Central Department of Mathematics, TU

Applications of Galois Theory

Presenter:

Mr. Sandesh Thakuri

Roll no: 43

Supervisor:

Asoc. Prof. Tulasi Prasad Nepal

2081-1-9

Figure: Portrait of Galois

In my thesis, I have explored the applications of Galois Theory in both pure and applied mathematics. Modern Galois Theory is the theory of field extension whose foundation was laid by the French Mathematician *Évariste Galois* in the 1800s who had died at the early age of 20.

Outlines

Let F be an extension field of a field K.

1. Galois Group

The set of all automorphisms of F that fixes K element-wise forms a permutation group.

This group is called the Galois group of F over K and it is denoted by Aut_K^F [3].

2. Galois Extension

The extension field F of K is said to be Galois extension if the fixed field of the Galois group Aut_K^F is K itself.

3. Fundamental Theorem of Galois Theory

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 $H = Aut_E^F$ is normal in $G = Aut_K^F$. In this case G/H is isomorphic to the Galois group Aut_K^E of E over K [3].*

This theorem connects Field Theory to Group Theory.

Let F be an Galois extension of a field K and E be the intermediate field of F over K:

$$K \subset E \subset F$$

Let G be the Galois group of F over K. Then H and e are its subgroups:

$$\{e\} \subset H \subset G$$

Then the one-to-one correspondence is as shown:

Galois-correspondence

$$\begin{tikzcd} F \arrow[r, leftrightarrow] \arrow[d] & \{e\} \\ E \arrow[r, leftrightarrow] \arrow[d] & H \arrow[u] \\ K \arrow[r, leftrightarrow] & G \arrow[u] \end{tikzcd}$$

4. Remark

The intermediate fields are getting larger as we go from bottom to top as the fields are getting extended. But the subgroups are getting smaller.

Nature of Number

The nature of a number depends upon the underlying field.
$\sigma : \{a + b\sqrt{2}\} \mapsto \{a - b\sqrt{2}\}$ denoted by $\sqrt{2} \longmapsto -\sqrt{2}$ is an automorphism of the field $\mathbb{Q}(\sqrt{2})$ that fixes $\mathbb{Q}$. So, any polynomial equation over $\mathbb{Q}$ satisfied by the number $\sqrt{2}$ is also satisfied by the number $-\sqrt{2}$. You can fluidly pass between these two numbers and the equation with a rational coefficient will not know. Hence the two numbers $\sqrt{2}$ and $-\sqrt{2}$ are algebraically same over $\mathbb{Q}$.

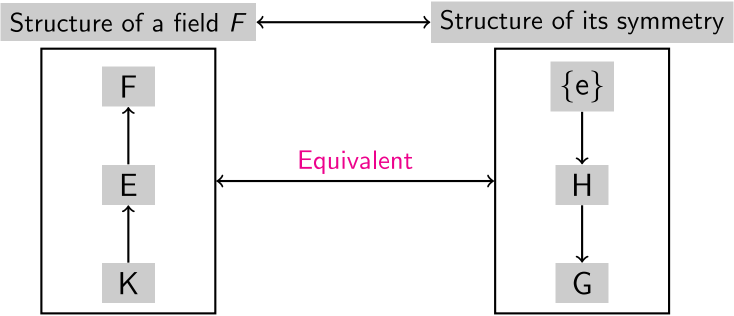
But the map $\sqrt{2} \longmapsto -\sqrt{2}$ does not fix $\mathbb{Q}(\sqrt{2})$ i.e doesn't fix itself. So, you cannot pass $\sqrt{2}$ for $-\sqrt{2}$ for every equation with coefficients in $\mathbb{Q}(\sqrt{2})$. Hence the two numbers $\sqrt{2}$ and $-\sqrt{2}$ are not algebraically same over $\mathbb{Q}(\sqrt{2})$.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}) \arrow[rr, leftrightarrow] & & \{e\} \arrow[d] \\
\mathbb{Q} \arrow[u] \arrow[rr, leftrightarrow] & & \{i,\, \sqrt{2} \mapsto -\sqrt{2}\}
\end{tikzcd}$$

Structure of a Field

The structure of a field as an extension field over some field is mirrored in the structure of the "group" of permutations of its elements that keeps the base field fixed. But these permutations are the symmetries of the field. So, the structure of a field extension equals to structure of its own symmetry.

The structure of a field is a complicated thing; specially if it is infinite. But the structure of a group is rather simple; especially if it is finite. So the Galois theory has fairly simplified the complicated thing in a very insightful and beautiful way.



