16/Aug/21

PAGE NO. :
DATE : / /

Ring :- A non-empty set R, together with two binary operations + and × is called a ring if it satisfies following properties -

(i) $(R, +)$ is an additive abelian group
under Addition - closure, Associative, Existence of Identity, Existence of Inverse, Commutative.

(ii) $(R, \times)$ is a multiplicative semi-group

(iii) Multiplication is distributive over addition, that is, for all $a, b, c \in R$

$$a \times (b+c) = a \times b + a \times c$$
$$(b+c) \times a = b \times a + c \times a$$

(The two distributive laws are respectively called the left distributive law and the right distributive law)

Examples :- (1) $(\mathbb{Z}, +, \times)$
(2) $(\mathbb{Q}, +, \times)$
(3) $(\mathbb{R}, +, \times)$
(4) $(\mathbb{C}, +, \times)$
(5) $(\mathbb{Z}_n, +_n, \times_n)$ ⇒ A ring with finite number of elements: the ring of Integers modulo n.

- Ring with Identity = Ring + (3)
- Commutative Ring with Identity = Ring + (3) + (5)
- Commutative Ring = Ring + (5)
- Division Ring = Ring + (4) + (3)
  Whenever (4) property is there then (3) will be there
- Field = Ring + (3) + (4) + (5)

$(R, +, \times)$
3. Identity
4. Inverse
5. Comm. under '×'

Scanned with CamScanner

PAGE NO. :
DATE : / /

17/Aug

Ring+(3)+(5) ⇒ Set of real numbers, Rational numbers, Integers form rings w.r.t usual addition and multiplication. These are all commutative rings with unity.

Z_n is always commutative ring with identity $\forall n$

Ring+(5) ⇒ (1) Set E of all even Integeres forms a commutative ring without unity. (2) $(nZ, +, \times)$ where $n \neq \pm 1$

Ring+(5) ⇒ $M = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} ; a, b \in \mathbb{C} \right\}$ forms a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ but it is not commutative.

Ring+(3)+(4)+(5) ⇒ 1. $(\mathbb{Q}, +, \times), (R, +, \times), (\mathbb{C}, +, \times)$

2. $(Z_n, +_n, \times_n)$ is field iff n is prime.

Ring+(3)+(4) ⇒ $\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in R \}$ with $i^2 = j^2 = k^2 = -1$ then $\mathbb{H}$ forms a Ring. This Ring $\mathbb{H}$ is called the ring of quaternions.

- $(Z_3, +_3, \times_3)$

  $Z_3 = \{0, 1, 2\}$

  $a \times_3 b \equiv r \pmod 3$

  s.t $a * e = a = e * a$ Here $e = 1$

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- $Z_n = \{0, 1, 2, \ldots, n-1\}$, $n \geq 2$

  $a \times_n b = ab \pmod n$

  $= ba \pmod n$

  $= b \times_n a$

- $Z_4 = \{0, 1, 2, 3\}$

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Scanned with CamScanner

17/Aug/21

PAGE NO. :
DATE : / /

Polynomial Rings :- Let R be a ring. Consider

$$R[x] = \{ f(x) = a_0 + a_1x + \dots + a_nx^n ;\ n \geq 0;\ a_i \in R \}$$

for $f(x), g(x) \in R[x]$

$f(x) = a_0 + a_1x + \dots + a_nx^n$; $n \geq 0$; a_i's $\in R$

$g(x) = b_0 + b_1x + \dots + b_mx^m$; $m \geq 0$; b_j's $\in R$

define $f(x) + g(x) = (a_0+b_0) + (a_1+b_1)x + \dots$

$f(x) \cdot g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \dots + (a_nb_m)x^{m+n}$

- $R = \mathbb{Z}$

$\mathbb{Z}[x] = \{ a_0 + a_1x + \dots + a_nx^n ;\ n \geq 0,\ a_i \in \mathbb{Z}\ \forall i \}$

Eg :- $\mathbb{Z}_4[x]$

$f(x) = 2 + 3x + 2x^2$

$g(x) = 2 + 2x + 3x^2$

$f(x) + g(x) = 0 + x + x^2$

$f(x) \cdot g(x) = 2x^2 + 2x + 2x^2 + x^3 + 2x^4$

$= 2x + x^3 + 2x^4$

$R[x] = \{ f(x) = a_0 + a_1x + \dots + a_nx^n ;\ n \geq 0;\ a_i \in R \}$

T.P :- $R[x]$ is a ring

(i) $(R[x], +)$ is an abelian group

(a) closure property :

let $f(x) = a_0 + a_1x + \dots + a_nx^n$, $a_i \in R$

$g(x) = b_0 + b_1x + \dots + b_mx^m$, $b_j \in R$ $\Big] \in R[x]$

Here $m \leq n$ & $m, n \geq 0$

$f(x) + g(x) = (a_0+b_0) + (a_1+b_1)x + \dots + (a_m+b_m)x^m + \dots + a_nx^n \in R[x]$

$\therefore$ closure property holds

Scanned with CamScanner

PAGE NO. :
DATE : / /

(b) **Associative property :-** let $f(x)$, $g(x)$ and $h(x) \in R[x]$

T.P :- $(f(x)+g(x))+h(x) = f(x)+(g(x)+h(x))$

Here $f(x) = a_0+a_1x+\dots+a_rx^r+\dots+a_tx^t$, $a_i=0\ \forall i>r$

$g(x) = b_0+b_1x+\dots+b_sx^s+\dots b_tx^t$, $b_j=0\ \forall j>s$

$h(x) = c_0+c_1x+\dots+c_tx^t$

let $r \le s \le t$

L.H.S :- $(f(x)+g(x))+h(x)$

$= [(a_0+b_0)+\dots+(a_t+b_t)x^t]+[c_0+c_1x+\dots+c_tx^t]$

$= [(a_0+b_0)+c_0]+[(a_1+b_1)+c_1]x+\dots+[(a_t+b_t)+c_t]x^t$

$= [a_0+(b_0+c_0)]+[a_1+(b_1+c_1)]x+\dots+[a_t+(b_t+c_t)]x^t$

Associative property holds

(c) **Existence of Identity :-**

let $f(x) = a_0+a_1x+a_2x^2+\dots+a_nx^n$

and $e(x) = 0_R+0_Rx+0_Rx^2+\dots+0_Rx^n$, 0_R is Identity of R

To prove :- $f(x)+e(x)=f(x)$

L.H.S $f(x)+e(x) = (a_0+0_R)+(a_1+0_R)x+(a_2+0_R)x^2+\dots$

$+(a_n+0_R)x^n$

$= a_0+a_1x+a_2x^2+\dots+a_nx^n$

$= f(x)$

$\therefore$ Identity of $(R[x],+)$ exists and it is $e(x)$ here

(d) **Existence of Inverse :-**

$f(x)+p(x)=0$

$p(x) = -f(x)$

$\therefore$ Inverse is $-a_0-a_1x-\dots-a_nx^n$

$f(x)+(-f(x)) = (a_0+a_1x+\dots+a_nx^n)+(-a_0-a_1x-\dots-a_nx^n)$

$= (a_0-a_0)+(a_1-a_1)x+\dots(a_n-a_n)x^n$

$= 0+0x+\dots+0x^n$

$= 0(x)$

(e) Commutative law :-

(ii

Scanned with CamScanner

PAGE NO. :
DATE : / /

Let $f(x), g(x) \in R[x]$ where $f(x) = a_0 + a_1x + \dots + a_nx^n$, $a_i \in R$
$g(x) = b_0 + b_1x + \dots + b_mx^m$, $b_i \in R$
where $m \le n$ & $m, n \ge 0$

T.P :- $f(x) + g(x) = g(x) + f(x)$

L.H.S :- $f(x) + g(x) = (a_0+b_0) + (a_1+b_1)x + \dots + (a_m+b_m)x^m + \dots + a_nx^n \in R[x]$

As $(R, +, \cdot)$ = Ring
$(R, +) \rightarrow$ Abelian Ring
$\forall a_i, b_i \in R$
$\Rightarrow a_i + b_i = b_i + a_i$

$= (b_0+a_0) + (b_1+a_1)x + \dots + (b_m+a_m)x^m + \dots + a_nx^n \in R[x]$
$= (b_0 + b_1x + \dots + b_mx^m) + (a_0 + a_1x + \dots + a_mx^m + a_nx^n)$
$= g(x) + f(x)$
$= R.H.S$
$\Rightarrow (R[x], +)$ is abelian group

(ii) $(R[x], \cdot)$ is Semi-group

(a) closure property :- let $f(x), g(x) \in R[x]$
T.P :- $f(x) \cdot g(x) \in R[x]$

$f(x) \cdot g(x) = (a_0 + a_1x + \dots + a_tx^t) \cdot (b_0 + b_1x + \dots + b_tx^t)$
$= a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \dots + (a_tb_t)x^t$

$\{(R, +, \cdot)$ Ring, $(R, \cdot) \rightarrow$ Semigp As $a_0, b_0, a_1, b_1, a_2, b_2 \dots \in R$
$a_0b_0, a_1b_0 + a_0b_1 \dots \in R\}$
$f(x) \cdot g(x) \in R[x]$

(b) Associative property :- let $f(x), g(x), h(x) \in R[x]$
T.P :- $[f(x) \cdot g(x)] \cdot h(x) = f(x) \cdot [g(x) \cdot h(x)]$

L.H.S :- $[f(x) \cdot g(x)] \cdot h(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \dots + (a_tb_t)x^t \cdot (c_0 + c_1x + \dots + c_tx^t)$
$= a_0b_0c_0 + (a_1b_0c_0 + a_0b_1c_1)x + \dots + (a_tb_tc_t)x^t$
$= d_0 + d_1x + \dots + d_kx^k$, $d_k \ge 0$ $\forall k > x$

Scanned with CamScanner

PAGE NO. :
DATE : / /

$= (a_0 + a_1x + \dots + a_tx^t) \cdot (b_0c_0 + b_1c_1)x + \dots + b_tc_t)x^t$

$= f(x) \cdot [g(x) \cdot h(x)]$

$(R[x], \cdot)$ is semi-group

(ii) $(R[x], +, \cdot)$ is distributive

let $f(x), g(x), h(x) \in R[x]$

$f(x) \cdot [g(x) + h(x)] = f(x) \cdot g(x) + f(x) \cdot h(x)$

L.H.S :- $f(x) \cdot [g(x) + h(x)] = (a_0 + a_1x + \dots + a_tx^t) +$
$[(b_0+c_0) + (b_1+c_1)x + \dots + (b_t+c_t)x^t]$

$= a_0(b_0+c_0) + a_1(b_1+c_1)x + \dots + a_t(b_t+c_t)x^t$
$= [a_0b_0 + (a_1b_1)x + \dots + (a_tb_t)x^t] + [a_0c_0 + (a_1c_1)x$
$+ \dots + (a_tc_t)x^t]$
$= f(x) \cdot g(x) + f(x) \cdot h(x)$
$= R.H.S$

Similarly, we can show that

$[f(x) + g(x)] \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x)$

L.H.S $[f(x) + g(x)] \cdot h(x) = [(a_0+b_0) + (a_1+b_1)x + \dots + (a_t+b_t)x^t] \cdot$
$(c_0 + c_1x + \dots + c_tx^t]$
$= (a_0+b_0)c_0 + (a_1+b_1)c_1x + \dots c_t(a_t+b_t)x^t$
$= [a_0c_0 + (a_1c_1)x + \dots + (a_tc_t)x^t] +$
$[b_0c_0 + (b_1c_1)x + \dots + (b_tc_t)x^t]$
$= f(x) \cdot h(x) + g(x) \cdot h(x)$
$= R.H.S$

In this way $R[x]$ is a ring called polynomial Ring.

Scanned with CamScanner

PAGE NO. :
DATE : / /

Property :- 1. Let R be a ring with identity. Is R[x] also a ring with identity?

proof :- ⇒ ∃ e∈R s.t.

$ae = a = ea \quad \forall a \in R$

$f(x) \in R[x]$

$f(x)\,e(x) = f(x) = e(x)\,f(x)$

$f(x).\ e = f(x) = e.f(x)$

$a_0e + a_1ex + \dots + a_nex^n$ $\quad e \in \mathbb{Z}$

$= a_0 + a_1x + \dots + a_nx^n$ $\quad e \in \mathbb{Z}[x]$

$= f(x)$

Yes, R[x] also a ring with identity.

Converse :- Let R[x] has identity e(x) (say)

Let $e(x) = e_0 + e_1x + e_2x^2 + \dots + e_mx^m$; $e_i \in R, m \geq 0$

and we have

$f(x).\ e(x) = e(x)\,f(x) = f(x) \quad \forall f(x) \in R[x]$

$a_0e_0 + (a_1e_0 + a_0e_1)x + \dots + a_ne_mx^{n+m} = a_0 + a_1x + \dots$

$\dots + a_nx^n = e_0a_0 + (e_1a_0 + e_0a_1)x + \dots + e_ma_nx^{n+m}$

$\Rightarrow a_0e_0 = a_0 = e_0a_0 \quad \forall a_0 \in R$

$\Rightarrow e_0 = e(0)$ is identity of R

Therefore, converse is also true.

(2) Is R is commutative, Is R[x] also commutative? what about converse?

proof :- (⇐) $R \subseteq R[x]$

$a, b \in R \Rightarrow a, b \in R[x] \Rightarrow ab = ba$ as R[x] is commutative

$\Rightarrow$ R is commutative

Converse True

(⇒) Let R be commutative

Let $f(x), g(x) \in R[x]$

T.P :- $f(x)g(x) = g(x)f(x)$

Scanned with CamScanner

Here $f(x) = a_0 + a_1x + \dots + a_nx^n$

$g(x) = b_0 + b_1x + \dots + b_mx^m$

$f(x)g(x) = (a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)$

$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_0 + a_0b_2 + a_1b_1)x^2 + \dots$

$\dots + a_nb_mx^{n+m}$

$g(x)f(x) = (b_0 + b_1x + b_2x^2 + \dots + b_mx^m)(a_0 + a_1x + \dots + a_nx^n)$

$= b_0a_0 + (b_1a_0 + b_0a_1)x + (b_0a_2 + b_2a_0 + b_1a_1)x^2 + \dots +$

$b_ma_nx^{m+n}$

on comparing the coefficients

$a_0b_0 = b_0a_0$

$a_0b_1 + a_1b_0 = b_1a_0 + b_0a_1$

$\Rightarrow R[x]$ is commutative.

24/Aug

(i) R is Ring with identity iff $R[x]$ is ring with identity.
(ii) R is commutative iff $R[x]$ is commutative.
(iii) If R is a field, is $R[x]$ also a field? What about converse?

Eg:-

$f(x) = 1 + 2x + 3x^2$

$g(x) = 2x + x^2 + 2x^3$

- what is the degree of $f(x)+g(x)$?

Ans 3

- what is the degree of $f(x)\cdot g(x)$?

Ans 5

- If $R[x] = \mathbb{Z}[x]$ then answer is same for $f(x)+g(x)$ and $f(x)\cdot g(x)$.

- If $R[x] = \mathbb{Z}_4[x]$ then

$f(x)+g(x) = 1 + 4x + 4x^2 + 2x^3 = 1 + 2x^3$

$\deg(f(x)+g(x)) = 3$

Scanned with CamScanner

PAGE NO. :
DATE : / /

$f(x)g(x) = 2x + x^2 + 2x^3 + 4x^2 + 2x^3 + 4x^4 + 6x^2 + 3x^4 + 6x^5$

$= 2x + 3x^2 + 3x^4 + 2x^5$

$\deg(f(x) \cdot g(x)) = 5$

- If $R[x] = \mathbb{Z}_6[x]$ then

  $\deg(f(x) + g(x)) = 3$

  $\deg(f(x) \cdot g(x)) = 4$

Thm :- Let $R[x]$ be the ring of polynomials over a ring R and suppose

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m$

$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$

are two non-zero polynomials of degree m and n respectively. Then

1. If $f(x) + g(x) \neq 0$, $\deg(f(x) + g(x)) \leq \max(m, n)$
2. If $f(x) \cdot g(x) \neq 0$, $\deg(f(x) \cdot g(x)) \leq m + n$
3. If R is Integral domain, $\deg(f(x) \cdot g(x)) = m + n$
4. R is an Integral domain iff $R[x]$ is an Integral domain.

Proof :- 1. $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_t + b_t)x^t$

where $t = \max.(m, n)$

and $a_k + b_k = 0 \ \forall k > t$

Rough

$f(x) = a_0 + a_1x + \dots + a_{10}x^{10}$

$g(x) = b_0 + b_1x + \dots + b_8x^8 + 0 \cdot x^9 + 0 \cdot x^{10}$

$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_8 + b_8)x^8 + (a_9 + b_9)x^9 + (a_{10} + b_{10})x^{10}$

$b_9 = 0$, $b_{10} = 0$

$\max(m, n) = \max(8, 10)$

$\Rightarrow \deg(f(x) + g(x)) \leq t$

depending on whether $a_t + b_t = 0$ or non-zero.

$\Rightarrow \deg(f(x) + g(x)) \leq \max(m, n)$

We also give an example for both the cases.

Scanned with CamScanner

PAGE NO. :
DATE : / /

- $f(x) = 1+2x-2x^2$
  $g(x) = 2+3x+2x^2$ in $\mathbb{Z}[x]$
  $f(x)+g(x) = 3+5x+2x^2-2x^2 = 3+5x$
  $\deg(f(x)+g(x)) = 1 < \max(2,2) = 2$

- $f(x) = 1+2x+2x^2+3x^3$
  $g(x) = 2+3x+2x^2$ in $\mathbb{Z}[x]$
  $\deg(f(x)+g(x)) = 3+5x+4x^2+3x^3$
  $= 3 = \max(3,2) = 3$

2. $f(x)\,g(x) = a_0b_0 + (a_0b_1+b_1a_0)x + (a_0b_2+a_1b_1+a_2b_0)x^2 +$
   $\ldots + (a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots + a_kb_0)x^k + \ldots + a_mb_nx^{m+n}$ ← (*)

   $\deg(f(x)\cdot g(x)) \leq m+n$ depending on $a_mb_n = 0$ or non-zero

   Example– $f(x) = 1+2x$
   $g(x) = 1+3x^2$ in $\mathbb{Z}[x]$
   $\deg(f(x)\cdot g(x)) = 3$

- $f(x) = 1+2x$, $g(x) = 1+3x^2$ in $\mathbb{Z}_6[x]$
  $\deg(f(x)\cdot g(x)) = \deg(1+2x+3x^2+6x^3)$
  $= \deg(1+2x+3x^2) = 2 \neq 1+2$

Integral – domain :– If $ab=0$ then $a=0$ or $b=0$

- $\mathbb{Z}_6$ not an I.D because
  $2\cdot 3 = 0$
  but $2\neq 0, 3\neq 0$

26/Aug/21

3. If R is Integral domain, then $a_m \neq 0$, $b_n \neq 0$ (given)
   $\Rightarrow a_mb_n \neq 0$
   from (*), $\deg(f(x)\cdot g(x)) = m+n$

Scanned with CamScanner

A non-zero commutative ring with identity is called field i.e. every non-zero element ~~have Inverse~~

PAGE NO. :
DATE : / /

4. Let $R[x]$ be Integral domain

T.P :- R is a Integral domain

Let $a, b \in R \setminus \{0\}$

then $a, b \in R[x] \setminus \{0\}$

$\Rightarrow ab \neq 0$ [$\because R[x]$ is I.D]

hence R is I.D

Converse :- Let R be I.D

Let $f(x), g(x)$ be two non-zero polynomials in $R[x]$

T.P :- $f(x) \cdot g(x) \neq 0$

Let $f(x) \cdot g(x) = 0$

where $f(x) = a_0 + a_1 x + \ldots + a_m x^m$

$g(x) = b_0 + b_1 x + \ldots + b_n x^n$

now $f(x) \cdot g(x) = 0$

$\Rightarrow a_0 b_0 + (a_0 b_1 + b_1 a_0)x + \ldots + (a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0)x^k + \ldots + a_m b_n x^{m+n} = 0$

$\Rightarrow \deg(f(x) \cdot g(x)) = \deg(0) = 0$

$\Rightarrow m + n = 0$

$\Rightarrow m = n = 0$ ($\because m, n$ are non-negative integers)

$\Rightarrow f(x) = a_0$, $g(x) = b_0$

$\Rightarrow a_0$ and b_0 are non-zero

($\because f(x)$ & $g(x)$ are non-zero polynomials)

$\Rightarrow a_0, b_0 \in R \setminus \{0\}$

$\Rightarrow a_0 b_0 \neq 0$ ($\because R$ is I.D)

$\Rightarrow f(x) g(x) \neq 0$

Hence, $R[x]$ is also an I.D.

26/Aug/24

* If R is a field, is $R[x]$ a field?

Let $f(x)$ be a non-zero polynomial in $R[x]$ and $g(x) \in R[x]$ s.t

$f(x)g(x) = e$

↓ Inverse of $f(x)$

PAGE NO. :
DATE : / /

$$\deg(f(x).g(x)) = \deg(e)$$
$$\Rightarrow \deg f(x) + \deg g(x) = 0$$
$$\Rightarrow \deg f(x) = 0 = \deg g(x)$$

So, the only invertible elements in $R[x]$ are the Invertible elements of R.
Hence, $R[x]$ is not a field.

- $R[x]$ Cannever be field so we cannot thing about the converse part.

- F: Ring $F[x]$ — F: Ring with id $F[x]$ — F: Comm Ring with id $F[x]$ — Field F $F[x]$ ✗

Division Algorithm for polynomials over field.

Thm:- Let F be a field. For $f(x), g(x) \in F[x]$ where $g(x) \neq 0$ $\exists$ unique $q(x)$ and $r(x)$ s.t $f(x) = g(x)q(x) + r(x)$ where either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$

proof:- Case1:- If $\deg f(x) < \deg g(x)$
then $f(x) = 0 \cdot g(x) + f(x)$
taking $q(x) = 0$, $r(x) = f(x)$
the condition is satisfied.

$f(x)$ $\quad$ $g(x)$ $\quad$ $q(x)$ $\quad$ $r(x)$
$x^2+1 = 0 \cdot (x^3+2) + x^2+1$

Case 2:- $\deg f(x) \geq \deg g(x)$
If $\deg f(x) = 1 \Rightarrow f(x) = ax+b$; $a, b \in F$, $a \neq 0$
$\Rightarrow g(x)$ $cx+d$; $c, d \in F$
then $f(x) = \frac{a}{c} g(x) + \left(b - \frac{ad}{c}\right)$ if $c \neq 0$
and $f(x) = \left(\frac{a}{d}x + \frac{b}{d}\right) g(x) = 0$ if $c = 0$

If $c = 0$

$$cx+d \;\overline{)}\; ax+b \;\left(\frac{a}{c}$$
$$ax + \frac{ad}{c}$$
$$b - \frac{ad}{c}$$

So conditions of division algorithm are satisfied.

Eg:-

If Ring is not a field and we choose any arbitrary thing then D.A is not applied.

PAGE NO. :
DATE : / /

Assume that division algorithm for all polynomials whose deg is $< m$

Now assume that deg $f(x) = m$

Let $f(x) = a_0 + a_1x + \dots + a_mx^m$; $a_m \neq 0$

$g(x) = b_0 + b_1x + \dots + b_nx^n$; $b_n \neq 0$, $n \leq m$

If $c = 0$

$$d\overline{)ax+b}\ \left(\frac{a}{d}x + \frac{b}{d}\right.$$

$$\frac{ax - \quad}{b}$$

$$\frac{b}{x}$$

$f_1(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$

$= $ polynomial of deg less than m

$a_m b_n^{-1} x^{m-n} \cdot b_n x^n$

$a_m x^m$

So by Induction $\exists\ q_1(x), r_1(x)$ s.t

$f_1(x) = g(x)\,q_1(x) + r_1(x)$ where either deg $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$

$\Rightarrow f(x) - a_m b_n^{-1} x^{m-n} g(x) = g(x)\,q_1(x) + r_1(x)$

$\Rightarrow f(x) = (a_m b_n^{-1} x^{m-n} + q_1(x))\,g(x) + r_1(x)$

$\Rightarrow f(x) = q(x)\,g(x) + r_1(x)$

where deg $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$

Uniqueness :- Let $f(x) = q_1(x)\,g(x) + r_1(x)$ — ①

and $f(x) = q_2(x)\,g(x) + r_2(x)$ — ②

where $0 \leq$ deg $r_1(x) <$ deg $g(x)$

$0 \leq$ deg $r_2(x) <$ deg $g(x)$

① − ②

$\Rightarrow (q_2(x) - q_1(x))\,g(x) = r_1(x) - r_2(x)$

$\Rightarrow$ deg $(q_2(x) - q_1(x))$ + deg $g(x)$ = deg $(r_1(x) - r_2(x))$

$\Rightarrow$ deg $g(x) \leq$ deg $(r_1(x) - r_2(x))$

⟶ ⟵ Not possible

Eg :- $\mathbb{Z}_6[x]$ — Not a field

$g(x) = 2x + 3$

$f(x) = 3x + 5$

$$2x+3\overline{)3x+5}\ \ 3\cdot 2^{-1}$$

$$2x + \frac{9}{2}$$

It is not possible to divide if we are not working in a field.

