University of Nairobi

School of Mathematics

ISSN: 2410-1397

Master Dissertation in Mathematics

Inverse Galois Problem

Research Report in Mathematics, Number 13, 2017

James Kigunda Kabori

August 2017

Submitted to the School of Mathematics in partial fulfilment for a degree in Master of Science in Pure Mathematics

Master Dissertation in Mathematics **University of Nairobi**
August 2017

Inverse Galois Problem

Research Report in Mathematics, Number 13, 2017

James Kigunda Kabori

School of Mathematics
College of Biological and Physical sciences
Chiromo, off Riverside Drive
30197-00100 Nairobi, Kenya

Master Thesis
Submitted to the School of Mathematics in partial fulfilment for a degree in Master of Science in Pure Mathematics

Prepared for The Director
Board Postgraduate Studies
University of Nairobi

Monitored by Director, School of Mathematics

Abstract

The goal of this project, is to study the Inverse Galois Problem. The Inverse Galois Problem is a major open problem in abstract algebra and has been extensive studied. This paper by no means proves the Inverse Galois Problem to hold or not to hold for all finite groups but we will, in chapter 4, show generic polynomials over $\mathbb{Q}$ satisfying the Inverse Galois Problem.

Master Thesis in Mathematics at the University of Nairobi, Kenya.
ISSN 2410-1397: Research Report in Mathematics

DISTRIBUTOR: School of Mathematics, University of Nairobi, Kenya

Declaration and Approval

I the undersigned declare that this dissertation is my original work and to the best of my knowledge, it has not been submitted in support of an award of a degree in any other university or institution of learning.

Signature Date

JAMES KIGUNDA KABORI
Reg No. I56/81944/2015

In my capacity as a supervisor of the candidate's dissertation, I certify that this dissertation has my approval for submission.

Signature Date

Dr. Damian Maingi
School of Mathematics,
University of Nairobi,
Box 30197, 00100 Nairobi, Kenya.
E-mail: dmaingi@uonbi.ac.ke

Dedication

To my amazing fiancée, Maryruth Njeri, without whom I would have been satisfied with my mediocrity.

Contents

Acknowledgments

First, I want to thank my parents for all they have done to get me here. They have gone way above what most would and I cannot say how much I am grateful. I also want to thank my sister Caroline Kiende for the encouragement and Virginia, Tabitha and Ryan for providing the, mostly unsolicited, breaks from the long research sessions. I also want to thank my colleagues for the interesting mathematical discussions. Lastly I want to thank all my friends who were a part of my support group with a special mention to James Wamutitu who pushed me to pursue this program at a time I contemplated pursuing other less important ventures. Finally I want to thank all my lecturers especially Dr. Maingi for his priceless guidance.

James Kigunda Kabori

Nairobi, 2017.

1 Introduction

The Inverse Galois Problem is posed as such. Can any finite group G be realised as a Galois group over $\mathbb{Q}$? In more precise wording let G be a finite group. Does there exist a Galois extension $E/\mathbb{Q}$ such that $\mathrm{Gal}(E/\mathbb{Q}) \cong G$?
The Inverse Galois problem was formulated in the early 19th century and remains open to this day. Ideally a solution in the positive would give a family of polynomials over $\mathbb{Q}$ whose Galois groups are isomorphic to finite groups. If the Inverse Galois problem were to have a solution in the negative the structure of the obstructions of those groups would be of exceptional interest.
This dissertation will be divided into the following chapters,

Chapter 2 - Galois Theory Basics: This will be an elementary introduction to Galois theory. Galois Theory in itself is a rich field that would in its entirety be beyond the scope of this paper. As such we will only introduce in this chapter the elements necessary to understand what the inverse Galois theory is about.

Chapter 3 - Major Results: Since the 1800's a lot of work has been done in Galois theory and more precisely on the Inverse Galois problem and provided answers for some classes of groups. In this chapter we will see some of the major results achieved in its solution.

Chapter 4 - Galois Groups as Permutation Groups: Since all finite groups can be realised as a subgroup of the symmetric group we will in this chapter consider Galois groups as subgroups of S_n at the end of the chapter we will explicitly show some subgroups of low order S_n as Galois groups.

2 Galois Theory Basics

To set up the Inverse Galois Problem we need a basic understanding of Galois theory and so we must first discuss the basics of field theory that are the building blocks of Galois theory. The concepts explained here are not restricted to the field $\mathbb{Q}$ but apply to all fields.

2.1 Field Extensions

Definition 2.1.1 For the fields E and F, if $F \subset E$ we say that E is an extension of F and write the extension as E/F. The extension E/F is therefore a base field F adjoined at least one element not in F. E can then be considered a vector space over F and see E as either finite or infinite field extension depending on its dimension.

Definition 2.1.2 For the fields E and F with E an extension of F, any $x \in E$ is said to be algebraic over the base field F if we can find a polynomial

$$a_0 + a_1 x + ... + a_k x^k = 0$$

with the coefficients $a_k (k \geq 1)$ in F and not every a_k equal to zero. If such a polynomial cannot be found then x is called a transcendental element.
The extension E/F is called an algebraic extension if each element $x \in E$ is algebraic over F.

Consider a field extension E/F. Taking E as a vector space over F we denote its dimension as $[E : F]$. A finite dimension field extension is called a finite extension while one with an infinite dimension is called an infinite extension. In the case of the Inverse Galois Problem we will concentrate on finite field extensions.

