PERMUTATION REPRESENTATION OF TRIANGLE GROUPS

Saima Anis

Supervised by

Prof. Dr. Qaiser Mushtaq

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2003

PERMUTATION REPRESENTATION OF TRIANGLE GROUPS

A dissertation authored by

Saima Anis

under the supervision of

Prof. Dr. Qaiser Mushtaq

and submitted in partial fulfillment of the

DEGREE OF MASTER OF PHILOSOPHY
IN
MATHEMATICS

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2003

CERTIFICATE

A dissertation on **Permutation Representation of Triangle Groups** authored by **Saima Anis** in partial fulfillment of the requirements for the degree of **Master of Philosophy** is accepted as conforming to the required standard.

1. Qaiser Mushtaq

Prof. Dr. Qaiser Mushtaq
(Supervisor)

2. M. Sarwar

Prof. Dr. M. Sarwar Kamran
(External Examiner)

3. Qaiser Mushtaq

Prof. Dr. Qaiser Mushtaq
(Chairman)

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2003

With everlasting love

and dedication

to my mother

and

to the memory of my late father

ACKNOWLEDGEMENT

All appreciation to "**ALMIGHTY ALLAH**" without whose Will and Consent we cannot proceed a single step. I offer my humblest Darood to the **HAZRAT MUHAMMAD** (peace be upon him) who is forever a guidance for humanity.

I wish to indebted my supervisor and chairman of the department **Professor Dr. Qaiser Mushtaq** for his continual encouragement, support, comments, invaluable discussion during the course of research and writing of this dissertation.

I express my heartiest gratitude to my mother, brother in law, sister and brothers for their prayers and moral support during my studies.

I wish to express my thanks to all my teachers and senior colleagues especially Major Tariq Maqsood and Sarwar Saeed for their help.

Last of all, I am thankful to my friends especially Sadaf Ashiq, Shazia Rana and Samia Khalid, for their co-operation and constant encouragement.

Saima Anis

PREFACE

The modular group $PSL(2,Z)$ has a long and rich history. It is one of the most useful linear groups. It is a free product of two cyclic groups of orders 2 and 3. The finite presentation of $PSL(2,Z)$ is $< x,y : x^2 = y^3 = 1 >$ where x and y are the linear-fractional transformations defined by $z \mapsto \frac{-1}{z}$ and $z \mapsto \frac{z-1}{z}$ respectively. By adjoining a new element $t : z \mapsto \frac{1}{z}$ with x, y, we obtain a finite presentation $< x,y,t : x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1 >$ of the extended modular group $PGL(2,Z)$.

The actions of $PSL(2,Z)$ on various sets and spaces have produced enormous bulk of significant results. Graham Higman has defined coset diagrams specifically for $PSL(2,Z)$ which are extensively used by a number of researchers to study the actions of $PSL(2,Z)$. The coset diagrams for the action of $PSL(2,Z)$ on the projective lines over Galois fields F_p are finite and give interesting and useful group-theoretic information.

In this dissertation, we have used these diagrams to find the number of subgroups of a given index in the modular group.

Our dissertation consists of four chapters.

In the first chapter we have given definitions. We also describe some related groups which are referred to in the work.

The second chapter consists of the graphical aspects of the groups and a brief historical description of evolution of coset diagrams. We have given here the coset diagrams for $PSL(2,Z)$, action of $PSL(2,Z)$ on projective line over Galois fields F_q, q is power of prime and parametrization by G. Higman.

In chapter three we have defined coset diagrams for the action of $PSL(2,Z)$ on $PL(F_p)$ and proved a number of theorems which help us to count subgroups of $PSL(2,Z)$ through the use of coset diagrams for the action of $PSL(2,Z)$ on $PL(F_p)$. Our main result is also contained in this chapter.

In chapter four we have formulated a program written in TC++ to find permutation representations of the actions of $PSL(2,Z)$ on $PL(F_p)$. This program also, helps us to obtain coset diagrams.

Contents

Chapter 1

Groups and Actions

In this chapter we have given the definitions referred to in this work along with a few examples to illustrate these definitions. A particular emphasis is placed on the modular group $PSL(2,Z)$.

Moreover, we have described Galois fields, Free product, Kurosh subgroup theorem, Modular group, Triangle groups, Projective line over the Galois fields and Transitivity.

1.1 Galois Fields

The ring Z of integers induces a natural ring structure on $Z_n = Z/nZ$, the integer modulo n; if n is a prime p, then Z_n is, in fact, a field under this structure. They are known as Galois fields also. Now the set $(Z_n)^r$ of sequence $(a_0, a_1, ..., a_{r-1})$, $a_i \in Z_n$, has an additive structure in which addition is performed coordinate-wise, and when n is a prime p, this set may be given a multiplicative structure which makes it a field. This is done by identifying the sequence $(a_0, a_1, ..., a_{r-1})$ with the polynomial $a_0 + a_1 t + ... + a_{r-1} t^{r-1}$ in the ring $Z_p[t]$.

Choosing a polynomial $f(t) \in Z_p[t]$ of degree r which is irreducible over Z_p (that is, has no zeros in Z_p), and defining multiplication to be polynomial multiplication in $Z_p[t]$ followed by reduction modulo $f(t)$. The polynomial t, or the sequence $(0,1,0,...,0)$, has the property that it is an element of the field, which is called $GF(p^r)$, can be written as $0, t, t^2, ..., t^{p^r-2}, t^{p^r-1} = 1$. For example, to construct $GF(3^2)$, note that $t^2 + 2t + 2$ is irreducible over $Z_3 = \{0,1,2\}$. Thus $GF(3^2)$ may be listed as follows.

i	0	t	t^2	t^3	t^4	t^5	t^6	t^7	t^8
ii	0	t	$t+1$	$2t+1$	2	$2t$	$2t+2$	$t+2$	1
iii	$(0,0)$	$(0,1)$	$(1,1)$	$(1,2)$	$(2,0)$	$(0,2)$	$(2,2)$	$(2,1)$	$(1,0)$

We summarize the relevant properties of the Galois fields as follows.

1.1.1 Remarks

1. There is a Galois field with q elements if and only if q is a prime power, $q = p^r$.

2. If F is a Galois field with p^r elements, $F = GF(p^r)$, in particular, the construction $GF(p^r)$ is independent of the choice of irreducible polynomial.

3. The multiplicative group of $GF(p^r)$ is the cyclic group Z_{p^r-1}. A generator of this group is called a primitive element of $GF(p^r)$. The group of field automorphisms of $GF(p^r)$ is cyclic group generated by the automorphism $x \longmapsto x^p$.

1.1.2 Example

Let F_q be a field of order q, the multiplicative group F_q^* of non-zero elements of F_q is a cyclic group of order $q-1$. The elements of F_q are roots of the polynomial $x^q - x$. For example, $F_7^* = \{1, 3, 2, 6, 4, 5\} = \{\alpha^6 = 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$, where $\alpha = 3$ is the primitive element of F_7^*.

1.2 Projective Line over the Galois Fields

Let q be a power of a prime p, that is, $q = p^n$ for some positive integer n. Then $PL(F_q)$, the projective line over the Galois field F_q contains the elements of F_q, together with the additional point ∞. If $n = 1$ then F_q is $\{1, 2, ..., p\}$. Let V be a vector space over a field F, $V^* = V - \{0\}$, and suppose $x, y \in V^*$, then the statement " for some $\lambda \in F^* = F - \{0\}$, $x = \lambda y$" defines an equivalence relation on V^*, and the set of equivalence classes is called the projective space $PG(V)$. We shall denote the class of $x \in V^*$ by $[x] \in PG(V)$, and define a subspace $[U]$ of $PG(V)$, to the image of a subspace U of V under the map $x \longrightarrow [x]$. For geometric reason it is convenient to say that if U has dimension k then $[U]$ has (projective) dimension $k-1$; in particular if $V = V(n, g)$, we write $PG(V) = PG(n-1, q)$.

As an example, consider $V = V(3,2)$. This has 7 non-zero points, each of which is equivalent only to itself, since F^* has only one element. A plane (2−dimensional subspace in $V(3,2)$) contains 3 non-zero points and defines a line (1−dimensional subspace) again with three points in $PG(2,2)$. If we choose a basis in $V(3,2)$, that a point x has coordinates (x_0, x_1, x_2), then writing $[x] = [x_0, x_1, x_2]$ we may represent the points and lines of $PG(2,2)$ as in the diagram;

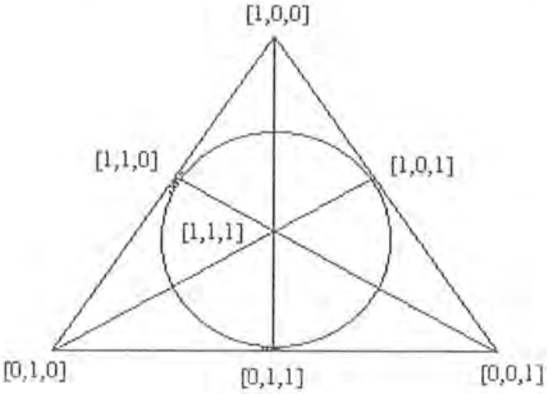


Figure 1.1

which gives a representation of the projective plane $PG(2,2)$.

