2†7

COSET DIAGRAMS FOR A TWO GENERATOR GROUP

by

Farhana Shaheen

Supervised by

Dr. Qaiser Mushtaq

Department of Mathematics
Quaid-i-Azam University
Islamabad

(1991)

To my nephews

COSET DIAGRAMS FOR A TWO GENERATOR GROUP

By

Farhana Shaheen

A thesis submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the subject of Mathematics.

COSET DIAGRAMS FOR A TWO GENERATOR GROUP

ABSTRACT

We study the actions of the group $G(2,n)$ with presentation $\langle x,y,t : x^2=y^n=t^2=(xt)^2=(yt)^2 = 1\rangle$ on the projective lines over the Galois Fields F_q with the help of coset diagrams $D(\vartheta,q,n)$. Specifically, we show that associated to these actions there are coset diagrams $D(\vartheta,q,n)$. These coset diagrams are graphs whose vertices belong to the projective lines over a Galois field F_q. We have parametrized these actions also. Finally, using the coset diagrams $D(\vartheta,q,6)$ we have proved the following result: Let $n = p + 1$, where p is a prime such that 6 and 12 are squares in F_p and $n = 2(1 + r)$, for a prime r. Then for all such n, both the alternating group A_n and symmetric group S_n occur as homomorphic images of the group $\Delta(2,6,6)$ with presentation

$$\langle x,y,t : x^2= y^6=(xy)^6= t^2=(xt)^2=(yt)^2= 1\rangle .$$

CONTENTS

ACKNOWLEDGEMENTS

It is a pleasure to thank my supervisor Dr.Qaiser Mushtaq under whose learned guidance this thesis has been prepared. I feel honoured being his first Senior Research Assistant. I admire his encouragement and guidance over the last three years, especially in moments of depression (when one feels almost like giving up).

I am also thankful to Dr.Asghar Qadir, the Chairman of our Department, for his help from time to time.

Sincere thanks to Professor Graham Higman F.R.S. and Dr.Gareth Jones for their valuable suggestions and guidance through personal correspondence.

I express my gratitude to my parents from the depth of my heart for all the help and assistance, plus the encouragement given to me throughout my research work. Without their moral support I would have never been able to complete my work.

My special thanks to R.Jahangiri for his help throughout. Not forgetting my colleagues for their full cooperation and help, I thank them all warmly.

FARHANA SHAHEEN

PREFACE

A coset diagram is a graphical representation of a permutation action of a finitely generated group. Graham Higman propounded the idea of coset diagrams for the (2,3,7) triangle group. He used these diagrams to prove that the alternating group A_n is a Hurwitz group for all but many positive integers n.

Q. Mushtaq has studied extensively coset diagrams for the actions of the extended modular group on the projective lines over Galois fields and has laid the foundations for the study of such diagrams. I have generalized many of the results contained in his D.Phil. thesis.

The thesis comprises five chapters. **Chapter 1** gives a brief discussion about the coset diagrams and also contains some discussion of the polyhedral groups and the coset diagrams related to them.

In **Chapter 2**, we have proved that associated to an action of $G(2,n) = \langle x,y,t: x^2 = y^n = t^2$

$=(xt)^2 = (yt)^2 = 1>$ on the projective lines over Galois fields F_q, there is a coset diagram. We have in fact parametrized, with the elements ϑ of F_q, the actions of $G(2,n)$ on $PL(F_q)$, the projective lines over finite fields F_q. Also for each such action we have developed a method to construct a coset diagram $D(\vartheta,q,n)$.

A fragment γ of a coset diagram is a pair of closed connected paths in the coset diagram which share a common vertex. We study the coset diagrams for the actions of the group $G(2,n)$ on $PL(F_q)$ and we find conditions for the existence of suitable fragments in such diagrams.

Coset diagrams arising from the non-degenerate actions of $G(2,n)$ on $PL(F_q)$ may be thought of as being composed of fragments, these fragments themselves being composed of a single circuit, or a number of circuits. These fragments are very useful in determining the group actions.

In **Chapter 3**, we have found conditions for the existence of certain standard simple circuits in $D(\vartheta,q,n)$, which occur quite frequently in $D(\vartheta,q,n)$. We have also considered the circuits in

$D(\vartheta,q,n)$ having fixed points of $\bar{x}$, $\bar{y}$, $\overline{xy}$ and $\bar{t}$, where $\bar{x}$, $\bar{y}$, $\bar{t}$ are all in $PGL(2,q)$.

The cases for the existence of more than one circuit in the coset diagrams $D(\vartheta,q,n)$ have been discussed in **Chapter 4**. We have in fact proved that: given a fragment γ of a coset diagram, there is a polynomial f in $\mathbb{Z}(z)$ such that if γ occurs in $D(\vartheta,q,n)$, then $f(\vartheta) = 0$. A converse is obtained by considering the actions of $G(2,n)$ on $F_{q^2} \cup \{\infty\}$.

The group $G(2,6)$ is an important one. We have shown applications of theorems, proved in the preceding chapters, by considering an action of $G(2,6)$ on $PL(F_q)$, where q is an odd prime. We have discussed some standard fragments of the coset diagrams for these actions in **Chapter 5**. Existence of some special types of fragments in $D(\vartheta,q,n)$ can be very useful. Conditions for the existence of some special types of fragments in $D(\vartheta,q,6)$ have been used to study an action of $\Delta(2,6,6) = \langle x,y: x^2 = y^6 = (xy)^6 = 1\rangle$ on $PL(F_q)$. Finally, by using coset diagrams for the triangle groups $\Delta(2,6,6)$, we have proved the following result: For a family of positive integers n, both the alternating and symmetric groups occur as homomorphic images of the group $\Delta(2,6,6)$.

A paper containing results from Chapter 2 has been submitted to a journal for consideration of publication. Another paper containing the results in Chapter 3 has been accepted in **Japonica Mathematica**.

The results embodied in Chapter 4 have recently been accepted in **Journal of Algebra**. One separate paper, comprising results of Chapter 5 has been accepted for publication in **Discrete** Mathematics.

CHAPTER ONE
GROUPS WITH GRAPHICAL REPRESENTATIONS

1.1 Introduction

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 e.g. [2], [3], [4], [9], [14] and [20]). 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 efficientway (see e.g., [3], [22] and [24]).

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 like W.Burnside [2], H.Coxeter and W.Moser [9], M.Dehn [10], A.Hurwitz [14], O.Schreier [22], J.Whitehead [28], etc., contributed seminal papers containing graphical representations of groups. In 1978, G.Higman propounded the idea of coset diagrams for the modular group. M.Conder [4] and Q.Mushtaq [19] in their separate works, have used these diagrams to solve certain 'Identification Problems' concerning Hurwitz groups.

In our next section we give a brief discussion about the *coset diagrams* and the works that have been done to prove certain important results using these diagrams.

1.2 Coset Diagrams

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 w (say), are joined by an S_i-edge, directed from v to w, whenever v S_i= w. It may well happen that v S_i= v, in which case the v-vertex is joined to itself by an S_i-loop or a fixed point.

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 of course a generalization of the Cayley colour graph corresponding to a (finite) presentation for G. 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 15 points) given by assigning permutations

x acting as (5,7)(10,12)

y acting as (1,6,11)

z acting as (1,2,3,4,5)(6,7,8,9,10)
(11,12,13,14,15)

This can be represented by the following diagram.

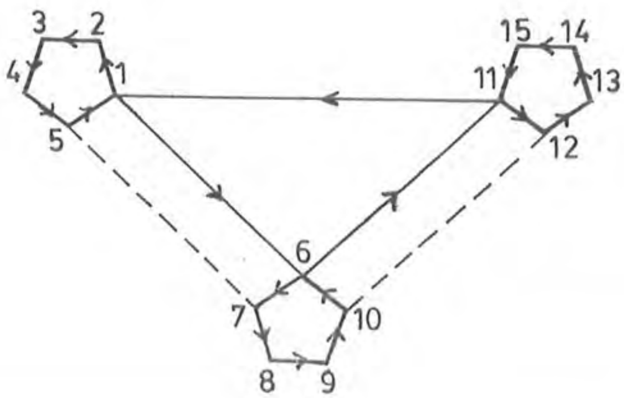

Figure 1

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 [22] generalized this notion by considering a graph whose vertices represent the cosets of any subgroup. In 1965, H. Coxeter and W. Moser [9] 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) = $<x,y : x^2 = y^3 = 1>$. This diagram is, in fact, a graphical way of representing a permutation action of the groups PSL(2,ℤ) or PGL(2,ℤ) with presentation

$$<x,y,t : x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1 >.$$

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. Coxeter and Moser [9] attribute these diagrams to Schreier. G. Higman has considered the special case of the modular group and has found that coset diagrams for this particular group could be used to show that for all n, large enough, the alternating group A_n can be generated by the elements x and y satisfying the relations $x^2 = y^3 = (xy)^7 = 1$.

We define coset diagrams for the two generator group $H(2,n)$, with presentation

$$\langle x,y : x^2 = y^n = 1\rangle \qquad (1.2.1)$$

as a graph which consists of a set of edges and n-gons. They are called coset diagrams because the vertices of the n-gons can be identified with cosets of the group. The actions of x and y are best illustrated by a coset diagram, in which the n-cycles of y are represented by n-sided polygons (whose vertices are permuted in an anti-clockwise fashion), and with the remaining edges indicating the cycles of the involution x. The fixed points of y are denoted by heavy dots; and to make the diagram less complicated, the loops representing the fixed points of x are omitted.

In our subsequent work, we have defined coset diagrams for the group $H(2,n)$ defined by (1.2.1) or the extended group $G(2,n)$ with presentation

$$\langle x,y,t: x^2= y^n= t^2 = (xt)^2=(yt)^2 = 1\rangle. \qquad (1.2.2)$$

Note that in this case the action of t is represented by reflection in the vertical axis of symmetry.

Steinberg [24] has proved that all finite simple groups of Lie type are two generator groups. It is also generally known that many, if not all, known finite simple groups are groups of Lie type. This means that all but a finite number of finite simple groups are two generator groups. The coset diagrams, defined for the group $H(2,n)$ or $G(2,n)$, thus can be useful in studying certain finite simple groups.

In the following, the notation $\Delta(k,l,m)$ shall indicate the triangle group with presentation $\langle x,y : x^k = y^l = (xy)^m = 1\rangle$ as defined by Coxeter and Moser in [9]. Also by $\Delta^*(k,l,m)$, we shall mean the extended triangle group with presentation

$$\langle x,y,t : x^k = y^l = t^2 = (xy)^m = (xt)^2 = (yt)^2 = 1\rangle.$$

In 1977, W. Stothers [25] has worked on subgroups of the triangle group $\Delta(2,3,7)$ using coset diagrams. With a subgroup of finite index in $\Delta(2,3,7)$, he associates a quintuple of non-negative integers (u,p,e,f,g) with $u \geq 1$ and $u = 84(p-1) + 21e + 28f + 36g$. He has shown that, with three exceptions, each quintuple satisfying the conditions corresponds to a subgroup. The proof uses coset diagrams and an analogous method of 'composition' of similar or different diagrams by handles.

It is well-known now that the Finite Simple Groups are classified into four categories, namely; (i) Sporadic Groups, (ii) Groups of Lie type, (iii) Cyclic groups of prime order and (iv) Alternating groups of degree n, where $n \geq 5$.

In 1978, G.Higman discovered that for all sufficiently large integers n the alternating group A_n can be generated by elements x,y satisfying the relations $x^2 = y^3 = (xy)^7 = 1$. He proved this by using a method for construction of transitive permutation representations of the triangle group $\Delta(2,3,7)$ of arbitrarily high degree, together with a clever argument based on a theorem of Jordan [29]. The work was never properly published. In 1980, then M.Conder [5] generalized this problem and proved certain results using coset diagrams. Specifically he proved that for $n > 167$, the symmetric group S_n is a homomorphic image of the infinite group

$$<x,y,t:\ x^2 = y^3 = t^2 = (xy)^7 = (xt)^2 = (yt)^2 = 1>. \qquad (1.2.3)$$

In his doctoral thesis [4], he has considered two-element generation of certain permutation groups, especially for finite alternating and symmetric groups. With the help of coset diagrams he has proved that if k is any integer greater than six, then all but finitely many of the alternating groups A_n can be generated by elements x,y which satisfy the relations

$$x^2 = y^3 = (xy)^k = 1. \qquad (1.2.4)$$

Also if k is even then the same is true for all but finitely many of the symmetric groups S_n. Most part of the thesis is devoted to showing that all but 64 of the alternating groups are Hurwitz groups. Note that a Hurwitz group is any finite non-trivial quotient of the triangle group $\Delta(2,3,7)$.

In [6], M.Conder has used the method of W.Stothers and G.Higman to show that for all but finitely many positive integers n, both the alternating group A_n and the symmetric group S_n occur as quotients of $G^{6,6,6}$ with presentation

$<x,y,t:x^2= y^6=(xy)^6= t^2=(xt)^2=(yt)^2=(xyt)^6=1>$.

In 1983, Q. Mushtaq [20] studied the coset diagrams for the modular group extensively and proved that for each element ϑ of a finite field F_q, where q is a prime-power, there exists a coset diagram for the natural permutation action of $PGL(2,\mathbb{Z})$ on $PL(F_q)$, the projective line over F_q containing the elements of F_q together with the additional point ∞. The thesis contains also some partial answers concerning the 'Reconstruction Conjecture'. That is, the way a diagram is reproducible from certain types of sub-diagrams or fragments. If we have certain fragments of a coset diagram, we can find the conditions for the existence of those fragments in the respective coset diagram. The condition in fact is a polynomial in $\mathbb{Z}[z]$. The modular group $PSL(2,\mathbb{Z}) = <x,y: x^2= y^3= 1>$ has many important homomorphic images. For many reasons connected with PGL(2,q) actions on surfaces it is important to know when PGL(2,q) is an image of the extended modular group $PGL(2,\mathbb{Z})$. The solution to that has been given in [20].

We study the coset diagrams for the actions of $G(2,n)$ on projective lines over finite fields and we find conditions for the existence of suitable fragments in such diagrams. Q.Mushtaq [20] laid the foundations for this study, in the case $n = 3$. We have extended his work to the cases in which $n > 3$, assuming that the characteristic p, where $p > 3$, of the finite field F_q in question is prime to $2n$. For, if p is not prime to $2n$, then for any positive integer d, with $1 < d < n$, $(p,2n) = d$, implying $d|p$ and $d|2n$. But $d|2n$ implies $d|n$ (since $d\nmid 2$). Now in our case we choose n to be the least positive integer such that $y^n = 1$, so that n has no positive divisors except 1 and n itself. Hence $d = 1$. Note that the case $n = 3$ becomes a special case of it.

The coset diagrams arising from the actions of $PGL(2,\mathbb{Z})$ on $PL(F_q)$ can be thought of as composed of fragments.The fragments themselves may be composed of a single circuit or of a number of circuits. A condition for the existence of a certain fragment of a coset diagram in a coset diagram for an action of $PGL(2,\mathbb{Z})$ on $PL(F_q)$ has been found in [16]. There are special types of fragments of coset diagrams which occur quite frequently in certain coset diagrams. The conditions for their existence in coset diagrams representing the actions of a factor group of $PSL(2,\mathbb{Z})$ on $PL(F_q)$ have been given in [19].

In [23], the author has discussed the coset diagrams for the homomorphic images of the group $\Delta(2,3,k)$, which has been defined by Coxeter and Moser in [9] as the group with presentation

$$\langle x, y : x^2 = y^3 = (xy)^k = 1\rangle \qquad (1.2.5)$$

for some $k \geq 2$. In fact we use coset diagrams to determine the group $\Delta(2,3,k)$. We can observe that x has order 2 and y has order 3, (by the triangles that we choose). Also since every vertex of the coset diagram is fixed by $(xy)^k$, for some $k \geq 2$, we in fact obtain a coset diagram for the permutation representation of the group $\Delta(2,3,k)$. In order to do so, we have found a condition for the existence of a coset diagram in which every vertex is fixed by $(xy)^k$. We have studied separately [18] the particular case when $k = 6$. The case for $k = 6$ has some special properties so we have given it a separate treatment. It should be noted, however, that all such cases (where xy has order 6), the subgroup generated by x and y is either cyclic (as discussed in [18]) or an extension by C_6 of an elementary Abelian group.

In our subsequent work we have generalized many of the results of Q. Mushtaq [20], by considering the actions of the group G(2,n), defined by (1.2.2), on $PL(F_q)$, where q is a prime-power, and we have studied the coset diagrams for these actions.

Let G(2,n) be the group defined by (1.2.2). Let α be a homomorphism from G(2,n) to PGL(2,q), the group of linear-fractional transformations

$$z \longrightarrow (az+b)/(cz+d) \qquad (1.2.6)$$

with a,b,c,d in F_q and $ad-bc \neq 0$. Then α is called degenerate if $\langle\bar{y}\rangle$ is normal in PGL(2,q), where $\bar{y} = y\alpha$. Otherwise it called non-degenerate. Relationships between the non-degenerate homomorphisms α and the parameters ϑ, where $\vartheta \in F_q$, have been found in Chapter 2. The role of the parameter ϑ is also explained in this chapter.

Apart from degenerate cases, when the image of <x,y,t> in PGL(2,q) does not contain PSL(2,q), the actions will be parametrized by an element ϑ of F_q, that describes the conjugacy class in PGL(2,q) of the projective transformations representing xy. Furthermore, for suitable fragments, containing only one cycle, there will be a polynomial $f(\vartheta)$ in $\mathbb{Z}[\vartheta]$ such that the presence of the fragment is equivalent to $f(\vartheta)$ being a square in F_q; and for suitable fragments containing two independent cycles, there will be a polynomial $f(\vartheta)$ in $\mathbb{Z}[\vartheta]$ such that the presence of the fragment is equivalent to $f(\vartheta) = 0$. We have given the conditions for the existence of such circuits in Chapters 3 and 4.

We can study the properties of some group just by taking a 'patch' of a coset diagram related to that group instead of studying the whole diagram which may be of larger degree. For this purpose, we need to find the conditions for the existence of such fragments in the respective coset diagrams.

In Chapter 3, we have studied just the single circuits of coset diagrams and have found the conditions for their existence in the coset diagrams. The cases for the existence of more than one circuit, which are interconnected, in the coset diagrams have been discussed in Chapter 4. We have given a method of joining any two or more fragments. We have found conditions for the existence of certain interconnected fragments in the coset diagrams.

