Applied Mathematics, 2014, 5, 1284-1291
Published Online May 2014 in SciRes. http://www.scirp.org/journal/am
http://dx.doi.org/10.4236/am.2014.58120

On Subsets of $\mathbb{Q}\left(\sqrt{m}\right)\setminus\mathbb{Q}$ under the Action of Hecke Groups $H\left(\lambda_q\right)$

Muhammad Aslam Malik[1], Muhammad Asim Zafar[2]

[1]Department of Mathematics, University of the Punjab, Quaid-e-Azam Campus, Lahore, Pakistan
[2]Center for Undergraduate Studies, University of the Punjab, Quaid-e-Azam Campus, Lahore, Pakistan
Email: malikpu@yahoo.com, asimzafar@hotmail.com

Received 2 February 2014; revised 2 March 2014; accepted 9 March 2014

Abstract

$\mathbb{Q}\left(\sqrt{m}\right)\setminus\mathbb{Q}$ is the disjoint union of $\mathbb{Q}^*\left(\sqrt{k^2m}\right)$ for all $k\in\mathbb{N}$, where $\mathbb{Q}^*\left(\sqrt{k^2m}\right)$ is the set of all roots of primitive second degree equations $ct^2+2at+b=0$, with reduced discriminant $\Delta=a^2-bc$ equal to k^2m. We study the action of two Hecke groups—the full modular group $H\left(\lambda_3\right)=PSL_2\left(\mathbb{Z}\right)$ and the group of linear-fractional transformations $H\left(\lambda_4\right)=\left\langle x,y:x^2=y^4=1\right\rangle$ on $\mathbb{Q}\left(\sqrt{m}\right)\setminus\mathbb{Q}$. In particular, we investigate the action of $H\left(\lambda_3\right)\cap H\left(\lambda_4\right)$ on $\mathbb{Q}^*\left(\sqrt{k^2m}\right)$ for finding different orbits.

Keywords

Quadratic Irrationals, Hecke Groups, Legendre Symbol, *G*-Set

1. Introduction

In 1936, Erich Hecke (see [1]) introduced the groups $H\left(\lambda\right)$ generated by two linear-fractional transformations $T\left(z\right)=\frac{-1}{z}$ and $S\left(z\right)=\frac{-1}{z+\lambda}$. Hecke showed that $H\left(\lambda\right)$ is discrete if and only if $\lambda=\lambda_q=2\cos\left(\frac{\pi}{q}\right)$, $q\in\mathbb{N}$, $q\geq 3$ or $\lambda\geq 2$. Hecke group $H\left(\lambda_q\right)$ is isomorphic to the free product of two finite cyclic group of order 2 and *q*, and it has a presentation

$$H\left(\lambda_q\right)=\left\langle T,S:T^2=S^q=1\right\rangle\cong C_2*C_q$$

How to cite this paper: Malik, M.A. and Zafar, M.A. (2014) On Subsets of $\mathbb{Q}\left(\sqrt{m}\right)\setminus\mathbb{Q}$ under the Action of Hecke Groups $H\left(\lambda_q\right)$. *Applied Mathematics*, **5**, 1284-1291. http://dx.doi.org/10.4236/am.2014.58120

The first few of these groups are $H(\lambda_3) = G = PSL(2,\mathbb{Z})$, the full modular group having special interest for mathematicians in many fields of Mathematics, $H(\lambda_4) = H$ and $H(\lambda_6) = M$.

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 $p^g = q$. Let $n = k^2 m$, where $k \in \mathbb{N}$ and *m* is a square free positive integer. Then

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

is the set of all roots of primitive second degree equations $ct^2 + 2at + b = 0$, with reduced discriminant $\Delta = a^2 - bc$ equal to *n* and

$$\mathbb{Q}\left(\sqrt{m}\right) \setminus \mathbb{Q} = \left\{t + w\sqrt{m} : t, 0 \neq w \in \mathbb{Q}\right\}$$

is the disjoint union of $\mathbb{Q}^*\left(\sqrt{n}\right)$ for all *k*. If $\alpha(a,b,c) \in \mathbb{Q}^*\left(\sqrt{n}\right)$ and its conjugate $\bar{\alpha}$ have opposite signs then α is called an ambiguous number [2]. The actual number of ambiguous numbers in $\mathbb{Q}^*\left(\sqrt{n}\right)$ has been discussed in [3] as a function of *n*. The classification of the real quadratic irrational numbers $\alpha(a,b,c)$ of $\mathbb{Q}^*\left(\sqrt{n}\right)$ in the forms $[a,b,c]$ modulo *n* has been given in [4] [5]. It has been shown in [6] that the action of the modular group $G = \langle x', y' : x'^2 = y'^3 = 1 \rangle$, where $x'(z) = \frac{-1}{z}$ and $y'(z) = \frac{-1}{z+1}$, on the rational projective line $\mathbb{Q} \cup \{\infty\}$ is transitive. An action of $H = \langle x, y : x^2 = y^4 = 1 \rangle$, where $x(z) = \frac{-1}{2z}$ and $y(z) = \frac{-1}{2(z+1)}$ and its proper subgroups on $\mathbb{Q} \cup \{\infty\}$ has been discussed in [7] [8].

