14/08/2016
Sunday:

Q.No. $2\mathbb{Z} \approx 3\mathbb{Z}$?

Soln: $f: 2\mathbb{Z} \to 3\mathbb{Z}$ has no one-one onto ring homo. then $2\mathbb{Z} \not\approx 3\mathbb{Z}$

Similarly $5\mathbb{Z} \not\approx 6\mathbb{Z}$

$m\mathbb{Z} \not\approx n\mathbb{Z}$ (if $m \neq n$ are different)

(i.e $m \neq n$

H.W.

Q.No. (i) $f: Q \times Q \longrightarrow Q$

(ii) $f: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, how many homomorphism?

Soln (i) Idemp. element in Q are 0 & 1

$f(x,y) = 0 \cdot x \Rightarrow \ker f = Q \times Q$ $\quad f(x,y) = 1 \cdot y \to \ker f = Q \times \{0\}$

$f(x,y) = 1 \cdot x \to \ker f = \{0\} \times Q$

then $f: Q \times Q \to Q$ has exactly 3 ring homo.

(ii) Idempt. element in R are 0 & 1 then

$f(x,y) = 0 \to \ker f = \mathbb{R} \times \mathbb{R}$

$f(x,y) = 1 \cdot x \to \ker f = \{0\} \times \mathbb{R}$

$f(x,y) = 1 \cdot y \to \ker f = \mathbb{R} \times \{0\}$

then $f: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ has exactly 3 ring homo.

Q.No. $Q[\sqrt{2}] \overset{R}{\approx} Q$?

Soln: (i) $f(x) = x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2})$ in $Q(\sqrt{2})$. But

$f(x) = x^2 - 2$ has no soln in Q then $Q(\sqrt{2}) \not\approx Q$

Q.No. $Q[i] \approx Q[\sqrt{3}]$?

Soln $f(x) = x^2 + 1$ has a soln in $Q[i]$ but not in $Q[\sqrt{3}]$ then $Q[i] \not\approx Q[\sqrt{3}]$.

Scanned with CamScanner

Q.No (i) $\mathbb{R} \cong \mathbb{Q}$?

(ii) $\mathbb{R} \cong \mathbb{C}$?

Soln :- (i) $f(x) = x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})$ in $\mathbb{R}$ but $\mathbb{R}$ has no roots, so $\mathbb{R} \ncong \mathbb{Q}$

(ii) $f(x) = x^2 + 1 = (x+i)(x-i)$ has a soln in $\mathbb{C}$ but not in $\mathbb{R}$ then

$\mathbb{R} \ncong \mathbb{C}$

H.P.

Polynomial Ring :- let R be a commutative Ring then the set $R[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots \mid a_i \in R\}$ is ring in x (one way)

$= \{a_0 + a_1x + a_2x^2 + \dots \mid a_i \in R\}$ (or another way)

Sum of two Polynomial of $R[x]$

$f(x) = a_0 + a_1(x) + a_2x^2 + \dots + a_nx^n$, $a_i \in R$

and $g(x) = b_0 + b_1(x) + b_2x^2 + \dots + b_nx^n$, $b_i \in R$

such that $f(x) + g(x) = (a_0+b_0) + (a_1+b_1)x + \dots + (a_n+b_n)x^n + \dots$

Product of two Polynomial of $R[x]$:-

Let $f(x) = a_0 + a_1x \in R[x]$

$g(x) = b_0 + b_1x \in R[x]$

s.t. $f(x)\cdot g(x) = (a_0+a_1x)(b_0+b_1x)$

$= a_0b_0 + (a_0b_1 + a_1b_0)x + a_1b_1x^2$

$\Rightarrow f(x)\cdot g(x) \in R[x]$

gmp

Note: If R is commutative Ring then R[x] is also commutative, is called commutative Ring.

