Far East J. Math. Sci. (FJMS) **16**(3) (2005), 369-378

DETECTION OF AMBIGUOUS NUMBERS IN THE ACTION OF THE GROUP $\langle x, y : x^2 = y^4 = 1\rangle$ ON $Q(\sqrt{n})$

M. ASLAM and Q. MUSHTAQ

(Received July 30, 2003)

Submitted by Arnold Knopfmacher

Abstract

By using the coset diagrams for the action of $G = \langle x, y : x^2 = y^4 = 1\rangle$ on $Q(\sqrt{n})$, we show that the linear fractional transformation x transforms a totally positive (negative) real quadratic irrational number to a totally negative (positive) real quadratic irrational number, and an ambiguous number into an ambiguous number. We show also that if α is an ambiguous number, then one of $(\alpha)y^j$ for $j = 1, 2, 3$ is ambiguous and the other two are totally negative. At the end we show that the action of the group G on $Q(\sqrt{n})$ is intransitive.

1. Introduction

Let F be an extension field of degree two over the field Q of rational numbers. Then any element $x \in F - Q$ is of degree two over Q and is a primitive element of F (that is, $F = Q[x]$ and $\{1, x\}$ is a base of F over Q). Let $F(x) = x^2 + bx + c$, where $b, c \in Q$, be the minimal polynomial of such an element $x \in F$. Then $2x = -b \pm \sqrt{b^2 - 4c}$ and so

2000 Mathematics Subject Classification: Primary 05C25; Secondary 11E04, 20G15.

Key words and phrases: real quadratic irrational numbers, linear fractional transformations, coset diagrams, closed paths, rational projective line.

$F = Q(\sqrt{b^2 - 4c})$. Here, since $b^2 - 4c$ is a rational number $\frac{u}{v} = \frac{uv}{v^2}$ with $u, v \in Z$. We obtain $F = Q(\sqrt{uv})$ with $u, v \in Z$. In fact, it is possible to write $F = Q(\sqrt{n})$, where n is a square free integer. If n is a positive square free integer, then $Q(\sqrt{n})$ is called a *real quadratic field* and the elements of $Q(\sqrt{n})$ are of the form $a + b\sqrt{n}$ with $a, b \in Q$.

Let M be a group generated by the linear fractional transformations x, y satisfying the relations $x^2 = y^m = 1$. If $y : z \to \frac{az + b}{cz + d}$ is to act on real quadratic fields, then a, b, c, d must be rational numbers and can be considered as integers. Thus $\frac{(a + d)^2}{ad - bc} - 2 = \omega + \omega^{-1}$, where ω a primitive m-th root of unity, is rational, only if $m = 1, 2, 3, 4$ or 6. The group M is cyclic of order two, D_∞ (an infinite dihedral group), or $PSL(2, Z)$ if $m = 1, 2,$ or 3. The case $m = 3$ has been discussed in detail in [2] and [5].

An element $\alpha = \frac{a + \sqrt{n}}{c} \in Q(\sqrt{n})$ and its conjugate $\overline{\alpha} = \frac{a - \sqrt{n}}{c}$ may have different signs for a fixed non-square positive integer n. If such is the case, then α is called an *ambiguous number*. If α and $\overline{\alpha}$ are both positive (negative), then α is called a *totally positive* (*negative*) *number*. Ambiguous numbers play an important role in the study of actions of the groups $M = \langle x, y : x^2 = y^m = 1\rangle$, for $m = 1, 2, 3, 4$ or 6, on $Q(\sqrt{n})$. In the action of M on $Q(\sqrt{n})$, $Stab_\alpha(M)$ are the only non-trivial stabilizers and in the orbit αM, there is only one (up to isomorphism) non-trivial stabilizer.

