

# APPLICATIONS OF GALOIS THEORY



THESIS SUBMITTED TO  
THE CENTRAL DEPARTMENT OF MATHEMATICS  
INSTITUTE OF SCIENCE AND TECHNOLOGY  
TRIBHUVAN UNIVERSITY  
KATHMANDU, NEPAL

BY  
**SANDESH THAKURI**

SUBMITTED FOR THE  
PARTIAL FULFILLMENT OF THE REQUIREMENT FOR  
THE MASTER IN SCIENCE/ARTS (M.SC./M.A.) DEGREE  
IN MATHEMATICS

MARCH 2024



# DEDICATION

To

My Mom and Dad

**Sharada Thakuri and Prem Bdr. Thakuri.**



## STUDENT'S DECLARATION

This thesis entitled “**Applications of Galois Theory**”, which has been submitted to the Central Department of Mathematics, Institute of Science and Technology (IOST), Tribhuvan University, Nepal for the partial fulfillment of the Master in Science/Arts (M.Sc./M.A.) Degree in Mathematics, is a genuine work that I carried out under my supervisor **Assoc. Prof. Tulasi Prasad Nepal** and that no sources other than those listed in the Bibliography have been used in this work. Moreover, this work has not been published or submitted elsewhere for the requirement of any degree programme.

---

Sandesh Thakuri

Batch: 2077

TU Registration Number: 5-2-37-1874-2016

Date: March 2024



## RECOMMENDATION

This is to recommend that Mr. **Sandesh Thakuri** has prepared this thesis entitled “**Applications of Galois Theory**” for the partial fulfillment of the Master in Science/Arts (M.Sc./M.A.) in Mathematics under my supervision. To my knowledge, this work has not been submitted for any other degree. He has fulfilled all the requirements laid down by the Central Department of Mathematics, Institute of Science and Technology (IOST), Tribhuvan University (TU), Kirtipur for the submission of the thesis for the partial fulfillment of M.Sc./M.A. Degree in Mathematics.

.....

Mr. Tulasi Prasad Nepal

**Supervisor**

Associate Professor

Date: March 2024



## LETTER OF APPROVAL

We certify that the Research Evaluation Committee of the Central Department of Mathematics, Tribhuvan University, Kirtipur approved this research work entitled “**Applications of Galois Theory**” carried out by Mr. **Sandesh Thakuri** in the scope and generality as a thesis in the partial fulfillment for the requirement of the M.Sc./M.A. degree in Mathematics.

.....  
(Name)  
External Examiner  
Institution  
Date:

.....  
Assoc. Prof. Tulasi Prasad Nepal  
Supervisor  
Central Department of Mathematics  
Institute of Science & Technology  
Tribhuvan University Kirtipur, Kathmandu,  
Nepal.  
Date: March 2024

.....  
Prof. Dr. Chet Raj Bhatta  
(Head of Department)  
Central Department of Mathematics  
Institute of Science & Technology  
Tribhuvan University Kirtipur, Kathmandu, Nepal.  
Date: March 2024

# ACKNOWLEDGMENTS

First of all I would like to thank my **supervisor** Mr. Tulasi Prasad Nepal (Associate Professor of Central Department of Mathematics).

I am thankful to former HOD of the department Prof. Dr. Tanka Nath Dhamala for his valuable support and time. Then I am thankful to Santosh Gyanwali sir for providing me the necessary articles. Then I am thankful to my friends and family.

.....  
**Sandesh Thakuri**  
Date: March 2024

# Contents

DEDICATION	ii
STUDENT DECLARATION	iii
RECOMMENDATION	iv
LETTER OF APPROVAL	v
ACKNOWLEDGMENTS	v
Contents	vii
Symbol Conventions Used	1
<b>I Galois Theory</b>	<b>2</b>
<b>1 Field Extension</b>	<b>3</b>
1.1 Approaches to the Theory . . . . .	3
1.2 Structure of a Field Extension . . . . .	4
1.3 Algebraic and Transcendental element . . . . .	4
<b>2 Galois Correspondence</b>	<b>5</b>
2.1 Galois Group . . . . .	5
2.2 Galois extension . . . . .	5
2.3 Fundamental Theorem of Galois Theory . . . . .	6
<b>3 Structure of Galois Extension</b>	<b>8</b>
3.1 Splitting Field . . . . .	8
3.2 Separable Extension . . . . .	9
3.3 Galois extension . . . . .	9