Question

Galois extension F of K is a field for which the fixed field of the Galois group Aut_K^F is K itself.

Questions:

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

Since, for $F = K(u)$, any $\sigma \in Aut_K^F$ is completely determined by its action on u [3]. Any algebraic Galois extension of K is generated by all roots u of a polynomial $f \in K[x]$ (all roots means f splits here).

Splitting Field

Such a minimal field F which contains all roots of $f \in K[x]$ is called a splitting field of f over K [3] because f splits into linear factors in F.

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

Example

The extension field $\mathbb{Q}(\sqrt{3})$ over the field $\mathbb{Q}$ is a Galois extension and it is also a splitting field of the polynomial $f(x) = x^2 - 3 \in \mathbb{Q}[x]$.

As, the roots of f are $\sqrt{3}$ and $-\sqrt{3}$ which are the generators of the field $\mathbb{Q}(\sqrt{3})$.

5. Galois Group

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 [3].

6. Characterization of Galois Groups

Let G be a Galois group of a polynomial $f \in K[x]$ of degree n.

- *G is a subgroup of symmetric group S_n [3].*

So, galois group of a quartic is a subgroup of S_4.

7. Resolvant Cubic of a Quartic

Let $u_1, u_2, ..., u_4$ be the roots of a quartic $f \in K[x]$ and
$\alpha = u_1 u_2 + u_3 u_4,\ \beta = u_1 u_3 + u_2 u_4,\ \gamma = u_1 u_4 + u_2 u_3.$

The cubic polynomial whose roots are α, β, γ is called the resolvant cubic of f which is a polynomial over K [3].

An Application of the Fundamental Theorem

Let $V = \{(1), (12)(34), (13)(24), (14)(23)\} \in S_4$.

Now under the Galois correspondence the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $G \cap V$ [3] 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 N of S_4 with $|N| \leq 6$ is V,

Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $Aut_K^{K(\alpha,\beta,\gamma)} = G/(G \cap V)$ [3].

8. Theorem

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[3].*

9. Theorem

If p is a prime and f is an irreducible polynomial of degree p over $\mathbb{Q}$ which has precisely two non-real roots, then the Galois group of f is S_p [3].

The polynomial is $f(x) = x^5 - 10x + 5 \in \mathbb{Q}[x]$. Its graph is shown below.

Figure: Plotted by the "GNU-Octave"

From its graph this polynomial has only three real roots. This polynomial is "irreducible over $\mathbb{Q}$ by the Eisenstein's criterion" [3] so by Theorem-12 its Galois group is S_5 which contains $5! = 120$ elements.

The polynomial is $f(x) = x^7 - 2x^5 - 4x^3 + 2x^2 + 4x - 2$ which is "irreducible over $\mathbb{Q}$ by the Eisenstein's criterion" [3]. Its graph is shown below.

Figure: Plotted by the "Geogebra"

The Graph shows this polynomial has exactly five real roots. So exactly two of its roots are complex. Hence by the Theorem-12 its Galois Group is S_7 which contains $7! = 5040$ elements.

Galois Group of Multi-variable Polynomials

The Galois group of a polynomial in single variable can be generalized to the Galois group of a multi-variable polynomial.

If the polynomial is $f(x, y) = x + y \in \mathbb{Q}[x, y]$. The roots of f span all over the complex numbers. Hence its Galois group is a subgroup of $S_{|\mathbb{C}|}$.

Example

The polynomials in $\mathbb{Q}[x, y]$ are:

$$y = x^2 + 1 \quad (1)$$

$$y = x \quad (2)$$

The roots of these simultaneous polynomials are ω, ω^2. Then the splitting field of this system is $\mathbb{Q}(\omega)$. Here the automorphisms of $\mathbb{Q}(\omega)$ are:
$\omega \longmapsto \omega$ and $\omega \longmapsto \omega^2$.
Hence the Galois group of this system is $\{(1), (12)\} = S_2$.

Question:

1. Is every polynomial equation solvable by the method of radicals?
2. In other words; does there exist an explicit "formula" which gives all solutions of a polynomial equation?

If the degree of the polynomial is at most four then the answer is **yes** [3].

10. Radical Extension

An extension field F of a field K is a radical extension 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 $K(u_1, ..., u_{i-1})$ [3].

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 $F \supset E \supset K$ [3].

11. Theorem

If F is a radical extension of K then Aut_K^F is a solvable group [3].

