Quasigroups and Related Systems **20** (2012), 21 − 28

Parametrization of actions of a subgroup of the modular group

Muhammad Ashiq, Qaiser Mushtaq and Tariq Maqsood

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 $\langle u,v,t : u^3 = v^3 = t^2 = (ut)^2 = (vt)^2 = 1\rangle$ on the projective line over finite Galois fields.

1. Introduction

It is well known [3, 4, 6] that the modular group $PSL(2,Z)$, where Z is the ring of integers, is generated by the linear-fractional transformations $x : z \longrightarrow \frac{-1}{z}$ and $y : z \longrightarrow \frac{z-1}{z}$ and has the presentation $\langle x, y : x^2 = y^3 = 1\rangle$.

Let $v = xyx$, and $u = y$. Then $(z)v = \frac{-1}{z+1}$ and thus $u^3 = v^3 = 1$. So, the group $G(2,Z) = \langle u,v\rangle$ is a proper subgroup of the modular group $PSL(2,Z)$ and the linear-fractional transformation $t{:}z \rightarrow \frac{1}{z}$ inverts u and v, that is, $t^2 = (ut)^2 = (vt)^2 = 1$ and so extends the group $G(2,Z)$ to $G^*(2,Z) = \langle u,v,t : u^3 = v^3 = t^2 = (ut)^2 = (vt)^2 = 1\rangle$.

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

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 $G^*(2,q)$ is then the group of linear-fractional transformations of the form $z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d \in F_q$ and $ad - bc \neq 0$, while $G(2,q)$ is its subgroup consisting of all those linear-fractional transformations of the form $z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d \in F_q$ and $ad-bc$ is a non-zero square in F_q.

We use coset diagrams for the group and study its action on $PL(F_q)$. Our coset diagrams consist of triangles; they are called coset diagrams because the vertices of the triangles are identified with cosets of the group. These diagrams are defined for a particular group which has a presentation with three generators. The coset diagrams defined for the actions of $G^*(2,Z)$ on $PL(F_q)$ are special in a number of ways [3]. First, they are defined for a particular group, namely, $G^*(2,Z)$, which has a presentation in terms of three generators t, u and v. Since there are only three

2010 Mathematics Subject Classification: 20F05; 20G40.
Keywords: Linear-fractional transformation, non-degenerate homomorphism, conjugacy classe, parametrization, projective line.

generators, it is possible to avoid using colors as well as the orientation of edges associated with the involution t. For u, and v both have order 3, there is a need to distinguish u from u^2 and v from v^2. The three cycles of the transformation u are denoted by three (blue) unbroken edges of a triangle permuted anti-clockwise by u and the three cycles of the transformation v are denoted by three (red) broken edges of a triangle permuted anti-clockwise by v. The action of t is depicted by the symmetry about vertical axis. Fixed points of u and v, if they exist, are denoted by heavy dots. The method is well explained in [1, 2].

G. Higman proposed the problem of parametrization of actions of $PGL(2, Z)$ on $PL(F_q)$. The problem was solved by Q. Mushtaq in [5]. In this paper, we take up the problem and parametrize the actions of $G^*(2, Z)$ on $PL(F_q)$. We have shown here that any non-degenerate homomorphism α from $G(2, Z)$ into $G(2, q)$ can be extended to a non-degenerate homomorphism α from $G^*(2, Z)$ into $G^*(2, q)$. It has been shown also that every element in $G^*(2, q)$, not of order 1 or 3, is the image of uv under α. It is also proved that the conjugacy classes of $\alpha : G^*(2, Z) \rightarrow G^*(2, q)$ are in one-to-one correspondence with the conjugacy classes of non-trivial elements of $G^*(2, q)$, under a correspondence which assigns to the homomorphism α the class containing $(uv)\alpha$.