<b>II Applications</b>	<b>10</b>
<b>4 Galois Group of a Polynomial</b>	<b>11</b>
4.1 Galois Group of Cubic polynomials . . . . .	11
4.2 Galois Group of Quartic polynomials . . . . .	12
4.3 Galois Group of some Polynomials . . . . .	13
4.4 Galois group of Quantic polynomials . . . . .	14
4.5 Galois Group of Reducible polynomials . . . . .	14
<b>5 The Classic Problem</b>	<b>15</b>
5.1 Formulation of the Classic Problem . . . . .	15
5.2 Group Theoretic Concepts . . . . .	16
5.3 Conclusion . . . . .	16
<b>6 Galois Fields</b>	<b>18</b>
<b>Bibliography</b>	<b>19</b>



# Symbol Conventions

Through out the thesis following Symbol Convention has been used.

- $\mathbf{K}$  a field.
- $\mathbf{F}$  an extension field of the field  $\mathbf{K}$

## Some Standard Symbols

1.  $\mathbb{Z}$  set of integers
2.  $\mathbb{Q}$  set of rationals
3.  $\mathbb{R}$  set of reals
4.  $\mathbb{C}$  set of complex numbers

# Part I

## Galois Theory

# Chapter 1

## Field Extension

Galois Theory is a popular and one of the important theory in Abstract Algebra. It's foundation was first laid by the French Mathematician *Évariste Galois* by determining the necessary and sufficient condition for solving the polynomial equation by radicals and thereby solving the problem that was open for 350 years old.

The core-part of the Galois Theory is the *Fundamental Theorem* of Galois Theory which links two main parts of Abstract Algebra; Field Theory and Group Theory. This is a profound result in Abstract Algebra.



Figure 1.1: Galois

### 1.1 Approaches to the Theory

1. Galois approached this problem by using the group of permutations of the roots of a polynomial equation. Only those permutations of the roots are considered which leaves any equation satisfied by the roots unchanged.
2. The modern approach is to use the **field extension** of the underlying field of the polynomial and examine the groups of automorphism of the extension field that fixes the underlying field.

## 1.2 Structure of a Field Extension

Let  $F = K(u)$  be a field extension of the field  $K$ . Then  $F$  is a vector space over  $K$  generated by  $u$ .

We have  $u^n \in F$  for all  $n \in \mathbb{Z}$  because  $F$  is a field. As  $F$  is a vector space over  $K$ ;  $F$  consists of all linear combinations of  $u^n$ 's, and the quotients of these linear combinations. A such linear combinations is:  $a_n u^n + a_{n-1} u^{n-1} + \dots + a_1 u + a_0$  which is given by the polynomial  $f(u)$ , where  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ .

So the structure of the extension field  $F = K(u)$  is:

$$F = \left\{ \frac{f(u)}{g(u)} \mid f, g \in K[x], g(u) \neq 0 \right\}.$$

**Theorem 1** (Existence of an Extension field). *If  $K$  is a field and  $f \in K[x]$  is a polynomial of degree  $n$ , then there exists a simple extension field  $F = K(u)$  of  $K$  such that  $u \in F$  is a root of  $f$ . [1]*

## 1.3 Algebraic and Transcendental element

**Theorem 2.** *Let  $F$  be an extension field of a field  $F$ .*

*A map  $\phi : K[X] \rightarrow K[u]$  where  $u \in F$  defined by  $\phi(f(x)) = f(u)$*

*i.e,  $\phi(a_0 + a_1 x + \dots + a_n x^n) = a_0 + a_1 u + \dots + a_n u^n$  is a ring homomorphism.*

Thus  $K[x]$  and  $K[u]$  are homomorphic.

1. If  $u$  is transcendental over  $K$  then  $K[u]$  is not a field and  $K[x] \cong K[u]$ .
2. If  $u$  is algebraic over  $K$  then,  $K[x] \not\cong K[u]$  because  $\text{Ker}\phi$  is non trivial and we have,
  - i)  $K(u) \cong K[u]$ ;
  - ii)  $K(u) \cong K[x]/(f)$ , where  $f \in K[x]$  is an 'irreducible monic polynomial of degree  $n \geq 1$ ;
  - iii)  $[K(u) : K] = n$  and  $\{1, u, u^2, \dots, u^{n-1}\}$  is a basis of the vector space  $K(u)$  over  $K$ .

