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

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

Copyright © 2014 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/

Abstract

$\mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$ is the disjoint union of $\mathbb{Q}^\ast(\sqrt{k^2m})$ for all $k \in \mathbb{N}$, where $\mathbb{Q}^\ast(\sqrt{k^2m})$ is the set of all roots of primitive second degree equations $ct^2 + 2at + b = 0$, with reduced discriminant $\Delta = a^2 - 4bc$ equal to $k^2m$. We study the action of two Hecke groups—the full modular group $H(\lambda) = \text{PSL}_2(\mathbb{Z})$ and the group of linear-fractional transformations $H(\lambda_q) = \{x, y : x^2 = y^2 = 1\}$ on $\mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$. In particular, we investigate the action of $H(\lambda_q) \cap H(\lambda_a)$ on $\mathbb{Q}^\ast(\sqrt{k^2m})$ for finding different orbits.

Keywords
Quadratic Irrationals, Hecke Groups, Legendre Symbol, $G$-Set

1. Introduction

In 1936, Erich Hecke (see [1]) introduced the groups $H(\lambda)$ generated by two linear-fractional transformations $T(z) = -\frac{1}{z}$ and $S(z) = -\frac{1}{z + \lambda}$. Hecke showed that $H(\lambda)$ 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 $H(\lambda_q)$ is isomorphic to the free product of two finite cyclic group of order 2 and $q$, and it has a presentation $H(\lambda_q) = \langle T, S : T^2 = S^q = 1 \rangle \cong C_2 \ast C_q$.

How to cite this paper: Malik, M.A. and Zafar, M.A. (2014) On Subsets of $\mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$ under the Action of Hecke Groups $H(\lambda_q)$. Applied Mathematics, 5, 1284-1291. http://dx.doi.org/10.4236/am.2014.58120
The first few of these groups are $H(\lambda_1) = G = PSL(2,\mathbb{Z})$, the full modular group having special interest for mathematicians in many fields of Mathematics, $H(\lambda_2) = H$ and $H(\lambda_3) = M$.

A non-empty set $\Omega$ with an action of the group $G$ on it, is said to be a $G$-set. We say that $\Omega$ is a transitive $G$-set if, for any $p, q$ in $\Omega$ there exists a $g$ in $G$ such that $p^g = q$. Let $n = k^2m$, where $k \in \mathbb{N}$ and $m$ is a square free positive integer. Then

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

is the set of all roots of primitive second degree equations $ct^2 + 2at + b = 0$, with reduced discriminant $\Delta = a^2 - 4bc$ equal to $n$ and

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

is the disjoint union of $Q'(\sqrt{n})$ for all $k$. If $\alpha(a, b, c) \in Q'(\sqrt{n})$ and its conjugate $\bar{\alpha}$ have opposite signs then $\alpha$ is called an ambiguous number [2]. The actual number of ambiguous numbers in $Q'(\sqrt{n})$ has been discussed in [3] as a function of $n$. The classification of the real quadratic irrational numbers $\alpha(a, b, c)$ of $Q'(\sqrt{n})$ 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 $y'(z) = \frac{-1}{z + 4}$, 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 $y(z) = \frac{1}{2z(z + 1)}$ and its proper subgroups on $\mathbb{Q} \cup \{ \infty \}$ has been discussed in [7] [8].

$Q'(\sqrt{n})$ invariant under the action of modular group $G$ but $Q'(\sqrt{n})$ 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 $Q''(\sqrt{n}) = \left\{ \alpha \in Q'(\sqrt{n}) : 2|c \right\}$ and $Q'(\sqrt{n}) \setminus Q''(\sqrt{n})$ is invariant under $H'$ and hence we find $G$-subsets of $Q'(\sqrt{n})$ and $H$-subsets of $Q''(\sqrt{n})$

or $Q''(\sqrt{n}) = \left\{ Q'(\sqrt{\frac{n}{4}}), Q'(\sqrt{\frac{n}{4}}) \right\} \cup Q''(\sqrt{n})$ according as $n \equiv 0(\text{mod} 4)$ or $n \equiv 0(\text{mod} 4)$ and $Q''(\sqrt{4n})$

for all non-square $n$. Also the partition of $Q'(\sqrt{n})$ has been discussed depending upon classes $[a, b, c]$ modulo $p, p_2$.