$\mathbb{Q}^*\left(\sqrt{n}\right)$ invariant under the action of modular group *G* but $\mathbb{Q}^*\left(\sqrt{n}\right)$ is not invariant under the action of *H*. Thus it motivates us to establish a connection between the elements of the groups *G* and *H* and hence to deduce a common subgroup $H^* = \langle xy, yx \rangle$ of both groups such that each of $\mathbb{Q}^{**}\left(\sqrt{n}\right) = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : 2 \mid c\right\}$ and $\mathbb{Q}^*\left(\sqrt{n}\right) \setminus \mathbb{Q}^{**}\left(\sqrt{n}\right)$ is invariant under H^* and hence we find *G*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$ and *H*-subsets of $\mathbb{Q}^{**}\left(\sqrt{n}\right)$ or $\mathbb{Q}^{*\sim}\left(\sqrt{n}\right) = \left(\mathbb{Q}^*\left(\sqrt{\frac{n}{4}}\right) \setminus \mathbb{Q}^{**}\left(\sqrt{\frac{n}{4}}\right)\right) \cup \mathbb{Q}^{**}\left(\sqrt{n}\right)$ according as $n \not\equiv 0 (mod\ 4)$ or $n \equiv 0 (mod\ 4)$ and $\mathbb{Q}^{*\sim}\left(\sqrt{4n}\right)$ for all non-square *n*. Also the partition of $\mathbb{Q}^*\left(\sqrt{n}\right)$ has been discussed depending upon classes $[a,b,c]$ modulo $p_1 p_2$.

2. Preliminaries

We quote from [5] [6] and [8] the following results for later reference. Also we tabulate the actions on $\alpha(a,b,c) \in \mathbb{Q}^*\left(\sqrt{n}\right)$ of x', y' and x, y, the generators of *G* and *H* respectively in **Table 1**.

Theorem 2.1 (see [5]) Let $n \equiv 2 (mod\ 8)$, $n \neq 2$. Then $B^1 = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : b \text{ or } c \equiv \pm 1 (mod\ 8)\right\}$ and $B^3 = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : b \text{ or } c \equiv \pm 3 (mod\ 8)\right\}$ are both *G*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$.

Theorem 2.2 (see [5]) Let $n \equiv 6 (mod\ 8)$. Then $B = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : b \text{ or } c \equiv 1 \text{ or } 3 (mod\ 8)\right\}$ and $-B = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : b \text{ or } c \equiv -1 \text{ or } -3 (mod\ 8)\right\}$ are both *G*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$.

Theorem 2.3 (see [6]) If $n \equiv 0 \text{ or } 3 (mod\ 4)$, then $S = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : b \text{ or } c \equiv 1 (mod\ 4)\right\}$ and $-S = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : b \text{ or } c \equiv -1 (mod\ 4)\right\}$ are exactly two disjoint *G*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$ depending upon classes $[a,b,c]$ modulo 4.

Theorem 2.4 (see [6]) If $n \equiv 1 (mod\ 4)$, then $\mathbb{Q}'\left(\sqrt{n}\right) = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : 2 \mid (b,c)\right\}$ and

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

$x'(\alpha)=\frac{-1}{\alpha}$	$-a$	c	b
$y'(\alpha)=\frac{\alpha-1}{\alpha}$	$-a+b$	$-2a+b+c$	c
$(y')^2(\alpha)=\frac{1}{1-\alpha}$	$-a+c$	c	$-2a+b+c$
$x'y'(\alpha)=\frac{\alpha}{1-\alpha}$	$a-b$	b	$-2a+b+c$
$y'x'(\alpha)=1+\alpha$	$a+c$	$2a+b+c$	c
$(y')^2x'(\alpha)=\frac{\alpha}{1+\alpha}$	$a+b$	b	$2a+b+c$
$x(\alpha)=\frac{-1}{2\alpha}$	$-a$	$\frac{c}{2}$	$2b$
$y(\alpha)=\frac{-1}{2(\alpha+1)}$	$-a-c$	$\frac{c}{2}$	$2(2a+b+c)$
$y^2(\alpha)=\frac{-(\alpha+1)}{2(\alpha)}$	$-3a-2b-c$	$2a+b+c$	$4a+4b+c$
$y^3(\alpha)=\frac{(2\alpha+1)}{2\alpha}$	$-a-2b$	$\frac{4a+4b+c}{2}$	$2(2a+b+c)$
$xy(\alpha)=\alpha+1$	$a+c$	$2a+b+c$	c
$yx(\alpha)=\frac{\alpha}{1-2\alpha}$	$a-2b$	b	$-4a+4b+c$
$y^2x(\alpha)=\frac{1-2\alpha}{2(-1+\alpha)}$	$3a-2b-c$	$\frac{-4a+4b+c}{2}$	$2(-2a+b+c)$
$y^3x(\alpha)=\alpha-1$	$a-c$	$2a+b+c$	c

$\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}'(\sqrt{n})=\{\alpha\in\mathbb{Q}^*(\sqrt{n}):2\nmid(b,c)\}$ are both G-subsets of $\mathbb{Q}^*(\sqrt{n})$.

