PAGE NO.
DATE: / /

UNIT-III

Why we study field Extension?

Field Extension

motivation:-
$x^2+1=0$ Q
$x = \pm i \notin Q$ field
$x^2+1 \in Q[x]$
but roots do not belong in Q.
$x^2+1 = (x+i)(x-i)$
$Q[x]$ $\notin Q[x]$ $\notin Q[x]$

Definition:- If F is a subfield of E then E is said to be an extension field of F or simply extension of F. We denote this extension as

notation $\left[\begin{array}{c} E \\ \uparrow \\ F \end{array}\right.$ $F \subseteq E$

natural Question arises whether x^2+1 does not split into linear factors in any field $E[x]$ other than $Q[x]$. s.t. $Q[x] \subseteq E[x]$

Ex: $\mathbb{R}$ is a subfield of $\mathbb{C}$ hence $\mathbb{C}$ is extension field of $\mathbb{R}$ i.e. $\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$

other examples are $\begin{array}{c} \mathbb{C} \\ | \\ Q \end{array}$, $\begin{array}{c} \mathbb{R} \\ | \\ Q \end{array}$ etc.

Degree of Extension

Definition:- Let E be an extension of F. then E is vector space over F

$E(F) \longrightarrow$ vector space over F.

The dimension of $E(F)$ is called the degree of extension and is denoted by $[E:F]$

If $[E:F] < \infty$
that means if dimension of vector space $E(F)$ is finite then $\begin{array}{c} E \\ | \\ F \end{array}$ is called finite extension of F o.w. infinite extension.

Ex ①
Find degree of extensions of the following
(a) $[C:\mathbb{R}] = 2$
Sol^n: $C[\mathbb{R}] \to$ v.s. $a+ib = a(1)+b(i)$ $\forall a,b \in \mathbb{R}$ dim $= 2$
(b) $[\mathbb{R}:\mathbb{R}]$ $a \in \mathbb{R}$ $a = a(1)$ $\forall a \in \mathbb{R}$ basis $= \{1\}$
$\therefore$ $[\mathbb{R}:\mathbb{R}] = 1$
(c) $[\mathbb{C}^2:\mathbb{C}]$

(d) $[\mathbb{R}:\mathbb{Q}]$

Sol^n: (a) $[\mathbb{C}:\mathbb{R}]$
$a+ib \in \mathbb{C}$ $a+ib = a(1)+b(i)$ $\forall a,b \in \mathbb{R}$
basis of $\mathbb{C}(\mathbb{R}) = \{1, i\}$
$\therefore [\mathbb{C}:\mathbb{R}] = 2$
In general dim $C^n[\mathbb{R}] = 2n$

(b) $[\mathbb{R}:\mathbb{R}]$
basis $= \{1\}$ $\therefore [\mathbb{R}:\mathbb{R}] = 1$

(c) $[\mathbb{C}^2:\mathbb{C}] = 2$
$(a+ib, c+id) \in \mathbb{C}^2$
$(a+ib, c+id) = (a+ib)(1,0) + (c+id)(0,1)$
basis $\{(1,0), (0,1)\}$

(d) $[\mathbb{R}:\mathbb{Q}] = \infty$

$a \in \mathbb{R}$; $a = a(1)$, $a \in \mathbb{R}$, $1 \in \mathbb{Q}$

~~none of~~ 1 can not generate $\mathbb{R}$ over $\mathbb{Q}$.

$\therefore$

$$[\mathbb{R}:\mathbb{Q}] = \infty$$

note:-

$[\mathbb{C}:\mathbb{R}]$, $[\mathbb{R}:\mathbb{R}]$, $[\mathbb{C}^2:\mathbb{C}]$ are finite extensions while $[\mathbb{R}:\mathbb{Q}]$ is infinite extension.

Splitting Fields

Definition Let E be an extension field of F i.e. $E \mid F$ and let $f(x) \in F[x]$. We say that $f(x)$ splits in E if $f(x)$ can be factored as a product of linear factors in $E[x]$ i.e.

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_i), \alpha_i \in E$$

we call E a splitting field for $f(x)$ over F if $f(x)$ splits in E but does not split in any proper subfield of E.

$$\begin{array}{ll} & E \\ & \mid \; K \\ f(x) \in F[x] \longleftarrow & F \end{array}$$

splits; does not split over K

See ☆
☆ $E \mid F$ — $f(x) \in F[x]$
$\Rightarrow f(x)$ splits over E iff $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in E[x]$

Examples:- Find splitting field of

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

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

PAGE NO.
DATE: / /

Solⁿ: (1) $x^2+1 \in R[x]$
we have to find splitting field E of R s.t x^2+1 splits over $E[x]$ but there does not exist any other field K s.t $R \subset K \subset E$

we know that
$$x^2+1 = (x+i)(x-i)$$
$$\mathbb{C}$$

$\mathbb{C}$ | R splitting field of $f(x) = x^2+1$ is $\mathbb{C}$.

degree of extension $[\mathbb{C} : R] = 2$

(2) $x^2+1 \in Q[x]$
$$x^2+1 = (x+i)(x-i)$$
$-i \quad i$

$\mathbb{C}$ | R | Q

$Q[i] = \{a+ib : a, b \in Q\}$, $\mathbb{C} = \{a+ib : a, b \in R\}$
$i \in Q[i]$, $-i \in Q[i]$

$x^2+1 = (x+i)(x-i)$
$\in Q[i] \quad \in Q[i]$ $\qquad Q \subset Q[i] \subset R \subset \mathbb{C}$

x^2+1 splits over $Q[i]$
$\therefore$ splitting field of x^2+1 is $Q[i]$

$[Q[i] : Q] = 2$

$a+ib$
$= a(1) + b(i)$
$a, b \in Q$