2016

Page:

① Let K be a field and $K[x]$ be the ring of polynomials over K in a single variable x. For a polynomial $f \in K[x]$ let (f) denote the ideal in $K[x]$ generated by f. Show that (f) is maximal ideal in $K[x]$ iff it is an irreducible polynomial over K. (10)

Solⁿ:- { THINGS TO KNOWS:

Irreducible polynomial :-

Defⁿ: Let R be an integral domain with unity. A polynomial $f(x) \in R[x]$ of positive degree (i.e. of deg ≥ 1) is said to be an irreducible polynomial over R if it can not be expressed as product of two polynomials of positive degree.

in other words, if whenever

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

then $\deg g = 0$ or $\deg h = 0$

A polynomial of positive degree which is not irreducible is called reducible over R.

eg:- $x^2+1 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$.

whereas it is reducible over $\mathbb{C}$.

as $x^2+1 = (x-i)(x+i)$

or x^2-2 is irreducible over $\mathbb{Z}$

but reducible over $\mathbb{R}$ as

$$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$$

Maximal Ideals:-

let R be a ring. An Ideal $M \neq R$ of R is called a maximal ideal of R if whenever A is an ideal of R $\ni$

$$M \subseteq A \subseteq R \text{ then}$$

either $A = M$ or $A = R$

Sol^n:- Suppose $f(x) \in (f)$ is irreducible and let I be an ideal of ~~F[x~~ $K[x]$ containg (f).

i.e. $(f) \subset I \subset K[x]$

$\because$ K is Field $\Rightarrow$ $K[x]$ is E.D

$\Rightarrow$ $K[x]$ is P.I.D

$\Rightarrow$ every Ideal of $K[x]$ is principal ideal.

$\Rightarrow$ $I = \langle p(x) \rangle$ $\quad p(x) \in K[x]$.

$\because$ $f(x) \in I$

$\Rightarrow$ $f(x) = p(x) \cdot q(x)$ for some $q(x) \in K[x]$

but f is irreducible

$\Rightarrow$ either $p(x)$ has degree 0 or $q(x)$ has degree 0.

if $p(x)$ has degree $0 \Rightarrow p(x)$ is unit in F.

$\Rightarrow$ $1 \in I$

$\Rightarrow$ $I = K[x]$ --- (i)

If $q(x)$ has deg 0 then

then $q(x)$ is unit in F and $\exists$ $q'(x)$ $\ni$

$f(x) \cdot q'(x) = p(x) \cdot 1$

$\Rightarrow$ $p(x) \in (f)$ — as $q'(x) \in K[x]$.

$\Rightarrow$ $I = (f)$ —— (ii)

hence we have assume that
$(f) \subseteq I \subseteq K[x]$
and from ① & ②
we are able to prove
either $(f) = I$ or $I = K$
hence (f) is maximal ideal.

<u>conversly:-</u>
suppose $I = \langle f(x) \rangle$ is a maximal ideal of $K[x]$. then ~~p(x)~~ $f(x) \neq 0$
If $f(x) = p(x) \cdot q(x)$ is proper factorisation of f then ~~either~~ both $q(x)$ and $p(x)$ have degree atleast 1 and $\langle q(x) \rangle$ and $\langle p(x) \rangle$ are proper ideal of $K[x]$ properly containing ~~I~~ f.
this contradicts the maximality of f. So we conclude that f is irreducible.

eg:- $p(x) = \langle x^2 - 6x + 9 \rangle$
but $(x^2 - 6x + 9) = (x - 3)(x - 3)$

$$\underbrace{(x^2-6x+9)}_{f(x)} = \underbrace{(x-3)}_{q(x)}\,\underbrace{(x-3)}_{p(x)}$$