Hint: let R is commutative Ring then $a_ib_j = b_ja_i \ \forall\ a_i, b_j \in R$

and $g(x) = b_0+b_1x \in R[x]$

$f(x)\cdot g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + a_1b_1x^2$

$= b_0a_0 + (b_1a_0 + b_0a_1)x + b_1a_1x^2$

$= (b_0+b_1x)(a_0+a_1x)$

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

then R[x] is commutative.

(ii) if R is commutative Ring with unity then R[x] is also Ring with unity.

Hint: let R be a commutative Ring with unity 1 then

$1 = 1 + 0x + 0x^2 + \cdots + 0x^n \in R[x]$

such that $f(x)\cdot 1 = 1\cdot f(x) = f(x)$

then R[x] is also commutative Ring with unity 1.

gmp

Q.No. If R is an integral domain then R[x] is also integral domain.

Soln: Hint: let R be an integral domain and

$R[x] = \{ a_0+a_1x+\cdots+a_nx^n \mid a_i \in R \}$

Let $0 \neq f(x) = a_0+a_1x+\cdots+a_nx^n \in R[x]$ of degree n then $a_n \neq 0$

and $0 \neq g(x) = b_0+b_1x+\cdots+b_mx^m \in R[x]$ of degree m, then $b_m \neq 0$

s.t. $f(x)\cdot g(x) = c_0 + c_1x + \ldots + a_n b_m x^{n+m}$ ——— (*)

$0 \neq a_n \in R$, $0 \neq b_n \in R$ and R is an integral domain then

$a_n \cdot b_n \neq 0$

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

then $R[x]$ is an integral domain.

(iv) gmp If F is field then $F[x]$ is an integral domain but not field.

Soln:- If F is field then $F[x]$ is an integral domain

$x \in F[x]$ but $x^{-1} \notin F[x]$

$x \cdot x^{-1} = 1$

then $F[x]$ is not field.

C.S.I.R

Q.No. $f(x) = x^3+x^2+x+1 \in R[x]$ and $g(x) = x^3-x^2+x-1 \in R[x]$ then find $\gcd(f(x), g(x))$ and $LCM(f(x), g(x))$

Soln:-

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

$\Rightarrow f(x) = (x^2+1)(x+1)$ ——— (1)

and $g(x) = x^3-x^2+x-1$

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

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

then $\gcd(f(x), g(x)) = (x^2+1)$

and $LCM(f(x), g(x)) = (x^2+1)(x-1)(x+1) = x^4-1$

Irreducible Polynomial:-

Let R be an integral domain. A non zero non unit polynomial $f(x) \in R[x]$ is said to be irreducible polynomial if $f(x) = g(x)h(x)$, $g(x) \in R[x]$, $h(x) \in R[x]$

non zero non unit polynomial consider करना है।

Scanned with CamScanner

then either $g(x)$ is unit of $h(x)$ is unit in $R[x]$.

H.Gmp Examples

① $f(x) = 11+33x^2 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$?

$\Rightarrow f(x) = 11+33x^2 \in \mathbb{Q}[x]$ because $\mathbb{Z} \subseteq \mathbb{Q}$

Now $f(x) = 11+33x^2 = 11(1+3x^2)$

$= g(x) \cdot h(x)$ where $g(x) = 11 \in \mathbb{Q}[x]$

" $h(x) = (1+3x^2) \in \mathbb{Q}[x]$

$g(x) = 11$ is unit in $\mathbb{Q}[x]$

then $f(x) = 11+33x^2$ is irreducible over $\mathbb{Q}$.

Gmp

Q.No. Show that $f(x) = 4+2x^2$ is irreducible over $\mathbb{Q}$ but not irreducible over $\mathbb{Z}$.

Soln:- $f(x) = 4+2x^2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$

$= 2(2+x^2)$

$= g(x)\, h(x)$ where $g(x) = 2 \in \mathbb{Q}[x]$

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

$g(x) = 2$ is unit in $\mathbb{Q}[x]$

then $f(x) = 4+2x^2$ is irreducible over $\mathbb{Q}$.

