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 Parents

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. Doc. Tanka Nath Dhamala
(Head of Department)
Central Department of Mathematics
Institute of Science & Technology
Tribhuvan University Kirtipur, Kathmandu, Nepal.
Date: March, 2024

Contents

Symbol Conventions

Through out the thesis following Symbol Convention has been used.

- **K** a field.
- **F** an extension field of the field **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

Introduction

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.

1.1 Approaches to the Theory

1. Galois approached this problem by using the properties of permutation groups to the roots of a polynomial equation solvable by radicals. And this linked Field theory to Group theory.

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 Life History of Galois

He was Born in an educated family in Paris in the era of Napoleon. Napoleon was at the height of his power in 1811 but by 1824 his French empire was falling apart and he was put into prison by the British.

Galois was by this time at school and enrolled in mathematics class in 1827(16 yrs) where he was described intelligent, singular and original. In 1829(18 yrs) he published his first paper on continued fractions and submitted his articles on the algebraic solution of equations where *Cauchy* was a referee of Galois' paper. He again submitted a new article which was sent to *Fourier*, to be considered for the Grand Prize in mathematics but Fourier died and Galois' paper was never found.

He was frustrated, and then became involved in the political revolution going on then in France against Napoleon. He got arrested was put into prison where he fell in love with *Stephanie*. He then fought a duel with *Prscheux* who was a solder. The reason of the fight is not clear. It is guessed that both of them loved Stephanie. He got shot in the duel and died the other day.

Figure 1.1: Galois

There is this legend that he spent his last night writing all he knew about group theory. Galois' papers were sent to Gauss,Jacobi and others. Later the paper reached to Liouville who published them in 1846.

Chapter 2

Galois Correspondence

2.1 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: $a_n u^n + a_{n-1}u^{n-1} + ... + a_1 u + a_0$ which is given by the polynomial $f(u)$, where $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$.

So the structure of the extension field $F = K(u)$ is:
$F = \{\frac{f(u)}{g(u)} \mid f, g \in K[x], g(u) \neq 0\}$.

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]*

2.1.1 Algebraic and Transcendental element

Theorem 2. *Let F be an extension field of a field F.*
A map $\phi : K[X] \to K[u]$ where $u \in F$ defined by $\phi(f(x)) = f(u)$
i.e, $\phi(a_0 + a_1 x + ... + a_n x^n) = a_0 + a_1 u + ... + a_n u^n$ 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, $K[x] \ncong K[u]$ because $Ker\phi$ is non trival 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 $\{1_k, u, u^2, ..., u^{n-1}\}$ 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.

2.2 Galois Group

Let F be a field. The set $AutF$ of all field-automorphisms $F \to F$ 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 $\sigma : E \to F$ is a K-module homomorphism then $\sigma(k) = \sigma(k1_E) = k\sigma(1_E) = k1_F = k$. i.e, σ fixes K element-wise.
Conversely, if a field homomorphism $\sigma : E \to F$ fixes K element-wise, then σ is a non-zero and for any $u \in E$, we have, $\sigma(ku) = \sigma(k)\sigma(u) = k\sigma(u)$ i.e σ is a K-module homomorphism.

Definition 1. A field-automorphism $\sigma \in AutF$ which is also K-homomorphism is called K-automorphism. In other words, a field-automorphism $\sigma \in AutF$ 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.

2.3 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.

2.3.1 Fixed Field

We have,
$H' \rightarrow$ fixed field and $E' \rightarrow Aut_E^F$. Let $Aut_K^F = G$ 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 $G = Aut_Q^{Q(u)} = 1$ so, $G' = F \neq K$.

Definition 3. Let F be an extension field of K such that the fixed field of the Galois group Aut_K^F is K itself. Then F is said to be a Galois extension of K or Galois over K.

2.4 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 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 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 $E' = Aut_E^F$ is normal in $G = Aut_K^F$.In this case G/E' is isomorphic to the Galois group 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 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 $H'' = H$.

2.4.1 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 $E \to E' = Aut_E^F$.

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 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 Aut_K^F has order $[F : K]$.

2.4.2 Stable Intermediate

Lemma 3. Let F be an extension field of K.

i) If E is a stable intermediate field of the extension, then $E' = Aut_E^F$ is a normal subgroup of the Galois group Aut_K^F;

ii) if H is a normal subgroup of Aut_K^F, then the fixed field H' of H is a stable intermediate field of the extension.

2.4.3 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. $E' = Aut_E^F$ is normal in Aut_K^F. Conversely if E' is normal in 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 is Galois over K), we have $|G/E'| = [G : E'] = [E'' = G'] =$

$[E : K]$. So, $G/E' = Aut_K^F/Aut_E^F$ is isomorphic to a subgroup of Aut_K^F. But by first part of the theorem, $|Aut_K^E| = [E : F]$(since E is Galois over K). This implies $G/E' = Aut_K^E$. $\square$

Chapter 3

Structure of Galois Extension

Galois extension F of K is a field for which the fixed field of the Galois group 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 $\sigma \in Aut_K^F$ 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 5. 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 in 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 6. 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 7. 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 $char K = 0$.

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 sates 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 8. 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 isomorphic to a transitive subgroup of S_n.

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 $G = \mathbb{Z}_2$.

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 9. Let K be a field with $charK \neq 2$ and $f \in K[x]$ a polynomial of degree n with n distinct roots $u_1, u_2, ..., u_n$ in some splitting field F of f over K. Let $\Delta = \prod\limits_{i<j}(u_i - u_j) = (u_1 - u_2)(u_1 - u_3)...(u_{n-1} - u_n) \in F$.
The discriminant of f is the element $D = \Delta^2$.

Theorem 8. *i) The discriminant Δ^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. $\sigma(\Delta) = -\Delta$].

Because the $\Delta^2 \in K$ and $\Delta \in F$, 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 $charK \neq 2, 3$. 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 $-4p^3 - 27q^2$.*

4.2 Galois Group of Quartic polynomials

Let K, f, F, u_i, V, and $G = Aut_K^F < S_4$ be as in the preceding paragraph.
If $\alpha = u_1u_2 + u_3 + u_4$, $\beta = u_1u_3 + u_2 + u_4$, $\gamma = u_1u_4 + u_2 + u_3$, then under the Galois correspondence the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$. Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $Aut_K^{K(\alpha,\beta,\gamma)} = G/(G \cap V$.

Definition 10 (Resolvant Cubic of a Quartic)**.** The elements α, β, γ play a crucial role in determining the Galois Groups of arbitrary quartics. The polynomial $(x - \alpha)(x - \beta)(x - \gamma)$ is called the resolvant cubic of f. The resolvant cubic is actually a polynomial over K.

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 α, β, γ be the roots of the resolvant cubic of f and let $m = [K(\alpha, \beta, \gamma) : K]$. Then:*

i) $m = 6 \Longleftrightarrow G = S_4$;

ii) $m = 3 \Longleftrightarrow G = A_4$;

iii) $m = 1 \Longleftrightarrow G = V$;

iv) $m = 2 \Longleftrightarrow G = D_4$ *or* $G = \mathbb{Z}_4$*; in this case* $G = \mathbb{Z}_4$ *if* f *is irreducible over* $K(\alpha, \beta, \gamma)$ *and* $G = \mathbb{Z}_4$ *otherwise.*

Chapter 5

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 11 (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 $charF = p(prime)$, then $P \cong \mathbb{Z}_p$.
2. If $charF = 0$, then $P \cong \mathbb{Q}$.

Theorem 11. *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 12. *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 Aut_K^F is cyclic.*

Bibliography

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