Quasigroups and Related Systems **14** (2006), 133 − 146

# Actions of a subgroup of the modular group on an imaginary quadratic field

*Muhammad Ashiq and Qaiser Mushtaq*

**Abstract**

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

## 1. Introduction

It is well known [6] that the modular group $PSL(2, Z)$, where $Z$ is the ring of integers, is generated by the linear-fractional transformations $x : z \longrightarrow \frac{-1}{z}$ and $y : z \longrightarrow \frac{z-1}{z}$ and has the presentation $< x, y : x^2 = y^3 = 1 >$ .

Let $v = xyx$, and $u = y$. Then $(z)v = \frac{-1}{z+1}$ and thus $u^3 = v^3 = 1$. So the group $G =< u, v >$ is a proper subgroup of the modular group $PSL(2, Z)$ [1].

The algebraic integer of the form $a + b\sqrt{n}$, where $n$ is square free, forms a quadratic field and is denoted by $Q(\sqrt{n})$. If $n > 0$, the field is a called *real quadratic field*, and if $n < 0$, it is called an *imaginary quadratic field*. The integers in $Q(\sqrt{1})$ are simply called the *integers*. The integers in $Q(\sqrt{-1})$ are called *Gaussian integers*, and the integers in $Q(\sqrt{-3})$ are called *Eisenstein integers*. The algebraic integers in an arbitrary quadratic field do not

2000 Mathematics Subject Classification: 05C25, 11E04, 20G15
Keywords: Imaginary quadratic field, linear fractional transformation, extension field, coset diagram.

necessarily have unique factorization. For example, the fields $Q(\sqrt{-5})$ and $Q(\sqrt{-6})$ are not uniquely factorable. All other quadratic fields $Q(\sqrt{n})$ with $n \leqslant 7$ are uniquely factorizable.

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

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

The imaginary quadratic fields are usually denoted by $Q(\sqrt{-n})$, where $n$ is a square free positive integer. We shall denote the subset

$$\left\{ \frac{a + \sqrt{-n}}{c} : a, \frac{a^2 + n}{c}, c \in Z, c \neq 0 \right\}$$

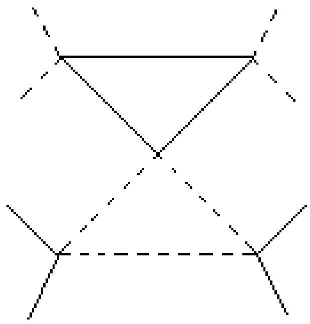
by $Q^*(\sqrt{-n})$. The imaginary quadratic fields are very useful in different branches of mathematics. For example, [3] the Bianchi groups are the groups $PSL_2(O_n)$, where $O_n$ is the ring of integers of the imaginary quadratic number field $Q(\sqrt{-n})$. Also it is known that $O_n$ is an Euclidean ring if and only if $n = 1, 2, 3, 7$ or 11.

In [2, 4], many properties of $Q(\sqrt{n})$ have been discussed. Here we discuss some fundamental results of $G =< u, v : u^3 = v^3 = 1 >$ on $Q^*(\sqrt{-n})$.

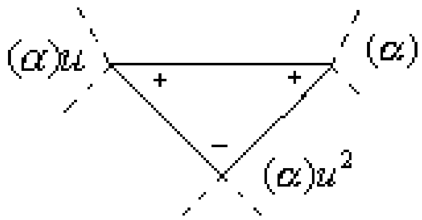
## 2. Coset diagrams

We use coset diagrams, as defined in [4] and [5], for the group $G$ and study its action on the projective line over imaginary quadratic fields. The coset diagrams for the group $G$ are defined as follows. The three cycles of the transformation $u$ are denoted by three unbroken edges of a triangle permuted anti-clockwise by $u$ and the three cycles of the transformation $v$ are denoted by three broken edges of a triangle permuted anti-clockwise by $v$. Fixed points of $u$ and $v$, if they exist, are denoted by heavy dots. This graph can be interpreted as a coset diagram with the vertices identified with the cosets of $Stab_{v_1}(G)$, the stabilizer of some vertex $v_1$ of the graph, or as 1-skeleton of the cover of the fundamental complex of the presentation which corresponds to the subgroup $Stab_{v_1}(G)$. Let $\alpha G$ denote the orbit of $\alpha$ in an action of $G$ on $Q^*(\sqrt{-n})$.

