Nalanda Open University

M.sc Part-I

Course : Mathematics

Paper I

Prepared by : Dr. L .K .SHARAN,

Rtd. Professor & Head, Dept. Of Mathematics,

V.K.S. University, ARA.

Mobile:- 9835228272

Email Id – lalitsharan9@gmail.com

UNIT IV

Extension Fields

Contents : Field Extension, Degree of Field Extension, Finite Field Extension, Simple Extension, Finitely Generated Field, Algebraic Element, Algebraic Extension of Field, Minimal Polynomial, Monic Polynomial, Root of a Polynomial, Splitting Field, Root Field, Multiple Root,

1. Field extensions, Finite field extensions, Simple extension of a field, Algebraic extensions of a field.

1.1 Introduction: A field is in fact a commutative ring with unity in which every non zero element has a multiplicative inverse. We shall make efforts to study the theory of finite field extensions and related properties.

1.2 Definitions:

Field Extension: Every field F is called an extension of its subfield K.

Degree of a Field Extension: If K is the extension of a field F then the dimension of the vector space K(F) is called the degree of K over F. It is denoted by [K:F].

Finite Field Extension: The extension of the field F is called finite if [K:F] is finite otherwise it is called an infinite field extension.

Simple Extension of a Field: The extension K of the field F is called simple extension of F if K =F(a) for some a in K. The element a is called Primitive element of K over F.

Finitely Generated Field: A field K is called finitely generated over the field F if we get $a_1, a_2, ...,a_n \in K$ such that $K = F(a_1, a_2, ...,a_n)$.

Algebraic Element: Let K be an extension of a field F then an element a of K is called algebraic over F if we get $\alpha_0, \alpha_1, ..., \alpha_n$ in F, not all 0, such that

$$\alpha_0 a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0$$

Algebraic Number: A complex number is called an algebraic number if it is algebraic over the field of rational number.

Algebraic Extension of a Field: The extension K of the field F is called an algebraic extension of F if every element of K is algebraic over F.

Minimal Polynomial: Let $a \in K$, K is an extension of a field F. a is algebraic over F. If p(x) is a polynomial over F of lowest positive degree satisfied by a, then p(x) is called minimal polynomial for a over F.

Monic Polynomial: A non zero polynomial $f(x) \in F(x)$ is said to be monic over F, if the coefficient of highest power of x in F(x) is 1 in F.

Examples

Ex 1 : R the set of all real numbers is an extension field of Q the set of rationals where as C, the set of all complex numbers is an extension field of R and Q.

Ex 2 : The field C of complex numbers is a finite extension of the field R of real numbers. Here [C : R] = 2. Also [F : F] = 1.

1.3 Theorems :

Theorem 1.3(1) : (Transitivity of Finite extension) :- Let L be a finite extension of K and if K is a finite extension of F, then L is a finite extension of F.

In other words [L: F] = [L : K] [K : F]

Proof:- By question $F \subseteq K \subseteq L$.

Let [L : K] = m and [K : F] = n.

Also let, $\alpha_1, \alpha_2, \ldots\ldots, \alpha_m$ be a basis of L(K)

And $\beta_1, \beta_2, \ldots\ldots, \beta_n$ is a basis of K (F)

Since $K \subseteq L \Rightarrow \beta_1, \beta_2, \ldots\ldots, \beta_n \in L$

$\Rightarrow (\alpha_1, \alpha_2, \ldots\ldots, \alpha_m)\ (\beta_1, \beta_2, \ldots\ldots, \beta_n) = \alpha_i \beta_j$ = m n elements are in L for i = 1,....., m, j = 1, 2,....,n

To show m n elements $\alpha_i \beta_j$ forms a basis for L(F)

That is to prove [L: F] = m n

For, let $l \in L$ be arbitrary

Clearly l can be expressed as linear combination of $\alpha_1, \alpha_2, \ldots\ldots, \alpha_m$

Thus $l = \sum_{i=1}^{m} K_i \alpha_i$, $K_i \in K$ (as K is field for L) ----------(1)

Again $K_i \in K$ and $\{\beta_1, \beta_2, \ldots\ldots, \beta_n\}$ is a basis for K(F)

Thus $K_i = \sum_{j=1}^{n} f_{ij} \beta_i$, $f_{ij} \in F$----------(2)

From (1) and (2)

$l = \sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij}(\alpha_i \beta_j)$, $f_{ij} \in F$

Thus l is a linear combination of $\alpha_i \beta_j$

This implies elements $\alpha_i \beta_j$ generates L(F).

Also if $\sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij}(\alpha_i \beta_j) = 0 \Rightarrow \sum_{i=1}^{m}(\sum_{j=1}^{n} f_{ij} \beta_j)\ \alpha_i = 0 \Rightarrow \sum_{j=1}^{n} f_{ij} \beta_j = 0$, i = 1, 2,....m

This implies $f_{ij} = 0$, i =1, 2,....m, j =1, 2, ...n

Implies $[\alpha_i \beta_j]$ is linearly independent over F

Thus the set of m n elements forms a basis for L(F)

Implies [L:M] = m n

⇨ [L: F] = [L : K] [K : F]

Theorem 1.3 (2) : Let F be a field and K be an extension of F. An element a∈ K is algebraic over F iff F(a) is a finite extension of F.

Proof:- First of all we assume F(a) is a finite extension of F.

To prove a is algebraic over F.

For this, let [F(a) : F] = m and a ∈ F(a) => m+1 elements 1, a, a^2,....., a^{m-1}, $a^m \in F(a)$

Also these m+1 elements are linearly dependent over F.

