INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Primitive Representations and the Modular Group

Muhammad Nadeem Bari[1]*, **Muhammad Aslam Malik**[1]

1 Department of Mathematics, University of the Punjab, Quaid-e-Azam Campus, Lahore, 54590, Pakistan

OPEN ACCESS

Received: 30-03-2020

Accepted: 19-05-2020

Published: 21.07.2020

Editor: Dr. Natarajan Gajendran

Citation: Nadeem Bari M, Malik MA (2020) Primitive Representations and the Modular Group. Indian Journal of Science and Technology 13(25): 2547-2557. https://doi.org/10.17485/IJST/v13i25.66

*__Corresponding author__.
Muhammad Nadeem Bari
Department of Mathematics, University of the Punjab, Quaid-e-Azam Campus, Lahore, 54590, Pakistan
drnadeembari@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

Abstract

Objectives: Primitive representations are useful to explore the modular group action on real quadratic field. **Methods/Statistical Analysis**: By using primitive representations structure of G-orbit are obtained. **Finding:** Conditions on n and $a,\ b,\ c$ are determined when $\alpha^G=(\bar{\alpha})^G$, $\alpha^G=(-\bar{\alpha})^G$, $\alpha^G=(-\alpha)^G$, $\alpha^G=(\bar{\alpha})^G=(-\bar{\alpha})^G=(-\alpha)^G$ *and* $\alpha^G\neq(\bar{\alpha})^G\neq(-\bar{\alpha})^G\neq(-\alpha)^G$, where $\alpha=\frac{a+\sqrt{n}}{c}$ with $b=\frac{a^2-n}{c}$ is real quadratic irrational number. We also find some elements of modular group PSL(2,$\mathbb{Z}$) that moves α to $\bar{\alpha}$, α to $-\bar{\alpha}$ and α to $-\alpha$. **Applications:** By using these conditions, we can construct the structure of the G-orbit. These results are verified by suitable examples.

Keywords: Primitive Representations; coset diagram; modular group; quadratic field

1 Introduction

Binary quadratic form is one of the subjects treated in elementary number theory. Another subject treated in elementary number theory is the possibility of representing a positive integer as a sum of two squares and difference of two squares. The representations $n=x^2+y^2$ and $n=x^2-y^2$ which are of our interest are special cases of general binary quadratic form $f(x,\ y)=ax^2+bxy+cy^2$ and the representation $n=x^2+y^2$ is primitive representation if $(x,\ y)=1$.

Let $n=k^2\ m$, where k $\in$ N and m is a square free positive integer. Take $Q^*(\sqrt{n})=\{\frac{a+\sqrt{n}}{c}: a,\ b=\frac{a^2-n}{c}, c\in Z,\ c\neq 0\ and\ (a,b,c)=1\}$ and
$Q^*_{red}\ (\sqrt{n})=\left(\alpha\in Q^*(\sqrt{n}):\ \alpha>1\ and\ -1<\bar{\alpha}<0\right\}$. Then
(Q($\sqrt{m}$)\Q)= $U_{k\in N}Q^*\left(\sqrt{k^2m}\right)$ contain $Q^*(\sqrt{n})$ and $Q^*_{red}(\sqrt{n})$ as G-subset and subsets respectively.

If $\alpha=\frac{a+\sqrt{n}}{c}\in Q*(\sqrt{n})$, if α and $\overline{\alpha}$ have different signs, then $\alpha$is said to be an ambiguous number. A quadratic irrational number α is said to be reduced if $\alpha>1$ and $-1<\overline{\alpha}<0$. The modular group $PSL(2,\ \mathbb{Z})$ is the group of all linear fractional transformations $z\rightarrow\frac{sz+t}{uz+v}$ with $sv-tu=1$, where $s,\ v,\ t,\ u$ are integers.

This group can be presented as $G=\left\langle x,y: x^2=y^3=1\right\rangle$, where $x: z\rightarrow\frac{-1}{z}, y: z\rightarrow\frac{z-1}{z}$

Modular group can be written in the matrix form as it is the set of 2×2 matrices with integral entries and determinant 1. It is generated by two matrices X= $\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$, Y = $\begin{bmatrix}1 & -1\\ 1 & 0\end{bmatrix}$ of orders 2 and 3 respectively.

Now the product of two transformations is the same as the product of corresponding matrices. For the sake of simplicity, we use matrices instead of transformations.

A coset diagram is a graph consisting of vertices and edges. It depicts a permutation representation of the modular group G, the 3-cycles of y are denoted by three vertices of a triangle permuted anticlockwise by y and the two vertices which are interchanged by x are joined by an edge.

In [1, 2], types of length 4, 6 satisfying exactly one of the conditions namely $\alpha^G = (\bar{\alpha})^G$, $\alpha^G = (-\bar{\alpha})^G$, $\alpha^G = (-\alpha)^G$, $\alpha^G = (\bar{\alpha})^G = (-\bar{\alpha})^G = (-\alpha)^G$ have been determined.

In [3, 4] formula for total numbers of ambiguous numbers in $Q^*(\sqrt{n})$ is determined. In [5] it is explored that if $p\equiv 1(mod\ 4)$ then $\left(\lfloor\sqrt{p}\rfloor+\sqrt{p}\right)^G$ include circuit of length 2 and in which $\alpha^G = (\bar{\alpha})^G = (-\bar{\alpha})^G = (-\alpha)^G$. In [6] it is describe that if $p\equiv 3(mod\ 4)$ then $\left(\lfloor\sqrt{p}\rfloor+\sqrt{p}\right)^G$ contains circuit of length 2 and in which $\alpha^G = (-\bar{\alpha})^G$.

2 Materials and Methods

Lemma 2.1 [7] Let $\alpha=\frac{a+\sqrt{n}}{c}$ be an ambiguous number. Then $x(\alpha)$, $y(\alpha)$, $y^2(\alpha)$ are always ambiguous numbers.