Since we study the coset diagrams for the actions of the group $G(2,n)$ on $PL(F_q)$, the projective lines over finite fields F_q, for a prime-power q, the degree of $G(2,n)$ is $|PL(F_q)| = q + 1$. Suppose we need to draw a coset diagram giving the transitive representations of the group $G(2,n)$ of very large degree. For a particular q, we can find the elements $f(\vartheta)$ being squares in F_q that guarantee the presence of certain fragments in the respective coset diagram. So, in a way, by joining those fragments we can finally obtain the main coset diagram giving the transitive representation of the group $G(2,n)$.

We have considered the actions of the particular group $G(2,6)$, with presentation

$$\langle x,y,t,\ x^2=y^6=t^2=(xt)^2=(yt)^2 = 1\rangle,$$

on $PL(F_q)$ and have discussed the circuits and the fragments of the coset diagrams for these actions in Chapter 5. Finally, by using the coset diagrams which depict the homomorphic images of the groups $\Delta(2,6,6)$, we have proved the following result: For a family of positive integers n, (with $n = q + 1$), both the alternating and symmetric groups occur as homomorphic images of the group $\Delta(2,6,6)$.

We now discuss the polyhedral groups and the coset diagrams related to them as follows.

1.3 Coset Diagrams and Polyhedral Groups

The triangle group $\Delta(k,l,m)$ as defined by Coxeter and Moser [9] has the presentation

$$\langle x,y,z : x^l = y^m = z^n = xyz = 1\rangle . \qquad (1.3.1)$$

Suppose S is a group with presentation

$$\langle x,y: x^k = y^l = (xy)^m = 1\rangle . \qquad (1.3.2)$$

Then (x,y) is a (k,l,m) generating pair for S, and S is a quotient of $\Delta(k,l,m)$ defined by (1.3.1). These types of groups known as polyhedral groups are discussed in detail in [9]. In our subsequent work we shall consider the particular case when x is an involution, that is, for k = 2. The group $\Delta(k,l,m)$ defined by (1.3.2) is finite if $1/k + 1/l + 1/m > 1$. These contain the dihedral group $\Delta(2,2,n)$, $S_3 \cong \Delta(2,3,2)$, $A_4 \cong \Delta(2,3,3)$, $S_4 \cong \Delta(2,3,4)$ and $A_5 \cong \Delta(2,3,5)$. For $1/k + 1/l + 1/m = 1$, we obtain the metablian group $\Delta(2,3,6)$ or $\Delta(2,4,4)$ which is infinite but soluble. The group $\Delta(k,l,m)$ is infinite and insoluble when $1/k + 1/l + 1/m < 1$. In fact this group is SQ-universal: that is, every countable group occurs as a subgroup of some quotient of $\Delta(k,l,m)$. We shall study the polyhedral groups $\Delta(2,l,m)$ with the help of coset diagrams. In fact, we are interested in studying actions of S (defined by (1.3.2)) on projective lines over Galois fields through coset diagrams.

In the case of a triangle group $\Delta(2,n,k)$, we may simplify the coset diagram by removing some of its edges , directions and even the colours. If (x,y) is a (2,n,k)-generating pair, then we may represent the n-cycles of y by (n-sided) polygons, (whose vertices are permuted anti-clockwise by y), or by heavy dots (indicating fixed points of y). Note that in our case we do not get cycles of y of length properly dividing n since we choose n to be the least positive integer satisfying $y^n = 1$, and hence we choose n-gons for the n-cycles of y. Also we draw lines (edges) to indicate the action of x (interchanging the points at the ends of each edge).

For example, consider the coset diagram for the action of the group

$$H(2,6) = \langle x,y: x^2 = y^6 = 1\rangle$$

on $PL(F_{11}) = F_{11} \cup \{\infty\}$. We choose x to be the linear fractional transformation $z \longrightarrow (-1)/z$ and y to be $z \longrightarrow (z+1)/(2-z)$. Hence x and y act as

$$(0,\infty)(1,10)(2,5)(3,7)(4,8)(6,9)$$

and

$$(0,6,1,2,\infty,10)(3,7,5,9,8,4)$$

respectively.

Thus we obtain the following diagram.

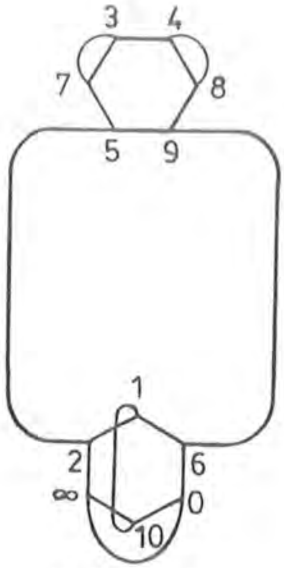

Figure 2

Every vertex is fixed by $(xy)^5$, thus giving $(xy)^5 = 1$, so that we get a homomorphic image of the group $\Delta(2,6,5)$.

Note that the diagram is not just a mean of illustrating the action of the group $\dot{H}(2,6)$ on $PL(F_{11})$, but it can be helpful when we come to examining some of its properties as well. For example, the property of the diagram being connected depicts the transitiveness of the group $\Delta(2,6,5)$. Also it is easy to read off the permutations induced by any given element of $\Delta(2,6,5)$ simply by chasing points around. For example in the above representation the element

$xy^{-1}xy$ acts as $(0,9,10,8,3,5)(1,6,\infty,2,7,4)$.

1.4 Actions of G(2,n) on $PL(F_q)$

Consider the group G(2,n) defined by (1.2.2) and let H(2,n) be its subgroup defined by (1.2.1). Let q be a prime-power. Then, as defined earlier, the group PGL(2,q) is the group of linear fractional transformations

$$z \longrightarrow (az+b)/(cz+d) \qquad (1.4.1)$$

where $a,b,c,d \in F_q$ and $ad - bc \neq 0$. Also, the group PSL(2,q) is the group of transformations (1.4.1) where $a,b,c,d \in F_q$ and $ad-bc$ is a quadratic residue in F_q. Since each element of PGL(2,q) is a permutation of $PL(F_q)$, so PGL(2,q) is a subgroup of the symmetric group S_{q+1}. The group PSL(2,q), for $q > 2$, contains only even permutations, so that it is a subgroup of A_{q+1}.

For a pair $(\bar{x},\bar{y})$, where $\bar{x},\bar{y} \in PGL(2,q)$, satisfying the relations (1.2.2), we denote by $D(\vartheta,q,n)$, where $\vartheta \in F_q$, the coset diagram corresponding to the action of the group G(2,n) on $PL(F_q)$ via a homomorphism $\alpha : G(2,n) \longrightarrow PGL(2,q)$, with parameter ϑ. We shall explain the role of ϑ in our next chapter.

As an example, consider the following coset diagram D(1,11,5) depicting an action of the group $H(2,5) = \langle x,y : x^2 = y^5 = 1\rangle$ on $PL(F_{11})$. Here we choose x,y to be the linear fractional transformations

$$x:z \longrightarrow (5z+2)/(2z-5) \text{ and } y: z \longrightarrow (2z+5)/(5z+2)$$

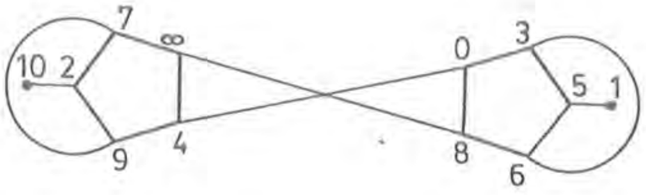

Figure 3

Here D(1,11,5) depicts the homomorphic image of $\Delta(2,5,3) = \langle x,y:x^2 = y^5=(xy)^3= 1\rangle$, isomorphic to the alternating group A_5.

CHAPTER TWO
PARAMETRIZATIONS OF NON-DEGENERATE HOMOMORPHISMS

2.1 Introduction

Let H(2,n) and G(2,n) be the groups defined by (1.2.1) and (1.2.2) respectively. Let α be a homomorphism from G(2,n) to PGL(2,q). Then α is called degenerate if $\langle\bar{y}\rangle$ is normal in PGL(2,q) = $\langle\bar{x},\bar{y},\bar{t}\rangle$. Otherwise it is called non-degenerate.
Let α be a non-degenerate homomorphism from G(2,n) to PGL(2,q) such that it maps x,y of G(2,n) to $\bar{x},\bar{y}$ of PGL(2,q). Then the images $\bar{x},\bar{y}$ of PGL(2,q), where $\bar{x} = x\alpha$, $\bar{y} = y\alpha$ satisfy the relations

$$\bar{x}^2 = \bar{y}^n = 1. \qquad (2.1.1)$$

Two homomorphisms α: G(2,n) $\longrightarrow$ PGL(2,q) and β: G(2,n) $\longrightarrow$ PGL(2,q) are said to be conjugate if there exists an inner automorphism ρ of PGL(2,q) satisfying $\beta = \alpha\rho$. In Section 2.2 we have considered the conjugacy classes of the non-degenerate homomorphisms.

We assume first that the field F_q is not of characteristic p if n happens to be the prime p. In fact we assume that the characteristic of the finite field F_q in question is prime to 2n (as given in the arguments of Section 1.1). In Section 2.3 we shall consider the cases for the field of characteristic p.

If M is a matrix mapped to the element u of PGL(2,q) by the natural map GL(2,q) to PGL(2,q), then $\vartheta = (tr(M))^2/det(M)$ is an invariant of the conjugacy class of u. We refer to it as the parameter of u, or of the conjugacy class. Here since we are considering actions of G(2,n) on $PL(F_q)$ via the non-degenerate homomorphism α, we take u to be $(xy)\alpha$. Hence ϑ is the parameter of the class represented by $\overline{x}\overline{y} = (xy)\alpha$. Now α is determined by the pair $(\bar{x},\bar{y})$ and each ϑ gives us the pair $(\bar{x},\bar{y})$, so that α is associated with the parameter ϑ. In this chapter we find a relation between the conjugacy classes of the non-degenerate homomorphisms and the parameters ϑ, (where ϑ is some element of the Galois field F_q).

In the following, we prove that there is a one to one correspondence between the conjugacy classes of non-degenerate homomorphisms of G(2,n) into PGL(2,q) and the conjugacy classes of elements of PGL(2,q) such that the correspondence assigns to any non-degenerate homomorphism α the class containing $(xy)\alpha$.

2.2 Relationship between the non-degenerate homomorphisms and the parameters

Let H(2,n) be the group satisfying the relations (2.1.1). Let α be a homomorphism from H(2,n) into PGL(2,q). Then α can be extended to a homomorphism of G(2,n), defined by (1.2.2), into PGL(2,q) if and only if we can find an element $\bar{t}$ in PGL(2,q) such that

$$\bar{t} = (\bar{t}\bar{x})^2 = (\bar{t}\bar{y})^2 = 1,$$

for $\bar{x},\bar{y}$ in PGL(2,q).

We define a pair $(\bar{x},\bar{y})$, satisfying the relations (2.1.1), in PGL(2,q) to be invertible if there exists $\bar{t}$ in PGL(2,q) such that $\bar{t}^2 = 1$, $\bar{t}\bar{x}\bar{t} = \bar{x}$ and $\bar{t}\bar{y}\bar{t} = \bar{y}^{-1}$.

To prove Lemma 2.2.2, we need a result from [20] which we state without proof.

Lemma 2.2.1

A non-singular 2x2 matrix with entries in F_q, (where q is not a power of 2), represents an involution in PGL(2,q) if and only if its trace is zero.

Lemma 2.2.2

Let $\bar{x},\bar{y}$ be the elements of PGL(2,q) such that $\bar{x}$ is of order 2 and $\bar{y}$ is of order n and let X and Y be the matrices representing $\bar{x}$ and $\bar{y}$, respectively. If r and m are the traces of XY and Y respectively, then either $r^2 = (4-m^2)\Delta$ or the pair $(\bar{x},\bar{y})$ is invertible (where Δ is the determinant of XY).

Proof

Let $\bar{x},\bar{y}$ be the elements of PGL(2,q), (where q is an odd prime-power), satisfying the relations

(2.1.1). Let the matrices corresponding to $\bar{x}$ and $\bar{y}$ be X and Y with

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } Y = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

respectively. Since $\bar{x}^2 = 1$, therefore by Lemma 2.2.1, we choose $X = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}$. Now since every element of GL(2,q) of trace zero has, upto scalar multiplication, a conjugate of the form $\begin{bmatrix} o & k \\ 1 & o \end{bmatrix}$, therefore we can assume that the matrix representing $\bar{x}$ has the form $\begin{bmatrix} o & k \\ 1 & o \end{bmatrix}$.

Also since $\bar{y}^n = 1$, Y^n is a scalar matrix and hence the determinant of Y is a square in F_q. Thus replacing Y by a suitable scalar multiple, we assume the determinant of Y to be equal to 1. So that we have $\det(Y^n) = 1$. We observe that $Y^n = I$ or $Y^n = -I$ depending upon the value of the integer n being odd or even. Let m be the trace of Y. Then the characteristic equation of Y is

$$Y^2 - mY + I = 0 . \qquad (2.2.1)$$

Thus m = e + h imply that h = m-e. Hence, we have $Y = \begin{bmatrix} e & f \\ g & m-e \end{bmatrix}$ thus giving det(Y) = e(m-e) -fg = 1. So that we have

$$1 + fg + e^2 - em = 0 . \qquad (2.2.2)$$

Now suppose that there exists an invertible element $\bar{t}$ in PGL(2,q) satisfying

$$\bar{t}^2 = (\bar{x}\bar{t})^2 = (\bar{y}\bar{t})^2 = 1. \qquad (2.2.3)$$

Let the matrix representing $\bar{t}$ be $T = \begin{bmatrix} u & v \\ w & j \end{bmatrix}$. Then, since $\bar{t}$ is an involution, we have by Lemma 2.2.1, $j = -u$ so that $T = \begin{bmatrix} u & v \\ w & -u \end{bmatrix}$.

Let XT be the matrix representing $\bar{x}\bar{t}$ of PGL(2,q). Then

$$XT = \begin{bmatrix} kw & -ku \\ u & v \end{bmatrix},$$

which by Lemma 2.2.1, implies

$$v = -kw, \qquad (2.2.4)$$

as $(\bar{x}\bar{t})^2 = 1$.

Similarly, choosing YT to be the matrix representing the element $\bar{y}\bar{t}$ of PGL(2,q), we thus obtain

$$YT = \begin{bmatrix} eu+fw & ev-fu \\ ug-w(m-e) & vg-u(m-e) \end{bmatrix}.$$

Since $\bar{y}\bar{t}$ is also an involution therefore by the arguments given above, we have

$$vg - u(m-e) = -(eu + fw),$$

which from Equation (2.2.4) gives

$$2ue + fw - kwg - um = 0.$$

That is,

$$u(2e-m) + w(f-kg) = 0. \qquad (2.2.5)$$

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

$$-u^2 + kw^2 \neq 0. \qquad (2.2.6)$$

Thus the necessary and sufficient conditions for the existence of $\bar{t}$ in PGL(2,q) are the Equations (2.2.4), (2.2.5) and (2.2.6). So that $\bar{t}$ exists in PGL(2,q) unless $kw^2 - u^2 = 0$.

If both $2e - m = f-kg = 0$, then the existence of $\bar{t}$ is trivial. If not, then

$$u/w = (f-kg)/-(2e-m),$$

and so Equation (2.2.6) is equivalent to

$$k(2e-m)^2 - (f-kg)^2 \neq 0.$$

Thus $\bar{t}$ exists in PGL(2,q) satisfying (2.2.3) unless

$$(f-kg)^2 = k(2e-m)^2 .$$

But this implies that

$$f^2+k^2g^2 - 2\,fkg = k(4e^2 + m^2 - 4em),$$

which by (2.2.2) gives

$$f^2+k^2g^2 - 2fkg = k(-4fg - 4+m^2).$$

That is,

$$f^2+k^2g^2 + 2fkg = m^2k-4k ,$$

or

$$(f+kg)^2 = -k(4-m\ )^2. \qquad (2.2.7)$$

Now

$$XY = \begin{bmatrix} kg & k(m-e) \\ e & f \end{bmatrix}$$

gives $tr(XY) = kg + f$, which we assume to be equal to r. Also, by (2.2.2), $det(XY) = kgf - kme + ke^2 = k(gf - em + e^2) = -k$. Let $det(XY) = \Delta$. So that $\Delta = -k$. Also, we have $r = kg + f$. Substituting these values in (2.2.7) we thus obtain

$$r^2 = (4 - m^2)\Delta. \qquad (2.2.8)$$

By the arguments of [20] we have that $PGL(2,q)$ contains two classes of involutions, both consisting of elements of trace zero. The classes of $PGL(2,q)$ not consisting of elements $\bar{x}$ such that $\bar{x}^2 = 1$ are in one to one correspondence with the non-zero elements ϑ of F_q. The class corresponding to ϑ consists of elements represented by matrices M with $\vartheta = r^2/\Delta$, where $r = tr(M)$ and $\Delta = det(M)$.

Remark 2.2.3

There are two classes, Cl_1 and Cl_2, of PGL(2,q) with parameter 0. Each of them is afforded by a matrix M with characteristic equation $z^2+k = 0$, where $k = \det(M)$. That is, if $k = 1$ we get Cl_1 and if k is a non-square in F_q, we get Cl_2, where both Cl_1 and Cl_2 are with the same parameter 0. If the field is of characteristic 2, there is only one class with parameter 0 and only one class of involutions.

We now define the dual homomorphism of the non-degenerate homomorphism $\alpha:G(2,n) \longrightarrow PGL(2,q)$ as follows.

Let δ be the automorphism of G(2,n) defined by $x\delta = xt$, $y\delta = y$ and $t\delta = t$. If $\alpha : G(2,n) \longrightarrow PGL(2,q)$ is a homomorphism, then $\alpha' = \delta\alpha$ is known as the dual homomorphism of α. That is, if α maps x,y,t to $\bar{x},\bar{y}$ and $\bar{t}$, then α' maps x,y,t to $\bar{x}\bar{t},\bar{y}$ and $\bar{t}$ respectively. Now since the elements $\bar{x},\bar{y},\bar{t}$ as well as $\bar{x}\bar{t},\bar{y},\bar{t}$ satisfy the relations

$$x^2= y^n= t^2=(xt)^2=(yt)^2 = 1, \qquad (2.2.9)$$

therefore the solutions of these relations occur in dual pairs. In our subsequent work we shall find a relationship between the parameters of dual homomorphisms. We first prove the following.

Lemma 2.2.4

There are just two conjugacy classes of non-degenerate homomorphisms α: $G(2,n) \longrightarrow PGL(2,q)$ in which $\bar{x}\bar{y}$ is of order 2, and two in which $\bar{x}\bar{y}\bar{t}$ is of order 2.

