Quasigroups and Related Systems **19** (2011), 183 – 192

Parametrization of actions of $\langle \mathbf{u}, \mathbf{v} : \mathbf{u}^6 = \mathbf{v}^6 = \mathbf{1} \rangle$

Muhammad Aslam and Qaiser Mushtaq

Abstract. Graham Higman proposed the problem of parametrization of actions of the extended modular group $PGL(2,Z)$ on the projective line over F_q. The problem was solved by Q. Mushtaq. In this paper, we take up the problem and parametrize the actions of $\langle u, v, t : u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle$ on the projective line over finite Galois fields.

1. Introduction

Graham Higman proposed the problem of parametrization of actions of the extended modular group $PGL(2,Z)$ on the projective line over F_q. The problem was solved by Q. Mushtaq. In this paper, we take up the problem and parametrize the actions of $\langle u, v, t : u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle$ on the projective line over finite Galois fields.

It is worthwhile to consider linear fractional transformations x, y satisfying the relations $x^2 = y^m = 1$, with a view to study actions of the group $\langle x, y \rangle$ on real quadratic fields. If $y : z \rightarrow \frac{az+b}{cz+d}$ is to act on all real quadratic fields, then a, b, c, d must be rational numbers and can be taken to be integers, so that $\frac{(a+d)^2}{ad-bc}$ is rational. But if $y : z \rightarrow \frac{az+b}{cz+d}$ is of order m one must have $\frac{(a+d)^2}{ad-bc} = \omega^2 + \omega^{-2} + 2$, where ω is a primitive mth root of unity. Now $\omega + \omega^{-1}$ is rational, for a primitive mth root ω, only if $m = 1, 2, 3, 4$, or 6. So these are the only possible orders of y. The group $\langle x, y \rangle$ is cyclic of order two when $m = 1$. When $m = 2$, it is an infinite dihedral group and does not give inspiring information while studying its action on the quadratic numbers. For $m = 3$, the group $\langle x, y \rangle$ is the modular group $PSL(2,Z)$ and its action on real quadratic numbers has been discussed in detail in [2] and [3].

It is well known [1, 5] that the group $G_{2,6}(2,Z)$, where Z is the ring of

2010 Mathematics Subject Classification: 20G40, 20B35
Keywords: Linear-fractional transformation, non-degenerate homomorphism, conjugacy classe, parametrization and projective line.

integers, is generated by the linear-fractional transformations $x : z \longrightarrow \frac{-1}{3z}$ and $y : z \longrightarrow \frac{-1}{3(z+1)}$ which satisfy the relations

$$x^2 = y^6 = 1. \tag{1}$$

Let $v = xyx$, and $u = y$. Then $(z)v = \frac{3z-1}{3z}$ and

$$u^6 = v^6 = 1 \tag{2}$$

So the group $G_{6,6}(2, Z) = \langle u, v\rangle$ is a proper subgroup of the group $G_{2,6}(2, Z)$.

The linear-fractional transformation $t : z \to \frac{1}{3z}$ inverts u and v, that is, $t^2 = (ut)^2 = (vt)^2 = 1$ and so extends the group $G_{6,6}(2, Z)$ to

$$G^*_{6,6}(2, Z) = \langle u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1\rangle. \tag{3}$$

As u and v have the same orders, there exists an automorphism which interchanges u and v yielding the split extension $G^*_{6,6}(2, Z)$.

Let $PL(F_q)$ denote the projective line over the Galois field F_q , where q is a prime, that is, $PL(F_q) = F_q \cup \{\infty\}$. The group $G^*_{6,6}(2, q)$ is then the group of linear-fractional transformations of the form $z \to \frac{az+b}{cz+d}$, where $a, b, c, d \in F_q$ and $ad - bc \neq 0$, while $G_{6,6}(2, q)$ is its subgroup consisting of all those linear-fractional transformations of the form $z \to \frac{az+b}{cz+d}$, where $a, b, c, d \in F_q$ and $ad - bc$ is a non-zero square in F_q.

