G-subsets and G-orbits of $Q^*(\sqrt{n})$ under action of the Modular Group.

M. Aslam Malik *and M. Riaz †

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

Abstract

It is well known that $G = \langle x, y : x^2 = y^3 = 1 \rangle$ represents the modular group $PSL(2, Z)$, where $x : z \to \frac{-1}{z}, y : z \to \frac{z-1}{z}$ are linear fractional transformations. Let $n = k^2m$, where k is any non zero integer and m is square free positive integer. Then the set

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

is a G-subset of the real quadratic field $Q(\sqrt{m})$ [12]. We denote $\alpha = \frac{a+\sqrt{n}}{c}$ in $Q^*(\sqrt{n})$ by $\alpha(a, b, c)$. For a fixed integer $s > 1$, we say that two elements $\alpha(a, b, c)$, $\alpha'(a', b', c')$ of $Q^*(\sqrt{n})$ are s-equivalent if and only if $a \equiv a'(mod\ s)$, $b \equiv b'(mod\ s)$ and $c \equiv c'(mod\ s)$. The class $[a, b, c](mod\ s)$ contains all s-equivalent elements of $Q^*(\sqrt{n})$ and E_s^n denotes the set consisting of all such classes of the form $[a, b, c](mod\ s)$.

In this paper we investigate proper G-subsets and G-orbits of the set $Q^*(\sqrt{n})$ under the action of Modular Group G.

---

*malikpu@yahoo.com

†mriaz@math.pu.edu.pk

1 Introduction

An integer $m > 0$ is said to be square free if its prime decomposition contains no repeated factors. It is well known that every irrational member of $Q(\sqrt{m})$ can be uniquely expressed as $\frac{a+\sqrt{n}}{c}$, where $n = k^2 m$ for some integer k and a, $\frac{a^2-n}{c}$ and c are relatively prime integers.

The set $Q^*(\sqrt{n}) = \{\frac{a+\sqrt{n}}{c} : a, c, b = \frac{a^2-n}{c} \in Z \text{ and } (a, b, c) = 1\}$ is a proper G-subset of $Q(\sqrt{m})$ [12]. If $\alpha = \frac{a+\sqrt{n}}{c}$ and $\bar{\alpha} = \frac{a-\sqrt{n}}{c}$ have different signs, then α is called an ambiguous number. These ambiguous numbers play an important role in the study of action of G on $Q(\sqrt{m}) \cup \{\infty\}$, as $\text{Stab}_\alpha(G)$ are the only non-trivial stabilizers and in the orbit α^G, there is only one (up to isomorphism).

G. Higman (1978) introduced the concept of the coset diagrams for the modular group $PSL(2, Z)$ and Q. Mushtaq (1983) laid its foundation. By using the coset diagrams for the orbit of the modular group $G = \langle x, y : x^2 = y^3 = 1 \rangle$ acting on the real quadratic fields Mushtaq [12] showed that for a fixed non-square positive integer n, there are only a finite number of ambiguous numbers in $Q^*(\sqrt{n})$, and that the ambiguous numbers in the coset diagram for the orbit α^G form a closed path and it is the only closed path contained in it. Let $C' = C \cup \{\pm\infty\}$ be the extended complex plane. The action of the modular group $PSL(2, Z)$ on an imaginary quadratic field, subsets of C', has been discussed in [11]. The action of the modular group on the real quadratic fields, subsets of C', has been discussed in detail in [2], [12] and [13]. The exact number of ambiguous numbers in $Q^*(\sqrt{n})$ has been determined in [7], [15] as a function of n. The ambiguous length of an orbit α^G is the number of ambiguous numbers in the same orbit [7], [15]. The Number of Subgroups of $PSL(2, Z)$ when acting on $F_p \cup \{\infty\}$ has been discussed in [14] and the subgroups of the classical modular group has been discussed in [10].
A classification of the elements $(a + \sqrt{p})/c$, $b = (a^2 - p)/c$, of $Q^*(\sqrt{p})$, p an odd prime, with respect to odd-even nature of a, b, c has been given in [3]. M. Aslam Malik et al. [8] proved, by using the notion of congruence, that for each non-square positive integer $n > 2$, the action of the group G on a subset $Q^*(\sqrt{n})$ of the real Quadratic field $Q(\sqrt{m})$ is intransitive.
If p is an odd prime,then $t \not\equiv 0 (mod\ p)$ is said to be a quadratic residue of p if there exists an integer u such that $u^2 \equiv t (mod\ p)$.
The quadratic residues of p form a subgroup Q of the group of nonzero inte-

gers modulo p under multiplication and $|Q| = (p-1)/2$. [1]

Lemma 1.1 If $v_1, v_2 \in Q$, $n_1, n_2 \notin Q$ (v_1, v_2 are quadratic residues, and n_1, n_2 are quadratic non-residue, Then

(a) $n_1 v_1$ is a quadratic non-residue.

