The Galois Group of a Polynomial

By

Muhammad Asif

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2010

بسم الله الرحمن الرحيم

The Galois Group of a Polynomial

By

Muhammad Asif

Supervised By

Prof. Dr. Qaiser Mushtaq

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2010

The Galois Group of a Polynomial

By

Muhammad Asif

A Dissertation Submitted in the Partial Fulfillment of the Requirements for The Degree of

MASTERS OF PHILOSOPHY
IN
MATHEMATICS

Supervised By

Prof. Dr. Qaiser Mushtaq

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2010

The Galois Group of a Polynomial

By

Muhammad Asif

CERTIFICATE

A DISSERTATION SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF THE MASTER OF PHILOSOPHY

We accept this dissertation as conforming to the required standard

1. ______________________

Prof. Dr. Qaiser Mushtaq
(Supervisor)

2. ______________________

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

3. ______________________

Prof. Dr. Muhammad Ayub
(Chairman)

Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN 2010

Dedicated

To my

Parents
Especially to my Mother

whose affection is a reason of every success in my life.
Who've always given me perpetual love, care, and cheers. Whose prayers have always been a source of great inspiration for me and whose sustained hope in me led me to where I stand today.

Acknowledgements

*Praise is to **Allah Almighty**, the omnipotent and the most compassionate, who bestowed on me the potential and ability to complete the research for my dissertation. All respects to the **Holy Prophet Hazrat Muhammad (S. A.W.W.)**, who is forever a source of guidance and knowledge for humanity as a whole.*

*I cannot fully express my gratitude towards my supervisor **Professor Dr. Qaiser Mushtaq**, for his cooperation, valuable instructions, beneficial remarks and superb guidance. He showed me the right way of doing research. His kind attitude and encouragement broadened my vision of the subject, my knowledge and also increase my capabilities of research and hard work.*

*My love and gratitude from the core of my heart towards my loving mother, caring father **Abdul Sattar Memon**, friendly uncles **Abdul Razzaque Memon** and **Farid Ahmed Memon**, my sisters and brothers namely **Aijaz Ahmed, Ayaz Ahmed** especially towards the twins **Danish** and **Adnan** for their prayers, support and encouragement. It is they who have always given me love, care and cheer and whose sustained hope in me led me to where I stand today. I have no words to express my sweet sensation of thanks for my friends **Javed Brohi, Abdul Manan, Nasir Siddiqui, Fazal ur Rehman, Tariq Nawaz, Gauhar Ali, Muhammad Raees, Muhammad Yousuf, Asif Mehmood, Atlas Khan, Shakoor Muhammad, Ikramullah, Imran Khan, Zubair Ahmed, Barkat Ali, Parvez Ali, Shahid Ali, Zafar Ali, Zubair Dayo, Kaleemullah Bhatti, Saqib Mazhar, Itrat Qarnain, Kamran Shafique, Adnan But and Zaheer Munawar.***

Almighty Allah may shower His choicest blessings and prosperity on all those who assisted me in any way during completion of my dissertation.

Muhammad Asif
Feb 2010

Contents

Preface

Actions of $PGL(2,\mathbb{Z})$ on projective lines over finite fields, $PL(F_q)$, where q is a prime power, have been parametrized by Q. Mushtaq in 1980. Corresponding to each θ in F_q, a class of non-degenerate homomorphisms from $PGL(2,\mathbb{Z})$ to $PGL(2,q)$ is associated. Each class is represented by a coset diagram $D(\theta,q)$. In this dissertation we consider $D(\theta,q)$ representing $\Delta(2,3,7)$. Certain fragments of these diagrams occur frequently. Q. Mushtaq has found conditions of their existence and the frequency with which they occur. Following his method we consider one of the fragments and determine condition of its existence and the frequency, which is related to the Galois group attached with it, with which it occurs in the coset diagram for $\Delta(2,3,7)$.

The first chapter is purely devoted to some relevant definitions. A few examples are given to illustrate these definitions.

In the second chapter our main focus is on the construction of the Galois Group. For this we introduce some relevant definitions along with few examples to illustrate these definitions. Particularly, we discuss Finite Fields, Extension Fields, Fixed Fields, Splitting Fields and the Galois Groups.

In the third chapter we give an introduction of graphs depicting group actions. In this chapter we describe parametrization of the conjugacy classes of actions of the infinite triangle group $\Delta(2,3,7)$ on projective lines over the finite fields F_q. For each $\theta \in F_q$ we associate a coset diagram $D(\theta,q)$ depicting the conjugacy class of actions of $\Delta(2,3,7)$ on $PL(F_q)$. Following Q. Mushtaq's method we consider one of the fragments and determine condition of its existence and the frequency, which is related to the Galois group attached with it, with which it occurs in the coset diagram for $\Delta(2,3,7)$.

Chapter 1

Important Groups

In this chapter we give some relevant definitions along with few examples to illustrate these definitions. Particularly, we discuss Permutation Groups, Dihedral Group, Linear Group, Modular Group, Triangle Groups and particularly, the Triangle Group $\Delta(2,3,7)$.

In the following section we give definitions of some important and relevant groups.

1.1 Permutation Groups

Let Ω be a non-empty set and $Sym(\Omega)$ be the set of all permutations from Ω to itself. Then $Sym(\Omega)$ is a group under function composition. It is called a permutation group on the set Ω. When Ω has n elements $Sym(\Omega)$ is denoted by S_n and is referred to as a symmetry group of degree n. The order of the permutation group is $n!$. For example for $n = 3$, $S_3 = \{I, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ is a permutation group on the set of three elements. Even permutations of S_n form a group well known as an alternating group and denoted by A_n.

The permutation groups have significant importance due to the fact that any finite group of order n is a subgroup of S_n. Abstract definitions of a few permutation groups are as follows.

$$S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$$
$$S_4 = \langle x, y : x^2 = y^3 = (xy)^4 = 1 \rangle$$
$$A_4 = \langle x, y : x^2 = y^3 = (xy)^3 = 1 \rangle$$
$$A_5 = \langle x, y : x^2 = y^3 = (xy)^5 = 1 \rangle.$$

Dihedral Groups

Let Δ_n denote a regular polygon with $n \geq 3$ number of vertices. The n rotations of Δ_n through angles $0, 2\pi/n, ..., 2(n-1)\pi/n$, together with n reflections about the line joining opposite vertices of Δ_n and the lines joining the midpoints of opposite edges of Δ_n (if n is even) or about the lines joining vertices of Δ_n to midpoints of opposite edges (if n is odd) form a group. This group is called a dihedral group of order $2n$ and is denoted by D_n or D_{2n}. If a denotes the rotation about the centre of Δ_n through an angle $2\pi/n$ and b is any one of the reflections in Δ_n then the abstract definition of D_{2n} is

$$D_{2n} = \langle a, b : a^n = b^2 = (ab)^2 = 1 \rangle.$$

In the set tabular form D_{2n} is the group $\{1, a, a^2, ..., a^{n-1}, b, ab, a^2b, ..., a^{n-1}b\}$. In fact D_{2n} is independent of the size of Δ_n and its position in the plane. It depends only on the number of edges of Δ_n. Since $a^{-1} \neq a$, the group D_{2n} is non-abelian.

Next section gives an introductory note on linear groups.

Linear Groups

Let F be a field and n a positive integer. The set of $n \times n$ matrices with entries from F is denoted by $M_n(F)$. Then $GL(n, F) = \{M \in M_n(F) : M \text{ is invertible}\}$ is a group under matrix multiplication. It is referred as an $n-$dimensional general linear group over F. If $|F| = r$ where r is finite, then $|GL(n, F)| = (q^n - 1)(r^n - r)(r^n - r^2)...(r^n - r^{n-1})$. The $n-$dimensional special linear group is defined by $SL(n, F) = \{M \in GL(n, F) : \det(M) = 1\}$. The group $SL(n, F)$ is a normal subgroup of $GL(n, F)$. Let $F^\times$ denote the multiplicative group of non-zero elements of F. Then the determinant map det:$GL(n, F) \longrightarrow F^\times$ is a group epimorphism and has $SL(n, F)$ as its kernel. Hence, $GL(n, F)/SL(n, F)$ is isomorphic to $F^\times$.

The projective groups are obtained from corresponding ordinary linear groups by identifying matrices that are scalar multiples of each other. Let F be a field and n be a positive integer. Then $Z = \{aI_n : a \in F^\times\}$ is the set of scalar matrices which is the normal subgroup of $GL(n, F)$ as $X^{-1}MX = M$ for all $X \in Z$ and for all $M \in GL(n, F)$. The $n-$dimensional projective linear group is the quotient group of $GL(n, F)$ by Z and defined by $PGL(n, F) = GL(n, F)/Z$.

The projective special linear group, denoted by $PSL(n, F)$, is obtained by taking factor group of $SL(n, F)$ with the intersection of $SL(n, F)$ and Z. Hence it is defined as

$$PSL(n, F) = SL(n, F)/(SL(n, F) \cap Z = SL(n, F)/Z.$$

1.2 Modular Group

The modular group is the group $PSL(2, \mathbb{Z})$, consisting of all Mobius transformations $z \longrightarrow \frac{az+b}{cz+d}$ where $a, b, c, d \in \mathbb{Z}$ with $ad-bc = 1$. This group has a finite presentation $< x, y : x^2 = y^3 = 1 >$ in terms of transformations $x : z \longrightarrow \frac{-1}{z}$ and $y : z \longrightarrow \frac{z-1}{z}$. $PSL(2, \mathbb{Z})$ is a free product of a cyclic group $< x >$ of order 2 and a cyclic group $< y >$ of order 3. The modular group $PSL(2, \mathbb{Z})$ is a discrete group.

In the following we give a list of normal subgroups of $PSL(2, \mathbb{Z})$ upto index 100.

$S.No$	$Index$	$Generators$
1	1	x, y
2	2	y
3	3	x
4	6	$xyxy^{-1}$
5	6	$xy^{-1}xy^{-1}$
6	12	$xy^{-1}xy^{-1}xy^{-1}$

S.No	*Index*	*Generators*
7	18	$xyxyxy^{-1}xy^{-1}$
8	24	$xyxy^{-1}xyxy^{-1}$
9	24	$xy^{-1}xy^{-1}xy^{-1}xy^{-1}$
10	42	$xyxyxy^{-1}xyxy^{-1}xy^{-1}, xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}$
11	42	$xyxy^{-1}xyxyxy^{-1}xy^{-1}, xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}$
12	48	$xyxyxyxy^{-1}xy^{-1}xy^{-1}$
13	48	$xyxy^{-1}xy^{-1}xyxy^{-1}xy^{-1}$
14	54	$xyxy^{-1}xyxy^{-1}xyxy^{-1}, xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}$
15	60	$xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}$
16	72	$xyxy^{-1}xyxy^{-1}xyxy^{-1}, xyxyxyxyxy^{-1}xy^{-1}xy^{-1}xy^{-1}$
17	72	$xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}, xyxy^{-1}xyxyxy^{-1}xyxy^{-1}xy^{-1}$
18	78	$xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}, xyxyxy^{-1}xyxy^{-1}xyxy^{-1}xy^{-1}$
19	78	$xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}, xyxy^{-1}xyxy^{-1}xyxyxy^{-1}xy^{-1}$
20	96	$xyxy^{-1}xyxy^{-1}xyxy^{-1}, xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}$
21	96	$xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1}, xyxy^{-1}xyxy^{-1}xyxy^{-1}xyxy^{-1}.$

The list of normal subgroups of $PSL(2,\mathbb{Z})$ upto index 1500 is available on the link www.designtheory.org/~peter/software/lowx/hecke/c2xc03.sp.gz.

