Quadratic Fields under the Action of Subgroups of M

Farkhanda Afzal, Qamar Afzal, and M. Aslam Malik

***Abstract*—Quadratic fields are a basic object of study and class of examples in algebraic number theory. While we look at group acting on a set, we hope to gain insight into the symmetry of set, at the same time, to obtain a better feel for the group. Group actions on fields have diverse applications in physics, symmetries, algebraic geometry and cryptology. Congruence is nothing more than a statement of divisibility. However, it often helps to discover proofs and it suggests new ideas to solve the problems. Therefore the congruence classes have been used to explore the action of Möbius groups on quadratic fields. We investigate some proper subgroups of the Mobius group M and used an important subgroup M' of M in order to investigate the proper $M-subsets$ of $Q(\sqrt{m})$. This paper particularly demonstrates the actions of Mobius groups M' and in particular it has been proved that $Q^*(\sqrt{n})$ is invariant under the action of M'.**

***Index Terms*—Congruence, group action, linear transformations, mobius groups, quadratic fields.**

I. Introduction

In the mathematical field of representation theory, group representations describe abstract groups in terms of linear transformations of vector spaces; in particular, they can be used to represent group elements as matrices so that the group operation can be represented by matrix multiplication. Representations of groups are important because they allow many group-theoretic problems to be reduced to problems in linear algebra, which is well-understood. They are also important in physics because, for example, they describe how the symmetry group of a physical system affects the solutions of equations describing that system.

The term representation of a group is also used in a more general sense to mean any "description" of a group as a group of transformations of some mathematical object. More formally, a "representation" means a homomorphism from the group to the automorphism group of an object. If the object is a vector space we have a linear representation. Some people use realization for the general notion and reserve the term representation for the special case of linear representations.

Group representations are a very important tool in the study of finite groups. They also arise in the applications of finite group theory to crystallography and to geometry. If the field of scalars of the vector space has characteristic p, and if p divides the order of the group, then this is called modular representation theory; this special case has very different properties

Group acting on a set involves thinking of elements of group as doing something to elements of other set, rather than as things satisfying a seemingly arbitrary list of axioms. For example in the group of symmetries of the square, the elements of the group rotate or reflect the point of square.

Quadratic Fields are a rudimentary object of study and class of examples in Algebraic Number theory. The theory of Numbers is closely tied to other areas of Mathematics most especially to Abstract Algebra, but also Linear Algebra, Combinatorial Structures, Geometry and even Topology

Theory of Numbers sometimes called the higher arithmetic is one of the oldest areas of Mathematics. In a broader sense it is concerned with the properties of the positive integers including divisibility, greatest common divisor of two integers and the study of primes and composite numbers. The problems and conjectures in the number theory are by and large easy to state but often quite difficult to prove.

The Theory of Congruence was introduced by Card Friedrich Gauss (1777-1855) one of the greatest Mathematicians of all times. Although, Pierre De Fermat (1601-1665) had earlier studied Number Theory. The Congruence is nothing more than a statement of divisibility. However, it often helps to discover proofs and we see that Congruence suggests new ideas to solve the problems that will lead to further interesting ideas.We have used congruence classes to explore the action of Möbius groups on the real quadratic fields in this paper.

The Möbiustransformations are projective transformations of the complex projective line. Together with its subgroups, it has numerous applications in mathematics and physics. Möbius transformations are named in honor of August Ferdinand Möbius (1790-1868); they are also variously named homographic transformations, linear fractional transformations, bilinear transformations or fractional linear transformations. August Ferdinand Möbius was a German Mathematician and a theoretical astronomer. His interest was in Number theory also. The important Möbius Function and the Möbius inversion formula are named after him. Möbius Groups have always been of ardent attention in finding group actions on quadratic fields.

Our interest is to discover linear transformation in general x, y satisfying the relations $x\text{^}2 = y\text{^}m = 1$, with a view to studying an action of the group $\langle x, y \rangle$ on real quadratic fields. The group $\langle x, y \rangle$ is trivial when $m = 1$. If $m = 2$, it is an infinite dihedral group and does not give inspiring information while studying its action on the real quadratic irrational numbers. For $m = 3$, the group $\langle x, y \rangle$ is a modular group $PSL(2, Z)$.

We are concerned in the group $\langle x, y \rangle$for $m = 6$.That is $M = \langle x, y;\ x^2 = y^6 = 1 \rangle$.