Thus for $\alpha_0, \alpha_1, \alpha_2$, ..., α_m in K, not all 0

$\alpha_0.1 + \alpha_1 a + \alpha_2 a^2 + \ldots\ldots + \alpha_m a^m = 0 \Rightarrow f(x) = \alpha_0. + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots + \alpha_m x^m \in F(x)$

That is a satisfies a non zero polynomial.

Hence a is algebraic.

Conversely:- Let a ∈ K is algebraic. To prove F(a) is a finite extension of F.

For this, let s(x) be a polynomial over F of lowest degree and a satisfies it.

Let degree of S(x) = n => a is algebraic of degree n over F.

So $F(a) = \{ \beta_0 + \beta_1 a + \beta_2 a^2 + \ldots\ldots + \beta_{n-1} a^{n-1} : \beta_0, \beta_1, \ldots\ldots, \beta_{n-1} \in F \}$

=> F(a) is a vector space over F, spanned by 1, a, a^2,....., a^{n-1}

Also elements of F(a) are linearly independent over F.

So let $c_0.1 + c_1 a + c_2 a^2 + ... + c_{n-1} a^{n-1} = 0, c_i \in F$

So a satisfies the polynomial $q(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{n-1} x^{n-1} \in F(x)$

But for s(x) to be polynomial of lowest positive degree satisfied by a

$q(x) = 0 \Rightarrow c_0 = 0, c_1 = 0, c_2 = 0, ... , c_{n-1} = 0$

- ⇨ 1, a, a^2,....., $a^{n-1} \in$ F(a) are linearly independent over F.
- ⇨ 1, a, a^2,....., a^{n-1} form a basis for F(a) over F.
- ⇨ [F(a) : F] = n => F(a) is finite extension of F,,

Theorem 1.3(3) : Every finite extension of a field F is algebraic.

Proof :- Let K be an algebraic extension of the field F.

Also let K(F) be n dimensional vector space . That is degree of K(F) = n.

To prove that K is algebraic extension.

For this, sufficient to prove that every element of K is algebraic element over F.

Let $\alpha \in K$ be an arbitrary and K is a field => $\alpha, \alpha^2, ..., \alpha^{n-1}, \alpha^n \in K$.

Also $1 \in K$ => the set [$1, \alpha, \alpha^2, ..., \alpha^{n-1}, \alpha^n$] of n+1 elements of K is linearly dependent because dimension of K over F is n.

Thus for { $1, \alpha, \alpha^2, ..., \alpha^{n-1}, \alpha^n$ }we can get $a_0, a_1, ..., a_n \in F$ such that

$a_0.1 + a_1 \alpha + a_2 \alpha^2 + ... + a_n \alpha^n = 0 \Rightarrow a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n \alpha^n = 0$

=> α is a root of non zero polynomial $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \in F(x)$

=> $\alpha \in$ K(F) but α is arbitrary => every element of K is algebraic over F.

Thus K is an algebraic extension of F.

Theorem 1.3(4) : If $\alpha, \beta \in K$ are algebraic over F, then $\alpha \pm \beta, \alpha . \beta, \alpha / \beta, (\beta \neq 0)$ are all algebraic over F. Hence, the elements in K which are algebraic over F form a sub-field K.

Proof:- Since $\alpha \in K$ is algebraic over the field F => [F(α) : F] is finite

Also $\beta \in K$ is algebraic over F so it satisfies a non zero polynomial over F, but F(α) is a super field of F.

It means every non zero polynomial over F is also non zero polynomial over F(a).

So β satisfies a non zero polynomial over F(α).

So, (F(α)) (β) = F[α, β] is a field generated by β over F(α), so that F(α, β) is a finite extension of F(α), i.e, [F(α, β) : F(α)] is finite.

Thus by Transitivity theorem [F(α, β) : F] = [F(α, β) : F(α)] [F(α) : F]

Since [F(α, β) , F(α)] and (F(α) , F) are finite => [F(α, β) : F] is finite.

Thus F(α, β) is a finite extension of F. => it is algebraic extension.

Thus every element of F(α, β) is a algebraic over the field F.

Since F(α, β) is a field so $\alpha, \beta \in F(\alpha, \beta) \Rightarrow \alpha \pm \beta \in F(\alpha, \beta)$, $\alpha . \beta \in F(\alpha, \beta)$

Now $\beta \neq 0 \Rightarrow \beta^{-1} \in F(\alpha, \beta) \Rightarrow \alpha / \beta \in F(\alpha, \beta)$

Thus $\alpha \pm \beta$, $\alpha . \beta$ and α / β $(\beta \neq 0)$ are all algebraic over F.

Theorem 1.3(5) : Let F be a field and K be an extension of F. If α and β in K are algebraic over F of degree m and n respectively then $\alpha \pm \beta$, $\alpha . \beta$ and α / β $(\beta \neq 0)$ are all algebraic over F of degree at most mn.

Proof :- Given $\alpha \in K$ is algebraic over F of degree m.

Thus [F(α) : F] = m

$\beta \in K$ is also an algebraic over degree n. => [F(β): F] = n

Clearly β must satisfy minimal polynomial of degree m over F.

Also F will satisfy minimal polynomial of degree utmost n over F as F(α) is a finite extension of F.

Thus [F(α, β) : F(α)] ≤ n

By Transitivity law of field we have

$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] [F(\alpha) : F] \subseteq m\ n$

- ⇨ $F(\alpha, \beta)$ is a finite extension of F.
- ⇨ $F(\alpha, \beta)$ is an algebraic extension of F of degree utmost m n.

Then clearly each element of $F(\alpha, \beta)$ is algebraic of degree utmost m n.