12. Corollary

If the equation $f(x) = 0$ is solvable by radicals, then the Galois group of f is a solvable group [3].

13. Theorem

The symmetric group S_n is not solvable for $n \geq 5$ [3].

Outcomes

The polynomial $f(x) = x^5 - 10x + 5 \in \mathbb{Q}[x]$ has Galois group "S_5, which is not a solvable group" [3].
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 [3].

Illustrations I

Galois theory gives the precise condition under which a polynomial of degree $n \geq 5$ is solvable by radicals or not.

Example

The polynomial is $x^5 - 1 \in \mathbb{Q}[x]$.
The set of roots of this polynomial are the fifth roots of unity which forms a group under addition modulo 5. Hence the Galois group is isomorphic to $\mathbb{Z}_5$ [3]. The group $\mathbb{Z}_5$ is cyclic and "every cyclic group is solvable" [1]. Hence this polynomial is solvable by radicals.

14. Cyclotomic Polynomial

The *nth*-cyclotomic polynomial is the polynomial Φ_n defined as $\Phi_n = \prod (x - \zeta)$, where ζ is a primitive-*nth* of unity [1].

15. Theorem

The Galois group of a nth-cyclotomic polynomial Φ_n of is $\mathbb{Z}_n$ [1].

Example

The polynomial is $f(x) = x^{12} - x^{10} + x^8 - x^6 - x^2 + 1 \in \mathbb{Q}[x]$ which is a 58th-cyclotomic polynomial [1] i.e this polynomial $f(x) = \Phi_{58}$. So its Galois group is $\mathbb{Z}_{58}$, which is abelian and hence is solvable. Therefore this polynomial $f(x)$ is solvable by radicals.

Galois fields are the finite fields. We denote Galois field with q elements by $GF(q)$.

Integer representation

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

16. Example

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

Polynomial representation

If F is a finite field and $f(x) \in F[x]$ is irreducible then $F[x]/(f(x))$ is finite field [1]. This field consists of all polynomials modulo $f(x)$.
If $F = GF(2^3)$ then $f(x) = x^8 + x^7 + ... + x + 1 \in F[x]$ 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 $F[x]/(f(x))$ [7].

In the Example-19, the number 5 has the representation $2^2 + 1$. This gives the polynomial representation $x^2 + 1 = (101)$(coefficient of x^2 is 1 of x is 0 and of constant is 1) Now the binary equivalent of 5 is 101.

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.

The loss of information is inevitable. It cannot be prevented or stopped.

1. Paintings gets deteriorated over time and has to be renovated.
2. The data stored in a CD is lost over time. [5].

So, we need a way of retrieving the loss information or correcting the false information.

- 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.
- So the fundamental of the coding theory in digital 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.

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. These codes that can correct themselves are called Error correcting codes [5].

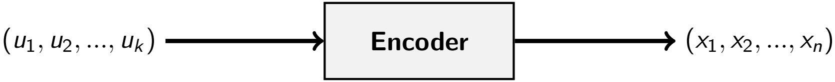
17. Linear Code

Let $K = GF(q)$ be a Galois field. Then a finite extension of K of dimension n is $V = GF(q)^n = GF(q^n)$.
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 [2].

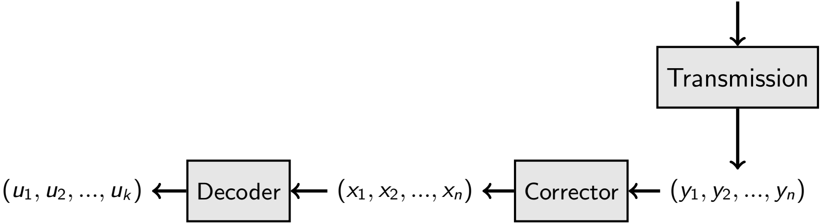
The usefulness of linear code is that they are vector spaces over the base field so they have a basis. All the code words can be generated with this basis. Instead of storing all 2^k number of code words (for k-dimensional binary codes), storing only k basis elements is sufficient which saves massive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

Illustration

To apply (n, k) coding first we need to group our information into blocks of length k. $u_1, \ldots, u_k,\ u_k, \ldots, u_{2k}, \ldots$. This space has dimension k. Now these block of codes are encoded separately each to a code of length n as shown [5].



Mathematically, the encoded vector x is obtained form the original vector u using the generator matrix G by the relation $x = uG$ [5].
To continue and complete the diagram.