Now, $f(x) = 4+2x^2 \in \mathbb{Z}[x]$

$= 2(2+x^2)$

$= g(x)\, h(x)$ where $g(x) = 2 \in \mathbb{Z}[x]$

and $h(x) = 2+x^2 \in \mathbb{Z}[x]$

But neither 2 is unit in $\mathbb{Z}[x]$ nor $h(x) = 2+x^2$ is unit in $\mathbb{Z}[x]$.

then $f(x) = 4+2x^2$ is not irreducible over $\mathbb{Z}$.

(or reducible over $\mathbb{Z}$)

Q.No. $f(x) = 8-2x^2 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$?

Soln:- $f(x) = 8-2x^2 = 2(4-x^2) \in \mathbb{Q}[x]$

$= g(x) \cdot h(x)$, where $g(x) = 2 \in \mathbb{Q}[x]$

and $h(x) = 4-x^2 \in \mathbb{Q}[x]$

Scanned with CamScanner

Note:- $g(x)=2$ is unit in $\mathbb{Q}[x]$ but $f(x)$ is not irreducible over $\mathbb{Q}$. because $h(x)=4-x^2$ is not irreducible over $\mathbb{Q}$.

*** Note

If $f(x)=g(x)h(x)$ and $g(x)$ is unit then behaviour of $f(x)$ depends on behaviour of $h(x)$.

$$\left[\underbrace{g(x)f(x)=k(x)}_{f(x)=[g(x)]^{-1}k(x)}\right]$$

Q.No. $f(x)$ is non zero non unit polynomial of $R[x]$ and $g(x)$ unit in $R[x]$ s.t. $g(x)\cdot f(x)$ is irreducible then $f(x)$ is irreducible over R.

Soln let $g(x)$ is unit in $R[x]$ and $g(x)\cdot f(x)=h(x)$ is irreducible polynomial

$\Rightarrow h(x)$ is irreducible.

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

$\Rightarrow f(x)=[g(x)]^{-1}h(x)$

Since $g(x)$ is unit in $R[x]$ then $[g(x)]^{-1}$ is also unit in $R[x]$ then the behaviour of $f(x)$ depends on $h(x)$.

and $h(x)$ is irreducible then $f(x)$ is irreducible over R.

Q.No. $f(x)=x^2+1$ is irreducible over $\mathbb{Q}$?

Soln $f(x)=x^2+1=(x+i)(x-i)$

$=g(x)\cdot h(x)$ But $g(x)=(x+i)\notin \mathbb{Q}[x]$

and $h(x)=(x-i)\notin \mathbb{Q}[x]$ then $f(x)=x^2+1$ is irreducible over $\mathbb{Q}$.

and it is reducible in $\mathbb{C}$ and $\mathbb{Q}[i]$.

Scanned with CamScanner

Q.No. Show that $f(x) = x^2+1$ is irreducible over $\mathbb{R}$ but not over $\mathbb{Q}[i]$ and $\mathbb{C}$.

Soln $f(x) = x^2+1 = (x+i)(x-i)$
$g(x)\ h(x)$, where $g(x) = x+i \notin \mathbb{R}[x]$
$h(x) = x-i \notin \mathbb{R}[x]$

then $f(x) = x^2+1$ is irreducible over $\mathbb{R}$

Now $f(x) = x^2+1 \in \mathbb{Q}[i][x] \mid \mathbb{C}[x]$ → oblique (दोनों में से एक)
$= (x+i)(x-i)$
$= g(x) \cdot h(x)$

where $g(x) = x+i \in \mathbb{Q}[i][x] \mid \mathbb{C}[x]$
& $h(x) = x-i \in \mathbb{Q}[i][x] \mid \mathbb{C}[x]$

but neither $g(x)$ nor $h(x)$ is unit in $\mathbb{Q}[i][x] \mid \mathbb{C}[x]$

Hence $f(x) = x^2+1$ is reducible over $\mathbb{Q}[i][x] \mid \mathbb{C}[x]$

$\Rightarrow f(x) = x^2+1$ is not irreducible over $\mathbb{Q}[i][x] \mid \mathbb{C}[x]$

Q.No. Show that $f(x) = x^2-2$ is irreducible over $\mathbb{Q}$ but not over $\mathbb{R}$.