Lemma 2.2 [8] If a natural number n can be written as sum of two squares of two rational numbers, then n can be written as sum of two squares of two integers.

Lemma 2.3 [9] Any two elements of the same order are conjugate in a group G.

Lemma 2.4 [6] $g\left(\bar{\alpha}\right) = \overline{g(\alpha)}$ for all $g\in G$ and $\alpha \in Q^*(\sqrt{n})$.

3 Results and Discussion

For $\alpha = \frac{a+\sqrt{n}}{c}\in Q^*(\sqrt{n})$, the elements α, $\overline{\alpha}$, $-\alpha$ and $-\overline{\alpha}$ play an important role in the study of modular group action on $Q(\sqrt{m}) \mid Q = U_{k\in N}Q^*(\sqrt{k^2m})$.

In this section we determine the elements of G and conditions on a, b, c when $\alpha^G = (\bar{\alpha})^G$, $\alpha^G = (-\bar{\alpha})^G$.

In the following theorem, we describe the elements of G that moves real quadratic irrational numbers to their conjugates.

Theorem 3.1: If $\alpha = \frac{a+\sqrt{n}}{c}\in Q^*(\sqrt{n})$ is such that $\alpha^G = (\bar{\alpha})^G$, then the element g of G such that $g(\alpha)=\bar{\alpha}$ is of the form g= $(g_1)^{-1}xg_1$ for some $g_1 \in G$.

Proof: Let $\alpha = \frac{a+\sqrt{n}}{c}\in Q^*(\sqrt{n})$ be such that $\alpha^G = (\bar{\alpha})^G$, then there exists an element g= $\begin{bmatrix}s & t\\ u & v\end{bmatrix}$ in G, which satisfy $\frac{s\alpha+t}{u\alpha+v} = \bar{\alpha}$.

That is $s\alpha+t = (u\alpha+v)\bar{\alpha}$.

This implies that $s\alpha+t = u\alpha\bar{\alpha}+v\bar{\alpha}$.

This can be written as $s\left(\frac{a+\sqrt{n}}{c}\right)+t = u\left(\frac{a^2-n}{c^2}\right)+s\left(\frac{-a+\sqrt{n}}{-c}\right)$.

This gives $as+ct = bu+av$, $s = -v$.

So, we have g = $\begin{bmatrix}s & t\\ \frac{2as+ct}{b} & -s\end{bmatrix}$.

Then

$$g^2 = \begin{bmatrix}s & t\\ \frac{2as+ct}{b} & -s\end{bmatrix}\begin{bmatrix}s & t\\ \frac{2as+ct}{b} & -s\end{bmatrix} = \begin{bmatrix}s^2+\frac{2ast+ct^2}{b} & 0\\ 0 & s^2+\frac{2ast+ct^2}{b}\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = I$$

Since g is an element of order 2, but any two elements of same order are conjugate by lemma 2.3. So, g is of the form $g = (g_1)^{-1}xg_1$.

Example 3.1: If $\alpha = \frac{-3+\sqrt{29}}{-10}$, then $\bar{\alpha} = \frac{3+\sqrt{29}}{10}$. The elements which moves α to $\bar{\alpha}$ are y^2xy and $(xy)^4x\left(y^2x\right)^4$ see Figure 1.

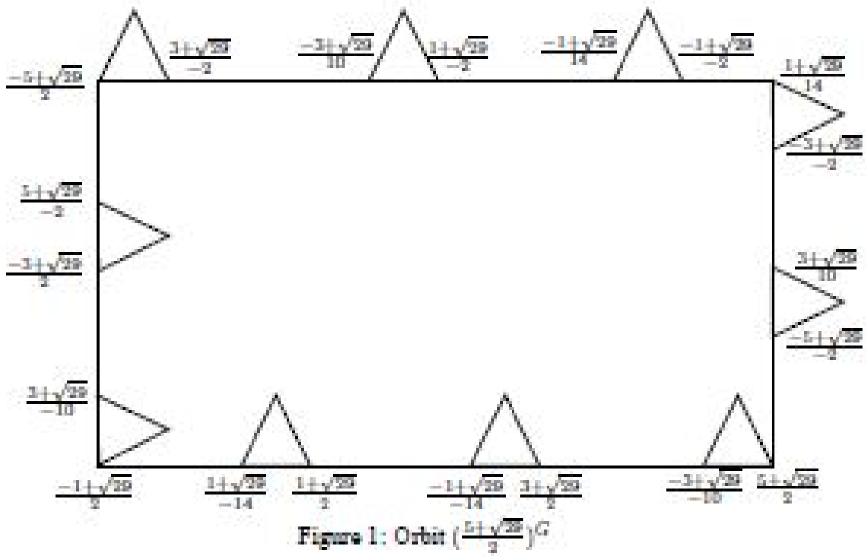

Fig 1. Orbit

But both elements can be written as $y^2xy = y^{-1}xy$ and $(xy)^4x\left(y^2x\right)^4 = \left(\left(y^2x\right)\right)^{-4}x\left(y^2x\right)^4$. Both elements of G are in $C_x = \{g^{-1}xg \, : \, g \in G\}$.

Corollary 3.2: If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$, then $x(\alpha) = \bar{\alpha}$ if and only if $b = -c$.

Proof: As $x\left(\frac{a+\sqrt{n}}{c}\right) = \frac{-a+\sqrt{n}}{-c}$ implies that $\frac{-a+\sqrt{n}}{b} = \frac{-a+\sqrt{n}}{-c}$. So, $b = -c$.

Conversely, if $b = -c$, then $x\left(\frac{a+\sqrt{n}}{c}\right) = \frac{-a+\sqrt{n}}{b} = \frac{-a+\sqrt{n}}{-c}$.

Corollary 3.3: If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$, then $x(\alpha) = \bar{\alpha}$ if and only if n has a primitive representation.