2. Conjugacy classes

A homomorphism $\alpha : G^*(2, Z) \rightarrow G^*(2, q)$ amounts to choosing $\overline{u} = u\alpha$, $\overline{v} = v\alpha$ and $\overline{t} = t\alpha$, in $G^*(2, q)$ such that

$$\overline{u}^3 = \overline{v}^3 = \overline{t}^2 = (\overline{u}\overline{t})^2 = (\overline{v}\overline{t})^2 = 1. \tag{1}$$

We call α to be a *non-degenerate homomorphism* if neither of the generators u, v of $G^*(2, Z)$ lies in the kernel of α. Two homomorphisms α and β from $G^*(2, Z)$ to $G^*(2, q)$ are called *conjugate* if there exists an inner automorphism ρ of $G^*(2, q)$ such that $\beta = \rho\alpha$. Let δ be the automorphism on $G^*(2, Z)$ 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 $\overline{t}\overline{u}\overline{t}$, $\overline{v}$, $\overline{t}$ satisfying the above relations, therefore the solutions of these relations occur in dual pairs. Of course, if α is conjugate to β then α' is conjugate to β'.

3. Parametrization

If the natural mapping $GL(2, q) \rightarrow G^*(2, q)$ maps a matrix M to the element of g of $G^*(2, q)$ 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 $G^*(2, q)$. 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 $G^*(2,q)$ 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 $G(2,q)$ 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 $G(2,q)$ 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 representation of $G^*(2,q)$ 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, $a^2+d^2-2ad+4bc = (a+d)^2-4(ad-bc) = r^2-4 = \theta-4$. Thus, g has fixed point in the representation of $G^*(2,q)$ 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 $G^*(2,q)$ with $\det(UV)=1$ and trace r, then for a positive integer k

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

Furthermore, suppose

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

The replacement of θ for r^2 in $f(r)$ yields a polynomial $f(\theta)$ in θ. Thus, one can find a minimal polynomial for positive integer k such that $q \equiv \pm 1 (\mathrm{mod}\ k)$ by the equation:

$$g_k(\theta) = \frac{f_k(\theta)}{g_{d_1}(\theta) g_{d_2}(\theta) \ldots g_{d_n}(\theta)} \tag{4}$$

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).

The degree of the minimal polynomial is obtained as:

$$\deg[g_k(\theta)] = \deg[f_k(\theta)] - \sum \deg[g_{d_i}(\theta)] \tag{5}$$

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, $\deg[g_{2^n}(\theta)] = \frac{2^n}{2} - \frac{2^{n-1}}{2}$, and $\deg[g_{p^n}(\theta)] = \frac{p^n}{2} - \frac{p^{n-1}}{2}$, if p is an odd 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	$\theta^2 - 5\theta + 5 = 0$

Table 1.

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 $\overline{u}^3 = 1$, U^3 is a scalar matrix, and hence the $\det(U)$ is a square in F_q. Thus, replacing U by a suitable scalar multiple, we assume that $\det(U) = 1$.

Since, for any matrix M, $M^3 = \lambda I$ if and only if $(tr(M))^2 = \det(M)$, we may assume that $tr(U) = a + d = -1$ and $\det(U) = 1$. Thus $U = \begin{bmatrix} a & b \\ c & -a-1 \end{bmatrix}$. Similarly, $V = \begin{bmatrix} e & f \\ g & -e-1 \end{bmatrix}$. Since $\overline{u}^3 = 1$ also implies that the $tr(\overline{u}) = -1$, every element of $GL(2,q)$ of trace equal to -1 has up to scalar multiplication, a conjugate of the form $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$. Therefore U will be of the form $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$.

Now let $\overline{t}$ be represented by $T = \begin{bmatrix} l & m \\ n & j \end{bmatrix}$. Since $\overline{t}^2 = 1$, the trace of T is zero. So, up to scalar multiplication, the matrix representing $\overline{t}$ 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 $G^*(2,q)$ will be: $U = \begin{bmatrix} a & kc \\ c & -a-1 \end{bmatrix}$, $V = \begin{bmatrix} e & gk \\ g & -e-1 \end{bmatrix}$, and $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ respectively, where $a, c, e, g, k \in F_q$. Then,

$$1 + a + a^2 + kc^2 = 0 \tag{6}$$

and

$$1 + e + e^2 + kg^2 = 0 \tag{7}$$

because the determinants of U and V are 1.