Scanned with CamScanner

31/Aug/21

PAGE NO. :
DATE : / /

Associates :- Two elements a and b in a ring R are called associates if ∃ some unit $u \in R$ s.t

$$a = bu, \quad a \sim b$$

Example :- $\mathbb{Z}$

$a \to | \sim -1 \to b$

$a = b(-1)$

$\forall n \mathbb{Z}, a \sim -a \quad \forall a \in \mathbb{Z}$.

$2 \sim 3$?

$2 = 3 \times x$

$\frac{2}{3} = x$

Prime element :- An element $p \in R$ is called a prime element if

(1) p is non-zero, non-unit

(2) If $p | ab$ then either $p | a$ or $p | b$

Example :- In $\mathbb{Z}$, every prime number is a prime element.

Irreducible element :- An element $a \in R$ is called irreducible element if

(i) a is non-zero and non-unit

(ii) If $a = bc$, then either b or c is a unit

Eg :- $2 = (-2)(-1)$

observation :- A prime element is always an irreducible element.

Proof :- Let $a \in R$ be a prime element

Consider $a = bc$ - ① for some $b, c \in R$

$\Rightarrow a | bc \quad \because a = 1.bc$

$\Rightarrow a | b$ or $a | c$

Case 1 :- If $a | b$

$\Rightarrow \exists$ some $x \in R$ s.t

$b = ax$

then from ①, $a = axc$

$\Rightarrow a(1 - xc) = 0$

$r, s \in R$

$r | s$ if $\exists$ some $t \in R$

$s = rt$

Scanned with CamScanner

PAGE NO. :
DATE : / /

$\Rightarrow 1-xc=0$ ($\because a\neq 0$ and R is I.D)

$\Rightarrow xc=1$

$\Rightarrow cx=1$

hence, c is a unit

Case 2:- If $a|c$

$\Rightarrow \exists$ some $y \in R$ s.t

$c=ay$

then from (1)

$a=ayb$

$\Rightarrow a(1-yb)=0$

$\Rightarrow 1-yb=0$ ($\because a\neq 0$ and R is I.D)

$\Rightarrow yb=1$

$\Rightarrow by=1$

hence, b is a unit

Converese:- Not always true

Eg:- $\mathbb{Z}[\sqrt{-5}]=\{a+\sqrt{-5}b;\ a,b\in\mathbb{Z}\}$

$\mathbb{Z}\subseteq\mathbb{Z}[\sqrt{-5}]$

Let $(a+\sqrt{-5}b)(c+\sqrt{-5}d)=0$

$(a-\sqrt{-5}b)(c-\sqrt{-5}d)=0$

$(a^2+5b^2)(c^2+5d^2)=0$

$\Rightarrow$ either $a^2+5b^2=0$ or $c^2+5d^2=0$

$a=0, b=0$ or $c=d=0$

hence either $a+\sqrt{-5}b=0$ or $c+\sqrt{-5}d=0$

$\Rightarrow \mathbb{Z}[\sqrt{-5}]$ is integral domain

For finding units

Let $(a+\sqrt{-5}b)(c+\sqrt{-5}d)=1$

$(a-\sqrt{-5}b)(c-\sqrt{-5}d)=1$

$(a^2+5b^2)(c^2+5d^2)=1$

$\Rightarrow a^2+5b^2=1$ or $c^2+5d^2=1$

Scanned with CamScanner

$a=\pm1, b=0$ or $d=0, c=\pm1$

$a+\sqrt{-5}b = \pm1$ are units of $\mathbb{Z}[\sqrt{-5}]$

Example :- $\mathbb{Z}[\sqrt{-5}] = \{a+\sqrt{-5}b ; a,b \in \mathbb{Z}\}$

Let $2+\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

T.P :- $2+\sqrt{-5}$ is irreducible

Let $2+\sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$2-\sqrt{-5} = (a-b\sqrt{-5})(c-d\sqrt{-5})$

$9 = (a^2+5b^2)(c^2+5d^2)$

Case 1 :- $a^2+5b^2=1$, $c^2+5d^2=9$

$\Rightarrow a^2+5b^2=1$

$\Rightarrow b=0, a=\pm1$

$\Rightarrow x$ is unit

Case 2 :- $a^2+5b^2=3=c^2+5d^2$

$a^2+5b^2=3$

If $b\neq0 \Rightarrow b^2\geq1$

$\Rightarrow 5b^2\geq5$

$\Rightarrow a^2+5b^2\geq5$

$\Rightarrow 3\geq5$

$\rightarrow\leftarrow$

$\Rightarrow b^2=0$

$\Rightarrow a^2=3$

not possible

Case 3 :- $a^2+5b^2=9$, $c^2+5d^2=1$

$\Rightarrow c^2+5d^2=1$

$\Rightarrow d=0, c=\pm1$

$\Rightarrow y$ is unit

Hence, $2+\sqrt{-5}$ is irreducible

Claim :- $2+\sqrt{-5}$ is not prime element

Now $2+\sqrt{-5} \mid 9$

as $9 = (2+\sqrt{-5})(2-\sqrt{-5})$

$\Rightarrow 2+\sqrt{-5} \mid 3.3$

If possible assume that $(2+\sqrt{-5}) \mid 3$

Scanned with CamScanner

$\Rightarrow 3 = (2+\sqrt{-5})(x+\sqrt{-5}y)$ — (*) for some $x, y \in \mathbb{Z}$

$\Rightarrow 3 = (2-\sqrt{-5})(x-\sqrt{-5}y)$

$\Rightarrow 9 = 9(x^2+5y^2)$

$\Rightarrow 9[1-x^2-5y^2] = 0$

$1-x^2-5y^2 = 0$

$\Rightarrow x^2+5y^2 = 1$

$\Rightarrow x = \pm 1, y = 0$

from (*)

$3+0\sqrt{-5} = (2+\sqrt{-5})(\pm 1)$

$3 = \pm 2, \pm 1 = 0$

$\rightarrow \leftarrow$

$2+\sqrt{-5}$ is not prime element.

3/Sep/21

Defⁿ :- Let R be an Integral domain (Commutative Ring with Id entity in which product of a non-zero element is non-zero) then R is called unique factorization domain (UFD) if

(i) Every non-zero, non-unit element in R can be written as a finite product of irreducible elements

(ii) If $a \in R$, a is non-zero, non-unit such that

$a = p_1 p_2 \dots p_k$

$= q_1 q_2 \dots q_r$

$6 = 2 \times 3$

$= (-3) \times (-2)$

where p_i's and q_j's are irreducibles in R, then $k = r$ and each $p_i \sim q_j$ for some j.

Example :- Ring of Integers

Thm :- Let R be a UFD, then ~~every~~ an element $a \in R$ is prime iff it is irreducible.

Proof :- Let $a \in R$ be a prime element

as R is UFD $\Rightarrow$ R is an Integral domain $\Rightarrow$ a is irreducible

(to prove)

Scanned with CamScanner

PAGE NO. :
DATE : / /

9/Sep/21

Converse :- Let a be irreducible in R
⇒ a is non-zero, non-unit
assume that ∃ b, c ∈ R s.t a | bc
⇒ bc = ak for some k ∈ R

case 1 :- If b is unit
⇒ $c = b^{-1}ak$
$= a(b^{-1}k)$
⇒ a | c

case 2 :- If c is unit
$b = a(kc^{-1})$ ⇒ a | b

case 3 :- If k is a unit
$a = b(ck^{-1})$
⇒ either b or ck^{-1} is unit
⇒ either b or $(ck^{-1})k$ is unit
⇒ either b or c is unit
⇒ a | c or a | b

case 4 :- If b, c, k are non-units
⇒ b, c and k have unique factorization as finite product of irreducibles.

Let $b = p_1 p_2 p_3 \cdots p_r$
$c = q_1 q_2 \cdots q_t$
$k = k_1 k_2 \cdots k_s$ where all p_i's, q_j's, k_t's are irreducible

$bc = ak = x$ (say)
⇒ $p_1 p_2 \cdots p_r q_1 q_2 \cdots q_t = ak_1 k_2 \cdots k_s = x \in R$
⇒ $r + t = s + 1$
and $a \nsim p_i$ or $a \nsim q_j$
⇒ $a | p_i$ or $a | q_j$
⇒ $a | p_1 p_2 \cdots p_r$ or $a | q_1 q_2 \cdots q_t$
⇒ a | b or a | c

Scanned with CamScanner

PAGE NO. :
DATE : / /

Thm: Let R be an Integral domain, in which
(i) each non-zero, non-unit element has factorization as finite product of irreducibles
(ii) Each irreducible element is prime
then R is UFD.

Proof:- To prove that R is UFD, we need to prove uniqueness of factorization

Let $a \in R$ be non-zero, non-unit element s.t
$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ be two factorization of a as product of irreducibles.

If $s=1$ $\quad a = p_1 p_2 \dots p_r = q_1$
$\Rightarrow q_1 \mid p_1 p_2 \dots p_r$

$\Rightarrow q_1 \mid p_i$ for some i ($\because q_i$ is prime (given))
$\Rightarrow p_i = q_1 K$, where K is some unit
$\Rightarrow q_1 K p_2 p_3 \dots p_r = q_1$
$\Rightarrow q_1 (K p_2 p_3 \dots p_r - 1) = 0$
$\Rightarrow K p_2 p_3 \dots p_r = 1$
$\Rightarrow p_2 p_3 \dots p_r$ are units
$\longrightarrow \longleftarrow$

hence $r = 1$

hence $r = 1 = s$

and $p_1 \sim q_1$

Assume that result is true if $s = n-1$

If $s = n$

$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_{n-1} q_n$ —— (*)
$\Rightarrow q_1 \mid p_1 p_2 \dots p_r$
as q_1 is prime (being irreducible)
$\Rightarrow q_1 \mid p_i$ for some i
Without loss of generality, we can assume $p_1 \mid q_1$
$\Rightarrow q_1 = p_1 u$ for some $u \in U(R)$
from (*)

say (1) Each non-zero, non-unit has factorisation and each element factorisation is prime.

$p_1 p_2 \cdots p_r = p_1 u q_2 q_3 \cdots q_{n-1} q_n$

$\Rightarrow p_1(p_2 p_3 \cdots p_r - u q_2 q_3 \cdots q_{n-1} q_n) = 0$

As $p_1 \neq 0$

$\Rightarrow p_2 p_3 \cdots p_r - u q_2 q_3 \cdots q_{n-1} q_n = 0$

$\Rightarrow u' p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_{n-1} q_n = y$ (say)

By Induction, we get

$r-1 = n-1$ and

each $q_i \sim p_j$ $\forall i \geq 2$

$\Rightarrow r = n$ and each $q_i \sim p_j$ $\forall i \geq 1$

Eg:- $2\mathbb{Z}$

$4, 6 \in 2\mathbb{Z}$

$\gcd(4,6) \neq 2$

$4 = 2 \cdot 2$

$6 = 2 \cdot 3$ ↓ $\notin 2\mathbb{Z}$

$LCM(4,6) = ?$

12, 24, 36 ... (divide)

In Ring, Two elements do not have gcd but this doesn't happen in UFD.

Whenever you have UFD, any two elements have gcd and lcm also.

Thm- In a UFD, any two non-zero elements have G.C.D.

proof- Let a and b be two non-zero elements in a UFD, R. If one of them say a is unit then

$b = a(a^{-1}b)$

$\gcd(a,b) = \gcd(a, a(a^{-1}b)) = a$

If none of a and b is unit

as R is UFD,

$\Rightarrow a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ where α_i's, β_j's ≥ 0

$50 = 2 \times 5^2 \times 7^0$

$343 = 7^3 \times 2^0 \times 5^0$

Thm:-

proof-

Ring — we study the properties of them — field

PAGE NO. :
DATE : / /

$\alpha_i - r_i \Rightarrow$ non negative
$\therefore r_i$ is min, cannot exceed α_i

Take $r_j = \min(\alpha_j, \beta_j)$
then

$$a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \left(p_1^{\alpha_1 - r_1} \cdots p_k^{\alpha_k - r_k}\right)$$
$$b = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \left(p_1^{\beta_1 - r_1} \cdots p_k^{\beta_k - r_k}\right)$$

claim :- $c = p_1^{r_1} p_2^{r_2} \cdots p_r^{r_r} = \gcd(a, b)$

i.e.

(i) $c \mid a$ & $c \mid b$

(ii) if $\exists\, d \in R$ s.t $d \mid a$ and $d \mid b$ then $c' \mid c$

clearly as $a = c \cdot (p_1^{\alpha_1 - r_1} \cdots p_r^{\alpha_r - r_r})$

$\Rightarrow c \mid a$

similarly $c \mid b$

now let $d \in R$ s.t $d \mid a$ and $d \mid b$

if d is unit $\Rightarrow c = d(d^{-1}c)$

$\Rightarrow d \mid c$

if d is not unit

$\Rightarrow d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_r^{\delta_r}$ and $\delta_i \geq 0$

$\delta_i \leq \alpha_i$ and $\delta_i \leq \beta_i$

$\Rightarrow \delta_i \leq \min\{\alpha_i, \beta_i\} = r_i$

$\Rightarrow c = p_1^{\delta_1} p_2^{\delta_2} \cdots p_r^{\delta_r} (p_1^{r_1 - \delta_1} \cdots p_k^{r_k - \delta_k})$

$= d\,(p_1^{r_1 - \delta_1} \cdots p_r^{r_r - \delta_r})$

$\Rightarrow d \mid c$ H.P

Thm :- Any two non zero elements in a UFD have an l.c.m.

proof – Let we have UFD, R

Let $a, b \in R$ and a, b are non-zero

Let 'a' be a unit in R

$\Rightarrow b = (aa^{-1})b \Rightarrow b = a(a^{-1}b)$

$\Rightarrow a \mid b$

also, $b = 1.b \Rightarrow b \mid b$

now let $\exists\, c \in R$ s.t $a \mid c$ and $b \mid c$

c cannot be unit.

we can write c as

$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$

since $a \mid c \Rightarrow \alpha_i \leq \gamma_i \;\forall\, 1 \leq i \leq n$

$b \mid c \Rightarrow \beta_i \leq \gamma_i \;\forall\, 1 \leq i \leq n$

Scanned with CamScanner

$\Rightarrow b = lcm(a,b)$

Why if b is unit $\Rightarrow a = lcm(a,b)$

→ now, let a, b are non-unit elements in R as R is UFD. So, we can represent a, b as product of irreducibles as follows

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$b = p_1^{\beta_1} p_1^{\beta_2} \cdots p_n^{\beta_n}$

(by suitably taking the powers)

now let

$\delta_i = \max(\alpha_i, \beta_i)$

claim: $d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$ is lcm of a, b

now

$d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$

$= (p^{\delta_1-\alpha_1} p_2^{\delta_2-\alpha_2} \cdots p_n^{\delta_n-\alpha_n})(p^{\alpha_1} p^{\alpha_2} \cdots p^{\alpha_n})$

$= (p_1^{\delta_1-\alpha_1} p_2^{\delta_2-\alpha_n} \cdots p_n^{\delta_n-\alpha_n})\, a$

$\Rightarrow a|d$

also, $d = (p^{\delta_1-\beta_1} p^{\delta_2-\beta_2} \cdots p^{\delta_n-\beta_n})(p^{\beta_1} p^{\beta_2} \cdots p^{\beta_n})$

$d = (p^{\delta_1-\beta_1} p^{\delta_2-\beta_2} \cdots p^{\delta_n-\beta_n})\, b$

$\Rightarrow b|d$

$\Rightarrow \max(\alpha_i, \beta_i) \le \gamma_i \ \forall\ 1 \le i \le n$

$\Rightarrow \delta_i \le \gamma_i \ \forall i$

$\Rightarrow c = (p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n})$

$= (p_1^{\gamma_1-\delta_1} p_2^{\gamma_2-\delta_2} \cdots p_n^{\gamma_n-\delta_n})(p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n})$

$\Rightarrow c = d(p_1^{\gamma_1-\delta_1} p_2^{\gamma_2-\delta_2} \cdots p_n^{\gamma_n-\delta_n})$

$\Rightarrow d|c$

now as $a|d$, $b|d$

and for any other common multiple c of a and b,

$d|c$

$\Rightarrow$ d is l.c.m

Hence proved.

Example :

10/Sep/21

PID (Principal Ideal Domain) – An integral domain R is called PID, if its every ideal is principal ideal (i.e. generated by a single element)

Eg:– $R = \mathbb{Z}$

$I = \langle 2,4 \rangle = 2R + 4R = 2\mathbb{Z} + 4\mathbb{Z} = \{\cdots -4, -2, 0, 2, \cdots\} + \{\cdots -4, 0, 4, 8, 12\}$

$= 2\mathbb{Z}$

$4\mathbb{Z} \subseteq 2\mathbb{Z}$

$I = \langle 3,6 \rangle = 3\mathbb{Z}$

Thm– $\mathbb{Z}$ is a prime ideal domain (PID)

Proof– $\mathbb{Z}$ is an integral domain and $I \triangleleft \mathbb{Z}$

If $I = 0$, then clearly I is principal ideal

If $I \neq 0 \Rightarrow$ I has atleast one +ve integer

So, by well-ordering property, we can choose

Scanned with CamScanner

$I = \{ \ldots, -8, -4, -2, 0, 2, 4, 6, \ldots \}$

PAGE NO.
DATE:

$0 < a \in I$, s.t a has least absolute value

Now let $b \in I$, so by divison algorithm

$$b = aq + r \; ; \; 0 \leq r < a$$

$$\Rightarrow r = b - aq \in I \quad (\because a, b \in I \text{ & } I \trianglelefteq \mathbb{Z})$$

If $r \neq 0$, then $0 < r < a \Rightarrow |r| < |a|$ and $r \in I$

$\longrightarrow \longleftarrow$ (To the choice of a)

If $r = 0$

$b = aq \in a\mathbb{Z}$

$\Rightarrow I \subseteq a\mathbb{Z}$

also $a\mathbb{Z} \subseteq I$ hence $I = a\mathbb{Z}$

Example of an Integral Domain which is not PID.

$\mathbb{Z}[x]$ is Integral domain as $\mathbb{Z}$ is I.D.

Let $I = \langle 2, x \rangle \trianglelefteq \mathbb{Z}[x]$

Claim :- I is not a Principal Ideal

Suppose I is a Principal Ideal

$\Rightarrow \exists f(x) \in \mathbb{Z}[x]$ s.t

$$I = \langle f(x) \rangle$$

also $I = \langle 2, x \rangle = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$

jin elements se ideal generate kare woh ideal ka belong karte hai

$2, x \in I$

as $2 \in I$ (I)

$\Rightarrow 2 = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$

also as $x \in I$

$\Rightarrow x = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$

$\Rightarrow xg(x) = f(x)h(x)g(x)$

$\Rightarrow xg(x) = 2h(x)$

$\Rightarrow 2 | xg(x) \quad \Rightarrow 2 | g(x)$

$\Rightarrow g(x) = 2t(x)$ for some $t(x) \in \mathbb{Z}[x]$

So from (I)

$$2 = 2f(x)t(x)$$

$$2(f(x)t(x) - 1) = 0$$

$$\Rightarrow f(x)t(x) = 1$$

Scanned with CamScanner

Ideal + Identity = Ring

PAGE NO. :
DATE : / /

$\Rightarrow 1 \in \langle f(x) \rangle = I$

$\Rightarrow 1 \in I$

$\Rightarrow 1.r \in I \quad \forall r \in R$

$\Rightarrow r \in I \quad \forall r \in R$

$\Rightarrow R \subseteq I$

$\Rightarrow I = R = \mathbb{Z}[x]$

but if we take

$K(x) = 1 + x \notin I$

$\Rightarrow$ This Ideal was not the principal Ideal

$I = \langle 2, x \rangle$
$= 2\mathbb{Z}[x] + x\mathbb{Z}[x]$

Thm- Every PID is UFD.

proof:-

$2 + 3x = 2(1) + x(3)$

$\mathbb{Z}[\sqrt{5}]$ - Not UFD
↓
Not PID

Lemma- If R is a PID, R cannot have an infinite ascending chain of Ideals.

$\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq 16\mathbb{Z} \ldots$

Infinite descending chain

$n\mathbb{Z} \quad 16\mathbb{Z} \subseteq 8\mathbb{Z} \subseteq 4\mathbb{Z} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$

proof:- Let $a_1R \subseteq a_2R \subseteq a_3R \subseteq \ldots$ be an infinite ascending chain of ideals in PID R.

Let $A = \bigcup a_iR$

Let $a, b \in A \Rightarrow a \in a_iR$ and $b \in a_jR$ for some i, j

Let $i \leq j \Rightarrow a_iR \subseteq a_jR$

$\Rightarrow a \in a_jR$.

$\Rightarrow a - b \in a_jR \subseteq A$

Now if $r \in R$

then $ar \in a_iR \subseteq A$

$\Rightarrow A \trianglelefteq R$

as R is PID $\Rightarrow A = aR$ for some $a \in R$

$\Rightarrow a \in A = \bigcup a_iR$

Scanned with CamScanner

$\Rightarrow a \in a_k R$ for some k

$\Rightarrow aR \subseteq a_k R$ for some k

$\Rightarrow A \subseteq a_k R$ for some k

also $a_k R \subseteq A$

Hence $A = a_k R$ for some K

$a_1 R \subseteq a_2 R \subseteq a_3 R \subseteq \ldots\ldots \subseteq a_k R$

Hence, A PID can never have an infinite ascending chain of ideals

11/Sep/21

Thm- Every PID is UFD.

proof- (1) Let a be a non-zero, non-unit element in R

If a is irreducible, nothing to prove.

If a is reducible $\Rightarrow a = bc$ where both b and c are non-units

If both b and c are finite product of irreducibles a is also. So, let b is not a finite product of irreducible.

$\Rightarrow b = xy$, where atleast one of x and y say x is not a finite product of irreducibles.

Also $aR \subseteq bR \subseteq xR \subseteq \ldots\ldots$ is an infinite ascending chain of ideals in R.

(2) We prove that every irreducible element in a PID is prime element.

Let $a \in R$ be an irreducible element

$\Rightarrow a$ is non-zero, non-unit

Let $a \mid bc$ for some $b, c \in R$

Assume that $a \nmid b$

$\Rightarrow b \notin aR$

$bR + aR$ is an ideal in R

but R is PID $\Rightarrow bR + aR = xR$ for some $x \in R$ (1)

$\Rightarrow a \in xR$

$\Rightarrow a = xy$ for some $y \in R$.

Scanned with CamScanner

as a is irreducible $\Rightarrow$ x or y is a unit

If y is unit

$\Rightarrow x = ay^{-1} \in aR$

$\Rightarrow xR \subseteq aR$

also $aR \subseteq xR$ (from (1))

$\Rightarrow xR = aR$

$\Rightarrow bR \subseteq aR \Rightarrow b \in aR$

$\Rightarrow a \mid b$

$\longrightarrow \longleftarrow$ as $a \nmid b \Rightarrow y \notin U(R)$

(2)

$\Rightarrow x$ is a unit

$\Rightarrow 1 \in xR \quad (\because 1 = x \cdot x^{-1})$

$\Rightarrow xR = R$

So (1) $\Rightarrow aR + bR = R$

$\Rightarrow 1 \in aR + bR$

$\Rightarrow \exists$ some $p, q \in R$ s.t

$1 = ap + bq$

$c = a(cp) + (bc)q$

$a \mid R.H.S \Rightarrow a \mid L.H.S$

$\Rightarrow a \mid c$

hence a is a prime element

3.