Graham Higman proposed the problem of parametrization of actions of $PGL(2, Z)$ on $PL(F_q)$. The problem was solved by Q. Mushtaq in [4]. In this paper, we take up the problem and parametrize the actions of $G^*_{6,6}(2, Z)$ on $PL(F_q)$, except for a few uninteresting ones, by the elements of F_q. We have shown that any non-degenerate homomorphism α from $G_{6,6}(2, Z)$ into $G_{6,6}(2, q)$ can be extended to a non-degenerate homomorphism α from $G^*_{6,6}(2, Z)$ into $G^*_{6,6}(2, q)$. It has been shown also that every element in $G^*_{6,6}(2, q)$, not of order $1, 2$, or 6, is the image of uv under α. It is also proved that the conjugacy classes of $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ are in one-to-one correspondence with the conjugacy classes of non-trivial elements of $G^*_{6,6}(2, q)$, under a correspondence which assigns to the homomorphism α the class containing $(uv)\alpha$. Of course, this will mean that we can actually parametrize the actions of $G^*_{6,6}(2, q)$ on $PL(F_q)$, except for a few uninteresting ones, by the elements of F_q.

2. Conjugacy classes

The transformations $u : z \to \frac{-1}{3(z+1)}$, $v : z \to \frac{3z-1}{3z}$ and $t : z \to \frac{1}{3z}$ generate $G^*_{6,6}(2, Z)$, subject to defining relations $u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1$. Thus to choose a homomorphism $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ amounts to choosing $\overline{u} = u\alpha, \overline{v} = v\alpha$ and $\overline{t} = t\alpha$, in $G^*_{6,6}(2, q)$ such that

$$\overline{u}^6 = \overline{v}^6 = \overline{t}^2 = (\overline{u}\overline{t})^2 = (\overline{v}\overline{t})^2 = 1. \tag{4}$$

We call α to be a *non-degenerate homomorphism* if neither of the generators u, v of $G^*_{6,6}(2, Z)$ lies in the kernel of α. Two homomorphisms α and β from $G^*_{6,6}(2, Z)$ to $G^*_{6,6}(2, q)$ are called *conjugate* if there exists an inner automorphism ρ of $G^*_{6,6}(2, q)$ such that $\beta = \rho\alpha$. Let δ be the automorphism on $G^*_{6,6}(2, Z)$ defined by $u\delta = tut, v\delta = v$, and $t\delta = t$. Then the homomorphism $\alpha' = \delta\alpha$ is called the *dual homomorphism* of α. This, of course, means that if α maps u, v, t to $\overline{u}$,$\overline{v}$, $\overline{t}$, then α' maps u, v, t to $\overline{t}\overline{u}\overline{t}$, $\overline{v}$, $\overline{t}$ respectively. Since the elements $\overline{u}$,$\overline{v}$,$\overline{t}$ as well as $\overline{t}\overline{u}\overline{t}$, $\overline{v}$, $\overline{t}$ satisfy the relations (4), therefore the solutions of these relations occur in dual pairs. Of course, if α is conjugate to β then α' is conjugate to β'.

2.1. Parametrization

If the natural mapping $GL(2, q) \to G^*_{6,6}(2, q)$ maps a matrix M to the element of g of $G^*_{6,6}(2, q)$, then $\theta = (tr(M))^2 / \det(M)$ is an invariant of the conjugacy class of g. We refer to it as the parameter of g or of the conjugacy class. Of course, every element in F_q is the parameter of some conjugacy class in $G^*_{6,6}(2, q)$. For instance, the class represented by a matrix with characteristic polynomial $z^2 - \theta z + \theta$ if $\theta \neq 0$ or $z^2 - 1$ if $\theta = 0$.

If q is odd, there are two classes with parameter 0. Of course a matrix M in $GL(2, q)$ represents an involution in $G^*_{6,6}(2, q)$ if and only if its trace is zero. This means that the two classes with parameter 0 contain involutions. One of the classes is contained in $G_{6,6}(2, q)$ and the other not. In any case, there are two classes with parameter 4; the class containing the identity element and the class containing the element $z \to z + 1$. Thus apart from these two exceptions, the correspondence between classes and parameters is one-to-one.

If q is odd and g is not an involution, then g belongs to $G_{6,6}(2, q)$ if and only if θ is a square in F_q. On the other hand $g : z \to \frac{az+b}{cz+d}$, where $a, b, c, d \in F_q$, has a fixed point k in the natural representation of $G^*_{6,6}(2, q)$

on $PL(F_q)$ if and only if the discriminant, $a^2+d^2-2ad+4bc$, of the quadratic equation $k^2c+k(d-a)-b=0$ is a square in F_q. Since the determinant $ad-bc$ is 1 and the trace $a+d$ is r, the discriminant is $(\theta-4)$. Thus, g has fixed point in the natural representation of $G^*_{6,6}(2,q)$ on $PL(F_q)$ if and only if $(\theta-4)$ is a square in F_q.