Proposition 2.1.3 For any finite extension K of F, K is algebraic over F.

Proof: For any $x \in K, x \neq 0$, the powers of x,

$$1, x, x^2, ..., x^m$$

can't have linear independence over F for every $m \geq 1$ else the dimension of K over F would not be finite. Then a relation, which is linear, between the powers of x gives that K is algebraic over F

Definition 2.1.4 Consider a field F and a polynomial $k \in F[X]$. We call an extension S/F the splitting field of f if f splits into factors that are linear in S, that is

$$k(X) = c(X - a_1)\dots(X - a_n)$$

with $a_j \in F, j = 1...n$ so that $S = F(a_1, ..., a_n)$ is generated by all the roots of k. It is not necessary that every root of k be distinct.
Every polynomial $k(X) \in F[X]$ will have a splitting field which is a field over F generated by the polynomial's roots.

Example 2.1.5 - The splitting field generated by the polynomial over the rational field $f(X) = X^3 - 3$ is $\mathbb{Q}(w, \sqrt[3]{3})$ because we have the roots of $f(X)$ as $\sqrt[3]{3}$, $w\sqrt[3]{3}$ and $w^2\sqrt[3]{3}$ where $w = e^{2\pi i/3}$.

Definition 2.1.6 Let $S = K(a_1, ..., a_n)$ be the splitting field of a polynomial $k \in K[X]$. S is called a normal extension of the polynomial k over K if every root of k is in S.
In other words if a root of the polynomial f is in S then it has all roots in S.

Definition 2.1.7 Consider a field F. If every $f \in$ F[X] with degree greater than or equal to 1 has one or more roots in F then the field is said to be an algebraic closure. For any algebraic extension E/F that is algebraically closed we say that E is an algebraic closure of F.

Definition 2.1.8 Consider a polynomial f over a base field F. We say that f is a separable polynomial if every root of the polynomial is distinct in the algebraic closure ofthe base field.

Definition 2.1.9 An algebraic field extension E/F is said to be separable if $\forall\ e \in E$ its minimal polynomial over the base field is separable.

Algebraic extensions of both finite and infinite fields are separable.

2.2 Galois Groups and the Fundamental Theorem of Galois Theory

Definition 2.2.0.1 By the automorphism of a field F we shall mean in the usual sense a map γ from E to itself such that

$$\gamma(x+y) = \gamma(x) + \gamma(y)$$

$$\gamma(xy) = \gamma(x)\gamma(y)$$

$\forall x, y \in E$. All these automorphisms then form what we call an automorphism group of the field. The automorphism group of E is denoted Aut(F).

Consider a finite field E/F so that $E = F[a_1, ..., a_n]$. The automorphisms group of E/F that we will denote as $\text{Aut}_F E$ is the group of automorphisms of E fixing F, that is

$$Aut_F E = \{\phi \in Aut(E) | \phi(a) = a, \forall a \in F\}$$

which map each a_i to a root of its minimal polynomial therefore $\text{Aut}_F E$ is finite.

Definition 2.2.0.2 We consider a field E and its group of automorphisms G. A fixed field of this group denoted F^G is the field $\{a \in E | \phi(a) = a, \forall \phi \in G\}$

Definition 2.2.0.3 Consider E/F an algebraic extension, its called Galois if its both normal and separable. $\text{Aut}_F E$ is said to be the Galois group of E/F.

Proposition 2.2.0.4 The finite extension K/F and $H = \text{Aut}_F E$ these are equivalent conditions.

1. $F = K^H$
2. K/F is a Galois extension
3. K/F is normal and separate.
4. K is the splitting field for a polynomial $g \in F[X]$.

Lemma 2.2.0.5 For a field F and G its group of automorphisms $F^G \subset F$

Proof. Let $m, n \in F^G$. Which means $\phi(m) = m$ and $\phi(n) = n$ then

$$\phi(m \pm n) = \phi(m) \pm \phi(n)$$

$$\phi(mn) = \phi(m)\phi(n)$$

so $m \pm n$ and mn are in F^G. Furthermore if $m \neq 0$ we have $\alpha(m^{-1}) = \alpha(m)^{-1} = m^{-1}$ and so $m-1$ is also in F^G. This means that $F^G \subset F$.

Before we proceed to the theorem central to galois theory we should mention something about intermediate fields. For an algebraic extension M/F we call the field K an intermediate field if $M \supseteq K \supseteq F$

Lemma 2.2.0.6 Let $M \supset K \supset N$ be fields with M/N galois. We have

1. M/K is galois.
2. K/N is galois iff $\alpha(K) = K, \forall \alpha \in Aut_F E$.

Proof: 1. M is the splitting field of a separable polynomial $g \in N[X]$. Since N $\subseteq$ K and K $\subseteq$ M we have the tower $E = F(\beta_1, ..., \beta_m, ..., \beta_n) \supset K = N(\beta_1, ..., \beta_m) \supset N$ with every β_i algebraic over N. β_i for i = m+1,...,n is algebraic over K and so M/K is galois.
2. IF K/N is galois we have that for each $\alpha \in K$, K has every root of a minimal polynomial of α over N. As $\phi(\alpha)$ must be such a root for any $\phi \in \text{Aut}_N M$ so $\phi(\alpha) \in K$. As a result $\phi K \subset K$ for all ϕ and since $[\phi K : N] = [K : N]$ we have $\phi K = K$.
Suppose now that $\phi N = N$ for all ϕ. Then $\text{Aut}_N M \to \text{Aut}_N K$ is surjective. Therefore the fixed field of $\text{Aut}_N M$ is the same as the one for $\text{Aut}_N K$ and so K/N is galois.