Euclidean domain (ED)

(Division algorithm)

behaves like Z as integer, they behave like Z if we define a func ϕ

Def^n :- An integral domain is called Euclidean domain if there exists a function $\phi : R \to \mathbb{Z}$ s.t

(1) If $a, b \in R^* \Rightarrow R - \{0\}$ and $b \mid a$ then $\phi(b) \leq \phi(a)$

(2) for each pair of elements $a, b \in R$, $b \neq 0$, $\exists\ q, r \in R$ s.t

$a = bq + r$ with $\phi(r) < \phi(b)$

(ii)

Example :- 1. $F[x]$ - Poly. Ring over field

PAGE NO. :
DATE : / /

2. $R = \mathbb{Z}$

Define $\phi : \mathbb{Z} \to \mathbb{Z}$

$\phi(a) = |a|$

$a|-a$ but $a \nmid a$

① If $b|a$ then $\phi(b) \leq \phi(a)$

If $b|a \Rightarrow a = bc$

$\Rightarrow |a| = |b||c|$

$\Rightarrow |a| \geq |b|$

$\Rightarrow \phi(a) \geq \phi(b)$

② let $a, b \in \mathbb{Z}$, $b \neq 0$

Then by division algorithm

$a = bq + r$, where $0 \leq r < |b|$

$\Rightarrow 0 \leq |r| < |b|$

$\Rightarrow a = bq + r$ where either $r = 0$

or $\phi(r) < \phi(b)$

Hence, $\mathbb{Z}$ is E.D.

3. $\mathbb{Z}[i] = \{a + bi ; a, b \in \mathbb{Z}\}$ (Ring of Guassian Integers)

claim :- $\mathbb{Z}[i]$ is a E.D.

Define $\phi : \mathbb{Z}[i] \to \mathbb{Z}$

$\phi(a+bi) = a^2 + b^2$

Let $x, y \in \mathbb{Z}[i]$

$x = a + bi$

$y = c + di$ s.t $x|y$

$\Rightarrow y = xz \Rightarrow (c+di) = (a+bi)(e+fi)$

$\Rightarrow (c-di) = (a-bi)(e-fi)$

$c^2 + d^2 = (a^2+b^2)(e^2+f^2)$

$c^2 + d^2 \geq a^2 + b^2$

(ii) Let $x = a + bi$

$y = c + di \neq 0$

$\Rightarrow xy^{-1} = \alpha + i\beta$ where α, β are Rational numbers

Scanned with CamScanner

KARAND

mid

$[\frac{1}{2}, \frac{1}{2}]$

PAGE NO.: 9+1
DATE: / /

Choose integers α_0 and β_0 s.t $|\alpha - \alpha_0| \leq \frac{1}{2}$ and

$$|\beta - \beta_0| \leq \frac{1}{2}$$

$$\Rightarrow x = y(\alpha + i\beta) = y[(\alpha_0 + \beta_0 i) + (\alpha - \alpha_0) + (\beta - \beta_0)i]$$

$$x = \underbrace{y(\alpha_0 + \beta_0 i)}_{z} + \underbrace{y(\alpha - \alpha_0) + y(\beta - \beta_0)i}_{r}$$

$$r = x - yq$$

$$z[i]$$

$$\phi(r) = \phi(y[(\alpha - \alpha_0) + (\beta - \beta_0)i])$$

$$= \phi(y)\,\phi[(\alpha - \alpha_0) + (\beta - \beta_0)i]$$

$y = xz$
$\phi(xz) = \phi(x)\,\phi(z)$ #

$$= \phi(y)\left((\alpha - \alpha_0)^2 + (\beta - \beta_0)^2\right)$$

$$\leq \phi(y)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}\phi(y) < \phi(y)$$

$$\phi(r) < \phi(y)$$

14/Sep/21

Thm:- Every E.D is a P.I.D.

proof:- We just need to show that every non-zero ideal I in a E.D. R is a principal ideal.

for each $a \in I$, $1 | a$ in R

$\Rightarrow \phi(1) \leq \phi(a)\ \forall a \in I$

$\Rightarrow S = \{\phi(a),\ a \in I \setminus \{0\}\}$ is bounded below by $\phi(1)$

S is a subset of natural numbers with $\phi(1)$ as a lower bound.

So, by well-ordering property of integers, $\exists$ some $d \in I$ s.t $\phi(a)$ is smallest element of S.

$\phi: R \to \mathbb{Z}^+ \cup \{0\}$
$\phi(x) \geq 0$ if $x \neq 0$ #

Ring $\rightleftarrows$ Ring (2D)

Scanned with CamScanner

PAGE NO. :
DATE : / /

claim :- $I = \langle d \rangle$

Let $b \in I$ be an arbitrary element

then $\exists\ q, r \in R$ s.t

$b = dq + r$ where $\phi(r) < \phi(d)$

$\Rightarrow r = b - dq \in I$

so, $r \in I$ with $\phi(r) < \phi(d)$

$\rightarrow\ \leftarrow$ to choice of d if $r \neq 0$

$\Rightarrow r = 0$

$\Rightarrow b = dq \in \langle d \rangle$

$\Rightarrow I = \langle d \rangle$

So, I is a principal ideal

Hence, Every E.D is a P.I.D

#

$\phi : \mathbb{Z} \to \mathbb{Z}$

If $a|b$ then $\phi(a) \leq \phi(b)$ $\forall a, b \in \mathbb{Z}$

$\phi(b) \leq \phi(a)$ ($\because$ every element in $\mathbb{Z}$ divides each other)

$\phi(a) = \phi(b)$ $a|b$ and $b|a$

$\forall a, b \in \mathbb{Z}$

$\frac{b}{q} \quad \frac{b}{q_1}$

$\frac{b_1}{q_1} = \frac{b}{q} \times \frac{q\,b_1}{b\,q_1}$

#

F - field (Every element is unit)

$\phi : f \to \mathbb{Z}$

$\phi(a) = 1$

$a \in f,\ b \in f^*$

$a = a(b^{-1} \cdot b) + 0$

f[x] is not field

- Fields becomes Euclidean domain

$\mathbb{Z}[\sqrt{-19}] = \{ a + b\sqrt{-19} ;\ a, b \in \mathbb{Z},\ a, b \text{ have same parity} \}$

$\mathbb{Z}[\sqrt{-19}] = \{ a + b\sqrt{-19}, f[x], \mathbb{Z} \}_{a,b \in \mathbb{Z}}$

$\mathbb{Z}[\sqrt{-5}]$ is not comparable

$M_2(\mathbb{R})$

$\mathbb{Z}$ Ring $\nrightarrow$ Ring with id $\nrightarrow$ Comm. Ring with id $\nrightarrow$ I.D $\nrightarrow$ UFD $\nrightarrow$ PID $\nrightarrow$ ED $\to$ Field

$\leftarrow \quad \leftarrow \quad \leftarrow \quad \leftarrow \quad \leftarrow \quad \leftarrow \quad \leftarrow$

Scanned with CamScanner

KARAN

$F[x] = Z/[x]$ – we do not divide two polys here

PAGE NO.: most fields we divide the poly we will DATE: some cases.

Thm – Let $R[x]$ be a ring of polynomials over a I.D. R. Let $f(x), g(x) \neq 0$ be polynomial in $R[x]$ of degrees m and n respectively. Let $K = \max(m-n+1, 0)$ and let a be leading coefficient of $g(x)$. Then $\exists$ unique polynomials $q(x)$ and $r(x)$ in $R[x]$ s.t

$$a^K f(x) = q(x)\,g(x) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

proof :- If $m < n$

then take $q(x) = 0$, $r(x) = f(x)$

we get $f(x) = g(x) \cdot q(x) + r(x)$

where $\deg r(x) = \deg f(x) = m < n = \deg g(x)$

If $m \geq n$

we prove the result by induction on m

If $m = 1$

then $n = 0$ or 1

If $n = 0 \Rightarrow g(x) = a$

then $a^k f(x) = g(x)\,q(x) + 0$, where $q(x) = f(x)$

If $n = 1$ then $g(x) = ax + b$

let $f(x) = cx + d$

then $af(x) = g(x)\,c + (ad - bc)$

($q(x)$, $r(x)$)

here $\deg r(x) = 0 < \deg g(x)$

$\Rightarrow$ result is true for $m = 1$

Let the result be true if $f(x)$ is of deg $m-1$

now if $\deg f(x) = m$

$$f(x) = (a_0 + a_1 x + \cdots + a_m x^m)$$

$$g(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + b_n x^n$$

$\frac{f(x)}{a} = \frac{x^2+1}{a}$

$a(x^2+1) = a(x^2+1)$ ($g(x)\,q(x)$)

$ax+b \;\big)\; acx + ad$ / $acx + bc$ / $ad - bc$; c

$x^3 - 1$ ÷ $2x+1$

$K = \max(3-1+1, 0) = 3$

$2^3 f(x)$

$4x^2 + 2x + 1$

$2x+1 \;\big)\; 8x^3 - 8$

$8x^3 - 4x^2$

$4x^2 - 8$

$4x^2 - 2x$

$-2x - 1$

$-2x + 1$

-2

$2x+1 = m=1$

$x^3 - 1 \quad m=3$

$K = \max(1-3+1, 0)$

$= 0$

$= 2^0 f(x)$

Scanned with CamScanner

PAGE NO. :
DATE : / /

$a f(x) - a_m x^{m-n} g(x) = f_1(x)$ is of deg $\leq m-1$

So, by induction

$k = \max(m-1-n+1, 0)$ then

$a^t f_1(x) = g(x) q(x) + r(x)$ where $r(x)=0$ or $\deg r(x) < \deg g(x)$

$a^t (a f(x) - a_m x^{m-n} g(x)) = g(x) q(x) + r(x)$

$a^{t+1} f(x) = g(x)[a^t a_m x^{m-n} + q(x)] + r(x)$

$a^t a_m x^{m-n} \rightarrow q_1(x)$

Where $r(x)=0$ or $\deg r(x) < \deg g(x)$

$t = \max(m-n, 0)$

$t+1 = \max(m-n+1, 1) \rightarrow$ (maximum 1 toh aagyahi aaya so 1 is replaced by 0)

$= \max(m-n+1, 0)$

Uniqueness –

Scanned with CamScanner

KARAN

$f(x) = a_0 + a_1x + \cdots + a_nx^n$

$gcd(a_0, \ldots, a_n) = \text{unit}$

PAGE NO.:
DATE: / /

17/Sep/21

Content of a Polynomial

Defn:- Let R be a UFD. Then $f(x) \in R[x]$ is called primitive polynomial if gcd of coefficients of $f(x)$ is a unit in R.

$\mathbb{Z}[x]$	$\mathbb{Q}[x]$
$f(x) = 2+4x$	$f(x) = 2+4x$
$gcd(2,4) = 2$	$gcd(2,4) = 2$ – unit
not primitive poly.	$\Rightarrow$ primitive polynomial

$gcd(2,4) = 2, -2 = -1 \times 2$

Coff. have only one gcd but if we have another gcd then other gcd is ~~multiple~~ of the type $-1 \times 2 = -2$

Content of a Polynomial – The gcd of coefficients of a polynomial $f(x) \in R[x]$ where R is UFD, is called content of the polynomial $f(x)$ and is denoted by $c(f)$.

$p|a, p|b \Rightarrow p|a \pm b$

NOTE:- $c(f)$ is unique upto associates.

Lemma (Guass) – Let R be a UFD. If $f(x), g(x) \in R[x]$ then $c(fg) = c(f)\,c(g)$. In particular, product of two primitive polynomials is primitive.

Eg:- $\mathbb{Z}[x]$

$f(x) = 2+4x$

$g(x) = 3+9x+3x^2$

$c(f) = 2$ $\quad c(fg) = 6$

$c(g) = 3$

$f(x) = 2+4x$
$= 2(1+2x)$
$\downarrow$
$\sim f(x)$

$\Rightarrow$ our suppo

Thm:-

proof:- Let $c(f) = c$, $c(g) = d$

Also $f(x) = cf_1(x)$ and $g(x) = dg_1(x)$ where $f_1(x)$ and $g_1(x)$ are primitive polynomials.

proof:-

$f g = c(f_1 g_1)\, f_1 g_1$

T.P :- $c(fg) = c(f_1 g_1)$ i.e. $c(f_1 g_1) = \text{unit}$

i.e. $f_1 g_1$ is primitive

Let $f_1(x) = a_0 + a_1 x + \dots + a_n x^n$

$g_1(x) = b_0 + b_1 x + \dots + b_m x^m$

Assume that f_1, g_1 is not primitive

$\Rightarrow \exists$ a prime $p \in R$ s.t $p \mid c(f_1 g_1)$

$\Rightarrow p$ divides each coefficient of $f_1 g_1$

Let a_r be the first coefficient of $f_1(x)$ s.t $p \nmid a_r$

Similarly let b_s be the first coefficient of $g_1(x)$ s.t $p \nmid b_s$

hence $p \nmid a_r b_s$ ($\because$ If $p \mid a_r b_s \Rightarrow p \mid a_r$ or $p \mid b_s$)

Coefficient of x^{r+s} in $f_1 g_1 = \lambda = a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \dots + a_{r+s} b_0$

$\Rightarrow p \mid \lambda$ — ①

also $p \mid a_0, p \mid a_1, \dots, p \mid a_{r-1}$

$\Rightarrow p \mid a_0 b_{r+s}, p \mid a_1 b_{r+s-1}, \dots, p \mid a_{r-1} b_{s+1}$

$\Rightarrow p \mid (a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r-1} b_{s+1}) \Rightarrow p \mid \lambda_1$ — ②

Similarly $p \mid b_{s-1}, p \mid b_{s-2}, \dots, p \mid b_0$

$\Rightarrow p \mid a_{r+1} b_{s-1}, p \mid (a_{s+2} b_{s-2}, \dots, p \mid a_{r+s} b_0)$

$\Rightarrow p \mid \lambda_2$ — ③

From ①, ② and ③

$p \mid \lambda - \lambda_1 - \lambda_2$

$\Rightarrow p \mid a_r b_s$

$\longrightarrow \longleftarrow$ as $p \nmid a_r b_s$

$\Rightarrow$ our supposition is wrong

So, product of two primitive polynomials is primitive

Thm :- If R is a UFD, so is $R[x]$

Proof :- (1) we firstly show that every non-zero, non-unit in $R[x]$ can be factorized as a finite product of irreducibles.

$c(f_1 g_1) \in R$ ↓ UFD

$c(f_1 g_1) \neq 0$, unit

$c(f_1 g_1)$ have prime factorization ja kofek prime hoga jo divide krega $c(f_1 g_1)$

$f(x) = 6 + 6x + 3x^2 + 9x^3$

$= 3(2 + 2x + x^2 + 3x^3)$

$\downarrow c \quad \downarrow f_1(x)$

$p \mid a, p \mid b \Rightarrow p \mid a \pm b$

$\mathbb{Z} = PID$

$\mathbb{Z}[x] \rightarrow$ Not UFD PID

F — field

F[x] — Not field

$\mathbb{Z}$ — ED

$\mathbb{Z}[x]$ — NotED

KARAN

For Uniqueness [product of irr = unique
every ~~element of~~ irreducible element is prime

PAGE NO. :
DATE : / /

$f(x) \in R[x]$

$f(x) = c\, f_1(x)$, where $f_1(x)$ is primitive poly.

as $c \in R$, R is UFD, we just need to show that $f_1(x)$ is finite product of irreducibles.

If $\deg f_1(x) = 0 \Rightarrow f_1(x) = a \in R$ so result is true

If $\deg f_1(x) = 1 \Rightarrow f_1(x) = ax+b$

which is already irreducible

Assume that the result is true for primitive polynomial of $\deg f_1(x) < n$

Let $\deg f_1(x) = n$

If $f_1(x)$ is irreducible, then NTP

If $f_1(x)$ is reducible $\longrightarrow [g(x) \neq 0, h(x) \neq 0]$

$f_1(x) = g(x)\, h(x)$ where $0 < \deg g(x) < \deg f_1(x)$

$0 < \deg h(x) < \deg f_1(x)$

also $g(x)$, $h(x)$ are primitive

So, by Induction $g(x)$, $h(x)$ are finite product of irreducibles and hence $f_1(x)$

Scanned with CamScanner

UNIT - 2

Thm :- Let R be a PID, which is not a field. Then an ideal $I \triangleq R$ is maximal ideal iff I is generated by an irreducible element.

Proof :- Let $a \in R$ be an irreducible element.

Claim :- $m = \langle a \rangle$ is maximal ideal of R

Let $m \subseteq I \subseteq R$ for some ideal I of R

as R is PID

$\Rightarrow I = \langle b \rangle$ for some $b \in R$

$\langle a \rangle \subseteq \langle b \rangle \subseteq R$

$\Rightarrow a \in \langle b \rangle$

$\Rightarrow a = bc$ for some $c \in R$.

but a is irreducible

$\Rightarrow$ b or c is a unit.

→ If b is unit

$\Rightarrow b^{-1}$ exist and $bb^{-1} \in I$

$\Rightarrow 1 \in I$

$\Rightarrow I \in R$

→ If c is unit $\Rightarrow$ then $a = bc$ implies $b = ac$

$\Rightarrow b = \langle a \rangle \Rightarrow \langle b \rangle \subseteq \langle a \rangle$

$\Rightarrow I \subseteq m$

also $m \subseteq I$

$\Rightarrow m = I$

Hence m is a maximal ideal.

Converse :-

Let m be a maximal ideal of R.

as R is PID

$\Rightarrow m = \langle a \rangle$ for some $a \in R$

(i) a is non zero

If $a = 0 \Rightarrow m = 0$ and $\frac{R}{m} = R$, which is not a field.

$\Rightarrow m$ is not maximal ideal. $\longrightarrow\leftarrow$

Hence $a \neq 0$

(ii) a is non unit

If a is unit

$\Rightarrow a a^{-1} \in m \Rightarrow 1 \in m \Rightarrow R = m$ $\longrightarrow\leftarrow$

Hence a is non unit

(iii) Now let $a = bc$ — (1) for $b, c \in R$.

Let $B = (b)$

then $a \in B \Rightarrow \langle a \rangle \subseteq B \Rightarrow m \subseteq B$

but m is maximal $\Rightarrow B = m$ or $B = R$

If $B = m$

$\Rightarrow b \in m \Rightarrow b = ac_0$ for some $c_0 \in R$.

Put in (1)

$a = ac_0 c$

$\Rightarrow a(1 - cc_0) = 0$

$1 - cc_0 = 0 \quad \because a \neq 0$

$\Rightarrow cc_0 = 1 \Rightarrow c$ is unit.

If $B = R$

$\Rightarrow 1 \in B \Rightarrow 1 = bb_0$ for some $b_0 \in R$

$\Rightarrow b$ is unit

Hence $a \in R$ is irreducible.

#

Eisenstein Irreducibility criterion :- Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in Z[x]$, $n \geq 1$, If there is a prime p such that $p^2 \nmid a_0$, $p \mid a_0$, $p \mid a_1$, $\cdots$ $p \mid a_{n-1}$, $p \nmid a_n$ then $f(x)$ is irreducible over $\mathbb{Q}$ and hence over Z.

Proof :- $f(x) = a_0 + a_1 x + \cdots + a_n x^n$

Let $f(x)$ be reducible over Z

$\Rightarrow \exists\ g(x), h(x) \in Z[x]$ s.t. $f(x) = g(x)\,h(x)$

Scanned with CamScanner

PAGE NO. :
DATE : / /

Let $g(x) = b_0 + b_1 x + \dots + b_r x^r$

$h(x) = c_0 + c_1 x + \dots + c_s x^s$

then $a_0 = b_0 c_0$

also $p \mid a_0 \Rightarrow p \mid b_0 c_0$

$\Rightarrow p \mid b_0$ or $p \mid c_0$

also $p^2 \nmid a_0$

$\Rightarrow p$ cannot divide both b_0 and c_0

$\Rightarrow p \mid b_0$ and $p \nmid c_0$ or $p \mid c_0$ and $p \nmid b_0$

→ Consider $p \mid c_0$ and $p \nmid b_0$

also $p \nmid a_n$ and $a_n = b_r c_s$

$\Rightarrow p \nmid b_r c_s$

$\Rightarrow p \nmid b_r$ and $p \nmid c_s$

let c_m be the first coefficient of $h(x)$ st $p \nmid c_m$ then,

coeff of x^m in $f(x) = a_m = b_0 c_m + b_1 c_{m-1} + \dots + b_m c_0$

If $m < n$, $p \mid a_m$

$\Rightarrow p \mid (b_0 c_m + b_1 c_{m-1} + \dots + b_m c_0)$

also $p \mid c_0, p \mid c_1 \dots \Rightarrow p \mid c_{m-1}$

$\Rightarrow p \mid b_m c_0, p \mid b_{m-1} c_1 \dots p \mid b_1 c_{m-1}$

$\Rightarrow p \mid (b_m c_0 + b_{m-1} c_1 + \dots + b_1 c_{m-1}) = \lambda_1$

$\Rightarrow p \mid (\lambda - \lambda_1) \Rightarrow p \mid b_0 c_m$

$\Rightarrow p \mid b_0$ or $p \mid c_m$

→ ←

So $f(x)$ is irreducible.

PAGE NO. :
DATE : / /

** For primitive polynomial $f(x) \in \mathbb{Z}[x]$

If $f(x)$ is reducible over $\mathbb{Z} \Rightarrow f(x)$ is reducible over $\mathbb{Q}$

If $f(x)$ is reducible over $\mathbb{Q} \Rightarrow f(x)$ is reducible over $\mathbb{Z}$

Example $f(x) = g(x) h(x)$

$f(x+a) = g(x+a) h(x+a)$

Suppose $f(x) = 1 + x + x^2$

$f(x+1) = 1 + (x+1) + (x+1)^2$

$= 1 + x + 1 + x^2 + 1 + 2x$

$= x^2 + 3x + 3$

Hence

$p^2 \nmid a_0$, $p \mid a_0$, $p \mid a_1$

Example $f(x) = 1 + x + x^2 + \dots + x^{p-1} = \frac{(x^p - 1)}{x - 1}$

$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1}$

$= \frac{(x+1)^p - 1}{x}$

$= \frac{1}{x}\left((x+1)^p - 1\right)$

$= \frac{1}{x}\left(pc_0 + pc_1 x + \dots + pc_p x^p - 1\right)$

$= pc_1 + pc_2 x + pc_3 x^2 + \dots + pc_p x^{p-1}$

$= p + \frac{p(p-1)}{2} x + \frac{p(p-1)(p-2)}{6} x^2 + \dots + x^{p-1}$

Hence $p^2 \nmid a_0$, $p \mid a_0$, $p \mid a_1$

Hence $f(x)$ is irreducible.

Scanned with CamScanner

Field Theory

Let $F \subset E$ be two fields. Then E_F is a vector space.

$[E:F]$ = deg of E over F = dimension of E_F

$[C:R]$ =

HW Find any two different basis of C_R ?

Theorem:- Let $F \subset E \subset K$ be fields If $[K:E]_{K_E} < \infty$ and $[E:F]_{E_F} < \infty$ then

(i) $[K:F] < \infty$

(2) $[K:F] = [K:E]\,[E:F]$

Proof:- Let $[K:E] = m$ and $[E:F] = n$

Let $\{v_1, v_2 \ldots v_m\}$ be a basis of K over E and $\{w_1, w_2 \ldots w_n\}$ be a basis of E over F

If $u \in K$, then $\exists$ scalars $\alpha_1, \alpha_2 \ldots \alpha_m \in E$ st

$$u = \sum_{i=1}^{m} \alpha_i v_i \quad \text{---} (1)$$

also as $\alpha_i \in E \ \forall\ 1 \le i \le m$ and $\{w_1, w_2 \ldots w_n\}$ is basis of E over F,

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij} w_j \quad \text{where } \beta_j \in F \ \forall\ 1 \le j \le n$$

(from (1)) $$u = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} w_j \right) v_i$$

$$= \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} w_j \cdot v_i$$

Claim:- $\{ w_j v_i \}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ is basis of K over F

We need only to show that $\{ w_j v_i \}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ is L.I over F

to assume that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} w_j v_i = 0 \quad \text{where } c_{ij} \in F \ \forall\ i,j$$

$$\sum_{i=1}^{m} \lambda_i v_i = 0 \quad \text{where } \lambda_i = \sum_{j=1}^{n} c_{ij} w_j \in E$$

$$\Rightarrow \sum_{i=1}^{m} \lambda_i v_i \text{ is L.C of elements of basis of } K_E$$

$$\Rightarrow \lambda_i = 0 \quad \forall\ 1 \le i \le m$$

$$\Rightarrow \sum_{j=1}^{n} c_{ij} w_j = 0$$

a_j is zero $\Rightarrow c_{ij} = 0 \ \forall\ 1 \le j \le n \ \forall\ 1 \le i \le n$

$\Rightarrow \{ w_j v_i \}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ is basis of K_F

$$\Rightarrow [K:F] = mn = [K:E]\,[E:F] < \infty$$

Lemma:- Let E and F be field. Let $\sigma : F \to E$ be an embedding of F into E. Then $\exists$ a field k such that F is a subfield of k and σ can be extended to an isomorphism of k onto E.

