Topics in Inverse Galois Problem

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Siddhant Sharma

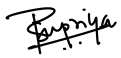
Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

May, 2021

Supervisor: Dr. Supriya Pisolkar

Certificate

This is to certify that this dissertation entitled Topics in Inverse Galois Problem towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Siddhant Sharma at Indian Institute of Science Education and Research under the supervision of Dr. Supriya Pisolkar, Associate Professor, Department of Mathematics , during the academic year 2020-2021.



Dr. Supriya Pisolkar

Committee:

Dr. Supriya Pisolkar

Dr. Vivek Mohan Mallick

This thesis is dedicated to my parents for giving me constant support during what has been a difficult year for everyone.

Declaration

I hereby declare that the matter embodied in the report entitled Topics in Inverse Galois Problem are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Supriya Pisolkar and the same has not been submitted elsewhere for any other degree.

Siddhant Sharma

Acknowledgments

I would like to express my deep gratitude to my project supervisor, Dr. Supriya Pisolkar for her guidance and encouragement in carrying out this project. I would like to especially thank her for showing patience with me throughout the duration of this project.

Abstract

The Inverse Galois Problem asks whether every finite group occurs as the Galois group of some field extension of the rational numbers, $\mathbb{Q}$. This is still an unsolved problem. This project explores various methods to try to answer this question, most notable among which is the rigidity method.

In this project, the required theory is presented to arrive at the Rigidity Criterion which is then applied to various finite simple groups, including the Mathieu groups, linear groups and the Monster group, to show their occurrence as Galois groups over $\mathbb{Q}$.

Contents

Introduction

Field extensions $E/\mathbb{Q}$ which satisfy certain properties can be expressed as the splitting field of a polynomial $p(x)$ with coefficients in $\mathbb{Q}$. We call such extension Galois extensions. To such extensions, a group is associated, called the Galois group, denoted by $Gal(E/\mathbb{Q})$. The Galois group permutes the roots of the polynomial $p(x)$. This is discussed in a little more detail in the next chapter.

Now an interesting question that arises is if we can do the converse i.e. for a given group G, is it possible to find such an extension with G as its Galois groups(up to a group isomorphism). The objective of this project is to try to answer this question.

This question was first studied by Hilbert in the 19th century which lead to the very important Hilbert's Irreducibility Theorem in his paper in 1892 [4]. A crucial breakthrough came with a J. Thompson's paper in 1984 [8], in which he developed the powerful rigidity method using which he showed that the Monster group occurs as a Galois group over $\mathbb{Q}$. The method has been used to show the occurrence of various finite simple groups, including all but 2 sporadic groups, as Galois groups over $\mathbb{Q}$.

In this project, various important results are proved which finally lead to the powerful rigidity criterion. The rigidity criterion provides a group theoretic method to check whether a group is realisable over the rational numbers. With the help of Hilbert's theorem, the results can be extended to number fields i.e. the finite extensions of $\mathbb{Q}$.

The proofs of these results will also show how various branches of mathematics come together in harmony.

Original Contribution: The thesis is for the most part a review of the known results pertaining to the Inverse Galois Problem primarily based on [6] and [10]. However some new examples have been discussed and certain details have been added in the proofs to fill in the gaps and make the proofs more comprehensible and easier to understand for the reader.

Also the calculations for the rigidity verification for the groups M_{12}, M_{22}, J_2 and Suz have been done using C programs written by me and are shown in the Appendix along with the outputs.

Chapter 1

Preliminaries

In this chapter, basic definitions and important results in Introductory Galois Theory have been presented which will be found useful later.

1.1 Galois Extensions

Definition 1.1.1. *An extension L/K is called* ***algebraic*** *if all elements of L are algebraic over K, i.e. every element is a root of some polynomial with coefficients in K.*

Examples: The extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$ are algebraic while $\mathbb{R}/\mathbb{Q}$ is not an algebraic extensions.

Definition 1.1.2. *An algebraic extension L/K is called* ***normal*** *if every irreducible polynomial over K with a root in L has all its roots in L.*

Examples: The extensions $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$ are normal while $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension.

Definition 1.1.3. *An polynomial $f(x) \in K[x]$ is called separable if it has distinct roots in an algebraic closure of K. An extension L/K is called* ***separable*** *if all elements of L are separable over K, i.e. their minimal polynomial over K is separable.*

Definition 1.1.4. *An extension L/K is called **Galois** if it is both normal and separable.*

Definition 1.1.5. *Let L/K be a Galois extension. Then the set of automorphisms of L which fix K element-wise form a group called the Galois group of L/K, denoted $Gal(L/K)$ or $G(L/K)$.*

Example: Consider the extension $\mathbb{Q}(\sqrt[3]{2}, \omega)$. This is a Galois extension and its Galois group is isomorphic to the symmetric group S_3.

We now state a few important results from Galois theory whose proofs may be looked at in any introductory book on Galois Theory like [7].

Theorem 1.1.1. *Let L/K be a finite Galois extension. Then there exists $\alpha \in L$ such that $L = K[\alpha]$. Such an element is called a **primitive element** of L.*

Theorem 1.1.2. ***Artin's Theorem.*** *Let G be a finite group of automorphisms of a field L with a fixed field K. Then L/K is a Galois extension with G as its Galois group.*

Theorem 1.1.3. ***Fundamental Theorem of Galois Theory.*** *Let L/K be a finite Galois extension. Then there is a one to one correspondence between the intermediate fields E and the subgroups H of $Gal(L/K)$ given by $E \mapsto Gal(L/E)$ on one side and $H \mapsto L^H$ on the other side where L^H is the fixed field of H. In addition, the correspondence satisfies the following*
1. For subgroups H_1, H_2 of $Gal(L/K)$, $H_1 \subseteq H_2$ if and only if $L^{H_2} \subseteq L^{H_1}$.
2. $[Gal(L/K) : H] = [L^H : K]$
3. E/K is Galois if and only if $Gal(L/E)$ is a normal subgroup of $Gal(L/K)$, in which case $Gal(E/K) \cong Gal(L/K)/Gal(L/E)$.

Chapter 2

Abelian Groups, Symmetric Groups and Alternating Groups

In this chapter, it is shown with the help of some basic Galois theory and Hilbert's theorem, that all finite abelian groups, symmetric groups and alternating groups are realisable over $\mathbb{Q}$.

The proofs presented are primarily based on basic results in Galois Theory. The proof of Dirichlet's Theorem presented was put together by me using some hints in [3].

2.1 Abelian Groups

Lemma 2.1.1. *Let $L|k$ and $K|k$ be two galois extensions such that $L \cap K = k$ i.e. $L|k$ and $K|k$ are linearly disjoint, then the galois group $Gal(LK|k)$ is isomorphic to $Gal(L|k) \times Gal(K|k)$.*

Proof. We have the natural map $\rho\colon Gal(LK|k) \to Gal(L|k) \times Gal(K|k)$ mapping $\sigma \mapsto (\sigma \restriction_L, \sigma \restriction_K)$. Clearly ρ is a group homomorphism with trivial kernel. Since the extensions $L|k$ and $K|k$ have trivial intersection, ρ is onto.

The following result by Dirichlet is proved using elementary facts about cyclotomic polynomials.(See [3] , 13.6, Ex. 14-17)

Dirichlet's Theorem. For any $n \geq 1$, there exist infinitely many primes p satisfying $p \equiv 1 \bmod(n)$.

Proof. Let Φ_n be the nth cyclotomic polynomial. Suppose p is a prime with $p \nmid n$. Then $x^n - 1$ is separable modulo p. Hence any root of Φ_n modulo p is a primitive root. If such a root exists, then by Lagrange's theorem for finite groups, we must have $n|p-1$ i.e. $p \equiv 1 \bmod(n)$. So we show that there exist infinitely many primes such that each one of them divides $\Phi_n(a)$ for some integer a. To see this, suppose $p_1, p_2, ..., p_k$ are the only such primes. Now we have $\Phi_n(M) = b \neq 0$ for some integers M and b. We note that the polynomial $f(x) = \frac{1}{b}\Phi_n(M + bp_1p_2...p_kx)$ has integer coefficients and $f(l) \equiv 1 \bmod(p_i)$ for each i and for all integers l. But there must be some integer N such that $f(N) \neq \pm 1$. Therefore there exists a prime q different from each p_i, such that $q|\Phi_n(M + bp_1p_2...p_kN)$, which is a contradiction. Since there are only finitely many primes dividing n, we have infinitely many primes $p \nmid n$ such that $\Phi_n(x)$ has a root modulo p. This completes the proof. □

Theorem 2.1.2. *Every finite abelian group is realisable over* $\mathbb{Q}$.

Proof. Let G be a finite abelian group. By structure theroem of finite abelian groups, $G = \prod_{i=1}^{k} C_{n_i}$, where C_{n_i} are cyclic groups of order n_i. By Dirichlet's theorem above, we can choose distinct primes p_i, such that for each i, $p_i \equiv 1 \bmod(n_i)$. Now $Gal(\mathbb{Q}(\zeta_{p_i})|\mathbb{Q})$ is cyclic and has order $p_i - 1$, so $\mathbb{Q}(\zeta_{p_i})$ contains an extension $L_i|\mathbb{Q}$ such that $Gal(L_i|\mathbb{Q}) \cong C_{n_i}$. Since $p_i s$ are distinct, $\Pi_{j \neq i} L_j \cap L_i = \mathbb{Q}$. Then taking $L = \prod_{i=1}^{k} L_i$, repeatedly applying Lemma 2.1.1, we see that $Gal(L|\mathbb{Q})$ is isomorphic to G. □

2.2 Symmetric and Alternating Groups

We will now show that the symmetric groups S_n and the alternating groups A_n are realisable over $\mathbb{Q}$. In fact, these groups are realisable over any number field. We will use the following theorem by Hilbert which we state without proof. For a proof see , Ch.1.

Hilbert's Irreducibility Theorem Let K be a number field and $f(t, X) \in K(t)[X]$ be an irreducible polynomial where t is an indeterminate. Then there exist infinitely many $a \in K$ such that $f(a, X)$ is well defined and irreducible over K. Moreover a can be chosen so that

$Gal(f(a,X)|K) \cong Gal(f(t,X)|K(t))$

We shall need the following lemma which follows from elementary Galois theory.

Lemma 2.2.1. *Let K be a field of characteristic zero and f be an irreducible polynomial over K, then $Gal(f|K)$ acts transitively on the roots of f. Moreover if, for every root α of f, $f(X)/(X-\alpha)$ is irreducible over $K(\alpha)$, the $Gal(f|K)$ acts doubly transitively on the roots of f.*

We now present a proof for S_n and A_n being realisable over $\mathbb{Q}$. The proof can be used to show that S_n and A_n are realisable over any number field using Hilbert's Irreducibility Theorem.

Theorem 2.2.2. *For all $n \in \mathbb{N}$, S_n is realisable over $\mathbb{Q}$.*

Proof. Consider the polynomial $f(t,X) = X^n + tX + t$. By Eisenstein's criterion, f is irreducible over $\mathbb{Q}(t)$. Let α be any root of f. We show that $f(t,X)/(X-\alpha)$ is irreducible over $\mathbb{Q}(t,\alpha)$. Noting that $t = -\frac{\alpha^n}{1+\alpha}$, we have $f(t,X)/(X-\alpha) = X^{n-1} + \alpha X^{n-2} + ... + \alpha^{n-1} - \frac{\alpha^n}{1+\alpha}$. Doing the substitution $Y = \alpha/X$, we see by Eisenstein's criterion that the polynomial $Y^{n-1} + \beta(Y^{n-2} + ... + Y + 1)$ is irreducible over $\mathbb{Q}(\beta)$ where $\beta = 1+\alpha$. Therefore $f(t,X)/(X-\alpha)$ is irreducible over $\mathbb{Q}(t,\alpha)$ and by lemma 2, $Gal(f|\mathbb{Q}(t))$ is a 2-transitive subgroup of S_n.
Now let $s = t + n^n/(1-n)^{n-1}$, we have

$$g(s,X) = f(t,X) = X^n + (s - n^n/(1-n)^{n-1})X + (s - n^n/1 - n^{n-1})$$

The discriminant

$$d(g) = (-1)^{n(n-1)/2}(1-n)^{n-1}s(s - \frac{n^n}{(1-n)^{n-1}})^{n-1}$$

Now $Gal(g(s,X)|\mathbb{C}((s))) \subset Gal(g(s,X)|\mathbb{Q}(s)) = Gal(f(t,X)|\mathbb{Q}(s))$. Also $Gal(g(s,X)|\mathbb{C}((s)))$ is non trivial since $d(g)$ is not a square in $\mathbb{C}((s))$.
We have $g(s,X) \cong X^n - n^n/(1-n)^{n-1})X + (-n^n/1 - n^{n-1})mod(s)$. After scaling X by $(1-n)/n$, we have the polynomial $X^n - nX + (n-1)$, which has 1 double root and $n-2$ simple roots in $\mathbb{C}$. By Hensel's Lemma [1], $g(s,X)$ has $n-2$ roots in $\mathbb{C}((s))$, so $Gal(g(s,X)|\mathbb{C}((s))$ acts by permuting the other two roots. Therefore $Gal(f(t,X)|\mathbb{Q}(t))$ is a 2-transitive subgroup of S_n containing a transposition. Hence $Gal(f(t,X)|\mathbb{Q}(t)) \cong S_n$. Now by Hilbert's

Irreducibility Theorem, S_n is realisable over $\mathbb{Q}$. $\square$

Theorem 2.2.3. *For all $n \in \mathbb{N}$, A_n is realisable over $\mathbb{Q}$.*

Proof. Let $f(t, X)$ be as in Theorem 2.2.2. The discriminant of f is $(-1)^{n(n-1)/2}t^{n-1}[(1-n)^{n-1}t + n^n]$.

