Occurrence of Finite Groups as Galois Group over $\mathbb{Q}(t)$: The Inverse Galois Problem

Vikas Srivastava

A dissertation submitted for the partial fulfilment of Integrated BS-MS dual degree

Indian Institute of Science Education and Research Mohali
April 2017

Certificate of Examination

This is to certify that the dissertation titled **"Occurrence of Finite Groups as Galois Group over $\mathbb{Q}(t)$: The Inverse Galois Problem"** submitted by **Vikas Srivastava** (Reg. No. MS12085) for the partial fulfillment of BS-MS dual degree program of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Amit Kulshrestha Dr. Chetan Balwe Dr. Kapil Paranjape
(Supervisor)

Dated: April 20, 2017

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Kapil Paranjape at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of work done by me and all sources listed within have been detailed in the bibliography.

Vikas Srivastava
(Candidate)

Dated: April 20, 2017

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Kapil Paranjape
(Supervisor)

"God exists since mathematics is consistent, and the Devil exists since we cannot prove it."

-André Weil

"One should study mathematics simply because it helps to arrange one's ideas."

-M.W. Lomonossow

"Algebraic geometry seems to have acquired the reputation of being esoteric, exclusive, and very abstract, with adherents who are secretly plotting to take over all the rest of mathematics. In one respect this last point is accurate..."

-David Mumford

"Algebra is the offer made by the devil to the mathematician. The devil says: I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvelous machine."

-Michael Atiyah

"As long as algebra and geometry traveled separate paths their advance was slow and their applications limited. But when these two sciences joined company, they drew from each other fresh vitality and thenceforward marched on at a rapid pace towards perfection."

-Joseph-Louis Lagrange

Acknowledgement

First of all, I want to thank my mentor and guide Dr. Kapil Paranjape for introducing me to this exciting area of mathematics. I have tasted some of the most delicious mathematics ever served to humanity!!. I am grateful to him for his patience and for his kind and generous support that I received not only while working on my project but through the five years at IISER Mohali.

I still remember the MTH101 course taken by him, although I didn't understand anything!!!, surprisingly I found myself inclined towards mathematics. When I came to IISER in August 2012, I knew nothing about computers and programming. He motivated me to learn all this. In September 2012, I switched to LINUX and the rest is history.

I want to thank Dr. Amit Kulshrestha, Associate Professor (Mathematics) IISER Mohali. He introduced me to GAP. I have learnt a lot of mathematics during numerous projects done under his able guidance.

I would like to thank my parents Mr. V.P. Srivastava and Mrs. Beena Srivastava and my brother Mr. Vaibhava Srivastava for their strong emotional support and most importantly allowing me to choose my own decisions in my life. I want to thank my brother for boosting up my spirits.

It would be negligent of me not to mention efforts of my friend Ms. Vandana. How can I forget the 3-4 hours late night mathematical discussions. (Mind it! She is a biology student). I don't know how she was able to bear so much "abstract nonsense".

I want to thank DST-INSPIRE for the generous financial support and the IISER Mohali Administration for the smooth completion of administrative paperwork.

Vikas Srivastava

Preface

The Inverse Galois Problem over $\mathbb{Q}(t)$ is concerned with determining whether a given finite group G occurs as Galois group of some finite regular (ramified) extension, say E of $\mathbb{Q}(t)$. Classical Inverse Galois Problem is concerned with solving the above problem over $\mathbb{Q}$ instead of $\mathbb{Q}(t)$. In this book, we describe various methods to construct Galois extension of $\mathbb{Q}(t)$. Due to theorem of Hilbert, also known as Hilbert's irreducibility theorem, which roughly speaking says that if a group G occurs as Galois group over $\mathbb{Q}(t)$, then it also occurs as Galois group over $\mathbb{Q}$. Therefore it is enough to work over $\mathbb{Q}(t)$. Working over $\mathbb{Q}(t)$ has geometric advantage, as extension of $\mathbb{Q}(t)$ corresponds to covering of $\mathbb{P}^1$ define over $\mathbb{Q}$.

The first part of the book (Chapter 1-4) lays the groundwork. It includes definitions, statement of theorems, important propositions that will be required for understanding rest of the book. Another purpose is to keep this book self contained. For readers, who already have a basic knowledge about these topics, may skip the Part I, and directly start reading part II . Chapter 1 gives a short introduction to covering space and fundamental theorem of Galois theory for covering spaces. Chapter 2 gives a short introduction to basic elements of algebraic geometry. the main goal is to show that there is a correspondence between covering of $\mathbb{P}^1$ defined over $\mathbb{Q}$ and field extension of $\mathbb{Q}(t)$. Chapter 3 gives a concise introduction to algebraic groups. If the field extension is not finite, classical Galois correspondence ceases to exist. In this case, we introduce a topology on Galois group, known as Krull's topology which gives G a structure of an algebraic group. As we will see, in some sense it restores this correspondence. Chapter 4 gives a short introduction to theory of rational function fields. We show that concepts of places, primes and valuations are same.

Part II (Chapter 5-7) is the heart of the book. It gives logical foundation to rest of the thesis. In these chapters we develop the main theory. we discuss ideas and methods to construct Galois extension of $\mathbb{Q}(t)$. The central result of this part is Basic Rigidity Theorem and the Rigidity Criterion (Chapter 7). This method has been very successfull in realizing finite simple groups as Galois group. In Chapter 6, we describe the strategy proposed by E. Noether in 1918 to attack the problem.

In Part III (Chapters 8-11) we apply the ideas/methods developed in part II to various finite groups. In chapter 8, we attack the problem using Noether's Trick. In Chapter 9 and Chapter 11, we apply the theory of rigidity and rationally to realize finite groups as Galois group over $\mathbb{Q}(t)$. In chapter 11, we have tried to realize the

sporadic simple groups as Galois group over $\mathbb{Q}(t)$, using the rigidity method. Since we have made extensive use of GAP and ATLAS, Chapter 10 serves the purpose of giving a short introduction on these topics.

Appendix contains a short exposition on Hilbert's irreducibility theorem. We have made a program in python to show that A_n is $(2, 3)$ generated. Using the theory of modular curves, we present a alternating way to realize the alternating groups as Galois group. This uses the fact that A_n is $(2, 3)$ generated.

If you find any mistake or flaw in this book kindly notify the author by sending an email to vikas.math123@gmail.com

Notation

Let $\mathbb{A}^n$ denote the affine space and $\mathbb{P}^n$ denote the projective space.
If X is a finite set, we denote the cardinality of X by $|X|$. V/K denote the variety defined over K. $V(L)$ denote the set of L-rational points of V.
We denote by $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ the filed of rational numbers, integers, real numbers and complex numbers respectively.

For a group G, we denote by $Aut(G)$ the automorphism group of G. Let $:=$ to denote "defined to be equal to". If K/k is field extension, $Aut(K/k)$ denote the group of automorphism of K that fixes k.

We say that G has property Gal_T, if there is a finite regular (ramified) Galois extension of $\mathbb{Q}(t)$ with Galois group G. We will write "Galois extension of $\mathbb{Q}(t)$" to denote the Galois extension with above properties.

Contents

Part I

Laying The Groundwork

Chapter 1

Covering Space Theory

1.1 Introduction

This chapter gives short introduction to Galois theory of covering spaces. We start with definition of covering spaces. In the last section, we will state the algebraic topology version of fundamental theorem of Galois theory.

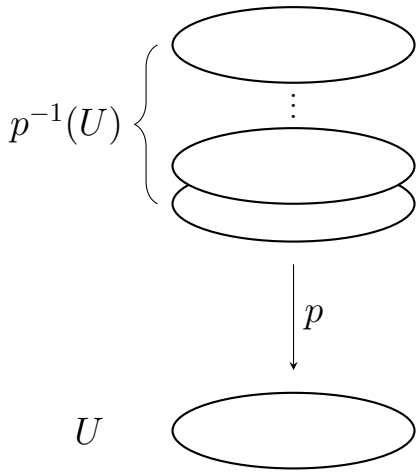
We have followed the approach of [26]. All definition, theorem and proofs are from the book *Introduction to Topological Manifolds* by J. Lee. See [26].

To keep the exposition short, we have left small details. There are lot of good book where the material presented here is covered. See [25], [28].

1.2 What is a Covering space?

Let us begin with definition first, then we will worry about why we are studying them. We will try to give some motivation for the topic.

Definition 1.1. A map $p : \tilde{X} \longrightarrow X$ is called a covering map if for every point $x \in X$, there is a neighborhood U of x so that $p^{-1}(U)$ is a disjoint union U_α of open sets in $\tilde{X}$, each mapped homeomorphically onto U by (the restriction of) p . X is called the *base space* of the covering; $\tilde{X}$ is called the *total space*.



Building the Intuition

Intuitively, p "wraps" $\tilde{X}$ onto X, We can visualize $p^{-1}(V)$ as **stack of pancakes** that are projected onto V by p.
There is another approach to understand this, a map $p : Y \longrightarrow X$ is a covering map if p locally looks like the projection from

$$X \times \{ \textit{ a discrete space}\} \to X.$$

More precisely: each point $x \in X$ has a neighbourhood U such that the map $p^{-1}(U) \to U$ is isomorphic to a projection

$$U \times \{ \textit{ a discrete space } \} \to U.$$

It is very similar to notion of fibre bundle, an object which appears a lot in topology and geometry. Loosely speaking *Covering spaces are the simplest example of fibre bundles with discrete fibres.*

Proposition 1.2.

- *Every covering map is a local homeomorphism, an open map, and a quotient map.*
- *An injective covering map is a homeomorphism.*
- *A finite product of covering maps is covering map.*
- *The restriction of a covering map to a saturated, connected, open subset is a covering map onto its image.*

Definition 1.3. A covering space is a universal covering space if it is simply connected.

Example 1.4. The exponential quotient map $\epsilon : \mathbb{R} \longrightarrow \mathbb{S}^1$ given by $\epsilon(x) = exp(2\pi\iota x)$ is a covering map.

Example 1.5. The $n-th$ power map $p_n : \mathbb{S}^1 \longrightarrow \mathbb{S}^1$.

The fundamental lemma is that covering spaces have the path lifting property:

Lemma 1.6. (**Path Lifting Properties**)Suppose $\tilde{X} \xrightarrow{p} X$ is a covering.

1. Given a path $\gamma : I \to X$ and a lift of the initial point $\tilde{x}_0 \in \tilde{X}$, there is a unique lift $\tilde{\gamma} : I \to \tilde{X}$ with $p\tilde{\gamma} = \gamma$.

2. If $\gamma \simeq \gamma'$ are homotopic paths in X, then they lift to homotopic paths $\tilde{\gamma} \simeq \tilde{\gamma'}$ in $\tilde{X}$ (in particular, the endpoints agree).

Immediate consequences of the path lifting property include

Corollary 1.7. If $\tilde{X} \xrightarrow{p} X$ is a covering then $p_* : \pi_1(\tilde{X}, \tilde{x}) \to \pi_1(X, x)$ is injective.

1.3 Monodromy

All the theorems and proof in this section can be found in the [26].

Theorem 1.8. *(***Monodromy Theorem***) Let $q : E \longrightarrow X$ be a covering map. Suppose f and g are path in X with the same initial point and same terminal point and $\tilde{f}_e, \tilde{g}_e$ are their lifts with the same initial point $e \in E$.*
a) $\tilde{f}_e \sim \tilde{g}_e$ if and only if $f \sim g$
b) If $f \sim g$ then $\tilde{f}_e(1) = \tilde{f}_e(1)$.

Proof. See [26] □

Theorem 1.9. *(***Injectivity Theorem***) Let $q : E \longrightarrow X$ be a covering map. For any point $e \in E$, the induced homomorphism $q_* : \pi_1(E, e) \longrightarrow \pi_1(X, q(e))$ is injective.*

Proof. [26] □

Definition 1.10. The above theorem shows that the fundamental group of a covering space is isomorphic to a certain subgroup of the fundamental group of the base. We call this the **subgroup induced by the covering**.

Definition 1.11. Suppose G is a group, a set S endowed with a left or right $G-$action is called a $G-set$. For any $s \in S$, the **isotropy group** of s, denoted by G_s, is the set of all elements of G that fix s:

$$G_s \ = \ \{g \in G \ : s.g = s\}.$$

One can check that action is free if and only if the isotropy group of every point is trivial.

Theorem 1.12. *(**The Monodromy Action**) Suppose $q : E \longrightarrow X$ is a covering map and $x \in X$. There is a transitive right action of $\pi_1(X, x)$ on the fibre $q^{-1}(x)$, called the monodromy action, given by $e.[f] = \tilde{f}_e(1)$ for $e \in q^{-1}(x)$ and $[f] \in \pi_1(X, x)$.*

Theorem 1.13. *(**Isotropy groups of the Monodromy Action**). Suppose $q : E \longrightarrow X$ is a covering map and $x \in X$. For each $e \in q^{-1}(x)$, the isotropy group of e under the monodromy action is $q_*\pi_1(E, e) \subseteq \pi_1(X, x)$.*

Proof. See [26] □

Corollary 1.14. Suppose $q : E \longrightarrow X$ is a covering map. The monodromy action is free on each fibre of q if and only if E is simply connected.

Corollary 1.15. Suppose $q : E \longrightarrow X$ is a covering map and E is simply connected. Then each fibre of q has the same cardinality as the fundamental group of X.

Corollary 1.16. Covering of Simply Connected Spaces If X is a simply connected space, every covering map $q : E \longrightarrow X$ is a homeomorphism.

Proposition 1.17. *(**Isotropy Groups of Transitive $G-$ sets**). Suppose G is a group and S is a transitive right G-set.*

a)For each $s \in S$ and $g \in G$

$$G_{s.g} \ = \ g^{-1}G_s g$$

b) The set $\{G_s : s \in S\}$ of all isotropy groups is exactly one conjugacy class of subgroups of G. This conjugacy class is called the isotropy type of S.

Theorem 1.18. *(**Conjugacy Theorem**.) Let $q : E \longrightarrow X$ be a covering map. For any $x \in X$, as e varies over the fiber $q^{-1}(x)$, the set of induced subgroups $q_*\pi_1(E, e)$ is exactly one conjugacy class in $\pi_1(X, x)$.*

Definition 1.19. A covering map $q : E \longrightarrow X$ is called a **normal(Galois) covering** if the induced subgroup $q_*\pi_1(E, e)$ is a normal subgroup of $\pi_1(X, q(e))$ for some $e \in E$.

Proposition 1.20. *(**Characterization of Normal Coverings**.) Suppose $q : E \longrightarrow X$ is a covering map. Then the following are equivalent:*

a)The subgroup $q_*\pi_1(E, e)$ is normal for some $e \in E$, i.e. q is normal.
b) For some $x \in X$, the subgroups $q_*\pi_1(E, e)$ are the same for all $e \in q^{-1}(x)$.
c) For every $x \in X$, the subgroups $q_*\pi_1(E, e)$ are the same for all $e \in q^{-1}(x)$.
d) The subgroups $q_*\pi_1(E, e)$ is normal for every $e \in E$.

1.4 The Automorphism Group of a Covering

Definition 1.21. Suppose $q : E \longrightarrow X$ is a covering map. An **automorphism of** q is a covering isomorphism from q to itself, that is, a homeomorphism $\phi : E \longrightarrow E$ such that $q \circ \phi = q$. Covering automorphisms are also variously known as **Deck transformation** or **covering transformations**.

Definition 1.22. Let $Aut_q(E)$ denote the set of all automorphism of the covering $q : E \longrightarrow X$. It is easy to see it forms a group and called the automorphism group of the covering(covering group).

Proposition 1.23. *(**Properties of Automorphism Group**). Let $q : E \longrightarrow X$ be a covering map.*

a) If two automorphisms of q agree at one point, they are identical.
b)Given $x \in X$, each covering automorphism restricts to a $\pi_1(X, x)-$ automorphism of the fibre $q^{-1}(x)$ with respect to monodromy action.
c)For any evenly covered open subset $U \subseteq X$, each covering automorphism permutes the components of $q^{-1}(U)$.
d)The group $Aut_q(E)$ acts freely on E by homeomorphism.

Proposition 1.24. *(**Normal Coverings/Galois Covering**). Let $q : E \longrightarrow X$ is a covering map, if $Aut_q(E)$ acts transitively on each fibre we say q is a normal covering.*

The next theorem is a central result concerning the relationship between covering spaces and fundamental groups. It gives an explicit for the automorphism group of a covering in terms of the fundamental groups of the covering space and the base.

Theorem 1.25. Covering Automorphism Group Structure Theorem *Suppose $q : E \longrightarrow X$ is a covering map, $e \in E$, and $x = q(e)$. Let $G = \pi_1(X, x)$ and $H = q_*\pi_1(E, e) \subseteq \pi_1(X, x)$ For each path class $\gamma \in N_G(H)$ there is a unique covering*

automorphism $\phi_\gamma \in Aut_q(E)$ *that satisfies* $\phi_\gamma(e) = e.\gamma$. *The map* $\gamma \mapsto \phi_\gamma$ *is a surjective group homomorphism from* $N_G(H)$ *to* $Aut_q(E)$ *with kernel equal to* H, *so it descends to an isomorphism from* $N_G(H)/H$ *to* $Aut_q(E)$*:*

$$Aut_q(E) \simeq N_{\pi_1(X,x)}(q_*\pi_1(E,e))/q_*\pi_1(E,e).$$

Corollary 1.26. If $q : E \longrightarrow X$ is a normal covering then for any $x \in X$ and any $e \in q^{-1}(x)$, the map $\gamma \mapsto \phi_\gamma$ above induces an isomorphism from $\pi_1(X,x)/q_*\pi_1(E,e)$ to $Aut_q(E)$.

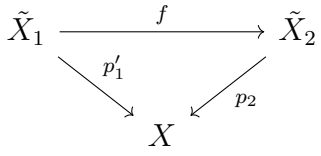
Corollary 1.27. If $q : E \longrightarrow X$ is a covering map and E is simply connected, then the automorphism group of the covering is isomorphic to the fundamental group of X.

1.5 Galois Correspondence

So Finally we are ready to state the correspondence between Galois theory and topology.

The Galois group of a covering Let us revisit automorphism group of covering.

Definition 1.28. A morphism from a covering $\tilde{X}_1 \xrightarrow{p_1} X$ to a covering $\tilde{X}_2, \xrightarrow{p_2} X$ is a continuous function $f : \tilde{X}_1 \to \tilde{X}_2$ satisfying $p_2 = fp_1$.



Definition 1.29. An automorphism of a cover $p : \tilde{X} \to X$ is called a covering transformation or a deck transformation. Let $G(\tilde{X}) := Aut(\tilde{X})$ denote the group of automorphisms of a cover $p : \tilde{X} \to X$. The group $G(\tilde{X})$ is called the Galois group or the deck group of the cover. If necessary, one can write $G(\tilde{X}, X)$ to indicate the dependence on the base space X.

Proposition 1.30. *We have two groups associated to a covering* $p : (\tilde{X}, \tilde{x}) \to (X, x)$*: namely, the fundamental group* $H = \pi_1(\tilde{X}, \tilde{x}) \subset G := \pi_1(X, x)$ *and the Galois group* $G(\tilde{X})$*. For spaces* X *satisfying a necessary local condition, we have a "Galois theory" of covering spaces, where based covers* $p : (\tilde{X}, \tilde{x}) \to (X, x)$ *correspond bijectively to subgroups* H *and*

- *Morphisms between covering spaces $\tilde{X}_1 \to \tilde{X}_2$ correspond to inclusions of subgroups $H_1 \to H_2$.*
- *There is a universal cover $\tilde{Y}$ corresponding to $H = \{e\}$ and $G(\tilde{Y}) \simeq G$. All other covers are obtained as quotients of the universal cover.*
- *A covering is called regular if $G(\tilde{x})$ acts transitively on the fibers. Regular covers correspond to normal subgroups G, and for a regular cover $\tilde{X}$, we have $G(\tilde{X}) \cong G/H$.*
- *If $\tilde{X}_1 \to \tilde{X}_2$ is a morphism between regular covers that is itself a regular cover, then $G(\tilde{X}_2, X) \cong G(\tilde{X}_1, X)/G(\tilde{X}_1, \tilde{X}_2)$.*

To appreciate this link between Galois Theory of Field Extensions and Galois theory of Covering spaces. Recall Fundamental theorem of Galois Theory

Theorem 1.31. *(**Fundamental Theorem of Galois Theory**) Let K/F be Galois and set $G = Gal(K/F)$. There is a bijection*

$$\{ \text{ subfields } E \text{ of } K \text{ with } F \subseteq E \subseteq K\} \longleftrightarrow \{ \text{ subgroups } H \leq G\}$$

with the following correspondences

$$E \longmapsto Gal(K/E)$$

and

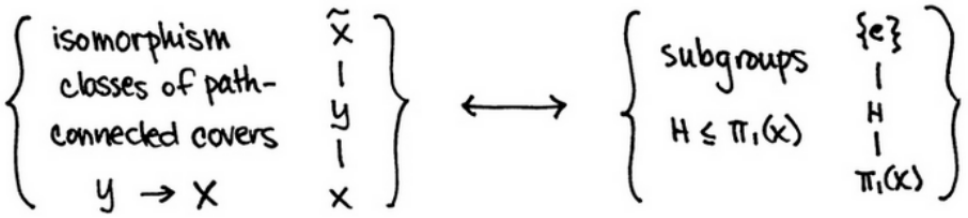
$$K^H = \{x \in K : \sigma(x) = x \quad \forall \sigma \in H\} \longleftarrow H$$

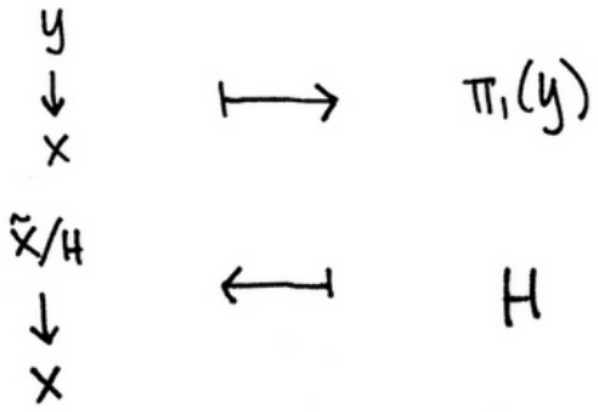
Under this correspondence:

1. *If E_1, E_2 correspond to H_1, H_2 respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$.*
2. *$[K : E] = |H|$ and $[E : F] = |G : H|$.*
3. *K/E is always Galois with Galois group $Gal(K/E) = H$.*
4. *E is Galois over F if and only if H is a normal subgroup in G, in which case $Gal(E/F) \simeq G/H$.*
5. *If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \cap E_2$ corresponds to the group $< H_1, H_2 >$ and E_1E_2 corresponds to $H_1 \cap H_2$.*

Theorem 1.32. *(**Fundamental Theorem of Galois Theory for Covering Spaces**) Let X be a path-connected, locally path-connected, and semilocally simply-connected space with universal cover $p : \tilde{X} \longrightarrow X$ Then there is a isomorphism between the fundamental group of X and the group of deck transformation of p(Sometimes we denote it by $G(\tilde{X})$)*

There is one to one correspondence between Isomorphism classes of path connected covers and subgroups of fundamental group $\pi_1(X)$. Following pictures make it more clear (Image credit: Math3ma.com).





Chapter 2

Smooth Curves and Their Function Fields

Our main goal is to show that there is a close connection between smooth curves and their function fields. We will need basic theory of algebraic geometry. For the sake of completeness, we describe the basic theory required to understand this beautiful connection.

The correspondence between coverings and field extension helps to rephrase the inverse Galois problem purely in geometric terms. Then the results of algebraic topology and covering space theory can be used to study the problem.
Let me fix some notation. We will use it throughout this chapter, K is a perfect field, $\bar{K}$ is algebraic closure of K and G_K denote the absolute Galois group of K.

All the definitions, proposition and theorems in this chapter are taken from [11].

2.1 Varieties

We start with definition of affine varieties. Roughly speaking they are common zeros of system of polynomial equations.