Manuscript received March 2, 2013; revised May 28, 2013.

Farkhanda Afzal is with the School of Mathematics and System Sciences, Beihang University, Beijing, China. (e-mail: farkhanda_imran@live.com).

Qamar Afzal and M. Aslam Malik are with the Department of Mathematics, University of Education, Okara, Pakistan. (e-mail: qamarafzal.edu@gmail.com, aslampu786@gmail.com).

G Higman introduced coset diagrams for showing the action of modular groups on number fields. QaiserMushtaq laid the foundation and developed it further.

In 1989, the extended modular group acting on the projective line over a Galois field is investigated. Some special circuits in coset diagrams have been shown. The authors discussed the group generated by two elements of orders 2 and 4 acting on real quadratic field. They have shown that ambiguous numbers in $Q^*(\sqrt{n})$ are finite and that part of the coset diagram containing these numbers forms a single closed path under the action of G and the set is invariant under the action of G [12]-[16].

The action of two generated group $H = \langle y, t: y\text{^}4 = t\text{^}4 = 1 \rangle$on $Q(\sqrt{m})$ has been studied by using the coset diagram. It has also been shown that if α is of the form $(\alpha + \sqrt{n})/2c$ then every element in the orbit αH is also of the form $(\alpha\text{^}' + \sqrt{n})/(2c')$ and $\alpha H \subset Q\text{^} * (\sqrt{n})$[8].

These results were generalized by using the notion of congruence. It has been proved that for each square free positive integer n>2, the action of group G on $Q\text{^} * (\sqrt{n})$ is intransitive[9]. Some significant properties of real quadratic irrational numbers under the action of $M = \langle x, y : x\text{^}2 = y\text{^}6 = 1 \rangle$has been presented in [11].

In [4] a classification of the real quadratic irrational numbers $(a + \sqrt{n})/c$ of $Q^*(\sqrt{n})$ with respect to $modulo 3^r$has been presented. A general formula has been ascertained for this classification, by finding and subdividing the elements into the corresponding classes.

A relationship among the actions of Group G and M on $Q(\sqrt{m})$ is established and an algorithm has also been generated by using Visual Basic for calculating the congruence classes of different moduli and manipulating the group action [3].

The notion of subgroups for finding the action of modular groups has been introduced and an important subgroup M' of M has been familiarized in this context. The system of linear congruence is acquainted in order to discover $M\ subsets$ [2].

II. Preliminaries

Let us write $g(\alpha)$ or α^g for the elements of X to which g moves α. In this way we think of a group G as acting on system X. The action is determined when for $g \in G$ and $\alpha \in X$ the corresponding element $g(\alpha)$ is specified. This simple notion of a **group action** has proved very fruitful. We shall find it profitable to build from a definition which generalizes the initial idea. Now we define the notion of a group action on a set.

Let us consider a group G and non-empty set X.

Define a mapping: $\varphi: GxX \longrightarrow X$ by $\varphi(g, \alpha) = g(\alpha)$ for $\alpha \in X$, $g \in G$. If $g(h(\alpha)) = gh(\alpha)$ and $e(\alpha) = \alpha$ for $g, h \in G, \alpha \in X$.

Then X is called $G - set$ and the elements of G may be operated upon with respect to the operation defined on G.

A finite group G is called a finitely generated group if it has a finite set of generators.

Properties: Every finite group is obviously finitely generated. Every finitely generated group in countable and any quotient of finitely generated is finitely generated.

An algebraic integer of the form $a + b\sqrt{m}$, where m is a square free, forms a **quadratic field** and is denoted by $Q(\sqrt{m})$. If $m > 0$, then $Q(\sqrt{m})$ is called **real quadratic field**. If $m < 0$, then it is called imaginary quadratic field.

Every real quadratic irrational number can be written uniquely as $(a + \sqrt{n})/c$ where n is a non-square positive integer and a, $((a\text{^}2 - n))/c, c$ are relatively prime integers.

Möbius Transformation or Map is a function f of a complex variable z that can be written in the form:
$f(z) = (az + b)/(cz + b)$ for some complex numbers $a, b, c\ and\ d$ with $ad - bc \neq 0$.

Let f be the Möbius map given above andIf $c \neq 0$, we define$f(\infty) = a/c, f(-d/c) = \infty$.

If $c = 0$, we define $f(\infty) = 0$.