Proof

If $\bar{x}\bar{y}$ is of order 2, we get the dihedral group of order 2n, with presentation

$$\langle x,y : \bar{x}^2 = \bar{y}^n = (\bar{x}\bar{y})^2 = 1\rangle.$$

Let $H = \langle\bar{y}\rangle$. Then since $(\bar{t}\bar{y})^2 = 1$, $\bar{t}H = H\bar{t}$. So that $\bar{t}$ normalizes $\langle\bar{y}\rangle$ which in this case is characteristic in $\langle\bar{x},\bar{y}\rangle = D_{2n}$. That is, in this case the homomorphism α in fact maps $G(2,n)$ into the normalizer of $PGL(2,q)$ of a cyclic group of order n. This normalizer is a dihedral group of order $2(q-1)$ or $2(q+1)$ according as $q \equiv 1 \pmod{n}$ or $q \equiv -1 \pmod{n}$. Since all elements of order n in $PGL(2,q)$ are conjugate, we can take $\bar{y}$ to be a fixed element of order n. Any further conjugation must take place within $N(\langle\bar{y}\rangle)$. In this group there are two classes of non-central involutions (because $q \pm 1$ is even), and we choose $\bar{x}$ from either. Then $\bar{x}\bar{y}$ is of order 2, and centralizes $\bar{x}$ and $\bar{y}$. So it is the unique non-trivial element of the centre of $N(\langle\bar{y}\rangle)$. Thus there are just two conjugacy classes of non-degenerate homomorphisms α: $G(2,n) \longrightarrow PGL(2,q)$.

If the dual α' of α maps x,y,t onto $\bar{x},\bar{y},\bar{t}$, then $\bar{x}\bar{y} = \bar{x}\bar{t}\bar{y} = \bar{t}\bar{x}\bar{y} = \bar{t}(\bar{x}\bar{y}\bar{t})\bar{t}$. Thus if $\bar{x}\bar{y}\bar{t}$ is of order 2, so is $\bar{x}\bar{y}$. Hence if we apply the dual α' of α we in fact interchange $\bar{x}$ with $\bar{x}\bar{t}$ throughout and so the case in which $\bar{x}\bar{y}\bar{t}$ is of order 2 remains exactly the same. Hence there are two conjugacy classes of non-degenerate homomorphisms in which $\bar{x}\bar{y}\bar{t}$ is of order 2.

In our subsequent work, we choose the matrices X,Y and T representing the elements $\bar{x}$, $\bar{y}$ and $\bar{t}$ of PGL(2,q) as follows.

$$X = \begin{bmatrix} a & cl \\ c & -a \end{bmatrix}, \quad Y = \begin{bmatrix} e & fl \\ f & m-e \end{bmatrix} \text{ and } T = \begin{bmatrix} 0 & -l \\ 1 & 0 \end{bmatrix},$$

where a,c,e,f,l are elements of F_q, with $l \neq 0$. We choose $m \equiv x \pmod q$, for some x in F_q where q is an odd prime-power.

Let us denote the trace of XY by r, and let the trace of XYT be equal to ls. For the following lemma, we exclude the cases in which r = 0 and s = 0, so that by Lemma 2.2.1 we choose the elements $\bar{x}\bar{y}$ and $\bar{x}\bar{y}\bar{t}$ of PGL(2,q) not of order 2. That is, $(\bar{x}\bar{y})^2 \neq 1$ and $(\bar{x}\bar{y}\bar{t})^2 \neq 1$. Note that the two cases $\bar{x}\bar{y}$ is of order 2 and $\bar{x}\bar{y}\bar{t}$ is of order 2 are dual. Let us denote the element, whose order is not equal to 2 and whose dual is also not of order 2 by $\bar{g}$, for the following Lemma.

Lemma 2.2.5

Any element $\bar{g}$ ($\neq$1), whose order is not equal to 2 and whose dual is also not of order 2, of PGL(2,q) is the image of xy under some non-degenerate homomorphism of G(2,n) into PGL(2,q).

Proof

Using Lemma 2.2.2 we show that every non-trivial element of PGL(2,q) is a product of an element of order 2 and an element of order n. So we find elements $\bar{x}, \bar{y}$ and $\bar{t}$ of PGL(2,q) satisfying the relations

$$\bar{x}^2 = \bar{y}^n = \bar{t}^2 = (\bar{x}\bar{t})^2 = (\bar{y}\bar{t})^2 = 1.$$

Let $\bar{x}, \bar{y}$ and $\bar{t}$ be represented by the matrices:

$$X = \begin{bmatrix} a & cl \\ c & -a \end{bmatrix}, \quad Y = \begin{bmatrix} e & fl \\ f & m-e \end{bmatrix} \text{ and } T = \begin{bmatrix} o & -l \\ 1 & o \end{bmatrix},$$

where a,c,e,f,l are elements of F_q, with $l \neq 0$. Also $m \equiv x \pmod q$, for some x in F_q. Let us denote by Δ the determinant of X, so that

$$-(a^2 + lc^2) = \Delta \neq 0. \qquad (2.2.10)$$

Also, assuming the determinant of Y to be equal to 1, we have

$$1 + lf^2 + e^2 - em = 0. \qquad (2.2.11)$$

We take $\bar{x}\bar{y}$ in a given conjugacy class. The matrix representing xy is given by

$$XY = \begin{bmatrix} ae+lcf & alf+cl(m-e) \\ ce-a\ f & lcf-a(m-e) \end{bmatrix}.$$

Its trace, which we denote by r, is given by

$$r = tr(XY) = a(2e-m) + 2lfc \qquad (2.2.12)$$

Also $\det(XY) = \det(X)\det(Y) = \Delta$, as determinant of Y is assumed to be equal to 1. Let $tr(XYT) = ls$, so that

$$s = 2af - c(2e-m) . \qquad (2.2.13)$$

Hence, we have

$$r^2 + ls^2 = (4-m^2)\Delta . \qquad (2.2.14)$$

Since $\bar{g} = \bar{x}\bar{y}$ (or its dual $\bar{x}\bar{y}\bar{t}$) are not of order 2, the class to which we want them to belong do not consist of involutions, so that $(\bar{x}\bar{y})^2 \neq 1$ and $(\bar{x}\bar{y}\bar{t})^2 \neq 1$. Thus the traces of the matrices XY and XYT are not equal to zero, by Lemma 2.2.1. Hence $r \neq 0$, and $s \neq 0$, so that we have $\vartheta = r^2/\Delta \neq 0$; and it is sufficient to show that we can choose a,c,e,l,f in F_q so that r^2/Δ is indeed equal to ϑ. Now $\vartheta = r^2/\Delta$ implies that $r^2 = \vartheta\ \Delta$; so that Δ is a square if and only if ϑ is, and not if ϑ is not, and we choose it arbitrarily in F_q to satisfy the conditions, and we then choose r to satisfy $\vartheta = r^2/\Delta$. From Equation (2.2.14), we have

$$ls^2 = (4-m^2)\Delta - r^2 .$$

If $r^2 \neq (4-m^2)\Delta$, we select l according to the above argument.

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, and q is odd. In particular, e^2-em and $-lf^2-1$ each take at least $(q+1)/2$ distinct values as e and f run through F_q. Hence we can find e and f so that $e^2-em = -lf^2-1$.

Finally by substituting the values of r,s,e,f,l in Equations (2.2.12) and (2.2.13) we can find the values of a and c. Now these two equations are linear equations for a and c with determinant

$$-(2e-m)^2 - 4lf^2 = 4-m^2 \qquad (2.2.15)$$

which is non-zero, so that we can find a and c satisfying Equation (2.2.10). Hence the proof.

The conjugacy classes corresponding to the parameter $\vartheta = 0$ and $\vartheta = 4 - m^2$ are already established in Lemma 2.2.4. We want next to show that any two such non-degenerate homomorphisms, with the parameter ϑ, are conjugate.

Lemma 2.2.6

Any two non-degenerate homomorphisms α, β of $G(2,n)$ into $PGL(2,q)$ are conjugate if $(xy)\alpha = (xy)\beta$.

Proof

Let α: G(2,n) $\longrightarrow$ PGL(2,q) be the non-degenerate homomorphism such that $\overline{x}\overline{y}$ has parameter ϑ constructed as in the proof of Lemma 2.2.5. We also suppose that the non-degenerate homomorphism β: G(2,n) $\longrightarrow$ PGL(2,q) has the same parameter ϑ.

First, since there are just two classes (Remark 2.2.3) of elements of order 2 in PGL(2,q), one in PSL(2,q) and the other not, we can pass to a conjugate of β in which $t\beta$ is represented by $\begin{bmatrix} 0 & -l' \\ 1 & 0 \end{bmatrix}$ for some $l' \neq 0$ in F_q. Then because $x\beta$ and $xt\beta$ are both of order 2, $x\beta$ must be represented by a matrix $\begin{bmatrix} a' & l'c' \\ c' & -a' \end{bmatrix}$ and because $y\beta$ is of order n and $yt\beta$ is of order 2, $y\beta$ must be represented by a matrix $\begin{bmatrix} e' & l'f' \\ f' & m-e' \end{bmatrix}$, with a',c',e',f',l' satisfying the Equations (2.2.2), (2.2.5) and (2.2.6). Then $\vartheta = r'^2/\Delta' = r^2/\Delta$, $(4-m^2) - \vartheta = l's'^2/\Delta' = ls^2/\Delta$. Here $\vartheta \neq 0$, $(4-m^2) - \vartheta \neq 0$; so it follows that l'/l is a square in F_q.

Now $y\alpha$ and $y\beta$ are both of order n and so are conjugate in PGL(2,q). So we can pass to a conjugate of β (which we still call β) with $y\alpha$ =

$y\beta$. Then $t\alpha$ and $t\beta$ are involutions which invert $y\alpha$, and so belong to $N(\langle y\alpha\rangle)$. In $N(\langle y\alpha\rangle)$ there are two classes of such involutions, one in PSL(2,q) and the other not. Because $t\alpha$ is $\begin{bmatrix} 0 & -l \\ 1 & 0 \end{bmatrix}$ and $t\beta$ is conjugate to $\begin{bmatrix} 0 & -l' \\ 1 & 0 \end{bmatrix}$ and l'/l is a square, $t\alpha$ and $t\beta$ either both belong to PGL(2,q) or neither. Hence they are conjugate in $C(\langle y\alpha\rangle)$. That is, passing to a new conjugate (still called β) we can assume $y\alpha = y\beta$, $t\alpha = t\beta$. This means that in the notations above, we can assume $l = l'$, $f = f'$ and $e = e'$. We can also, by multiplying the matrix representing $x\beta$ by a scalar, assume $\Delta = \Delta'$, $r = r'$ and $s = s'$. Then the Equations (2.2.10), (2.2.11), (2.2.12) and (2.2.13) with a,c,e,f,l and then with a',c',e',f',l' ensure that $a = a'$, $c = c'$. That is $\alpha = \beta$. Hence the proof is completed.

We now put together the Lemmas (2.2.4), (2.2.5) and (2.2.6) to obtain the following.

Theorem 2.2.7

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

We now find a relationship between the parameters of the dual non-degenerate homomorphisms.

Let α be a non-degenerate homomorphism of G(2,n) into PGL(2,q) such that it maps x,y to $\bar{x},\bar{y}$. Let ϑ be the parameter of the class represented by $\bar{x}\bar{y}$. Now α is determined by $(\bar{x},\bar{y})$ and each ϑ gives us this pair $(\bar{x},\bar{y})$, so that α is associated with ϑ. We shall call the parameter ϑ of the class represented by $\bar{x}\bar{y}$, the parameter of the non-degenerate homomorphism of G(2,n) into PGL(2,q).

Now $XT = \begin{bmatrix} cl & -al \\ -a & -cl \end{bmatrix}$ implies $\det(XT) = l\Delta$, where $\Delta = -(a^2 + lc^2)$. Also,

$$(XT)Y = \begin{bmatrix} cle - alf & cl^2f - al(m-e) \\ -ae-clf & -alf-cl(m-e) \end{bmatrix}$$

implies $tr((XT)Y) = 2cle - 2alf - clm$

$$= -l(2af - c(2e-m)) = -ls.$$

Note that if $\bar{x},\bar{y},\bar{t}$ satisfy the relations

$$\bar{x}^2 = \bar{y}^n = \bar{t}^2 = (\bar{x}\bar{t})^2 = (\bar{y}\bar{t})^2 = 1 , \qquad (2.2.16)$$

then so do $\bar{x}\bar{t},\bar{y},\bar{t}$. So that the solutions of (2.2.16) occur in dual pairs. Hence replacing the solutions in Lemma 2.2.5 by $\bar{x}\bar{t}$, $\bar{y}$, $\bar{t}$, we interchange r by $-ls$ (where $r = tr(XY)$), Δ with $l\Delta$ to get the new parameter ls^2/Δ. We then find the relationship between the parameters of dual non-degenerate homomorphisms.

Let α: $G(2,n) \longrightarrow PGL(2,q)$ be a non-degenerate homomorphism satisfying the relations $x\alpha = \bar{x}$, $y\alpha = \bar{y}$ and $t\alpha = \bar{t}$. Let α' be the dual of α. As in Lemma 2.2.5, we take the matrices

$$X = \begin{bmatrix} a & cl \\ c & -a \end{bmatrix}, \quad Y = \begin{bmatrix} e & fl \\ f & m-e \end{bmatrix} \text{ and } T = \begin{bmatrix} 0 & -l \\ 1 & 0 \end{bmatrix},$$

representing $\bar{x},\bar{y}$ and $\bar{t}$, respectively, of $PGL(2,q)$. Now by Lemma 2.2.1, we have $tr(XY) = 0$ if and only if $(\bar{x}\bar{y})^2 = 1$. Also, we have $\{tr(XYT)\}/l = s = 0$ if and only if $(\bar{x}\bar{y}\bar{t})^2 = 1$. Now $det(XY) = \Delta$, thus giving the parameter of $\bar{x}\bar{y}$ equal to $r^2/\Delta = \vartheta$, say. Also since $tr(XYT) = ls$ and $det(XYT) = l\Delta$ (since $det(X) = \Delta$, $det(Y) = 1$ and $det(T) = l$), we obtain the parameter of $\overline{x}\overline{y}\overline{t}$ equal to ls^2/Δ, which we will denote by ϕ. Thus $\vartheta + \phi = r^2/\Delta + ls^2/\Delta$. Substituting the values from Equation (2.2.14), we thus obtain $\vartheta + \phi = 4 - m^2$. Thus if ϑ is the parameter of the non-degenerate homomorphism α, then $\phi = (4-m^2) - \vartheta$ is the parameter of the dual α' of α.

In Section 2.2 we have studied the actions of the group G(2,n) defined by (1.2.2) on projective lines over finite fields. In that case we have assumed the characteristic of the finite field F_q to be prime to 2n. So that we have excluded the cases where F_q is of characteristic p if n happens to be the prime p. In the following section we discuss the cases for the field of characteristic p, if n = p.

2.3 Fields of prime characteristics

In the case when the field is of characteristic 2, both $\overline{x}$ and $\overline{t}$ have a common fixed point lying on the vertical axis of symmetry. So that in this case there is a fragment which is always contained in the diagram. This case has been discussed in [20] for the coset diagrams for the actions of G(2,3) on $PL(F_q)$ as follows.

The elements $\bar{x}$ and $\bar{t}$ satisfy the relations $\bar{x}^2 = \bar{t}^2 = (\bar{x}\bar{t})^2 = 1$, and so generate a 2-group. In characteristic 2, the only irreducible linear representation of 2-group is the trivial representation, and it follows that in any projective representation there is a fixed vertex. The same case is true in general, that is when we are studying the coset diagrams for the actions of the groups G(2,n) on $PL(F_q)$, where F_q is of characteristic 2.

For example, consider the fragment of a coset diagram for the actions of G(2,5) on $PL(F_q)$, ($q = 2^r$, for some positive integer r). In this case we always obtain the fragment:

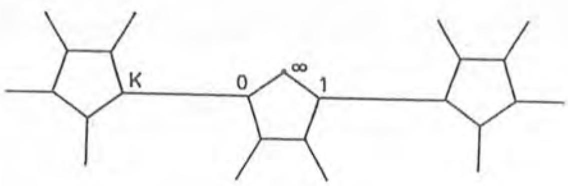

Figure 4

We recall that the labelling of the vertices of the diagram by elements of $PL(F_q)$ changes, when we pass to a conjugate homomorphism; and that the change is induced by applying to the labels an element of PGL(2,q). So that we can assume the labels ∞, 0, 1 are given to the points shown, and then take k to be the label of the vertex to which we have attached it. We observe that $\bar{x}$, $\bar{y}$ and $\bar{t}$ are the linear fractional transformations $z \longrightarrow z + k$, $z \longrightarrow -1/(z + 1)$ and $z \longrightarrow z + 1$, respectively. Let X, Y be the matrices representing $\bar{x}$, $\bar{y}$. Then,

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

thus giving $XY = \begin{bmatrix} k & -1+k \\ 1 & 1 \end{bmatrix}$, so that we have $\vartheta = (tr(XY))^2/det(XY) = k^2 + 1$. Since every element in a finite field of characteristic 2 has a unique square, we get a unique diagram for each value of ϑ.

If for the group G(2,n), defined by (1.2.2), n happens to be a prime $p > 2$, we proceed as follows.

Considering the case for the field of characteristic $p > 2$, we observe that since number of elements in $PL(F_q)$ is $p^r + 1$, for $r \geq 1$, the element $\bar{y}$ of PGL(2,q) has a unique fixed vertex. Also since $(\bar{t}\bar{y})^2 = 1$, $\bar{t}$ normalizes $\langle\bar{y}\rangle$, (where $\bar{y}^p = 1$). To make it clear, we give an example of a fragment of a coset diagram for the action of G(2,5) on $PL(F_q)$ where the field is of characteristic $p > 2$.

Consider the fragment:

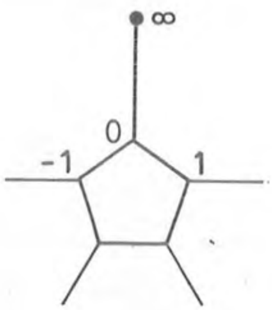

Figure 5

Here the vertex labelled ∞ is the vertex fixed by both $\bar{y}$ and $\bar{t}$ and hence lies on the vertical axis of symmetry. We assign the labels 0, 1, -1 as indicated. Then $\bar{x}$, $\bar{y}$, $\bar{t}$ are the linear fractional transformations $z \longrightarrow a/z$, $z \longrightarrow z + 1$ and $z \longrightarrow -z$ respectively, for some integer $a \neq 0$. Thus if X and Y are the matrices representing $\bar{x}$, $\bar{y}$, then $X = \begin{bmatrix} 0 & a \\ 1 & 0 \end{bmatrix}$ and $Y = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ thus giving the matrix $XY = \begin{bmatrix} 0 & a \\ 1 & 1 \end{bmatrix}$. Thus $\vartheta = -1/a$, so that each ϑ occurs uniquely except $\vartheta = 0$.

