Extension fields and Galois Theory

B.Nithya [#1], Dr.V. Ramadoss [*2]

[#1]*M.Phil (Scholar)& Mathematics & PRIST University*
Vallam, Thanjavur, Tamilnadu, India.
[*2]*M.Sc.,M.Phil.,Phd., Asst.Prof & M.Phil (Mathematics) & PRIST University*
Vallam, Thanjavur, Tamilnadu, India.

Abstract— *Galois Theory, a wonderful part of mathematics with historical roots date back to the solution of cubic and quantic equations in the sixteenth century. However, besides understanding the roots of polynomials, Galois Theory also gave birth too many of the central concepts of modern algebra, including groups and fields. In particular, this theory is further great due to primarily for two factors: first, its surprising link between the group theory and the roots of polynomials and second, the elegance of its presentation. This theory is often described as one of the most beautiful parts of mathematics. Here I have specially worked on field extensions. To understand the basic concept behind fundamental theory, some necessary Theorems, Lammas and Corollaries are added with suitable examples containing Lattice Diagrams and Tables. In principle, I have presented and solved a number of complex algebraic problems with the help of Galois theory which are designed in the context of various rational and complex numbers.*

Keywords — *Galois Theory, group theory, roots of polynomials.*

I. INTRODUCTION

In algebra, fields are one of the important objects of study. Since they provide a useful generalization of many number systems such as a the rational numbers. Fields also appear in many other areas of mathematics. Fields theory considers sets, such as real number , on which all the usual arithmetic hold, those governing addition, multiplication and division. The study of fields through Galois theory is important for the study of polynomial equations and thus has application to number theory. Specifically, a field is a commutative ring in which every non zero element is assumed to have a multiplicative inverse. Algebraic extensions are those in which every element of K is the root of polynomial with co efficient in F, elements of K which are not algebraic are trace dental over fetus C is an algebraic extension of R, and the field of rational function F(x) is one variable is trace dental over F. the most significant topic in field theory proper involves the study of field extensions K/F, in particular Galois theory. Galois theory arises out of the study of polynomials over fields and adjoining roots of polynomials to construct new fields. An algebraic field extension by looking at the action of group of auto orphisms of a given extension. Galois Theory is the interplay between fields and groups.

II. BASIC DEFINITIONS AND EXAMPLES

Definition 1:1

A non empty set G together with an operation $*$ is called a group**.** If the following conditions are satisfied.

Closure axiom:

For all a, b $\in$ G $\Rightarrow$ a*b $\in$ Ga

Associative law

(a*b) *c = a*(b*c) for all a, b, c $\in$ G

Existence of identity:

There exist an element e $\in$ G called identity such that a*e = e*a = a for all a $\in$ G.

Existence of inverse:

For every a $\in$ G, there exist a^{-1} $\in$ G such that $a^{-1}*a = a*a^{-1} = e$ an element a^{-1} is called inverse of ‘a’

Definition 1:2

Let R be a non empty set and a,b,c $\in$ R be arbitrary. The set R with two binary operations addition and multiplication is called a ***ring.***

If the following conditions are satisfied.

(R,+) is an abelian group,

Closure axiom: a,b $\in$ R $\Rightarrow$ a+b $\in$ R

Existence of identity:

There exist 0 $\subset$ R, called additive identity or zero element such that a + 0 = 0+a = a.

Existence of inverse : For all a $\in$ R $\Rightarrow$ -a $\in$ R, called additive inverse of ‘a’ such that -a + a = a + (-a) = 0

Associative law: (a+b) +c = a + (b+c)

Commutative law: $a + b = b+ a$
(R,) is semi group
Closure axiom: $a,b \in R \Rightarrow ab \in R$
Associative law: $(ab)\, c = a(bc)$
Distributive law: ie., $a\,(b+c) = ab + ac$
$(b+c)\, a = ba + ca$

Definition 1:3

A ***field*** is a commutative ring with unit element in which every non zero element has a multiplicative inverse.