The linear fractional transformation $t : z \longrightarrow \frac{1}{z}$ inverts x and y, that is, $t^2 = (xt)^2 = (yt)^2 = 1$ and extends the group $PSL(2,\mathbb{Z})$ to $PGL(2,\mathbb{Z})$. The extended modular group $PGL(2,\mathbb{Z})$ is then generated by x, y and t and its defining relations are:

$$x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1.$$

1.3 Triangle Groups

Triangle groups and their significance are well explained in [1] and [6]. Triangle groups are represented by $\Delta(l,m,n) = < x, y : x^l = y^m = (xy)^n = 1 >$ where $l, m, n \in \mathbb{Z}$ and $l, m, n > 1$.

Every countable group occurs as a subgroup of some quotient of $PSL(2,\mathbb{Z})$ [5]. The symmetric group of degree k $(k = 5, 6, 8)$ is itself a quotient of $PSL(2,\mathbb{Z})$. Similar properties are true even of the triangle groups with $n \geq 7$ [5]. The group $\Delta(l, m, n)$ is independent of the order in which l, m, n are listed.

It is known that $\Delta(l, m, n)$ is finite precisely when $\delta = \frac{1}{l} + \frac{1}{m} + \frac{1}{n} - 1 > 0$, and the groups which arise in this case are

$\Delta(1, n, n) \cong C_n$	Cyclic group of order n,
$\Delta(2, 2, n) \cong D_{2n}$	Dihedral group of order $2n$,
$\Delta(2, 3, 3) \cong A_4$	Tetrahedral group,
$\Delta(2, 3, 4) \cong S_4$	Octahedral group and
$\Delta(2, 3, 5) \cong A_5$	Icosahedral group.

If $\delta = \frac{1}{l} + \frac{1}{m} + \frac{1}{n} - 1 = 0$ that is if $(l, m, n) = (2, 3, 6), (2, 4, 4)$ or $(3, 3, 3)$ then the group $\Delta(l, m, n)$ is infinite. The commutator subgroup and the factor commutator group is cyclic of order n. The triangle groups $\Delta(l, m, n)$ are infinite if and only if

$$\delta = \frac{1}{l} + \frac{1}{m} + \frac{1}{n} - 1 \leq 0.$$

The triangle groups $\Delta(2, 3, n)$ are especially important for being homomorphic images of $PSL(2,\mathbb{Z})$. These triangle groups are infinite if and only if $n \geq 6$. The finite groups $\Delta(2, 3, n)$, $n \leq 5$ are well known and they are:

(*i*) Trivial

(*ii*) $S_3 =< x, y : x^2 = y^3 = (xy)^2 = 1 >$

(*iii*) $A_4 =< x, y : x^2 = y^3 = (xy)^3 = 1 >$

(*iv*) $S_4 =< x, y : x^2 = y^3 = (xy)^4 = 1 >$

(*v*) $A_5 =< x, y : x^2 = y^3 = (xy)^5 = 1 >$.

When $n = 6$, $\Delta(2, 3, 6)$ is an infinite group but soluble. Its commutator subgroup is a free abelian group on two generators, and the associated factor-commutator group is cyclic of order n.

Chapter 2

Fields and The Galois Groups

In this chapter our main focus is on the constructions of the Galois Groups and for this we introduce some relevant definitions along with few examples to illustrate these definitions. Particularly, we discuss Finite Fields, Extension Fields, Fixed Fields, Splitting Fields and The Galois Groups.

2.1 Finite Fields

The fields which have finitely many elements, play an important role in many branches of mathematics, such as number theory, group theory, projective geometry and many others. The most familiar examples of such fields are the fields $\mathbb{Z}_p$ for prime p, but these are not all. A finite field is uniquely determined up to isomorphism by the number of elements it contains; that this must be a power of a prime; that is for every prime p and integer $r > 0$, there exists a field with p^r elements. There do not exist fields with 6, 10, 12, 14, 18, 20, ... elements. The field with $q = p^r$ elements is written by $GF(q)$ or F_q, where GF stands for the Galois field.

The ring $\mathbb{Z}$ of integers induces a natural ring structure on $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, the integer modulo n. If n is a prime p, then $\mathbb{Z}_p$ is a field under this structure. Similarly

$(\mathbb{Z}_n)^r = \{(a_0, a_1, ..., a_{r-1}) : a_i \in \mathbb{Z}_n\}$, where n is prime, is a field. It is obtained in the following way.

1. Identify the sequence $(a_0, a_1, ..., a_{r-1})$ with the polynomial $a_0 + a_1t + a_2t^2 + ... + a_{r-1}t^{r-1}$ in the ring of polynomials $\mathbb{Z}_p[t]$.

2. Choose a polynomial $f(t)$ of degree r, which is irreducible in $\mathbb{Z}_p[t]$.

3. Define a multiplication of two sequences by multiplying the corresponding polynomials in $\mathbb{Z}_p[t]$ and then reducing modulo $f(t)$. It is always possible to choose $f(t)$ in such a way that the non zero elements of the field are just the powers: $t, t^2, t^3, ..., t^{p^r-1}$, the last of these being the multiplicative identity 1. The field constructed in this way is sometimes called the Galois field with p^r elements and is denoted by $GF(p^r)$.

Theorem 1 *A finite field $GF(p^r)$ of p^r elements exists for every prime power p^r.*

Example 2 *$GF(2^4)$ is constructed by choosing an irreducible polynomial. Here $f(t) = t^4+t+1$ is an irreducible polynomial of degree 4 in $\mathbb{Z}_2$.*

Elements of F_{2^4}	modulo $f(t)$ ..
0	0
t	t
t^2	t^2
t^3	t^3
t^4	$t+1$
t^5	t^2+t
t^6	t^3+t^2
t^7	t^3+t+1
t^8	t^2+1
t^9	t^3+t
t^{10}	t^2+t+1
t^{11}	t^3+t^2+t
t^{12}	t^3+t^2+t+1
t^{13}	t^3+t^2+1
t^{14}	t^3+1
t^{15}	1.

We summarize the relevant properties of a finite field.

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

2. If F is a finite field with q elements then F is isomorphic to the Galois field $GF(q)$. In particular, the structure of the field does not depend upon the choice of the irreducible polynomial $f(t)$.

3. The multiplicative group of $GF(p^r)$ is a cyclic group of order $p^r - 1$. A generator of this group is called a primitive element of the field.

4. The group of field automorphisms of $GF(p^r)$ is a cyclic group of order r generated by the automorphism $x \longrightarrow x^p$.

2.2 Extension Fields

A field E is an extension field of a field F if F is a subfield of E, that is, $F \leq E$.

Theorem 3 *Let F be a field and $f(x)$ be a non-constant polynomial in $F[x]$ then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Consider $F = \mathbb{R}$ and $f(x) = x^2 + 1 \in \mathbb{R}[x]$.

Since $f(x) = x^2 + 1$ is irreducible over $\mathbb{R}$ then $< x^2 + 1 >$ is a maximal ideal in $\mathbb{R}[x]$. So $\frac{\mathbb{R}[x]}{<x^2+1>}$ is a field.

Let $E = \frac{\mathbb{R}[x]}{<x^2+1>}$. Then we can view $\mathbb{R}$ as a subfield of E. Now let $\alpha \in E$ such that $\alpha = x + < x^2 + 1 >$ then by computing in $\frac{\mathbb{R}[x]}{<x^2+1>}$, we find

$$\begin{aligned} \alpha^2 + 1 &= \left(x + < x^2 + 1 >\right)^2 + 1 \\ &= \left(x^2 + 1\right) + < x^2 + 1 > \\ &= 0. \end{aligned}$$

Thus α is a zero of $x^2 + 1$.

An element α of an extension field E of a field F is algebraic over F if $f(\alpha) = 0$ for some non-zero $f(x) \in F[x]$. If α is not algebraic over F, then α is transcendental over F.

For instance, $\sqrt{2}$ is algebraic over $\mathbb{Q}$ for it is the zero of $x^2 - 2 \in \mathbb{Q}[x]$. In the following

$\sqrt{1+\sqrt{3}}$ is algebraic over $\mathbb{Q}$ because if

$\alpha = \sqrt{1+\sqrt{3}}$ then

$\alpha^2 = 1 + \sqrt{3}$ or

$\left(\alpha^2 - 1\right)^2 = 3$ or

$\alpha^4 - 2\alpha^2 - 2 = 0.$

Hence α is a zero of $x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$.

Let F be the additive group of all functions from $\mathbb{R}$ into $\mathbb{R}$. Consider $\mathbb{R}$ as the additive group of real numbers, and let c be any real number. Then $\Phi_c : F \longrightarrow \mathbb{R}$ is the evaluation homomorphism defined by $\Phi_c(f) = f(c)$ for all $f \in F$.

The following theorem shows the importance of the concept of the evaluation homomorphism.

Theorem 4 *Let E be an extension field of a field F and let $\alpha \in E$. Let $\Phi_\alpha : F[x] \longrightarrow E$ be the evaluation homomorphism such that $\Phi_\alpha(b) = b$ for $b \in F$ and $\Phi_\alpha(x) = \alpha$, then α is transcendental over F if and only if Φ_α gives an isomorphism of $F[x]$ with a subdomain of E, that is Φ_α is a one-to-one map.*

2.3 Fixed Fields

Let θ be an isomorphism of a field E onto some field. Then an element $a \in E$ is called left fixed by θ if $\theta(a) = a$. A collection S of isomorphisms of E leaves a subfield F of E fixed if each $b \in F$ is left fixed by every $\theta \in S$.

For instance, let $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Then the map $\theta : E \longrightarrow E$ defined by

$$\theta\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

for $a, b, c, d \in \mathbb{Q}$ is an automorphism of E. If we view E as $\left(\mathbb{Q}[\sqrt{2}]\right)[\sqrt{3}]$, then θ leaves $\mathbb{Q}[\sqrt{2}]$ fixed.

Theorem 5 *Let E be a field, and let F be a subfield of E. Then the set $G\left(\frac{E}{F}\right)$ of all automorphisms of E leaving F fixed forms a subgroup of the group of all automorphisms of E.*

The symbol $\frac{E}{F}$ does not mean in $G\left(\frac{E}{F}\right)$ a quotient space of some sort, but rather it means E is an extension field of the field F.

Let E be a finite extension of a field F. The number of isomorphisms of E onto a subfield $\overline{F}$ leaving F fixed is the index $\{E : F\}$ of E over F.

Theorem 6 *If $F \leq E \leq K$ where K is a finite extension field of the field F, then*

$$\{K : F\} = \{K : E\}\{E : F\}.$$

Let E be a field and F be a subfield of E. The dimension of the vector space E over F is called the degree of $\frac{E}{F}$ and is denoted by $[E : F]$.

A finite field extension E of F is a separable extension of E if

$$\{E : F\} = [E : F].$$

Theorem 7 *If K is a finite extension of E and E is a finite extension of F, that is $F \leq E \leq K$, then K is separable over F if and only if K is separable over E and E is separable over F.*

Let E be a field extension of F. A subfield L of E is called an intermediate field of $\frac{E}{F}$ if $F \leq L \leq E$.