For n odd, set $u = \sqrt{(-1)^{n(n-1)/2}[(1-n)^{n-1}t + n^n]}$. Defining L as the splitting field of $f(t, X)$ over $\mathbb{Q}(t)$, we get a quadratic sub-extension $\mathbb{Q}(u)|\mathbb{Q}(t)$. Then using Theorem 2, we see that $Gal(L|\mathbb{Q}(u)) \cong Gal(L|\mathbb{Q}(t))/Gal(\mathbb{Q}(u)|\mathbb{Q}(t)) \cong A_n$.

For n even, set $s = 1/t$ and consider the polynomial $h(s, X) = f(1/s, X)$. Then $d(h) = (-1)^{n(n-1)/2}[(1-n)^{n-1} + n^n s]/s^n$.
Letting $v = \sqrt{(-1)^{n(n-1)/2}[(1-n)^{n-1} + n^n s]}$, similar to the case n odd, we get $Gal(L|\mathbb{Q}(v)) \cong A_n$. Hilbert's Irreducibility Theorem now gives us Galois realisation of A_n over $\mathbb{Q}$. $\square$

Chapter 3

Riemann's Existence Theorem - Topological Version

Rigidity method relies crucially on the Riemann's Existence Theorem. The theorem guarantees the existence of Galois realisations of finite groups over the field $\mathbb{C}(x)$. This chapter introduces some necessary definitions and results from algebraic topology , which finally help in proving a topological version of the Riemann's Existence Theorem .
This chapter is primarily based on the theory developed in [10] and some basic results from introductory Algebraic Topology. A few examples have been added to illustrate the definitions and results.

3.1 Homotopy and The Fundamental Group

Let X be a topological space and p, q be two points in X. Then a path in X from p to q is a continuous map $\gamma\colon [0,1] \to X$ such that $\gamma(0) = p$ and $\gamma(1) = q$. Two such paths γ_0 and γ_1 are homotopic if there is a continuous map $F\colon [0,1] \times [0,1] \to X$ such that $F(0,t) = \gamma_0(t)$, $F(1,t) = \gamma_1(t)\ \forall t \in [0,1]$ and $\forall s \in [0,1], F(s,0) = p$ and $F(s,1) = q$. This defines an equivalence relation.
The product of two paths α and β such that $\alpha(1) = \beta(0)$, is defined as
$\beta\alpha(t) = \alpha(2t)$, if $t \in [0,1/2]$ and $\beta\alpha(t) = \beta(2t-1)$, otherwise
The inverse path of γ is defined as γ^{-1}, with $\gamma^{-1}(t) = \gamma(1-t)\ \forall t \in [0,1]$. The above product

also induces a product on the equivalence classes of paths. Let $\pi(X,p)$ be the set of all equivalence classes of loops in X at p(i.e. the paths which both end and start at p). $\pi(X,p)$ forms a group with this product and $[\gamma]^{-1} = [\gamma^{-1}]$. This group is known as the fundamental group of X at p.
A topological manifold is a space that is Hausdorff, second countable and locally euclidean. From now on, we assume X is a topological manifold.

A covering of X is a surjective map $f\colon Y \to X$ such that for each point $p \in X$, there is a neighbourhood U of p for which $f^{-1}(U)$ is a disjoint union of open subsets of Y, each of which is mapped by f, homeomorphically onto U. A simple example of a covering is the map $f : \mathbb{R} \mapsto S^1$, defined by $f(t) = e^{2\pi it}$, where the circle S^1 is the subset of complex numbers of modulus equal to 1.

For a path γ in X, a path $\tilde{\gamma}$ in Y is called a lift of γ if $f \circ \tilde{\gamma} = \gamma$. We recall a few results from algebraic topology [5].

Theorem 3.1.1. *Let $f\colon Y \to X$ be a covering and γ a path in X starting at p. Then for each $y \in f^{-1}(p)$, there exists a unique lift of gamma in Y with starting point y. Moreover, lift of two homotopic paths are homotopic if they have the same starting point.*

The Fundamental group $\pi(X,p)$ has a natural action on the fiber $f^{-1}(p)$ in the following way: For $[\gamma] \in \pi(X,p)$ and $y \in Y$, we define $[\gamma]y$ as the end point of the unique lift of γ in Y beginning at y. For a connected space X, the action is transitive iff Y is connected.

Lemma 3.1.2. *Let $f\colon Y \to X$ be a covering where X is connected. LetA be a connected component of Y. Then f restricts to a covering from A to X and if $f^{-1}(p)$ is contained in A, then $A = Y$ i.e. Y is connected.*

Lemma 3.1.3. *Let $f_i\colon Y_i \to X$ be two coverings, $i = 1, 2$ with Y_1, Y_2 connected. Let $y_i \in Y_i$ such that $f_i(y_i) = p$ for each i. Suppose for each $[\gamma] \in \pi(X,p)$, $[\gamma]$*

3.2 Galois Coverings

Definition 3.2.1. *Two coverings $f_1\colon Y_1 \to X$ and $f_2\colon Y_2 \to X$ are called equivalent if there exists a homeomorphism $\alpha\colon Y_1 \to Y_2$ such that $f_2 \circ \alpha = f_1$. Also if $Y_1 = Y_2 = Y$ and*

$f_1 = f_2 = f$, then such a homeomorphism is called a deck transformation of f. The set of deck transformations, under composition, forms a group denoted by Deck(f).

$Deck(f)$ has a natural action on the fibres $f^{-1}(p)$ for each $p \in X$ defined just by mapping x to $h(x)$ for any $h \in Deck(f)$ and $x \in f^{-1}(p)$. It is easily seen that this action commutes with the action of $\pi(X, p)$ on $f^{-1}(p)$.

Lemma 3.2.1. *Let $f\colon Y \to X$ be a covering and Y connected. Then if a deck transformation fixes a point y in Y, the it is equal to the identity map on Y. Also if a subgroup G of $Deck(f)$ acts transitively on a fibre of f, then $G = Deck(f)$.*

The deck transformation group of the covering of S^1 defined earlier can be shown to be isomorphic to the group of integers with addition. The group has a generator h which maps x to $x + 1$ for each $x \in \mathbb{R}$. This group acts transitively on the fibres of the covering. Hence it is a Galois covering.

If X is connected, then each fibre has the same cardinality and is called the degree of f. This is clear by noting that the cardinality of fibres is locally constant in X.

Definition 3.2.2. *A covering $f\colon Y \to X$ is called a Galois covering if Y is connected and $Deck(f)$ acts transitively on the fibres of f.*

The degree of a Galois covering f is equal to the cardinality of $Deck(f)$. This can be shown by defining an obvious bijection from $Deck(f)$ to a fibre $f^{-1}(p)$.

Proposition 3.2.2. *Let $f\colon Y \to X$ be a Galois covering and $y \in Y$, $p \in X$. There exists a unique surjective homomorphism $\Phi_y\colon \pi(X, p) \to Deck(f)$ such that $\forall[\gamma] \in \pi(X, p)$, $\Phi_y([\gamma])$ maps $[\gamma]y$ to y.*

3.3 Coverings of the Punctured Sphere

Let $\mathbb{P}^1$ be the Riemann sphere and P be a finite subset of $\mathbb{P}^1$. Let $f\colon R \to \mathbb{P}^1 \setminus P$, a finite galois covering and $D = B(p, r)$ be an open disc disjoint from P and $D^* = D \setminus P$. Now

define the map,

$$\begin{aligned} \kappa_p : D^* &\to \mathbb{K}(r) \\ z &\mapsto \begin{cases} z-p & p \neq \infty \\ \frac{1}{z} & p = \infty \end{cases} \end{aligned} \tag{3.1}$$

where $\mathbb{K}(r)$ is the unit disc in $\mathbb{C}$ minus the origin.

Let E be a connected component of $f^{-1}(D^*)$, and define $f_E = \kappa_p \circ f|_E$. This defines a covering $f|_E : E \to \mathbb{K}(r)$. E is called a circular component of level r over p. Let $0 < \widehat{r} < r$. There is a bijection between circular components E of level r and circular components $\widehat{E}$ of level $\widehat{r}$ over p since there is exactly one component $\widehat{E} \subset E$, and $f_{\widehat{E}}$ is the restriction of f_E to $\widehat{E}$. Hence we can define an equivalence relation on the set of circular components over $p : E \sim E'$ if $E \subset E'$ or $E' \subset E$. The equivalence classes are called the ideal points of R over p.

Lemma 3.3.1. *The group Deck (f) permutes the components E of $f^{-1}(D^*)$ transitively. Let H_E is the stabiliser of E in $H := \mathrm{Deck}(f)$, then the restriction to E defines an isomorphism $H_E \to \mathrm{Deck}(f_E)$.*

Proof. H acts on $f^{-1}(D^*)$ and permutes the components E. Let $h \in H$. Since the circular components are pairwise disjoint, if h maps one point of E to E', some other component, then h maps all of E to E'. This implies that if h a $p \in E$ into E, then $h \in H_E$. Let $p^* \in D^*$ and $F_E = f^{-1}(p^*) \cap E$, a fiber of the $f|_E$. H acts transitively on the fiber $f^{-1}(p^*)$, any two points of F_E can be mapped into each other by some $h \in H$. We have just seen that this means $h \in H_E$. Thus H_E acts transitively on F_E. That the homomorphism $H_E \to \mathrm{Deck}(f_E)$ given by restriction to E follows now from Lemma 3.2.1. □

The group H_E is cyclic of size e, where e is the degree of f_E, since it is isomorphic to the deck transformation group of a punctured disc in $\mathbb{C}$. This deck transformation group has a unique element σ with the following property: For each homeomorphism $\varphi : E \to \mathbb{K}\left(r^{1/e}\right)$ with $\varphi^e = f$ we have $\varphi \circ \sigma^{-1} = \zeta_e \varphi$, where $\zeta_e = \exp(2\pi\sqrt{-1}/e)$. This σ generates Deck (f) and is called the distinguished generator. Let h_E be the distinguished generator of H_E corresponding to σ. The h_E's are all conjugates to each other and lie in a conjugacy class C_p.

Let $f : R \to \mathbb{P}^1 \backslash P$ be a finite Galois covering. Let $\bar{R}$ be the disjoint union of R and all ideal points over all $p \in P$. Define a topology on $\bar{R}$ by $V \subset \bar{R}$ is open if $V \cap R$ is open in

R and the following holds: for each ideal point $\pi \in V$ there is an $E \in \pi$ with $E \subset V$. Then R is a connected compact Hausdorff space [10].
Moreover we can extend $f : R \to \mathbb{P}^1 \backslash P$ to a continuous surjective map $\bar{f} : \bar{R} \to \mathbb{P}^1$ by setting $\bar{f}(\pi) = p$ where π is an ideal point over p and each $\alpha \in \mathrm{Deck}(f)$ also extends uniquely to a homeomorphism $\bar{\alpha} : \bar{R} \to \bar{R}$ such that $\bar{f} \circ \bar{\alpha} = \bar{f}$.