Definition 2.1. Affine n-space (over K) is the set of n-tuples,

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \cdots, x_n) : x_i \in \bar{K}\}.$$

We define the set of K-**rational points** of $\mathbb{A}^n$ by

$$\mathbb{A}^n(K) = \{P = (x_1, \cdots, x_n) : x_i \in K\}.$$

Definition 2.2. A subset of affine space $\mathbb{A}^n$ is called **affine algebraic set** if it is of the form V_I for some I. If V is an algebraic set, we define the **ideal** of V to be

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0 \; for \; all \; P \in V\}$$

Definition 2.3. We say that an algebraic set is **defined over** K if its ideal $I(V)$ can be generated by polynomials in $K[X]$. We denote this by V/K. If V is defined over K, then the set of K-rational points of V is the set

$$V(K) = V \cap \mathbb{A}^n(K)$$

Notation From now on by V/K we will mean that variety V is defined over K. To each variety V, a geometric object we associate a polynomial ring, an algebraic object. Later we will see that many interesting results about varieties can be obtained by just studying the affine coordinate ring. We say two varieties are isomorphic (we will define it in next section) if and only if their affine coordinate ring is isomorphic. Many concepts like dimension of variety is defined using coordinate ring.

Definition 2.4. The **affine coordinate ring** of V/K is given by $K[X]/I(V/K)$. The ring $K[V]$ is an integral domain. Its quotient field (field of fractions) is denoted by $K(V)$ and is called the function field of V/K.

We are studying geometric objects so it's natural to talk about notion of smoothness.

Definition 2.5. Let V be a variety, $P \in V$, and $f_1, \cdots, f_m \in \bar{K}[X]$ a set of generators for $I(V)$. then we say that V is **non-singular(or smooth)** at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{1 \leq i \leq m, 1 \leq j \leq n}$$

has rank $n - dim(V)$. If V is nonsingular at every point, then we say that V is nonsingular or smooth.

Definition 2.6. Let V be a variety. The **dimension of** V, denoted by $dim(V)$, is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Let's describe another characterization of smoothness, in terms of the functions on the variety V.

Definition 2.7. For each point $P \in V$, we define **an ideal** M_P

$$M_P = \{f \in \bar{K}[V] : f(P) = 0\}.$$

Notice that M_P is a maximal ideal, since there is an isomorphism $\bar{K}[V]/M_P \to \bar{K}$ given by $f \to f(P)$. The quotient M_P/M_P^2 is a finite-dimensional $\bar{K}$ vector space.

Proposition 2.8. *Let Let V be a variety. A point $P \in V$ is* ***nonsingular*** *if and only if*

$$dim_{\bar{K}}\ M_P/M_P^2 = dim\ V.$$

To each point P of variety V, we associate a ring of functions.

Definition 2.9. The **local ring of V at P**, denoted by $\bar{K}[V]_P$, is the localization of $\bar{K}[V]$ at M_P. The functions in $\bar{K}[V]_P$ are said to be **regular or defined at P**.

Definition 2.10. (**Projective Space**)Projective n-space (over K) denoted by $\mathbb{P}^n$ is the set of all $(n+1)$ tuples

$$(x_0, \cdots, x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is nonzero, modulo the equivalence relation

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n)$$

if there exists a $\alpha \in \bar{K}^\times$ such that $x_i = \alpha y_i$ for all i. An equivalence class

$$\{(\alpha x_0, \cdots, \alpha x_n) : \alpha \in \bar{K}^\times\}$$

is denoted by $[x_0, \cdots, x_n]$, and the individual $x_0, \cdots, x_n$ are called **homogeneous coordinates** for the corresponding point in $\mathbb{P}^n$. The set of K-rational points in $\mathbb{P}^n$ is the set

$$\mathbb{P}^n(K) = \{[x_0, \cdots, x_n] \in \mathbb{P}^n :\ all\ x_i\ \in K\}.$$

Definition 2.11. A polynomial $f \in \bar{K}[X_0, \cdots, X_n]$ is **homogeneous** of degree d if

$$f(\alpha X_0, \cdots, \alpha X_n) = \alpha^d f(X_0, \cdots, X_n)$$

for all $\alpha \in \bar{K}$.

We say that an **ideal I is homogeneous** if it is generated by homogeneous polynomials.

Let f be a homogeneous polynomial and let $P \in \mathbb{P}^n$. Now it makes sense to ask whether $f(P) = 0$ as it does not depend on the choice of homogeneous coordinates for P. To illustrate this, choose a non homogeneous polynomial say $f = x^2 - y$. Consider the points $P = (1, 1)$ and $Q = (-1, -1)$. Note that $P \sim Q$ (take $\lambda = -1$),

but $f(P) = 1^2 - 1 = 1$ is not equal to $f(Q) = (-1)^2 - (-1) = 1 + 1 = 2$. To each homogeneous ideal I we associate a subset of projective space by the rule

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \; for \; all \; homogeneous \; f \in I\}.$$

Definition 2.12. A (projective) algebraic set is any set of the form V_I for a homogeneous ideal I. If V is a projective algebraic set, the (homogeneous) ideal of V , denoted by $I(V)$, is the ideal of $\bar{K}[X]$ generated by

$$\{f \in \bar{K}[X] : f \; is \; homogeneous \; and \; f(P) = 0 \; for \; all \; P \in V\}.$$

Definition 2.13. As in the affine case, we say V is defined over K, denoted by V/K, if its ideal $I(V)$ can be generated by homogeneous polynomials in $K[X]$. If V is defined over K, then the set of K-rational points of V is the set

$$V(K) = V \cap \mathbb{P}^n(K).$$

Now we will show that in some sense, affine space cover the projective space. Precisely speaking $\mathbb{P}^n$ contains many **copies of** $\mathbb{A}^n$. For example, for each $0 \leq i \leq n$, There is an inclusion

$$\phi_i : \mathbb{A}^n \longrightarrow \mathbb{P}^n,$$

$$(y_1, \cdots, y_n) \mapsto [y_1, \cdots, y_{i-1}, 1, y_i, \cdots, y_n].$$

We let H_i denote the hyperplane in $\mathbb{P}^n$ given by $X_i = 0$,

$$H_i = \{P = [x_0, \cdots, x_n] \in \mathbb{P}^n : x_i = 0\},$$

and we let U_i to be the complement of H_i,

$$U_i = \{P = [x_0, \cdots, x_n] \in \mathbb{P}^n : x_i \neq 0\}$$

There is a natural bijection,

$$\phi_i^{-1} : U_i \longrightarrow \mathbb{A}^n,$$

$$[x_0, \cdots, x_n] \mapsto (x_0/x_i, \cdots, x_{i-1}/x_i, x_{i+1}/x_i, \cdots, x_n/x_i)$$

For a fixed i, we identify $\mathbb{A}^n$ with the set U_i in $\mathbb{P}^n$ via the map ϕ_i.

Definition 2.14. Let V be a projective algebraic set with homogeneous ideal $I(V) \subset$

$\bar{K}[X]$. Then $V \cap \mathbb{A}^n$, by which we mean $\phi_i^{-1}(V \cap U_i)$ for some fixed i, is an affine algebraic set with ideal given by

$$I(V \cap \mathbb{A}^n) = \{f(Y_1, \cdots, Y_{i-1}, 1, Y_{i+1}, \cdots, Y_n) : f(X_0, \cdots, X_n) \in I(V)\}.$$

So heart of the above discussion is that most properties of a projective variety V may be defined in terms of the affine subvariety $V \cap \mathbb{A}^n$.

Definition 2.15. Let V/K be a projective variety and choose $\mathbb{A}^n \subset \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \emptyset$. The dimension of V is the dimension of $V \cap \mathbb{A}^n$. The function field of V, denoted by $K(V)$, is the function field of $V \cap \mathbb{A}^n$.

Definition 2.16. Let V be a projective variety, let $P \in V$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then V is nonsingular (or smooth) at P if $V \cap \mathbb{A}^n$ is nonsingular at P. The local ring of V at P, denoted by $\bar{K}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P.

As you can see above all the theory we have developed in affine case can be used to study projective varieties.

2.2 Maps between Varieties

Next obvious question to ask is: What maps are allowed between the geometric objects we just constructed in the above section ? What are morphism between varieties. We follow from [11].

Definition 2.17. Let V_1 and $V_2 \subset \mathbb{P}^n$ be projective varieties. A **rational map** from V_1 to V_2 is a map of the form

$$f : V_1 \to V_2, \quad \phi = [f_0, ..., f_n],$$

where the functions $f_0, ..., f_n \in \bar{K}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, ..., f_n$ are all defined,

$$\phi(P) = [f_0(P), ..., f_n(P)] \in V_2.$$

Definition 2.18. If there is some $\lambda \in \bar{K}^\times$ such that

$$\lambda f_0, ..., \lambda f_n \in K(V_1),$$

then ϕ is said to be over K.

Definition 2.19. A rational map

$$\phi = [f_0, ..., f_n] : V_1 \to V_2$$

is **regular (or defined)** at $P \in V_1$ if there is a function $g \in \bar{K}(V_1)$ such that

1. each gf_i is regular at P;
2. there is some i for which $(gf_i)(P) \neq 0$.

If such a g exists, then we set

$$\phi(P) = [(gf_0)(P), ..., (gf_n)(P)].$$

A rational map that is **regular** at every point is called a **morphism**.

Definition 2.20. Now using the definitions above, we can describe the notion of "isomorphism" of varieties. Let V_1 and V_2 be varieties. We say that V_1 and V_2 are **isomorphic**, and write $V_1 \cong V_2$, if there are morphisms $\phi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on V_1 and V_2, respectively. We say that V_1/K and V_2/K are isomorphic over K if ϕ and ψ can be defined over K.

Proposition 2.21. *Let C be a curve and $P \in C$ a smooth point. Then $\bar{K}[C]_p$ is a discrete valuation ring.*

Definition 2.22. Let C be a curve and $P \in C$ a smooth point. The (normalized) **valuation** on $\bar{K}[C]_p$ is given by

$$ord_P : \bar{K}[C]_p \to \{0, 1, 2, ...\} \bigcup \{\infty\},$$

$$ord_P(f) = sup\{d \in \mathbb{Z} : f \in M_P^d\}.$$

Using $ord_P(f/g) = ord_P(f) - ord_P(g)$, we extend ord_P to $\bar{K}(C)$,

$$ord_P : \bar{K}(C) \to \mathbb{Z} \bigcup \infty.$$

Definition 2.23. A **uniformizer** for C at P is any function $t \in \bar{K}(C)$ with $ord_P(t) = 1$, i.e., a generator for the ideal M_P.

2.3 Digression: Approach of Hartshorne

Many books follows the notation of [4]. So for the sake of readers, we are providing a short summary of approach taken in the book Algebraic Geometry by Hartshorne. See [4]. Hartshorne, [4] defines the ring of regular functions of a point P on Y in the following manner. Observe that both definition conveys the same idea. Since the definitions are fundamental to mathematics, we have not made any attempt to alter it.

Definition 2.24. Let Y be a variety. We denote by $\mathcal{O}(Y)$ the ring of all regular functions on Y. If P is a point of Y, we define the local ring of P on Y, $\mathcal{O}_{P,Y}$ (or $\mathcal{O}_P$) to be the ring of germs of regular functions on Y near P. In other words, an element of $\mathcal{O}_P$ is a pair (U, f) where U is an open subset of Y containing P, and f is a regular function on U, and where we identify two such pairs (U, f). and (V, g). if $f = g$ on $U \cap V$.

In this case also, we can see that $\mathcal{O}(Y)$ is a local ring: its maximal ideal $\mathfrak{m}$ is the set of germs of regular functions which vanish at P. Because if $f(P) \neq 0$, then $1/f$ is regular in some neighborhood of P. The residue field $\mathcal{O}(Y)/\mathfrak{m}$ is isomorphic to K.

He defines the function field of variety in the following way:

Definition 2.25. If Y is a variety, we define the function field $K(Y)$ of Y as follows: an element of $K(Y)$ is an equivalence class of pairs (U, f) where U is a nonempty open subset of Y, f is a regular function on U, and where we identify two pairs (U, f)

and (V, g) if $f = g$ on $U \cap V$. The elements of $K(Y)$ are called rational functions on Y.

$K(Y)$ is a field (Why ?). Since Y is irreducible, any two nonempty open sets have a nonempty intersection. Hence we can define addition and multiplication in $K(Y)$, making it a ring. Then if $(U, f) \in K(Y)$ with $f \neq 0$, we can restrict f to the open set $V = U - U \cap Z(f)$ where it never vanishes, so that $1/f$ is regular on V, hence $(V, 1/f)$ is an inverse for (U, f).

So what we have done so far is that, Given any variety Y, we have the associated to it, ring of global functions $\mathcal{O}(Y)$ the local ring $\mathcal{O}_p$ at a point of Y, and the function field $K(Y)$.

There is a beautiful connection between the the ring of global functions $\mathcal{O}(Y)$, the local ring $\mathcal{O}_p$ at a point of Y, and the function field $K(Y)$. We have this beautiful theorem which relate these three concepts. Fir proof, see (page 16, Chapter I) of [4]

Theorem 2.26. *Let $Y \subseteq \mathbb{A}^n$ be an affine variety with affine coordinate ring $A(Y)$. Then:*

(a) $\mathcal{O}(Y) \simeq A(Y)$;
(b) for each point $P \in Y$, let $\mathfrak{m}_p \subseteq A(Y)$ be the ideal of functions vanishing at P. Then $P \longrightarrow \mathfrak{m}_p$ gives a $1-1$ correspondence between the points of Y and the maximal ideals of $A(Y)$;
(c) for each P, $\mathcal{O}_p \simeq A(Y)_{\mathfrak{m}_p}$ and $dim\mathcal{O}_p = dim\ Y$;
(d) $K(Y)$ is isomorphic to the quotient field of $A(Y)$, and hence $K(Y)$ is a finitely generated extension field of k, of transcendence degree = dim Y.

There is a similar theorem for projective variety

Theorem 2.27. *Let $Y \subseteq \mathbb{P}^n$ be an variety with coordinate ring $S(Y)$. Then:*

(a) $\mathcal{O}(Y) \simeq k$;
(b) for each point $P \in Y$, let $\mathfrak{m}_p \subseteq S(Y)$ be the ideal of homogeneous functions vanishing at P .then for each P, $\mathcal{O}_p \simeq S(Y)_{(\mathfrak{m}_p)}$ and $dim\mathcal{O}_p = dim\ Y$;
(d) $K(Y) \simeq S(Y)_{((0))}$

2.4 Smooth Curves and Their Function Fields

In this section we will show that there is a closed connection between smooth projective curves and their function. Our main aim is to understand the bijective correspondence

between covers of $\mathbb{P}^1$ defined over $\mathbb{Q}$ and the field extension of $\mathbb{Q}(t)$. By curve I will always mean a smooth projective curve of dimension 1.

Theorem 2.28. *Let C be a curve, let $V \subset \mathbb{P}^N$ be a variety, let $P \in C$ be a smooth point, and let $\phi : C \longrightarrow V$ be a rational map. Then ϕ is regular at P. In particular, if C is smooth, then ϕ is a morphism.*

Proof. See [11] □

Proposition 2.29. *Let C/K be a smooth curve and let $f \in K(C)$ be a function. Then using f we can define a rational map, which we also denote by f,*

$$C \to \mathbb{P}^1,$$

$$P \mapsto [f(P), 1].$$

This map is actually a morphism. It is given by

$$f(P) = \begin{cases} [f(P), 1] & \text{if } f \text{ is regular at} P, \\ [1, 0] & \text{if } f \text{ has a pole at} P. \end{cases}$$

In other direction, Let

$$\phi : C \to \mathbb{P}^1.$$

$\phi = [f, g]$ be a rational map defined over K. We have two cases. Case I: $g = 0$, in that case ϕ is constant map $\phi = [1, 0]$, Case II ϕ is the map corresponding to the function $f/g \in K(C)$. Let's denote the former map by ∞, we thus obtain a bijective correspondence

$$K(C) \cup \{\infty\} \leftrightarrow \{maps\ C \to \mathbb{P}^1\ defined\ over\ K\}$$

We need the following proposition.

Proposition 2.30. *Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Let C_1/K and C_2/K be two curves and let $\phi : C_1 \to C_2$ be a nonconstant rational map defined over K. Then composition with ϕ induces an injection of function fields fixing K,

$$\phi^\star : K(C_2) \to K(C_1), \quad \phi^\star f = f \circ \phi.$$

We obtain our **central result**,

Theorem 2.31. *Let C_1/K and C_2/K be curves.*

- *Let $\phi : C_1 \to C_2$ be a nonconstant map defined over K. Then $K(C_1)$ is a finite extension of $\phi^\star(K(C_2))$.*
- *Let $i : K(C_2) \to K(C_1)$ be an injection of function fields fixing K. Then there exists a unique nonconstant map $\phi : C_1 \to C_2$ (defined over K) such that $\phi^\star = i$*
- *Let $\mathbb{K} \subset K(C_1)$ be a subfield of finite index containing K. Then there exist a smooth curve C'/K, unique up to K-isomorphism, and a nonconstant map $\phi : C_1 \to C'$ defined over K such that $\phi^\star : K(C') = \mathbb{K}$*

We conclude from the above theorem that there is a bijection between covers of $\mathbb{P}^1$ and field extensions of $\mathbb{Q}(t)$ We summarize it as:

$$\begin{bmatrix} \textit{Objects}\text{: smooth} \\ \text{curves defined over } K \\ \textit{Maps:} \text{ nonconstant} \\ \text{rational maps} \\ \text{(equivalently} \\ \text{surjective morphisms)} \\ \text{defined over } K \end{bmatrix} \rightsquigarrow \begin{bmatrix} \textit{Objects:} \text{ finitely} \\ \text{generated extensions} \\ \mathbb{K}/K \text{ of} \\ \text{transcendence degree} \\ 1 \text{ and} \\ \mathbb{K} \cap \bar{K} = K \\ \textit{Maps:} = \text{field} \\ \text{injections fixing } K \end{bmatrix}$$

$$C/K \rightsquigarrow K(C)$$

$$\phi : C_1 \to C_2 \rightsquigarrow \phi^\star : K(C_2) \to K(C_1)$$

Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the degree of ϕ to be 0. Otherwise we say that ϕ is a finite map and we define its degree to be

$$deg\ \phi = [K(C_1) : \phi^\star K(C_2)].$$

Definition 2.32. Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves, and let $P \in C_1$. The ramification index of ϕ at P, denoted by $e_\phi(P)$, is the quantity $e_\phi(P) = ord_P(\phi^\star t_{\phi(P)})$, where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. Note that $e_\phi(P) \geq 1$. We say that ϕ is unramified at P if $e_\phi(P) = 1$, and that ϕ is unramified if it is unramified at every point of C_1.

Definition 2.33. Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves.

- For every $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg(\phi).$$

- For all but finitely many $Q \in C_2$,

$$|\phi^{-1}(Q)| = deg_s(\phi)$$

A map $\phi : C_1 \to C_2$ is unramified if and only if

$$|\phi^{-1}(Q)| = deg_s(\phi) \quad for\ all\ Q \in C_2.$$

Chapter 3

Algebraic Tori, Profinite Groups and Infinite Galois Theory

3.1 Introduction

We know about the Galois correspondence between subgroups of Galois groups of finite Galois extensions and intermediate fields. But what happens for infinite Galois extension? It turns out that it is not valid for infinite Galois extension. We define a topology on Galois group, Krull's topology which helps to restore this correspondence.It is a well known fact in Galois theory that Galois groups are inverse limits of finite groups, that is they are profinite groups. In other direction, we can define profinite groups, independently of Galois theoretic properties. One can show that profinite group are realizable as Galois group.

This chapter gives a short presentation on this topic. Since profinite groups are example of algebraic groups. We will start with the definition of algebraic groups. We will state several important result which will be used throughout the chapter.

3.2 Definitions, Example and Morphisms

Definition 3.1. An algebraic group G is an algebraic variety as well as a group such that the maps, $m : G \times G \to G$ and $i : G \to G$, given by $m(x, y) = xy, i(x) = x^{-1}$ are morphism of algebraic varieties.

Definition 3.2 (Morphism of Algebraic groups)**.** If G and $G^{'}$ are algebraic groups, a map $\phi : G \to G^{'}$ is a homomorphism of algebraic groups if ϕ is a morphism of varieties and a group homomorphism. Similarly ϕ is an isomorphism of algebraic groups if ϕ is an isomorphism of varieties and a group isomorphism.

Example 3.3. The group GL_n, SL_n, Sp_{2n}, SO_n, O_n, U_n, etc are some of the standard examples of affine algebraic group.

3.3 Multiplicative Group and Algebraic Tori

Definition 3.4. As a special case, for $n = 1, GL_1 = \mathbb{G}_m = k^*$ and the coordinate ring is $k[GL_1] = k[x][x^{-1}]$ We call $\mathbb{G}_m$ the multiplicative group.
It has the underlying structure of punctured line $\mathbb{A}^1_k - \{(0)\} \subseteq \mathbb{A}^1_k$. The map m is given by

$$k[t, t^{-1}] \to k[u, v, u^{-1}, v^{-1}] : t \mapsto uv$$

and the inverse map i is given by

$$k[t, t^{-1}] \to k[t, t^{-1}] : t \mapsto t^1$$

Definition 3.5 (Linear Algebraic Group)**.** A linear algebraic group is an algebraic group isomorphic to an algebraic subgroup of GL_n for some n. Note the underlying variety of a linear algebraic group is affine.

Algebraic tori are the simplest examples of algebraic groups.

Definition 3.6 (K-Torus)**.** A K-Torus is an algebraic group over K which becomes isomorphic to a product of multiplicative group

$$\mathbb{G}_m \times \mathbb{G}_m \ldots \times \mathbb{G}_m$$

over the algebraic closure $\bar{K}$ of K.

Definition 3.7 (Split Torus)**.** If the above isomorphism is defined over K, then the torus is said to be split.

Definition 3.8 (Isogeny)**.** An isogeny between algebraic groups is a surjective morphism with finite kernel; two tori are said to be isogenous if there exists an isogeny from the first to the second. For any isogeny $\phi : T \to T'$ there exists a "dual" isogeny $\psi : T' \to T$ such that $\psi \circ \phi$ is a power map. In particular being isogenous is an equivalence relation between tori.

Before moving on to the next topic: Quasi Split Torus, Let's recollect some basic definitions

The **Jacobson radical** of an algebra over a field is the ideal consisting of all elements that annihilate every simple left-module. The radical contains all nilpotent

ideals, and if the algebra is finite-dimensional, the radical itself is a nilpotent ideal. A finite-dimensional algebra is then said to be **semisimple** if its radical contains only the zero element.

Definition 3.9. Let K be a field. An associative K-algebra A is said to be separable if for every field extension L/K, the algebra $A \otimes K$ is semisimple.

Definition 3.10 (Quasi Split Torus)**.** Let A be a finite-dimensional separable k-algebra. Then there is a linear algebraic group G given by $G(B) = \mathbb{G}_m(A \otimes_k B) = (A \otimes_k B)^\times$, denoted $\mathrm{Res}_{A/k}\, \mathbb{G}_m$.

Definition 3.11 (Character Group)**.** Character of an algebraic group G is a homomorphism $G \to \mathbb{G}_m$. The characters of G form an abelian group under point wise multiplication, denoted $X^*(G)$.

3.4 Profinite Groups

In this section on we have followed the *Field Arithmetic* by Fried, Michael D., Jarden, Moshe. [30]

Definition 3.12. (**Inverse limit**)

An inverse system(also called a projective system) over a directed partially ordered set $(I, \leq)$ is a data $(S_i, \pi_{ji})_{i,j\in I}$ where S_i is a set and $\pi_{ji} : S_j \to S_i$ is a map for all $i, j \in I$ with $i \leq j$ satisfying the following rules:

(2a) π_{ii} the identity map for each $i \in I$.

(2b) $\pi_{ki} = \pi_{ji} \circ \pi_{kj}$ if $i \leq j \leq k$.

Let S be the subset of the cartesian product $\prod_{i\in I} S_i$ consisting of all elements $s = (s_i)_{i\in I}$ with $\pi_{ji}(s_j) = s_i$ for all $i \leq j$. We say $(S, \pi_i)_{i\in I}$ is the inverse (or projective) limit of the family $(S_i)_{i\in I}$ with respect to the maps π_{ji}. Denote S by $\varprojlim S_i$.