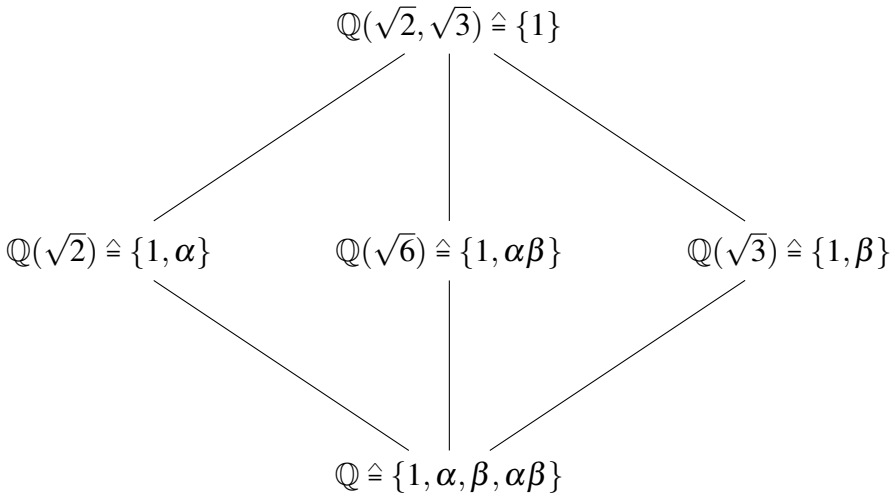
2.2.1 The Fundamental Theorem of Galois Theory

Theorem 2.2.1.1 Consider a Galois extension E/F with Galois group G=Aut$(_F E)$. Let K be the set of all intermediate fields and H the set of all subgroups of G. The maps $\alpha : K \longrightarrow H$ and $\beta : H \longrightarrow K$ defined as $\alpha(J) =$Aut(E/J) and $\beta(L) = K^L$ for $J \in K, L \in H$ give a well defined and bijective correspondence between K and H with the properties,

1. When $K_1 \in K$ and $K_2 \in K$ correspond to $H_1 \in H$ and $H_2 \in H$ respectively then $K_1 \subset K_2$ iff $H_2 < H_1$.
2. If $J \in K$ corresponds to $L \in H$ then $[E : J] = [L]$ and $[J : F]$ and $[G : L]$.
3. $\forall K_i \in K$, E/K_i is Galois.
4. Let $J \in K$ corresponds to $L \in H$. Then J/F is Galois iff L is normal in G and if so $Aut(J/F) \cong Aut(E/F)/Aut(E/J)$
5. If $K_1 \in K$ and $K_2 \in K$ correspond to $H_1 \in H$ and $H_2 \in H$ respectively, then $K_1 \cap K_2$ corresponds to $\langle H_1, H_2 \rangle$, and the compositum $K_1 K_2$ corresponds to $H_1 \cap H_2$.

We can illustrate the correspondence with an example

Example 2.2.1.2 $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is the splitting field for $f=(x^2-2)(x^2-3)$ having an automorphism group of order 4 which is isomorphic to the Klein four-group with the automorphisms 1(identity) that fixes everything, α that fixes $\sqrt{2}$ while mapping $\sqrt{3}\mapsto -\sqrt{3}$, β that fixes $\sqrt{3}$ and maps $\sqrt{2}\mapsto -\sqrt{2}$, and the composition $\alpha\beta$ fixing $\sqrt{6}$. We can then see the correspondence between the subgroups and the intermediate fields in the lattice diagram below



3 Major Historical Milestones

3.1 Noether Problem

Emmy Noether asked the following.

For a finite group G, if G acts faithfully on a finite set of indeterminates $x_1, x_2, ..., x_n$ is $F(x_1, x_2, ..., x_n)^G$ a rational extension(purely transcendental) of F?

In our case the field F is $\mathbb{Q}$ though the problem can be asked over any field and not just $\mathbb{Q}$.

As it turns out the answer is not always in the affirmative which then raise a different question as to which groups G does the Noether Problem fail to have an affirmative solution and whether these groups can be easily parameterised. For the alternating groups the problem remains open with a solution for $A_n, n \geq 6$. Maeda in 1989 showed the answer for A_5 in the affirmative.

Gröbner in 1934 also gave an affirmative answer for the quarternion group Q_8. In 1925 Furtwangler showed a positive solution for every solvable transitive subgroup T of S_p for p=3,5,7,11 over $\mathbb{Q}$.

3.2 Hilbert Irreducibility Theorem

Definition 3.2.0.1 Let $f(t, X) \in K(t)[X]$ be an irreducible polynomial over two variables in an algebraic number field K. K is called Hilbertian or is said to be endowed with the hilbertian property if there exists infinitely many regular point of $f(t, X)$ that is there exists infinitely many $t_0 \in K$ such that $f(t_0, X)$ is irreducible in $K[X]$.