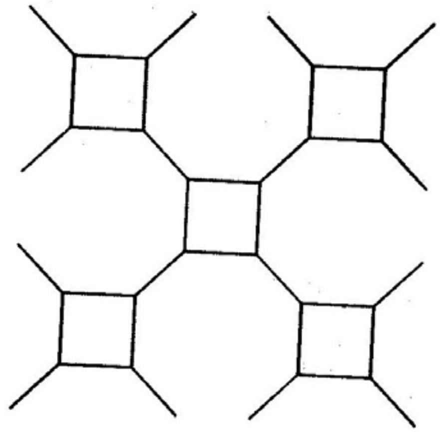
In this short note we are interested in the group M for $m = 4$, that is, $G = \langle x, y : x^2 = y^4 = 1\rangle$, acting on the real quadratic irrational numbers, where $(z)x = \frac{-1}{2z}$ and $(z)y = \frac{-1}{2(z + 1)}$ are linear fractional transformations. An action of G on real quadratic irrational numbers has been considered in [3]. It has been shown there that the set of ambiguous numbers is finite and that part of the coset diagram containing these numbers forms a single closed path, and it is the only closed path in the orbit of α.

We discuss here some basic properties of the real quadratic irrational numbers α under the action of G by using coset diagrams. We show that if α is totally positive, then $(\alpha)y^j$ for $j = 1, 2, 3$ are totally negative. Also the linear fractional transformation x transforms a totally positive (negative) number to a totally negative (positive) number, and an ambiguous number into an ambiguous number. We also show that if α is an ambiguous number, then one of $(\alpha)y^j$ for $j = 1, 2, 3$ is ambiguous and the other two are totally negative. Finally, we show that if $\alpha = \frac{a + \sqrt{n}}{2c} \in Q^*(\sqrt{n})$, where $Q^*(\sqrt{n}) = \left\{\frac{a + \sqrt{n}}{c} : b = \frac{a^2 - n}{c}, c \neq 0, a, b, c \in Z\right\}$, then $\alpha G \subset Q^*(\sqrt{n})$ and the action of G on $Q^*(\sqrt{n})$ and consequently on $Q(\sqrt{n})$ is always intransitive.

2. Coset Diagrams

We use coset diagrams for the group G and study its action on the projective line over real quadratic fields. The coset diagrams for the group G are defined as follows. The four cycles of the transformation y are denoted by four edges of a square permuted anti-clockwise by y and the two vertices which are interchanged by x are joined by an edge. Fixed points of x and y, if they exist, are denoted by heavy dots. This graph can be interpreted as a coset diagram, with the vertices identified with the cosets of $Stab_\alpha(G)$, the stabilizer of some vertex α of the graph, or as 1-skeleton of the cover of the fundamental complex of the presentation, which corresponds to the subgroup $Stab_\alpha(G)$.

A general fragment of the coset diagram of the action of G on $Q(\sqrt{n})$ will look as follows.



Consider a coset diagram for the action of G on the projective line over a real quadratic field. If $k \neq 0, \frac{-1}{2}, -1, \infty$ is one of the four vertices of a square in the coset diagram, then k and $(k)x$ are end points of an edge. Since $(k)x = \frac{-1}{2k}$, one of k and $(k)x$ is positive and the other is negative. Since $(z)y = \frac{-1}{2(z+1)}$,

(i) if $z < -1$, then $(z)y > 0$,

(ii) if $z > 0$, then $\frac{-1}{2} < (z)y < 0$,

(iii) if $\frac{-1}{2} < z < 0$, then $-1 < (z)y < \frac{-1}{2}$, and

(iv) if $-1 < z < \frac{-1}{2}$, then $(z)y < -1$.

That is, if vertices $(k)y^j$ for $j = 0, 1, 2, 3$ of a square are not $0, \frac{-1}{2}, -1$ and ∞, then just one of them lies in each of the intervals: $(-\infty, -1)$, $\left(-1, \frac{-1}{2}\right)$, $\left(\frac{-1}{2}, 0\right)$ and $(0, \infty)$. Thus, in particular, of the vertices $(k)y^j$ for $j = 0, 1, 2, 3,$ one is positive and three are negative.

3. Main Results

For a given sequence of positive integers $n_1, n_2, \ldots, n_{2k}$ the circuit of the type $(n_1, n_2, \ldots, n_{2k'}, n_1, n_2, \ldots, n_{2k'}, \ldots, n_1, n_2, \ldots, n_{2k'})$, where k' divides k, is said to have a period of length $2k$. Before we prove that the linear fractional transformations x and y generate the group G which is the free product of two cyclic groups, one of order 2 and the other of order 4, first it is necessary to point out that in any action of the modular group on any subset of rational number field or real quadratic fields, there does not exist any circuit which has a period of length $2k'$, where k' divides k. The proof is available in [4]. A similar result for the group G has been proved in [6] using the same technique as in [4].

