Journal of Nepal Mathematical Society (JNMS)
ISSN: 2616-0153 (Print), 2616-0161 (Online)
Vol. 7, Issue 2, 2024 (Dec.): 90-99
DOI: https://doi.org/10.3126/jnms.v7i2.73108

Research Article
Received Date: June 13, 2024
Accepted Date: Dec. 20, 2024
Published Date: Dec. 29, 2024

Applications of Galois Theory

Sandesh Thakuri[1], Bishnu Hari Subedi[2,*]

[1,2]Central Department of Mathematics, Tribhuvan University, Kirtipur, Kathmandu, Nepal

*Correspondence to: Bishnu Hari Subedi, Email: subedi.abs@gmail.com

Abstract: *This paper gives an insight to the Galois theory and discusses its applications in both pure and applied mathematics. First, the Fundamental theorem of Galois theory is applied to compute the Galois groups of polynomials and to prove the non-existence of a formula for solving a polynomial equation in rational coefficients having degree $n \geq 5$. Then the Galois fields which are finite fields are applied to the error-correcting codes and cryptography in computer science. There are no general rules to compute the Galois groups of polynomials of degree more than four. Two new examples of Galois groups of polynomials of degree greater than four are introduced and the concept of Galois group of a single variable polynomial is extended to the Galois group of a multi-variable polynomial.*

Keywords: Fundamental theorem, Galois group, Galois field, Error-correcting codes, Cryptography

1 Introduction

The foundation of Galois theory was laid by the French mathematician *Évariste Galois* (1811-1832) by determining the necessary and sufficient condition for solving a polynomial equation by radicals [1]. Galois theory has evolved a lot from then and has found its applications in wide range of fields from pure mathematics especially in abstract algebra, algebraic number theory to algebraic geometry, and to applied mathematics. This paper is limited to its applications in abstract algebra and in computer science.

Modern Galois theory is a theory of field extension which is a vast theory. The core-part of the Galois theory is the *Fundamental theorem of Galois theory* [3]. The Fundamental theorem links a Galois extension to its Galois group. Let F be an extension field of a field K. The group of all automorphisms of F that fixes K is called the *Galois group* of F over K, and it is denoted by Aut_K^F [3]. The extension field F of K is said to be a Galois extension of K or Galois over K if the fixed field of the Galois group Aut_k^F is K itself [3].

Theorem 1.1 (**The Fundamental Theorem** [3])**.** *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:*

1. *the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups. In particular Aut_K^F has order $[F : K]$;*
2. *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.*

A field E such that $K \subset E \subset F$ is said to be an intermediate field of F over K [3]. The index of a subgroup H of a group G is the order of G over H [3].

The Fundamental theorem links field theory to group theory. This allows us to use the tools of group theory to solve the problems of field theory. Solving a polynomial equation is a problem of field theory. We can use the insights of group theory to solve this problem of field theory which is discussed in some detail in the coming section. Also, the Fundamental theorem gives some insights of the structure of a field extension. The structure of a field as an extension field over some field is mirrored in the structure of its Galois group which is a group of automorphisms but these automorphisms are the symmetries of the field. *So, the structure of field extension is equals to its own symmetry.* And, the structure of a field is a complicated thing; specially if it is infinite. But the structure of a group is rather a simple thing; especially

if it is finite. So the Galois theory has fairly simplified the complicated thing in a very insightful and beautiful way. So, Galois theory gives a new sights of study of fields which is study of fields via study of its automorphisms.

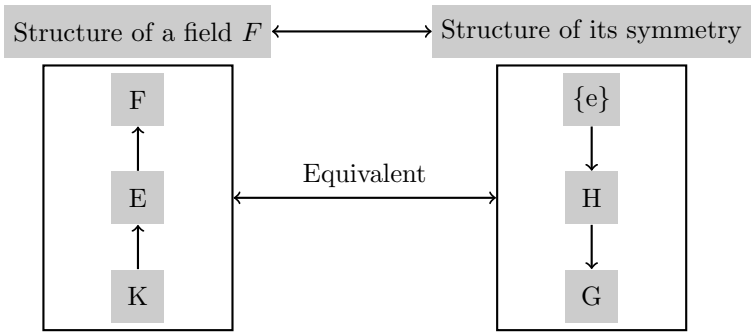


Figure 1: Equivalency

The Fundamental theorem also gives a beautiful insights to the nature of a number which depends upon the underlying field. $\sigma : \{a+b\sqrt{2}\} \mapsto \{a-b\sqrt{2}\}$ where $a, b \in \mathbb{Q}$ is a field-automorphism of $\mathbb{Q}(\sqrt{2})$ that fixes $\mathbb{Q}$. This map σ is also denoted by $\sqrt{2} \longmapsto -\sqrt{2}$. So, any polynomial equation over $\mathbb{Q}$ satisfied by the number $\sqrt{2}$ is also satisfied by the number $-\sqrt{2}$. We 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 the field $\mathbb{Q}(\sqrt{2})$ i.e does not fix itself. The only automorphism of $\mathbb{Q}(\sqrt{2})$ is the identity map. So, we 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 $\mathbb{Q}(\sqrt{2})$.