Theorem 3.2.0.2 (Hilbert) $\mathbb{Q}$ is Hilbertian.

This theorem was the first used to prove that S_n can be realised as a Galois group over $\mathbb{Q}$

3.2.1 S_n as a Galois group over $\mathbb{Q}$

Let $G = S_n$ act on $M = \mathbb{Q}(t_1, ..., t_n)$. The field of S_n-invariants is $K = M^{S_n} = \mathbb{Q}(e_1, ..., e_n)$ where

$$e_i = \sum_{1 \leq l_1 < ... < l_i \leq n} X$$

denotes the i^{th} elementary symmetric polynomial for i = 1,2,...,n. K is a purely transcendental extension of degree n, and M is a Galois extension of K with Galois group S_n. Furthermore, M is the splitting field of the irreducible polynomial

$$f(e_1,...,e_n,X) = X^n - e_1X^{n-1} + e_2X^{n-2} + \cdots + (-1)^n e_n \in K[X]$$

We may assign to each e_i a value $a_i \in \mathbb{Q}$ for i = 1,2,...,n. The Hilbert Irreducibility Theorem then asserts that there exist infinitely many n-tuples $(a1, a2, .., an) \in \mathbb{Q}^n$ such that the polynomial

$$f(X) = X^n - a_1X^{n-1} + a_2X^{n-2} + \cdots + (-1)^n a_n \in \mathbb{Q}[X]$$

is irreducible over $\mathbb{Q}$ and the Galois group of the splitting field is isomorphic to S_n.

3.3 Kronecker-Weber Theorem

A mth root of unity for an integer $m \geq 1$ is the solution to the polynomial $x^m - 1$ of which there are at most m different solutions expressed as $e^{2\pi ik/m}$. The roots of unity make up a cyclic group.
An extension $E = F(\zeta_m)$ of F where ζ_m is a primitive mth root of unity is called a cyclotomic extension of F.
We now state the global Kronecker-Weber theorem.

Theorem 3.3.1 Each extension of the rational field that is both finite and abelian is contained in some cyclotomic extension of the field.

The Kronecker-Weber theorem helps solve the Inverse Galois Problem for finite abelian groups as below.

Theorem 3.3.2 Each group that is finite abelian is realizable as the Galois group of some finite extension of the rational field.

Proof: Set $G = C_1 \times ... \times C_m$ as a finite abelian group where $(C_i)_{1 \leq i \leq m}$ are its cyclic factors. To prove the theorem we need to realize all the $C_i = \mathbb{Z}/n\mathbb{Z}$ for positive integers n as linearly disjoint Galois groups of finite Galois extensions of $\mathbb{Q}$ and G will be the Galois group of the compositum of these extensions.
To this end for each $C_i = \mathbb{Z}/n\mathbb{Z}$ we find a distinct prime $p \equiv 1$(mod n) and now consider $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ which is an Abelian extension with Galois group $\mathbb{Z}/(p-1)\mathbb{Z}$ since n divides p-1 there is an extension E_i with C_i as the Galois group.
Since each E_i is contained in a cyclotomic extension for a distinct p their intersection is $\mathbb{Q}$ and so are linearly disjoint. We now pick

$$E = \prod_{i=1}^{m} E_i$$

and so $G = Gal(E/\mathbb{Q})$. $\square$

Example 3.3.3 Let

$$G = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$$

be a finite group. We intend to find Galois extensions over $\mathbb{Q}$ of the factors of G in such a way that they are linearly disjoint.
Starting with $\mathbb{Z}/7\mathbb{Z}$ the first prime $p \equiv 1(\text{mod } 7)$ is 29. The extension $\mathbb{Q}(\zeta_{29})/\mathbb{Q}$ has $\mathbb{Z}/28\mathbb{Z}$ as a Galois group and since 7 is a divisor of 28 by Theorem 3.3.1 there exists a subfield A_1 of $\mathbb{Z}/28\mathbb{Z}$ whose Galois group is $\mathbb{Z}/7\mathbb{Z}$.
Doing the same for $\mathbb{Z}/11\mathbb{Z}$ we find a prime $p \equiv 1(\text{mod } 11)$ and the first such p is 23. Gal$(\mathbb{Q}(\zeta_{23})/\mathbb{Q}) \cong \mathbb{Z}/22\mathbb{Z}$. This means that by Kronecker-Weber we can also find a subfield A_2 of $\mathbb{Q}(\zeta_{23})/\mathbb{Q}$ whose Galois group is $\mathbb{Z}/11\mathbb{Z}$.
For the final cyclic factor we pick another prime $p \equiv 1(\text{mod } 11)$ that is different from the one used to find A_2. For p=67 we get Gal$(\mathbb{Q}(\zeta_{67})/\mathbb{Q}) \cong \mathbb{Z}/66\mathbb{Z}$ and so we can find a subfield A_3 of $\mathbb{Q}(\zeta_{67})/\mathbb{Q}$ whose Galois group is $\mathbb{Z}/11\mathbb{Z}$.

Finally getting $E = A_1A_2A_3$ to be the compositum of these extensions over $\mathbb{Q}$,

$$Gal(E/\mathbb{Q}) \cong G$$

3.4 The Embedding Problem

Let F be a field, G a group and $A \trianglelefteq G$. A necessary condition for the realization of G as a Galois group over F is that the group $G'' = G/A$ is realizable as a Galois group over F. This brings up the following generalization of the Inverse Galois Problem known as the embedding problem.