Theorem 3.1. *The linear fractional transformations* $x : z \to \frac{-1}{2z}$ *and* $y : z \to \frac{-1}{2(z+1)}$ *generate* G *and* $x^2 = y^4 = 1$ *are defining relations for the group* G.

Proof. Suppose that $x^2 = y^4 = 1$ are not defining relations of G. Then there is a relation of the form $xy^{\eta_1}xy^{\eta_2} \ldots xy^{\eta_n} = 1$, where $n \geq 1$, $\eta_i = 1, 2$ or $3, 1 \leq i \leq n$. We note that neither x nor y can be 1.

In Theorem 2 [4], we have shown that if k is any positive rational number (vertex) in the coset diagram of the action of the group G on the rational projective line $PL(Q) = Q \cup \{\infty\}$, where $k \neq \frac{-1}{2}, -1, \infty$ and 0, then there exists a unique sequence of positive rational numbers $k_0 (= k)$, $k_1, k_2, \ldots, k_n$ such that $\| k_0 \| > \| k_1 \| \geq \| k_2 \| \geq \cdots \geq \| k_n \|$, $k_m = \frac{1}{2}$ or 1. That is, the coset diagram for the action of the group G on the rational projective line $PL(Q) = Q \cup \{\infty\}$ does not contain any circuit except the circuit in the square with the vertices $0, \frac{-1}{2}, -1$ and ∞. Suppose a contradiction, that is, a circuit exists in the coset diagram. Let there be n squares, depicting y, in the circuit. Since a square always contains one positive number (vertex) and three negative numbers (vertices), we label positive vertices by $k_1, k_2, \ldots, k_n$. If we let $\| k \| = \max(|a|, |b|)$, where $k = \frac{a}{b}$ is a rational number, then $\| k_1 \| \geq \| k_2 \| \geq \cdots \geq \| k_n \| \geq \| k_1 \|$ gives a contradiction. Thus the coset diagram does not contain any circuit other than the circuit in the square with the vertices $0, \frac{-1}{2}, -1$ and ∞.

This shows that there are vertices in the diagram such that the path connecting them with ∞ is of arbitrary length. Choose $k > 0$, so that the path between k and ∞ is of length greater than n. Define $k_0 = k$, $k_i = kxy^{\eta_1}xy^{\eta_2}\cdots xy^{\eta_i}$, where $i = 1, 2, \ldots, n$. Then $k_0, k_1, k_2, \ldots, k_n$ form a circuit, which gives us a contradiction. Thus $xy^{\eta_1}xy^{\eta_2}\cdots xy^{\eta_n} \neq 1$ and so $x^2 = y^4 = 1$ are defining relations for the group G.

We will need the following results from [1].

Lemma 3.2. *Let* $\alpha = \frac{a + \sqrt{n}}{c} \in Q(\sqrt{n})$, *where* $c \neq 0$ *and* $b = \frac{a^2 - n}{c}$ *is an integer. Then*

(i) α *is a totally positive number if and only if either* $a, b, c > 0$ *or* $a, b, c < 0$.

(ii) α *is a totally negative number if and only if either* $a < 0$, $b > 0$, $c > 0$ *or* $a > 0, b < 0, c < 0$.

(iii) α *is an ambiguous number if and only if* $bc < 0$.

Next, we shall show the following results concerning $\alpha \in Q(\sqrt{n})$.

Proposition 3.3. *If* $\alpha = \frac{a + \sqrt{n}}{c} \in Q(\sqrt{n})$ *is a totally positive number, then* $(\alpha)y^j$ *for* $j = 1, 2, 3$ *are totally negative numbers.*

Proof. Since $(z)y = \frac{-1}{2(z+1)}$, therefore $(\alpha)y = \frac{-1}{2(\alpha+1)} = \frac{-a-c+\sqrt{n}}{2(2a+b+c)}$ $= \frac{a_1 + \sqrt{n}}{c_1}$, where $a_1 = -a - c$, $c_1 = 2(2a + b + c)$ and $b_1 = \frac{a_1^2 - n}{c_1} = \frac{c}{2}$.