CHAPTER THREE
CONDITIONS FOR THE EXISTENCE OF CIRCUITS IN $D(\vartheta,q,n)$

3.1 Introduction

It has been shown in Chapter 2 that for each ϑ in F_q there exists a non-trivial conjugacy class of pairs $(\bar{x},\bar{y})$, with $\bar{x},\bar{y}$ in PGL(2,q) satisfying the relations (1.2.2). Each pair $(\bar{x},\bar{y})$ determines the non-degenerate homomorphism α from G(2,n) to PGL(2,q). We have in fact proved that the conjugacy classes of non-degenerate homomorphisms of the group G(2,n) into PGL(2,q) are in one to one correspondence with the non-trivial conjugacy classes of elements of PGL(2,q), such that the correspondence assigns to any non-degenerate homomorphism α the class containing $(xy)\alpha$. Thus the homomorphism α gives an action of the group G(2,n) on $PL(F_q)$. The pair $(\bar{x},\bar{y})$ gives a coset diagram for this action. So for each ϑ in F_q we can find a unique coset diagram. It is unique in the sense that the diagram is the same for each conjugacy class of pairs $(\bar{x},\bar{y})$, only the labelling of the vertices of the diagram differs. That is, if we draw coset diagrams for two pairs $(\bar{x}_1,\bar{y}_1)$ and $(\bar{x}_2,\bar{y}_2)$ in the same conjugacy class we get the same diagram except that the labelling of the vertices of the diagram will vary. Therefore, if we know ϑ we can find some homomorphism α and hence we can draw a coset diagram. The method for finding the pair $(\bar{x},\bar{y})$ from a given ϑ is also given in the previous chapter. It is important to mention that we are not only interested in ϑ but in the irreducible equation over F_q which it satisfies.

A coset diagram is said to be composed of several fragments, each fragment being composed of circuits, that is, closed paths. As mentioned in earlier chapters, one can study the properties of a certain group with the help of the coset diagram arising from the action of $G(2,n)$ on $PL(F_q)$ depicting the homomorphic image of the group. We can also study properties of the group with the help of just a fragment of a coset diagram, instead of studying the whole diagram depicting the transitive permutation representation of larger degrees. We shall find conditions for the existence of these particular fragments in the respective coset diagrams in our next chapter. In this chapter, we discuss the conditions for the existence of certain single circuits in the respective coset diagrams. We in fact find a relationship between single circuits and the parameters ϑ.

There are two types of circuits: periodic and non-periodic. Both have different conditions for their existence in the corresponding coset diagrams. We have discussed both the cases separately in Sections 3.3 and 3.4. In the following we give a brief description about the coset diagrams whose vertices are the cosets of the trivial stabilizer of the group G(2,n).

3.2 Regular Representations of a Coset Diagram

A path P in a coset diagram, defined as usual, is a sequence of edges $E_1E_2...E_m$, such that, for $i = 1,2,...,m-1$, E_{i+1} begins at the end point of E_i. The path P^{-1} described backwards is called the inverse path, defined by $P^{-1} = E_m^{-1} \ldots E_2^{-1} E_1^{-1}$. The path P is closed if its initial vertex coincides with its final vertex. In such a case it is called a circuit. A coset diagram is said to be connected if every pair of its vertices can be joined by a path along a set of consecutively adjacent edges. The coset diagrams which represent the actions of G(2,n) on $PL(F_q)$ are composed of several circuits. However, there are certain results which do not necessarily depend upon this action. In this section we discuss only such cases.

The coset diagram for the group H(2,n), defined by (1.2.1), in its regular representation is defined as follows. It is a tree of valency n in which every vertex is replaced by an n-sided polygon giving a graph of valency three. As in the case of a connected coset diagram, the elements of

$PL(F_q)$ are identified with the cosets Ng where N is the stabilizer of some arbitrary element of F_q and $g \in H(2,n)$. We choose the trivial stabilizer to obtain the coset diagram for the regular representation of H(2,n). So that the vertices of such a graph, being the cosets of the trivial stabilizer, represent the elements of the group H(2,n).

A diagram D, for the group H(2,n) in its regular representation will always be a covering diagram, for a connected coset diagram D′ for H(2,n) in the following sense. We choose a vertex u in D and a vertex u′ in D′. Any vertex v in D is joined to u by a path P which is unique if we do not allow successive x-edges, or successive y-edges. There is a corresponding path in D′, starting with u′, and having x-edges where P does, and positive y-edges where P does. This path will end at a point V′, uniquely determined by V. In this way (mapping V to V′) we get a mapping μ from D to D′, in which x-edges correspond to x-edges and positive y-edges to positive y-edges. This map will not be one to one unless D is D′ itself.

For example, the corresponding diagram is the coset diagram for the group $H(2,4) = \langle x,y : x^2 = y^4 = 1\rangle$ in its regular representation.

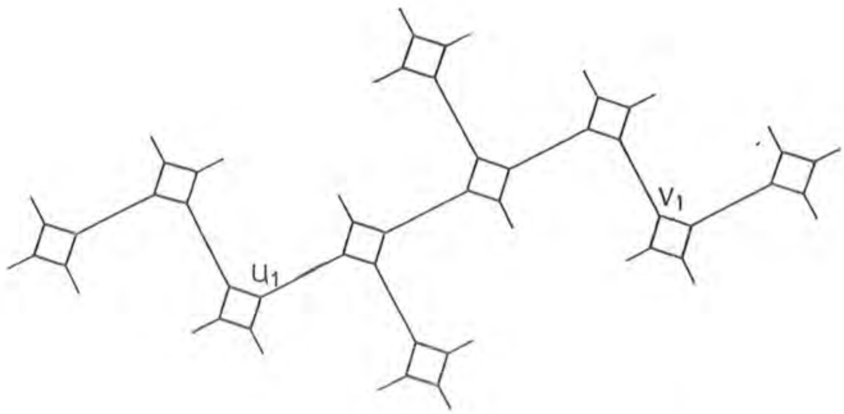

Figure 6

Any path along the edges of the coset diagram corresponds to an element of the group. For example,the path from the vertex u_1 to V_1 in the above diagram correspond to the element $g = xy^2xy^2xyx$ of the group $H(2,4) = \langle x,y : x^2 = y^4 = 1\rangle$.

If $V \neq u$ maps onto u', the path from u to V in D maps onto a circuit in D′. If g is the element of the group H(2,n), defined by Equation (1.2.1), labelling V′, then V′ maps onto u′ if and only if g belongs to the stabilizer of u′ in the representation of H(2,n) of which D′ is the diagram. Thus circuits in the diagram D′ correspond to elements of H(2,n) which have fixed points. For example, we consider the group $H(2,4) = \langle x,y : x^2 = y^4 = 1\rangle$. Let the elements g_1 and g_2 of this group be such that $g_1 = (xy^{-1})(xy)^2(xy^2)(xy)$ and $g_2 = (xy^{-1})(xy)^3(xy^{-1})^2$. The circuits γ_1 and γ_2 corresponding to these elements are as follows. The vertices u_1 and u_2 are fixed by the elements g_1 and g_2 respectively.

γ_1:

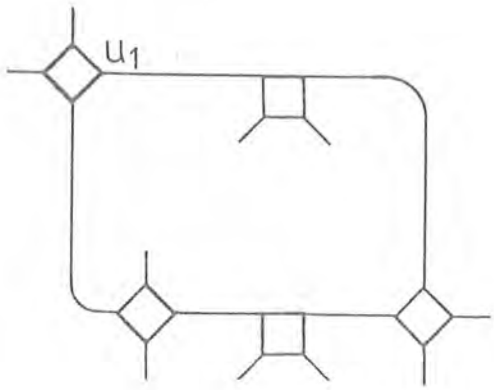

Figure 7

and

γ_2:

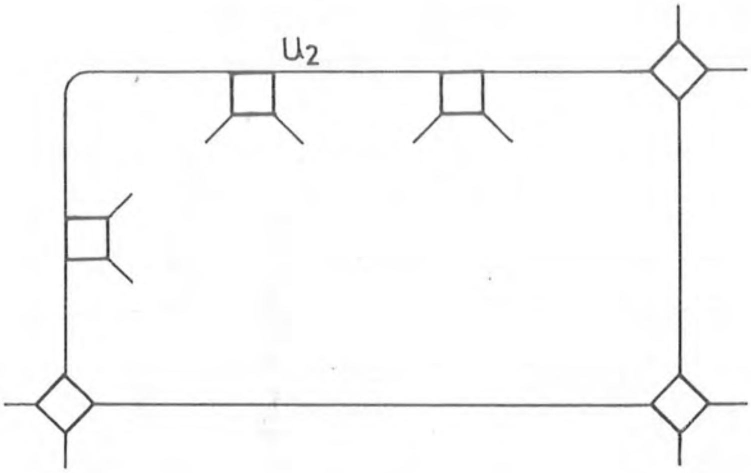

Figure 8

The two circuits are simple circuits. The circuit γ_3 can be obtained by connecting γ_1 and γ_2 in the following way.

γ_3:

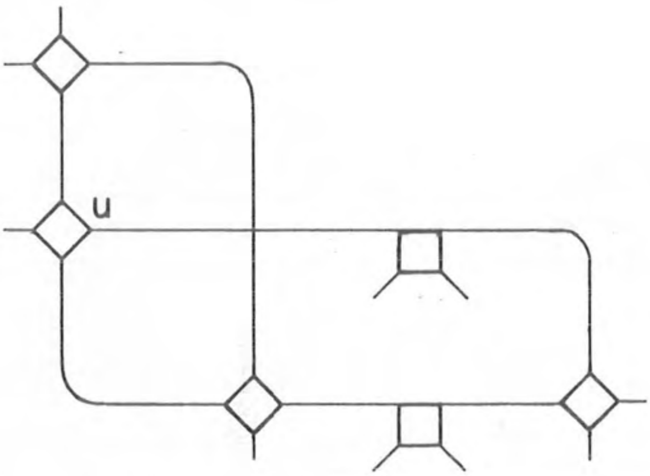

Figure 9

Here u is the fixed vertex both of g_1 and g_2. Then u is also a fixed vertex of g_1g_2. But the coset diagram for the regular representation of the group H(2,4) does not contain the simple circuit corresponding to g_1g_2, which is:

γ_4:

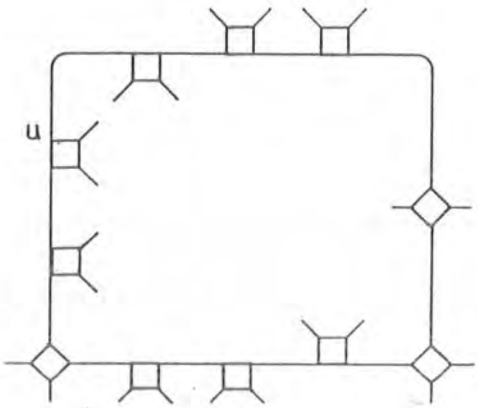

Figure 10

but a non-simple circuit, which , in a natural sense, is a homomorphic image of it. That is, the vertices of γ_4 can be mapped onto the vertices of γ_3, in such a way that u maps to u′, x-edges maps to x-edges, and positive y-edges to positive y-edges.

In any coset diagram, a circuit corresponds to an element of the group H(2,n), expressed as a product of the generators and their powers, with fixed points. Given a simple circuit of a particular form, we can find an element g of H(2,n) such that a diagram contains the circuit only if, in the corresponding permutation representation, g has a fixed vertex. If g has a fixed point then conversely the diagram contains either the circuit or a homomorphic image of it. In case if the coset diagram for the group H(2,n) is not a regular representation we get circuits having fixed vertex of the generators x or y, showing that x or y is in the stabilizer of the fixed vertex. The conditions for the existence of fixed vertices of x and y in the coset diagram which determines the action of H(2,n) on $PL(F_q)$ have been found in our later chapters. Here we deal with the circuits corresponding to the existence of fixed points of elements which are comparatively simple.

A circuit is non-trivial if the word, corresponding to the path of the circuit is in the reduced form. For example, the circuits:

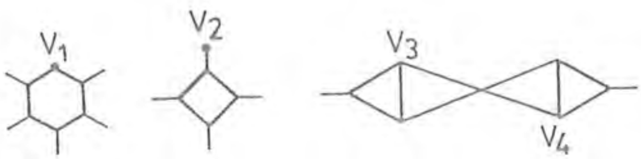

Figure 11

are non-trivial circuits in which the vertices V_1, V_2, V_3 and V_4 are respectively fixed by x,y and $xy^{-1}xy$. If a diagram contains a non-trivial circuit, we can choose a particular vertex on the circuit, which determines an element of the group H(2,n).

Let g be a non-trivial element of H(2,n) of the form $xy^{\epsilon_1}xy^{\epsilon_2}\ldots xy^{\epsilon_k}$ for some positive integer k, where ϵ_i may be one of the elements 1,2,...,n-1 for i = 1,2,...,k. If $\epsilon_1 = \epsilon_2 = \epsilon_k = 1$ then g will be of the form $(xy)^k$ for some $k \geq 1$. If $g = (xy)^k$ for $k > 1$, where g is an element of H(2,n) and if in some coset diagram, for the action of H(2,n) on $PL(F_q)$, each vertex is fixed by g, then $(xy)^k = 1$.

Thus $g = (xy)^k$ becomes a relator, giving a homomorphic image of the group $\Delta(2,n,k)$. Such groups are discussed in detail in the last chapter.

In our next section we deal with circuits corresponding to the elements $(xy)^k$ and find the conditions for its existence in the coset diagrams $D(\vartheta,q,n)$.

3.3 Circuits in $D(\vartheta,q,n)$ fixed by the elements $(xy)^k$

Let h be some element of $H(2,n)$, chosen to be equal to xy. Let $g = h^k$ for $k \geq 1$. The element g is said to be of proper power if $k > 1$. Now for any arbitrary element z in $H(2,n)$ with $z = xy^{\epsilon_1}xy^{\epsilon_2}\ldots xy^{\epsilon_k}$, z and z^{-1} always have the same fixed points. Therefore we just consider the case for z only. Hence we shall consider just $(xy)^k$, for $k \geq 1$. When $k = 1$, that is, for $g = xy$, the only circuit for the fixed point of xy is a loop, as for example in the case of a hexagon, we will have the following fragment:

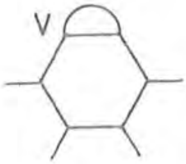

Figure 12

Here the vertex V is fixed by xy, thus giving $xy = 1$. Now if $xy \neq 1$, the fixed points of $(xy)^k$ are same as the fixed points of xy as long as $(xy)^k \neq 1$ for $k>1$. So that no coset diagram $D(\vartheta,q,n)$ will contain a circuit in which some vertex is fixed by $(xy)^k$ unless $(xy)^k = 1$. We shall therefore consider the circuits corresponding to $(xy)^k$, for $k \geq 2$.

Theorem 3.3.1

Let C be the circuit corresponding to $(xy)^k$, $k \geq 2$. Then there is a polynomial f in $\mathbb{Z}[z]$ such that, if q does not divide k, then

(i) if the circuit C occurs in $D(\vartheta,q,n)$ then $f(\vartheta) = 0$, and

(ii) if $f(\vartheta) = 0$, then every vertex in

$D(\vartheta,q,n)$ is in a circuit C, or in the homomorphic image of it.

Proof

Suppose the circuit exists in $D(\vartheta,q,n)$. It follows from the above discussion that $\bar{x}\bar{y}$ has order k. Thus if M is a matrix corresponding to $\bar{x}\bar{y}$ then M^k is a scalar matrix, but $M^{k'}$ is not if k′ is a proper divisor of k. Now since q does not divide k, this implies that over a suitable extension field of F_q some scalar multiple of M is conjugate to $\begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix}$ where ρ is a primitive k-th root of unity if k is odd, but a primitive 2k-th root of unity if k is even. Then $\vartheta = r^2/\Delta = \rho^2 + \rho^{-2} + 2$. Since ρ^2 is in either case a primitive k-th root of unity, ϑ is a zero of f(z), where $z^{1/2(\phi_k)} f(z + z^{-1} + 2) = \Phi_k(z)$, ϕ_k being Euler's function, and Φ_k the k-th cyclotomic polynomial.

Conversely, if ϑ satisfies $f(z)=0$, then $\vartheta = \sigma + \sigma^{-1} + 2$, where σ is a primitive k-th root of unity. We put $\sigma = \rho^2$, where ρ can be taken to be a primitive k-th root of unity if k is odd, but a primitive 2k-th root of unity if k is even. Then a matrix M has the same characteristic equation as some scalar multiple of $\begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix}$. It follows that M^k is a scalar matrix, so that $(\bar{x}\bar{y})^k$ is in the kernel of the homomorphism.

Theorem 3.3.2

Let C be a simple circuit corresponding to an element g of the group H(2,n) which is not a proper power. Then there exists a polynomial f in $\mathbb{Z}[z]$ such that if C occurs in $D(\vartheta,q,n)$ then $f(\vartheta)$ is a square in F_q, and if $f(\vartheta)$ is a square in F_q then either C or a homomorphic image of it occurs in $D(\vartheta,q,n)$.

