Gamma_\tau$, that is, $T(k) = k$, where $T(z) = \frac{az+b}{cz+d}$, $a, b, c, d \in \mathbb{Z}[i]$. This implies that $ck^2 + (d-a)k - b = 0$, or $k^2 + (\frac{d-a}{c})k - \frac{b}{c} = 0$. If $\frac{d-a}{c}$ and $\frac{b}{c} \in \mathbb{Z}$, then the roots are algebraic integers. \blacksquare

The fixed points of the generators A, B, C and D of Γ are algebraic integers. If α and $\bar{\alpha}$ are conjugates, then $T(\alpha)$ and $T(\bar{\alpha})$ are also conjugates, where T is a linear fractional transformation. This means the diagram formed by applying elements of Γ on α is same as the diagram formed by applying the same elements of Γ on $\bar{\alpha}$. We denote the latter diagram as "conjugate diagram". If an edge joins two vertices of a triangle, then we denote this edge by a "cap".

Proposition 59 *The fragment of the coset diagram containing the fixed points of generators A and C have four vertices and all of them are algebraic integers.*

Proof. The fixed points of generators A and C are $\frac{i \pm \sqrt{3}}{2}$ and $\frac{-1 \pm \sqrt{3}i}{2}$ respectively, which are of course the algebraic integers of $\mathbb{Q}(i, \sqrt{3})$.

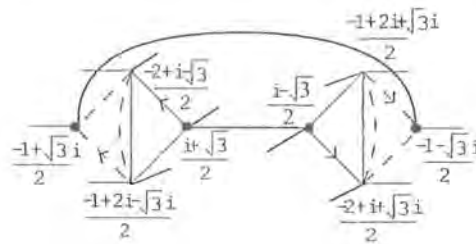


Figure 30

First, consider a fragment of the coset diagram which contains $\frac{i + \sqrt{3}}{2}$. By applying

generator C on $\frac{i + \sqrt{3}}{2}$, we get $\frac{-2 + i - \sqrt{3}}{2}$ and $C^2\left(\frac{i + \sqrt{3}}{2}\right) = \frac{-1 + 2i - \sqrt{3}i}{2}$.

Also, by applying generator A on above values, that is,

$$A\left(\frac{-2 + i - \sqrt{3}}{2}\right) = \frac{-1 + 2i - \sqrt{3}i}{2} \text{ and } A^2\left(\frac{-2 + i - \sqrt{3}}{2}\right) = \frac{-1 + \sqrt{3}i}{2}, \text{ which}$$

is the fixed point of C . Further applications of A and C on these values give the same

elements. This means that we get only four elements of $\mathbb{Q}(i, \sqrt{3})$ in the diagram

containing the fixed points of A and C , namely, $\frac{i + \sqrt{3}}{2}$ and $\frac{-1 + \sqrt{3}i}{2}$. So the Cay-

ley's diagram of A_4 is reduced to a diagram having four vertices because of the fixed

points of A and C . As $D\left(\frac{i + \sqrt{3}}{2}\right) = \frac{i - \sqrt{3}}{2}$ is conjugate of $\frac{i + \sqrt{3}}{2}$, so the diagram

formed by applying generators A and C on $\frac{i - \sqrt{3}}{2}$ is conjugate diagram. It is same

to the diagram formed by applying generators A and C on $\frac{i + \sqrt{3}}{2}$ because if α and $\bar{\alpha}$

are conjugates, then $T(\alpha)$ and $T(\bar{\alpha})$ are also conjugates, where T is a linear fractional

transformation. Similarly, it can be proved that the conjugate diagram containing

$\frac{i - \sqrt{3}}{2}$ and $\frac{-1 - \sqrt{3}i}{2}$ also contains four elements as shown in Figure 30. ■

Proposition 60 *The triangles in diagram of S_3 , generated by A and D , in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$, have the same number of algebraic integers.*

Proof. Let α be an algebraic integer of $\mathbb{Q}(i, \sqrt{3})$. By Theorem 2, $\alpha = \frac{1}{2}((a + bi) + (c + di)\sqrt{3})$ where $a \equiv d \pmod{2}$, $b \equiv c \pmod{2}$. By applying transformation DA on α , we get $DA(\alpha) = -\alpha + i = \frac{1}{2}\{-a - (b - 2)i - (c + di)\sqrt{3}\}$, where $b - 2 \equiv c \pmod{2}$ since $b \equiv c \pmod{2}$. This means that $DA(\alpha)$ is again an algebraic integer. So if α is a vertex of a triangle having broken edges, then the application of transformation DA

on α yields an algebraic integer β in another triangle having broken edges such that $DA(\alpha) = \beta$.

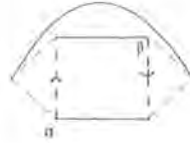


Figure 31

These two triangles are joined by three edges which represent generator D . Hence, if all the three vertices of a triangle with broken edges are labelled by algebraic integers, then the triangle joined with this triangle by edges also contain three algebraic integers. ■

Proposition 61 *The triangles in diagram of S_3 , generated by B and C , in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$, have the same number of algebraic integers.*

Proof. Let $\alpha \in \mathbb{Q}(i, \sqrt{3})$ be an algebraic integer. By Theorem 2, $\alpha = \frac{1}{2}((a + bi) + (c + di)\sqrt{3})$, where $a \equiv d \pmod{2}$, $b \equiv c \pmod{2}$. Now $CB(\alpha) = C(B(\alpha)) = -1 - \alpha = \frac{1}{2}\{-(2 + a) - bi - (c + di)\sqrt{3}\}$. Then $a + 2 \equiv d \pmod{2}$ since $a \equiv d \pmod{2}$. This implies that $CB(\alpha)$ is also an algebraic integer. Similarly, for other vertices of the triangle with unbroken edges, that is, if all the three vertices of a triangle with unbroken edges are labelled by algebraic integers, then the triangle with unbroken edges joined with this triangle by bold edges, also labelled by three algebraic integers.

■

Proposition 62 *There are exactly four diagrams of A_4 , which contains six algebraic integers in each diagram, in the orbit containing fixed points of A and C .*

Proof. It is clear from Proposition 59 and Figure 30 that one portion of the diagram containing the fixed points of generators A and C contains four vertices or two triangles, one having broken edges and the other having unbroken edges. Each of the triangles is labelled by three algebraic integers. By Proposition 60, the three algebraic integers of the triangle having broken edges are mapped to the triangle having broken edges of another diagram of A_4 by edges, whose vertices are also labelled by algebraic integers. By Proposition 61, the three algebraic integers of the triangle having unbroken edges are mapped to the triangle having unbroken edges of another diagram of A_4 by bold edges, whose vertices are also labelled by algebraic integers. Since CA maps an algebraic integer to an algebraic integer, so there are six algebraic integers in a diagram of A_4 . Consider the same argument for another fragment having the fixed points of A and C . So this fragment is connected to two other diagrams of A_4 having six algebraic integers. So, in total there are four diagrams of A_4 which contain six algebraic integers. ■

Remark 63 *The fragment of a coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ whose all vertices are labelled by algebraic integers.*

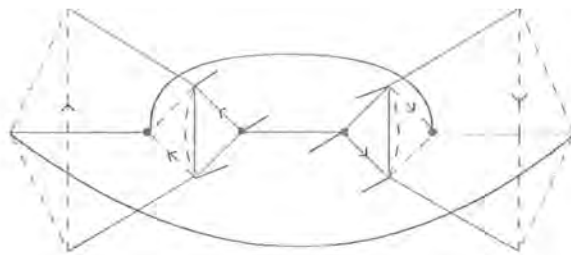


Figure 32

Proposition 64 *If a triangle in a diagram of S_3 does not have any algebraic integers, then the other triangle joined with it by edges does not have any algebraic integers.*

Proof. Let α, β and γ be vertices of a triangle having broken edges representing three cycles of generator A and they be not algebraic integers, where $\alpha, \beta, \gamma \in \mathbb{Q}(i, \sqrt{3})$. Let $\alpha = \frac{1}{e} \{(a + bi) + (c + di) \sqrt{3}\}$, where $a \not\equiv d \pmod{2}$ or $b \not\equiv c \pmod{2}$.

Let $a \not\equiv d \pmod{2}$, $b \equiv c \pmod{2}$ and $e = 2$. Then $DA(\alpha) = \frac{1}{2} \{(-a - (b - 2)i) - (c + di) \sqrt{3}\}$. Since $a \not\equiv d \pmod{2}$, so $DA(\alpha)$ is not an algebraic integer. Let $a \equiv d \pmod{2}$, $b \not\equiv c \pmod{2}$ and $e = 2$. Then $(b - 2) \not\equiv c \pmod{2}$. So $DA(\alpha)$ is not an algebraic integer. Similarly, β_2 and γ_2 are not algebraic integers. ■

Theorem 65 *The algebraic integers in the orbit containing the fixed points of A and C are of the form $\left\{ \frac{(\pm k \pm li) \pm \sqrt{3}i}{2} : k \text{ is odd integer, } l \text{ is even integer} \right\}$ and $\left\{ \frac{(\pm k \pm li) \pm \sqrt{3}}{2} : k \text{ is even and } l \text{ is odd integer} \right\}$.*

Proof. The Fixed points of A and C are $\frac{i \pm \sqrt{3}}{2}$ and $\frac{-1 \pm \sqrt{3}i}{2}$ respectively. By applying CD and DC^2 repeatedly on $\frac{i \pm \sqrt{3}}{2}$, we get the series $\frac{\pm k + i \pm \sqrt{3}}{2}$ such

that k is even. By applying A^2B or BA on $\frac{i \pm \sqrt{3}}{2}$, we get $\frac{li \pm \sqrt{3}}{2}$ such that l is odd. So we get the series $\frac{\pm k \pm li \pm \sqrt{3}}{2}$, where k is even and l is odd integer. By applying CD and DC^2 repeatedly on $\frac{-1 \pm \sqrt{3}i}{2}$, we get $\frac{\pm k \mp \sqrt{3}i}{2}$ where k is odd. By applying A^2B or BA on $\frac{-1 \pm \sqrt{3}i}{2}$, we get $\frac{-1 \pm li \pm \sqrt{3}i}{2}$ such that l is even. By combining above two forms we get the series $\frac{\pm k \pm li \pm \sqrt{3}i}{2}$, where k is odd and l is even integer. ■