Soln $f(x) = x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$
$= g(x) \cdot h(x)$ where $x-\sqrt{2} = g(x) \notin \mathbb{Q}[x]$
where $h(x) = x+\sqrt{2} \notin \mathbb{Q}[x]$

then $f(x) = x^2-2$ is irreducible over $\mathbb{Q}$.

Now, $f(x) = x^2-2 \in \mathbb{R}[x]$
$= (x-\sqrt{2})(x+\sqrt{2})$ where $g(x) = x-\sqrt{2} \in \mathbb{R}$
$h(x) = x+\sqrt{2} \in \mathbb{R}$

But neither $g(x)$ nor $h(x)$ is unit in $\mathbb{R}$

Hence $f(x) = x^2-2$ is not irreducible over $\mathbb{R}$

Q.No. $f(x) = x^3+x^2+x+1 \in \mathbb{Z}[x]$ is irreducible over ~~$\mathbb{Z}[0] = ?$~~ $\mathbb{Z} \mid \mathbb{Q}$?

Soln $f(x) = x^3+x^2+x+1$
$= x^2(x+1)+1(x+1)$
$= (x^2+1)(x+1)$ where $g(x) = x^2+1 \in \mathbb{Z}[x] \mid \mathbb{Q}[x]$

Scanned with CamScanner

then neither $g(x)$ is unit nor $h(x)$ is unit in $\mathbb{Z}[x] \mid \mathbb{Q}[x]$.
then $f(x) = x^3+x^2+x+1$ is not irreducible over $\mathbb{Z} \mid \mathbb{Q}$.

Q.No. (i) $f(x) = x^3-x^2+x+1 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z} \mid \mathbb{Q}$?

(ii) $f(x) = x^3+1$ " " " " "

(iii) $f(x) = x^3-1$ " " " " "

(1) Soln $f(x) = (x^3-x^2+x+1) = (x^2+1)(x-1) = g(x) \cdot h(x)$

where $g(x) = x^2+1 \in \mathbb{Z}[x] \mid \mathbb{Q}[x]$

$h(x) = x-1 \in \mathbb{Z}[x] \mid \mathbb{Q}[x]$

But neither $g(x)$ is unit nor $h(x)$ is unit in $\mathbb{Z}[x] \mid \mathbb{Q}[x]$
then $f(x) = x^3-x^2+x-1$ is not irreducible
over $\mathbb{Z} \mid \mathbb{Q}$.

2. Soln $f(x) = x^3+1 = (x+1)(x^2-x+1) = g(x) \cdot h(x)$

where $g(x) = x+1 \in \mathbb{Z}[x] \mid \mathbb{Q}[x]$

$f(x) = x^2-x+1 \in$ " "

But neither $h(x)$ nor $g(x)$ is unit in $\mathbb{Z}[x] \mid \mathbb{Q}[x]$
then $f(x) = x^3+1$ is not irreducible.

3. Soln $f(x) = x^3-1 = (x-1)(x^2+x+1)$

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

where $g(x) = x-1 \in \mathbb{Z}[x] \mid \mathbb{Q}[x]$

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

But neither $g(x)$ nor $h(x)$ is unit in $\mathbb{Z}[x] \mid \mathbb{Q}[x]$
then $f(x) = x^3-1$ is not irreducible.

H.P.

Scanned with CamScanner

Einestein's Irreducibility Criterion:

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$. If $\exists$ prime p s.t. $p \mid a_0, p \mid a \cdots p \mid a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$.

For Example:

① $f(x) = 2 + 6x + 4x^3 + 6x^4 + x^5 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$?