Let Gal$(E/F) \cong G'$ and

$$1 \to A \to G \xrightarrow{\phi} G' \to 1 \tag{3.4.1}$$

be an exact sequence.
Solving the embedding problem for E/F and (3.4.1) involves determining whether there exists a Galois extension K/F such that E is in K, Gal$(K/F) \cong G$ and the homomorphism of restriction to E of the automorphisms from G coincides with ϕ.

3.5 Finite Simple Groups

The projective groups PSL(2,p) for some primes p were among the first simple groups to be realised as Galois groups over Q. The existence of these Galois groups was established by Shih in 1974 but the polynomials were only later constructed by Malle and Matzat.

Of the 26 sporadic simple groups all but the Mathieu group M_{23} have been realised as Galois groups over $\mathbb{Q}$ by Matzat et al.

Thompson in 1984 managed to show that the Fischer-Griess group M, the simple sporadic group with the biggest cardinality, also called the monster group is a Galois group over the rational field.

[Zyw] gives a list of simple groups with cardinality of at most 10^8 that can be realised as a Galois group for an extension of $\mathbb{Q}$.

4 Galois Groups as Permutation Groups

We will primarily follow the work of [Kcon] in this chapter.

Cayley's Theorem Any group of order n is isomorphic to a subgroup of S_n.

Because of Cayley's Theorem it is natural to expect that a comprehensive proof of the Inverse Galois Problem would be found in the structure of symmetric groups . For this reason we will consider Galois Groups as subgroups of S_n. We start by showing that the Galois groups of some extensions define different subgroups of S_n up to conjugation. We can use an example to illustrate this

Example 4.0.1 The polynomial $X^4 - 3$ over $\mathbb{Q}$ has the splitting field $E = \mathbb{Q}(\sqrt[4]{3}, i)$ with $\mathrm{Gal}(E/\mathbb{Q}) \cong D_4$. Let α and β be the generators of $\mathrm{Gal}(E/\mathbb{Q})$ with $\alpha(\sqrt[4]{3}) = i\sqrt[4]{3}$ and $\beta(i) = -i$ and so the Galois group is generated as below

Table 1. D_4 **automorphisms**

Automorphism	1	α	α^2	α^3	β	$\alpha\beta$	$\alpha^2\beta$	$\alpha^3\beta$
α	$\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$-i\sqrt[4]{3}$	$\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$-i\sqrt[4]{3}$
β	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Which is then isomorphic to the following two different subgroups of S_4

Table 2. Subgroup generated by (1234) and (24)

Automorphism	1	α	α^2	α^3	β	$\alpha\beta$	$\alpha^2\beta$	$\alpha^3\beta$
Permutation	(1)	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)

Table 3. Subgroup generated by (1243) and (14)

Automorphism	1	α	α^2	α^3	β	$\alpha\beta$	$\alpha^2\beta$	$\alpha^3\beta$
Permutation	(1)	(1243)	(14)(23)	(1342)	(14)	(13)(24)	(23)	(12)(34)

Definition 4.0.2 A Galois group $G \subset S_n$ is called transitive if for each $i \neq j$ in the roots {1,...,n} of its minimal polynomial there is an automorphism in G mapping i to j.

Example 4.0.3 The subgroups of S_4 in both Table 2 and Table 3 are transitive.

Example 4.0.4 The Galois Group G = Gal($\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$) which is the Klein 4 group is not a transitive subgroup of S_4 as there is no automorphism in G mapping $\sqrt{2}$ to $\sqrt{3}$.

Theorem 4.0.5 Consider a field F and $f \in F$ separable with degree n with E its splitting field. $f(X)$ is irreducible in $F[X]$ iff G = Gal(E/F) $\subset S_n$ and is transitive.

Proof: Suppose $f(X)$ is irreducible. For any two roots x_1 and x_2 of $f(X)$ and some automorphism $\alpha \in$ G we can write $\alpha(x_1) = x_2$. Therefore G as a subgroup of S_n maps each root x_i to x_j for $i \neq j$ and so it is a transitive subgroup of S_n. Now suppose $f(X)$ is reducible. Since it is a separable polynomial it is a product of distinct irreducible factors. Let x_1 and x_2 be roots of different factors of $f(X)$ and so those factors are the minimal polynomial over K for their respective root. Since for any $\alpha \in G$ $\alpha(x_1)$ has the same minimal polynomial over K as x_1 we can't have $\alpha(x_1) = x_2$. So as a subgroup of S_n G does not map all x_i to x_j for $i \neq j$ and is therefore not a transitive subgroup on S_n. □

Theorem 4.0.6 Consider a field K and $f \in F$ separable of degree n with E as the splitting field. G = Gal(E/F) has an order divisible by n.

Proof: For some root x of $f \in F$, $[F(x) : F]$ = n is a factor of the degree of E/F which is the size of G.

4.1 S_p as a Galois group for p a prime.

We show that a Galois group of prime degree p is as large as possible, that is S_p

Lemma 4.1.1 A permutation $\phi \in S_p$ of order p is a p-cycle.