(b) $n_1 n_2$ is a quadratic residue.

(c) $v_1 v_2$ is a quadratic residue.

In the sequel, $q.r$ and $q.nr$ will stand for quadratic residue and quadratic non-residue respectively. The Legendre symbol (a/p) is defined as 1 if a is a quadratic residue of p otherwise it is defined by -1. [1]

We denote the element $\alpha = \frac{a+\sqrt{n}}{c}$ of $Q^*(\sqrt{n})$ by $\alpha(a, b, c)$ and say that two elements $\alpha(a, b, c)$ and $\alpha'(a', b', c')$ of $Q^*(\sqrt{n})$ are s-equivalent (and write $\alpha(a, b, c) \sim_s \alpha'(a', b', c')$ or $\alpha \sim_s \alpha'$) if and only if $a \equiv a'(mod\ s)$, $b \equiv b'(mod\ s)$ and $c \equiv c'(mod\ s)$. Clearly the relation $\sim_s$ is an equivalence relation, so for each integer $s > 1$, we get different equivalence classes $[a, b, c]$ modulo s of $Q^*(\sqrt{n})$. [8]

Let E_s denote the set consisting of classes of the form $[a, b, c]$ $(mod\ s)$, n modulo s whereas if $n \equiv i(mod\ s)$ for some fixed $i \in \{0, 1, ..., s-1\}$ and the set consisting of elements of the form $[a, b, c]$ with $n \equiv i(mod\ s)$ is denoted by E_p^i (or E_s^n). Obviously $\cup_{i=1}^{s-1} E_s^i = E_s$ and $E_s^i \cap E_s^j = \phi$ for $i \neq j$. [6]

The classification of the real quadratic irrational numbers by taking prime modulus is very helpful in studying the modular group action on the real quadratic fields. Thus it becomes interesting to determine the proper G-subsets of $Q^*(\sqrt{n})$ by taking the action of G on the set $Q^*(\sqrt{n})$ and hence to find the G-orbits of $Q^*(\sqrt{n})$ for each non square n.

2 Modular group G acting on $Q^*(\sqrt{n})$.

In [8], it was shown that the action of the group on $Q^*(\sqrt{2})$ is transitive, whereas the action of G on $Q^*(\sqrt{n})$, $n \neq 2$ is intransitive. Specifically, it was proved with the help of classes $[a, b, c](mod\ 2^2)$ of the elements of $Q^*(\sqrt{n})$ that $Q^*(\sqrt{n})$, $n \not\equiv 2(mod\ 4)$, has two proper G-subsets.

Q. Mushtaq [12], In the case of $PSL(2, 13)$, showed one G-orbit of length 13 in the coset diagram for the natural action of $PSL(2, Z)$ on any subset of the real projective line. In [6] it was proved that there exist two proper G-subsets of $Q^*(\sqrt{n})$ when $n \equiv 0$ $(mod\ p)$ and four G-subsets of $Q^*(\sqrt{n})$ when $n \equiv 0$ $(mod\ pq)$. In the present studies, with the help of the idea of

quadratic residues, we generalize this result and prove some crucial results which provide us proper G-subsets and G-orbits of $Q^*(\sqrt{n})$.
We extend this idea to determine four proper G-subsets of $Q^*(\sqrt{n})$ with $n \equiv 0 \ (mod \ 2pq)$.

Lemma 2.1
Let $n \equiv 0(mod \ 2pq)$ where p and q are two distinct odd primes, Let $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ then the sets
$S_1 = \{\alpha \in Q^*(\sqrt{n}) : (c/pq) = 1 \text{ or } (b/pq) = 1 \}$,
$S_2 = \{\alpha \in Q^*(\sqrt{n}) : (c/p) = -1 \text{ or } (b/p) = -1 \text{ with } (c/q) = 1 \text{ or } (b/q) = 1 \}$,
$S_3 = \{\alpha \in Q^*(\sqrt{n}) : (c/p) = 1 \text{ or } (b/p) = 1 \text{ with } (c/q) = -1 \text{ or } (b/q) = -1 \}$,
and $S_4 = \{\alpha \in Q^*(\sqrt{n}) : (c/p) = -1 \text{ or } (b/p) = -1 \text{ with } (c/q) = -1 \text{ or } (b/q) = -1 \}$ are four proper G-subsets of $Q^*(\sqrt{n})$.