If U and V are two non-singular 2×2 matrices corresponding to the generators $\overline{u}$ and $\overline{v}$ of $G^*_{6,6}(2,q)$ with $\det(UV)=1$ and trace r, then for a positive integer k

$$\begin{aligned}(UV)^k &= \{\binom{k-1}{0}r^{k-1}-\binom{k-2}{1}r^{k-3}+\ldots\}UV \\ &\quad -\{\binom{k-2}{0}r^{k-2}-\binom{k-3}{1}r^{k-4}+\ldots\}I. \end{aligned} \tag{5}$$

Furthermore, suppose

$$f(r)=\binom{k-1}{0}r^{k-1}-\binom{k-2}{1}r^{k-3}+\ldots \tag{6}$$

The replacement of θ for r^2 in $f(r)$ yields a polynomial $f(\theta)=f_k(\theta)$ in θ. Thus, one can find a minimal polynomial $g_k(\theta)$, which is equal to $f_k(\theta)$ if k is a prime number, otherwise for any positive integer k such that $q\equiv \pm 1(\operatorname{mod} \mathrm{k})$ by the equation:

$$g_k(\theta)=\frac{f_k(\theta)}{g_{d_1}(\theta)g_{d_2}(\theta)\ldots g_{d_n}(\theta)} \tag{7}$$

where $d_1,d_2,\ldots,d_n$, are the divisors of k such that $1<d_i<k$, $i=1,2,\ldots,n$ and $f_k(\theta)$ is obtained by the equation (3.2).

The degree of the minimal polynomial is obtained as:

$$\deg[g_k(\theta)]=\deg[f_k(\theta)]-\sum\deg[g_{d_i}(\theta)], \tag{8}$$

where $\deg[f_k(\theta)]=\left\{\begin{array}{ll}\frac{k-1}{2} & \text{if } k \text{ is odd,}\\ \frac{k}{2} & \text{if } k \text{ is even}\end{array}\right\}$. Also, $\deg[g_{p^n}(\theta)]=\frac{p^n}{2}-\frac{p^{n-1}}{2}$, where p is a prime.

Thus:

k	**Minimal equation satisfied by θ**
1	$\theta-4=0$
2	$\theta=0$

3	$\theta - 1 = 0$
4	$\theta - 2 = 0$
5	$\theta^2 - 3\theta + 1 = 0$
6	$\theta - 3 = 0$
7	$\theta^3 - 5\theta^2 + 6\theta - 1 = 0$
8	$\theta^2 - 4\theta + 2 = 0$
9	$\theta^3 - 6\theta^2 + 9\theta - 1 = 0$
10	$\theta^2 - 5\theta + 5 = 0$
11	$\theta^5 - 9\theta^4 + 28\theta^3 - 35\theta^2 + 15\theta - 1 = 0$
12	$\theta^2 - 4\theta + 1 = 0$
13	$\theta^6 - 11\theta^5 + 45\theta^4 - 84\theta^3 + 70\theta^2 - 21\theta + 1 = 0$
14	$\theta^6 - 120\theta^5 + 55\theta^4 - 120\theta^3 + 126\theta^2 - 56\theta + 7 = 0$
15	$\theta^7 - 13\theta^6 + 66\theta^5 - 165\theta^4 + 210\theta^3 - 126\theta^2 + 28\theta - 1 = 0$
16	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 106\theta^2 - 40\theta + 4 = 0$
17	$\theta^8 - 15\theta^7 + 91\theta^6 - 286\theta^5 + 495\theta^4 - 462\theta^3 + 210\theta^2 - 36\theta + 1 = 0$
18	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 105\theta^2 - 36\theta + 3 = 0$
19	$\theta^9 - 17\theta^8 + 120\theta^7 - 455\theta^6 + 1001\theta^5 - 1287\theta^4 + 924\theta^3 - 330\theta^2 + 45\theta - 1 = 0$
20	$\theta^8 - 16\theta^7 + 104\theta^6 - 352\theta^5 + 661\theta^4 - 680\theta^3 + 356\theta^2 - 80\theta + 5 = 0,$

and so on.