2. Preliminaries

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

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

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

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

**Theorem 2.4** (see [6]) If $n \equiv 1(\text{mod} 4)$, then $Q'(\sqrt{n}) = \left\{ \alpha \in Q'(\sqrt{n}) : 2|(b, c) \right\}$ and
Table 1. The action of elements of $G$ and $H$ on $\alpha \in \mathbb{Q}^*(\sqrt{n})$.

<table>
<thead>
<tr>
<th>Action</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x'(\alpha) = \frac{-1}{\alpha}$</td>
<td>$-a$</td>
</tr>
<tr>
<td>$y'(\alpha) = \frac{\alpha - 1}{\alpha}$</td>
<td>$-a + b$</td>
</tr>
<tr>
<td>$(y')^2(\alpha) = \frac{1}{1 - \alpha}$</td>
<td>$-a + c$</td>
</tr>
<tr>
<td>$x'y'(\alpha) = \frac{\alpha}{1 - \alpha}$</td>
<td>$a - b$</td>
</tr>
<tr>
<td>$y'x'(\alpha) = 1 + \alpha$</td>
<td>$a + c$</td>
</tr>
<tr>
<td>$(y')^3(x'(\alpha) = \frac{\alpha}{1 + \alpha}$</td>
<td>$a + b$</td>
</tr>
<tr>
<td>$x(\alpha) = \frac{-1}{2\alpha}$</td>
<td>$-a$</td>
</tr>
<tr>
<td>$y(\alpha) = \frac{-1}{2(\alpha + 1)}$</td>
<td>$-a - c$</td>
</tr>
<tr>
<td>$y^2(\alpha) = \frac{-(\alpha + 1)}{2(\alpha)}$</td>
<td>$-3a - 2b - c$</td>
</tr>
<tr>
<td>$y^3(\alpha) = \frac{2(\alpha + 1)}{2\alpha}$</td>
<td>$-a - 2b$</td>
</tr>
<tr>
<td>$xy(\alpha) = a + 1$</td>
<td>$a + c$</td>
</tr>
<tr>
<td>$yx(\alpha) = \frac{a + 1}{1 - 2\alpha}$</td>
<td>$a - 2b$</td>
</tr>
<tr>
<td>$y'x(\alpha) = \frac{-1 - 2a}{2(-1 + \alpha)}$</td>
<td>$3a - 2b - c$</td>
</tr>
<tr>
<td>$y'x(\alpha) = a - 1$</td>
<td>$-a - c$</td>
</tr>
</tbody>
</table>

$\mathbb{Q}^*(\sqrt{n}) \setminus \mathbb{Q}^*(\sqrt{n}) = \{ \alpha \in \mathbb{Q}^*(\sqrt{n}) : 2 \nmid (b, c) \}$ 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 $n \neq 0 \pmod{4}$ then $\frac{\alpha}{2} \in \mathbb{Q}^*(\sqrt{n})$ if and only if $2 \nmid b$.

2) $\frac{\alpha}{2} \in \mathbb{Q}^*(\sqrt{n})$ 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 $n = 1, 2$ or $3 \pmod{4}$, $\mathbb{Q}^*(\sqrt{n}) = \{ \alpha \in \mathbb{Q}^*(\sqrt{n}) : 2 \nmid c \}$ 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
\[ H = \langle x, y : x^r = y^s = 1 \rangle, \] 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 \( y^3 = \frac{1}{2} (x'(y')^2)^2 x' \).
2. \( xy = y'x' \) and \( yx = (x'y')^2 \).
3. \( y^2x = x'(y')^2 \) and \( xy^3 = (y')^2 (x') \).
4. \( y^2x = \frac{1}{2} \left( x'(y')^2 \right)^2 (x'y') \) and \( xy^2 = \frac{1}{2} (y'x')(y')^2 x' \).
5. \( x' = 2x \) and \( y' = (2x)(2y) \).
6. \( x'y' = 2(2y)(2x) \) and \( x'(y')^2 = y'x' \). In particular \( (x'y')^{-1} = 2 \left( xy^2 \right)^{-1} \) and \( x'(y')^2 = xy \).