3.3.1 Ramification Type

Let $p_1, \ldots, p_n \in \mathbb{C}$ distinct and set $S = \mathbb{C} \backslash \{p_1, \ldots, p_n\}$. It is possible to choose a point such that the straight line between this point and the p_i hit no other p_j. Let $q_0 \in S$ be such a point. Can write $p_i = q_0 + \rho_i e^{i\nu_i}$. Relabel the p_i so that the v_i are increasing. Here of course ν_i represents the angle the line from q_0 to p_i makes with the real line. Now divide the complex plane up, into connected components S_i, with rays, $M_1, \ldots, M_n$ emanating from q_0 such that each p_i lies in S_i. Let D_i be a disc about p_i entirely contained within S_i. Define paths γ_i starting from q_0, travelling along the straight line from q_0 to p_i until it hits the boundary of D_i, traversing the boundary once clockwise, and travelling back to q_0 along this same line. It can be shown that the classes $[\gamma_i]$'s generate the fundamental group $\pi(S, q_0)$. We will need the following result to finally prove the topological version of Riemann's Existence Theorem. The proof is quite long and may be looked at in [10].

Theorem 3.3.2. *Let $S = \mathbb{C} \backslash \{p_1, \ldots, p_n\}$. Let G be a group with generators $g_1, \ldots, g_n$. Then $\exists$ a Galois covering $f : R \to S$, an isomorphism $\theta : \mathrm{Deck}(f) \to G$ and a point $b \in f^{-1}(q_0)$ such that the composition of θ with the surjection $\Phi_b : \pi_q(S, q_0) \to \mathrm{Deck}(f)$ in Proposition 3.2.2 maps $[\gamma_i]$ to g_i for $i = 1, \ldots, n$. Now $G \cong \mathrm{Deck}(f)$. If G is finite then $f : R \to \mathbb{P}^1 \backslash \{p_1, \ldots, p_n, \infty\}$ is a finite Galois covering, and the associated conjugacy classes $C_i = C_{p_i}$ and C_∞ of G are such that $g_i \in C_i$ and $(g_1 \cdots g_n)^{-1} \in C_\infty$ for $i = 1, \ldots, n$.*

Definition 3.3.1. *Let $f : R \to \mathbb{P}^1 \backslash P$ be a finite Galois covering. Let $H = \mathrm{Deck}(f)$, and for $p \in P$, let C_p be the associated conjugacy class of H. Let $P' = \{p \in P : C_p \neq \{1\}\}$. We define the ramification type of f to be the class of the triple $\left(H, P', (C_p)_{p \in P'}\right)$.*

Theorem 3.3.3. ***Riemann's Existence Theorem - Topological Version*** *Let $\mathcal{T} = \left[G, P, (K_p)_{p \in P}\right]$ be a ramification type. Let $r = |P|$ and label the elements of P as $p_1, \ldots, p_r$. Then there exists a finite Galois covering of $\mathbb{P}^1 \backslash P$ of ramification type $\mathcal{T}$ if and only if there exist generators $g_1, \ldots, g_r$ of G with $g_1 \cdots g_r = 1$ and $g_i \in K_{p_i}$*

Proof. Changing the coordinates, we can assume that $\infty \in P$, and we label the elements such that $p_r = \infty$. Now $f : R \to \mathbb{P}^1 \backslash P$ is a finite Galois covering of ramification type $\mathcal{T}$. Let $q_0 \in \mathbb{P}^1 \backslash P$ and paths $\gamma_1, \ldots, \gamma_{r-1}$ as earlier. Let $\gamma_r = (\gamma_1 \cdot \gamma_{r-1})^{inv}$. Consider the fiber $f^{-1}(q_0)$, and fix some point b in this fiber. Then $\Phi_b : \pi_1(\mathbb{P}^1 \backslash P, q_0) \to G$ is a surjective homomorphism. Let $g_i := \Phi_b([\gamma_i])$. Then the g_i generate G and $g_i \in C_{p_i} = C_i$ by Theorem 3.3.2. Finally, $\gamma_1 \cdots \gamma_r = 1$ by the definition of γ_r. Thus $g_1 \cdots g_r = 1$ as Φ_b is a homomorphism. Conversely, suppose we have generators $g_1, \ldots, g_r$ of G with $g_1 \cdots g_r = 1$ and $g_i \in K_{p_i}$. By Theorem 3.3.2, there is a finite Galois covering $f : R \to \mathbb{P}^1 \backslash P$ and an isomorphism between $\mathrm{Deck}(f)$ and G such that g_i lies in the class of C_{p_i} associated to p_i for $i = 1, \ldots, r-1$. $g_r = (g_1 \cdots g_{r-1})^{-1} \in C_\infty = C_{p_r}$. Hence $\mathrm{Deck}(f) \cong G$, and $C_p = K_p$ $\forall p \in P$. Therefore we have a covering f of ramification type $\mathcal{T}$. $\square$

Chapter 4

Rigidity and Riemann's Existence Theorem - Algebraic Version

This chapter discusses finite Galois extensions of $C(x)$. The idea of branch point arises and we arrive at an algebraic definition of ramification type and the algebraic version of Riemann's Existence Theorem. The idea of rigidity is introduced for the ramification types.

This chapter is also primarily based on [10] with some details added to the proofs. The proof left to the reader in [10] has also been provided here and new example has been added to illustrate the result.

4.1 Galois Extensions of Laurent Series Fields

Definition 4.1.1. *Let k be a field. Then the set of formal series $\sum_{i=N}^{\infty} a_i t^i$, where $a_i \in k$ and $N \in \mathbb{Z}$, forms a field with the obvious addition and multiplication operations. We denote it by Λ. The subring of Λ comprising of $\sum_{i=N}^{\infty} a_i t^i$ with $N \geq 0$. is denoted by $k[[t]]$.*

Consider a polynomial $F(y) \in k[[t]][y]$. By going modulo t, we obtain a polynomial $F_0(y)$ over k. Then we have the following lemma.

Lemma 4.1.1. *Let $F(y) \in k[[t]][y]$ be a monic polynomial such that $F_0(y)$ factors as a product of two coprime monic polynomials, g and h. The F also factors as a product of two*

monic polynomials G and H with $G_0 = g$ and $H_0 = h$.

Let e be a natural number and Λ_e be the field $k((t^{1/e}))$. The Λ is a subfield of Λ_e. Let τ be such that $\tau^e = t$. If k contains a primitive eth root of unity, the Λ_e/Λ is a cyclic extension. The Galois group is generated by ω which fixes k and maps τ to $\zeta_e\tau$ and ω is called the distinguished generator of $G(\Lambda_e/\Lambda)$.

We first prove a useful lemma.

Lemma 4.1.2. *Let k be an algebraically closed field of characteristic 0. Let $F(y)$ be a monic, non-constant polynomial over $k[[t]]$. Then there exists $e \in \mathbb{N}$ such that Λ_e contains a root of F.*

Proof. Let F be the polynomial of minimal degree for which the lemma is false. Clearly, the degree n of F is at least 2. By changing the variable, it can be assumed that the coefficient of $y^{n-1} = 0$. Now we claim that $F_0 = y^n$. Since k is algebraically closed F_0 is a product of monic linear factors. Now if they are not all equal, then F_0 factors a product of two monic coprime polynomials. By Lemma 4.1.1, F also factors as a product of two monic polynomials, which contradicts the minimality of degree of F. So $F_0 = (y-\alpha)^n$, with $\alpha \in \Lambda$. Noting that $\mathrm{char}(k)$ is 0 and coefficient of y^{n-1} is 0, we must have $F_0 = y^n$.
Now $F = y^{n-1} + \lambda_{n-1}y^{n-1} + ... + \lambda_0$ with λ_is in $k[[t]]$. Now there must be some $s \leq n-2$ such that $\lambda_s \neq 0$, otherwise $F = y^n$ has a root in Λ. Let m_s be the lowest power of t with non-zero coefficient in λ_s. Then $m_s > 0$. Let u be the minimum among all $m_s/(n-s)$. Express u as d/e where d, e are positive integers. Consider the polynomial F^* over Λe, $F^* = \tau^{-dn}F(\tau^d y)$, which also has degree n. It can be checked that all coefficients of F^* lie in $k[[\tau]]$ and that F^* has non-zero constant term. So once again F^* factors into monic polynomials of degree less than n. By minimality of n, these factors have a root in some $\Lambda_e(\tau^{1/e'})$. So F^* has a root in $\Lambda_{ee'}$ and consequently F has a root in $\Lambda_{ee'}$. □

Now we can prove the following theorem.

Theorem 4.1.3. *Let k be an algebraically closed field of characteristic 0 and Δ be a degree e extension of Λ_e. Then $\Delta = \Lambda(\alpha)$ where α is an eth root of t. In particular Δ is isomorphic to Λ_e.*

Proof. By primitive element theorem, $\Delta = \Lambda(\beta)$. The primitive element β has an irreducible polynomial $F(y)$. By the previous lemma F has a root γ in some $\Lambda_{e'}$, which

implies that $\Delta \subset \Lambda_{e'}$. Clearly e divides e', so by Galois correspondence there is a unique subextension of degree e(since $\Lambda_{e'}/\Lambda$ is cyclic). Therefore $\Delta = \Lambda(t^{1/e})$. □

4.1.1 Branch Points

Let's first fix a compatible system of primitive roots of unity $(\zeta_e)_{e\in\mathbb{N}}$ in k, an algebraically closed field. The roots satisfy the condition $\zeta_{mn}^n = \zeta_m$ for all m, n positive integers.

Define $\mathbb{P}_1^k$ to be $k \cup \{\infty\}$ and for each $p \in \mathbb{P}_1^k$, let v_p be the isomorphism from $k(x)$ to $k(t)$ which fixes k and maps x to $t + p$ if p is not ∞ and to $1/t$ otherwise.
Consider a finite Galois extension $L/k(x)$ and G its Galois group.

Lemma 4.1.4. *The isomorphism v_p can be extended to an isomorphism $v\colon L \to L_v$, for some subfield L_v of a finite Galois extension Δ/Λ. Moreover L_v is invariant under the action of $Gal(\Delta/\Lambda)$.*

Proof. Let F be the irreducible polynomial of a primitive element α of $L/k(x)$ and F_p the polynomial obtained by applying v_p to the coefficients of F. Let H be an irreducible factor of F_p and $\Delta = \Lambda[y]/(H)$ be the extension obtained by adjoining the root of H to Λ. Now F_p has a root γ in Δ, so v_p naturally extends to an isomorphism from $L = k(x)(\alpha)$ to $L_v = k(t)(\gamma)$. Noting that the roots of F_p generate L_v and $Gal(\Delta/\Lambda)$ permutes them, we see that L_v is invariant under the action of $Gal(\Delta/\Lambda)$. □

Since $G = Gal(\Delta/\Lambda)$ leaves L_v invariant, $g_v = v^{-1}\omega v$ is an element of G. The question now is what if we choose a different Δ and v. It turns out that the element g_v remains in the same conjugacy class regardless of these choices. We denote this class by C_p which only depends on L and p.

Definition 4.1.2. *The ramification index of L at p is defined as the common order of the elements in C_p. We will denote it by $e_{L,p}$ or simply e when the context is clear.*

Definition 4.1.3. *The points p in $\mathbb{P}_1^k$ for which $e_{L,p} > 1$ are called the branch points of $L/k(x)$.*

The following result follows now easily from the definitions of g_v and C_p.

Proposition 4.1.5. *Let L/k(x) and L'/k(x) be finite Galois extensions of degree n. For every point p in $\mathbb{P}^k_1$, we have the Galois groups G, G' resp. and the conjugacy classes of p, C_p, C'_p resp. Now let α be an automorphism of k and m an integer satisfying $\alpha^{-1}(\zeta_n) = \zeta_n^m$. If α extends to an isomorphism $\lambda\colon L \to L'$ fixing x, let λ^* be the induced group isomorphism from G to G' via conjugation by λ. Then $\lambda^*(C_p)^m = C'_{\alpha(p)}$.*

4.2 Algebraic Riemann's Existence Theorem

From now onwards we assume k is an algebraically closed subfield of $\mathbb{C}$ and the compatible set of roots of unity is given by $\zeta_n = exp(2\pi\sqrt{-1}/n)$ for each $n \in \mathbb{N}$.

Definition 4.2.1. *Let G be a group, P a finite subset of $\mathbb{P}^1$, and $\{C_p\}_{p\in P}$ be a collection of conjugacy classes in G, together we have a tuple $\{G, P, \{C_p\}_{p\in P}\}$. We say two such tuples, $\{G, P, \{C_p\}_{p\in P}\}$ and $\{H, Q, \{C_q\}_{q\in Q}\}$ are equivalent if $P = Q$ and there is an isomorphism from G to H taking C_p to C'_p for each $p \in P$. This is an equivalence relation and the equivalence classes are called* ***ramification types****, denoted as $[G, P, \{C_p\}_{p\in P}]$*

Now we can state the algebraic version of Riemann's Existence Theorem. We will not go into details of the proof, since it is quite involved. The proof can be found in [10].

