Galois Fields and some of its Applications

Kwasi Baah Gyamfi[1], **Emmanuel Akweittey**[2], **Matilda Adusei Sarpong**[3]

[1]Mathematics Department, Kwame Nkrumah University of Science and Technology, Ghana
[2]Mathematics Department, Presbyterian University College, Ghana
[3]Mathematics Department, SDA College of Education, Ghana

DOI: 10.29322/IJSRP.10.05.2020.p10139
http://dx.doi.org/10.29322/IJSRP.10.05.2020.p10139

Abstract- Galois theory is about the connection between groups, fields and their extensions. It is the interplay between polynomials, fields, and groups. Galois field is about fields and their extensions. It has got many useful applications in computing and some other areas of abstract algebra and it has also been used to produce many useful theorems.

Keywords: Galois Fields, Cyclotomic, Primitive, Polynomials, Applications

1 Introduction

The existence of an explicit formula for finding the roots of an arbitrary polynomial has been one of great historical importance [1]. The roots of the linear case can be trivially found and by the use of 'completing the square', a formula could be found for finding the roots of a quadratic equation which is known as the quadratic formula. In the sixteenth century, based on work of Cardan, Taraglia, and Dal Ferro the solution to the cubic was founded. A mathematician named Ferrari brought together ideas from the used algorithms to find the roots of both the quadratic and cubic. Mathematicians endeavored for close to 300 years to find a solution of the quintic, but all attempts were to no avail. Ruffini and Abel found a solution of the quintic using ideas that Evariste Galois introduced in the early nineteenth century. In the area of basic abstract algebra, Galois theory is regarded as an area with an elegant interaction of topics. In mathematics, more specifically in abstract algebra, Galois theory, named after Evariste Galois, provides a connection between field theory and group theory. One of the greatest tragedies in the scientific world was the loss of Evariste Galois. The life of Evariste Galois, riddled with rejection and misunderstanding, brought about one of the most important mathematical works of the nineteenth century. His theory of field extensions had evolutionary implications, which still greatly influence the study of mathematics today. Galois at the age of 20 years had already produced work that would make him famous. He died in a very tragic circumstance at the age of 20. Unluckily, his lifetime met many setbacks and he was even seen to be a troublemaker by the government and also unaccepted by the mathematical establishment. In 1846, Joseph Liouville published some of Galois' work in his Journal de mathematiques. The significance of Galois results were realized since then and has been a stepping stone for many developments in algebra. An aspect of this theory which is the Galois field and some of its applications are the subject of this thesis work.

2 Preliminaries

This section discusses the general concept of group, rings and fields looking at some definitions, theorems, lemmas, and examples that will aid us better under- stand the concept of Galois field.

Definition 2.1 An automorphism of a field E is a one-to-one mapping $\theta : E \to E$, which preserves addition and multiplication, thus $\theta(\alpha+\beta) = \theta\alpha+\theta\beta$ and $\theta(\alpha\beta) = (\theta\alpha)(\theta\beta)$. Let μ and ϕ be automorphisms of the field E, then their composition $\mu\phi$ is also an automorphism. The inverse of an automorphism is also an automorphism. If μ is an automorphism of a field E onto some field, then an element α of E is left fixed by μ if $\mu(a) = a$. A collection S of isomorphisms of E leaves a subfield F of E fixed if each $\alpha \in F$ is left fixed by every $\alpha \in S$. If α_i leaves F fixed then μ leaves F fixed [2].

Example 2.1 Let $Q(\sqrt{2}, \sqrt{3})$ and $\delta : E \to E$ which is defined by $\delta(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = \delta(a) + \delta(b\sqrt{2}) + \delta(c\sqrt{3}) + \delta(d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$. For every $a, b, c, d \in Q$, is an automorphism of E and it is the conjugation isomorphism $\phi\sqrt{3}, \sqrt{3}$ of E onto itself, thus if E is viewed as $(Q[\sqrt{2}]\sqrt{3})$, then δ leaves $Q(\sqrt{2})$ fixed.

Theorem 2.1 Let $\alpha_i \mid i \in I$ be a collection of automorphism of a field E. The set $E\alpha_i$ of all $\alpha \in E$ left fixed by every α_i for $i \in I$ forms a subfield of E [3].