Proof

Let $\bar{g} = \bar{x}\bar{y}^{\epsilon_1}\ \bar{x}\bar{y}^{\epsilon_2} \ldots \bar{x}\bar{y}^{\epsilon_l}$, where $\bar{x},\bar{y}$ are in PGL(2,q) and ϵ_i is any of the integers $1,2,\ldots,n-1$ for $i = 1,2,\ldots,l$. Let C be the simple circuit corresponding to $\bar{g}$ having a fixed vertex. Let X and Y be the matrices corresponding to $\bar{x}$ and $\bar{y}$ of PGL(2,q). Then the matrix representing $\bar{g}$ of PGL(2,q) will be

$$M = XY^{\epsilon_1}\ XY^{\epsilon_2} \ldots XY^{\epsilon_l}\ . \qquad (3.3.1)$$

As in Lemma 2.2.2, we let $\det(X) = \Delta \neq 0$ and assume that $\det(Y) = 1$, so that $\det(XY) = \Delta$. Similarly we choose r to be the trace of XY, and m the trace of Y, where $m \equiv x (\mathrm{mod}\ q)$, for some x in F_q, where q is an odd prime-power. Now since $\bar{x}^2 = 1$, we have by Lemma 2.2.1, $\mathrm{tr}(X) = 0$, so that the characteristic equation of X becomes

$$X^2 + \Delta I = 0 . \qquad (3.3.2)$$

Also the characteristic equations of Y and XY are respectively given by

$$Y^2 - mY + I = 0 \qquad (3.3.3)$$

and

$$(XY)^2 - r\,XY + \Delta I = 0. \qquad (3.3.4)$$

From Equations (3.3.2), (3.3.3) and (3.3.4) we can easily deduce the following equations:

$$XYX = rX + \Delta Y - m\Delta I \qquad (3.3.5)$$

$$YXY = rY + X \qquad (3.3.6)$$

$$YX = rI - XY + mX. \qquad (3.3.7)$$

From Equation (3.3.3), we can easily obtain $Y^n = I$ if n is odd and $Y^n = -I$ if n is even. Now since $\det(XY) = \Delta$, we have $\det(M) = \det(XY^{\epsilon_1} XY^{\epsilon_2} \ldots XY^{\epsilon_l}) = \Delta^l$. Using Equations (3.3.2) to (3.3.7) we can express the matrix M , defined by (3.3.1), as $M = \lambda_o I + \lambda_1 X + \lambda_2 Y + \lambda_3 XY$, where λ_i, $i = 0,1,2,3$ is a polynomial in r and Δ. Therefore, we have $tr(M) = tr(\lambda_o I + \lambda_1 X + \lambda_2 Y + \lambda_3 XY) = \lambda_o tr(I) + \lambda_1 tr(X) + \lambda_2 tr(Y) + \lambda_3 tr(XY) = 2\lambda_o + m\lambda_2 + r\lambda_3$. Hence the characteristic equation of M will be

$$M^2 - (2\lambda_o + m\lambda_2 + r\lambda_3)\ M + \Delta^l I = 0\ . \qquad (3.3.8)$$

Its discriminant $d(r,\Delta)$ will then be

$$d(r,\Delta) = (2\lambda_o + m\lambda_2 + r\lambda_3)^2 - 4\Delta^l\ , \qquad (3.3.9)$$

which is a polynomial in r and Δ.

Regarding r as of degree 1, and Δ as of degree 2, we can show by induction on l that the polynomial (3.3.9) is homogeneous of degree $2l$. Therefore, for some suitable $h(\vartheta)$, where $\vartheta = r^2/\Delta$, the polynomial (3.3.9) is $h(\vartheta)\Delta^l$.

Now $\bar{g}$ has a fixed vertex in $PL(F_q)$ if the characteristic equation of M has roots in F_q, or in other words, if the discriminant $h(\vartheta)\Delta^l$ is a square in F_q. Since $r^2 = \vartheta\Delta$, Δ is a square if and only if ϑ is, we put $f(\vartheta) = h(\vartheta)$ if l is even and $f(\vartheta) = h(\vartheta)\vartheta$ if l is odd. Hence the result.

Consider an element $\bar{g} = \bar{x}\bar{y}^{-1}\bar{x}\bar{y}$ of PGL(2,q) where $\bar{x},\bar{y}$ are in PGL(2,q). Consider the non-trivial simple circuit corresponding to $\bar{g}$. Since $\bar{g}$ is not a proper power, we can apply Theorem 3.3.2 to obtain a polynomial $f(\vartheta)$ satisfying the conditions of Theorem 3.3.2. We find this polynomial in the result that follows. Now since we are considering the circuits in the coset diagrams $D(\vartheta,q,n)$, so that $\bar{y}^n = 1$ and hence we choose n-gons to represent the relator $\bar{y}^n$. For example, for n to be equal to 4 or 6 we shall consider the following circuits respectively,

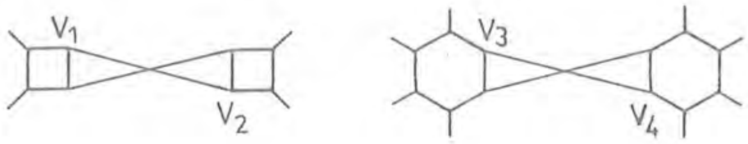

Figure 13

in which the vertices V_1, V_2, V_3, V_4, are all fixed by $\bar{x}\bar{y}^{-1}\bar{x}\bar{y}$. In our last chapter we shall find conditions for the existence of such circuits in $D(\vartheta,q,n)$ for certain q's. Here we give, in general, the condition for the existence of such circuits in $D(\vartheta,q,n)$.

Corollary 3.3.3

Let C be a circuit corresponding to an element $\bar{g} = \overline{xy}^{-1}\overline{xy}$ of PGL(2,q), such that C contains a vertex which is fixed by $\bar{g}$. Then C or its homomorphic image, exists in $D(\vartheta,q,n)$ if and only if

$$f(\vartheta) = \vartheta^2 - 2(2-m^2)\vartheta + ((2-m^2)^2-4)$$

is a square in F_q.

Proof

Consider the vertex V in the circuit C which is fixed by $\overline{xy}^{-1}\overline{xy}$, where $\bar{x},\bar{y}$ are in PGL(2,q). Let X and Y be the matrices representing $\bar{x}$ and $\bar{y}$. Let us denote by M the matrix corresponding to the element $\bar{g}$, so $M = XY^{-1}XY$. Now by the arguments of Theorem 3.3.2, as $\bar{y}^n = 1$, we have $Y^n = I$ for n to be odd and $Y^n = -I$ for n to be even. Hence we can find the value of Y^{-1} depending upon the parity of n.

Substituting the values of X^2, Y^2 and $(XY)^2$

from Equations (3.3.2),(3.3.3) and (3.3.4) we obtain

$$M = -rXY + \Delta I - m\Delta Y , \qquad (3.3.10)$$

where m and r are the traces of Y and XY respectively. From (3.3.10), we have $tr(M) = tr(-rXY + \Delta I - m\Delta Y) = -rtr(XY) + \Delta tr(I) - m\Delta tr(Y) = -r^2 + 2\Delta - m^2\Delta = -r^2 + \Delta(2 - m^2)$. Also, we have $\det(M) = \det(XY^{-1}XY) = \Delta^2$, since $\det(X) = \Delta$ and we assume $\det(Y) = 1$. Thus we get the characteristic equation of M as

$$M^2-(-r^2+(2-m^2)\Delta)M + \Delta^2 I = 0,$$

giving the discriminant as

$$\begin{aligned} d(r,\Delta) &= [-r^2 + (2-m^2)\Delta]^2 - 4\Delta^2 \\ &= r^4 + (2-m^2)^2\Delta^2 - 2(2-m^2)r^2\Delta - 4\Delta^2 \\ &= r^4 - 2(2-m^2)r^2\Delta + [(2-m^2)^2-4]\Delta^2. \end{aligned}$$

Substituting $r^2 = \vartheta\Delta$ we get the equation in ϑ as

$$f(\vartheta) = \vartheta^2-2(2-m^2)\vartheta + [(2-m^2)^2-4]. \qquad (3.3.11)$$

Thus the circuit C, or its homomorphic image exists in the coset diagram $D(\vartheta,q,n)$ if and only if $f(\vartheta)$ is a square in F_q.

Consider the following as an example.

Example 3.3.4

Consider the circuit

γ:

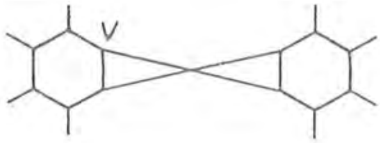

Figure 14

in which the vertex V is fixed by the element $\bar{x}\bar{y}^{-1}\bar{x}\bar{y}$ of PGL(2,q). We find the condition for this circuit to exist in the coset diagram $D(\vartheta,q,6)$.

Let X and Y be the matrices corresponding to the elements $\bar{x}$ and $\bar{y}$ of PGL(2,q). Let M be the matrix corresponding to the element $\bar{x}\bar{y}^{-1}\bar{x}\bar{y}$, so that M can be expressed as $M = XY^{-1}XY$. Here, of course, Y^{-1} is the matrix Y^5. Now since $\bar{y}^6 = 1$, we calculate the trace of Y to be equal to $\sqrt{3}$. From Equation (3.3.11), substituting $m = \sqrt{3}$, we obtain

$f(\vartheta) = \vartheta^2 + 2\vartheta - 3 = (\vartheta+3)(\vartheta-1)$. Thus, by Corollary 3.3.3, the circuit γ exists in $D(\vartheta,q,6)$ if and only if $f(\vartheta)$ is a square in F_q.

In the following section, we consider the circuits in $D(\vartheta,q,n)$ having the fixed points of $\bar{x},\bar{y},\overline{xy}$ and $\bar{t}$, where $\bar{x},\bar{y},\bar{t}$ are all in PGL(2,q).

3.4 Fixed Points in $D(\vartheta,q,n)$

We shall now consider the circuits in $D(\vartheta,q,n)$ having the fixed points of $\bar{x},\bar{y},\overline{xy}$ and $\bar{t}$, where $\bar{x},\bar{y},\bar{t}$ are all in PGL(2,q). Note that for this purpose we choose q not to be of characteristic p, where p is a prime, if n = p. Therefore, as discussed in Section 2.3, the fixed points of $\bar{x},\bar{y}$ do not lie on the vertical axis of symmetry, so that they are not the fixed points of $\bar{t}$ also. The case for the fixed points of $\bar{t}$ (lying on the vertical axis of symmetry) has been discussed in the following theorem. We first make the following observations.

Remark 3.4.1

(i) A circuit having a fixed point of $\bar{x}$ exists in $D(\vartheta,q,n)$ if and only if $-\vartheta$ is a square in F_q. For, by Theorem 3.3.2, the matrix representing $\bar{x}$ of PGL(2,q) will be M = X. So that from Equation (3.3.2), its characteristic equation will be $X^2+\Delta I = 0$, thus giving the discriminant as -4Δ. Now since $r^2 = \vartheta\Delta$, ϑ is a square if and only if Δ is, hence the result.

(ii) Let C be a circuit having a fixed point of $\bar{y}$. The matrix representing $\bar{y}$ shall be M = Y. So that the characteristic equation of Y, from Equation (3.3.3) is $Y^2- mY + I = 0$. Thus we obtain the discriminant as $d = m^2- 4$. Hence C exists in $D(\vartheta,q,n)$ if and only if m^2-4 is a square in F_q.

(iii) Consider now the circuits having fixed points of $\bar{x}\bar{y}$. These circuits exist in $D(\vartheta,q,n)$ if and only if $\Delta(\vartheta-4)$ is a square in F_q. This is a direct consequence of Theorem 3.3.2. By taking the matrix representing $\bar{x}\bar{y}$ as M = XY and considering the discriminant of the characteristic equation of XY, given by Equation (3.3.4), and substituting $r^2 = \vartheta\Delta$ we obtain the required result.

We now consider coset diagrams having the fixed vertices of $\bar{t}$ on the vertical axis of symmetry in the following.

Theorem 3.4.2

The element $\bar{t}$ of PGL(2,q) has fixed vertices in D(ϑ,q,n) if and only if $\vartheta[\vartheta-(4-m^2)]$ is a square in F_q.

Proof

We recall from Remark (3.4.1) (i), that in the non-degenerate homomorphism α with parameter ϑ, x maps to an element of PSL(2,q) if and only if $-\vartheta$ is a square in F_q. Since changing to the dual homomorphism interchanges both x and xt, and ϑ and $(4-m^2)-\vartheta$, it follows that xt maps to an element of PSL(2,q) if and only if $-[(4-m^2)-\vartheta]$ is a square in F_q. Since $\bar{t}$ is in PSL(2,q) if both or neither of $\bar{x}$ and $\bar{x}\bar{t}$ is, but not if just one of them is, $\bar{t}$ is in PSL(2,q) if and only if $\vartheta[(4-m^2)-\vartheta]$ is a square in F_q. Now $\bar{t}$ has fixed vertices in PL(F_q) if either $\bar{t}$ belongs to PSL(2,q) and $q \equiv 1 \pmod 4$ or $\bar{t}$ does not belong to PSL(2,q) and $q \equiv 3 \pmod 4$. Since '$q \equiv 1 \pmod 4$' is equivalent to '-1 is a square in F_q', we see that $\bar{t}$ has fixed vertices if and only if $\vartheta[\vartheta-(4-m^2)]$ is a square in F_q.

3.5 Circuits when the Discriminant is Zero

Let C be a circuit such that it contains a vertex which is fixed by an element $\bar{g}$ of PGL(2,q). The characteristic equation of the matrix corresponding to $\bar{g}$ will, of course, have equal eigen-values if the discriminant of the characteristic equation is equal to zero. This means that $\bar{g}$ will have just one fixed vertex in $D(\vartheta,q,n)$, but the exact type will depend upon the circuit concerned.

For example, we first consider some circuits occuring in the coset diagrams $D(\vartheta,q,6)$ for an action of the group G(2,6) on $PL(F_q)$.

Let C be a circuit in $D(\vartheta,q,6)$ such that a vertex in it is fixed by an element $\bar{g}$ of PGL(2,q). Then the characteristic equation of the matrix (say M) corresponding to the element $\bar{g}$ has roots in F_q.

So that $\bar{g}$ has fixed vertex in $PL(F_q)$ if the discriminant $d(\vartheta)$ of the characteristic equation of M is a square in F_q. We now check for the conditions on C if this discriminant is zero. In that case the characteristic equation has equal eigen values, meaning $\bar{g}$ will have just one fixed vertex in $D(\vartheta,q,6)$.

For example, consider the circuit

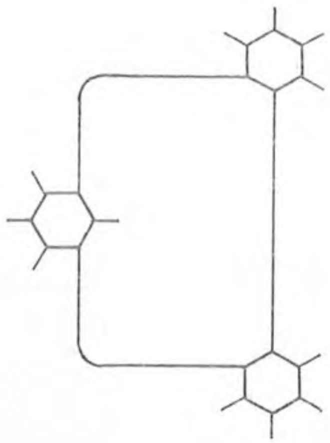

Figure 15

in $D(\vartheta,q,6)$. Since $D(\vartheta,q,6)$ admits the axis of symmetry, the image of the circuit under the permutation $\bar{t}$ will also occur. The vertices v and $v\bar{t}\bar{y}^2$ on the circuits:

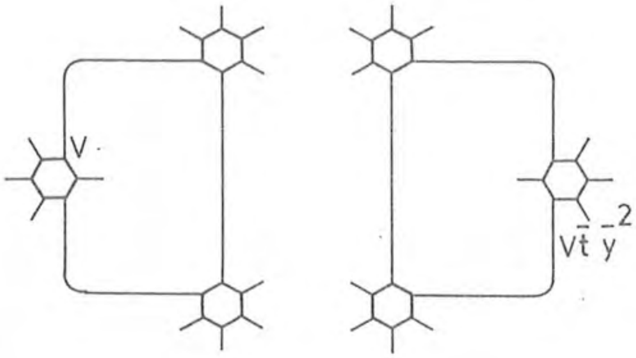

Figure 16

are both fixed by an element $\bar{g} = \overline{xyxyxy}^2$ of PGL(2,q). So if the discriminant of the characteristic equation of the matrix corresponding to $\bar{g}$ is equal to zero, then $v = v\bar{t}\bar{y}^2$. This means that the circuit C, which has a symmetry, lies on the vertical axis of symmetry as shown in Figure 17.

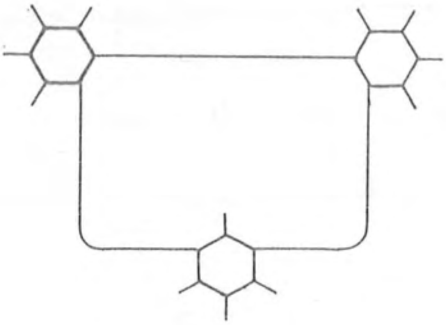

Figure 17

Consider now the homomorphic image of the circuit in Figure 18 that occurs in $D(\vartheta,q,6)$.

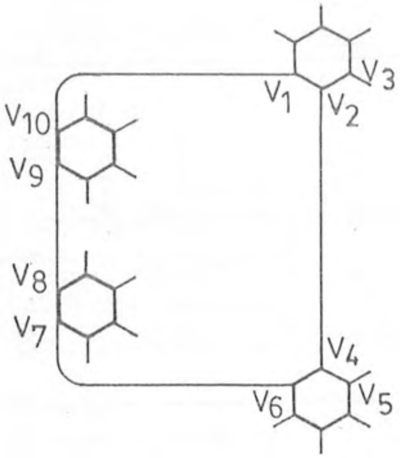

Figure 18

Here the vertices v_1 and v_{10} are fixed by the element $g = \overline{xyxyxy}^{-1}\,\overline{xy}^{-1}$ of PGL(2,q). Now if the discriminant of the characteristic equation of the matrix corresponding to $\bar{g}$ is zero, then we get a homomorphic image of the circuit in which $v = v\bar{x}$. So that a homomorphic image of the circuit will be as shown in Figure 19, which will be, in fact symmetrical about the vertical line of symmetry.

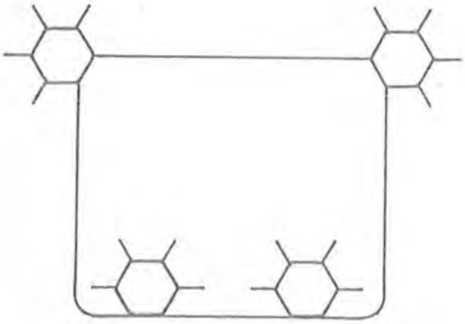

Figure 19

Let us now consider the circuit having fixed point of $\overline{xy}$ as discussed in Remark (3.4.1) (iii). Taking the discriminant $\Delta(\vartheta-4) = 0$ we have $\vartheta = 4$, since Δ, being the determinant of the matrix X, is non-zero. Hence by the above arguments, there will be only one vertex in D(4,q,n) fixed by $\bar{x}\bar{y}$. Since the action of $\bar{t}$ represents reflection about the vertical line of symmetry, the circuit (having the fixed the point of $\bar{x}\bar{y}$) will, in this case, lie on the vertical axis of symmetry.

Example 3.5.1

Consider the coset diagram D(4,23,4) for the action of the group G(2,4) on $PL(F_{23})$.