Proposition 66 *In a diagram of A_4 , algebraic integers are present in pairs.*

Proof. If $\alpha = \frac{(a + bi) + (c + di)\sqrt{3}}{2}$ is an algebraic integer, where $a \equiv d \pmod{2}$, $b \equiv c \pmod{2}$, then $CA(\alpha) = -1 + i - \alpha = \frac{\{-(2 + a) + (2 - b)i\} - (c + di)\sqrt{3}}{2}$. Since $d \equiv a + 2 \pmod{2}$ and $c \equiv 2 - b \pmod{2}$, therefore $CA(\alpha)$ is also an algebraic integer. ■

Proposition 67 *If there is one diagram of A_4 having two algebraic integers, then there are infinite diagrams of A_4 having two algebraic integers in an orbit.*

Proof. Suppose α, β exist in a diagram of A_4 , where α, β are algebraic integers. Then $CA(\alpha) = \beta$ or $CA(\beta) = \alpha$, where α is a vertex of a triangle representing three cycles of A as well as a vertex of a triangle representing three cycles of C . Thus, by Propositions 60 and 61, we get two different diagrams of A_4 each containing one algebraic integer. Application of transformation CA gives another algebraic integer in the same diagram of A_4 . By applying DA and BC on β we get two more diagrams of A_4 each containing one algebraic integer and by the transformation CA , we get

another algebraic integer in the same diagram of A_4 . In the same way by applying transformations DA , BC and CA on other diagrams of A_4 which contain algebraic integers, we get infinite diagrams of A_4 which have two algebraic integers in them. ■

Proposition 68 *The fragment of the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$, containing fixed points of the generators B and D has six vertices and four of them are algebraic integers.*

Proof. The fixed points of generators B and D are ± 1 and $\pm i$ respectively which lie in the orbit $\mathbb{Q}(i)$ of $\mathbb{Q}(i, \sqrt{3})$. The diagram containing the fixed points of both generators B and D , that is, -1 and i , have six vertices in total. Starting from -1 and applying transformations C and C^2 , that is, $C(-1) = 0$ and $C^2(-1) = \infty$. Now by considering i , $C(i) = (-1+i)$ and $C^2(i) = \frac{-1+i}{2}$. Also $A(-1+i) = -1$ and $A^2(-1+i) = \frac{-1+i}{2}$. We have $A(0) = i$ and $A^2(0) = \infty$.

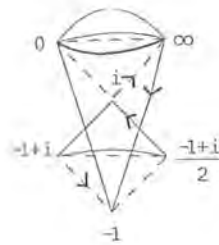


Figure 33

So we get six vertices in total and $0, -1, -1+i$ and i are algebraic integers. ■

Proposition 69 *There are three diagrams of A_4 , in the orbit containing fixed points of generators B and D , which contain four algebraic integers.*

Proof. By Proposition 68, the fragment containing fixed points of both generators B and D have four algebraic integers, namely $0, -1, -1 + i$ and i . Each triangle with unbroken edges contains two algebraic integers as shown in Figure 33. These two triangles are joined with two more diagrams of A_4 by bold edges, so in total we have three diagrams of A_4 . By Proposition 61, each triangles of other diagrams of A_4 which are joined by bold edges, also have two algebraic integers. Since the transformation CA maps an algebraic integer to an algebraic integer, so both of the diagrams of A_4 contain four algebraic integers. ■

We conclude this section with the following observations for the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$. The ambiguous numbers of the form $\frac{a + b\sqrt{3}}{c}$ make a closed path and it is the only closed path of ambiguous numbers in the orbit. These elements exist in two layers, in each layer they are connected by the generators D and C . The two layers are connected by the generator B . The orbit which contains ambiguous numbers also contains algebraic integers. The behaviour of ambiguous numbers as well as algebraic integers show that the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is intransitive.

3.1 Tessellations of Picard group

Let $H^3 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_3 > 0\}$ be the upper half space equipped with the hyperbolic metric ρ which is derived from the line element $ds = \frac{|dx|}{x_3}$, where $x = (x_1, x_2, x_3)$. With this metric, (H^3, ρ) becomes a model for hyperbolic 3-space. In terms of quaternions \mathbb{H} , $H^3 = \{z \in \mathbb{H} : z = x_1 + x_2i + x_3j, x_3 > 0\}$, where $i^2 = j^2 = -1$ and $ij + ji = 0$. Let $\mathbb{Q}(i) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$.

The Picard group Γ acts on H^3 by its generators defined by $a(z) = \frac{-1}{z}$, $t(z) = z + 1$, $u(z) = z + i$, and $l(z) = izi$. The fundamental domain F for Γ is $\{z = x + yi + rj \in H^3 : |x| \leq \frac{1}{2}, 0 \leq y \leq \frac{1}{2} \text{ and } (x^2 + y^2 + r^2)^{\frac{1}{2}} \geq 1\}$. When we act Γ on F , its images cover the entire space. For every $z \in H^3$, there is a $\gamma \in \Gamma$ such that $\gamma(z) \in F$. Moreover, if z and w lie in the interior of F and $z = \gamma(w)$ for $\gamma \in \Gamma$, then $\gamma = \pm I$, where I is the identity element of Γ . We have divided F into four parts by choosing two colours, that is, black and grey to visualize a pattern in H^3 . We have taken any point from H^3 and then applied generators of Γ on it. By this application that point transformed within F . As F is divided into coloured regions so we have given colour to that point according to its location in F . By applying the same procedure for different points we get the whole figure. This action can be visualize in Figures 34 and 36 below, which is output of a program developed in Matlab.

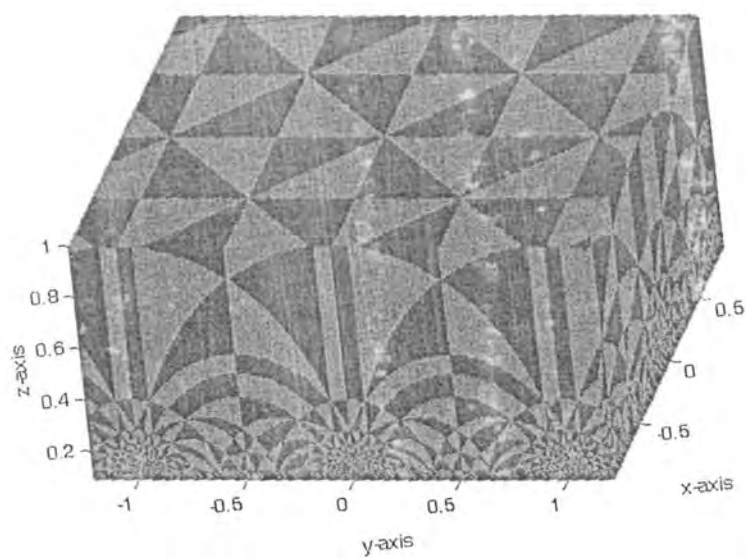


Figure 34

The above figure is for $-0.92 \leq x \leq 0.92$, $-1.2 \leq y \leq 1.2$ and $0.1 \leq r \leq 1$.
 Another cross section of the tessellation of Γ in H^3 is for $-0.92 \leq x \leq 0.92$, $-1.2 \leq y \leq 1.2$ and $0.1 \leq r \leq 0.5$ is given below.

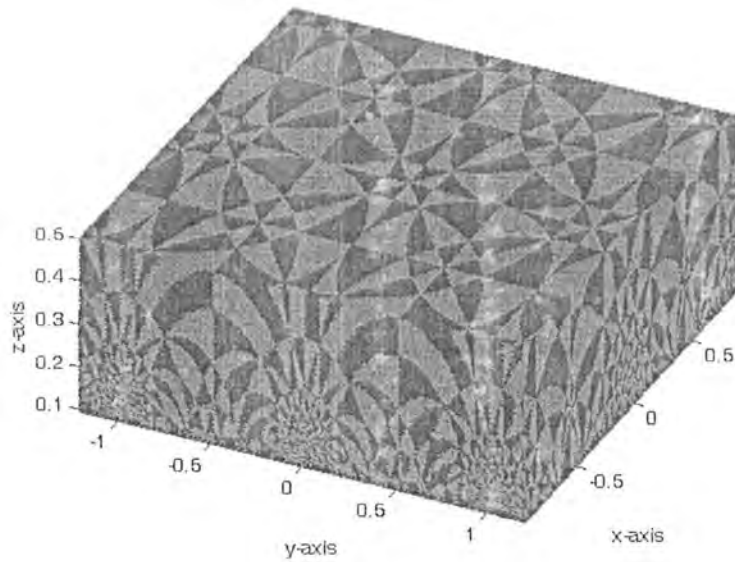


Figure 35

Primarily this program is written for the Picard group but after some minor modifications, it can be used to find tessellations of other groups in H^3 .

Γ also acts on $\mathbb{Q}(i)$. We have defined a mapping $\phi : \mathbb{Q}(i) \rightarrow Y$ by

$$\phi(x + yi) = x + yi + j,$$

where $Y = \{x + yi + j \in H^3 : x, y \in \mathbb{Q}\}$. Clearly ϕ is bijection from $\mathbb{Q}(i)$ to $Y \subset H^3$.

The figure below, shows the image of $\mathbb{Q}(i)$, which is developed by Matlab.