For instance, in the case of $G$ acting on the projective line over the field $Q^*(\sqrt{n})$, a fragment of a coset diagram will look as follows:

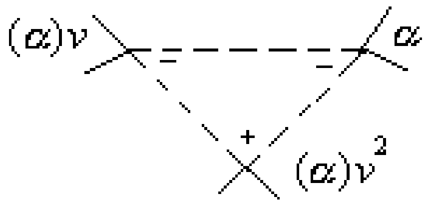


(1) If $k \neq 1, 0, \infty$ then of the vertices $k, ku, ku^2$ of a triangle, in a coset diagram for the action of $G$ on any subset of the projective line, one vertex is negative and two are positive.




(2) If $k \neq -1, 0, \infty$ then of the vertices $k, kv, kv^2$ of a triangle, in a coset diagram for the action of $G$ on any subset of the projective line, one

vertex is positive and two are negative.




**Theorem 1.** *If* $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$, *then* $n$ *does not change its value in* $\alpha G$.

*Proof.* Let $\alpha = \frac{a+\sqrt{-n}}{c}$ and $b = \frac{a^2+n}{c}$. Since $(\alpha)u = \frac{\alpha-1}{\alpha} = 1 - \frac{1}{\alpha} = 1 - \frac{c}{a+\sqrt{-n}} = \frac{b-a+\sqrt{-n}}{b}$. Therefore, the new values of $a$ and $c$ for $(\alpha)u$ are $b-a$ and $b$ respectively. The new value of $b$ for $(\alpha)u$ is $\frac{(b-a)^2+n}{b} = -2a+b+c$. Now $(\alpha)v = \frac{-1}{\alpha+1} = \frac{-c}{a+c+\sqrt{-n}} = \frac{-a-c+\sqrt{-n}}{b+c+2a}$. Therefore the new values of $a$ and $c$ for $(\alpha)v$ are $-a-c$ and $2a+b+c$ respectively. The new value of $b$ for $(\alpha)v$ is $\frac{(-a-c)^2+n}{2a+b+c} = c$. Similarly, we can calculate the new values of $a, b$ and $c$ for $(\alpha)u^2, (\alpha)v^2, (\alpha)uv, (\alpha)u^2v, (\alpha)vu, (\alpha)uv^2, (\alpha)vu^2$ and $(\alpha)v^2u$ as follows:

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

*Table* 1

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

As we know from [5] the real quadratic irrational numbers are fixed points of the elements of $PSL(2,Z) =< x^2 = y^3 = 1 >$ except for the group theoretic conjugates of $x, y^{\pm 1}$ and $(xy)^n$. Now we want to see that when imaginary quadratic numbers are fixed points of the elements of $G$.

## 3. Existence of fixed points in $Q^*(\sqrt{-3})$

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

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

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

If $a + d = 0$ then $g$ is an involution. But there is no involution in $G$. Now, if $a + d = \pm 1$ then as $(trace(g))^2 = \det(g)$, order of $g$ will be three and hence it is conjugate to the linear fractional transformations $u^{\pm 1}$ and $v^{\pm 1}$. Since the fixed points of the linear fractional transformations $u$ and $v$ (by Remark 1) are $\frac{1\pm\sqrt{-3}}{2}$ and $\frac{-1\pm\sqrt{-3}}{2}$ respectively, therefore, the roots of the quadratic equation $cz^2 + (d-a)z - b = 0$ belong to the imaginary quadratic field $Q^*(\sqrt{-3})$. If two elements of $G$ are conjugate, then their corresponding determinants are also equivalent. $\square$

## 4. Orbits of $Q^*(\sqrt{-n})$

**Definition 1.** If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ is such that $ac < 0$ then $\alpha$ is called a *totally negative imaginary quadratic number* and *totally positive imaginary quadratic number* if $ac > 0$.