$\therefore f(x) \in \langle q(x) \rangle$

(2) let p be a prime number and $\mathbb{Z}_p$ denote the additive group of Integers modulo p. Show that every non-zero element of $\mathbb{Z}_p$ generates $\mathbb{Z}_p$. (15)

a ∈ G, least +ve int n, $a^n = e$

Things to know:-

$\mathbb{Z}_5$:- $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\bar{3} \rightarrow 5 \cdot 3 = 3+3+3+3+3$
$= 15 = 0$

$\forall$ non zero element a in $\mathbb{Z}_5$
$5a = 0$

$n \cdot a = a + a + a + \dots + a$ (n)

$\mathbb{Z}_6$:- $\{0, 1, 2, 3, 4, 5\}$
$\forall \; a \in \mathbb{Z}_6$
$6 \cdot a = 0$

but $\exists$ $b \in \mathbb{Z}_6$, $b < 6$ $\ni$
$b \cdot p = 0$,

eg:- $3 \in \mathbb{Z}_6$ $\quad 3 \cdot 2 = 6 = 0$
$\Rightarrow 2 + 2 + 2 = 0$

$\therefore H = \{0, 2, 2+2\} = \{0, 2, 4\}$ is subgroup of $\mathbb{Z}_6$.

$o(H) \mid o(G) = \mathbb{Z}_6$
$\Rightarrow 3 \mid 6$.

Scanned with CamScanner

Solⁿ:- $\mathbb{Z}_p = \{0, 1, 2, 3, \ldots p-1\}$

we know that $\forall\, a \neq 0$ in $\mathbb{Z}_p$

$pa = a + a + \cdots + a$ (p times)

$= 0$

if we are able to prove that

$\nexists$ any $q \in \mathbb{Z} \ni 0 < q < p$

$\ni qa = 0$ for any $a \in \mathbb{Z}_p$, $a \neq 0$

suppose $\exists\, q \in \mathbb{Z} \ni 0 < q < p$

$qa = 0$ for some $a \in \mathbb{Z}_p$

$\Rightarrow o(a) = q$

and $H = \langle a \rangle = \{a, 2a, 3a, (q-1)a, 0\}$

is subgroup of $\mathbb{Z}_p$.

$\therefore$ by lagrange's theorm.

$o(H) \mid o(\mathbb{Z}_p)$

but $o(\mathbb{Z}_p) = p$

p is prime.

so only divisor of p is 1 and p.

but $o(a) = q < p$

$\Rightarrow o(a) = q = 1$

but $a \neq 0$

hence it is contradiction.

$\nexists$ any $q \in \mathbb{Z} \ni 0 < q < p$

and $qa = 0$ for any $a \neq 0 \in \mathbb{Z}_p$

$\Rightarrow \forall\, a \neq 0 \quad o(a) = p = o(\mathbb{Z}_p)$

hence every non zero elements in $\mathbb{Z}_p$ generates $\mathbb{Z}_p$.

Scanned with CamScanner

③ let K be an extension of a field F prove that the element of K which are algebraic over F form a subfield of K Further If $F \subset K \subset L$ are fields, L is algebraic over K and K is algebraic over F then prove that L is algebraic over F.

(20)

∴ Things to know:-

Defn:- Extension Field:-

A Field E is an extension field of a field F if $F \subseteq E$ and the operations of F are those of E ristricted to F. i.e. F is subfield of E.

Algebraic element:-

let K be an extension of F. $a \in K$ is said to be algebraic over F if $\exists$ non-zero polynomial $f(x) \in F[x] \ni f(a) = 0$ otherwise it is called transcedental element.

eg:- $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ $\because f(x) = x^2 - 2 \in \mathbb{Q}[x]$

Theorem:-

If E is a finite extension of F, then E is an algebraic extension of F.

proof:-

PROOF:- suppose that $[E:F]=n$ and $a \in E$ is arbitrary. then the set $\{1, a, a^2, \dots a^n\}$ is linearly dependent over F. that is there are elements $c_0, c_1, \dots c_n$ in F not all zero $\ni$

$$c_n a^n + c_{n-1} a^{n-1} + \dots + c_1 a + c_0 = 0$$

clearly, then a is a zero of the non-zero polynomial

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

hence a is algebraic element.