Let $\exists\ p = 2$ s.t. $2 \mid 2, 2 \mid 6, 2 \mid 0, 2 \mid 6$ but $2 \nmid 1$ and $2^2 \nmid 2$
(a_n) ($a_0(x)$)

then $f(x) = 2 + 6x + 4x^3 + 6x^4 + x^5$ is irreducible over $\mathbb{Q}$.

H.W:

Q.No. $f(x) = 6 + 8x + 6x^2 + 12x^3 + x^4$ is irreducible over $\mathbb{Q}$?

Soln:- $p = 2$ s.t.

$2 \mid 12, 2 \mid 6, 2 \mid 8, 2 \mid 12$ but $2 \nmid 1$ and $2^2 \nmid 6$

then $f(x)$ is irreducible over $\mathbb{Q}$.

Q.No. $f(x) = 12 + 18x + 6x^2 + 24x^3 + x^4$ is irreducibility over $\mathbb{Q}$?

Soln:- $p = 3$ s.t. $3 \mid 12, 3 \mid 18, 3 \mid 6, 3 \mid 24$ but $3 \nmid 1$ and $3^2 \nmid 12$ then $f(x)$ is irreducible over $\mathbb{Q}$.

Scanned with CamScanner

Note:- $f(x)=x^2+1$ is irreducible over $\mathbb{Q}$ but not satisfy Einestein irredubility criterion. (i.e. E.I.C.)

Q.No. Showthat $f(x)=x^2-2$ is irreducible over $\mathbb{Q}$?

Soln $f(x)=x^2-2=x^2+0x-2$, $\exists$ exist $p=2$ s.t. $2\nmid -2$, $2\mid 0$, But $2\nmid 1$ and $2^2\nmid -2$

then $f(x)=x^2-2$ is irreducible over $\mathbb{Q}$.

C.S.I.R.

Q.No. $f(x)=x^3+312312x+123123$ is irreducible over $\mathbb{Q}$?

Soln $f(x)=x^3+0x^2+312312x+123123$

$\exists$ $p=3$ s.t. $3\mid 123123$, $3\mid 312312$, $3\mid 0$ But $3\nmid 1$ and $3^2\nmid 123123$.

then $f(x)=x^3+312312x+123123$ is irreducible over $\mathbb{Q}$.

Q.No. Note: let $0\neq a\in F$ and F is field

(i) if $f(x+a)$ is irreducible over F then $f(x)$ is irreducible over F.

(ii) if $a\cdot f(x)$ is irreducible over F then $F[x]$ is irreducible over F.

(iii) if $f(ax)$ is irreducible over F then $f(x)$ is irreducible over F.

Q.No. $f(x)=x^2+1$ is irreducible ?

Soln $f(x)=x^2+1$ — (i)

Put $x=x+1$ then

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

$=x^2+2x+2$

$\exists$ $p=2$ s.t. $2\nmid 2$, $2\mid 2$, $2\nmid 1$ also $2^2\nmid 2$.

then $f(x+1)$ is irreducible over $\mathbb{Q}$ then $f(x)$ is irreducible over $\mathbb{Q}$.

gmp

Q.No. Show that $f(x) = 1+x+x^2+x^3+\cdots x^{p-1}$ is irreducible over Q.

Soln $f(x) = 1+x+x^2+\cdots x^{p-1}$ — (i) is G.P. Series

$$f(x) = \frac{x^p-1}{x-1} \quad \text{— (ii)}$$

$0 \neq 1 \in Q$ then $f(x+1) = \frac{(x+1)^p-1}{(x+1)-1} = \frac{1}{x}\left[(x+1)^p-1\right]$

$$= \frac{1}{x}\left[{}^pC_0 + {}^pC_1 x^1 + {}^pC_2 x^2 + \cdots + 1\cdot x^p - 1\right]$$

$$= \left[p + \frac{p(p-1)}{2}x + \cdots + px^{p-2} + x^{p-1}\right] \quad \text{— (*)}$$

$p \mid p,\ p \mid \frac{p(p-1)}{2}, \cdots p \mid p$ but $p \nmid 1$ and $p^2 \nmid p$

then $f(x+1)$ is irreducible over Q.

then $f(x) = 1+x+x^2+\cdots x^{p-1}$ is irreducible over Q.