**Theorem 3** (Isomorphism of Extension fields). *Let  $K$  be a field.*

*Then ' $u$ ' and ' $v$ ' are roots of the same irreducible polynomial  $f \in K[x]$  if and only if there is an isomorphism of fields  $K[u] \cong K[v]$  which sends  $u$  onto  $v$  and is the identity on  $K$ .*

# Chapter 2

## Galois Correspondence

### 2.1 Galois Group

Let  $F$  be a field. The set  $Aut F$  of all field-automorphisms  $F \rightarrow F$  forms a group under the function composition.

Let  $E$  and  $F$  be the extension fields of a field  $K$ .

If a non-zero field-homomorphism  $\sigma : E \rightarrow F$  is a  $K$ -module homomorphism then  $\sigma(k) = \sigma(k1_E) = k\sigma(1_E) = k1_F = k$ . i.e,  $\sigma$  fixes  $K$  element-wise.

Conversely, if a field homomorphism  $\sigma : E \rightarrow F$  fixes  $K$  element-wise, then  $\sigma$  is a non-zero and for any  $u \in E$ , we have,  $\sigma(ku) = \sigma(k)\sigma(u) = k\sigma(u)$  i.e  $\sigma$  is a  $K$ -module homomorphism.

**Definition 1.** A field-automorphism  $\sigma \in Aut F$  which is also  $K$ -homomorphism is called  $K$ -automorphism. In other words, a field-automorphism  $\sigma \in Aut F$  that fixes  $K$  element-wise is called  $K$ -automorphism.

**Definition 2.** The group of all  $K$ -automorphisms of  $F$  is called the Galois group of  $F$  over  $K$  and it is denoted by  $Aut_K^F$ .

### 2.2 Galois extension

Let  $E$  be an intermediate field and  $H$  be a subgroup of  $Aut_K^F$ , then:

- i)  $H' = \{v \in F \mid \sigma(v) = v, \text{ for all } \sigma \in H\}$  is an intermediate field of the extension field  $F$  of  $K$ ;
- ii)  $E' = \{\sigma \in Aut_K^F \mid \sigma(u) = u, \text{ for all } u \in E\} = Aut_E^F$  is a subgroup of  $Aut_K^F$ .

The field  $H'$  is called the fixed field of the subgroup  $H$  in  $F$ .

### 2.2.1 Fixed Field

We have,

$H' \rightarrow$  fixed field and  $E' \rightarrow \text{Aut}_E^F$ . Let  $\text{Aut}_K^F = G$  then the field fixed by it is  $G'$ . It is not necessary that the field fixed by  $G$  is  $K$  i.e,  $G' = K$ .

**Example 1.** For  $f(x) = x^3 - 2 \in Q[x]$ . Let  $u \in F$  such that  $f(u) = 0$  and let  $F = Q[u]$ . Then  $G = \text{Aut}_Q^{Q(u)} = 1$  so,  $G' = F \neq K$ .

**Definition 3.** Let  $F$  be an extension field of  $K$  such that the fixed field of the Galois group  $\text{Aut}_K^F$  is  $K$  itself. Then  $F$  is said to be a Galois extension of  $K$  or Galois over  $K$ .

## 2.3 Fundamental Theorem of Galois Theory

**Theorem 4.** If  $F$  is a finite dimensional Galois extension of  $K$ , then there is a one-to-one correspondence between the set of all intermediate fields of  $F$  over  $K$  and the set of subgroups of the Galois group  $\text{Aut}_K^F$  such that:

- i) the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups. In particular  $\text{Aut}_K^F$  has order  $[F : K]$ ;
- ii)  $F$  is Galois over every intermediate field  $E$ , but  $E$  is Galois over  $K$  if and only if the corresponding subgroup  $E' = \text{Aut}_E^F$  is normal in  $G = \text{Aut}_K^F$ . In this case  $G/E'$  is isomorphic to the Galois group  $\text{Aut}_K^E$  of  $E$  over  $K$ .

We already have a correspondence between the intermediate fields and the subgroup of Galois group.

That is to each intermediate field  $E$ , there is a subgroup  $\text{Aut}_E^F$  and to each subgroup  $H$  there is a fixed field  $H'$ . But this correspondence is one-to-one if and only if for each intermediate field  $E$ , it satisfies  $E'' = E$  and for each subgroup  $H$ , it satisfies  $H'' = H$ .

### 2.3.1 Closed Field and Subgroup

We have, i)  $F' = 1$  and  $K' = G$ ; ii)  $1' = F$ .