Proof: It has been proved in [5], that $x(\alpha) = \bar{\alpha}$ if and only if $n = a^2 + c^2$. It remains only to show that this representation is primitive.

As $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$, then $(a,\ b,\ c) = 1$. Now by Lemma 3.2, $x(\alpha) = \bar{\alpha}$ if and only if $b = -c$. Thus $(a,\ b,\ c) = (a, -c, c) = (a, c) = 1$. As required.

Remark 3.4 Corollary 3.3 holds only when n has primitive representation.

Example 3.5: Consider $n = 2^2 + 6^2$, then this representation is not primitive. By using corollary 3.3, we have $\alpha = \frac{2+\sqrt{40}}{6}$ corresponding this representation. Then $x(\alpha) = x\left(\frac{2+\sqrt{40}}{6}\right) = \frac{-2+\sqrt{40}}{-6} = \bar{\alpha}$. But $\alpha = \frac{2+\sqrt{40}}{6} = \frac{1+\sqrt{10}}{3} \notin Q * \left(\sqrt{40}\right)$

Corollary 3.6 : If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$ $and\, x(\alpha) = \bar{\alpha}$. Then $x(-\alpha) = -\bar{\alpha}$.

Proof: If $x(\alpha) = \bar{\alpha}$ then by lemma 3.2 $b = -c$.

Now $x(-\alpha) = x\left(\frac{a+\sqrt{n}}{-c}\right) = \frac{-a+\sqrt{n}}{\frac{a^2-n}{-c}} = \frac{-a+\sqrt{n}}{-b} = \frac{-a+\sqrt{n}}{c} = -\,\bar{\alpha}$.

Corollary 3.7 : If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$ $and\, x(\alpha) = \bar{\alpha}$. Then $\left(\frac{c+\sqrt{n}}{a}\right)x = \frac{-c+\sqrt{n}}{-a}$.

Proof: It has been proved in [5], that $x(\alpha) = \bar{\alpha}$ if and only if $n = a^2 + c^2$.

Also $n = c^2 + a^2$ if and only if $x\left(\frac{c+\sqrt{n}}{a}\right) = \frac{-c+\sqrt{n}}{-a}$.

Corollary 3.8: If $\alpha = \frac{\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$, then $x(\alpha) \neq \bar{\alpha}$.

Proof: We prove this result by contradiction.

On contrary, we suppose that $(\alpha) = \bar{\alpha}$.

Then, $x\left(\frac{\sqrt{n}}{c}\right) = \frac{\sqrt{n}}{-c}$. This implies that $\left(\frac{\sqrt{n}}{c}\right) = \frac{\sqrt{n}}{-c}$.

That is, $\left(\frac{\sqrt{n}}{\frac{-n}{c}}\right) = \frac{\sqrt{n}}{-c}$.

Thus $n = c^2$, a contradiction. So, $(\alpha) \neq \bar{\alpha}$.

Example 3.9: If $\alpha = \sqrt{2}$, then $\bar{\alpha} = \frac{\sqrt{2}}{-1}$ and $x\left(\sqrt{2}\right) \neq \frac{\sqrt{2}}{-1}$.

Corollary 3.10: If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ and $x(\alpha) = \bar{\alpha}$, then $\exists\ \gamma \in \alpha^G$ such that $x(\gamma) = \bar{\gamma}$.

Proof: If $x(\alpha) = \bar{\alpha}$, then by theorem 3.1, the elements of G which moves α to $\bar{\alpha}$ are x and $g^{-1}xg$ see example 3.1. One element is in anticlockwise direction, other element is in clockwise direction and g depends on the type of circuit of α^G. Now $g^{-1}xg\ (\alpha) = \bar{\alpha}$ this implies that $xg\ (\alpha) = g\left(\bar{\alpha}\right)$. By substituting $g\ (\alpha) = \gamma$ and using Lemma 2.4, we have $x(\gamma) = \bar{\gamma}$.

In the following theorem we determine condition on ,b, c when $\alpha^G = (-\bar{\alpha})^G$ and this result is verified by a suitable example.

Theorem 3.2: If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is such that either $\frac{-2a}{b}$ or $\frac{-2a}{c}$ is integer, then $\alpha^G = (-\bar{\alpha})^G$.

Proof: **Case I.** If $\frac{-2a}{c} \in \mathbb{Z}$, we show $\alpha^G = (-\bar{\alpha})^G$.

Consider $(yx)^{\frac{-2a}{c}}(\alpha) = \alpha - \frac{2a}{c}$ because $(yx)^l(\alpha) = \alpha + l$.

This implies that, $(yx)^{\frac{-2a}{c}}(\alpha) = \frac{a+\sqrt{n}}{c} - \frac{2a}{c}$.

That is, $(yx)^{\frac{-2a}{c}}(\alpha) = \frac{-a+\sqrt{n}}{c} = -\bar{\alpha}$. So, $\alpha^G = (-\bar{\alpha})^G$.

Case II. If $\frac{-2a}{b} \in \mathbb{Z}$, we show $\alpha^G = \left(-\bar{\alpha}\right)^G$.

Consider $(y^2x)^{\frac{-2a}{b}}(\alpha) = \frac{\alpha}{\frac{-2a(\alpha)}{b}+1}$ because $(y^2x)^l(\alpha) = \frac{\alpha}{l\alpha+1}$.