Lemma 2.5 (see [8]) Let $\alpha(a,b,c)\in\mathbb{Q}^*(\sqrt{n})$. Then:

1) If $n\not\equiv 0(mod\ 4)$ then $\frac{\alpha}{2}\in\mathbb{Q}^{**}(\sqrt{n})$ if and only if $2|b$.

2) $\frac{\alpha}{2}\in\mathbb{Q}^{**}(\sqrt{4n})$ if and only if $2\nmid b$.

Theorem 2.6 (see [8]) The set $\mathbb{Q}''(\sqrt{n})=\left\{\frac{\alpha}{t}:\alpha\in\mathbb{Q}^*(\sqrt{n}),t=1,2\right\}$, is invariant under the action of H.

Theorem 2.7 (see [8]) For each non square positive integer $n\equiv 1,2$ or $3(mod\ 4)$, $\mathbb{Q}^{**}(\sqrt{n})=\{\alpha\in\mathbb{Q}^*(\sqrt{n}):2|c\}$ is an H-subset of $\mathbb{Q}''(\sqrt{n})$.

3. Action of $H(\lambda_3)\cap H(\lambda_4)$ on $\mathbb{Q}^*(\sqrt{n})$

We start this section by defining a common subgroup of both groups $G=\langle x',y':x'^2=y'^3=1\rangle$ and

$H=\langle x,y:x^2=y^4=1\rangle$, where $x'(\alpha)=\frac{-1}{\alpha}$, $y'(\alpha)=\frac{\alpha-1}{\alpha}$, $x(\alpha)=\frac{-1}{2\alpha}$ and $y(\alpha)=\frac{-1}{2(\alpha+1)}$. For this, we need the following crucial results which show the relationships between the elements of *G* and *H*.

Lemma 3.1 Let x',y' and x,y be the generators of *G* and *H* respectively defined above. Then we have:

1) $y^2=(x'y')^2(y'x')$ and $y^3=\frac{1}{2}\left(x'(y')^2\right)^2x'$.

2) $xy=y'x'$ and $yx=(x'y')^2$.

3) $y^3x=x'(y')^2$ and $xy^3=\left((y')^2x'\right)^2$.

4) $y^2x=\frac{1}{2}\left(x'(y')^2\right)(x'y')$ and $xy^2=\frac{1}{2}(y'x')\left((y')^2x'\right)$.

5) $x'=2x$ and $y'=(2x)(2y)(2x)$.

6) $x'y'=2(yx)\frac{1}{2}$ and $x'(y')^2=y^3x$. In particular $(x'y')^{-1}=2(xy^3)\frac{1}{2}$ and $\left(x'(y')^2\right)=xy$.

Following corollary is an immediate consequence of Lemma 3.1.

Corollary 3.2 1) By Lemma 3.1, since $xy=y'x'$ and $yx=(x'y')^2$ so $H^*=\langle xy,yx\rangle$ is a common subgroup of *G* and *H* where xy,yx are the transformations defined by $xy(\alpha)=\alpha+1$ and $yx(\alpha)=\frac{\alpha}{1-2\alpha}$.

2) As $yxxy=y^2$, $xyyx=xy^2x$, so $\langle y^2,xy^2x\rangle$ is a proper subgroup of H^*.

3) $\langle H^*,x\rangle=\langle H^*,y\rangle=H$ and $\langle H^*,x'\rangle=\langle H^*,y'\rangle=G$.

Since for each integer *n*, either $(n/p)=0$ or $(n/p)=\pm1$ for each odd prime *p*. So in the following lemma, we classify the elements of $\mathbb{Q}^*(\sqrt{n})$ in terms of classes $[a,b,c](mod\ p)$ with 0 modulo *p* or *qr*, *qnr* nature of *a*, *b* and *c* modulo *p*.

Lemma 3.3 Let p be prime and $n\equiv0(mod\ p)$. Then $\mathbb{E}_p^0$ 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 $[qnr,qnr,qnr]$.

Proof. Let $[a,b,c](mod\ p)$ be any class of $\alpha(a,b,c)$. Then $a^2\equiv bc(mod\ p)$ leads us to exactly three cases. If $a\equiv0(mod\ p)$ then exactly one of b,c is $\equiv0(mod\ p)$ and the other is qr or qnr of p as otherwise $(a,b,c)\neq1$ and hence the class $[a,b,c]$ is one of the forms $[0,0,qr]$, $[0,0,qnr]$, $[0,qr,0]$, $[0,qnr,0]$. If $(a/p)=1$ then $(bc/p)=1$ and the class takes the form $[qr,qr,qr]$ or $[qr,qnr,qnr]$. In third case if $(a/p)=-1$ then $(a^2/p)=1$ so again $(bc/p)=1$. This yields the class in the forms $[qnr,qr,qr]$ or $[qnr,qnr,qnr]$. Hence the result. ■

Lemma 3.4 Let $(n/p)=1$ and let $[a,b,c](mod\ p)$ be the class of $\alpha_n(a,b,c)$ of $\mathbb{Q}^*(\sqrt{n})$. Then:

1) If $p\equiv1(mod\ 4)$ 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 $[qr,0,0]$ only.