The collection of all subsets of $S = \varprojlim S_i$ of the form $\pi_i^{-1}(U_i)$ with U_i open in S_i is a basis for the topology of S forms a basis for topology.

Definition 3.13. An inverse limit of an inverse system of finite discrete spaces is called a **profinite space**.

Proposition 3.14. *Let $(G_i, \pi_{ji})_{i,j\in I}$ be an inverse system of topological groups and continuous homomorphisms $\pi_{ji} : G_j \to G_i$, for each $i, j \in I$ with $j \geq i$. Then $G = \varprojlim G_i$ is a topological group and the projections $\pi_i : G \to G_i$ are continuous homomorphisms. Let $\langle G_i'.\pi_{ji}'\rangle_{i,j\in I}$ be another system of topological groups with $G' = \varprojlim G_i'$. Suppose $\theta_i : G_i \to G_i', i \in I$, is a compatible system of continuous homomorphisms. Then the corresponding map $\theta : G \to G'$ is a continuous homomorphisms.*

Theorem 3.15. *For proof, look [30]*

Definition 3.16. Consider an inverse system of finite groups $(G_i, \pi_{ji})_{i,j\in I}$. Assume that each of the G_i has the discrete topology. We call the inverse limit $G = \varprojlim G_i$ a profinite group.

We summarize some important results. For detailed analysis, see [30].

- A subgroup H of G is open if and only if H is closed of a finite index. The intersection of all normal closed subgroups of G is 1. Every open subset of G is a union of cosets g_iN_i with N_i open normal and $g_i \in G$.

- Every profinite group is compact, Hausdorff, and has a basis for its topology consisting of open-closed sets.
- A subset C of a profinite group is closed if and only if C is compact.
- A subset B of a profinite group is open-closed if it is a union of finitely many cosets g_iN with N open normal and $g_i \in G$ (use (a) and the compactness of B).
- Every homomorphism $\varphi : G \to H$ is tacitly assumed to be continuous. In particular, φ maps compact subsets of G onto compact subsets of H. hence, φ maps closed subsets of G onto closed subsets of H (use (c)).
- By the first isomorphism theorem for compact groups, every epimorphism $\varphi : G \to H$ of profinite groups is an open map. In particular, φ maps open subgroups of G onto open subgroups of H.

3.5 Infinite Galois Theory

Let N be a Galois extension of a field K. By definition, the Galois group $Gal(N/K)$ associated with N/K consists of all automorphisms of N that fix each element of K. If N/K is a finite extension and G_1, G_2 are subgroups of $Gal(N/K)$ with the same fixed fields in N, the $G_1 = G_2$. This result fails to hold if the extension is not finite.

We will now introduce the notion of **Krull's Topology**

Definition 3.17. Let $\mathcal{L}$ denote the set of all intermediate fields $K \subseteq L \subseteq N$, with L/K finite and Galois. If $L' \in \mathcal{L}$ and $L \subseteq L'$, then $res_L : Gal(L'/K) \to Gal(L/K)$ is an surjective homomorphism of groups.

Definition 3.18. (**Krull's Topology**) Now consider the inverse limit $\varprojlim Gal(L/K)$, with L ranging over $\mathcal{L}$. Let's take $\sigma \in Gal(N/K)$ correspondingly we define a element $(res_L\sigma)_{L\in\mathcal{L}}$ of $\varprojlim Gal(L/K)$. This element is unique. Conversely, every $(\sigma_L)_{L\in\mathcal{L}} \in \varprojlim Gal(L/K)$ defines a unique $\sigma \in Gal(N/K)$ with $res_L\sigma = \sigma_L$ for each $L \in \mathcal{L}$. Thus, $\sigma \mapsto (res_L\sigma)_{L\in\mathcal{L}}$ is an isomorphism $Gal(N/K) \cong \varprojlim Gal(L/K)$.

This isomorphism gives a topology on $Gal(N/K)$ which arises from the topology on $\varprojlim Gal(L/K)$.

We call this topology: the **Krull's topology**. Under this topology, $Gal(N/K)$ becomes a profinite group.

Definition 3.19. Let L be a finite extension of K contained in N. Then we define Galois closure $\hat{L}$ is the smallest Galois extension of K that contains L. It is finite over K and is contained in N. We can write $Gal(N/L)$ as a union of right cosets of $Gal(N/\hat{L})$.

If S is a set of automorphisms of N, then $N(S) = x \in N | \sigma x = x$ for every $\sigma \in S\}$ is the fixed field of S in N.

Theorem 3.20. *Let N be a Galois extension of a field K. Then $L \mapsto Gal(N/L)$ is a bijection from the family of fields L lying between K and N onto the family of closed subgroups of $G = Gal(N/K)$. The inverse map is $H \mapsto N(H)$.*

Proof. See [29] □

Chapter 4

Field Arithmetic

4.1 Introduction

In Chapter 2 we saw that there is a bijective correspondence between covers of $\mathbb{P}^1$ defined over $\mathbb{Q}$ and the field extensions of $\mathbb{Q}(t)$. This serves as a source of inspiration for studying function fields and their extensions. In this chapter we give a short introduction to function fields. We will show that concept of valuation and primes are same. We further show that there is a bijective correspondence between k-rational points and places. The idea is that to each point we can associate a maximal ideal.

We will generalize the notion of absolute values on rational numbers. A famous theorem in number theory states that up to equivalence there are only two non trivial absolute value on $\mathbb{Q}$, either a given absolute value is equivalent to usual real absolute value or p-adic absolute value.

4.2 Transcendental Extensions

A function field K over k is just a finitely generated transcendental extension of k, with transcendence degree one. In this chapter we will study these fields. We will try to generalize the notion of absolute value on $\mathbb{Q}$. Later we will see how concepts of valuations, places, valuation rings are same.

Definition 4.1. Let L/K be any field extension. A subset S of L is called algebraically dependent over K if there exist a natural number n, a nonzero polynomial $f(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ and n distinct elements $s_1, \cdots, s_n$ of S such that $f(s_1, \cdots, s_n) = 0$. If S is not algebraically dependent over K, it is called algebraically independent over K.

Definition 4.2. Let L/K be a field extension. A transcendental basis of L over K is a maximal subset of L algebraically independent over K .

Note that L/K is algebraic if and only if S is the empty set.

Definition 4.3. A field extension L/K is called purely transcendental if $L = K(S)$, where S is a transcendental basis of L over K . In this case, $K(S)$ is called a field of rational functions in $|S|$ variables over K.

Definition 4.4. Let L/K be a field extension. The cardinality of any transcendental basis of L over K is called the transcendental degree of L over K and is denoted by $tr(L/K)$.

Definition 4.5. Let k be an arbitrary field. A field of algebraic functions K over k is a finitely generated field extension of k with transcendence degree $r \geq 1$. K is called a field of algebraic functions of r variables.

Definition 4.6. Let K/k be a function field. The algebraic closure of k in K, that is, the field

$$k^{'} = \{\alpha \in K \mid \alpha \; is \; algebraic \; over \; k\}$$

is called the field of constants of K.

4.3 Valuation, Places and Primes

Definition 4.7. An ordered group G is an abelian group $(G, +)$ with a relation $<$ satisfying, for $a, b, c \in G$:

- $a < b$ or $b < a$ or $a = b$ (trichotomy),
- If $a < b$ and $b < c$ then $a < c$ (transitivity),
- If $a < b$ then $a + c < b + c$ (preservation of the group operation).

Example 4.8. examples of ordered groups are $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ with the sum and the usual order

Definition 4.9. Let K be an arbitrary field. A valuation v over K is a surjective function

$$v : K^{\times} \to G,$$

where G is an ordered group called the value group or valuation group, satisfying

- For $a, b \in K^{\times}$, $v(ab) = v(a) + v(b)$, that is, v is a group epimorphism,

- For $a, b \in K^\times$ such that $a + b \neq 0$, $v(a + b) \geq min\{v(a), v(b)\}$.

We define $v(0) = \infty$, where ∞ is a symbol such that $\infty \notin G$, $a < \infty$ for all $a \in G$ and

$$\infty + \infty = \infty + a = a + \infty = a$$

for all $a \in G$.

Example 4.10. As an example of valuation we have $K = \mathbb{Q}$, $G = \mathbb{Z}$, and $v = v_p$ the p-adic valuation, for p prime. That is, for $x \in \mathbb{Q}^\times$ we write

$$x = p^n \frac{a}{b},\ n \in \mathbb{Z}\ p \nmid b,\ v_p(x) = n$$

Definition 4.11. Consider an arbitrary field K and a valuation of K with values in an ordered group G. Consider,

$$\mathcal{V}_v = \{x \in K \mid v(x) \geq 0\}.$$

Note that $\mathcal{V}_v$ is a ring. Units of $\mathcal{V}_v$ are

$$\mathcal{V}_v^\times = \{x \in K \mid v(x) = 0\}.$$

Definition 4.12. Let

$$\mathcal{P}_v = \{x \in K \mid v(x) > 0\}$$

consist of nonunits of $\mathcal{V}_v$. It's easy to check that it is an ideal of $\mathcal{V}_v$ and in fact it is the unique maximal ideal of $\mathcal{V}_v$. Therefore $\mathcal{V}_v$ is a local ring with unique maximal ideal $\mathcal{P}_v$.

Let's **summarize** what we have developed,
If K is a field and v a valuation over K, then

$$\mathcal{V}_v = \{x \in K \mid v(x) \geq 0\}$$

is a subring of K such that for all $x \in K$, $x \in \mathcal{V}_v$ or $x^{-1} \in \mathcal{V}_v$. In particular, $\mathcal{V}_v$ is a local ring with unique maximal ideal

$$\mathcal{P}_v = \{x \in K \mid v(x) > 0\}.$$

Also we have $quot(\mathcal{V}_v) = K$.

Definition 4.13. Every integral domain A that is not a field and such that each $x \in quot(A)$ satisfies $x \in A$ or $x^{-1} \in A$ is called a valuation ring.

Proposition 4.14. *If A is a valuation ring and $K = quot(A)$, then $K^\times/A^\times$ is an ordered group and the natural projection is a valuation with valuation ring A and value group $K^\times/A^\times$*

The above discussion shows that concepts of valuations and concept of valuation rings is essentially same.

Definition 4.15. Two valuations v_1, v_2 over a field K with value groups G_1, G_2 respectively are equivalent if and only if there exists an order-preserving group isomorphism $\phi : G_1 \to G_2$ such that $\phi v_1 = v_2$. Also, two valuations over a field are equivalent if and only if they have the same valuation ring.

Let's define the concept of place. Let E be an arbitrary field, and let ∞ be a symbol such that $\infty \notin E$. We define the set $E_1 = E \cup \{\infty\}$ with these additional properties,

$$x + \infty = \infty + x = \infty \; \forall x \in E,$$

$$x.\infty = \infty.x \; \forall \; x \in E^\times,$$

and

$$\infty.\infty = \infty.$$

Definition 4.16. A place on a field K is a function $\phi : K \to E \cup \{\infty\}$ (E a field) satisfying:

- $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in K$;
- $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in K$;
- There exists an element $a \in K$ such that $\phi(a) = \infty$;
- There exists an element $b \in K$ such that $\phi(b) = \infty$ and $\phi(b) = 0$.

Definition 4.17. Given a place ϕ we define

$$\mathcal{V}_\phi = \{x \in K \mid \phi(x) \neq \infty\}.$$

We can show that $\mathcal{V}_\phi$ is an integral domain.

Proposition 4.18. *For any $x \in K$ we have $x \in \mathcal{V}_\phi$ or $x^{-1} \in \mathcal{V}_\phi$, in other words $\mathcal{V}_\phi$ is a valuation ring. The maximal ideal $\mathcal{P}$ of $\mathcal{V}_\phi$ is the set of all nonunits of $\mathcal{V}_\phi$, that is $x \in \mathcal{P}$ if $x = 0$ or $x \neq 0$ and $x^{-1} \notin \mathcal{V}_\phi$*

Now we have seen how to obtain valuation ring from a place. For the converse, we have the following proposition.

Proposition 4.19. *Consider a valuation ring $\mathcal{V}$, $\mathcal{P}$ its maximal ideal and $K = quot(\mathcal{V})$. Let E be the field $\mathcal{V}/\mathcal{P}$ and $E_1 = E \cup \{\infty\}$. Let $\phi : K \to E_1$ be given by*

$$\phi(x) = \begin{cases} x \bmod \mathcal{P} & x \in \mathcal{V} \\ \infty & x \notin \mathcal{V} \end{cases}$$

Then ϕ is a place and by definition, we have

$$\mathcal{V}_\phi = \{x \in K \mid \phi(x) \neq \infty\}.$$

Concept of valuation and place are essentially same.

Definition 4.20. Two places ϕ_1 and ϕ_2 over a field K are equivalent if and only if $\mathcal{V}_{\phi_1} = \mathcal{V}_{\phi_2}$.

Proposition 4.21. *Let K be a field and let v be a valuation over K. If the value group G of v is contained in $(\mathbb{R}, +)$, then the valuation defines a function $|\ | : K \to \mathbb{R}$ given by*

$$|x|_v = e^{-v(x)},$$

where $v(0) = \infty$, and $e^{-\infty} = 0$.
The function defined above by the valuation v over K is a non archimedean absolute value that is nontrivial over K.
Let $|\ | : K \to \mathbb{R}$ be a nonarchimedean absolute value over K . Then the function $v_{|\ |}$ defined by

$$v_{|\ |} = -ln|x|,$$

where by definition $-ln|0| = +\infty$ is a valuation with value group contained in $(\mathbb{R}, +)$.

Proof. See [29]. □

By usisng the above proposition, we conclude that notion of nonarchimedean absolute value, valuation with value group contained in $\mathbb{R}$, valuation ring, and place are essentially the same concept.

Definition 4.22. Let K be a field. A prime divisor, or simply a prime, of K is an equivalence class of the set of nontrivial absolute values of K . If the absolute values in the class are archimedean, the prime is called infinite; it is called finite otherwise.

Notation

In the nonarchimedean case, a prime divisor can be considered a place or the maximal ideal of the valuation ring associated with the absolute value.

We say the valuation is discrete if the value group is $\mathbb{Z}$.

4.4 Valuations in Rational Function Fields

in this section, we will characterize all the valuations in Rational function fields. We have followed from [29] and [30].

You can read the full proof here [29].

Theorem 4.23. *The set of valuations v over $k(x)$ such that $v(a) = 0$ for $a \in k^\times$ is exactly*

$$\{v_f \mid f \in k[x] \text{ is a monic irreducible polynomial}\} \cup \{v_\infty\}$$

Furthermore, all of them are pairwise inequivalent and the residue field is a finite extension of k. In case the valuation is v_f , the degree of the residue field is equal to the degree of the polynomial f and in case the valuation is v_∞, the degree of the residue field is equal to one. Finally, all these valuations are discrete.

4.5 Galois Theory and Extension of Places

In this chapter, we will give a brief introduction to Galois theory of function fields. We will talk about extension of places under field extension.

Let $K \subseteq L$ be a field extension and let $\phi_K : K \to E \cup \{\infty\}$ be a place over K. Aim is to show that there exists a place over L, $\phi_L : L \to E_1 \cup \{\infty\}$, such that $E \subset E_1$ and $\phi_L|_K = \phi_K$.

Theorem 4.24. *Let K be a field, and let $\mathcal{V}$ subseteq$K$ be a subring. Let $\phi : \mathcal{V} \to F$ be a ring homomorphism, where F is an algebraically closed field. Then ϕ can be extended to a monomorphism of K to F or to a place of K to $F \cup \{\infty\}$.*

Proof. See [29] □

As a consequence of the above theorem we get the following

Corollary 4.25. If $K \subseteq L$ is a field extension and $\phi : K \to E \cup \{\infty\}$ is a place of K, then ϕ can be extended to a place of L

We will use the following notation from now on,

Notation: If v is a valuation in K, $\mathcal{P}$ the associated maximal ideal, and $\mathcal{V}_{\mathcal{P}}$ the valuation ring, we will write $k(\mathcal{P})$ to denote the associated residue field.
Let K/k be a function field and let $\mathcal{P}$ be a maximal ideal associated to a place of K. Then $f_{\mathcal{P}} = d_K(\mathcal{P}) = [k(\mathcal{P}) : k] < \infty$.

Definition 4.26. The number $f_{\mathcal{P}} = d_K(\mathcal{P}) = [k(\mathcal{P}) : k]$ is called the degree of the place .

Definition 4.27. Given a function field K , the free abelian group generated by all the places is called the divisor group of K and will be denoted by D_K . The places are also called prime divisors.

Definition 4.28. Let K/k and L/L be two function fields. We say that L is an extension of K if $K \subseteq L$ and $l \cap K = k$.

Definition 4.29. Let L be an extension of K. A place $\mathcal{P}$ of L is called variable or trivial over K if $v_{\mathcal{P}}(x) = 0$ for all $x \in K^{\times}$. This is equivalent to saying that $K \subseteq \mathcal{V}_{\mathcal{P}}$.

Definition 4.30. If $\mathcal{P}$ is nontrivial over K, then $v_{\mathcal{P}} \restriction_K$ defines a nontrivial valuation in K . In other words, there exists a prime divisor $\mathscr{P}$ of K such that $v_{\mathcal{P}} \restriction_K \simeq v_{\mathscr{P}}$

Definition 4.31. When $\mathcal{P}$ is nontrivial over K and hence $v_{\mathcal{P}} \restriction_K \simeq v_{\mathscr{P}}$, we say that $\mathcal{P}$ is above $\mathscr{P}$ or that $\mathcal{P}$ divides $\mathscr{P}$ and this is denoted by $\mathcal{P}|\mathscr{P}$ or $\mathcal{P} \restriction_K = \mathscr{P}$

Definition 4.32. Consider an extension L of K, $\mathcal{P}$ a nontrivial place of L over K and $\mathcal{P} \restriction_K = \mathscr{P}$. Since the valuation are discrete, $v_{\mathcal{P}}$ and $v_{\mathscr{P}}$ are surjective but on the other hand $v_{\mathcal{P}} \restriction_K \simeq v_{\mathscr{P}}$ is not surjective in general, so $v_{\mathcal{P}}(K^{\times}) = e\mathbb{Z}$ for some $e \geq 1$. Thus we have $v_{\mathcal{P}}(x) = ev_{\mathscr{P}}(x)$ for all $x \in K$. The number e obtained above is called the ramification index of $\mathcal{P}$ over $\mathscr{P}$ and it is denoted by $e = e(\mathcal{P} \restriction_{\mathscr{P}})$

Definition 4.33. Let L/K be an extension of function fields, and let $\mathcal{P}$ be a place of L over a place $\mathscr{P}$ of K. We define the relative degree of $\mathcal{P}$ over $\mathscr{P}$ by

$$d_{L/K}(\mathcal{P}/\mathscr{P}) = [l(\mathcal{P}) : k(\mathscr{P})]$$

Theorem 4.34. *Let L/l be an algebraic extension of K/k. given a place $\mathscr{P}$ of K, the number of places of L over $\mathscr{P}$ is finite and nonzero.*

The central result of this section is

Theorem 4.35. *Let L/l be an extension of K/k. let $\mathscr{P}$ be a place of K and let $\mathcal{P}_1, \cdots, \mathcal{P}_h$ be the places of L over $\mathscr{P}$. Then*

$$[L : K] = \sum_{i=1}^{h} e(\mathcal{P}_i \restriction_{\mathscr{P}}) d(\mathcal{P}_i \restriction_{\mathscr{P}})$$

For proof, see [29], [30], [31]

Definition 4.36. Let L/l and M/m be two extensions of K/k and let $\sigma : L \to M$ be a field isomorphism such that $\sigma(l) = m$ and $\sigma \restriction_K = Id_K$. Then for a place $\mathcal{P}$ of L we define the place $\sigma(\mathcal{P})$ of M by means of the valuation $v_{\sigma\mathcal{P}}$ defined by $v_{\sigma\mathcal{P}}(x) = v_{\mathcal{P}}(\sigma^{-1}x)$ for all $x \in M$.

Proposition 4.37. *Let L/l be a normal finite extension of K/k. Let $\mathcal{P}$ be a place of L over the place $\mathscr{P}$ of K. Let $\mathcal{P}'$ be any other place of L over $\mathscr{P}$. Then there exists $\sigma \in G = Aut(L/K)$ such that $\sigma(\mathcal{P}) = \mathcal{P}'$. In other words, G acts transitively on the places of L that divide a given place of K.*

Definition 4.38. Let L/l be a finite normal extension of K/k. If $\mathcal{P}$ is a place of L over $\mathscr{P}$ of K, we define the decomposition group of $\mathcal{P}$ by

$$D(\mathcal{P} \restriction_{\mathscr{P}}) = \{\sigma \in Aut(L/K) \mid \sigma(\mathcal{P}) = \mathcal{P}\}$$

Definition 4.39. In any extension L/l of K/k, a place $\mathcal{P}$ of L is called ramified if $e = e_{L/K}(\mathcal{P}/\mathscr{P}) > 1$. Also we say that $\mathscr{P}$ is ramified in L/K if every prime lying over it is ramified.

Part II

Central Theory

Chapter 5

Constructing Galois Extension of $\mathbb{Q}(T)$: The Property Gal_T

5.1 Introduction

In this chapter we describe the problem we are primarily interested in. Given a finite group G, our goal is to construct Galois extension of rational function field $\mathbb{Q}(t)$ with the Galois group G. In the chapter on algebraic geometry we saw that there is a close connection between smooth curves and it's function field. So the problem of constructing Galois extension of $\mathbb{Q}(t)$ can be rephrased in language of covering space theory.

This problem is also known as Inverse Galois Problem. Classical Inverse Galois problem is concerned with realization of groups as Galois group over $\mathbb{Q}$.

5.2 Problem

Given a finite group G, can we construct finite Galois (ramified) extension of $\mathbb{Q}(t)$ with group G. Using the bijective correspondence between smooth curves and function fields, we can **rephrase** the problem in geometric terms.

Let E be a finite Galois Extension of $\mathbb{Q}(T)$ with group G which is *regular*, i.e. $\overline{\mathbb{Q}} \cap E = \mathbb{Q}$. Geometrically E can be viewed as the function field of a smooth projective curve C which is absolutely irreducible over $\mathbb{Q}$.

The inclusion

$$\mathbb{Q}(T) \overset{i}{\hookrightarrow} E$$

corresponds to a (ramified) Galois covering

$$C \to \mathbb{P}^1$$

define over $\mathbb{Q}$ with group G. See Chapter 2.

Definition 5.1 (The property Gal_T)**.** Let us say that G has property Gal_T if there is a regular G-covering $C \to \mathbb{P}^1$ as above.

Remark If a regular G-covering exists over $\mathbb{P}^n, n \geq 1$, then such a covering also exist over $\mathbb{P}^1$, by Bertini's theorem. See [15].

5.3 Historical Remarks

- Hilbert (1892) first studied this problem systematically. Using the irreducibility theorem, he could show that over $\mathbb{Q}$ and more generally over every field finitely generated over $\mathbb{Q}$, there exist infinitely many Galois extension with S_n and A_n.
- Work of E. Noether (1918), Scholz (1937) contributed a lot towards this problem. Then came the celebrated theorem by Safarevic (1954), He solved the Inverse Galois Problem over arbitrary number fields for all solvable groups.
- The next set of results were furnished by the works of Shih (1974), Fried (1977), Belyi (1979), Matzat(1979, 1984) and Thompson(1984). Thompson introduced the concept of Rigidity and Rationality of finite groups. We have extensively used this idea to realize many finite groups as Galois group over $\mathbb{Q}(t)$.

5.4 Current Status Of The Problem

As of now, this problem is still open. Lot of work has been done in the last $10 - 20$ years. Problem is solved over $\mathbb{C}(t)$. Krull and Neukrich in (1971) showed that **Every finite group occur as Galois group over** $\mathbb{R}(t)$. In 1984, D. Harbater solved the **Inverse Galois Problem over** $\bar{\mathbb{F}}_p(t)$. In 1987, David Harbater solved the **Inverse Galois Problem over** $\mathbb{Q}_p(t)$.

