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.

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

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

....
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

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.

Figure 1.1: Portrait of Galois

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 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: $a_n u^n + a_{n-1}u^{n-1} + ... + a_1 u + a_0$ 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]*

1.3 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.

Chapter 2

Galois Correspondence

2.1 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.

2.2 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,
$H' \to$ fixed field and $E' \to Aut_E^F$. 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.

2.3 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 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 $H'' = H$.

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

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 $[F : K]$.

2.3.2 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 $\sigma \in Aut_K^F$.

Lemma 3. 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.

2.3.3 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. $E' = Aut_E^F$ 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 $G/E' = Aut_K^E$. □

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 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 $char K = 0$.

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 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 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 $charK \neq 2$ 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. $\sigma(\Delta) = -\Delta$].

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 $charK \neq 2, 3$. 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 $-4p^3 - 27q^2$ [1].*

4.2 Galois Group of Quartic polynomials

Definition 11 (Resolvant Cubic of a Quartic)**.** Let K, f, F, u_i, V, and $G = Aut_K^F < S_4$ 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 $Aut_K^{K(\alpha,\beta,\gamma)} = G/(G \cap V$.

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 α, β, γ 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* $G = \mathbb{Z}_4$ *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 resolvant 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 $G = Aut_{\mathbb{Q}}^F$ 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:
$u \mapsto u$, $-u \mapsto -u$, $ui \mapsto -ui$ and $-ui \mapsto ui$.
This induces a $\mathbb{Q}$-automorphism τ 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 σ and τ 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)
		τ	σ	σ^2	σ^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	$-i$	$-i$	$-i$

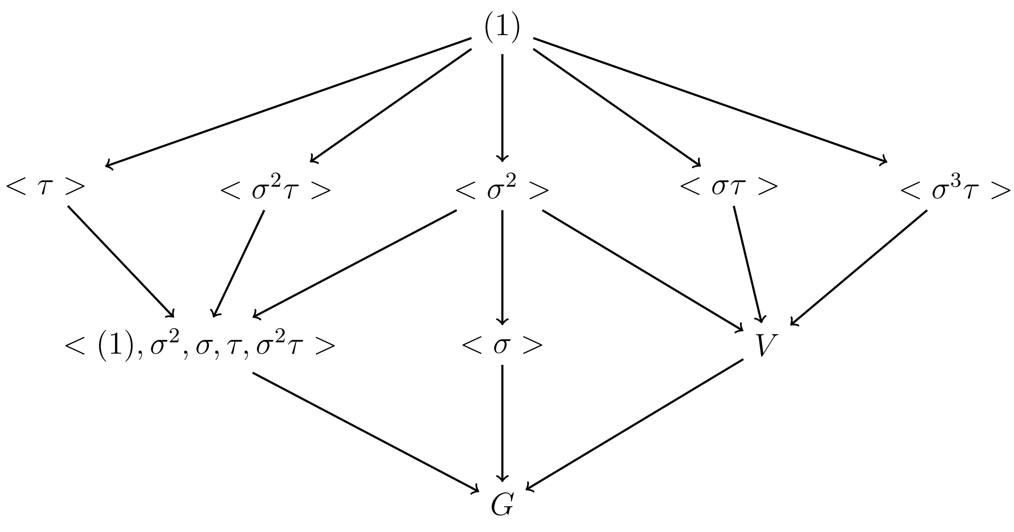


Figure 4.1: Subgroup diagram of the Galois group

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 $f_1 f_2 ... f_k$ and compute the Galois group G_i of f_i for each $i = 1, 2, ..., k$. 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 trival 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 nth roots. The existence of a "formula" means there is a finite sequence of steps, each step being a field operatioin or the extraction of an nth roots, which yields all solutions of the given polynomial. Performing a field operatioin leaves the base field unchanged, but the extraction of an nth root of an element c in a field K amounts to constructing an extenstion 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

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

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

$$E_n = K(u_1, u_2, ..., u_n)$$

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

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

Remark. If $u_i^m \in K(u_1, ..., u_{i-1})$ then u_i is a root of $x^m - u_i^m \in K(u_1, ..., u_{i-1})[x]$. Therefore every radical extenstion 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 extenstion 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 extenstion of K and E is an intermediate field, then 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 Theoritic Concepts

Let G be a group.