Proof: Let $\phi \in S_p$ have order p and decompose into disjoint nontrivial cycles as $\phi = \phi_1 \cdots \phi_m$ with the order of each cycle ϕ_i being n_i. Since the order of a product of disjoint cycles is the least common multiple of the order of the cycles we have p = lcm($n_1, ..., n_m$). Being that p is prime and each ϕ non trivial so $n_i > 1$ we have $n_i = p, \forall i$. Thus ϕ is a product of disjoint p-cycles. Since ϕ is in S_p it can't have even two disjoint p-cycles and so ϕ is a single p-cycle. □

Theorem 4.1.2 Let $f(X) \in \mathbb{Q}(X)$ be an irreducible polynomial of prime degree p with all but two real roots and with the splitting field E = $\mathbb{Q}(x_1, ..., x_p)$. Then Gal($E/\mathbb{Q}$) $\cong S_p$

Proof: The permutation of the x_i's by Gal($E/\mathbb{Q}$) provide an embedding Gal($E/\mathbb{Q}$) $\hookrightarrow S_p$ and the order of Gal($E/\mathbb{Q}$) is divisible by p by the last theorem which means that Gal($E/\mathbb{Q}$) has an element of order p thus the image of Gal($E/\mathbb{Q}$) in S_p contains a p-cycle.
Since the complex field is algebraically closed we may take $E \subset \mathbb{C}$. Complex conjugation restricted to E is a member of Gal($E/\mathbb{Q}$). Since f contains only 2 complex roots the complex

conjugation of 2 of the roots of f fixing the rest so Gal($E/\mathbb{Q}$) contains transpositions of the roots of f.
It remains to show the only subgroup of S_p with a p-cycle and a transposition is S_p. By labeling the numbers from 1 to p we may let 1 be a number moved by the transposition and so our subgroup contains the transpositon (1a). Let α be a p-cycle in the subgroup. As a p-cycle, α acts on 1,2,...,p by a single orbit, so some α^i with $1 \leq$ i $\leq$ p-1 sends 1 to a: α^i = (1a...). This is also a p-cycle, because α^i has order p in S_p and all elements of order p in S_p are p-cycles, so writing α^i as α and suitably reordering the numbers 2,...,p (which replaces our subgroup by a conjugate subgroup), we may suppose our subgroup of S_p contains the particular transposition (12) and the particular p-cycle (12...p). For n $\geq$ 2, it is a theorem in group theory that the particular transposition (12) and n-cycle (12...n) generate S_n, so our subgroup is S_p.

4.2 Alternating Groups

In (3.2.1) we saw that all S_n can be realised as the Galois group for the splitting field of some minimal polynomial over $\mathbb{Q}$. We aim in this section to show when the Galois group $G \subset S_n$ is in fact A_n. For this we use the discriminant.

Definition 4.2.1 For a $f(X) \in \mathbb{Q}[X]$ with roots $\{x_1, ...x_n\}$ that factors as

$$f(X) = a(T - x_i) \cdots (T - x_n)$$

its discriminant denoted Δ as

$$\Delta = \prod_{i<j} (x_i - x_j)^2$$

The discriminant is important in telling us the nature of the roots of a polynomial. Since we use polynomials to determine field extensions this makes the discriminant an important value in determining the nature of a Galois group.
The discriminant of a polynomial over $\mathbb{Q}$ is zero if and only if the polynomial is not separable. This is easy to see since for $\Delta = \prod_{i<j}(x_i - x_j)^2$ to be zero there must be at least one factor $(x_i - x_j)^2$ that should be zero and in that case $x_i = x_j$ and so all the roots are not distinct and hence the polynomial is not separable.
For low degree monic polynomials over $\mathbb{Q}$ we have the following formulas for their discriminant and what the implication is for the case of a non zero discriminant.

Degree 2 - The polynomial $x^2 + bx + c$ has the discriminant $b^2 - 4c$. Over $\mathbb{Q}$ it has a positive discriminant when it has two real roots since $(a - b)^2$ is positive if and only if a and b are real roots and negative if and only if both roots are complex conjugates.

Degree 3 - The polynomial x^3+bx+c has the discriminant $-4b^3-27c^2$. Over $\mathbb{Q}$ the discriminant is positive when each root is real because $\Delta=(b-a)(c-a)(c-b)$ to be positive the three roots a,b,c must be real. This polynomial with rational coefficients would then have a negative discriminant when it has one real root (with the other two being complex conjugate of each other).

Degree 4 - The polynomial x^4+bx+c has the discriminant $-27b^4+256c^3$. Over $\mathbb{Q}$ the discriminant is positive when either every root is real or every root is complex. Is is negative if 2 roots are real numbers and the other two roots complex conjugates.

Degree 5 - The polynomial x^5+bx+c has the discriminant $256b^5+3125c^4$.

Having discussed the discriminant we use the next theorem to prove for a separable $f\in\mathbb{Q}$ with Δ a square, its the Galois group is A_n.

Theorem 4.2.2 Consider a separable polynomial $f\in\mathbb{Q}$ with roots $(x_1,...,x_n)$. Then $\text{Gal}(\mathbb{Q}(x_1,...,x_n)/\mathbb{Q})\cong A_n$ if and only if its discriminant is a rational square.