Note: It is easy to see that for $ad - bc = 0$ the function f becomes constant.

$$f(z) - f(w) = ((ad - bc)(z - w))/((cz + d)(cw + d))$$

$$for\ ad = bc\ \ f(z) - f(w) = 0$$

$$\Longrightarrow f(z) = f(w)$$

The set $C \cup \{\infty\}$ is called the Extended Complex Plane. The set of all Möbius Transformation forms a group under composition called the **Möbius group.** Every Möbius map is a bijection of $C \cup \{\infty\}$onto itself, and the Möbius map form the Möbius group M with respect to the composition.

One of the most important subgroups of Möbius group is the modular group $PSL(2, Z)$. Consisting of all Linear Functional Transformation:

$x'$and y', where $x': Z \longrightarrow -\frac{1}{Z}$ and $y': Z \longrightarrow \frac{(Z-1)}{Z}$Another important subgroup of modular group is defined as: $M = \langle x, y: x\text{^}2 = y\text{^}6 = 1 \rangle$,where:

$$x: z \longrightarrow -\frac{1}{3z} \text{and } y: z \longrightarrow -\frac{1}{3(z+1)}$$

are fractional linear transformations. In our work we are mainly concerned with M.

Let $n = k^2 m$, where m a square free positive integer and $k > 0$ be an integer, then

$$Q^*(\sqrt{n}) := \left\{ \frac{a + \sqrt{n}}{c} : a, 0b := \frac{a^2 - n}{c}, 0\ c \in Z \text{ and } \left(a, 0\frac{a^2 - n}{c}, 0c\right) = 1 \right\}$$

is a proper $G -$ subset of $Q(\sqrt{m})$ for all k.

Let $n = k^2 m$, where m is a square free positive integer and k is any non –zero integer, then $Q'''(\sqrt{n})$ and $Q^{***}(\sqrt{n})$ are defined as

$$Q'''(\sqrt{n}) = \left\{ \frac{\alpha}{t}; \alpha \in Q^*(\sqrt{n});\ t = 1, 3 \right\}$$

$$Q^{***}(\sqrt{n}) = \left\{ \frac{a + \sqrt{n}}{c} \in Q^*(\sqrt{n}):\ 3|c \right\}$$

Aslam *et al*. [5] have proved that the subsets $Q'''(\sqrt{n})Q^{***}(\sqrt{n})$ of $Q(\sqrt{m})$ are M-subsets of $Q(\sqrt{m}) \cup \{\infty\}$.

They have also shown that:

$$Q'''(\sqrt{n}) = \left\{\frac{\alpha}{t}; \alpha \in Q^*(\sqrt{n});\ t = 1,3\right\}$$

is invariant under the action of M.

It was shown in [5] that for $n \not\equiv 0 (\mathrm{mod}\ 9)$, then

$$Q^{***}(\sqrt{9n}) \cup \left\{\frac{a}{3};\ a = \frac{3a+\sqrt{9n}}{c} \in Q^*(\sqrt{n}) \middle|\ Q^{***}(\sqrt{9n})\right\}$$

is an $M-$subset of $Q'''(\sqrt{n})$, where

$$Q^{***}(\sqrt{9n}) = Q'''(\sqrt{n}) \middle|\ Q^{***}(\sqrt{n})$$

Lemma 2.1[4]:

Let *n* be non-square positive integer.

$$\alpha \in Q^*(\sqrt{n}) \text{with} b = (a^2 - n)/c.$$

If $n \not\equiv 0\ (mod\ 9)$, then $\alpha/3$ belongs to $Q^*(\sqrt{n}\ )$ if and only if $3 \mid b$.

$\alpha/3$belongs to $Q^*(\sqrt{9n}\ )$ if and only if $3 \nmid b$.

If n and m are two distinct integers then $Q^*(\sqrt{n}\ )$ and $Q^*(\sqrt{m}\ )$ are disjoint sets whereas $Q''''(\sqrt{n})$ and $Q''''(\sqrt{m})$are not necessarily disjoint [2].

In this paper we describe few important results relevant to action of some subgroups of Mobius group:

$M = \langle x, y: x\text{^}2 = y\text{^}6 = 1\rangle$on the real quadratic fields and we proof that $Q^*(\sqrt{n}\ )$is invariant under the action of M'.

Our first lemma produces that if $(a+\sqrt{n})/c \in Q^{***}(\sqrt{n}\ )$ with $n \equiv 0\ (mod\ 3)$ then $a \equiv 0\ (mod\ 3\ )$.