2.4 Splitting Fields

Let K be a field. A polynomial $f(x) \in K[x]$ is said to split over a field $S \supseteq K$ if $f(x)$ can be factored as a product of linear factors in $S[x]$. A field S containing K is said to be a splitting field for $f(x)$ over K if $f(x)$ splits over S, but over no proper intermediate field $\frac{S}{K}$.

For instance, $\mathbb{C}$ is the splitting field for the polynomial $f(x) = x^2 + 1$ over $\mathbb{R}$. Since $x^2 + 1 = (x + i)(x - i) \in \mathbb{C}[x]$ and $\frac{\mathbb{C}}{\mathbb{R}}$ has no proper intermediate field.

2.5 The Galois Groups

Let E be a field, and let F be a subfield of E. Then the set $G\left(\frac{E}{F}\right)$ of all automorphisms of E leaving F fixed forms a subgroup of the group of all automorphisms of E is called the Galois group of E over F. If $p(x)$ is an irreducible polynomial with coefficients in F, then it also has a Galois group, namely the Galois group of its splitting field.

For instance, consider the polynomial $p(x) = x^4 - 5x^2 + 6x$ in $\mathbb{Q}[x]$. It splits in the field $\mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right]$ into $\left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)\left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right)$.

We define the automorphism $\Psi_1 : \mathbb{Q}\left[\sqrt{2},\ \sqrt{3}\right] \rightarrow \mathbb{Q}\left[\sqrt{2},\ \sqrt{3}\right]$ by

$\Psi_1\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$. Similarly we can define

$\Psi_2\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$. Now

$\Psi_3 = \Psi_1 \circ \Psi_2$ because the composition of two automorphisms is again an automorphism and the Identity mapping is also an automorphism. Hence the set $G = \{I,\ \Psi_1,\ \Psi_2,\ \Psi_3\}$ is the group of automorphisms of $\mathbb{Q}\left[\sqrt{2},\ \sqrt{3}\right]$ under the composition of mappings.

Chapter 3

Coset Diagrams

In this chapter we give an introduction of graphs depicting group actions. In this chapter we describe parametrization of the conjugacy classes of actions of the infinite triangle group $\Delta(2,3,7)$ on projective lines over the finite fields F_q. For each $\theta \in F_q$ we associate a coset diagram $D(\theta, q)$ depicting the conjugacy class of actions of $\Delta(2,3,7)$ on $PL(F_q)$. We obtain conditions on θ and q, which guarantee only those coset diagrams which depict homomorphic images of $\Delta(2,3,7)$ in $PGL(2,q)$. We use Cebotarev's Density Theorem to find with what frequency certain fragments of coset diagrams occur in the homomorphic images of $\Delta(2,3,7)$.

3.1 Graphs and Coset Diagrams

Intuitively, a graph is a finite set of points in space being joined by arcs. In many papers the graphs have shown to be an economical mathematical technique to prove certain results. For instance, M. D. E. Conder in [3] has made use of graphs and has given proofs of the facts that all but a finite number of the alternating groups are Hurwitz groups.

For finite groups of small order the graphs can be used instead of multiplication tables; they give the same information but in a much more efficient way. See for example [2] and [6]. Graphical methods have been used in many papers in the theory of finitely generated and finitely related groups.

The concept of graphs was first introduced in 1878 by A. Cayley [2]. A number of group theorists used Cayley's diagrams to prove many important results on finitely generated groups.

Later, Schreier generalized the notion of graphs of groups introduced by A. Cayley. Since then graphical methods started appearing in mathematical literature. Today graphs and their applications in various mathematical disciplines have emerged as a significant theory on its own right. In 1978, G. Higman introduced the concept of the coset diagrams for the modular group and in 1980, Q. Mushtaq being his doctoral student laid the foundations and developed it into a useful theory.

In Cayley's diagrams, the elements of the group are represented by the vertices, whereas in the Schreier's diagrams, the vertices represent the coset of a subgroup G. Some examples of these types of diagrams are given below.

Consider the symmetric group on three letters, that is:

$$S_3 =< x, y : x^2 = y^3 = (xy)^2 = 1 > .$$

Since S_3 has six elements, its Cayley graph has six vertices. Elements of S_3 are $\{1, x, y, xy, y^2, xy^2\}$. Here x is represented by broken lines and y by solid lines. The diagram of S_3 can be drawn as given below.

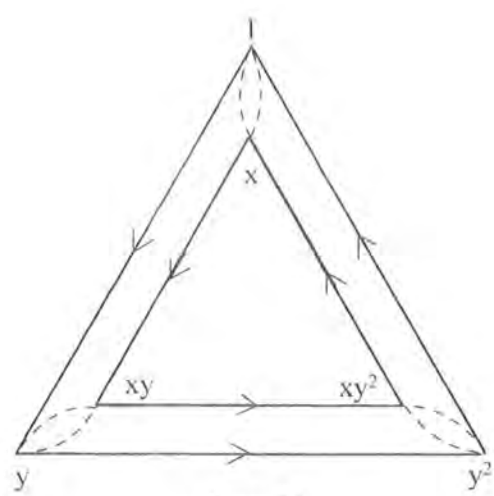

Figure 3.1

Consider the alternating group

$$A_5 = < x, y : x^2 = y^3 = (xy)^5 = 1 > .$$

Now using the cyclic subgroup $H =< y >$, the figure 3.2 represents the Schreier diagram for A_5, where x is denoted by broken edges and y is denoted by solid edges. There are 12 vertices, representing 12 cosets of the subgroup H of order 5. Recall that the order of A_5 is 60.

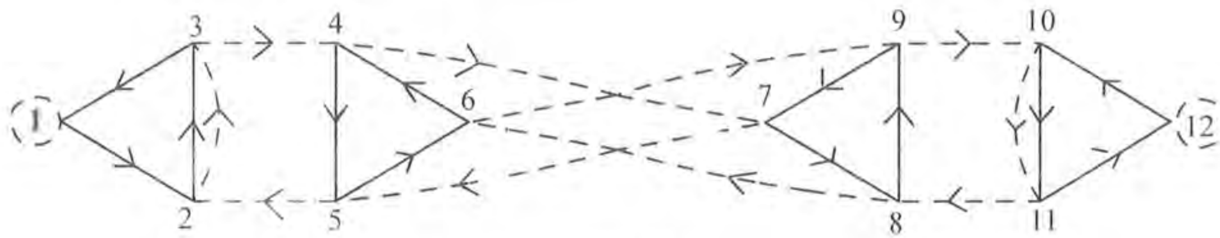

Figure 3.2

In 1978, G. Higman introduced this special type of diagrams particularly for the modular and the extended modular groups. (See for details [3] and [4]).

A coset diagram for the modular group G consists of a set of small triangles and a set of edges. The three cycles of y are denoted by small triangles whose vertices are permuted counter-clockwise by y and any two vertices which are interchanged by x are joined by an edge. The action of t is represented by reflection about the vertical line of axis, in case of the extended modular group. The fixed points of x and y, if they exist, are denoted by heavy dots. Notice that $(yt)^2 = 1$ is equivalent to $tyt = y^{-1}$, which means that t reverses the orientation of the triangles representing the three cycles of y (as reflection does); because of this, there is no need to make the diagram more complicated by introducing t-edges. These diagrams are called the coset diagrams because here the vertices are identifiable with the right cosets in a permutation group G, of the stabilizer N of any point of the set Ω, so that an edge of colour i joins the set Ng to the set Ngx_i, for each element g of G.

For example, the action of $PSL(2, \mathbb{Z}) = \langle x, y : x^2 = y^3 = 1 \rangle$ on $PL(F_{17})$ by $x : z \longrightarrow \frac{-1}{z}$, $y : z \longrightarrow \frac{z-1}{z}$ to give the following permutation representation

$x = (0\ \infty)\,(1\ 16)\,(2\ 8)\,(3\ 11)\,(4)\,(5\ 10)\,(6\ 14)\,(7\ 12)\,(9\ 15)\,(13)$

$y = (0\ \infty\ 1)\,(2\ 9\ 16)\,(3\ 12\ 8)\,(4\ 5\ 11)\,(6\ 15\ 10)\,(7\ 13\ 14)$.

The coset diagram for the action of $PSL(2,\mathbb{Z})$ on $PL(F_{17})$ is:

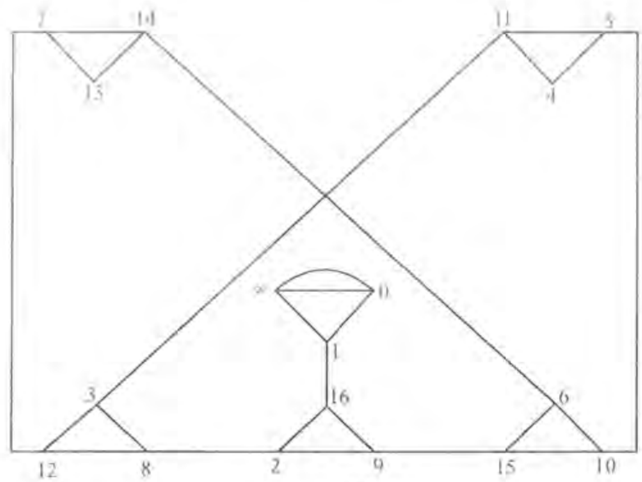

Figure 3.3

The coset diagrams have many useful applications. We can find a presentation for a subgroup H of finite index n in a finitely-presented group $G =< X \mid R >$.

The coset diagrams provide an elegant proof of the following theorem, "If G is a group generated by permutations $x_1, x_2, ..., x_d$ of a set Ω of size n, such that $x_1x_2...x_d$ is the identity permutation, and c_i is the number of orbits of $< x_i >$ on Ω, then G is transitive on Ω only if $c_1 + c_2 + ... + c_d \leq (d-2)n + 2$. This was obtained by Ree and Singerman using the Riemann-Hurwitz formula.

The coset diagrams can often be used to prove that certain groups are infinite, by joining diagrams together to construct permutation representations (of a given group) of arbitrarily large degree.

An edge whose both vertices, namely initial and final, coincide with each other is called a loop.

If $\pi = \{v_0, e_1, v_1, e_2, v_2, ..., e_k, v_k\}$ is an alternating sequence of vertices v_i and edges e_i of a graph then π is a path in the graph, joining v_0 and v_k, where e_i joins v_{i-1} and v_i for each i and $e_i \neq e_j$ $(i \neq j)$. The path P described before is called the inverse path. A path P is called a closed path if its initial vertex coincides with its terminal vertex.

If a word C satisfies the relation $C = I$, where I is the identity element, then any path corresponding to C is called a circuit. In other words a circuit is a closed path. So, loop is an example of a circuit. A circuit in which the elements are fixed just by one word and its inverse is called a simple circuit. Otherwise, it is called a non-simple or connected circuit.

If any two vertices in a coset diagram are joined by a path, then it is called a connected coset diagram. In other words a coset diagram is connected if the action is transitive.