Let $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $GL(2, q)$ corresponding to $\overline{u}$. Then, since $\overline{u}^6 = 1$, U^6 is a scalar matrix, and hence $\det(U)$ is a square in F_q, where $q = \pm 1 (\mathrm{mod}\, 12)$. Thus, replacing U by a suitable scalar multiple, we assume that $\det(U) = 1$.

Since, for any matrix M, such that M^2 and M^3 are not scalar matrices, $M^6 = \lambda I$ if and only if $(tr(M))^2 = 3 \det(M)$, we may assume that $tr(U) = a + d = \sqrt{3}$ and $\det(U) = 1$. Thus $U = \begin{bmatrix} a & b \\ c & -a + \sqrt{3} \end{bmatrix}$. Similarly, $V = \begin{bmatrix} e & f \\ g & -e + \sqrt{3} \end{bmatrix}$. Since $\overline{u}^6 = 1$ also implies that the $tr(\overline{u}) = \sqrt{3}$, every element of $GL(2, q)$ of trace equal to $\sqrt{3}$ has upto scalar multiplication, a conjugate of the form $\begin{bmatrix} 0 & -1 \\ 1 & \sqrt{3} \end{bmatrix}$. Therefore U will be of the form $\begin{bmatrix} 0 & -1 \\ 1 & \sqrt{3} \end{bmatrix}$.

Now let $\bar{t}$ be represented by $T = \begin{bmatrix} l & m \\ n & j \end{bmatrix}$. Since $\bar{t}^2 = 1$, the trace of T is zero. So, upto scalar multiplication, the matrix representing $\bar{t}$ will be of the form $\begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$. Because $(\overline{u}\overline{t})^2 = (\overline{v}\overline{t})^2 = 1$, the $tr(\overline{u}\overline{t}) = tr(\overline{v}\overline{t}) = 0$ and so $b = kc$ and $f = gk$.

Thus the matrices corresponding to generators $\overline{u}$, $\overline{v}$ and $\overline{t}$ of $G^*_{6,6}(2,q)$ will be:
$U = \begin{bmatrix} a & kc \\ c & -a+\sqrt{3} \end{bmatrix}$, $V = \begin{bmatrix} e & gk \\ g & -e+\sqrt{3} \end{bmatrix}$, and $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ respectively, where $a, c, e, g, k \in F_q$. Then,

$$1 + a^2 + kc^2 - \sqrt{3}a = 0 \tag{9}$$

and

$$1 + e^2 + kg^2 - \sqrt{3}e = 0, \tag{10}$$

because the determinants of U and V are 1.

This certainly evolves elements satisfying the relations $U^6 = \lambda_1 I, V^6 = \lambda_2 I$, where λ_1 and λ_2 are non-zero scalars and I is the identity matrix. The non-degenerate homomorphism α is determined by $\overline{u}, \overline{v}$ because one-to-one correspondence assigns to α the class containing $\overline{u}\ \overline{v}$. So it is sufficient to check on the conjugacy class of $\overline{u}\ \overline{v}$. The matrix UV has the trace

$$r = 2(ae + kcg) + 3 - \sqrt{3}(a + e). \tag{11}$$

If $tr(UVT) = ks$, then

$$s = 2ag - c(2e - \sqrt{3}) - \sqrt{3}g. \tag{12}$$

So the relationship between (3.7) and (3.8) is

$$r^2 + ks^2 = 3r - 2. \tag{13}$$

We set

$$\theta = r^2. \tag{14}$$

Lemma 1. *Either* $\overline{uv}$ *is of order* 3 *or there exists an involution* $\overline{t}$ *in* $G^*_{6,6}(2,q)$ *such that* $\overline{t}^2 = (\overline{u}\overline{t})^2 = (\overline{v}\overline{t})^2 = 1$.

Proof. Let U be an element of $GL(2,q)$ which yields the element $\overline{u}$ of $G^*_{6,6}(2,q)$. Since $(\overline{u})^6 = 1$, therefore we can assume that U has the form $\begin{bmatrix} 0 & -1 \\ 1 & -\sqrt{3} \end{bmatrix}$.

Let $V = \begin{bmatrix} a & b \\ c & -a-\sqrt{3} \end{bmatrix}$ and $T = \begin{bmatrix} l & m \\ n & -l \end{bmatrix}$ where $1+a^2+bc-\sqrt{3}a = 0$.