Lemma 2.2: Let $(a+\sqrt{n})/c \in Q^{***}(\sqrt{n}\ )$ with $n \equiv 0\ (mod\ 3)$ then $a \equiv 0\ (mod\ 3\ )$ only.

Proof:

As we know that $a^2 - bc \equiv n\ (mod\ 3)$.

Thus$a^2 \equiv bc + n\ (mod\ 3)$.

So $a\text{^}2 \equiv 0\ (mod\ 3)$.

Since $c \equiv 0\ (mod\ 3)$ for all $(a+\sqrt{n})/c \in Q\text{^}(***)(\sqrt{n})$. Therefore $a \equiv 0\ (mod\ 3)$.

III. SUBGROUPS OF *M*

We present the concept of subgroups of the Mobius group M in [2] and explore the action of some important subgroups of M on $Q(\sqrt{m}\ )$. A subgroup of a group M is a subset of M which itself form a group under the operation defined on the group M.

Since M is a finitely generated group. Then it contains infinitely many two generator subgroups. Given group M and an element x of M, the set of all powers of x is a subgroup of M. Then this subgroup is called the subgroup generated by x and written $\langle x \rangle$.

It is observed here that investigating the actions through the subgroups gives very useful and interesting results and this will become a fruitful technique to explore more M - subsets.

IV. A SUBGROUP *M*'

Let us focus mainly in studying an action of group M':

$M' = \langle u, v \rangle$ where $u = xy$ and $v = yx$ are linear fractional transformations:

$$u: \alpha \longrightarrow \alpha + 1 \text{ and} v: \alpha \longrightarrow \alpha/(1-3\alpha)$$

It is easy to see that:

$$u^n = \alpha + n \text{and} v^n = \alpha/(1-3n(\alpha)\ )\ ; n = 1,2,\cdots$$

These equations imply that u , v are of infinite order.

By using fundamental relations between $u$and v, we can derive more relations. Since each $g \in M'$is a word in xy, yx, y^2 and y^4. Therefore $u, v, (vu), u(vu), u(vu)^2, (vu)v$ and $(vu)^2$ are important elements of M'. Since for u, v are generators of M', $u = xy$ and $v = yx$.

Note that:

$$vu = yxxy = y^2 \text{and} uv = xyyx = xy^2\, x$$

Clearly , $(vu)^3 = (uv)^3 = 1$.

The group *G* and *M*' are overlapping.

Since, $xy = y'\, x'$then $xy\,(\alpha) = y'\, x'\,(\alpha)$, for all$\alpha \in Q^*(\sqrt{n})$.

Therefore one of the generators of the group M' can be written in the words of the group G but other generator of M' that is yx cannot be written in the words of G. Thus G and $M'$are not same rather both groups are overlapping. In the next section we explore the $M-subsets$.

Lemma 4.1[4]:

Let $M = \langle x, y: x^2 = y^6 = 1 \rangle$ and $M' = \langle u, v \rangle$, then $\langle M',\ x \rangle = M$.

We also notice that many subgroups of the of Mobius group M exist.

Let us take $M'' = \langle xy \rangle$and $M''' = \langle yx \rangle$.

Notice that $\langle xy, x \rangle = M$ and $\langle yx, x \rangle = M$ which ensures that $\langle M'',\ x\rangle = M$ and $\langle M''', x\rangle = M$.

Thus M', M'' and M''' are the proper subgroups of the Möbius group M.

Since we are concerned here with two generator groups, therefore the group $M\text{^}'$ is of much importance.

Now we discuss properties of real quadratic irrational numbers under the action of M'. In particular we prove that $Q^*(\sqrt{n})$ is invariant under the action of M'. For this we need the following lemmas.

Lemma 4.2:

Let $G = \langle x', y': x'^2 = y'^3 = 1$ and $M = \langle x\, y: x^2 = y6=1$.

Consider $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})\backslash Q^{***}(\sqrt{n})$.

Then $xy\,(\alpha) \in Q^*(\sqrt{n})$ and $yx\,(\alpha) \in Q^*(\sqrt{n})$.

Proof:

Clearly xy = y′x′ .Since y′x′ ∈ G.

Therefore $xy\,(\alpha) \in Q^*(\sqrt{n})$ for all $\alpha \in Q^*(\sqrt{n}\ ) as\ \ Q^*(\sqrt{n}\ )$ is invariant under the action of G.