Again $\beta \neq 0 \Rightarrow \beta^{-1}$ exists and $\beta^{-1} \in F(\alpha, \beta) \Rightarrow \alpha, \beta^{-1} \in F(\alpha, \beta)$

Therefore $\alpha \pm \beta$, $\alpha\ \beta$ and $\alpha / \beta\ (\beta \neq 0)$ or equivalently $\alpha\ \beta .1$ are all α of degree utmost m n.

Theorem 1.3(6) : (Transitivity of Algebraic Field Extension) :

Let L be a algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.

Proof :- Let α be an arbitrary element of L.

To show that α is to satisfy non zero monic polynomial over F.

Now $\alpha \in L$ and L (K) is algebraic $\Rightarrow \alpha$ must satisfy non zero monic polynomial over F.

Polynomial $p(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots\ldots + a_{n-1} x + a_n$ over K.

Clearly $a_1, a_2, \ldots\ldots, a_n \in K$ and $K \alpha$.

- ⇨ Each of $a_1, a_2, \ldots\ldots, a_n$ algebraic over F.

Thus the extension $K = F (a_1, a_2, \ldots\ldots, a_n)$ is a finite extension of F.

Also α is algebraic over K $\Rightarrow$ K(α) is finite extension of K

By Transitivity of finite extension fields we shall have :

$[K(\alpha) : F] = [K(\alpha) : K] [K : K]$

- ⇨ $[K(\alpha) : K]$ is finite as $[K(\alpha) : K]$ and $[K : K]$ both are finite
- ⇨ K(α) is finite extension of F
- ⇨ α is algebraic over F but α is arbitrary.

Thus each and every element of L is algebraic over F.

Therefore L is an algebraic extension of F.

1. ROOTS OF POLYNOMIAL

1.1 Introduction :

In this section we consider a polynomial p(x) on F(x) where F is a field. We also try to get an extension K of F in which p(x) has a root.

1.2 Definition :

Root of a Polynomial : Let F be a field. If $p(x) \in F[x]$ then an element α lying in some extension field of F is called a root of p(x) if $p(\alpha) = 0$.

2.3 Theorems :

Theorem 2.3(1) (Remainder Theorem) : If $p(x) \in F[x]$ and if K is an extension field of the field F, then for any element $c \in K$,

$p(x) = (x-c) q (x) + p(c)$ where $q(x) \in K[x]$ and degree q(x) = degree p(x) -1

Proof :- Since $F \subseteq K$, $F[x] \subseteq K[x]$

So we can assume that $p(x) \in K[x]$

By division algorithm for polynomials in K[x] $\exists$ q (x) in K[x] such that,

$p(x) = (x-c) q (x) + r$ ----------(1)

Where r = 0 or deg. r = 0. In either case $r \in K$.

Now $p(c) = (c-c) q (c) + r = r$ (due to (1))

⇨ $p(x) =(x-c) q (x) + p(c)$

Thus clearly degree of q(x) = degree p(x)-1

Theorem 2.3(2) : A polynomial of degree n over a field can have utmost n roots in any extension field.

Proof :- Let K be an extension of F, $f(x) \in F[x]$ be a polynomial of degree n over F.

In order to establish this theorem we shall use the method of induction.

For this, if n = 1 then $p(x) = a_0 x + a_1$, $a_0 \neq 0$, $a_0, a_1 \in K$

$x = - a_1/ a_0$ is an unique root of $f(x) \in F[x]$ which is in K.

⇨ The theorem is true for n = 1

Let n > 1 so by law of induction we can assume that the theorem is true for each polynomial of degree.

Now there is a root of multiplicity m $\alpha \in K$ of f(x)f

Then $\exists$ a polynomial q(x) is in K[x] such that

$f(x) = (x- \alpha)^{m} q(x)$, with $q(x) \neq 0$

Clearly, degree (q(x)) = n – m < n.

Thus by induction q(x) will have utmost (n-m) roots in K.

Since $q(x) \neq 0 \Rightarrow \alpha$ is not a root of q(x).

Also any root of f(x) in K other than α is a root of q(x).

Let $\beta \neq \alpha$ be any root of f(x) in K, then n = 1,

We have $f(\beta) = (\beta - \alpha)^{m} q(\beta)$ but $f(\beta) = 0$ then $(\beta - \alpha)^{m} . q(\beta) = 0 \Rightarrow q(\beta) = 0$

As $(\beta - \alpha)^{m} \neq 0 \Rightarrow \beta$ is a root of q(x) in K.

- ⇨ q(x) has utmost n – m roots in K other than α.
- ⇨ f(x) has utmost n – m roots in K other than α.

Thus, f(x) has utmost (n – m) + m = n roots in K.

Theorem2.3(3) (Kroncker's Theorem) : Let f(x) be an irreducible polynomial of positive degree in F[x]. Then $\exists$ an extension K of F in which f(x) has a root. Also

[K : F] = deg f(x)

Proof :- Let deg f(x) = n (a positive integer)

Given : f(x) is irreducible in F[x] => f(x) is maximal ideal of F[x]

Hence F[x]/ f(x) is a field and an extension of F.

If K = F[x]/ f(x) and $K^1 = [f(x) + a : a \in F] \Rightarrow K^1 \subseteq K$

Let $(f(x) + a), (f(x) + b) \in K^1$ be arbitrary and $f(x) + b \neq f(x)$

Then $(f(x) + b)^{-1} \in K \Rightarrow f(x) + b^{-1} \in K \Rightarrow b^{-1} \in F$ [$b \neq 0$ and $K^1 \subseteq K$]

Thus $(f(x) + a) ((f(x) + b))^{-1} (f(x) + a) (f(x) + b^{-1}) = (f(x)) + a b^{-1} \in K^{-1}$.