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 \( \mathcal{H} = \langle x, y \rangle \) 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 \( yxyx = y'^2 \), \( xyxy = xy^2 x \), so \( \langle y^2, x^2 \rangle \) is a proper subgroup of \( \mathcal{H} \).
3) \( \langle \mathcal{H}, x \rangle = \langle \mathcal{H}', y \rangle = H \) and \( \langle \mathcal{H}', x' \rangle = \langle \mathcal{H}', y' \rangle = G \).

Since for each integer \( n \), either \( (n/p) = 0 \) or \( (n/p) = \pm 1 \) for each odd prime \( p \). So in the following lemma, we classify the elements of \( \mathbb{Q}^{\sqrt{n}} \) in terms of classes \( \mathbb{Z} \) \( (a, b, c)(mod \ p) \) with 0 modulo \( p \) or \( qr, qnr \) nature of \( a, b \) and \( c \) modulo \( p \).

**Lemma 3.3** Let \( p \) be prime and \( n = 0 (mod \ p) \). Then \( \mathbb{E}_p \) consists of classes \( [0, 0, qr], [0, 0, qnr], [0, qr, 0], [0, qnr, 0], [qr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr] \) or \( [qnr, qnr, qnr] \).

Proof. Let \( \langle a, b, c \rangle (mod \ p) \) be any class of \( \mathcal{A}(a, b, c) \). Then \( a = b \langle mod \ p \rangle \) leads us to exactly three cases. If \( a = b \langle mod \ p \rangle \) then exactly one of \( b, c \) is \( = 0 \langle mod \ p \rangle \) and the other is \( qr \) or \( qnr \) of \( p \) as otherwise \( (a, b, c) \neq 1 \) and hence the class \( \mathcal{A}(a, b, c) \) is one of the forms \( [0, 0, qr], [0, 0, qnr], [0, qr, 0], [0, qnr, 0], [qr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr] \).

If \( a = b \langle mod \ p \rangle \) then \( (bc) = 1 \) and the class takes the form \( [qr, qr, qr] \) or \( [qr, qnr, qnr] \). In third case if \( a = b \langle mod \ p \rangle \) then \( (c/p) = 1 \) so again \( (bc) = 1 \). This yields the class in the forms \( [qr, qr, qr] \) or \( [qr, qnr, qnr] \). Hence the result. \( \blacksquare \)

**Lemma 3.4** Let \( (n/p) = 1 \) and let \( \langle a, b, c \rangle (mod \ p) \) be the class of \( \mathcal{A}(a, b, c) \) of \( \mathbb{Q}^{\sqrt{n}} \).

Then:
1. If \( p = 1(mod \ 4) \) then \( \langle a, b, c \rangle (mod \ p) \) has the forms \( [0, qr, qr], [0, qnr, qnr], [qr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr] \) or \( [qnr, qnr, qnr] \) only.
2. If \( p = 3(mod \ 4) \) then \( \langle a, b, c \rangle (mod \ p) \) has the forms \( [0, qr, qnr], [0, qnr, qr], [qr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr], [qnr, qnr, qnr], [qnr, qnr, qnr] \) or \( [qnr, qnr, qnr] \) only.

Proof. Let \( \langle a, b, c \rangle (mod \ p) \) be the class of \( \mathcal{A}(a, b, c) \) with \( a^2 - n = bc \). As \( (n/p) = 1 \) so if \( (a/p) = 0 \) then \( (a^2 - n)/p = \pm 1 \) according as \( p = 1(mod \ 4) \) or \( p = 3(mod \ 4) \). Thus we have \( [0, qr, qr], [0, qnr, qnr] \) if \( p = 1(mod \ 4) \) and \( [0, qr, qnr], [0, qnr, qr] \) if \( p = 3(mod \ 4) \). If \( (a/p) = \pm 1 \) then \( (a^2 - n)/p = 0 \), so we get \( [qr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr], [qnr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr] \) or \( [qr, qnr, qnr] \) only. This proof is now complete. \( \blacksquare \)

**Lemma 3.5** Let \( (n/p) = -1 \) and let \( \langle a, b, c \rangle (mod \ p) \) be the class of \( \mathcal{A}(a, b, c) \) of \( \mathbb{Q}^{\sqrt{n}} \).