We take $V = V(2,q)$ for a vector space of dimension 2 over a Galois field F_q. V has q^2 elements. The projective space over $V = V(2,q)$ is the $PG(1,q)$ (called the projective line $PL(F_q)$) has $q+1$ points. It may be represented by q symbols $[1,z]$, (where z runs through F_q) and the additional symbol $[0,1]$. We often think of $PG(1,q) = PL(F_q)$ as the set $F_q \cup \{\infty\}$, where ∞ is image of $[0,1]$ under the bijection $[x_0, x_1] \longleftrightarrow \frac{x_1}{x_0}$. Thus $PL(F_q) = PG(1,q) = F_q \cup \{\infty\} = \{0, 1, 2, 3, ..., q-1\} \cup \{\infty\}$.

Let $q = p^r$ where $r > 0$ and p is a prime number. Then an element $\omega \in F_q$ is said to be a non-zero square in F_q if $\omega \equiv a^2 (\text{mod } p)$ for some non-zero element a in F_q. For example, if we have $F_{11} = \{0, 1, 2, ..., 10\}$ then $130 \equiv 3^2 (\text{mod } 11)$, thus 130 is a non-zero square in F_{11}.

1.3 Free Product

A group G is said to be the free product of its subgroups H_α (α ranges over some index set) if the subgroups H_α generate G, that is, if every element g of G is the product of a finite number of the elements of the H_α,

$$g = a_1 a_2 ... a_n,\ a_i \epsilon H_{\alpha_i},\ i = 1, 2, ..., n, \tag{1.1}$$

and if every element g of G, $g \neq 1$, has a unique representation in the form equation(1.1) subject to the condition that all the elements a_i are different from the unit element and that in equation(1.1) no two adjacent elements are in the same subgroup H_α although the product equation (1.1) may, in general, contain several factors from one and the same subgroup.

The free product is denoted, by the symbol

$$G = \prod_\alpha * H_\alpha, \tag{1.2}$$

and if G is the free product of a finite number of subgroups $H_1, H_2, ..., H_k$, by the symbol

$$G = H_1 * H_2 * ... * H_k.$$

The subgroups H_α are called the free factors of the free decomposition equation(1.2) of G.

Let A and B be subgroups of a group G. B is said to be conjugate of A in G if $B = g^{-1}Ag$ for $g \epsilon G$.

1.4 Kurosh Subgroup Theorem

If

$$G = \prod_\alpha * H_\alpha$$

and if H is an arbitrary subgroup of G, then there exists a free decomposition of H

$$H = F * \prod_\beta * B_\beta$$

where F is a free group and every B_β is conjugate in G to a subgroup of one of the free factors H_α.

1.5 General Linear Groups

Let F be a field and n a positive integer. We write $M_n(F)$ for the ring of all $n \times n$ matrices with entries from F. Then $GL\,(n, F) = \{A \in M_n(F) : A \; is \text{ invertible}\}$, the set of all $n \times n$ invertible matrices, with entries from F forms a group under the matrix multiplication. The group $GL\,(n, F)$ is known as the n-dimensional general linear group over F. The n dimensional special linear group $SL\,(n, F)$, is defined to be the group of all $n \times n$ matrices with entries from F and determinant 1, that is, $SL\,(n, F) = \{A \in GL(n, F) : \det(A) = 1\}$. The group $SL\,(n, F)$ is a normal subgroup of $GL\,(n, F)$.

Since the determinant map $\det : GL(n, F) \longrightarrow F^*$, where F^* denotes the multiplicative group of non-zero elements of F, is a group epimorphism and has $SL\,(n, F)$ as its kernel, we have $GL(n, F)/SL(n, F) \cong F^*$.

If F is a finite field having q elements, then F can be denoted by F_q. In this case, the general linear group of dimension n, over the field F_q is $GL\,(n, F_q)$. Similarly we define $SL\,(n, F_q)$.

Since all finite fields of the same order are isomorphic, therefore $GL\,(n, F_q)$ and $SL\,(n, F_q)$ are written as $GL\,(n, q)$ and $SL\,(n, q)$ respectively.

Let V be an n-dimensional vector space over a field F. Then an isomorphism of V into itself is called an automorphism of the vector space V. The general linear group $GL\,(n, q)$ can be considered as the group of all automorphisms of n-dimensional vector space over the field F_q of q elements. The special linear group $SL\,(n, q)$ is its normal subgroup consisting of the automorphisms of determinant 1. The centre of either of these groups consists of the operations of the form $x \longmapsto kx$ where $k \in F_q$ and we obtain the corresponding projective groups, namely $PGL\,(n, q)$ and $PSL\,(n, q)$, by factoring out these centres.

The modular group $PSL\,(2, Z)$ is the group of all linear-fractional transformations $z \longmapsto (az + b) / (cz + d)$ where a, b, c, d are integers and $ad - bc = 1$. $PSL\,(2, Z)$ is generated by two linear-fractional transformations $x : z \longmapsto -1/z$ and $y : z \longmapsto (z - 1) / z$ which satisfy the relations

$$x^2 = y^3 = 1 \tag{1.3}$$

The extended modular group $PGL\,(2, Z)$ is the group of all the linear-fractional transformations $z \longmapsto (az+b)\,/\,(cz+d)$ where a, b, c, d are integers and $ad - bc = \pm 1$. If t is the linear-fractional transformation $z \longmapsto 1/z$, which belongs to $PGL\,(2, Z)$ but not to $PSL\,(2, Z)$, then x, y, t satisfy the relations

$$x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1 \tag{1.4}$$

These relations are the defining relations for $PGL\,(2, Z)$ which is generated by x, y and t.

The modular group has the property that every alternating and symmetric group is its homomorphic image except A_6, A_7, A_8, S_5, S_7 and S_8 [7].

The group $PGL\,(2, q)$ is the group of all the linear-fractional transformations

$z \longmapsto (az+b)\,/\,(cz+d)$ where a, b, c, d are in F_q and $ad - bc \neq 0$,while the group $PSL\,(2, q)$ is its subgroup consisting of all those linear-fractional transformations where $ad - bc$ is a non zero square in F_q.

Every element of $PGL\,(2, q)$ gives a permutation of the points of $PL\,(F_q)$, and so $PGL\,(2, q)$ is a subgroup of the symmetric group S_{q+1}. The elements of $PSL\,(2, q)$ give only even permutations, so $PSL\,(2, q)$ is a subgroup of the alternating group A_{q+1}.

1.6 Triangle Groups

In [1], a group is called a triangle group if it can be presented in the form

$$\Delta\,(l, m, k) = \langle x, y : x^l = y^m = (xy)^k = 1 \rangle\,, \tag{1.5}$$

where $l, m, k > 1$. For $l = 2$ and $m = 3$, triangle groups are, therefore, quotients of the modular group [4]. Every countable group occurs as a subgroup of some quotient of the modular group. The symmetric group of degree n ($n \neq 5,\ 6,\ 8$) is itself a quotient of the modular group. Similar properties are true even if the triangle groups with $k \geqslant 7$. From [6], we come to know that triangle groups are infinite if and only if $\frac{1}{l} + \frac{1}{m} + \frac{1}{k} \leqslant 1$.

In our dissertation, we are interested in triangle groups $\Delta(l, m, k)$ where $l = 2$, $m = 3$ in equation (1.5). So, now onwards by the triangle groups $\Delta(2, 3, k)$ we shall mean the groups

$$\langle x, y : x^2 = y^3 = (xy)^k = 1 \rangle. \tag{1.6}$$

Let M denote a 2×2 matrix, $\triangle$ and r its determinant and trace respectively. Then the characteristic equation of the matrix M is defined as

$$M^2 - rM + \triangle I = O$$

where O and I are respectively the null and the identity matrices of order 2×2. A homomorphism $\alpha : PGL(2, Z) \longrightarrow PGL(2, q)$ is called a non-degenerate homomorphism if x, y and t do not lie in the kernel of α, so that $\overline{x} = x\alpha$, $\overline{y} = y\alpha$ and $\overline{t} = t\alpha$ are of orders $2, 3$ and 2 respectively. As always two non-degenerate homomorphisms α and β are called conjugate if there exists an inner automorphism ρ of $PGL(2, q)$ such that $\beta = \alpha\rho$.