Theorem 4.2.1. ***The Algebraic Riemann's Existence Theorem***
Let $\mathcal{T} = [G, P, \{C_p\}_{p\in P}]$ be a ramification type. Then there exists a finite galois extension of type $\mathcal{T}$ over $\mathbb{C}(x)$ iff G has generators $g_1, g_2, .., g_r$ such that $g_1 g_2 .. g_r = 1$ and $g_i \in C_{p_i}$ for each i.

Note that this implies that every finite group occurs as a Galois group over $\mathbb{C}(x)$.

Definition 4.2.2. *Let $(C_1, ..., C_r)$ be a tuple of conjugacy classed in a finite group G. We say this tuple is* ***rigid*** *if*
1. G has generators $g_1, ..., g_r$ lying in the classes $C_1, ..., C_r$ resp. such that their product is equal to 1, and
2. For any other set of such generators $g'_1, ..., g'_r$, there exists a unique $g \in G$ which conjugates each g_i to g'_i.

In the above definition, if we have an automorphism of G instead of the element g, which maps each g_i to g_i', we say that the tuple is **weakly rigid**.

Definition 4.2.3. *A ramification type $\mathcal{T} = [G, P, \{C_p\}_{p\in P}]$ is called rigid(weakly rigid resp.) if the classes $(C_p)_{p\in P}$ form a rigid(weakly rigid resp.) tuple.*

4.2.1 Rigidity and Irreducible Characters

We prove a simple lemma will help in verifying rigidity of a tuple of conjugacy using the character table of the group.

Lemma 4.2.2. *Let $\chi_1, \chi_2, .., \chi_s$ be the irreducible characters of a finite group G. Let C_1,C_2 and C_3 be conjugacy classes in G with $c_i = |C_i|$. Then the number of triples $(g_1, g_2, g_3) \in C_1 \times C_2 \times C_3$ with $g_1g_2g_3 = 1$ is*

$$\frac{c_1c_2c_3}{|G|}\sum_{i=1}^{s}\frac{\chi_i(C_1)\chi_i(C_2)\chi_i(C_3)}{\chi_i(1)}$$

Proof. For a character χ of G, let σ_χ be the corresponding representation. By Schur's lemma, for every $g \in G$, there is a complex number $\omega(g)$ such that

$$\frac{1}{|G|}\sum_{h\in G}\sigma_\chi(g^h) = \omega(g)I_n$$

where the group action is via conjugacy.
Taking traces, we see that $\omega(g) = \chi(g)/\chi(1)$. Now for any two elements g, g' of G, we have

$$\frac{1}{|G|}\sum_{h\in G}\sigma_\chi(g^hg') = \frac{\chi(g)}{\chi(1)}\sigma_\chi(g')$$

Proceeding similarly we get,

$$\frac{1}{|G|^3}\sum_{(h_1,h_2,h3)\in G^3}\sigma_\chi(g_1^{h_1}g_2^{h_2}g_3^{h_3}g') = \frac{\chi(g_1)\chi(g_2)\chi(g_3)}{\chi(1)^3}\sigma_\chi(g')$$

Putting $g' = 1$ and then taking traces we obtain,

$$\frac{1}{|G|^3} \sum_{(h_1,h_2,h3)\in G^3} \chi(g_1^{h_1} g_2^{h_2} g_3^{h_3}) = \frac{\chi(g_1)\chi(g_2)\chi(g_3)}{\chi(1)^3}$$

The number of triples $(g_1, g_2, g_3) \in G^3$ with $g_1 g_2 g_3 = 1$ is

$$m = \sum_{(h_1,h_2,h3)\in G^3} \epsilon(g_1^{h_1} g_2^{h_2} g_3^{h_3})$$

where $\epsilon = \frac{1}{|G|} \sum_{\chi\in Irr(G)} \chi(1)\chi$ is the characteristic function of the identity element in G. So,

$$m = |G|^2 \sum_{\chi\in Irr(G)} \frac{\chi(g_1)\chi(g_2)\chi(g_3)}{\chi(1)}$$

Now the number of triples $(g_1, g_2, g_3) \in C_1 \times C_2 \times C_3$ with $g_1 g_2 g_3 = 1$ is

$$n = \frac{m}{|\mathcal{C}_G(g_1)||\mathcal{C}_G(g_3)||\mathcal{C}_G(g_3)|}$$

where $\mathcal{C}_G$ denotes the centraliser and g_is are elements from C_is. Substituting $|\mathcal{C}_G| = |G|/c_i$ for each i, we obtain the desired result. □

Let us consider an example to illustrate the use of the above formula. Consider the Dihedral group $D_n = \langle r, s | r_n = s^2 = 1, srs = r^{-1} \rangle$. We only consider the case when n is odd. Consider the classes C_1, C_2, C_3 containing the elements r, sr, s respectively. Clearly these three elements generate the group D_n and their product is equal to one. The orders of the classes are $c_1 = 2$, $c_2 = c_3 = n$. Now using the character table for D_n, it can be easily verified that

$$\frac{c_1 c_2 c_3}{|D_n|} \sum_{i=1}^{s} \frac{\chi_i(C_1)\chi_i(C_2)\chi_i(C_3)}{\chi_i(1)} = 2n = |D_n|$$

Chapter 5

Descent and the Rigidity Criterion

In the last chapter, we saw that Riemann's Existence Theorem ensures the the Galois realisation of every finite group over the field $\mathbb{C}(x)$. Our goal now is to get a criterion for Galois realisation of groups over $\mathbb{Q}$. This goal is achieved by the Rational Rigidity Criterion.

This chapter is based on the rigidity theory developed in [10] with some gaps in the proofs filled and new examples have been added to illustrate the use of the rigidity criterion.

5.1 Descent

In this section k is an algebraic closed subfield of the complex numbers, $L/k(x)$ a finite Galois extension of degree n and $G = Gal(L/k(x)$. Let κ be a subfield of k.

Definition 5.1.1. *An extension K/κ is called regular if the intersection of K with $k = \bar{\kappa}$ is κ.*

Definition 5.1.2. *We say $L/k(x)$ is defined over κ if there exists a subfield L_κ of L, Galois over $\kappa(x)$, regular over κ such that $[L_\kappa : \kappa(x)] = [L : k(x)] = n$.*

Lemma 5.1.1. *Let L be defined over κ. Then*
1. For a primitive element θ of $L_\kappa/\kappa(x)$, $L = k(x)(\theta)$. In fact L is now defined over every field κ' between κ and k, with $L_{\kappa'} = \kappa'(x)(\theta)$
2. $Gal(L/k(x)) \cong Gal(L_\kappa/\kappa(x))$

3. If G has a trivial center or κ is algebraically closed, then L_κ is the unique degree n Galois extension of $\kappa(x)$ contained inside L, regular over κ.
4. If k is algebraically closed then, $L/k(x)$ and $L_\kappa/\kappa(x)$ have the same ramification type.

Proof. 1. Let $F(y)$ be the irreducible polynomial of θ over $\kappa(x)$. F remains irreducible over κ' since the extension is regular over κ. Hence $L_{\kappa'} = \kappa'(x)(\theta)$ has degree n over $\kappa'(x)$ and is regular over κ'. It is also Galois over $\kappa'(x)$ since all the roots of F are contained in $L_\kappa \subset L_{\kappa'}$. Also taking $\kappa' = k$, we have $L = k(x)(\theta)$.
2. That the restriction map from G to $Gal(L_\kappa/\kappa(x))$ is injective follow from above. But since the order of both groups is n, the map is In fact bijective, hence an isomorphism.
3. Let $\widetilde{L}_\kappa$ be another subfield of L satisfying Definition 5.1.2. Consider the subfield K of L generated by $\widetilde{L}_\kappa$ and L_κ. As both of them are Galois over $\kappa(x)$, K is also Galois over $\kappa(x)$. Let κ' be the algebraic closure of κ in K. Then κ' and thus $\kappa'(x)$ are invariant under $\mathrm{Gal}(K/\kappa(x))$, so $\kappa'(x)$ is Galois over $\kappa(x)$. Let θ be a primitive element for $L_\kappa/\kappa(x)$. Then, $L_\kappa \subseteq K \Rightarrow |K : \kappa(x)| \geq |\kappa'(x)(\theta) : \kappa'(x)| = n$. Let γ be a primitive element for $K/\kappa'(x)$. Due to regularity, the minimal polynomial for γ remains irreducible over $k(x)$. Therefore $|K : \kappa'(x)| \leq n = |L/k(x)|$. Therefore $|K/\kappa'(x)| = n$. That is $K = \kappa'(x)(\theta)$. If κ is algebraically closed then $\kappa' = \kappa$. So $K = \kappa'(x)(\theta) = \kappa(x)(\theta) = L_\kappa$ by definition of θ.
Now assume G has a trivial center. Since L_κ is regular over κ, $\kappa'(x) \cap L_\kappa = \kappa(x)$. Also, $L_\kappa and \kappa'(x)$ generate K. So from Galois correspondence, $Gal(K/\kappa(x))$ is the direct product of $Gal(K/L_\kappa)$ and $G' = Gal(K/\kappa'(x))$. The same is true if replace L_κ by $\widetilde{L}_\kappa$. Since G has trivial center and $G' \cong G$, G' also has trivial center. This implies that $Gal(K/L_\kappa) = Gal(K/\widetilde{L}_\kappa) =$ centraliser of G' in $Gal(K/\kappa(x))$. By Galois correspondence $L_\kappa = \widetilde{L}_\kappa$.
4. Let θ be as in 1, $p \in \kappa \cup \{\infty\}$, and $v : L \to \Delta$ an extension of $v_p : k(x) \to k(t)$, where Δ is a finite Galois extension of $\Lambda = k((t))$(from Lemma 4.1.4). Let $\theta' = v(\theta)$. Then $v(\kappa(x)) = \kappa(t)$, hence $v(L_\kappa) = \kappa(t)(\theta')$. Hence the restriction of v gives an embedding $\tilde{v}$ of L_κ into $\Delta_\kappa := \kappa((t))(\theta')$. We can see that the restriction of the distinguished generator of $Gal(\Delta/\Lambda)$ gives us the distinguished generator of $Gal(\Delta_\kappa/\kappa((t)))$. This means that $g_{\tilde{v}}$ is the restriction of g_v. Therefore the restriction isomorphism from G to $\widetilde{G}$ maps the the classes of p, C_p in G to the classes of p, $\widetilde{C}_p$ in $\widetilde{G}$. The branch points of $L/k(x)$ and $L_\kappa/\kappa(x)$ are same. Hence the extensions have the same ramification type. □

5.1.1 Descent from the algebraic closure

Let α be an automorphism of k. This extends to an automorphism of $k(x)$ by fixing x. Consider two finite Galois extensions L and L' of $k(x)$. An **α-isomorphism** $\lambda\colon L \to L'$ is an isomorphism which when restricted to $k(x)$ is equal to α. Such λ induces a group isomorphism λ^* via conjugation by λ.

Lemma 5.1.2. *Let $L/k(x)$ be a finite Galois extension and α and automorphism of k. Then there exists a finite Galois extension $L'/k(x)$ and an α-isomorphism from L to L'. Also if L is defined over κ, and α is identity on κ, then we can take $L' = L$ and $\lambda^* = id$.*

Proof. We can write $L = k(x)[y]/(F)$ for some irreducible polynomial F. Now we extend α to $k(x)[y]$ by fixing x and y. Denote this map by f mapping to f^α. Take $L' = k(x)[y]/(F^\alpha)$. Then the map $f \mapsto f^\alpha$ defines an isomorphism λ from L to L'. Clearly L' is a finite Galois extension of $k(x)$ and λ is an α-isomorphism.
Now if L is defined over κ, by lemma 5.1.1 (1.), we can choose F such that $L_\kappa = \kappa(x)[y]/(F)$. Also if restriction of α on κ is identity, then $F^\alpha = F$, and therefore $L' = L$. Let θ be the primitive element as in the previous lemma. Since λ fixes all elements of L_κ, $\lambda^*(g)(\theta) = g(\theta)$ for every $g \in G$. Hence $\lambda^* = id$. □

We are interested in the descent from the algebraic closure, so from now onwards, we take $k = \tilde{\kappa}$, the algebraic closure of κ in the complex numbers field. For this case we have the following result.