This certainly evolves elements satisfying the relations $U^3 = V^3 = \lambda I$, where λ is a scalar 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

$$r = a(2e+1) + 2kgc + (e+1) \tag{8}$$

If $tr(UVT) = ks$, then

$$s = 2ag - c(2e+1) + g \tag{9}$$

So the relationship between (8) and (9) is

$$r^2 + ks^2 = r + 2. \tag{10}$$

We set

$$\theta = r^2 \tag{11}$$

4. Main results

Lemma 4.1. *Either $\overline{uv}$ is of order 3 or there exists an involution $\overline{t}$ in $G^*(2,q)$ such that $\overline{t}^2 = (\overline{ut})^2 = (\overline{vt})^2 = 1$.*

Proof. Let $tr(UV) = r = gk - g + e + 1$. Then, $gk - g = r - e - 1$. Also $\det(UV) = -g^2k - e^2 - e = -(g^2k + e^2 + e) = 1$. Because, $\overline{t}^2 = (\overline{ut})^2 = (\overline{vt})^2 = 1$, $m = n - l$ and so

$$(2e - g + 1)l + (gk + g)n = 0 \tag{12}$$

Now for T to be a non-singular matrix, we should have $det(T) \neq 0$, that is

$$nl - l^2 - n^2 \neq 0. \tag{13}$$

Thus the necessary and sufficient conditions for the existence of $\overline{t}$ in $G^*(2,q)$ are the equations (12), and (13). Hence $\overline{t}$ exists in $G^*(2,q)$ unless $nl - l^2 - n^2 = 0$. Of course, if both $2e-g+1$ and $gk+g$ are equal to zero, then the existence of $\overline{t}$ is trivial. If not, then $l/n = -(gk+g)/(2e-g+1)$, and so equation (13) is equivalent to $(gk+g)^2+(2e-g+1)^2+(2e-g+1)(gk+g) \neq 0$. Thus there exists $\overline{t}$ in $G^*(2,q)$ such that $\overline{t}^2 = (\overline{ut})^2 = (\overline{vt})^2 = 1$ unless $(gk+g)^2+(2e-g+1)(gk+g) = -(2e-g+1)^2$. But if $(gk+g)^2 + (2e-g+1)(gk+g) = -(2e-g+1)^2$, then, $g^2k^2+g^2+2g^2k+2egk+2eg -g^2k-g^2+gk+g = -(4e^2+g^2+1+4e-2g-4eg) = -\{4e^2+4e+1+g^2-2g-4eg\} = -\{-4g^2k - 3 + g^2 - 2g - 4eg\}$. So, after simplification

$$(gk-g)^2 + (gk-g) + 2e(gk-g) - g^2k = 3 \tag{14}$$

Since $gk - g = r - e - 1$, equation (14) can be further simplified as

$$r^2 - 2 = r \tag{15}$$

Square both sides of equation (15), and substitute $r^2 = \theta$ in the equation $\theta^2 - 5\theta + 4 = 0$ giving $\theta = 1, 4$.

By Table 1, $\theta = 1$ implies that the order of $\overline{u}\,\overline{v}$ is 3 and $\theta = 4$ implies that the order of $\overline{u}\,\overline{v}$ is 1. $\square$

It can happen that both $\overline{u}\,\overline{v}$ is of order 3 and the pair $(\overline{u}, \overline{v})$ is invertible if $\overline{u}\,\overline{v} = \overline{v}\,\overline{u}$. For example, if $U = \begin{bmatrix} 2 & 2 \\ 2 & -3 \end{bmatrix}$, $V = \begin{bmatrix} 2 & 2 \\ 2 & -3 \end{bmatrix}$, and $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. In fact, because of the following result this is the only case in which $\overline{t}$ exists and $\overline{u}\,\overline{v}$ is of order 3.

Lemma 4.2. *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 4.3. *Any non trivial element* $\overline{g}$ *of* $G^*(2, q)$ *whose order is not equal to* 2 *or* 6 *is the image of* uv *under some non-degenerate homomorphism* α *of* $G^*(2, Z)$ *into* $G^*(2, q)$.