For Example :-

(i) $f(x) = 1+x+x^2$ is irreducible over Q.

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

Q.No. Show that $f(x) = 1-x+x^2-x^3+x^4-\cdots x^{p-1}$ is irreducible over Q.

Soln $0 \neq -1 \in Q$ s.t. $f(-1x) = 1+x+x^2+x^3+\cdots+x^{p-1}$ is irreducible over Q.

then $f(x) = 1-x+x^2-x^3+\cdots+x^{p-1}$ is irreducible.

H.W.

Q.No. Show that $f(x) = -1-x-x^2-x^3\cdots x^{p-1}$ is irreducible over Q?

Soln $0 \neq -1 \in Q$ s.t. [$\because -1$ is unit]

$-1f(x) = 1+x+x^2+\cdots+x^{p-1}$

is irreducible over Q.

then $f(x) = -1-x-x^2-\cdots x^{p-1}$ is irreducible over Q.

Q.g. $f(x) = x-1$ is irr. over Q.

Soln $f(x+3) = x+2$ or

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

Let $p=2$, then $p \mid 2$ but

$p \nmid 1$ and $p \nmid 2^2$

So, $f(x) = x-1$ is

irred. over Q.

Scanned with CamScanner

Q.No. If F is field and $f(x) \in F[x]$ of degree one then $f(x)$ is not irreducible over F.

Soln let $f(x) \in F[x]$ of degree one and $f(x) = g(x) \cdot h(x)$ where $g(x) \neq 0$ and $h(x) \neq 0$

$\therefore$ degree of $f(x) = 1$

Case I let degree of $g(x) = 1$ then $0 \neq h(x)$ constant of $F[x]$. then $h(x)$ is unit. ($\because$ If is field)

Case II let degree of $g(x) \neq 1$ then $g(x)$ is non zero constant of $F[x]$.

then $g(x)$ is unit in $F[x]$

From case I & II, we get either $h(x)$ is unit or $g(x)$ is unit.

then $f(x)$ is irreducible over F.

Hence single degree polynomial always irreducible over F.

For Example:- ① $f(x) = x+4$ is irreducible over Q | IR | F | $Q[x]/Q$

② $f(x) = 6x+18$ " " " "

③ $f(x) = 2x-2$ " " " "

Note: The above result need not be true if F is not field.

① $f(x) = 2x-4 = 2(x-2)$ is single degree polynomral But it is not irreducible over Z.

② $f(x) = 16x+4 = 4(4x+1)$ is single degree polynomial but it is not irreducible over $Z[i]$.

Note:- ① If $f(x) \in Z[x]$ and degree of $f(x) > 1$ then $f(x)$ is always reducible over F.

Scanned with CamScanner

(iii) if $f(x) \in \mathbb{Z}[x]$ and degree of $f(x) > 2$ then $f(x)$ is always Reducible over $\mathbb{R}$.

Q.No. if $f(x) \in \mathbb{Z}[x]$ and degree of $f(x) = 4$ then $f(x)$ is Reducible over $\mathbb{R}$.

Soln let $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ has no real roots.
then all roots of $f(x)$ are complex, but no real
say $a \pm ib, c \pm id$
then $f(x) = (x - (a+ib))(x - (a-ib))(x - (c+id))(x - (c-id))$

$$= ((x-a)-ib)((x-a)+ib)((x-c)-id)((x-c)+id)$$
$$= ((x-a)^2+b^2)((x-c)^2+d^2)$$
$$= (x^2 - 2ax + a^2+b^2)(x^2 - 2cx + c^2+d^2)$$
$$= g(x) \cdot h(x)$$

where $g(x) \in \mathbb{R}(x)$
$h(x) \in \mathbb{R}(x)$

then neither $g(x)$ is unit nor $h(x)$ is unit in $\mathbb{R}[x]$ then $f(x)$ is not irreducible over $\mathbb{R}$.