Proof: If $\alpha_i(a) = a$ and $\alpha_i = b \forall i \in I$, then $\alpha_i(a \pm b) = \alpha_i(a) \pm \alpha_i(b) = a \pm b$ and $\alpha_i(a)\alpha_i b = ab$. Provided $b \neg 0$ for all $i \in I$ then $\alpha_i(a \mid b) = \alpha_i(a) \mid \alpha_i(b) = a \mid b$. Again for all $i \in I$, α_i are automorphisms, hence $\alpha_i(0) = 0$ and $\alpha_i(1) = 1 \forall i \in I$. Therefore $0, 1 \in E\alpha_i$. Hence $E\alpha_i$ is a subfield of E. The field $E\alpha_i$ of the above theorem is the field of $\alpha_i \mid i \in I$. Given a single automorphism α_i, then $E\alpha_i$ can be referred to as the fixed field of α[3].

Definition 2.2 Let F be an extension field of the field E, $Aut(F/E)$ is the automorphism of F which fix $E =$ the set of F automorphisms of $E =$ Galois group of $F/E =$ Gal(F/E). Thus $Gal(F/E) = \varphi : F \to F$ such that $\varphi a = a \forall a \in F$.

Definition 2.3 Let H be a group of automorphisms of the field E, we denote E_H as the set of all $a \in E$ such that a is fixed by every element in H. $E_H = a \in E : \delta(a), \forall a \in H$[4].

Theorem 2.2 Let H be a group of automorphisms of the field E, then E_H is a subfield of E, called the fixed field of E for H. Moreover, if E/F is a field extension, then $E_H(E/F)$ is said to be an intermediate field of E/F[4].

Proof: $0, 1 \in E_H$, hence $E_H \neq 0$. Let $c, d \in E_H$, and $\delta \in H$, then

i. $\delta(c - d) = \delta(c) - \delta(d) = c - d$. Then $c - d \in E_H$

ii. $\delta(cd^{-1}) = \delta(c)\delta(d^{-1}) = cd^{-1}$, $cd^{-1} \in E_H$. Hence E_H can be said to be a subfield of E[4].

Definition 2.4 If K is a finite normal extension of a field F, then $G(K/F)$ is the Galois group of K over F[2].

Definition 2.5 For every prime p and positive integer n, there is exactly one field of order p^n, which is finite. Such a field is known as a finite field. Thus a finite field is a field with a finite order. The field denoted as $GF(p^n)$ is referred to as the Galois field of order p^n. Thus a field with finitely many elements. A finite field with q elements is denoted as F_q[2].

Theorem 2.3 Let E be a finite extension of degree n over a field F. If F has q elements, then E has q^n elements[2].

Proof: Let $w_1, \ldots, w_n$ be a basis for E as a vector space over F. Every $\beta \in E$ can be uniquely written in the form $\beta = b_1 w_1 + b_2 w_2 + \cdots + b_n w_n$ for each $b_i \in F$. Each b_i may be any of the q of F, the total number of such distinct linear combinations of w_i in q^n[2].

Lemma 2.1 Let F be a finite field containing a subfield E with q elements. Then F has q^m elements, where $[F : E] = m$.

Proof: F is a vector space over E, since F is finite, it is also finite-dimensional as a vector space over E. Assume $[F : E] = r$ has a basis over E which consists of r elements $a_1, \ldots, a_r$. Thus every element of F can be uniquely represented in the form $a_1 b_1 + a_2 b_2 + \cdots + a_r b_r$, where $b_1, b_2, \ldots, b_r \in E$. Because each b_i can have q elements, F has exactly q^m elements.

Theorem 2.4 Let F be a finite field, then F has p^n elements, where the prime number p is the characteristic of F and n is the degree of F over its prime subfields.

Lemma 2.2 If F is a finite field with q elements, then every $a \in F$ satisfies $a^q = a$.

Proof: The identity $a^q = a$ is to be trivial for $a = 0$. Conversely, the non zero elements of F form a group of order $q - 1$ under multiplication. Thus $a^{q-1} = 1$, for all $a \in F$ with $a \neq 0$.

Theorem 2.5 For every positive integer n and every prime p, there exist a finite field with pn elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over F_p.