Definition 1:4

A subset S of a field (F, +,) is said to be a subfield**.** If S is closed with respect to addition and multiplication in F and is itself a field with two conditions.

1) $a \in S$, $b \in S \Rightarrow a+b \in S$
2) $a \in S$, $b \in S\ (b \neq 0) \Rightarrow ab^{-1} \in S$

Definition 1:5

Let K be an extension field of a field F then K is a vector space over F. The dimension of the vector space K(F) is called ***degree*** of K over F and is denoted by [K:F].

Definition 1:6

Let F be a given field, K is said to be an ***extension*** of ***field*** F if F is a subfield of K. ie, $K \supset F$.

Definition 1:7

If the dimension of the vector space K over F is finite then K is a ***finite field extension*** of the field F.

Definition 1:8

Let (F, +,) be a field. Then a non empty set V together with two binary compositions vector addition and scalar multiplication. ie., external composition is called a ***vector space*** over the field F. If the following conditions are satisfied.

(V, +) is an aphelion group
Any $u \in V$, and $a \in F \Rightarrow au \in V$
This law must satisfy the following conditions:
Multiplication by scalar is distributive over vector addition
$a(u+v) = au + av$ for all $u,v \in V$ and $a,b \in F$
$(ab)\, u = a(bu)\ \forall\ a,b \in F$ and $u \in V$
For the unit element, $1 \in F$
$1\, u = u$ for all $u \in V$.

Definition: 1:9

Let v(F) be a vector space and a vector u express in the form $u = a_1 u_1 + a_2 u_2 + \ldots\ldots.+ a_n u_n$ ie.,) $u = \sum_{i=1}^{n} a_i u_i$ is called a ***linear combination*** of vectors $u_1, u_2, \ldots.u_n$ belonging to V, where $a_i \in F$ for all i.

Definition: 1:10

A set containing the vectors $u_1, u_2, \ldots.u_r$ defined over a field F is said to be ***linearly dependent.*** If there exist scalars $a_1 , a_2 \ldots\ldots.a_r \in R$ (not all zero) such that $a_1 u_1 + a_2 u_2 + \ldots\ldots.+ a_r u_r = 0$.

Definition: 1:11

A set containing the vectors $u_1, u_2, \ldots.u_r$ defined over a field F is said to be ***linearly independent.*** If it is not linearly dependent.

Definition: 1:12

Let F be a field. A one-to-one map $\sigma : F \rightarrow F$ is called auto ***Orphism*** of the field F if

i) $\sigma(x+y) = \sigma(x) + \sigma(y)$
ii) $\sigma(xy) = \sigma(x)\sigma(y)$

Definition: 1:13

A group in which each element can be expressed as power of another element is called ***cyclic group.***

Definition: 1:14

If R is a commutative ring then $a \neq 0 \in R$ is said to be a ***zero divisor.*** if there exists an element $b \in R$, $b \neq 0$ such that $ab = 0$.

Definition: 1:15

A commutative ***ring*** is an integral domain. If it has no zero divisors.

Definition: 1:16

A mapping $\emptyset$:G$\to\bar{G}$ is said to be a ***homomorphism.*** If for all a,b ∊ G then $\emptyset(ab) = \emptyset$(a) $\emptyset$(b).

Example: 1.1

Let $\emptyset$: G $\to\bar{G}$ defined by $\emptyset$(x) = 2x be a homomorphism. Where G be a group of integers under multiplication and $\bar{G}$ = G for integer x ∊ G.

Proof:

$\emptyset$(xy) = 2 (xy)
= 2x. 2y
= $\emptyset$(x) $\emptyset$(y)

Therefore, $\emptyset$ is a homomorphism

Definition: 1:17

An integral domain D is said to be of characteristic **0.** If the relation ma = 0. Where a $\neq$ 0 is in D and where m is an integer can hold only if m = 0.

Definition: 1:18

A homomorphism $\emptyset$: G $\to\bar{G}$ is said to be an ***isomorphism.*** If $\emptyset$ is 1-1.