Proposition 5.1.3. *Let $L/k(x)$ be a finite Galois extension whose Galois group G has trivial center. Then L is defined over κ iff for each α in $Gal(k/\kappa)$, there is an α-automorphism λ, of L such that λ^* is identity.*

Proof. The only if part follows from the previous lemma. So assume that for every $\alpha \in Gal(k/\kappa)$, there is an α-automorphism λ, of L with $\lambda^* = id$. It is easy to see that L is defined over some finite galois extension κ_1 of κ. So let $L_1 = L_{\kappa_1}$ and α_1 be an arbitrary element of $Gal(\kappa_1/\kappa)$ and extend it to α, an element of $G(k/\kappa$. Choose λ from the hypothesis. Then $\lambda(L_1) = L_1$ by lemma 5.1.1 (3.). The restriction λ_1 of λ to L_1 is an α_1-automorphism. Since $Gal(\kappa_1/\kappa) \cong Gal(\kappa_1(x)/\kappa(x))$, we can extend λ_1 to an element of $Aut(L_1/\kappa(x))$. This implies that L_1 is Galois over $\kappa(x)$. Since λ^* is identity, the restriction λ_1 is in the centraliser

C of $G_1 = Gal(L_1/\kappa_1(x))$ in $H = Gal(L_1/\kappa(x))$. Since α_1 was chosen arbitrarily, the natural map from C to $G(\kappa_1(x)/\kappa(x)) \cong H/G_1$ is surjective. This implies that $H = CG_1$. $C \cap G_1$ is trivial since it lies in the center of G_1, which is trivial by the hypothesis. Therefore H is a direct product of C and G_1. Now take L_κ as the fixed field of C in L_1, which is Galois over $\kappa(x)$ with the Galois group isomorphic to $H/C \cong G_1 \cong G$. Also since $\kappa_1(x)$ is the fixed field of G_1, we have $L_\kappa \cap \kappa_1(x) = \kappa(x)$. $L\kappa$ is regular over κ since $L_\kappa \subset L_1$ and L_1 is regular over κ_1. So we have shown that L is defined over κ. □

5.2 The Rational Rigidity Criterion

We saw that rigidity ensured the Galois realisation of finite groups over $\mathbb{C}(x)$. To do the same for the field of rational numbers, we shall need some additional conditions. To go in this direction, we first make the following definition of rationality.

Definition 5.2.1. *Let $\mathcal{T} = [G, P, \{C_p\}_{p\in P}]$ be a ramification type and n be the size of G. We say that $\mathcal{T}$ is κ-rational if $P \subset \tilde{\kappa} \cup \{\infty\}$ and for every $p \in P$ and $\alpha \in Gal(\bar{\kappa}/\kappa)$, $\alpha(p) \in P$ and $C_{\alpha(p)} = C_p^m$ for some integer m satisfying $\alpha^{-1}(\zeta_n) = \zeta_n^m$.*

In the case of $\kappa = \mathbb{Q}$, this is simplified to just demanding that the conjugacy classes are rational, i.e. $C_p^m = C_p$ for every integer coprime to n.

We saw earlier the condition of κ-rational type is necessary for L to be defined over κ. It turns out that it is also sufficient if the ramification type is rigid.

Theorem 5.2.1. *Let $L/k(x)$ be a finite Galois extension and $\bar{\kappa} = k$. If L has a rigid and κ-rational ramification type then L is defined over κ.*

Proof. Since $L/k(x)$ has a rigid type, $G = Gal(L/k(x))$ has a trivial center. Now we want to apply Proposition 5.1.3 to L, so let α be an element of $Gal(k/\kappa)$. There exists a finite Galois extension $L'/k(x)$ and an α-isomorphism λ from L to L'. Let G' be its Galois group, and C_p, C'_p be corresponding conjugacy classed of p in G and G' respectively. By the hypothesis, $q = \alpha(p)$ is in P. Now by Prop. 4.1.5 and κ-rationality, we have $\lambda^*(C_q) = \lambda^*(C_p) = C'_q$, with m as in the Definition 5.2.1. So L' has the same ramification type as L. It follows easily from the definition that extensions of $k(x)$ with the same rigid

type must be isomorphic. Hence we have an isomorphism μ from L' to L which also respects the conjugacy classes from the ramification type. Define $\chi = \mu\lambda$, then χ is an α-isomorphism. Also, $\chi^*(C_q) = \mu^*(\lambda^*(C_q)) = \mu^*(C'_q) = C_q$. Since the type is rigid and χ^* fixes all conjugacy classes, there exists $g \in G$ such that χ^* acts via conjugation by g. Now take $\phi = g^{-1}\chi$. Then $\phi^* = id$. So by Prop. 5.1.3. L is defined over κ. □

It should be noted that ramification types are κ-rational if and only if the conjugacy classed C_p are rational.

The following theorem is the most important step in our quest to find a rigidity criterion for the rational numbers.

Theorem 5.2.2. *Let $\mathcal{T} = [G, P, \{C_p\}_{p\in P}]$ be a rigid and κ-rational type. Then there exists a unique finite Galois extension $L/\mathbb{C}(x)$ of type $\mathcal{T}$, defined over a purely transcendental extension $\kappa(t_1, ..., t_r)$ of κ and G occurs as a Galois group of a purely transcendental extension of κ, regular over κ.*

. *Proof.* Since $\mathcal{T}$ is rigid, there is a unique finite Galois extension of type $\mathcal{T}$, $L/\mathbb{C}(x)$. L is now defined over some finitely generated extension of κ, $\kappa_1 = \kappa(x_1, x_2, ..., x_s)$. Select a subset $t_1, ..., t_r$ from the x_is which is maximal with respect to being algebraically independent. Then κ_1 is a finite extension of $\kappa_0 = \kappa(t_1, ..., t_r)$. Let k be the algebraic closure of κ_0. Then by lemma 5.1.1, L is defined over k and $L/k(x)$ has ramification type $\mathcal{T}$. Since every α in $Gal(k/\kappa_0)$ restricts to an element of $Gal(\bar{\kappa}/\kappa)$ and $\mathcal{T}$ is κ-rational, it is also κ_0-rational. Hence by Theorem 5.2.1, L_κ is defined over κ_0 and consequently L is also defined over κ_0. Lemma 5.1.1. now implies that $G = Gal(L/\mathbb{C}(x) \cong Gal(L_{\kappa_0}/\kappa_0(x))$. The last group is equal to $Gal(L_{\kappa_0}/\kappa(t_1, ..., t_r, x)$. Since L_{κ_0} is regular over κ_0 and κ_0 is regular over κ, it follows that L_{κ_0} is regular over κ. This completes the proof. □

From the above theorem, the following rigidity criteria immediately follow.

Theorem 5.2.3. ***Rational Rigidity Criterion***
Let G be a finite group with a rigid and rational tuple of conjugacy classes $(C_1, ..., C_r)$. Then G occurs regularly over $\mathbb{Q}$.

Theorem 5.2.4. *Let G be a finite group with rigid tuple of conjugacy classes $(C_1, ..., C_r)$. Then G is a Galois group over the field $\mathbb{Q}^{ab}$.*

Proof. In the case of $\mathbb{Q}^{ab}$, rationality is trivial since every α in $Gal(\bar{\mathbb{Q}}/\mathbb{Q}^{ab})$ fixes the roots of unity, so we can take $m = 1$ and so $(C_{\alpha(p)})^m = C_p$. □

Dihedral Group: Recall the example of Dihedral group D_n we did in the last chapter. Again assume that n is odd. Clearly since n is odd, D_n has trivial center. We have generators r, sr and s in the classes C_1, C_2 and C_3 resp. The number of triples $(g_1, g_2, g_3) \in C_1 \times C_2 \times C_3$ with $g_1 g_2 g_3 = 1$ was calculated and found to be equal to the size of the group. Together this implies that D_n has a rigid tuple of conjugacy classes. So D_n is realisable over $\mathbb{Q}^{ab}$ when n is odd. However the class of r is not rational, so the rational rigidity criterion cannot be applied here.

Chapter 6

Galois Realisations of Finite Simple Groups

In this chapter we will apply the rigidity criteria proved in the last chapter to obtain Galois realisations of various finite simple groups including the Projective Linear Groups, various Sporadic groups and finally the Monster Group,s over the field of rational numbers.

This chapter is primarily based on the results in [6] and [10]. Some details have been added for easier comprehension of the proofs.
We shall need the following simple lemma before proceeding. Its proof follows directly from the definition of rigidity.

Lemma 6.0.1. *Let G be a finite group with a tuple of conjugacy classes, (C_1, C_2, C_3) and generators g_1, g_2, g_3 in C_1, C_2, C_3 resp. such that $g_1g_2g_3 = 1$. Suppose G has a trivial center and for every $g_2' \in C_2$ satisfying $(g_1g_2')^{-1} \in C_3$ and $G =< g_1, g_2' >$, there exists $g \in G$, which conjugates g_1 into g_1 and g_2 into g_2', then the tuple of conjugacy classes (C_1, C_2, C_3) is rigid.*

6.1 The Projective Linear Group $PSL_2(q)$

We will first need to modify the rigidity criterion slightly to make it useful for groups with non-trivial centers. Let G be a finite group with a tuple of conjugacy classes, $(C_1, C_2, ..., C_r)$. We say this tuple is **quasi-rigid** if it is weakly rigid and any automorphism of G that fixes

each C_i is an inner automorphism. For quasi-rigid tuples we have the following result. The proof is essentially the same as the rigid case.

Theorem 6.1.1. *Let G be a finite group with a quasi-rigid and κ-rational tuple of conjugacy classes, $(C_1, C_2, ..., C_r)$. Then $G/Z(G)$ occurs regularly over κ where $Z(G)$ denotes the center of G.*

We now try to realise the $PSL_2(q)$ group over the fields $\mathbb{Q}$ and $\mathbb{Q}^{ab}$. We only consider the case when q is a power of an odd prime.

Lemma 6.1.2. *Let $U_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U \in SL_2(q)$ of trace 2, not upper triangular. Then $\exists A \in SL_2(q)$ such that A commutes with (U_1 and conjugates U into a matrix of the form $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$*

Proof. Consider $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(q)$ not upper triangular, so $c \neq 0$. Let $A = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, which clearly centralises U_1. Then

$$AUA^{-1} = \begin{pmatrix} a+mc & * \\ c & * \end{pmatrix}$$

Taking $m = c^{-1}(1-a)$, we get $AUA^{-1} = \begin{pmatrix} 1 & * \\ c & * \end{pmatrix}$. But, $\text{trace}(U) = 2 \Rightarrow \text{trace}\,(AUA^{-1}) = 2$ and $AUA^{-1} \in SL_2(q) \Rightarrow \det(AUA^{-1}) = 1$. This implies

$$AUA^{-1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

Lemma 6.1.3. *There are exactly two conjugacy classes of non-identity elements of $SL_2(q)$ with trace 2, say C_1, C_2, where C_1 is the class containing U_1.*

Proof. The non-identity elements in $SL_2(q)$ of trace 2 are of the form $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}$ where $u, v \neq 0$ in $\mathbb{F}_q$. The claim is that these elements belong to C_1 if and only if u or $-v$ are

square in $\mathbb{F}_q$, respectively. Consider $U \in SL_2(q)$ of trace 2. If U is upper triangular, then it is of the form $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$. If U is not upper triangular then by the previous lemma, it is conjugate to some $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$. We also see that

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -v \\ 0 & 1 \end{pmatrix}$$

This means that U is conjugate to a matrix of the form $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ in each case. Now we need to see when a matrix of this form is conjugate to U_1. Suppose $B \in SL_2(q)$ is such that

$$BU_1B^{-1} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

U_1 has eigenvalue 1 with corresponding eigenspace $W = span\{(1,0)\}$. Since B fixes this W, B must be upper triangular. Since B has determinant equal to 1, this means that B is of the form $\begin{pmatrix} w & * \\ 0 & w^{-1} \end{pmatrix}$. Now

$$\begin{pmatrix} w & * \\ 0 & w^{-1} \end{pmatrix} U_1 \begin{pmatrix} w & * \\ 0 & w^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & w^2 \\ 0 & 1 \end{pmatrix}$$

This completes the proof. □

We will need the following result by Dickson for applying the quasi-rigidity criterion to $PSL_2(q)$.