3.2 Parametrization and Coset Diagrams

The group $PGL(2,q)$ has a natural permutation representation on $PL(F_q)$, and therefore, any homomorphism $\alpha : PGL(2,\mathbb{Z}) \to PGL(2,q)$ gives rise to an action of $PGL(2,\mathbb{Z})$ on $PL(F_q)$. We denote the generators $x\alpha$, $y\alpha$ and $t\alpha$ of $PGL(2,q)$ by $\bar{x}, \bar{y}$ and $\bar{t}$. If neither of the generators x and y for $PSL(2,\mathbb{Z})$ lies in the kernel of α, so that $\bar{x}$ and $\bar{y}$ are of order 2 and 3 respectively, then α is said to be a non-degenerate homomorphism. Two such homomorphisms α and β are said to be conjugate if $\beta = \alpha\rho$ for some inner automorphism ρ of $PGL(2,q)$. It has been proved in [12], the conjugacy classes of non-degenerate homomorphisms of $PGL(2,\mathbb{Z})$ into $PGL(2,q)$ correspond in a one-to-one fashion with the conjugacy classes of non-trivial elements of $PGL(2,q)$, under a correspondence which assigns to the non-degenerate homomorphism α the class containing $(xy)\alpha$. This of course, means that we can actually parametrize the conjugacy classes of non-degenerate homomorphisms $\alpha : PGL(2,\mathbb{Z}) \to PGL(2,q)$ except for a few uninteresting ones, by the elements of F_q. That is, we can in fact parametrize the actions of $PGL(2,\mathbb{Z})$ on $PL(F_q)$.

If α is such a homomorphism and X, Y and T denote elements of $GL(2,q)$ which yield the elements $\bar{x}$, $\bar{y}$ and $\bar{t}$ in $PGL(2,q)$, where F_q is not of characteristic 2 or 3, then because of this and because of the fact that $\bar{x}$, $\bar{y}$ and $\bar{t}$ are of order 2, 3 and 2 respectively, we can take the matrices X, Y and T to be:
$X = \begin{bmatrix} a & lc \\ c & -a \end{bmatrix}$, $Y = \begin{bmatrix} d & lf \\ f & -d-1 \end{bmatrix}$ and $T = \begin{bmatrix} 0 & -l \\ 1 & 0 \end{bmatrix}$ where $a, c, d, f, l \in F_q$ with $l \neq 0$. We shall write

$$a^2 + lc^2 = -\Delta \neq 0 \tag{3.1}$$

and require that

$$d^2 + d + lf^2 + 1 = 0. \qquad (3.2)$$

This certainly yields elements satisfying the relations $X^2 = \lambda_1 I$, $Y^3 = \lambda_2 I$ and $T^2 = \lambda_3 I$, where λ_1, λ_2 and λ_3 are some non-zero scalars and I is the identity matrix. The non-degenerate homomorphism α is determined by $\bar{x}\bar{y}$ because the one-to-one correspondence assigns to α the class containing $\bar{x}\bar{y}$. So we only have to check on the conjugacy class of $\bar{x}\bar{y}$. The matrix XY has the trace

$$r = a\,(2d+1) + 2lcf \qquad (3.3)$$

If $trace\,(XYT) = ls$, then

$$s = 2af - c\,(2d+1) \qquad (3.4)$$

so that

$$3\Delta = r^2 + ls^2 \qquad (3.5)$$

and set

$$\theta = \frac{r^2}{\Delta}. \qquad (3.6)$$

Thus, given the values of q and θ we can always find the matrices X and Y by using equations (3.1) to (3.6).

For instance, given $\theta = 4$ in F_{11}, we can find a coset diagram $D\,(4, 11)$ associated with the non-degenerate homomorphism $\alpha : PGL\,(2,\mathbb{Z}) \to PGL\,(2, 11)$ as follows. By equation (3.6), $\theta = \frac{r^2}{\Delta}$ and so $\theta = 4$ implies that $r^2 = 4\Delta$. Since 4 is a square in F_{11} therefore, Δ is a square also. So, we can assume that $\Delta = 1$ so that $r = \pm 2$. Let us choose $r = 2$ and substitute these values of Δ and r in equation (3.5) to obtain $s^2 = \frac{-1}{l}$. By letting $l = -1$, we can choose $s = 1$. Similarly, if we let $d = 0$, the equation (3.2) yields $f = \pm 1$. Without any loss of generality, we can choose $f = 1$ and substitute the values of r, s, d, l and f in equations (3.3) and (3.4), to obtain

$2 = a - 2c$

$1 = 2a - c.$

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

$X=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, Y=\begin{bmatrix}0 & -1\\ 1 & -1\end{bmatrix}$

so we can take $\bar{x}$ as the transformation $z\rightarrow\frac{-1}{z}$, and $\bar{y}$ as the transformation $z\rightarrow\frac{z-1}{z}$. We can calculate the permutation representations of $\bar{x}$ and $\bar{y}$ as

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

$\bar{y}=(0\ \ \infty\ \ 1)(2\ \ 10\ \ 6)(3\ \ 5\ \ 8)(4\ \ 7\ \ 9)$.

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

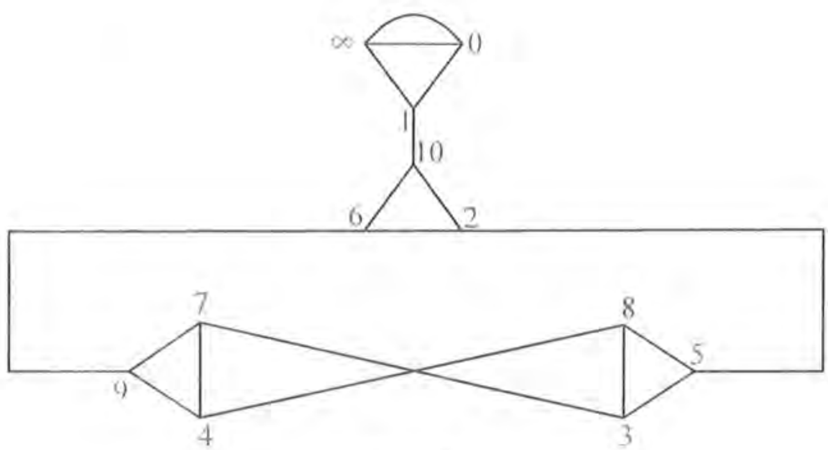

Figure 3.4

In [11] Q. Mushtaq has proved the following results for Hurwitz groups.

Theorem 8 *For each zero of $f(z)=z^3-5z^2+6z-1$ in F_q there exists a conjugacy class of non-degenerate homomorphisms form $\Delta(2,3,7)$ into $PGL(2,q)$.*

Proof. Suppose q itself is a prime and is congruent to ±1 (mod 7). Then due to a result of Macbeath [8], there are three distinct traces r_1 , r_2 , r_3 of elements of the group $SL(2,q)$ that yield elements of order 7 in $PSL(2,q)$, and thus there are three conjugacy classes of non-degenerate homomorphisms α from $\Delta(2,3,7)$ into $PGL(2,q)$. On the other hand, when $q=p^3$ for some prime p congruent to ±2 or ±3 (mod 7), there are still three such traces, but these are all conjugate under automorphism of F_q, and so there is just one cojugacy class of non-degenerate homomorphism α from $\Delta(2,3,7)$ into $PGL(2,q)$. In both cases every element of $PSL(2,q)$ that comes from an element of $SL(2,q)$ with trace r_1 , r_2 or r_3 must have order 7. Indeed except when the trace is ±2, the trace of any element of $SL(2,q)$ determines its order.

Now suppose A is any element of $SL(2,q)$ which has trace r, where $r = r_1$, r_2 or r_3. As A is conjugate in $GL(2,q^2)$ to a matrix B of the form $\begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix}$ where ρ is a primitive $7-th$ root of unity in F_{q^2} we have $r = trace(A) = trace(B) = \rho + \rho^{-1}$. Next $r^2 = (\rho + \rho^{-1})^2 = \rho^2 + \rho^{-2} + 2$, so $r^2 - 2 = \rho^2 + \rho^{-2}$, which is the trace of B^2; and $r^3 = (\rho + \rho^{-1})^3 = \rho^3 + 3\rho + 3\rho^{-1} + \rho^{-3}$, so $r^3 - 3r = \rho^3 + \rho^{-3}$, which is the trace of B^3.

Now, since $\rho^7 = 1$ and $\rho \neq 1$, we have $\rho^6 + \rho^5 + \rho^4 + \rho^3 + \rho^2 + \rho + 1 = 0$. But $\rho^7 = 1$ implies that $\rho^6 = \rho^{-1}$, $\rho^5 = \rho^{-2}$ and $\rho^4 = \rho^{-3}$ so $\rho^6 + \rho^5 + \rho^4 + \rho^3 + \rho^2 + \rho + 1 = 0$ becomes $(\rho + \rho^{-1}) + (\rho^2 + \rho^{-2}) + (\rho^3 + \rho^{-3}) + 1 = 0$. Substituting the values of $(\rho + \rho^{-1})$, $(\rho^2 + \rho^{-2})$ and $(\rho^3 + \rho^{-3})$ in terms of r, we get $r + (r^2 - 2) + (r^3 - 3r) + 1 = 0$. That is $r(r^2 - 2) = 1 - r^2$. Since the trace of matrix B is r and the determinant is 1, we substitute these values in equation $r^2 = \Delta\theta$ to obtain $\theta = r^2$; and thus converting the equation $r(r^2 - 2) = 1 - r^2$ into an equation in θ. That is, $r(\theta - 2) = 1 - \theta$. On squaring both sides of this equation and substituting θ for r^2, we obtain $f(\theta) = \theta^3 - 5\theta^2 + 6\theta - 1 = 0$. Thus if q is not a power of 7, then $\bar{x}\bar{y}$ has order 7 if $f(\theta) = 0$. If ρ is a primitive $7-th$ root of unity in the appropriate characteristic, the roots of this equation are:

$\theta_1 = \rho + \rho^{-1} + 2$

$\theta_2 = \rho^2 + \rho^{-2} + 2$

$\theta_3 = \rho^4 + \rho^{-4} + 2.$

If the characteristic p satisfies $p \equiv \pm 1 \pmod 7$, then θ_1, θ_2, θ_3 lie in F_p. Otherwise θ_1, θ_2, θ_3 are conjugate elements of F_{p^3}. Thus we get three different coset diagrams in the first case, but only one in the second case.

Note that the coset diagram $D(\theta, q)$, where θ is a zero of $f(z) = z^3 - 5z^2 + 6z - 1$ in F_q, will be such that each vertex in the coset diagram will be fixed by $(\bar{x}\bar{y})^7$.

Above theorem can alternatively be proved as:

let X, Y and XY be the matrices in $GL(2,p)$ corresponding to the elements $\bar{x}$, $\bar{y}$ and $\bar{x}\bar{y}$ respectively. Notice that the $\det(XY) = \Delta$, and the $trace(XY) = r$. Now the characteristic equation of XY will be

$$(XY)^2 - rXY + \Delta I = 0$$

implies that

$$(XY)^2 = rXY - \Delta I$$

$$\begin{aligned}
(XY)^4 &= \left(r^2 - \Delta\right)(XY)^2 - r\Delta XY \\
&= \left(r^2 - \Delta\right)(rXY - \Delta I) - r\Delta XY \\
&= \left(r^3 - 2r\Delta\right)XY + \left(-\Delta r^2 + \Delta^2\right)I
\end{aligned}$$

$$\begin{aligned}
(XY)^5 &= \left(r^3 - 2r\Delta\right)(XY)^2 + \left(-\Delta r^2 + \Delta^2\right)XY \\
&= \left(r^3 - 2r\Delta\right)(rXY - \Delta I) + \left(-\Delta r^2 + \Delta^2\right)XY \\
&= \left(r^4 - 3\Delta r^2 + \Delta^2\right)XY + \left(-r^3\Delta + 2r\Delta^2\right)I.
\end{aligned}$$

Continuing in the similar way we get

$$(XY)^6 = \left(r^5 - 4r^3\Delta + 3r\Delta^2\right)XY + \left(-r^4\Delta + 3r^2\Delta^2 - \Delta^3\right)I$$

$$(XY)^7 = \left(r^6 - 5r^4\Delta + 6r^2\Delta^2 - \Delta^3\right)XY + \left(-r^5\Delta + 4r^3\Delta^2 - 3r\Delta^3\right)I.$$

But $(XY)^7 = \lambda I$, so we must have

$$r^6 - 5r^4\Delta + 6r^2\Delta^2 - \Delta^3 = 0.$$

But $r^2 = \Delta\theta$, so

$$\theta^3\Delta^3 - 5\theta^2\Delta^3 + 6\theta\Delta^3 - \Delta^3 = 0$$

or

$$\theta^3 - 5\theta^2 + 6\theta - 1 = 0$$

is the required condition for $(XY)^7 = 1$. ∎

Theorem 9 *The transformation* $\bar{t}$ *has fixed vertices in* $D(\theta, q)$ *if and only if* $\theta(\theta - 3)$ *is a square in* F_q.