Chapter 6

Noether's Trick: Action of Group on Varieties

6.1 A Little Diversion : Action of Group on Varieties

We know about concept of group acting on a set. We defined the quotient space corresponding to a group action to be the set of orbits. Now what happens if our group G acts on a variety say X. We can ask several questions, First of all Is X/G a variety ? Are the G-invariant elements finitely generated ? The branch of mathematics which studies these topics is known as **Geometric Invariant Theory**. Interested readers can refer [8], [9].

Theorem 6.1. *Let A be a finitely generated algebra over k and G a finite group of automorphisms of A. Assume that the order n of G is not divisible by char k. Write A^G for the subalgebra of elements $a \in A$ such that $g(a) = a$ for all $g \in G$. Then A^G is finitely generated as an algebra over k.*

We will need knowledge of commutative algebra. See Chapter 5 and Chapter 7 of [55] for more details.

Proposition 6.2. *The following are equivalent:*

- *$x \in B$ is integral over A*
- *$A[x]$ is a finitely generated A-module;*

- *$A[x]$ is contained in a subring C of B such that C is a finitely generated A-module.*

Proof. See Proposition 5.1, [55]. □

Let B be a ring and A be a subring of B. Both A and B are assumed to be commutative rings with unity. We say that $x \in B$ is **integral over** A, if x is a root of a monic polynomial with coefficient in A.

Proposition 6.3. *(Artin-Tate, 1951) Let $A \subseteq B \subseteq C$ be rings. Suppose that A is Noetherian, C is finitely generated as an A algebra and C is either finitely generated as a B-module or C is integral over B. Then B is finitely generated as an A-algebra.*

Proof. For original proof, See [55], Proposition 7.9 □

Remark: The lemma was introduced by E. Artin and J. Tate in 1951. [56].

Proposition 6.4. *The ring extension $A^G \subset A$ is integral*

Proof. Take $a \in A$, we want to construct a polynomial with coefficients in A^G. Consider the polynomial

$$q(t) = \prod_{h \in G} (t - h.a).$$

Observe that $q(a) = 0$. Consider the action of G pn A and extend it to a action of G on $A[t]$ by setting the rule that G acts trivially on t. Hence

$$g.q(t) = \prod_{h \in G} (t - g.(h.a)) = \prod_{h \in G} (t - h.a) = q(t).$$

We see that coefficient of $q(t)$ are invariant under the action of G. hence they belong to A^G. We conclude that a in integral over A^G. □

Proof. (Proof of Theorem 6.1) Consider the chain of extensions

$$k \subset A^G \subset A.$$

Using the above proposition and Artin-Tate Lemma. We conclude our result. □

Theorem 6.5. *An algebra A over a field k is isomorphic to a coordinate ring $k[X]$ of some closed subset X if and only if A has no nilpotents (that is $f^n = 0$ implies that $f = 0$ for $f \in A$) and is finitely generated as an algebra over k.*

Proof. See Page 30, Chapter I, [54] □

The following discussion is taken from page 30**, Example** 1.21 **[54]**. Let X be a closed set and G a finite group of automorphisms of X. Suppose that the characteristic of the field k does not divide the order N of G. Let $A = k[X]$, and let A^G be the subalgebra of A as above, that is

$$A^G = \{f \in A \mid g^*(f) \ = \ f \text{ for all } g \in G\}.$$

According to above Theorem 6.1, the algebra A^G is finitely generated over k. From the Theorem 6.5, there exists a closed set Y such that $A^G \simeq k[Y]$, and a regular map $\phi : X \to Y$ such that $\phi^*(k[Y]) = A^G$. This set Y is called the **quotient variety or quotient space** of X by the action of G, and is written X/G.

6.2 Main Strategy/Idea:The Noether's Trick

Emmy Noether proposed the **following strategy** to tackle the inverse Galois problem. (Source: See Chapter I, [1].) It first appeared here, [57] in 1918.

Proposition 6.6. *We take a finite group G, by Cayley Theorem, we know that every finite group is isomorphic to a subgroup of symmetric group. So we embed G in S_n. We define a G-action on the field $\mathbb{Q}(X_1, \ldots X_n) = \mathbb{Q}(\underline{X})$. Let E be the fixed field under this action. Then $\mathbb{Q}(\underline{X})$ is a Galois extension of E with Galois group G. In **geometric terms**, the extension $\mathbb{Q}(\underline{X})$ of E corresponds to the projection of varieties:*

$$\pi : \mathbb{A}^n \to \mathbb{A}^n/G$$

where $\mathbb{A}^n$ is affine n-space over $\mathbb{Q}$. Let P be a $\mathbb{Q}$-rational point of A_n/G for which π is unramified, and lift it to $Q \in \mathbb{A}^n(\overline{\mathbb{Q}})$.
$Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on Q, Under this action the conjugates of Q are precisely sQ. Here s belongs to decomposition group at Q. We denote it by H_Q. If $H_Q = G$, then Q generates a field extension of $\mathbb{Q}$ with Galois group G.

See [57] for proof.

Definition 6.7. A variety is said to be rational over $\mathbb{Q}$ (or $\mathbb{Q}$-rational) if it is birationally isomorphic over $\mathbb{Q}$ to the affine space $\mathbb{A}^n$ (equivalently to projective space)

for some n, or equivalently, if its function field is isomorphic to $\mathbb{Q}(T_1, \ldots T_n)$, where the T_i are indeterminate.

Hilbert in 1892, proved the below theorem. Using this theorem, it is enough to show that variety is $\mathbb{Q}$ rational.

Theorem 6.8 (Hilbert)**.** *If $\mathbb{A}^n/G$ is $\mathbb{Q}$-rational, then there are infinitely many points P, Q as above such that $H_Q = G$.*

Proof. See [58] □

In the Chapter 8 we will apply this trick to various finite groups.

Chapter 7

Rigidity and Rationality Property

7.1 Introduction

In this chapter, we will develop the basic theory of rigidity and rationality of finite groups. The term rigidity was coined by Thompson. It gives a purely group-theoretic conditions for occurrence of finite groups as Galois group over $\mathbb{Q}(t)$. In this chapter, we will prove the rigidity criterion. We will see how it can be applied to symmetric group and alternating groups in the Chapter 9.

We will start with some classical results, we have used them while developing the theory of rigidity. We start with a theorem of Grothendieck. We will use it as a result. For proof, look [3]. Notation used in this theorem will be used throughout this chapter.

All the definitions, theorems and propositions in this chapter are taken from [3].

Theorem 7.1. *(Grothendieck (1971)). Let $\bar{k}$ be an algebraically closed subfield of $\mathbb{C}$, $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$, $\mathcal{X}(\bar{k}) = \mathbb{P}^1(\bar{k})$, $\mathcal{S} = \{\mathcal{P}_1, \cdots, \mathcal{P}_s\}$ a finite subset of $\mathcal{X}(\bar{k})$, $\mathbb{S} = \{\mathcal{B}_1, \cdots, \mathcal{B}_s\}$ the set of valuations ideals of $\bar{k}(X)$ corresponding to $\mathcal{S}$, and $\bar{M}_{\mathbb{S}}$ the maximal algebraic extension field of $\bar{k}(\mathcal{X}) \simeq \bar{k}(t)$ unramified outside $\mathbb{S}$. then the algebraic fundamental group $Gal(\bar{M}_{\mathbb{S}}/\bar{k}(\mathcal{X}))$ has the form*

$$\langle \gamma_1, \gamma_2, \cdots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle^{\wedge}.$$

More over the elements γ_i are generators of inertia group of valuation ideal $\hat{\mathcal{B}}_i$ of $\bar{M}_{\mathbb{S}}/\bar{k}$ lying over $\mathcal{B}_i$;

$$I(\hat{\mathcal{B}}_i/\mathcal{B}_i) = \langle \gamma_i \rangle^{\wedge}.$$

Notation: From now on, $\bar{k}$, we will always mean the field of all algebraic numbers

$\bar{\mathbb{Q}}$. We will denote the group $Gal(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(\mathcal{X}))$ by Γ_s. We use another classical result known as Splitting Theorem. For the proof, kindly see [3].

Theorem 7.2. *(Splitting Theorem) Let $\bar{k}$ be as above, and assume that $\mathbb{S}$ is invariant under the absolute Galois group $\Gamma_{\mathbb{Q}}$, then $\bar{M}_{\mathbb{S}}$ is Galois over $\mathbb{Q}(t)$ and we have*

$$Gal(\bar{M}_{\mathbb{S}}/\mathbb{Q}(t)) \simeq \Gamma_s \rtimes \Gamma_{\mathbb{Q}}.$$

7.2 Action via Cyclotomic Character

Take any $\delta \in \Gamma_{\mathbb{Q}}$. It sends the n-th root of unity $\zeta_n := e^{2\pi i/n}$ to a primitive power $\zeta_n^{c_n(\delta)}$, with $c_n(\delta) \in (\mathbb{Z}/n\mathbb{Z})^\times$. This defines a continuous homomorphism

$$c : \Gamma_{\mathbb{Q}} \longrightarrow \hat{\mathbb{Z}}^\times,$$

$$\delta \mapsto c(\delta) := (c_n(\delta))_{n\in\mathbb{N}}$$

where $\hat{\mathbb{Z}}^\times$ denote the non units in profinite completion of integers.

Definition 7.3. The homomorphism c is called the cyclotomic character of $\Gamma_{\mathbb{Q}}$

In the statement of Splitting theorem, we assumed that the set $\mathbb{S}$ of prime ideals ramified in $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ is invariant under $Gal(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$. If we keep that assumption, then we get the following:

Definition 7.4. The elements $\mathcal{B}_1, \cdots, \mathcal{B}_s$ of $\mathbb{S}$ are permuted by absolute Galois group of $\mathbb{Q}$. The action defined by

$$\delta : \mathbb{S} \to \mathbb{S},$$

$$\mathcal{B}_i \to \mathcal{B}_{(i)\delta} := \mathcal{B}_i^\delta.$$

hence we get a permutation representation of $\Gamma_{\mathbb{Q}}$ on $\mathbb{S}$. In other, this induces a permutation representation into the group S_s, symmetric group on s letters.

We will denote by Γ the group $\Gamma_s \rtimes \Gamma_{\mathbb{Q}}$. See Theorem 7.2. Let Γ_s denote the Galois group of the maximal algebraic Galois extension $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}(t)}$ unramified outside $\mathbb{S}$. See Theorem 7.1

Proposition 7.5. *Each element $\delta \in Gal(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)) \cong \Gamma_{\mathbb{Q}}$ may be lifted uniquely to an automorphism $\tilde{\delta} \in \Gamma$ inside a given closed complement of Γ_s, It permutes the*

closed subgroups of Γ_s. *We can use the Galois correspondence to conclude that it also permutes the intermediate fields of* $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$. *Now let* Ψ *be an open normal subgroup of* Γ_s *with fixed field* $\bar{N}$ *and*

$$G := Gal(\bar{N}/\bar{\mathbb{Q}}(t)) = \Gamma_s/\Psi.$$

Both the normal subgroup $\Psi^{\tilde{\delta}}$ *and the field* $\bar{N}^{\tilde{\delta}}$ *are independent of the particular lifting* $\tilde{\delta}$ *of* δ, *we denote it by* Ψ_δ, $\bar{N}^\delta$ *respectively.*

Proof. See [3] □

7.3 Rigidity Theorem

Definition 7.6. Let $\sigma = (\sigma_1, ..., \sigma_s) \in G^s$ be the image of $\gamma = (\gamma_1, ..., \gamma_s)$ under the natural homomorphism $\psi : \Gamma_s \to G$. Then σ is a generating system of G satisfying the product relation $\sigma_1 ... \sigma_s = 1$. We call such a system a generating s-system of G. The set of all generating s-systems of G is denoted by

$$\Sigma_S(G) := \{\sigma \in G^s | \langle\sigma\rangle = G, \sigma_1 ... \sigma_s = 1\}.$$

We will use this fact that, if we take $\sigma \in \Sigma_s(G)$ there exists precisely one (continuous) $\psi_\sigma \in Hom(\Gamma_s, G)$ with $\psi_\sigma(\gamma) = \sigma$, the kernel of which constitutes a closed subgroup of Γ_s denoted by $ker(\sigma)$.

Proposition 7.7. *There is a well defined action of* $\Gamma_{\mathbb{Q}}$ *on* $\Sigma_s(G)/Inn(G)$:

$$\Sigma_s(G)/Inn(G) \times \Gamma_{\mathbb{Q}} \to \Sigma_s(G)/Inn(G), \quad ([\sigma], \delta) \to [\sigma]^{\delta^{-1}} := [\sigma^{\tilde{\delta}^{-1}}].$$

where $\sigma^{\tilde{\delta}} := \psi_\sigma(\gamma^{\tilde{\delta}})$

We introduced the action of $\Gamma_{\mathbb{Q}}$ on $\Sigma_s(G)/Inn(G)$ above. Let's fix the **notation** $\Delta := Gal(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$

Proposition 7.8. Δ *acts on the classes of generating systems via the cyclotomic character. More precisely, we have Let* $\delta \in Gal(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$, $[\sigma] \in \Sigma_s(G)/Inn(G)$, *and denote by* C_i, *resp.* C_i^δ, *the conjugacy class of the* i*-th component of a representative in* $[\sigma]$, *resp.* $[\sigma]^\delta$. *Then we have*

$$C_i^{\delta} = C_{(i)\delta}^{c(\delta)}.$$

We are leaving the proof. See *page 27*, [3], for in-depth analysis.

Proposition 7.9. *Let $C = (C_1, ..., C_s) \in Cl(G)^s$ be a class vector of G. Then the fixed field $\mathbb{Q}_C := \bar{\mathbb{Q}}^{\Delta_c}$ is an abelian number field of degree*

$$[\mathbb{Q}_C : \mathbb{Q}] = d(C).$$

It is generated over $\mathbb{Q}$ by the values of the complex irreducible characters of G on the classes $C_1, ..., C_s$:

$$\mathbb{Q}_C = \mathbb{Q}(\{\chi(C_i) | \chi \in Irr(G), i = 1, ..., s\}).$$

Proof. Look [3] □

We will use the above proposition to set up definitions which will form the base of this chapter.

Definition 7.10. A class vector $C \in Cl(G)^s$ will be called **rational** if $d(C) = 1$ and hence $\mathbb{Q}_C = \mathbb{Q}$.

For $C = (C_1, ..., C_s) \in Cl(G)_s$ let

$$\Sigma(C) := \{\sigma \in \Sigma_s(G) | \sigma_i \in C_i\}$$

We denote by

$$l(C) := |\Sigma(C)/Inn(G)|$$

the number of generating s-system classes $[\sigma]$ of G with components $\sigma_i \in C_i$.
Thompson (1984a),

Definition 7.11. A class vector C is called rigid if $l(C) = 1$. It is called rationally rigid if moreover C is rational.

We directly state the central result of this. We are omitting the proof. It can be found in any standard text on Inverse Galois theory like [3]. This result is due to

Theorem 7.12. *(Basic Rigidity Theorem). Let G be a finite group in which the center has a complement, and $C \in Cl(G)^s$ a rigid class vector of G. Then for any arbitrarily chosen set $\mathbb{S}$ of s prime divisors $\beta_i \in \mathbb{P}(\mathbb{Q}_C(t)/\mathbb{Q}_C)$ of degree one there exists a Galois extension $N/\mathbb{Q}_C(t)$ unramified outside $\mathbb{S}$ with*

$$Gal(N/\mathbb{Q}_C(t)) \cong G$$

such that the inertia groups over the β_i are generated by elements $\sigma_i \in C_i$.

If the class vector is rationally rigid, we have $\mathbb{Q}_C = \mathbb{Q}$.

It is possible to obtain Galois extension over $\mathbb{Q}(t)$ even if the class vector is not rational. We will fix some notations and introduce some basic concepts and then we will state a stronger version of Theorem 7.12.

For $C \in Cl(G)^s$ let

$$Sym(C) := \{\omega \in S_s | C^\omega \in C^*\}$$

with $(C_1, ..., C_s)^\omega := (C_{1^\omega}, ..., C_{s^\omega})$ be the full symmetry group of C and $V \leq Sym(C)$ a symmetry group of C. For such a V let

$$C^V := \{C^\omega | \omega \in V\} \subseteq C^*.$$

Furthermore,

Definition 7.13.

$$d^V(C) := |C^*|/|C^V|$$

is called the V-**symmetrized irrationality degree** of C.

Using the earlier definitions we have $d^V(C) = 1$ precisely when $C^V = C^*$. In this situation we call class vector C is V-symmetric. We denote

$$\Delta_C^V := \{\delta \in \delta | C^{c(\delta)} \in C^V\}$$

for the stabilizer of C^V in Δ under its action via the cyclotomic character. Analogous to the previous situation where there was no choice of ramification points, we have the following:

Proposition 7.14. *The fixed field $\mathbb{Q}_C^V := \bar{\mathbb{Q}}^{\Delta_C^V}$ of Δ_C^V is an abelian number field contained in $\mathbb{Q}_C$, of degree*

$$[\mathbb{Q}_C^V : \mathbb{Q}] = d^V(C).$$

In particular we have $\mathbb{Q}_C^V = \mathbb{Q}$ if and only if the class vector C is V-symmetric.

Using the ideas developed above we state a more stronger version of rigidity theorem 7.12. We will call it Strong Rigidity Theorem. See [3] for proof of the theorem.

Theorem 7.15. *(Strong Rigidity Theorem). Let G be a finite group whose center possesses a complement and with a rigid class vector $C \in C1(G)^s$. Furthermore let V be a symmetry group of C with the property that for each $\delta \in \Delta_C^V$ there exists precisely one $\omega \in V$ with $C^{c(\delta)} = C^{\omega}$. Then there exists a geometric Galois extension $N/\mathbb{Q}_C^V(t)$ with*

$$Gal(N/\mathbb{Q}_C^V(t)) \cong G.$$

If moreover C is V-symmetric, then we have $\mathbb{Q}_C^V = \mathbb{Q}$.

7.4 Rigidity Criterion

Our aim in this section is to prove a group theoretic criterion to check whether a given class vector is rigid or not. This section is very important and forms the heart of the thesis. The formula proved in this section will be used to show that many sporadic groups occurs as Galois group over $\mathbb{Q}(t)$. We first enlarge the set $\Sigma(C)$.

$$\bar{\Sigma}(C) := \{\sigma \in G^s | \sigma_i \in C_i, \sigma_1 ... \sigma_s = 1\}$$

of not necessarily generating s-systems. The group G also acts on this set by conjugation in the components.

Definition 7.16. The quotient

$$n(C) := |\bar{\Sigma}(C)|/|Inn(G)|$$

constitutes an estimate for the number of orbits under this action; it will be called the normalized structure constant of C.

Using the class equation for the action of G on $\bar{\Sigma}(C)$, normalized structure constant of a class vector $C \in C1(G)^s$ of a finite group G is given by

$$n(C) = \sum_{[\sigma] \in \bar{\Sigma}(C)/Inn(G)} \frac{|\mathcal{Z}(G)|}{|\mathcal{C}_G(\langle \sigma_1, ..., \sigma_s \rangle)|}.$$

Using the above formula we can readily conclude that, for a class vector $C \in Cl(G)^s$ of a finite group G we have $l(C) \leq n(C)$ and equality holds if and only if $\bar{\Sigma}(C) = \Sigma(C)$.

The most interesting part is yet to come. The normalize structure constant of C may be computed directly from the values complex irreducible

character values of G. Hence we can determine the value of $n(C)$ by just using the character tables. As you will see in the next chapters, we have implemented this formula in GAP to do the computations efficiently.

We have taken the proof from the book *Inverse Galois Theory* Malle and Matzat. See [3]. For an alternative approach you can look of the book by J. P. Serre titled *Topics in Galois Theory*. See [1].

Theorem 7.17. *Let $C = (C_1, ..., C_s) \in C1(G)^s$ be a class vector of a finite group G, where $s \geq 2$. Then we have*

$$n(C) = |\mathcal{Z}(G)| \sum_{\chi \in Irr(G)} \frac{|G|^{s-2}}{\chi(1)^{s-2}} \prod_{i=1}^{s} \frac{\chi(\sigma_i)}{|\mathcal{C}_G(\sigma_i)|} \quad , \sigma_i \in C_i.$$

Proof. For $\chi \in Irr(G)$ let $R : G \to GL_n(\mathbb{C})$ denote a corresponding matrix representation. By the Schur's Lemma for each $\sigma \in G$ there exists an $\omega(\sigma) \in \mathbb{C}$ satisfying

$$\frac{1}{|G|} \sum_{\rho \in G} R(\sigma^\rho) = \omega(\sigma) I_n, \qquad \text{where } \omega(\sigma) = \frac{\chi(\sigma)}{\chi(1)},$$

as follows from the evaluation of traces. Hence for all pairs $(\sigma, \tau) \in G^2$ we have

$$\frac{1}{|G|} \sum_{\rho \in G} R(\sigma^\rho \tau) = \frac{\chi(\sigma)}{\chi(1)} R(\tau).$$

Induction on s now yields

$$\frac{1}{|G|^s} \sum_{\rho \in G^s} R(\sigma_1^{\rho_1} ... \sigma_s^{\rho_s} \tau) = \frac{\chi(\sigma_1) ... \chi(\sigma_s)}{\chi(1)^s} R(\tau),$$

and evaluation of traces for $\tau = 1$ then leads to

$$\frac{1}{|G|^s} \sum_{\rho \in G^s} \chi(\sigma_1^{\rho_1} ... \sigma_s^{\rho_s}) = \frac{\chi(\sigma_1) ... \chi(\sigma_s)}{\chi(1)^{s-1}},$$

Now let

$$\epsilon := |G| \sum_{\chi \in Irr(G)} \chi(1) \chi$$

be the characteristic function of the identity in G. Accordingly, multiplying the previous equation by $\chi(1)|G|^{s-1}$ and summing over $\chi \in Irr(G)$ we hence obtain

$$m(C) := \sum_{\rho \in G^s} \epsilon(\sigma_1^{\rho_1} ... \sigma_s^{\rho_s}) = |G|^{s-1} \sum_{\chi \in Irr(G)} \frac{\chi(\sigma_1) ... \chi(\sigma_s)}{\chi(1)^{s-2}}.$$

Here $m(C)$ counts the number of solutions $\rho \in G^s$ of $\sigma_1^{\rho_1} ... \sigma_s^{\rho_s} = 1$.

$$n(C) = \frac{1}{|Inn(G)|}|\{\sigma \in C | \sigma_1 ... \sigma_s = 1\}|$$

can be expressed as

$$n(C) = \frac{m(C)}{|Inn(G)|} \prod_{i=1}^{s} |\mathcal{C}_G(\sigma_i)|^{-1}.$$

□

A frequently used criterion for rigidity is: A class vector $C \in C1(G)^s$ of a finite group G is rigid, if the following two conditions are satisfied:

1. $G = \langle \sigma_1, ..., \sigma_s \rangle$ for some $\sigma_i \in C_i$ with $\sigma_1 ... \sigma_s = 1$,
2. $\Sigma_{\chi \in Irr(G)} \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^{s-2}} = \frac{|\mathcal{C}_G(\sigma_1)| ... |\mathcal{C}_G(\sigma_s)|}{|G|^{s-2} |\mathcal{Z}(G)|}$.

We have a group criterion to check whether a given class vector of finite group is rigid. Basic Rigidity Theorem (See Theorem 7.12) is due to joint efforts Belyi, Matzat, Thompson and Fried. The result proved above (see Theorem 7.17) is very helpful because, in general it is not easy to check whether a given tuple of conjugacy classes of a finite group is rigid. See the Chapter 9 and Chapter 11 for application of rigidity to finite groups.

Part III

Application

Chapter 8

Application of Noether's Trick

8.1 Introduction

In this chapter, we will see how the theory developed in chapter on Noether's Trick can be applied to various finite groups. The idea is simple, we will try to show that the quotient variety $\mathbb{A}^n/G$ is $\mathbb{Q}$ rational. We first consider the case of Symmetric group.

8.2 Symmetric Groups

Let S_n, be the symmetric group on n-letters. Let's revisit the Fundamental theorem of Elementary Symmetric Function.