Similarly, we can find new values of a, b, c for $(\alpha)y^j$, where $j = 1, 2, 3,$ that is,

α	a	b	c
$j = 1$	$-a-c$	$\frac{c}{2}$	$2(2a+b+c)$
$j = 2$	$-3a-2b-c$	$2a+b+c$	$4a+4b+c$
$j = 3$	$-a-2b$	$\frac{4a+4b+c}{2}$	$2b$

Since α is totally positive, therefore, by Lemma 3.2(i), either $a, b, c > 0$ or $a, b, c < 0$. For both $a, b, c > 0$ and $a, b, c < 0$, using the above information and Lemma 3.2(ii), it is easy to see that $(\alpha)y^j$, where $j = 1, 2, 3,$ are totally negative numbers.

Proposition 3.4. *If* $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$, *then* x *transforms a totally positive (negative) number* α *into a totally negative (positive) number.*

Proof. Let $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ be a totally positive number. Then either $a, b, c > 0$ or $a, b, c < 0$. Now, $(\alpha)x = \frac{-1}{2\alpha} = \frac{-a+\sqrt{n}}{2b} = \frac{a_1+\sqrt{n}}{c_1}$, where $a_1 = -a$, $c_1 = 2b$ and $b_1 = \frac{a_1^2 - n}{c_1} = \frac{c}{2}$. For both $a, b, c > 0$ and $a, b, c < 0$, using Lemma 3.2(ii), $(\alpha)x$ is totally negative.

Similarly, one can prove that if α is totally negative, then $(\alpha)x$ is totally positive.

Proposition 3.5. *If* $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$, *then* x *transforms an ambiguous number* α *into an ambiguous number.*

Proof. Since $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ is an ambiguous number, therefore, $bc < 0$. Now, $(\alpha)x = \frac{-1}{2\alpha} = \frac{-a+\sqrt{n}}{2b} = \frac{a_1+\sqrt{n}}{c_1}$, where $a_1 = -a$, $c_1 = 2b$ and $b_1 = \frac{a_1^2 - n}{c_1} = \frac{c}{2}$. Therefore, $b_1 c_1 = bc < 0$. Hence by Lemma 3.2(iii), $(\alpha)x$ is an ambiguous number.

Theorem 3.6. *Let* $\alpha = \frac{a+\sqrt{n}}{c} \in Q(\sqrt{n})$ *be an ambiguous number. Then one of* $(\alpha)y^j$ *for* $j = 1, 2, 3$ *is ambiguous and the other two are totally negative.*

Proof. It is easy to see that $\overline{(\alpha)y^j} = (\overline{\alpha})y^j$, for $j = 1, 2$ and 3. If $(\alpha)y^j$, for $j = 0, 1, 2$ and 3 representing four vertices of a square in a coset diagram, then $\overline{(\alpha)y^j}$, for $j = 0, 1, 2$ and 3 also represent four vertices of a square in a coset diagram.

Since α is an ambiguous number, therefore, $\alpha\overline{\alpha} < 0$. Also one of α and $(\alpha)x$ is positive, and without any loss of generality, we consider the ambiguous number α as positive. So the only possibilities for the signs of $(\alpha)y^j$, for $j = 1, 2$ and 3 are:

α	$(\alpha)y$	$(\alpha)y^2$	$(\alpha)y^3$	$\overline{\alpha}$	$\overline{(\alpha)y}$	$\overline{(\alpha)y^2}$	$\overline{(\alpha)y^3}$
+	–	–	–	–	+	–	–
				–	–	+	–
				–	–	–	+

Hence one of $(\alpha)y^j$ for $j = 1, 2, 3$ is ambiguous and the other two are totally negative.

Theorem 3.7. *If* $\alpha = \frac{a+\sqrt{n}}{2c} \in Q^*(\sqrt{n})$, *then every element in* αG *is of the form* $\frac{a+\sqrt{n}}{2m}$, *where* $m \in Z$ *and* $\alpha G \subseteq Q^*(\sqrt{n})$.