Proof. First we show that the fixed points of $\bar{x}$ exist in $D(\theta, q)$ if $q \equiv 1 \pmod 4$ and there do not exist fixed points of $\bar{x}$ if $q \equiv 3 \pmod 4$.

Since $\bar{y}$ and $\bar{x}\bar{y}$ have odd orders, they lie in $PSL(2, q)$ and hence so does $\bar{x}$. This implies that the permutation induced by $\bar{x}$ is even. Since $r^2 = \Delta\theta$, Δ is a square if and only if θ is. This means that $\bar{x}$ is in $PSL(2, q)$ if and only if -1 is not a square in F_q and $q \equiv 1 \pmod 4$. Thus $\bar{x}$ has fixed vertices in $D(\theta, q)$ if $q \equiv 1 \pmod 4$ and it does not have fixed vertices if $q \equiv 3 \pmod 4$. This means that for the non-degenerate homomorphism with parameter θ, $\bar{x}$ is an element of $PSL(2, q)$ if and only if $-\theta$ is a square in F_q.

Let δ be the automorphism of $PGL(2, \mathbb{Z})$, defined by $x\delta = xt$, $y\delta = y$ and $t\delta = t$. Then if $\alpha : PGL(2, \mathbb{Z}) \longmapsto PGL(2, q)$ maps x, y, t to $\bar{x}$, $\bar{y}$, $\bar{t}$ the homomorphism $\alpha' = \delta\alpha$ maps x, y, t to $\bar{x}\bar{t}$, $\bar{y}$, $\bar{t}$. If we let X, Y and T denote elements of $GL(2, q)$ which yield the elements $\bar{x}$, $\bar{y}$ and $\bar{t}$ in $PGL(2, q)$, then obviously X, Y and T can be taken as follows:

$$X = \begin{bmatrix} a & lc \\ c & -a \end{bmatrix}, \; Y = \begin{bmatrix} d & lf \\ f & -d-1 \end{bmatrix} \text{ and } T = \begin{bmatrix} 0 & -l \\ 1 & 0 \end{bmatrix}$$ where $l \neq 0$ and $a, c, d, l, f \in F_q$ such that they satisfy the equations (3.1) to (3.6). We recall that, by lemma 3.2 in [12], $\bar{x}\bar{y}$ will be of order 2 if and only if $trace(XY) = r = 0$ and similarly $\bar{x}\bar{y}\bar{t}$ will be of order 2 if and only if $\frac{trace(XYT)}{l} = s = 0$. Recall that, Δ is the determinant of XY so that the parameter of $\bar{x}\bar{y}$ is $\frac{r^2}{\Delta}$, which we have denoted by θ.

Also ls is the trace of XYT and $l\Delta$ is its determinant. If we let $\Phi = \frac{ls^2}{\Delta}$, we get $\theta + \Phi = \frac{r^2 + ls^2}{\Delta}$. Substituting the values of r and s, from the equations (3.3) and (3.4), in $\theta + \Phi = \frac{r^2 + ls^2}{\Delta}$, and then making the substitution of the equation (3.2) and $\Delta = -\left(a^2 + lc^2\right)$, we obtain $\theta + \Phi = 3$. That is, if θ is the parameter of α then $3 - \theta$ is the parameter of α'. Since change from α to α' interchanges both $\bar{x}$ and $\bar{x}\bar{t}$ and θ and $\theta - 3$, it follows that $\bar{x}\bar{t}$ maps to an element of $PSL(2, q)$ if and only if $-(\theta - 3)$ is a square if F_p. 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 $\theta(\theta - 3)$ is a square in F_q. Now $\bar{t}$ has fixed points 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 $q \equiv -1 \pmod 4$ is equivalent to saying that -1 is a square in F_q, we conclude that $\bar{t}$ has fixed vertices in $D(\theta, q)$ if and only if $-\theta(3 - \theta)$ is a square in

F_q. Hence the result.

In Particular, if $q = 7$ or $q = p$ where $p \equiv \pm 1 \pmod 7$ or $q = p^3$, where $p \equiv \pm 2$ or ± 3 (mod 7) then $(\bar{x}\bar{y})^7 = 1$, and so $\bar{x}$ belongs to $PSL(2, q)$. Therefore, $-\theta$ is a square in F_q. Thus, we have the following corollary. ∎

Corollary 10 *If $q = 7$ or $q = p$, where $p \equiv \pm 1 \pmod 7$ or $q = p^3$, where $p \equiv \pm 2$ or ± 3 (mod 7) then the transformation $\bar{t}$ has fixed vertices in $D(\theta, q)$ if and only if $\theta - 3$ is a square in F_q.*

As an illustration, let us consider what happens when $q = 13$. Here the zeros of the polynomial $f(z) = z^3 - 5z^2 + 6z - 1$ are $9, 10, 12$ and of these only $12 - 3$ is a square in F_q. The three corresponding diagrams are given below, in each case with suitable conditions for the linear-fractional transformations $\bar{x}$, $\bar{y}$ and $\bar{t}$:

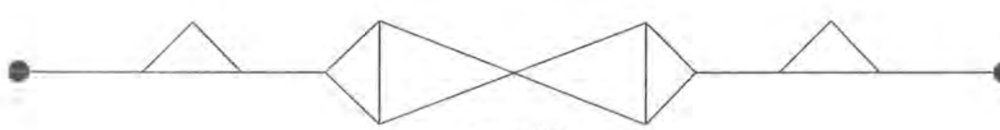

Figure 3.5

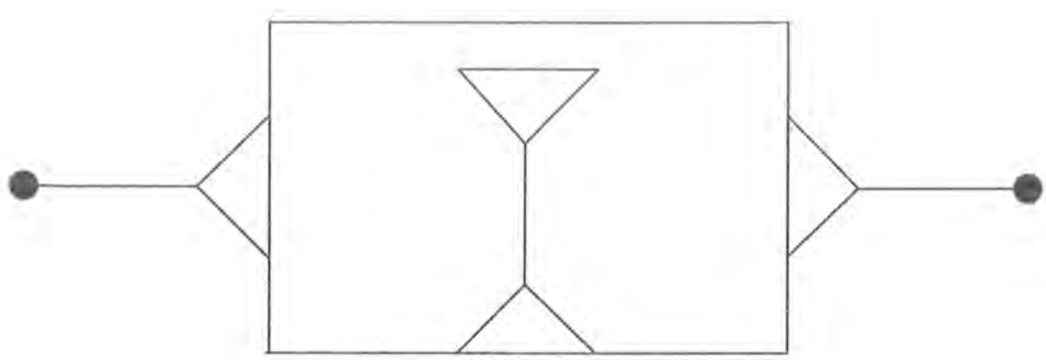

Figure 3.6

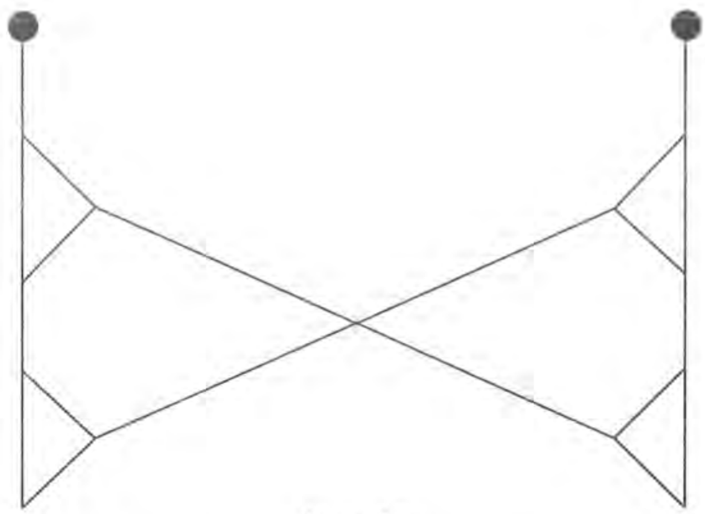

Figure 3.7

In the first and third cases the reflection t fixes no points and so $< x, y, t >= PGL(2, 13)$. In the second case $t \in PSL(2, 13)$ and hence $< x, y, t > = PSL(2, 13) \times C_2$.

As a consequence of above theorem, one can make the following deductions.

Corollary 11 *$PGL(2, q)$ is generated by $\bar{x}$, $\bar{y}$, $\bar{t}$ such that*

$$\bar{x}^2 = \bar{y}^3 = \bar{t}^2 = (\bar{x}\bar{t})^2 = (\bar{y}\bar{t})^2 = (\bar{x}\bar{y})^7 = 1$$

with the subgroup $< \bar{x}, \bar{y} >$ being non-trivial and of index 2 in $PGL(2, q)$ if and only if either $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$ and two of the zeros of the polynomial $f(z) = z^3 - 5z^2 + 6z - 1$ are non-squares in F_q.

Corollary 12 *$PSL(2, q) \times C_2$ is generated by $\bar{x}$, $\bar{y}$, $\bar{t}$ such that*

$$\bar{x}^2 = \bar{y}^3 = \bar{t}^2 = (\bar{x}\bar{t})^2 = (\bar{y}\bar{t})^2 = (\bar{x}\bar{y})^7 = 1$$

with the subgroup $< \bar{x}, \bar{y} >$ being non-trivial and of index 2 in $PSL(2, q) \times C_2$, if and only if either $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$ and two of the zeros of the polynomial $f(z) = z^3 - 5z^2 + 6z - 1$ are non-squares in F_q.

Now $PGL(2, q)$, for q an odd prime power, contains two classes of involutions both consisting of matrices of trace zero. Recall that the classes of $PGL(2, q)$, not consisting of elements

$\bar{x}$, such that $\bar{x}^2 = 1$, are in a one-to-one correspondence with the non-zero elements θ of F_q. The class corresponding to θ consists of elements represented by matrix M with $\theta = \frac{r^2}{\Delta}$, where $r = trace(M)$ and $\Delta = \det(M)$. Thus, if X, Y are elements of $SL(2, q)$ which yield the elements $\bar{x}$ and $\bar{y}$ of $PSL(2, q)$ then

$x^2 + \Delta I = 0$

$(XY)^2 - r(XY) + \Delta I = 0$

$Y^2 + Y + I = 0$

where the above equations are the characteristic equations of X, XY and Y respectively. More details about these equations can be found in [10].