Lemma 6.1.4. *Let q be a power of the odd prime p and $\mathbb{F}_q = \mathbb{F}_p(c)$ for some $c \neq 0$. Then the following matrices generate $SL_2(q)$ except possibly when $q = 9$.*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

Lemma 6.1.5. *Let q be as in the previous lemma. Let $\mathbb{F}_q = \mathbb{F}_p(\tau)$ with $\tau \neq 2$. Let $C(\tau)$ be the class of $SL_2(q)$ containing $\sigma_3 := \begin{pmatrix} \tau - 1 & 1 \\ \tau - 2 & 1 \end{pmatrix}^{-1}$. Then we have the following two cases*

1. *If $2-\tau$ is nonsquare in $\mathbb{F}_q$ then $(C_1, C_2, C(\tau))$ is a quasi-rigid tuple in $SL_2(q)$ or*
2. *If $2-\tau$ is a square in $\mathbb{F}_q$ then $(C_1, C_1, C(\tau))$ is quasi-rigid tuple in $SL_2(q)$.*

Proof. Let $g_1 = U_1, g_2 = \begin{pmatrix} 1 & 0 \\ \tau-2 & 1 \end{pmatrix}$. By Lemma 6.1.3, $g_2 \in C_2$ if $2-\tau$ is nonsquare in $\mathbb{F}_q$ C_2, otherwise $g_2 \in C_1$. We can easily check that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \tau-2 & 1 \end{pmatrix} = \begin{pmatrix} \tau-1 & 1 \\ \tau-2 & 1 \end{pmatrix}$$

With this combined with Dickson's result, we see that there exist generators g_1, g_2, g_3 of the group $G = SL_2(q)$, such that $g_i \in C_i$ for each i and their product is equal to 1. By modifying Lemma 6.0.1 to include quasi-rigidity, it is enough to show that if $2-\tau$ is nonsquare(resp. square) in $\mathbb{F}_q$, all $g_2' \in C_2$(resp.)C_1 with $g_1 g_2'$ of trace τ and $\langle g_1, g_2' \rangle = G$ are conjugate under the centraliser of g_1 in G. Now g_2' cannot be upper triangular since g_1 is upper triangular and g_1, g_2' generate G. Then by Lemma 6.1.2, g_2' is conjugate to $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ under the centraliser of g_1 in G. Also it easily verified that $c = \tau - 2$ by noting that $g_1 \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ has trace τ. This finishes the proof. □

Theorem 6.1.6. *$PSL_2(q)$ occurs regularly over $\mathbb{Q}^{ab}$ for $q = p^n$ for every odd prime p and positive integer n.*

Proof. For $q \neq 9$, we have quasi-rigid and $\mathbb{Q}^{ab}$-rational tuple of conjugacy classes in the group $G = PSL_2(q)$ as seen in the above lemma. Noting that $Z(G) = \{\pm 1\}$, Theorem 6.1.1 proves the required result. For $q = 9$, we have $PSL_2(q) \cong A_6$ which as we have already seen occurs regularly over $\mathbb{Q}^{ab}$. □

Theorem 6.1.7. *$PSL_2(p)$ occurs regularly over $\mathbb{Q}$ for every prime p such that $p \not\equiv \pm 1$ mod 24.*

Proof. We only need to consider $p \geq 5$, since $PSL_2(3) \cong S_3$ and $PSL_2(3) \cong A_4$. Let $\tau \neq 1 \in \mathbb{F}_p$ such that $2-\tau$ is a non square. Then we have a quasi-rigid tuple $(C_1, C_2, C(\tau))$ in $G = SL_2(p)$. Since for any $m \not\equiv 0 \bmod (p)$, (C_1^m, C_2^m) is a permutation of (C_1, C_2), $(C_1, C_2, C(\tau))$ is $\mathbb{Q}$-rational iff $C(\tau)^m = C(\tau)$ for every such m.

Now if 2(resp. 3) is non-square in $\mathbb{F}_p$, then take $\tau = 0$(resp. $\tau = -1$). Then $C(\tau)$ has elements of order 4(resp. 3) which are conjugates to their inverses. Hence $C(\tau)$ is a rational class. But 2 or 3 being non-square in $\mathbb{F}_p$ is equivalent to $p \not\equiv \pm 1 \bmod 24$ (Using quadratic reciprocity). □

6.2 Sporadic Groups

In this section we show that various sporadic groups have Galois realisations over $\mathbb{Q}$. For verifying rigidity, we shall use an Atlas by Conway[2]. The class names are taken from the same Atlas. We first prove the following lemma for subgroups of index 2.

Lemma 6.2.1. *Let G be a finite group with rationally rigid tuple of conjugacy classes (C_1, C_2, C_3). Let H be an index 2 subgroup of G. Then H occurs regularly over $\mathbb{Q}$.*

Proof. Take any distinct points $p_1, p_2, p_3 \in \mathbb{Q}$. From these points and the conjugacy classes obove, we obtain a $\mathbb{Q}$-rational rigid ramification type $\mathcal{T}$. Then by Theorem 5.2.2, there exists a purely transcendental extension $\kappa_0 = \mathbb{Q}(t_1, t_2, ..., t_r)$ inside $\mathbb{C}$ and a finite Galois extension $L/\mathbb{C}(x)$ of type $\mathcal{T}$ defined over κ_0. The we have $Gal(L_{\kappa_0}/\kappa_0(x)) \cong G$. By Galois correspondence, H corresponds to a quadratic extension M_0 of $\kappa_0(x)$ contained in L_{κ_0}. Then we may write $M_0 = \kappa_0(x)(\sqrt{f})$, with f being a polynomial with all irreducible factors appearing exactly once. Now let $M = \mathbb{C}(x)(\sqrt{f})$, which is a degree 2 extension of $\mathbb{C}(x)$. From the proof of Lemma 4.1.4, we see that the branch points of $M/\mathbb{C}(x)$ are among the same branch points of $L/\mathbb{C}(x)$ which are p_1, p_2 and p_3. Since the number of branch points of quadratic extension must be even[10] and at least 2, M has exactly two branch points, p_1, p_2 without any loss of generality. Hence $f = a(x - p_1)(x - p_2)$ with $a \in \kappa_0$. So we have $M_0 = \kappa_0(x)(\sqrt{f}) = \kappa_0(x)(\sqrt{f}/(x - p_2)) = \kappa_0(x)(z)$ with $z^2 = \frac{a(x-p_1)}{x-p_2}$. Since this is a linear fractional in x, we can solve for x as a rational function of z^2. Hence $M_0 = \kappa_0(z)$. Hence $H = Gal(L_{\kappa_0}/M_0) = Gal(L_{\kappa_0}/\kappa_0(z))$, hence H occurs regularly over κ_0. By Hilbert's Irreducibilty theorem H, occurs regularly over $\mathbb{Q}$. □

6.2.1 Mathieu Groups

Mathieu Groups are a family of sporadic groups due to Mathieu, consisting of five groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24}. The groups M_{11}, M_{12} and M_{22} are known to be realisable over the field of rational numbers [6]. Below we use the rigidity criterion to prove this for the groups M_{12} and M_{22}.

Proposition 6.2.2. *(2C, 3A, 12A) is a rationally rigid tuple in $Aut(M_{12})$.*

Proof. Using the character table for $G = Aut(M_{12})$ in [2] and Lemma 4.2.2, we find that the number of triples $(g_1, g_2, g_3) \in 2C \times 3A \times 12A$ with $g_1g_2g_3 = 1$ is equal to the size of the group [See Appendix]. So now to show rigidity, it suffices to prove that any triple $(g_1, g_2, g_3) \in 2C \times 3A \times 12A$ with $g_1g_2g_3 = 1$ generates $Aut(M_{12})$. Assume to the contrary that we have such a tuple generating a proper subgroup H. Now H must be contained in a proper subgroup of G. Again using the information in the Atlas, we see that H must contain elements from 3A and 6A. Using the permutation characters of the maximal subgroups, we see that the only maximal subgroup containing these classes is $M = S_4 \times S_3$. Hence $H \subseteq M$. Considering the fact that $g_1g_2g_3 = 1$, we must have $\mathbf{C} \cap M = ((2) \times (1), (3) \times (3), (4) \times (3))$, where $(2), (3), (4)$ denote the classes containing 2-cycles, 3-cycles and 4-cycles respectively. The class $(1) \times (3)$ has centraliser of order 72 in M. Looking at the orders of centralisers of classes in G, we see that this class must fuse into $3B$. Also clearly the class $(3) \times (3)$ fuses into $3A$. Now the remaining class in M $(3) \times (1)$, with order 3 elements can fuse into $3A$ or $3B$. Depending on that the permutation character χ of M in G, takes either the values $\chi(3A) = 12$, $\chi(3B) = 5$ or $\chi(3A) = 18$, $\chi(3B) = 1$. In either case we have a contradiction to the fact that $\chi(3A) \equiv \chi(3B)(mod\ 3)$. Hence the classes 2C, 3A and 12A form a rigid tuple in G. The rationality is easily checked using the second rows in the table given in the atlas. □

Proposition 6.2.3. *(2B, 4C, 11A) is a rationally rigid tuple in $Aut(M_{22})$.*

Proof. We do the same calculation as above for $G = Aut(M_{22})$ and see the same conclusion as before [See Appendix]. Again let H be as in the previous proposition. Since H contains an element of order 11, the maximal subgroup M must have order divisible by 11. So from the atlas, we see that $M = PGL_2(11) = PSL_2(11) : 2$. Again looking at the permutation character corresponding to M. we see that M can't contain elements of the

class $2B$. Hence H must not be contained in M. Therefore the classes 2B, 4C, 11A form a rigid tuple in G. Just as before the rationality is easily verified using the atlas. This finishes the proof. □

Theorem 6.2.4. *The groups M_{12} and M_{22} are realisable over the field of rational numbers.*

Proof. From the atlas we see that for the groups $G = M_{12}$ and M_{22}, $Aut(G) = G.2$ From the above two propositions we have rationally rigid tuples in $Aut(G)$ and G is an index 2 subgroup of $Aut(G)$ in each case. Now from Lemma 6.2.1, it follows that G is realisable over $\mathbb{Q}$. □

6.2.2 Leech Lattice Groups

The sporadic groups, Janko group J_2 and Suzuki group Suz can be described as stabilisers of a set of vectors in the lattice known as the Leech Lattice. We show using the rigidity criterion that these two groups occur as Galois groups over $\mathbb{Q}$.

Proposition 6.2.5. *(i.) (3A, 8C, 14A) is a rationally rigid tuple in $Aut(J_2)$.*
(ii.) (2C, 8D, 13A) is a rationally rigid tuple in $Aut(Suz)$.

Proof. Employing the same strategy as before, we verify the calculations [See Appendix] and set H as the subgroup as before. In the case (i.), the maximal subgroup M must have order divisible by 7, which means M is among the subgroups $U_3 : 2 \cong G_2(2)$ and $PGL_2(7) \times 2$. But we can check from the character table that $G_2(2)$ has no element of order 14, so M is not $G_2(2)$. So $H \subseteq PGL_2(7) \times 2$. Consider the natural map from H to $PGL_2(7) \times 2/L_2(7) \cong Z_2 \times Z_2$. The map has kernel equal to $H \cap L_2(7)$. Thus $H/(H \cap L_2)7))$ is a subgroup of $Z_2 \times Z_2$. Since H is generated by a triplet of elements from $(3A, 8C, 14A)$, $H/(H \cap L_2)7))$ is isomorphic to Z_2. Now by third isomorphism theorem for groups, we have $H.L_2(7)/L_2(7) \cong Z_2$. This implies that $H \subseteq PGL_2(7)$ or $H \subseteq L_2(7) \times 2$, but from the atlas we see that the first does not contain elements of order 14, while $L_2(7)$ has no elements of order 8. Hence H is not a proper subgroup of $Aut(J_2)$.

In the case (ii.), the possible maximal subgroups with orders divisible by 13 are $G_2(4) : 2$ and $L_2(25) : 2$. The latter must be $L_2(25) : 2_2$ since $L_2(25).2_3$ is non-split and $L_2(25) : 2_1$ has order two elements which centralise an element of order 13 but the centralisers of 13

elements have size 13, implying $L_2(25) : 2_1$ is not contained in $Aut(Suz)$. But as can be seen from the atlas, $L_2(25) : 2_2$ has no element of order 8. So $H \subseteq G_2(4) : 2$. Looking at the permutation character of $G_2(4)$ in $Aut(Suz)$ which vanishes on the class 8D, we see that 8D is not contained in $G_2(4)$. So the rigidity follows. In both the cases rationality is verified from the atlas easily. □

Theorem 6.2.6. *The groups J_2 and Suz are realisable over the field of rational numbers.*

From the above proposition, the automorphism groups of both these groups posses rationally rigid tuples of conjugacy classes. Moreover from the atlas, it is easily seen that the groups lie as index 2 subgroups inside their respective automorphism groups. Hence using Lemma 6.2.1, it follows that J_2 and Suz are realisable over the field of rational numbers.