Proof. Using Lemma4.1, we show that every non-trivial element of $G^*(2, q)$ is a product of two elements of orders 3. So we find elements $\overline{u}, \overline{v}$ and, $\overline{t}$ of $G^*(2, q)$ satisfying the equation (1) 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 (10), yields $ks^2 = 2 + r - r^2$. If $r^2 \neq 2 + r$, 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, $e^2 + e$ and $-kg^2 - 1$ each take at least $(q + 1)/2$ distinct values as e and g run through F_q. Hence we can find e and g so that $e^2 + e = -kg^2 - 1$ (equation 7).

Finally by substituting the values of r, s, e, g, k in equations (8) and (9) we obtain the values of a and c. □

It is clear from (10) and (11) that $\theta = 0$ when $r = 0$ and $\theta = 1$ or 4 when $s = 0$. The possibility that $\theta = 0$ gives rise to the situation where $\overline{uv}$ is of order 2. Similarly, the possibility $\theta = 1$ leads to the situation where $\overline{u}\,\overline{v}$ is of order 3, and similarly $\theta = 4$ yields $\overline{u}\,\overline{v}$ of order 1.

Lemma 4.4. *Any two non-degenerate homomorphisms* α, β *of* $G^*(2, Z)$ *into* $G^*(2, q)$ *are conjugate if* $(uv)\alpha = (uv)\beta$.

Proof. Let α: $G^*(2, Z) \to G^*(2, q)$ be such that $\overline{u}\,\overline{v}$ has parameter θ constructed as in the proof of lemma 4.3. We also suppose that β:$G^*(2, Z) \to G^*(2, q)$ has the same parameter θ.

First, since there are just two classes of elements of order 2 in $G^*(2,Z)$, one in $G^*(2,Z)$ and the other not, we can pass to a conjugate of β in which $t\beta$ is represented by $\begin{bmatrix} 0 & -k' \\ 1 & 0 \end{bmatrix}$ for some $k' \neq 0$ in F_q. Then because $u\beta$ and $v\beta$ are both of orders 3, $u\beta$ must be represented by a matrix $\begin{bmatrix} a' & k'c' \\ c' & -a'-1 \end{bmatrix}$ and $v\beta$ must be represented by a matrix $\begin{bmatrix} e' & k'g' \\ g' & -e'-1 \end{bmatrix}$, with a', c', e', g', k' satisfying the equations from (6) to (9). Then $\theta = r'^2 = r^2$ and $(2+r) - \theta = k's'^2 = ks^2$. Here since θ and $(2+r)-\theta$ are non-zero, so it follows that k'/k is a square in F_q.

Now $v\alpha$ and $v\beta$ are both of orders 3 and so are conjugate in $G^*(2,q)$. So we can pass to a conjugate of β (which we still call β) with $v\alpha = v\beta$. As $t\alpha$ and $t\beta$ are involutions which invert $v\alpha$, and so belong to $N(\langle v\alpha \rangle)$ there are two classes of such involutions, one in $G^*(2,q)$ and the other not. Because $t\alpha$ is $\begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ and $t\beta$ is conjugate to $\begin{bmatrix} 0 & -k' \\ 1 & 0 \end{bmatrix}$ and k'/k is a square, $t\alpha$ and $t\beta$ either both belong to $G^*(2,q)$ or neither. Hence they are conjugate in $N(\langle v\alpha \rangle)$. That is, passing to a new conjugate (still called β) we can assume $v\alpha = v\beta, t\alpha = t\beta$. This means that in the notations above, we can assume $k' = k$, $g = g'$ and $e = e'$. We can also, by multiplying the matrix representing $u\beta$ by a scalar, assume $r = r'$ and $s = s'$. Then the equations from (6) to (9) with a, c, e, g, k and then with a', c', e', g', k' and ensure that $a = a'$and $c = c'$. That is $\alpha = \beta$. □

Theorem 4.5. *The conjugacy classes of non-degenerate homomorphisms of* $G^*(2,Z)$ *into* $G^*(2,q)$ *are in one-to-one correspondence with the non-trivial conjugacy classes of elements of* $G^*(2,q)$ *under a correspondence which assigns to any non-degenerate homomorphism* α *the class containing* $(uv)\alpha$.