That is

$$(y^2x)^{\frac{-2a}{b}}(\alpha) = \frac{\frac{a+\sqrt{n}}{c}}{\frac{-2a}{b}\left(\frac{a+\sqrt{n}}{c}\right)+1}$$

After simplification, we have

$$(y^2x)^{\frac{-2a}{b}}(\alpha) = \frac{b\,(a+\sqrt{n})}{-2a^2-2a\sqrt{n}+bc}$$

After rationalization, we have

$$(y^2x)^{\frac{-2a}{b}}(\alpha) = \frac{b\left(-2a^3+abc+2an+bc\sqrt{n}\right)}{(-2a^2+bc)^2-4a^2n}$$

This can be written as

$$(y^2x)^{\frac{-2a}{b}}(\alpha) = \frac{b\left(-2a\left(a^2-n\right)+abc+bc\sqrt{n}\right)}{4a^4+b^2c^2-4a^2bc-4a^2n}$$

After simplification, we have

$$(y^2x)^{\frac{-2a}{b}}(\alpha) = \frac{b(-abc+bc\sqrt{n})}{b^2c^2} = \frac{-a+\sqrt{n}}{c} = -\bar{\alpha}. \text{ So, } \alpha^G = (-\bar{\alpha})^G$$

Following corollary is an immediate consequence of the above result.

Corollary 3.11: If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is such that b or c *divides* $-2a$, then $\alpha^G = (-\bar{\alpha})^G$.

Proof: As in such cases $\frac{-2a}{b}$ or $\frac{-2a}{c}$ becomes integer.

Example 3.12: In the orbit $\left(\frac{2+\sqrt{6}}{1}\right)^G$ as shown in Figure 2 we have $\alpha = \frac{2+\sqrt{6}}{1}$ with $a = 2, c = 1,\ b = -2$.

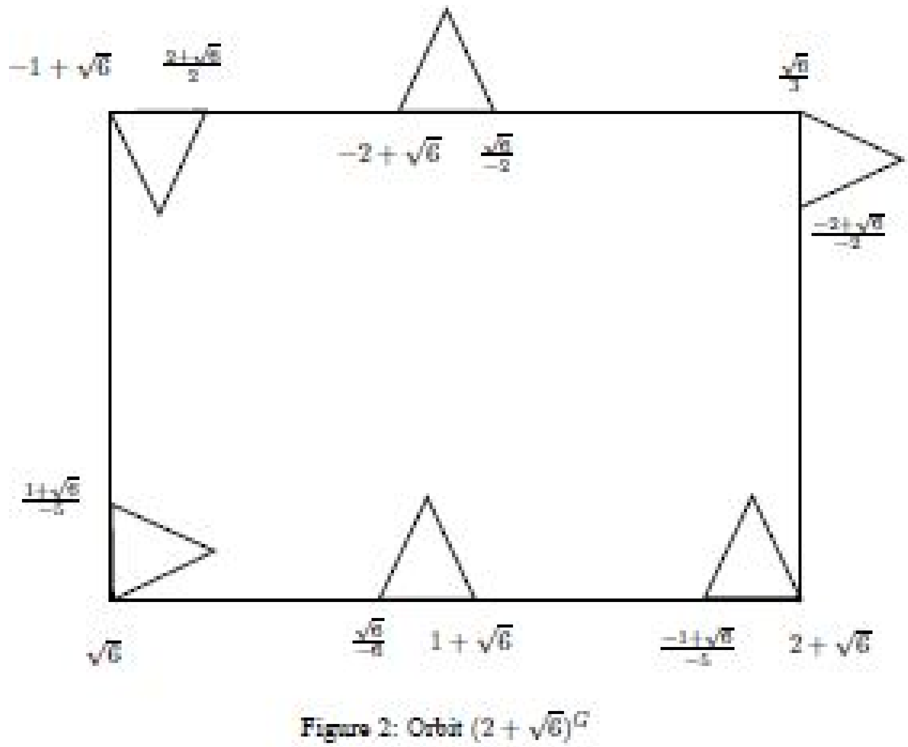

Fig 2. Orbit

Now

$$\frac{-2a}{c}=\frac{-2(2)}{1}=-4.\text{ So, }\left(\frac{2+\sqrt{6}}{1}\right)^{G}=\left(\frac{-2+\sqrt{6}}{1}\right)^{G}$$

Similarly, for $\alpha=\frac{1+\sqrt{6}}{-5}$ with $a=1, c=-5,\; b=1$.
As

$$\frac{-2a}{b}=\frac{-2(1)}{1}=-2,\text{ so }\left(\frac{1+\sqrt{6}}{-5}\right)^{G}=\left(\frac{-1+\sqrt{6}}{-5}\right)^{G}$$

In [1, 2] types of lengths 4, 6 have been determined in which all the four orbits $\alpha^G, (-\alpha)^G, (\bar{\alpha})^G$ and $(-\bar{\alpha})^G$ are distinct.
The following corollary follows from theorem 3.2 and corollary 3.2.

Corollary 3.13: If $\alpha=\frac{a+\sqrt{n}}{c}\in Q^*\left(\sqrt{n}\right)$ is such that $\frac{-2a}{c}$ is integer and b=$-c$, then $\alpha^G=(\bar{\alpha})^G=(-\alpha)^G=(-\bar{\alpha})^G$.

Example 3.14 : In the orbit $\left(\frac{2+\sqrt{5}}{1}\right)^G$ as shown in Figure 3, we have $\alpha=\frac{2+\sqrt{5}}{1}$ with $a=2, c=1,\; b=-1$.