The conjugacy class as thus obtained contain all those homomorphisms from $PGL(2, Z)$ to $PGL(2, q)$ which are conjugate to each other. If the natural mapping $GL(2, q) \longrightarrow PGL(2, q)$ maps a matrix M to the element g of $PGL(2, q)$, then $\theta = (trace(M))^2 / \det(M)$ is an invariant of the conjugacy class of g. We refer to it as the parameter of g or the conjugacy class of which g is the representative. Of course every element in F_p is the parameter of some conjugacy class in $PGL(2, q)$. It has been shown in [13] that there is a one-to-one correspondence between conjugacy classes of elements of order greater than 2 in $PGL(2, q)$ and the non-zero elements of F_q, such that the class corresponding to an element $\theta \in F_q$ consists of all the elements represented by matrices M with $\theta = r^2/\triangle$, where as described earlier $r = trace(M)$ and $\triangle = det(M)$.

The conjugacy classes of α are in fact conjugacy classes of the actions of $PGL(2, Z)$ on $PL(F_q)$.

1.7 Transitivity

Let G be a group and Ω a set. By an action of G on Ω we mean a function $\mu : \Omega \times G \longrightarrow \Omega$ such that for all $\omega \in \Omega$ and all $g, h \in G$,

$$((\omega, g)\,\mu, h)\,\mu = (\omega, gh)\,\mu$$

and for all $\omega \in \Omega$

$$(\omega, 1)\,\mu = \omega$$

where 1 denotes an identity element of the group G. In practice one finds it convenient to do without an explicit name for the action μ and we write ω^g for $(\omega, g)\,\mu$ whenever there is no risk of confusion. In this notation the axioms look rather simpler:

$$(\omega^g)^h = \omega^{gh}$$

and

$$\omega^1 = \omega$$

for all $\omega \in \Omega$ and all $g, h \in G$.

If G acts on a set Ω, then Ω is called G-set or a G-space. By a permutation group on the set Ω we mean simply a subgroup of $\mathrm{Sym}(\Omega)$. Such a group G has a natural action μ on Ω defined by

$$(\omega, g)\,\mu = \omega g$$

where right hand side of the definition means, of course, the image of ω under the permutation (bijective mapping on Ω). Here definition of the action will become the statement

$$(\omega g)\,h = \omega\,(gh)$$

and

$$\omega 1 = \omega$$

and these are certainly true, the former, by definition of composition of mappings (the group multiplication in G) and the latter, by definition of the identity function on Ω. More generally a homomorphism $\rho : G \longrightarrow Sym\left(\Omega\right)$ gives rise to an action μ of G on Ω defined by

$$\omega^g = \left(\omega, g\right)\mu = \omega\left(g\rho\right), \ \forall\, \omega \in \Omega \text{ and } g \in G.$$

We call a homomorphism $\rho : G \longrightarrow Sym\left(\Omega\right)$ a permutation representation of G, or a representation of G as a group of transformations of Ω. There is a useful relationship between a permutation representation and an action. The relationship is established in the following theorem.

Theorem 1 *Every permutation representation $\rho : G \longrightarrow Sym(\Omega)$ gives rise to an action of G on Ω and that, conversely every action gives rise to a permutation representation.*

Proof. Define a mapping $\mu : \Omega \times G \longrightarrow Sym(\Omega)$ as follows $\omega^g = (\omega, g)\mu = \omega(g\rho)$ for all $\omega \in \Omega$ and $g \in G$. This is an action because, $(\omega^g)^h = (\omega(g\rho))(h\rho) = \omega((g\rho)(h\rho)) = \omega((gh)\rho) = \omega^{gh}$ for all $\omega \in \Omega$ and $g, h \in G$. Also, $\omega^1 = \omega(1\rho) = \omega^1 = \omega$.

Conversely, suppose that μ is an action of G on Ω. For a fixed $g \in G$, define a mapping $\rho_g : \Omega \longrightarrow \Omega$ by $\rho_g : \omega \longmapsto \omega^g$. This is bijective: it has two sided inverse, which is $\rho_{g^{-1}}$, because, for all $\omega \in \Omega$, $\omega\rho_g\rho_{g^{-1}} = (\omega^g)^{g^{-1}} = \omega^1 = \omega$ and similarly, $\omega\rho_{g^{-1}}\rho_g = \omega$, which shows that $\rho_g\rho_{g^{-1}} = \rho_{g^{-1}}\rho_g = 1$.

In this way each element of G acts as a permutation of Ω. Furthermore, the map $\rho : G \longrightarrow Sym(\Omega)$, defined by $\rho : g \longrightarrow \rho_g$ is a homomorphism. This is the first axiom describing action because for all $\omega \in \Omega$ we have $\omega\rho_{gh} = \omega^{gh} = (\omega^g)^h = (\omega\rho_g)\rho_h = \omega(\rho_g\rho_h)$, and so for all $g, h \in G$ we have $\rho_{gh} = \rho_g\rho_h$. ■

If a group G acts on itself then the corresponding permutation representation $\rho : G \longrightarrow Sym\left(G\right)$ of G is said to be regular permutation representation of G and the $G-$space G is called regular $G-$space.

Let Ω be a G-space. We define a relation of equivalence under G by the rule $\alpha \equiv \beta (\bmod G)$ if and only if there exists g in G such that $\alpha^g = \beta$. Under this equivalence relation, let Ω_i, $i \in I$ be the equivalence classes as subsets of Ω then each one of these is called an orbit where Ω_i is called a G-orbit for a particular i. If $\alpha \in \Omega$ we define α^G (or αG where G consists of mappings of Ω) by the set $\{\alpha^g \colon g \in G\}$. This is called a G-orbit that contains α. For $\alpha \in \alpha^G$, if $\omega \in \alpha^G$ then $\omega = \alpha^h$ for some $h \in G$ and so $\omega^g = \alpha^{hg} \in \alpha^G$ for all $g \in G$. Thus α^G is a subspace of Ω.

Let G be a group and Ω be a set, we say G acts on Ω transitively if $\Omega \neq \phi$ and for any α, β $\epsilon\Omega$ there exists g ϵG such that $\alpha^g = \beta$. Of course, such an element g will depend upon α and β that is, a regular G-space is transitive for if $\alpha, \beta \in \Omega = G$, and if we take $g = \alpha^{-1}\beta$, then $\alpha^g = \beta$.

Theorem 2 *Every G-space can be expressed in just one way as the disjoint union of a family of orbits.*

Remark 3 *If a G-space has one orbit then the action of G on Ω is transitive.*

Chapter 2

Parametrization of the Actions

In this chapter we have defined a diagrammatic argument, called coset diagrams for the modular group $PGL(2,Z)$ and explain the method of parametrization. Also explain the action of the modular group on projective line over finite field F_q with example.

2.1 Definitions

The group $PGL(2,q)$ has a natural permutation representation on $PL(F_q)$, and therefore any homomorphism $\alpha : PGL(2,Z) \rightarrow PGL(2,q)$ gives rise to an action of $PGL(2,Z)$ on $PL(F_q)$. We denote the generators $x\alpha$, $y\alpha$ and $t\alpha$ of $PGL(2,q)$ by $\overline{x}$, $\overline{y}$ and $\overline{t}$. If neither of the generators x and y for $PSL(2,Z)$ lies in the kernel of α, so that $\overline{x}$ and $\overline{y}$ are of orders 2 and 3 respectively, then α is said to be a non-degenerate homomorphism. Two such homomorphisms α and β are said to be conjugate if $\beta = \alpha\rho$ for some inner automorphism ρ of $PGL(2,q)$. It has been proved in [13] that the conjugacy classes of non-degenerate homomorphisms of $PGL(2,Z)$ into $PGL(2,q)$ correspond in a one-to-one fashion with the conjugacy classes of non-trivial elements of $PGL(2,q)$, under a correspondence which assigns to the non-degenerate homomorphism α the class containing the element $(xy)\alpha$. This of course, means that we can actually parametrize the conjugacy classes of non-degenerate homomorphisms $\alpha : PGL(2,Z) \rightarrow PGL(2,q)$, except for a few uninteresting ones, by the elements of F_q. That is, we can in fact parametrize the actions of $PGL(2,Z)$ on $PL(F_q)$.Action of $PSL(2,Z)$ or of $PGL(2,Z)$ on $PL(F_q)$ via the homomorphism α is depicted by a coset diagram. This is a graph whose vertices are labelled by the elements of $PL(F_q)$.