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

**Theorem 3.**

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

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

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

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

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

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

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

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

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

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

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

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

**Theorem 4.**

(*i*) *If $\alpha = \frac{a+\sqrt{-n}}{c}$ where $c > 0$ then the numerator of every element in $\alpha G$ is also positive.*

(*ii*) *If $\alpha = \frac{a+\sqrt{-n}}{c}$ where $c < 0$ then the numerator of every element in* *the orbit $\alpha G$ is also negative.*

*Proof.* $(i)$ Since $\alpha = \frac{a+\sqrt{-n}}{c}$ with $c > 0$, therefore, $b$ is also positive. As $b$ and $c$ always have the same sign. Using this fact we can easily see from the information given in Table 1 that every element in $\alpha G$ has positive numerator.

$(ii)$ Since $\alpha = \frac{a+\sqrt{-n}}{c}$ with $c < 0$, therefore, $b$ is also negative. As $b$ and $c$ always have the same sign. Using this fact we can easily see from the information given in Table 2 that every element in $\alpha G$ has negative numerator. □

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

**Theorem 5.**

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

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

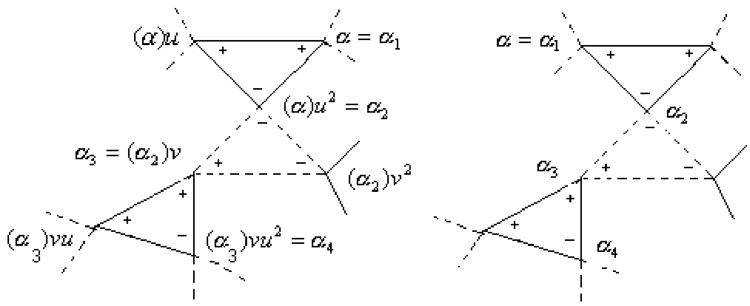
*Proof.* $(i)$ Let $\alpha$ be a totally negative imaginary quadratic number. Then either, $a < 0$ and $b, c > 0$ or $a > 0$ and $b, c < 0$. Let us take $a < 0$ and $b, c > 0$. Then, by Theorem 3$(i)$ $(\alpha)u$ and $(\alpha)u^2$ both are totally positive imaginary quadratic numbers. Thus, $\|(\alpha)u\| = |b - a| > |a| = \|\alpha\|$, and $\left\|(\alpha)u^2\right\| = |c - a| >= |a| = \|\alpha\|$. Similarly, we have the same result for $a > 0$ and $b, c < 0$.

$(ii)$ Let $\alpha$ be a totally positive imaginary quadratic number. Then either, $a$, $b$, $c > 0$ or $a$, $b$, $c < 0$. Let us take $a, b, c > 0$. Now, using the information given in Table 1, we can easily see that $\|(\alpha)v\| = |-a - c| = |a + c| > |a| = \|\alpha\|$ and $\left\|(\alpha)v^2\right\| = |-a - b| = |a + b| > |a| = \|\alpha\|$. Similarly, we have the same result for $a, b, c < 0$. □

**Theorem 6.** *Let $\alpha$ be a totally positive or negative imaginary quadratic number. Then there exists a sequence $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ such that $\alpha_i$ is alternately totally negative and totally positive number for $i = 1, 2, 3, \ldots, m-1$ and $\|\alpha_m\| = 0$ or $1$.*

*Proof.* Let $\alpha = \alpha_1$ be a totally positive imaginary quadratic number. Then, by Theorem 3$(i)$, $(\alpha)u$ or $(\alpha)u^2$ is a totally negative imaginary quadratic number. If $(\alpha)u$ is a totally negative imaginary quadratic number, then put $\alpha_2 = (\alpha)u$ and by Theorem 5$(i)$, $\|(\alpha_1)\| > \|\alpha_2\|$. Now if $(\alpha)u^2$ is a totally negative imaginary quadratic number, then put $\alpha_2 = (\alpha)u^2$. In this case we have also $\|(\alpha_1)\| > \|\alpha_2\|$.