2) If $p\equiv3(mod\ 4)$ 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. Let $[a,b,c](mod\ p)$ be the class of $\alpha_n(a,b,c)$ with $a^2-n=bc$. As $(n/p)=1$ so if $(a/p)=0$ then $\left((a^2-n)/p\right)=\pm1$ according as $p\equiv1(mod\ 4)$ or $p\equiv3(mod\ 4)$. Thus we have $[0,qr,qr]$, $[0,qnr,qnr]$ if $p\equiv1(mod\ 4)$ and $[0,qnr,qr]$, $[0,qr,qnr]$ if $p\equiv3(mod\ 4)$. If $(a/p)=\pm1$ then $\left((a^2-n)/p\right)=0$, so we get $[qr,0,qr]$, $[qr,0,qnr]$, $[qr,qr,0]$, $[qr,qnr,0]$, $[qnr,0,qr]$, $[qnr,0,qnr]$, $[qnr,qr,0]$, $[qnr,qnr,0]$, $[qnr,0,0]$ or $[qr,0,0]$ only. This proof is now complete. ■

Lemma 3.5 Let $(n/p)=-1$ and let $[a,b,c](mod\ p)$ be the class of $\alpha(a,b,c)$ of $\mathbb{Q}^*(\sqrt{n})$. Then:

1) If $p\equiv1(mod\ 4)$ then $[a,b,c](mod\ p)$ has the forms $[0,qnr,qr]$, $[0,qr,qnr]$, $[qr,qr,qr]$, $[qr,qnr,qnr]$, $[qnr,qr,qr]$ or $[qnr,qnr,qnr]$ only.

2) If $p\equiv3(mod\ 4)$ then $[a,b,c](mod\ p)$ has the forms $[0,qr,qr]$, $[0,qnr,qnr]$, $[qr,qr,qnr]$, $[qr,qnr,qr]$, $[qnr,qr,qnr]$ or $[qnr,qnr,qr]$ only.

Proof. The proof is analogous to the proof of Lemma 3.4. ■

Note: If $(n/2)=0$ then $[1,1,1]$, $[0,0,1]$ and $[0,1,0]$ are three classes of $\mathbb{Q}^*(\sqrt{n})$ in modulo 2. If n is an odd then three classes of $Q^*(\sqrt{n})$ are $[1,0,1]$, $[1,1,0]$ and $[0,1,1]$ modulo 2. These are the only classes of $\mathbb{Q}^*(\sqrt{n})$ if $n\equiv 3(mod\ 4)$. But if $n\equiv 1(mod\ 4)$ then $[1,0,0]$ is also a class of $Q^*(\sqrt{n})$ and there are no further classes. These classes in modulo 2 of $\mathbb{Q}^*(\sqrt{n})$ do not give any useful information during the study of action of G on $\mathbb{Q}^*(\sqrt{n})$ except that if $n\equiv 1(mod\ 4)$ then the set consisting of all elements of $\mathbb{Q}^*(\sqrt{n})$ of the form $[1,0,0]$ is invariant under the action of the group G. Whereas the study of action of H^* on $Q^*(\sqrt{n})$ gives some useful information about these classes. The following crucial result determines the H^*-subsets of $\mathbb{Q}^*(\sqrt{n})$ depending upon classes $[a,b,c]$ modulo 2. It is interesting to observe that $\mathbb{Q}^*(\sqrt{n})$ splits into $\mathbb{Q}^{**}(\sqrt{n})$ and $\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n})$ in modulo 2. Each of these two H^*-subsets further splits into proper H^*-subsets in modulo 4.

Lemma 3.6 $\mathbb{Q}^{**}(\sqrt{n})$ and $\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n})$ are two distinct H^*-subsets of $\mathbb{Q}^*(\sqrt{n})$ depending upon classes $[a,b,c]$ modulo 2.

Theorem 3.7 and Remarks 3.8 are extension of Lemma 3.6 and discuss the action of H^* on $\mathbb{Q}^*(\sqrt{n})$ depending upon classes $[a,b,c]$ modulo 4. Proofs of these follow directly by the equations $xy\left(\frac{a+\sqrt{n}}{c}\right)=\frac{a+c+\sqrt{n}}{c}$, $yx\left(\frac{a+\sqrt{n}}{c}\right)=\frac{a-2b+\sqrt{n}}{-4a+4b+c}$ and classes $[a,b,c]$ modulo 4 given in [6].

Theorem 3.7 Let n be any non-square positive integer. Then $\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n})$ splits into two proper H^*-subsets $A_1=\{\alpha\in\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n}):c\equiv 1(mod\ 4)\}$, $A_2=\{\alpha\in\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n}):c\equiv 3(mod\ 4)\}$. Similarly $\mathbb{Q}^{**}(\sqrt{n})$ splits into two proper H^*-subsets $B_1=\{\alpha\in\mathbb{Q}^{**}(\sqrt{n}):c\equiv 0(mod\ 4)\}$ and $B_2=\{\alpha\in\mathbb{Q}^{**}(\sqrt{n}):c\equiv 2(mod\ 4)\}$.