Let $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}\ )$.

Then $3\alpha = \frac{3a+\sqrt{9n}}{c}$, where$b' = \frac{9a^2-9c}{c} = 9b$

Put $3\alpha = \frac{a'+\sqrt{n'}}{c'}; a' = 3a, b' = 9b, c' = c$

$(a,b,c) = 1 \Leftrightarrow (3a, 9b, c) = 1 \ \because c \not\equiv 0 \pmod 3$.

Thus $y''x'(3\alpha) \in Q^*(\sqrt{n})$

$\because x', y'', PSL(2,Z)$.

$$y''x'(3\alpha) = \frac{3a - 9b + \sqrt{9c}}{-6a + 9b + c} \quad \text{by Table I}$$

$$\frac{1}{3}y''x'(3\alpha) = \frac{a - 3b + \sqrt{n}}{-6a + 9b + c}$$

This implies that

$$a'' = a - 3b,\ b'' = b,\ c'' - 6a + 9b + c$$

Since $c \not\equiv 0 \pmod 3$, therefore $c'' \not\equiv 0 \pmod 3$

$$\Rightarrow (a'', b'', c'') = 1$$

$$\Rightarrow \frac{1}{3}y''x'(3\alpha) \in Q^*(\sqrt{n})$$

We know that:

$$yx(\alpha) = \frac{1}{3}y''x'(3\alpha)$$

Therefore, $yx(\alpha) \in Q^*(\sqrt{n})$

This completes the proof.

In the last lemma it has been proved that $Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ is invariant under the actions of xy and yx. Also we know, if a non-square positive integer $n \equiv 1,3,4,6 \text{ or } 7 \pmod 9$ then $Q^{***}(\sqrt{n})$ is invariant underthe actions of xy and yx.

Thus we need to show that for each $n \equiv 0 \pmod 9$, $Q^{***}(\sqrt{n})$ is invariant under the actions of xy and yx. For this we have the following theorem.

Theorem 4.1:

If $n \equiv 0 \pmod 9$ be a non-square positive integer then $xy(\alpha)$ and $yx(\alpha) \in Q^{***}(\sqrt{n})$ for all $\alpha \in Q^*(\sqrt{n})$.

Proof:

Let $n \equiv 0 \pmod 9$ and $(a + \sqrt{n})/c \in Q^{***}(\sqrt{n})$.

Then from Lemma 2.1, we have $a \equiv 0 \pmod 3$.

Also b≢0(mod 3)$\because (a,b,c) = 1$.

Now $\alpha = (a + \sqrt{n})/c$

$$\Rightarrow \alpha aah = (3a' + \sqrt{9n'}))/3c'$$

$$\Rightarrow \alpha = \frac{a' + \sqrt{n'}}{c'}$$

$$\Rightarrow b = \frac{9a'^2 - 9n'}{3c'}$$

$$= 3[(a'^2 - n')/c'] = 3b'$$

Since $b \not\equiv 0 \pmod 3$, so $3 \mid c'$.

Therefore we take $c' = 3c''$.

$$\text{Thus} \quad = \left(\frac{a' + \sqrt{n'}}{3c''}\right) \qquad (1)$$

Also $(a,b,c) = 1 \Leftrightarrow (a', b', c'') = 1$.

[1] $x'y'(3\alpha) = x'y'\left(3\left(\frac{a' + \sqrt{n'}}{3c''}\right)\right)$ by Equation(1).

$$\Rightarrow x'y'(3\alpha) = x'y'\left(\frac{a' + \sqrt{n'}}{c''}\right)$$

$b' = \frac{a'^2 - n'}{c''}$ and $\frac{a' + \sqrt{n'}}{c''} \in Q^{***}(\sqrt{n'})$

$$x'y'(3\alpha) = \left(\frac{a' - b' + \sqrt{n'}}{2a' + b' + c''}\right) \text{ by Table I}$$

Thus, $\frac{1}{3}[x'y'(3\alpha)] \in Q^{***}(\sqrt{9n'})$ by Lemma 2.2.

Therefore :

$$yx(\alpha) = \frac{1}{3}y''x'(3\alpha) = \frac{1}{3}x'y'(3\alpha) \in Q^{***}(\sqrt{n})$$

$$\Rightarrow yx(\alpha) \in Q^{***}(\sqrt{n}).$$

Also, $xy(\alpha) = y'x'(\alpha) \in Q^{***}(\sqrt{n})$ is obvious. Therefore, $xy, yx \in Q^{***}(\sqrt{n})$ for all $\alpha \in Q^{***}(\sqrt{n})$ .Hence the result.