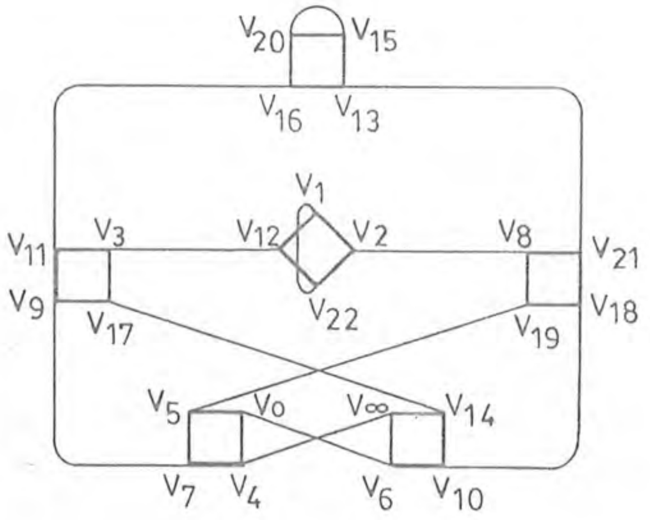

Figure 20

Here v_{20} is the only vertex fixed by the element $\bar{x}\bar{y}$

of PGL(2,23). Note that in this case, (where we choose $Y^4 = \lambda I$, for some scalar λ), we obtain tr(Y) $= \sqrt{2}$; so that, from Theorem 3.4.2, $\bar{t}$ has fixed vertices, namely v_1 and v_{22} since $\vartheta(\vartheta-2) = 8$ is a square in F_{23}.

CHAPTER FOUR
SOME SPECIAL FRAGMENTS OF COSET DIAGRAMS

4.1 Introduction

In [9], it has been shown how an automorphism of a given group enables us to adjoin a new element so as to obtain a larger group. For example, the cyclic and non-cyclic groups of order 4 yield the quaternion group and the tetrahedral group respectively. We can do the same in a much simpler way with the help of graphs. By joining graphs representing groups of smaller degree we can get a 'big' graph representing a group of larger degree. Then it is also easy to study the properties of the new group just by studying its graph. Therefore the graphs enable us both to see what steps to take and to check that our results are 'sensible'. We have different methods of 'joining' graphs together, to give transitive representations of the group G of larger degree. M.Conder, in [4] and [5], has adopted a method of using 'j handles' to join the coset diagrams for groups of smaller degrees to obtain coset diagrams for groups of larger degrees. The method that he has used is called (j)-composition (where j = 1,2 or 3). It has been described in [25]. We also give a method of forming groups of larger degrees by joining fragments of coset diagrams representing groups of smaller degrees. Our method is much simpler as we need not have to study the entire group of a smaller degree. We can do that just by studying a fragment of it and find conditions for the existence of that fragment in the coset diagram, so that if that fragment exists in a coset diagram of larger degree, we can study the properties of that diagram for the related group of larger degree.

A fragment is said to be composed of a single circuit or more than one circuit. In Chapter 3 we have studied the single circuits, and found conditions for their existence in the respective coset diagrams $D(\vartheta,q,n)$. The purpose of this chapter is to study the fragments composed of at least two interconnected circuits, both periodic and non-periodic, and to find the conditions for their existence in the coset diagrams $D(\vartheta,q,n)$. (By a periodic circuit, we shall mean a circuit corresponding to an element $g = h^k$, $k > 0$ of $G(2,n)$, so that g belongs to the kernel of α.)

Recall that each class of non-degenerate homomorphisms α from $G(2,n)$ to $PGL(2,q)$ can be represented by a unique coset diagram. In order to know which class(es) a diagram comes from, we need to consider this question: Given a fragment of a coset diagram for an action of $G(2,n)$ (or $H(2,n)$) on $PL(F_q)$ or $PL(F_{q^2})$, for what values of q and ϑ can it be found in $D(\vartheta,q,n)$? In our next section we have found the condition for the existence of a fragment in $D(\vartheta,q,n)$, for the conjugacy class of α related to ϑ, to be a polynomial f in $\mathbb{Z}[z]$ such that $f(\vartheta) = 0$.

4.2 Fragments in $D(\vartheta,q,n)$ and Related Polynomials

In [20], Q.Mushtaq has proved that, given a fragment γ, there is a polynomial f in $\mathbb{Z}[z]$ such that if γ occurs in $D(\vartheta,q,3)$ then $f(\vartheta) = 0$ and if $f(\vartheta) = 0$ then the fragment, or a homomorphic image of it, occurs in $D(\vartheta,q,3)$ or in the coset diagram for the action of $G(2,3)$ on $PL(F_{q^2})\backslash PL(F_q)$. We have generalized the same result by taking the action of $G(2,n)$ on $PL(F_q)$.

Before proving the main result, we state a lemma for use in our subsequent work. (The proof is given in [16].)

Lemma 4.2.1

Two 2x2 matrices M and N over the field F_q have a common eigen vector over F_q or F_{q^2} if and only if the algebra A that they generate, has dimension less than or equal to 3.

As defined earlier, by a periodic circuit, we shall mean a circuit corresponding to an element $g = h^k$, $k > 0$ of $G(2,n)$, so that g belongs to the kernel of α. Here $h = (xy^{\epsilon_1})^{l_1}(xy^{\epsilon_2})^{l_2}\ldots(xy^{\epsilon_j})^{l_j}$, for $1 \le \epsilon_i \le n - 1$, where $i = 1,2,\ldots,j$, and h does not have a fixed vertex.

We now prove the main theorem.

Theorem 4.2.2

Given a fragment γ, there is a polynomial f in $\mathbb{Z}[z]$ such that

(i) if the fragment γ occurs in $D(\vartheta,q,n)$, then $f(\vartheta) = 0$;

(ii) if $f(\vartheta) = 0$ then the fragment, or a homomorphic image of it, occurs in the coset diagram $D(\vartheta,q^2,n)$.

Proof

Suppose γ exists in $D(\vartheta,q,n)$ and assume that C_1 and C_2 are any two non-periodic, interconnected circuits which compose the fragment γ. Let a vertex v belongs to both C_1 and C_2. Then the elements, namely

$$\bar{w}_1 = (\bar{x}\bar{y}^{t_1})^{l_1}(\bar{x}\bar{y}^{t_2})^{l_2}\ldots(\bar{x}\bar{y}^{t_{k_1}})^{l_{k_1}},$$

and

$$\bar{w}_2 = (\bar{x}\bar{y}^{s_1})^{j_1}(\bar{x}\bar{y}^{s_2})^{j_2}\ldots(\bar{x}\bar{y}^{s_{k_2}})^{j_{k_2}},$$

where $1 \leq t_i, s_i \leq n - 1$, of PSL(2,q) are induced by the paths (with the initial point v) P_1 and P_2 of circuits C_1 and C_2. This implies that $v = v\bar{w}_1$ and $v = v\bar{w}_2$. If X and Y are the matrices, representing the elements $\bar{x}, \bar{y}$ of PSL(2,q) and also X,Y satisfy the relations

$$X^2 = Y^n = \lambda I , \qquad (4.2.1)$$

for some scalar λ, then we can represent the elements $\bar{w}_1$ and $\bar{w}_2$ in the matrices form as

$$W_1 = (XY^{t_1})^{l_1} (XY^{t_2})^{l_2} \ldots (XY^{t_{k_1}})^{l_{k_1}}$$

and

$$W_2 = (XY^{s_1})^{j_1} (XY^{s_2})^{j_2} \ldots (XY^{s_{k_2}})^{j_{k_2}}$$

respectively, where $k_1, k_2 > 0$.

Since X and Y are the matrices with entries from F_q, and X,Y satisfy the relations (4.2.1), therefore we can choose $\bar{x}, \bar{y}$ to be represented by

$$X = \begin{bmatrix} a & cl \\ c & -a \end{bmatrix} \text{ and } Y = \begin{bmatrix} e & fl \\ f & m-e \end{bmatrix}$$

as in Chapter 2. Also X and Y satisfy the Equations (2.2.10), (2.2.11) and (2.2.12). So by the arguments in Section 3.3, as $\det(X) = \Delta$, $\det(Y) = 1$, $\det(XY) = \Delta$ and $tr(XY) = r$, $tr(X)=0$, $tr(Y) = m$, we obtain the characteristic equations of X,Y and XY (as in Equations (3.3.2),(3.3.3) and (3.3.4)) respectively as

$$X^2 + \Delta I = 0, \tag{4.2.2}$$

$$Y^2 - my + I = 0, \tag{4.2.3}$$

$$(XY)^2 - r(XY) + \Delta I = 0. \tag{4.2.4}$$

On recursion, Equation (4.2.4) gives

$$(XY)^n = \{{}^{n-1}C_o r^{n-1} - {}^{n-2}C_1 r^{n-3}\Delta + {}^{n-3}C_2 r^{n-5}\Delta^2 - \ldots\}XY$$
$$-\{{}^{n-2}C_o r^{n-2} - {}^{n-3}C_1 r^{n-4}\Delta + \ldots\}\Delta I$$

$$\tag{4.2.5}$$

Using Equations (3.3.2) to (3.3.7) and also (4.2.5), we can express the matrices W_1 and W_2 as

$$W_1 = \lambda_o I + \lambda_1 X + \lambda_2 Y + \lambda_3 XY$$

and

$$W_2 = \mu_o I + \mu_1 X + \mu_2 Y + \mu_3 XY ,$$

where λ_i and μ_i, for i = 0,1,2,3 are expressions in r and Δ.

Since $v = v\bar{w}_1$ and $v = v\bar{w}_2$, the 2x2 matrices W_1 and W_2 have an eigen-vector in common. So by Lemma 4.2.1, this means that the algebra generated by W_1 and W_2 has dimension 3. The algebra contains

I, W_1, W_2 and W_1W_2 and so these must be linearly dependent. Using Equations (3.3.2) to (3.3.7), the matrix W_1W_2 can be expressed as

$$W_1W_2 = \nu_o I + \nu_1 X + \nu_2 Y + \nu_3 XY,$$

where ν_i, for $i = 0,1,2,3$ can be calculated in terms of λ_i and μ_i, using Equations (3.3.2) to (3.3.7) along with (4.2.5). The condition that I, W_1, W_2 and W_1W_2 are linearly dependent, can be expressed as

$$\begin{vmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix} = 0. \qquad (4.2.6)$$

If we carry out the calculations of ν_1, ν_2 and ν_3 in terms of λ_i and μ_i, and substitute in Equation (4.2.6) we get

$$\begin{aligned}[(\lambda_2\mu_3-\mu_2\lambda_3)^2+(\lambda_1\mu_2-\mu_1\lambda_2)^2 \\ + m\{(\lambda_1\mu_2-\mu_1\lambda_2)(\lambda_3\mu_2-\mu_3\lambda_2)\} \\ + r\{(\lambda_1\mu_3-\mu_1\lambda_3)(\lambda_3\mu_2-\mu_3\lambda_2)\} \\ +\Delta\{(\lambda_1\mu_3-\mu_1\lambda_3)^2\}] = 0.\end{aligned}$$

(4.2.7)

The expression (4.2.7) is a homogeneous equation in r and Δ, and so we can substitute $\vartheta\Delta$ for r^2 to get an equation in ϑ.

If conversely, ϑ satisfies $f(z)=0$, then the determinant (4.2.6) is zero and so W_1, W_2 and W_1W_2 are linearly dependent. Now each of W_1, W_2 and $W_1W_2 = W_3$ is a 2×2 matrix and therefore satisfies the equation $W_i^{\,2}=k_iW_i+l_iI$. Using these equations, and the fact that W_1 and W_2 are non-singular, it is easy to express W_2W_1, $W_1W_2W_3$ and $W_2W_1W_2$ linearly in I, W_1, W_2 and W_1W_2. Thus the algebra generated by W_1 and W_2 is spanned by I, W_1, W_2 and W_1W_2. Since W_1, W_2 and W_1W_2 are linearly independent, this algebra has therefore dimension less than 4 .Thus, by Lemma 4.2.1, W_1 and W_2 have a common fixed vertex, necessarily in $PL(F_{q^2})$. Hence we have circuits (or their homomorphic images) with appropriate common vertex. That is, we have the fragment γ, or a homomorphic image of it.

We now give an example to find a polynomial from a given fragment of a coset diagram.

Example 4.2.3

Let X and Y be two 2x2 matrices with entries from F_q and let them satisfy the relations

$$X^2 = Y^4 = \lambda I ,$$

for some scalar λ. Now since $Y^4 = \lambda I$, $tr(Y) = \sqrt{2}$, so that we can choose the matrices X and Y as

$$X = \begin{bmatrix} a & cl \\ c & -a \end{bmatrix} \text{ and } Y = \begin{bmatrix} e & fl \\ f & \sqrt{2}-e \end{bmatrix}$$

where a, l, c, e, f are in F_q, with $l \neq 0$, for an odd prime-power q. Now from Equations (3.3.2) to (3.3.4), we get

$$X^2 + \Delta I = 0, \text{ that is, } X^2 = -\Delta I, \tag{4.2.8}$$

$$Y^2 - \sqrt{2}Y + I = 0, \text{ that is, } Y^2 = \sqrt{2}Y - I, \tag{4.2.9}$$

$$(XY)^2 - rXY + \Delta I = 0, \text{ that is, } (XY)^2 = rXY - \Delta I. \tag{4.2.10}$$

Also by putting $m = \sqrt{2}$ in Equations (3.3.5) to (3.3.7), we get

$$XYX = rX + \Delta Y - \sqrt{2}\Delta I, \tag{4.2.11}$$

$$YXY = rY + X, \tag{4.2.12}$$

$$YX = rI - XY + \sqrt{2}X. \tag{4.2.13}$$

Also for n = 3 and n = 4, we get from Equation (4.2.5),

$$(XY)^3 = (r^2 - \Delta)XY - \Delta rI \tag{4.2.14}$$

and

$$(XY)^4 = (r^3 - 2r\Delta)XY + (\Delta^2 - r^2\Delta I) \tag{4.2.15}$$

respectively.

We now consider the following fragment of $D(\vartheta,q,4)$.

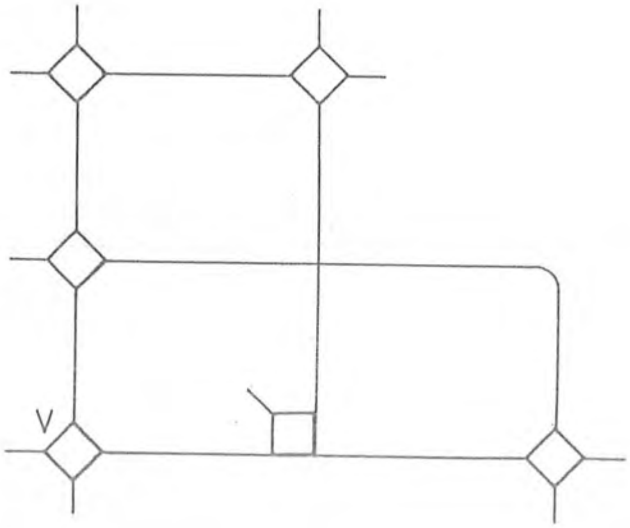

Figure 21

This is composed of two non-periodic and connected circuits with a common vertex v. The paths $\overline{xyxyxy}^3\,\overline{xy}$ and $\overline{xy}^2\,\overline{xyxyxy}^2\,\overline{xy}$ fix the vertex v. That is, if $\bar{w}_1 = \overline{xyxyxy}^3\,\overline{xy}$ and $\bar{w}_2 = \overline{xy}^2\,\overline{xyxyxy}^2\,\overline{xy}$, then $v = v\bar{w}_1$ and $v = v\bar{w}_2$.

Let X and Y be the matrices corresponding to $\bar{x}$ and $\bar{y}$ of PGL(2,q) satisfying the relations $X^2 = Y^4 = \lambda I$, for some scalar λ. Also let X and Y satisfy the Equations (4.2.8) to (4.2.15). Then $\bar{w}_1$ and $\bar{w}_2$ can be expressed as

$$W_1 = XYXYXY^3XY = (XY)^3Y^2(XY) \qquad (4.2.16)$$

and

$$W_2 = XY^2XYXYXY^2XY = XY^2(XY)^3(YXY). \qquad (4.2.17)$$

Now using Equations (4.2.8) to (4.2.15) and solving (4.2.16) we get

$$W_1 = (\Delta^2-r^2\Delta)I - (\sqrt{2}\Delta r)X - (\sqrt{2}\Delta^2)Y + r^3XY$$

$$= \lambda_o I + \lambda_1 X + \lambda_2 Y + \lambda_3 XY,$$

where $\lambda_o = \Delta^2-r^2\Delta$, $\lambda_1 = -\sqrt{2}\Delta r$, $\lambda_2 = -\sqrt{2}\Delta^2$ and $\lambda_3 = r^3$. Similarly, we can express Equation (4.2.17) as

$$W_2 = (-2r^3\Delta+3r\Delta^2)I + 0\,X + (\sqrt{2}r^3\Delta-2\sqrt{2}r\Delta^2)Y + (2r^4 - 4r^2\Delta + \Delta^2)XY$$

$$= \mu_o I + \mu_1 X + \mu_2 Y + \mu_3 XY,$$

where $\mu_o = -2r^3\Delta+3r\Delta^2$, $\mu_1 = 0$, $\mu_2 = \sqrt{2}r^3\Delta-2\sqrt{2}r\Delta^2$ and $\mu_3 = 2r^4 - 4r^2\Delta + \Delta^2$. Now by multiplying W_1 and W_2, we obtain

$$W_1W_2 = (\lambda_o\mu_o-\lambda_1\mu_1\Delta + r\lambda_2\mu_1 - \lambda_2\mu_2-\sqrt{2}\Delta\lambda_3\mu_1-\lambda_3\mu_3\Delta)I$$
$$+ (\lambda_o\mu_1+\lambda_1\mu_o+\sqrt{2}\lambda_2\mu_1+\lambda_2\mu_3+r\ \lambda_3\mu_1-\lambda_3\mu_2)X$$
$$+ (\lambda_o\mu_2-\lambda_1\mu_3\Delta+\lambda_2\mu_o+\sqrt{2}\lambda_2\mu_2+r\lambda_2\mu_3+\Delta\lambda_3\mu_1)Y$$
$$+ (\lambda_o\mu_3+\lambda_1\mu_2-\lambda_2\mu_1+\lambda_3\mu_o+\sqrt{2}\lambda_2\mu_2+r\lambda_3\mu_3)XY$$
$$= \nu_oI + \nu_1X + \nu_2Y + \nu_3XY,$$

where

$$\nu_o = \lambda_o\mu_o - \lambda_1\mu_1\Delta+\lambda_2\mu_1r-\lambda_2\mu_2-\sqrt{2}\Delta\lambda_3\mu_1-\lambda_3\mu_3\Delta,$$
$$\nu_1 = \lambda_o\mu_1 + \lambda_1\mu_o + \sqrt{2}\lambda_2\mu_1+\lambda_2\mu_3+r\lambda_3\mu_1-\lambda_3\mu_2,$$
$$\nu_2 = \lambda_o\mu_2 - \lambda_1\mu_3\Delta + \lambda_2\mu_o+\sqrt{2}\lambda_2\mu_2+r\lambda_2\mu_3+\lambda_3\mu_1\Delta,$$
$$\nu_3 = \lambda_o\mu_3 + \lambda_1\mu_2 - \lambda_2\mu_1 + \lambda_3\mu_o + \sqrt{2}\lambda_2\mu_2+r\lambda_3\mu_3$$

Now the conditions that I, W_1, W_2 and W_1W_2 are linearly dependent, can be expressed as

$$\begin{vmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix} = 0 ,$$

which implies that

$$\lambda_1(\mu_2\nu_3- \mu_3\nu_2) - \lambda_2(\mu_1\nu_3- \mu_3\nu_1)+\lambda_3(\mu_1\nu_2- \mu_2\nu_1) = 0. \tag{4.2.18}$$

Substituting the values of ν_1,ν_2,ν_3 in Equation (4.2.18) we thus obtain

$$\{(\lambda_1\mu_2 - \lambda_2\mu_1)^2 + (\lambda_2\mu_3 - \lambda_3\mu_2)^2\}$$
$$+ \sqrt{2}\ \{(\lambda_1\mu_2 - \lambda_2\mu_1)(\lambda_3\mu_2 - \lambda_2\mu_3)\}$$
$$+ r\{(\lambda_1\mu_3 - \lambda_3\mu_1)(\lambda_3\mu_2 - \lambda_2\mu_3)\}$$
$$+ \Delta\{(\lambda_1\mu_3 - \lambda_3\mu_1)^2\} = 0. \qquad (4.2.19)$$

Now substituting the values of λ_1, λ_2, λ_3 and μ_1, μ_2, μ_3 in (4.2.19), we get

$$2r^{12}\Delta^2 - 12r^{10}\Delta^3 + 22r^8\Delta^4 - 8r^6\Delta^5 - 12r^4\Delta^6 + 8r^2\Delta^7 - 2\Delta^8 = 0$$

which gives, by substituting $r^2 = \Delta\vartheta$,

$$2\vartheta^6 - 12\vartheta^5 + 22\vartheta^4 - 8\vartheta^3 - 12\vartheta^2 + 8\vartheta - 2 = 0.$$

Let $f(\vartheta) = 2\vartheta^6 - 12\vartheta^5 + 22\vartheta^4 - 8\vartheta^3 - 12\vartheta^2 + 8\vartheta - 2$. Then by Theorem 4.2.2, for any ϑ in F_q satisfying $f(\vartheta) = 0$, the diagram $D(\vartheta,q,4)$ shall contain the fragment (Figure 21) or a homomorphic image of it.