Remark 3.8 1) Let $n\equiv 1(mod\ 4)$. Then $\mathbb{Q}'(\sqrt{n})=\{\alpha\in\mathbb{Q}^{**}(\sqrt{n}):2|(b,c)\}$ and $\mathbb{Q}^{**}(\sqrt{n})\setminus\mathbb{Q}'(\sqrt{n})$ are H^*-subsets of $\mathbb{Q}^{**}(\sqrt{n})$. In particular if $n\equiv 5(mod\ 8)$, then $B_1=\mathbb{Q}^{**}(\sqrt{n})\setminus\mathbb{Q}'(\sqrt{n})$ and $B_2=\mathbb{Q}'(\sqrt{n})$ are H^*-subsets of $\mathbb{Q}^{**}(\sqrt{n})$. Whereas if $n\equiv 1(mod\ 8)$, then $C_1=\{\alpha\in\mathbb{Q}'(\sqrt{n})\cap B_1:a\equiv 1(mod\ 4)\}$, $C_2=\{\alpha\in\mathbb{Q}'(\sqrt{n})\cap B_1:a\equiv 3(mod\ 4)\}$, $C_3=\{\alpha\in Q'(\sqrt{n}):c\equiv 2(mod\ 4)\}$ and $C_4=\mathbb{Q}^{**}(\sqrt{n})\setminus\mathbb{Q}'(\sqrt{n})$ are H^*-subsets of $\mathbb{Q}^{**}(\sqrt{n})$. Specifically, $B_1=C_1\cup C_2\cup C_4$, $B_2=C_3$.

2) As we know that if n and c are even, then a must be even as $(a,b,c)=1$. If $n\equiv 2(mod\ 4)$, then $B_2=\mathbb{Q}^{**}(\sqrt{n})$ and $B_1=\phi$.

3) If $n\equiv 0$ or $3(mod\ 4)$, then B_2 or B_1 is empty according as $n\equiv 0$ or $3(mod\ 4)$. As we know that if n and c are even, then a must be even as $(a,b,c)=1$. However $D_1=\{\alpha\in\mathbb{Q}^{**}(\sqrt{n}):b\equiv 1(mod\ 4)\}$, $D_2=\{\alpha\in\mathbb{Q}^{**}(\sqrt{n}):b\equiv 3(mod\ 4)\}$ are proper H^*-subsets of $\mathbb{Q}^{**}(\sqrt{n})$ depending upon classes $[a,b,c]$ modulo 4.

Lemma 3.9 Let n be any non-square positive integer. Then $\mathbb{Q}^{**}(\sqrt{4n})$ and $\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n})$ are distinct H^*-subsets of an H-set $\mathbb{Q}^{*\sim}(\sqrt{4n})=\mathbb{Q}^{**}(\sqrt{4n})\cup\left(\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n})\right)$.

Proof. Follows by the equations $x\left(\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n})\right)=\mathbb{Q}^{**}(\sqrt{4n})$ and vice versa. Hence $\mathbb{Q}^*(\sqrt{n})\setminus\mathbb{Q}^{**}(\sqrt{n})$ is equivalent to $\mathbb{Q}^{**}(\sqrt{4n})$.

Clearly $\left|\mathbb{Q}_1^*(\sqrt{n})\setminus\mathbb{Q}_1^{**}(\sqrt{n})\right|=\left|\mathbb{Q}_1^{**}(\sqrt{4n})\right|$ where $\mathbb{Q}_1^*(\sqrt{n})$ denotes the set of all ambigious numbers in

$\mathbb{Q}^*\left(\sqrt{n}\right)$ (see [8]).

Remark 3.10 1) Each *G*-subset *X* of $\mathbb{Q}^*\left(\sqrt{n}\right)$ splits into two H^*-subsets $X\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)$ and $X\cap\mathbb{Q}^{**}\left(\sqrt{n}\right)$ and $x'\left(X\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)\right)=x'\left(X\cap\mathbb{Q}^{**}\left(\sqrt{n}\right)\right)=X$.

2) Each *H*-subset *Y* of $\mathbb{Q}^{*\sim}\left(\sqrt{4n}\right)$ splits into two H^*-subsets $Y\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)$ and $Y\cap\mathbb{Q}^{**}\left(\sqrt{4n}\right)$.

3) Each *H*-subset *Y* of $\mathbb{Q}^{*\sim}\left(\sqrt{n}\right)$, $n\not\equiv 0\left(mod\ 4\right)$ splits into two H^*-subsets $Y\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)$ and $Y\cap\mathbb{Q}^{**}\left(\sqrt{4n}\right)$.

4) Each *H*-subset *Y* of $\mathbb{Q}^{**}\left(\sqrt{n}\right)$, $n\not\equiv 0\left(mod\ 4\right)$ splits into two H^*-subsets $Y\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)$ and $Y\cap\mathbb{Q}^{**}\left(\sqrt{4n}\right)$.