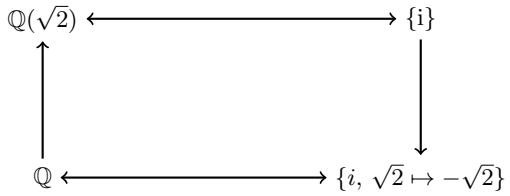


Figure 2: Field containing $\sqrt{2}$

After the Fundamental theorem, next concept in Galois theory we are applying is the *Galois field*. The Galois field GF(q) is a field containing q number of elements. Since a Galois field contains a finite number of elements, and it can be represented using finite number of integers [1] and Galois fields are the finite extension of prime fields.

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

where p is a prime. This representation of a Galois field is called the integer representation. Then

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

Here, the digits $2, 3, .., 7$ of the field $GF(2^3)$ do not lie in 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 as shown in Table 1.
For a field F and an irreducible polynomial $f(x) \in F[x]$ the quotient ring $F[x]/(f(x))$ is a field [1]. If F is a finite field and $f(x) \in F[x]$ is irreducible then $F[x]/(f(x))$ is a 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 $F[x]/(f(x))$ [7]. In the field $GF(2^3)$, the number 5 has the representation $2^2 + 1$. This gives the

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

Table 1: This is actually binary representation of the finite field over GF(2).

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.

2 Application to the Galois Groups of Polynomials

The fundamental theorem finds its application directly in determining and computing the Galois group of a polynomial. The Galois group of a polynomial gives insights about the nature of roots of the polynomial and tells us whether the polynomial equation can be solved by radicals or not. The Galois group G of a polynomial $f\in K[x]$ is the group Aut_K^F, where F is a splitting field of f over K [3]. 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 [3].

First, we know the nature of the Galois group G using the fundamental theorem. The group of automorphism of F is given by the permutations of roots of f. Hence G is a subgroup of the symmetric group S_n [3]. Since the F is a splitting field of irreducible f over K this field F **is a Galois extension** of the field K if all the roots $u_1,...,u_n$ of f are simple roots (i.e if f is separable over K) so $F=K(u_1,...,u_n)$. Now for $u_i\neq u_j$ there exists an field-homomorphism $\sigma: K(u_i)\mapsto K(u_j)$ which extends to field-automorphism of F that fixes K. Thus for each $u_i\neq u_j$ there exists $\sigma\in G$ such that $\sigma(u_i)=u_j$ and hence the G is a transitive subgroup of S_n.

Theorem 2.1 ([3]). *Let G be a Galois group of a polynomial $f\in K[x]$. G is isomorphic to a subgroup of some symmetric group S_n. If f is separable of degree n, then n divides $|G|$ and G isomorphic to a transitive subgroup of S_n.*

If f is irreducible over the field of rationals $\mathbb{Q}$, then f is separable [3]. So first, we discuss the Galois group of irreducible polynomials. The only non-trivial transitive subgroup of S_2 is S_2 itself. and hence the Galois groups of an irreducible quadratic polynomial is S_2. The non-trivial transitive subgroups of S_3 are A_3 and S_3 itself. Hence the Galois group of a irreducible cubic is A_3 or S_3. The technique to compute the Galois group of an irreducible quartic is to first determine its resolvant cubic. The cubic polynomial whose roots are α, β, γ where, $\alpha=u_1u_2+u_3u_4$, $\beta=u_1u_3+u_2u_4$, $\gamma=u_1u_4+u_2u_3$ and u_1,u_2,u_3,u_4 are the roots of f, is called the resolvant cubic of f [3]. The resolvant cubic is actually a polynomial over K [3]. If $V=\{(1),(12)(34),(13)(24),(14)(23)\}$, then under the Galois correspondence the subfield $K(\alpha,\beta,\gamma)$ corresponds to the normal subgroup $V\cap G$ [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].