Proof: Set

$$\delta=\prod_{i<j}(x_j-x_i)$$

Since f is separable, $\delta\neq 0$ and so $\delta\in\mathbb{Q}(x_1,...,x_n)$ and $\delta^2=\Delta\in\mathbb{Q}$.
For any $\alpha\in\text{Gal}(\mathbb{Q}(x_1,...,x_n)/\mathbb{Q})$ we let $\varepsilon_\alpha=\pm 1$ be the sign as a permutation of the roots which by definition

$$\alpha(\delta)=\prod_{i<j}(\alpha(x_j)-\alpha(x_i))=\varepsilon_\alpha\prod_{i<j}(x_j-x_i)=\varepsilon_\alpha\delta$$

so $\alpha(\delta)=\pm\delta$. Since δ is non zero and f(x) is over $\mathbb{Q}$, $\delta\neq-\delta$. We have $\alpha in A_n$ iff $\varepsilon_\alpha=1$ which means $\alpha\in A_n$ iff $\delta(d)=\delta$ and so $\text{Gal}(\mathbb{Q}(x_1,...,x_n)/\mathbb{Q})\cong A_n$ iff δ if fixed by all the automorphism of $\text{Gal}(\mathbb{Q}(x_1,...,x_n)/\mathbb{Q})$ which is similar to δ being in the fixed field $\mathbb{Q}$.

Example 4.2.3 Let $f(x)=x^3-3x-1$ and $g(x)=x^3-4x-1$ be polynomials over $\mathbb{Q}$. They both have three real roots but their Galois groups are not the same subgroup of S_n. $f(x)$ has a discriminant of 81 and $g(x)$ has a discriminant of 229. Since the discriminant of $f(x)$ is a rational square its Galois group ov $\mathbb{Q}$ is A_3 and the discriminant of $g(x)$ is a prime which by Theorem 4.1.2 makes its Galois group over $\mathbb{Q}$ S_3

4.3 Subgroups of low degree S_n

We in this section aim to show all subgroups, up to conjugation, of S_n for n < 6 as Galois groups over $\mathbb{Q}$ using methods discussed in this chapter. The reason we won't give explicit polynomials for the subgroups of S_n for $n\geq 6$ is entirely for brevity's sake because for S_6

there are 56 conjugacy classes of 1455 subgroups that quickly rise to even higher counts for subsequent $n > 6$

4.3.1 S_3

S_3 is the group of permutations of (123) which is of order 6.
A polynomial of the form $x^3 - a$ provided that the third root of a is not a rational number has the splitting field $\mathbb{Q}(w, \sqrt[3]{a})$ over $\mathbb{Q}$ with w being the non trivial cube root of unity.

Example $x^3 - 3$ has three roots namely $\sqrt[3]{3}, w\sqrt[3]{3}$ and $w^2\sqrt[3]{3}$ therefore its splitting field over the rational field is $\mathbb{Q}(w, \sqrt[3]{3})/\mathbb{Q}$ which has 6 automorphisms and so $\text{Gal}(\mathbb{Q}(w, \sqrt[3]{3})/\mathbb{Q}) \cong S_3$.

S_3 has 6 total subgroups with 4 non trivial proper subgroups. The four are isomorphic to $\mathbb{Z}_2$ (3 of them) and Z_3. As we have seen from the Kronecker Weber theorem in chapter 2 all abelian groups of order n can be realised as the Galois group of an extension of $\mathbb{Q}$ with $f(x)$ being a n degree cyclotomic polynomial. S_3 subgroups as Galois group are broken down as in the table below.

Table 4. S_3 **subgroup breakdown.**

Isomorphism Group	Count	Order	Polynomial over $\mathbb{Q}$
Trivial	1	1	
$\mathbb{Z}_2$	3	2	$x^2 + 1$
$\mathbb{Z}_3$	1	3	$x^3 + 1$
S_3	1	6	$x^3 - 4x - 1$

4.3.2 S_4

S_4 is the group of permutations of (1,2,3,4) of order 24. Though S_4 has 30 subgroups they are only 7 distinct non trivial subgroups upto isomorphism which we will now find the Galois group associated with them.

$\mathbb{Z}_2$ - Just as with $\mathbb{Z}_2 \subset S_3$, $\mathbb{Z}_2 \subset S_4$ is the Galois group for some polynomial of degree 2 over $\mathbb{Q}$ that has its roots as the second root of unity.

$\mathbb{Z}_4$ - Just as with $\mathbb{Z}_2 \subset S_3$, $\mathbb{Z}_4 \subset S_4$ is the Galois group for some polynomial of degree 4 has its roots as the fourth root of unity.

$\mathbb{Z}_2 \times \mathbb{Z}_2$ - The Klein 4 group is the Galois group for $\mathbb{Q}(\sqrt{a}, \sqrt{b})$

D_4 - D_4 is the Galois group of the splitting field of the polynomial $X^4 - 3$ over $\mathbb{Q}$ as seen in Table 1.

A_4 - The polynomial $f(X) = X^4 + 8X + 12$ has a discriminant of 331776 = 576^2 and the splitting field of f over $\mathbb{Q}$ is A_4

S_4 - The Galois group of f=$X^4 - X - 1$ over the rational field is S_4

Table 5. S_4 **subgroup breakdown.**

Isomorphism Group	Count	Order	Polynomial over $\mathbb{Q}$
Trivial	1	1	
$\mathbb{Z}_2$	9	2	x^2+1
$\mathbb{Z}_3$	4	3	x^3+1
$\mathbb{Z}_4$	3	4	x^4+1
$\mathbb{Z}_2 \times \mathbb{Z}_2$	4	4	$(x^2-2)(x^2-3)$
D_4	3	8	x^4-3
A_4	1	12	$x^4+8x+12$
S_3	4	6	x^3-x-1
S_4	1	24	x^4-x-1

4.3.3 S_5

S_5 is the group of permutations of (1,2,3,4,5) of order 120. There are 19 subgroups up to conjugation of a total of 156 subgroups. The subgroups not in S_4 or S_3 are the following ones.