Proof. We can easily tabulate the following information

α	a	b	$2c$
$(\alpha)x$	$-a$	c	$2b$
$(\alpha)y$	$-a-2c$	c	$2(2a+b+2c)$.

Since every element in G is of the form $x^{\varepsilon_1}y^{\eta_1}x^{\varepsilon_2}y^{\eta_2}\cdots x^{\varepsilon_n}y^{\eta_n}$, where $\varepsilon_1 = 0$ or 1, $\varepsilon_2, \varepsilon_3, \ldots, \varepsilon_n = 1$, $\eta_1, \eta_2, \ldots, \eta_n = 1$, 2 or 3 and $\eta_n = 0$, 1, 2 or 3, therefore, every element in αG is of the form $\frac{a+\sqrt{n}}{2m}$, where $m \in Z$. Also the new value of b for any element of αG is an integer, and so $\alpha G \subseteq Q^*(\sqrt{n})$.

Theorem 3.8. *The action of G on the projective line over $Q(\sqrt{n})$ is intransitive.*

Proof. Since n is a positive integer, so it may be even or odd.

Let n be even, that is, $n = 2m$, $m \in Z$. If we take $k = \frac{\sqrt{n}}{2}$, then $a = 0$, $c = 2$ and $b = \frac{a^2 - n}{c} = -m$. Hence $k \in Q^*(\sqrt{n})$. Also if we take $k = \sqrt{n}$, then $k \in Q^*(\sqrt{n})$. Since the elements of the form $\frac{a+\sqrt{n}}{2c}$ and $\frac{a+\sqrt{n}}{2c+1}$ lie in different orbits, as shown in Theorem 3.7, therefore, so do $\sqrt{n}$ and $\frac{\sqrt{n}}{2}$. Thus there are at least two orbits of $Q(\sqrt{n})$. Hence the action of G on the projective line over $Q(\sqrt{n})$ is intransitive.

Let n be odd, that is, $n = 2m+1$, $m \in Z$. If we take $k = \frac{1+\sqrt{n}}{2}$, then $a = 1$, $c = 2$ and $b = \frac{a^2 - n}{c} = -m$ and so $k \in Q^*(\sqrt{n})$. Also if we take $k = \sqrt{n}$, then $k \in Q^*(\sqrt{n})$. Thus there are at least two orbits of $Q(\sqrt{n})$, one containing $\frac{1+\sqrt{n}}{2}$ and the other containing $\sqrt{n}$. Hence the action of G on the projective line over $Q(\sqrt{n})$ is intransitive.

We conclude this paper with the following observations.

Observations 3.9. The situation here is very different from the one in [2]. If α is of the form $\frac{a+\sqrt{n}}{2c}$, then we can find a closed path in the coset diagram of αG in which all the elements are of the form $\frac{a+\sqrt{n}}{2c}$ and they all belong to $Q^*(\sqrt{n})$. But if α is of the form $\frac{a+\sqrt{n}}{2c+1}$, then we can find a closed path in the coset diagram of αG in which all the elements do not belong to $Q^*(\sqrt{n})$.

References

[1] I. Kauser, S. M. Husnaine and A. Majeed, Behaviour of ambiguous and totally positive or totally negative elements of $Q^*(\sqrt{n})$ under the action of the modular group, Math. J. Univ. Punjab 30 (1997), 11-34.

[2] Q. Mushtaq, Modular group acting on real quadratic fields, Bull. Austral. Math. Soc. 37 (1988), 303-306.

[3] Q. Mushtaq and M. Aslam, Group generated by two elements of order 2 and 4, Acta Math. Sinica (N.S.) 9(1) (1993), 48-54.

[4] Q. Mushtaq and M. Aslam, Transitive action of a two generator group on rational projective line, Southeast Asian Bull. Math. 1 (1997), 203-207.

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

[6] S. Mustafa, Group $\langle x, y : x^2 = y^4 = 1 \rangle$ acting on certain fields, M.Phil. Dissertation, Quaid-i-Azam University, Islamabad, Pakistan, 2001.

Department of Mathematics
Quaid-i-Azam University
Islamabad 44000, Pakistan
e-mail: qmushtaq@isb.apollo.net.pk