Here $G\subseteq S_4$ so if $[K(\alpha,\beta,\gamma):K=6]$, then from the statement-(i) of the fundamental theorem we have $|G/(G\cap V|=[K(\alpha,\beta,\gamma):K]=6$, this gives the Galois group G of f is S_4 itself as $|V|=4$ and $|G/(G\cap V|=6$ is possible only if $|G|=24$. Similarly $[K(\alpha,\beta,\gamma):K]=3$ the $G=A_4$ and so on.
The determination and computation of Galois groups of polynomials of degree $n\geq 5$ is not as easy and straight forward as above because there are no general rules to compute it [3]. However we have the following theorem and using this theorem we have computed the Galois groups of two polynomials one of degree 5 and another of degree 7.

Theorem 2.2 ([3]). *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.*

The polynomial is $f(x)=x^5-10x+5\in\mathbb{Q}[x]$ (quintic). Its graph is shown above. From its graph this polynomial has only three real roots. This polynomial is irreducible over $\mathbb{Q}$ by the Eisenstein's criterion

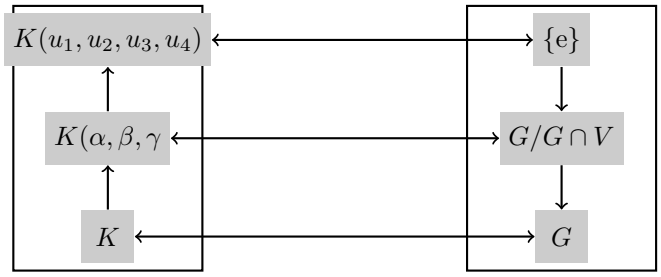


Figure 3: Galois correspondence of the quartic

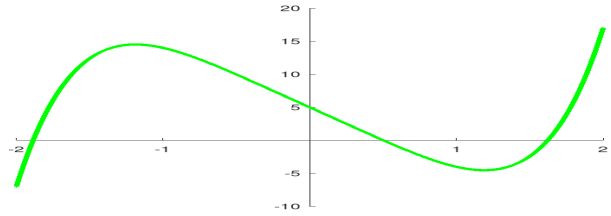


Figure 4: Plotted by the "GNU-Octave", graph of $f(x) = x^5 - 10x + 5$

[3], so by Theorem-2.2, its Galois group is S_5 which contains $5! = 120$ elements.

Likewise, 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 5: The graph of $f(x) = x^7 - 2x^5 - 4x^3 + 2x^2 + 4x - 2$

The graph shows this polynomial has exactly five real roots. So exactly two of its roots are complex. Hence by the Theorem-2.2 its Galois group is S_7 which contains $7! = 5040$ elements.

The Galois group of a **reducible polynomial** is computed by factoring it into irreducibles. For an reducible polynomial $f \in K[x]$, we factor f into irreducibles 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 $\prod G_i$ [4].

Example 2.3. Let $f(x) = x^4 - 7x^2 + 15 = f(x) = (x^2 - 3)(x^2 - 5)$, it is reducible over $\mathbb{Q}$. Let $f_1(x) = (x^2 - 3)$ and $f_2(x) = (x^2 - 5)$. Then f_1, f_2 are both irreducible over $\mathbb{Q}$. The splitting field for f_1 is $\mathbb{Q}(\sqrt{3})$ so its Galois group is $\mathbb{Z}_2$ [3]. The splitting field for f_2 is $\mathbb{Q}(\sqrt{5})$ so its Galois group is also $\mathbb{Z}_2$. Now we have the Galois group of f is a subgroup of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Since the intersection of $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ is trivial the Galois group of f is G itself.

Example 2.4. The polynomial $f(x) = x^7 - 5x^5 - 10x^3 + 5x^2 + 50x - 25 \in \mathbb{Q}[x]$ factors into irreducibles over $\mathbb{Q}$ as $(x^2 - 5)(x^5 - 10x + 5)$. The Galois group of $x^2 - 5$ is $\mathbb{Z}_2$ [4] and of $x^5 - 10x + 5$ is S_5 from above. Also the roots of $x^2 - 5$ are $\sqrt{5}$ and $-\sqrt{5}$ which are not the roots of $x^5 - 10x + 5$ from the its graph, Figure-2. So the intersection of the splitting fields of these two factor polynomials of f is trivial. Hence the Galois group of f is $\mathbb{Z}_2 \times S_5$.