If  $F$  is Galois over  $K$  then by definition,  $G' = K$ . Since  $K' = G$  we have  $K = K''$  if and only if  $F$  is Galois over  $K$ .

**Definition 4.** Let  $X$  be an intermediate field or subgroup of the Galois group.  $X$  will be called **closed** provided  $X = X''$ .

**Lemma 1.** . If  $F$  is an extension field of  $K$ , then there is one-to-one correspondence between the closed intermediate fields of the extension and the closed subgroups of the Galois group, given by  $E \rightarrow E' = \text{Aut}_E^F$ .

**Lemma 2.** . Let  $F$  be an extension field of  $K$ ,  $L$  and  $M$  intermediate fields with  $L \subset M$ , and  $H, J$  subgroups of Galois group  $\text{Aut}_K^F$  with  $H < J$ .

- i) If  $L$  is closed and  $[M : L]$  finite, then  $M$  is closed and  $[L' : M'] = [M : L]$ ;
- ii) if  $H$  is closed and  $[J : H]$  finite, then  $J$  is closed and  $[H' : J'] = [J : H]$ ;
- iii) if  $F$  is a finite dimensional Galois extension of  $K$ , then all intermediate fields and all subgroups of the Galois group are closed and  $\text{Aut}_K^F$  has order  $[F : K]$ .

### 2.3.2 Stable Intermediate

**Definition 5.** An intermediate field  $E$  of  $F$  over  $K$  is said to be stable intermediate if  $\sigma(E) \subseteq E$  for every  $\sigma \in \text{Aut}_K^F$ .

- Lemma 3.**
- i) If  $E$  is a stable intermediate field of the extension, then  $E' = \text{Aut}_E^F$  is a normal subgroup of the Galois group  $\text{Aut}_K^F$ ;
  - ii) if  $H$  is a normal subgroup of  $\text{Aut}_K^F$ , then the fixed field  $H'$  of  $H$  is a stable intermediate field of the extension.

### 2.3.3 Proof of the Fundamental Theorem

*Proof.* From the above section there is one-to-one correspondence between closed intermediate fields of the extension and closed subgroups of the Galois group. But in this case all intermediate fields and all subgroups are closed. Thus follows statement(i) of the theorem.

$F$  is Galois over  $E$  since  $E$  is closed.  $E$  is finite dimensional over  $K$  since  $F$  is and hence algebraic over  $K$ . Consequently, if  $E$  is Galois over  $K$ , then  $E$  is stable.  $E' = \text{Aut}_E^F$  is normal in  $\text{Aut}_K^F$ . Conversely if  $E'$  is normal in  $\text{Aut}_K^F$ , then  $E''$  is stable intermediate field. But  $E = E''$  since all intermediate fields are closed and hence  $E$  is Galois over  $K$ .

Suppose  $E$  is an intermediate field that is Galois over  $K$ . Since  $E$  and  $E'$  are closed and  $G' = K(F \text{ is Galois over } K)$ , we have  $|G/E'| = [G : E'] = [E'' = G'] = [E : K]$ . So,  $G/E' = \text{Aut}_K^F / \text{Aut}_E^F$  is isomorphic to a subgroup of  $\text{Aut}_K^F$ . But by first part of the theorem,  $|\text{Aut}_K^E| = [E : F]$  (since  $E$  is Galois over  $K$ ). This implies  $G/E' = \text{Aut}_K^E$ . □

# Chapter 3

## Structure of Galois Extension

Galois extension  $F$  of  $K$  is a field for which the fixed field of the Galois group  $\text{Aut}_K^F$  is  $K$  itself.

But for what extension field  $F$  of  $K$  the Galois group keeps the base field  $K$  fixed? What is the structure of Galois field and how do we construct(obtain) a Galois field?

### 3.1 Splitting Field

Since, for  $F = K(u)$ , any  $\sigma \in \text{Aut}_K^F$  is completely determined by its action on  $u$ . Any algebraic Galois extension of  $K$  is generated by all roots  $u$  of a polynomial  $f \in K[x]$ .

**Definition 6.** Such a minimal field  $F$  where a polynomial  $f \in K[x]$  splits into linear factors and thus contains all roots of  $f(x)$  is called a splitting field of  $f$  over  $K$ .

Thus, an algebraic Galois extension is going to be characterized by a splitting field of a polynomial over the base field.