Proof:- Let S be a set whose cardinality is same as of cardinality of $E - \sigma(F)$. and $S \cap F = \phi$

Now, Card S = Card $(E - \sigma(F))$

Let f be one-one, onto mapping from S to $E - \sigma(F)$

Let $K = F \cup S$

Define $\sigma^* : K \to E$ as follows

$$\sigma^*(a) = \begin{cases} \sigma(a) & \text{if } a \in F \\ f(a) & \text{if } a \notin F \end{cases}$$

then σ^* is extension of σ.

σ^* is 1-1, Let $\sigma^*(a) = \sigma^*(b)$

if $\sigma^*(a) = \sigma^*(b) \in \sigma(F)$

$\Rightarrow \sigma(a) = \sigma(b)$

$\Rightarrow a = b \quad (\because \sigma \text{ is 1-1})$

Scanned with CamScanner

If $\sigma^k(a) = \sigma^k(b) \in E - \sigma(F)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow a = b$

$\Rightarrow \sigma^*$ is 1-1

Hence the cardinality is same and 1-1 also, hence σ^* is onto.

$\sigma^* : K \to E$

for $a, b \in K$

$a+b = \sigma^{*-1}(\sigma^*(a) + \sigma^*(b))$ — (*)

$ab = \sigma^{*-1}(\sigma^*(a)\,\sigma^*(b))$ — (**)

$\sigma^*(a+b) = \sigma^*(a) + \sigma^*(b)$

$\sigma^*(a+b) = \sigma^*(\sigma^{*-1}(\sigma^*(a) + \sigma^*(b)))$

$= \sigma^*(a) + \sigma^*(b)$

$\sigma^*(ab) = \sigma^*(\sigma^{*-1}(\sigma^*(a)\,\sigma^*(b)))$

$= \sigma^*(a)\,\sigma^*(b)$

Theorem :- Let $p(x)$ be an irreducible polynomial in $F[x]$, then $\exists$ an extension E of F in which $p(x)$ has a root.

Eg: ① $x^2+1 \in \mathbb{Q}[x]$ irreducible {Here, $\mathbb{Q}[x] \to F[x]$}

$(x+i)(x-i) \Rightarrow \mathbb{C}[x]$ {$\mathbb{C}[x] \to E[x]$}

Root $\in \mathbb{C}[x]$

② $x^4 + 4x^2 + 4 \in \mathbb{Q}[x]$ Reducible.

$(x^2+2)(x^2+2)$

Proof :- As $F[x]$ is PID and $p(x)$ is irreducible

$\Rightarrow \langle p(x) \rangle$ is maximal ideal in $F[x]$ and hence

$\frac{F[x]}{\langle p(x) \rangle}$ is field.

Eg: $x^2+1 \in \mathbb{R}[x]$

$\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \to$ field.

$\cong \mathbb{R}[i] \cong \mathbb{C}$

Image of x: $x + \langle x^2+1 \rangle$, $x^2+1 = 0$, $x = i$

Scanned with CamScanner

$\sigma : F \to \frac{F[x]}{\langle p(x) \rangle} = E$

$\sigma(a) = a + \langle p(x) \rangle$ (By lemma)

then σ is embedding.

so every element a of F, can be treated as $a + \langle p(x) \rangle = \bar{a}$

Let $p(x) = a_0 + a_1 x + \dots + a_n x^n$; $a_i \in F$

$\Rightarrow \overline{p(x)} = \overline{a_0 + a_1 x + \dots + a_n x^n}$

$= \bar{a}_0 + \bar{a}_1 \bar{x} + \dots + \bar{a}_n \bar{x}^n$

$p(x) + \langle p(x) \rangle = a_0 + a_1 \bar{x} + \dots + a_n \bar{x}^n$

$\Rightarrow 0 + \langle p(x) \rangle = a_0 + a_1 \bar{x} + \dots + a_n \bar{x}^n$

$\bar{0} = a_0 + a_1 \bar{x} + \dots + a_n \bar{x}^n$

$\Rightarrow \bar{x}$ is a root of $p(x)$.

Theorem :- (Kronecker Theorem)

Let $f(x) \in F(x)$ be a non-constant polynomial. Then $\exists$ extension E of F in which $f(x)$ has a root.

Proof :- If $f(x)$ has a root in F

then $E = F$

If $f(x)$ does not have a root in F

$f(x) \in F[x] \to$ UFD

$\Rightarrow f(x)$ = product of irreducible polynomial over F and each irreducible polynomial has a root in some $E \supseteq F$

$\Rightarrow f(x)$ has a root in some extension E of F.

Notation :- Let $p(x)$ be an irreducible polynomial having a root say u, in an extension field E of F. We denote by $F(u)$ the subfield of E generated by F and u,

that is, the smallest field containing F and u.

Example :- $x^2 + 1 \in \mathbb{R}[x]$

$x = i$

$\mathbb{R}(i)$ ($\mathbb{R}(i)$ smallest field that contain given field and root)

E

(ii) $x^2 + 1 \in \mathbb{Q}[x]$

$x = i$

$\mathbb{Q}(i)$ element of $a(i)$

$\mathbb{Q}[i] = \frac{a}{b} + \frac{c}{d} i$

Proof :- Consider the mapping $\phi : F[x] \to E$ defined by

$\phi(a_0 + a_1 x + \dots + a_n x^n) = (a_0 + a_1 u + \dots + a_n u^n)$

then ϕ is homomorphism

$\ker \phi = \{ f(x) \in F[x] ; f(u) = 0 \}$

$\supseteq \{ p(x) \}$

as $\ker \phi \trianglelefteq F[x] \Rightarrow \ker \phi$ is a principal ideal

let $\ker \phi = \langle g(x) \rangle$ for some $g(x) \in F[x]$

as $p(x) \in \ker \phi \Rightarrow p(x) = g(x) h(x)$ for some $h(x) \in F[x]$

but $p(x)$ is irreducible

$\Rightarrow h(x)$ is a unit in $F[x]$

$\Rightarrow \deg h(x) = 0 \Rightarrow h(x) =$ constant $\in F$

$g(x) \cdot$ constant $= p(x) \Rightarrow g(x) = (\text{constant})^{-1} p(x)$

$\ker \phi = \langle g(x) \rangle = \langle p(x) \rangle$

$\phi : F[x] \to \phi(F[x])$

$\Rightarrow \frac{F[x]}{\langle p(x) \rangle} \cong \phi(F[x]) \cong F[u]$

$\Rightarrow F[u]$ is a field, hence $F[u] = F(u)$

If the degree of $p(x)$ is n.

then u can not satisfy a poly of deg $< n$.

$\Rightarrow [F[u] : F] = n$

Scanned with CamScanner

Corollary :-

Theorem :- Let $p(x)$ be an irreducible polynomial of degree n over F. Let u be a root of $p(x)$ in some extension E of F. Then,

(1) $F(u)$, the smallest field generated by F and u is same as $F[u]$

(2) $\{1, u, u^2, \ldots u^{n-1}\}$ form a basis of $F[u]$ over F and $[F(u) : F] = n$ = deg of $p(x)$

Example (1) $p(x) = x^2 + x + 1 \in Z_2[x]$
(irr poly)

$\Rightarrow p(x)$ has a root in $\frac{Z_2[x]}{\langle x^2+x+1 \rangle} \cong Z_2[u]$

$[Z_2[u] : Z_2] = 2$.

$Z_2[u] = \{a + bu ; a, b \in Z_2\}$

$= \{0, 1, u, 1+u\}$

(2) $x^2+1 \in R[x]$ irreducible over R.
If u is root of $p(x)$ in some extension E of R. Then, E has all the roots of $p(x)$
Let u be root of $p(x)$ in some extension E of R

$E = R[u] = \{a + bu ; a, b \in R\}$

now if u is root of x^2+1,
then $-u$ is also root of x^2+1

$-u \in E$

$\because -u = 0 + (-1)u$

Ex $p(x) = x^2 - x - 1 \in Z_3[x]$
show $p(x)$ is irreducible over $Z_3[x]$ & u is root of $p(x)$ in some extension E of Z_3. Then find all the elements of E.

Algebraic Extensions

Definition :- (Algebraic Element) :- Let E be an extension of F. Then an element $\alpha \in E$ is called algebraic over F if $\exists\ p(x) \in F[x]$ s.t. $p(\alpha) = 0$

Theorem :- Let E be an extension of F and $u \in E$ is algebraic over F. Let $p(x) \in F[x]$ be polynomial of least degree s.t. $p(u) = 0$. Then

(1) $p(x)$ is irreducible over F

Scanned with CamScanner

(2) If $g(x) \in F[x]$ s.t. $g(u) = 0$ then $p(x) \mid g(x)$

(3) There is exactly one monic poly. $p(x) \in F[x]$ of least deg s.t. $p(u) = 0$

$F = \mathbb{Q}$

$E = \mathbb{R}$

$u = \sqrt{2}$

$f(x) = x^2 - 2$

$g(x) = x^4 - 5x^2 + 6 = (x^2-2)(x^2-3)$

$h(x) = 2x^2 - 4$

Proof:- (1) Let $p(x)$ be reducible

$\Rightarrow p(x) = p_1(x)\, p_2(x)$, where $1 \le \deg p_1(x) < n$, $1 \le \deg p_2(x) < n$

$\Rightarrow p(u) = 0$ (given)

$\underbrace{p_1(u)}_{E}\,\underbrace{p_2(u)}_{E} = 0$

$\Rightarrow p_1(u) = 0$ or $p_2(u) = 0$

$\Rightarrow u$ satisfies a poly of deg $< n$ $\longrightarrow \longleftarrow$

(2) Apply DA on $g(x)$ and $p(x)$

$g(x) = p(x)\, q(x) + r(x)$ ——— (1)

where $r(x) = 0$ or $\deg r(x) < \deg p(x)$

$\Rightarrow g(u) = p(u)\, q(u) + r(u)$

$0 = 0 + r(u)$

$\Rightarrow r(u) = 0$

If $r(x) \neq 0 \Rightarrow r(x)$ is poly. of deg $< n$ s.t. $r(u) = 0$ $\longrightarrow \longleftarrow$

$\Rightarrow r(x) = 0$

Hence $p(x) \mid g(x)$ (from (1))

(3) Let $g(x)$ be the monic irreducible poly. of least deg s.t. $g(u) = 0$.

$\Rightarrow p(x) \mid g(x)$

and $g(x) \mid p(x)$

$\Rightarrow$

(3) let $g_1(x)$ and $g_2(x)$ be two monic irr. poly. of least deg s.t. $g_1(u) = 0 = g_2(u)$

then by (2) $g_1(x) \mid g_2(x)$

$g_2(x) \mid g_1(x)$

$\Rightarrow g_1(x) = g_2(x)$ (∵ both $g_1(x)$ and $g_2(x)$ are monic)

The monic irreducible poly in $F[x]$ of which u is a root will be called the minimal polynomial of u over F

An extension field E of F is called an Algebraic extension if each element of E is Algebraic over F. and extensions which are not Algebraic extension are called Transcedental extension $\{\pi, e\}$

Theorem:- If E is finite extension of F. Then E is algebraic extension of F.

Proof:- Let $[E:F] = n$ (say)

Let $u \in E$

then $\{1, u, u^2, \ldots, u^n\}$ is linearly dependent over F

$\exists\ a_0, a_1, \ldots, a_n \in F$ s.t.

$a_0 \cdot 1 + a_1 u + \ldots + a_n u^n = 0$ where not all a_i's $= 0$

$\Rightarrow u$ is the root of the poly $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$

Scanned with CamScanner

⇒ u is algebraic over F
⇒ E is algebraic extension of F

Theorem If E is algebraic extension of F and $u \in E$ is algebraic over F, then $F(u)$ is algebraic extension of F.

Proof:- Let $p(x)$ be the union monic irreducible polynomial of u over F.
and $\deg(p(x)) = n$

$$[F(u) : F] = \deg(p(x)) = n$$

⇒ $F(u)$ is finite extension of F
⇒ $F(u)$ is algebraic extension of F

converse

Algebraic Extension may not be finite extension

$F = \mathbb{Q}$
and $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5} \ldots)$
$= \mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5}) \ldots$

$x^2 - 2$ is of degree 2

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$
$$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$
$$= 2 \times 2 = 4$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq \ldots \subseteq E$$

$$[E : F] = [E : E_0][E_0 : E_1] \ldots [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$
$x = \sqrt{p}$ is of degree 2

Suppose field E_1 is finite
$E_1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2} \ldots \sqrt{p_n})$
$E_1 \neq E$

By induction, If $n=0$, then $E_1 = \mathbb{Q}$
then $\sqrt{2} \in E$, but $\sqrt{2} \notin \mathbb{Q}$

$\sqrt{2} \notin \mathbb{Q}$ (reason)
$\sqrt{2} = \frac{p}{q}$ $(p,q) = 1$, $q \neq 0$
$2 = \frac{p^2}{q^2}$
$2q^2 = p^2$ — (i)
$\Rightarrow p^2$ is even
$\Rightarrow p$ is even
$\Rightarrow p = 2k$
$2q^2 = 4k^2$
$q^2 = 2k^2$
$\Rightarrow q^2$ even
$\Rightarrow q$ is even
$\Rightarrow q = 2t$
Thus we get (p,q) ≠ Not same

Let the result be true for $n-1$.
$\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2} \ldots \sqrt{p_{n-1}}) \neq E$
$F_0 \qquad E_0$

TP. $E_0(\sqrt{p_n}) \neq E$
Let q be a prime s.t $q \neq p_i$ for $1 \leq i \leq n$
Claim $\sqrt{q} \in E$ but $\sqrt{q} \notin F_0$
Let $\sqrt{q} \in F_0$
$\Rightarrow \sqrt{q} = a + b\sqrt{p_n}$, where $a, b \in E_0$
$\Rightarrow q = a^2 + b^2 p_n + 2ab\sqrt{p_n}$
$\Rightarrow \sqrt{p_n} = \frac{q - a^2 - b^2 - p_n}{2ab} \in E_0$

Finitely generated Extension:- An extension E of F is called finitely generated if $\exists$ a finite number of elements $u_1, u_2 \ldots u_n \in E$ s.t smallest subfield of E containing F and $u_1, u_2 \ldots u_n$ is E itself and we write $E = F(u_1, u_2 \ldots u_n)$

Example finitely generated extension need not be algebraic and need not be finite.
F - field
$F[x] \rightarrow$ polynomial ring over F

Scanned with CamScanner

$E = F(x)$

= field of quotient of $F[x]$

$= \left\{ \frac{p(x)}{q(x)} , p(x), q(x) \in F[x] \text{ but } q(x) \neq 0 \right\}$

$\mathbb{Q} = \left\{ \frac{p}{q} , p, q \in \mathbb{Q}, q \neq 0 \right\}$

E is finitely generated extension of F.
If E is algebraic extension of F, then
x satisfies some polynomial over F.
which is not true as x is a variable
Further E is also not finite ext. of F
(∵ if E is finite ext. of F)
then $[E:F]$ = deg (minimpoly. of x) but
x does not satisfy any poly. over F.

Theorem :- Let $E = F[u_1, u_2 \ldots u_n]$ be a finitely generated ext. of F. such that each u_i is algebraic over F. Then E is finite and hence algebraic extension of F.

Proof :- Let $E_i = F[u_1, u_2 \ldots u_i] \; \forall \; 1 \leq i \leq n$
If u_2 is algebraic over F.
$\Rightarrow u_2$ is algebraic over $F(u_1)$ $\forall 2 \leq i \leq n$
In general, each u_i is algebraic over E_{i-1}
as $F \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_{n-1} \subseteq E_n = E$

$[E:F] = [F(u_1, u_2 \ldots u_n) : F]$

$= [F(u_1, u_2 \ldots u_n) : F(u_1, u_2 \ldots u_{n-1})]$

$[E:F] = [E_n : F]$

$[E_n : E_{n-1}] [E_{n-1} : F] = [E_n : E_{n-1}] [E_{n-1} : E_{n-2}]$

$\ldots\ldots [E:F]$

$= n_n \times n_{n-1} \times \ldots \times m_1$, where n_i is the deg of minimal polynomial of u_i over E_{i-1} $\forall \; 1 \leq i \leq n$

= finite

$\Rightarrow E$ is algebraic extension of F.

Theorem :- Let E be an extension of F. If K is subset of E, consisting of all those elements of E, which are alg. over F. Then K is a subfield of E and an algebraic extension of F.

Proof :- Let $a, b \in K$, $a \neq 0$.
TP that K is subfield of E, we need to show that $a-b$, ab, $a^{-1} \in K$.
ie $a-b$, ab, a^{-1} are alg. over F.
$F(a,b)$ is alg. ext. of F
$\Rightarrow a-b$, ab, $a^{-1} \in F(a,b)$ (∵ $F(a,b)$ is field)
and $a-b$, ab, a^{-1} are alg. over F.

Definition :- The subfield K consisting of all elements of E, which are algebraic over F, is called algebraic closure of F in E.

Definition :- Let K and L be extension fields of a field F then a non zero homomorphism.
$\sigma : K \to L$ st. $\sigma(a) = a \; \forall \; a \in F$
is called an F- homomorphism of K into L.

Scanned with CamScanner

F-homomorphism.

Examples: $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{3})$

$\sigma : K \to L$

$$\sigma(a) = \begin{cases} a & \text{if } a \in \mathbb{Q} \\ \sqrt{3} & \text{if } a = \sqrt{2} \end{cases}$$

Thm: Let E be an algebraic Extension of F and $\sigma : E \to E$ be an F-embedding of E into itself over F. Then σ is onto and hence an automorphism of E.

Proof: Let $a \in E$

$\Rightarrow a$ is algebraic over F

Let $p(x)$ be minimal polynomial of a over F

Let E' be the subfield of E containing F and generated over F by all roots of $p(x)$ which lie in E.

$\Rightarrow E'$ is finitely generated by elements which are algebraic over F.

$\Rightarrow E'$ is finite and hence algebraic ext. of F.

$\sigma : E \to E$

If b is root of $p(x) = a_0 + a_1 x + \dots + a_n x^n \in F[x]$

$\Rightarrow a_0 + a_1 b + \dots + a_n b^n = 0$

$\Rightarrow \sigma(a_0 + a_1 b + \dots + a_n b^n) = \sigma(0) = 0$

$\Rightarrow \sigma(a_0) + \sigma(a_1)\sigma(b) + \dots + \sigma(a_n)\sigma(b^n) = 0$

$\Rightarrow a_0 + a_1 \sigma(b) + \dots + a_n (\sigma(b))^n = 0$

$\Rightarrow p(\sigma(b)) = 0$

$\Rightarrow \sigma(b)$ is also a root of $p(x)$

$\Rightarrow \sigma(E') \subseteq E'$

Further $\sigma(E') \cong E'$ $\{ \because \sigma$ is $1\text{-}1 \}$

$\Rightarrow [\sigma(E') : F] = [E' : F]$

$\Rightarrow \sigma(E')$ is subspace of E'

$\Rightarrow \sigma(E') = E'$ $\exists$ some $c \in E'$ s.t. $a = \sigma(c)$

So σ is automorphism.

$\mathbb{Q} \subseteq \mathbb{Q}(2^{1/3})$

$x = 2^{1/3}$

$x^3 - 2 = 0$

$2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2$

UNIT - 3

Def: A field K is called algebraically closed if it possesses no proper algebraic extension.

Theorem: For any field K, the following conditions are equivalent —

(1) K is algebraically closed.

(2) Every irreducible polynomial in $K[x]$ is of degree 1.

(3) Every polynomial in $K[x]$ of positive degree factors completely in $K[x]$ in

Scanned with CamScanner

$$y_i = \begin{cases} 0 & \text{if } x_{ii} = 1 \\ 1 & \text{if } x_{ii} = 0 \end{cases} \quad \forall\ i \in \mathbb{Z}_+$$

$$\Rightarrow \quad \left.\begin{array}{l} y \neq f(1) \\ y \neq f(2) \\ \vdots \\ y \neq f(3) \\ \vdots \end{array}\right\}$$

$\Rightarrow$ y has no pre-image

$\longrightarrow\ \longleftarrow$ to the fact that $f : \mathbb{Z}_+ \longrightarrow X^{\omega}$ is a surjective map

Our supposition was wrong

Thus, X^{ω} is not countable

$\Rightarrow$ X^{ω} is uncountable.

Exercise :- Show that the set S of all functions $f : \mathbb{Z}_+ \longrightarrow \{0, 1\}$ is uncountable

$S = \{ f \mid f : \mathbb{Z}_+ \longrightarrow \{0, 1\} \}$, S - uncountable

Exercise :- Show that the set of polynomials with rational coefficients is a countable set

Topological Space

Let X be a non empty set

A collection $\mathcal{T}$ of subsets of X, is said to be a Topology on X if it satisfies the following properties —

TS1 $\phi, X \in \mathcal{T}$

TS3 Finite intersection of members of $\mathcal{T}$ is again in $\mathcal{T}$

Scanned with CamScanner

7/oct/21

Unit-3

PAGE NO.:
DATE: / /

Definition:- A field K is called algebraically closed if it possesses no proper algebraic extension.

- $\mathbb{R} \subseteq \mathbb{C}$

  $x = i$

  $x^2 + 1 = 0$

  $\mathbb{R} \subseteq \mathbb{R}(i)$

  $\mathbb{R}$ is not algebraically closed and $\mathbb{R}(i)$ is algebraically closed.

Eg:- $\mathbb{C}$ is algebraically closed
(field of complex numbers)

Thm:- For any field K, the following are equivalent
(1) K is algebraically closed
(2) Every irreducible polynomial in $K[x]$ is of degree 1
(3) Every polynomial in $K[x]$ of positive degree factors completely in $K[x]$ in linear factors.
(4) Every polynomial in $K[x]$ of +ve degree has atleast one root in K.

proof:- (1) $\Rightarrow$ (2)

Let $p(x) \in K[x]$ be irreducible polynomial
let $\deg(p(x)) = n$
$\Rightarrow \exists$ a field E s.t $p(x)$ has a root in E and $[E:K] = n$
$\Rightarrow$ E is finite extension of K
$\Rightarrow$ E is algebraic extension of K
but K is algebraically closed
$\Rightarrow E = K \Rightarrow [E:K] = [E:E] = 1$
Hence $n = 1$.

(2) $\Rightarrow$ (3)

Let $f(x) \in K[x]$ be any polynomial of +ve degree n

Scanned with CamScanner

If $n=1$, then $f(x)$ is already linear.
If $n \geq 2$ then $f(x)$ is reducible
$\Rightarrow f(x) = f_1(x) f_2(x)$ where $1 \leq \deg f_1(x) < n$
$1 \leq \deg f_2(x) < n$
Keep on doing this procedure for polynomials $f_1(x)$ & $f_2(x)$, we get that $f(x)$ factors into linear polynomials.