Next we generalize the Galois group of a polynomial in single variable to the **Galois group of a multi-variable polynomial**. The polynomial is $f(x, y) = x + y \in \mathbb{Q}[x, y]$. Now the roots of f over all the complex numbers. Hence its Galois group is $S_{|\mathbb{C}|}$.

Example 2.5. The polynomials in $\mathbb{Q}[x, y]$ are:

$$y = x^2 + 1 \tag{1}$$
$$y = x \tag{2}$$

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 $S_2 \cong \mathbb{Z}_2$.

2.1 Application to the classic problem

The question: *is every polynomial equation solvable by the method of radicals?* is considered the classic problem. To answer the question first we need to **formulate** the classic problem into a problem of field theory. The formula by the method of radicals means the formula involving only field operations and the extraction of *nth* roots [3]. The existence of a formula means there is a finite sequence of steps, each step being a field operation or the extraction of an *nth* roots, which yields all solutions of the given polynomial. Performing a field operation leaves the base field unchanged, but the extraction of an *nth* 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

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

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} [3]. An extension field $F = K(u_1, ..., u_n)$ of K such that some power of u_1 lies in K and for each $i \geq 2$ some power of u_i lies in $K(u_1, ..., u_{i-1})$ is called a **radical extension** of K [3]. Thus the polynomial equation $f(x) = 0$ in rationals is *solvable by radicals* if there exists a radical extension F of K and splitting field E of f over K such that $F \supset E \supset K$. 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 [3]. Now that we made a formulation our problem we make a use of the following theorems to deduce the result. A group G is *solvable* if it has a solvable series and a finite chain of subgroups $G = G_0 > G_1 > ... > G_n = e$ such that G_{i+1} is normal in G_i for $0 \leq i < n$ and each factor group G_i/G_{i+1} is abelian is called a *solvable series.*

Theorem 2.6 ([3])**.** *The following facts are holds by fundamental theorem of Galois group.*

1. *If F is a radical extension of K and E is an intermediate field, then Aut_K^E is a solvable group*
2. *If the polynomial equation $f(x) = 0$ in rationals is solvable by radicals, then the Galois group of f is a solvable group.*
3. *The symmetric group S_n is not solvable for $n \geq 5$.*

The polynomial $f(x) = x^5 - 10x + 5 \in \mathbb{Q}[x]$ has Galois group S_5, which is not a solvable [3]. The quintic polynomial equations over $\mathbb{Q}$ are not solvable by radicals. That is there does not exist an explicit formula for solving the quintics. Moreover, polynomial equations of degree $n \geq 5$ are not solvable by radicals [3]. Galois theory gives the precise condition under which a polynomial of degree $n \geq 5$ is solvable by radicals or not.

Example 2.7. The roots of polynomial is $x^5 - 1 \in \mathbb{Q}[x]$ are 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 can be solved by radicals.

3 Application to the Coding Theory

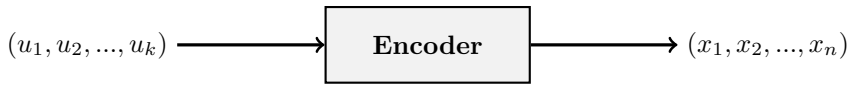
The Galois fields are applied in coding theory of computer science. To be able to detect and correct errors during transmission of information in digital system, coding theory is developed. In digital system, information are transmitted as strings of 0 and 1. So the fundamental of the coding theory is 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 finite field is a Galois field. The widely used field for coding in electronically transmitting device is an extension 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" [2]. 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 are called error-correcting codes [5]. One of such error-correcting code is a linear code which is a linear space.

Definition 3.1. [2] [**Linear code**] Let $K = GF(q)$ be a Galois field. Then a finite extension of K of dimension n is $V = GF(q)^n$. 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.

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. For the code C the generator matrix is defined as follows:

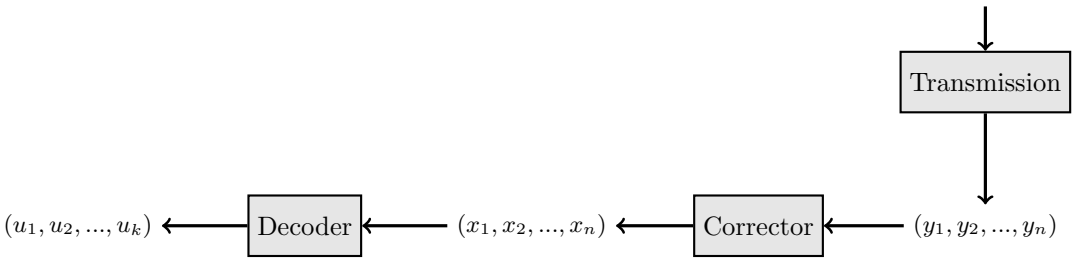
Definition 3.2. [2] [**Generator Matrix**] Let $\{v_1, v_2, ..., v_k\}$ be a basis of C. A generator matrix is the $k \times n$ matrix $G = \begin{pmatrix} v_1 \\ v_2 \\ ... \\ v_k \end{pmatrix}$.