$\mathbb{Z}_5$ - The cyclic group of order 5 is the Galois group of the splitting field of the polynomial $x^5 + 1$ over $\mathbb{Q}$.

$\mathbb{Z}_6$ - The cyclic group of order 6 is the Galois group of the splitting field of the polynomial $x^6 + 1$ over $\mathbb{Q}$.

D_5 - The dihedral group of order 10 has is the Galois group of $\mathbb{Q}(\sqrt[5]{a}, i)/\mathbb{Q}$ provided $\sqrt[5]{a}$ is not rational. Therefore it is the Galois group of $x^5 - 2$ over $\mathbb{Q}$

A_5 - The polynomial $x^5 + 20x + 16$ over $\mathbb{Q}$ is separable and has a discriminant of $1.024 \times 10^9 = 32000^2$ by theorem 4.2.2 its Galois group over $\mathbb{Q}$ is A_5

S_5 - The polynomial $x^5 - 4x - 1$ over $\mathbb{Q}$ is separable and of prime degree with all but two real roots. By theorem 4.1.2 its Galois group over $\mathbb{Q}$ is S_5

Table 6. S_5 subgroup breakdown.

Isomorphism Group	Count	Order	Polynomial over $\mathbb{Q}$
Trivial	1	1	
$\mathbb{Z}_2$	25	2	x^2+1
$\mathbb{Z}_3$	10	3	x^3+1
$\mathbb{Z}_4$	15	4	x^4+1
$\mathbb{Z}_5$	6	4	x^5+1
$\mathbb{Z}_6$	10	4	x^6+1
$\mathbb{Z}_2 \times \mathbb{Z}_2$	19	4	$(x^2-2)(x^2-3)$
D_4	15	8	x^4-3
D_5	5	10	x^5-2
A_4	5	12	$x^4+8x+12$
D_6	10	12	x^6-2
A_5	1	60	$x^5+20x+16$
S_3	20	6	x^3-x-1
S_4	5	24	x^4-x-1
S_5	1	120	x^4-x-1

5 Conclusion

A lot of effort has been put to the classification of finite groups and though it has been achieved for simple groups a lot more would be required to achieve it for all groups. Had that classification existed it would go a long way towards finding generic polynomials for which the Inverse Galois Problem would have a solution. Should a solution not exists though this classification would very likely help enlighten us on the structure of groups that can not be realised as a Galois groups over $\mathbb{Q}$

5.1 Future Research

The closest we have to a coherent structure of all finite groups is their realisation as subgroups of the symmetric groups. Since symmetric groups and their subgroups are finitely generated it may be of interest to see if the generating sets have a relationship with any form of separable polynomial. Furthermore if a class of subgroups can be generated by transposition and one can find polynomials over $\mathbb{Q}$ to describe any such transposition then all subgroups up to conjugation of S_n will have a positive Inverse Galois Problem solution.

Bibliography

[UAN] U. Jensen, A. Ledet, N. Yui. *Generic Polynomials Constructive Aspects of the Inverse Galois Problem*, Cambridge University Press, 2002.

[MiZ] Ivo M. Michailov, Nikola P. Ziapkov. *On realizability of p-groups as Galois groups*, 2012.

[Zyw] David Zywina. *Inverse Galois Problem for small simple groups*

[Kcon] Keith Conrad. *Galois Groups as Permutation Groups*

[Zyw] Ivo M. Michailov. *"On Galois cohomology and realizability of 2-groups as Galois groups"*, Central European Journal of Mathematics, 01/17/2011

[Eck] J.P. Eckmann. *On the computation of the Galois group over the quotient field of* $\mathbb{C}[\gamma]$, Numerische Mathematik, 03/1976

[CAN] Christian U. Jensen, Arne Ledet, Noriko Yui. *Generic Polynomials Constructive Aspects of the Inverse Galois Problem*, Cambridge University Press 2002

[BSL] Bary-Soroker. *Irreducibility and embedding problems*, Journal of Algebra, 05/2012

[Ram] Ramji Lal. *Chapter 8, Field Theory, Galois Theory*, Springer Nature, 2017

[Hen] Henri Bourles. *Galois Theory and Skew Polynomials*, Lecture Notes in Control and Information Sciences, 2011

[Hil] D. Hilbert, *Ueber die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. reine angew. Math. 110, 1892

[Ros] Rose J, *A course on group theory*. Cambridge University Press, Cambridge-New York-Melbourne, 1978

[Jba] Jonathan Bayless, *On the subgroup of* S_n *generated by an n-cycle and an involution*, 7/2001

[Bhm] B. H. Matzat, *Konstruktion von Zahl-und Funktionenkörpern mit vorgegebener Galoisgruppe*, J. reine angew. Math. 349 (1984)

[Serre] J. P. Serre, *Topics in Galois Theory*, USA, AK Peters Ltd, 1992