Theorem 3.11 a) If *A* is an H^*-subset of $\mathbb{Q}^{**}\left(\sqrt{n}\right)$ or $\mathbb{Q}^*\left(\sqrt{n}\right)\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)$, then $A\cup x'\left(A\right)$ is a *G*-subset of $\mathbb{Q}^*\left(\sqrt{n}\right)$.

b) If *A* is an H^*-subset of $\mathbb{Q}^{**}\left(\sqrt{n}\right)$, then $A\cup x\left(A\right)$ is an *H*-subset of $\mathbb{Q}^{**}\left(\sqrt{n}\right)$ or $\mathbb{Q}^{*\sim}\left(\sqrt{n}\right)$ according as $n\not\equiv 0\left(mod\ 4\right)$ or $n\equiv 0\left(mod\ 4\right)$.

c) If *A* is an H^*-subset of $\mathbb{Q}^*\left(\sqrt{n}\right)\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)$, then $A\cup x\left(A\right)$ is an *H*-subset of $\mathbb{Q}^{*\sim}\left(\sqrt{4n}\right)$ for all non-square *n*.

Proof. Proof of a) follows by the equation $x'\left(\mathbb{Q}^{**}\left(\sqrt{n}\right)\right)=\mathbb{Q}^*\left(\sqrt{n}\right)\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)$.

Proof of b) follows by the equations $x\left(\mathbb{Q}^{**}\left(\sqrt{n}\right)\right)=\mathbb{Q}^{**}\left(\sqrt{n}\right)$ or $x\left(\mathbb{Q}^{**}\left(\sqrt{n}\right)\right)=\mathbb{Q}^*\left(\sqrt{\frac{n}{4}}\right)\setminus\mathbb{Q}^{**}\left(\sqrt{\frac{n}{4}}\right)$ according as $n\not\equiv 0\left(mod\ 4\right)$ or $n\equiv 0\left(mod\ 4\right)$.

Proof of c) follows by the equation $x\left(\mathbb{Q}^*\left(\sqrt{n}\right)\setminus\mathbb{Q}^{**}\left(\sqrt{n}\right)\right)=\mathbb{Q}^{**}\left(\sqrt{4n}\right)$. ■

Following examples illustrate the above results.

Example 3.12 1) Let $n=8$. Then $\alpha=\frac{1+\sqrt{8}}{1}\in\mathbb{Q}^*\left(\sqrt{8}\right)$ but $\frac{\alpha}{2}=\frac{1+\sqrt{8}}{2}=\frac{2+\sqrt{32}}{4}\in\mathbb{Q}^{**}\left(\sqrt{32}\right)$. Also $\beta=\frac{2+\sqrt{8}}{1}\in\mathbb{Q}^*\left(\sqrt{8}\right)$ but $\frac{\beta}{2}=\frac{1+\sqrt{2}}{1}\in\mathbb{Q}^*\left(\sqrt{2}\right)\setminus\mathbb{Q}^{**}\left(\sqrt{2}\right)$. Similarly $\gamma=\frac{2+\sqrt{8}}{4}\in\mathbb{Q}^{**}\left(\sqrt{8}\right)$ whereas $\frac{\gamma}{2}=\frac{4+\sqrt{32}}{16}\in\mathbb{Q}^*\left(\sqrt{32}\right)$. Also $\mathbb{Q}^{*\sim}\left(\sqrt{8}\right)=\left(\sqrt{2}\right)^H\cup\left(-\sqrt{2}\right)^H$, $\mathbb{Q}^{*\sim}\left(\sqrt{32}\right)=\left(\sqrt{8}\right)^H\cup\left(-\sqrt{8}\right)^H$. So $Q''\left(\sqrt{8}\right)$ has exactly 4 orbits under the action of *H* whereas $\mathbb{Q}^*\left(\sqrt{8}\right)$ splits into two *G*-orbits namely $\left(\sqrt{8}\right)^G$, $\left(-\sqrt{8}\right)^G$.

2) $\mathbb{Q}''\left(\sqrt{37}\right)$ splits into nine *H*-orbits. Also

$$\mathbb{Q}^{*\sim}\left(\sqrt{148}\right)=\left(\sqrt{37}\right)^H\cup\left(-\sqrt{37}\right)^H\cup\left(\frac{1+\sqrt{37}}{3}\right)^H\cup\left(\frac{1+\sqrt{37}}{-3}\right)^H\cup\left(\frac{-1+\sqrt{37}}{-3}\right)^H\cup\left(\frac{-1+\sqrt{37}}{-3}\right)^H$$

and

$$\mathbb{Q}^{**}\left(\sqrt{37}\right)=\left(\frac{1+\sqrt{37}}{2}\right)^H\cup\left(\frac{1+\sqrt{37}}{4}\right)^H\cup\left(\frac{-1+\sqrt{37}}{-4}\right)^H.$$