**Theorem 5** (Existence of a Splitting field). *If  $K$  is a field and  $f \in K[x]$  has degree  $n \geq 1$ , then there exists a splitting field  $F$  of  $f$  with  $[F : K] \leq n!$ .*

#### 3.1.1 Algebraic Closure of a Field

A field  $F$  is said to be algebraically closed if every nonconstant polynomial  $f \in F[x]$  has a root in  $F$ . For example the field of complex number  $\mathbb{C}$  is algebraically closed.



**Definition 7.** An extension field  $F$  of a field  $K$  is said to be algebraic closure of  $K$  if,

- i)  $F$  is algebraically closed and,
- ii)  $F$  is algebraic over  $K$ .

So,  $\mathbb{C}$  is algebraically closed field but is not an algebraic closure of  $\mathbb{Q}$  because  $\mathbb{C}$  is not algebraic over  $\mathbb{Q}$ . But  $\mathbb{C}$  is an algebraic closure of  $\mathbb{R}$ .

This shows algebraic closure is an special case of a splitting field.

## 3.2 Separable Extension

An irreducible polynomial  $f \in K[x]$  is said to be separable if in some splitting field of  $f$  over  $K$  every root of  $f$  is a simple root.

An algebraic element  $u \in F$  is said to be separable over  $K$  provided its irreducible polynomial is separable.

**Definition 8.** If every element of  $F$  is separable over  $K$ , then  $F$  is said to be a separable extension of  $K$ .

### Characteristic of a Separable extension

*Remark.* Every algebraic extension field of a field of characteristic 0 is separable.

It is clear that a separable polynomial  $f \in K[x]$  has no multiple roots in any splitting field of  $f$  over  $K$ . This shows that an irreducible polynomial in  $K[x]$  is separable if and only if its derivative is nonzero. Hence every irreducible polynomial is separable if  $\text{char} K = 0$ .

## 3.3 Galois extension

**Theorem 6.**  $F$  is algebraic and Galois over  $K$  if and only if  $F$  is separable over  $K$  and  $F$  is a splitting field over  $K$  of a set  $S$  of polynomials in  $K[x]$ .

This proves the **Generalized Fundamental Theorem of Galois Theory**, which states the *Fundamental Theorem of Galois Theory* still holds if the extension field  $F$  is not finite dimensional as-well i.e, if  $F$  is algebraic and Galois over  $K$ .

# Part II

## Applications

# Chapter 4

## Galois Group of a Polynomial

**Definition 9.** The Galois group of a polynomial  $f \in K[x]$  is the group  $Aut_K^F$ , where  $F$  is a splitting field of  $f$  over  $K$ .

**Theorem 7.** Let  $G$  be a Galois group of a polynomial  $f \in K[x]$ .

- i)  $G$  is isomorphic to a subgroup of some symmetric group  $S_n$ .
- ii) If  $f$  is separable of degree  $n$ , the  $n$  divides  $|G|$  and  $G$  is isomorphic to a transitive subgroup of  $S_n$ .

Because the Galois group  $Aut_K^F$  is a group of automorphisms of  $F$  which is given by the permutations of the roots. So, the Galois group of a polynomial is identified with the subgroup of  $S_n$ .

**Corollary 7.1.** i) If the degree of  $f$  is 2 then its Galois group  $G \cong \mathbb{Z}_2$ .

ii) If the degree of  $f$  is 3 then its Galois group  $G$  is either  $S_3$  or  $A_3$ .

### 4.1 Galois Group of Cubic polynomials

**Definition 10.** Let  $K$  be a field with  $char K \neq 2$  and  $f \in K[x]$  a polynomial of degree  $n$  with  $n$  distinct roots  $u_1, u_2, \dots, u_n$  in some splitting field  $F$  of  $f$  over  $K$ . Let  $\Delta = \prod_{i < j} (u_i - u_j) = (u_1 - u_2)(u_1 - u_3) \dots (u_{n-1} - u_n) \in F$ .

The discriminant of  $f$  is the element  $D = \Delta^2$ .

**Theorem 8.** i) The discriminant  $\Delta^2$  of  $f$  actually lies in  $K$ .

ii) For each  $\sigma \in Aut_K^F < S_n$ ,  $\sigma$  is an even [resp. odd] if and only if  $\sigma(\Delta) = \Delta$  [resp.  $\sigma(\Delta) = -\Delta$ ].