Now if $(\alpha)u$ a is totally negative imaginary quadratic number, then $(\alpha)uv$ or $(\alpha)uv^2$ is a totally positive imaginary quadratic number. If $(\alpha)uv$ is a totally positive imaginary quadratic number, put $(\alpha)uv = \alpha_3$ and so by Theorem 5$(ii)$ $\|(\alpha)uv\| < \|(\alpha)u\| < \|\alpha\|$ or $\|\alpha_3\| < \|\alpha_2\| < \|\alpha_1\|$ and continuing in this way we obtain an alternate sequence $\alpha_1, \alpha_2, \ldots, \alpha_m$ of totally positive and totally negative numbers such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$. Since $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ is a decreasing sequence of non negative integers, therefore, it must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-n}}{c}$ such that $\|\alpha_m\| = |a'| = 0$ or 1. It can be shown diagrammatically as:




□

**Theorem 7.** *There are exactly eight orbits of $Q^*(\sqrt{-n})$ under the action of the group $G$ when $n = 3$.*

*Proof.* As we have seen in Theorem 6, we get a decreasing sequence of non negative integers $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ which must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-3}}{c}$ such that $\|\alpha_m\| = |a'| = 0$ or 1.

If $\alpha_m = \frac{1\pm\sqrt{-3}}{2}$ or $\frac{-1\pm\sqrt{-3}}{2}$ then because $\frac{\pm1\pm\sqrt{-3}}{2}$ are the fixed points of $u$ and $v$, therefore, we cannot reach at an imaginary quadratic number whose norm is equal to zero. So in this case there are four orbits, namely $\frac{1+\sqrt{-3}}{2}G$, $\frac{1-\sqrt{-3}}{2}G$, $\frac{-1+\sqrt{-3}}{2}G$ and $\frac{-1-\sqrt{-3}}{2}G$ of $Q^*(\sqrt{-3})$.

Now, if we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-3}}{c}$ such that $\|\alpha_m\| = |a\prime| = 0$ then $\alpha_m = \frac{\sqrt{-3}}{c}$. Since $\alpha_m = \frac{\sqrt{-3}}{c} \in Q^*(\sqrt{-3})$, therefore, $c = \pm1, \pm3$. That is, $\alpha_m = \frac{\sqrt{-3}}{1}, \frac{\sqrt{-3}}{3}, \frac{\sqrt{-3}}{-1}$, and $\frac{\sqrt{-3}}{-3}$.

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

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

Hence from the above table, we see that $\sqrt{-3}$, $\frac{1+\sqrt{-3}}{4}$ and $\frac{-1+\sqrt{-3}}{4}$ lie in $\alpha G$.

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

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

**Remark 2.**

1. If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$ then $Stab_\alpha(G)$ is non-trivial only if $n = 3$. Particularly, if $\alpha = \frac{\pm 1 \pm \sqrt{-3}}{2}$ then $Stab_\alpha(G) \cong C_3$.
2. In $Q^*(\sqrt{-3})$, there are four elements of norm zero, namely $\frac{\sqrt{-3}}{1}$, $\frac{\sqrt{-3}}{-1}$, $\frac{\sqrt{-3}}{3}$, and $\frac{\sqrt{-3}}{-3}$.
3. In $Q^*(\sqrt{-3})$, there are twelve elements of norm one, namely $\frac{\pm 1 \pm \sqrt{-3}}{2}$, $\frac{\pm 1 \pm \sqrt{-3}}{4}$, and $\frac{\pm 1 \pm \sqrt{-3}}{1}$.

**Theorem 8.** *Let $\alpha \in Q^*(\sqrt{-n})$, where $n \neq 3$. Then*

$(i)$ *if $\alpha = \sqrt{-n}$, then $\sqrt{-n}$, $\frac{1+\sqrt{-n}}{n+1}$ and $\frac{-1+\sqrt{-n}}{n+1}$ lie in $\alpha G$,*

$(ii)$ *if $\alpha = \frac{\sqrt{-n}}{n}$, then $\frac{\sqrt{-n}}{n}$, $\frac{1+\sqrt{-n}}{1}$ and $\frac{-1+\sqrt{-n}}{1}$ lie in $\alpha G$,*

$(iii)$ *if $\alpha = \frac{\sqrt{-n}}{2}$, where $n$ is even and $l_1 = \frac{n}{2}$, then $\alpha$ is the only element of norm zero in $\alpha G$,*

$(iv)$ *if $\alpha = \frac{\sqrt{-n}}{n_1}$, where $k_1 = \frac{n}{n_1}$ and $n_1 \neq 1$, 2 or $n$, then $\alpha$ is the only element of norm zero in $\alpha G$, and*

$(v)$ *if $\alpha = \frac{1+\sqrt{-n}}{c_1}$, where $1 + n = c_1 c_2$ and $c_1 \neq 1$ or $n + 1$, then $\alpha$ is the only element of norm one in $\alpha G$.*

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

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

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

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

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

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

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

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

Hence from the above table, we see that $\alpha$ is the only element of norm zero in $\alpha G$.