The elementary symmetric polynomials in n variables $X_1, \ldots, X_n$, written $e_k(X_1, \ldots, X_n)$ for $k = 0, 1, \ldots, n$ are defined by

$$\begin{aligned} e_0(X_1, X_2, \ldots, X_n) &= 1, \\ e_1(X_1, X_2, \ldots, X_n) &= \textstyle\sum_{1 \le j \le n} X_j, \\ e_2(X_1, X_2, \ldots, X_n) &= \textstyle\sum_{1 \le j < k \le n} X_j X_k, \\ e_3(X_1, X_2, \ldots, X_n) &= \textstyle\sum_{1 \le j < k < l \le n} X_j X_k X_l, \end{aligned}$$

and so forth, ending with

$$e_n(X_1, X_2, \ldots, X_n) = X_1 X_2 \cdots X_n.$$

In general, for $k \geq 0$ we define

$$e_k(X_1, \ldots, X_n) = \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} X_{j_1} \cdots X_{j_k}$$

Fundamental Theorem of Elementary Symmetric Functions

Theorem 8.1. *For any commutative ring A, denote the ring of symmetric polynomials in the variables $X_1, \ldots, X_n$ with coefficients in A by $A[X_1, \ldots, X_n]^{S_n}$. $A[X_1, \ldots, X_n]^{S_n}$ is a polynomial ring in the n elementary symmetric polynomials $e_k(X_1, \ldots, X_n)$ for $k = 1, \ldots, n$.*

(Note that e_0 is not among these polynomials; since $e_0 = 1$ it cannot be member of any set of algebraically independent elements.)

It implies that for every symmetric polynomial $P(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]^{S_n}$ we have

$$P(X_1, \ldots, X_n) = Q(e_1(X_1, \ldots, X_n), \ldots, e_n(X_1, \ldots, X_n))$$

for some polynomial $Q \in A[Y_1, \ldots, Y_n]$. In other words $A[X_1, \ldots, X_n]^{S_n}$ is isomorphic to the polynomial ring $A[Y_1, \ldots, Y_n]$ through an isomorphism that sends Y_k to $e_k(X_1, \ldots, X_n)$ for $k = 1, \ldots, n$.

Construction

By Fundamental Theorem above and using the theory developed in **Chapter 6**, we conclude that Symmetric group acts on affine space $\mathbb{A}^n$ with quotient space $\mathbb{A}^n$, affine space of same dimension. The quotient is $\mathbb{Q}$-rational.
Hence S_n has property Gal_T.

8.3 Abelian Groups

Definition 8.2 (Permutation torus)**.** A torus defined over $\mathbb{Q}$ is said to be a *"permutation torus" if its character group has a $\mathbb{Z}$-basis which is stable under the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, or equivalently if it can be expressed as a product of tori of the form $\mathrm{Res}_{K_i/\mathbb{Q}}\mathbb{G}_m$, where the K_i are finite extensions of $\mathbb{Q}$. A permutation torus is clearly rational over $\mathbb{Q}$.*

Now, let A be a finite abelian group. We have a beautiful result which says that any abelian group can be embedded in a algebraic torus, see [1].

Theorem 8.3. *There exists a torus S over $\mathbb{Q}$, and an embedding of A in $S(\mathbb{Q})$, such that the quotient $S' = S/A$ is a permutation torus and S' is a $\mathbb{Q}$-rational variety.*

Proof. For proof see [1]. □

Using the above theorem, we are done.

8.4 Dihedral Groups

Theorem 8.4. *Let G be a finite group having property Gal_T, and let M be a finite abelian group with G-action. Then the semi-direct product $G' = M \cdot G$ also has property Gal_T.*

Proof. See [1], Chapter 4. □

Let D_n denote the dihedral group. It has following presentation,

$$D_n = \langle a, b \mid a^n = e,\ b^2 = e,\ b^{-1}ab = a^{-1} \rangle$$

Let C_n denote the cyclic group of order n, generated by a, and let C_2 denote the cyclic group of order 2 generated by b.

D_n is semidirect product of C_2 and C_n and C_2 acts on C_n by inversion. Hence by the above theorem we conclude that D_n has the property Gal_T.

8.5 Double Group Trick and Alternating Group A_n

.

Theorem 8.5. *(**Double Group trick**) Let G be the Galois group of a regular extension $K/k(T)$, ramified at most at three places which are rational over k, and let H be a subgroup of G of index 2. Then the fixed field K_1 of H is rational.*

Proof. In the proof we will use the Riemann-Hurwitz formula. If we have a finite degree N map of curves $Y \to X$ over a number field of genus g_Y, g_X respectively, then we have:

$$2g_Y - 2 = N(2g_X - 2) + \sum_{P \in Y} (e_P - 1)$$

where e_P is the ramification index at P.

We have already seen the bijective correspondence between smooth curves and function fields. Using it in our case, we have $X = \mathbb{P}^1_k$ and the function field corresponding to it is $k(T)$. It is given that H has index 2 in G. So we have a curve Y of degree 2 over X such that fixed field of H is the function field of Y. As given in the statement of theorem, it is ramified at most above 3 points. Since the map is of degree 2, the ramification indices are all either 1 or 2.

$$2g_Y - 2 = 2 \cdot (-2) + (0 \text{ or } 1) + (0 \text{ or } 1) + (0 \text{ or } 1)$$

since g_Y is a positive integer, we get that $g_Y = 0$. It also shows that Y is ramified only at two points. Since genus is zero and curve has rational point. The lemma follows. See [59], Theorem A.4.3.1, page 75 and page 144, Chapter 5, Proposition 2.15 of [61] □

I want to thank `mathoverflow.net` user oxeimon (user id:15242) for helping me with proof. [60].

Application to Alternating Group, A_n

We know that alternating group is a index 2 subgroup of symmetric group S_n. In fact more is true, it is the unique index 2 subgroup of S_n. We have already shown that S_n has property Gal_T, so by the above theorem we get a field extension of $\mathbb{Q}(t)$ with Galois group A_n.

Chapter 9

Application of Rigidity and Rationality I

In chapter 7 we developed the theory of rigidity. In this chapter, we will apply those ideas in practical situations. We will use the Basic Rigidity Theorem, and its stronger version to show that Symmetric groups and Alternating groups occurs as Galois group over $\mathbb{Q}(t)$.

9.1 Galois Realization of Symmetric group S_n

We will apply theory developed in Chapter 7 to S_n, Symmetric group on n letters. See [2] for original discussion.

Observation:

Suppose (C_1, C_2, C_3) are conjugacy classes in a group G, and there exist generators g_1, g_2, g_3 of G with $g_i \in C_i$ and $g_1 g_2 g_3 = 1$. We can observe that the if the triple (C_1, C_2, C_3) is rigid in G then G has trivial center and for each $g_2' \in C_2$ with $(g_1 g_2')^{-1} \in C_3$ and $\langle g_1, g_2' \rangle = G$ there is $h \in H$ with $h g_1 h^{-1} = g_1$ and $h g_2' h^{-1} = g_2$.

Let $C^{(i)}$ be the class of i -cycles in S_n, $n \geq 3$. Then the classes $C^{(2)}$, $C^{(n-1)}$ and $C^{(n)}$ form a **rigid triple** in S_n.

Theorem 9.1. *Let G be a group and X be a set with cardinality greater than equal to 3. Suppose G acts on X, then action is doubly transitive if and only if for each $x \in X$, the $Stab(x)$ acts transitively on $X - \{x\}$.*

Proof. Assume that for each $x \in X$ the action of $Stab(x)$ is transitive on the complement of x. Take two ordered pairs (x_1, x_2) and (y_1, y_2) in $X \times X$ with $x_1 \neq x_2$ and

$y_1 \neq y_2$. Let $Stab(x_1)$ and $Stab(y_2)$ denote the stabilizer of x_1 and y_2 respectively. By hypothesis $Stab(x_1)$ acts transitively on $X - \{x_1\}$, so we get element in G that takes

$$(x_1, x_2) \mapsto (x_1, y_2).$$

Similarly $Stab(y_2)$ acts transitively on complement of y_2, so we get a element in G that takes

$$(x_1, y_2) \mapsto (y_1, y_2).$$

The above method fails when $x_1 = y_2$. In that case choose from z not equal to x_1 and y_1 in X. We can find such z as we have taken the cardinality of X to be atleast three. Now we can find a element in $Stab(x_1)$ that takes

$$(x_,x_2) \mapsto (x_1, z).$$

Use element of $Stab(z)$ to map

$$(x_1, z) \mapsto (y_1, z)$$

and finally use element of $Stab(y_1)$ to take

$$(y_1, z) \mapsto (y_1, y_2).$$

For the reverse direction: Observe that any doubly transitive action is transitive. □

Using the above theorem and the fact that S_n is generated by transpositions. We conclude, if a subgroup of S_n contains an n-cycle and an $(n-1)$-cycle then it is doubly transitive.

Let $\tau = (n-1, n)$, $\sigma = (1, ..., n-1)$, and $\pi = (n-1n, n-2, ..., 2, 1)$. Then $\sigma.\tau.\pi = 1$. These elements generate S_n see the above paragraph. Now we have to show that any transposition τ' such that $\sigma\tau'$ is an n-cycle is conjugate to τ under a power of σ . Choose τ' as $\tau' = (j, n)$ for some $j = 1, ..., n-1$. Then σ^{n-1-j} maps j to $n-1$ while fixing n. therefore we get that σ^{n-1-j} conjugates τ' into τ. We are done.

Since all classes in S_n are rational (See [23]) and we have shown above that class vector is rigid, therefore by basic rigidity theorem, we conclude G occurs as Galois group over $\mathbb{Q}(t)$

Remark: One can show that any conjugacy triple of S_n of the form $(nA, 2A, (n-k)A)$ is rigid if $(k, n) = 1$. See [1].

9.2 Galois Realization of Alternating groups

Since A_n has index 2 in S_n. Result follows from the double group trick.

9.3 Rigid Classes of A_5

We will show that class vector $C = (2A, 3A, 5A)$ of A_5 is rigid. The character table of A_5 looks like,(See [35] for more details).

characters ↓	60 $1A$	4 $2A$	3 $3A$	5 $5A$	5 $5B$	orders of ←centralizers ← classes
χ_1	1	1	1	1	1	
χ_2	3	-1	0	z'	z	$z = \frac{1+\sqrt{5}}{2}$
χ_3	3	-1	0	z	z'	$z' = \frac{1-\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1	
χ_5	5	1	-1	0	0	

Order of Group is 60
Order of centralizer are $4, 3, 5$ respectively.
Recall the rigidity criterion

1. $G = \langle \sigma_1, ..., \sigma_s \rangle$ for some $\sigma_i \in C_i$ with $\sigma_1 ... \sigma_s = 1$,
2. $\Sigma_{\chi \in Irr(G)} \frac{\chi(\sigma_1)\cdots\chi(\sigma_s)}{\chi(1)^{s-2}} = \frac{|\mathcal{C}_G(\sigma_1)|...|\mathcal{C}_G(\sigma_s)|}{|G|^{s-2}|\mathcal{Z}(G)|}$.

It's straightforward to check that second condition is satisfied. We know that A_5 can be generated by a 3-cycle and a 5-cycle. Hence we have shown that the class vector C is rigid.

Not every class vector of A_5 is rigid, for example if we take $C = (2A, 2A, 5A)$ of A_5. It is easy to see that the triple in C generate a dihedral group of order 10. Hence the triple of conjugacy class $C = (2A, 2A, 5A)$ is not rigid.

Given a group G, there can be many class vectors which are rigid. To illustrate this fact, consider the class vector $C = (2A, 5A, 5B)$, $C = (3A, 5A, 5B)$, $C = (3A, 5A, 5B)$. We can show that all these class vectors are rigid.

We can also print the character table using GAP. See the introductory chapter on GAP and *ATLAS*. For example,

```
gap> G:=CharacterTable("A5");
CharacterTable( "A5" )
gap> Display(G);
A5

     2 2 2 . . .
     3 1 . 1 . .
     5 1 . . 1 1

       1a 2a 3a 5a 5b
    2P 1a 1a 3a 5b 5a
    3P 1a 2a 1a 5b 5a
    5P 1a 2a 3a 1a 1a

X.1 1 1 1 1 1
X.2 3 -1 . A *A
X.3 3 -1 . *A A
X.4 4 . 1 -1 -1
X.5 5 1 -1 . .

A = -E(5)-E(5)^4
  = (1-Sqrt(5))/2 = -b5
gap>
```

9.4 Rigid Class of $SL_2(8)$

See [3] for original discussion. Let $G = SL_2(8)$. Let $C = (9A, 9B, 9C)$ be the triple of conjugacy class containing elements of order 9 (where $9B = (9A)^2$ and $9C = (9A)^4$).

	504	8	9	7	7	7	9	9	9	orders of
	$1A$	$2A$	$3A$	$7A$	$7B$	$7C$	$9A$	$9B$	$9C$	←centralizers
										← classes
χ_1	1	1	1	1	1	1	1	1	1	
χ_2	7	−1	−2	0	0	0	1	1	1	
χ_3	7	−1	1	0	0	0	x	$x^{'}$	$x^{''}$	
χ_4	7	−1	1	0	0	0	$x^{''}$	x	$x^{'}$	
χ_5	7	−1	1	0	0	0	$x^{'}$	$x^{''}$	x	
χ_6	8	0	−1	1	1	1	−1	−1	−1	
χ_7	9	1	0	y	$y^{'}$	$y^{''}$	0	0	0	
χ_8	9	1	0	$y^{''}$	y	$y^{'}$	0	0	0	
χ_9	9	1	0	$y^{'}$	$y^{''}$	y	0	0	0	

$$x = -2\cos\tfrac{2\pi}{9}, \quad x^{'} = -2\cos\tfrac{4\pi}{9}, \quad x^{''} = -2\cos\tfrac{8\pi}{9}, \quad xx^{'}x^{''} = 1;$$
$$y = 2\cos\tfrac{2\pi}{7}, \quad y^{'} = 2\cos\tfrac{4\pi}{7}, \quad y^{''} = 2\cos\tfrac{8\pi}{7}, \quad yy^{'}y^{''} = 1.$$

From the character table given above, we can calculate the structure constant.

$$n(C) = \frac{|G|}{|\mathcal{C}_G(\sigma_1|^3} \sum_{\chi \in Irr(G)} \frac{\chi(\sigma_1)\chi(\sigma_2)\chi(\sigma_3)}{\chi(1)}$$

$$= \frac{504}{9^3}(1 + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} - \frac{1}{8} + 0 + 0 + 0) = 1.$$

Now we want to show that no $\sigma \in C$ generate a proper subgroup of G. Assuming the contrary, let's say there is some $\sigma \in C$ with $\sigma_1\sigma_2\sigma_3 = 1$ which generate a proper subgroup of G.

Using GAP, we calculated that the only maximal subgroups of G with order divisible by 9 are dihedral groups D_{18}. It has order 18. As a result we have $\langle\sigma\rangle = Z_9$. This implies $\sigma_2 \in \{\sigma_1^2, \sigma_1^7\}$ and $\sigma_3 \in \{\sigma_1^4, \sigma_1^5\}$. But we have $\sigma_1\sigma_2\sigma_3 = 1$, so their is a contradiction. Hence the triple $C = (9A, 9B, 9C)$ is a rigid.

We can use the GAP to print the character tables. See next chapter for details. In case of $SL_2(8)$

```
gap> Display(group);
L2(8)
```

```
     2 3 3 . . . . . .
     3 2 . 2 . . . 2 2 2
     7 1 . . 1 1 1 . . .

       1a 2a 3a 7a 7b 7c 9a 9b 9c
    2P 1a 1a 3a 7b 7c 7a 9b 9c 9a
    3P 1a 2a 1a 7c 7a 7b 3a 3a 3a
    7P 1a 2a 3a 1a 1a 1a 9b 9c 9a

X.1 1 1 1 1 1 1 1 1 1
X.2 7 -1 -2 . . . 1 1 1
X.3 7 -1 1 . . . D F E
X.4 7 -1 1 . . . E D F
X.5 7 -1 1 . . . F E D
X.6 8 . -1 1 1 1 -1 -1 -1
X.7 9 1 . A C B . . .
X.8 9 1 . B A C . . .
X.9 9 1 . C B A . . .

A = E(7)+E(7)^6
B = E(7)^3+E(7)^4
C = E(7)^2+E(7)^5
D = E(9)^2+E(9)^4+E(9)^5+E(9)^7
E = -E(9)^4-E(9)^5
F = -E(9)^2-E(9)^7
gap>
```

Compare it with the previous character table of $SL_2(8)$.

Chapter 10

Basic Introduction to GAP and ATLAS

10.1 Introduction

In this chapter we give a short introduction to GAP and $ATLAS$. We have extensively used them to compute structure constants, maximal subgroups and for constructing character Table. We have also used the $ATLAS$ notation in our proofs. Due to these reasons, familiarity with $ATLAS$ and GAP is necessary for better understanding of the topic.
We have followed The ATLAS of Finite Groups (Conway et. al. 1985). We have used the **exact notations and definitions** to avoid any confusion. See [35] for more detailed introduction.

GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra provides a programming language, together with thousands of inbuilt functions for efficient computation. GAP is very powerful tool which is used both in teaching and research. It is helpful for people working in the area of group theory, algebra and combinatorial structures. For more information about GAP see [38].

There are lot of good resources available on web. A good place to start is [37]. We have used the character table library of GAP to do the computation. See [36] for more details.

10.2 ATLAS

The ATLAS of Finite Groups commonly known as ATLAS is a group theory book by group of following mathematicians, John Horton Conway, Robert Turner Curtis, Simon Phillips Norton, Richard Alan Parker and Robert Arnott Wilson (with computational assistance from J. G. Thackray). It was published in December 1985 by Oxford University Press. It contain basic information about 93 finite simple groups, For example it contain the following data about the group: Schur multiplier, outer automorphism group, order and various constructions (such as presentations), conjugacy classes of maximal subgroups (with characters group action they define) and most importantly, character tables.

We will be mainly concerned with Character Table and list of maximal subgroups of G and its automorphism group G. It is extensively used by group theorist to solve problems or study properties of groups. When I first learned it, It was bit confusing as there was whole mess of notation which were completely new to me, but it is good to know about ATLAS. It is truly a beautiful piece of mathematics.

If you have access to the ATLAS you can read chapter $4, 5, 6, 7$ to get going. For the sake of readers, we start with a short introduction to some of the notations used in the book. Proofs and GAP library will use the same notation.

Definition 10.1. A maximal subgroup H of G is a proper subgroup of G that is contained in no strictly larger proper subgroup of G.
ATLAS list all maximal subgroups H of a given group G upto conjugacy

Definition 10.2. $A \times B$ is the direct product, or Cartesian product, of A and B. It may be defined as the set of ordered pairs (a, b) $(a \in A, b \in B)$, with $(a, b)(a', b') = (aa', bb')$.

$A.B$ or AB denotes any group having a normal subgroup of structure A, for which the corresponding quotient group has structure B. This is called an upward extension of A by B, or a downward extension of B by A.

Definition 10.3. $A : B$ indicates a case of $A.B$ which is a split extension, or semi-direct product. The structure can be completely described by giving the homomorphism $\phi : B \to Aut(A)$ which shows how B acts by conjugation on A. It may

be defined to consist of the ordered pairs $(b, a)(b \in B, a \in A)$, with $(b, a)(b', a') = (bb', a^{\phi(b')}a')$.

ATLAS use the notation $[m]$ for m an integer, to denote an arbitrary group of order m.

m denoting a cyclic group of order m. A^n for the direct product of n groups of structure A. In particular p^n where p is prime, indicates the elementary abelian group of that order.

Definition 10.4. Class Names:
The conjugacy classes that contain elements of order n are named nA, nB, nC, ...

Definition 10.5. Permutation character
The permutation character of G associated with H is the character of the permutation representation of G acting by right multiplication on the right cosets of H in G. The irreducible constituents of this representation are indicated by their degrees followed by lower case letters $a, b, c, \ldots$, which indicate the successive irreducible representations of G of that degree, in the order in which they appear in the ATLAS character table. A sequence of small letters (not necessarily distinct) after a single number indicates a sum of irreducible constituents all of the same degree.

Relation between the characters of G and $G.2$

The splitting case

The first possibility is that a character χ of G may extend to $G.2$. It then necessarily does so in two ways, giving two characters χ^0 and χ^1 of $G.2$, whose values on elements of $G.2$ outside G are negatives of each other. ATLAS put the splitting symbol (:) in the fusion column to denote the splitting case.

The fusion case

The other possibility is that two characters χ_m and χ_n of G may fuse to give a single character $\chi_{m,n}$ of $G.2$, with values

$$\chi_{m,n} = \chi_m(g) + \chi_n(g),$$

for elements of G

$$\chi_{m,n} = 0,$$

for elements of $G.2$ outside G. ATLAS indicate this case by drawing a fusion join between dots against χ_m and χ_n in the fusion column, and then continuing only the first of these two rows into the $G.2$ detachment, with the indicator of $\chi_{m,n}$ in the indicator column, and the values (all 0) of $\chi_{m,n}$ on elements of $G.2$ outside G in the remaining columns of the $G.2$ detachment. Any class of G on which χ_m and χ_n take distinct values fuses with the class on which those values are taken in the other order to give a single class of $G.2$.

For example If I take $G = M_{12}$ then it has 15 irreducible characters. See the following GAP code. After fusion and splitting of irreducible characters, the character table of $Aut(G)$ has following irreducible characters.

```
gap> ct:=CharacterTable("M12");
CharacterTable( "M12" )

gap> AtlasLabelsOfIrreducibles(ct);
[ "\\chi_{1}", "\\chi_{2}", "\\chi_{3}", "\\chi_{4}",
"\\chi_{5}", "\\chi_{6}", "\\chi_{7}", "\\chi_{8}",
"\\chi_{9}", "\\chi_{10}", "\\chi_{11}", "\\chi_{12}",
"\\chi_{13}", "\\chi_{14}", "\\chi_{15}" ]
gap> automorphismgroup:=CharacterTable("M12.2");
CharacterTable( "M12.2" )
gap> AtlasLabelsOfIrreducibles(automorphismgroup);
[ "\\chi_{1,0}", "\\chi_{1,1}", "\\chi_{2+3}", "\\chi_{4+5}",
"\\chi_{6,0}", "\\chi_{6,1}", "\\chi_{7,0}", "\\chi_{7,1}", "\\chi_{8,0}",
  "\\chi_{8,1}", "\\chi_{9+10}", "\\chi_{11,0}", "\\chi_{11,1}",
  "\\chi_{12,0}", "\\chi_{12,1}", "\\chi_{13,0}", "\\chi_{13,1}",
  "\\chi_{14,0}", "\\chi_{14,1}", "\\chi_{15,0}", "\\chi_{15,1}" ]
```

10.3 GAP

In this section I will explain in short how to use CharacterTable Library of GAP to do the computation. If you are interested and want to learn more about it, see [36], [37], [40]

Installing GAP on your machine

Open the terminal(I work on Linux OS) and type the below mentioned command to install GAP on your computer.

```
$ sudo apt-get install gap-core
```

```
gap> InstalledPackageVersion( "ctbllib" ) <> fail
true
```

If the result is false you need to install the Character Table Library package "ctbllib" from here.
It is easy to do the computation using GAP than looking at ATLAS tables and doing all the calculation by hand, but sill one should know about it.