Now suppose that there exists a transformation $\bar{t}$ in $G^*_{6,6}(2, Z)$ such that $\bar{t}^2 = (\overline{u}\bar{t})^2 = (\overline{v}\bar{t})^2 = 1$. Let r be the trace of UV. Then $r = 3 + b - c - \sqrt{3}a$. Now

$$UT = \begin{bmatrix} 0 & -1 \\ 1 & -\sqrt{3} \end{bmatrix} \begin{bmatrix} l & m \\ n & -l \end{bmatrix} = \begin{bmatrix} -n & l \\ l-\sqrt{3}n & m-\sqrt{3}l \end{bmatrix}$$

give us $-n + m - \sqrt{3}l = 0$ or $m = n + \sqrt{3}l$.

Also

$$VT = \begin{bmatrix} a & b \\ c & -a+\sqrt{3} \end{bmatrix} \begin{bmatrix} l & m \\ n & -l \end{bmatrix} = \begin{bmatrix} al+bn & am-bl \\ cl-an+\sqrt{3}n & cm+al-\sqrt{3}l \end{bmatrix}$$

yields $2al + bn + cm - \sqrt{3}l = 0$ or $2al + bn + c(n + \sqrt{3}l) - \sqrt{3}l = 0$ or $2al + bn + cn + \sqrt{3}cl - \sqrt{3}l = 0$. Hence

$$(2a + \sqrt{3}c - \sqrt{3})l + (b + c)n = 0. \tag{15}$$

Now for T to be a non-singular matrix, we have $det(T) \neq 0$, that is, $-l^2 - mn \neq 0$ or $l^2 + mn \neq 0$ or $l^2 + n(n + \sqrt{3}l) \neq 0$ or $l^2 + n^2 + \sqrt{3}nl \neq 0$ or

$$\left(\frac{l}{n}\right)^2 + 1 + \sqrt{3}\left(\frac{l}{n}\right) \neq 0. \tag{16}$$

Thus the necessary and sufficient conditions for the existence of $\bar{t}$ in $G^*_{6,6}(2, q)$ are the equations (15) and (16). Hence $\bar{t}$ exists in $G^*_{6,6}(2, q)$ unless

$$\left(\frac{l}{n}\right)^2 + 1 + \sqrt{3}\left(\frac{l}{n}\right) = 0.$$

Of course, if both $2a + \sqrt{3}c - \sqrt{3}$ and $b + c$ are equal to zero, then the existence of $\bar{t}$ is trivial. If not, then $\frac{l}{n} = \frac{-(b+c)}{2a+\sqrt{3}c-\sqrt{3}}$, and so equation (16) is equivalent to $(b + c)^2 + (2a + \sqrt{3}c - \sqrt{3})^2 + (2a + \sqrt{3}c - \sqrt{3})(b + c) \neq 0$. Thus there exists $\bar{t}$ in $G^*_{6,6}(2, q)$ such that $\bar{t}^2 = (\overline{u}\bar{t})^2 = (\overline{v}\bar{t})^2 = 1$ unless

$$(b + c)^2 + (2a + \sqrt{3}c - \sqrt{3})^2 = \sqrt{3}(2a + \sqrt{3}c - \sqrt{3})(b + c).$$

This yields $(b - c)^2 + 4bc + 4a^2 + 3c^2 + 3 + 4\sqrt{3}ac - 4\sqrt{3}a - 6c = \sqrt{3}(2ab + \sqrt{3}bc - \sqrt{3}b + 2ac + \sqrt{3}c^2 - \sqrt{3}c)$.

After simplification we get $r^2 - 3r + 2 = 0$. So, $r^2 = 3r - 2$ and after squaring both sides, we get $\theta^2 - 5\theta + 4 = 0$. This implies that $\theta = 1$ or $\theta = 4$.

By the preceding table, $\theta = 1$ implies that the order of $\overline{uv}$ is 3 and $\theta = 4$ gives the order of $\overline{uv}$ is 1, so neglecting it because $(\overline{u}\,\overline{v}) \neq 1$, the parameter of $\overline{uv}$ is 1 and the order of $\overline{uv}$ is 3. □

Lemma 2. *One and only one of the following holds:*
(*i*) *The pair* $(\overline{u}, \overline{v})$ *is invertible.*
(*ii*) $\overline{u}\,\overline{v}$ *has order* 3 *and* $\overline{u}\,\overline{v} \neq \overline{v}\,\overline{u}$. □

In what follows we shall find a relationship between the parameters of the dual homomorphisms. We first prove the following.