6.2.3 The Monster Group M

Monster Group is the largest sporadic group. Its size is $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$. The biggest result that came from Thompson's paper in which he developed the rigidity criterion is the Galois realisation of the Monster Group M over $\mathbb{Q}$ [8]. This results gives an indication of the power of the rigidity method.

Lemma 6.2.7. *Suppose a finite group G is generated by three elements g_1, g_2 and g_3 whose orders p, q and r respectively, are pairwise coprime. Also let $g_1 g_2 g_3 = 1$. Then G is perfect i.e. $G = [G, G]$. Moreover $G = \langle g_1 \rangle^G$*

Proof. Consider the images of the generators in the quotient $G/[G, G]$. Now the order $o(\bar{g_1})$ divides $o(g_1) = p$. Also since $g_1 g_2 g_3 = 1$, $o(\bar{g_1})$ also divides $o(g_2 g_3) = qr$. Hence g_1 must belong to $[G, G]$ as the order of $o(\bar{g_1})$ is equal to one. Similarly it can be seen that g_2 and g_3 also belong to $[G, G]$. Therefore G is generated by elements from $[G, G]$ and $G = [G, G]$. Now let $H = \langle g_1 \rangle^G$ and $\bar{g_2}, \bar{g_3}$ be the images in the quotient G/H. Then ${\bar{g_2}}^q = {\bar{g_3}}^r = \bar{g_2}\bar{g_3} = 1$. Since q and r are coprime, this means that $\bar{g_2}, \bar{g_3} = 1$. Hence $H = G$. □

Proposition 6.2.8. *(2A, 3B, 29A) is a rationally rigid tuple in the Monster Group M.*

Proof. We follow the same method as before. Since the group M is simple , its center is trivial. Therefore to show rigidity, we just choose one element each from the classes 2A,

3B, 29A and show that they generate M. Suppose they generate proper subgroup H, which must now lie in a maximal subgroup. But not all maximal subgroups of M are known. We note that orders of the generators are pairwise coprime. So by the above lemma, H is a perfect group. Now let L be a maximal normal subgroup of H. The previous lemma now implies that 29 divides the order of the quotient $S = H/L$. Now using the classification of finite simple groups, S is isomorphic to one of the groups among $L_2(29), L_2(59), Rv, Fi'_{24}$ and M. The elements in the class $2A$ are 3, 4, 5, 6-transpositions, so order of product of any two elements in $2A$ can be at most 6. But the order 2 element classes in the groups $L_2(29), L_2(59)$ and Rv are not 3, 4, 5, 6-transpositions.
But H cannot be isomorphic to Fi'_{24}. This can be seen by looking at the character table and noting that the character 196883_a of M does not restrict to Fi'_{24}. So if $S \cong Fi'_{24}$, then $L \neq 1$. It can be checked that orders of 2, 3, 5 and 7 modulo 29 are 28, 28, 14 and 7 respectively and that for every elementary abelian 2-group E inside M has order less than or equal to 2^{24}. Also note from the atlas that the centraliser of the elements of 29A in M has order 3.29. Again using the atlas, all of above implies that $H = 3.Fi'_{24}$ or $H = M$.
Now if $H = 3.Fi'_{24}$, then $H = \mathcal{C}_M(x)$ for $x \in 3A$. Consider any triple $u \in 2A$, $v \in 3B$, $w \in 29A$ with $uvw = 1$. Then we have another triple u, vx, $x^{-1}w$ with product equal to 1. since x commutes with all elements in H, we have o$(vx) = 3$ and $o(x^{-1}w) = 87$. The calculation from Lemma 4.2.2 for the tuples $(2A, 3A, 87A)$ and $(2A, 3B, 87A)$ gives us zero. So vx must belong to the class $3C$. Using the classification of finite simple groups, $\langle v, x\rangle$ must contain at least 2 Suzuki elements, 2 Fischer elements and 2 Thompson elements [11]. $\mathcal{C}_M(vx) \cong 3 \times E$ with E an elementary abelian 2-group. The character 196883_a restricts to $3 \times E$ as $(1 + \omega + \bar{\omega}) \otimes 1_a + (\omega + \bar{\omega}) \otimes 248_a + (1 + \omega + \bar{\omega}) \otimes 4123_a + 1 \otimes 30628_a + 1 \otimes 30875_a + (\omega + \bar{\omega}) \otimes 61256_a$ [11]. From the character table we have $196883_a(3A) = 728$, $196883_a(3B) = 53$ and $196883_a(3C) = -1$. So the class 3A in E fuses to 3A in M, and $3B, 3C$ in E fuse to $3B$ in M. But $196883_a(xz) = -1$ whenever z is in one of the classes 3A, 3B and 3C in E, so $xz \in 3C$ in M . Therefore every elementary abelian subgroup of order 9 in M contains 0 or 6 Thompson elements. This means $H \neq 3.Fi'_{24}$ [11] which implies that H must be the full Monster Group M and the tuple (2A, 3B, 29A) is rigid in M. The rationality is seen easily from the table of M in the atlas. □

Now the above proposition combined with the Rational Rigidity Criterion proves our final result.

Theorem 6.2.9. *The Monster Group M is realisable over the field of rational numbers $\mathbb{Q}$.*

Chapter 7

Conclusion

The primary aim of this project was to understand the Inverse Galois Problem and explore various methods to study the problem. It was seen how the Structure Theorem for Finite Abelian groups made the problem quite trivial for the Finite Abelian groups. The Irreducibility theorem due to Hilbert was a crucial step in making the problem a bit easier to solve. In fact it allowed us to give explicit examples of polynomials with the symmetric and alternating groups as their Galois groups.

With the help of homotopy theory, the ideas of ramification types were introduced by studying the finite Galois coverings of punctured Riemann's sphere. This led us to the crucial topological variant of the Riemann's Existence Theorem. Building up on this, the Galois extensions of the Laurent series fields we examined and the idea of branch points was introduced. These ideas helped in proving the algebraic variant of the Riemann's Existence Theorem which solved the Inverse Galois Problem over the field $\mathbb{C}(x)$.

Introducing the idea of rigid ramification types and rigid tuples of conjugacy classes, we arrived at the powerful method, the Rigidity Criterion, to tackle the Inverse Galois Problem over the rational numbers.

Finally various finite simple groups like the linear groups, Mathieu groups and the largest sporadic group, the Monster group, were realised over the rational numbers using the Rational Rigidity Criterion with the aid of Conway's Atlas [2].

But the problem is still only partially solved. An important step towards solving the Inverse Galois Problem was achieved by Shafarevich who proved that all finite solvable groups are realisable over $\mathbb{Q}$.

In the project, the connections between different areas of Mathematics like Topology, Geometry and Algebra were also observed. This was beautifully demonstrated by studying the Reiemann's Existence Theorem and arriving at an analogous algebriac variant of the theorem.

Appendix A

Codes

The C programs for the verification of rigidity are shown below.

A.1 M_{12}

```
/*Calucations for the group Aut(M12)*/

#include<stdio.h>
#include<math.h>
double rproduct(double r1, double im1, double r2, double im2); /* Product
    of complex numbers Real Part*/
double improduct(double r1, double im1, double r2, double im2); /* Product
     of complex numbers imaginary Part*/
double rdiv(double r1, double im1, double r2, double im2);/* Product of
    complex numbers Real Part*/
double improduct(double r1, double im1, double r2, double im2);/* Product
    of complex numbers Img Part*/
double check(int a , int b, int c, double rchi[21][4], double imchi
    [21][4], double centraliser[4]); /* Function for verifying the formula
    */

double rproduct(double r1, double im1, double r2, double im2)
    {
        double rp;
        rp = r1*r2-im1*im2;
```

```
        return rp;
    }


double improduct(double r1, double im1, double r2, double im2)
{
    double imp;
    imp = r1*im2+r2*im1;
    return imp;
}

 double rdivision(double r1, double im1, double r2, double im2)
{
        double rdiv = r1*r2+im1*im2;
        double mod2 = r2*r2+im2*im2;
        rdiv = rdiv/mod2;
        return rdiv;
}

double idivision(double r1, double im1, double r2, double im2)
{
    double idiv = r2*im1-r1*im2;
    double mod2 = r2*r2+im2*im2;
    idiv = idiv/mod2;
    return idiv;
}

double check(int a , int b, int c, double rchi[21][4], double imchi
   [21][4], double centraliser[4]){
    int i = 0, j = 0, k = 0, l = 0;
    double rflag = 0;
    double rflag1 = 0;
    double imflag = 0;

    for (i = 0; i < 21; i = i+1)
    {
        rflag1= rproduct(rchi[i][a],imchi[i][a], rproduct(rchi[i][b],
   imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b], imchi[i][b
   ], rchi[i][c], imchi[i][c]));
        rflag1 = rflag1/rchi[i][0];
        /*printf("%lf, ", i, rflag1);*/
```

```
53          rflag = rflag+rflag1;
54
55          imflag= imflag + improduct(rchi[i][a], imchi[i][a], rproduct(rchi[
    i][b], imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b],
    imchi[i][b], rchi[i][c], imchi[i][c]));
56          imflag = imflag/rchi[i][0];
57
58          /*printf("cumulative value is %lf\n", rflag);  Verifying Steps if
    needed */
59      }
60
61      double pr = (centraliser[0]*centraliser[0])/(centraliser[a]*
    centraliser[b]*centraliser[c]);
62      printf("Pr is %lf\n", pr);
63      rflag = rflag*pr;
64      return rflag;
65
66  }
67
68
69  int main(){
70      /*Img Parts of the character values on the classes 1A,3A,2C,12A
    respectively */
71      double imchi[21][4];
72      /*Img Parts of the character values on the classes 1A,3A,2C,12A
    respectively */
73      double rchi[21][4] = {{1,1,1,1},
74                  {1,1,-1,-1},
75                  {22,4,0,0},
76                  {32,-4,0,0},
77                  {45,0,5,1},
78                  {45,0,-5,-1},
79                  {54,0,0,0},
80                  {54,0,0,0},
81                  {55,1,5,-1},
82                  {55,1,-5,1},
83                  {110,2,0,0},
84                  {66,3,6,0},
85                  {66,3,-6,0},
86                  {99,0,1,-1},
87                  {99,0,-1,1},
```

```
                {120,3,0,0},
                {120,3,0,0},
                {144,0,4,-1},
                {144,0,-4,1},
                {176,-4,4,1},
                {176,-4,-4,-1}};
    int i, j = 0;
    for(i=0; i < 21; i = i+1)
    {
        for(j=0; j < 4; j = j+1)
        {
            imchi[i][j] = 0;
        }
    }

    double centraliser[4] = {190080,108,240,12}; /*Sizes of centralisers
   of the classes 1A,3A,2C,12A respectively */

    printf("n(%d,%d,%d) is %lf\n", 1, 2, 3, check(1, 2, 3, rchi, imchi,
   centraliser));/* This is the required number from the formula */
}

```

The output is shown below.

```
Pr is 116160.000000
n(1,2,3) is 190080.000000
```