3.3 Cebotarev's Density Theorem

Theorem 13 *Let f be an irreducible polynomial of degree n over Z. Let $\theta_1, \theta_2, ..., \theta_n$ be the roots of f in a field of characteristic 0. Then $K = \mathbb{Q}[\theta_1, \theta_2, ..., \theta_n]$ is a normal extension of $\mathbb{Q}$. Let $G\left(\frac{K}{\mathbb{Q}}\right)$ denote the Galois group of K over $\mathbb{Q}$. If S is the ring of integers over K. Let $\bar{p}$ be a prime in S such that $\bar{p}$ divides p (where p is prime in $\mathbb{Z}$) then $S/\bar{p}$ is a finite field of characteristic p.*

The Galois group of $S/\bar{p}$ over $\mathbb{Z}/p$ is cyclic and is generated by $\sigma : \mu \to \mu^p$ for all μ in $S/\bar{p}$. Then there exists an automorphism δ of S such that the following diagram commutes.

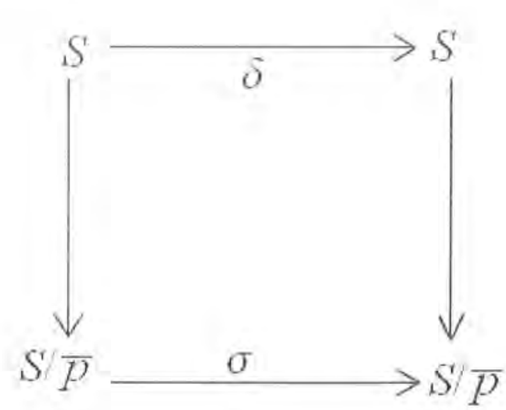

Figure 3.8

If p does not divide the discriminant of S then δ is unique, and if we replace $\bar{p}$ by another divisor p_1 then we replace δ by conjugate. This gives a map from the set p of rational primes (except those dividing the discriminant) to the set of conjugacy classes of the Galois group $G\left(\frac{K}{\mathbb{Q}}\right)$ in which p maps to the conjugacy class containing S. Cebotarev's Density Theorem [7] says that this map is onto; and the density of the set of primes, mapping onto a particular conjugacy class is proportional to the size of the class.

We shall see, at the end of this chapter, the application of Cebotarev's Density Theorem in the case of some special examples of coset diagrams arising from the actions of $\Delta(2,3,7)$ on $PL(F_q)$, where $q \equiv \pm 1 \pmod 7$

The coset diagrams, which depict the action of $\Delta(2,3,7)$ on $PL(F_q)$, frequently contain some special fragments, namely γ_1, γ_2, γ_3, and γ_4 respectively;

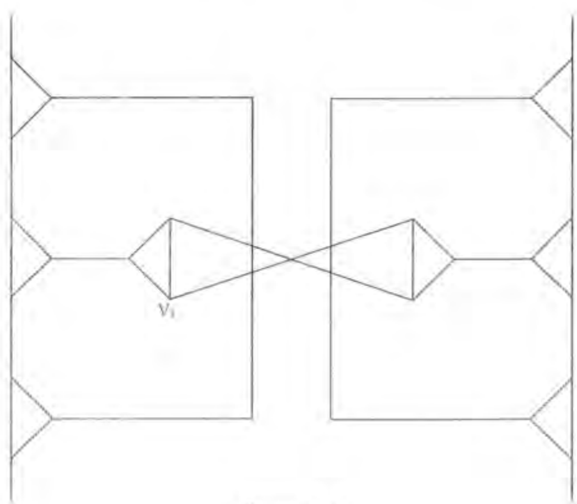

Figure 3.9

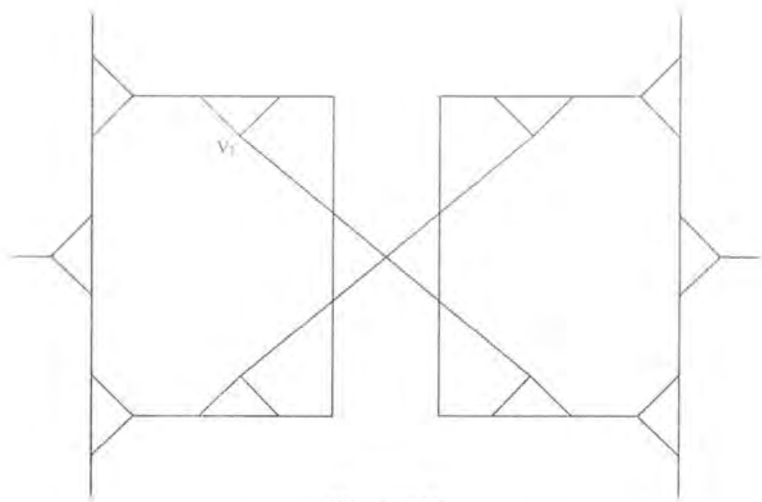

Figure 3.10

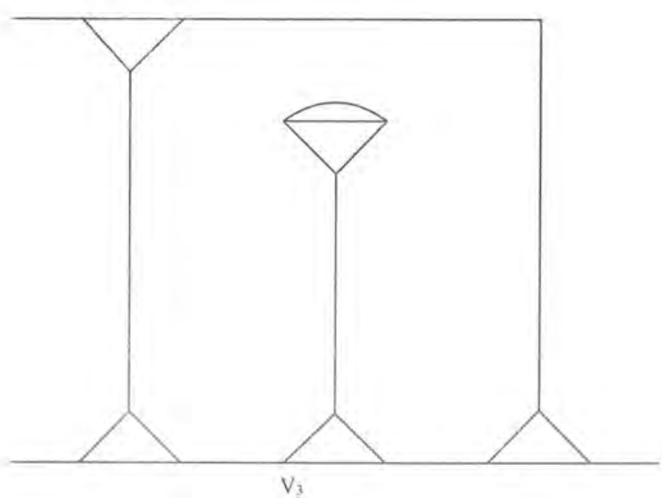

Figure 3.11

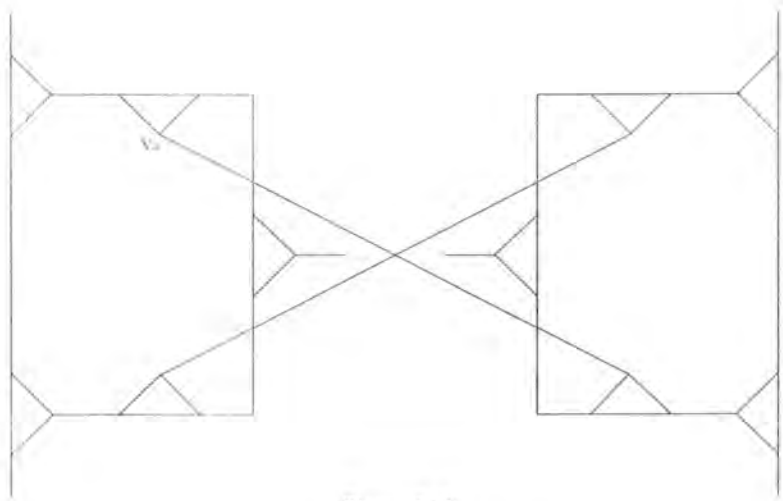

Figure 3.12

It is important for us to know when certain types of fragments exist in $D(\theta, q)$. In the following we determine conditions in terms of θ and q, for the existence of the fragments in $D(\theta, q)$ depicting homomorphic image of $\Delta(2,3,7)$.

The existence of these fragments in the coset diagrams for the Hurwitz groups is important because it tells how frequently the Hurwitz groups occur in the class of groups emerging from the action of $PGL(2,\mathbb{Z})$ on $PL(F_q)$, where q is a prime power. Q. Mushtaq has considered fragment γ_1 and used the Cebotarev's Density Theorem to show how frequently they occur in the action of $PGL(2,\mathbb{Z})$ on $PL(F_q)$. In this chapter we use the same technique in a similar fashion to find the frequency with which fragments γ_2, γ_3 and γ_4 occur.

Theorem 14

(1) *The fragment* γ_1 *will occur in* $D(\theta, q)$ *if* 13 *is a square in* F_q.

(2) *The fragment* γ_2 *will occur in* $D(\theta, q)$ *if* 29 *is a square in* F_q.

(3) *The fragment* γ_3 *will occur in* $D(\theta, q)$ *if* 7 *is a square in* F_q.

(4) *The fragment* γ_4 *will occur in* $D(\theta, q)$ *if* 41 *is a square in* F_q.

Proof. The vertices v_1, v_2, v_3, v_4 are fixed by the elements $XYXY^{-1}$, $XYXYXY^{-1}XY^{-1}$, $XYXYXYXY^{-1}$, and $XYXYXYXY^{-1}XY^{-1}XY^{-1}$. Notice that $\det(X) = \Delta$, $trace(X) = 0$, $\det(Y) = 1$, $trace(Y) = -1$, $\det(XY) = \Delta$, and $trace(XY) = r$. It is not very hard to deduce, after suitable manipulation, the equations

$$XYX = rX + \Delta I + \Delta Y \tag{3.7}$$

$$YXY = rY + X \tag{3.8}$$

$$YX = rI - X - XY \tag{3.9}$$

from the equations

$$X^2 + \Delta I = 0 \tag{3.10}$$

$$(XY)^2 - r(XY) + \Delta I = 0 \tag{3.11}$$

$$Y^2 + Y + I = 0 \tag{3.12}$$

where X, Y are the matrices corresponding to the linear fractional transformations $\overline{x}$, $\overline{y}$.

(1) In fragment γ_1 the vertex v_1 is fixed by $XYXY^{-1}$. The matrix corresponding to $XYXY^{-1}$ will be $M_1 = XYXY^{-1}$. The determinant of M_1 will be equal to $\det(M_1) = \det(XYXY^{-1}) = \det(XYXY^2) = \det(X)\det(Y)\det(X)\det(Y)\det(Y) = \Delta^2$.

Now M_1 can be written as

$M_1 = XYXY^2$

$= XYX(-Y - I)$

$= -(XY)^2 - XYX$

$= -rXY + \Delta I - rX - \Delta I - \Delta Y = -rXY - rX - \Delta Y$.

So the trace of $M_1 = trace(-rXY) - trace(rX) - trace(\Delta Y)$, that is, $trace(M_1) = -r^2 + \Delta$. This implies that the discriminant of the characteristic equation of M_1 will be

$$(-r^2 + \Delta)^2 - 4\Delta^2 = r^4 - 3\Delta^2 - 2r^2\Delta.$$

But $r^2 = \Delta\theta$. That is, the discriminant will be $\theta^2\Delta^2 - 3\Delta^2 - 2\theta\Delta^2$. Since Δ is a square if and only if θ is, we can eliminate Δ^2, as we are in the field F_q. So the discriminant of the characteristic equation of M_1 corresponding to the element $XYXY^{-1}$ of $PGL(2,q)$ will be $\theta^2 - 2\theta - 3$.

The fragment γ_1 will occur in $D(\theta, q)$ if and only if $d_1(\theta) = (\theta - 3)(\theta + 1)$ is a square in F_q. So if $\theta_1, \theta_2, \theta_3$ are the roots of $f(z) = z^3 - 5z^2 + 6z - 1 = 0$ then $\prod_{i=1}^{3} d_1(\theta_i) = f(3) f(-1) = 13$. Thus, γ_1 will occur in some $D(\theta_i, q)$ if 13 is a square in F_q.