18. Syndrome of a code

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. A generator matrix H of the dual code $C^{\perp}$ of the code C called a parity check matrix [2].

Correcting 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 correction of y [2].

This e is also called "error vector" [2].

Suppose we have the parity check matrix is $H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and the code 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 [2].

1. The $(3, 1)$ binary code is used in the short-range wireless communication system like *Bluetooth*^{TM} [6].

2. The Hamming Code $(7, 4)$ is used in memory devices like RAM [5].

3. The Cyclic codes are used in storing data in CDs and DVDs [5].

Application to Cryptography

Cryptography is the science of safe-guarding information by converting the original information into something unreadable. Galois Fields are the life of modern cryptography used in digital communication.

Advance Encryption Standard(AES)

The Advance Encryption Standard is a Computer Security Standard for cryptography which is approved by the "Federal Information Processing Standards Publications" of USA which became effective on May 26, 2002.

In 2000, NIST announced the selection of the "Rijndael" block cipher family which was developed by two Belgian cryptographers, *(Vincent Rijmen and Joan Daemen)* as the winner of the AES competition and since then AES has been the standard for digital cryptography.

The generic algorithm of AES consists of smaller sub-algorithms namely Sub-Bytes, Shift-Rows, Mix-Columns and Add-Round-Key [7].

1. **The State**

   First the data is broken into blocks, each of size 16 byte. Each block is then represented in a 4×4 matrix, whose each entry is a byte of the block. This matrix is called the State.

   Suppose the block is $b_1, b_2, ..., b_{16}$. Then the state is $\begin{bmatrix} b_1 & b_5 & \dots & \dots \\ b_2 & b_6 & \dots & \dots \\ b_3 & b_7 & \dots & \dots \\ b_4 & b_8 & \dots & b_{16} \end{bmatrix}$

   Mathematical operations are not applicable to the data directly so the significance of this step is to make the data applicable for mathematical operations.

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, $x \mapsto Ax + b$ [7].

Mathematical Preliminaries

Each byte in the state i.e each entry in the matrix, is interpreted as one of the 256 elements of a finite field $GF(2^8)$. Then the addition, multiplication operations are performed according to the respective field operations of the field $GF(2^8)$.

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 [7].

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

is the matrix after Shit-Row

Algorithm III

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 [7].

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 [7].

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 representation 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 [7].

Conclusions of my Research

1. Galois Theory is still a relevant field of research today.
2. It has found its development as a linking theory of Field theory and Group Theory.
3. It has found its applications in both pure and applied mathematics; where-ever "Field Theory" has anything to do with.
4. Many concepts of Abstract algebra, Algebraic number theory, Algebraic geometry, etc rely heavily on Galois theory because they are developed on field extensions, and the computer science relies heavily on Galois field.

References

[1] J. P. Escofier. *Galois Theory*. Springer, New York:219-225,2000.

[2] G. R. Holdman. *Error Correcting Codes Over Galois Rings*. Graduate Dissertation, Department of Mathematics, Whitman college, 345 Boyer Ave. Walla Walla, Washington, U.S.A, 2019.

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

[4] A. Lenstra, H. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*,261,12,1982.

[5] A. Neubaer and J. Freudenberger and V. Kuhn. *Coding Theory, Algorithms, Architectures, and Applications*. John Wiley and Sons Ltd, Chichester, West Sussex, England:1-93,2007.

[6] D. Sarma. Implementation of Galois Field for Application in Wireless Communication Channels. *MATEC Web of Conferences*,2010:03012,2018.

[7] National Institute of Standards and Technology. Advanced Encryption Standard (AES). *(Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS*. 197-upd1, 2001. updated May 9, 2023. doi:10.6028/NIST.FIPS.197-upd1.

Acknowledgments

First of all I would like to thank my **supervisor** Assoc. Prof. Tulasi Prasad Nepal. Then I am thankful to former HOD of the department Prof. Dr. Tanka Nath Dhamala for his support and time.

I am grateful to Kathmandu Center for Research and Education Chinese Academy of Sciences-TU for awarding me with KCRE Excellent Student Thesis Grant 2023(Grant number: 08092023).

I would like thank Mr. Santosh Gnawali for providing me the necessary articles and to Mr. Dipak Babu Amgain for assisting me with the bibliography and to Dr. Bishnu Hari Subedi for helping me to write an article. Finally I am thankful to the HoD of the CDM Prof. Dr. Chet Raj Bhatta for organizing this defence in time.

Thank You

Sandesh Thakuri