Since  $\Delta^2 \in K$  and  $\Delta \in F$ , and  $K(\Delta)$  is a stable intermediate; in the Galois correspondence the subfield  $K(\Delta)$  corresponds to the subgroup  $G \cap A_n$ . In particular,  $G$  consists of even permutations if and only if  $\Delta \in K$ .

**Corollary 8.1.** If  $f$  is a separable polynomial of degree 3, then the Galois group of  $f$  is  $A_3$  if and only if the discriminant of  $f$  is the square of an element of  $K$ .

**Theorem 9.** Let  $K$  be a field of  $\text{char} K \neq 2, 3$ . If  $f(x) = x^3 + bx^2 + cx + d \in K[x]$  has three distinct roots in some splitting field, then the polynomial  $g(x) = f(x - b/3) \in K[x]$  has the form  $x^3 + p^2 + q$  and the discriminant of  $f$  is  $-4p^3 - 27q^2$  [1].

## 4.2 Galois Group of Quartic polynomials

**Definition 11** (Resolvant Cubic of a Quartic). Let  $K, f, F, u_i, V$ , and  $G = \text{Aut}_K^F < S_4$  be as in the preceding paragraph and  $\alpha = u_1u_2 + u_3u_4$ ,  $\beta = u_1u_3 + u_2u_4$ ,  $\gamma = u_1u_4 + u_2u_3$ . The polynomial  $(x - \alpha)(x - \beta)(x - \gamma)$  is called the resolvant cubic of  $f$ . The resolvant cubic is actually a polynomial over  $K$ .

Now under the Galois correspondence the subfield  $K(\alpha, \beta, \gamma)$  corresponds to the normal subgroup  $V \cap G$  because  $K(\alpha, \beta, \gamma)$  is a splitting field of the resolvant cubic whose Galois group is a subgroup of  $S_3$  and only normal subgroup of  $N$  of  $S_4$  with  $|N| \leq 6$  is  $V$ .

Hence  $K(\alpha, \beta, \gamma)$  is Galois over  $K$  and  $\text{Aut}_K^{K(\alpha, \beta, \gamma)} = G/(G \cap V)$ .

*Remark.* If  $K$  is a field and  $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$ , then the resolvant cubic of  $f$  is the polynomial  $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$ .

**Theorem 10.** Let  $K$  be a field and  $f \in K[x]$  a separable quartic with Galois Group  $G$ . Let  $\alpha, \beta, \gamma$  be the roots of the resolvant cubic of  $f$  and let  $m = [K(\alpha, \beta, \gamma) : K]$  then,

- i)  $m = 6 \iff G = S_4$ ;
- ii)  $m = 3 \iff G = A_4$ ;
- iii)  $m = 1 \iff G = V$ ;
- iv)  $m = 2 \iff G = D_4$  or  $G = \mathbb{Z}_4$ ; in this case  $G = \mathbb{Z}_4$  if  $f$  is irreducible over  $K(\alpha, \beta, \gamma)$  and  $G = D_4$  otherwise.

This is because we have  $[K(\alpha, \beta, \gamma) : K] = |G/G \cap V|$ .

### 4.3 Galois Group of some Polynomials

**Example 2.** The polynomial is  $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ .

This polynomial is irreducible and therefore separable over  $\mathbb{Q}$ . The resolvent cubic is  $x^3 + 8x = x(x + 2i\sqrt{2})(x - 2i\sqrt{2})$  and  $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(i\sqrt{2})$  has dimension 2 over  $\mathbb{Q}$ .  $x^4 - 2$  is irreducible over  $\mathbb{Q}(i\sqrt{2})$  because  $\sqrt[4]{2} \notin \mathbb{Q}(i\sqrt{2})$ . Therefore the Galois group  $G \cong D_8$ .

Let  $F \subset \mathbb{C}$  be a splitting field over  $\mathbb{Q}$  of  $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ . If  $u$  is the positive real fourth root of 2, then the roots of  $f$  are  $u, -u, ui, -ui$ . In order to consider the Galois group  $G = \text{Aut}_{\mathbb{Q}}^F$  of  $f$  as a subgroup of  $S_4$ , we must choose an ordering of the roots, say  $u_1 = u, u_2 = ui, u_3 = -u, u_4 = -ui$ . The complex conjugation is an  $\mathbb{R}$ -automorphism of  $\mathbb{C}$  which clearly sends:

$$u \mapsto u, -u \mapsto -u, ui \mapsto -ui \text{ and } -ui \mapsto ui.$$

This induces a  $\mathbb{Q}$ -automorphism  $\tau$  of  $F = \mathbb{Q}(u, ui)$ . As an element of  $S_4$ ,  $\tau = (24)$ . Now the generator of  $D_8$  containing  $\tau = (24)$  is  $\sigma = (1234)$ . We have  $F = \mathbb{Q}(u, ui) = \mathbb{Q}(u, i)$ , so every  $\mathbb{Q}$ -automorphism of  $F$  is completely determined by its action on  $u$  and  $i$ . Thus the elements of  $G$  may be described either in terms of  $\sigma$  and  $\tau$  or by their action on  $u$  and  $i$ . The information is summarized in the table:

