Research Journal of Applied Sciences, Engineering and Technology 5(6): 1916-1922, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: June 07, 2012 Accepted: July 09, 2012 Published: February 21, 2013

$\mathbb{Q}(\sqrt{m})\setminus\mathbb{Q}$ Under the Action of $PSL_2(\mathbb{Z})\cap\langle x,y : x^2 = y^6 = 1\rangle$

M. Aslam Malik and M. Asim Zafar
Department of Mathematics, University of the Punjab Quaid-e-Azam Campus,
Lahore-54590, Pakistan

Abstract: This study is concerned with the natural action (as Möbius transformations) of some subgroups of $PGL_2(\mathbb{Z})$ on the elements of quadratic number field over the rational numbers. We start with two groups- the full modular group $G = PSL_2(\mathbb{Z})$ and another group of Möbius transformations $M = \langle x,y : x^2 = y^6 = 1\rangle$. We consider different sets of numbers with fixed discriminants in the quadratic field and look at structure of the orbits orbits of the actions of G, M, $G\cap M$ and their subgroups on these sets. The results of earlier studies on the number of orbits and the properties of elements belonging to them are extended by similar results related to the new twist connected to the group *M* which has nontrivial intersection with *G* and opens a possibility to look at orbits which were not computed in earlier studies.

Keywords: G-set, legendre symbol, linear fractional transformations

INTRODUCTION

A non-empty set Ω with an action of the group G on it, is said to be a G set. We say that Ω is a transitive G-set if, for any p,q in Ω there exists a g in G such that $p^g = q$. Since every element of $\mathbb{Q}(\sqrt{m})\setminus\mathbb{Q} = \{t + w\sqrt{m} : t,0 \neq w \in \mathbb{Q}\}$ can 122^3be expressed uniquely as $\frac{a+\sqrt{n}}{c}$, where $n = k^2m$, K is any positive integer and $a,b = \frac{a^2-n}{c}$ and c are relatively prime integers and we denote it by $\alpha(a,b,c)$. Then:

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

is a proper G-subset of $\mathbb{Q}(\sqrt{m})\cup\{\infty\}$ and since $\mathbb{Q}^*(\sqrt{n})\cap\mathbb{Q}^*(\sqrt{n'}) = \varphi$ for distinct n,n' non-square integers so $\mathbb{Q}(\sqrt{m})\setminus\mathbb{Q}$ is the disjoint union of $\mathbb{Q}^*(\sqrt{k^2m})$ for all $k \in \mathbb{N}$. Thus it reduces the study of action on $\mathbb{Q}(\sqrt{m})/Q$ to the study of action on $\mathbb{Q}^*(\sqrt{n})$. If $\alpha(a,b,c) \in \mathbb{Q}^*(\sqrt{n})$ and its conjugate $\bar{\alpha}$ have opposite signs then α is called an ambiguous number (Mushtaq, 1988). The actual number of ambiguous numbers in $\mathbb{Q}^*(\sqrt{n})$ has been discussed by Husnine *et al*. (2005) as a function of n. The classification of the elements of $\mathbb{Q}^*(\sqrt{n})$ in the form $[a,b,c]$ modulo p has been given by Farkhanda *et al*. (2012).

This study is concerned with the natural action (as Möbius transformations) of some subgroups of $PGL_2(\mathbb{Z})$ on the elements of quadratic number field over the rational numbers. That is it investigate the study of action on projective line over rationals with emphases on irrationals of the form $\frac{a+\sqrt{n}}{c}$ with $(a,\frac{a^2-n}{c},c) = 1$. We start with two groups-the full modular group $G = \langle x',y' : x'^2 = y'^3 = 1\rangle$ where $x'(z) = \frac{-1}{z}$ and $y'(z) = \frac{-1}{z+1}$ and another group of Möbius transformations $M = \langle x,y : x^2 = y^6 = 1\rangle$, $x(z) = \frac{-1}{3z}$ and $y(z) = \frac{-1}{3(z+1)}$ (Sahin and Bizim, 2003). We consider different sets of numbers with fixed discriminants in the quadratic field and look at different orbits of the action of G, M, $G\cap M$ and their subgroups on these sets. The results of earlier studies (Aslam *et al*., 2003-04, 2012; Aslam and Zafar, 2011) on the numbers of orbits and the properties of elements belonging to them are extended by similar results related to the new twist connected to the group *M* which has nontrivial intersection with *G* and opens a possibility to look at orbits which were not computed in earlier studies.