Thus K^1 is a subfield of K

Consider a mapping $\psi : F \rightarrow K$ given by $\psi(a) = (f(x) + a)$, for every $a \in F$.

We now see that,

For a, b in F, $\psi(a) = \psi(b) \Rightarrow f(x) + a = f(x) + b \Rightarrow a-b \in (f(x))$

$\Rightarrow$ $a - b = f(x) \cdot g(x)$, for some $g(x) \in F[x]$

Supposition f(x) is irreducible so f(x) . (any non zero polynomial) $\neq$ constant polynomial.

Thus $g(x) = 0 \Rightarrow a - b = 0 \Rightarrow a = b$

That is $\psi(a) = \psi(b) \Rightarrow a = b \Rightarrow \psi$ is one-one

Also, let $(f(x)) + a \in K^1$ such that $a \in K$ then

$\psi(a) = (f(x)) + a$, for every a in F $\Rightarrow \psi$ is onto also.

Also for $a, b \in F$ we can see that

$\psi (a+ b) = (f(x)) + (a+ b) = (f(x)) + a + (f(x)) + b = \psi(a) + \psi(b)$.

Thus $\psi : F \rightarrow K$ is isomorphic and K^1 is a subfield of K

Thus F can be regarded as a subfield of K.

That is K is an extension of F

We can see by a previous theorem that elements $v + 1, v + x, v + x^2, ..., v + x^{n-1}$ form a basis of K (F)

[K : F] = n = degree f(x)

Now we show that f(x) has a root in K.

For this, let $f(x) = a_0.+ a_1 x + a_2 x^2+ ..... + a_n x^n$, $a_n \neq 0$, $a_0, a_1, ..., a_n \in F$

Since $f (x) \in F (x)$.

$\Rightarrow$ $(f(x)) + f(x) = f(x) \Rightarrow (f(x)) + (a_0.+ a_1 x + a_2 x^2+ ..... + a_n x^n) = (f(x))$

$\Rightarrow$ $(f(x) + a_0) + (f(x) + a_1 x) + ... (f(x) + a_n x^n) = (f(x))$

$\Rightarrow a_0 ((f(x)) + 1) + a_1 ((f(x)) + x) + ... + a_n ((f(x)) + x^n) = (f(x))$

$\Rightarrow a_0 ((f(x)) + x)^0 + a_1 ((f(x)) + x)^1 + ... + a_n ((f(x)) + x)^n = (f(x))$

But (f(x)) is the zero element of F[x]/ f(x) = K

It means every element (f(x)) + x in K satisfies the polynomial f(x)

Thus f(x) has root in K.

2. SPLITTING FIELDS AND ROOT FIELDS

2.1 Introduction : We study about a function in a given field F which is factored into linear factors in an extension field K of the field F.

2.2 Definition :

Root Field : Let K be a simple extension of a field F. Let f(x) be an irreducible polynomial in F[x]. Then K is said to be a root field of f(x) if K contains a root of f(x).

Splitting Field : If $f(x) \in F[x]$ then a finite extension K of F is said to be splitting field over F for f(x) in K [x], but not over any proper subfield of K, f(x) can be factored as a product of linear factors.
Equivalently : a field K is a splitting field of f(x) over F if K is a minimal extension field of F in which f(x) has n roots, where n = deg. f(x).

Automorphism of a field K : By an automorphism we mean a one -to-one mapping f of K onto itself such that

(i) f(a+b) = f(a) + f(b) and

(ii) f(a) . f(b), for all $a,b \in K$.

Also two automorphism f and g of the field are said to be distinct if $f(a) \neq g(a)$ for some $a \in K$.

We now give below a theorem which guarantees the existence of a splitting field foe every p(x) in F[x].

Theorem (3.3) 1 : There exists a splitting field for every p(x) in F[x].

Proof :- Let F[x] be the ring of polynomial in x over F and let

M = (p(x)) be the ideal in F[x] generated by p(x).

Since p(x) is irreducible over so the ideal M is maximal ideal in

F[x]. Thus be a theorem E = F[x] / M is a field.

We show that E is an extension field of F.

For this, since F is isomorphic to a subfield F_1 of E.

Let $F_1 = \{ \alpha + M : \alpha \in F \}$.

We claim that F_1 is subfield of E isomorphic to F.

If $\psi : F[x] \to F[x] / M = E$ given by $f(x) \to f(x) + M$, then the restriction

of ψ to F induces an isomorphism of F onto F_1.

Using this isomorphism we identify F onto F_1.

In this way we can consider E to be an extension of F.

We now claim that E is a finite extension of F of degree n = deg p(x).

For the elements $1+M, x+M, (x+M)^2, \ldots\ldots\ldots, (x+M)^i, \ldots\ldots\ldots (x+M)^{n-1}$

Where $(x+M)^2 = x^2+M, \ldots\ldots\ldots, (x+M)^i = x^i+M, \ldots\ldots\ldots, (x+M)^{n-1} = x^{n-1}+M$

Which forms a basis of E (F).

Let us denote $\psi(x) = x + M$ in the field E be a then given $f(x) \in F[x]$

We claim that $\psi f(x) = f(a)$.

For, since ψ is a Homomorphism so if $f(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \ldots\ldots\ldots + \beta_k x^k$, then

$\psi(f(x)) = \psi(\beta_0) + \psi(\beta_1)\psi(x) + \ldots\ldots\ldots + \psi(\beta_k)(\psi(x))^k$.

Using the identification indicated above of $\psi(\beta)$ with β, we can see that

$\psi(f(x)) = \beta_0 + \beta_1 a + \beta_2 a^2 + \ldots\ldots\ldots + \beta_k a^k = f(a)$

In particular, since $p(x) \in M$, $\psi(p(x)) = 0$ but $\psi(p(x)) = p(a)$

Thus $a = \psi(x)$ in E is a root of p(x).