(3) $\Rightarrow$ (4)
Let $f(x) \in K[x]$ be a polynomial of +ve degree say n.
by (3), $f(x) = (a_1x+b_1)(a_2x+b_2)\ldots\ldots(a_nx+b_n)$
where each $a_ix+b_i \in K[x]$; $a_i \neq 0$
then $-\frac{b_i}{a_i} \in K$ and these are all the roots of $f(x)$

(4) $\Rightarrow$ (1)
Let $K \subseteq E$ and E be algebraic extension of K
$\Rightarrow$ If $u \in E$, then u is algebraic over K
$\Rightarrow \exists$ some $p(x) \in K[x]$ $\xleftarrow{\deg p(x) = n}$ s.t $p(u) = 0$
$\Rightarrow$ By (4), we can write
$p(x) = (a_1x+b_1)\, p_1(x)$
where $a_1, b_1 \in K$, $p_1(x) \in K[x]$ and $\deg p_1(x) = \deg p(x) - 1$
again by (4),
$p_1(x) = (a_2x+b_2)\, p_2(x)$
where $a_2, b_2 \in K$, $p_2(x) \in K[x]$, $\deg p_2(x) = \deg p_1(x) - 1$

doing this procedure n times, we get

$p(x) = (a_1x+b_1)(a_2x+b_2)\ldots\ldots(a_nx+b_n)$
where $a_i \neq 0$, $a_i, b_i \in K$ $\forall i$
$\Rightarrow$ all roots of $p(x)$ lie in K
$\Rightarrow u \in K$
Hence $E \subseteq K$
also $K \subseteq E$, hence $E = K$
Hence, K is algebraically closed

Def^n:- If F is a subfield of field E, then E is called algebraic closure of F if
(i) E is an algebraic extension of F
(ii) E is algebraically closed

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3})$
$\mathbb{Q}$ → not algebraically closed

$\mathbb{R} \subseteq \mathbb{C}$ → algebraically closed
$\mathbb{R}$ not algebraically closed
$\Rightarrow \mathbb{C}$ is algebraic closure of $\mathbb{R}$ i.e. biggest algebraic extension over $\mathbb{R}$

Lemma (★) :- Let F be a field and $\sigma : F \to L$ be an embedding of F into an algebraically closed field L. Let $E = F(\alpha)$ be an algebraic extension of F. Then σ can be extended to an embedding $\eta : E \to L$ and the number of such extensions is equal to the number of distinct roots of the minimal polynomial of α.

proof :- Let $p(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n \in F[x]$ be the minimal polynomial of α.
define $p^\sigma(x) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_{n-1})x^{n-1} + x^n \in L[x]$
Let β be the root of $p^\sigma(x)$ in L

$\eta : F(\alpha) \to L$
$\eta(b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1})$
$= \sigma(b_0) + \sigma(b_1)\beta + \ldots + \sigma(b_{n-1})\beta^{n-1}$
(then η is extension of σ)

$u \to p(x)$
$[F(u) : F] = n$
$\{1, u, u^2, \ldots u^n\}$

Then η is a well defined mapping
η is a homomorphism
$\eta\left(\sum_{i=0}^{n-1} b_i\alpha^i + \sum_{i=0}^{n-1} c_i\alpha^i\right) = \eta\left(\sum_{i=0}^{n-1}(b_i+c_i)\alpha^i\right) = \sum_{i=0}^{n-1}\sigma(b_i+c_i)\beta^i$

$= \sum_{i=0}^{n-1}\sigma(b_i)\beta^i + \sum_{i=0}^{n-1}\sigma(c_i)\beta^i$

Scanned with CamScanner

$$= \eta\left(\sum_{i=0}^{n-1} b_i\alpha^i\right) + \eta\left(\sum_{i=0}^{n-1} c_i\alpha^i\right)$$

$$\eta\left[\left(\sum_{i=0}^{n-1} b_i\alpha^i\right)\left(\sum_{j=0}^{n-1} c_j\alpha^j\right)\right] = \eta\left(\sum_{i+j=k} (b_ic_j)\alpha^{i+j}\right) = \sum_{k}\sum_{i+j=k} (b_ic_j)\beta^{i+j}$$

$$= \sum_{k}\sum_{i+j=k} \sigma(b_ic_j)\beta^{i+j}$$

$$= \sum_{k}\sum_{i+j=k} \sigma(b_i)\sigma(c_j)\beta^i\beta^j$$

$$= \left(\sum_{i=0}^{n-1} \sigma(b_i)\beta^i\right)\left(\sum_{j=0}^{n-1} \sigma(c_j)\beta^j\right)$$

(Last page)

η is 1-1 map

$$\eta\left(\sum_{i=0}^{n-1} b_i\alpha^i\right) = \eta\left(\sum_{i=0}^{n-1} c_i\alpha^i\right) \Rightarrow \sum_{i=0}^{n-1} \sigma(b_i)\beta^i = \sum_{i=0}^{n-1} \sigma(c_i)\beta^i$$

$$\Rightarrow \sigma(b_i) = \sigma(c_i)$$

$$\Rightarrow b_i = c_i$$

$$\Rightarrow \sum_{i=0}^{n-1} b_i\alpha^i = \sum_{i=0}^{n-1} c_i\alpha^i$$

Thus, η is an embedding of $F(\alpha)$ into $\Rightarrow$ η extends σ $\because \eta(a) = \sigma(a)\ \forall a \in F$

18 Oct '21

Zorn's Lemma

The whole set may not be ordered with respect to some relation but its subset can be ordered with respect to that relation

Partially Ordered Set – A set S with relation '$\leq$' is called partially ordered set if
S has reflexive property w.r.t '$\leq$'
S has anti-symmetric property – If $a \leq b$ & $b \leq a$ then $a = b$
S has transitive property – If $a \leq b$, $b \leq c \Rightarrow a \leq c$

Chain :- A chain in a partially ordered set S, is a subset of S say C, where if $a, b \in C$ then either $a \leq b$ or $b \leq a$

Upper bound of a Chain – An element $u \in S$ is called an upper bound of chain C if $a \leq u\ \forall a \in C$

Maximal Element of S – An element $m \in S$ is called maximal element of S if $m \leq a$, $a \in S \Rightarrow m = a$

Zorn's lemma – If each chain in a Poset S has an upper bound, then S has a maximal element.

$\alpha \in E$
$\alpha \notin K \neq E$
F
$\sigma: F \to L$
$\sigma: K \to L$

Thm– Let E be an algebraic extension of a field F and let $\sigma: F \to L$ be an embedding of F into algebraically closed field L. Then σ can be extended to an embedding $\eta: E \to L$.

Proof:- Let S be the set of all pairs (K, θ) where K is a field s.t $F \subseteq K \subseteq E$ and θ is extension of σ from K to L.

$S \neq \phi$ $\because (F, \sigma) \in S$

define $(K, \theta) \leq (K', \theta')$ iff $K \subseteq K'$ and $\theta'|_K = \theta$

Because $(F, \sigma) \in S$, $S \neq \phi$. Also, if $\{(K_i, \theta_i)\}$ is a chain in S, we set $K = \cup K_i$ and define θ on K as follows.

let $a \in K$. Then $a \in K_i$ for some i and we define

$\theta(a) = \theta_i(a)$

θ is well defined

Let $a \in K_i$ and $a \in K_j$. Because either $K_i \subset K_j$ or $K_j \subset K_i$ by def^n of a chain in S, we get $\theta_i(a) = \theta_j(a)$.

Hence, θ is well-defined.

Let $C = \{(K_i, \theta_i)\}$ be some chain in S

Take $K = \cup K_i$ and $\theta: K \to L$ as $\theta(a) = \theta_i(a)$ if $a \in K_i$

claim :- (K, θ) is upper bound of C

if $(K_i, \theta_i) \in C$ then $(K_i, \theta_i) \leq (K, \theta)$ which is obvious $\because K_i \subseteq K$ and $\theta|_{K_i} = \theta_i$ (by def^n of θ)

$(K_1, \theta_1) \leq (K_2, \theta_2) \leq \ldots \cup K_i, \theta$

$\theta: \cup K_i \to L$

$\theta(a) = \theta_i(a)$

So by zorn's lemma, S has a maximal element say (K, η)

claim :- $K = E$

let $K \neq E$

$\Rightarrow \exists$ some $\alpha \in E$ s.t $\alpha \notin K$ where α is alg. over F as $F \subseteq K$

$\Rightarrow \alpha$ is alg. over K also.

So, by previous lemma, η can be extended to $\bar{\eta}: K(\alpha) \to L$

Scanned with CamScanner

$\Rightarrow (K(\alpha), \eta^*) \in S$
and $(K, \eta) \leq (K(\alpha), \eta^*)$
$\Rightarrow K(\alpha) = K$
$\Rightarrow \alpha \in K$
$\longrightarrow\!\leftarrow$
$\Rightarrow E = K$

Thm– Let K and K' be algebraic closures of a field F. Then $K \cong K'$ under an isomorphism that is an identity on F. $\sigma: K \to K'$ $\sigma(a) = a \ \forall a \in F$

Proof– $F \subseteq K$, $F \subseteq K'$
Let $\sigma: F \to K'$ defined by $\sigma(a) = a \ \forall a \in F$ is an embedding
By previous thm, σ can be extended to $\sigma^*: K \to K'$
$\Rightarrow K \cong \sigma^*(K) \leq K'$ also $F \subseteq \sigma^*(K) \leq K'$
also K' is algebraic extension of F $\Rightarrow$ K' is algebraic extension of $\sigma^*(K)$ also but $\sigma^*(K)$ is algebraically closed as $\sigma^*(K) \cong K$
$\Rightarrow \sigma^*(K) = K'$
$\Rightarrow \sigma^*$ is onto also
$\Rightarrow K \cong K'$

21/10/21

Def Splitting field –

Def^n– Let $f(x)$ be some polynomial in $F[x]$ of degree ≥ 1. Then an extension K of F is called splitting field of $f(x)$ over F if
1. $f(x)$ factors into linear factors in $K[x]$ i.e. $f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$; $\alpha_i \in K$
2. $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ i.e. K is generated over F by all roots of $f(x)$ in K.

Eg: $F = \mathbb{Q}$
$x^2 - 2 \in \mathbb{Q}[x]$ $\quad x^3 - 3 \in \mathbb{Q}[x]$

$(x-\sqrt{2})(x+\sqrt{2})$ → factors
$\mathbb{Q}(\sqrt{2})$ – splitting field.

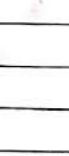
Properties of Splitting field

Thm– If K is splitting field of $f(x) \in F[x]$ over F. Then K is finite extension and hence an algebraic extension of F.

Proof– Let $\deg f(x) = n$. Then $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where α_i's are roots of $f(x)$.
Then K is finitely generated extension of F and each α_i is algebraic over F.
$\Rightarrow$ K is finite extension of F.
Hence, K is algebraic extension of F.

Thm– Uniqueness of Splitting field – Let K be splitting field of polynomial $f(x) \in F[x]$ over F. If E is another splitting field of $f(x)$ over F, then there exist an isomorphism $\sigma: E \to K$ that is identity on F. ($\sigma: E \to K$ $\forall a \in F$)

Proof– Let $\bar{K}$ be algebraic closure of K. Then $\bar{K}$ is algebraic extension of K. Also K is algebraic extension of F. So, $\bar{K}$ is algebraic extension of F.
Also $\bar{K}$ is algebraic closed $\Rightarrow \bar{K}$ is algebraic closure of F
$\Rightarrow \bar{K} = \bar{F}$



Let $\sigma: F \to \bar{K}$ be defined by
$\sigma(a) = a$
Then, σ is embedding
So by (*), we can extend σ to $\sigma^*: E \to \bar{F}$
and σ^* is embedding
$\Rightarrow \sigma^*: E \to \sigma^*(E)$ is isomorphism
claim: $\sigma^*(E) = K$
Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$

Scanned with CamScanner

Splitting field is ...

PAGE NO. :
DATE : / /

$f^{\sigma^*}(x) = \sigma^*(a_0) + \sigma^*(a_1)x + \dots + \sigma^*(a_n)x^n$

$= a_0 + a_1x + \dots + a_nx^n$

$\Rightarrow f^{\sigma^*}(x) = f(x)$

Let $f(x) = c(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ with α_i's $\in E$

$f^{\sigma^*}(x) = \sigma^*(c)(x-\sigma^*(\alpha_1))(x-\sigma^*(\alpha_2))\dots(x-\sigma^*(\alpha_n))$,
$f(x)$ $\sigma^*(\alpha_i) \in \bar{K}$

but since $f(x)$ has a factorisation in K, say

$f(x) = c(x-\beta_1)(x-\beta_2)\dots(x-\beta_n)$; β_j's $\in K \subseteq \bar{K}$

$\Rightarrow \{\beta_1, \beta_2, \dots, \beta_n\}$ and $\{\sigma^*(\alpha_1), \sigma^*(\alpha_2), \dots, \sigma^*(\alpha_n)\}$ are same

$K = F(\beta_1, \beta_2, \dots, \beta_n)$

$= F(\sigma^*(\alpha_1), \dots, \sigma^*(\alpha_n))$

$= \sigma^*(F(\alpha_1, \alpha_2, \dots, \alpha_n))$

$= \sigma^*(E)$

Eg - $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ By Eisenstein criteria $x^3 - 2 \in \mathbb{Q}[x]$ is irr over $\mathbb{Q}$.
$p = 2$
$2 \mid 2$, $p \nmid 1$
$p^2 = 4 \Rightarrow 4 \nmid 2$

$x^3 - 2 = (x - 2^{1/3})(x^2 + 2^{1/3}x + 2^{2/3})$

$x - 2^{1/3} = 0$

$x = 2^{1/3}$ $\therefore$ it is the min poly of $2^{1/3}$.

$2^{1/3}, \alpha = a+ib, \bar{\alpha} = a-ib$

$[\mathbb{Q}(2^{1/3}, \alpha) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}, \alpha) : \mathbb{Q}(2^{1/3})][\mathbb{Q}(2^{1/3}) : \mathbb{Q}]$

$= [\mathbb{Q}(2^{1/3}) : \mathbb{Q}]$

$= 2 \times 3 = 6$

$\mathbb{Q}(2^{1/3}, \alpha)$
| basis $\{1, \alpha\}$
$\mathbb{Q}(2^{1/3})$
| basis $\{1, 2^{1/3}, 2^{2/3}\}$
$\mathbb{Q}$

$\Rightarrow$ Basis

$f(\alpha) = \mathbb{Q}(2^{1/3}, \alpha) \to \{1, \alpha\}$

$f = \mathbb{Q}(2^{1/3}) \to \{1, 2^{1/3}, 2^{2/3}\}$

$\mathbb{Q}\{1, \alpha, 2^{1/3}, 2^{1/3}\alpha, 2^{2/3}, 2^{2/3}\alpha\}$

This set is α.I

Eg - The splitting field of $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/4}, i)$ and its degree of extension is 8.

soln - $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$. We find $f(x)$ has a root $2^{1/4}$. So, $f(x)$ is the minimal poly. of $2^{1/4}$ over $\mathbb{Q}$. Thus,

$[\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = 4$ the degree of $f(x)$

Now $f(x) = (x - 2^{1/4})(x + 2^{1/4})(x^2 + 2^{1/2})$ and $x^2 + 2^{1/2}$ is irreducible over $\mathbb{Q}(2^{1/4})$. Thus, the root $2^{1/4}i$ has $x^2 + 2^{1/2}$ as its minimal polynomial over $\mathbb{Q}(2^{1/4})$, whence

$[\mathbb{Q}(2^{1/4})(2^{1/4}i) : \mathbb{Q}(2^{1/4})] = 2$

Because $\mathbb{Q}(2^{1/4})(2^{1/4}i) = \mathbb{Q}(2^{1/4}, i)$ is clearly the splitting field and

$[\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}] = [\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}(2^{1/4})][\mathbb{Q}(2^{1/4}) : \mathbb{Q}]$

$= 4 \cdot 2 = 8$

We have completed the solution. We illustrate it in the following diagram:

$\mathbb{Q}(2^{1/4}, i)$
| basis $\{1, 2^{1/4}, 2^{1/2}, 2^{3/4}\}$
$\mathbb{Q}(2^{1/4})$
| basis $\{1, 2^{1/4}, 2^{1/2}, 2^{3/4}\}$
$\mathbb{Q}$

25/04/21

Example - Let p be prime. $f(x) = x^p - 1 \in \mathbb{Q}[x]$. Find splitting field K of $f(x)$ and $[K : \mathbb{Q}]$

soln :

$f(x) = x^p - 1$

$= (x-1)(1 + x + x^2 + \dots + x^{p-1})$

[Roots : $1, \alpha$] clearly, 1 is root of $f(x)$

Let $\alpha (\neq 1)$ be another root of $f(x)$

claim - $\alpha, \alpha^2, \dots, \alpha^{p-1}$ are distinct roots of $f(x)$

α is root of $f(x) = \alpha^p - 1 = 0$

$f(\alpha^i) = (\alpha^i)^p - 1$

$= (\alpha^p)^i - 1$

$= 1^i - 1 = 0$

Let $\alpha^i = \alpha^j$ for some $1 \le i < j \le p-1$

$\alpha^{p-1} = 0$
$x^{p-1} = 1$
$x = (1)^{\frac{1}{p-1}}$
$= (\cos 0 + i \sin 0)^{\frac{1}{p-1}}$
$= \cos\frac{2n\pi}{p-1} + i\sin\frac{2n\pi}{p-1}$
$= e^{\frac{2n\pi i}{p-1}}$, $n = 0, 1, \dots, p-2$

Scanned with CamScanner

$\Rightarrow \alpha^{j-i} = 1$

$\Rightarrow p \mid j-i$ $\quad \rightarrow \leftarrow$

$\Rightarrow \mathbb{Q}[\alpha]$ is the splitting field

$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ = deg of min. poly of $\alpha = p-1$

Eg – Let $F = \mathbb{Z}_2$. Prove that S.f of $x^3+x^2+1 \in F[x]$ is a finite field with 8 elements.

$f(x) = x^3+x^2+1 \in \mathbb{Z}_2[x]$ $\quad x^2+1 = x^2-1 \in \mathbb{Z}_2[x]$ $= \{0,1\}$

$f(0) = 1 \neq 0$ in $\mathbb{Z}_2$ $\quad 2=0$, $1=-1$

$f(1) = 3 = 1 \neq 0$ in $\mathbb{Z}_2$ $\quad (x-1)(x+1)$

Let α be a root of $f(x)$ in some extension field of $\mathbb{Z}_2$.

$f(\alpha) = 0$

$\Rightarrow 1+\alpha^2+\alpha^3 = 0$

$1+x^2+x^3 = (x-\alpha)(x^2+(1+\alpha)x+\alpha+\alpha^2)$

$f(x) = (x-\alpha)(x+\alpha^2)(x+1+\alpha+\alpha^2)$

S.f $= \mathbb{Z}_2[\alpha]$

	x^3	x^2	x	Const.
α	1	1	0	1
$\downarrow \alpha$		α	$\alpha+\alpha^2$	$\alpha^2+\alpha^3$
1		$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2+\alpha^3 = 0$

$[\mathbb{Z}_2[\alpha] : \mathbb{Z}_2] = 3$

	a	b	c
a	a^2	ab	ac
b	ba	b^2	bc
c	ca	cb	c^2

$\mathbb{Z}_2[\alpha] = \{a+b\alpha+c\alpha^2 ; a,b,c \in \mathbb{Z}_2\}$

Normal Extension

Defⁿ – An extension E of a field F is called normal extension if one of the following two conditions hold:

(1) Every irr. poly. in $F[x]$, that has a root in E, splits in linear factors in E.

(2) E is a splitting field of a family of polynomials over F.

Example – 1. $F = \mathbb{R}$; $E = \mathbb{C}$ — Normal Extension

2. $F = \mathbb{Q}$; $E = \mathbb{Q}(2^{1/3})$

$\alpha = 2^{1/3}$

$x^3 - 2 = 0$

Roots are $2^{1/3}$, $2^{1/3}\omega$, $2^{1/3}\omega^2 \notin \mathbb{Q}(2^{1/3})$

$\Rightarrow$ Not a normal Extension

Eg – $F = \mathbb{Q}$

$\alpha = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$

$E = \mathbb{Q}(\alpha)$

$x = \alpha = e^{i\frac{\pi}{4}}$

$x^4 = -1 \Rightarrow 1+x^4 = 0$ is the irreducible polynomial which satisfies

$\Rightarrow x = (\cos\pi + i\sin\pi)^{1/4}$

α is root of irr. poly $1+x^4 = 0$

Eg – $[\mathbb{C} : \mathbb{R}] = 2$

Any extension of degree 2 is always a normal Extension.

RESULT – Let F be a field. Any Extension E of F s.t $[E:F] = 2$ is normal extension.

Pf – as $[E:F] = 2 \Rightarrow$ E is algebraic Extension of F.

If $\alpha \in E \setminus F$ then α satisfies some polynomial over F.

and $F \subset F(\alpha)$

$[E:F] = [E:F(\alpha)]\,[F(\alpha):F]$

$2 = [E:F(\alpha)] \times 2$

$\Rightarrow [E:F(\alpha)] = 1$

$\Rightarrow E = F(\alpha)$

Scanned with CamScanner

Let $f(x)$ be minimum poly. of α

$f(x) = x^2 + ax + b \in F[x]$

Let β be another root of $f(x)$

$\alpha + \beta = -a$

$\beta = -a - \alpha \in F(\alpha) = E$

Converse of this thm is not true.

30/Oct/21

Multiple Roots

$\frac{df}{dx} = 0 \Rightarrow f = C$ $\quad f(x) = x^5 \quad F = \mathbb{Z}_5$

$f'(x) = 5x^4$

$= 0$

Def^n – Let K be a splitting field of a polynomial $f(x) \in F[x]$. Let α be a root of $f(x)$ in K. Then $(x-\alpha) | f(x)$ in $K[x]$.

$x^2+1 \in R[x]$

$R[i] = \mathbb{C}$ $\quad [x^2+1 = (x-i)(x+i)]$

$(x-i) | x^2+1$ in $\mathbb{C}$

If n is the highest power of $(x-\alpha)$ s.t $(x-\alpha)^n | f(x)$ in $K[x]$ then α is called a root of multiplicity n. If $n=1$, then α is called simple root.

Result – (1) $(f(x)+g(x))' = f'(x) + g'(x)$

(2) $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$

Theorem – Let $f(x) \in F[x]$ be a polynomial of deg ≥ 1 with α as a root. Then α is a multiple root iff $f'(\alpha) = 0$

proof – Let α be a root of $f(x)$ s.t $f'(\alpha) = 0$

$\Rightarrow f(x) = (x-\alpha)g(x) + r(x) = 0$ (By division algorithm)

$\Rightarrow f'(x) = (x-\alpha)g'(x) + g(x)$

$\Rightarrow f'(\alpha) = g(\alpha)$

$\Rightarrow g(\alpha) = 0$

$\Rightarrow x - \alpha$ is a root of $g(x)$.

$\Rightarrow g(x) = (x-\alpha)h(x)$

$\Rightarrow f(x) = (x-\alpha)^2 h(x)$

$\Rightarrow (x-\alpha)^2 | f(x)$

$\Rightarrow \alpha$ is a multiple root of $f(x)$.

Converse :– Let α be a multiple root of $f(x)$

$\Rightarrow (x-\alpha)^2 | f(x)$

$\Rightarrow f(x) = (x-\alpha)^2 g(x)$

$\Rightarrow f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$

$\Rightarrow f'(\alpha) = 0$

Cor – Let $f(x)$ be an irreducible polynomial over F. Then $f(x)$ has a multiple root iff $f'(x) = 0$.

proof – Let a be leading coefficient of $f(x)$

$\Rightarrow p(x) = a^{-1} f(x)$ is monic irreducible polynomial.

If α is root of $p(x)$, then $p(x)$ is minimal polynomial of α.

If α is multiple root of $p(x) \Rightarrow p'(\alpha) = 0$

$\Rightarrow \alpha$ satisfies $p'(x)$

$\Rightarrow p(x) | p'(x)$

Which is possible only when $p'(x) = 0$

$(\because \deg p'(x) < \deg p(x))$

$\Rightarrow (a^{-1} f(x))' = 0$

$\Rightarrow a^{-1} f'(x) = 0$

$\Rightarrow f'(x) = 0$

Characteristic of a Ring – Let R be a ring. The characteristic of R is least +ve integer n s.t $na = 0$ $\forall a \in R$.

Eg – $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$n=6 \quad n=3 \quad n=2 \quad n=3 \quad n=6$

$\text{Char } \mathbb{Z}_6 = 6$

Scanned with CamScanner

$a_1, a_2 \to 8$
$a_3 \to 9$ $\quad lcm(8,9) = 9$
$8a_1 = 0$ $\quad 7a_2 = 0, 7a_2 = 0$
$9a_1 = a_1$

1	1,3
2	2,3
4	1,3
5	1,3
	1,1

Eg – $\mathbb{Z}$, $ch(\mathbb{Z}) = 0$

* In ring with Identity, char is the least element which makes ↑ identity becomes zero.

Int. D – $\mathbb{Z}$, $\mathbb{Z}_5$, $\mathbb{Z}_p$
$ch(\mathbb{Z}) = 0$ $\quad ch(\mathbb{Z}_5) = 5$ $\quad ch(\mathbb{Z}_p) = p$

* pq, p^2 – ?
$pq.1 = 0$
$(p.1)(q.1) = 0$
$\Rightarrow p.1 = 0$ or $q.1 = 0$
char is not product of two primes.