Corresponding Author: M. Aslam, Department of Mathematics, University of the Punjab, Quaid-e-Azam Campus, Lahore-54590, Pakistan

Table 1: The action of elements of G on $\alpha \in \mathbb{Q}^*(\sqrt{n})$

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

Since $xy = y'x'$ and $yx = (x'y')^3$ so one of the interesting subgroups of $G \cap M$ is $M^* = \langle xy, yx \rangle$. We determine, for each non-square n, the all M^*-subsets of $\mathbb{Q}^*(\sqrt{n})$ by using classes $[a,b,c](mod\ n)$ and we prove that for each M^* subset A of $\mathbb{Q}^{***}\sqrt{n}) = \{\alpha(a,b,c) \in \mathbb{Q}^*(\sqrt{n}) : 3 \mid c\}$ or $\mathbb{Q}^*(\sqrt{n}) \setminus \mathbb{Q}^{***}(\sqrt{n})$, $A \cup x'(A)$ is a G-subset of $Q^*(\sqrt{n})$. We also prove that for each M^* subset A of $\mathbb{Q}^{***}(\sqrt{n})$, $A \cup x(A)$ is an M-subset of $Q^{***}(\sqrt{n})$ or $\mathbb{Q}^{*\cdot}(\sqrt{n})$ according as $n \not\equiv 0(mod\ 9)$ or $n \equiv 0(mod\ 9)$ similarly if A is an M^* subset of $\mathbb{Q}^*(\sqrt{n}) \setminus \mathbb{Q}^{***}(\sqrt{n})$ then $A \cup x(A)$ is an M-subset of $\mathbb{Q}^{*\cdot}(\sqrt{9n}) = (\mathbb{Q}^*(\sqrt{n}) \setminus \mathbb{Q}^{***}(\sqrt{n})) \cup \mathbb{Q}^{***}(\sqrt{9n})$ for each non-square n. Thus M^*-subsets (resp. M^*-orbits) help us in determining the M-subsets and G-subsets (resp. M-orbits and G-orbits) of $\mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$.

PRELIMINARIES

We quote from Andrew and John (1995), Aslam *et al*. (2003-2004, 2005), Aslam and Zafar (2011) and Afzal *et al*. (2012) the following results for later reference. Also We tabulate the actions on $\alpha(a,b,c) \in \mathbb{Q}^*(\sqrt{n})$ of x', y' and x, y ,the generators of G and H respectively, in Table 1 and 2.

Theorem 1:

- If $(a,p) = 1$, then $x^2 \equiv a(mod\ p^k)$ has no solutions if $x^2 \equiv a(mod\ p)$ is not solvable and exactly two solution if $x^2 \equiv a(mod\ p)$ is solvable.
- Suppose a is an odd integer. Then $x^2 \equiv a(mod\ 2^k)$, with $k \geq 3$, is solvable if and only if

Table 2: The action of elements of M on $\alpha(a,b,c) \in \mathbb{Q}^*(\sqrt{n})$

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

$a \equiv 1(mod\ 8)$, in which case there are exactly four solutions. In particular, if S is any solution, then all of the solutions are given by ±s and ±s + 2^{k-1}. For k = 3, x = 1, 3, 5, 7 (mod 2^3) are exactly four solutions (Andrew and John, 1995).

Theorem 2: $Q^{'''}(\sqrt{n}) = \{\frac{\alpha}{t} : \alpha \in Q^{*}(\sqrt{n}), t = 1,3\}$ is invariant under the action of M (Aslam *et al*., 2003-2004).

Theorem 3: For each $n \equiv 1,3,4,6 \ or \ 7(mod\ 9)$, $Q^{***}\sqrt{n}) = \{\alpha(a,b,c) \in Q^{*}(\sqrt{n}) : 3 \mid c\}$ is an M-subset of $Q^{'''}(\sqrt{n})$ (Aslam *et al.*, 2003-2004).

Theorem 4: Let $n \equiv 0(mod\ 3)$. Then the sets $A_1^3 = \{\alpha \in Q^{*}(\sqrt{n}) : c \equiv 1(mod\ 3)\}$ and $A_2^3 = \{\alpha \in Q^{*}(\sqrt{n}) : c \equiv 2(mod\ 3)\}$ are two M^{*}-subsets of $Q^{*}(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ depending upon classes [a, b, c] modulo 3 (Afzal *et al*., 2012).

Theorem 5: Let $n \equiv 0(mod\ 3)$. Then the sets $B_1^3 = \{\alpha \in Q^{***}(\sqrt{n}) : b \equiv 1(mod\ 3)\}$ and $B_2^3 = \{\alpha \in Q^{***}(\sqrt{n}) : b \equiv 2(mod\ 3)\}$ are two M^{*}-subsets of $Q^{***}(\sqrt{n})$ depending upon classes [a, b, c] modulo 3 (Afzal *et al*., 2012).