Thus the theorem is shown.

Theorem (3.3) 2 : Let ψ be an isomorphism of a field F_1 onto a field F_2.

Such that $\alpha\psi = \alpha'$ for every $\alpha \in F_1$. Then there is a isomorphism φ of $F_1[x]$ onto $F_2[t]$ with the property $\alpha\varphi = \alpha\psi = \alpha'$, for each $\alpha \in F_1$.

Proof :- Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n =$ be an arbitrary polynomial of $F_1[x]$, where $a_0, a_1, \ldots\ldots, a_n \in F_1$

Let $\varphi : F_1[x] \to F_2[t]$ such that $\varphi f(x) = (a_0 + a_1 x + a_2 x^2 + ... + a_n x^n)\varphi$

$= a_0\psi + a_1\psi t + a_2\psi t^2 + ... + a_n\psi t^n = a_0 + a_1 t + a_2 t^2 + ... + a_n t^n = f'(t)$ (say).

For $f(x)$ and $g(x) \in F_1[x]$ such that,

$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ and

$g(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + ... + \beta_m x^m$

we find that :

$f(x)\varphi = g(x)\varphi \Rightarrow (a_0 + a_1 x + a_2 x^2 + ... + a_n x^n)\varphi = (\beta_0 + \beta_1 x + \beta_2 x^2 + ... + \beta_m x^m)\varphi$

- $\Rightarrow \alpha_0 + \alpha_1 t + \alpha_2 t^2 + ... + \alpha_n t^n = \beta_0 + \beta_1 t + \beta_2 t^2 + ... + \beta_m t^m$
- $\Rightarrow$ $n = m$ and $\alpha_i = \beta_i$ for each $i = 0, 1, 2, ... , n.$
- $\Rightarrow$ $n = m$ and $\alpha_i\psi = \beta_i\psi$ for each i
- $\Rightarrow$ $n = m$ and $\alpha_i = \beta_i$ for each i
- $\Rightarrow$ $f(x) = g(x)$
- $\Rightarrow$ φ is one-one

We now verify φ to be onto.

For, let $b_0 + b_1 t + b_2 t^2 + ... + b_n t^n$ be any element of $F_2[x]$, $b_0, b_1, ... , b_n \in F_2$

Since ψ is onto F_2 , so $\exists\ b_0, b_1, ... , b_n \in F_1$ such that

$b_0\psi = b_0$, $b_1\psi = b_1$, ... , $b_n\psi = b_n$,

Now $b_0 + b_1 x + b_2 x^2 + ... + b_n x^n \in F[x]$.

Also $[b_0 + b_1 x + b_2 x^2 + ... + b_n x^n]\varphi = b_0 + b_1 t + b_2 t^2 + ... + b_n t^n$

Therefore φ is onto.

Further :

Let $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$,

$g(x) = b_0 + b_1 x + b_2 x^2 + ... + b_m x^m \in F_1[x]$

let $n \geq m$.

Case I :- when $n > m$ then

$[f(x) + g(x)]\varphi = [(a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_n x^n]\varphi$

$= (a_0 + b_0)\psi + (a_1 + b_1)\psi\ t + ...+ (a_m + b_m)\psi\ t^m + a_{m+1}\psi\ t^{m+1} + ... + a_n\psi\ t^n$

$= (a_0\psi + b_0\psi) + (a_1\psi + b_1\psi)t + ...+ (a_m\psi + b_m\psi)t^m + a_{m+1}\psi\ t^{m+1} + ... + a_n\psi\ t^n$

$= (a_0 + a_1 t + ... + a_m t^m + a_{m+1}\ t^{m+1} + ... + a_n\ t^n) + (b_0 + b_1 t + b_2 t^2 + ... + b_m t^m)$

$= f(x)\varphi + g(x)\varphi$

Thus φ preserves addition of polynomials for $n > m$

Similarly for $n = m$ we can again show that $[f(x) + g(x)]\varphi = f(x)\varphi + g(x)\varphi$

Finally, $[f(x) . g(x)]\varphi = [(a_0 + a_1 x + a_2 x^2 + ... + a_n x^n)(b_0 + b_1 x + b_2 x^2 + ... + b_m x^m)]\varphi$

$= [a_0 b_0 + (a_0 b_1 + a_1 b_0)x + ... + a_n b_m\ x^{m+n}]\varphi$

$= (a_0\ b_0)\psi + (a_0 b_1 + a_1 b_0)\psi\ t + ... + (a_n b_m)\psi\ t^{m+n}$

$= a_0 b_0 + (a_0 b_1 + a_1 b_0)\ t + ... + (a_n b_m)\ t^{m+n}$

$= (a_0 + a_1 t + a_2 t^2 + ... + a_n t^n)(b_0 + b_1 t + b_2 t^2 + ... + b_m t^m)$

$= [f(x)\varphi][g(x)\varphi]$

Hence φ is an isomorphism of $F_1[x]$ and $F_2[t]$.

Also, if $f(x) \in F_1[x]$ be simply taken as α, where $\alpha \in F_1$ then as per the definition of φ, we have

$$\alpha\varphi = \alpha\psi = \alpha'$$

Theorem (3.3) 3 : Splitting fields are algebraic extensions.

Proof :- Let $f(x)$ be a polynomial over a field and K be its Splitting field.

Let $\alpha_1, \alpha_2, ..., \alpha_n$ be the roots of $f(x)$

To show that K is an algebraic extension of F.