V. Conclusion

We conclude this paper with the following immediate consequences: $Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ is invariant under the action of $M'.Q^{***}(\sqrt{n})$ is invariant under M for $n \equiv 1,3,4,6 \text{ or } 7 \pmod 9$. Since $M'$is a subgroup of M. So the result holds for M' also If$n \equiv 0 \pmod 9$, be a non-square positive integer then $Q^{***}(\sqrt{n})$is invariant under the action of $M' = \langle xy, yx \rangle$.The idea of action through subgroups can be extended to other Mobius groups. Furthermore action of subgroups can be defined for imaginary quadratic fields and one can get several interesting results.

Appendix

	α	***a***	***b***	***c***
$x(a)$	$\frac{-1}{3\alpha}$	$-a$	$\frac{c}{3}$	$3b$
$y(a)$	$\frac{-1}{3(\alpha+1)}$	$-a$	$\frac{c}{3}$	$3(2a+b+c)$
$y^2(a)$	$\frac{-(\alpha+1)}{3\alpha+2}$	$-5a-3b-2c$	$2a+b+c$	$12a+9b+4c$
$y^3(a)$	$\frac{-(3\alpha+2)}{3(2\alpha+1}$	$-7a-6b-2c$	$\frac{12a+9b+4c}{3}$	$3(4a+4b+c)$
$y^4(a)$	$\frac{-(2\alpha+1)}{3\alpha+1}$	$-5a-6b-c$	$4a+4b+c$	$6a+9b+c)$
$y^5(a)$	$\frac{-(3\alpha+1)}{3\alpha}$	$-a-3b$	$\frac{(6a+9b+c)}{3}$	$3b$
$xy(a)$	$\alpha+1$	$a+c$	$2a+b+c$	c
$xy^2(a)$	$\frac{3\alpha+2}{3(\alpha+1)}$	$5a+3b+2c$	$\frac{(12a+9b+4c)}{3}$	$3(2a+b+c)$

$xy^3(a)$	$\frac{2\alpha+1}{3\alpha+2}$	$7a+6b+2c$	$4a+4b+c$	$12a+9b+4c$
$xy^4(a)$	$\frac{3\alpha+1}{3(2\alpha+1}$	$5a+6b+c$	$\frac{(6a+9b+c)}{3}$	$3(4a+4b+c)$
$xy^5(a)$	$\frac{\alpha}{3\alpha+1}$	$a+3b$	b	$6a+9b+c$
$yx(a)$	$\frac{\alpha}{1-3\alpha}$	$a-3b$	b	$-6a+9b+c)$
$y^2x(a)$	$\frac{1-3\alpha}{3(-1+2\alpha)}$	$5a-6b-c$	$\frac{(-6a+9b+c)}{3}$	$3(-4a+4b+c$
$y^3x(a)$	$\frac{1-2\alpha}{-2+3\alpha)}$	$7a-6b-2c$	$-4a+4b+c$	$-12a+9b+4c$
$y^4x(a)$	$\frac{2-3\alpha}{3(-1+\alpha)}$	$5a-3b-2c$	$\frac{(-12a+9b+4c)}{3}$	$3(-2a+b+c)$
$y^5x(a)$	$\alpha-1$	$5a-3b-2c$	$-2a+b+c$	c

ACKNOWLEDGMENT

The authors wish to thank the anonymous referees for their helpful comments. Our paper improved after making corrections and adaptations according to referee's guidelines.

REFERENCES

[1] A. Adler and J. E Coury, *The Theory of Numbers*, by Jones and Barlett Publishers, 1995.

[2] F. Afzal, Q. Afzal, and M. A, Malik, "Modular Group Action on Quadratic Field by Linear congruence," *Novi Sad Journal of Mathematics*, vol. 42, no. 2, pp. 127 – 137, 2012.

[3] F. Afzal, Q. Afzal, and M. A. Malik, "A Classification of the Real Quadratic irrational numbers $(a+\sqrt{n})/c$ of Q^* ($\sqrt{n}$) w.r.t modulo 3^r," *International Mathematical Forum*, vol. 7, no. 39, pp. 1915–1924, 2012.