Definition 14 (Solvable Series)**.** A finite chain of subgroups $G = G_0 > G_1 > ... > G_n = e$ 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 Aut_K^E has a solvable series where E is an intermediate field. So 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 quantic polynomials over $\mathbb{Q}$ are not solvable by radicals. That is there does not exist an explicit formula for solving the quantics.
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 $\mathbb{R}$.

Part III

Galois-Field

Chapter 6

Galois Fields

Galois fields are the finite fields. They can be completely characterized in terms of splitting fields of some polynomials. It is found that the Galois group of an extension of a finite field by a finite field is cyclic. The Galois field with q elements is denoted by $GF(q)$.

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

Theorem 14. *A finite field F has p^n number of elements where $p \in \mathbb{Z}_+$ is a prime and it has p^n number of 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 Aut_K^F is cyclic.*

6.1 Representation of Finite Fields

Basically there are two types of representation of a finite field. These two representations are equivalent.

6.1.1 Integer representation

$GF(p^n) = \{0, 1, ..., p-1\} \cup \{p, p+1, ..., p+p-1\} \cup ... \cup \{p^{n-1}, p^{n-1}+1, ..., p^{n-1}+p^{n-2}+...+p-1\}$.

Example 5. $GF(2) = \{0, 1\}$
$GF(2^3) = \{0, 1\} \cup \{2, 2+1\} \cup \{2^2, 2^2+1, 2^2+2, 2^2+2+1\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$

But the digits $2, 3, .., 7$ of the field $GF(2^3)$ do not lie on the field $GF(2)$. If we look the field $GF(2^3)$ as an extension field of $GF(2)$ and write its elements using only the elements of the base field $GF(2)$ then we have the following representations:

Digits		Binary rep..
3	$2+1$	011
4	$2^2 + 2^1 \times 0 + 2^0 \times 0$	100
5	$2^2 + 1$	110

This is actually **Binary representation** of the field $GF(2^3)$

6.1.2 Polynomial representation

For a field F and an irreducible polynomial $f(x) \in F[x]$ the quotient ring $F[x]/(f(x))$ is field.
If F is a finite field consisting of p elements and $f(x) \in F[x]$ is irreducible then $F[x]/(f(x))$ is finite field. This field consists of all polynomials modulo $f(x)$. If $F = GF(2^3)$ then $x^8 + x^7 + ... + x + 1 \in F[x]$ is irreducible in $F[x]$. Since F has 8 elements which are modulo 8, elements of F is represented by the elements of the factor ring $F[x]/(f(x))$.

In the example-5, the number 5 has the representation $2^2 + 1$. This gives the polynomial representation $x^2 + 1 = (1, 0, 1)$(coefficient of x^2 is 1 of x is 0 and of constant is 1) Now the binary equivalent of 5 is 101.

6.2 Operations in Galois Field

Let the Galois field be $GF(p^n)$. Since the elements of a Galois field can be represented as polynomials the operations are similar to polynomial operations. Let $f(x) = a_0 + a_1x + .. + a_{n-1}x^{n-1}$ and $g(x) = (b_0 + b_1x + ... + b_{n-1}x^{n-1}$.

1. Addition
   $f(x) + g(x) \quad (modp)$

2. Multiplicaiton
   $f(x).g(x) \quad (modp)$

Chapter 7

Application in Coding Theory

Any information gets deteriorated or lost over time.

1. Paintings gets deteriorated over time and has to be renovated.
2. Some of the words spoken by teacher in the class is missed due to noise.

To be able to over come this issue , i.e to be able to detect and correct errors during transmission of information in digital system "coding theory" is developed. In digital system, information are transmitted as strings of 0 and 1. The idea of coding theory is to append some extra digits to the information and use this to detect and possibly correct the errors during transmission. So the fundamental of the coding theory in computer system is the manipulation of strings of binary digits. The proper and complete manipulation of these strings is possibly only if the space of the strings is a field. This field is finite so this field is a **Galois field**. This is where the application of Galois theory comes. Another advantage of using field is that the space of code forms a vector space over the base field. The widely used field for coding in electronically transmitting device is the field $\mathbb{Z}_2$ which is the field $GF(2)$ consisting of 0 and 1. Recent works has shown that it is possible to extend codes to more general type of numbers called rings. This rings are called "Galois rings".