	(1)	(24)	(1234)	(13)(24)	(1432)	(12)(34)	(13)	(14)(32)
		$\tau$	$\sigma$	$\sigma^2$	$\sigma^3$	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
$u \mapsto$	$u$	$u$	$ui$	$-u$	$-ui$	$ui$	$-u$	$-ui$
$i \mapsto$	$i$	$-i$	$i$	$i$	$i$	$-i$	$-i$	$-i$

(1)

$$< \tau > \quad < \sigma^2\tau > \quad < \sigma^2 > \quad < \sigma\tau > \quad < \sigma^3\tau >$$

## 4.4 Galois group of Quantic polynomials

There are very less techniques for computing Galois groups of polynomials of degree greater than 4 over arbitrary fields.

**Theorem 11.** *If  $p$  is a prime and  $f$  is an irreducible polynomial of degree  $p$  over  $\mathbb{Q}$  which has precisely two nonreal roots, then the Galois group of  $f$  is  $S_p$ .*

**Example 3.** The graph of the polynomial  $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$  shows it has only three real roots. This polynomial is irreducible over  $\mathbb{Q}$  so its Galois group is  $S_5$ .

## 4.5 Galois Group of Reducible polynomials

For any polynomial  $f \in K[x]$  we factor  $f$  as  $f_1 f_2 \dots f_k$  and compute the Galois group  $G_i$  of  $f_i$  for each  $i = 1, 2, \dots, k$ . Then the Galois group  $G$  of  $f$  is isomorphic to a subgroup of  $\prod G_i$ .

**Example 4.** The polynomial is  $f(x) = x^4 - 5x^2 + 6$

Here,  $f(x) = (x^2 - 2)(x^2 - 3)$  so it is reducible over  $\mathbb{Q}$ . Let  $f_1(x) = (x^2 - 2)$  and  $f_2(x) = (x^2 - 3)$ . Then  $f_1, f_2$  are both irreducible over  $\mathbb{Q}$ .

The splitting field for  $f_1$  is  $\mathbb{Q}(\sqrt{2})$  so its Galois group is  $\mathbb{Z}_2$ . The splitting field for  $f_2$  is  $\mathbb{Q}(\sqrt{3})$  so its Galois group is also  $\mathbb{Z}_2$ . Now we have the Galois group of  $f$  is a subgroup of  $G = \mathbb{Z}_2 \mathbb{Z}_2$ .

Since the intersection of  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt{3})$  is trivial the Galois group of  $f$  is  $G$  itself which is *Klein 4-group*.

# Chapter 5

## The Classic Problem

1. Is every polynomial equation solvable by the method of radicals?
2. Equivalently, does there exist an explicit "formula" which gives all solutions of an arbitrary polynomial equation?

If the degree of the polynomial  $f$  is at most four then the answer is "yes".

### 5.1 Formulation of the Classic Problem

The "formula" by the method of radicals means the formula involving only field operations and the extraction of  $n$ th roots. The existence of a "formula" means there is a finite sequence of steps, each step being a field operation or the extraction of an  $n$ th roots, which yields all solutions of the given polynomial. Performing a field operation leaves the base field unchanged, but the extraction of an  $n$ th root of an element  $c$  in a field  $K$  amounts to constructing an extension field  $K(u)$  with  $u^n \in K$ . Thus the existence of a "formula" for solving  $f(x) = 0$  would imply the existence of a finite tower of fields

$$K = E_0 \subset E_1 \subset \dots \subset E_n$$

such that  $E_n$  contains a splitting field of  $f$  over  $K$  and for each  $i \geq 1$ ,  $E_i = E_{i-1}(u_i)$  with some positive power of  $u_i$  lying in  $E_{i-1}$ .