The dual code of C is the set $C^{\perp} = \{x \in V \mid x.y = 0 \ \ \forall y \in V\}$ [2]. 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**. To apply (n, k) coding first we need to group our information into the 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 [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.



We have a way of correcting the received information if it is distorted. This way of correcting is called **Syndrome correcting** because it makes use of the syndrome of the received vector which is defined as follows:

Definition 3.3. [2] [**Syndrome**] 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. Two vectors in V have the same syndrome if and only if they are in the same co-set of C [2]. Then we have the following correcting process. Suppose the signal received is the vector y.

1. 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].

Example 3.4. 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
$C = \{(0,0,0,0), (1,0,1,0), (0,1,1,1), (1,0,1,1)\} \subset GF(2^4)$.

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].

There is a more sophisticated error-correcting code than the linear codes called the **cyclic code**. Linear codes are simple to implement but the correcting algorithm of linear codes are not efficient as it makes use of matrix which is the generating matrix. The code C as defined in 3.1 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 $\{(a_0, a_1, ..., a_{n-1}), (a_1, ..., a_{n-1}, a_0), ..., (a_{n-1}, a_0, ..., a_{n-2})\} \longmapsto a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1}$. This map Φ is a homomorphism. This shows that the cyclic code C can be embedded into the ring $R_n = F[x]/(x^n - 1)$ [2]. For this reason cyclic codes are represented using polynomial representation. We have the following theorem that characterizes the cyclic code.

Theorem 3.5 ([2])**.** *A subset S of R_n corresponds to a cyclic code if and only if S is an ideal of R_n and if $S = (g(x))$ if and only if $g(x)$ divides $x^n - 1$.*

This theorem determines all cyclic codes of a Galois field $GF(p^n)$. They are ideals of R_n and these ideals are generated by the polynomials that divides $x^n - 1$. Thus cyclic codes have a generator polynomial which is computationally simpler than having a generator matrix. Due to this some cyclic codes have efficient correcting algorithms.

Example 3.6. 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 $F[x]/(g(x)) = \{(0), (1 + x), (1 + x^2), (x + x^2)\}$ using the binary notation from the polynomial notation we have the corresponding cyclic code is $\{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ [2].

4 Application to the Cryptography

Cryptography is the science of safe-guarding information by converting the original message into something different. Galois fields are the life of modern cryptography used in digital communication. Advance Encryption Standard (AES) is one of the widely used cryptography standard developed by two Belgian cryptographers Vincent Rijmen and Joan Daemen [7]. The AES 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. "The AES algorithm is a *symmetric block cipher* that can encrypt and decrypt digital information" [7]. Symmetric key cryptography is used to share information between two parties where the two parties share a secret "key" and a public encryption algorithm [6]. The generic algorithm of AES consists of smaller sub-algorithms namely "Sub-Bytes, Shift-Rows, Mix-Columns and Add-Round-Key" [7].

The State

First the data is broken into *blocks* and each block is broken into smaller *chunks* of a size byte (16 bytes for a block of size 128 bits). This block is then represented in a which consisting of bytes of the word. This matrix is called the *state*. 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 [7].

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 $GF(2^8)$.

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].

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

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].

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].

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 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].

5 Conclusion

The Galois theory that begun in the 19th century due to the french mathematician *Évariste Galois* is still a relevant field of research today. Over the 200 years this theory has found its development as a linking theory of the two main theories: Group theory and field theory. It has found its applications in both pure and applied mathematics; where-ever "Field Theory" has anything to do with. 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.

Acknowledgments

The first author would like to thank *Kathmandu Center for Research and Education, Chinese Academy of Sciences-TU* for awarding him with *KCRE Excellent Student Thesis Grant 2023(Grant number: 08092023)*.

References

[1] Escofier, J. P., 2000, *Galois Theory*, Springer, New York.

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

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

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

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

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

[7] National Institute of Standards and Technology, 2001, Advanced Encryption Standard (AES), *(Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS*. 197-upd.1 updated May 9, 2023. DOI: 10.6028/NIST.FIPS.197-upd1