The non-empty set of symbols for the code $\mathcal{A}$ called **alphabet**. A finite sequence of elements from $\mathcal{A}$ is called a **word** over $\mathcal{A}$. Let $\mathcal{A}^*$ be the set of all words over $\mathcal{A}$. A subset C of $\mathcal{A}$ is called a code. If the cardinality of the alphabet $\mathcal{A}$ is q then the code C is called $q-arycode$. For $q = 2$ it is called binary and for $q = 3$ it is caled terniary.

7.1 Linear Codes

Let $K = GF(q)$ be a Galois field. Then a finite extension of K of dimension n is $V = GF(q)^n = GF(q^n)$.

Definition 17. A linear code C is a subspace of V.
The code C has dimension $k \leq n$ and the length n. It is called a (n, k) code.

The usefulness of linear code is that they are vector spaces over the base field so they have a basis. All the code words can be generated with this basis. Instead of storing all 2^k number of code words (for k-dimensional binary codes), storing only k basis elements is sufficient which saves massive storage.

Let C be (n, k) code which is a subspace of V.

Definition 18 (Generator Matrix)**.** Let $\{v_1, v_2, ..., v_k\}$ be a basis of C. A generator matrix is the $k \times n$

$$G = \begin{pmatrix} v_1 \\ v_2 \\ . \\ . \\ . \\ v_k \end{pmatrix}$$

Definition 19 (Parity check matrix)**.** The dual code of C is the set $C^{\perp} = \{x \in V \mid x.y = 0 \ \ \forall y \in V\}$. The dual code is a code in itself and has dimension $n - k$. The $C^{\perp}$ is linear so it has a generator matrix. A generator matrix H of $C^{\perp}$ is called a parity check matrix.

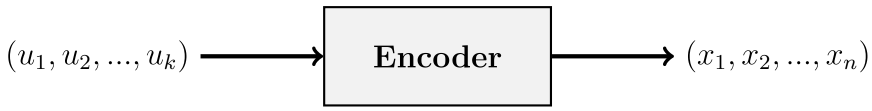
Theorem 16. *If $G = (I_{k\times k}, A_{k\times(n-k)})$ is a generator matrix of an (n, k) code C then its parity check matrix is $H = (I_{(n-k)\times(n-k)}, A'$ where A' is the transpose of A.*

Definition 20. The *Hamming distance* between $v, w \in V$ is defined by $d_h(v, w) = |\{i \mid v_i \neq w_i;\ 1 \leq i \leq n\}|$.
The *minimum distance* of a code C is defined as $min\{d_h(v, w) \mid d_h(v, w) \neq 0, v, w \in C\}$.
The weight of a vector is its distance from zero and the *minimum weight* of a code C is the minimum weight of all non-zero weights of the vectors in C.

Theorem 17. *A linear code C with minimum weight d can correct strings having number of errors up to $t = \lfloor (d - 1)/2 \rfloor$.*

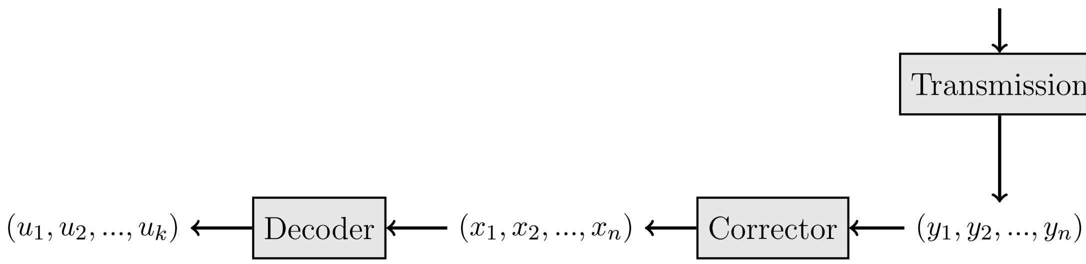
7.2 Illustration

To apply (n, k) coding first we need to group our information into blocks of length k. $u_1, ..., u_k$, $u_k, ..., u_{2k}$,... . This space has dimension k. Now these block of codes are encoded separately each to a code of length n as shown.