Theorem 6: If $n \equiv 0 \ or \ 3(mod\ 4)$, then $S = \{\alpha \in Q^{*}(\sqrt{n}) : b \ or \ c \equiv 1(mod 4)\}$ and $-S = \{\alpha \in Q^{*}(\sqrt{n}) : b \ or \ c \equiv -1(mod\ 4)\}$ are exactly two disjoint G-subsets of $Q^{*}(\sqrt{n})$ depending upon classes [a, b, c] modulo 4 (Aslam *et al*., 2005).

Theorem 7: If $n \equiv 1(mod\ 4)$, then $Q'(\sqrt{n}) = \{\alpha \in Q^{*}(\sqrt{n}) : 2 \mid (b, c)\}$ and $Q^{*}(\sqrt{n}) \setminus Q'(\sqrt{n}) = \{\alpha \in Q^{*}(\sqrt{n}) : 2 \ (b,c)\}$ are both G-subsets of $Q^{*}(\sqrt{n})$ (Aslam *et al*., 2005).

Theorem 8: Let p be an odd prime factor of n. Then both of $S_1^p = \{\alpha \in Q^{*}(\sqrt{n}) : (b/p) \ or \ (c/p) = 1\}$ and $S_2^p = \{\alpha \in Q^{*}(\sqrt{n}) : (b/p) \ or \ (c/p) = -1\}$ are G-subsets of $Q^{*}(\sqrt{n})$. In particular, these are the only G-subsets of $Q^{*}(\sqrt{n})$ depending upon classes [a, b, c] modulo p (Aslam and Zafar, 2011).

ACTION OF $PSL_2(Z) \cap (x, y: x^2 = y^6 = 1)$ ON $Q^{*}(\sqrt{n})$

Recall that $G = \langle x', y' : x'^{2} = y'^{3} = 1 \rangle$, $M = \langle x, y : x^2 = y^6 = 1 \rangle$, where $x'(\alpha) = \frac{-1}{\alpha}$, $y'(\alpha) = \frac{\alpha - 1}{\alpha}$, $x(\alpha) = \frac{-1}{3\alpha}$ and $y(\alpha) = \frac{-1}{3(\alpha + 1)}$. The proper subset $Q^{*}(\sqrt{n})$ of $Q(\sqrt{m}) \setminus Q$ is invariant under the action of modular group G but $Q^{*}(\sqrt{n})$ is not invariant under the action of Möbius group *M*. Thus it motivates us to establish a connection between the elements of the groups *G* and *M* and hence to deduce a common subgroup $M^{*} = \langle xy, yx \rangle$ of both groups under the action of which both $Q^{***}(\sqrt{n})$ and $Q^{*}(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ are invariant. Which helps us in finding the G-subsets of $Q^{*}(\sqrt{n})$ and M-subsets of $Q^{***}(\sqrt{n})$, $Q^{*:}(\sqrt{n}) = (Q^{*}(\sqrt{\frac{n}{9}}) \setminus Q^{***}(\sqrt{\frac{n}{9}})) \cup Q^{***}(\sqrt{n})$ according as $n \not\equiv 0(mod\ 9)$ or $n \equiv 0(mod\ 9)$ and $Q^{*:}(\sqrt{n}) = (Q^{*}(\sqrt{n}) \setminus Q^{***}(\sqrt{n})) \cup Q^{***}(\sqrt{9n})$ for all non-square *n*. The following Lemma shows the relationships between the elements of *G* and *M* (Table 1 and 2).

Lemma 1: Let x', y' and x, y be the generators of G and M respectively defined above (Afzal *et al*., 2012). Then we have:

- $y^2 = (x'y')^2(x'y'^2)(x')$ and $y^3 = \frac{1}{3}(x'(y')^2)(x'y')(x'(y')^2)(x')$
- $y^4 = [(x'y')^2(x'y'^2)(x')]^2$ and $y^5 = \frac{1}{3}(x'(y')^2)(x'y')^2(y'^2x')$
- $xy = y'x'$ and $yx = (x'y')^3$
- $xy^2 = \frac{1}{3}(y'x')^2((y')^2x')$ and $xy^3 = ((y')^2x')(y'x')(y'^2x')$
- $xy^4 = \frac{1}{3}(y'x')^2(y'^2x')^2$ and $xy^5 = ((y')^2x')^3$
- $x' = 3x$ and $y' = (3x)(3y)(3x)$
- $x'y' = 3(yx)\frac{1}{3}$ and $x'(y')^2 = y^5x$. In particular $(x'y') = 3(yx)\frac{1}{3}$ and $(x'(y')^2) = y^5x$

The following corollary is an immediate consequence of Lemma 1.