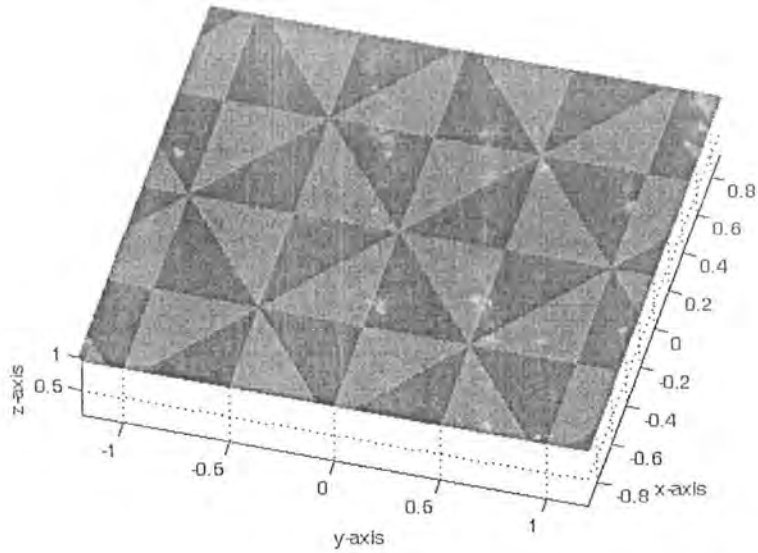


Figure 36

In other words if we take $D = \{z = x + yi + j \in H^3 : x, y \in \mathbb{Q}, |x| \leq \frac{1}{2}, 0 \leq y \leq \frac{1}{2}$ and $(x^2 + y^2 + r^2)^{\frac{1}{2}} \geq 1\}$ as a subset of fundamental domain then by the action of the generators t, u and l on D we get a plane Y . Ofcourse by taking any $r \in \mathbb{Q}$ we can define a bijection mapping from $\mathbb{Q}(i)$ to Y , but for an action of Γ we have to take $r > \frac{1}{\sqrt{2}}$. Since it is the smallest value of r to satisfy $(x^2 + y^2 + r^2)^{\frac{1}{2}} \geq 1$.

Similarly, we can define a bijective mapping from $\mathbb{Q}(i, \sqrt{3})$ to $X = \{u + vi + j \in H^3 : u, v \in \mathbb{Q}(\sqrt{3})\}$ by

$$\psi(u + vi) = u + vi + j.$$

Again the figure formed for the action of Γ on $\{z = u + ui + j \in H^3 : x, y \in \mathbb{Q}(\sqrt{3}), |u| \leq \frac{1}{2}, 0 \leq v \leq \frac{1}{2}$ and $|z| \geq 1\}$ by this bijection is a plane X having the same pattern as shown in Figure 36.

Program

This program has been developed in Matlab. This program gives the tessellation of the Picard group on H^3 .

```
clear all

i=1;

j=1;

k=1;

l=1;

count=1;

while count<=3

    if (count==1)

        rmin=1;

        xmin=-0.92;

        xmax=0.92;

        ymin=-1.2;

    end

    if (count==2)

        rmin=0.1;

        xmin=-0.92;

        xmax=-0.92;

        ymin=-1.2;
```

```
end

if (count==3)
    rmin=0.1;
    xmin=-0.92;
    xmax=0.92;
    ymin=1.2;
end

x0=xmin;

while x0<=xmax
    y0=ymin;
    while y0<=1.2
        r0=rmin;
        while r0<=1
            x=x0;
            y=y0;
            r=r0;
            zmod= (x.^2)+(y.^2)+(r.^2);
            while ((abs(x)>0.5) | (abs(y)>0.5)| (zmod<1))
                if (x<-0.5)
                    x=x+1;
                elseif (x>0.5)
```

```
        x=x-1;
    end
    if (y<-0.5)
        y=y+1;
    elseif (y>0.5)
        y=y-1;
    end
    zmod= (x.^2)+(y.^2)+(r.^2);
    if(zmod<1)
        x=-x./zmod;
        y=y./zmod;
        r=r./zmod;
        zmod= (x.^2)+(y.^2)+(r.^2);
    end
end % while
if (y<0)
    x=-x;
    y=-y;
end
if ((x>=(-0.5)) & (x < 0))
    if (y <=(-x))
```

```
X3(1,k)=x0;  
Y3(1,k) = y0;  
R3(1,k)=r0;  
k=k+1;  
else  
X4(1,l)=x0;  
Y4(1,l)=y0;  
R4(1,l)=r0;  
l=l+1;  
end  
else  
if(y < x)  
X1(1,i)=x0;  
Y1(1,i)=y0;  
R1(1,i)=r0;  
i=i+1;  
else  
X2(1,j) = x0;  
Y2(1,j) = y0;  
R2(1,j)=r0;  
j=j+1;
```

```
        end
    end
    r0=r0+0.02;
end % while
y0=y0+0.01;
end % while
x0=x0+0.01;
end % while
count=count+1;
end % while
plot(X1,Y1,R1,'r',X2,Y2,R2,'b',X3,Y3,R3,'b',X4,Y4,R4,'r');
grid on
xlim([-0.92 0.92])
ylim([-1.2 1.2])
zlim([0.1 1])
campos([7.684 -4.568 -6.06])
```

Chapter 4

Closed Paths of Ambiguous Numbers

Coset diagrams for the orbit of Γ in biquadratic field $\mathbb{Q}(i, \sqrt{3})$ give some interesting information. In chapter 3, it has been shown that ambiguous numbers of the form $\frac{a + b\sqrt{3}}{c}$ make a single closed path and it is the only closed path in the orbit $\Gamma\alpha$, where α is ambiguous. In this chapter we have classified these closed paths. We have found the types of these closed paths and the linear fractional transformations associated with them. We have observed that there are three types of closed paths that may occur in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$. They are:

- (i) closed paths which contain ambiguous numbers α with their conjugates $\bar{\alpha}$,
- (ii) closed paths which contain ambiguous numbers α with the ambiguous numbers $\frac{1}{\alpha}$, and

(iii) closed paths which contain ambiguous numbers α with the ambiguous numbers $\frac{1}{\bar{\alpha}}$.

First notice that there is a mapping from $\mathbb{Q}(i, \sqrt{3}) \cup \{\infty\}$ onto $F_p \cup \{\infty\}$, where $p-1$ and 3 are squares in F_p . By this mapping $\alpha = \frac{(a+bi) + (c+di)\sqrt{3}}{e} \in \mathbb{Q}(i, \sqrt{3})$ in its lowest terms is mapped on to $\frac{\{(a+bi) + (c+di)\sqrt{3}\} \pmod{p}}{e \pmod{p}}$. If $3 \equiv n^2 \pmod{p}$, then $3 \equiv (p-n)^2 \pmod{p}$. Also, if $p-1 \equiv m^2 \pmod{p}$, then $p-1 \equiv (p-m)^2 \pmod{p}$. Thus there are four mappings from $\mathbb{Q}(i, \sqrt{3}) \cup \{\infty\}$ onto $F_p \cup \{\infty\}$. If $g : z \rightarrow \frac{az+b}{cz+d}$ is any element of Γ , then g can be taken to act on $F_p \cup \{\infty\}$ by $z \rightarrow \frac{[a]z + [b]}{[c]z + [d]}$ (where $[a], [b], [c]$ and $[d]$ are residues modulo p of a, b, c and d respectively) and the mapping commutes with the action of Γ . Thus the coset diagram for the action of Γ on $F_p \cup \{\infty\}$ is obtained from the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3}) \cup \{\infty\}$ by identifying appropriate points.

In this chapter, we have found conditions under which the closed paths of the types (i), (ii) and (iii) exist in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ or for the action of Γ on a projective line over a finite field F_p , where p is a prime number.

Theorem 70 *Every element of Γ has real quadratic irrational numbers as fixed points, except: (i) the elements of order 2 and 3, (ii) the elements which are conjugates of $(DC^2)^n$ and $(A^2B)^n$, and (iii) the elements whose trace is qi in matrix form.*

Proof. Let $g : z \mapsto \frac{az+b}{cz+d} \in \Gamma$ and k be a fixed point of g . Then $ck^2 + (d-a)k - b = 0$ has real roots only when $(d-a)^2 + 4bc \geq 0$. But $(d-a)^2 + 4bc = a^2 + d^2 - 2ad + 4bc$. Since $ad - bc = 1$, therefore $bc = ad - 1$. That is, the discriminant becomes

$a^2 + d^2 - 2ad + 4ad - 4 = (a + d)^2 - 4 \geq 0$, where $a + d$ is the trace of the matrix corresponding to g . If the roots are complex, then $(a + d)^2 < 4$, that is, when $(a + d) = 0$ or 1 or qi , where $q \neq 0 \in \mathbb{Z}$.

(i) If $a + d = 0$, then g will take the form $z \mapsto \frac{az + b}{cz + d}$ and so $g^2 = 1$.

If $a + d = \pm 1$, then we can replace a, b, c, d by $-a, -b, -c$ and $-d$ in g . So we can assume that $a + d = -1$. This means that the matrix $M(g) = \begin{pmatrix} a & b \\ c & -a - 1 \end{pmatrix}$ for g gives $M^2 + M + I = 0$ as its characteristic equation, which yields $M^3 - I = 0$. This implies that $g : z \mapsto \frac{az + b}{cz - (a + 1)}$ has order 3.

If $a + d = \pm m > 2$, then $(a + d)^2 - 4 > 0$ and so the roots are real. In fact $(d - a)^2 + 4bc$ is a perfect square when $d - a = 0$ and $b = c = 1$. Therefore the only possibility for $ad - bc = \pm 1$ is that $a = d = 0$. Hence $M(g) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which is transformation B .