Whereas $\mathbb{Q}^*\left(\sqrt{37}\right)$ splits into four *G*-orbits namely $\left(\sqrt{37}\right)^G$, $\left(\frac{1+\sqrt{37}}{2}\right)^G$ $\left(\frac{1+\sqrt{37}}{3}\right)^G$ and $\left(\frac{-1+\sqrt{37}}{-3}\right)^G$. (see **Figure 1**) ◆

Theorem 3.13 Let *p* be an odd prime factor of *n*. Then $S_1^p=\left\{\alpha\in\mathbb{Q}^*\left(\sqrt{n}\right):\left(b/p\right)\text{or}\left(c/p\right)=1\right\}$ and $S_2^p=\left\{\alpha\in\mathbb{Q}^*\left(\sqrt{n}\right):\left(b/p\right)\text{or}\left(c/p\right)=-1\right\}$ are two H^*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$. In particular, these are the only H^*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$ depending upon classes $\left[a,b,c\right]$ modulo *p*.

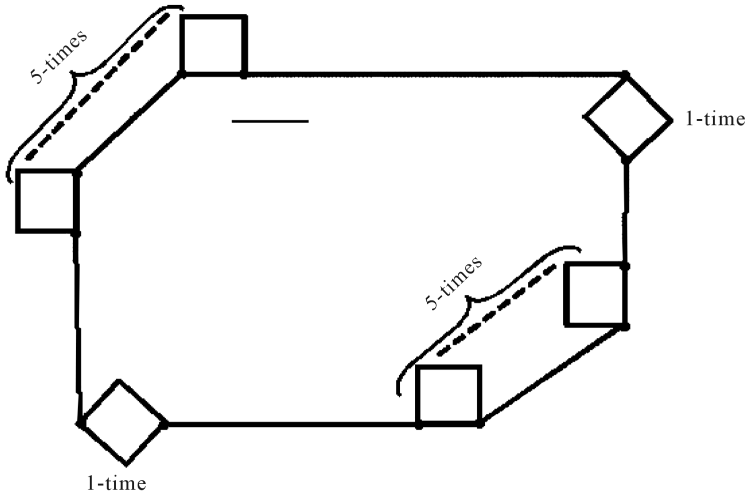

Figure 1. Orbit of $\beta = \frac{1+\sqrt{37}}{2}$ and $(xy)^3(xy^2)(xy^3)^5(xy^2)(xy)^2(\beta) = \beta$.

Proof. Let $[a,b,c](mod\ p)$ be the class of $\alpha(a,b,c) \in \mathbb{Q}^*(\sqrt{n})$. In view of Lemma 3.3, either both of b,c are qrs or qnrs and the two equations $xy(\alpha(a,b,c)) = \alpha'(a+c, 2a+b+c, c)$, $yx(\alpha(a,b,c)) = \alpha'(a-2b, b, -4a+4b+c)$ 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 H^*-subsets of $\mathbb{Q}^*(\sqrt{n})$ depending upon classes modulo p. ■

The following corollary is an immediate consequence of Lemma 3.6 and Theorem 3.13.

Corollary 3.14 Let p be an odd prime and $n \equiv 0(mod\ 2p)$. Then $\mathbb{Q}^*(\sqrt{n})$ splits into four proper H^*-subsets 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 $a^2 \equiv bc(mod\ 2)$. By Theorem 3.13 S_1^p, S_2^p are H^*-subsets and then, by Lemma 3.6, each of S_1^p and S_2^p further splits into two H^*-subsets $S_1^p \cap \mathbb{Q}^{**}(\sqrt{n})$, $S_2^p \cap \mathbb{Q}^{**}(\sqrt{n})$, $S_1^p \setminus \mathbb{Q}^{**}(\sqrt{n})$ and $S_2^p \setminus \mathbb{Q}^{**}(\sqrt{n})$. ■

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

Theorem 3.15 Let p be an odd prime and $(n/p) = \pm 1$. Then $\mathbb{Q}^*(\sqrt{n})$ is itself an H^*-set depending upon classes $[a,b,c]$ modulo p.

Proof. follows from Lemmas 3.4, 3.5 and the equations $xy(\alpha) = \alpha + 1$ and $yx(\alpha) = \frac{\alpha}{1-2\alpha}$ given in **Table 1**.

Let us illustrate the above theorem in view of Theorem 3.4. If $(n/3) = 1$, then the set $\{[0,1,2],[0,2,1],[1,0,1],[1,1,0],[2,0,2],[2,0,1],[2,1,0],[2,2,0],[1,2,0],[1,0,2],[1,0,0],[2,0,0]\}$ is an H^*-set. That is, $\mathbb{Q}^*(\sqrt{n})$ is itself an H^*-set depending upon classes $[a,b,c]$ modulo 3. Similarly for $(n/3) = -1$.

Theorem 3.16 Let p be an odd prime and n is a quadratic residue (quadratic non-residue) of 2p. Then $\mathbb{Q}^*(\sqrt{n})$ is the disjoint union of three H^*-subsets $\mathbb{Q}^*(\sqrt{n}) \setminus \mathbb{Q}^{**}(\sqrt{n})$, $\mathbb{Q}^{**}(\sqrt{n}) \setminus \mathbb{Q}'(\sqrt{n})$ and $\mathbb{Q}'(\sqrt{n})$ depending upon classes $[a,b,c]$ modulo 2p.