Corollary 1:

- By Lemma 1, since $xy = y'x'$ and $yx = (x'y')^3$ so $M^{*} = \langle xy, yx \rangle$ is a common subgroup of G and M

where xy, yx are the transformations defined by $xy(\alpha) = \alpha + 1$ and $yx(\alpha) = \frac{\alpha}{1-3\alpha}$.

- As yxxy = y^2, xyyx = xy^2x, so $\langle y^2, xy^2x \rangle$ is a proper subgroup of M^*.
- $\langle M^*, x \rangle = \langle M^*, y \rangle = M$ and $\langle M^*, x' \rangle = \langle M^*, y' \rangle = G +$

We now see the action of this subgroup M^* on $Q^*(\sqrt{n})$ where n has an odd prime factor.

Theorem 9: Let $p \neq 3$ be an odd prime factor of n. Then $S_1^p = \{\alpha \in Q^*(\sqrt{n}) : (b/p) \text{ or } (c/p) = 1\}$ and $S_2^p = \{\alpha \in Q^*(\sqrt{n}) : (b/p) \text{ or } (c/p) = -1\}$ are two M^*-subsets of $Q^*(\sqrt{n})$. In particular, these are the only M^*-subsets of $Q^*(\sqrt{n})$ depending upon classes [a, b, c] modulo p.

Before proving this theorem and running through a few quick consequences, we quote here two Lemmas 2 and 3 from Malik and Asim (2012). These results give us the classification of the elements of $Q^*(\sqrt{n})$ in the form of classes [a, b, c] modulo p.

Lemma 2: Let P be prime and $n \equiv 0(mod\ p)$. Then E_p^0 consists of classes [0, 0, qr], [0, 0, qnr], [0, qr, 0], [0, qnr, 0], [qr, qr, qr], [qnr, qr, qr], [qr, qnr, qnr] or [qnr, qnr, qnr].

Lemma 3: Let $(n/p) = 1$ and let $[a,b,c](mod\ p)$ be the class of $\alpha(a,b,c)$ of $Q^*(\sqrt{n})$. Then:

- If p = 1 (mod 4) then [*a*, b, c] (mod p) has the forms $[0, qr, qr]$, $[0, qnr, qnr]$, $[qr, 0, qr]$, $[qr, 0, qnr]$, $[qr, qr, 0]$, $[qr, qnr, 0]$, $[qnr, 0, qr]$, $[qnr, 0, qnr]$, $[qnr, qr, 0]$, $[qnr, qnr, 0]$, $[qnr, 0, 0]$ or $o[qr, 0, 0]$ only.
- If p = 3 (mod 4) then [*a*, b, c] (mod p) has the forms $[0, qnr, qr]$, $[0, qr, qnr]$, $[qr, 0, qr]$, $[qr, qr, 0]$, $[qr, 0, qnr]$, $[qr, qnr, 0]$, $[qnr, 0, qr]$, $[qnr, qr, 0]$, $[qnr, 0, qnr]$, $[qnr, qnr, 0]$, $[qnr, 0, 0]$ or $[qr, 0, 0]$ only.

Proof of theorem 9: Let $[a,b,c](mod\ p)$ be the class of $\alpha(a,b,c) \in Q^*(\sqrt{n})$. In view of Lemma 2, either both of b, c are qrs or qnrs and the two equations $xy(\alpha(a,b,c)) = \alpha'(a+c, 2a+b+c, c)$, $yx(\alpha(a,b,c)) = \alpha'(a-3b, b, -6a+9b+c)$ fix b, c modulo p. If $a \equiv b \equiv 0(mod\ p)$ then $((2a+b+c)/p) = 1$ or $((2a+b+c)/p) = -1$ according as $(c/p) = 1$ or $(c/p) = -1$. similarly for $a \equiv c \equiv 0(mod\ p)$. This shows that the sets S_1^p and S_2^p are M^*-subsets of $Q^*(\sqrt{n})$ depending upon classes modulo p. ■

The following corollary is an immediate consequence of Theorem 1.

Corollary 2: Let $p \neq 3$ be an odd prime such that $n \equiv 0(mod\ 2p)$. Then $Q^*(\sqrt{n})$ is the disjoint union of S_1^p and S_2^p depending upon classes modulo 2p.