Proof.
Let $\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ and $n \equiv 0(mod \ 2pq)$, then $a^2 - n = bc$ forces that

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

where a, b, c are belonging to the complete residue system $\{0, 1, 2, ..., 2\bar{p}q-1\}$. The congruence (1) implies $a^2 \equiv bc(mod \ 2)$, $a^2 \equiv bc(mod \ p)$ and $a^2 \equiv bc(mod \ q)$. Since 1 is the only quadratic residue of 2 and there is no quadratic non-residue of 2. Thus by Lemma 1.1 the quadratic residues and quadratic non residues of pq and $2pq$ are the same. We know that, if $(t, m) = 1$ and $m = 2pq$, then the congruence $x^2 \equiv t \ (mod \ m)$ is solvable and has four incongruent solutions if and only if t is quadratic residue of m [1], and in this case congruence (1) is solvable and has exactly four incongruent solutions.
If $a = b = c$ and each of a, b, c are quadratic residue of pq then there exist four distinct classes

$$[a, b, c], [-a, b, c], [a, -b, -c], [-a, -b, -c](mod \ pq)$$

Thus for each member $[a, b, c](mod \ pq)$, we have four cases.
Case(i) The classes $[a, b, c](mod \ pq)$ with $(bc/pq) = 1$, Then all these classes are contained in S_1.
case(ii) The classes $[a, b, c](mod \ pq)$ with $(b/p) = -1$, $(b/q) = 1$, Then all these classes are contained in S_2.
case(iii) The classes $[a, b, c](mod \ pq)$ with $(b/p) = 1$, $(b/q) = -1$, Then all these classes are contained in S_3.

4

case(iv) The classes $[a, b, c](mod\ pq)$ with $(b/p) = -1$, $(b/q) = -1$, Then all these classes are contained in S_4.

As $x(\alpha) = \frac{-a+\sqrt{n}}{b} = \frac{a_1+\sqrt{n}}{c_1}$, where $a_1 = -a$, $b_1 = c$, $c_1 = b$ and $y(\frac{a+\sqrt{n}}{c}) = \frac{-a+b+\sqrt{n}}{b} = \frac{a_2+\sqrt{n}}{c_2}$, where

$$a_2 = -a + b, \quad b_2 = -2a + b + c, \text{ and } c_2 = b$$

then by the congruence (1) we have

$$(-a + b)^2 \equiv (-2a + b + c)b(mod\ p) \tag{2}$$

Since the modular group $PSL(2, Z)$ has the representation $G = \langle x, y : x^2 = y^3 = 1 \rangle$ and every element of G is a word in the generators x, y of G, to prove that S_1 is invariant under the action of G, it is enough to show that every element of S_1 is mapped onto an element of S_1 under x and y. Thus clearly by the congruences (1) and (2) the sets S_1, S_2, S_3 and S_4 are G-subsets of $Q^*(\sqrt{n})$. □

Remark 2.2

Since the quadratic residues and quadratic non residues of pq and $2pq$ are the same. Therefore the number of G-subsets of $Q^*(\sqrt{n})$ when $n \equiv 0(mod\ pq)$ or $n \equiv 0(mod\ 2pq)$ are same.

Illustration 2.3

In the coset diagram for $Q^*(\sqrt{15})$ there are four G-orbits namely

$$(\sqrt{15})^G, (-\sqrt{15})^G, (\frac{\sqrt{15}}{3})^G \text{ and } (\frac{\sqrt{15}}{-3})^G$$

and similarly there are four G-orbits for $Q^*(\sqrt{30})$ namely

$$(\sqrt{30})^G, (-\sqrt{30})^G, (\frac{\sqrt{30}}{2})^G \text{ and } (\frac{\sqrt{30}}{-2})^G$$

. In the closed path lying in the orbit $(\sqrt{15})^G$, the transformation

$$(yx)^3(y^2x)(yx)^3$$

fixes $k = \sqrt{15}$, that is $g_1(k) = ((yx)^3(y^2x)(yx)^3)(k) = k$.

Let k is an ambiguous number then $x(k)$ is also ambiguous but one of the

number $y(k)$ or $y^2(k)$ is ambiguous. The orientation of edges in the coset diagram is associated with the involution x and the small triangles with y which has order 3. One of k and $x(k)$ is positive and other is negative but one of k, $y(k)$ or $y^2(k)$ is negative but other two are positive. We use an arrow head on an edge to indicate its direction from negative to a positive vertex. The following table shows the details of the orbits α^G, transformations which fixes α, and the ambiguous lengths of each orbit.

Table 1: The Orbits of $\alpha \in Q^*(\sqrt{n})$.