Mathematically, the encoded vector x is obtained form the original vector u using the generator matrix G by the relation $x = uG$.

To continue and complete the diagram.



7.3 Syndrome Decoding

Definition 21. The syndrome of a vector $y \in V$ is defined as

$$syn(y) = \begin{pmatrix} y.h_1 \\ y.h_2 \\ . \\ . \\ . \\ y.h_{n-k} \end{pmatrix}, \qquad \text{where} \begin{pmatrix} h_1 \\ h_2 \\ . \\ . \\ . \\ h_{n-k} \end{pmatrix} \text{is the parity check matrix of } C.$$

Now the code C is a subgroup of V under addition. Moreover, it is a normal subgroup of V.

Theorem 18. *Two vectors in V have the same syndrome if and only if they are in the same co-set of C.*

7.3.1 Decoding Process

Suppose the signal received is the vector y.

1. First we determine its syndrome, $syn(y)$.
2. Determine the co-set of C containing $syn(y)$, say $e + C$.
3. Then $y = e + x$ for some $x \in C$. This implies $x = y - e$. Since $x \in C$, this x is the required decoding of y.

This e is also called "error vector".

Example 6. Consider a generator matrix $G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$. Then the parity check matrix is $H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. And the code generated by G is $C = \{(0,0,0,0), (1,0,1,0), (0,1,1,1), (1,0,1,1)\} \quad \subset GF(2)^4$.

Suppose the received vector is $y = (1,1,1,0)$. Then $y \notin C$ so the information is distorted from the original information. To get the original information:
$syn(y) = \begin{pmatrix} y.h_1 \\ y.h_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ where h_1 is the first row and h_2 is the second row of H.
Now if $e = (0,1,0,0)$ then $e + C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ so $y - e = (1,1,1,0) - (0,1,0,0) = (1,0,1,0) \in C$ is the original information.

7.4 Perfect Code

The code $C \subseteq V$ as of above is perfect if the union of all the spheres of radius t about its code-words is the vector space V.
This code is C is called perfect because every received vector with the number of errors given by t can be decoded to a code-word of C.

Example 7. The code $C = V$ is a perfect code. This code cannot correct any errors because every possible code word is in the C. Therefore this perfect code is trivial.

Example 8. The general binary Hamming code H_r, $r \in \mathbb{N}$ whose parity check matrix H column consisting of non-zero r-tuples.

7.5 Cyclic Code

The code C as of above is cyclic if $(a_0, a_1, ..., a_{n-1}) \in C \implies (a_{n-1}, a_0, ..., a_{n-2}) \in C$.

Suppose C is a code over a Galois field $F = GF(q)$. Then there exist a correspondence $\Phi : C \mapsto F[x]/(x^n - 1)$ such that $(a_0, a_1, ..., a_{n-1}) \longmapsto a_0 + a_1 x + a_2 x^2 + ... + a_{n-1}x^{n-1}$.
This shows that the cyclic code C can be embedded into the ring $R_n = F[x]/(x^n - 1)$.

Theorem 19. *1. A subset S of R_n corresponds to a cyclic code if and only if S is an ideal of R_n and*

2. if $S = (g(x))$ if and only if $g(x)$ divides $x^n - 1$

This theorem determines all cyclic codes. They are ideals of R_n and these ideals are generated by the polynomials that divides $x^n - 1$.

Example 9. The divisors of $x^3 - 1 \in F = GF(2)^3$ are $1, x+1, x^2+x+1, x^3-1$. For $g(x) = x + 1$ we have $F[x]/(g(x)) = \{(0), (1 + x), (1 + x^2), (x + x^2)\}$ so the corresponding cyclic code is $\{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\}$.