Proof: Since $a^2 - n = bc$ implies that $a^2 \equiv bc(mod\ 2p)$. This is equivalent to congruences $a^2 \equiv bc(mod\ p)$ and $a^2 \equiv bc(mod\ 2)$. As 1 is the quadratic residue of every prime and second congruence forces that b, or c is 1. Hence by Theorem 1, S_1^p, S_2^p are M^*-subsets of $Q^*(\sqrt{n})$. ■

Remark 1: For an odd prime $p \neq 3$, $Q^{***}(\sqrt{n}) = \varnothing$ if and only if $n \equiv 0(mod\ 2p)$.

Corollary 3: Let p = 3 be an odd prime and $n \equiv 0(mod\ 6)$. Then $Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ is the disjoint union of S_1^p and S_2^p. Furthermore $Q^{***}(\sqrt{n})$ is the disjoint union of $B_1^p = \{a,b,c) \in Q^{***}(\sqrt{n}) : (b/p) = 1\}$ and $B_2^p = \{\alpha(a,b,c) \in Q^{***}(\sqrt{n}) : (b/p) = -1\}$ depending upon classes modulo 6.

Proof: Let $\alpha(a,b,c) \in Q^*(\sqrt{n})$ and suppose $c \not\equiv 0(mod\ 3)$. The two equations $xy(\alpha(a,b,c)) = \alpha'(a+c, 2a+b+c, c)$ and $yx(\alpha(a,b,c)) = \alpha'(a-3b, b, -6a+9b+c)$ fix b, c in modulo 3. So $\alpha(a,b,c)$ belongs to S_1^p or in S_2^p according as $(c/3) = 1$ or $(c/3) = -1$. Similarly B_1^p and B_1^p are M^*-subsets of $Q^{***}(\sqrt{n})$. Hence $Q^{***}(\sqrt{n}) = B_1^p \cup B_2^p$. ■

The next theorem is more interesting in a sense that whenever $(n/p) = \pm 1$, $p \neq 3$, $Q^*(\sqrt{n})$ is itself an M^*-set depending upon classes [a, b, c] modulo p.

Theorem 10: Let $p \neq 3$ be an odd prime and $(n/p) = \pm 1$. Then $Q^*(\sqrt{n})$ is itself an M^*-set depending upon classes [a, b, c] modulo p.

Proof: Follows from Lemma 3 and the equations $xy(\alpha) = \alpha + 1$ and $yx(\alpha) = \frac{\alpha}{-3\alpha + 1}$ given in Table 2. ■

Let us illustrate the above theorem in view of Lemma 3. If (n/5) = 1, then the set:

{[0,1,4], [4,0,4], [3,2,4], [2,2,4], [1,0,4] ,
[1,0,3], [4,0,3], [2,1,3], [0,3,3] , [3,1,3] ,
[1,3,0], [1,0,0], [1,2,0], [1,4,0], [1,1,0], [4,4,0] ,
[4,2,0], [4,0,0] ,[4,3,0] ,[4,1,0], [4,0,1], [0,4,1] ,
[1,0,1], [2,3,1], [3,3,1], [3,4,2], [0,2,2], [2,4,2], [4,0,2] ,
[1,0,2]} is an M^* set. That is, $Q^*(\sqrt{n})$ is itself an M^*-set depending upon classes [a, b, c] modulo 5. Similarly for $(n/5) = -1$. The next two theorems discuss the cases $n \equiv p(mod\ 2p)$ and $(n/2p) = \pm 1$.

Theorem 11: Let $p \neq 3$ be an odd prime and $n \equiv p(mod\ 2p)$. Then $Q^*(\sqrt{n}) \setminus Q'(\sqrt{n})$ is the disjoint union of S_1^p and S_2^p. Furthermore $Q'(\sqrt{n})$ is the disjoint union of $C_1^p = \{\alpha(a,b,c) \in Q'(\sqrt{n}) : (b/p)\ or\ (c/p) = 1\}$ and $C_2^p = \{\alpha(a,b,c) \in Q'(\sqrt{n}) : (b/p)\ or\ (c/p) = -1\}$ depending upon classes modulo 2p .