G-orbits	Transformations	Ambiguous Length
$(\sqrt{15})^G$	$(yx)^3(y^2x)(yx)^3$	14
$(-\sqrt{15})^G$	$(yx)^3(y^2x)(yx)^3$	14
$(\frac{\sqrt{15}}{3})^G$	$(yx)(y^2x)^3(yx)$	10
$(\frac{\sqrt{15}}{-3})^G$	$(yx)(y^2x)^3(yx)$	10
$(\sqrt{30})^G$	$(yx)^5(y^2x)^2(yx)^5$	24
$(-\sqrt{30})^G$	$(yx)^5(y^2x)^2(yx)^5$	24
$(\frac{\sqrt{30}}{2})^G$	$(yx)^2(y^2x)(yx)^2(y^2x)(yx)^2$	16
$(\frac{\sqrt{30}}{-2})^G$	$(yx)^2(y^2x)(yx)^2(y^2x)(yx)^2$	16

Now we extend this idea when $n \equiv 0(mod \ p_1p_2...p_r)$.

Theorem 2.4
Let $n \equiv 0(mod \ p_1p_2...p_r)$, where $p_1, p_2, ...p_r$ are distinct odd primes, then there are exactly 2^r, G-subsets of $Q^*(\sqrt{n})$.

6

Proof.

Let $\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ and $n \equiv 0(mod\ p_1 p_2...p_r)$ where $p_1, p_2, ...p_r$ are distinct odd primes, then $a^2 - n = bc$ gives

$$a^2 \equiv bc(mod\ p_1 p_2...p_r) \tag{3}$$

The congruence (3) implies $a^2 \equiv bc(mod\ p_1)$,

$$a^2 \equiv bc(mod\ p_2), ...,\ \text{and}\ a^2 \equiv bc(mod\ p_r)$$

.

We know that, if $(t, m) = 1$ and $m = p_1 p_2...p_r$, then the congruence $x^2 \equiv t\ (mod\ m)$ is solvable if and only if t is quadratic residue of m [1], and in this case congruence (3) is solvable and has exactly 2^r incongruent solutions. Since all values of b or c which are quadratic residues and quadratic non-residues of m lie in the distinct G-subsets and m is the product of r distinct primes, Thus consequently we obtain 2^r, G-subsets of $Q^*(\sqrt{n})$. $\quad\square$

Corollary 2.5

Let $n \equiv 0(mod\ 2p_1 p_2...p_r)$ where $p_1, p_2, ...p_r$ are distinct odd primes, then there are exactly 2^r, G-subsets of $Q^*(\sqrt{n})$.

Proof.

Let $\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ and $n \equiv 0(mod\ 2p_1 p_2...p_r)$ where $p_1, p_2, ...p_r$ are distinct odd primes, then $a^2 - n = bc$ gives

$$a^2 \equiv bc(mod\ 2p_1 p_2...p_r) \tag{4}$$

The congruence (4) implies $a^2 \equiv bc(mod\ 2)$, $a^2 \equiv bc(mod\ p_1)$,

$$a^2 \equiv bc(mod\ p_2), ...,\ \text{and}\ a^2 \equiv bc(mod\ p_r)$$

Since 1 is the only quadratic residue of 2 and there is no quadratic non-residue of 2. Thus by Lemma 1.1 the quadratic residues and quadratic non residues of $p_1 p_2...p_r$ and $2p_1 p_2...p_r$ are same. Hence the result follows by the Theorem 2.4. $\quad\square$

Remark 2.6

The number of G-orbits of $Q^*(\sqrt{n})$ when $n \equiv 0(mod\ p_1 p_2...p_r)$ or $n \equiv 0(mod\ 2p_1 p_2...p_r)$ are same.

Illustration 2.7

Take $n = 3.5.7.11 = 1155$, Under the action of G on $Q^*(\sqrt{1155})$ there are sixteen G-orbits in the coset diagram for $Q^*(\sqrt{1155})$ namely

$$(\sqrt{1155})^G, \quad (\frac{\sqrt{1155}}{-1})^G, \quad (\frac{\sqrt{1155}}{3})^G, \quad (\frac{\sqrt{1155}}{-3})^G,$$

$$(\frac{\sqrt{1155}}{5})^G, \quad (\frac{\sqrt{1155}}{-5})^G, \quad (\frac{\sqrt{1155}}{7})^G, \quad (\frac{\sqrt{1155}}{-7})^G,$$

$$(\frac{\sqrt{1155}}{11})^G, \quad (\frac{\sqrt{1155}}{-11})^G, \quad (\frac{\sqrt{1155}}{15})^G, \quad (\frac{\sqrt{1155}}{-15})^G,$$

$$(\frac{\sqrt{1155}}{21})^G, \quad (\frac{\sqrt{1155}}{-21})^G, \quad (\frac{\sqrt{1155}}{33})^G, \quad (\frac{\sqrt{1155}}{-33})^G.$$