Lemma 3. *Any non trivial element* $\overline{g}$ *of* $G^*_{6,6}(2, q)$ *whose order is not equal to* 2 *or* 6 *is the image of* uv *under some non-degenerate homomorphism* α *of* $G^*_{6,6}(2, , Z)$ *into* $G^*_{6,6}(2, q)$.

Proof. Using Lemma 1, we show that every non-trivial element of $G^*_{6,6}(2, q)$ is a product of two elements of orders 3. So we find elements $\overline{u}, \overline{v}$ and, $\overline{t}$ of $G^*_{6,6}(2, q)$ satisfying the relations (4) with $\overline{u}\,\overline{v}$ in a given conjugacy class.

The class to which we want $\overline{u}\ \overline{v}$ to belong do not consist of involutions because $\overline{g} = \overline{u}\,\overline{v}$ is not of order 2. Thus the traces of the matrices UV and UVT are not equal to zero. Hence $r \neq 0$, and $s \neq 0$, so that we have $\theta = r^2 \neq 0$; and it is sufficient to show that we can choose a, c, e, g, k, in F_q so that r^2 is indeed equal to θ. The solution of θ is therefore arbitrarily in F_q. We can choose r to satisfy $\theta = r^2$, equation (13), yields $ks^2 = 3r - 2 - r^2$. If $r^2 \neq 3r - 2$, we select k as above.

Any quadratic polynomial $\lambda z^2 + \mu z + \nu$, with coefficients in F_q takes at least $(q + 1)/2$ distinct values, as z runs through F_q; since the equation $\lambda z^2 + \mu z + \nu = k$ has at most two roots for fixed k; and there are q elements in F_q, where q is odd. In particular, $a^2 - \sqrt{3}a$ and $-kc^2 - 1$ each taking at least $(q+1)/2$ distinct values as a and c run through F_q. Similarly, $e^2 - \sqrt{3}e$ and $-kg^2 - 1$ each takes at least $(q + 1)/2$ distinct values as e and g run through F_q. Hence we can find a and c so that $a^2 - \sqrt{3}a = -kc^2 - 1$ and e, g so that $e^2 - \sqrt{3}e = -kg^2 - 1$.

Finally, by substituting the values of r, s, a, c, e, g, k in equations (11) and (12) we obtain the values of e and g. These equations are linear equations for e and g with determinant $(2a - \sqrt{3})^2 + 4kc^2 = 4a^2 + 3 - 4\sqrt{3}4kc^2 = 4(a^2 + kc^2 - \sqrt{3}a) + 3 = -4 + 3 = -1$. It is non-zero, so that we can find e and g satisfying equation (10). It is obvious from (13) and (14) that $\theta = 0$ when $r = 0$ and $\theta = 1$ or 4 when $s = 0$. By the preceding table, the possibility that $\theta = 0$ gives rise to the situation where $\overline{u}.\overline{v}$ is of order 2. Similarly, the possibility $\theta = 1$ leads to the situation where $\overline{u}\,\overline{v}$ is of order 3 and $\theta = 4$ yields $\overline{u}\,\overline{v}$ of order 1. □

Theorem 1. *The conjugacy classes of non-degenerate homomorphisms of $G^*_{6,6}(2, Z)$ into $G^*_{6,6}(2, q)$ are in one-to-one correspondence with the non-trivial conjugacy classes of elements of $G^*_{6,6}(2, q)$ under a correspondence which assigns to any non-degenerate homomorphism σ the class containing $(uv)\sigma$.*

Proof. Let $\sigma : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ be a non-degenerate homomorphism such that it maps u, v to $\overline{u}$,$\overline{v}$. Let θ be the parameter of the class represented by $\overline{u}\,\overline{v}$. Now α is determined by $\overline{u}$,$\overline{v}$ and each θ evolves a pair $\overline{u}$,$\overline{v}$, so that σ is associated with θ. We shall call the parameter θ of the class containing $\overline{u}\,\overline{v}$, the parameter of the non-degenerate homomorphism of $G^*_{6,6}(2, Z)$ into $G^*_{6,6}(2, q)$. Now $UT = \begin{bmatrix} ck & -ak \\ -a + \sqrt{3} & -ck \end{bmatrix}$ implies that $\det(UT) = -k(a^2 - \sqrt{3}a + kc^2) = k$ (equation 9). Also, $(UT)V = \begin{bmatrix} kec - akg & k^2gc + ak(e - \sqrt{3}) \\ -ae + e\sqrt{3} - kgc & -akg + kg\sqrt{3} + ck(e - \sqrt{3}) \end{bmatrix}$ implies that $Tr((UT)V) = 2kec - 2akg + \sqrt{3}kg - \sqrt{3}kc = -k(-2ce + 2ag - \sqrt{3}g + \sqrt{3}c) = -ks$. If $\overline{u}, \overline{v}, \overline{t}$ satisfy the relations (4), then so do $\overline{t}\overline{u}\overline{t}, \overline{v}, \overline{t}$. So that the solution of relations (4) occur in dual pairs. Hence replacing the solutions in Lemma 3 by $\overline{t}\overline{u}\overline{t}, \overline{v}, \overline{t}$, we have $\theta = \frac{[Tr((UT)V]^2}{\det(UT)} = \frac{k^2s^2}{k} = ks^2$. We then find a relationship between the parameters of the dual non-degenerate homomorphisms. □