Every field is I.D, so
$ch(\mathbb{Z}; \mathbb{R}, \mathbb{C}) = 0$
$char(\mathbb{Z}_p) = p$

2/NOV/21

Cor – Any irreducible polynomial $f(x)$ over a field of ch 0 has simple roots. Also any irreducible polynomial $f(x)$ over a field of $ch\ p \neq 0$ has multiple roots iff $\exists\ g(x) \in F[x]$ s.t $f(x) = g(x^p)$

proof – Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be irreducible polynomial of deg n

$\Rightarrow f'(x) = \sum_{i=1}^{n-1} i a_i x^{i-1}$

If $ch\ F = 0$
$f(x)$ has multiple roots iff $f'(x) = 0$
$\Rightarrow i a_i = 0\ \forall\ 1 \le i \le n-1$
$\Rightarrow a_i = 0\ \forall\ 1 \le i \le n$
$\Rightarrow f(x) = a_0$
$\longrightarrow \longleftarrow$

$\Rightarrow f(x)$ cannot have multiple roots

If $ch\ F = p$
$f(x)$ has multiple root iff $f'(x) = 0$
$\Rightarrow i a_i = 0 \neq 1 \le i \le n-1$
$\Rightarrow p \mid i \Rightarrow i = pk_i$
$\Rightarrow f(x) = a_0 + a_1 x^{pk_1} + a_2 x^{pk_2} + \dots + a_n x^{pk_n}$

$f(x) = a_0 + a_1 y^{k_1} + \dots + a_n y^{k_n}$
where $y = x^p$
$f(x) = g(y)$
$\Rightarrow f(x) = g(x^p)$

$f(x) = x^3 + x + 6$ over $\mathbb{R}$
$= g(x) h(x)$ ($f(x)$ has atleast one root in $\mathbb{R}$)
1 $\quad$ 1, 2, 3, 6, −2, −3, −1, −6
$f(x) = x^3 + x + 6 \quad ch\ F = 3$
$f(x) = x^3 + x - \mathbb{Z}_3$
$= x(x^2 + 1)$
$f'(x) = 3x^2 + 1 = 1$

Thm – Let $f(x) \in F[x]$ be irreducible over F. Then all the roots of $f(x)$ have the same multiplicity.

proof – Let α and β be two distinct roots of $f(x)$ in extension field of F.

$$F[\alpha] \cong \frac{F[x]}{\langle f(x) \rangle} \cong F[\beta]$$

$$F(\alpha) \xrightarrow{\sigma} \frac{F[x]}{\langle f(x) \rangle} \xrightarrow{\eta} F(\beta)$$

$\eta \circ \sigma : F(\alpha) \to F(\beta)$
So, $F[\alpha]$ and $F[\beta]$ are isomorphic under the isomorphism defined by

$F = \mathbb{Q}$
$f(x) = x^3 - 2$
$2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2$
$\mathbb{Q}(2^{1/3}) \cong \frac{\mathbb{Q}[x]}{\langle f(x) \rangle} \cong \mathbb{Q}(2^{1/3}\omega)$
$\alpha \quad f(x) \quad \beta$

Scanned with CamScanner

$\sigma : F[x] \to F[\beta] \subseteq \bar{F}$

$\sigma(\alpha) = \beta$

Then we can extend σ an isomorphism σ^* from $\bar{F}$ to $\bar{F}$.
(Any two algebraic closures are isomorphic)

σ^* induces an isomorphism

$\bar{F}[x] \to \bar{F}[x]$

$\sigma^*(a_0 + a_1x + \cdots + a_nx^n) = \sigma^*(a_0) + \sigma^*(a_1)x + \cdots + \sigma^*(a_n)x^n$

Then $\sigma^*(f(x)) = f(x)$

Let $(x-\alpha)^k \mid f(x)$

$\sigma^*((x-\alpha)^k) = (x-\beta)^k$

also $\sigma^*(f(x)) = f(x)$

$\Rightarrow \sigma^*((x-\alpha)^k) \mid \sigma^*(f(x))$

$\Rightarrow (x-\beta)^k \mid f(x)$

$\Rightarrow$ multiplicity of $\alpha \leq$ multiplicity of β

Interchanging the role of α and β

multiplicity of $\beta \leq$ multiplicity of α

Cor – If $f(x) \in F[x]$ is irreducible polynomial over F. Then $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)^k$, where α_i's are roots of $f(x)$ in splitting field and K is multiplicity of each root.

sol^n :- $f(x) = af_1(x)$

$= a(x-\alpha_1)^k(x-\alpha_2)^k \cdots (x-\alpha_r)^k$

$= a\prod_{i=1}^{n}(x-\alpha_i)^k$

Prime field – A field is called prime if it has no proper subfield.

F

Ch F = 0 | ch p

$Q \subseteq F = \{0, 1, 2, 3, \cdots\}$

$-1, -2, -3, \cdots$

$\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots$

$p \mid q$; $p, q \in \mathbb{Z}$, $q \neq 0$

ch F = p

$\mathbb{Z}_p \subseteq F = \{0, 1, 2, 3, \cdots, p-1\}$

Definition – The intersection of the family of subfields of a field is called its prime field.

Thm – The prime field of a field is either isomorphic to Q to $\mathbb{Z}_p$, p prime.

proof – Consider the mapping $f : \mathbb{Z} \to F$ defined by

$f(n) = ne$ where e is the unity of F.

then f is a homomorphism and $\ker f \triangleq \mathbb{Z}$

Case 1 – $\ker f = \{0\}$

then f can be extended from $Q \to F$ by

$f\left(\frac{m}{n}\right) = \frac{me}{ne}$

then $\frac{Q}{\ker f^*} = \text{Im}(f^*)$

$Q \cong$ subfield of F

Case 2 – $\ker f = n\mathbb{Z}$, $n \neq 0$

$\frac{\mathbb{Z}}{\ker f} \cong \text{Im}(f)$

$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong$ Subfield of F

$\Rightarrow n$ must be a prime

$\Rightarrow \frac{\mathbb{Z}}{p\mathbb{Z}} \cong$ Subfield of F.

Hence, the prime field of F is isomorphic to $\mathbb{Z}_p$.

Scanned with CamScanner

25/11/21

PAGE NO.:
DATE: / /

Finite fields –

Thm – Let F be a finite field. Then the number of elements in F is p^n, $n \in \mathbb{Z}^+$ and p is some prime.

Proof – If F is finite field $\Rightarrow$ chF = p for some prime p
$\Rightarrow \mathbb{Z}_p$ is prime field of F.
$\Rightarrow$ F is a vector space over $\mathbb{Z}_p$.
$\Rightarrow$ F has finite dimension say n over $\mathbb{Z}_p$.
$\Rightarrow$ F has p^n elements

Thm – The multiplicative group of non-zero elements of a finite field is cyclic.

proof –

> Result – Let a and b be two elements of a finite abelian group G. Then $\exists$ an element $c \in G$ s.t
> $o(c) = LCM(o(a), o(b))$

Let F^* be multiplicative group of non-zero elements of field F.
as F^* is finite abelian gp.
we can find an element $\alpha \in F^*$, whose order is LCM of order of all the elements of F^* say that order is r.

$\Rightarrow \alpha^r = 1 \quad \forall \alpha \in F^*$
$\Rightarrow \alpha \in F^*$ is a root of polynomial $x^r - 1 = 0$
also $x^r - 1$ has exactly r roots.
$\Rightarrow o(F^*) \leq r$
also $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$ are elements of F^* and are distinct too.
$\because$ if $\alpha^i = \alpha^j$ for some $1 \leq i \leq j \leq r-1$
$\Rightarrow \alpha^{j-i} = 1 \quad 0 < j-i < r$
$\longrightarrow \longleftarrow$

PAGE NO.:
DATE: / /

$\Rightarrow o(F^*) \nless r$
$\Rightarrow o(F^*) = r$ and $\alpha^r = 1$
$\Rightarrow F^*$ has an element of order r.
$\Rightarrow F^*$ is cyclic.

Converse – If multiplicative group of non-zero elements of a field is cyclic, then field must be finite.

proof – Let $F^* = \langle \alpha \rangle$
If F^* is finite $\Rightarrow$ F is finite
So assume that F^* is infinite cyclic group.
Case 1 – If chF = p > 0
$\Rightarrow F = \mathbb{Z}_p(\alpha)$
Consider $1 + \alpha = 0$
$\Rightarrow \alpha^2 = 1$
$\Rightarrow o(\alpha)$ is finite
$\longrightarrow \longleftarrow$

$\Rightarrow 1 + \alpha = \alpha^r$
$\Rightarrow \alpha$ is a root of polynomial $x^r - x - 1 = 0$
$\Rightarrow$ minimal polynomial of α has degree $\leq r$.
$[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p]$ = deg of minimum poly of $\alpha = n \leq r$
$\Rightarrow \mathbb{Z}_p(\alpha)$ has finite basis as a vector space over $\mathbb{Z}_p$ consisting of n elements
$\Rightarrow |\mathbb{Z}_p(\alpha)| = p^n$

Case 2 – chF = 0
$\Rightarrow \alpha^r = -1$ where for some $r \in \mathbb{Z}$
$\Rightarrow \alpha^{2r} = 1$
$\Rightarrow o(\alpha)$ is finite
$\longrightarrow \longleftarrow$ Not possible

$0 \in F, 1 \in F \Rightarrow 0 - 1 \in F$ and operation is polynomial by x^{-1} to x^{r-1}

Hence, our supposition is wrong
$\therefore F^*$ is finite cyclic group

Scanned with CamScanner

26/Nov/21

Theorem Any finite field with p^n elements is Splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$ Consequently any two fields with p^n elements are isomorphic.

Proof:- Let F be a field with p^n elements.

$\Rightarrow F^*$ is multiplicative cyclic group with $p^n - 1$ elements.

$\Rightarrow \lambda^{p^n - 1} = 1 \quad \forall \lambda \in F^*$ [$\because$ If G is a finite group of order n, then $a^{o(G)} = e \ \forall a \in G$]

$\Rightarrow \lambda^{p^n} = \lambda \quad \forall \lambda \in F^*$

$\Rightarrow$ each $\lambda \in F^*$ satisfies $x^{p^n} - x$

also $0 \in F$ satisfies $x^{p^n} - x$

Each element of F is a root of $x^{p^n} - x$

also $o(F) = p^n$

$\Rightarrow$ F is S.F of $x^{p^n} - x$.

Thm- For each prime p and each +ve integer $n \geq 1$, the roots of $x^{p^n} - x \in \mathbb{Z}_p[x]$ in its S.F over $\mathbb{Z}_p$ are all distinct and form a field with p^n elements.

Proof- $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$

$f'(x) = p^n x^{p^n - 1} - 1$

$= -1$

$\Rightarrow f'(x) \neq 0$ for any x. So $f(x)$ has distinct roots.

If α and β are two roots of $f(x)$.

T.P - $\alpha - \beta$, $\alpha\beta^{-1}$ is also a root

Now $(\alpha - \beta)^{p^n} = {}^{p^n}C_0 \alpha^{p^n} + {}^{p^n}C_1 \alpha^{p^n - 1}\beta + \dots + {}^{p^n}C_{p^n} \beta^{p^n}$

$= \alpha^{p^n} - \beta^{p^n}$

$= \alpha - \beta$

$(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{p^n})^{-1}$

$= \alpha\beta^{-1}$

Thm- If F is a finite field with p^n elements and m is a +ve integer then $\exists$ an extension field E of F s.t $[E:F] = m$ and all such extensions are isomorphic.

Soln:- Let $\bar{F}$ be algebraic closure of F.

Consider the polynomial $f(x) = x^{p^{mn}} - x \in F[x]$

If $0 \neq u \in F$, $u^{p^n - 1} = 1$

$n \mid mn \Rightarrow (p^n - 1) \mid (p^{mn} - 1)$

$\Rightarrow p^{mn} - 1 = k(p^n - 1)$

$\Rightarrow u^{p^{mn} - 1} = u^{k(p^n - 1)} = (1)^k = 1$

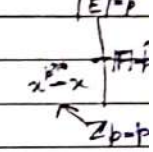
$\Rightarrow u^{p^{mn}} = u$

If E is S.F of $x^{p^{mn}} - x$ over $\mathbb{Z}_p$ then

$\mathbb{Z}_p \subseteq F \subseteq E$

where $|F| = p^n$, $|E| = p^{mn}$

$\Rightarrow [E:F] = m$



27/Nov/21

Thm- Let F be a finite field. Then $\exists$ an irreducible polynomial of any given degree over F.

Proof- If F is finite field, then we can find an extension of any degree n over F. Let E be such extension then E is also finite and so E^* is a multiplicative cyclic group say $E^* = \langle \alpha \rangle$

then $F \subset F(\alpha) \subset E$ also $E \subseteq F(\alpha) \Rightarrow F(\alpha) = E$

$[E:F] = n \Rightarrow [F(\alpha):F] = n$

$\Rightarrow \deg(\text{min poly of } \alpha) = n$

$\Rightarrow p(x) \in F[x]$ is irreducible poly. of degree n

Eg - $\frac{\mathbb{Z}_2[x]}{I = \langle x^2+x+1 \rangle} = \{f(x) + \langle x^2+x+1 \rangle ; f(x) \in \mathbb{Z}_2[x]\}$

$= \{1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + \langle x^2+x+1 \rangle\}$

$= \{(1+x^3)(1+x+x^2) + \langle x^2+x+1 \rangle\}$

$= \{x^6 + kx^2 + x + 1\}$

Scanned with CamScanner

$= \{1 + x(1+x+x^2) + x^4(1+x+x^2) + \langle x^2+x+1 \rangle\}$

$\{0+I, 1+I, x+I, \ldots\} = \{1 + \langle x^2+x+1 \rangle\}$

⇒ In this way we can find field of any order.

Result – A finite field F of p^n elements has exactly one subfield with p^m elements for each divisor m of n.

Proof – $o(F) = p^n \Rightarrow o(F^*) = p^n - 1$ and F^* is multiplicative cyclic group

Now if $m|n \Rightarrow p^m - 1 \mid p^n - 1$

⇒ F^* has a unique multiplicative subgroup H of order $p^m - 1$ for each $m|n$.

⇒ Each element of H satisfies $x^{p^m - 1} = 1$ and hence satisfies $x^{p^m} = x$

⇒ Each element of $H \cup \{0\}$ satisfies $x^{p^m} = x$

⇒ $H \cup \{0\}$ is a field of order p^m

30/Nov/21

Unit-4

Separable Extensions –

Defⁿ – An irreducible polynomial $f(x) \in F[x]$ is called a separable polynomial if all its roots are simple.

- A polynomial $f(x) \in F[x]$ is called separable, if its every irreducible factor is a separable polynomial.

Defⁿ – Let E be an extension of a field F. An element $\alpha \in E$, which is algebraic over F is called separable over F, if its minimal polynomial over F is separable.

An algebraic extension E of F is called separable if each $\alpha \in E$ is separable.

1. If $ch\, F = 0$ then every irreducible polynomial $f(x) \in F[x]$ has simple roots.

Conclusion – If $ch\, F = 0$ and E is algebraic extension of F, then E is Separable.

2. If $ch\, F = p$. Any irreducible polynomial $f(x)$ over a ~~case 1 – If F is finite field~~ field F of $ch\, p \neq 0$ has multiple roots iff $\exists\, g(x) \in F[x]$ s.t $f(x) = g(x^p)$

Case 1 – If F is finite

⇒ $|F| = p^n$ for some integer $n > 0$

now $f(x)$ has multiple roots iff

$$f(x) = \sum_{i=0}^{m} a_i (x^p)^i \; ; \; a_i \in F \; \forall i$$

$$\Rightarrow a_i^{p^n} = a_i \quad \forall\, 0 \le i \le m$$

$$\Rightarrow f(x) = \sum_{i=0}^{m} (a_i^{p^n})(x^p)^i = \left(\sum_{i=0}^{m} b_i x^i\right)^p$$

Scanned with CamScanner

$a_0 p^n + a_1 p^{n-1} x + a_2 p^{n-2} x^2 + a_3 p^{n-3} x^3$ $(b_0 + b_1 x + b_2 x^2 + b_3 x^3)^3$

$(b_0)^3 = a_0 p^n$

$\Rightarrow f(x)$ is reducible.

$\longrightarrow \longleftarrow$

$\Rightarrow$ If F is finite field with $ch\, F = p \neq 0$, then every irreducible polynomial over F is separable and hence every polynomial over F is separable.

Example of an irreducible polynomial over an infinite field F with $ch\, F = p \neq 0$ which has multiple roots.

proof – Let $K = F(x)$ be the field of rational functions over field F with $ch\, F = 3$.

Let $f(y) = y^3 - x \in K[y]$

let $f(y)$ be reducible over K

$\Rightarrow \exists \frac{p(x)}{q(x)} \in K$ s.t. $f\left(\frac{p(x)}{q(x)}\right) = 0$

$\Rightarrow \left(\frac{p(x)}{q(x)}\right)^3 - x = 0$

$(p(x))^3 = x(q(x))^3$

$\Rightarrow 3 \deg p(x) = 1 + 3 \deg q(x)$

$\Rightarrow 3(\deg p(x) - \deg q(x)) = 1$

$\longrightarrow \longleftarrow$

Hence, our assumption is wrong

$\Rightarrow f(y)$ is irreducible over K

$f(y) = y^3 - x \in K[y]$

Let β_1 & β_2 be two roots of $f(y)$ in some extension of K.

$\Rightarrow \beta_1^3 - x = \beta_2^3 - x$

$(\beta_1 - \beta_2)^3 = \beta_1^3 - \beta_2^3 - 3\beta_1\beta_2(\beta_1 - \beta_2)$

$= \beta_1^3 - \beta_2^3 = 0$

$\Rightarrow \beta_1 = \beta_2$

$[K(\beta_1) : K = 3]$

$\Rightarrow$ All the roots of $f(y)$ are same.

$f[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m,\ a_i \in F,\ m \geq 0\}$

$1 + x \cdot \frac{1}{1+x} = 1$

$F(x) = \left\{\frac{p(x)}{q(x)};\ p(x) \in F[x],\ q(x) \in F[x],\ q(x) \neq 0\right\}$

Perfect field – A field is called perfect, if its every algebraic extension is separable.

Example – ① $\mathbb{R}$

② Every field F with $ch = 0$

③ Every finite field

④ $\mathbb{Z}_3(x)$ – Non perfect field $[K(\beta_1) : K = 3]$

Theorem – If E is a finite separable extension of a field F, then E is a simple extension of E.

proof –

If F is finite $\Rightarrow$ E is also finite field

$\Rightarrow E^*$ is multiplicative cyclic group generated by α (say)

then $F(\alpha) = E$

So assume that F is infinite

$d \in E, F \subseteq E$

$E \subseteq F(\alpha)$

as E is finite extension of $F \Rightarrow E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ where all α_i's are algebraic over F.

We show that if $E = F(\alpha, \beta)$ where α and β are algebraic over F then $E = F(\theta)$ for some $\theta \in E$

Assume that $p(x)$ and $q(x)$ are minimal polynomial of α and β respectively over F.

Let roots of $p(x)$ be $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ and roots of $q(x)$ are $\beta = \beta_1, \beta_2, \dots, \beta_m$ as E is separable extension of F, all α_i's and all β_j's are distinct.

As F is infinite, $\exists$ some $a \in F$ s.t. $a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$ for any

$1 \leq i \leq n,\ 2 \leq j \leq m$.

$\Rightarrow a(\beta - \beta_j) \neq \alpha_i - \alpha$

$\Rightarrow a\beta + \alpha \neq \alpha_i + a\beta_j$

Let $\theta = a\beta + \alpha$

then $\theta - a\beta_j = a\beta + \alpha - a\beta_j \neq \alpha_i \ \forall\ 1 \leq i \leq n, 2 \leq j \leq m$

Define $h(x) = p(\theta - ax) \in F(\theta)[x]$

Scanned with CamScanner

then $h(\beta) = p(\theta - a\beta) = p(\alpha) = 0$

for $j \neq 1$

also $h(\beta_j) = p(\theta - a\beta_j) \neq 0$

$\Rightarrow$ only β_1 is the root of $h(x)$ and $\beta_2, \ldots, \beta_m$ are not the roots of $h(x)$.

also β_1 is a root of $g(x) \in F[x] \subseteq F(\theta)[x]$

Let $A(x)$ be minimal polynomial of β over $F(\theta)$

Then $A(x) \mid g(x)$ similarly $A(x) \mid h(x)$

$\Rightarrow A(x) \mid$ common factor of $g(x)$ and $h(x)$

$\Rightarrow A(x) \mid x - \beta$

$\rightarrow A(x) = x - \beta \in F(\theta)[x]$

$\Rightarrow \beta \in F(\theta)$

$\theta = a\beta + \alpha$

$\Rightarrow \alpha = \theta - a\beta \in F(\theta)$

$\Rightarrow F(\alpha, \beta) \subseteq F(\theta)$

also $F(\theta) \subseteq F(\alpha, \beta)$

$\Rightarrow F(\alpha, \beta) = F(\theta)$

Thm– Let E be an extension of field F and let $\alpha \in E$ be alg. over F. Then α is separable over F iff $F(\alpha)$ is separable extension of F.

soln:– If $F(\alpha)$ is separable extension of F, clearly α is separable over F.

converse $\Rightarrow$ Let $\beta \in F(\alpha)$

$\Rightarrow F \subseteq F(\beta) \subseteq F(\alpha)$

Let L be algebraic closed field

$\Rightarrow \sigma : F \rightarrow L$ is an embedding from (*) (Unit-3)

Suppose $p_1(x)$ is minimal polynomial of β over F which has m distinct roots

Let $p_2(x)$ be minimal polynomial of α over

Then σ can be extended to

$\sigma i : F(\beta) \rightarrow L$ in exactly m ways

Let $p_2(x)$ be minimal polynomial of α over $F(\beta)$ with n distinct roots then each σi can be extended as $F(\alpha) \rightarrow L$ in n ways.

Let $p_3(x)$ be minimal polynomial of α over F.

Then $[F(\alpha) : F]$ = deg of min polynomial of α over F

= number of distinct roots of $p_3(x)$

= Number of extensions of embedding $\sigma : F \rightarrow L$ to $F(\alpha) \rightarrow L = mn$

$[F(\alpha) : F(\beta)]$ = deg. of minimal polynomial of α over $F(\beta)$

= number of distinct roots of minimal polynomial of α over $F(\beta)$

$= n$

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

$= n[F(\beta) : F]$

$\Rightarrow [F(\beta) : F] = m$

Also minimal polynomial of β over F has m distinct roots.

$\Rightarrow \beta$ is separable over F.

7/Dec/21

Thm– Suppose $F \subseteq E \subseteq K$ be three fields such that E is finite separable extension of F, K is finite separable extension of E, then K is finite separable extension of F.

proof– $E = F(\alpha)$ for some $\alpha \in E$

$K = E(\beta)$ for some $\beta \in K$

$K = E(\beta) = F(\alpha)(\beta) = F(\alpha, \beta)$

Let $\gamma \in F(\alpha, \beta)$, $\gamma \notin F(\alpha)$

T.P – γ is separable over F.

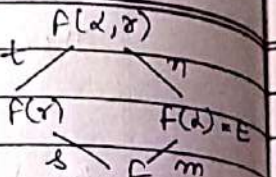
Scanned with CamScanner

Let $p_1(x)$ = minimal polynomial of α over F with deg m

$p_2(x)$ = minimal polynomial of γ over $F(\alpha)$ with deg n

$p_3(x)$ = minimal polynomial of γ over F with deg s.

$p_4(x)$ = minimal polynomial of α over $F(\gamma)$ with deg t



$[F[\alpha,\gamma]:F] = mn = st$

Suppose L is algebraically closed field containing F.

$\sigma : F \to L$ is embedding

$\Rightarrow$ σ can be extended from $F(\alpha) \to L$ in m ways

($\because$ minimal polynomial of α has deg m and α is separable over F)

say $\sigma_1, \sigma_2, \ldots, \sigma_m$.

Each σ_i can be extended from $F(\alpha,\gamma) \to L$ in n ways

[$\because$ deg of min. poly. of γ over $F(\alpha)=E$ is n and γ is separable over E]

i.e $\sigma : F \to L$ can be extended to $F(\alpha,\gamma) \to L$ in mn ways or st ways. — (1)

Now if γ is not separable over F, then embedding $\sigma : F \to L$ can be extended to $F(\gamma) \to L$ in less than s ways

$\Rightarrow$ No. of total extensions of $\sigma : F \to L$ to $F(\alpha,\gamma) \to L$ are $< st$

$\longrightarrow \leftarrow$ to statement (1)

Hence, γ must be separable over F.

Thm — If K is a field of $ch\ p \neq 0$, then K is perfect iff $K^p = K$.

proof :- Let $ch\ K = p$ and K is perfect.

Clearly, $K^p \subseteq K$

[$\because a \in K^p \Rightarrow a = b^p$ for some $b \in K \Rightarrow a \in K$]

Let $a \in K$

T.P that $a \in K^p$, we need to show that the poly. $f(x) = x^p - a \in K[x]$ has a solution in K.

$f(x)$ has a root 'b' in some extension of K.

Let $p(x)$ be minimal polynomial of b over K.

As K is perfect $\Rightarrow K(b)$ is separable extension of K

$\Rightarrow$ $p(x)$ has distinct roots.

as $f(b) = 0$

$\Rightarrow b^p = a \in K$

and $x^p - b^p = g(x) \in K[x]$

$g(b) = 0$

$\Rightarrow p(x) \mid g(x)$

also $g(x) = x^p - b^p = (x-b)^p$ [$\because ch\ K = p$]

$\Rightarrow p(x) \mid g(x) \Rightarrow p(x) \mid (x-b)^p$

$\Rightarrow p(x) = (x-b)^r$ where $r \leq p$

as $p(x)$ has distinct roots $\Rightarrow r = 1$

$p(x) = x - b \in K[x]$

$\Rightarrow b \in K$

also $a = b^p \Rightarrow a \in K^p \Rightarrow K \subseteq K^p$

converse :- Let $K^p = K$

To show that K is perfect, we show that every irreducible polynomial over K has distinct roots.