Similarly for $n = 2.3.5.7.11 = 2310$, Under the action of G on $Q^*(\sqrt{2310})$ there are sixteen G-orbits in the coset diagram for $Q^*(\sqrt{2310})$ namely

$$(\sqrt{2310})^G, \quad (\frac{\sqrt{2310}}{-1})^G, \quad (\frac{\sqrt{2310}}{2})^G, \quad (\frac{\sqrt{2310}}{-2})^G,$$

$$(\frac{\sqrt{2310}}{5})^G, \quad (\frac{\sqrt{2310}}{-5})^G, \quad (\frac{\sqrt{2310}}{7})^G, \quad (\frac{\sqrt{2310}}{-7})^G,$$

$$(\frac{\sqrt{2310}}{10})^G, \quad (\frac{\sqrt{2310}}{-10})^G, \quad (\frac{\sqrt{2310}}{11})^G, \quad (\frac{\sqrt{2310}}{-11})^G,$$

$$(\frac{\sqrt{2310}}{14})^G, \quad (\frac{\sqrt{2310}}{-14})^G, \quad (\frac{\sqrt{2310}}{22})^G, \quad (\frac{\sqrt{2310}}{-22})^G.$$

Theorem 2.8

Let $h = 2k + 1 \geq 3$ then there are exactly two G-orbits of $Q^*(\sqrt{2^h})$ namely $(2^k\sqrt{2})^G$ and $(\frac{2^k\sqrt{2}}{-1})^G$.

Proof.

Let $\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{2^h})$, then $a^2 - n = bc$ forces that

$$a^2 - 2^h \equiv bc \pmod{2^h} \quad \Rightarrow \quad a^2 \equiv bc \pmod{2^h}$$

But the congruence $a^2 \equiv bc \pmod{2^h}$ is solvable if and only if $bc \equiv 1 \pmod 8$, Moreover the quadratic residue of $2^h, h \geq 3$ are those integers of the form $8l + 1$ which are less than 2^h. Since all values of b or c which are quadratic residues and quadratic non-residues of 2^h lie in the distinct orbits. Thus the

8

classes $[a, b, c]$ (modulo 2^h) with b or c quadratic residues of 2^h lie in the orbit $(2^k\sqrt{2})^G$ and similarly the classes $[a, b, c]$ (modulo 2^h) with b or c quadratic non-residues of 2^h lie in the orbit $(\frac{2^k\sqrt{2}}{-1})^G$, This proves the result. □

Illustration 2.9
There are exactly two G-orbits of $Q^*(\sqrt{2^7})$ namely $(2^3\sqrt{2})^G$ and $(\frac{2^3\sqrt{2}}{-1})^G$, In the closed path lying in the orbit $(2^3\sqrt{2})^G$, the transformation

$$(yx)^{11}(y^2x)^3(yx)^5(y^2x)^3(yx)^{11}$$

fixes $2^3\sqrt{2}$. Similarly in the closed path lying in the orbit $(\frac{2^3\sqrt{2}}{-1})^G$, the transformation

$$(yx)^{11}(y^2x)^3(yx)^5(y^2x)^3(yx)^{11}$$

fixes $-2^3\sqrt{2}$.

3   Action of the subgroup $G^* = \langle yx \rangle$ and $G^{**} = \langle yx, y^2x \rangle$ on $Q^*(\sqrt{n})$.

Let us suppose that $G^* = \langle yx \rangle$ and $G^{**} = \langle yx, y^2x \rangle$ are two subgroups of G. In this section, we determine the G-subsets and G-orbits of $Q^*(\sqrt{n})$ by subgroup G^* and G^{**} acting on $Q^*(\sqrt{n})$. Let $yx(\alpha) = \alpha + 1$ and $y^2x(\alpha) = \frac{\alpha}{\alpha+1}$. Thus $yx(\frac{a+\sqrt{n}}{c}) = \frac{a_1+\sqrt{n}}{c_1}$, with $a_1 = a + c$, $b_1 = 2a + b + c$, $c_1 = c$ and $y^2x(\frac{a+\sqrt{n}}{c}) = \frac{a_2+\sqrt{n}}{c_2}$, with $a_2 = a + b$, $b_2 = b$, and $c_2 = 2a + b + c$.
In the next Lemma we see that the transformation yx fixes the classes $[0, 0, c]$ (modulo p) and the chain of these classes help us in finding G^*-subsets of $Q^*(\sqrt{n})$.

Lemma 3.1
Let p be any prime, $n \equiv 0(mod\ p)$, Then for any $k \geq 1$, $(yx)^k[0, 0, c] = [kc, k^2c, c]$ $(mod\ p)$ and in particular $(yx)^p[0, 0, c] = [0, 0, c]$ $(mod\ p)$.
Proof.
Let $\alpha = [0, 0, c]$ $(mod\ p)$ be a class contained in E_p^0. Applying the linear fractional transformation yx on α successively we see $yx[0, 0, c] = [c, c, c]$, $(yx)^2[0, 0, c] = [2c, 4c, c]$, $(yx)^3[0, 0, c] = [3c, 9c, c]$ continuing this process k-times we obtain