(ii) If $a + d = \pm 2$. Then g is parabolic element since $tr^2(g) = 4$ and is of the form $az + b$ and is conjugate to $(DC^2)^n : z \mapsto z + n$ or $(A^2B)^n : z \mapsto z + ni$, for some positive integer n . This implies that ∞ is the only fixed point of g

(iii) If $a + d = qi$, $q \neq 0 \in \mathbb{Z}$, then $(a + d)^2 - 4 = -q^2 - 4 < 0$.

Thus $(d+a)^2 - 4$ cannot be a perfect square because otherwise we shall be dealing with a coset diagram for rational numbers in which case ∞ is the only fixed point. As $(d+a)^2 - 4$ cannot be a perfect square so the fixed points are real but irrational numbers. Thus elements of orders 2 and 3, conjugates of $(DC^2)^n$ and $(A^2B)^n$, and the elements having qi as its trace in matrix form, are the only exceptions where we do not get real quadratic irrational numbers as fixed points. ■

Consideration of the action of Γ on biquadratic field $\mathbb{Q}(i, \sqrt{3})$ suggests the importance of closed paths. If n_1, n_2, \dots, n_{2k} is a sequence of positive integers, then by a closed path of type $(n_1, n_2, \dots, n_{2k})$, we mean a closed path in which n_1 triangles have one vertex outside the closed path and n_2 triangles have one vertex inside the closed path and n_3 triangles have one vertex outside the closed path and so on. This closed path induces an element $g = (DC^{-1})^{n_{2k}} \dots (DC^{-1})^{n_2} (DC)^{n_1}$ of Γ and fixes a particular vertex of a triangle lying on the closed path. If k is the number of sets of triangles with one vertex outside the closed path and \hat{k} is the number of sets of triangles on the closed path with one vertex inside, then $k = \hat{k}$ and so the total number of sets of triangles in a closed path is $2k$. In the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$, a point ρ is on a closed path of ambiguous numbers if and only if it is fixed by some element $g = (DC^{-1})^{n_{2k}} \dots (DC^{-1})^{n_2} (DC)^{n_1}$, $n_i > 0$ of Γ and this means that the closed paths are permuted by any permutation which normalizes the set $\{DC, DC^{-1}\}$. One such permutation is $S : \alpha \mapsto \bar{\alpha}$ and the other is $B : \alpha \mapsto \frac{1}{\alpha}$. Since $B^2 = S^2 = (BS)^2 = 1$ so we have a 4-permutation group permuting the closed paths.

Question arises if $(n_1, n_2, \dots, n_{2k})$ is the closed path, then under what conditions it contains:

- (i) α with its image $\bar{\alpha}$ under the linear fractional transformation $S : \alpha \mapsto \bar{\alpha}$,
- (ii) α with its image $\frac{1}{\alpha}$ under the linear fractional transformation $B : \alpha \mapsto \frac{1}{\alpha}$,

and

- (iii) α with its image $\frac{1}{\bar{\alpha}}$ under the linear fractional transformation $BS : \alpha \mapsto \frac{1}{\bar{\alpha}}$.

We have proved that the closed paths pertaining to case (i), (ii) and (iii) must be of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$, that is, this type of closed path in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ contains α with $\bar{\alpha}$, $\frac{1}{\alpha}$ and $\frac{1}{\bar{\alpha}}$.

Lemma 71 *Let α and $\frac{1}{\alpha}$ exist in a closed path. If α is a vertex of a triangle having one vertex inside/outside the closed path, then the triangle containing $\frac{1}{\alpha}$ also has one vertex inside/outside the closed path.*

Proof. Let α and $\frac{1}{\alpha}$ belong to a closed path. Let us index vertices of the triangles belonging to the closed path by α_i , where $i \in \{1, 2, \dots, m\}$. If α occupies the vertex of a triangle with one vertex inside the closed path, then $\frac{1}{\alpha}$ also occupies the vertex of a triangle with one vertex inside the closed path to satisfy the relation $(BC)^2 = 1$.

■

Lemma 72 *If α occupies a vertex labelled odd/even, then $\frac{1}{\alpha}$ occupies vertex labelled even/odd.*

Proof. If the α 's occupy vertices with odd labels, then no $\frac{1}{\alpha}$'s can occupy any of

these vertices. For otherwise, $B(\alpha_r) = \frac{1}{\alpha_r}$, where $r \leq m$, is odd. By Lemma 71, if α occupies the triangle with one vertex outside the closed path, then $\frac{1}{\alpha_r}$ occupies the triangle with one vertex outside.

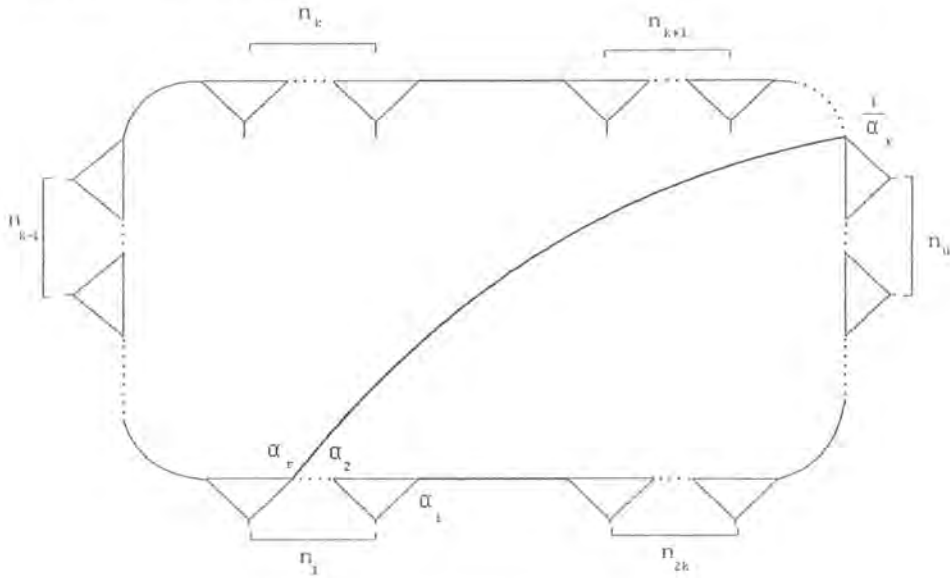


Figure 37

We have $(BC)^2(\alpha_r) = \alpha_r$, this implies that $BC(\alpha_r) = C^2B(\alpha_r)$. But $C^2B(\alpha_r)$ does not belong to closed path, as shown in Figure 37. A contradiction arises because if $C(\alpha_r)$ belongs to closed path, then by Lemma 36, $BC(\alpha_r)$ also belongs to the closed path. So $\frac{1}{\alpha_r}$ must occupies even vertex. ■

Lemma 73 *If α and $\bar{\alpha}$ exist in a closed path, then either both triangles (containing α and $\bar{\alpha}$ as a vertex) have one vertex inside the closed path or both have one vertex outside the closed path.*

Proof. Let α and $\bar{\alpha}$ belong to a closed path. Let us index vertices of the triangles belonging to the closed path by α_i , where $i \in \{1, 2, \dots, m\}$. If α occupies the vertex

of a triangle with one vertex inside the closed path, then $\bar{\alpha}$ also occupies the vertex of a triangle with one vertex inside the closed path to satisfy the relation $(BS)^2 = 1$.

■

Lemma 74 *If α occupies a vertex labelled odd/even, then $\bar{\alpha}$ also occupies vertex labelled odd/even.*

Proof. We label the vertices of the triangles in the closed path by α_i , where $i \in \{1, 2, \dots, m\}$.

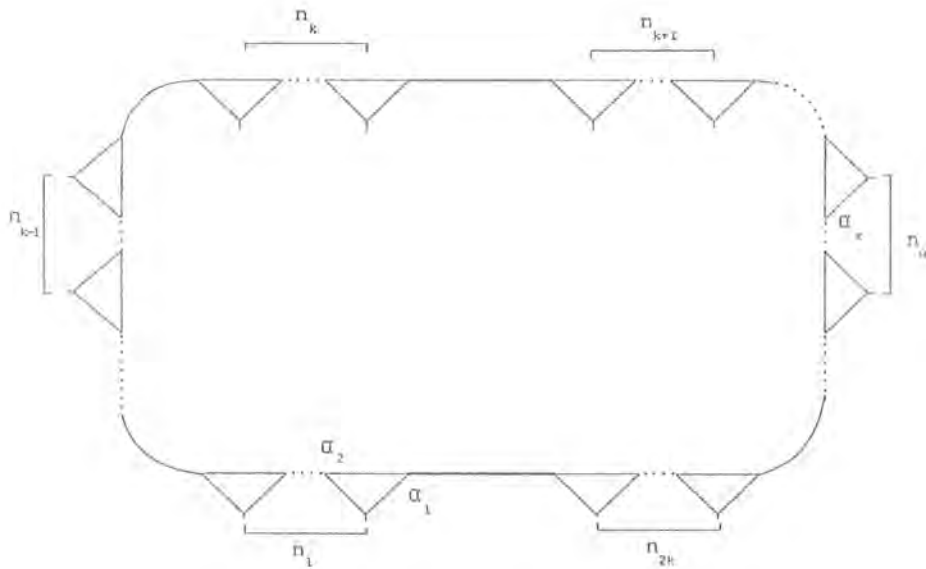


Figure 38

Let $\alpha = \alpha_1$, that is, α occupies the vertex of the triangle with odd label. Let $\bar{\alpha} = \alpha_r$, where r is even and $r \leq m$. By Lemma 73, it must occupy the triangle whose one vertex is outside the closed path, as shown in the Figure 38. This

implies that there exists $g \in \Gamma$ such that $g(\alpha) = \bar{\alpha}$, where g is of the form $g = C \dots (DC^{-1})(DC^{-1})^{n_k} \dots (DC^{-1})^{n_2}(DC)^{n_1}$. Thus since $h(\alpha)$ and $h(\bar{\alpha})$ are conjugates if α and $\bar{\alpha}$ are, for $h \in \Gamma$, so $C(\alpha)$ is a conjugate of $C(\bar{\alpha})$. But $C(\bar{\alpha}) = C(\alpha_r)$, which does not belong to the closed path, as in the Figure 38. This is a contradiction because conjugate of ambiguous numbers are also ambiguous and belong to the closed path. This shows that $\bar{\alpha}$ cannot occupy even label. So $\bar{\alpha}$ must occupies odd label when α occupies odd label. Similarly, it can be proved that if α occupies even vertex, then $\bar{\alpha}$ also occupies even vertex. ■

Let us denote a closed path, which is represented by the word having generators C and D of Γ , by $C - D$ closed path while a closed path, which is represented by the word having generators B, C and D of Γ , is denoted by $B - C - D$ closed path. We denote a $C - D$ closed path containing α by C_α and a $C - D$ closed path containing $\frac{1}{\alpha}$ by $C_{\frac{1}{\alpha}}$, where α is an ambiguous number of $\mathbb{Q}(i, \sqrt{3})$.