CHAPTER FIVE
THE GROUP $\langle x,y:x^2=y^6=1\rangle$ ACTING ON PROJECTIVE LINES OVER GALOIS FIELDS

5.1 Introduction

There is a well-known relation between the action of $z \longrightarrow (az+b)/(cz+d)$ of $PSL(2,\mathbb{Z}) = \langle x,y:x^2=y^3=1\rangle$ on $\mathbb{R} \cup \{\infty\}$ and continued fractions. (See e.g. [1]). There is a large body of literature relating to the connection between geodesics on the modular surface (the quotient of the hyperbolic plane by the modular group $PSL(2,\mathbb{Z})$) and continued fractions. Let α denote a real quadratic irrational number $(a+\sqrt{n})/c$, where n is a non-square positive integer and a, $(a^2-n)/c$, c are relative prime integers. Let G be the modular group. In [15] it has been proved that classifying real quadratic irrational numbers into the orbits αG is almost the same as classifying indefinite binary quadratic forms. A good account of the relationship between continued fractions and indefinite binary quadratic forms is given in [13]. In this chapter we shall replace $PSL(2,\mathbb{Z})$ by $H(2,6) = \langle x,y : x^2 = y^6 = 1 \rangle$.

In [17], Q. Mushtaq has determined a condition for the existence of closed paths in the coset diagrams for the action of $PSL(2,\mathbb{Z})$ on $Q(\sqrt{n}) \cup \{\infty\}$. It has been shown that, if such a closed path exists, then under certain conditions the closed path contains a real quadratic irrational number α along with its algebraic conjugate $\bar{\alpha}$. Also, necessary and sufficient conditions have been determined for the existence of two closed paths in the diagram; one containing α along with $1/\alpha$ and the other containing α together with $1/\bar{\alpha}$. In our later work we shall study the actions of $H(2,6)$ on the projective lines over Galois Fields F_q, denoted by $PL(F_q)$, and see under what conditions these closed paths appear in the case of finite coset diagrams for the action of $H(2,6)$ on $PL(F_q)$. Our interest in this case is motivated by the fact that there is a homomorphism between $\mathbb{Q}(\sqrt{n}) \cup \{\infty\}$ and $PL(F_q)$.

In [6], M. Conder has used coset diagrams to give an important result on the group $G^{6,6,6}=\langle x,y,t : x^2=y^6=(xy)^6=t^2=(xt)^2=(yt)^2=(xyt)^6=1\rangle$.

In fact, it is shown that for all but finitely many positive integers n, both the alternating group A_n and the symmetric group S_n occur as quotients of the group $G^{6,6,6}$. The proof of this result is obtained by diagramatic argument, using coset diagrams for the latter group. In the last section we have studied the coset diagrams for the actions of $\Delta^*(2,6,6)$ with presentation $\langle x,y,t : x^2= y^6= t^2= (xt)^2=(yt)^2=(xy)^6= 1\rangle$ on $PL(F_q)$ and have found the conditions for the existence of some special circuits in $D(3,q,6)$. Here $\vartheta = 3$ is the only parameter which gives rise to the coset diagrams for the actions of $\Delta^*(2,6,6)$ on $PL(F_q)$.

5.2 Parametrization of the Actions

Let us denote by $H(2,6)$ the group generated by two elements x and y satisfying the relations

$$x^2 = y^6 = 1 . \tag{5.2.1}$$

We choose the linear fractional transformations

$x : z \longrightarrow (-1)/z$ and $y : z \longrightarrow (z+1)/(2-z)$ (5.2.2)

satisfying (5.2.1). Let q be a prime-power. We then parametrize the actions of $H(2,6)$ on $PL(F_q)$ using the method described in Section 2.2. Let X, Y and T denote the elements of $GL(2,\mathbb{Z})$ which yield the elements $\bar{x}$, $\bar{y}$ and $\bar{t}$ in $PGL(2,q)$, where $\bar{x} = x\alpha$, $\bar{y} = y\alpha$ and $\bar{t} = t\alpha$, for some non-degenerate homomorphism α from the group $G(2,6)$ with presentation

$$\langle x,y,t : x^2 = y^6 = t^2 = (xt)^2 = (yt)^2 = 1\rangle$$

into $PGL(2,q)$. Then X, Y and T will satisfy the relations

$$X^2 = Y^6 = T^2 = (XT)^2 = (YT)^2 = \lambda I \qquad (5.2.3)$$

for some scalar λ. As in Section 2.2, we choose the matrices X, Y and T to be

$$\begin{bmatrix} a & cl \\ c & -a \end{bmatrix}, \begin{bmatrix} e & fl \\ f & m-e \end{bmatrix} \text{ and } \begin{bmatrix} o & -l \\ 1 & o \end{bmatrix},$$

respectively, where $l \neq 0$ and a,c,e,f,l are in F_q. Also, $m \equiv x \pmod q$, for some x in F_q. To find m, the trace of Y, we adopt the following method.

Since $y^6 = 1$, we have $Y^6 = \lambda I$. As in Theorem 3.3.1, we deduce that some scalar multiple of Y is conjugate to the matrix $\begin{bmatrix} z & o \\ o & z^{-1} \end{bmatrix}$, where z is 12th root of unity. So that we have $z^{12} = 1$, thus giving $(z^6-1)(z^6+1) = 0$.

Now since $z^6-1 \neq 0$ (as $z^6 \neq 1$), therefore $z^6 + 1 = 0$, thus giving $(z^2+1)(z^4-z^2+1) = 0$. This further implies that

$$z^4-z^2+ 1 = 0, \qquad (5.2.4)$$

because $z^2+ 1 \neq 0$. Now $z^6 + 1 = 0$ implies that $z^6 = -1$, so that $z^4 = -z^{-2}$. Hence Equation (5.2.4) becomes

$$z^2 + z^{-2} - 1 = 0. \qquad (5.2.5)$$

But $m = z + z^{-1}$; so that $m^2 - 2 = z^2 + z^{-2}$. Substituting in (5.2.5), we obtain $m^2 - 2 - 1 = 0$, or $m^2 = 3$, implying that $m = \pm \sqrt{3}$.

Let $m = \sqrt{3}$, so that $tr(Y) = \sqrt{3}$ where Y satisfies the relation $Y^6 = \lambda I$ for some scalar λ.

We now find some conditions on q for the existence of some special fragments in $D(\vartheta,q,6)$ in our next section.

5.3 Some Special Fragments in $D(\vartheta,q,6)$

Consider the fragments γ_1, γ_2 and γ_3 having fixed points of $\bar{x}$, $\bar{y}$ and $\bar{t}$ respectively.

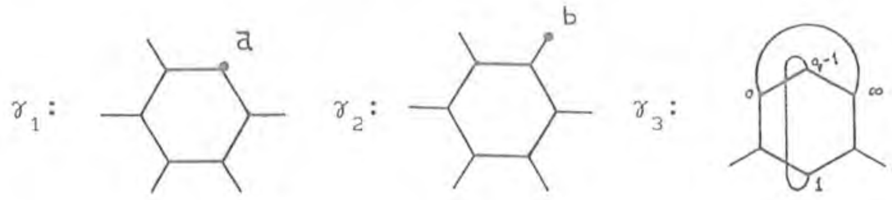

Figure 22

REMARK 5.3.1

We observe that the fragment:

(i) γ_1 exists in $D(\vartheta,q,6)$ iff $q \equiv 1 \pmod 4$

(ii) γ_2 exists in $D(\vartheta,q,6)$ iff $q \equiv 1 \pmod 3$

(iii) γ_3 exists in $D(\vartheta,q,6)$ iff $q \equiv \pm 1 \pmod{12}$.

Note that since $\bar{x}^2 = 1$, we can choose $\bar{x}$ to be the linear fractional transformation $\bar{x} : z \longrightarrow (-1)/z$. Thus for the fixed point of $\bar{x}$, say a, we have $(a)x = -1/a = a$, giving the equation $a^2 + 1 = 0$ or the discriminant equal to -4. Hence the circuit γ_1 exists in $D(\vartheta,q,6)$ if and only if -4 is a square in F_q, provided q is not a power of 2. Also since $\bar{y}^6 = 1$, we choose $\bar{y}$ to be the linear fractional transformation $z \longrightarrow (z+1)/(2-z)$. Thus for any fixed point b of $\bar{y}$, we have $(b)\bar{y} = (b+1)/(2-b) = b$, which implies $b^2 - b + 1 = 0$, so that the discriminant is equal to -3. Hence γ_2 exists in $D(\vartheta,q,6)$ if and only if $q \equiv 1 \pmod 3$.

Note that since $\bar{t}$ is the linear fractional transformation $z \longrightarrow 1/z$, the points 1 and q-1 are fixed by $\bar{t}$ and hence lie on the vertical axis of symmetry. Also we have observed that γ_3 exists in $D(\vartheta,q,6)$ iff $q \equiv \pm 1 \pmod{12}$.

5.4 The Coset Diagrams D(3,q,6)

In this section we find the conditions for the existence of some circuits in the coset diagrams $D(3,q,6)$. Here $\vartheta = 3$ is the only parameter which gives the coset diagrams for the actions of $\Delta^*(2,6,6)$, with presentation

$$<x,y,t:x^2=y^6=t^2=(xt)^2=(yt)^2=(xy)^6=1>, \qquad (5.4.1)$$

on $PL(F_q)$. Let $\bar{g}$ be an element of $PGL(2,q)$. We choose $\bar{g} = \bar{x}\bar{y}$ and discuss only those coset diagrams in which every element is fixed by $(\bar{x}\bar{y})^6$.

By substituting n = 6 in the Equation (4.2.5), we observe that $(XY)^6 = \lambda I$, for some scalar λ, if and only if ${}^5C_0 r^5 - {}^4C_1 r^3\Delta + {}^3C_2 r\Delta^2 = 0$, implying that $r(r^4 - 4r^2\Delta + 3\Delta^2) = 0$. Since $r^2 = \vartheta\Delta$, we multiply the above equation by r/Δ and thus obtain the polynomial equation in ϑ as $\vartheta(\vartheta^2-4\vartheta+3) = 0$, or $\vartheta(\vartheta-3)(\vartheta-1) = 0$, thus giving $\vartheta = 0$, 1 and 3 as its roots.

Now for $\vartheta = 0$, the coset diagram D(0,q,6) depicts the actions of the dicyclic groups $\Delta(2,6,2)$ on $PL(F_q)$. Also for $\vartheta = 1$, the coset diagram D(1,q,6) depicts the actions of the groups $\Delta(2,6,3)$ on $PL(F_q)$.

Consider, for example, the coset diagrams D(0,11,6)

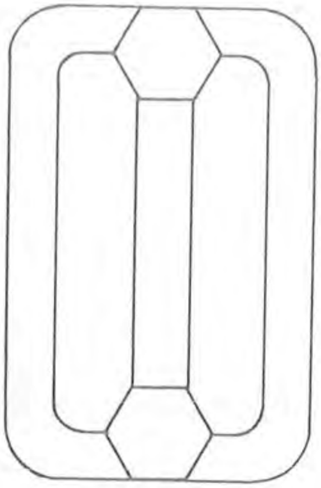

Figure 23

and D(1,13,6)

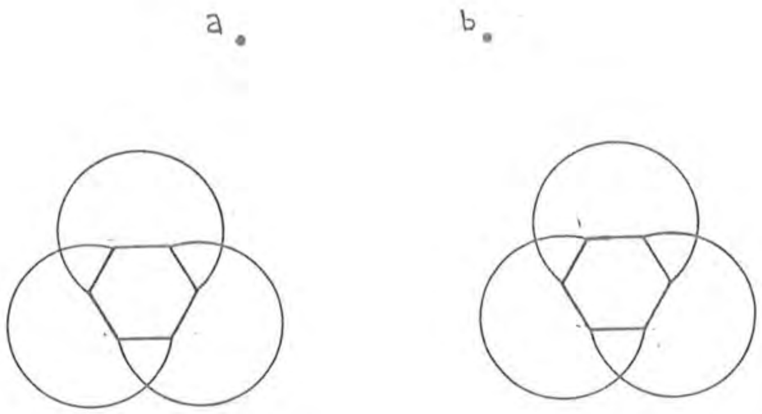

Figure 24

depicting the images of the groups $\Delta(2,6,2)$ and $\Delta(2,6,3)$, on $PL(F_{11})$ and $PL(F_{13})$, respectively. In Figure 24, the points a and b are fixed points of both $\bar{x}$ and $\bar{y}$.

Considering the case for $\vartheta = 3$, we observe that this is the only parameter which gives the coset diagrams D(3,q,6) for the actions of $\Delta(2,6,6)$ on $PL(F_q)$.

We shall now discuss some special fragments of D(3,q,6) and find the conditions for their existence in D(3,q,6). First consider the fragments, namely:

γ_4 :

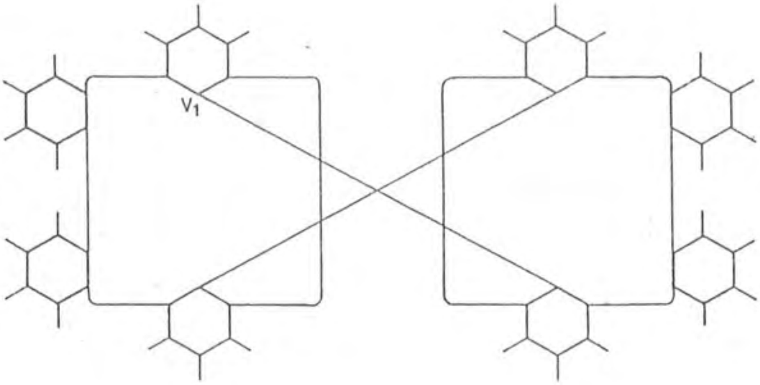

Figure 25

γ_5 :

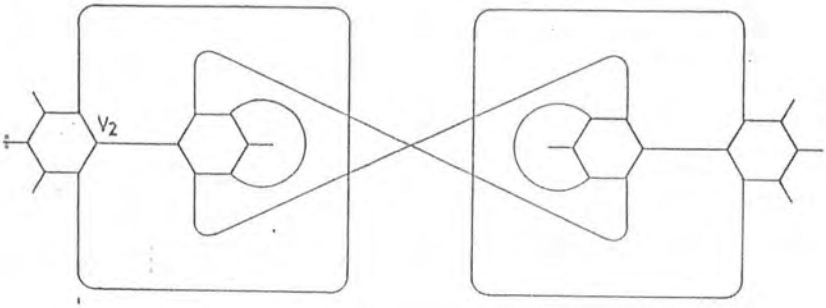

Figure 26

γ_6 :

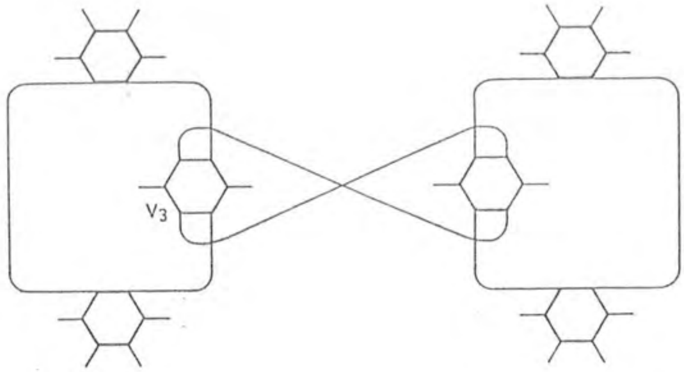

Figure 27

γ_7 :

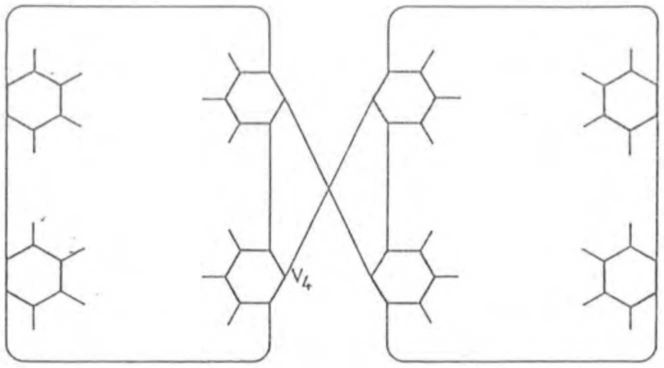

Figure 28

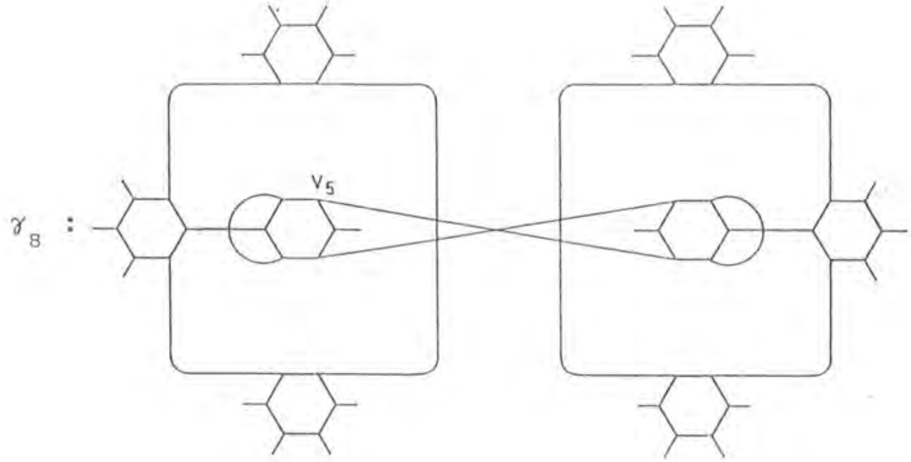

Figure 29

Theorem 5.4.1

The fragment γ_4 will occur in D(3,q,6) if and only if 60 is a square in F_q.