$(yx)^k[0,0,c] = [kc, k^2 c, c] \ (mod \ p)$

In particular for $k = p$, $kp \equiv 0 (mod \ p)$ and $k^2 p \equiv 0 (mod \ p)$. Thus we get $(yx)^p[0,0,c] = [0,0,c] \ (mod \ p)$. $\quad\square$

Lemma 3.2

Let p be an odd prime, $n \equiv 0 (mod \ p)$ and $G^* = \langle yx \rangle$, Then the sets

$A_1 = \{\alpha \in Q^*(\sqrt{n}) : (c/p) = 1\}$, $A_2 = \{\alpha \in Q^*(\sqrt{n}) : (c/p) = -1\}$,

$C_1 = \{\alpha \in Q^*(\sqrt{n}) : c \equiv 0 (mod \ p) \text{ with } (b/p) = 1\}$, $C_2 = \{\alpha \in Q^*(\sqrt{n}) : c \equiv 0 (mod \ p) \text{ with } (b/p) = -1\}$,

are G^*-subsets of $Q^*(\sqrt{n})$.

Proof.

For any $\alpha = \frac{a+\sqrt{n}}{c} \in A_1$ with $n \equiv 0 (mod \ p)$, $a^2 - n = bc$ gives

$$a^2 \equiv bc (mod \ p) \tag{5}$$

we have two cases.

(i) If $a \equiv 0 (mod \ p)$, The congruence (5) forces that $bc \equiv 0 (mod \ p)$, Then either $b \equiv 0 (mod \ p)$ or $c \equiv 0 (mod \ p)$ but not both. So in this case α belongs to the class $[0, b, 0]$ or $[0, 0, c]$ modulo p.

(ii) If $a \not\equiv 0 (mod \ p)$, $a^2 \equiv bc (mod \ p)$, Then (5) forces that either both b, c are quadratic residues of p or both quadratic non-residues of p.

As $yx : [a, b, c] \rightarrow [a+c, 2a+b+c, c]$, Then it is clear that the set A_1 is invariant under the action of the mapping yx, So the set A_1 is a G^*-subset $Q^*(\sqrt{n})$. Similarly the set A_2 is G^*-subset of $Q^*(\sqrt{n})$.

Again for any $\alpha = \frac{a+\sqrt{n}}{c} \in C_1$ by congruence (5) $c \equiv 0 (mod \ p) \Rightarrow a \equiv 0 (mod \ p)$, with $b \not\equiv 0 (mod \ p)$, so the classes belonging to the set C_1 are of the form $[0, b, 0]$ with b quadratic residue of p. Since the mapping yx fixes the classes $[0, b, 0]$. Thus clearly the set C_1 is a G^*-subsets. Similarly the set C_2 is G^*-subsets of $Q^*(\sqrt{n})$. $\quad\square$

In the next theorem we determine two G-subsets of $Q^*(\sqrt{n})$ by using A_1, A_2, C_1 and C_2 as given in Lemma 3.2.

Theorem 3.3

The sets $S_1 = A_1 \cup C_1$ and $S_2 = A_2 \cup C_2$ are two G-subsets of $Q^*(\sqrt{n})$.

Proof.

Let $\alpha = \frac{a+\sqrt{n}}{c} \in S_1$ then either $\alpha \in A_1$ or $\alpha \in C_1$ with $n \equiv 0 (mod \ p)$. Thus it is clear that the classes $[a, b, c] \ (mod \ p)$ with b or c quadratic residues of p is contained in $A_1 \cup C_1$. By Lemma 3.1 yx fixes the classes $[0, 0, c]$ (modulo p).

Also the classes belonging to A_1, A_2 are connected to the classes belonging to C_1, C_2, respectively under x. Since the modular group $PSL(2, Z)$ has the representation $G = \langle x, y : x^2 = y^3 = 1 \rangle$ and every element of G is a word in its generators x, y, to prove that S_1 is invariant under the action of G, it is enough to show that every element of S_1 is mapped onto an element of S_1 under x and y. Thus clearly we see that $S_1 = A_1 \cup C_1$ and $S_2 = A_2 \cup C_2$ are both G-subsets of $Q^*(\sqrt{n})$. $\qquad \square$

In view of the above theorem we observe that for $n = 2$ the action of G on $Q^*(\sqrt{n})$ is transitive. Since 1 is the only quadratic residue of 2 and there is no quadratic non-residue of 2, Therefore the set S_2 becomes empty and S_1 is the only G-subset of $Q^*(\sqrt{2})$. While the action of G on $Q^*(\sqrt{n})$, $n \neq 2$ is intransitive.