$\therefore$ E is algebraic extension of F.

Sol^n:- First we will prove set of all algebraic element forms subfield of K. suppose that $a, b \in K$ are algebraic over F. and $b \neq 0$, to show that $a+b$, $a-b$, $a \cdot b$ and a/b are algebraic over F, it suffices to show that $[F(a,b):F]$ is finite, $\because$ each of these four elements belongs to $F(a,b)$. but note that

$$[F(a,b):F] = [F(a,b):F(b)][F(b):F]$$

Also, $\because$ a is algebraic over F it is certainly algebraic over $F(b)$. Thus, both $[F(a,b):F(b)]$ and $[F(b):F]$ are finite.

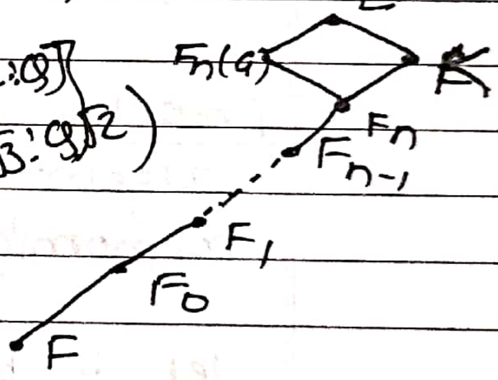
now we prove that
If L is algebraic over K and K is algebraic over F
$F \subset K \subset L$ then
L is algebraic over F.

let ~~$a \in K$~~ $a \in L$ .. It suffices to show that $a \in$ some finite extension of F.
since a is algebraic over K
we know that a is zero of some irreducible polynomial in $K[x]$.
say $P(x) = b_n x^n + \cdots + b_0$
where $b_n, b_{n-1}, \cdots b_0 \in K$

now we construct a tower of field extension of F as follows,

$F_0 = F(b_0)$
$F_1 = F_0(b_1)$
$F_2 = F_1(b_2)$
$\vdots$
$F_n = F_{n-1}(b_n)$

$\{ [\mathbb{Q}\sqrt{2} : \mathbb{Q}]$
$[(\mathbb{Q}\sqrt{2})\sqrt{3} : \mathbb{Q}\sqrt{2})$



in particular,
$F_n = F(b_0, b_1, \cdots b_n)$

so that $P(x) \in F_n[x]$.
thus $[F_n(a) : F_n] = n$ and because each b_i is algebraic over F, we know that each $[F_{i+1} : F_i]$ is finite.
so $[F_n(a) : F] = [F_n(a) : F_n][F_n : F_{n-1}] \cdots [F_1 : F_0][F_0 : F]$
is finite.
hence L is algebraic over F.

(4) Show that every algebraically closed field is infinite. (15)

Soln: Things to know:-

Defn:- Algebraically closed field:-

A Field K is called algebraically closed if every polynomial f over K splits in K.

By Fundamental theorem of Algebra, every polynomial over $\mathbb{C}$, the field of complex number splits in $\mathbb{C}$. So $\mathbb{C}$ is algebraically closed field. However, $\mathbb{R}$ the field of Real is not algebraically closed as $x^2+1 \in \mathbb{R}[x]$ does not split in $\mathbb{R}$.

PROOF:- A Field F is said to be algebraiclly closed if each non-constant polynomial in $F[x]$ has a root in F.

let F be a finite field and consider the polynomial

$$f(x) = 1 + \prod_{a \in F} (x-a)$$

The coefficient of $f(x)$ lie in the field F and thus $f(x) \in F[x]$. ofcourse, $f(x)$ is a non-constant polynomial.

Note that for each $a \in F$ we have $f(a) = 1 \neq 0$
so the polynomial $f(x)$ has no root in F.
hence the finite field F is not algebraic closed.

It follows that every algebraically closed field must be infinite.