Example: 1.2

Let $\emptyset$: G $\to\bar{G}$ defined by $\emptyset$ (x) = 2^x is an isomorphism. Where G be a group of all real numbers under addition and $\bar{G}$ be the group of non zero real numbers with ordinary multiplication.

Proof:

Let x ∊ G, y ∊ G

Now $\emptyset$(x) = 2^x
$\emptyset$(y) = 2^y
$\emptyset$(x) = $\emptyset$(y)
$2^x = 2^y$
x = y is one-to-one.

Hence is isomorphism.

III. Galois theory

Definition: 4.1

Let K be extension field of F. so that F is a subfield of K. Then group of Automorphism of K relative to F is called ***Galois group*** of K over F is denoted by G (K,F) ie., an automorphism σ is in G (K,F) if σ(x) = x $\forall$ x ∊ F. G (K,F) is a subgroup of the group of automorphism of K.

Definition: 4.2

A field F with P^n elements is called a ***Galois field*** and is denoted by GF (P^n) P being a prime positive integer.

Theorem: 4.1

The multiplicative group of Galois field is cyclic.

Proof:

Let F be a finite field of characteristic P, where P is a prime number.

Let n be a positive integer and K be the splitting field for the polynomial $x^q - x$ Over F. where q = P^n

K is called Galois field and is denoted by GF (P^n)

K contains Pn = q elements

The elements of K are the roots of the polynomial $x^q - x$ in K.

Let K' denote the set of non-zero elements of K.

$x^q - x = x (x^{q-1} - 1)$

Hence elements of K' are the roots of the polynomial,

x^{q-1} - 1= $xp^{n-1} - 1$
= $x^m - 1$

Where m = p^{n-1}

The elements of K' form a multiplicative group

To prove K' is cyclic.

It is enough to prove that K' has an element of order $p^n - 1 = m$. if 'a' and 'b' are the elements of a finite abelian group such that 0(a) = r and 0(b) = s.

Then there exist an element $C \in G$ such that 0(c) = least common multiple of r and s. since order of elements of K' are finite and hence there exist an Element in K'.

The order is the least common multiple of all the others.

Let this order be m'.

Consider the polynomial $xm'^{\,-1}$

Any $\alpha \in K'$.

$\Rightarrow$ α is a root of $x^{m'} -1$

$\Rightarrow$ α satisfies $x^{m'} -1$

$\Rightarrow$ $x^{m'} -1$ has m' root. Where $m' \leq m$

Since $x^{m'} -1$ cannot have more than m' roots in the field.

Therefore m = m', Hence the multiplicative group of galois field is cyclic, Hence K is cyclic.

Theorem: 4.2

Let K' be a subfield of the Galois group GF (P^n) then there exists an Integer m such that K' contains p^m elements and m/n.

Proof:

Given that K' be a subfield of the galois group GF (P^n)

To prove then there exists an integer $m \ni K'$ contains (p^m) element and m/n. And K' is the subfield of GF (P^n) and characteristic of GF (P^n) is p.

Hence characteristic K' = p.

Consequently K' contains pm elements for some positive integer m.

GF (P^n) can be regarded as a vector space over K'.

Since GF (P^n) is finite.

Hence GF (P^n) is the finite dimensional vector space over K'.

Let $u_1 , u_2, \ldots\ldots\ldots u_s$ as a basis of GF (P^n) then S is a finite integer.

Consider $\alpha \in K'$, $x \in GF\ (P^n)$. then the scalar product αx is the same as $\alpha a \in GF\ (P^n)$ and $(p^m)^s = p^{ms}$ = number of elements in GF (P^n) = P^n , $p^{ms} = P^n$, ms = n, m/n

Hence K' contains p^m elements and m/n.

Theorem: 4.3

Let F be any subfield of K and group of automorphism of K. then Fixed field of G is a subfield of K and G be any group of automorphism of K.

Proof:

Given that F be any subfield of K and G be any group of automorphism of K . to prove fixed field of G is a subfield of K.