Illustration 3.4
Let $p = 5$ and $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$, with $n \equiv 0 (mod\ 5)$, is of the form $[a, b, c](mod\ 5)$.
In modulo 5, the squares of the integers $1, 2, 3, 4$ are

$$1^2 \equiv 4^2 \equiv 1 \ \text{ and } \ 2^2 \equiv 3^2 \equiv 4$$

Consequently, the quadratic residues of 5 are $1, 4$, and the non residues are $2, 3$. Thus A_1 consists of elements of $Q^*(\sqrt{n})$ of the form

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

Then A_1 is invariant under yx, Thus A_1 is G^*-subset of $Q^*(\sqrt{n})$.
The elements of A_2 are of the form

$$[0, 0, 2], [0, 0, 3], [2, 2, 2], [3, 2, 2], [2, 3, 3], [4, 3, 2],$$
$$[4, 2, 3], [1, 2, 3), [1, 3, 2] \text{ and } [3, 3, 3] \text{ mod } 5 \text{ only.}$$

Again A_2 is invariant under yx, Thus A_2 is also G^*-subset of $Q^*(\sqrt{n})$.
The elements of C_1 are of the form $[0, 1, 0]$ and $[0, 4, 0]$, and the elements of C_2 are of the form $[0, 2, 0]$ and $[0, 3, 0]$ Thus C_1 and C_2 are G^*-subsets.
Then clearly the sets $S_1 = A_1 \cup C_1$ and $S_2 = A_2 \cup C_2$ are two G-subsets of $Q^*(\sqrt{n})$.

11

In the next lemma we find the conditions when n is quadratic residue of p.

Lemma 3.5
For any $\alpha(a, b, c) \in Q^*(\sqrt{n})$, n is quadratic residue of p if and only if either c or $b \equiv 0 (mod\ p)$.
Proof.
Let $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$, Then $a^2 - n = bc$ forces that

$$a^2 - n \equiv bc (mod\ p) \tag{6}$$

Let either $b \equiv 0 (mod\ p)$ or $c \equiv 0 (mod\ p)$
then congruence (6) implies that $a^2 \equiv n (mod\ p)$ which shows that n is quadratic residue of p
Conversely let n be quadratic residue of p then clearly $a^2 \equiv n (mod\ p)$ that shows either $b \equiv 0 (mod\ p)$ or $c \equiv 0 (mod\ p)$. $\quad\square$
Further we see the action of $G^{**} = \langle yx, y^2x \rangle$ on $Q^*(\sqrt{n})$ with n quadratic residue of p and determine four proper G^{**}-subsets of $Q^*(\sqrt{n})$.

Theorem 3.6
Let p be an odd prime and n is quadratic residue of p, let $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$
and $G^{**} = \langle yx, y^2x \rangle$, then the sets
$G_1 = \{\alpha \in Q^*(\sqrt{n}) : (c/p) = 1\}$, $G_2 = \{\alpha \in Q^*(\sqrt{n}) : (c/p) = -1\}$,
are two G^{**}-subsets of $Q^*(\sqrt{n})$. $\quad\square$
Proof.
Let $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$, with $a^2 - n \equiv bc (mod\ p)$, and a, b, c modulo p are belonging to the set $\{0, 1, 2, ..., p-1\}$.
Let p is an odd prime with n quadratic residue of p, then either $b \equiv 0 (mod\ p)$ or $c \equiv 0 (mod\ p)$.
Since $yx : [a, b, c] \rightarrow [a+c, 2a+b+c, c]$ and $y^2x : [a, b, c] \rightarrow [a+b, b, 2a+b+c]$,
Since every element of G^{**} is a word in its generators yx, y^2x, Then clearly the sets G_1, G_2, are two G^{**}-subsets of $Q^*(\sqrt{n})$. $\quad\square$

Corollary 3.7 $\langle G^{**}, x \rangle = G$
Proof.
We know that $G = \langle x, y : x^2 = y^3 = 1 \rangle$ and $G^{**} = \langle yx, y^2x \rangle$, the result follows from the fact that the generators x, y of G can be written as word by the elements of $\langle G^{**}, x \rangle$. $\quad\square$
Finally we find G-orbits of $Q^*(\sqrt{37})$ with help of G^{**}-subsets as given in

Theorem 3.6. It is important to note that 37 is the smallest prime which have four G-orbits and all odd primes less than 37 has exactly two G-orbits.