Conversely suppose there exists such a tower of fields and that  $E_n$  contains a splitting field of  $f$ . Then

$$E_n = K(u_1, u_2, \dots, u_n)$$

and each solution is of the form  $f(u_1, \dots, u_n)/g(u_1, \dots, u_n)$  where  $f, g \in K[x_1, \dots, x_n]$ . Thus each solution is expressible in terms of a finite number of elements of  $K$ , a finite number of field operations and  $u_1, \dots, u_n$ . But this amounts to saying that there is a "formula" for the solutions of the particular given equation.

**Definition 12** (Radical Extension). An extension field  $F$  of a field  $K$  is a radical extension of  $K$  if  $F = K(u_1, \dots, u_n)$ , some power of  $u_1$  lies in  $K$  and for each  $i \geq 2$ , some power of  $u_i$  lies in  $K(u_1, \dots, u_{i-1})$ .

*Remark.* If  $u_i^m \in K(u_1, \dots, u_{i-1})$  then  $u_i$  is a root of  $x^m - u_i^m \in K(u_1, \dots, u_{i-1})[x]$ . Therefore every radical extension  $F$  of  $K$  is finite dimensional algebraic over  $K$ .

**Definition 13.** The equation  $f(x) = 0$  is *solvable by radicals* if there exists a radical extension  $F$  of  $K$  and splitting field  $E$  of  $f$  over  $K$  such that  $F \supset E \supset K$ .

**Theorem 12.** If  $F$  is a radical extension of  $K$  and  $E$  is an intermediate field, then  $\text{Aut}_K^E$  is a solvable group.

**Corollary 12.1.** If the equation  $f(x) = 0$  is solvable by radicals, then the Galois group of  $f$  is a solvable group.

## 5.2 Group Theoretic Concepts

Let  $G$  be a group.

**Definition 14** (Solvable Series). A finite chain of subgroups  $G = G_0 > G_1 > \dots > G_n = e$  such that  $G_{i+1}$  is normal in  $G_i$  for  $0 \leq i < n$  is called a subnormal series of  $G$ .

A subnormal series is a solvable series if each factor group  $G_i/G_{i+1}$  is abelian.

**Definition 15** (Solvable Group). A group is solvable if and only if it has a solvable series.

If  $F$  is a radical extension of  $K$  then  $F$  is Galois over  $K$  and by the Fundamental Theorem of Galois  $\text{Aut}_K^E$  has a solvable series where  $E$  is an intermediate field. So  $\text{Aut}_K^E$  is solvable.

## 5.3 Conclusion

**Theorem 13.** The symmetric group  $S_n$  is not solvable for  $n \geq 5$ .

The polynomial  $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$  has Galois group  $S_5$ , which is not a solvable group.

The quintic polynomials over  $\mathbb{Q}$  are not solvable by radicals. That is there does not exist an explicit formula for solving the quintics.

Moreover, polynomials of degree  $n \geq 5$  are not solvable by radicals.



*Remark.* The base field plays an important role here. The polynomial  $x^5 - 4x + 2$  is not solvable by radicals over  $\mathbb{Q}$ , but it is solvable by radicals over  $\mathbb{R}$  of real numbers. In fact, every polynomial equation over  $\mathbb{R}$  is solvable by radicals since all the solutions lie in the algebraic closure  $\mathbb{C}$  which is a radical extension of  $\mathbb{R}$ .

# Chapter 6

## Galois Fields

Galois fields are the finite fields. They can be completely characterized in terms of splitting fields and the Galois group of an extension of a finite field by a finite field is shown to be cyclic.

**Definition 16** (Prime Fields). Let  $F$  be a field and let  $P$  be the intersection of all subfields of  $F$ . Then  $P$  is a field with no proper subfields. This field  $P$  is called the Prime subfield of  $F$ .

1. If  $\text{char} F = p(\text{prime})$ , then  $P \cong \mathbb{Z}_p$ .
2. If  $\text{char} F = 0$ , then  $P \cong \mathbb{Q}$ .

**Theorem 14.** *A field  $F$  is a finite field with  $p^n$  elements if and only if  $F$  is a splitting field of  $x^{p^n} - x$  over  $\mathbb{Z}_p$ .*

**Theorem 15.** *If  $F$  is a finite dimensional extension field of a finite field  $K$ , then  $F$  is finite and is Galois over  $K$ . The Galois group  $\text{Aut}_K^F$  is cyclic.*

# Bibliography

- [1] T. W. Hungerford. *Algebra*. Springer (India), New Dheli, 2012.