Then:
1. If \( p = 1(mod \ 4) \) then \( \langle a, b, c \rangle (mod \ p) \) has the forms \( [0, qr, qr], [0, qnr, qnr], [qr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr] \) or \( [qnr, qnr, qnr] \) only.
2. If \( p = 3(mod \ 4) \) then \( \langle a, b, c \rangle (mod \ p) \) has the forms \( [0, qr, qr], [0, qnr, qnr], [qr, qr, qr], [qr, qnr, qnr], [qnr, qnr, qnr] \) or \( [qnr, qnr, qnr] \) 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 \(\mathbb{Q}^*(\sqrt{n})\) are \([1,0,1]\), \([1,1,0]\) and \([0,1,1]\) modulo 2. These are the only classes of \(\mathbb{Q}^*(\sqrt{n})\) if \(n \equiv 3 \text{ (mod } 4)\). But if \(n \equiv 1 \text{ (mod } 4)\) then \([1,0,0]\) is also a class of \(\mathbb{Q}^*(\sqrt{n})\) 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 \(n \equiv 1 \text{ (mod } 4)\) 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 \(\mathbb{Q}^*(\sqrt{n})\) 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 \(\mathbb{Q}^*(\sqrt{n})\) 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 \(\mathbb{Q}^*(\sqrt{n})\) 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

\[
\begin{align*}
xy(a + \sqrt{n}c) - a + c + \sqrt{n}c &= 0, \\
\alpha = \alpha' = \alpha' = \alpha' = \alpha' = \alpha' = \alpha'.
\end{align*}
\]

Remark 3.8 1) Let \(n \equiv 1 \text{ (mod } 4)\). Then \(\mathbb{Q}^*(\sqrt{n}) = \{\alpha \in \mathbb{Q}^*(\sqrt{n}) : c = 1 \text{ (mod } 4)\}\) and \(\mathbb{Q}^*(\sqrt{n}) = \{\alpha \in \mathbb{Q}^*(\sqrt{n}) : c = 3 \text{ (mod } 4)\}\) are \(H^*\)-subsets of \(\mathbb{Q}^*(\sqrt{n})\). In particular if \(n = 5 \text{ (mod } 8)\), 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 \(n = 1 \text{ (mod } 8)\), then \(C_1 = \{\alpha \in \mathbb{Q}^*(\sqrt{n}) \cap B : a = 1 \text{ (mod } 4)\}\),

\[
\begin{align*}
C_2 &= \{\alpha \in \mathbb{Q}^*(\sqrt{n}) \cap B : a = 3 \text{ (mod } 4)\}, \\
C_3 &= \{\alpha \in \mathbb{Q}^*(\sqrt{n}) : c = 2 \text{ (mod } 4)\}
\end{align*}
\]

are \(H^*\)-subsets of \(\mathbb{Q}^*(\sqrt{n})\). Specifically, \(B_1 = C_1 \cup C_2 \cup C_3\), \(B_2 = C_3\).

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

3) If \(n = 0\) or \(3 \text{ (mod } 4)\), then \(B_2\) or \(B_1\) is empty according as \(n = 0\) or \(3 \text{ (mod } 4)\). As we know that if \(n\) and \(c\) are even, then \(a\) must be odd as \((a,b,c) = 1\). However \(D_1 = \{\alpha \in \mathbb{Q}^*(\sqrt{n}) : b = 1 \text{ (mod } 4)\}\),

\[
\begin{align*}
D_2 &= \{\alpha \in \mathbb{Q}^*(\sqrt{n}) : b = 3 \text{ (mod } 4)\}
\end{align*}
\]

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 \(\mathbb{Q}^*(\sqrt{n}) = \mathbb{Q}^*(\sqrt{n})\setminus \mathbb{Q}^*(\sqrt{n})\) are distinct \(H^*\)-subsets of an \(H\)-set \(\mathbb{Q}^*(\sqrt{n}) = \mathbb{Q}^*(\sqrt{n})\setminus \mathbb{Q}^*(\sqrt{n})\) and vice versa. Hence \(\mathbb{Q}^*(\sqrt{n}) \setminus \mathbb{Q}^*(\sqrt{n})\) is equivalent to \(\mathbb{Q}^*(\sqrt{n})\).
$Q^*(\sqrt{n})$ (see [8]).

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

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

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

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

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

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

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

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

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

Proof of c) follows by the equation $x(Q^*(\sqrt{n}) \setminus Q^*(\sqrt{n})) = Q^*(-\sqrt{n})$.

Following examples illustrate the above results.