Now $\frac{-2a}{c}=\frac{-2(2)}{1}=-4$ and $b=-c=-1$. So,

$$\left(\frac{2+\sqrt{5}}{1}\right)^{G}=\left(\frac{-2+\sqrt{5}}{1}\right)^{G}=\left(\frac{2+\sqrt{5}}{-1}\right)^{G}=\left(\frac{-2+\sqrt{5}}{-1}\right)^{G}$$

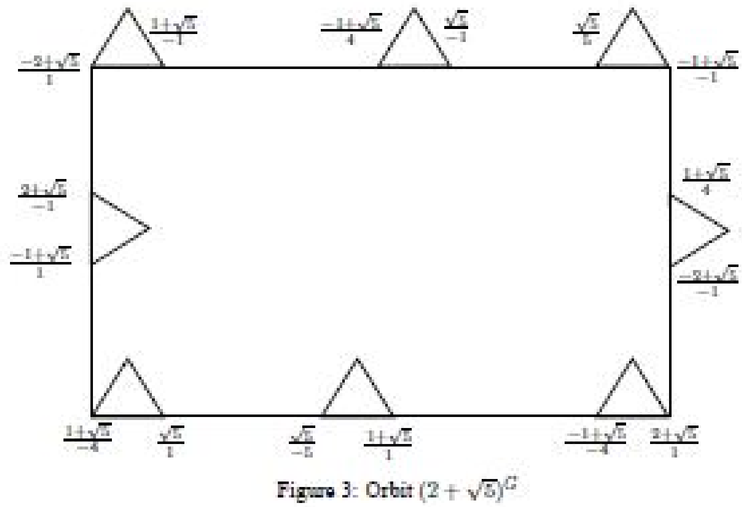

Fig 3. Orbit

Corollary 3.15 : If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is such that $\frac{-2a}{c} \in \mathbb{Z}$ and $b = -c$, then the element of G which moves α to $-\alpha$ is of the form $x(yx)^{\frac{-2a}{c}}$.

Proof: In theorem 3.2, it is derived that if $\frac{-2a}{c} \in \mathbb{Z}$, then $(yx)^{\frac{-2a}{c}}(\alpha) = \frac{-a+\sqrt{n}}{c}$. This implies that $x(yx)^{\frac{-2a}{c}}(\alpha) = x\left(\frac{-a+\sqrt{n}}{c}\right) = \frac{a+\sqrt{n}}{b} = \frac{a+\sqrt{n}}{-c}$. As required.

Corollary 3.16 : If $\alpha = \frac{\sqrt{n}}{c} \in Q^*(\sqrt{n})$ then the element g which moves α to $-\alpha$ is of the form $g = (g_1)^{-1} x g_1$ for some $g_1 \in G$.

Proof: If $\alpha = \frac{\sqrt{n}}{c} \in Q^*(\sqrt{n})$ then in this case $\bar{\alpha} = -\alpha$, so by theorem 3.1 the element g which moves α to $-\alpha$ is of the form g= $(g_1)^{-1} x g_1$ for some $g_1 \in G$.

Corollary 3.17 : If $\alpha = \frac{\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is such that $\left(\frac{\sqrt{n}}{c}\right)^G = \left(\frac{\sqrt{n}}{-c}\right)^G$, then $\alpha^G = (\bar{\alpha})^G = (-\alpha)^G = (-\bar{\alpha})^G$.

Proof: Here $\alpha = \frac{\sqrt{n}}{c}$ then $\frac{-2a}{c} = 0 \in \mathbb{Z}$, so by theorem 3.2, we have $\alpha^G = (-\bar{\alpha})^G$. Also $\left(\frac{\sqrt{n}}{c}\right)^G = \left(\frac{\sqrt{n}}{-c}\right)^G$, then $\alpha^G = (\bar{\alpha})^G = (-\alpha)^G = (-\bar{\alpha})^G$.

Converse of above result is not hold because

$$\left(\frac{1+\sqrt{5}}{2}\right)^G = \left(\frac{-1+\sqrt{5}}{2}\right)^G = \left(\frac{1+\sqrt{5}}{-2}\right)^G = \left(\frac{-1+\sqrt{5}}{-2}\right)^G$$

But the orbit does not contain these ambiguous numbers $\frac{\sqrt{5}}{1}$, $\frac{\sqrt{5}}{-1}$, $\frac{\sqrt{5}}{5}$ and $\frac{\sqrt{5}}{-5}$.

Corollary 3.18: If the orbit α^G is such that $\alpha^G \neq (\bar{\alpha})^G \neq (-\alpha)^G \neq (-\bar{\alpha})^G$, then all ambiguous numbers which lies on G-circuit neither satisfy $\frac{-2a}{c} \in \mathbb{Z}$ nor $b = -c$.

Proof: By taking contrapositive to corollary 3.13, we get this result.

It has been proved in [5], that $(\alpha)x = \bar{\alpha}$ if and only if $n = a^2 + c^2$. In the following theorem, we generalize this result. In particular, we describe the condition on n when $\alpha^G = (\bar{\alpha})^G$.

Theorem 3.3: If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is such that $\alpha^G = (\bar{\alpha})^G$, then n can be written as the sum of two squares and this representation is primitive.

Proof: Let $\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ be such that $\alpha^G = (\bar{\alpha})^G$, then there exists an element g= $\begin{bmatrix} s & t \\ u & v \end{bmatrix}$ in G, which satisfy $\frac{s\alpha+t}{u\alpha+v} = \bar{\alpha}$.

That is $s\alpha + t = (u\alpha + v)\bar{\alpha}$.

This implies that $s\alpha + t = u\alpha\bar{\alpha} + v\bar{\alpha}$.

This can be written as

$$s\left(\frac{a+\sqrt{n}}{c}\right)+t=u\left(\frac{a^2-n}{c^2}\right)+v\left(\frac{-a+\sqrt{n}}{-c}\right)$$

This gives $as+ct=bu+av,\ \ s=\ -v$.

Combining both equations, we have $as+ct=ub-as$.

After simplification, we obtain $-t=\ \frac{2as-ub}{c}$.

But $sv-tu=1$.

By substitution, we have $-s^2+\ \frac{(2as-ub)u}{c}\ =1$.

This can be written as $-cs^2+2asu-bu^2=c$.

After substituting, the value of b, we have

$$-cs^2+2asu-\left(\frac{a^2-n}{c}\right)u^2=c.$$

After simplification, we obtain

$$-cs^2+2asu-\frac{a^2u^2}{c}+\frac{nu^2}{c}=c.$$

This can be written as

$$n=\left(\frac{c}{u}\right)^2+\left(-a+\frac{cs}{u}\right)^2 \tag{1}$$

In this expression $u\neq 0$, because if $u=0$ then $s=-v$ and $sv-tu=1$ implies that $s^2=-1$ which is not possible.