Using Character Table Library in GAP

We can access the character table from the GAP Character Table Library by calling CharacterTable function. For example;

```
gap> CharacterTable("A5");
CharacterTable( "A5" )

gap> CharacterTable("S5");
CharacterTable( "A5.2" )

gap> CharacterTable("ON");
CharacterTable( "ON" )

gap> CharacterTable("J2");
CharacterTable( "J2" )

gap> CharacterTable("Suz");
CharacterTable( "Suz" )
```

Remark: Variables and Assignment

```
gap> FirstOddPrime:=3;
3
gap> 2+FirstOddPrime;
5
gap>
```

There are some other ways to access the character table, This will be helpful, if you don't know the admissible name of group. You can call functions like `AllCharacterTableNames( Size, n)` to get the admissible name.

```
gap> AllCharacterTableNames( Size, 120 );
[ "2.A5", "2.A6M2", "2xA5", "A5.2", "A6.2_1M3", "D120", "L2(25)M3" ]
```

This library also contain the information about maximal subgroups and their character tables. Let's see how we can access it.

```
gap> ct:=CharacterTable("M12");
CharacterTable( "M12" )

gap> m:=Maxes(ct);
[ "M11", "M12M2", "A6.2^2", "M12M4", "L2(11)", "3^2.2.S4", "M12M7",
"2xS5", "M8.S4", "4^2:D12", "A4xS3" ]

gap> CharacterTable("A4xS3");
CharacterTable( "A4xS3" )
gap>s1:=CharacterTable(m[1]);
CharacterTable( "M11" )

gap> ct:=CharacterTable("A5");
CharacterTable( "A5" )

gap> Maxes(ct);
[ "a4", "D10", "S3" ]



gap> CharacterTable("D10");
CharacterTable( "D10" )

gap> ct:=CharacterTable("ON");
CharacterTable( "ON" )

gap> Maxes(ct);
[ "L3(7).2", "ONM2", "J1", "4_2.L3(4).2_1", "ONM5", "3^4:2^(1+4)D10",
  "L2(31)", "ONM8", "4^3.L3(2)", "M11", "ONM11", "A7", "A7" ]
gap> Maxes(ct)[2];
```

```
"ONM2"
gap> CharacterTable(Maxes(ct)[4]);
CharacterTable( "4_2.L3(4).2_1" )
gap> Length(Maxes(ct));
13
gap>
```

By calling `Maxes` you can get the list of all maximal subgroups of G up to conjugacy. You can either use `m[i]` or directly type the admissible name to access the character table of maximal subgroups.

Primitive Permutation Characters

To compute the primitive permutation characters of a group G, that is, the characters of the permutation actions of G on the cosets of its maximal subgroups, We can proceed by the following method, Let's work it out by example, take $G = A_5$

```
gap> group:= CharacterTable( "A5" );;
gap> m:= List( Maxes(group), CharacterTable );;
gap> t:= List( m, s -> TrivialCharacter( s )^group);;
gap> Display( group,
> rec( chars:= t, centralizers:= false, powermap:= false ) );
A5

       1a 2a 3a 5a 5b

Y.1  5  1  2  .  .
Y.2  6  2  .  1  1
Y.3 10  2  1  .  .
gap>
```

In the *ATLAS of finite groups*, permutation character of A_5 are given in following notation. If you are confused please read the introductory section on ATLAS.

```
gap> PermCharInfo(group, t).ATLAS;
[ "1a+4a", "1a+5a", "1a+4a+5a" ]
gap>
```

Another example,

```
gap> group:=CharacterTable("L2(7)");
CharacterTable( "L3(2)" )
gap> m:=List(Maxes(group), CharacterTable);;
gap> t:=List(m,s->TrivialCharacter(s)^group);;
gap> Display(group,
> rec( chars:= t, centralizers:= false, powermap:= false ) );
L3(2)

         1a 2a 3a 4a 7a 7b

Y.1  7  3  1  1  .  .
Y.2  7  3  1  1  .  .
Y.3  8  .  2  .  1  1


gap> PermCharInfo(group,t).ATLAS;
[ "1a+6a", "1a+6a", "1a+7a" ]
gap>
```

Computing all the permutation characters.

```
gap> ctt:=CharacterTable( "A5" )
gap> p:=PermChars(ctt);
[ Character( CharacterTable( "A5" ), [ 1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( "A5" ), [ 5, 1, 2, 0, 0 ] ),
  Character( CharacterTable( "A5" ), [ 6, 2, 0, 1, 1 ] ),
  Character( CharacterTable( "A5" ), [ 10, 2, 1, 0, 0 ] ),
  Character( CharacterTable( "A5" ), [ 12, 0, 0, 2, 2 ] ),
  Character( CharacterTable( "A5" ), [ 15, 3, 0, 0, 0 ] ),
  Character( CharacterTable( "A5" ), [ 20, 0, 2, 0, 0 ] ),
  Character( CharacterTable( "A5" ), [ 30, 2, 0, 0, 0 ] ),
  Character( CharacterTable( "A5" ), [ 60, 0, 0, 0, 0 ] ) ]

gap> t:=CharacterTable("S5");
CharacterTable( "A5.2" )
gap> PermChars(t);
```

```
[ Character( CharacterTable( "A5.2" ), [ 1, 1, 1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( "A5.2" ), [ 2, 2, 2, 2, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 5, 1, 2, 0, 3, 1, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 6, 2, 0, 1, 0, 2, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 10, 2, 1, 0, 4, 0, 1 ] ),
  Character( CharacterTable( "A5.2" ), [ 10, 2, 4, 0, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 12, 4, 0, 2, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 15, 3, 0, 0, 3, 1, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 20, 0, 2, 0, 2, 0, 2 ] ),
  Character( CharacterTable( "A5.2" ), [ 20, 0, 2, 0, 6, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 20, 4, 2, 0, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 24, 0, 0, 4, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 30, 2, 0, 0, 0, 2, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 30, 2, 0, 0, 6, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 30, 6, 0, 0, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 40, 0, 4, 0, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 60, 0, 0, 0, 6, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 60, 4, 0, 0, 0, 0, 0 ] ),
  Character( CharacterTable( "A5.2" ), [ 120, 0, 0, 0, 0, 0, 0 ] ) ]
gap>
```

```
gap> group:=CharacterTable("M12");
CharacterTable( "M12" )
gap> max:=Maxes(group);
[ "M11", "M12M2", "A6.2^2", "M12M4", "L2(11)", "3^2.2.S4", "M12M7", "2xS5", "M8.S4", "4
gap> s:= CharacterTable( max[1] );
CharacterTable( "M11" )
gap> TrivialCharacter( s )^group;
Character( CharacterTable( "M12" ), [ 12, 0, 4, 3, 0, 0, 4, 2, 0, 1, 0, 2, 0, 1, 1 ] )
gap> group:=CharacterTable("M12");
```

You can find the **order of class representative of conjugacy classes** by calling OrdersClassRepresentatives and order of centralizer by calling SizesCentralizers. Let's work it out by an example.

```
gap> ct:=CharacterTable("ON");
CharacterTable( "ON" )
```

```
gap> OrdersClassRepresentatives(ct);
[ 1, 2, 3, 4, 4, 5, 6, 7, 7, 8, 8, 10, 11, 12, 14, 15, 15,
16, 16, 16, 16, 19, 19, 19, 20, 20, 28, 28, 31, 31 ]

gap> SizesCentralizers(ct);
[ 460815505920, 161280, 3240, 80640, 256, 180,
72, 1372, 49, 32, 32, 20, 11, 36, 28, 45, 45, 16,
16, 16, 16, 19, 19, 19, 20, 20, 28, 28, 31, 31 ]
gap>
```

Using Display function, you can also print the character table on terminal.

```
gap> group:=CharacterTable("A4");
CharacterTable( "a4" )
gap> Display(group);
a4

     2 2 2 . .
     3 1 . 1 1

       1a 2a 3a 3b
    2P 1a 1a 3b 3a
    3P 1a 2a 1a 1a

X.1 1 1 1 1
X.2 1 1 A /A
X.3 1 1 /A A
X.4 3 -1 . .

A = E(3)
  = (-1+Sqrt(-3))/2 = b3

gap> SizesCentralizers(group);
[ 12, 4, 3, 3 ]

gap> OrdersClassRepresentatives(group);
[ 1, 2, 3, 3 ]
gap>
```

Zeros in the table are represented by dots. The top part of table lists on the left prime dividing the order of group. In the example above order of group is 120 so the prime divisors are $2, 3, 5$. You can see it on top left corner first column. After that table list for each conjugacy class, exponents of prime factorization of centralizer order, but it's better to directly print it by calling `SizesCentralizers`.

Another example

```
gap> group:=CharacterTable("2.A6");
CharacterTable( "2.A6" )
gap> Display(group);
2.A6

      2 4 4 3 1 1 1 1 3 3 1 1 1 1
      3 2 2 . 2 2 2 2 . . . . . .
      5 1 1 . . . . . . . 1 1 1 1

         1a 2a 4a 3a 6a 3b 6b 8a 8b 5a 10a 5b 10b
     2P  1a 1a 2a 3a 3a 3b 3b 4a 4a 5b 5b 5a 5a
     3P  1a 2a 4a 1a 2a 1a 2a 8b 8a 5b 10b 5a 10a
     5P  1a 2a 4a 3a 6a 3b 6b 8b 8a 1a 2a 1a 2a

X.1  1  1  1  1  1  1  1  1  1  1  1  1  1
X.2  5  5  1  2  2 -1 -1 -1 -1  .  .  .  .
X.3  5  5  1 -1 -1  2  2 -1 -1  .  .  .  .
X.4  8  8  .  -1 -1 -1 -1  .  .  B  B -*B -*B
X.5  8  8  .  -1 -1 -1 -1  .  . -*B -*B  B  B
X.6  9  9  1  .  .  .  .  1  1 -1 -1 -1 -1
X.7 10 10 -2  1  1  1  1  .  .  .  .  .  .
X.8  4 -4  .  -2  2  1 -1  .  . -1  1 -1  1
X.9  4 -4  .  1 -1 -2  2  .  . -1  1 -1  1
X.10 8 -8  .  -1  1 -1  1  .  .  B -B -*B  -*B
X.11 8 -8  .  -1  1 -1  1  .  . -*B  -*B  B -B
X.12 10 -10  .  1 -1  1 -1  A -A  .  .  .  .
X.13 10 -10  .  1 -1  1 -1 -A  A  .  .  .  .

A = E(8)-E(8)^3
  = Sqrt(2) = r2
```

```
B = -E(5)-E(5)^4
  = (1-Sqrt(5))/2 = -b5
gap>
```

```
gap> OrdersClassRepresentatives(group);
[ 1, 2, 4, 3, 6, 3, 6, 8, 8, 5, 10, 5, 10 ]

gap> SizesCentralizers(group);
[ 720, 720, 8, 18, 18, 18, 18, 8, 8, 10, 10, 10, 10 ]
gap>
```

If you want to print the values taken by some particular irreducible character(say χ_4 as in the example above). You can use the following command.

```
gap> group:=CharacterTable("A4");
CharacterTable( "a4" )

gap> Irr(group)[2];
Character( CharacterTable( "a4" ), [ 1, 1, E(3), E(3)^2 ] )

gap> Irr(group)[3];
Character( CharacterTable( "a4" ), [ 1, 1, E(3)^2, E(3) ] )

gap> ScalarProduct(Irr(c)[2],Irr(c)[3]);

gap> ScalarProduct(Irr(group)[2],Irr(group)[3]);
0
```

Class names in ATLAS notation can be printed by calling `ClassNames`. For example in the above table,

```
gap> ClassNames(group);
[ "1a", "2a", "3a", "3b" ]
gap>
```

`CharacterTableDirectProduct( tbl1, tbl2 )` prints the character table of the direct product of the groups

`CharacterTableWreathSymmetric( tbl, n )` prints the character table of the wreath product of an arbitrary group G with the full symmetric group S_n.

Some examples,

```
gap> cyclicgroup2:=CharacterTable("Cyclic", 2);
CharacterTable( "C2" )
gap> cyclicgroup1:=CharacterTable("Cyclic", 3);
CharacterTable( "C3" )
gap> prod:=CharacterTableDirectProduct(cyclicgroup1, cyclicgroup2);
CharacterTable( "C3xC2" )
gap> Display(prod);
C3xC2

     2 1 1 1 1 1 1
     3 1 1 1 1 1 1

       1a 2a 3a 6a 3b 6b
    2P 1a 1a 3b 3b 3a 3a
    3P 1a 2a 1a 2a 1a 2a

X.1 1 1 1 1 1 1
X.2 1 -1 1 -1 1 -1
X.3 1 1 A A /A /A
X.4 1 -1 A -A /A -/A
X.5 1 1 /A /A A A
X.6 1 -1 /A -/A A -A

A = E(3)
  = (-1+Sqrt(-3))/2 = b3
gap>

gap> cyclicgroup1:=CharacterTable("Cyclic", 2);
CharacterTable( "C2" )
gap> altgroup1:=CharacterTable("Alternating", 4);
CharacterTable( "Alt(4)" )
gap> prod:=CharacterTableDirectProduct(cyclicgroup1, altgroup1);
CharacterTable( "C2xAlt(4)" )
gap> Display(prod);
C2xAlt(4)
```

```
     2 3 3 1 1 3 3 1 1
     3 1 . 1 1 1 . 1 1

       1a 2a 3a 3b 2b 2c 6a 6b
    2P 1a 1a 3b 3a 1a 1a 3b 3a
    3P 1a 2a 1a 1a 2b 2c 2b 2b

X.1 1 1 1 1 1 1 1 1
X.2 3 -1 . . 3 -1 . .
X.3 1 1 A /A 1 1 A /A
X.4 1 1 /A A 1 1 /A A
X.5 1 1 1 1 -1 -1 -1 -1
X.6 3 -1 . . -3 1 . .
X.7 1 1 A /A -1 -1 -A -/A
X.8 1 1 /A A -1 -1 -/A -A

A = E(3)
  = (-1+Sqrt(-3))/2 = b3
gap>
```

```
gap> cyclicgroup:= CharacterTable("Cyclic", 2);
CharacterTable( "C2" )

gap> wreathpro:= CharacterTableWreathSymmetric(cyclicgroup, 3);
CharacterTable( "C2wrS3" )

gap> Display(wreathpro);
C2wrS3

      2 4 4 4 4 3 3 3 3 1 1
      3 1 . . 1 . . . . 1 1

        1a 2a 2b 2c 2d 4a 2e 4b 3a 6a
     2P 1a 1a 1a 1a 1a 2b 1a 2b 3a 3a
     3P 1a 2a 2b 2c 2d 4a 2e 4b 1a 2c

X.1  1  1  1  1  1 -1 -1 -1 -1  1  1
X.2  3  1 -1 -3 -1 -1  1  1  .  .
X.3  3 -1 -1  3 -1  1 -1  1  .  .
X.4  1 -1  1 -1 -1  1  1 -1  1 -1
X.5  2  2  2  2  .  .  .  . -1 -1
X.6  3 -1 -1  3  1 -1  1 -1  .  .
X.7  3  1 -1 -3  1  1 -1 -1  .  .
X.8  2 -2  2 -2  .  .  .  . -1  1
X.9  1  1  1  1  1  1  1  1  1  1
X.10 1 -1  1 -1  1 -1 -1  1  1 -1
gap>
```

We end this chapter by showing how to print character table of some known and frequently used finite groups.

```
gap> group2:=CharacterTable("Quaternionic", 8);
CharacterTable( "Q8" )
gap> Display(group2);
Q8

     2 3 2 3 2 2

       1a 4a 2a 4b 4c
```

```
     2P 1a 2a 1a 2a 2a

X.1  1  1  1  1  1
X.2  1  1  1 -1 -1
X.3  1 -1  1  1 -1
X.4  1 -1  1 -1  1
X.5  2  .  -2 .  .


gap> group1:=CharacterTable("Dihedral", 8);
CharacterTable( "Dihedral(8)" )
gap> Display(group1);
Dihedral(8)

      2 3 2 3 2 2

        1a 4a 2a 2b 2c
     2P 1a 2a 1a 1a 1a

X.1  1  1  1  1  1
X.2  1  1  1 -1 -1
X.3  1 -1  1  1 -1
X.4  1 -1  1 -1  1
X.5  2  .  -2 .  .
gap>

gap> group2:=CharacterTable("Symmetric",4);
CharacterTable( "Sym(4)" )
gap> Display(group2)
> ;
Sym(4)

      2 3 2 3 . 2
      3 1 . . 1 .

        1a 2a 2b 3a 4a
     2P 1a 1a 1a 3a 2b
```

```
    3P 1a 2a 2b 1a 4a

X.1  1 -1  1  1 -1
X.2  3 -1 -1  .  1
X.3  2  .  2 -1  .
X.4  3  1 -1  . -1
X.5  1  1  1  1  1
gap>
```

Remark: In general we can use `CharacterTable( "Alternating", n )`, `CharacterTable( "Cyclic", n )`, `CharacterTable( "Dihedral", 2n )`, `CharacterTable( "Symmetric", n )` for printing character tables of alternating group, cyclic group, symmetric group, dihedral group.

Chapter 11

Application of Rigidity II: Sporadic Groups

11.1 Introduction

In this chapter, we will apply the ideas developed in chapter on Rigidity and Rationality of finite groups to some sporadic groups. The algorithm is simple, we will start with triple of conjugacy class, show that value of structure constant $n(C) = 1$ and then show that no triple in C, generate a proper subgroup of G. In short our aim will be to show that $C = (C_1, C_2, C_3)$ is rationally rigid and then we can use the *Rigidity Criterion* to conclude that given group occurs as Galois group over $\mathbb{Q}(t)$.
As of now there is no unified proof, we will do the case by case analysis. We have made extensive application of computer program GAP, and Atlas of Finite Groups. Look [35] and [36].
Note: We will use the Double Group Trick, which roughly speaking says that if G occurs as Galois group then index 2 subgroup of G also occurs as Galois group. We have already proved this result, so readers are advised to go through it once.
To make yorself familiar with GAP and ATLAS, kindly go through the Chapter 10.

11.2 Galois Realization of Co_1

The Conway group Co_1 is a sporadic simple group of order roughly around 4×10^{18}. Co_1 is one of the 26 sporadic groups. It was discovered by John Horton Conway in 1968. Out of three Conway groups, this is the largest. The outer automorphism group is trivial and the Schur multiplier has order 2. Wilson in (1983) found the 22 maximal subgroups of Co_1 upto conjugacy.

Let's define the group in GAP. We use the command Maxes to get the information about the maximal subgroups of G.

```
gap> G:=CharacterTable("Co1");;max:=Maxes(G);
[ "Co2", "3.Suz.2", "2^11:M24", "Co3", "2^(1+8)+.O8+(2)",
"U6(2).3.2", "(A4xG2(4)):2", "2^(2+12):(A8xS3)", "2^(4+12).(S3x3S6)",
  "3^2.U4(3).D8", "3^6:2M12", "(A5xJ2):2", "3^(1+4).2U4(2).2",
  "(A6xU3(3)):2", "3^(3+4):2(S4xS4)", "A9xS3", "(A7xL2(7)):2",
  "(D10x(A5xA5).2).2", "5^(1+2):GL2(5)", "5^3:(4xA5).2", "7^2:(3x2A4)", "5^2:2A5" ]
gap> len:=[1..22];
```

There are 22 maximal subgroups upto conjugacy.

Claim:

The class vector $(3A, 5C, 13A)$ of Co_1 is rationally rigid.

Let's compute the value of structure constant $n(C)$, using the code written in GAP,

It is found to be $n(C) = 1$.

```
ms:=function( table, class )
      local exp;
      exp := Length( class ) - 2;
      if exp < 0 then
          Error( "length␣should␣be␣atleast␣least␣2" );
      fi;
      return Sum( Irr( table ), function ( chi )
                  return Product( chi{class}, 1 ) / chi[1] ^ exp;
              end, 0 ) * Product( SizesConjugacyClasses( table ){class}, 1 ) / Size( table );
end;
```

We can look up the order of class and class names as used in the ATLAS, [35] by using the following commands.

```
gap> OrdersClassRepresentatives(G);
[ 1, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4,
  5, 5, 5, 6, 6, 6, 6, 6, 6, 6, 6, 6, 7, 7, 8,
  8, 8, 8, 8, 8,
  9, 9, 9, 10, 10, 10, 10, 10, 10, 11,
  12, 12, 12, 12, 12, 12,
  12, 12, 12, 12, 12, 12, 12, 13, 14,
  14, 15, 15, 15, 15, 15, 16, 16, 18, 18, 18,
  20, 20, 20, 21, 21, 21, 22, 23, 23, 24, 24,
```

```
  24, 24, 24, 24, 26, 28, 28, 30, 30, 30, 30,
  30, 33, 35, 36, 39, 39, 40, 42, 60 ]
gap> ClassNames(G);
[ "1a", "2a", "2b", "2c", "3a", "3b", "3c", "3d", "4a",
  "4b", "4c", "4d", "4e", "4f", "5a", "5b", "5c", "6a", "6b",
   "6c", "6d", "6e", "6f",
  "6g", "6h", "6i", "7a", "7b", "8a", "8b", "8c", "8d",
  "8e", "8f", "9a", "9b", "9c", "10a", "10b", "10c", "10d",
  "10e", "10f", "11a", "12a",
  "12b", "12c", "12d", "12e", "12f", "12g",
  "12h", "12i", "12j", "12k", "12l", "12m", "13a", "14a",
  "14b", "15a", "15b", "15c", "15d", "15e",
  "16a", "16b", "18a", "18b", "18c", "20a", "20b",
  "20c", "21a", "21b", "21c", "22a", "23a", "23b", "24a",
  "24b", "24c", "24d", "24e", "24f",
  "26a", "28a", "28b", "30a", "30b", "30c", "30d", "30e",
  "33a", "35a", "36a", "39a", "39b", "40a", "42a", "60a" ]
```

Let's find out which maximal subgroups have order divisible by 13.

```
gap> for i in len do
> if Size(CharacterTable(max[i])) mod 13 = 0 then
> Print(max[i],"\n");
> fi;
> od;
3.Suz.2
(A4xG2(4)):2
```

Now we will show that no $\sigma \in C$ generate a proper subgroup of G, for this purpose we will use the knowledge of maximal subgroups of G. Let H denote the proper subgroup of G generated by $\sigma \in C$. We will try to arrive at a contradiction.

So there are only two maximal subgroups of G whose order is divisible by 13. As you can see from above, 9 does not divide the order of centralizer of $5C$-elements. In $A4 \times G2(4)$, all 5-elements have centralizer order 12.300, (using GAP). Hence this possibility is cancelled out. See [3] for rest of the proof.

11.3 Galois Realization of M_{22}

Mathieu group M_{22} is a sporadic simple group of order 443520. This group was discovered by Mathieu in $(1861, 1873)$. The outer automorphism group has order 2.

First we will show that $Aut(M_{22})$ occurs as Galois group over $\mathbb{Q}(t)$.

Claim:

The conjugacy class triple $(2B, 4C, 11A)$ of of $Aut(M_{22})$ is rationally rigid.

As done earlier, we compute the value of $n(C)$, It is found to be 1.

```
gap> G:=CharacterTable("M22.2");
CharacterTable( "M22.2" )
gap> Maxes(G);
[ "M22", "L3(4).2_2", "M22.2M3", "M22.2M4",
"2x2^3:L3(2)", "A6.2^2",
  "L2(11).2" ]
gap> length:=[1..7];
[ 1 .. 7 ]
gap> m:=Maxes(G);
[ "M22", "L3(4).2_2", "M22.2M3", "M22.2M4", "2x2^3:L3(2)", "A6.2^2",
  "L2(11).2" ]
gap> for i in length do
> if Size(CharacterTable(m[i])) mod 11=0 then
> Print(m[i],"\n");
> fi;
> od;
M22
L2(11).2
gap>
```

We find that only $PGL_2(11)$ has order divisible by 11, Let H be a proper subgroup generated by $\sigma \in C$. Now suppose H is contained in $PGL_2(11)$, then the intersection of this maximal subgroup with G is equal to $L_2(11)$. Elements present in outer class of involution of $PGL_2(11)$ fuse into $2B$ (see [3] for proof). Using character table, we see that the centralizer order for $2B$ in $Aut(M_{22})$ is not divisible by 5, but in $PGL_2(11)$, it is divisible. Hence we arrive at the contradiction.

Conclusion:

$Aut(M_{22})$ and M_{22} (being the index 2 subgroup) occurs as Galois group over $\mathbb{Q}(t)$.

11.4 Digression: Congruence properties of Character Values

The goal of this section is to state a result about congruence property of character value. We will be using the result in the next section. We have tried to keep the exposition short and concise. All the proofs can be found [24]. Please keep in mind that proofs given in this section are not original. Let's start with a proposition.

Proposition 11.1. *Let p be a prime number and let $g \in G$ then there exist $x, y \in G$ such that*

- $g = xy = yx$
- *the order of x is a power of p and*
- *the order of y is a coprime to p.*

Proof. Let the order of g be up^v, where $u, v \in \mathbb{Z}$ and $gcd(u, p) = 1$. By Bezout's lemma, there exist integers a, b such that

$$au + bp^v = 1.$$

Now, put $x = g^{au}$ and $y = g^{bp^v}$.Then we get,

$$xy = yx = g$$

$$x^{p^v} = g^{aup^v} = 1$$

,

$$y^u = g^{bup^v} = 1$$

Here the order of x is a power of p and the order of y divides u, so is now coprime to p. therefore x and y satisfy all the conditions.