2.2 Correspondence between F_q and the Set of Conjugacy Classes of the Actions

If α is any such non-degenerate homomorphism, and X, Y and T denote elements of $GL(2,q)$ which yield the elements $\overline{x}$, $\overline{y}$ and $\overline{t}$ in $PGL(2,q)$, where F_q is not of characteristic 2 or 3, then because of this and the fact that $\overline{x}$, $\overline{y}$ and $\overline{t}$ are of order 2, 3 and 2 respectively, then letting $\theta = \frac{r^2}{\Delta}$, where $r = trace(XY)$ and $\Delta = det(XY)$, we associate the parameter θ with the homomorphism α. We can take the matrices X, Y and T to be:

$$X = \begin{bmatrix} a & kc \\ c & -a \end{bmatrix}, \; Y = \begin{bmatrix} d & kf \\ f & -d-1 \end{bmatrix} \text{ and } T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$$

where $a, c, d, f, k \in F_q$.

We shall write

$$a^2 + kc^2 = -\Delta \neq 0, \tag{2.1}$$

and require that

$$d^2 + d + kf^2 + 1 = 0. \tag{2.2}$$

This certainly yields elements satisfying the relations $X^2 = Y^3 = T^2 = \lambda I$, where λ is some non-zero scalar and I is the identity matrix. The non-degenerate homomorphism α is determined by $\overline{x}\,\overline{y}$ because the one-to-one correspondence assigns to α the class containing $\overline{x}\,\overline{y}$. So we only have to check on the conjugacy class of $\overline{x}\,\overline{y}$. The matrix XY has the trace

$$r = a(2d+1) + 2kcf \tag{2.3}$$

If trace $(XYT) = ks$, then,

$$s = 2af - c(2d+1) \tag{2.4}$$

so that

$$3\triangle = r^2 + ks^2 \tag{2.5}$$

and set

$$\theta = \frac{r^2}{\triangle} \tag{2.6}$$

Thus, given the values of q and θ we can always find the matrices X and Y by using the equations (2.1) to (2.6).

2.3 Coset Diagrams for the Modular Group

The theory of graphs has a wide application in several branches of mathematics. Graphs provide methods by which various algebraic and topological structures can be visualized. Graphical methods have been explicitly used to study the finitely generated groups. The graphs have proven themselves as an economical mathematical technique to prove certain important results (see for example, [2], [3], and [5]). For finite groups of small order the graphs can be used instead of multiplication tables. They give the same information but in a much more efficient way (see for example, [3], [14]).

The method of representing group actions by graphs has a long and rich history. The first paper that appeared on this subject in 1878 was by A. Cayley [3]. Later, mathematicians W. Burnside [2], H.S.M. Coxeter and W.O.J. Moser [5], J. Whitehead, [16], etc., contributed seminal papers containing graphical representations of groups.

A coset diagram is, in fact, a graph whose vertices are the (right) cosets of a subgroup of finite index in a finitely generated group. The vertices representing cosets v and u (say), are joined by an S_i-edge, of "colour i" directed from vertex v to vertex u, whenever $vS_i = u$.

$$v \rightarrow v\,\mathrm{S}_i = u$$

It may well happen that $vS_i = v$, in which case the $v-$vertex is joined to itself by an S_i-loop and is called a fixed point of S_i also.

Formally a coset diagram, corresponding to a subgroup H of finite index in a finitely generated group G, is a directed edge, coloured graph, whose vertices are the (right) cosets of H in G and whose edges are defined as follows: we take a specific set of generators for G, and for each generator x and each vertex Hg, for some g in G, draw an edge of colour E^x from Hg to Hgx. This is very similar to the notion of a Schreier coset graph whose vertices represent the cosets of any given subgroup in a finitely-generated group, and also to that of a Cayley graph whose vertices are the group elements themselves, with trivial stabilizer. These diagrams may be drawn for any finitely generated groups depicting actions on any arbitrary sets or spaces. For example, take the group $< x, y, z : x^2 = y^3 = z^5 = 1 >$, and consider a transitive permutation representation on a set containing 15 points given by assigning permutations

$$x \text{ acts as} : (5,7)(10,12),$$

$$y \text{ acts as} : (1,6,11), \text{and}$$

$$z \text{ acts as} : (1,2,3,4,5)(6,7,8,9,10)(11,12,13,14,15).$$

This can be represented by the following diagram.

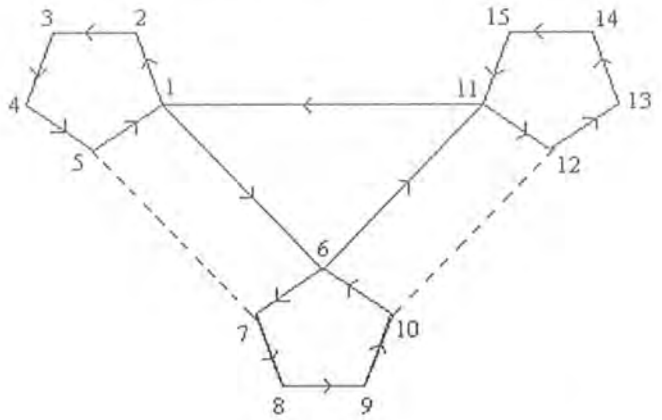


Figure 1.3

A. Cayley [3] used graphs to study certain groups in 1878. He represented the multiplication table of a group with given generators by a graph, and proposed the use of colours to distinguish the edges of the graphs associated with different generators. The Cayley diagram for a given group is a graph whose vertices represent the elements of the group, which are the cosets of the trivial subgroup. O. Schreier generalized this notion by considering a graph whose vertices represent the cosets of any subgroup. In 1965, H.S.M. Coxeter and W.O.J. Moser [5] used both Cayley and Schreier diagrams to prove some results on finitely generated groups. Then in 1978, G. Higman introduced the coset diagrams for the modular group $PSL(2,Z)$. Coset diagrams defined by G. Higman for the actions of $PSL(2,Z)$ are special in a number of ways. First, they are defined for a specific group, namely $PSL(2,Z)$, which has a presentation in terms of two generators x and y. Since there are only two generators, it is possible to avoid using colours as well as the orientation of edges associated with the involution x. For y, which has order 3, there is a need to distinguish y from y^2. The 3-cycles of y are therefore represented by small triangles, with the convention that y permutes their vertices counterclockwise, while the fixed points of x and y, if any, are denoted by heavy dots. Thus the geometry of the figure makes the distinction between $x-$edges and $y-$edges obvious. We illustrate this concept in the following section.

2.4 Action of the Modular Group on $PL(F_q)$

$PGL(2,Z)$ acts on $PL(F_{19})$ by the function $\mu : PL(F_{19}) \times PGL(2,Z) \longrightarrow PL(F_{19})$ such that for all $z\epsilon PL(F_{19})$ and all $g\epsilon PGL(2,Z)$

$$((z,g)\mu,h)\mu = (z,gh)\mu$$

and for all $z\epsilon PL(F_{19})$

$$(z,1)\mu = z.$$

$(z)g$ is the image of z under the map g. This action is called the natural action of $PGL(2,Z)$ on $PL(F_{19})$. For infinite groups we consider only generators of the group, not all elements.

We can calculate the permutation representations of x, y and t as $x(z) = \frac{-1}{z}$, $y(z) = \frac{z-1}{z}$, $t(z) = \frac{1}{z}$, where $z \in PL(F_{19})$.

$\overline{x} : (0\ \infty)(1\ 18)(2\ 9)(3\ 6)(4\ 14)(5\ 15)(7\ 8)(10\ 17)(11\ 12)(13\ 16)$,

$\overline{y} : (0\ \infty\ 1)(2\ 10\ 18)(3\ 7\ 9)(4\ 15\ 6)(5\ 16\ 14)(8)(12)(13\ 17\ 11)$, and

$\bar{t} : (0\ \infty)(1)(2\ 10)(3\ 13)(4\ 5)(6\ 16)(7\ 11)(8\ 12)(9\ 17)(14\ 15)(18).$

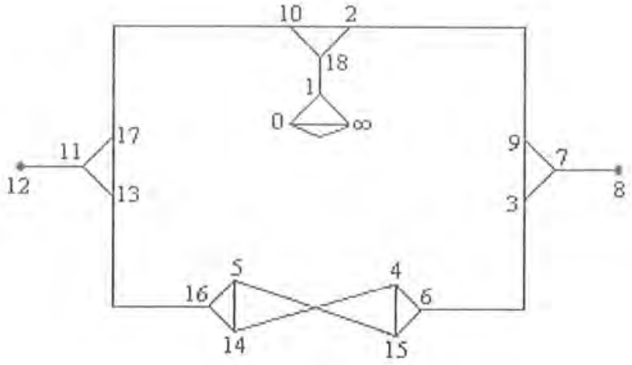


Figure 1.4

Every connected coset diagram for a finitely generated group G on a set of n points corresponds to a transitive permutation representation of G on that set, which is in fact equivalent to the natural action of G on the cosets of some subgroup H of index n. H.S.M. Coxeter and W.O.J. Moser [5] attribute these diagrams to O.Schreier.