Proof: Let $\alpha(a,b,c) \in Q^*(\sqrt{n})$. we show that $xy(\alpha(a,b,c))$ and $yx(\alpha(a,b,c))$ are belong to S_1^p according as (b/p) or $(c/p) = 1$. Similarly $xy(\alpha(a,b,c))$ and $yx(\alpha(a,b,c))$ are belong to S_2^p according as (c/p) or (b/p) = -1. As $xy(\alpha(a,b,c)) = \alpha'(a+c, 2a+b+c, c)$ and $(a+c)^2 - (2a+b+c)c = n$, so we have the congruence $(a+c)^2 - (2a+b+c)c \equiv p(mod\ 2p)$ which is equivalent to the congruences $(a+c)^2 - (2a+b+c)c \equiv p(mod\ 2)$ and $(a+c)^2 \equiv (2a+b+c)c(mod\ p)$. First congruence is trivially true so we discuss the second congruence only. Let $(a/p) = 0$ then $((2a+b+c)/p) = \pm 1$ or $((2a+b+c)/p) = 0$ according as $(c/p) = 0$ or $(c/p) = \pm 1$. Let $(a/p) = \pm 1$ then $((2a+b+c)/p) = (c/p) = 1$ or $((2a+b+c)/p) = (c/p) = -1$ because $((a+c)^2/p) = 1$. Now $yx(\alpha(a,b,c)) = \alpha'(a-3b, b, -6a+9b+c)$ and $(a-3b)^2 - b(-6a+9b+c) = n$. With similar arguments we can show that $yx(\alpha(a,b,c))$ belongs to S_1^p or S_2^p. Hence the sets S_1^p and S_2^p are M^*-subsets of $Q^*(\sqrt{n})$ depending upon classes modulo 2p. Similarly it is easy to see that C_1^p and C_2^p are M^*-subsets. ■

Theorem 12: Let $p \neq 3$ be an odd prime and $(n/2p) = \pm 1$. Then $Q'(\sqrt{n})$ and $Q^*(\sqrt{n}) \setminus Q'(\sqrt{n})$ are two M^*-subsets of $Q^*(\sqrt{n})$.

Proof: Follows from Theorem 6 and 7. ■
The following result is a generalization of Theorem 1.

Theorem 13: Let $p \neq 3$ be an odd prime and $n \equiv 0(mod\ p^r)$. Then S_1^p and S_2^p are exactly two M^*-subsets of $Q^*(\sqrt{n})$ depending upon the classes [a, b, c] modulo p^r.

Proof: Let P be an odd prime such that $n \equiv 0(mod\ p^r)$ and $[a,b,c](mod\ p^r)$ be the class of $\alpha(a,b,c) \in Q^*(\sqrt{n})$. Then:

$$a^2 \equiv bc(mod\ p^r) \tag{1}$$

implies

$$a^2 \equiv bc(mod\ p) \tag{2}$$

By Theorem 9, the congruence: (1) has exactly two solutions (i.e., two values of a) if (2) is solvable. So it is enough to see the class $[a,b,c](mod\ p^r)$ in modulo p. Thus by Theorem 9 we get the required result. ■

The following lemma is a particular case of the above theorem.

Lemma 4: Let $r \geq 1$ and $n \equiv 0(mod\ 3^r)$. Then
$S_1^3 = \{\alpha \in Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n}) : (b/p)\ or\ (c/p) = 1\}$
$S_2^3 = \{\alpha \in Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n}) : (b/p)\ or\ (c/p) = -1\}$
are M^*-subsets of $Q^*(\sqrt{n})$. Moreover $B_1^3 = \{\alpha \in Q^{***}(\sqrt{n}) : (b/3) = 1\}$, $B_2^3 = \{\alpha \in Q^{***}(\sqrt{n}) : (b/3) = -1\}$ are M^*-subsets of $Q^{***}(\sqrt{n})$. In particular, these are the only M^*-subsets of $Q^*(\sqrt{n})$ depending upon classes [a, b, c] modulo 3^r.

Proof: Follows from Theorems 4, 5 and 13.

Next theorem discuss the G and M-subsets with the help of M^*-subsets.

Theorem 14:

- If A is an M^*-subset of $Q^{***}(\sqrt{n})$ or $Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$, then $A \cup x'(A)$ is A G-subset of $Q^*(\sqrt{n})$.
- If A is an M^*-subset of $Q^{***}(\sqrt{n})$, then $A \cup x(A)$ is an M-subset of $Q^{***}(\sqrt{n})$ or $Q^{*:}(\sqrt{n})$ according as $n \not\equiv 0(mod\ 9)$ or $n \equiv 0(mod\ 9)$.
- If A is an M^*-subset of $Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$, then $A \cup x(A)$ is an M-subset of $Q^{*:}(\sqrt{9n})$ for all non-square n.

Proof:

- Follows by the equation:

$$x'(Q^{***}(\sqrt{n})) = Q^{*}(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$$

- Follows by the equations $x(Q^{***}(\sqrt{n})) = Q^{***}(\sqrt{n})$ or:

$$x(Q^{***}(\sqrt{n})) = Q^{*}\left(\sqrt{\frac{n}{9}}\right) \setminus Q^{***}\left(\sqrt{\frac{n}{9}}\right)$$

according as $n \not\equiv 0(mod\ 9)$ or $n \equiv 0(mod\ 9)$.