A subset A of k such that, $A = (x \in K: \sigma(x) = x \ \forall \ \sigma \in G)$ is called fixed of field of G.

To prove A is a subfield of K.

$x,y \in A$

$\Rightarrow$ $x,y \in K$ such that $\sigma(x) = x$ and $\sigma(y) = y \ \forall \ \sigma \in K$.

$\Rightarrow$ $x\text{-}y \in K$ such that $\sigma(x\text{-}y) = \sigma(x + (\text{-}y))$

$= \sigma(x) + \sigma(\text{-}y)$

By the property of automorphism

$$\sigma(x\text{-}y) = \sigma(x) + \sigma(\text{-}y)$$

$$= \sigma(x) - \sigma(\text{-}y)$$

$$= x\text{-}y$$

$$\sigma(x\text{-}y) = x\text{-}y$$

$x\text{-}y \in K \Rightarrow x\text{-}y \in A$

$x,y \in A$ such that $y \neq 0$

$\Rightarrow \sigma(x) = x$

$\Rightarrow \sigma(y) = y$

$\sigma \in G$ and $x, y \in K \ni y \neq 0$

$\Rightarrow xy^{-1} \in K$

Since σ is isomorphism

$\Rightarrow xy^{-1} \in K$ such that $\sigma(xy^{-1}) = xy^{-1} \ \forall \ \sigma \in G$

$\Rightarrow xy^{-1} \in A$

$x-y \in A \Rightarrow x-y \in A$

And $x, y \in A$ such that $y \neq 0$

$\Rightarrow xy^{-1} \in A$

Also $A \subset K$

Hence A is a subfield of K.

Theorem: 4.4

Let F be any subfield of K and G any group of automorphism of K then G(K,F) is a subgroup of the automorphism group of K.

Proof:

Given that F be a subfield of K, so that F itself is a field and G be the Group of automorphism of K. To prove G(K,F) is a subgroup of the automorphisms group of K.

G is the group of mapping σ such that $\sigma: K \to K$ is one-one onto And $\sigma(x+y) = \sigma(x) + \sigma(y)$

$\sigma(x+y) = \sigma(x)\sigma(y)$

Define $G(K, F) = \{\sigma \in G: \sigma(x) = x \; \forall \; x \in F\}$

$G(K, F) \subset G.$

To prove G (K, F) is a subgroup of G

Let $f, g \in G(K,F)$ be arbitrary. Then f,g are automorphisms of K such that $f(x) = x$, $g(x) = x \; \forall \; x \in F$ f and g are automorphisms of K.

$f: K \to K$ and $g: K \to K$ are one to one onto map

$f(x + y) = f(x) + f(y)$

$f(xy) = f(x) f(y) \; \forall \; x,y \in F$

$\Rightarrow fg: K \to K$ is one-one onto map

If $x, y \in K$, then

$(fg)(x+y) = f(g(x+y))$

$= f[g(x) + g(y)]$

$= f[g(x)] + f[g(y)]$

$= (fg)(x) + (fg)(y)$

Also $(fg)(xy) = f[g(xy)]$

$=f[g(x) g(y)]$ by (3)

$= f[g(x)] f[g(y)]$

$= (fg)(x) (fg)(y)$

To show that $fg : K \to K$ is one to one onto map such that

$(fg)(x+y) = (fg)(x) + (fg)(y)$

$(fg)(xy) = (fg)(x) (fg)(y)$

This proves that fg is an automorphism of K and hence $fg \in G$:

$(fg)(x) = f[g(x)] = f(x)$

$= x \; \forall \; x \in F$

ie., $(fg)(x) = x \; \forall \; x \in F$

$\Rightarrow fg \in G(K,F)$

$\Rightarrow f^{1}: K \to K$ is one to one onto map

Let $f(x) = x'$

$f(y) = y' \; \forall \; x,y \in F$

Then x’, $y' \in K$ and f1 $(x') = x$

$f^{1}(y') = y$

$f(x+y) = f(x) + f(y)$

$f^{1}(x+y) = x' + y'$

This $\Rightarrow x+y = f^{1}(x' + y')$

$\Rightarrow f^{1}(x' + y') = x+y$

$f^{1}(x' + y') = f^{1}(x') + f^{1}(y')$

$\Rightarrow f^{1}(x' + y') = f^{1}(x') + f^{1}(y')$

And $f(xy) = f^{1}(xy)$

$f(xy) = x'y'$

$\Rightarrow xy = f^1(x'y')$

$= f^1(x')\, f^1(y')$

$\Rightarrow f^1(x'y') = f^1(x')\, f^1(y')$

If $x \in F$,

Then $f(x) = x$

So that $f^1(x') = x$

To show that $f^1: K \rightarrow K$ is one-one onto map

and $f^1(x' + y') = f^1(x') + f^1(y')$

$f^1(x'y') = f^1(x')\, f^1(y')\ \forall\ x', y' \in K$

$f^1(x') = x\ \forall\ x \in F$

To prove that f^1 is an automorphism of K such that $f^1(x') = x\ \forall\ x \in F$

Consequently $f^1 \in G(K,F)$

$fg \in G(K,F)$

$\Rightarrow fg, f^1 \in G(K,F)$

$\Rightarrow$ G(K,F) is a subgroup of G.

Hence G(K,F) is a subgroup of the automorphisms group of K is proved.

Theorem:4.5

Let K be a field and let $\sigma_{1,}\ \sigma_2\ \ldots\ldots\ldots\ldots,\ \sigma_n$ be distinct automorphisms of K. Then it is impossible to find elements

$a_1, a_2, \ldots\ldots.. a_n$ not all zero, in K such That

$a_1\sigma_1(u) + a_2\sigma_2(u) + \ldots\ldots.. + a_n\sigma_n(u) = 0\ \forall\ u \in K.$

Proof: Given that K be a field and $\sigma_{1,}\ \sigma_2\ \ldots\ldots..,\ \sigma_n$ be distinct automorphisms of K. To prove it is impossible to find elements

$a_1, a_2, \ldots\ldots.. a_n$ not all zero, in K such That

$a_1\sigma_1(u) + a_2\sigma_2(u) + \ldots\ldots.. + a_n\sigma_n(u) = 0\ \forall\ u \in K.$

Suppose if possible,

To find elements $a_1, a_2, \ldots\ldots.. a_n$ not all zero, in K such that

$a_1\sigma_1(u) + a_2\sigma_2(u) + \ldots\ldots.. + a_n\sigma_n(u) = 0\ \forall\ u \in K$ **……………(1)**

In equation (1), to find a relation which has a few non zero terms as possible.

Let the minimal relation be $a_1\sigma_1(u) + a_2\sigma_2(u) + \ldots\ldots.. + a_m\sigma_m(u) = 0$

$\forall\ u \in K$……..(2)

Where each $a_r \neq 0$ for $1 \leq r \leq m$

If m=1,

Then (2) $\Rightarrow a1\sigma_1(u) = 0\ \forall\ u \in K.$

$\Rightarrow a_1\sigma_1(1) = 0$

$\Rightarrow a_1 1 = 0$

$\Rightarrow a_1 = 0$

It is contradiction to $a_1 \neq 0$

Hence $m > 1$

By assumption $\sigma_1 \neq \sigma_m$ and so there exist an element $c \in K$ such that

$\sigma_1(c) \neq \sigma_m(c)$

Also $c, u \in K$

$\Rightarrow c\,u \in K$

Equ (2) $\Rightarrow a_1\sigma_1 c(u) + a_2\sigma_2 c(u) + \ldots\ldots.. + a_m\sigma_m c(u) = 0\ \forall\ u \in K$

$\Rightarrow a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_2(c)\sigma_2(u) + \ldots + a_m\sigma_m(c)\sigma_m(u) = 0$**……(3)**