2.5 Example

We parametrize in the following the action of $PGL(2, Z)$ on $PL(F_{11})$ as an illustration. Choose $\theta = 4$ from F_{11}. We can find a coset diagram $D(4, 11)$ associated with the non-degenerate homomorphism

$\alpha : PGL(2, Z) \rightarrow PGL(2, 11)$ as follows.

By equation (2.6), $\theta = \frac{r^2}{\Delta}$ and so $\theta = 4$ implies that $r^2 = 4\Delta$. Since 4 is a square, therefore Δ is a square also. So, we can assume that $\Delta = 1$ so that $r = \pm 2$. Let us choose $r = 2$ and substitute these values of Δ and r in equation (2.5) to obtain $s^2 = \frac{-1}{k}$. By letting $k = -1$, we can make the right hand side of this equation a square so that we can choose $s = 1$. Similarly, if we let $d = 0$, the equation (2.2) yields $f = \pm 1$. Without any loss of generality, we can choose $f = 1$ and substitute the values of r, s, d, k and f in equations (2.3) and (2.4), to obtain

$$2 = a - 2c$$

$$1 \;=\; 2a - c$$

solving these equations for a and c, we get $a = 0$ and $c = -1$. Thus,

$$X = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \text{and} \quad Y = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

So we can take $\overline{x}$ as the transformation $z \longrightarrow \frac{-1}{z}$, $\overline{y}$ as the transformation $z \longrightarrow \frac{-1}{z-1}$ and $\overline{t}$ as the transformation $z \longrightarrow \frac{1}{z}$. We can calculate the permutation representations of $\overline{x}$, $\overline{y}$ and $\overline{t}$ as

$$\overline{x} : (0\ \infty)(1\ 10)(2\ 5)(3\ 7)(4\ 8)(6\ 9),$$

and

$$\overline{y} : (0\ \infty\ 1)(2\ 10\ 6)(3\ 5\ 8)(4\ 7\ 9),$$

$$\overline{t} : (0\ \infty)(2\ 6)(3\ 4)(5\ 9)(7\ 8).$$

The associated diagram $D(4, 11)$ is given below.

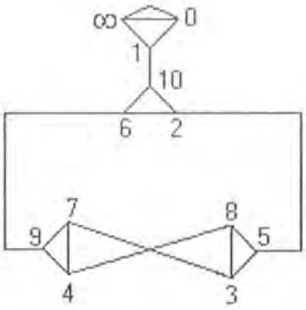


Figure 2.3

Chapter 3

Number of Subgroups of PSL(2, Z)

3.1 Coset Diagrams for the action of $PSL(2, Z)$ on $PL(F_p)$

We have considered transitive actions of $PSL(2, Z)$ on $PL(F_p)$, where p is prime. The coset diagrams for the action of $PSL(2, Z)$ on $PL(F_p)$ and their one to one correspondence as the conjugacy classes of non-degenerate homomorphisms $\alpha : PSL(2, Z) \longrightarrow PSL(2, p)$, discussed in chapter 2 are an alternative description of the legitimate pairs and the equivalence relation in [15] and [8].

By $D(\theta, p)$ we shall mean a coset diagram depicting the conjugacy class of actions of $PSL(2, Z)$ on $PL(F_p)$ corresponding to $\theta \in F_p$.

A coset diagram which consists of $(p + 1)$ vertices labelled by the elements of $PL(F_p)$, together with fixed points of x and y, triangles and edges such that

(a) each vertex has a fixed point of y or is a vertex of precisely one triangle,

(b) each vertex has a fixed point of x or is an end of precisely one edge,

(c) the edges and triangles give a connected figure,

is called a diagram of order $(p + 1)$. We will consider only connected coset diagrams.

Let Γ be the set of diagrams of order $(p + 1)$. A permutation σ of $PL(F_p)$ induces a map $\Gamma \rightarrow \Gamma$, which we also denote by σ. For D, D$'$ $\epsilon\Gamma$, we say D is equivalent to D$'$if there is a permutation $\sigma$of $PL(F_p)$ with $\sigma\,(l) = l$, $(l\epsilon PL(F_p)$ as the special element) and $\sigma\,$(D) =D$'$.

We take $PSL(2, Z)$ as the free product of C_2 and C_3, the cyclic groups of order 2 and 3. By the Kurosh subgroup theorem, a subgroup of $PSL(2, Z)$ is the free product of L_x copies of

C_2, L_y of C_3 and L_∞ of C_∞. If a subgroup has a finite index, then L_x, L_y and L_∞ are finite, and the index $p+1$ is given by

$$p+1 = 3L_x + 4L_y + 6(L_\infty - 1). \tag{3.1}$$

A subgroup will be free if and only if $L_x = L_y = 0$.

We have taken action of $PSL(2, Z)$ on $PL(F_p)$. If $\pi = \{v_0, e_1, v_1, e_2, ..., e_k, v_k\}$ is an alternating sequence of vertices and edges of a coset diagram, then π is a path in the diagram, joining v_0 and v_k, if e_i joins v_{i-1} and v_i for each i and $e_i \neq e_j (i \neq j)$.

A coset diagram is called connected if any two vertices in the diagram are joined by a path.

The order of coset diagram obtained by the action of $PSL(2, Z)$ on $PL(F_p)$ has order $p+1$. We will prove that the number of triangles that is., m is $\lfloor \frac{p+1}{3} \rfloor$ with vertices labelled by elements of $PL(F_p)$. For L_∞ such that $2m + 2 \geq L_\infty \geq 0$, we can make a connected figure by adding edges between $m + L_\infty - 1$ disjoint pairs of vertices. Let $\tau(L_\infty, m)$ be the set of such figures, in which there are no fixed points of y, two being distinct if a pair of vertices are joined by an edge in one, but not in the other. Let $T(L_\infty, m) = |\tau(L_\infty, m)|$.

For $F \epsilon \tau(L_\infty, m)$, the vertex x of F is free if it is not involved in an edge.

In the language of diagrams, [15] and [8] contains the following results:

Theorem 4 *(i) There is a one to one correspondence between subgroups of index $p+1$ in $PSL(2, Z)$ and equivalence classes of diagrams of order $p+1$. (ii) If a subgroup has L_x copies of C_2, L_y copies of C_3, then a corresponding diagram has L_x fixed points of x and L_y fixed points of y.*

Lemma 5 *An equivalence class of diagrams of order $p+1$ has $p!$ elements.*

Lemma 6 *Suppose that m and L_∞ are positive integers with $m \geq 2L_\infty - 2$. The number of subgroups of type $(3m, m - 2L_\infty + 2, 0, L_\infty)$ is*

$$\frac{T(L_\infty, m)}{3^{m-1}(m-1)!}.$$

Proposition 7 *For $m \geq \max\{2, 2L_\infty - 1\}$,*

$$T(L_\infty, m) = \frac{6m(2m - L_\infty - 1)}{(m - 2L_\infty + 2)} T(L_\infty, m - 1)$$

Directly from the definition, $T(0,1) = 1$ and $T(1,1) = 3$.

Proposition 8 *The number of elements in $\tau(0,m)$ are*

$$T(0,m) = 3^m (2m)! / (m+2)!, T(1,m) = \frac{1}{4} 12^m (m-1)!.$$

We put $N_f(p+1)$ for the number of free subgroups of index $p+1$. Such a subgroup has $L_x = L_y = 0$, so that $p+1 = 6k$, k is positive integer, with $m = 2k$, $L_\infty = k+1$, from equation (3.1) .Thus

$$N_f(p+1) = \frac{T(k+1, 2k)}{3^{2k-1}(2k-1)!}$$

by lemma (6) .

For $L_\infty \geq 2$, we put $T_{L_\infty} = N_f(6(L_\infty - 1))$. By [15] $T_2 = 5$.

Proposition 9 *For $L_\infty > 2$,*

$$T_{L_\infty} = 6(L_\infty - 1) T_{L_\infty - 1} + \sum_{i=2}^{L_\infty - 2} T_i T_{L_\infty - 1}.$$

Theorem 10 *No non-trivial linear fractional transformation of $PGL(2, Z)$ can fix more than two elements of $PL(F_p)$* [11] .

Theorem 11 *The linear fractional transformation $x : z \longrightarrow \frac{-1}{z}$ has fixed vertices in $D(\theta, p)$ if and only if -1 and θ are either both squares or both non-squares in F_p* [12] .