- Follows by the equation:

$$x\left(Q^{*}(\sqrt{n}) \setminus Q^{***}(\sqrt{n})\right) = Q^{***}(\sqrt{9n}) \blacksquare$$

The following example describes the above theorem.

Example: Let $n = 27$. Then:

$$\alpha = \frac{1+\sqrt{27}}{1} \in Q^{*}(\sqrt{27})$$

but

$$\frac{\alpha}{3} = \frac{1+\sqrt{27}}{3} = \frac{3+\sqrt{243}}{9} \in Q^{***}(\sqrt{243})$$

Also

$$\beta = \frac{3+\sqrt{27}}{1} \in Q^{*}(\sqrt{27})$$

but

$$\frac{\beta}{3} = \frac{1+\sqrt{3}}{1} \in Q^{*}(\sqrt{3}) \setminus Q^{***}(\sqrt{3})$$

Similarly

$$\gamma = \frac{3+\sqrt{27}}{18} \in Q^{***}(\sqrt{27})$$

whereas

$$\frac{\gamma}{3} = \frac{9+\sqrt{243}}{162} \in Q^{***}(\sqrt{243})$$

The next three theorems are the generalization of Theorem 9 to the case when n involves two distinct prime factors.

Theorem 15: Let $p_1 \neq 3$ and $p_2 \neq 3$ be distinct odd primes factors of n. Then $S_{1,1} = S_1^{p_1} \cap S_1^{p_2}$, $S_{1,2} = S_1^{p_1} \cap S_2^{p_2}$, $S_{2,1} = S_2^{p_1} \cap S_1^{p_2}$ and $S_{2,2} = S_2^{p_1} \cap S_2^{p_2}$ are four M*-subsets of $Q^{*}(\sqrt{n})$. More precisely these are the only M*-subsets of $Q^{*}(\sqrt{n})$ depending upon classes [a, b, c] modulo p_1p_2.

Proof: Let $[a,b,c](mod\ p_1p_2)$ be any class of $\alpha(a,b,c) \in Q^{*}(\sqrt{n})$ with $n \equiv 0(mod\ p_1p_2)$. Then $a^2 - n = bc$ implies that:

$$a^2 \equiv bc(mod\ p_1p_2) \quad (3)$$

This is equivalent to congruences $a^2 \equiv bc(mod\ p_1)$ and $a^2 \equiv bc\ (mod\ p_2)$. By Theorem 9, the congruence $a^2 \equiv bc(mod\ p_1)$ gives two M*-subsets $S_1^{p_1} = \{\alpha \in Q^{*}(\sqrt{n}) : (c/p_1)\ or\ (c/p_1) = 1\}$ and $S_2^{p_1} = \{\alpha \in Q^{*}(\sqrt{n}) : (c/p_1)\ or\ (c/p_1) = -1\}$ of $Q^{*}(\sqrt{n})$. As $a^2 \equiv bc\ (mod\ p_2)$, again applying Theorem 9 on each of S_1^{p1} and S_2^{p1} we have four M*-subsets $S_{1,1}$, $S_{1,2}$, $S_{2,1}$ and $S_{2,2}$ of $Q^{*}(\sqrt{n})$. ■

Theorem 16: Let $p \neq 3$ be any odd prime and $n \equiv 0(mod\ 3p)$. Then $A_{1,1} = S_1^{p} \cap A_1^{3}$, $A_{1,2} = S_1^{p} \cap A_2^{3}$, $A_{2,2} = S_2^{p} \cap A_2^{3}$ and $A_{2,1} = S_2^{p} \cap A_1^{3}$ are four M*-subsets of $Q^{*}(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ depending upon classes [a, b, c] modulo 3p.

Proof: Follows from Theorems 4 and 15. ■

Theorem 17: Let $p \neq 3$ be any odd prime and $n \equiv 0(mod\ 3p)$. Then $B_{1,1} = S_1^{p} \cap B_1^{3}$, $B_{2,2} = S_2^{p} \cap B_2^{3}$, $B_{1,2} = S_1^{p} \cap B_2^{3}$ and $B_{2,1} = S_2^{p} \cap B_1^{3}$ are four M*-subsets of $Q^{***}(\sqrt{n})$ depending upon classes [a, b, c] modulo 3p.

Proof: Follows from Theorems 4 and 15. ■

We now state the concluding theorem of this study.