A.2 M_{22}

```
 /*Calucations for the group Aut(M22)*/
#include<stdio.h>
#include<math.h>
double rproduct(double r1, double im1, double r2, double im2); /* Product
   of complex numbers Real Part*/
double improduct(double r1, double im1, double r2, double im2); /* Product
    of complex numbers imaginary Part*/
double rdiv(double r1, double im1, double r2, double im2);/* Product of
   complex numbers Real Part*/
```

```
7  double improduct(double r1, double im1, double r2, double im2);/* Product
       of complex numbers Img Part*/
8  double check(int a , int b, int c, double rchi[21][4], double imchi
       [21][4], double centraliser[4]); /* Function for verifying the formula
       */
9
10 double rproduct(double r1, double im1, double r2, double im2)
11     {
12         double rp;
13         rp = r1*r2-im1*im2;
14         return rp;
15     }
16
17
18 double improduct(double r1, double im1, double r2, double im2)
19 {
20     double imp;
21     imp = r1*im2+r2*im1;
22     return imp;
23 }
24
25  double rdivision(double r1, double im1, double r2, double im2)
26 {
27         double rdiv = r1*r2+im1*im2;
28         double mod2 = r2*r2+im2*im2;
29         rdiv = rdiv/mod2;
30         return rdiv;
31 }
32
33 double idivision(double r1, double im1, double r2, double im2)
34 {
35     double idiv = r2*im1-r1*im2;
36     double mod2 = r2*r2+im2*im2;
37     idiv = idiv/mod2;
38     return idiv;
39 }
40
41 double check(int a , int b, int c, double rchi[21][4], double imchi
       [21][4], double centraliser[4]){
42     int i = 0, j = 0, k = 0, l = 0;
43     double rflag = 0;
```

```
44      double rflag1 = 0;
45      double imflag = 0;
46      for (i = 0; i < 21; i = i+1)
47      {
48          rflag1= rproduct(rchi[i][a],imchi[i][a], rproduct(rchi[i][b],
    imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b], imchi[i][b
    ], rchi[i][c], imchi[i][c]));
49          rflag1 = rflag1/rchi[i][0];
50          /*printf("%lf, ", i, rflag1);*/
51          rflag = rflag+rflag1;
52
53          imflag= imflag + improduct(rchi[i][a], imchi[i][a], rproduct(rchi[
    i][b], imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b],
    imchi[i][b], rchi[i][c], imchi[i][c]));
54          imflag = imflag/rchi[i][0];
55
56          /*printf("cumulative value is %lf\n", rflag);  Verifying Steps if
    needed */
57      }
58
59      double pr = (centraliser[0]*centraliser[0])/(centraliser[a]*
    centraliser[b]*centraliser[c]);
60      printf("Pr is %lf\n", pr);
61      rflag = rflag*pr;
62      return rflag;
63
64  }
65
66
67  int main(){
68      /*Img Parts of the character values on the classes 1A,11A,2B,4C
    respectively */
69      double imchi[21][4];
70      /*Real Parts of the character values on the classes 1A,11A,2B,4C
    respectively */
71      double rchi[21][4] = {{1,1,1,1},
72                  {1,1,-1,-1},
73                  {21,-1,7,-1},
74                  {21,-1,-7,1},
75                  {45,1,3,3},
76                  {45,1,-3,-3},
```

```
                {45,1,3,3},
                {45,1,-3,-3},
                {55,0,13,1},
                {55,0,-13,-1},
                {99,0,15,3},
                {99,0,-15,-3},
                {154,0,14,2},
                {154,0,-14,-2},
                {210,1,14,-2},
                {210,1,-14,2},
                {231,0,7,-1},
                {231,0,-7,1},
                {560,-1,0,0},
                {385,0,21,-3},
                {385,0,-21,3}
                };
    int i, j = 0;
    for(i=0; i < 21; i = i+1)
    {
        for(j=0; j < 4; j = j+1)
        {
            imchi[i][j] = 0;
        }
    }

    double centraliser[4] = {887040,11,2688,96}; /*Sizes of centralisers
   of the classes 1A,11A,2B,4C respectively */

    printf("n(%d,%d,%d) is %lf\n", 1, 2, 3, check(1, 2, 3, rchi, imchi,
   centraliser)); /*This is the required number from the formula*/
}

```

The output is shown below.

```
Pr is 277200.000000
n(1,2,3) is 887040.000000
```

A.3 J_2

```
 /*Calucations for the group Aut(J2)*/
#include<stdio.h>
#include<math.h>
double rproduct(double r1, double im1, double r2, double im2); /* Product
   of complex numbers Real Part*/
double improduct(double r1, double im1, double r2, double im2); /* Product
    of complex numbers imaginary Part*/
double rdiv(double r1, double im1, double r2, double im2);/* Product of
   complex numbers Real Part*/
double improduct(double r1, double im1, double r2, double im2);/* Product
   of complex numbers Img Part*/
double check(int a , int b, int c, double rchi[27][4], double imchi
   [27][4], double centraliser[4]); /* Function for verifying the formula
   */

double rproduct(double r1, double im1, double r2, double im2)
    {
        double rp;
        rp = r1*r2-im1*im2;
        return rp;
    }


double improduct(double r1, double im1, double r2, double im2)
{
    double imp;
    imp = r1*im2+r2*im1;
    return imp;
}

 double rdivision(double r1, double im1, double r2, double im2)
{
        double rdiv = r1*r2+im1*im2;
        double mod2 = r2*r2+im2*im2;
        rdiv = rdiv/mod2;
        return rdiv;
}

double idivision(double r1, double im1, double r2, double im2)
```

```
{
    double idiv = r2*im1-r1*im2;
    double mod2 = r2*r2+im2*im2;
    idiv = idiv/mod2;
    return idiv;
}

double check(int a , int b, int c, double rchi[27][4], double imchi
   [27][4], double centraliser[4]){
    int i = 0, j = 0, k = 0, l = 0;
    double rflag = 0;
    double rflag1 = 0;
    double imflag = 0;
    for (i = 0; i < 27; i = i+1)
    {
        rflag1= rproduct(rchi[i][a],imchi[i][a], rproduct(rchi[i][b],
   imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b], imchi[i][b
   ], rchi[i][c], imchi[i][c]));
        rflag1 = rflag1/rchi[i][0];
        /*printf("%lf, ", i, rflag1);*/
        rflag = rflag+rflag1;

        imflag= imflag + improduct(rchi[i][a], imchi[i][a], rproduct(rchi[
   i][b], imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b],
   imchi[i][b], rchi[i][c], imchi[i][c]));
        imflag = imflag/rchi[i][0];

        /*printf("cumulative value is %lf\n", rflag);  Verifying Steps if
   needed */
    }

    double pr = (centraliser[0]*centraliser[0])/(centraliser[a]*
   centraliser[b]*centraliser[c]);
    printf("Pr is %lf\n", pr);
    rflag = rflag*pr;
    return rflag;

}


int main(){
```

```
68      /*Img Parts of the character values on the classes 1A,3A,8C,14A
    respectively */
69      double imchi[27][4];
70      /*Real Parts of the character values on the classes 1A,3A,8C,14A
    respectively */
71      double rchi[27][4] = {{1,1,1,1},
72                {1,1,-1,-1},
73                {28,10,0,0},
74                {42,6,0,0},
75                {36,9,2,-1},
76                {36,9,-2,1},
77                {63,0,1,0},
78                {63,0,-1,0},
79                {140,14,0,0},
80                {90,9,0,-1},
81                {90,9,0,1},
82                {126,-9,-2,0},
83                {126,-9,2,0},
84                {160,16,0,1},
85                {160,16,0,-1},
86                {175,-5,-1,0},
87                {175,-5,1,0},
88                {378,0,0,0},
89                {448,16,0,0},
90                {225,0,-1,1},
91                {225,0,1,-1},
92                {288,0,0,1},
93                {288,0,0,-1},
94                {300,-15,-2,-1},
95                {300,-15,2,1},
96                {336,-6,0,0},
97                {336,-6,0,0}
98                };
99      int i, j = 0;
100     for(i=0; i < 27; i = i+1)
101     {
102         for(j=0; j < 4; j = j+1)
103         {
104             imchi[i][j] = 0;
105         }
106     }
```

```
107
108     double centraliser[4] = {1209600,2160,32,14};/*Sizes of centralisers
        of the classes 1A,3A,8C,14A respectively */
109
110     printf("n(%d,%d,%d) is %lf\n", 1, 2, 3, check(1, 2, 3, rchi, imchi,
        centraliser));/* This is the require number from the formula */
111 }
112
```

The output is shown below.

```
Pr is 1512000.000000
n(1,2,3) is 1209600.000000
```

A.4 Suz

```
1  /*Calucations for the group Aut(Suz)*/
2 /*Since the number of characters is too large, only the ones which are non
       zero on the classes 8D and 13A are included in the calculations.*/
3 #include<stdio.h>
4 #include<math.h>
5 double rproduct(double r1, double im1, double r2, double im2); /* Product
     of complex numbers Real Part*/
6 double improduct(double r1, double im1, double r2, double im2); /* Product
       of complex numbers imaginary Part*/
7 double rdiv(double r1, double im1, double r2, double im2);/* Product of
     complex numbers Real Part*/
8 double improduct(double r1, double im1, double r2, double im2);/* Product
     of complex numbers Img Part*/
9 double check(int a , int b, int c, double rchi[6][4], double imchi[6][4],
     double centraliser[4]); /* Function for verifying the formula*/
10
11 double rproduct(double r1, double im1, double r2, double im2)
12     {
13         double rp;
14         rp = r1*r2-im1*im2;
15         return rp;
16     }
17
```

```
18
19 double improduct(double r1, double im1, double r2, double im2)
20 {
21     double imp;
22     imp = r1*im2+r2*im1;
23     return imp;
24 }
25
26  double rdivision(double r1, double im1, double r2, double im2)
27 {
28         double rdiv = r1*r2+im1*im2;
29         double mod2 = r2*r2+im2*im2;
30         rdiv = rdiv/mod2;
31         return rdiv;
32 }
33
34 double idivision(double r1, double im1, double r2, double im2)
35 {
36     double idiv = r2*im1-r1*im2;
37     double mod2 = r2*r2+im2*im2;
38     idiv = idiv/mod2;
39     return idiv;
40 }
41
42 double check(int a , int b, int c, double rchi[6][4], double imchi[6][4],
    double centraliser[4]){
43     int i = 0, j = 0, k = 0, l = 0;
44     double rflag = 0;
45     double rflag1 = 0;
46     double imflag = 0;
47
48     for (i = 0; i < 6; i = i+1)
49     {
50         rflag1= rproduct(rchi[i][a],imchi[i][a], rproduct(rchi[i][b],
    imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b], imchi[i][b
    ], rchi[i][c], imchi[i][c]));
51         rflag1 = rflag1/rchi[i][0];
52         /*printf("%lf, ", i, rflag1);*/
53         rflag = rflag+rflag1;
54
55         imflag= imflag + improduct(rchi[i][a], imchi[i][a], rproduct(rchi[
```

```
    i][b], imchi[i][b], rchi[i][c], imchi[i][c]), improduct(rchi[i][b],
    imchi[i][b], rchi[i][c], imchi[i][c]));
56          imflag = imflag/rchi[i][0];
57
58          /*printf("cumulative value is %lf\n", rflag);  Verifying Steps if
    needed */
59      }
60
61      double pr = (centraliser[0]*centraliser[0])/(centraliser[a]*
    centraliser[b]*centraliser[c]);
62      printf("Pr is %lf\n", pr);
63      rflag = rflag*pr;
64      return rflag;
65
66  }
67
68
69  int main(){
70      /*Img Parts of the character values on the classes 1A,2C,8D,13A
    respectively */
71      double imchi[6][4];
72      /*Real Parts of the character values on the classes 1A,2C,8D,13A
    respectively */
73      double rchi[6][4] = {{1,1,1,1},
74                  {1,-1,-1,1},
75                  {5940,90,10,-1},
76                  {5940,-90,-10,-1},
77                  {133056,336,-16,1},
78                  {133056,-336,16,1}
79                  };
80      int i, j = 0;
81      for(i=0; i < 6; i = i+1)
82      {
83          for(j=0; j < 4; j = j+1)
84          {
85              imchi[i][j] = 0;
86          }
87      }
88
89      double centraliser[4] = {896690995200,2419200,46080,13}; /*Sizes of
    centralisers of the classes 1A,2C,8D,13A respectively */
```

```
90
91      printf("n(%d,%d,%d) is %lf\n", 1, 2, 3, check(1, 2, 3, rchi, imchi,
        centraliser)); / *This is the required number from the formula */
92  }
93
94
```

The output is shown below.

```
Pr is 554827553280.000000
n(1,2,3) is 896690995199.999878
```

Bibliography

[1] Gouvêa F. Q., P-adic Numbers: An Introduction, Springer International Publishing, Germany, 1997.

[2] Conway J. H., Curtis R. T., Norton S. P., Parker R. A. and Wilson, R. A., An Atlas of Finite Groups, Oxford Univeristy Press, Oxford, 1985.

[3] Dummit D. S., Foote R. M., Abstract Algebra, 2nd Ed., Wiley India Pvt. Limited, India, 2008.

[4] Hilbert D., *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, Journ. f. reine angew. Math. Bd. (1892). 110, S. 104–129.

[5] Hatcher A., Algebraic Topology, Cambridge University Press, Cambridge, 2002.

[6] Malle G. and Matzat B. H., Inverse Galois Theorey, Springer, New York, 1999.

[7] Rotman J. J., Galois Theory, Springer, New York, 1998.

[8] Thompson, J. G., *Some finite groups that appear as* $Gal(L/K)$*, where* $K \subset Q(\mu_n)$, Journal of Algebra 89 (1984), 437–499.

[9] Shafarevich I. R., *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Ser. Mat., 18:6 (1954), 525–578.

[10] Volklein H., Groups as Galois Groups, Cambridge University Press, Cambridge, 1996.

[11] Hunt D. C., *Rational Rigidity and the Sporadic Groups*, Journal of Algebra 99 (1986), 577–592.