Theorem 2.6 Let F_q be the finite field with $q = p^n$ elements and every subfield of F_q has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there exist exactly one subfield of F_q with p^m elements.

http://dx.doi.org/10.29322/IJSRP.10.05.2020.p10139

Proof: A subfield E of F_q has order p^m for some positive integer $m \leq n$. $q = p^n$ must be a power of p^m and so m is necessarily a divisor of n. Assuming m is a positive divisor of n, $p^m - 1$ divides $p^n - 1$. Hence $xp^{m-1} - 1$ divides $xp^{n-1} - 1$ in $F_p(x)$. Again, $xp^m - x$ divides $xp^n - x$ in $F_p(x)$. Implying that every root of $xp^m - x$ is also a root of $x^q - x$ and hence belong to F_q. Following that as a subfield F_q must contain a splitting field of $x^{p^m} - x$ over F_q. Thus by theorem 3.5, such a splitting field has order p^m. If there were two distinct subfields of order p^m in F_q, then they would jointly contain more than p^m roots of $x^{p^m} - x \in F_q$ which is a contradiction. Therefore the unique subfield of F_q of order p^m, with m as a positive divisor of n, consist exactly of the roots of the polynomial $x^{p^m} - x \in F_p(x)$ in F_{p^m}.

3 Main Result

In this section some of the applications of Galois fields are discussed together with some definitions, theorems, and examples.

3.1 Construction of Cyclotomic Polynomials

In this section we seek to construct a number of cyclotomic polynomials. Thus $\Phi_n(x) \in Q[X]$ for $n \geq 1$.

Definition 3.1 Assume there exist a field E whose characteristic does not divide m, which is a positive integer. We let the set of all primitive mth roots of unity in the splitting field F for $x^m - 1$ over E be $u_1, u_2, \dots, u_n$, then we say that the polynomial $\Phi_m(x) = (x - u_1)(x - u_2)\dots(x - u_n) \in F(x)$ is known as the mth cyclotomic polynomial over E. Thus $\Phi_m(x) = (x - u_i)$, where the u_i are the primitive mth roots of unity in E and Φ_m is the mth cyclotomic polynomial over E.

Theorem 3.1 Let $m \geq 2$ be a prime. Then the mth cyclotomic polynomial denoted as $\Phi_m[x]$ is given by $\phi_m[x] = \frac{x^p-1}{x-1} = C_1x^{p-1} + C_2x^{p-2} + \cdots + C_{n-1}x + C_n$, where $C_1, C_2, \dots, C_{n-1}, C_n$ are all unity.

Example 3.1

i. *Consider the polynomial* $f(x) = x - 1$, $x - 1$, *then* $x = 1$. *Therefore* $\Phi(x) = x - 1$.

ii. *lets consider* $n = 2$, *thus* $f(x) = x^2 - 1$
$C_k = e^{\frac{2\pi ik}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$
$C_k = e^{\frac{2\pi ik}{2}} = \cos\frac{2\pi k}{2} + i\sin\frac{2\pi k}{2}$.
When $k = 0, C_0 = e^{\pi k} = \cos\pi k + i\sin\pi k = 1$
$k = 1, C_1 = e^{\pi} = \cos\pi + i\sin\pi = -1$
$C_1 = \omega = -1$
$\Phi_2(x) = (x - (-1)) = x + 1$

3.2 Primitive Element Theory

Definition 3.2 let F_q be a finite field and F_q^* be the multiplicative group of nonzero elements of F_q. If $F_q^n = F_q(\alpha)$ and α is the generator of F_q^n. Then α is said to be the primitive element of the field extension $F_q \subset F_q^n$. In other words the generator of the cyclic group F_{q^*} is known as a primitive element of F_q[5].

Example 3.2

i. *Considering* F_5, *the elements of* F_5^* *are* $\{1, 2, 3, 4\}$. *Let* K *be the elements of* F_5^*. *Because* F_q^* *is cyclic, any nonzero* m *can be written as* $m = n^k$.

Table 1: F_5 Table showing $m = n^k$

k	1	2	3	4
2^k	2	4	3	1
3^k	3	4	2	1
4^k	4	1	4	1

The elements 2 and 3 produce all the elements of F_5^* *and 4 produces only the elements 1,4 hence, it is not a primitive element of* F_5^*.

http://dx.doi.org/10.29322/IJSRP.10.05.2020.p10139

ii. Consider F_7, $F_7^* = \{1, 2, 3, 4, 5, 6\}$. See table 2
It is seen from the table that, the two elements 3 and 5 of F_7^* produces all its elements and are therefore the primitive elements of F_7^*. Again, 2, 4 and 6 are non primitive elements since they do not generate all the elements of F_7^*.