From above results following results are deduced:

Proposition 12 *Let p be a prime number. Let $D(\theta, p)$ be a coset diagram for the transitive action of $PSL(2, Z)$ on $PL(F_p)$, with m triangles and $p + 1 - 2m + L_\infty - 1$ edges. then*

1. $m = \lfloor \frac{p+1}{3} \rfloor$,

2. if one of -1 or θ is a square in F_p and other is not, then $L_\infty = \frac{1}{2}\{4\lfloor \frac{p+1}{3} \rfloor - p + 1\}$,

3. if -1 and θ are either both squares or both non-squares in F_p, then $L_\infty = \frac{1}{2}\{4\lfloor \frac{p+1}{3} \rfloor - p - 1\}$.

Proof. (1) Since each vertex has a fixed point of y or is a vertex of precisely one triangle, the triangles are distinct, $m \leq \frac{p+1}{3}$, the remaining vertices that cannot be a vertex of triangle has a fixed point of y. So $(p+1) - 3\lfloor \frac{p+1}{3} \rfloor$ vertices not in triangles must have fixed points of y, this shows $m = \lfloor \frac{p+1}{3} \rfloor$.

(2) From theorem(11) coset diagrams contains fixed point of x that is, L_x if and only if -1 and θ are either both squares or both non-squares in F_p, so when it is not then $L_x = 0$. We have

$$\begin{aligned} L_x &= (p+1) - 2\{p + 1 - 2\lfloor \frac{p+1}{3} \rfloor + L_\infty - 1\} \\ &= 4\lfloor \frac{p+1}{3} \rfloor - 2L_\infty - p + 1 \end{aligned}$$

Put $L_x = 0$,

$$4\lfloor \frac{p+1}{3} \rfloor - 2L_\infty - p + 1 = 0$$

This implies that

$$L_\infty = \frac{1}{2}\{4\lfloor \frac{p+1}{3} \rfloor - p + 1\}$$

(3) Since $m = \lfloor \frac{p+1}{3} \rfloor$, the $(p+1) - 3\lfloor \frac{p+1}{3} \rfloor$ vertices not in triangles must have fixed points of y, that is,

$$L_y = p + 1 - 3\lfloor \frac{p+1}{3} \rfloor.$$

Since we are considering connected coset diagrams, there must be at least $\lfloor \frac{p+1}{3} \rfloor - 1$ edges joining vertices of distinct triangles and $p + 1 - 3\lfloor \frac{p+1}{3} \rfloor$ further edges each joining a vertex with a fixed point of y to a vertex of a triangle. The fixed points of x are

$$L_x = (p+1) - 2\{p + 1 - 2\lfloor \frac{p+1}{3} \rfloor + L_\infty - 1\}$$

$$= 4\lfloor\frac{p+1}{3}\rfloor - p - 2L_\infty + 1 \tag{3.2}$$

According to theorem (11), $D(\theta, p)$ contains fixed points of x because -1 and θ are either both squares or both non-squares in F_p. From theorem (10) since no non-trivial linear-fractional transformation fixes more than two vertices of $PL(F_p)$, we have $L_x = 2$.

L_x cannot be one due to vertical symmetry. By substituting $L_x = 2$ in equation (3.2) ,

$$2 = 4\lfloor\frac{p+1}{3}\rfloor - p - 2L_\infty + 1$$

Hence

$$L_\infty = \frac{4\lfloor\frac{p+1}{3}\rfloor - p - 1}{2}.$$

■

Theorem 13 *Let $D(\theta, p)$ be a coset diagram for the action of $PSL(2, Z)$ on $PL(F_p)$. Then the number of subgroups for the coset diagrams of order $p+1$ are:*

1.

$$N(p+1) = \frac{p+1}{3^{\lfloor\frac{p+1}{3}\rfloor}\lfloor\frac{p+1}{3}\rfloor!}T(\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p + 1\},\ \lfloor\frac{p+1}{3}\rfloor),$$

provided -1 or θ is a square in F_p.

2.

$$N(p+1) = \frac{(p+1)\ (p+3-3\lfloor\frac{p+1}{3}\rfloor)!}{2\times 3^{\lfloor\frac{p+1}{3}\rfloor}\ \lfloor\frac{p+1}{3}\rfloor!(\ p+1-3\lfloor\frac{p+1}{3}\rfloor\ )!}T(\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p - 1\},\ \lfloor\frac{p+1}{3}\rfloor),$$

provided -1 and θ are either both squares or both non-squares in F_p.

Proof. (1) From proposition (12) we have

$$L_\infty = \frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p + 1\},\ m = \lfloor\frac{p+1}{3}\rfloor.$$

Using the elements of $PL(F_p)$, we can label $\lfloor\frac{p+1}{3}\rfloor$ oriented triangles in

$$\frac{(p+1)!}{3^{\lfloor\frac{p+1}{3}\rfloor}\ \lfloor\frac{p+1}{3}\rfloor!(\ p+1-3\lfloor\frac{p+1}{3}\rfloor\ )!}$$

ways. Let $F\epsilon\tau(L_\infty, m)$ for these triangles. We take $(p+1) - 3\lfloor\frac{p+1}{3}\rfloor$ new vertices, each with a fixed point of y, labelled by the unused elements of $PL(F_p)$. Now, F has $4\lfloor\frac{p+1}{3}\rfloor - p - 2L_\infty + 1$ free vertices, as $p+1$ is $3\lfloor\frac{p+1}{3}\rfloor$ for $\tau(L_\infty, m)$, so $\lfloor\frac{p+1}{3}\rfloor - 2L_\infty + 2$ free vertices, so we can join the new vertices to $(p+1) - 3\lfloor\frac{p+1}{3}\rfloor$ of these by edges. This can be done in $(p+1-3\lfloor\frac{p+1}{3}\rfloor)!$ ways. The resulting figure becomes a diagram of order $p+1$ when we add an x-loop at each vertex still not involved in an edge. Clearly, each choice of labelling of triangles, of an element of the $\tau(L_\infty, m)$, and of addition of new vertices leads to a different diagram. Taking

$$L_\infty = \frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p + 1\}, m = \lfloor\frac{p+1}{3}\rfloor$$

and applying lemma (5) gives the result:

$$\begin{aligned} N(p+1) &= \frac{(p+1)!\,(p+1-3\lfloor\frac{p+1}{3}\rfloor)!}{3^{\lfloor\frac{p+1}{3}\rfloor}\,\lfloor\frac{p+1}{3}\rfloor!(\,p+1-3\lfloor\frac{p+1}{3}\rfloor\,)!p!}T(\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p + 1\},\ \lfloor\frac{p+1}{3}\rfloor), \\ &= \frac{(p+1)}{3^{\lfloor\frac{p+1}{3}\rfloor}\,\lfloor\frac{p+1}{3}\rfloor!}T(\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p + 1\},\ \lfloor\frac{p+1}{3}\rfloor). \end{aligned}$$

(2) From proposition (12) we have

$$L_\infty = \frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p - 1\},\ m = \lfloor\frac{p+1}{3}\rfloor.$$

Using the elements of $PL(F_p)$, we can label $\lfloor\frac{p+1}{3}\rfloor$ oriented triangles in

$$\frac{(p+1)!}{3^{\lfloor\frac{p+1}{3}\rfloor}\lfloor\frac{p+1}{3}\rfloor!(p+1-3\lfloor\frac{p+1}{3}\rfloor)!}$$

ways.

Let $F\epsilon\ \tau(L_\infty, m)$ for these triangles. We take $(p+1) - 3\lfloor\frac{p+1}{3}\rfloor$ new vertices, each with a fixed point of y, labelled by the unused elements of $PL(F_p)$. Now, F has $4\lfloor\frac{p+1}{3}\rfloor - p - 2L_\infty + 1$ free vertices, as $p+1$ is $3\lfloor\frac{p+1}{3}\rfloor$ for $\tau(L_\infty, m)$, so $\lfloor\frac{p+1}{3}\rfloor - 2L_\infty + 2$ free vertices, so we can join the new vertices to $(p+1) - 3\lfloor\frac{p+1}{3}\rfloor$ of these by edges. This can be done in

$$\frac{(p+3-3\lfloor\frac{p+1}{3}\rfloor)!}{2}$$

ways. The resulting figure becomes a diagram of order $p+1$ when we add a fixed point of x at each vertex still not involved in an edge. Clearly, each choice of labelling of triangles, of an element of the $\tau(L_\infty, m)$, and of addition of new vertices leads to a different diagram.