Proof. Follows by Theorems 2.6, 2.7 and 3.15. ■

The following example justifies the above result.

Example 3.17 Since $17 \equiv 5(mod\ 6)$, then $\mathbb{Q}^*(\sqrt{15})$ splits into these three H^*-subsets

$\{[0,1,1],[1,2,1],[2,5,1],[3,4,1],[4,5,1],[5,2,1],[0,5,5],[5,4,5],[4,1,5],[3,2,5],[2,1,5],[1,4,5]\}$,

$\{[1,1,2],[3,5,2],[5,1,2],[3,1,4],[1,5,4],[5,5,4]\}$, $\{[1,2,4],[5,2,4],[3,4,4],[1,4,2],[3,2,2],[5,4,2]\}$. ◆

The next theorem is a generalization of Theorem 3.13 to the case when n involves two distinct prime factors.

Theorem 3.20 Let p_1 and p_2 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 H^*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$. More precisely these are the only H^*-subsets of $\mathbb{Q}^*\left(\sqrt{n}\right)$ depending upon classes $[a,b,c]$ modulo $p_1 p_2$.

Proof. Let $[a,b,c](mod\ p_1 p_2)$ be any class of $\alpha(a,b,c) \in \mathbb{Q}^*\left(\sqrt{n}\right)$ with $n \equiv 0(mod\ p_1 p_2)$. Then $a^2 - n = bc$ implies that

$$a^2 \equiv bc(mod\ p_1 p_2) \tag{1}$$

This is equivalent to congruences $a^2 \equiv bc(mod\ p_1)$ and $a^2 \equiv bc(mod\ p_2)$. By Theorem 3.14, the congruence $a^2 \equiv bc(mod\ p_1)$ gives two H^*-subsets $S_1^{p_1} = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : (c/p_1) \text{ or } (c/p_1) = 1\right\}$ and $S_2^{p_1} = \left\{\alpha \in \mathbb{Q}^*\left(\sqrt{n}\right) : (c/p_1) \text{ or } (c/p_1) = -1\right\}$ of $\mathbb{Q}^*\left(\sqrt{n}\right)$. As $a^2 \equiv bc(mod\ p_2)$, again applying Theorem 3.13 on each of $S_1^{p_1}$ and $S_2^{p_1}$ we have four H^*-subsets $S_{1,1}$, $S_{1,2}$, $S_{2,1}$ and $S_{2,2}$ of $\mathbb{Q}^*\left(\sqrt{n}\right)$.

References

[1] Sahin, R. and Bizim, O. (2003) Some Subgroups of the Extended Hecke Groups $\bar{H}(\lambda_q)$. *Mathematica Acta Scientia*, **23B**, 497-502.

[2] Mushtaq, Q. (1988) Modular Group Acting on Real Quadratic Fields. *Bulletin of the Australian Mathematical Society*, **3**, 303-309.

[3] Husnine, S.M., Aslam Malik, M. and Majeed, A. (2005) On Ambiguous Numbers of an Invariant Subset $\mathbb{Q}^*\left(\sqrt{k^2 m}\right)$ of $\mathbb{Q}\left(\sqrt{m}\right)$ under the Action of the Modular Group PSL(2,Z). *Studia Scientiarum Mathematicarum Hungarica*, **42**, 401-412. http://dx.doi.org/10.1556/SScMath.42.2005.4.5

[4] Aslam Malik, M. and Asim Zafar, M. (2011) Real Quadratic Irrational Numbers and Modular Group Action. *Southeast Asian Bulletin of Mathematics*, **35**, 439-445.

[5] Malik, M.A. and Asim Zafar, M. (2013) *G*-Subsets of an Invariant Subset $\mathbb{Q}^*\left(\sqrt{k^2 m}\right)$ of $\mathbb{Q}\left(\sqrt{m}\right) \backslash Q$ under the Modular Group Action. *Utilitas Mathematica*, **91**, 377-387.

[6] Aslam Malik, M., Husnine, S.M. and Majeed, A. (2005) Intrasitive Action of the Modular Group $PSL_2(\mathbb{Z})$ on a Subset $\mathbb{Q}^*\left(\sqrt{k^2 m}\right)$ of $\mathbb{Q}\left(\sqrt{m}\right)$. *PUJM*, **37**, 31-38.

[7] Mushtaq, Q. and Aslam, M. (1997) Transitive Action of a Two Generator Group on Rational Projective Line. *Southeast Asian Bulletin of Mathematics*, **1**, 203-207.

[8] Aslam Malik, M., Husnine, S.M. and Asim Zafar, M. (2012) Certain *H*-Subsets of $\mathbb{Q}\left(\sqrt{m}\right) \backslash \mathbb{Q}$ under the Action of $H = \langle x, y : x^2 = y^4 = 1 \rangle$. *Pakistan Journal of Science*, **64**, 67-74.