Illustration 3.9

In the coset diagram for $Q^*(\sqrt{37})$, There are exactly four G-orbits of $Q^*(\sqrt{37})$ given by
$(\sqrt{37})^G$, $(\frac{1+\sqrt{37}}{2})^G$, $(\frac{1+\sqrt{37}}{-3})^G$, $(\frac{-1+\sqrt{37}}{-3})^G$.
The G_1 contains three orbits $(\sqrt{37})^G$, $(\frac{1+\sqrt{37}}{-3})^G$, $(\frac{-1+\sqrt{37}}{-3})^G$, While the set G_2 contains only one orbit $(\frac{1+\sqrt{37}}{2})^G$.
In the closed path lying in the orbit $(\sqrt{37})^G$, the transformation

$$g_1 = (yx)^6(y^2x)^{12}(yx)^6$$

fixes $k = \sqrt{37}$, that is $g_1(k) = ((yx)^6(y^2x)^{12}(yx)^6)(k) = k$, and so gives the quadratic equation $k^2 + 37 = 0$, the zeros, $\pm\sqrt{37}$, of this equation are fixed points of the transformations g_1.
In the closed path lying in the orbit $(\frac{1+\sqrt{37}}{2})^G$, the transformations

$$g_2 = (yx)^3(y^2x)(yx)(y^2x)^5(yx)(y^2x)(yx)^2$$

fixes $l = \frac{1+\sqrt{37}}{2}$ and so gives the quadratic equation $l^2 - l - 9 = 0$, the zeros, $\frac{1\pm\sqrt{37}}{2}$, of this equation are fixed points of g_2.
Similarly in the closed path lying in the orbit $(\frac{1+\sqrt{37}}{-3})^G$ the transformation

$$g_3 = (yx)^2(y^2x)^2(yx)(y^2x)^3(yx)^2(y^2x)(yx)$$

fixes $(\frac{1+\sqrt{37}}{-3})$ and corresponding to the closed lying in the orbit $(\frac{-1+\sqrt{37}}{-3})^G$, the transformation

$$g_4 = (yx)(y^2x)(yx)^2(y^2x)^3(yx)(y^2x)^2(yx)^2$$

fixes $(\frac{-1+\sqrt{37}}{-3})$.
By [7], [15] we see that $\tau^*(37) = 124$, That is there are 124 ambiguous numbers in the coset diagram for $Q^*(\sqrt{37})$ while the ambiguous length of the orbits are 48, 28, 24 and 24 respectively. □

13

References

[1] Andrew Adler and John E. Coury: *The Theory of Numbers.* Jones and Barlett Publishers, Bostan London (1995).

[2] G. Higman and Q. Mushtaq: Coset Diagrams and Relations for PSL(2,Z). Gulf J.Sci. Res. (1983) 159-164.

[3] I. Kouser, S.M. Husnine, A. Majeed: A classification of the elements of $Q^*(\sqrt{p})$ and a partition of $Q^*(\sqrt{p})$ Under the Modular Group Action. PUJM,Vol.31 (1998) 103-118.

[4] I. N. Herstein: *Topics in Algebra.* John Wiley and Sons, Second Edition (1975).

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson: An Atlas of Finite Groups. Oxford Univ. Press, Oxford, (1985).

[6] M. Aslam Malik, M. Asim Zafar: Real Quadratic Irrational Numbers and Modular Group Action. (Submitted), (2008).

[7] M. Aslam Malik, S. M. Husnine and A. Majeed: Modular Group Action on Certain Quadratic Fields. PUJM, Vol.28 (1995) 47-68.

[8] M. Aslam Malik, S. M. Husnine and A. Majeed: Intrasitive Action of the Modular Group $PSL(2, Z)$ on a subset $Q^*(\sqrt{k^2m})$ of $Q(\sqrt{m})$. PUJM,Vol.37, (2005) 31-38.

[9] M. Aslam Malik, S. M. Husnine, and A. Majeed: Properties of Real Quadratic Irrational Numbers under the action of group $H = \langle x, y : x^2 = y^4 = 1 \rangle$. Studia Scientiarum Mathematicarum Hungarica Vol.42(4) (2005) 371-386.

[10] M. H. Millington: Subgroups of the classical modular group. J. London Math. Soc. 1:351-357 (1970) 133-146.

[11] Muhammad Ashiq and Q. Mushtaq: Actions of a subgroup of the Modular Group on an imaginary Quadratic Field. QuasiGroups and Related Systems Vol. 14, (2006) 133-146.

[12] Q. Mushtaq: Modular Group acting on Real Quadratic Fields. Bull. Austral. Math. Soc. Vol. 37, (1988) 303-309, 89e: 11065.

[13] Q. Mushtaq: On word structure of the Modular Group over finite and real quadratic fields. Discrete Mathematics179 (1998). 145-154.

[14] S. Anis, Q. Mushtaq: The Number of Subgroups of PSL(2,Z) when acting on $F_p \cup \{\infty\}$. Communication in Algebra, VOl 36 4276-4283 (2008).

[15] S. M. Husnine, M. Aslam Malik, and A. Majeed: On Ambiguous Numbers of an invariant subset $Q^*(\sqrt{k^2 m})$ of $Q(\sqrt{m})$ under the action of the Modular Group PSL(2,Z). Studia Scientiarum Mathematicarum Hungarica Vol.42(4) (2005) 401-412.