[4] F. Afzal , I. S. Bhatti, and M. A. Malik, "Action of G and M on $Q(\sqrt{m}$) & Algorithmic Implementation of Group Actions," *Journal of Hyperstructures*, vol. 1, no. 1, pp. 42 – 52, 2012.

[5] K. H. Rosen, *Elementary Number Theory and its Applications*, by AT&T Laboratories, 2005.

[6] M. Ashiq, "Action of a Two Generated Group on Real Quadratic Fields," *Southeast Asian Bulletin of Mathematics*, vol. 30, pp. 399-404, 2006.

[7] M. Aslam, Q. Mushtaq, T. Masood, and M. Ashiq, "Real Quadratic irrational numbers and the group $\langle x, y; x^2=y^6=1\rangle$," *Southeast Asian Bulletin of Mathematics*, vol. 27, pp. 409-415, 2003.

[8] M. Aslam and Q. Mushtaq, "Action of $\langle y, t; y^4=t^4=1\rangle$ on $Q(\sqrt{n}$)," *Southeast Asian Bulletin of Mathematics*, vol. 31, pp. 1049-1056, 2007.

[9] M. A. Malik, S. M. Husnine, and A. Majeed, "On Invariant subsets of certain Quadratic Fields under Modular Group Action," *PUJM*, vol. 29, pp. 20-26, 1996.

[10] M. A. Malik, S. M. Husnine, and A. Majeed, "Action of a group $M=\langle x,y; x^2=y^6=1\rangle$ on Certain Real Quadratic Fields," *PUJM*, vol. 36, pp. 71-88, 2003-4.

[11] M. A. Malik, S. M. Husnine, and A. Majeed, "Action of a group $M=\langle x,y; x^2=y^6=1\rangle$ on Certain Real Quadratic Fields-II," *PUJM*, vol. 43, pp. 1-7, 2012.

[12] Q. Mushtaq, "Some Remarks on Coset Diagrams for the Modular Group. Math," *Chronical*, vol. 16, pp. 69-77, 1987.

[13] Q. Mushtaq, "Modular Group Acting on Real Quadratic Fields," *Bull Austral, Math*, Soc. vol. 37, pp. 303-309, 1988.

[14] Q. Mushtaq, "The Extended Modular Group Acting on the projective line over a Galois Field," *Indian J. Pure App. Math*, vol. 20, no. 8, pp. 755-760, 1989.

[15] Q. Mushtaq and F. Shaheen, "Some Special Circuits in Coset Diagrams," *Math. Japonica*, vol. 37, no. 1, pp. 149-158, 1992.

[16] Q. Mushtaq and M. Aslam, "Group Generated by Two Elements of Orders Two and six acting on R and $Q(\sqrt{n}$)," *Discrete Mathematics*, vol. 179, pp. 145-154, 1998.

Farkhanda Afzal is a Ph.D. scholar at School of Mathematics and System Sciences, Beihang University, Beijing, China. She has completed her MS from University of the Punjab, Lahore Pakistan in 2008.MsFarkhanda has taught as a lecturer Mathematics at University of Education, Lahore, Krl Model College for Women, Kahuta and Bahria University, Islamabad, Pakistan for four years till 2012. She is a member of Mathematical Science Research Institute (MSRI), Berkeley, USA. International Association of Computer Science and Information Technology (IACSIT), Singapore and SCIence and Engineering Institute (SCIEI), USA. Her interests are Abstract Algebra, Group Theory, Number Theory, Computer Algebra and Symbolic Computation.

Qamar Afzal is serving as lecturer Mathematics in Department of Mathematics, University of Education, Okara, Pakistan. She has obtained her MS degree in Pure Mathematics from University of the University of the Punjab, Lahore in 2010. Her interests include Pure Mathematics especially Algebra, Group Theory and Number Theory.

M. Aslam Malik is an associate professor at Department of Mathematics, University of the Punjab, Lahore, Pakistan. Dr. Aslam Malik obtained Ph.D. from University of the Punjab, Lahore Pakistan in 2004 . Then he served as an Assistant Professor at Government College University Lahore and as a visiting faculty in Lahore University of Management Sciences. After that he went United Kingdom for Post Doc at Birmingham University and completedin 2007. Since then he is serving at University of the Punjab, Lahore. He is also anAssociate Editor, Punjab University Journal of Mathematics. His interests area are Pure Mathematics particullary Algebra, Group Theory, Number Theory and Graph Theory