(2) In fragment γ_2 the vertex v_2 is fixed by $XYXYXY^{-1}XY^{-1}$. The matrix corresponding to $XYXYXY^{-1}XY^{-1}$ will be $M_2 = XYXYXY^{-1}XY^{-1}$. The determinant of M_2 will be equal to $\det(XYXYXY^{-1}XY^{-1}) = \det(XYXYXY^2XY^2) = \det(X)\det(Y)\det(X)\det(Y)\det(X)$ $\det(Y)\det(Y)\det(X)\det(Y)\det(Y) = \Delta^4$.

Now M_2 can be written as

$$\begin{aligned}
M_2 &= XYXYXY^{-1}XY^{-1} \\
&= XYXYXY^2XY^2 \\
&= XYXYX(-y - I)XY^2 \\
&= (-XYXYXY - XYXYX)XY^2 \\
&= -XYXYXYXY^2 - XYXYX^2Y^2 \\
&= -XYXYXYX(-y - I) - XYXY(-\Delta)Y^2 \\
&= XYXYXYXY + XYXYXYX + \Delta XYXY(-y - I) \\
&= (XY)^4 + (XY)^3 X - \Delta XYXY^2 - \Delta XYXY \\
&= (XY)^4 + (XY)^2(XYX) - \Delta XYX(-y - I) - \Delta(XY)^2 \\
&= (XY)^4 + (XY)^2(XYX) + \Delta XYXY + \Delta(XYX) - \Delta(XY)^2 \\
&= (XY)^4 + (XY)^2(XYX) + \Delta(XY)^2 + \Delta(XYX) - \Delta(XY)^2 \\
&= (XY)^4 + (XY)^2(XYX) + \Delta(XYX) \\
&= \left((XY)^2\right)^2 + (XY)^2(XYX) + \Delta(XYX) \\
&= r^2(XY)^2 - 2r\Delta(XY) + \Delta^2 + r^2(XYX) + r\Delta(XY) + r\Delta(XY^2) - r\Delta X - \Delta^2 - \Delta^2 Y \\
&\quad + r\Delta X + \Delta^2 + \Delta^2 Y \\
&= r^2(XY)^2 - r\Delta(XY) + \Delta^2 + r^2(XYX) + r\Delta(XY^2) \\
&= r^2(XY)^2 - r\Delta(XY) + \Delta^2 + r^2(XYX) + r\Delta(X(-y - I)) \\
&= r^2(XY)^2 - r\Delta(XY) + \Delta^2 + r^2(XYX) - r\Delta(XY) - r\Delta X \\
&= (r^3(XY)) - 2r\Delta(XY) + r^2\Delta Y + \Delta^2 - r\Delta X.
\end{aligned}$$

So the trace of M_2 will be $trace(r^3(XY)) - trace(2r\Delta(XY)) + trace(r^2\Delta Y) + trace(\Delta^2) - trace(r\Delta X)$. That is $trace(M_2) = r^4 - 3r^2\Delta + 2\Delta^2$. This implies that the discriminant of the characteristic equation of M_2 will be

$$\left(r^4 - 3r^2\Delta + 2\Delta^2\right)^2 - 4\Delta^4 = r^8 - 6r^6\Delta + 13r^4\Delta^2 - 12r^2\Delta^3.$$

But $r^2 = \Delta\theta$. This means that the discriminant, in fact,

$$\theta^4\Delta^4 - 6\theta^3\Delta^4 + 13\theta^2\Delta^4 - 12\theta\Delta^4 = \left(\theta^4 - 6\theta^3 + 13\theta^2 - 12\theta\right)\Delta^4.$$

Since Δ is a square if and only if θ is, we can eliminate Δ^4, as we are in the field F_q. So the discriminant of the characteristic equation of the matrix corresponding to the element $XYXYXY^{-1}XY^{-1}$ of $PGL(2,q)$ will be $\theta^4 - 6\theta^3 + 13\theta^2 - 12\theta = \theta(\theta - 3)\left(\theta^2 - 3\theta + 4\right)$.

The fragment γ_2 will occur in $D(\theta, q)$ if and only if $d_2(\theta) = \theta(\theta - 3)\left(\theta^2 - 3\theta + 4\right)$ is a square in F_q. Now $d_2(\theta)$ can further be written as $d_2(\theta) = (\theta - 0)(\theta - 3)\left(\theta - \left(\frac{3+\sqrt{-7}}{2}\right)\right)\left(\theta - \left(\frac{3-\sqrt{-7}}{2}\right)\right)$. So if $\theta_1, \theta_2, \theta_3$ are the roots of $f(z) = z^3 - 5z^2 + 6z - 1 = 0$ then

$$\prod_{i=1}^{3} d_2(\theta_i) = f(0)\,f(3)\,f\left(\frac{3+\sqrt{-7}}{2}\right) f\left(\frac{3-\sqrt{-7}}{2}\right) = 29.$$

Thus, γ_2 will occur in some $D(\theta_i, q)$ if 29 is a square in F_q.

(3) In fragment γ_3 the vertex v_3 is fixed by $XYXYXYXY^{-1}$. The matrix corresponding to $XYXYXYXY^{-1}$ will be $M_3 = XYXYXYXY^{-1}$. The determinant of M_3 will be equal to $\det(XYXYXYXY^{-1}) = \det(XYXYXYXY^2) = \det(X)\det(Y)\det(X)\det(Y)\det(X)\det(Y)$ $\det(X)\det(Y)\det(Y) = \Delta^4$.

Now M_3 can be written as

$$\begin{aligned}
M_3 &= XYXYXYXY^{-1} \\
&= XYXYXYXY^2 \\
&= XYXYXYX(-Y - I) \\
&= -XYXYXYXY - XYXYXYX \\
&= -(XY)^4 - (XY)^3 X \\
&= -(XY)^4 - (XY)^2 (XYX) \\
&= -\left((XY)^2\right)^2 - (XY)^2 (XYX) \\
&= -(r(XY) - \Delta)^2 - (r(XY) - \Delta)(rX + \Delta I + \Delta Y)
\end{aligned}$$

$$= -r^2(XY)^2+2r\Delta(XY)-\Delta^2-r^2(XYX)-r\Delta(XY)-r\Delta(XY^2)+r\Delta X+\Delta^2+\Delta^2Y$$
$$= -r^2(r(XY)-\Delta)+2r\Delta(XY)-r^2(rX+\Delta I+\Delta Y)-r\Delta(XY)-r\Delta(-XY-X)$$
$$+r\Delta X+\Delta^2Y$$
$$= -r^3(XY)+r^2\Delta+2r\Delta(XY)-r^3X-r^2\Delta-r^2\Delta Y-r\Delta(XY)+r\Delta(XY)+r\Delta X$$
$$+r\Delta X+\Delta^2Y$$
$$= -r^3(XY)+2r\Delta(XY)-r^3X-r^2\Delta Y+2r\Delta X+\Delta^2Y.$$

So the trace of $M_3 = trace\left(-r^3(XY)\right)+trace\left(2r\Delta(XY)\right)-trace\left(r^3X\right)-trace\left(r^2\Delta Y\right)+trace\left(2r\Delta X\right)+trace\left(\Delta^2Y\right)$, that is $trce\left(M_3\right)=-r^4+3r^2\Delta-\Delta^2$.

This implies that the discriminant of the characteristic equation of M_3 will be

$$\left(-r^4+3r^2\Delta-\Delta^2\right)^2-4\Delta^4=r^8-6r^6\Delta+11r^4\Delta^2-6r^2\Delta^3-3\Delta^4.$$

But $r^2=\Delta\theta$. This means that the discriminant, in fact,

$$\theta^4\Delta^4-6\theta^3\Delta^4+11\theta^2\Delta^4-6\theta\Delta^4-3\Delta^4=\left(\theta^4-6\theta^3+11\theta^2-6\theta-3\right)\Delta^4.$$

Since Δ is a square if and only if θ is, we can eliminate Δ^4, as we are in the field F_q. So the discriminant of the characteristic equation of M_3 corresponding to the element $XYXYXYXY^{-1}$ of $PGL(2,q)$ will be $\theta^4-6\theta^3+11\theta^2-6\theta-3$.

The fragment γ_3 will occur in $D(\theta,q)$ if and only if $d_3(\theta)=\theta^4-6\theta^3+11\theta^2-6\theta-3$ is a square in F_q. Now $d_3(\theta)$ can be expressed as $(\theta-4)$, because $\theta^3-5\theta^2+6\theta-1=0$ implies that $\theta^4-6\theta^3+11\theta^2-6\theta-3=5\theta^3-6\theta^2+\theta-6\theta^3+11\theta^2-6\theta-3=-\theta^3+5\theta^2$ $-5\theta-3=-5\theta^2+6\theta-1+5\theta^2-5\theta-3=\theta-4$. So if $\theta_1,\theta_2,\theta_3$ are the roots of $f(z)=z^3-5z^2+6z-1=0$ then $\prod_{i=1}^{3}d_3(\theta_i)=f(4)=7$. Thus, γ_3 will occur in some $D(\theta_i,q)$ if 7 is a square in F_q.

(4) In fragment γ_4 the vertex v_4 is fixed by $XYXYXYXY^{-1}XY^{-1}XY^{-1}$. The matrix corresponding to $XYXYXYXY^{-1}XY^{-1}XY^{-1}$ will be $M_4=XYXYXYXY^{-1}XY^{-1}XY^{-1}$.

The determinant of M_4 will be equal to

$$\begin{aligned} det\left(XYXYXYXY^{-1}XY^{-1}XY^{-1}\right) &= \det\left(XYXYXYXY^2XY^2XY^2\right) \\ &= \det(X)\det(Y)\det(X)\det(Y)\det(X)\det(Y) \\ &\quad \det(X)\det(Y)\det(Y)\det(X)\det(Y)\det(Y) \\ &\quad \det(X)\det(Y)\det(Y) \\ &= \Delta^6. \end{aligned}$$

Now M_4 can be written as

$$\begin{aligned} M_4 &= XYXYXYXY^{-1}XY^{-1}XY^{-1} \\ &= (XY)^3\left(XY^{-1}\right)^3 \\ &= (XY)^3\left(XY^2\right)^3 \\ &= (XY)^3\left(X(-Y-I)\right)^3 \\ &= (XY)^3(-XY-X)^3 \\ &= (XY)^3\left(-r^2XY+\Delta XY-r^2X+\Delta X+r\Delta I\right)^3 \\ &= -r^3(XY)^2+3\Delta r^2(XY)^2-r^4(XYX)-r^3\Delta\left(XY^2\right)+2\Delta r^2(XYX)+r\Delta^2\left(XY^2\right) \\ &\quad -\Delta^2(XY)^2-\Delta^2(XYX)-r\Delta^2(XY) \\ &= -r^4(rXY-\Delta I)+3\Delta r^2(rXY-\Delta I)-r^4(rX+\Delta I+\Delta Y)-r^3\Delta X(-Y-I) \\ &\quad +2\Delta r^2(rX+\Delta I+\Delta Y)+r\Delta^2X(-Y-I)-\Delta^2X(rXY-\Delta I)-\Delta^2(rX+\Delta I+\Delta Y) \\ &\quad -r\Delta^2XY \\ &= -r^5XY+4r^3\Delta(XY)-r^2\Delta^2I-r^5X-r^4\Delta Y+3r^3\Delta X+2r^2\Delta^2Y-3r\Delta^2(XY) \\ &\quad -2r\Delta^2X-\Delta^3Y. \end{aligned}$$