Let $p(x) \in K[x]$ be irreducible and it does not have distinct roots.

$\Rightarrow p(x) = g(x^p)$ for some polynomial $g(x) \in K[x]$

$\Rightarrow p(x) = a_0 + a_1 x^p + a_2 x^{2p} + \ldots + a_n x^{np}$ — (1) where a_i's $\in K$

as $K^p = K \Rightarrow a_i = b_i^p$ for some $b_i \in K$

$p(x) = b_0^p + b_1^p x^p + \ldots + b_n^p x^{np}$

$= (b_0 + b_1 x + \ldots + b_n x^n)^p$

$\Rightarrow p(x)$ is reducible

$\longrightarrow \leftarrow$

Hence, K is perfect.

Scanned with CamScanner

10/11/21

Galois Theory-

Defⁿ:- Let E be an extension of field F. We denote $G(E|F)$ the group of automorphisms of E leaving each element of F fixed. $G(E|F)$ is also called the group of F-automorphisms of E.

$G(E|F) = \{ f : E \to E \; ; \; f \text{ is isomorphism}, f(a) = a \; \forall a \in F \}$

$Id = f : E \to E$

$f(x) = x$

$G(E|F) = \phi$

$fg = fog$

F is always finite separable extension

$\Rightarrow E = F(\alpha)$ $\qquad F(\alpha) = F[\alpha]$

$G(E|F) = G(F(\alpha)|F)$

$f : F(\alpha) \to F(\alpha)$

$f(a_0 + a_1\alpha + \dots + a_n\alpha^n) = f(a_0) + f(a_1)f(\alpha) + \dots + f(a_n)(f(\alpha))^n$

$= a_0 + a_1 f(\alpha) + \dots + a_n (f(\alpha))^n$

$\sigma : F \to L \to$ algebraic closure.

$\sigma : F(\alpha) \to L$ #

Let E be finite separable extension of F $\Rightarrow E = F(\alpha)$ for some $\alpha \in E$

$\Rightarrow$ If $f \in G(F(\alpha)|F) = G(E|F)$ then f is an embedding from $F(\alpha) \to L$, keeping each element of F fixed (here L is algebraic closure of F)

$\Rightarrow$ f is an extension of embedding $\sigma : F \to L$

Conversely, if $\sigma : F \to L$ is an embedding keeping each element of F fixed, then extension of σ from $F(\alpha) \to L$, may or may not $\in G(E|F)$.

$\Rightarrow |G(E|F)| \leq$ No. of extensions of embedding $\sigma : F \to L$ to an embedding $\sigma^* : F(\alpha) \to L$

= No. of distinct roots of min. polynomial of α over F

= deg. of min. poly. of α [$\because$ E is separable ext. of F]

= n (say)

eg:- $F = \mathbb{R}$, $E = \mathbb{C}$

$G(E|F) = G(\mathbb{C}|\mathbb{R}) \leq 2$ $\qquad [E:F] = 2 = \{1, i\}$

$f : \mathbb{C} \to \mathbb{C}$ $\qquad |G(F(\alpha)|F)| \leq n = [F(\alpha):F]$

$f(a+ib) = f(a) + f(i)f(b)$

$= a + f(i)b$

$-1 = f(-1) = f(i^2) = f(i \cdot i) = f(i) \cdot f(i) = (f(i))^2$

$(f(i))^2 = -1$

$\Rightarrow f(i) = \pm\sqrt{-1} = \pm i$

eg:- $|G(\mathbb{Q}(2^{1/3})|\mathbb{Q})| \leq 3$ $\qquad G(\mathbb{Q}(2^{1/3})) = \{1, 2^{1/3}, 2^{2/3}\}$

Let $f \in G(\mathbb{Q}(2^{1/3})|\mathbb{Q})$ $\qquad \mathbb{Q}$

$f : \mathbb{Q}(2^{1/3}) \to \mathbb{Q}(2^{1/3})$

$f(a_0 + a_1 2^{1/3} + a_2 2^{2/3}) = a_0 + a_1 f(2^{1/3}) + a_2 (f(2^{1/3}))^2$

$2 = f(2) = (f(2^{1/3}))^3 = (f(2^{1/3}))^3$

$f(2^{1/3}) = 2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2$

$f(2^{1/3}) \in \mathbb{Q}(2^{1/3})$

$\Rightarrow f(2^{1/3}) = 2^{1/3}$

$f(a_0 + a_1 2^{1/3} + a_2 2^{2/3}) = a_0 + a_1 2^{1/3} + a_2 2^{2/3}$

$\Rightarrow f(a) = a \; \forall a \in \mathbb{Q}(2^{1/3})$

Defⁿ:- Let E be any field and let H be subgroup of the group of automorphisms of E. Then the set $E_H = \{x \in E ; \sigma(x) = x \; \forall \sigma \in H\}$ is called the fixed field of group of automorphisms H.

To verify that E_H is a subfield of E.

If E is an extension of a field F and $H < G(E|F)$

Then $F \subset E_H \subset E$.

for example, $C_H = \mathbb{R}$

where $H = G(\mathbb{C}|\mathbb{R})$ and

$\mathbb{Q}(\sqrt[3]{2})_H = \mathbb{Q}(\sqrt[3]{2})$ where $H = G(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$

Scanned with CamScanner

PAGE NO.:
DATE: / /

Thm – Let H be a finite subgroup of the group of automorphisms of field E then
$$[E : E_H] = |H|$$

Proof – Dedekind Lemma –

Let F and E be fields and $\sigma_1, \sigma_2, \ldots \sigma_n$ be distinct embeddings of F into E. Suppose that for $a_1, a_2, \ldots a_n \in E$, $\sum_{i=1}^{n} a_i \sigma_i(a) = 0 \ \forall a \in F$. Then $a_i = 0 \ \forall 1 \le i \le n$

OR

Distinct embedding of F into E are linearly independent over E.

proof – Suppose $\exists$ elements $a_1, a_2, \ldots, a_n \in E$ not all zero s.t.
$a_1\sigma_1 + a_2\sigma_2 + \ldots + a_n\sigma_n = 0$
i.e. $(a_1\sigma_1 + a_2\sigma_2 + \ldots + a_n\sigma_n)(x) = 0 \ \forall x \in F$
Among all these combinations choose the one which has least number of non-zero terms.
Let $b_1\sigma_1(x) + b_2\sigma_2(x) + \ldots + b_m\sigma_m(x) = 0 \ \forall x \in F$ – (1)
as σ_i's are different $\Rightarrow \exists$ some $y \in F$ s.t $\sigma_1(y) \neq \sigma_2(y)$
Replace x by xy in (1)

$$b_1\sigma_1(x)\sigma_1(y) + b_2\sigma_2(x)\sigma_2(y) + \ldots + b_m\sigma_m(x)\sigma_m(y) = 0 \quad (2)$$

$\sigma_1(y)$ (1) – (2)

$$b_2\sigma_2(x)(\sigma_1(y) - \sigma_2(y)) + b_3\sigma_3(x)(\sigma_1(y) - \sigma_3(y)) + \ldots + b_m\sigma_m(x)(\sigma_1(y) - \sigma_m(y)) = 0$$

Dividing throughout by $\sigma_1(y) - \sigma_2(y)$

$$b_2\sigma_2(x) + b_3\sigma_3(x)\frac{\sigma_1(y) - \sigma_3(y)}{\sigma_1(y) - \sigma_2(y)} (\lambda_3) + \ldots + b_m\sigma_m(x)\frac{\sigma_1(y) - \sigma_m(y)}{\sigma_1(y) - \sigma_2(y)} = 0$$

λ_m

$\Rightarrow (b_2\sigma_2 + b_3\lambda_3\sigma_3 + b_4\lambda_4\sigma_4 + \ldots + b_m\lambda_m\sigma_m)(x) = 0 \ \forall x \in F$

$\Rightarrow (b_2\sigma_2 + b_3'\sigma_3 + b_4'\sigma_4 + \ldots + b_m'\sigma_m)(x) = 0 \ \forall x \in F$, $b_2, b_i' \in E$

Therefore, All embeddings are Linearly Independent.

Scanned with CamScanner

11/12/21

Thm – Let H be a finite subgroup of group of Automorphisms of E. Then $[E:E_H] = |H|$

Proof – Let $H = \{e = g_1, g_2, \ldots, g_n\}$ and let $[E:E_H] = m$

Suppose $m < n$

Let $\{a_1, a_2, \ldots, a_m\}$ be basis of E over E_H.

Consider the system of n homogeneous linear equations

$g_1(a_j)y_1 + g_2(a_j)y_2 + \ldots + g_n(a_j)y_n = 0 \quad \forall\, 1 \le j \le m$

Let $\alpha \in E$ then $\alpha = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_m a_m$, where α_i's $\in E_H$ then

$$g_1(\alpha)y_1 + g_2(\alpha)y_2 + \ldots + g_n(\alpha)y_n = g_1\left(\sum_{i=1}^{m} \alpha_i a_i\right)y_1 + g_2\left(\sum_{i=1}^{m} \alpha_i a_i\right)y_2 + \ldots + g_n\left(\sum_{i=1}^{m} \alpha_i a_i\right)y_n$$

$$= \sum_{i=1}^{m} \alpha_i g_1(a_i)y_1 + \sum_{i=1}^{m} \alpha_i g_2(a_i)y_2 + \ldots + \sum_{i=1}^{m} \alpha_i g_n(a_i)y_n$$

$$= \sum_{i=1}^{m} \alpha_i \left(g_1(a_i)y_1 + g_2(a_i)y_2 + \ldots + g_n(a_i)y_n\right)$$

$$= 0$$

$\Rightarrow (g_1y_1 + g_2y_2 + \ldots + g_ny_n)(\alpha) = 0 \quad \forall\, \alpha \in E$

① – $\begin{bmatrix} g_1(a_1)y_1 + \ldots + g_n(a_1)y_n \\ g_1(a_m)y_1 + \ldots + g_n(a_m)y_n = 0 \end{bmatrix}$

Non-trivial sol^n

$y_1 = y_2 = \ldots = y_n = 0$ (not all zero)

No. of Eq^n < No. of variable

$AX = 0$

$m \times n$

$m < n$

$\Rightarrow$ y_i's are $\neq 0$ (∵ system of Equations ① has non-trivial solution as no. of Equations < No. of variables)

which is a contradiction.

So assume $m \ge n$

$\Rightarrow [E:E_H] \ge n+1$

$\Rightarrow \exists$ a set of $n+1$ elements, which is L.I over E_H

Let such set be $\{a_1, a_2, \ldots, a_{n+1}\}$

Consider the family of n homogeneous linear equations

② – $g_j(a_1)x_1 + g_j(a_2)x_2 + \ldots + g_j(a_{n+1})x_{n+1} = 0 \;;\; 1 \le j \le n$

These are n equations in $n+1$ variables

$\Rightarrow \exists$ a non-trivial solution $y_1, y_2, \ldots, y_{n+1} \in E$ s.t not all y_i's are zero.

Choose $y_1, y_2, \ldots, y_{n+1}$, so that as few as possible are non-zero and renumber. So that,

$y_i \neq 0,\ i = 1, 2, \ldots, r$ & $y_i = 0 \ \forall\, i = r+1, \ldots, n+1$

So, ② becomes

$g_j(a_1)y_1 + g_j(a_2)y_2 + \ldots + g_j(a_r)y_r = 0 \quad \forall\, 1 \le j \le n$ – ③

Let $g \in H$

$\Rightarrow g(g_j(a_1)y_1 + g_j(a_2)y_2 + \ldots + g_j(a_r)y_r) = g(0) \quad \forall\, 1 \le j \le n$

$\Rightarrow g(g_j(a_1))g(y_1) + g(g_j(a_2))g(y_2) + \ldots + g(g_j(a_r))g(y_r) = 0 \quad \forall\, 1 \le j \le n$

which is same as system

$g_j(a_1)y_1 + g_j(a_2)y_2 + \ldots + g_j(a_r)y_r = 0 \ \forall\, 1 \le j \le n$ – ④

$g(y_1)$ ③ $- y_1$ ④ gives

$g_j(a_2)[y_2g(y_1) - y_1g(y_2)] + g_j(a_3)[y_3g(y_1) - y_1g(y_3)] + \ldots + g_j(a_r)[y_rg(y_1) - y_1g(y_r)] = 0 \quad \forall\, 1 \le j \le n$

We get a non-trivial solution of system of equations ② with $< r$ coefficient non-zero if we can prove that $y_ig(y_1) - y_1g(y_i) \neq 0 \ \forall\, 2 \le i \le r$

Now $y_ig(y_1) - y_1g(y_i) = 0$

$\Rightarrow y_ig(y_1) = y_1g(y_i)$

$\Rightarrow g(y_1)(g(y_i))^{-1} = y_i^{-1}y_1$

$\Rightarrow g(y_1y_i^{-1}) = y_1y_i^{-1}$

$\Rightarrow y_1y_i^{-1} \in E_H$

Scanned with CamScanner

$\Rightarrow \exists\ z_1, z_2, \ldots, z_n \in E_{n+1}$ s.t

$y_i = y_1 z_i \quad \forall\ 1 \le i \le n$

So, system of equations (3) becomes $(\because a_1 = 1)$

$g_1(a_1)y_1 z_1 + g_1(a_2)y_1 z_2 + \ldots + g_1(a_n)y_1 z_n = 0$

$\Rightarrow g_1(a_1)z_1 + g_1(a_2)z_2 + \ldots + g_1(a_n)z_n = 0 \quad (\because y_1 \neq 0)$

$\Rightarrow g_1(a_1)g_1(z_1) + g_1(a_2)g_1(z_2) + \ldots + g_1(a_n)g_1(z_n) = 0$

$\Rightarrow g_1(a_1 z_1 + a_2 z_2 + \ldots + a_n z_n) = 0$

$\Rightarrow a_1 z_1 + a_2 z_2 + \ldots + a_n z_n = 0$

$\Rightarrow a_1, a_2, \ldots, a_n$ are L.I over E_{n+1}

but $\{a_1, a_2, \ldots, a_n\} \subseteq \{a_1, a_2, \ldots, a_{n+1}\}$

which is a contradiction.

$\Rightarrow m = n$

Hence proved.

Thm- Let E be finite Separable extension of a field F. Then TFAE

(1) E is normal Extension of F

(2) F is fixed field of $G(E|F)$

(3) $[E:F] = |G(E|F)|$

Example :- Find $G(\mathbb{Q}(\alpha)|\mathbb{Q})$, where α satisfies $x^5 = 1, \alpha \neq 1$

Soln :- $|G(\mathbb{Q}(\alpha)|\mathbb{Q})| \le [\mathbb{Q}(\alpha):\mathbb{Q}]$ = deg. of min poly. of α over $\mathbb{Q}$ = 4

As α satisfies $x^5 = 1$

$\Rightarrow \alpha^5 = 1$

$\Rightarrow (\alpha - 1)(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4) = 0$

as $\alpha \neq 1$

$\Rightarrow 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$

$\Rightarrow$ Irreducible polynomial

$f: \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ s.t

$f(a) = a \quad \forall\ a \in \mathbb{Q}$

To find $f(\alpha)$

$\alpha^5 = 1 \Rightarrow f(\alpha^5) = f(1) = 1$

$\Rightarrow (f(\alpha))^5 = 1 \Rightarrow f(\alpha)$ is root of $x^5 = 1$

$\Rightarrow f(\alpha) = x, \alpha, \alpha^2, \alpha^3, \alpha^4$

[If $f(\alpha) = 1$ $\Rightarrow f: \mathbb{Q}(\alpha) \to \mathbb{Q}$]

$\Rightarrow \alpha, \alpha^2, \alpha^3, \alpha^4$ are automorphisms

$f: \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$

$f(a_0 + a_1 x + a_2 x^2 + a_3 x^3) = a_0 + a_1 f(\alpha) + a_2 (f(\alpha))^2 + a_3 (f(\alpha))^3$

$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \xrightarrow{f_1} a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$

$\xrightarrow{f_2} a_0 + a_1\alpha^2 + a_2\alpha^4 + a_3\alpha$

$\xrightarrow{f_3} a_0 + a_1\alpha^3 + a_2\alpha + a_3\alpha^4$

$\xrightarrow{f_4} a_0 + a_1\alpha^4 + a_2\alpha^3 + a_3\alpha^2$

$\{f_1, f_2, f_3, f_4\} = G(\mathbb{Q}(\alpha)|\mathbb{Q})$

$o(f_i) \quad f_i^4 = id$

Scanned with CamScanner

Galois Theory Eqs imp

PAGE NO.: DATE: / /

13/12/21

Definition – Let $f(x) \in F[x]$ be a polynomial and K be its splitting field over F. Then the group $G(K|F)$ is called Galois group of $f(x)$ over F.

Definition – A finite, separable and normal extension of field F is called Galois extension of F.

Fundamental Theorem of Galois Theory –

Statement – Let E be a Galois extension of field F. Let K be any subfield of E containing F. Then the mapping $K \to G(E|K)$ sets a one-one correspondence from the set of subfields of E containing F to the subgroups of $G(E|F)$ such that

(1) $K = E_{G(E|K)}$ $\quad E_H = \{x \in E ; \sigma(x) = x \ \forall \sigma \in H\}$

(2) for any subgroup H of $G(E|F)$, $H = G(E|E_H)$

(3) $[E:K] = |G(E|K)|$, $[K:F]$ = index of $G(E|K)$ in $G(E|F)$

(4) K is normal extension of F iff $G(E|K)$ is normal subgroup of $G(E|F)$

(5) If K is normal extension of F, then $G(E|F) \cong \frac{G(E|F)}{G(E|K)}$

Example – Let $E = \mathbb{Q}(2^{1/3}, \omega)$ where $\omega^3 = 1$, $\omega \neq 1$
Let σ_1 be identity automorphism of E & $\sigma_2 : E \to E$ is F automorphism such that

$$\sigma_2(\omega) = \omega^2, \ \sigma_2(2^{1/3}) = \omega \cdot 2^{1/3}$$

If $G_1 = \{\sigma_1, \sigma_2\}$, find E_{G_1}.

Sol^n :
$E_G = \{x \in E ; \sigma_1(x) = x \ \& \ \sigma_2(x) = x\}$
$= \{x \in E ; x = x \ \& \ \sigma_2(x) = x\}$
$= \{x \in E ; \sigma_2(x) = x\}$

$\mathbb{Q}(2^{1/3}, \omega)$
$\{1, 2^{1/3}, 2^{2/3}\}$ | $\mathbb{Q}(\omega)$
$(1, \omega)$ | $\mathbb{Q}$

PAGE NO.: DATE: / /

basis of E over $\mathbb{Q} = \{1, 2^{1/3}, 2^{2/3}, \omega, 2^{1/3}\omega, 2^{2/3}\omega\}$

$\sigma_2 : E_a \to E$

$\sigma_2(a_0 + a_1\omega + a_2 2^{1/3} + a_3 2^{1/3}\omega + a_4 2^{2/3} + a_5 2^{2/3}\omega) =$
$a_0 + a_1\omega^2 + a_2 2^{1/3}\omega + a_3 2^{1/3}\omega\omega^2 + a_4 2^{1/3}\omega^2 + a_5 2^{2/3}\omega^2\omega^2$
$= a_0 + a_1\omega^2 + a_2 2^{1/3}\omega + a_3 2^{1/3} + a_4 2^{2/3}\omega^2 + a_5 2^{2/3}\omega$

$\sigma_2(\lambda) = \lambda$

$\Rightarrow a_0 + a_1\omega + a_2 2^{1/3} + a_3 2^{1/3}\omega + a_4 2^{2/3} + a_5 2^{2/3}\omega = a_0 + a_1(-1-\omega) + a_2 2^{1/3}\omega + a_3 2^{1/3} + a_4 2^{2/3}(-1-\omega) + a_5 2^{2/3}\omega$

$\lambda = a_0 - a_2\omega^2 2^{1/3} + a_5 \omega 2^{2/3} = a_0(1) + a_2(\omega^2 2^{1/3}) + a_5(\omega^2 2^{1/3})^2$

$E_G = F(\omega^2 2^{1/3})$
fixed field

Scanned with CamScanner

$X = \{1, 2, 3\}$
$|S| = 3!$
$S_3 = \{ \sigma : X \to X \text{ bijection} \}$

PAGE NO.:
DATE: (123), (132)

Ex- If $f(x) \in F[x]$ has r distinct roots in its splitting field E over F then $G(E|F) \leq S_r$ ⇒ permutation gp

soln:- Let $f(x) = a_0 + a_1 x + \dots + a_n x^n \in F[x]$. Let $\alpha_1, \alpha_2, \dots, \alpha_r$ be distinct roots of $f(x)$.

If $\sigma \in G(E|F)$

$\sigma : E \to E$ is automorphism s.t $\sigma(a) = a \ \forall a \in F$

$\sigma : F(\alpha_1, \alpha_2, \dots, \alpha_r) \to F(\alpha_1, \alpha_2, \dots, \alpha_r)$

$\because \alpha_1$ is root of $f(x) \Rightarrow a_0 + a_1\alpha_1 + \dots + a_n\alpha_1^n = 0$

$\Rightarrow \sigma(a_0 + a_1\alpha_1 + \dots + a_n\alpha_1^n) = 0$

$\Rightarrow a_0 + a_1\sigma(\alpha_1) + \dots + a_n(\sigma(\alpha_1))^n = 0$

$\Rightarrow \sigma(\alpha_1)$ is root of $f(x)$ & $\sigma(\alpha_1) \in E$

$\Rightarrow \sigma(\alpha_1) = \alpha_i$ for some $1 \leq i \leq r$

In the similar manner, we get that each $\sigma(\alpha_i) = \alpha_j$ for some $1 \leq j \leq r$.

Also as σ is $1-1 \Rightarrow \sigma(\alpha_i) \neq \sigma(\alpha_j)$ for $i \neq j$

Let us set $\phi_\sigma(\alpha_i) = \sigma(\alpha_i) \ \forall i = 1, 2, \dots, r$

then $\phi_\sigma \in S_r$

Define a mapping $f : G(E|F) \to S_r$ by

$f(\sigma) = \phi_\sigma$

For homomorphism

$f(\sigma_1\sigma_2) = \phi_{\sigma_1\sigma_2}$

$f : \{1, \omega, \omega^2\} \to \{e, (12)\} \leq S_3$

$f(1) = e, f(-1) = (12)$

and $\phi_{\sigma_1\sigma_2}(\alpha_i) = \sigma_1\sigma_2(\alpha_i)$

$= \sigma_1(\sigma_2(\alpha_i))$

$= \phi_{\sigma_1}(\sigma_2(\alpha_i))$

$= \phi_{\sigma_1}\phi_{\sigma_2}(\alpha_i)$

$\Rightarrow \phi_{\sigma_1\sigma_2} = \phi_{\sigma_1}\phi_{\sigma_2}$

$f(\sigma_1\sigma_2) = \phi_{\sigma_1\sigma_2} = \phi_{\sigma_1}\phi_{\sigma_2} = f(\sigma_1)f(\sigma_2)$

Mapping is homomorphism

Let $\sigma \in \ker f$

$\Rightarrow f(\sigma) = e$

$\Rightarrow \phi_\sigma = e$

$\Rightarrow \phi_\sigma(\alpha_i) = \alpha_i \Rightarrow \sigma(\alpha_i) = \alpha_i \ \forall 1 \leq i \leq r$

$\Rightarrow \sigma$ = identity

Mapping is $1-1$.

Ex- Let F be a field of $ch \neq 2$. Let $f(x) = x^2 - a \in F[x]$ be irreducible over F. Then Galois group of $f(x)$ over F is of order 2.