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

2) $Q^*(\sqrt{37})$ splits into nine $H$-orbits. Also

$$Q^*(\sqrt{48}) = (\sqrt{37})^H \cup (\sqrt{37})^H \cup \left(\frac{1+\sqrt{37}}{3}\right)^H \cup \left(\frac{1+\sqrt{37}}{-3}\right)^H \cup \left(\frac{-1+\sqrt{37}}{-3}\right)^H \cup \left(\frac{-1+\sqrt{37}}{3}\right)^H$$

and

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

Whereas $Q^*(\sqrt{37})$ splits into four $G$-orbits namely $(\sqrt{37})^G, \left(\frac{1+\sqrt{37}}{2}\right)^G, \left(\frac{1+\sqrt{37}}{3}\right)^G$ 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 $S^*_1 = \{ \alpha \in Q^*(\sqrt{n}) : (b/p) \text{ or } (c/p) = 1 \}$ and $S^*_2 = \{ \alpha \in Q^*(\sqrt{n}) : (b/p) \text{ or } (c/p) = -1 \}$ are two $H^*$-subsets of $Q^*(\sqrt{n})$. In particular, these are the only $H^*$-subsets of $Q^*(\sqrt{n})$ depending upon classes $[a,b,c]$ modulo $p$. 

1289
\textbf{Proof.} Let \([a,b,c](\text{mod } p)\) 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 qns 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 \(a=b=0(\text{mod } p)\) then \(((2a+b+c)/p)=1\) or \(((2a+b+c)/p)=-1\) according as \((c/p)=1\) or \((c/p)=-1\). Similarly for \(a=c=0(\text{mod } p)\). This shows that the sets \(S_p^o\) and \(S_p^e\) are \(H^*\)-subsets of \(Q^*(\sqrt{n})\) depending upon classes modulo \(p\).

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

\textbf{Corollary 3.14} Let \(p\) be an odd prime and \(n \equiv 2(\text{mod } 2p)\). Then \(Q^*(\sqrt{n})\) splits into four proper \(H^*\)-subsets depending upon classes modulo \(p\).

\textbf{Proof.} Since \(a^2-n=bc\) implies that \(a^2 \equiv bc(\text{mod } 2p)\). This is equivalent to congruences \(a^2 \equiv bc(\text{mod } 2)\) and \(a^2 \equiv bc(\text{mod } 2p)\). By Theorem 3.13 \(S_p^o\), \(S_p^e\) are \(H^*\)-subsets and then, by Lemma 3.6, each of \(S_p^o\) and \(S_p^e\) further splits into two \(H^*\)-subsets \(S_p^o \cap Q^*(\sqrt{n})\), \(S_p^e \cap Q^*(\sqrt{n})\), \(S_p^o \setminus Q^*(\sqrt{n})\) and \(S_p^e \setminus Q^*(\sqrt{n})\). \(\blacksquare\)

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

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

\textbf{Proof.} follows from Lemmas 3.4, 3.5 and the equations \(xy(\alpha)=\alpha^2+1\) 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 \([0,1,2],[0,2,1],[1,0,1],[1,1,0],[2,0,2],[2,0,1],[2,1,0],[2,2,0],[1,0,2],[1,0,0],[2,0,0]\) is an \(H^*\)-set. That is, \(Q^*(\sqrt{n})\) is itself an \(H^*\)-set depending upon classes \([a,b,c]\) modulo 3. Similarly for \((n/3)=-1\).

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

\textbf{Proof.} Follows by Theorems 2.6, 2.7 and 3.15. \(\blacksquare\)

The following example justifies the above result.

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

\([0,1,1],[2,5,1],[3,4,1],[4,5,1],[5,2,1],[0,5,5],[5,5,5],[4,1,5],[3,2,5],[2,1,5],[1,4,5]\), \([1,1,2],[3,5,2],[5,1,2],[3,1,4],[1,5,4],[5,5,4]\), \([1,2,4],[5,2,4],[3,4,4],[1,4,2],[3,2,2],[5,4,2]\). \(\blacksquare\)
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 $S_{1,1} = S_1^h \cap S_2^p$, $S_{1,2} = S_1^h \cap S_2^p$, $S_{2,1} = S_2^h \cap S_1^p$ and $S_{2,2} = S_2^h \cap S_1^p$ 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 $p_1p_2$.

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

$$a^2 \equiv bc \pmod{p_1p_2} \quad (1)$$

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