By Lemma 2.2 if a natural number n can be written as sum of two squares of two rational numbers, then n can be written as sum of squares of two integers. It is enough to prove this representation is primitive.

Let $d=(\frac{c}{u},-a+\frac{cs}{u})$. Then $d|\frac{c}{u}$ and $d|(-a+\frac{cs}{u})$.

This shows that $ud|c$ and $ud|(-au+cs)$. That is $ud|cs$ and $ud|(-au+cs)$.

This implies that $ud|(-au+cs-cs)$. So, $d|a$.

Also, $d|c$ and $d^2|n$ From equation 1. Thus, $d^2|(a^2-bc)$, as $d^2|a^2$.

This implies that $d^2|bc$, but $d|c$. So, $d|b$.

Thus $d|\ (a,\ b,\ c)$, but $(a,\ b,\ c)$= 1. So, $d=1$.

Example 3.19 :

In the orbit $\left(\frac{-1+\sqrt{13}}{-6}\right)^G$, the element of G which moves $\frac{-1+\sqrt{13}}{-6}$ to $\frac{1+\sqrt{13}}{6}$ is $y^2\ xy$ as shown in Figure 4 .

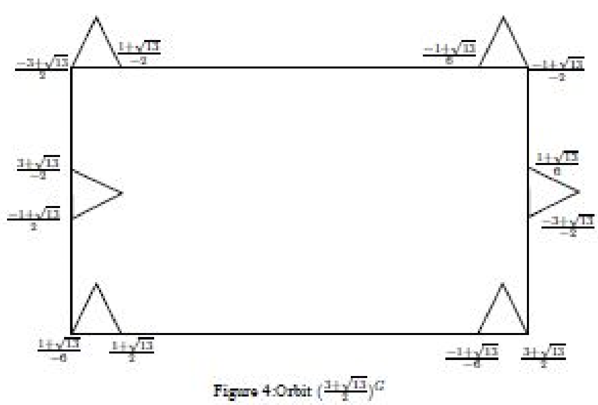

Fig 4. Orbit

Now corresponding element in matrix form is given by:

$$y^2xy = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ -2 & 1 \end{bmatrix}$$

Here $s = -1,\ t = 1,\ u = -2,\ v = 1$ and $a = -1,\ c = -6,\ b = 2$.

Now $n = \left(\frac{c}{u}\right)^2 + \left(-a + \frac{cs}{u}\right)^2$.

After substituting the values of $s,\ t,\ u,\ v,\ a,\ b,\ c$, we get

$$n = \left(\frac{-6}{-2}\right)^2 + \left(-(-1) + \frac{(-6)(-1)}{-2}\right)^2 = 3^2 + 2^2.$$

As required.

In the following theorem, we generalize the results of [5]. In particular, we describe the condition on n when $\alpha^G = (-\alpha)^G$.

Theorem 3.4: If $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$ is such that $\alpha^G = (-\alpha)^G$, then n can be written as the sum of two squares and this representation is primitive.

Proof: Let $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*\left(\sqrt{n}\right)$ be such that $\alpha^G = (-\alpha)^G$, then there exists an element g= $\begin{bmatrix} s & t \\ u & v \end{bmatrix}$ in G, which satisfy $\frac{s\alpha+t}{u\alpha+v} = -\alpha$.

That is $s\alpha + t = -(u\alpha + v)\alpha$.

This implies that $s\alpha + t = -u\alpha^2 - v\alpha$.

This can be written as

$$s\left(\frac{a+\sqrt{n}}{c}\right) + t = -u\left(\frac{a+\sqrt{n}}{c}\right)^2 - v\left(\frac{a+\sqrt{n}}{c}\right).$$

Which gives $\frac{as}{c} + t = \frac{-u\left(a^2+n\right)}{c^2} - \frac{va}{c}$ and $cs = -2au - vc$.

Combining both equations, we have

$$\frac{as}{c} + t = \frac{-u\left(a^2+n\right)}{c^2} - a\left(\frac{-s}{c} - \frac{2au}{c^2}\right)$$

After simplification, we obtain $\frac{as}{c} + t = \frac{acs - un + a^2u}{c^2}$.

This implies that $-t = \frac{-ub}{c}$. But $sv - tu = 1$.

By substituting the value of v and t, we have $s\left(\frac{-2au}{c} - s\right) - \frac{u^2b}{c} = 1$.

After substituting the value of b, we obtain $-s^2 - \frac{2aus}{c} - \frac{u^2\left(a^2-n\right)}{c^2} = 1$.

After some simplification, we have $u^2n = c^2s^2 + 2acus + u^2a^2 + c^2$.

This can be written as

$$n = \left(\frac{c}{u}\right)^2 + \left(\frac{cs+au}{u}\right)^2 \tag{2}$$

In this expression $u \neq 0$, because if $u = 0$ then $s = -v$ and $sv - tu = 1$ implies that $s^2 = -1$ which is not possible.

By Lemma 2.2 if a natural number n can be written as sum of two squares of two rational numbers then n can be written as sum of two squares of two integers. It is enough to prove this representation is primitive.

Let $d = \left(\frac{c}{u}, a + \frac{cs}{u}\right)$. Then $d|\frac{c}{u}$ and $d|\left(a + \frac{cs}{u}\right)$.

This shows that $ud|c$ and $ud|(au + cs)$. This can be written $ud|cs$ and $ud|(au + cs)$.

This implies that $ud|(au + cs - cs)$. So, $d|a$.

Also, $d|c$ and $d^2|n$ From equation 2. Thus $d^2|(a^2 - bc)$, as $d^2|a^2$.

This implies that $d^2|bc$, but $d|c$. So, $d|b$.

Thus $d|(a,\ b,\ c)$, but $(a,\ b,\ c)$= 1. So, $d = 1$.