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

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

Hence from the above table, we see that $\alpha$ is the only element of norm zero in $\alpha G$.

$(v)$ Let $\alpha = \frac{1+\sqrt{-n}}{c_1}$, where $1+n = c_1c_2$ and $c_1 \neq 1$ or $n+1$, then the new values of $a$, $b$, and $c$ can be calculated as:

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

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

Now if $c_1 \neq 1, 2$ or $\frac{n+1}{2}, n+1$, that is, $c_2 \neq n+1, \frac{n+1}{2}$ or 1, then $\frac{1+\sqrt{-n}}{c_1}$ lie in $\alpha G$. $\square$

**Example 1.** By using Theorem 8, the orbits of $Q^*(\sqrt{-14})$ are:

$(i)$ $\sqrt{-14}$, $\frac{1+\sqrt{-14}}{15}$ and $\frac{-1+\sqrt{-14}}{15}$ lie in $\sqrt{-14}G$,
$(ii)$ $\frac{\sqrt{-14}}{-1}$, $\frac{1+\sqrt{-14}}{-15}$ and $\frac{-1+\sqrt{-14}}{-15}$ lie in $\frac{\sqrt{-14}}{-1}G$,
$(iii)$ $\frac{\sqrt{-14}}{14}$, $\frac{1+\sqrt{-14}}{1}$ and $\frac{-1+\sqrt{-14}}{1}$ lie in $\frac{\sqrt{-14}}{14}G$,
$(iv)$ $\frac{\sqrt{-14}}{-14}$, $\frac{1+\sqrt{-14}}{-1}$ and $\frac{-1+\sqrt{-14}}{-1}$ lie in $\frac{\sqrt{-14}}{-14}G$,
$(v)$ $\frac{\sqrt{-14}}{2}$ lies in $\frac{\sqrt{-14}}{2}G$,
$(vi)$ $\frac{\sqrt{-14}}{-2}$ lies in $\frac{\sqrt{-14}}{-2}G$,
$(vii)$ $\frac{\sqrt{-14}}{7}$ lies in $\frac{\sqrt{-14}}{7}G$,
$(viii)$ $\frac{\sqrt{-14}}{-7}$ lies in $\frac{\sqrt{-14}}{-7}G$,
$(ix)$ $\frac{1+\sqrt{-14}}{3}$ lies in $\frac{1+\sqrt{-14}}{3}G$,
$(x)$ $\frac{-1+\sqrt{-14}}{3}$ lies in $\frac{-1+\sqrt{-14}}{3}G$,
$(xi)$ $\frac{1+\sqrt{-14}}{-3}$ lies in $\frac{1+\sqrt{-14}}{-3}G$,
$(xii)$ $\frac{-1+\sqrt{-14}}{-3}$ lies in $\frac{-1+\sqrt{-14}}{-3}G$,
$(xiii)$ $\frac{1+\sqrt{-14}}{5}$ lies in $\frac{1+\sqrt{-14}}{5}G$, .
$(xiv)$ $\frac{-1+\sqrt{-14}}{5}$ lies in $\frac{-1+\sqrt{-14}}{5}G$,
$(xv)$ $\frac{1+\sqrt{-14}}{-5}$ lies in $\frac{1+\sqrt{-14}}{-5}G$, and
$(xvi)$ $\frac{-1+\sqrt{-14}}{-5}$ lies in $\frac{-1+\sqrt{-14}}{-5}G$.

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

**Remark 3.**

1. If $\alpha = \frac{a+\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$, then $\alpha G$ contains the conjugates of the ele-

ments of $\alpha G$. Since $\alpha = \frac{a+\sqrt{-n}}{c}$ and $\overline{\alpha} = \frac{a-\sqrt{-n}}{c}$ lie in two different orbits, therefore, $\alpha G$ and $\overline{\alpha}G$ are always disjoint.