For a given sequence of positive integers n_1, n_2, \dots, n_{2k} , the closed path of the type

$$(n_1, n_2, \dots, n_{2k}, n_1, n_2, \dots, n_{2k}, \dots, n_1, n_2, \dots, n_{2k}),$$

where \acute{k} divides k , is said to have a period of length $2\acute{k}$.

Theorem 75 [*[31], Theorem 2.3*] *For given positive integers n_1, n_2, \dots, n_{2k} , there does not exist a closed path which has a period of length $2\acute{k}$, where \acute{k} divides k .*

Lemma 76 *A closed path is $B - C - D$ if and only if the closed path is of the type*

$$(n_1, \dots, n_k, n_k, \dots, n_1).$$

Proof. Let α be an ambiguous number of $\mathbb{Q}(i, \sqrt{3})$. Then by Theorem 44, we get a closed path of ambiguous numbers, which is represented by

$$g = (DC^{-1})^{n_k} \dots (DC^{-1})^{n_2} (DC)^{n_1},$$

where α is fixed point of g . We call it a closed path of α and denote it by $C_\alpha = (n_1, \dots, n_k)$. By applying B on α , we get $\frac{1}{\alpha}$ and by repeatedly applying transformations C, C^2 and D we get another closed path of ambiguous numbers in which $h(\frac{1}{\alpha}) = \frac{1}{\alpha}$, where $h \in \Gamma$, let us denote it by $C_{\frac{1}{\alpha}}$. By Lemma 71, if α_i is the vertex of the triangle having one vertex outside the closed path C_α , then $\frac{1}{\alpha_i}$ is also the vertex of the triangle having one vertex outside the closed path $C_{\frac{1}{\alpha}}$, where $i = 1, \dots, m$, and m is the total number of vertices in C_α . Since $(BC)^2 = 1$, if we apply B on each α_i , then we get m vertices in $C_{\frac{1}{\alpha}}$, such that h fixes $\frac{1}{\alpha}$ and is of the form $(CD)^{n_1} \dots (CD)^{n_{k-1}} (C^{-1}D)^{n_k}$ as shown in Figure 39.

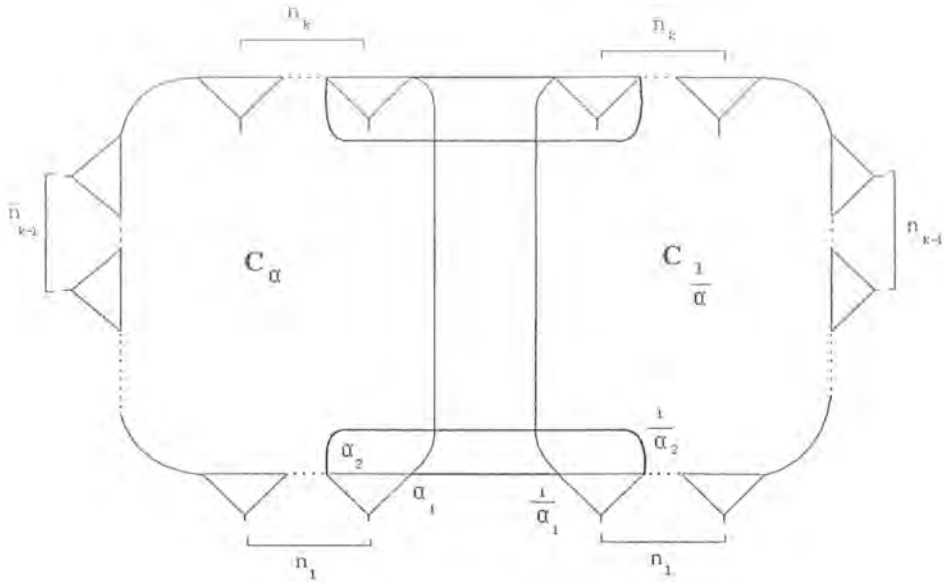


Figure 39

This shows that C_α is of the type (n_1, \dots, n_k) and $C_{\frac{1}{\alpha}}$ is of the type (n_k, \dots, n_1) . If we combine C_α and $C_{\frac{1}{\alpha}}$ by generator B , then we get the closed path of the form $(n_1, \dots, n_k, n_k, \dots, n_1)$ which is represented by $BD(DC)^{n_1} \dots (DC^{-1})^{n_k} BD(DC^{-1})^{n_k} \dots (DC^{-1})^{n_2} (DC)^{n_1}$.

Conversely, let the closed path which contains α is of type $(n_1, \dots, n_k, n_k, \dots, n_1)$ and let it is a $C - D$ closed path. The closed path $(n_1, \dots, n_k, n_k, \dots, n_1)$ induces an element

$$g = (DC^{-1})^{n_1} \dots (DC)^{n_k} (DC^{-1})^{n_k} \dots (DC^{-1})^{n_2} (DC)^{n_1}$$

of Γ . By Lemma 36, generator B maps an ambiguous number to an ambiguous number. So there is another closed path or $C - D$ closed path of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$

since $(BC)^2 = 1$ and $(BD)^2 = 1$. Combining the both closed paths we get

$$(n_1, \dots, n_k, n_k, \dots, n_1, n_1, \dots, n_k, n_k, \dots, n_1),$$

which induces an element $h = g^2$. But this is a contradiction by Theorem 75. Thus

$(n_1, \dots, n_k, n_k, \dots, n_1)$ is a $B - C - D$ closed path. ■

In the following Theorem we have given the necessary and sufficient condition for a closed path to contain $\alpha = \frac{a + b\sqrt{3}}{c}$ with its conjugate $\bar{\alpha} = \frac{a - b\sqrt{3}}{c}$.

Theorem 77 *A closed path contains α with its conjugate $\bar{\alpha}$ if and only if it is of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$.*

Proof. First we note that if α and $\bar{\alpha}$ are conjugates, then so are $g(\alpha)$ and $g(\bar{\alpha})$ for every g in Γ and so the Theorem is true for every element on the closed path if it is true for any one element.

Let α and $\bar{\alpha}$ belong to $C - D$ closed path, which is, (n_1, n_2, \dots, n_k) . There exists $g \in \Gamma$ such that $g(\alpha) = \bar{\alpha}$ that is, $g = (DC^{-1})^{n_r} \dots (DC^{-1})^{n_2} (DC)^{n_1}$, where $r < k$. Now we index vertices of the triangles on the closed path as in Figure 35 by α_i , where $i \in \{1, 2, \dots, m\}$. Let $h \in \Gamma$ fixes α , where $h = (DC^{-1})^{n_k} \dots (DC^{-1})^{n_2} (DC)^{n_1}$. By Lemmas 73 and 74, $f = (DC^{-1})^{n_r} \dots (DC)^{n_1} (DC^{-1})^{n_k} \dots (DC)^{n_{r+1}}$, where f fixes $\bar{\alpha}$. Since α and $\bar{\alpha}$ are conjugates, therefore they are fixed by the same element of Γ , and so f must be equal to h . But this is not the case because if it is so, then $h = (g_1)^s$ for some $s > 1$, $g_1 \in \Gamma$ and, then α will be a fixed point of g_1 . By Theorem 75, this cannot

happen except for $h^t, t \geq 1$ and so gives a contradiction. Thus $\bar{\alpha}$ belongs to $B-C-D$ closed path. By Lemma 76, the closed path is of the type $(n_1, \dots, n_k, n_{k+1}, \dots, n_1)$.

Conversely, let closed path is of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$. Let $\alpha \in C_\alpha$ where $C_\alpha = (n_1, n_2, \dots, n_k)$ and $B(\alpha) = \frac{1}{\alpha}$ such that $\frac{1}{\alpha} \in C_{\frac{1}{\alpha}}$ where $C_{\frac{1}{\alpha}} = (n_k, n_{k-1}, \dots, n_1)$. Let $g_1(\alpha) = \alpha$ where $g_1 \in \Gamma$ is of the form $g_1 = (DC^{-1})^{n_k} \dots (DC^{-1})^{n_2} (DC)^{n_1}$ and $g_2(\frac{1}{\alpha}) = \frac{1}{\alpha}$, where $g_2 = (CD)^{n_1} \dots (CD)^{n_{k-1}} (C^{-1}D)^{n_k}$. By reversing the direction, we get

$$\begin{aligned} g_2 &= (DC)^{n_k} \dots (DC)^{n_2} (DC^{-1})^{n_1} \\ &= (C^{-1}D)^{-n_k} \dots (C^{-1}D)^{-n_2} (CD)^{-n_1}. \end{aligned}$$

Since n_1, n_2, \dots, n_k , shows the number of triangles whose one vertex is inside or outside of the closed path, so we can take them positive, that is, there exist $g_3 \in \Gamma$ such that g_3 is a word in $C_{\frac{1}{\alpha}}$ such that

$$\begin{aligned} g_3 &= (C^{-1}D)^{n_k} \dots (C^{-1}D)^{n_2} (CD)^{n_1} \\ &= D(DC^{-1})^{n_k} \dots (DC^{-1})^{n_2} (DC)^{n_1} D. \end{aligned}$$