□

The most beautiful part is that the element x and y of G which satisfy this condition is unique. Do it as a small exercise.

Definition 11.2. We call the element y which appears in the previous lemma the $p^{'}$-part if g.

Example 11.3. if $p = 2$ and g has order 6 the the $p^{'}$-part of g is g^{-2}

Let n be a positive integer and let $\zeta = e^{2\pi i/n}$. Define $\mathbb{Z}[\zeta]$ to be the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and ζ

Let p be a prime number and let $p\mathbb{Z}[\zeta] = \{pr : r \in \mathbb{Z}[\zeta]\}$ is a Principal ideal of $\mathbb{Z}[\zeta]$

Proposition 11.4. *There are only finitely many ideals I of $\mathbb{Z}[\zeta]$ which contain $p\mathbb{Z}[\zeta]$.*

Proof. By ideals correspondence, It's enough to show that there are only finitely many ideals in factor ring $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$.

So consider the factor ring $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$. By definition, this has its element all the cosets $p\mathbb{Z}[\zeta] + r$ where $r \in \mathbb{Z}[\zeta]$. Every such coset contain an element of the form $a_0 + \cdots + a_{n-1}\zeta^{n-1}$ with $a_i \in \mathbb{Z}$ and $0 \leq a_i \leq p-1$ for all i.

As there only finitely such elements, we can conclude that factor ring is finite. therefore there are finitely many such ideals.

□

Recall, We say a proper ideal M of a ring R is maximal if it is not contained in any larger proper ideal. By proper ideal, I mean an ideal which is not equal to R.
We deduce from the previous proposition that there is a maximal ideal P of $p\mathbb{Z}[\zeta]$ which contains $\mathbb{Z}[\zeta]$

Proposition 11.5. *We have $P \cap \mathbb{Z} = p\mathbb{Z}$*

Proof. Let $m \in P \cap \mathbb{Z}$. If p does not divide m then there are integers a, b with $am + bp = 1$ but this implies that $1 \in P$, which is false, since P is proper. Thus p divides m. Reverse inclusion is easy as $p \in P$.

□

Theorem 11.6. *Let $g \in G$ and let y be the p' part of g. If χ is any character if G then*

$\chi(g) - \chi(y) \in P$.

Corollary 11.7. Let p be a prime number. Suppose that $g \in G$ and that y is the p'-part of g. If χ is a character of G such that $\chi(g)$ and $\chi(y)$ are both integers, then

$$\chi(g) \equiv \chi(y)(\ mod\ p)$$

Proof. As $\chi(g)$ and $\chi(y)$ are both integers. We can conclude the result from the previous lemma

□

Corollary 11.8. Let p be a prime number. Suppose that $g \in G$ and the order of g is a power of p. If χ is a character of G such that

$$\chi(g) \equiv \chi(1)(\ mod\ p).$$

Proof. As $p^{'}$ part of g is 1, so from previous corollary, result is immediate.

□

11.5 Galois Realization of M_{12}

M_{12} was discovered by Mathieu. It belongs to the list of 26 sporadic group. It has order 95040.

Automorphism group of M_{12} contain M_{12} as index 2 subgroup. As done in previous section, first we will show that $Aut(G)$ occurs as Galois group and since G is a normal subgroup of index 2, by Double Group Trick proven earlier G also occurs as Galois group over $\mathbb{Q}(t)$.

Claim:
The class vector $(2C, 3A, 12A)$ of $Aut(M_{12})$ is rationally rigid.

Let's define the group in GAP.

```
gap> G:=CharacterTable("M12.2");
CharacterTable( "M12.2" )
gap> Maxes(G);
[ "M12", "L2(11).2", "M12.2M3", "(2^2xA5):2", "D8.(S4x2)", "4^2:D12.2",
  "3^(1+2):D8", "S4xS3", "A5.2" ]
gap>
```

Using the code below, value of $n(C)$ is found to be 1.

```
ms:=function( table, class )
      local exp;
      exp := Length( class ) - 2;
      if exp < 0 then
          Error( "length␣should␣be␣atleast␣least␣2" );
      fi;
      return Sum( Irr( table ), function ( chi )
                  return Product( chi{class}, 1 ) / chi[1] ^ exp;
```

```
                end, 0 ) * Product( SizesConjugacyClasses( table ){class}, 1 ) / Size( table );
end;
```

Let H be a proper subgroup of G generated by triple in C. Using the code below, we find that only maximal subgroup containing H is $M = S_4 \times S_3$.

```
ts:=function(ct,C)
for name in Maxes(ct) do
  ctm:=CharacterTable(name);
  fus:=Filtered(ComputedClassFusions(ctm),y->y.name="M22.2")[1].map;
        if IsSubset(fus,C) then
        Print(name); Cm:=List(C, x->Positions(fus,x));
        Print("\n", List(Cm, x->ClassNames(ctm){x}), "\n");
                for Ch in Cartesian(Cm[1],Cm[2],Cm[3]) do
                 cs:=ClassStructureCharTable(ctm, Ch);
                 if cs <> 0 then
                  Print("alpha_", ClassNames(ctm){Ch}, "=", cs/Size(ctm),"*|H|\n");
                 fi;
                od;
        fi;
 od;
end
```

Suppose M has a $(2, 3, 12)$-system, then what possibility we have for the last class. The only possible option is option is : 4-cycles in S_4 times the 3-cycles in S_3. Hence

$$C \cap M = ((2) \times (1), (3) \times (3), (4) \times (3)).$$

Now M has three classes of elements of order three, namely $(1) \times (3), (3) \times (1)$ and $(3) \times (3)$, with centralizer in M of order $72, 18$ and 9 respectively. See [35]. If structure constant does not vanish in M, then first class fuses into $3B$ and third into $3A$, see [35]. possible value of permutation character is $\chi(3A) = 12, \chi(3B) = 5$ or $\chi(3A) = 18, \chi(3B) = 1$.

Conclusion

Using the result proved in previous section, we arrive at the contradiction as we should have $\chi(3A) \equiv \chi(3B) \bmod 3$. Therefore $Aut(M_{12})$ and hence M_{12} occurs as Galois group over $\mathbb{Q}(t)$.

See [3] for original proof.

11.6 Sporadic group O'Nan and its Galois realization over $\mathbb{Q}(t)$

O'Nan group $O'N$ is a sporadic simple group of order roughly around $5 \times 10^1 1$. $O'N$ is one of the 26 sporadic groups. It was constructed by Michael O'Nan (1976) in a study of groups with a Sylow 2-subgroup of Alperin type.

The Schur multiplier of $O'N$ has order 3, and its outer automorphism group has order 2. R. L. Griess demonstrated that O'Nan cannot be a subquotient of the monster group. Thus it is one of the 6 sporadic groups called the pariahs.

Claim:
The class vector $(2B, 4A, 22A)$ of $Aut(ON)$ is rationally rigid.

First we compute the value of structure constant using the code,

```
ms:=function( table, class )
      local exp;
      exp := Length( class ) - 2;
      if exp < 0 then
          Error( "length␣should␣be␣atleast␣least␣2" );
      fi;
      return Sum( Irr( table ), function ( chi )
                  return Product( chi{class}, 1 ) / chi[1] ^ exp;
              end, 0 ) * Product( SizesConjugacyClasses( table ){class}, 1 ) / Size( table );
end;
```

It is found to be 1.

```
gap> G:=CharacterTable("ON");
CharacterTable( "ON" )
gap> M:=Maxes(G);
[ "L3(7).2", "ONM2", "J1", "4_2.L3(4).2_1", "ONM5", "3^4:2^(1+4)D10",
  "L2(31)", "ONM8", "4^3.L3(2)", "M11", "ONM11", "A7", "A7" ]
gap> G:=CharacterTable("ON.2");
CharacterTable( "ON.2" )
gap> M:=Maxes(G);
[ "ON", "J1x2", "4_2.L3(4).(2^2)_{12*3}", "(3^2:4xA6).2^2",
  "3^4:2^(1+4).(5:4)", "4^3.(L3(2)x2)", "7^(1+2)_+:(3xD16)", "31:30",
```

```
  "A6.2_2", "L3(2).2" ]
gap> Length(M);
10
gap> l:=[1..10];
[ 1 .. 10 ]
gap> for i in l do
> if Size(CharacterTable(M[i])) mod 11=0 then
> Print(M[i],"\n");
> fi;
> od;
ON
J1x2
gap>
```

Let H be a proper subgroup generated by triple $\sigma \in C$. Using the program written, we find the maximal subgroup of $Aut(ON)$ whose order is divisible by 11. If we see which maximal subgroup have order divisible by 11, we find out that there is only one type $J_1 \times 2$. But J_1 does not contain an element of order 4, hence $J_1 \times 2$ also. Hence $H = Aut(ON)$.

Conclusion:

We conclude that $Aut(ON)$ occurs as Galois group over $\mathbb{Q}(t)$. Since ON sits inside $Aut(ON)$ as index 2 subgroup, by Double Group Trick, we conclude that ON also occurs as Galois group over $\mathbb{Q}(t)$.

Appendices

Appendix A

On Galois Covering of A_n

ON CONSTRUCTING GALOIS COVER OF $\mathbb{P}^1$ WITH ALTERNATING GROUPS AS GALOIS GROUP

VIKAS SRIVASTAVA

Dedicated To my parents and Prof. Kapil Paranjape

Abstract. This paper presents a method of Constructing Galois Cover of $\mathbb{P}^1$ with Alternating Groups as Galois Group. The construction works for all values of n, except $n = 6, 7$ and 8, where n is the degree of Alternating Group.

.

1. Theory

1.1. **Basic Ideas: Free Product and Group Action.** Let's introduce the notion of free product and free amalgamated products. Intuitively It is a construction that "glues" two groups along a common subgroup.

Definition 1.1 (Free product with amalgamation, universal property)**.** Let A be a group and let $\alpha_1 : A \to G_1$ and $\alpha_2 : A \to G_2$ be group homomorphisms. A group G together with homomorphisms $\beta_1 : G_1 \to G$ and $\beta_2 : G_2 \to G$ satisfying $\beta_1 \circ \alpha_1 = \beta_2 \circ \alpha_2$ is called *amalgamated free product of G_1 and G_2 over A (with respect to α_1 and α_2)* if the following universal property is satisfied:
For any group H and any two group homomorphisms $\phi_1 : G_1 \to H$ and $\phi_2 : G_2 \to H$ with $\phi_1 \circ \alpha_1 = \phi_2 \circ \alpha_2$ there is exactly one homomorphism $\phi : G \to H$ of groups with $\phi \circ \beta_1 = \phi \circ \beta_2$.
Such a free product with amalgamation is denoted by $G_1 *_A G_2$.

Definition 1.2 (Free Product)**.** If A is trivial group, the we write $G_1 * G_2 := G_1 *_A G_2$ and call $G_1 * G_2$ the free product of G_1 and G_2.

Let's give purely abstract and generalized definition of group action. Those who don't know about category theory, Don't worry!. We will also give a simplified definition.

Definition 1.3 (Group Action)**.** Let G be a group, Let C be a category and let X be an object in C. An action of G on X in the category C is a group homomorphisms $G \to Aut_C(X)$. In other words, a group action of G on X consist of a family $(f_g)_{g \in G}$ of automorphism of X such that

$$f_g \circ f_h = f_{g.h}$$

holds for all $g, h \in G$.

Definition 1.4. Let G be a group and let X be a set. A *(left) group action* of G on X is a function $\alpha : G \times X \to X$ satisfying:

Date: November 2016.

(1) $\alpha(e,x)=x$ for all $x\in X$.
(2) $\alpha(gh,x)=\alpha(g,\alpha(h,x))$ for all $g,h\in G$ and $x\in X$.

We will use the following notation, $\alpha(g,x):=g.x$.

Definition 1.5. (Orbit and Quotient Space) Let G be a group action on a set X. The *orbit* of an element $x\in X$ with respect to this group action is the set

$$G.x:=\{g.x|g\in G\}.$$

We define the *quotient* of X by a given G-action(or *orbit space*) is the set

$$G\setminus X:=\{G.x|x\in X\}$$

of orbits.

1.2. **Ping Pong Lemma.** We will need the Ping Pong Lemma. If the reader is interested, look up [1], for more information.

Theorem 1.6. *(Ping-pong Lemma) Let G be a group, generated by elements a and b. Suppose there is a G-action on a set X such that there are non empty subsets $A,B\subset X$ with B not included in A and such that for all $n\in\mathbb{Z}\setminus\{0\}$ we have*

$$a^n.B\subset A \qquad \text{and} \qquad b^n.A\subset B$$

Then G is a free of rank 2, freely generated by $\{a,b\}$.

We will use the following version of *"Ping pong lemma"*

Theorem 1.7. *Let G be a group, let G_1 and G_2 be two subgroups of G with $|G_1|\geq 3$ and $|G_2|\geq 2$, and suppose that G is generated by the union $G_1\cup G_2$. If there is a G -action on a set X such that there are non-empty subsets $X_1,X_2\subset X$ with X_2 not included in X_1 and such that*

$$\forall_{g\in G_1\setminus\{e\}} g.X_2\subset X_1 \qquad \text{and} \qquad \forall_{g\in G_2\setminus\{e\}} g.X_1\subset X_2$$

then $G\simeq G_1*G_2$.

1.3. **Some results on $PSL(2,\mathbb{Z})$ and A_n.** Let us denote by $SL(2,\mathbb{Z})$ the set of 2×2-matrices with integer entries whose determinant is 1, and by $PSL(2,\mathbb{Z})$ the quotient $SL(2,\mathbb{Z})/\{\pm\mathrm{Id}\}$.

Before proceeding to the next result, Let me comment on $SL(2,\mathbb{Z})$. It lies discretely inside $SL(2,\mathbb{R})$. It is the most basic example of a discrete nonabelian group. It has a role, which is very similar to that of $\mathbb{Z}$ inside $\mathbb{R}$.

Theorem 1.8. *Let*

$$S=\begin{pmatrix}0&-1\\1&0\end{pmatrix} \qquad \text{and} \qquad T=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

The matrix S and T generate $SL(2,\mathbb{Z})$

Proof. The matrix S has order 4, while T has infinite order and

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

has order 6. Let $G=\langle S,T\rangle$ be the subgroup of $SL(2,\mathbb{Z})$ generated by S and T. Let's see what is the effect of S and T^n on any matrix,

$$S.\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

$$T^n.\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$$

Now pick any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $SL(2,\mathbb{Z})$.
Suppose $c \neq 0$. If $|a| \geq |c|$, write $a = cq + r$ with $0 \leq r < |c|$. Then $T^{-q}\gamma$ has upper left entry $a - qc$, Now observe that $|a - qc| < |c|$. Applying S, switch the entries (with a sign change), and we apply the Euclidean lemma again if the lower entry is non zero.
Eventually multiplication of γ on the left by enough copies of S and powers of T gives a matrix in $SL(2,\mathbb{Z})$ with lower left entry 0. Such a matrix, since it is integral with determinant 1, has the form $\left(\begin{smallmatrix} \pm 1 & m \\ 0 & \pm 1 \end{smallmatrix}\right) = T^m$ or T^{-m}, where $m \in \mathbb{Z}$. We can deduce that for some $g \in G$ and $\in \mathbb{Z}$, $g\gamma = \pm T^n$. Since $T^n \in G$ and $-I_2 = S^2 \in G$, we conclude that $\gamma \in G$.

□

Theorem 1.9. $PSL(2,\mathbb{Z}) \simeq \mathbb{Z}_2 * \mathbb{Z}_3$

Proof. Let $PSL(2,\mathbb{Z})$ acts on set of irrational numbers via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.r = \frac{ar+b}{cr+d}$$

Since r is irrational, $cr + d \neq 0$ for all $c, d \in \mathbb{Z}$ We will be using the "Ping Pong lemma" to give the result. By the previous theorem we know that following matrices

$$B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

generate $SL(2,\mathbb{Z})$. Let $C = AB$ Then B and C also generate $SL(2,\mathbb{Z})$. Since $B^2 = -I_2$, It has order 2 in $PSL(2,\mathbb{Z})$ and $C^3 = -I_2$, therefore It has order 3 in $PSL(2,\mathbb{Z})$. Since B and C generate $SL(2,\mathbb{Z})$ their images generate the quotient $PSL(2,\mathbb{Z})$.

Observe

$$B = B^{-1} : z \to \frac{1}{z}$$

$$C : z \to 1 - \frac{1}{z}$$

and

$$C^{-1} : z \to \frac{1}{1-z}.$$

Now let $\mathcal{P}$ and $\mathcal{N}$ denote the set of positive and negative irrational respectively. Clearly $B.\mathcal{P} \subset \mathcal{N}$ and $C^{\pm 1}.\mathcal{N} \subset \mathcal{P}$

Now to finish the proof, we show that for any alternating word w from $\mathbb{Z}_2 \simeq \langle B \rangle$ and $\mathbb{Z}_3 = \langle C \rangle$, $w \neq 1$ in $PSL(2,\mathbb{Z}$
CASE 1: If w has odd length. then either w begins and ends with a B, hence $w.\mathcal{P} \subset \mathcal{N}$ or w begins and ends with a $C^{\pm 1}$, hence $w.\mathcal{N} \subset \mathcal{P}$. In particular $w \neq 1$ in $PSl(2,\mathbb{Z})$.

CASE 2: If w has even length. Without loss of generality we may suppose that w begins with a $C^{\pm 1}$, otherwise just conjugate w by B. Then either w begins with a C and ends with a B, hence

$$w.\mathcal{P} \subset C.\mathcal{N} \subset \{\text{r irrational} \mid r > 1\}$$

or w begins with a C^{-1} and ends with a B, hence

$$w.\mathcal{P} \subset C^{-1}.\mathcal{N} \subset \{\text{r irrational} \mid r < 1\}$$

In either case we deduce that $w \neq 1$ in $PSL(2, \mathbb{Z})$ □

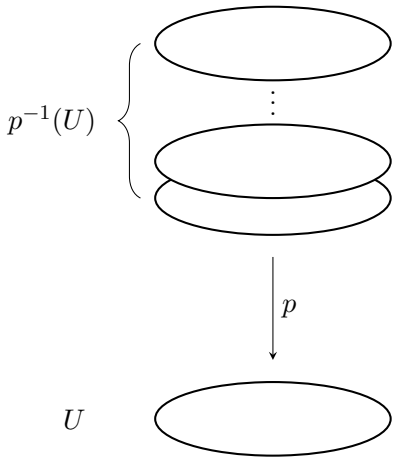
Theorem 1.10. *Let A_n denote the alternating group of degree n. Then except for $n = 6, 7$ and 8, we can find two element , one having order 2 and another having order 3, which generate A_n. We refer this property by saying that A_n is $(2, 3)$ generated.*

G. A. Miller proved this result in 1901,[3]. It is based on the truth of Bertrand's postulate and his generators depend on choosing a prime p in the range $n-2 > p > n/2$, here n is the degree of groups under discussion. Proof is bit longer and wordier, so we omit the proof. For another proof, see [2], The basis of the method is to give an element a of order 3 and two elements x, y of order 2 in the relevant symmetric group S_n , with x even and y odd, such that $\langle a, x\rangle$ and $\langle a, y\rangle$ are primitive on the n symbols and both contain some cyclic permutation of prime order p (the prime may differ in the two cases) such that $p < n - 2$.

Now the following theorem of (Jordan,1873)[4] can be applied. *Let p be a prime and G a primitive group of degree $n = p + k$ with $k \geq 13$. If G contains an element of degree and order p, then G is either alternating or symmetric.*

1.4. **Basic theory of Covering Spaces.**

Definition 1.11. A map $p : \tilde{X} \longrightarrow X$ is called a covering map if for every point $x \in X$, there is a neighborhood U of x (an *evenly covered neighborhood*) so that $p^{-1}(U)$ is a disjoint union U_α of open sets in $\tilde{X}$, each mapped homeomorphically onto U by (the restriction of) p . X is called the *base space* of the covering; $\tilde{X}$ is called the *total space*.



Definition 1.12. Suppose $q : E \longrightarrow X$ is a covering map. An **automorphism of** q is a covering isomorphism from q to itself, that is, a homeomorphism $\phi : E \longrightarrow E$ such that $q \circ \phi = q$. Covering automorphisms are also variously known as **Deck transformation** or **covering transformations**

Definition 1.13. Let $Aut_q(E)$ denote the set of all automorphism of the covering $q : E \longrightarrow X$. It is easy to see it forms a group and called the automorphism group of the covering (covering group).

Definition 1.14. (*Normal(Galois) Cover*) A covering space $p : \tilde{X} \to X$ is called normal if for each $x \in X$ and each pair of lifts $\tilde{x}, \tilde{x}^{'}$ of x there is a deck transformation taking $\tilde{x}$ to $\tilde{x}^{'}$.

Definition 1.15. (*Covering Space Action*)Suppose we are given an action by a group Γ on a topological space E. It is called a covering space action if Γ acts by homeomorphism and every point $e \in E$ has a neighbourhood U satisfying the following condition:

$$for \ \ each \ \ g \in \Gamma, \ \ U \cap (g.U) = \emptyset \ \ unless \ g = 1$$

Given a covering space action of a group G on a space Y, We have

1 The quotient map $p : Y \to Y/G$ is a normal covering.
2 G is the group of deck transformation of this covering space if Y is path connected.

2. Construction

Let Γ denote the modular group $PSL(2, \mathbb{Z})$. Let $\mathcal{H}$ denote the complex upper half plane and $\mathcal{H}^*$ denote the extended upper half plane.

Definition 2.1. Define $\Gamma(N)$ to be the kernel of following natural map

$$PSL(2, \mathbb{Z}) \to PSL(2, \mathbb{Z}/N\mathbb{Z})$$

We call it *Principal Congruence subgroup of level N*

Notice that,

$$\Gamma(1) = PSL(2, \mathbb{Z})$$

Definition 2.2. (*Modular Curve* $X(N)$) Let $\Gamma(N)$ acts on $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. We define,

$$X(N) := \Gamma(N) \backslash \mathbb{H}^*$$

.

Remark 2.3. The j-invariant is a Γ invariant holomorphic and surjective map from $\mathbb{H} \to \mathbb{C}$, and descends to a holomorphic bijection

$$j : X(1) \to \mathbb{C}$$

which has a pole at infinity. $\Gamma(N)$ acts on $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ with quotient $X(N)$ which is compact, and the j-invariant becomes a holomorphic bijection

$$X(1) \to \mathbb{P}^1(\mathbb{C})$$

with holomorphic inverse. In particular, $X(1) \cong \mathbb{P}^1(\mathbb{C})$ as Riemann surfaces.

We know, A_n is $(2,3)$ generated (*Theorem 1.9*). More precisely A_n is generated by two elements, Let's give them a name, say a and x where order of a is 3 and order of x is 2. Also $PSL(2,\mathbb{Z})$ is a free product of cyclic group of order 2 and cyclic group of order 3 (*Theorem 1.8*). Therefore, We have a surjective map

$$\pi : \mathbb{Z}_2 * \mathbb{Z}_3 \simeq PSL(2,\mathbb{Z}) = \Gamma(1) \to G$$

defined by sending generators of $PSL(2,\mathbb{Z})$, (as in the *Theorem 1.8*) to a and x. Namely send B to x and C to a. So A_n can be thought of as quotient of $\mathbb{Z}_2 * \mathbb{Z}_3$

Let Γ_{A_n} denote the kernel of epimorphism π

We will use the following result from Hatcher's Algebraic Topology, [5] without proof. Proof is omitted because it is bit long.

Theorem 2.4. *Given a covering space action of a group G on a path-connected, locally path-connected space X, then each subgroup H in G determines a composition of covering spaces $X \to X/H \to X/G$. Show:*

1. *Every path-connected covering space between X and X/G is isomorphic to X/H for some subgroup H in G.*
2. *Two such covering spaces X/H_1 and X/H_2 of X/G are isomorphic iff H_1 and H_2 are conjugate subgroups of G.*
3. *The covering space $X/H \to X/G$ is normal iff H is a normal subgroup of G, in which case the group of deck transformations of this cover is G/H.*

Let's apply the above theorem, Take $G = PSL(2,\mathbb{Z}) = \Gamma(1)$, $X = \mathcal{H}^*$ and $H = \Gamma_{A_n}$. Action of $PSL(2,\mathbb{Z})$ is a covering space action as it is discrete subgroup of $PSL(2,\mathbb{R})$. As $\Gamma_{A_n} \trianglelefteq \Gamma(1)$, By the part 3 of above theorem,

$$\Gamma_{A_n} \setminus \mathcal{H}^* \to \Gamma(1) \setminus \mathcal{H}^*$$

is a Galois Covering with Galois group A_n.