Proof

Let v_1 be the vertex fixed by the element $\overline{x}\overline{y}\overline{x}\overline{y}\overline{t}$ of PGL(2,q). Then $\overline{x}\overline{y}\overline{x}\overline{y}\overline{t} = (\overline{x}\overline{y})^2(\overline{x}\overline{y}^{-1})^2$. Let M be the matrix representing the element $(\overline{x}\overline{y})^2(\overline{x}\overline{y}^{-1})^2$ so that

$$M = (XY)^2(XY^{-1})^2 = (XY)^2(XY^5)^2 , \qquad (5.4.2)$$

where X and Y are the matrices representing $\bar{x}$ and $\bar{y}$ respectively. Considering the characteristic equation of XY, namely, $(XY)^2 - rXY + \Delta I = 0$, we obtain $(XY)^2 = rXY - \Delta I$. Here $r = tr(XY)$ and $\Delta = det(XY)$, as defined in Chapter 2. Also from the characteristic equation of Y, that is, $Y^2 - \sqrt{3}Y + I = 0$, we get $Y^5 = Y - \sqrt{3}$.

Thus substituting the values of $(XY)^2$ and Y^5 in (5.4.2), we get

$$M = (r^3-5r\Delta)XY + (-2\sqrt{3}r^3+4\sqrt{3}r\Delta)X+(-2\sqrt{3}r^2\Delta+2\sqrt{3}\Delta^2)Y + (5r^2\Delta-2\Delta^2)I.$$

Since $tr(XY) = r$, $tr(X) = 0$, $tr(Y) = \sqrt{3}$ and $tr(I) = 2$, we thus obtain $tr(M) = r^4 - r^2\Delta + 2\Delta^2$. Also, since $det(X) = \Delta$, and $det(Y) = 1$, by our assumption, we have $det(M) = \Delta^4$. Hence the characteristic equation of M will be

$$M^2-(r^4-r^2\Delta+2\Delta^2)M + \Delta^4 I = 0, \qquad (5.4.3)$$

giving the discriminant as

$$d(r,\Delta) = r^8 - 2r^6\Delta + 5r^4\Delta^2 - 4r^2\Delta^3. \qquad (5.4.4)$$

Substituting $r^2 = \vartheta\Delta$ in (5.4.4), we get the polynomial in ϑ as $f(\vartheta) = \vartheta^4 - 2\vartheta^3 + 5\vartheta^2 - 4\vartheta$. Thus for $\vartheta = 3$, we have $f(3) = 60$.

Hence we conclude that the fragment γ_4 will occur in D(3,q,6) iff 60 is a square in F_q.

Theorem 5.4.2

The fragments γ_5 and γ_6 will occur in D(3,q,6) if and only if 60 is a square in F_q.

Proof

Here the vertices v_2 and v_3 are fixed by the elements $\overline{xyxy}^{-2}\overline{xyx}$ and $\overline{xy}^{4}\overline{xy}^{2}$ of PGL(2,q), respectively. Following the same method as used in the proof of Theorem 5.4.1, we find that both the fragments γ_5 and γ_6 will occur in D(3,q,6) if and only if 60 is a square in the field F_q.

Hence γ_4, γ_5 as well as γ_6 will occur in D(3,q,6) if and only if 60 is a square in F_q.

Also, considering the fragments γ_7 and γ_8, we notice that the vertices v_4 and v_5 are fixed by the elements $(\overline{xy})^2(\overline{xy}^{-1})^2$, which is same as for the fragment γ_4. So that a diagram D(3,q,6) can contain any of the fragments γ_4, γ_7 and γ_8.

Let γ_9, γ_{10} and γ_{11} denote respectively the following fragments.

γ_9:

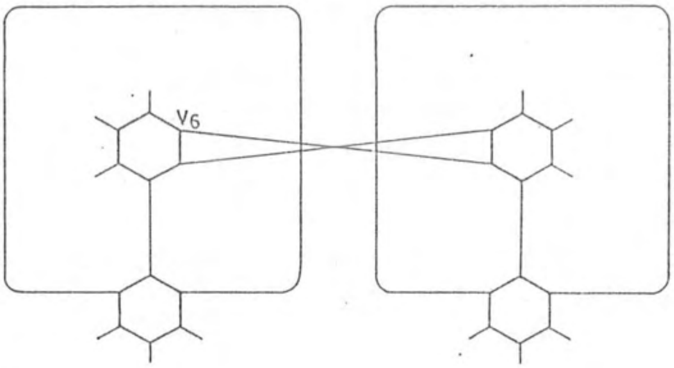

Figure 30

γ_{10}:

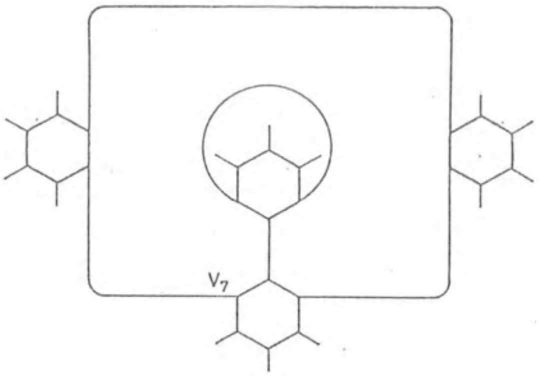

Figure 31

γ_{11}:

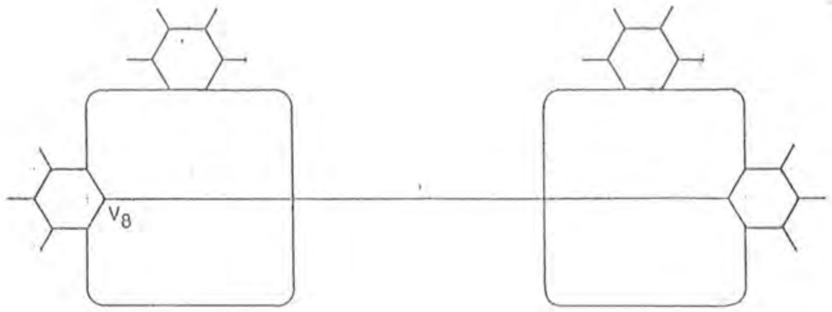

Figure 32

Then following the procedure as adopted in the proof of Theorem 5.4.1, we have the following result.

Theorem 5.4.3

The diagram D(3,q,6) will contain the fragment (or a homomorphic image of) :

(i) γ_9 iff 12 is a square in F_q

(ii) γ_{10} iff 15 is a square in F_q

(iii) γ_{11} iff 8 is a square in F_q .

Note that all these fragments are symmetric about the vertical axis.

Example 5.4.4

If we draw the coset diagram D(3,71,6) for the action of $\Delta(2,6,6)$ on $PL(F_{71})$, then since 8,12,15 and 60 are all squares in F_{71}, the diagram contains the fragments γ_4, γ_5, γ_6, γ_9, γ_{10} and γ_{11}.

We now find the primes p for which 3 is a quadratic residue using the classical Legendre symbolism. Clearly 3 is residue of 2. Suppose p is a prime other than 2 or 3. Since $3 \equiv 3 \pmod 4$, we have

$$(3/p) = \begin{cases} (p/3) & \text{if } p \equiv 1 \pmod 4 \\ -(p/3) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

We know that $p \equiv 1$ or $2 \pmod 3$ and that $(1/3) = 1$ and $(2/3) = -1$. So that, $(3/p) = 1$ if and only if

$$p \equiv 1 \pmod 4 \text{ and } p \equiv 1 \pmod 3 \qquad \text{(i)}$$

or

$$p \equiv 3 \pmod 4 \text{ and } p \equiv 2 \pmod 3. \qquad \text{(ii)}$$

Then conditions in (i) are equivalent to $p \equiv 1 \pmod{12}$; those in (ii) to $p \equiv -1 \pmod{12}$. Thus we have shown that $(3/p) = 1$ if and only if $p = 2$ or $p \equiv \pm 1 \pmod{12}$. So that the prime numbers p that we choose for the coset diagrams D(3,p,6), (p having squares of 3), are of the form 12k ± 1, where $k \in \mathbb{Z}^+$.

To prove our main result, we shall need the coset diagrams D(3,p,6) containing the fragment γ_9 (Figure 30). As shown in Figure 33, we just consider the patch having the pattern of 'holding hands'.

γ_{12}:

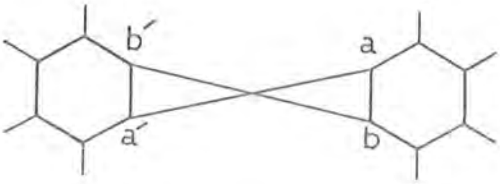

Figure 33

If we consider the vertices a,b,a',b' in Figure 33 as fixed points (of x) by 'breaking' the edges aa' and bb', we see that the whole diagram shall still be the coset diagram D(3,p,6) depicting the homomorphic images of the group Δ(2,6,6). For, if $(ab'c_1c_2c_3c_4)$ and $(a'bd_1d_2d_3d_4)$ are the cycles of xy before 'breaking' the edges aa' and bb', then $(abc_1c_2c_3c_4)$ and $(a'b'd_1d_2d_3d_4)$ shall be the cycles of xy after we 'break' the 'hands' aa' and bb', and consider the vertices a,b,a',b' as fixed points of x. All other cycles of xy are unchanged. In particular, xy still has order 6.

For our required result, we also need the coset diagrams containing the fragment γ_{13} as shown in the following figure.

γ_{13}:

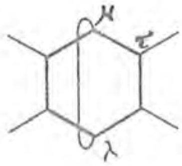

Figure 34

The vertices labelled λ, τ and μ have been indicated for a reason that shall be explained later. First we find a condition for the existence of γ_{13} in D(3,p,6) in the form of a theorem that follows. Note that the vertices λ and μ are the fixed points of t, so that the edge $\lambda\mu$ lies on the vertical axis of symmetry.

Let ϕ be the parameter for the dual homomorphism α' of the non-degenerate homomorphism

α. Then as shown in Chapter 2, $\vartheta+\phi = 4-m^2$, where, as defined earlier, m is the trace of the matrix Y satisfying $Y^n = \lambda I$, for some scalar λ. Now since we are dealing with the group H(2,6) we find m to be equal to $\sqrt{3}$, so that we have $\vartheta+\phi = 4-(\sqrt{3})^2 = 4-3 = 1$. Thus if ϑ is the parameter for α then $(1-\vartheta)$ shall be the parameter for α'.

Next we prove the following:

Theorem 5.4.5

The fragment γ_{13} exists, with λ, μ fixed by $\bar{t}$, in D(3,p,6) if and only if 6 is a square in F_p.

Proof

The proof is a direct consequence of Theorem 3.4.2, by substituting $m = \sqrt{3}$ and $\vartheta = 3$.

Having found the conditions for ϑ and p in the coset diagram D(3,p,6) and the existence of certain special fragments in D(3,p,6), we finally give our main result in the form of a theorem.

5.5 Application of Coset diagrams and their Fragments

Conder [6], uses small coset diagrams as building blocks and connects them together to form a large diagram. The method of pasting together these diagrams is called j-composition. Though j-composition preserves the orders of x, y and xy, but it preserves very little else, so that it is hard to control the structure of the group that emerges. But for the coset diagrams for the actions of the group G(2,n) on $PL(F_q)$, the situation is quite otherwise.

Theorem 5.5.1

Let n = p+1, where p is a prime such that 6 and 12 are squares in F_p and n = 2(1+r) for a prime r. Then for all such n, both A_n and S_n occur as homomorphic images of $\Delta(2,6,6)$.

Proof

To prove our result we choose a prime number p such that $p = 12k \pm 1$, where $k \in \mathbb{Z}^+$. Also these p's are such that the fields F_p should contain squares of 6 and 12, so that the coset diagrams D(3,p,6) should contain the fragments γ_{12} and γ_{13}. Let us denote the coset diagrams, having these properties by $D^*(3,p,6)$. Now since we are considering the actions of the group $G(2,6)$ on $PL(F_p)$, the degree of this group will be $n = p + 1$. Let us express this n as $n = 2(1+r)$, for some positive integer r. Considering the points a, b, a′, b′ of γ_{12} (in Figure 33) as fixed points of x, we trace out the cycles of xyt and find the parity of these cycles. We observe that the vertices a, a′ form a cycle (of xyt) of length 2. The other cycles, containing b and b′ then form either cycles of length r separately or a single cycle of length 2r containing the points b and b′.

Now we need to consider only those coset diagrams $D^*(3,p,6)$ in which r is some prime integer. So that the length of the cycles containing b and b′, separately, is a prime number, concluding $(xyt)^s = 1$ for some $r = s$. We see that the cycle containing the point b, which is now of some prime length, also contains the vertices λ , μ and τ (as shown in Figure 34). So that we form a block, say B, in $D^*(3,p,6)$ containing the points λ, μ, τ as well as b. It is obvious, from Figure 34, that $\lambda x = \mu$, $\tau y = \mu$ and $\mu t = \mu$, (where λ, τ and μ

$\in B$), so that B is preserved by x, y and t. This implies that B is a union of orbits of $\langle x,y,t \rangle$. But from the connectedness of $D^*(3,p,6)$, we can easily check that the group $\Delta(2,6,6)$ is transitive. Hence $|B| = n$, thus also proving the primitivity of the group $\Delta(2,6,6)$. The group $\Delta(2,6,6)$ being primitive and having an element xyt of prime order, we can now use Jordan's theorem 13.9 in [29], to conclude the proof.

REFERENCES

[1] R. Bowen and C. Series, Markov maps associated with Fuchsian groups, Publ. Math. IHES, 50(1979), 153-170.

[2] W. Burnside, 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(1878b), 174-176.

[4] M.D.E. Conder, Minimal generating pairs for permutation groups, D.Phil. thesis, University of Oxford, (1980).

[5] M.D.E. Conder, Generators for alternating and symmetric groups, Jour. London Math. Soc., (2), 22(1980), 75-86.

[6] M.D.E. Conder, On the group $G^{6,6,6}$, Quat. J. Math. Oxford (2), 39(1988), 175-183.

[7] M.D.E. Conder, More on generators for alternating and symmetric groups, Quat. J. Math. Oxford (2), 32(1981), 137-163.

[8] M.D.E. Conder, A note on Cayley graphs, J.Combinatorial Theory, Series B, (3), 40(1986), 362-368.

[9] H.S.M. Coxeter and W.O.J. Moser, Generators and relations for discrete groups, Springer Verlag, 1965, Berlin.

[10] M. Dehn, Uberunedliche diskontinuierliche gruppen, Math. Ann. 71, 114-116.

[11] I.M.S. Dey and J. Wiegold, Generators for alternating and symmetric groups, J. Australian Math. Soc. 12(1971), 63-68.

[12] H. Hilton, An introduction to the theory of groups of finite orders, Oxford, Clarendon Press, 2908.

[13] M.G. Humbert, Sur les fractions continues et les formes quadratiques binaries indefinies, C.R. Acad. Sci. Paris, 162(1916), 23-26, 67-73.

[14] A. Hurwitz, Uber algebraishe Gebilde mit eindeutsgen transformationen in sich Math. Ann., 41(1883), 403-442.

[15] Q. Mushtaq, Reduced indefinite binary quadratic forms and orbits of the modular groups, Radovi. Mat., 4(1988), 33-36.

[16] Q. Mushtaq, A condition for the existence of a fragment of a coset diagram, Quart. J. Math., Oxford, (2), 39(1988), 81-95.

[17] Q. Mushtaq, On Word structure of the modular group over finite and real quadratic fields, (submitted).

[18] Q.Mushtaq and F.Shaheen, On subgroups of polyhedral groups, Math. Japonica, 35, 5 (1990), 1-5.

[19] Q.Mushtaq, Coset diagrams for Hurwitz groups, Comm. in Algebra, (11), 18(1990), 3857-3888.

[20] Q. Mushtaq, Coset diagrams for the modular group, D.Phil. thesis, University of Oxford, 1983.

[21] P.M. Neumann, The SQ-universality of some finitely presented groups, J. Austral. Math., Soc. 16(1973), 1-6.

[22] O. Schreier, Die untergruppen der freien gruppen, Abh. Math., Sem. Univ. Hamburg, 5(1927), 161-183.

[23] F. Shaheen, Graphical representations of certain groups, M.Phil. thesis, 1986, Quaid-i-Azam University, Islamabad.

[24] R. Steinberg, Finite reflection groups, Trans. Amer. Math., Soc. 91(1959), 493-504.

[25] W.W. Stothers, Subgroups of (2,3,7) triangle group, Manuscripta Math., 20(1977), 323-334.

[26] T.W. Tucker, Finite groups acting on surfaces and the genus of a group, J. Combinatorial Theory Ser.B, 34(1983), 82-98.

[27] T.W. Tucker, A refined Hurwitz theorem for imbeddings of irredundant Cayley graphs, J. Combinatorial Theory B, 36(1984), 244-268.

[28] J.H.C. Whitehead, On certain sets of elements in a free group, Proc. London. Math., Soc. Ser.2, 41(1936a), 48-56.

[29] H. Wielandt, Finite permutation groups, Academic Press, New York and London, 1964.