Example 3.20:

In the orbit $\left(\frac{3+\sqrt{17}}{2}\right)^G$, the element of G which moves $\frac{3+\sqrt{17}}{2}$ to $\frac{3+\sqrt{17}}{-2}$ is $x\left(y^2x\right)^3 yxy^2\, x$ as shown in Figure 5.

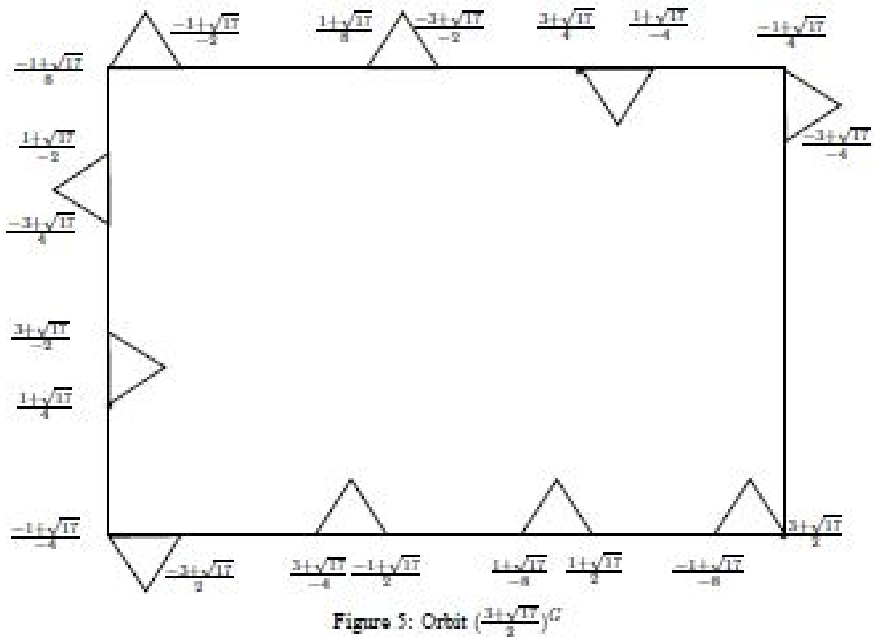

Fig 5. Orbit

Now corresponding element in matrix form is given by:

$$x\left(y^2x\right)^3 yxy^2x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} -7 & -4 \\ 2 & 1 \end{bmatrix}$$

Here $s=-7,\ t=-4,\ u=\ 2,\ v=1$ and $a=3,\ c=2,\ b=-4$.

Now $n=\left(\frac{c}{u}\right)^2+\left(a+\frac{cs}{u}\right)^2$.

After substituting the values of $s,\ t,\ u,\ v,\ a,\ b,\ c$, we get

$$n=\left(\frac{2}{2}\right)^2+\left((3)+\frac{(2)(-7)}{2}\right)^2=1^2+4^2.$$

As required.

Theorem 3.5 If $\alpha=\frac{a+\sqrt{n}}{c}\in Q^*\left(\sqrt{n}\right)$ is such that $\alpha^G=\left(-\bar{\alpha}\right)^G$, then n can be written as the difference of two squares of two rational numbers.

Proof: Let $\frac{a+\sqrt{n}}{c}\in Q^*\left(\sqrt{n}\right)$ be such that $\alpha^G=\left(-\bar{\alpha}\right)^G$, then there exists an element g= $\begin{bmatrix} s & t \\ u & v \end{bmatrix}$ in G , which satisfy $\frac{s\alpha+t}{u\alpha+v}=-\bar{\alpha}$.

That is $s\alpha+t=-\left(u\alpha+v\right)\bar{\alpha}$.

This implies that $s\alpha+t=-u\alpha\bar{\alpha}-v\bar{\alpha}$.

This can be written as

$$s\left(\frac{a+\sqrt{n}}{c}\right)+t=-u\left(\frac{a^2-n}{c^2}\right)-v\left(\frac{-a+\sqrt{n}}{-c}\right).$$

This gives $as+ct=-bu-av,\ \ s=\ v$.

Combining both equations, we have $2as+ct+ub=0$.

After simplification, we obtain $-t=\ \frac{2as+ub}{c}$.

But $sv-tu=1$. By substitution, we have $s^2+\ \frac{(2as+ub)u}{c}\ =1$.

This can be written as $cs^2+2asu+bu^2=c$.

After substituting, the value of b, we have

$$cs^2 + 2asu + \left(\frac{a^2 - n}{c}\right) u^2 = c.$$

After simplification, we obtain

$$cs^2 + 2asu + \frac{a^2u^2}{c} - \frac{nu^2}{c} = c.$$

This can be written as

$$n = \left(a + \frac{cs}{u}\right)^2 - \left(\frac{c}{u}\right)^2$$

If $u = 0$, then $t \neq 0$. Otherwise $g = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

In the similar way, by eliminating s and u we can obtain $n = \left(a + \frac{bv}{t}\right)^2 - \left(\frac{b}{t}\right)^2$. *As required*.

Example 3.21: In the orbit $\left(\frac{2+\sqrt{8}}{1}\right)^G$, the element of G which moves $\frac{2+\sqrt{8}}{1}$ to $\frac{-2+\sqrt{8}}{1}$ is $y^2\,x$ as shown in Figure 6.