Since g_3 is a word in a closed path $C_{\frac{1}{\alpha}}$, so there exist some h which is a word in a closed path $C_{\frac{1}{\alpha}}$ such $h = (DC^{-1})^{n_k} \dots (DC^{-1})^{n_2} (DC)^{n_1}$. So $g_1 = h$ where g_1 is a word of C_α and h is a word of $C_{\frac{1}{\alpha}}$. This shows that $\bar{\alpha}$ is a fixed point of h . ■

Corollary 78 *If $\alpha = b\sqrt{3}$, where $b \in \mathbb{Z}$ is constant, then α and $\bar{\alpha}$ exist in a closed path if and only if the closed path is of $B-C-D$ type or closed path is of the type $(n_1, \dots, n_k, n_{k+1}, \dots, n_1)$.*

Proof. Let $\alpha = b\sqrt{3}$. Then all the ambiguous numbers in the closed path containing α is of the form $\frac{a + b\sqrt{3}}{c}$. The conjugate of α is $\bar{\alpha} = -b\sqrt{3}$. We know that BD and DB maps z to $-z$, where $z \in \mathbb{Q}(i, \sqrt{3})$, so $BD(\alpha) = \bar{\alpha}$. Also if α and $\bar{\alpha}$ are conjugates, then $g(\alpha)$ is a conjugate of $g(\bar{\alpha})$, for $g \in \Gamma$. This shows that if β belongs to the closed path of α , then $\bar{\beta}$ also belongs to the closed path. Therefore if α and $\bar{\alpha}$ exists in the closed path, then the closed path is of $B - C - D$ type and by Theorem 76, the closed path is of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$.

Conversely, suppose that $B - C - D$ is the closed path, then $BD(\alpha) = -\alpha = \bar{\alpha}$, where $\alpha = b\sqrt{3}$. Also if $g(\alpha) = \beta$, then $g(\bar{\alpha}) = \bar{\beta}$, for every $\beta \in C_\alpha$. This shows that α and $\bar{\alpha}$ exist in the closed path. ■

Example 79 Let $\alpha = 2\sqrt{3}$ and $\bar{\alpha} = -2\sqrt{3}$ exist in the following closed path. Clearly it is a $B - C - D$ closed path and it is of the type $(2, 6, 6, 2)$.

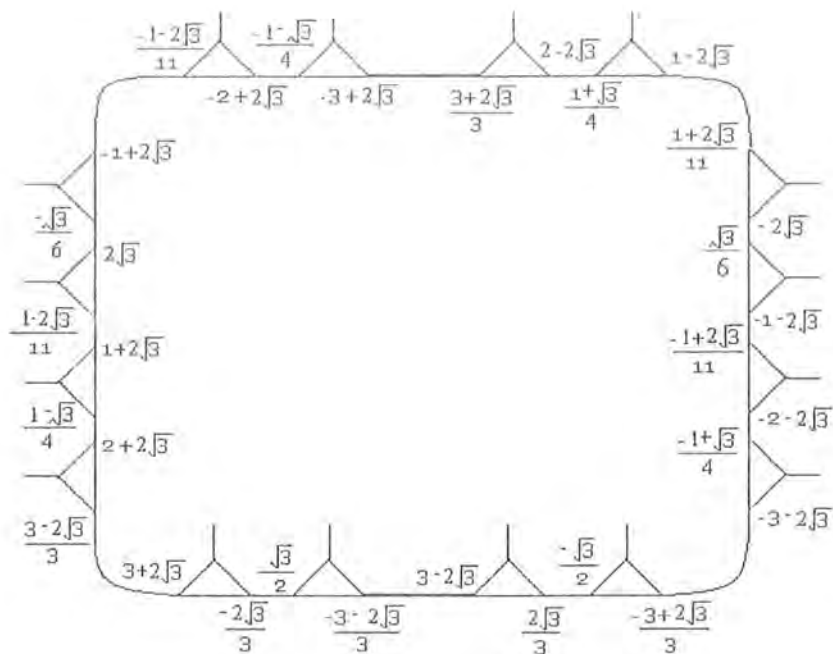


Figure 40

Theorem 80 A closed path contains α with $\frac{1}{\alpha}$ if and only if it is of the type

$$(n_1, \dots, n_k, n_k, \dots, n_1).$$

Proof. Let α with $\frac{1}{\alpha}$ exist in a closed path $(n_1, n_2, \dots, n_{2k})$. Since $B(\alpha) = \frac{1}{\alpha}$, this implies that the closed path which contains α with $\frac{1}{\alpha}$ is a $B - C - D$ closed path.

By Lemma 76, it is of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$.

Conversely, let the closed path which contains α is of type $(n_1, \dots, n_k, n_k, \dots, n_1)$.

By Lemma 76, $(n_1, \dots, n_k, n_k, \dots, n_1)$ is a $B - C - D$ closed path and thus $B(\alpha) = \frac{1}{\alpha}$

belongs to this closed path. ■

Theorem 81 A closed path contains α with $\frac{1}{\alpha}$ if and only if it is of the type

$$(n_1, \dots, n_k, n_k, \dots, n_1).$$

Proof. Let α with $\frac{1}{\bar{\alpha}}$ exist in (n_1, \dots, n_{2k}) if and only if $B\left(\frac{1}{\bar{\alpha}}\right) = \bar{\alpha}$ also exist in the closed path. By Theorem 77, a closed path contains α with its conjugate $\bar{\alpha}$ if and only if it is of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$. ■

Remark 82 1. Let α and $\bar{\alpha}$ exist in a closed path, then by Theorem 77, the closed path is of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$. We know that $B(\alpha) = \frac{1}{\bar{\alpha}}$. Let us denote the transformation $\alpha \mapsto \bar{\alpha}$ by S , then $BS(\alpha) = B(\bar{\alpha}) = \frac{1}{\alpha}$, and $(BS)^2\alpha = \alpha$. This gives us the presentation $\langle B, S : B^2 = S^2 = 1, BS = SB \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. The closed path in a coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is of the type $(n_1, \dots, n_k, n_k, \dots, n_1)$ and it contains $\bar{\alpha}, \frac{1}{\bar{\alpha}}$ and $\frac{1}{\alpha}$ with α , where α is an ambiguous number in $\mathbb{Q}(i, \sqrt{3})$. It is the only type of closed path which contains ambiguous numbers in the coset diagram of action of Γ on $\mathbb{Q}(i, \sqrt{3})$.

Example 83 Figure 41 is a closed path of ambiguous numbers of the form $\frac{a + 4\sqrt{3}}{c}$. Let $\alpha = \frac{\sqrt{3}}{4}$. Then $B(\alpha) = \frac{1}{\bar{\alpha}} = \frac{4\sqrt{3}}{3}$, $S(\alpha) = \bar{\alpha} = \frac{-\sqrt{3}}{4}$ and $BS(\alpha) = \frac{1}{\alpha} = \frac{-4\sqrt{3}}{3}$ exist in this closed path and the closed path is of the type $(4, 3, 3, 4)$.

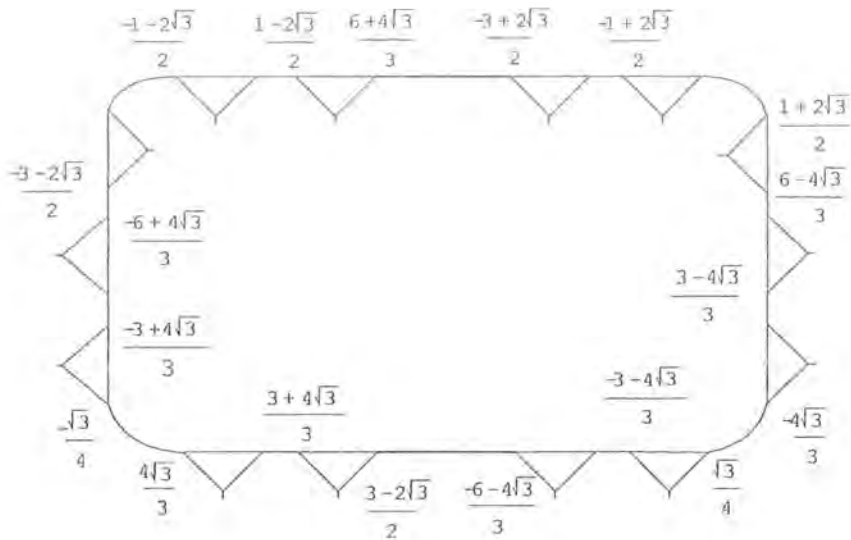


Figure 41

4.0.1 Action of Γ on $PL(F_p)$

Suppose there exists a closed path of the type $(n_1, n_2, \dots, n_{2k})$ in a coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$. The following questions can be raised: When does a homomorphic image of this closed path occur and for what values of p , in the coset diagram representing the action of Γ on $PL(F_p)$, where p is prime? Γ acts on $PL(F_p)$ only when $p - 1$ is a square in F_p . In other words p is a Pythagorean prime because Γ is the group of linear fractional transformations $T(z) = \frac{az + b}{cz + d}$ with $ad - bc = 1$ and $a, b, c, d \in \mathbb{Z}[i]$, that is, i is equivalent to $\sqrt{p-1}$ in F_p .

If there exists a closed path in the coset diagram for the action of Γ on $PL(F_p)$, then, since there are four mappings from $\mathbb{Q}(i, \sqrt{3}) \cup \{\infty\}$ to $F_p \cup \{\infty\}$, there are four

such closed paths. The four such closed paths are not necessarily distinct. We have observed that only one copy of the closed path of ambiguous numbers of the form $\frac{a+b\sqrt{3}}{c}$ exists in the coset diagram for the action of Γ on $PL(F_p)$.