Theorem 18: Let $n = 3^k p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where $p_1, p_2, ..., p_r$ are distinct odd primes. Then the number of M*-subsets of $Q^{*}(\sqrt{n})$ is 2^r namely $A_{1 \le i_1, i_2, i_3, ..., i_r \le 2}$ if $k = 0$. Moreover if $k \ge 1$, then each M*-subset X of these M*-subsets further splits into two proper M*-subsets $\{\alpha \in X : b\ or\ c \equiv 1(mod\ 3)\}$ and

$\{\alpha \in X : b \text{ or } c \equiv -1(mod\ 3)\}$. Thus the number of M*-subsets of $Q^*(\sqrt{n})$ depending upon classes [a, b, c] modulo n is 2^{r+1} if $k \geq 1$.

Proof: Let $k = 0$. Then, by Theorem 13 and 15, $Q^*(\sqrt{n})$ is the disjoint union of 2^r subsets $S_{1\leq i_1,i_2,i_3,\ldots,i_r\leq 2}$ which are invariant under the action of M^*. However if $k \geq 1$ then by Theorems 16 and 17 we know that each of these M^*-subsets splits into four M^*-subsets $S_{1\leq i_1,i_2,i_3,\ldots,i_r\leq 2} \cap A_1^3$, $S_{1\leq i_1,i_2,i_3,\ldots,i_r\leq 2} \cap A_2^3$, $S_{1\leq i_1,i_2,i_3,\ldots,i_r\leq 2} \cap B_1^3$ and $S_{1\leq i_1,i_2,i_3,\ldots,i_r\leq 2} \cap B_2^3$. Thus by lemma 4, $Q^*(\sqrt{n})$ is the disjoint union of 2^{r+2} subsets of $Q^*(\sqrt{n})$ which are invariant under the action of M^*. More precisely these are the only M^*-subsets of $Q^*(\sqrt{n})$ depending upon classes [a, b, c] modulo n. Hence the result. ■

REFERENCES

Afzal F., S. Bhatti, M. A. Aslam, 2012. Action of *G* and *M* on $Q(\sqrt{m})$ and algorithmic implementation For Group Actions. J. Hyperstructures, 1(1): 41-51.

Andrew, A. and E.C. John, 1995. The Theory of Numbers. Jones and Bartlett Publishers, Inc., Sudbury, Mass, U.A.

Aslam, M.M. and M.A. Zafar, 2011. Real Quadratic irrational numbers and modular group action. Southeast Asian Bull. Math., 35(3): 439-445.

Aslam, M.M., S.M. Husnine and A. Majeed, 2003-2004. Action of the group $M = \langle x, y : x^2 = y^6 = 1\rangle$ on certain real quadratic fields. PUJM, 36: 71-88.

Aslam, M.M., S.M. Husnine and A. Majeed, 2005. Intrasitive action of the modular group $PSL_2(Z)$ on a subset $Q^*(\sqrt{k^2m})$ of $Q(\sqrt{m})$. PUJM, 37: 31-38.

Aslam, M.M., S.M. Husnine and A. Majeed, 2012. Action of the möbius group $M = \langle x, y : x^2 = y^6 = 1\rangle$ on certain real quadratic fields. PUJM, pp: 42.

Aslam, M.M. and M.A. Zafar, Year. $Q(\sqrt{m}) \setminus Q$ under the Action of $PSL_2(Z) \cap \left\langle x, y : x^2 = y^4 = 1\right\rangle$, (Submitted for Publication).

Farkhanda, A., Q. Afzal and M. Aslam Malik, 2012. A classification of the real quadratic irrational numbers $\frac{a+\sqrt{n}}{c}$ of $Q^*(\sqrt{n})$ w.r.t modulo 3^r. Int. Math. Forum, 7(39): 1915-1924.

Husnine, S.M., M.A. Malik and A. Majeed, 2005. On ambiguous numbers of an invariant subset $Q^*(\sqrt{k^2m})$ of $Q(\sqrt{m})$ under the action of the modular group $PSL_2(Z)$. Stud. Sci. Math. Hung., 42(4): 401-412.

Mushtaq, Q., 1988. Modular group acting on real quadratic fields. Bull. Austral. Math. Soc., 3(7): 303-309, 89e:11065.

Sahin, R. and O. Bizim, 2003. Some subgroups of the extended Hecke groups $\overline{H}(\lambda_q)$. Math. Acta Sci., 23B(4): 497-502.

Shin-Ichi, K., *et al*., 2009. Orbit of quadratic irrationals modulo p by the modular group. Gomal Univ. J. Res., 25(1): 1-5.