Fundamental thm of Algebra -

Thm- Every polynomial $f(x) \in \mathbb{C}[x]$ splits into linear factors in $\mathbb{C}[x]$.

proof:- Let $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{C}[x]$

$g(x) = (x^2 + 1)(a_0 + a_1 x + \dots + a_n x^n)(\bar{a_0} + \bar{a_1} x + \dots + \bar{a_n} x^n)$

$\in \mathbb{R}[x]$

Let E be splitting field of $g(x)$ over $\mathbb{R}$.

then $\mathbb{R} \subseteq \mathbb{C} \subseteq E$

claim :- $\exists$ doesnot exist any subfield K of E s.t $[K : \mathbb{C}] = 2$

Suppose such a field exists then K is finite separable extension of $\mathbb{C}$ and so simple

$\Rightarrow K = \mathbb{C}[\alpha]$ for some $\alpha \in K$

Let $p(x)$ be minimal polynomial of α over $\mathbb{C}$

then $\deg(p(x)) = 2$

Let $p(x) = x^2 + 2ax + b \in \mathbb{C}[x]$

$= (x+a)^2 - (a^2 - b) = ((x+a) - \sqrt{a^2-b})((x+a) + \sqrt{a^2-b})$

$\Rightarrow p(x)$ splits into linear factors over $\mathbb{C}$ ⟶ ⟵

$\Rightarrow \nexists$ any K s.t $K \subseteq E$ and $[K : \mathbb{C}] = 2$.

Now let $G(E|\mathbb{R}) = G$ (Galois group of $g(x)$ over $\mathbb{R}$)

Let $|G| = 2^m q$, where $m \geq 0$, q is an odd integer

Let H be Sylow 2-subgroup of G.

i.e. $|H| = 2^m$, $H \leq G$

Scanned with CamScanner

PAGE NO. :
DATE : / /

Let L be corresponding subfield of E

then $[E:L] = 2^m$

$\Rightarrow [L:\mathbb{R}][E:L] = 2^m q$

$\Rightarrow [L:\mathbb{R}] = q$

$\Rightarrow L = \mathbb{R}(\beta)$ ($\because L$ is finite, separable $\Rightarrow L$ is simple)

$\Rightarrow \exists$ an irr. poly. of deg q over $\mathbb{R}$.

but this is not possible (By Intermediate Value property)

$\Rightarrow q = 1$

$\Rightarrow [E:\mathbb{R}] = 2^m$

$[E:\mathbb{R}] = [E:\mathbb{C}][\mathbb{C}:\mathbb{R}]$

$2^m = [E:\mathbb{C}]2$

$\Rightarrow [E:\mathbb{C}] = 2^{m-1}$

$\Rightarrow G(E|\mathbb{C})$ is subgp of $G(E|\mathbb{R})$ and $|G(E|\mathbb{C})| = 2^{m-1}$

If $m > 1$

Let H' be subgroup of $G(E|\mathbb{C})$ of order 2^{m-2}

Let L' be corresponding subfield of E.

then $L' \supseteq \mathbb{C}$

and $[E:L'] = 2^{m-2}$

$\Rightarrow [E:\mathbb{C}] = 2^{m-1} = [E:L'][L':\mathbb{C}]$

$= 2^{m-2}[L':\mathbb{C}]$

$\Rightarrow [L':\mathbb{C}] = 2$

$\longrightarrow \longleftarrow$

$\Rightarrow m = 1$

$[E:\mathbb{R}] = 2^m q$

$= 2$

$[\mathbb{C}:\mathbb{R}] = 2$

$\Rightarrow \mathbb{C} = E$

Hence proved.

Scanned with CamScanner

9/Nov/21

Unit-4

PAGE NO. :
DATE : / /

Separable Extensions —

Def^n — An irreducible polynomial $f(x) \in F[x]$ is called a separable polynomial if all its roots are simple.

- A polynomial $f(x) \in F[x]$ is called separable, if its every irreducible factor is a separable polynomial.

Def^n — Let E be an extension of a field F. An element $\alpha \in E$, which is algebraic over F is called separable over F, if its minimal polynomial over F is sepdrable.

An algebraic extension E of F is called separable if each $\alpha \in E$ is separable.

1. If $ch\,F = 0$ then every irreducible polynomial $f(x) \in F[x]$ has simple roots.

   Conclusion — If $ch\,F = 0$ and E is algebraic extension of F, then E is Separable.

2. If $ch\,F = p$, Any irreducible polynomial $f(x)$ over a field F of $ch\,p \neq 0$ has multiple roots iff $\exists\, g(x) \in F[x]$ s.t $f(x) = g(x^p)$

   Case 1 — If F is finite

   $\Rightarrow |F| = p^n$ for some Integer $n \geq 0$

   now $f(x)$ has multiple roots iff

   $$f(x) = \sum_{i=0}^{m} a_i (x^p)^i \quad ; a_i \in F \ \forall i$$

   $$\Rightarrow a_i^{p^n} = a_i \quad \forall\, 0 \leq i \leq m$$

   $$\Rightarrow f(x) = \sum_{i=0}^{m} (a_i^{p^n})(x^p)^i = \left(\sum_{i=0}^{m} b_i x^i\right)^p$$

Scanned with CamScanner

Scanned with CamScanner

$a_0 p^n + a_1 p^{n-1} + a_2 p^{n-2} + a_3 p^{n-3}$ $\quad (b_0 + b_1 x + b_2 x^2 + b_3 x^3)^p$

$(b_0)^p = a_0 p^n$

$\Rightarrow f(x)$ is reducible.

$\longrightarrow \longleftarrow$

$\Rightarrow$ If F is finite field with $\text{ch } F = p \neq 0$, then every irreducible polynomial over F is separable and hence every polynomial over F is separable.

Example of an irreducible polynomial over an infinite field F with $\text{ch } F = p \neq 0$ which has multiple roots.

proof – Let $K = F(x)$ be the field of rational functions over field F with $\text{ch } F = 3$.

Let $f(y) = y^3 - x \in K[y]$

Let $f(y)$ be reducible over K

$\Rightarrow \exists \frac{p(x)}{q(x)} \in K$ s.t $f\left(\frac{p(x)}{q(x)}\right) = 0$

$\Rightarrow \left(\frac{p(x)}{q(x)}\right)^3 - x = 0$

$(p(x))^3 = x(q(x))^3$

$\Rightarrow 3 \deg p(x) = 1 + 3 \deg q(x)$

$\Rightarrow 3(\deg p(x) - \deg q(x)) = 1$

$\longrightarrow \longleftarrow$

Hence, our assumption is wrong

$\Rightarrow f(y)$ is irreducible over K

$f[x] = \{a_0 + a_1 x + \dots + a_m x^m, \; a_i \in F, n \geq 0\}$

$1 + x \cdot \frac{1}{1+x} = 1$

$F(x) = \left\{ \frac{p(x)}{q(x)} ; p(x) \in F[x], \; q(x) \in F[x], \; q(x) \neq 0 \right\}$

$f(y) = y^3 - x \in K[y]$

Let β_1 & β_2 be two roots of $f(y)$ in some extension of K.

$\Rightarrow \beta_1^3 = x = \beta_2^3$

$(\beta_1 - \beta_2)^3 = \beta_1^3 - \beta_2^3 - 3\beta_1\beta_2(\beta_1 - \beta_2)$

$= \beta_1^3 - \beta_2^3 = 0$

$\Rightarrow \beta_1 = \beta_2$ $\quad [K(\beta_1) : K = 3]$

$\Rightarrow$ All the roots of $f(y)$ are same.

Perfect field – A field is called perfect, if its every algebraic extension is separable.

Example – ① $\mathbb{R}$

② Every field F with $\text{ch} = 0$

③ Every finite field.

④ $\mathbb{Z}_3(x)$ – non perfect field $\quad [K(\phi) : K = 3]$

6 Dec '21

Thm – If E is a finite separable extension of a field F, then E is a simple extension of E.

proof – If F is finite $\Rightarrow E$ is also finite field

$\Rightarrow E^*$ is multiplicative cyclic group generated by α (say)

then $F(\alpha) = E$

So assume that F is infinite

as E is finite extension of $F \Rightarrow E = F(\alpha_1, \dots, \alpha_n)$ where all α_i's are algebraic over F.

$\alpha \in E, F \subseteq E$

$E \subseteq F(\alpha)$

We show that if $E = F(\alpha, \beta)$ where α and β are algebraic over F then $E = F(\theta)$ for some $\theta \in E$

Assume that $p(x)$ and $q(x)$ are minimal polynomial of α and β respectively over F.

Let roots of $p(x)$ be $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ and roots of $q(x)$ are $\beta = \beta_1, \beta_2, \dots, \beta_m$ as E is separable extension of F, all α_i's and all β_j's are distinct.

As F is infinite, $\exists$ some $a \in F$ s.t $a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$ for any

$1 \leq i \leq n, \; 2 \leq j \leq m$.

$\Rightarrow a(\beta - \beta_j) \neq \alpha_i - \alpha$

$\Rightarrow a\beta + \alpha \neq \alpha_i + a\beta_j$

Let $\theta = a\beta + \alpha$

Then $\theta - a\beta_j = a\beta + \alpha - a\beta_j \neq \alpha_i \; \forall \; 1 \leq i \leq n, 2 \leq j \leq m$

Define $h(x) = p(\theta - ax) \in F(\theta)[x]$

Scanned with CamScanner

then $h(\beta) = f(\theta - q\beta) = f(\alpha) = 0$

for $j \neq 1$

also $h(\beta_j) = f(\theta - q\beta_j) \neq 0$

$\Rightarrow$ only β_1 is the root of $h(x)$ and $\beta_2, \ldots, \beta_m$ are not the roots of $h(x)$.

also β_1 is a root of $g(x) \in F[x] \in F(\theta)[x]$

Let $A(x)$ be minimal polynomial of β over $F(\theta)$

Then $A(x) \mid g(x)$ similarly $A(x) \mid h(x)$

$\Rightarrow A(x) \mid$ common factor of $g(x)$ and $h(x)$

$\Rightarrow A(x) \mid x - \beta$

$\Rightarrow A(x) = x - \beta \in F(\theta)[x]$

$\Rightarrow \beta \in F(\theta)$

$\theta = q\beta + \alpha$

$\Rightarrow \alpha = \theta - q\beta \in F(\theta)$

$\Rightarrow F(\alpha, \beta) \subseteq F(\theta)$

also $F(\theta) \subseteq F(\alpha, \beta)$

$\Rightarrow F(\alpha, \beta) = F(\theta)$

Thm – Let E be an extension of field F and let $\alpha \in E$ be alg. over F. Then α is separable over F iff $F(\alpha)$ is separable extension of F.

sol^n – If $F(\alpha)$ is separable extension of F, clearly α is separable over F.

Converse $\Rightarrow$ Let $\beta \in F(\alpha)$

$\Rightarrow F \subseteq F(\beta) \subseteq F(\alpha)$

Let L be algebraic closed field

$\Rightarrow \sigma : F \to L$ is an embedding

from (A) (Unit-3)

Suppose $p_1(x)$ is minimal polynomial of β over F which has m distinct roots

Let $p_2(x)$ be minimal polynomial of α over

Then σ can be extended to

$\sigma_i : F(\beta) \to L$ in exactly m ways

$1 \leq i \leq m$

Let $p_2(x)$ be minimal polynomial of α over $F(\beta)$ with n distinct roots then each σ_i can be extended as $F(\alpha) \to L$ in n ways.

Let $p_3(x)$ be minimal polynomial of α over F.

Then $[F(\alpha) : F]$ = deg of min polynomial of α over F

= number of distinct roots of $p_3(x)$

= Number of extensions of embedding

$\sigma : F \to L$ to $F(\alpha) \to L = mn$

$[F(\alpha) : F(\beta)]$ = deg. of minimal polynomial of α over $F(\beta)$

= number of distinct roots of minimal polynomial of α over $F(\beta)$

$= n$

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

$= n[F(\beta) : F]$

$\Rightarrow [F(\beta) : F] = m$

Also minimal polynomial of β over F has m distinct roots.

$\Rightarrow \beta$ is separable over F.

7) Dec 21

Thm – Suppose $F \subseteq E \subseteq K$ be three fields such that E is finite separable extension of F, K is finite separable extension of E, then K is finite separable extension of F.

proof – $E = F(\alpha)$ for some $\alpha \in E$

$K = E(\beta)$ for some $\beta \in K$

$K = E(\beta) = F(\alpha)(\beta) = F(\alpha, \beta)$

Let $\gamma \in F(\alpha, \beta)$, $\gamma \notin F(\alpha)$

T.P – γ is separable over F.

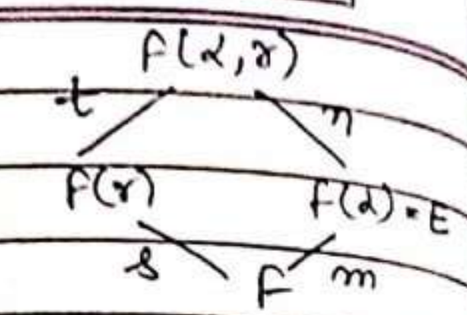
Scanned with CamScanner

Let $p_1(x)$ = minimal polynomial of α over F with deg m

$p_2(x)$ = minimal polynomial of γ over $F(\alpha)$ with deg n

$p_3(x)$ = minimal polynomial of γ over F with deg s.

$p_4(x)$ = minimal polynomial of α over $F(\gamma)$ with deg t



$[F[\alpha,\gamma]:F] = mn = st$

Suppose L is algebraically closed field containing F.

$\sigma : F \to L$ is embedding

$\Rightarrow$ σ can be extended from $F(\alpha) \to L$ in m ways

($\because$ minimal polynomial of α has deg m and α is separable over F)

say $\sigma_1, \sigma_2, \ldots, \sigma_m$.

Each σ_i can be extended from $F(\alpha,\gamma) \to L$ in n ways

[$\because$ deg of min. poly. of γ over $F(\alpha) = E$ is n and γ is separable over E]

i.e. $\sigma : F \to L$ can be extended to $F(\alpha,\gamma) \to L$ in mn ways a.k.a st ways. — (1)

Now if γ is not separable over F, then embedding $\sigma : F \to L$ can be extended to $F(\gamma) \to L$ in less than s ways

$\Rightarrow$ No. of total extensions of $\sigma : F \to L$ to $F(\alpha,\gamma) \to L$ are $< st$

$\longrightarrow \longleftarrow$ to statement (1)

Hence, γ must be separable over F.

Thm — If K is a field of $ch\ p \neq 0$, then K is perfect iff $K^p = K$.

proof :- Let $ch\ K = p$ and K is perfect.

Clearly, $K^p \subseteq K$

[$\because a \in K^p \Rightarrow a = b^p$ for some $b \in K \Rightarrow a \in K$]

Let $a \in K$

T.P that $a \in K^p$, we need to show that the poly. $f(x) = x^p - a \in K[x]$ has a solution in K.

$f(x)$ has a root 'b' in some extension of K.

Let $p(x)$ be minimal polynomial of b over K.

As K is perfect $\Rightarrow$ K(b) is separable extension of K

$\Rightarrow$ $p(x)$ has distinct roots.

as $f(b) = 0$

$\Rightarrow b^p = a \in K$

and $x^p - b^p = g(x) \in K[x]$

$g(b) = 0$

$\Rightarrow p(x) \mid g(x)$

also $g(x) = x^p - b^p = (x-b)^p$ [$\because ch\ K = p$]

$\Rightarrow p(x) \mid g(x) \Rightarrow p(x) \mid (x-b)^p$

$\Rightarrow p(x) = (x-b)^r$ where $r \leq p$

as $p(x)$ has distinct roots $\Rightarrow r = 1$

$p(x) = x - b \in K[x]$

$\Rightarrow b \in K$

also $a = b^p \Rightarrow a \in K^p \Rightarrow K \subseteq K^p$

converse:- Let $K^p = K$

To show that K is perfect, we show that every irreducible polynomial over K has distinct roots.

Let $p(x) \in K[x]$ be irreducible and it does not have distinct roots.

$\Rightarrow p(x) = g(x^p)$ for some polynomial $g(x) \in K[x]$

$\Rightarrow p(x) = a_0 + a_1 x^p + a_2 x^{2p} + \ldots + a_r x^{rp}$ — (1) where a_i's $\in K$

as $K^p = K \Rightarrow a_i = b_i^p$ for some $b_i \in K$

$p(x) = b_0^p + b_1^p x^p + \ldots + b_r^p x^{rp}$

$= (b_0 + b_1 x + \ldots + b_r x^r)^p$

$\Rightarrow p(x)$ is reducible

$\longrightarrow \longleftarrow$

Hence, K is perfect.

Scanned with CamScanner

PAGE NO. :
DATE : / /

PAGE NO. :
DATE : / /

Scanned with CamScanner

Scanned with CamScanner

PAGE NO. :
DATE : / /

PAGE NO. :
DATE : / /

Scanned with CamScanner

Scanned with CamScanner

11/12/24

Thm – Let H be a finite subgroup of group of Automorphisms of E. Then $[E:E_H] = |H|$

Proof – Let $H = \{e = g_1, g_2, \ldots, g_n\}$ and let $[E:E_H] = m$

Suppose $m < n$

Let $\{a_1, a_2, \ldots, a_m\}$ be basis of E over E_H.

Consider the system of n homogenous linear equations

$$g_1(a_j)y_1 + g_2(a_j)y_2 + \ldots + g_n(a_j)y_n = 0 \quad \forall\, 1 \le j \le m$$

Let $\alpha \in E$ then $\alpha = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_m a_m$, where α_i's $\in E_H$ then

$$g_1(\alpha)y_1 + g_2(\alpha)y_2 + \ldots + g_n(\alpha)y_n = g_1\left(\sum_{i=1}^{m} \alpha_i a_i\right)y_1 + g_2\left(\sum_{i=1}^{m} \alpha_i a_i\right)y_2 + \ldots + g_n\left(\sum_{i=1}^{m} \alpha_i a_i\right)y_n$$

$$= \sum_{i=1}^{m} \alpha_i g_1(a_i)y_1 + \sum_{i=1}^{m} \alpha_i g_2(a_i)y_2 + \ldots + \sum_{i=1}^{m} \alpha_i g_n(a_i)y_n$$

$$= \sum_{i=1}^{m} \alpha_i \left(g_1(a_i)y_1 + g_2(a_i)y_2 + \ldots + g_n(a_i)y_n\right)$$

$$= 0$$

$$\Rightarrow (g_1y_1 + g_2y_2 + \ldots + g_ny_n)(\alpha) = 0 \quad \forall\, \alpha \in E$$

① – $\begin{bmatrix} g_1(a_1)y_1 + \ldots + g_n(a_1)y_n \\ g_1(a_m)y_1 + \ldots + g_n(a_m)y_n = 0 \end{bmatrix}$

Non-trivial sol^n

$y_1 = y_2 = \ldots = y_n = 0$ (not all y_i's)

No. of Eq^n < No. of variable

$AX = 0$

$m \times n$

$m < n$

$\Rightarrow g_i$'s are L.D (∵ system of Equations ① has non-trivial solution ~~solution~~ as no. of Equations < no. of variables)

which is a contradiction.

So assume $m \ge n$

$\Rightarrow [E:E_H] \ge n+1$

$\Rightarrow \exists$ a set of $n+1$ elements, which is L.I over E_H

Let such set be $\{a_1, a_2, \ldots, a_{n+1}\}$

Consider the family of n homogenous linear equations

② – $g_j(a_1)x_1 + g_j(a_2)x_2 + \ldots + g_j(a_{n+1})x_{n+1} = 0 \quad ; 1 \le j \le n$

There are n equations in $n+1$ variables

$\Rightarrow \exists$ a non-trivial solution $y_1, y_2, \ldots, y_{n+1} \in E$ s.t not all y_i's are zero.

Choose $y_1, y_2, \ldots, y_{n+1}$, so that as few as possible are non-zero and renumber. So that,

$y_i \ne 0 ; i = 1, 2, \ldots, r$ & $y_i = 0 \ \forall i > r$

So, ② becomes

$$g_j(a_1)y_1 + g_j(a_2)y_2 + \ldots + g_j(a_r)y_r = 0 \quad \forall\, 1 \le j \le n \quad \text{—③}$$

Let $g \in H$

$$\Rightarrow g(g_j(a_1)y_1 + g_j(a_2)y_2 + \ldots + g_j(a_r)y_r) = g(0) \quad \forall\, 1 \le j \le n$$

$$\Rightarrow g(g_j(a_1))g(y_1) + g(g_j(a_2))g(y_2) + \ldots + g(g_j(a_r))g(y_r) = 0 \quad \forall\, 1 \le j \le r$$

which is same as system

$$g_j(a_1)g(y_1) + g_j(a_2)g(y_2) + \ldots + g_j(a_r)g(y_r) = 0 \quad \forall\, 1 \le j \le r \quad \text{—④}$$

$g(y_1)$③ – $y_1$④ gives

$$g_j(a_2)[y_2g(y_1) - y_1g(y_2)] + g_j(a_3)[y_3g(y_1) - y_1g(y_3)] + \ldots + g_j(a_r)[y_rg(y_1) - y_1g(y_r)] = 0 \quad \forall\, 1 \le j \le n$$

we get a non-trivial solution of system of equation ② with $r-1$ coefficient non-zero if we can prove that $y_ig(y_1) - y_1g(y_i) = 0 \quad \forall\, 2 \le i \le r$

Now $y_ig(y_1) - y_1g(y_i) = 0$

$\Rightarrow y_ig(y_1) = y_1g(y_i)$

$\Rightarrow g(y_1)(g(y_i))^{-1} = y_i^{-1}y_1$

$\Rightarrow g(y_1y_i^{-1}) = y_1y_i^{-1}$

$\Rightarrow y_1y_i^{-1} \in E_H$

Scanned with CamScanner

$\Rightarrow \exists\ z_1, z_2, \ldots, z_n \in E_H$ s.t

$y_i = y_j z_i \quad \forall\ 1 \le i \le n$

So, system of equations (3) becomes $(\because a_1 = 1)$

$g_1(a_1) y_1 z_1 + g_1(a_2) y_1 z_2 + \ldots + g_1(a_n) y_1 z_n = 0$

$\Rightarrow g_1(a_1) z_1 + g_1(a_2) z_2 + \ldots + g_1(a_n) z_n = 0 \quad (\because y_1 \neq 0)$

$\Rightarrow g_1(a_1) g_1(z_1) + g_1(a_2) g_1(z_2) + \ldots + g_1(a_n) g_1(z_n) = 0$

$\Rightarrow g_1(a_1 z_1 + a_2 z_2 + \ldots + a_n z_n) = 0$

$\Rightarrow a_1 z_1 + a_2 z_2 + \ldots + a_n z_n = 0$

$\Rightarrow a_1, a_2, \ldots, a_n$ are L.I over E_H

but $\{a_1, a_2, \ldots, a_n\} \subseteq \{a_1, a_2, \ldots, a_{n-1}\}$

which is a contradiction.

$\Rightarrow m = n$

Hence proved.

Thm- Let F be finite separable extension of a field f.
Then TFAE

(1) F is normal Extension of f
(2) f is fixed field of $G(F|f)$
(3) $[F:f] = |G(F|f)|$

Example :- find $G(\mathbb{Q}(\alpha)|\mathbb{Q})$, where α satisfies $x^5 = 1, \alpha \neq 1$

Sol^n:- $|G(\mathbb{Q}(\alpha)|\mathbb{Q})| \le [\mathbb{Q}(\alpha):\mathbb{Q}]$ = deg. of min poly. of α over $\mathbb{Q}$ = 4

As α satisfies $x^5 = 1$

$\Rightarrow \alpha^5 = 1$

$\Rightarrow (\alpha - 1)(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4) = 0$

as $\alpha \neq 1$

$\Rightarrow 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$

$\Rightarrow$ Irreducible polynomial

$f : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ s.t

$f(a) = a \quad \forall\ a \in \mathbb{Q}$

To find $f(\alpha)$

$\alpha^5 = 1 \Rightarrow f(\alpha^5) = f(1) = 1$

$\Rightarrow (f(\alpha))^5 = 1 \Rightarrow f(\alpha)$ is root of $x^5 = 1$

$\Rightarrow f(\alpha) = x, \alpha, \alpha^2, \alpha^3, \alpha^4$

If $f(\alpha) = 1$
$\Rightarrow f : \mathbb{Q}(\alpha) \to \mathbb{Q}$

$\Rightarrow \alpha, \alpha^2, \alpha^3, \alpha^4$ are automorphisms

$f : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$

$f(a_0 + a_1 x + a_2 x^2 + a_3 x^3) = a_0 + a_1 f(\alpha) + a_2 (f(\alpha))^2 + a_3 (f(\alpha))^3$

$a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 \xrightarrow{f_1} a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3$

$\xrightarrow{f_2} a_0 + a_1 \alpha^2 + a_2 \alpha^4 + a_3 \alpha$

$\xrightarrow{f_3} a_0 + a_1 \alpha^3 + a_2 \alpha + a_3 \alpha^4$

$\xrightarrow{f_4} a_0 + a_1 \alpha^4 + a_2 \alpha^3 + a_3 \alpha^2$

$\Rightarrow \{f_1, f_2, f_3, f_4\} = G(\mathbb{Q}(\alpha)|\mathbb{Q})$

$o(f_i) \quad f_i^5 = id$

Scanned with CamScanner