For this,

Clearly $K = F(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n)$

Then $K_1 = F(\alpha_1)$

$K_2 = K_1(\alpha_2) = F(\alpha_1, \alpha_2)$

$K_3 = K_2(\alpha_3) = F(\alpha_1, \alpha_2, \alpha_3)$

.....

$K = K_n = K_{n-1}(\alpha_n) = F(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n)$

Also $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n$ are all algebraic elements over F (since $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n$ are roots of non zero polynomial over f)

Also each of the fields F, $K_1, K_2, K_3, ..., K_n = K$ can be obtain on adjoining an algebraic element to its predecessor field extension so that each of the degrees

$[K_1: F], [K_2: K_1], ... , [K: K_{n-1}]$ is finite

Thus by transitivity of extension fields

$[K: F] = [K: K_{n-1}] [K_{n-1}: K_{n-2}] ..... [K_2: K_1] [K: F]$ is finite

Which implies that K is a finite extension of F.

We also know that every finite extension of a field is an algebraic extension.

Therefore, K is an algebraic extension of F.

4 : MULTIPLE OF A ROOT

4.1 Introduction:

It is the largest positive integer of the power of the linear factor for a root of the polynomial in a field.

4.2 Definition:

Multiple roots : Let f(x) be a polynomial in F[x] and K be a Splitting field of f(x). If α be a root of f(x) then $(x- \alpha) | f(x)$ over K. If m is the largest positive integer for which $(x- \alpha)^m | f(x)$ in K[x], then m is called the multiple of α.

4.3 Theorems:

Theorem (4.3) 1 : Let K be an extension of a field F and f(x) be a polynomial of positive degree over F. Then $\alpha \in K$ is a multiple root of f(x) if and only if α is a common root of f(x) and f '(x).

Proof :- Let f(x) be a polynomial of positive degree over F.

Also let α be a multiple root of f(x), m be the multiplicity so that $m \geq \alpha$ then $f(x) = (x - \alpha)^m g(x)$, $g(\alpha) \neq 0$, $g(x) \in K[x]$.

Also, $f'(x) = m(x - 2)^{m-1} g(x) + (x - \alpha)^m g'(x) \Rightarrow f'(\alpha) = 0$

Thus α is a common root of $f(x) = 0$ and $f'(x) = 0$

Conversely, let α be the common root of f(x) & f'(x)

To show that α is a multiple root of f(x).

If possible, let for a moment α is the simple root of f(x).

Then $f(x) = (x - \alpha) g(x)$, for $g(x) \in K[x]$ and $g(\alpha) \neq 0$

Again, $f(x) = g(x) + (x - \alpha) g(x) \Rightarrow f(\alpha) = g(\alpha) + 0 = g(\alpha) \neq 0$

Then α is not a common root of $f(x) = 0$ and $f'(x) = 0$

This goes against out assumption that α is the common root of f(x) & f'(x)

Thus α is not simple.

Hence, α is a multiple root of f(x).

Theorem (4.3) 2 : Let F be a field of characteristic 0 (zero) and if a, b are algebraic over F, then $\exists$ an element $c \in F[a, b]$ such that $F[a, b] = F(c)$

That is F [a, b] is a simple extension

Proof :- Let a and b be any two elements algebraic over F.

Also let f(x) and g(x) be the irreducible polynomials over F such that a, b satisfy (x) and g(x) respectively.

Also let deg. f(x) = m and deg. g(x) = n.

Let K be an extension of F such that f(x) and g(x) split completely.

Since f(x) is irreducible and characteristic of F = 0

Then by a theorem all roots of f(x) must be distinct.

In a similar way all roots of g(x) will also be distinct.

Let the roots of f(x) be $a_1, a_2, \ldots\ldots, a_m$ and

the roots of g(x) be $b_1, b_2, \ldots\ldots, b_n$

We now write $a_1 = a$ and $b_1 = b$ for our convenience

Also in K we have $a_i + \lambda\, b_j = a + \lambda\, b$ where i = 1, 2, ... , m and j = 1, 2, ... , n

Then $\lambda = a_i - a \,/\, b_j - b$ is an unique element of K.

In this way for each pair of valued i and j ($j \neq 1$) equation $a_i + \lambda\, b_j = a + \lambda\, b$ has only one solution in K.

Also F contain an infinite number of elements and its characteristic is zero.

Let finite number of elements such that $a_i + \lambda\, b_j = a + \lambda\, b$ are in E

Thus we shall get an element t in F such that $a_i + t\, b_j \neq a + t\, b$ for all i and for all $j \neq 1$

Let c = a + t b and a, b, $t \in F$ [a, b] => $c \in F$ [a, b]

To show that F (a, b) = F (c)

Also $c \in F$ (a, b) => F (c) $\subseteq$ F (a, b) ---------- (1)

Now let a, b $\in$ F (a, b)

Also b satisfies g(x) over F => g(x) can be regarded as over F(c)

Let F(c) = K and h(x) = f (c – tx)

Since c $\in$ K and t $\in$ F => t $\in$ K => h(x) is polynomial in K [x]

Hence h(b) = f (c – tb) = f(a) = 0

It means b satisfies g(x) and h(x) both in K [x]

Implies that (x – b) is a common factor in some extension E of K.

We need to show that (x – b) is the g.c.d of g(x) and λ(x) in K[x].

For this, let $b_j \neq b$ another root of g(x) then $h(b_j) = f(c - t\, b_j) \neq 0$

- ⇨ b_j is not a root of h(x).
- ⇨ If any factor of g(x) in E(x) ≠ (x – b) is not a factor of h(x).

Also g(x) has all distinct roots => $(x - b)^r$, $r \geq 2$ is not a divisor of g(x)

Thus (x – b) is the g.c.d of g(x) and h(x) in the extension E of K.