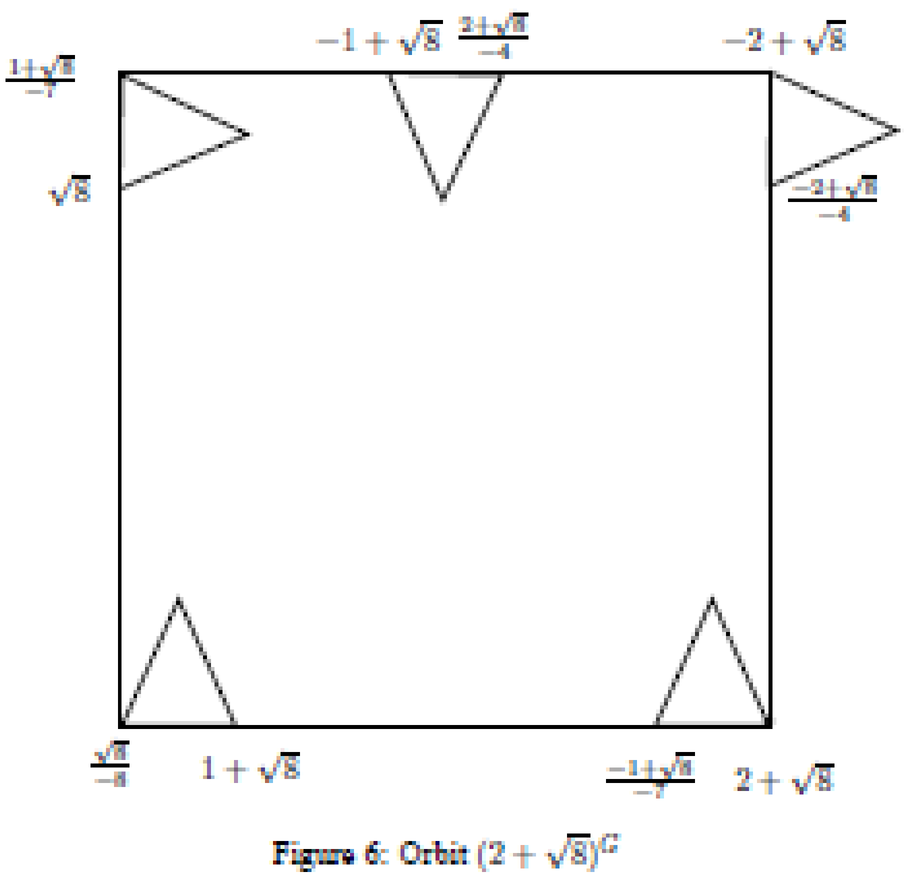

Fig 6. Orbit

Now corresponding element in matrix form is given by $y^2x = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

Here $s=1,\ t=0,\ u=\ 1,\ v=1$ and $a=2,\ c=1,\ b=-4$.
Now $n=\left(a+\frac{cs}{u}\right)^2-\left(\frac{c}{u}\right)^2$.
After substituting the values of $s,\ t,\ u,\ v,\ a,\ b,\ c$ in equation 3, we get
$n=\left((2)+\frac{(1)(1)}{1}\right)^2-\left(\frac{1}{1}\right)^2=3^2-1^2$. As required.
The element of G which moves $\frac{1+\sqrt{8}}{1}$ to $\frac{-1+\sqrt{8}}{1}$ is $yxy^2\ xyx$ as shown in Figure 6.
Now corresponding element in matrix form is given by

$$yxy^2xyx=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}=\begin{bmatrix}2 & 3\\ 1 & 2\end{bmatrix}$$

Here $s=2,\ t=3,\ u=\ 1,\ v=2$ and $a=1,\ c=1,\ b=-7$.
Now $n=\left(a+\frac{cs}{u}\right)^2-\left(\frac{c}{u}\right)^2$.
After substituting the values of $s,\ t,\ u,\ v,\ a,\ b,\ c$ in equation 3, we get

$$n=\left((1)+\frac{(1)\,(2)}{1}\right)^2-\left(\frac{1}{1}\right)^2=3^2-1^2$$

As required.

4 Conclusion

The idea of study the elements that moves α to $\bar{\alpha}$, α to $-\bar{\alpha}$ and α to $-\alpha$ given in this paper is new and original. We have determined the conditions on n and a, $b,\ c$ when $\alpha^G=\ (-\bar{\alpha})^G$, $\alpha^G=\ (-\alpha)^G$,$\alpha^G=\ (\bar{\alpha})^G$, $\alpha^G=\ (-\bar{\alpha})^G$=$(-\alpha)^G$=$(\bar{\alpha})^G$ and$\alpha^G\neq(-\bar{\alpha})^G\neq(-\alpha)^G\neq(\bar{\alpha})^G$, where $\alpha\in Q^*\left(\sqrt{n}\right)$ under the action of modular group G. These results are verified by some suitable examples.

References

1. Aslam MA, Sajjad A. Reduced Quadratic Irrational Numbers and Types of G-circuits with Length Four by Modular Group. *Indian Journal of Science and Technology.* 2018;11(30):1-7.
2. Sajjad A, Aslam MA. Classification of PSL(2, Z) Circuits Having Length Six. *Indian Journal of Science and Technology.* 2018;11(42):1-18.
3. Aslam M, Husnine S, Majeed A. Modular group action on certain quadratic fields. *Punjab University Journal of Mathematics.* 1995;28:47-68.
4. Husnine S, Aslam M, Majeed A. On ambiguous numbers of an invariant subset of under the action of the modular group PSL(2, Z). *Studia Scientcrum Mathematic Arum Hungarica.* 2005;42(4):401-412.
5. Aslam M, Husnine S, Majeed A. The Orbits of Q^* (√p), p=2 or p≡1(mod 4) Under the action of Modular Group. *Punjab University Journal of Mathematics.* 2000;33:37-50.
6. Aslam M, Husnine S, Majeed A. The Orbits of Q^* (√p), p≡3(mod 4) Under the action of Modular Group. *Punjab University Journal of Mathematics.* 2003;36:1-14.
7. Mushtaq Q. Modular group acting on real quadratic fields. *Bulletin of the Australian Mathematical Society.* 1988;37(2):303-309.
8. Adler A, John EC. *The Theory of Numbers.* London: Jones and Bartlett Publishers, Inc 1995.
9. Humphreys J. *A Course in Group Theory.* Liverpool: Oxford University Press 1996.