There is an interesting relationship between the parameters of the dual non-degenerate homomorphisms.

Corollary 1. *If $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ is a non-degenerate homomorphism, α' is its dual and θ, φ are their respective parameters then $\theta + \varphi = 3r - 2$.*

Proof. Let $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ be a non-degenerate homomorphism satisfying the relations $u\alpha = \overline{u}$, $v\alpha = \overline{v}$ and $t\alpha = \overline{t}$. Let α' be the dual of α. As we choose the matrices $U = \begin{bmatrix} a & ck \\ c & -a + \sqrt{3} \end{bmatrix}$, $V = \begin{bmatrix} e & g\,k \\ g & -e + \sqrt{3} \end{bmatrix}$

and $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$, representing $\overline{u}, \overline{v}$ and $\overline{t}$, respectively such that they satisfy the equations from (9) to (13). Now $(\overline{u}\,\overline{v})^2 = 1$, implies that $Tr(UV) = 0$. Also, we have $\{Tr(UVT)\}/k = s = 0$ if and only if $(\overline{u}\,\overline{v}\overline{t})^2 = 1$. Then $\det(UV) = 1$, thus giving the parameter of $\overline{u}\,\overline{v}$ equal to $r^2 = \theta$. Also since $Tr(UVT) = ks$ and $\det(UVT) = k$ (since $\det(U) = 1$, $\det(V) = 1$ and $\det(T) = k$), we obtain the parameter of $\overline{uvt}$ equal to ks^2, which we denote by φ. Thus $\theta + \varphi = r^2 + ks^2$. Substituting the values from equation (13), we therefore obtain $\theta + \varphi = 3r - 2$. Hence if θ is the parameter of the non-degenerate homomorphism α, then $\varphi = 3r - 2 - \theta$ is the parameter of the dual α' of α. □

Theorem 1, of course, means that we can actually parametrize the non-degenerate homomorphisms of $G^*_{6,6}(2, Z)$ to $G^*_{6,6}(2, q)$ except for a few uninteresting ones, by the elements of F_q. Since $G^*_{6,6}(2, q)$ has a natural permutation representation on $PL(F_q)$, any homomorphism $\sigma : G^*_{6,6}(2, Z) \rightarrow G^*_{6,6}(2, q)$ gives rise to an action of $G^*_{6,6}(2, Z)$ on $PL(F_q)$.

References

[1] **M. Aslam and Q. Mushtaq**, *Closed paths in the coset diagrams for $\langle y, t : y^6 = t^6 = 1\rangle$ acting on real quadratic fields*, Ars Comb. **71** (2004), 267 – 288.

[2] **Q. Mushtaq**, *Coset diagrams for the modular group*, Ph.D. thesis, University of Oxford, 1983.

[3] **Q. Mushtaq**, *Modular group acting on real quadratic fields*, Bull. Austral. Math. Soc. **37** (1988), 303 – 306.

[4] **Q. Mushtaq**, *Parametrization of all homomorphisms from $PGL(2, Z)$ into $PGL(2, q)$*, Comm. Algebra **20** (1992), 1023 – 1040.

[5] **Q. Mushtaq and M. Aslam**, *Group generated by two elements of orders two and six acting on R and $Q(\sqrt{n})$*, Disc. Math. **179** (1998), 145 – 154.

Received January 03, 2011

Department of Mathematics Quaid-i-Azam University, Islamabad, Pakistan
E-emails: draslamqau@yahoo.com (M.Aslam), qmushtaq@apollo.net.pk (Q.Mushtaq)