Taking

$$L_\infty = \frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p - 1\}, m = \lfloor\frac{p+1}{3}\rfloor$$

and applying lemma (5) gives the result:

$$\begin{aligned} N(p+1) &= \frac{(p+1)!\,(p+3-3\lfloor\frac{p+1}{3}\rfloor)!}{2\times 3^{\lfloor\frac{p+1}{3}\rfloor}\,\lfloor\frac{p+1}{3}\rfloor!(\,p+1-3\lfloor\frac{p+1}{3}\rfloor\,)!p!} T(\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p - 1\},\, \lfloor\frac{p+1}{3}\rfloor), \\ &= \frac{(p+1)\,(p+3-3\lfloor\frac{p+1}{3}\rfloor)!}{2\times 3^{\lfloor\frac{p+1}{3}\rfloor}\,\lfloor\frac{p+1}{3}\rfloor!(\,p+1-3\lfloor\frac{p+1}{3}\rfloor\,)!} T(\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p - 1\},\, \lfloor\frac{p+1}{3}\rfloor). \end{aligned}$$

■

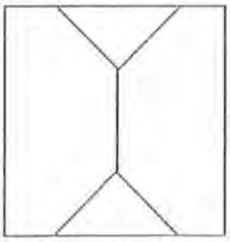
Above theorem can be restated as:

Theorem 14 *Let $D(\theta, p)$ be a coset diagram for the action of $PSL(2, Z)$ on $PL(F_p)$. Then the number of subgroups, $N(p+1)$, of $PSL(2, Z)$ are*

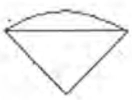
$$N(p{+}1) = \sum_{L_\infty=\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p-1\}}^{\frac{1}{2}\{4\lfloor\frac{p+1}{3}\rfloor - p+1\}} \frac{(p+1)(\lfloor\frac{p+1}{3}\rfloor - 2L_\infty + 2)!}{3^{\lfloor\frac{p+1}{3}\rfloor}\lfloor\frac{p+1}{3}\rfloor!(p+1-3\lfloor\frac{p+1}{3}\rfloor)!(4\lfloor\frac{p+1}{3}\rfloor - p - 2L_\infty + 1)!} T(L_\infty, \lfloor\frac{p+1}{3}\rfloor).$$

Theorem 15 *For any prime $p \neq 2$ the action of $PSL(2, Z)$ on $PL(F_p)$ is intransitive when $\theta = 0$.*

Proof. From the table given in [13] , when $\theta = 0$ the order of xy is 2. The only connected diagrams in which xy is of order 2 are:



(a)



(b)

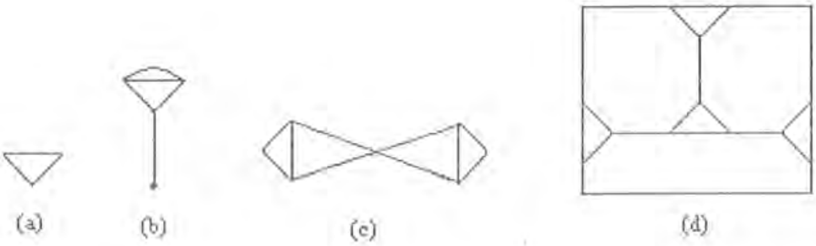
$D(0,2)$ is (b) which is connected. In $D(0,5)$, by theorem (11), the fixed points of x exist in $D(\theta,p)$ if and only if -1 and θ are either both squares or both non-squares in F_p. For $\theta = 0$, 0 is a square in F_p and -1 is congruent to 4 is a square in F_5, so $D(0,5)$ contains fixed points of x, which means that $D(0,5)$ is not the diagram (a), so is disconnected.

Obviously $D(0,p)$ for $p > 5$ contains diagrams (a) or (b) as disconnected circuits, since for this case $D(0,p)$ contains more than 2 triangles, if not as in case of $p = 7$ where number of triangles is 2 but it contains fixed points of y, which cannot be connected with diagram (a) or (b), since in that case the order of (a) or (b) will not remain 2.

Thus it is also disconnected. ■

Theorem 16 *For a prime $p \neq 2,3,5$ or 11, the action of $PSL(2,Z)$ on $PL(F_p)$ is intransitive whenever $\theta = 1$.*

Proof. From [13], we note that the order of xy is 3 if $\theta = 1$. The only connected coset diagrams in which xy is of order 3 are:



(a) exists for $D(1,2)$.

(b) exists for $D(1,3)$.

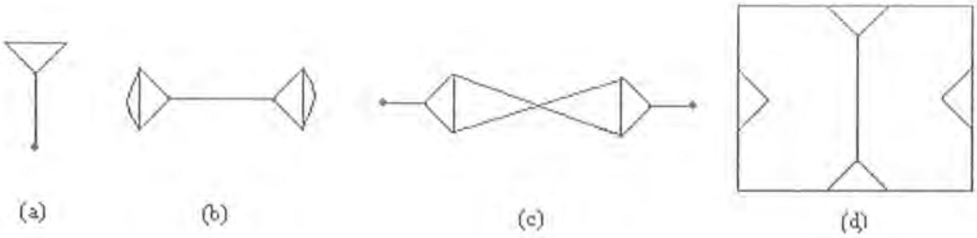
(c) exists for $D(1,5)$.

(d) exists for $D(1,11)$.

For other primes the above diagrams also exist but in form of two or more copies, so they are disconnected, since any above circuits cannot be joined by an edge because it will change the order of xy. Thus the action is intransitive. ■

Theorem 17 *For any prime $p \neq 2,3,5,7$ or 11, the action of $PSL(2,Z)$ on $PL(F_p)$ is intransitive if $\theta = 2$.*

Proof. From [13], we have that the order of xy is 4 when $\theta = 2$. The only connected coset diagrams in which xy is of order 4 are:



since $\theta = 2$ so we will not consider $p = 2$, since $\theta = 2$ is congruent to 0.

$D(2,3)$ is (a).

$D(2,5)$ is (b).

$D(2,7)$ is (c).

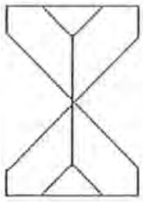
$D(2,11)$ is (d).

For other primes, the above figures also exist but in form of two or more copies, so they are disconnected, since any of the above circuits cannot be joined by an edge because it will change the order of xy. Thus the action is intransitive. ■

Theorem 18 *For any prime $p > 5$, the action of $PSL(2, Z)$ on $PL(F_p)$ is intransitive when $\theta = 3$.*

Proof. Obviously, in F_2 or F_3, $\theta = 1$ and 0, respectively, discussed earlier. From [13], we have that the order of xy is 6 when $\theta = 3$.

In this case the only connected coset diagram for xy of order 6 is:



which is $D(3,5)$. For other primes, the above figure also exists but consisting of two or more copies of $D(3,5)$, so they are disconnected, because any of the two circuits cannot be joined by an edge as it will change the order of xy. Thus the action is intransitive. ■

Chapter 4

Subgroups of S_{p+1} as Homomorphic Images of $PSL(2, Z)$

In order to determine whether an action of $PSL(2, Z)$ on $PL(F_p)$ is transitive or not, we consider its coset diagram. We take a prime p and an element θ of F_p and parametrize the action to get permutations of $\overline{x}$, $\overline{y}$ and $\overline{t}$ as discussed in chapter 2 and then apply these permutations on elements of $PL(F_p)$ to make the corresponding coset diagram. We can also check the transitivity by using the permutations and obtaining the orbits of the group action.

To compute the orbits in $PSL(2, Z)$-space $PL(F_p)$, one therefore can begin with any element z of $PL(F_p)$, apply to it the generators x, y of $PSL(2, Z)$, each in turn until one has reason to know that no new elements of $PL(F_p)$ result. By z^x or z^y we mean x and y acting on z respectively. Then $\{z, z^x, z^y, ...\}$ is a $PSL(2, Z)-$orbit that is, $Orb_1(PL(F_p))$. If $Orb_1(PL(F_p)) = PL(F_p)$ the process is finished. Otherwise we choose z_2 from $PL(F_p)\backslash Orb_1(PL(F_p))$ and we list the set $\{z_2,\ z_2^x,\ z_2^y, ...\}$ which will be our second orbit $Orb_2(PL(F_p))$.

The action of $PSL(2, Z)$ on $PL(F_p)$ is of course transitive if we get just one orbit.