Also g(x) and h(x) have non-trivial factor over E so g(x) and h(x) will have on K also.

It means they must have common and non-trivial factor over K.

Thus they must have a non-trivial g.c.d over K which must be a divisor of(x – b).

But degree of (x – b) is one. Hence (x – b) is itself g.c.d of g(x) and h(x) in K[x]. Then $b \in K = f(c)$

Again c, t, $b \in F(c) \Rightarrow c - tb \in F(c) \Rightarrow a \in F(c) \Rightarrow a, b \in F(c)$

Now $a, b \in F(c) \Rightarrow F(a, b) \subseteq F(c) \Rightarrow F[a, b] \subseteq F(c)$ ---------- (2)

Thus from (1) and (2) we can conclude that

$F(a, b) = F(c)$

Theorem (4.3) 3 : Any finite extension of a field of characteristic 0 (zero) is a simple extension.

Proof :- Let K be a finite extension of a field F which characteristic is 0 (zero).

Then K is algebraic extension of F.

Thus in this situation we can obtain we can obtain K by adjoining a finite number of algebraic elements of F.

Let $K = F[\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n]$

We have to show that $\exists$ an element c in K such that K = F(c) .

For this,

We consider $K = F(\alpha_1, \alpha_2, ..., \alpha_{n-2}, \alpha_{n-1}, \alpha_n)$

$= (F(\alpha_1, \alpha_2, ..., \alpha_{n-2}))(\alpha_{n-1}, \alpha_n) = (F(\alpha_1, \alpha_2, ..., \alpha_{n-2}))$

Where $d \in (F(\alpha_1, \alpha_2, ..., \alpha_{n-2}))(\alpha_{n-1}, \alpha_n) = F(\alpha_1, \alpha_2, ..., \alpha_{n-1}, \alpha_n) = K$ [By a theorem]

$= F(\alpha_1, \alpha_2, ..., \alpha_{n-1}, d)$

Thus by a theorem

K = F(c), where $c \in F(c) = K$

Thus, K is a simple extension of F.

5 : Solved Examples

Example 1 : If $a \in K$ is algebraic over F of odd degree

Show that $F(a) = F(a^2)$

Solution : Since a is an algebraic element of odd degree over F, so F(a) is the extension of F of odd degree.

F(a) is a field so $a \in F(a)$ implies that $a^2 \in F(a)$, thus a^2 is algebraic over F and $F(a^2) \subseteq F(a)$. As a is a root of the polynomial $x^2 - a^2$ with coefficients in $F(a^2)$, so a is algebraic of degree at most 2 over $F(a^2)$ i.e $[F(a) : F(a^2)] \leq 2$.

More over $[F(a) : F] = [F(a) : F(a^2)] [F(a^2) : F]$

$\Rightarrow$ $[F(a) : F(a^2)] [F(a) : F]$

But $[F(a) : F(a^2)] \leq 2$ and $[F(a) : F]$ is odd, then we must have $[F(a) : F(a^2)] = 1$

Hence $F(a) = F(a^2)$

Example 2 : Describe the splitting field of $x^3 - 2$ over Q, the field of rationals.

Solution : Let $f(x) = x^3 - 2$

If f(x) is reducible over Q, the f(x) has a rational root.

Let it be m/n, ($n \neq 0$), (m, n) = 1.

$m^3 = 2 n^3 \Rightarrow 2 \mid m^3 \Rightarrow 2 \mid m \Rightarrow m = 2K \Rightarrow 8K^3 = 2 n^3 \Rightarrow 4K^3 = n^3 \Rightarrow 2 \mid n^3 \Rightarrow 2 \mid n$

$2 \mid (m, n) = 1$ is a contradiction.

Thus f(x) is not reducible over Q.

Hence f(x) is irreducible over Q.

Now let a be a root of f(x) such that a is real.

Hence $(x^3 - a) = (x - a)(x^2 + ax + a^2) = (x - a)(x - a\omega)(x - a\omega^2)$

Where $\omega = -1 \pm \sqrt{3}\, i / 2$

Hence splitting field of f(x) over Q is $K = Q(a, a\omega, a\omega^2) = Q(a, \sqrt{3}\, i)$

Now $Q \subseteq Q(a) \subseteq K$

Since f(x) = 3, $[K : Q] \leq \lfloor 3 = 6$.

Since a is real Q(a) is subfield of real numbers, while K is a subfield of complex numbers as $\sqrt{3}\, i \in K$.

Thus $K \neq Q(a)$ then $[K : Q(a)] \geq 2$

But $[Q(a) : Q]$ = degree irreducible (Q, a) = deg. $f(x) = 3$

Thus $[K : Q] = [K : Q(a)] [Q(a) : Q] \geq 6$.

Hence $[K : Q] = 6$.

Example 3 : Let $f(x) = x^4 + x^2 + 1 \in Q[x]$.show that the splitting field of f(x) over Q is $Q(\omega)$ and $[Q(\omega) : Q] = 2$

Solution : Since $\omega^2 + \omega + 1 = 0$

Or, $\omega^4 + \omega^3 + \omega^2 = 0$

$\therefore$ ω is a root of $x^4 + x^2 + 1$

$\therefore$ $-\omega$ is also a root of $x^4 + x^2 + 1$

$\therefore$ $f(x) = x^4 + x^2 + 1 = (x^2 - \omega^2)(x^2 - \omega)$

$= (x^2 - \omega^2)(x^2 - \omega^4)$ as $\omega^4 = \omega$

$= (x - \omega)(x + \omega)(x - \omega^2)(x + \omega^2)$

$\therefore$ splitting field of $x^4 + x^2 + 1$ over Q is $Q(\omega, -\omega, \omega^2, -\omega^2) = Q(\omega)$.