Let's denote by $X_{A_n} := \Gamma_{A_n} \setminus \mathcal{H}^*$. Also $X(1) \simeq \mathbb{P}^1$. Then by above discussion, we conclude that

$$X_{A_n} \to \mathbb{P}^1$$

is a Galois Covering of $\mathbb{P}^1$ with Galois Group A_n.

References

1. Clara Löh, *Geometric Group Theory, an introduction*, http://www.mathematik.uni-regenburg.de/loeh/
2. I.M.S. Dey and James Wiegold, *Generators of Alternating group and Symmetric groups*, Journal of the Australian Mathematical Society, Volume 12, Issue 1, February 1971, pp. 63-68
3. G. A. Miller, *'On the groups generated by two operator'*, Bull. Amer. Math. Soc. 7 (1901), 424-426.
4. Helmut Wielandt, *Finite Permutation groups*, Academic Press, New York, 1964
5. Allen Hatcher, *Algebraic Topology*,
6. Martin W. Liebeck and Aner Shalev, *Classical Groups, Probabilistic Methods, and the (2, 3)-Generation Problem*, Annals of Mathematics, Second Series, Vol. 144, No. 1 (Jul., 1996), pp. 77-125
7. Robin Hartshorne, *Algebraic Geometry*, New York: Springer-Verlag, 1977; corrected 6th printing, 1993. GTM 52, ISBN 0-387-90244-9
8. J.S. Milne, *Elliptic curves*, BookSurge Publishers, 2006
9. John M. Lee, *Introduction to Topological Manifolds*, Graduate Texts in Mathematics, ISBN: 978-1-4419-7939-1

10. Andrew Sutherland, *http://math.mit.edu/classes/18.783/index.html*, 18.783 - Elliptic Curves

Current address: Department of Mathematics, IISER Mohali 140306
E-mail address: vikas.math123@gmail.com

Appendix B

Hilbert's Irreducibility Theorem

B.1 Introduction

The purpose of this chapter is to give a short and concise introduction to Hilbert's theorem. His theorem is important in the sense that, it provides motivation for working over $\mathbb{Q}(t)$. Roughly speaking, his theorem says that if a group G occurs as Galois group over $\mathbb{Q}(t)$ then G also occurs as Galois group over $\mathbb{Q}$. So it is a important tool in solving Classical Inverse Galois Problem(CIGP) which is concerned with occurrence of finite groups as Galois group over $\mathbb{Q}$. It has a historical significance also. Hilbert first studied this problem. This theorem was one of the major step towards the solution of CIGP. We will take Hilbert's Irreducibility Theorem for granted. For interested readers we would like to recommend **[1], [3], [2]**.

The subsequent theory is based on **[2]**.

B.2 Hilbert's Irreducibility Theorem

Theorem B.1. *The following conditions on k are equivalent:*

(1) For each irreducible polynomial $f(x, y)$ in two variables over k, of degree ≥ 1 in y, there are infinitely many $b \in k$ such that the specialized polynomial $f(b, y)$ (in one variable) is irreducible.

(2) Given a finite extension l/k, and $h_1(x, y), ..., h_m(x, y) \in l[x][y]$ that are irreducible as polynomials in y over the field $l(x)$, there are infinitely many $b \in k$ such that the specialized polynomials $h_1(b, y), ..., h_m(b, y)$ are irreducible in $l[y]$.

(3) For any $p_1(x, y), ..., p_t(x, y) \in k[x][y]$ that are irreducible and of degree > 1 when viewed as polynomial in y over $k(x)$, there are infinitely many $b \in k$ such that none of the specialized polynomials $p_1(b, y), ..., p_t(b, y)$ has a root in k.

Proof. For proof, see [2]. □

Definition B.2. A field k is called hilbertian if it satisfies (one of) the 3 equivalent conditions.

Using (1) and (2) we see that every finite extension of a hilbertian field is hilbertian.

Proposition B.3. *Suppose k is hilbertian, and $f(x_1, ..., x_s)$ is an irreducible polynomial in $s \geq 2$ variables over k, of degree ≥ 1 in x_s.*

(i) Then there are infinitely many $b \in k$ such that the polynomial $f(b, x_2, ..., x_s)$ (in $s-1$ variables) is irreducible over k.

(ii) For any nonzero $p \in k[x_1, ..., x_{s-1}]$ there are $b_1, ..., b_{s-1} \in k$ such that $p(b_1, ..., b_{s-1}) \neq 0$ and $f(b_1, ..., b_{s-1}, x_s)$ is irreducible (as polynomial in one variable).

Proposition B.4. *Let $f(x_1, \cdots, x_s)$ be a polynomial in $s \geq 2$ variables over k,of degree ≥ 1 in x_s. Then f is irreducible as polynomial in s variables if and only if f is irreducible and primitive when viewed as polynomial in x_s over the ring $D = k[x_1, \cdots, x_s]$. Note that f is irreducible over D if and only if f is irreducible over $F = k(x_1, \cdots, x_s)$.*

Corollary B.5. If k is hilbertian then so is every finitely generated extension field of k.

Proof. For proof, see [2]. □

We can conclude from above:

Every algebraic number field (of finite degree over $\mathbb{Q}$) is hilbertian.

By the previous result, we can easily show that,

Theorem B.6. *Suppose k is hilbertian. If a finite group G occurs as Galois group over $k(x_1, \cdots, x_m)$ then G also occurs as Galois group over k.*

Definition B.7. Let G be a finite group. We say G occurs regularly over k if for some $m \geq 1$ there is a Galois extension of $k(x_1, \cdots, x_m)$, regular over k, with Galois group isomorphic to G.

Corollary B.8. Suppose G occurs regularly over k. Then G occurs regularly over every extension field k_1 of k. Thus G is a Galois group over k_1 if k_1 is hilbertian.

Proof. **Proof is taken from [2]** Suppose $x_1, ..., x_m$ are independent transcendentals over k_1, and set $x = (x_1, ..., x_m)$. We can assume $G = G(K/k(x))$, with K regular over k. Set $n = |G| = [K : k(x)]$. Write K in the form $K = k(x)[y]/(f)$, for some

$f(x, y) \in k(x)[y]$. Then f is irreducible over $\bar{k}_1(x)$. Hence $K_1 = k_1(x)[y]/(f)$ is a field extension of $k_1(x)$ of degree n, regular over k_1. Clearly, K_1 is Galois over $k_1(x)$ (because all the roots of f over $k_1(x)$ are already contained in K). Now $G(K_1/k_1(x))$ and $G(K/k(x))$ have the same order, and the former group embeds into the latter via restriction. Hence they are isomorphic. This proves the first claim. The second follows by Theorem B.6. □

Theorem B.9. *(Hilbert's irreducibility theorem) The field $\mathbb{Q}$ is hilbertian.*

Appendix C

Alternating group is $(2, 3)$ generated: A Python implementation

First question would be what does it mean to say A_n is $(2, 3)$ is generated. $(2, 3)$ generation means that there is an element of order 2 and an element of order 3 generating A_n. We made a computer program based on an algorithm developed by **I.M.S. Dey and James Wiegold**.

User inputs the n, the degree of alternating group and the program in output return the generators of alternating group A_n with relations.

We have used Python programming language to do all the coding.

See [17], [18] for more details.

```
#These Classes were originally defined Kragen Javier Sittler
( http://canonical.org/~kragen/about/).

class Permutation:
    """Eleemnt of Symmetric group.

    """
```

```
def ___init___(self, items):
    self.items = tuple(items)
    assert set(self.items) == set(range(len(self.items)))

def ___mul___(self, other):
    "Function␣composition."
    return Permutation(self(other(item))
                       for item in range(max(self.end(), other.end())))

def ___eq___(self, other):
    return all(self(item) == other(item)
               for item in range(max(self.end(), other.end())))

def ___hash___(self):
    return 1 + hash(self.items)

def ___pow___(self, power):
    """Compose a permutation with itself N times."""
    if power < 0:
        return self.inverse() ** -power
    if power == 0:
        return cycle()
    if power == 1:
        return self
    return (self * self) ** (power // 2) * self ** (power % 2)

def ___call___(self, index):
    return self.items[index] if index < len(self.items) else index

def ___repr___(self):
    "Using␣Python␣cycle␣notation."
    cycles = list(self.cycles())
    if not cycles:
        return 'cycle()'

    return '␣*␣'.join('cycle(%s)' % ',␣'.join(map(repr, cycle))
                      for cycle in cycles)
```

```
def ___str___(self):
    "Using␣NORMAL␣cycle␣notation."
    cycles = list(self.cycles())
    if not cycles:
        return '()'

    return '␣'.join('(%s)' % '␣'.join(map(str, cycle)) for cycle in cycles)

def cycles(self):



    """
    leftovers = set(self.items)
    min_leftover = 0

    while leftovers:
        while min_leftover not in leftovers:
            min_leftover += 1
            assert min_leftover < len(self.items)

        ii = min_leftover
        cycle = []
        cycle_set = set()
        while ii not in cycle_set:
            cycle.append(ii)
            cycle_set.add(ii)
            leftovers.remove(ii)
            ii = self(ii)

        if len(cycle) > 1:
            yield cycle

def end(self):
    return len(self.items)

def inverse(self):
```

```
        items = range(len(self.items))
        for index, item in enumerate(self.items):
            items[item] = index

        return Permutation(items)

def cycle(*seq):
    "Generate a permutation from a single cycle."
    items = range(max(seq or [-1])+1)
    for ii in range(len(seq)):
        items[seq[ii]] = seq[(ii+1) % len(seq)]

    return Permutation(items)

def reversal(start, end):
    return Permutation(range(start) + list(reversed(range(start, end))))
##############################################################################

def a_n(n):
    an=cycle(1)
    k=n/3
    for i in range(k):
        an=an*cycle(1+3*i,2+3*i,3+3*i)
    return an

#########################################
def c_k(k):
    ck=cycle(1)
    for r in range(1,k+1):
        #print r
        ck=ck*(cycle(6*r,6*r+3)*cycle(6*r+1,6*r+4)*cycle(6*r+2,6*r+5))
        #print ck
    return ck
#########################################

def alt_grp_gen(n):
    m=n//6
```

```
#####################################################

    if (n%6==0 and m>3):
        a=a_n(n-3)
        b1=cycle(1,4)*cycle(2,n-2)*cycle(3,n-1)*cycle(n-6,n-3)*cycle(n-5,n)*c_k(m-2)
        b2=b1*cycle(n-11,n-8)
        if (m%2==0):
            x=b2
            relation="(ax)^{78} ia a 11- cycle"
        else:
            x=b1
            relation="(ax)^{42} is an 11- cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation


#####################################################

    elif (n%6==1 and m>2):
        a=a_n(n-1)
        b1=cycle(1,4)*cycle(2,n)*cycle(3,n-1)*cycle(n-6,n-3)*cycle(n-5,n-2)*c_k(m-2)
        b2=b1*cycle(n-12,n-9)
        if m==3:
            x=b1
            relation='(ax)^{6} is a 13 cycle'
        else:
            if (m%2==0):
                x=b2
                relation="(ax)^18 is a 13 cycle"
            else:
                x=b1
                relation="(ax)^6 is a 13 cycle"

        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
```

```
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation

#########################################################

    elif (n%6==2 and m>2):
        a=a_n(n-2)
        b1=cycle(1,4)*cycle(2,n-1)*cycle(3,n)*cycle(n-8,n-5)*cycle(n-6,n-3)*c_k(m-2)
        b2=b1*cycle(n-7,n-4)
        if (m%2==0):
            x=b2
            relation="(ax)^6 is an 11 cycle "
        else:
            x=b1
            relation="(ax)^18 is an 11 cycle "

        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation

#########################################################

    elif (n%6==3 and m>2):
        a=a_n(n-3)
        b1=cycle(1,4)*cycle(2,n-2)*cycle(3,n-1)*cycle(n-3,n)*c_k(m-1)
        b2=b1*cycle(n-8,n-5)
        if (m%2==0):
            x=b2
            relation="(ax)^{60} is an 11 cycle "
        else:
            x=b1
            relation="(ax)^12 is an 11 cycle"
```

```
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation


#########################################

    elif (n%6==4 and m>2):
        a=a_n(n-1)
        b1=cycle(1,4)*cycle(2,n)*cycle(3,n-3)*cycle(n-10,n-7)*cycle(n-8,n-5)*c_k(m-2)
        b2=b1*cycle(n-9,n-6)
        if (m%2==0):
            x=b2
            relation= " (ax)^6 is a 13 cycle"
        else:
            x=b1
            relation= "(ax)^18 is a 13 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation

#########################################
    elif (n%6==5 and m>2):
        a=a_n(n-2)
        b1=cycle(1,4)*cycle(2,n-1)*cycle(3,n)*cycle(n-5,n-2)*c_k(m-1)
        b2=b1*cycle(n-10,n-7)
        if (m%2==0):
            x=b2
            relation= "(ax)^12 is an 11 cycle"
        else:
            x=b1
            relation= "(ax)^6 is an 11 cycle"
```

```
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation

##########################################

    elif (n==2 or n==3 ):
        print "trivial, nothing interesting"
    elif(n==7 or n==6 or n==8):
        print "Sorry to inform you but it is not (2,3) generarted, inconvenience is regreted"
    elif (n==4):
        print "(1,2,3) and (1,2)(3,4) generate the group"

##########################################
    elif (n==5):
        a=a_n(3)
        x=cycle(1,4)*cycle(2,5)
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x



##########################################
    elif(n==9):
        a=a_n(9)
        x=cycle(1,4)*cycle(2,9)*cycle(3,7)*cycle(5,6)
        relation="(ax)^5 is a 3 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation

##########################################
    elif(n==10):
```

```
        a=a_n(9)
        x=cycle(1,4)*cycle(6,9)*cycle(3,10)*cycle(2,8)
        relation="(ax)^7 is a 3 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation

##########################################

    elif(n==11):
        a=a_n(9)
        x=cycle(1,4)*cycle(2,10)*cycle(3,11)*cycle(6,9)
        relation="[a,x,a]^5 is a 3 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation


##########################################
    elif (n==12):
        a=a_n(9)
        x=cycle(1,4)*cycle(2,10)*cycle(3,8)*cycle(6,9)*cycle(7,11)*cycle(5,12)
        relation="(ax)^7 is a 5 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation



##########################################
    elif(n==13):
        a=a_n(12)
        x=cycle(1,4)*cycle(2,13)*cycle(3,5)*cycle(6,9)*cycle(7,10)*cycle(8,11)
        relation="(ax)^8 is a 3 cycle"
```

```
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation


#########################################
    elif(n==14):
        a=a_n(12)
        x=cycle(1,4)*cycle(2,13)*cycle(3,14)*cycle(6,9)*cycle(7,10)*cycle(8,11)
        relation= "(ax)^11 is a 3 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation


#########################################
    elif(n==15):
        a=a_n(15)
        x=cycle(1,4)*cycle(3,14)*cycle(6,9)*cycle(7,10)*cycle(12,15)*cycle(5,13)
        relation=" (ax)^35 is a 3 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation


#########################################
    elif(n==16):
        a=a_n(15)
        x=cycle(1,4)*cycle(2,16)*cycle(6,9)*cycle(7,10)*cycle(8,11)*cycle(3,13)
        relation=" (ax)^13 is a 3 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation
```

```
##########################################
    elif(n==17):
        a=a_n(15)
        x=cycle(1,4)*cycle(2,16)*cycle(3,17)*cycle(12,15)*cycle(6,9)*cycle(7,10)*cycle(8,11)
        relation=" (ax)^5 is 11 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation



##########################################
    else:
        a=a_n(15)
        x=cycle(1,4)*cycle(2,16)*cycle(3,17)*cycle(12,15)*cycle(13,18)*cycle(6,9)*cycle(7,10
        relation=" (ax)^11 is a 7 cycle"
        print colored("<a,x> generates the group where", 'cyan')
        print colored("a is ", 'cyan'), a
        print colored("x is ", 'cyan'), x
        print colored("and ",'cyan'), relation


##########################################
import sys
from termcolor import colored

print colored("Hello Prof. Paranjape,", "red", attrs=['bold'])
print " "
print colored("This program is based on a research paper titled \"Generators For Alternatin
print colored('Note: For n=6,7 and 8, Result is not true' , 'green')

print "\n"
print colored("Input:",'red')
print "Enter the degree of Alternating group, A_{n}, a positive integer."
```

```
print colored("Output:", 'red')
print "Explicit generators for the group."
print "\n"
vvv=raw_input('Press the enter to continue: ')
n=input('Enter the degree of the alternating group (A_{n}): ')
alt_grp_gen(n)
```

Bibliography

[1] J. P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Jones and Bartlett Publishers.

[2] Helmut Volklein, *Groups as Galois Groups*, Cambridge University Press, 1996.

[3] Gunter Malle B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg, 1999.

[4] Robin Hartshorne, *Algebraic Geometry*, New York: Springer-Verlag, 1977; corrected 6th printing, 1993. GTM 52, ISBN 0-387-90244-9

[5] J.S. Milne, *Elliptic curves*, BookSurge Publishers, 2006.

[6] Andrew Sutherland, *http://math.mit.edu/classes/18.783/index.html*, 18.783 - Elliptic Curves.

[7] J.P. Serre, *Local Fields*, Springer-Verlag, 1979 (GTM 67).

[8] *Geometric Invariant Theory*, David Mumford and al., Springer 1994

[9] *Lectures on Invariant Theory*, I. Dolgachev, Cambr.Univ.Press, 2003.

[10] *Galois coverings of arithmetic line*, D. Harbater, Lect. Notes in Math. 1240, Springer-Verlag, 1987, 165-195

[11] Joseph H. Silverman *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer-Verlag New York, 2009.

[12] *Galois Groups and Fundamental Groups*, Tamas Szamuely

[13] *SGA 1*, A. Grothendieck

[14] *TIFR-Lecture Notes on Algebraic Groups*, Dipendra Prasad

[15] J-P. Jouanolou. Theoremes de Bertini et applications, Brikhauser, 1983

[16] Clara Löh, *Geometric Group Theory, an introduction*, http://www.mathematik.uni-regenburg.de/loeh/

[17] I.M.S. Dey and James Wiegold, *Generators of Alternating group and Symmetric groups*, Journal of the Australian Mathematical Society, Volume 12, Issue 1, February 1971, pp. 63-68.

[18] G. A. Miller, *'On the groups generated by two operator'*, Bull. Amer. Math. Soc. 7 (1901), 424-426.

[19] Helmut Wielandt, *Finite Permutation groups*, Academic Press, New York, 1964.

[20] Martin W. Liebeck and Aner Shalev, *Classical Groups, Probabilistic Methods, and the (2, 3)-Generation Problem*, Annals of Mathematics, Second Series, Vol. 144, No. 1 (Jul., 1996), pp. 77-125

[21] Daniel Gorenstein, *Finite Groups*, American Mathematical Soc., 2007.

[22] J. P. Serre, *Linear Representation of Finite Groups*, Springer-Verlag, 1977

[23] Benjamin Steinberg, *Representation Theory of Finite Groups*, Universitext, Springer-Verlag New York, 2012

[24] Gordan James and Martin Liebeck, *Representation And Characters of Groups*, Second Edition, Cambridge University Press, 1993.

[25] Allen Hatcher, *Algebraic Topology*, Cambridge University Press,2002.

[26] John M. Lee, *Introduction to Topological Manifolds*, Graduate Texts in Mathematics, Springer, 2011.

[27] John Terilla, CUNY, *Covering Spaces*, Online notes.

[28] M. A. Armstrong, *Basic Topology*, Springer International Edition, 1983.

[29] Gabriel Daniel Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Birkhauser Boston, 2006.

[30] Fried, Michael D., Jarden, Moshe *Field Arithmetic* , Springer-Verlag Berlin Heidelberg, 2005.

[31] C.P. Ramanujam, *Lectures on The Theory of Algebraic Functions of One Variable by M. Deuring*, TIFR Lecture Notes, 1959.

[32] Wei Lei, *Algebraic Function Fields, Lecture 2, http://www1.spms.ntu.edu.sg/ weil0005.*

[33] Michael Artin, *Algebra*, $2^n d$ Edition, PHI publication.

[34] Jacobson, N. *Basic Algebra I*, San Francisco: Freeman, 1974.

[35] Professor J. H. Conway, others Professor R.T. Curtis, Professor R.A. Wilson, Professor S.P. Norton, and Professor R.A. Parker, *ATLAS of Finite Groups Maximal Subgroups and Ordinary Characters for Simple Groups*, 1985, Oxford University Press.

[36] *CTblLib1.2.1,*, Breuer, T. , *The GAP Character Table Library,*, *May, 2012*, http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib

[37] Alexander Hulpke, *Abstract Algebra in GAP*, 2011.

[38] GAP - Groups, Algorithms, Programming -a System for Computational Discrete Algebra, `https://www.gap-system.org/`

[39] Martin SchÃűnert together with Hans Ulrich Besche, Thomas Breuer, Frank Celler, Volkmar Felsch, Alexander Hulpke, JÃijrgen Mnich, GÃűtz Pfeiffer, Udo Polis, Heiko Theissen (Lehrstuhl D fÃijr Mathematik, RWTH Aachen) *GAP Manual Release 3.4*

[40] Alexander Hulpke, *Mathematics 666, Advanced Algebra.*

[41] Wikipedia.com, *relevant pages on mathematics*, en.wikipedia.org.

[42] *math.stackexchange.com* and *mathoverflow.net*

[43] Herbert Pahlings, Klaus Lux, *Representations of Groups A Computational Approach*, Cambridge Studies in Advance Mathematics, 124.

[44] Gerald J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

[45] Leila Schneps, *Galois Groups and Fundamental Groups*, Cambridge University Press, 2003.

[46] *Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata*, Academic Press, 1988.

[47] Emil Artin, *Galois Theory*, Notre Dame Mathematical Lectures Number 2, 1942.

[48] C.U. jensen and N. Yui. *Quaternions Extensions*, Algebraic Geometry and Commutative Algebra, in honor of M. Nagata, 1987.

[49] S. Abhyankar, *Coverings of Algebraic Curves*, Amer, J. of Math., 1957.

[50] J. P. Serre, *Lectures on the Mordell-Weil theorem*, translated and edited by M. Brown from notes by M. Waldschmidt, Vieweg-Verlag, 1989.

[51] J. G. Thompson, *Some finite groups which appear as* $Gal(L/K)$*, where* $K \subseteq \mathbb{Q}(\mu_n)$, J. of Algebra 89 (1984), 437-499.

[52] J. G. Thompson, PLS_3 *and Galois groups over* $\mathbb{Q}$, Proc. Rutgers group theory year 1983-1984, cambridge University press, 1984, 309-319.

[53] Emil Artin, *Algebraic Numbers and Algebraic Functions*, 1967.

[54] Shafarevich, Igor R., *Basic Algebraic Geometry 1*, Springer-Verlag Berlin Heidelberg, 1994.

[55] M. F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[56] E Artin, J.T Tate, "A note on finite ring extensions," J. Math. Soc Japan, Volume 3, 1951, pp. 74âĂŞ77

[57] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. 78(1918), 221-229.

[58] D. Hilbert, *Ueber die Irreduzibilitat ganzer rationaler Funktionenmit ganzzahligen Koeffzienten*, J. Crelle 110 (1892), 104-129.

[59] Marc Hindry, Joseph H. Silverman, *Diophantine Geometry: An Introduction*, Springer, Graduate Text in Mathematics.

[60] oxeimon (https://mathoverflow.net/users/15242/oxeimon), Reference for the proof of this lemma. "Double group trick", URL (version: 2016-11-14): https://mathoverflow.net/q/254668

[61] Rick Miranda, *Algebraic Curves and Riemann Surfaces*, Graduate Studies in Mathematics, AMS, 1995.