Table 2: F_7 Table showing $m = n^k$

k	1	2	3	4	5	6
2^k	2	4	1	2	4	1
3^k	3	2	6	4	5	1
4^k	4	2	1	4	2	1
5^k	5	4	6	2	3	1
6^k	6	1	6	1	6	1

3.3 Primitive Polynomial

Definition 3.3 A polynomial $g \in F_q[x]$ whose degree $n \geq 1$ is said to be a primitive polynomial over F_q if the polynomial f is the minimal polynomial over F_q with a primitive element of F_q^n [5]. It can be described in order words as a monic polynomial which is irreducible over F_q which also has $\alpha \in F_q^n$ as its roots. This α generates F_q^{*n} which is the multiplicative group of F_q^n [6]. Again, if $f(x) \in Z(x)$, then the polynomial $f(x)$ is said to be a primitive polynomial if the greatest common divisor of the coefficient of $f(x)$ is 1.

Construction of polynomials in $F_q[x]$ might produce polynomials whose degree is greater than or equal to $n-1$. We therefore make use of an irreducible polynomials $\pi(x)$ with degree n in $F_p[x]$ which is such that $F_p[x \bmod \pi(x)]$ results in a polynomial as a remainder which is of degree less than or equal to $n-1$. Throughout this study, we will consider our choice of $\pi(x)$ to be zero for the convenience of our calculations.

Example 3.3

i. Let $q = 4 = 2^2 = p^m$
F_{p^m} = *polynomials of degree less than or equal to* $1 : \alpha_i \in F_p$, *where* $p = 2$ *and* $m = 2$.
We let the possible elements of $F_4 = 0, 1, \alpha, \alpha^2$
We take an irreducible polynomial, $\pi(x) = x^2 + x + 1$.
For $\phi(x) = 0, x^2 + x + 1 = 0$ *which implies that* $x^2 = x + 1$
$\alpha = x$
$\alpha^2 = x^2 = x + 1$
$\alpha^3 = 1$
$\alpha^4 = 0$
Therefore $F_4 = 0, 1, x, x + 1, = 0, 1, \alpha, \alpha^2$. *The roots of the polynomial are* $0, 1, x, x + 1$. *Thus the primitive polynomial* $x^2 + x + 1$ *generates the elements of* F_4 *which are* $0, 1, x, x + 1$.

ii. Again let's consider when $q = 8 = 2^3 = p^m$, *thus* $p = 2$ *and* $m = 3$.
F_{p^m} *equals polynomials whose degree is less than or equal to* $2 : \alpha_i \in F_p$.
We let the possible elements of $F_8 = 0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$, *where* $\alpha^7 = 1$ *and also* $\alpha^8 = 0$.
Using the irreducible primitive polynomial $\pi(x) = x^3 + x + 1$
$\alpha(x) = 0$ *implies,* $x^3 = x + 1$
$\alpha = x, \alpha^2 = x^2, \alpha^3 = x^3 = x + 1$
$\alpha^4 = x.x^3 = x(x + 1) = x^2 + x$
$\alpha^5 = \alpha.\alpha^4 = x.(x^2 + x) = (x + 1) + x^2 = x^2 + x + 1$
$\alpha^6 = \alpha.\alpha^5 = x.(x^2 + x + 1) = x^3 + x^2 + x = (x + 1) + x^2 + x = x + x + 1 + x^2 = 2x + 1 + x^2 = x^2 + 1$
Therefore $F_8 = 0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1$

it is seen from each of the cases considered that the elements of $F_{p^m}[x]$ are generated by an irreducible primitive polynomials of degree m in F_{p^m}.