Now,

$$\begin{aligned} trace(M_4) &= trace(-r^5XY+4r^3\Delta(XY)-r^2\Delta^2I-r^5X-r^4\Delta Y+3r^3\Delta X+2r^2\Delta^2Y \\ &\quad -3r\Delta^2(XY)-2r\Delta^2X-\Delta^3Y) \\ &= -r^5trace(XY)+4r^3\Delta trace(XY)-r^2\Delta^2trace(I)-r^5trace(X) \\ &\quad -r^4\Delta trace(Y)+3r^3\Delta trace(X)+2r^2\Delta^2trace(Y)-3r\Delta^2trace(XY) \\ &\quad -2r\Delta^2trace(X)-\Delta^3trace(Y) \\ &= -r^6+5r^4\Delta-7r^2\Delta^2+\Delta^3. \end{aligned}$$

So the discriminant of the characteristic equation of M_4 will be

$$\left(-r^6+5r^4\Delta-7r^2\Delta^2+\Delta^3\right)^2-4\Delta^6=r^{12}-10r^{10}\Delta+39r^8\Delta^2-72r^6\Delta^3$$
$$+59r^4\Delta^4-14r^2\Delta^5-3\Delta^6$$

But $r^2=\Delta\theta$. This means that the discriminant, in fact,

$\theta^6\Delta^6-10\theta^5\Delta^6+39\theta^4\Delta^6-72\theta^3\Delta^6+59\theta^2\Delta^6-14\theta\Delta^6-3\Delta^6$. Since Δ is a square if and only if θ is, we can eliminate Δ, as we are in the field F_q. So the discriminant of the characteristic equation of the matrix corresponding to the element $XYXYXYXY^{-1}XY^{-1}XY^{-1}$ of $PGL(2,q)$ will be $\theta^6-10\theta^5+39\theta^4-72\theta^3+59\theta^2-14\theta-3=(\theta-1)^2(\theta-3)(\theta^3-5\theta^2+7\theta+1)$.

The fragment γ_4 will occur in $D(\theta,q)$ if and only if $d_4(\theta)=(\theta-1)^2(\theta-3)(\theta^3-5\theta^2+7\theta+1)$ is a square in F_q. Now $d_4(\theta)$ can be expressed as $(\theta-3)(\theta+2)$ because $\theta^3-5\theta^2+6\theta-1=0$ implies that $\theta^3-5\theta^2+7\theta+1=\theta+2$; and $\theta-1$ is a square in F_q. So if $\theta_1,\theta_2,\theta_3$ are the roots of $f(z)=z^3-5z^2+6z-1=0$ then $\prod_{i=1}^{3}d_4(\theta_i)=f(3)f(-2)=41$. Thus, γ_4 will occur in some $D(\theta_i,q)$ if 41 is a square in F_q. ■

3.4 Application of Cebotarev's Density Theorem

The diagram with parameter θ_i has vertices on the line of symmetry if and only if $\theta_i(\theta_i-3)$ is a square in F_q. Now we shall consider cases, in which $\bar{x}^2=\bar{y}^3=(\bar{x}\bar{y})^7=1$. In these cases, of course, $\bar{x}$ lies in $PSL(2,q)$, so θ_i is a square. Thus we are led to ask: is θ_i-3 a square?

Now $(\theta_1-3)(\theta_2-3)(\theta_3-3)=1$, so that of the elements θ_1-3, θ_2-3, θ_3-3 either all three are squares, or exactly one is a square. In particular, if $p\not\equiv\pm1\ (mod\ 7)$, so that θ_1, θ_2, θ_3 are conjugate, each θ_i-3 is a square. In this case, the diagram has vertices on the line of symmetry. If $p\equiv\pm1\ (mod\ 7)$, we are left with two possibilities, and we want to show that both occur, in the appropriate ratio.

We shall consider the Galois theory of $\mathbb{Q}(\lambda_1,\lambda_2,\lambda_3)$, where $\lambda_i=\sqrt{\theta_i-3}$ and θ_1, θ_2, θ_3 are the zeros of the polynomial $f(z)=z^3-5z^2+6z-1$ in F_q. Now $\mathbb{Q}(\theta_1,\theta_2,\theta_3)$ is a subfield of $\mathbb{Q}(\lambda_1,\lambda_2,\lambda_3)$. The elements of the Galois group which fix this subfield element-wise map each λ_i to $\pm\lambda_i$. Because $(\theta_1-3)(\theta_2-3)(\theta_3-3)=1$, we can assume that $\lambda_1\lambda_2\lambda_3=1$, whence the number of minus signs must be even. That is, the elements in question are 1, σ_1, σ_2, σ_3, where $\lambda_i\sigma_i=\lambda_i$, but $\lambda_i\sigma_j=-\lambda_i$, if $i\neq j$. Then $\{1,\sigma_1,\sigma_2,\sigma_3\}$ is a normal subgroup of the Galois group, and the factor group is the Galois group of $\mathbb{Q}(\theta_1,\theta_2,\theta_3)$ over $\mathbb{Q}$. This group is a cyclic group of order 3, and contains $1, \tau, \tau^2$, where $\theta_1\tau = \theta_2$, $\theta_2\tau = \theta_3$, $\theta_3\tau = \theta_1$. Since $\tau^{-1}\sigma_1\tau = \sigma_2$, $\tau^{-1}\sigma_2\tau = \sigma_3$, $\tau^{-1}\sigma_3\tau = \sigma_1$. Therefore, the Galois group is isomorphic to the alternating group A_4.

We now make the application of Cebotarev's Density Theorem [7], which concerns the distribution of primes in algebraic number fields. The conjugacy classes of the Galois group are:

$C_1 = \{1\}$

$C_2 = \{\sigma_1, \sigma_2, \sigma_3\}$

$C_3 = \{\tau, \tau\sigma_1, \tau\sigma_2, \tau\sigma_3\}$

$C_4 = \{\tau^{-1}, \tau^{-1}\sigma_1, \tau^{-1}\sigma_2, \tau^{-1}\sigma_3\}$.

A prime p congruent to ± 2 modulo 7, corresponds to the conjugacy class C_3, and a prime p, congruent to ± 4 modulo 7 to the conjugacy class C_4, and in these cases we get nothing new. But of the primes congruent to ± 1 modulo 7, approximately $\frac{1}{4}$ will correspond to the conjugacy class C_1 and for these all three diagrams will have vertices on the line of symmetry. The remainder will correspond to C_2, and for these, one of the diagrams will have vertices on the line of symmetry, but the other two will not.

We have seen in theorem 14(2) that the condition for the existence of the fragment γ_2 in the coset diagram is that $(\theta_i - 3)\left(\theta_i^3 - 3\theta_i^2 + 4\theta_i\right)$ is a square. So we put

$\mu_i = \sqrt{(\theta_i - 3)\left(\theta_i^3 - 3\theta_i^2 + 4\theta_i\right)}$. In this case we have either :

$$(\theta_1 - 3)\left(\theta_1^3 - 3\theta_1^2 + 4\theta_1\right) = 29,\ (\theta_2 - 3)\left(\theta_2^3 - 3\theta_2^2 + 4\theta_2\right) = 29,$$

$$(\theta_3 - 3)\left(\theta_3^3 - 3\theta_3^2 + 4\theta_3\right) = 29, \text{ or}$$

$$(\theta_1 - 3)\left(\theta_1^3 - 3\theta_1^2 + 4\theta_1\right)(\theta_2 - 3)\left(\theta_2^3 - 3\theta_2^2 + 4\theta_2\right)(\theta_3 - 3)\left(\theta_3^3 - 3\theta_3^2 + 4\theta_3\right) = 29.$$

Thus if 29 is a square *mod* p, one or all of $(\theta_i - 3)\left(\theta_i^3 - 3\theta_i^2 + 4\theta_i\right)$ are squares; and if 29 is not a square *mod* p, none, or two of $(\theta_i - 3)\left(\theta_i^3 - 3\theta_i^2 + 4\theta_i\right)$ are squares. Once again, if $p \not\equiv \pm 1$ (*mod* 7), so that there is essentially only one diagram, this settles the matter.

For primes not congruent to ± 1 modulo 7, the fragment occurs if and only if 29 is a square modulo p. But for primes $p \equiv \pm 1$ (*mod* 7) we again get ambiguity, and we have to appeal to

Cebotarev's Density Theorem to get the complete answer.

We are now interested in the Galois Theory of $\mathbb{Q}(\mu_1, \mu_2, \mu_3)$. This time, because $\mu_1\mu_2\mu_3 = \sqrt{29}$, the Galois group is $A_4 \times \mathbb{Z}_2$. The subgroup, A_4 is the Galois group of $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$, and contains all those elements which map $\sqrt{29}$ on itself. $\mathbb{Z}_2$ is generated by an element ε , which fixes each element of $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$, and maps each μ_i to $-\mu_i$, so mapping $\sqrt{29}$ to $-\sqrt{29}$.

The conjugacy classes are:

$C_1' = \{\varepsilon\}$

$C_2' = \{\sigma_1\varepsilon, \sigma_2\varepsilon, \sigma_3\varepsilon\}$

$C_3' = \{\tau\varepsilon, \tau\sigma_1\varepsilon, \tau\sigma_2\varepsilon, \tau\sigma_3\varepsilon\}$

$C_4' = \{\tau^{-1}\varepsilon, \tau^{-1}\sigma_1\varepsilon, \tau^{-1}\sigma_2\varepsilon, \tau^{-1}\sigma_3\varepsilon\}$.

Once again, the primes not congruent to ± 1 modulo 7 correspond to the classes C_3, C_3', C_4 and C_4' depending upon whether $p \equiv \pm 2 \ (mod\ 7)$ or $p \equiv \pm 4 \ (mod\ 7)$ and whether 29 is a square *mod* p or not. In these cases the use of Cebotarev's Density Theorem gives no new information. But primes which are congruent to ± 1 modulo 7 correspond to class C_1 or C_2, in the ratio 1 : 3, if 29 is a square modulo p and to class C_1' or C_2', in the same ratio, if 29 is not a square *mod* p. Thus, among the primes:

in $\frac{1}{8}$ of the cases no diagram contains the fragment (and 29 is not a square),

in $\frac{3}{8}$ of the cases one diagram contains the fragment (and 29 is a square),

in $\frac{3}{8}$ of the cases two diagrams contain the fragment (and 29 is not a square),

in $\frac{1}{8}$ of the cases all three diagrams contain the fragment (and 29 is a square).

Bibliography

[1] G. Baumslag, J. W. Morgan and P.B. Shalen, Generalized triangle groups, Math. Proc. Cambridge Philos. Soc., 102 (1987) , 25 – 31.

[2] A. Cayley, The theory of groups, graphical representation, Amer. J. Math., 1 (B) , 1878, 174 – 176.

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

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

[5] M. D. E. Conder, Three relator quotients of the modular group, Quart. J. Math., Oxford (2) , 38 (1987) , 427 – 447.

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

[7] Cebotarev's Density Theorem, Encyclopedic Dictionary of Mathematics, Math. Soc. Japan, M. I. T. Press, 1980, 16 – 17.

[8] A. M. Macbeath, Generators of linear fractional groups, Number Theory, Proc. of Symposia in pure Math. 12 AMS, 1969, 14 – 32.

[9] W. Magnus, Non-Euclidean tessellations and their groups, Acad. Press, New York, 1974.

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

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

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