Multiply equ (2) by $\sigma_1(c)$

$a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_1(c)\ \sigma_2(u) + \ldots\ldots.. + a_m\sigma_1(c)\ \sigma_m(u) = 0\ \forall\ u \in K$ **………(4)** From (3) - (4)

$$a_1 \sigma_1(c)\,\sigma_1(u) + a_2 \sigma_2(c)\,\sigma_2(u) + \ldots\ldots\ldots + a_m \sigma_m(c)\,\sigma_m(u)$$

$$-a_1 \sigma_1(c)\,\sigma_1(u) + a_2 \sigma_1(c)\,\sigma_2(u) + \ldots\ldots\ldots + a_m \sigma_1(c)\,\sigma_m(u) = 0$$

$$a_2 \sigma_2(u)\,[\sigma_2(c) - \sigma_1(c)] + \ldots\ldots\ldots\ldots\quad a_m \sigma_m(u)\,[\sigma_m(c) - \sigma_1(c)] = 0$$

set $bi = ai\ [\sigma_i(c) - \sigma_1(c)]$ for $i = 1,2,\ldots\ldots.m$

since $a_m \neq 0$, $\sigma_m(c) \neq \sigma_1(c)$

$\Rightarrow b_m \neq 0$

Also $bi \in K$

Hence $b_2 \sigma_2(u) + b3\,\sigma_3(u) + \ldots.. + b_m \sigma_m(u) = 0$ **……………(5)**

This is true $\forall$ $u \in K$. Equation (5) contains m-1 terms such that $b_m \neq 0$. Now it is possible for us to find a relation of type (1) having less than m non Zero terms. It is contradiction to initial assumption equ (2) is a minimal relation. Hence our initial assumption is wrong. Hence it is impossible to find Element a_1, $a_2, \ldots\ldots..a_n$ not all zero, in K such that $a_1 \;\; _1(u) + a_2 \;\; _2(u) + \ldots\ldots.. + a_n \;\; _n(u) = 0$ $u \in K$.

IV. CONCLUSIONS

Finite fields are used in application of coding theory, many codes are Constructed as subspaces of vector spaces over finite fields . counting solutions of Equations over finite fields into deep questions in algebraic geometry. Galois Theory uses groups to describe the symmetric of the root of Polynomials. The theory being one of the historical roots of group theory. It is used to yield new results in areas as such as class field theory. One advantage in splitting is the save of space in some situations. Ex., a long Text field for extra comments or notes, which is used only rarely, its economical to Separable it to a different table. Galois theory not only provides a beautiful answer to this question, it also Explains in detail why it possible to solve equations of degree four or lower in the Above manner and why their solutions take the form that they do. Further, it gives a Conceptually clear and often practical, means of telling when some particular Equations of higher degree can be solved in that manner. Galois theory originated in the study of symmetric functions the co-efficient Of a monic polynomial are the elementary symmetric polynomials in the roots. Algebraic extensions involve splitting field of polynomials. Field is algebraic Study of single polynomials. The general algebraic extension of an polynomial could Appropriately occur in many subfields of number theory or field theory, for example, The extension field generates in algebraic number theory. The algebraic study of general collections of polynomial is appropriate for ring theory , specific families of polynomials.

REFERENCES

[1] GARRETT BIRKHOFF, SAUNDERS Mac LANE – “ A SURVEY OF MODERN ALGEBRA” , Universities press private (India) limited, first edition.

[2] GOYAL GUPTA - “ ADVANCED COURSE IN MODERN ALGEBRA” First edition.

[3] I.N HERSTEIN - “ TOPICS IN ALGEBRA” , Wiley Easter Limited, Second Edition.

[4] M.L. KANNA – “MODERN ALGEBRA” , Jai Prakash Nath & Co, Meerut, sixteenth edition - 2004 .

[5] I.S LUTHER, I.B.S. PASSI – “FIELD THEORY” , Narosa Publishing house 2004.

[6] MICHEAL ARTIN - “ ALGEBRA” , Printice – Hall of India Private limited, New Delhi, 2005.

[7] SERGELANG - “ ALGEBRA” , Springer publications , third Edition.