Lemma 84 *The fixed points of generators A and C exist in the coset diagrams for the action of Γ on $PL(F_p)$ if and only if p can be written as $12k+1$, where $k \geq 1$.*

Proof. Fixed points of generators A and C are $\frac{i \pm \sqrt{3}}{2}$ and $\frac{-1 \pm \sqrt{-3}}{2}$ respectively. We know that number of fixed points of A and C is same, that is, $(p+1) - 3\lfloor \frac{p+1}{3} \rfloor$ because both the generators have order 3. For a particular p if fixed points of A exist, then fixed points of C also exist. As there are two fixed points of A and C in $\mathbb{Q}(i, \sqrt{3})$ so in $PL(F_p)$ there are also 2 fixed points. This implies that $(p+1) \equiv 2 \pmod{3}$ or $p \equiv 1 \pmod{3}$ and p is also Pythagorean prime, that is, $p-1$ is perfect square in F_p or p can be written as $4k+1$, where $k \in \mathbb{Z}^+$. As p can be written as $3k+1$ and $4k+1$, so p can be written as $12k+1$. ■

Theorem 85 *If a closed path of ambiguous numbers of the form $\frac{a+b\sqrt{3}}{c}$ exists in the coset diagram for the action of Γ on $PL(F_p)$, then p is of the form $12k+1$, where $k \geq 1$.*

Proof. If $p-1$ is a perfect square in F_p , then Γ acts on $PL(F_p)$. The ambiguous numbers of the form $\frac{a+b\sqrt{3}}{c}$ exist in this coset diagram when 3 is a perfect square in F_p . We know that fixed points of generator A are $\frac{i \pm \sqrt{3}}{2}$ or $\frac{\sqrt{p-1} \pm \sqrt{3}}{2}$. They exist in the coset diagram when $p-1$ and 3 are squares in F_p except for $p=2$. This

implies that when the closed path of ambiguous numbers exists in the coset diagram for the action of Γ on $PL(F_p)$, then the fixed points of A also exist. By Lemma 84, p can be written as $12k + 1$.

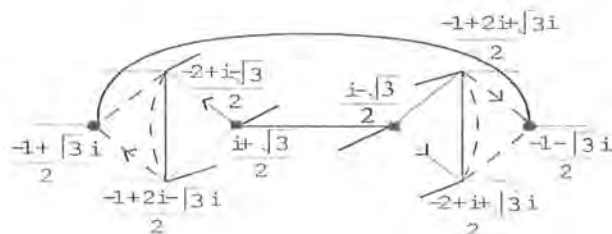


Figure 42

Hence if the closed path of ambiguous numbers exists in the coset diagram for the action of Γ on $PL(F_p)$, then p can be written as $12k + 1$, where $k \in \mathbb{Z}^+$. ■

Proposition 86 *If Γ acts on $PL(F_p)$, then the fixed points of the generators B and D exist in the coset diagram for the action of Γ on $PL(F_p)$.*

Proof. Since the fixed points of generators B and D are ± 1 and $\pm i$ respectively, so they are equivalent to $1, p - 1, \sqrt{p - 1}$ and $p - \sqrt{p - 1}$ respectively. These fixed points exist in those coset diagrams for the action of Γ on $PL(F_p)$ in which $p - 1$ is square in F_p . Also, if $p - 1$ is square in F_p , then Γ acts on $PL(F_p)$ because Γ consists of linear fractional transformations $T(z) = \frac{az + b}{cz + d}$ with $ad - bc = 1$ and $a, b, c, d \in \mathbb{Z}[i]$. Hence the coset diagrams for the action of Γ on $PL(F_p)$ contain fixed points of generators B and D . ■

Theorem 87 *If p can be written as $12k + 1$, where $k \in \mathbb{Z}^+$, then the copy of the closed path of n ambiguous numbers exists in the coset diagram for the action of Γ on $PL(F_p)$, when $p \geq \frac{3n}{2} + 1$.*

Proof. Let p can be written as $12k + 1$. Let there are n ambiguous numbers in a closed path in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$. This means that there are $\frac{n}{2}$ triangles representing 3-cycles of the generator C in the closed path, since every triangle contains two ambiguous numbers. By Lemma 84 and Proposition 86, the fixed points of generators A, B, C and D exist in the coset diagram for the action of Γ on $PL(F_p)$. Since the world representing the closed path does not contain generator A , we will not discuss its fixed points. Let an ambiguous number be mapped to the fixed point of the generator C , by the mapping $\mathbb{Q}(i, \sqrt{3}) \cup \{\infty\}$ to $PL(F_p)$. Then the closed path formed in the coset diagram for the action of Γ on $PL(F_p)$ contains $n - 2$ ambiguous numbers, because of the presence of two fixed points of generator C . Thus there are $\frac{3n}{2}$ elements in $PL(F_p)$ for $\frac{n}{2}$ triangles. To avoid reduction in the closed path due to the fixed points of the generator C , there should be $\frac{3n}{2} + 2$ elements in $PL(F_p)$. The fixed points of generators B and D can be avoided. If an ambiguous number mapped to the fixed point of generator D , then after the application of generator B we can get a new ambiguous number and the same procedure can be repeated for the fixed points of generator B . Thus p should be at least $\frac{3n}{2} + 1$ to contain the closed path of n ambiguous numbers without reduction.

■

Remark 88 If $p = 12k + 1$, $k \in \mathbb{Z}^+$, then $p - 1$, 3 and $p - 3$ are square in F_p .

Example 89 Take $p = 37 = 12(3) + 1$. Consider the action of Γ on $PL(F_{37})$ defined by $A(z) = \frac{1}{z - \sqrt{p-1}}$, $B(z) = \frac{1}{z}$, $C(z) = \frac{1+z}{-z}$ and $D(z) = \frac{-1}{z}$, where $z \in PL(F_{37})$. Then we can calculate the permutation representations of A, B, C and D as follows:

$$\bar{A} = (\infty \ 0 \ 6) (1 \ 22 \ 7) (2 \ 9 \ 25) (3 \ 12 \ 31) (4 \ 18 \ 34) (5 \ 36 \ 21) (29) (8 \ 19 \ 20)$$

$$(10 \ 28 \ 32) (11 \ 15 \ 33) (13 \ 16 \ 26) (14) (17 \ 27 \ 30) (23 \ 24 \ 35),$$

$$\bar{B} = (0 \ \infty) (1) (2 \ 19) (3 \ 25) (4 \ 28) (5 \ 15) (6 \ 31) (7 \ 16) (8 \ 14) (9 \ 33) (10 \ 26)$$

$$(11 \ 27) (12 \ 34) (13 \ 20) (17 \ 24) (18 \ 35) (21 \ 30) (22 \ 32) (23 \ 29) (36),$$

$$\bar{C} = (0 \ \infty \ 36) (1 \ 35 \ 18) (2 \ 17 \ 12) (3 \ 11 \ 9) (4 \ 8 \ 22) (5 \ 21 \ 6) (7 \ 20 \ 23) (10)$$

$$(13 \ 16 \ 29) (14 \ 28 \ 32) (15 \ 31 \ 30) (19 \ 34 \ 24) (25 \ 33 \ 27) (26), \text{ and}$$

$$\bar{D} = (0 \ \infty) (1 \ 36) (2 \ 18) (3 \ 12) (4 \ 9) (5 \ 22) (6) (7 \ 21) (8 \ 23) (10 \ 11) (13 \ 17)$$

$$(14 \ 29) (15 \ 32) (16 \ 30) (19 \ 35) (20 \ 24) (25 \ 34) (26 \ 27) (28 \ 33) (31).$$

The coset diagram for the action of Γ on $PL(F_{37})$ is shown in Figure 43. We have omitted some edges of generators B and D for clear visibility of the coset diagram.

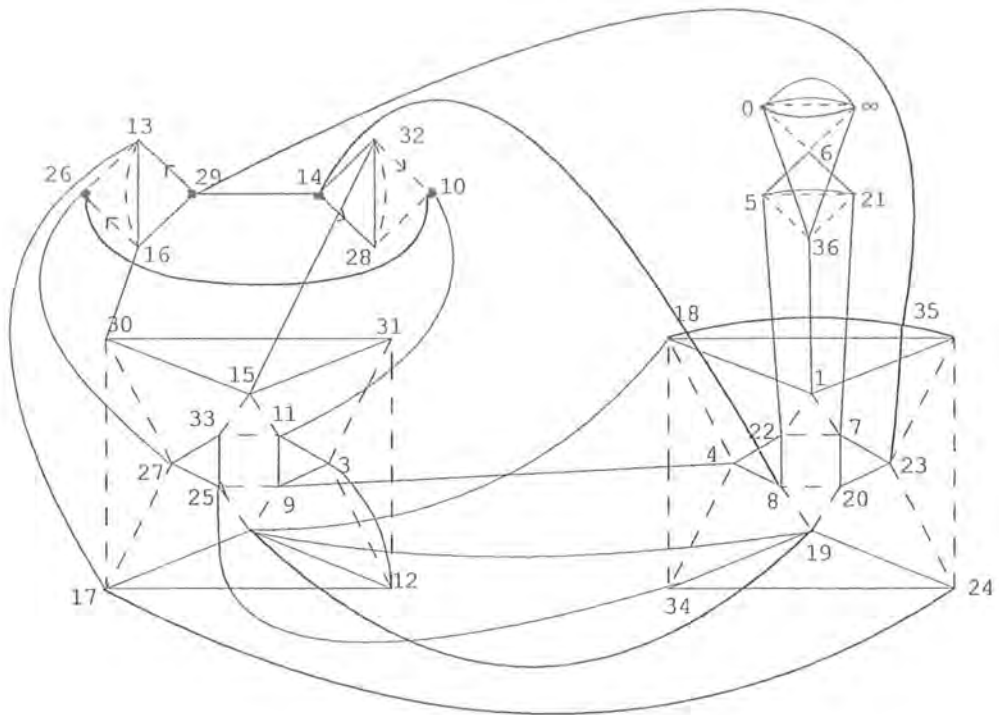


Figure 43

The closed path of ambiguous numbers which contains elements of the form $\frac{a + \sqrt{3}}{c}$, occurs in the above coset diagram, as shown in Figure 44.