Similar to general linear codes which are defined using the generator matrix or the parity-check matrix, cyclic codes are defined using generator polynomial or parity-check polynomial and due to this efficient algebraic decoding algorithm exist.

7.5.1 Usages

1. The $(3, 1)$ binary code is used in the short-range wireless communication system like $Bluetooth^{TM}$.
2. The Hamming Code $(7, 4)$ is used in memory devices like RAM.

Chapter 8

Application in Cryptography

8.1 Cryptography

It is the science of safe-guarding messages during transmission by converting the original message into something unreadable.
Galois Fields are the life of modern cryptography used in digital communication.

8.2 Advance Encryption Standard(AES)

This is the standard of Encryption used these days. The generic algorithm of AES consists of smaller sub-algorithms namely Sub-Bytes, Shift-Rows, Mix-Columns and Add-Round-Key.

8.2.1 States

First the data is broken into smaller chunks of bytes called states which is representation by the entries of a matrix. Mathematical operations are not applicable to the data directly so the significance of this step is to make the data applicable for mathematical operations.
For the 128-bit key encryption the algorithm forms a 4×4 matrix with each entry of a size one byte. This matrix can afford to evaluate a data of size 16 byte at a time.

8.2.2 Sub-Bytes

In this step, first each byte of the matrix is replaced with its multiplicative inverse if it has one. Then it transforms each bytes using an invertible affine transformation, $x \mapsto Ax + b$.

8.2.3 Shift-Rows

In this step entries of a row is shifted to scramble data. Row-n shifted to the left by $n-1$ unit. Here,
$1-1=0$, so row-1 is left unchanged. $2-1=1$, so row-2 is shifted to the left by 1 unit and row-3 by 2 unit and so on as shown below.

$$\text{If } A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \quad \text{then } A' = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{22} & a_{23} & a_{24} & a_{21} \\ a_{33} & a_{34} & a_{31} & a_{32} \\ a_{44} & a_{41} & a_{42} & a_{43} \end{bmatrix}$$

is the matrix after Shit-Row

8.2.4 Mix-Columns

In this step each column is transformed using a linear transformation, $c \mapsto Bc$ where c is a column of the matrix obtained above. Since linear transformation is invertible this step is invertible. Note every step of this algorithm must be invertible to be able to decrypt the data.

8.2.5 Add-Round-Key

This is the step where the encrypted data gets uniqueness. Each user is assigned an "unique key" and this key is added to the matrix obtained from the last step.

8.3 Illustration

Let us encrypt the sentence "Fun Cryptography". This consists of exactly 16 characters.

1. First we write the ASCII representation of each character of the sentence as shown below. We do so because the ASCII representation gives the binary representation of each character which has a size of a byte. The ASCII representaion of "F" is 70 which is 01000110 in binary.

$$\begin{bmatrix} 70 & 117 & 110 & 32 \\ 67 & 114 & 121 & 112 \\ 116 & 111 & 103 & 114 \\ 97 & 112 & 104 & 121 \end{bmatrix} = \begin{bmatrix} 01000110 & 01110110 & 01101110 & 00010000 \\ 01000011 & 01110010 & 01111001 & 01110000 \\ 01110100 & 01101111 & 01100111 & 01110010 \\ 01100001 & 01110000 & 01101000 & 01111001 \end{bmatrix}$$

2. After performing Sub-Bytes, Shift-Rows, Mix-Columns, we get the following matrix.

$$\begin{bmatrix} 11100111 & 00011000 & 00100100 & 01110000 \\ 00101010 & 10101011 & 00111001 & 01100011 \\ 00010101 & 01100101 & 11110111 & 10100111 \\ 10101011 & 11110110 & 00000011 & 10100100 \end{bmatrix} = \begin{bmatrix} 231 & 24 & 36 & 112 \\ 42 & 171 & 57 & 99 \\ 21 & 101 & 247 & 167 \\ 171 & 246 & 3 & 164 \end{bmatrix}$$

3. We have omitted the Add-Round-Key step just for the sake of simplicity. The matrix obtained at last in step-2 translates to something different from our original sentence.

4. The decryption process is applying the inverse of the encryption process.

Bibliography

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