Proof. Let $\alpha : G^*(2,Z) \to G^*(2,q)$ be 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 α is associated with θ. We shall call the parameter θ of the class containing $\overline{u}\ \overline{v}$, the parameter of $G^*(2,Z) \to G^*(2,q)$. Now

$$UT = \begin{bmatrix} ck & -ak \\ -a-1 & -ck \end{bmatrix}$$

implies that $\det(UT) = -k(a^2 + a + kc^2) = k$ (equation 6). Also,

$$(UT)V = \begin{bmatrix} kec - akg & k^2gc + ak(e+1) \\ -ae - e - kgc & -akg - kg + ck(e+1) \end{bmatrix}$$

implies that the $tr((UT)V) = 2kec - 2akg - kg + kc = -1(2akg - 2kec + kg - kc) = -ks$. If $\overline{u}, \overline{v}, \overline{t}$ satisfy equation (1), then so do $\overline{t}\overline{u}\overline{t}, \overline{v}, \overline{t}$. So that the solution of equation (1) occur in dual pairs. Hence replacing the solutions in lemma-4.3 by

$\overline{t}\overline{u}\overline{t}, \overline{v}, \overline{t}$, we obtain $\theta = \frac{[tr((UT)V]^2}{\det(UT)} = \frac{k^2s^2}{k} = ks^2$. 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 4.6. *If $\alpha : G^*(2, Z) \to G^*(2, q)$ is a non-degenerate homomorphism, α' is its dual and θ, φ are their respective parameters then $\theta + \varphi = r + 2$.*

Proof. Let $\alpha : G^*(2, Z) \to G^*(2, q)$ satisfy 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 $U = \begin{bmatrix} a & ck \\ a & -a-1 \end{bmatrix}$, $V = \begin{bmatrix} e & g\,k \\ g & -e-1 \end{bmatrix}$ 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 (6) to (10). Now, $(\overline{u}\,\overline{v})^2 = 1$ implies that $tr(UV) = 0$. Also, we have $\{tr(UVT)\}/k = s = 0$ if and only if $(\overline{u}\,\overline{v}\overline{t})^2 = 1$. Now $\det(UV) = 1$, thus giving the parameter of $\overline{u}\ \overline{v}$ equal to $r^2 = \theta$, say. 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 $\overline{u}\ \overline{v}\overline{t}$ equal to ks^2, which we denote by φ. Thus $\theta + \varphi = r^2 + ks^2$. Substituting the values from equation (10), we thus obtain $\theta + \varphi = r + 2$. Hence if θ is the parameter of the non-degenerate homomorphism α, then $\varphi = r + 2 - \theta$ is the parameter of the dual α' of α. □

Theorem 4.5, of course, means that we can actually parametrize the non-degenerate homomorphisms of $G^*(2, Z)$ to $G^*(2, q)$ except for a few uninteresting ones, by the elements of F_q. Since $G^*(2, q)$ has a natural permutation representation on $PL(F_q)$, any homomorphism $\alpha : G^*(2, Z) \to G^*(2, q)$ gives rise to an action of $G^*(2, Z)$ on $PL(F_q)$.

References

[1] **M. Ashiq and Q. Mushtaq**, *Finite presentation of a linear-fractional group*, Algebra Colloquium **12** (2005), 585 – 589.

[2] **M. Ashiq and Q. Mushtaq**, *Coset diagrams for a homomorvarphic image of* $\triangle(3, 3, k)$, Acta Math. Sci. **28B** (2008), 363 – 370.

[3] **M. H. Millington**, *Subgroups of the classical modular group*, J. Lond. Math. Soc. **1** (1970), 351 – 357.

[4] **Q. Mushtaq**, *Coset diagrams for Hurwitz groups*, Commun. Algebra **18** (1990), 3857 – 3888.

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

[6] **W. W. Stothers**, *Subgroups of the modular group*, Proc. Camb. Philos. Soc. **75** (1974), 4139 – 154.

Received February 14, 2011