2. The elements of norm zero and one in $Q^*(\sqrt{-n})$, play a vital role to identify the orbits of $Q^*(\sqrt{-n})$.

**Definition 2.** If $n$ is a positive integer then $d(n)$ denotes the arithmetic function defined by the number of positive divisors of $n$.

For example, $d(1) = 1, d(2) = 2, d(3) = 2, d(4) = 3, d(5) = 2$ and $d(6) = 4$.

**Theorem 9.** *If $n \neq 3$, then the total number of orbits of $Q^*(\sqrt{-n})$ under the action of $G$ are:*

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

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

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

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

**Example 2.** Now, by using Theorem 9,

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

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

and

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

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

**Theorem 10.** *There are $2d(n)$ elements of $Q^*(\sqrt{-n})$ of norm zero under the action of $G$.*

*Proof.* As we have seen in Theorem 6, we get a decreasing sequence of non-negative integers $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ which must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-n}}{c}$ such that $\|\alpha_m\| = |a\prime| = 0$. Thus $\alpha_m = \frac{\sqrt{-n}}{c}$. Since $\alpha_m = \frac{\sqrt{-n}}{c} \in Q^*(\sqrt{-n})$, therefore, $c$ must be a divisor of $n$. Hence there are $2d(n)$ elements of $Q^*(\sqrt{-n})$ of norm zero under the action of $G$. □

**Theorem 11.** *There are $4d(n+1)$ elements of $Q^*(\sqrt{-n})$ of norm one under the action of $G$.*

*Proof.* As we have seen in Theorem 6, there exists a decreasing sequence of non-negative integers $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \ldots > \|\alpha_m\|$ which must terminate and that happens only when ultimately we reach at an imaginary quadratic number $\alpha_m = \frac{a\prime+\sqrt{-n}}{c}$ such that $\|\alpha_m\| = |a\prime| = 1$. Then $\alpha_m = \frac{\pm1+\sqrt{-n}}{c}$, where $b = \frac{a^2+n}{c} = \frac{1+n}{c}$, that is, $c$ must be a divisor of $n+1$. Hence there are $4d(n+1)$ elements of $Q^*(\sqrt{-n})$ of norm one under the action of $G$. □

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

*Proof.* If $n$ is even, then the minimum value of $n$ in $Q^*(\sqrt{-n})$ is two. So, by Theorem 9, the total number of orbits are $2[d(n) + 2d(n+1) - 4] = 2[2 + 2(2) - 4] = 4$. So, the action of $G$ on $Q^*(\sqrt{-n})$ must be intransitive.

Now, if $n$ is odd, then the minimum value of $n$ in $Q^*(\sqrt{-n})$ is five, when $n \neq 3$. So, by Theorem 10, the total number of orbits are $2[d(n) + 2d(n+1) - 6] = 2[2+2(4)-6] = 8$. So, the action of $G$ on $Q^*(\sqrt{-n})$ is intransitive.

According to Theorem 7, there are exactly eight orbits of $Q^*(\sqrt{-n})$ when $n = 3$ under the action of the group $G$. Hence the proof. □

# References


[1] **M. Ashiq and Q. Mushtaq:** *Finite presentation of a linear-fractional group*, Algebra Colloquium **12** (2005), 585 – 589.

[2] **M. Aslam, Q. Mustaq, T. Maqsood and M. Ashiq:** *Real quadratic irrational numbers and the group $< x, y : x^2 = y^6 = 1 >$*, Southeast Asian Bull. Math. **27** (2003), 409 – 415.

[3] **A. W. Mason:** *Free quotients of subgroups of the Bianchi groups whose kernels contain many elementary matrices*, Math. Proc. Camb. Phil. Soc. **116** (1994), 253 – 273.

[4] **Q. Mushtaq:** *Modular group acting on real quadratic fields*, Bull. Austral. Math. Soc. **37** (1988), 303 – 306.

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

[6] **W. W. Stothers:** *Subgroups of the modular group*, Proc. Camb. Philos. Soc. **75** (1974), 139 – 154.

Received February 14, 2006

M. Ashiq
Department of Basic Sciences & Humanities, College of E & ME, National University of Sciences and Technology, Rawalpindi, Pakistan,
E-mail: ashiqjaved@yahoo.co.uk

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