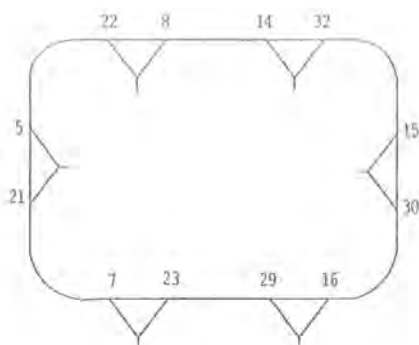


Figure 44

The closed path is of the type $(1, 2, 2, 1)$. As the field $PL(F_{37})$ consists of 38 elements, so the closed path of ambiguous numbers of the form $\frac{a + 2\sqrt{3}}{c}$, which contains 32 ambiguous numbers, exists in the reduced form, as Theorem 87 states.

Remark 90 1. The following two fragments have some triangles with clockwise direction.

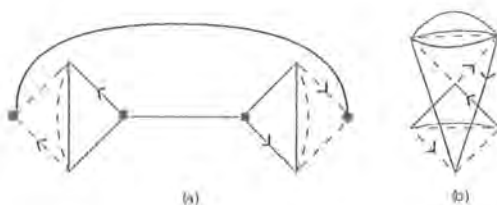


Figure 45

The fragment (a) exists only for those primes in which $p - 1$, $p - 3$ and 3 are

squares in F_p or, in other words, when p is of the form $12k + 1$ and the fragment (b) exists when $p - 1$ is square in F_p .

2. Although $\sqrt{3}$ is equal to two values in F_p , that is, n and $p - n$ where 3 is square in F_p . But there exists only one closed path in the coset diagram for the action of Γ on $PL(F_p)$. Because if $\alpha = \frac{a + b\sqrt{3}}{c}$ exist in the closed path, then $\bar{\alpha} = \frac{a - b\sqrt{3}}{c}$ also exist. The value $\frac{a + b\sqrt{3}}{c}$ become $\frac{a + bn}{c}$ and $\frac{a - b\sqrt{3}}{c}$ becomes $\frac{a - b(p - n)}{c}$ in $PL(F_p)$. So n and $p - n$, both exist in same closed path.

Remark 91 The coset diagrams for the action of Γ on $PL(F_p)$, where p is a Pythagorean prime, possess following properties:

1. In each coset diagram, there are two caps of generator B and two caps of generator D , because of two fixed points of each generator.

2. Number of triangles having broken and unbroken edges is $3\lfloor\frac{p+1}{3}\rfloor$ and the number of edges is $\frac{p-1}{2}$ for each generator B and D .

3. The number of fixed points of generators A and C is equal in a coset diagram for the action of Γ on $PL(F_p)$, that is, $(p+1) - 3\lfloor\frac{p+1}{3}\rfloor$. There are two fixed points of each generator A and C when p is of the form $12k + 1$ where $k \in \mathbb{Z}^+$ otherwise there are no fixed points of the generators A and C in the coset diagram.

Table of some primes p used in our work are:

$p - 1$ is square in F_p	3 is square in F_p	primes of the form $12k + 1$
2	2	13
5	3	37
13	11	61
17	13	73
29	23	97
37	37	109
41	47	157
53	59	181
61	61	193

We now conclude that the closed paths of ambiguous numbers in the coset diagram for the action of Γ on $\mathbb{Q}(i, \sqrt{3})$ is of only one type, that is, $(n_1, n_2, \dots, n_{k-1}, n_k, n_k, n_{k-1}, \dots, n_2, n_1)$. This closed path contains α with $\bar{\alpha}$, $\frac{1}{\alpha}$ and $\frac{1}{\bar{\alpha}}$. The homomorphic image of this closed path exists in the coset diagram for the action of Γ on $PL(F_p)$ if and only if $p - 1$ and $p - 3$ is square in F_p or p is of the form $12k + 1$.

Bibliography

- [1] S. Anis and Q. Mushtaq, The number of subgroups of $PSL(2, \mathbb{Z})$ when acting on $F_p \cup \{\infty\}$, *Comm. Algebra*, 36 (11) (2008), 4276 – 4283.
- [2] A. F. Beardon, *The geometry of discrete groups*, Springer-Verlag, New York, 1983.
- [3] N. L. Biggs and A. T. White, *Permutation groups and combinatorial structures*, Cambridge University Press, Cambridge, 1979.
- [4] N. H. Bong and Q. Mushtaq, Fibonacci and Lucas numbers through the action of the modular group on real quadratic fields, *Fibonacci Quart.*, 42 (1) (2004), 20 – 27.
- [5] A. M. Brunner, M. L. Frame, Y. W. Lee and N. J. Wielenberg, Classifying torsion-free subgroups of the Picard group, *Trans. Amer. Math. Soc.*, 282(1) (1984), 205 – 235.

- [6] A. M. Brunner, A two-generator presentation for the Picard group, Proc. Amer. Math. Soc., 115 (1) (1992), 45 – 46.
- [7] R. P. Burn, *Groups: a path to geometry*, Cambridge University Press, Cambridge, 1994.
- [8] W. Burnside, *Theory of groups of finite order*, 2nd Ed., Dover Pub. Inc., New York, 1995.
- [9] C. M. Campbell, M. D. E. Conder and E. F. Robertson, Defining relations for Hurwitz groups, Glasg. Math. J., 36 (1994), 363 – 370.
- [10] A. Cayley, The theory of groups: graphical representations, Amer. J. Math., 1 (1878), 174 – 176.
- [11] P. M. Cohn, A presentation of SL_2 for Euclidean imaginary quadratic number fields, Mathematika, 15(1968), 156 – 163.
- [12] M. D. E. Conder, Generators for alternating and symmetric groups, J. Lond. Math. Soc., 2 (1980), 75 – 86.
- [13] M. D. E. Conder, Some results on quotients of triangle groups, Bull. Aust. Math. Soc., 29 (1984), 73 – 90.
- [14] H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups*, 4th Ed., Springer-Verlag, New York, 1980.

- [15] B. Fine, Fuchsian subgroups of the Picard group, *Canad. J. Math.*, 28 (1976), 481 – 485.
- [16] B. Fine and M. Newman, The normal subgroup structure of the Picard group, *Trans. Amer. Math. Soc.*, 302 (2) (1987), 769 – 786.
- [17] B. Fine, *Algebraic theory of Bianchi groups*, Marcel Dekker, New York, 1989.
- [18] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th Ed., Clarendon Press, Oxford, 1960.
- [19] G. Higman and Q. Mushtaq, Coset diagrams and relations for $PSL(2, \mathbb{Z})$, *Arab Gulf J. Sci. Res.*, 1 (1) (1983), 159 – 164.
- [20] W. Magnus, *Non-Euclidean tessellations and their groups*, Academic Press, New York, 1974.
- [21] W. Magnus, Use of 2×2 matrices in combinatorial group theory, *Resultate der Mathematik*, 4 (1981), 171 – 192.
- [22] H. Maschke, The representation of finite groups, especially of the rotation groups of the regular bodies in three and four dimensional spaces, *Amer. J. Math.*, 18 (1896), 156 – 194.
- [23] Q. Mushtaq, *Coset diagrams for the modular group*, D.Phil. Thesis, Oxford University, 1983.

- [24] Q. Mushtaq and F. Shaheen, Coset diagrams for a homomorphic image of $\Delta(2, 3, 6)$, *Acta Comb.*, 23A (1987), 187 – 193.
- [25] Q. Mushtaq, Modular group acting on real quadratic fields, *Bull. Aust. Math. Soc.*, 37 (1988), 303 – 309.
- [26] Q. Mushtaq, A condition for the existence of a fragment of a coset diagram, *Quart. J. Math.*, 39 (2) (1988), 81 – 95.
- [27] Q. Mushtaq, Coset diagrams for an action of the extended modular group on the projective line over a finite field, *Indian J. Pure Appl. Math.*, 20 (8) (1989), 747 – 754.
- [28] Q. Mushtaq, The extended modular group acting on the projective line over a Galois field, *Indian J. Pure Appl. Math.*, 20 (8) (1989), 755 – 760.
- [29] Q. Mushtaq, Coset diagrams for Hurwitz groups, *Comm. Algebra*, 18 (11) (1990), 3857 – 3888.
- [30] Q. Mushtaq and H. Servatius, Permutation representation of the symmetry groups of regular hyperbolic tessellations, *J. Lond. Math. Soc.*, 48 (2) (1993), 77 – 86.
- [31] Q. Mushtaq, On word structure of the modular group over finite and real quadratic fields, *Disc. Math.*, 178 (1998), 155 – 164.

- [32] I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, 2nd Ed., John Wiley & Sons Inc., New York, 1966.
- [33] N. Y. Özgür, On the subgroups of the Picard group, *Contrib. Algebr. Geo.*, 44 (2) (2003), 383 – 387.
- [34] R. Riley, Applications of a computer implementation of Poincare's Theorem on fundamental polyhedra, *Math. Comp.*, 40 (162) (1983), 607 – 632.
- [35] J. H. C. Whitehead, On certain sets of elements in a free group, *Proc. Lond. Math. Soc.*, 41 (2) (1936), 48 – 56.
- [36] K. S. Williams, Integers of biquadratic fields, *Canad. Math. Bull.*, 13 (4) (1970), 519 – 526.
- [37] N. Yilmaz and İ. N. Cangül, The normaliser of the modular group in the Picard group, *Bull. Inst. Math. Acad. Sinica*, 28 (2) (2000), 125 – 129.