For this procedure we have created the program as follows.

```
//This program takes values of prime and theta and calculates permutations of x, y, and t.
//infinity is denoted by -1.
#include<iostream.h>
#include<conio.h>
```

```
#include<math.h>
int iscomplete(int val)
{
     int getint=sqrt(val);
     float result,getfloat=sqrt(val);
     result=getfloat-getint;
     return result==0?1:0;
}
void main()
{
     clrscr();
      int p=1,a,a1,c,c1,th,f1=0,f2=0,s1=0,k=0,s=0,f=0,dt=0,r=0,d=0,nu,de,count,
     z=-1;
     int no,no1;
     do{
          cout<<"Enter Prime No as a value of P : ";
          cin>>p;
          no1=0;
          for (int i=1;i<p;i++)
               {    no=p%i;
                    if(no==0)
                    no1=no1+1;
               }
      }
     while(no1>1);
     do{
          cout<<"\nEnter the value of Theta from 0 to "<< p-1<<"\t";
          cin>>th;
      }
      while(th < 0 || th > p-1 || ( p==3 && th==0));
```

```
   if (th==0 ||iscomplete(th))
  {
        dt=1;
  }
   else
        dt=th;
  cout<<"\n delta = "<<dt;
   r=sqrt(dt*th);
  if (p==3) { r=-r; r=r+p;}
  cout<<"\n r = "<<r;
   s1=3*dt-(r*r);
   while(s1<0)
  {
        s1=s1+p;
  }
  if(s1==0||iscomplete(s1))
        k=1;
 else
        k=s1;
  cout<<"\n k = "<<k;
  s=sqrt(s1/k);
  if (p==3)
  {       s=-s;
        s=s+p;
  }
 cout<<"\n s = "<<s;
 for(d=0;d<p;d++)
 {
        f1=-(d*d)-d-1;
       while (f1<0) f1=f1+p;
```

```
    while ((f1/k)<=(p-1)*(p-1))
    {
        if(f1%k!=0)
            f1=f1+p;
        else
            break;
    }
    f2=f1/k;
    while (f2<0)
    f2=f2+p;
    while(!iscomplete(f2)&&f2<=(p-1)*(p-1))
    {
        f2=f2+p;
    }
    if (iscomplete(f2))
        break;
}
f=sqrt(f2);
if (p==3)
{     f=-f;
     f=f+p;
}
cout<<”\n d = ”<<d<<”\n f = ”<<f;
nu=(2*d+1)*r+2*k*f*s;
while (nu<0) nu=nu+p;
if (p==3)
    nu=nu/3;
else
    nu=nu%p;
    de=4*d*d+4*d+1+4*k*f*f;
```

```
while (de<0) de=de+p;
if (p==3)
      de=de/3;
 else
      de=de%p;
 a1=nu%de;
if (a1==0)
      a=nu/de;
else
{      while (nu%de!=0)
         nu=nu+p;
        a=nu/de;
 }
int nuc,dec;
 nuc=2*f*a-s;
 while (nuc<0) nuc=nuc+p;
dec=2*d+1;
 while (dec<0) dec=dec+p;
nuc=nuc%p;
dec=dec%p;
 c1=nuc%dec;
if (c1==0)
       c=nuc/dec;
else
{      while (nuc%dec!=0)
      nuc=nuc+p;
       c=nuc/dec;
 }
cout<<"\nThe value of a = "<<a;
cout<<"\nthe value of c = "<<c;
```

```
// mapping x
    const int arraysize= 100;
     cout<<”\n\nx:-”;
    int x,x1,j,q,v;
    int va[arraysize][2];
     int nux,dex;
     v=(p+3)/2;
     z=-1;
     for (j=0;j<=v;j++)
    {      if (z==p)
                break;
         va[j][0]=z;
          if (z==-1)
         {
             nux=a;
             if (c==0) {x=-1; goto again;}
            else
                 goto ag1;
         }
          nux=a*z+k*c;
          while (nux<0)
          nux=nux+p;
         dex=c*z-a;
          while (dex<0)
         dex=dex+p;
          nux=nux%p;
         dex=dex%p;
         if(dex==0)
         {    x=-1;
              goto again;
```

```
        }
        while (nux%dex!=0)
             nux=nux+p;
         x =nux/dex;
again:   va[j][1]=x;
        cout<<" ("<< va[j][0]<<" "<<va[j][1]<<")";
ag1:    z=z+1;
        count=0;
        while (count<=j)
        {
              for (q=0;q<=j;q++)
              {       if (z==va[q][1])
                             z=z+1;
              }
              count=count+1;
        }
   }
//mapping y
    cout<<"\n\ny:-";
   int va2[68][3];
    int y,v1,v2,v3,fly=0,count2=0,j2,nux2,dex2,q2;
    z=-1;
    v1=(p+1)/3;
    v2=(p+1)%3;
   v3=v1+v2;
    for(j2=0;j2<v3;j2++)
   {     fly=0;
         va2[j2][0]=z;
          if (z==p)
               break;
```

```
again3:  if (z==-1)
         {     nux2=d;
               dex2=f;
               while(nux2%dex2!=0)
                    nux2=nux2+p;
              y=nux2/dex2;
              goto again2;
          }
         nux2=d*z+k*f;
         while(nux2<0)
              nux2=nux2+p;
         dex2=f*z-d-1;
          while(dex2<0)
         dex2=dex2+p;
          nux2=nux2%p;
         dex2=dex2%p;
         if(dex2==0)
          {    y=-1;
              goto again2;
         }
         while(nux2%dex2!=0)
              nux2=nux2+p;
         y=nux2/dex2;
         if(fly==1) va2[j2][2]=y;
again2:  if (fly==0)
         {    va2[j2][1]=y;
              z=y;
          }
         if(fly==0&&y!=va2[j2][0])
         {    fly=1;
```

```
          goto again3;
      }
      else
          va2[j2][2]=y;
       cout<<" ("<<va2[j2][0]<<" "<<va2[j2][1]<<" "<<va2[j2][2]<<" )";
       z=j2;
      while(count2<=j2)
      {      for(q2=0;q2<=j2;q2++)
          {    if(z==va2[q2][0])
                    z=z+1;
                if(z==va2[q2][1])
                    z=z+1;
                 if( z==va2[q2][2])
                     z=z+1;
          } //end of for
          count2=count2+1;
       } //end of while
      count2=0;
   } //end of for
//mapping t
   cout<<"\n\nt:-";
    int t,j1,nux1,dex1,count1,q1;
   int va1[arraysize][2];
   z=0;
   for (j1=0;j1<v;j1++)
   {    if (z==p)
             break;
        va1[j1][0]=z;
        nux1=-k;
        while (nux1<0)
```

```
                nux1=nux1+p;
            dex1=z;
           nux1=nux1%p;
           if(dex1==0)
           {     t=-1;
                goto again1;
            }
            while (nux1%dex1!=0)
            nux1=nux1+p;
           t =nux1/dex1;
  again1:  va1[j1][1]=t;
           cout<<” (”<< va1[j1][0]<<” ”<<va1[j1][1]<<”)”;
            z=z+1;
           count1=0;
            while (count1<=j1)
            {      for (q1=0;q1<=j1;q1++)
                {      if (z==va1[q1][1])
                              z=z+1;
                }
                count1=count1+1;
            }
      }//end of for
      getch();
}//end of main.
```

References

1. G. Baumslag. J. W. Morgan and Peter B. Shalen, Generalized triangle groups, Math. Proc. Camb. Phil. Soc., 102, 1987, 25 – 31.

2. W. Bunrside. Theory of groups of finite order, Dover Publications, Inc. New York, 2nd ed., 1955.

3. A. Cayley, The theory of groups: graphical representations, Amer. J. Math., 1, 1878, 174 – 176.

4. M. D. E. Conder, Some results on quotients of triangle groups, Bull. Austral. Math. Soc., 30, 1984, 73 – 90.

5. H.S.M. Coxeter and W.O.J. Moser, Generators and relations for discrete groups, Springer Verlag, 4th ed.. 1980.

6. B. Fine and G. Rosenberger, A note on generalized triangle groups, Abh. Math. Sem. Univ. Hamburg, 56, 1986, 233 – 244.

7. A. M. Macbeath, Generators of linear fractional groups, Number theory, Proc. Symp. Pure Mathematics, Amer. Math. Soc., Providence, 12, 1969.

8. M. H. Millington, Subgroups of the classical modular group, J. London Math. Soc. 1, 1970, 351 – 357.

9. Q.Mushtaq, Some remarks on coset diagrams for the modular group, Math. Chronicle, 16, 1987, 69 – 77.

10. Q. Mushtaq and F. Shaheen, Coset diagrams for a homomorphic image of $\triangle(2,3,6)$, Ars Comb., 23A, 1987, 187 – 193.

11. Q.Mushtaq, The extended modular group acting on the projective line over a Galois field, Indian J. Pure Appl. Math., 20(8), 1989, 755 – 760.

12. Q. Mushtaq, Coset diagrams for Hurwitz groups, Comm. Algebra, 18(11), 1990, 3857 – 3888.

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

14. R. Steinberg, Finite reflection groups, Trans. Amer. Math. Soc., 91, 1959, 493 – 504.

15. W.W.Stothers, The number of subgroups of given index in the modular group, Proc. Royal Soc. Edin., $78A$, 1977, 105 – 112.

16. J.H.C. Whitehead, On certain sets of elements in a free group, Proc. London Math. Soc., 2(41), 1936, 48 – 56.