Example 4 : Show that the splitting field of $x^4 + 1$ over Q is $Q(\sqrt{2}, i)$ whose degree over Q is 4.

Solution : Since roots of $x^4 + 1$ is given by:

$x = (-1)^{1/4} = (\cos (2r + 1) \prod + i \sin (2r + 1) \prod)^{1/4}$, r = 0, 1, 2, 3.

$= \cos (2r + 1) \prod / 4 + i \sin (2r + 1) \prod / 4$, r = 0, 1, 2, 3.

$= 1 / \sqrt{2} (1 + i)$, $- 1 / \sqrt{2} (1 - i)$, $- 1 / \sqrt{2} (1 + i)$, $1 / \sqrt{2} (1 - i)$

Thus splitting field K of $x^4 + 1$ over Q is $K = Q (\pm 1 / \sqrt{2} (1 + i), \pm 1 / \sqrt{2} (1 - i)) = Q (\sqrt{2}, i)$

As $2 \in Q \subseteq K$, $1 / \sqrt{2} (1 + i) \in K \Rightarrow \sqrt{2}(1 + i) \in K$

Also $- \sqrt{2} + \sqrt{2}\, i \in K$

Hence $2 \sqrt{2}\, i \in K \Rightarrow \sqrt{2}\, i \in K$ but $1 / \sqrt{2} (1 - i) \in K \Rightarrow i (1 - i) \in K$

$\Rightarrow i + 1 \in K \Rightarrow i \in K \Rightarrow \sqrt{2} \in K \Rightarrow Q(\sqrt{2}, i) \subseteq K$

Again $\sqrt{2}, i \in Q(\sqrt{2}, i) \Rightarrow \pm 1/\sqrt{2}(1+i), \pm 1/\sqrt{2}(1-i) \in Q(\sqrt{2}, i)$

⇨ $K \subseteq Q(\sqrt{2}, i) \Rightarrow K = Q(\sqrt{2}, i)$

Also $Q \subseteq Q(\sqrt{2}) \subseteq Q(\sqrt{2}, i)$ and $x^2 + 1 \in Q(\sqrt{2})[x]$ is irreducible over $Q(\sqrt{2})$.

⇨ $[Q(\sqrt{2}, i) : Q(\sqrt{2})]$ = degree irreducible $(Q\sqrt{2}, i) = 2$ as i satisfies $x^2 + 1$

But $[Q(\sqrt{2}) : Q]$ = degree irreducible $(Q, \sqrt{2})$ = degree $(x^2 - 2) = 2$

Hence $[K : Q] = [K : Q(\sqrt{2})][Q(\sqrt{2}) : Q] = 2 \cdot 2 = 4$.

Example 5(2018) : Find necessary and sufficient conditions a and b so that the splitting field of irreducible cubic $x^3 + ax + b$ has degree 3 over Q.

Solution : Let $f(x) = x^3 + ax + b \in Q[x]$

Let K be splitting field of f(x) over Q and

$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ then $K = Q(\alpha_1, \alpha_2, \alpha_3)$

Now $\alpha_1 + \alpha_2 + \alpha_3 = 0$, $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = a$, $\alpha_1\alpha_2\alpha_3 = -b$

Let $D = [(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)]^2$

Then $D = -4a^3 - 27b^2$

Now $Q(\sqrt{D}, \alpha_3) \subseteq K$ as $\alpha_1, \alpha_2, \alpha_3 \in K \Rightarrow \alpha_1 - \alpha_2, \alpha_2 - \alpha_3, \alpha_3 - \alpha_1 \in K$

⇨ $(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in K \Rightarrow \sqrt{D} \in K$, also $\alpha_3 \in K$

⇨ $Q(\sqrt{D}, \alpha_3) \subseteq K$

Now $\sqrt{D} = (\alpha_1 - \alpha_2)[\alpha_3(\alpha_1 + \alpha_2) - \alpha_3^2 - \alpha_1\alpha_2] \in Q(\sqrt{D}, \alpha_3)$

Since $\alpha_1\alpha_2 = -b/\alpha_3 \in Q(\sqrt{D}, \alpha_3)$ and $\alpha_1 + \alpha_2 = -\alpha_3 \in Q(\sqrt{D}, \alpha_3)$

$\alpha_1 - \alpha_2 \in Q(\sqrt{D}, \alpha_3) \Rightarrow \alpha_1, \alpha_2 \in Q(\sqrt{D}, \alpha_3)$

Thus $K \subseteq Q(\sqrt{D}, \alpha_3) \Rightarrow K = Q(\sqrt{D}, \alpha_3)$

Now let $\sqrt{D} \in Q$ then $K = Q(\alpha_3)$

Thus $[K : Q] = [Q(\alpha_3) : Q]$ = degree irreducible (Q, α_3) = deg. $f(x) = 3$.

Conversely : Let [K : Q] = 3

Let $\sqrt{D} \notin Q$ then $Q \subseteq Q(\sqrt{D}) \subseteq Q(\sqrt{D}, \alpha_3) = K$

But $\sqrt{D}$ satisfies $x^2 - D \in Q[x]$

Thus $[Q(\sqrt{D}) : Q] = 2$ as $x^2 - D$ is irreducible over Q

Also $[K : Q] = [K : Q(\sqrt{D})] [Q(\sqrt{D}) : Q]$

$3 = [K : Q(\sqrt{D})] 2$ is a contradiction $\Rightarrow \sqrt{D} = Q$

Therefore a necessary sufficient condition for the splitting field of irreducible cubic $x^3 + ax + b$ over Q to have degree 3 is $\sqrt{D} \in Q$.