Lemma 3.1 *If $f(x), g(x) \in Z[x]$ are primitive polynomials, then their product $f(x)g(x)$ is also primitive*

Example 3.4

i. $f(x) = x^2 + 2x + 4$ *and* $g(x) = x^3 + 3x^2 + 5x + 7$
$f(x)g(x) = (x^2 + 2x + 4)(x^3 + 3x^2 + 5x + 7) = x^5 + 5x^4 + 15x^3 + 29x^2 + 34x + 28$
Thus the gcd of $f(x)g(x)$ is 1 and hence the product $f(x)g(x)$ is primitive.

ii. $h(x) = x^3 + x^2 + 1$, $f(x) = x^3 + x + 1$
$h(x)f(x) = (x^3 + x^2 + 1)(x^3 + x + 1) = x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1$
The gcd of the product $h(x)f(x)$ is , therefore the polynomial, $h(x)f(x)$ is also primitive.

http://dx.doi.org/10.29322/IJSRP.10.05.2020.p10139

3.4 Primitive Root Theorem

Definition 3.4 Let n be a prime integer. Then for $1 \leq p \leq n, p^{n-1} = 1 \bmod n$ and if $\forall i, 1 \leq i \leq n-1$ and $m^i = 1 \bmod n$. Then p is said to be a primitive root of n[6].

To show whether p is a primitive root of n, we go through the following;

i. find the primitive factors of $n-1$

ii. for every prime factor q, check if $p^{\frac{n-1}{q}} \neq 1 \bmod n$

iii. once the above test is satisfied for all prime factors of $n-1$, then p is a primitive root of n and if $p^{\frac{n-1}{q}} = 1 \bmod n$, then it is not a primitive root of n.

iv. the test is repeated for all possible values of $p : 2, 3, 4, \ldots, n-1$.

Example 3.5

i. Consider $n = 3$, $n - 1 = 3 - 1 = 2$. *We now check if* $p^{\frac{n-1}{q}} \neq 1$ *mod* n. *The only prime factor of 2 is 2 itself implying that* $q = 2$ *and* $p = 2$
$2^{\frac{2}{2}} = 2$. *Hence 2 mod* $3 \neq 1$ *mod 3. Thus 2 is a primitive root of 3.*

ii. Consider $n = 7, n - 1 = 6$
The prime factors of 6 are 2, 3. That is $q = 2, 3$ *and* $p : 2, 3, 4, 5, 6$. *For each of the values of* p *and* q *we check if* $p^{\frac{n-1}{q}} \neq 1$ *mod* n.
Consider $p = 2$, *when* $q = 2$
$2^{\frac{6}{2}} = 8$. *8 = 1 mod 7.*

4 Conclusion

We have been discussing Galois fields or finite fields as well some of its applications in abstract algebra which comprises of the construction of Cyclotomic polynomials where we found out that where p is prime, $\Phi_p(x) = C_1x^{p-1} + C_2x^{p-2} + \cdots + C_{n-1}x + C_n$, where $C_1, C_2, \ldots, C_{n-1}, C_n$ are all unity and when p is not prime, that is composite, the degree of the cyclotomic polynomial $\Phi_n(x)$ is equal to the number of primitive roots of unity it contains. We also discussed the Primitive element theory and got to the conclusion that every finite field F_q, can have more than one primitive element. Finally, the Primitive Root Theorem was studied in this research alongside with some definitions and examples.

5 Recommendation

The study revealed that Galois fields are not an area without applications as some perceived. These applications are not only in abstract algebra but there are other applications including computer cryptography and coding theory in computing. We, therefore recommend that future researchers look at how the field of Galois is applied in computing and other related areas.

References

[1] M.C. Barnes. Galois theory and insolvability of the quintic. Master's thesis, Texas Technical University, 1998.

[2] John B Fraleigh. *A first course in abstract algebra.* Pearson Education India, 2003.

[3] Allan Clark. *Elements of abstract algebra.* Courier Corporation, 1984.

[4] A Eid. Galois theory and application. Master's thesis, University of Bahraian, 2006.

[5] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications.* Cambridge university press, 1994.

[6] R Cantor and M Wilson. Constructive galois theory, 2000.

http://dx.doi.org/10.29322/IJSRP.10.05.2020.p10139

Authors

First Author - Kwasi Baah Gyamfi, Phd Pure Mathematics, Kwame Nkrumah University of Science and Technology, Ghana.
kwasibaahgyamfi1@gmail.com
Second Author - Emmanuel Akweittey, MSc Pure Mathematics, Presbyterian University College, Ghana.
emmanuel.akweittey@presbyuniversity.edu.gh
Third Author - Matilda Adusei Sarpong, MPhil Pure Mathematics, SDA College of Education, Ghana.
masarp1910@gmail.com

Corresponding Author - Emmanuel Akweittey, emmanuel.akweittey@presbyuniversity.edu.gh

http://dx.doi.org/10.29322/IJSRP.10.05.2020.p10139