For Example: $f(x) = 2 + 7x^2 + 3x^3 + x^4$ is irreducible over $\mathbb{R}$?

Hint: degree of $f[x] = 4 > 2$ then
$f(x)$ is not irreducible over $\mathbb{R}$.

Q. $a_0 + a_1x + a_2x^2 \in \mathbb{Z}[x]$ then $f(x)$ is irreducible over $\mathbb{R}$? where $f(x)$ is non zero non unit polynomial.

Soln Need Not

for Example:- $f(x) = x^2 + x + 1$ over $\mathbb{R}$

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a} = \frac{-1 \pm \sqrt{1-4 \cdot 1 \cdot 1}}{2} = \frac{-1 + \sqrt{3}\,i}{2}$$

$$f(x) = x^2 + x + 1 = \left(x - \left(\frac{-1+\sqrt{3}\,i}{2}\right)\right)\left(x - \left(\frac{-1-\sqrt{3}\,i}{2}\right)\right)$$
$$= g(x) \cdot h(x)$$

Thus $f(x) = x^2 + x + 1$ is irreducible $\mathbb{R}$.

(ii) $f(x) = x^2 - 5 = (x-\sqrt{5})(x+\sqrt{5})$

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

where $g(x) = (x-\sqrt{5}) \in R[x]$

$h(x) = (x+\sqrt{5}) \in R[x]$

But neither $g(x)$ unit nor $h(x)$ unit in $R[x]$.

Q. $f(x) = x^2 + x + 5$ is irreducible over Z_{11}?

Soln :- let $(x^2+x+5) = (x+a)(x+b)$ — (i)

$\Rightarrow x^2+x+5 = x^2 + (a+b)x + ab$ — (ii)

from eqn (ii) we get

$a+b=1$
$ab=5$ } — (iii)

Find a and b from Z_{11} s.t.

$a+b=1$ i.e. $a+b=1$

$(a,b) = (1,0), (2,10), (3,9), (4,8), (5,7), (6,6)$

$3,9 \in Z_{11}$ s.t. $3+9=1$ and $3 \cdot 9 = 5$

then $f(x) = x^2+x+5 = (x+3)(x+9)$

$g(x)\ h(x)$

where $g(x) = x+3 \in Z_{11}[x]$

$h(x) = x+9 \in Z_{11}[x]$

But neither $g(x) = x+3$ is unit nor $h(x) = x+9$ is unit in $Z_{11}[x]$.

then $f(x) = x^2+x+5$ is not irreducible over Z_{11}.

Q. $f(x) = 2x+3$ is irreducible over Z_5?

Soln $f(x) = 2x+3$ is single degree polynomial and Z_5 is field then $f(x) = 2x+3$ is irreducible over Z_5.

Q. $f(x) = x^2+1$ is irreducible over Z_7?

Soln

Scanned with CamScanner

let $f(x) = x^2+1 = (x+a)(x+b)$ — (i)

$\Rightarrow x^2+1 = x^2+(a+b)x+ab$ — (ii)

$\Rightarrow a+b=0$ and $ab=1$

Find a and in Z_7 s.t. $a+b=0$

$(a,b) = (0,0), (1,6), (2,5), (3,4)$

$a\cdot b = 0\cdot 0 = 0,\ 1\cdot 6 = 6,\ 2\cdot 5 = 10,\ 3\cdot 4 = 12$

then no a,b exist in Z_7 s.t. $a+b=0$ and $a\cdot b=1$ then $f(x)=x^2+1$ is irreducible over Z_7.

Note:- $f(a)\neq 0$ $\forall$ $a\in Z_p$ then $f(x)$ is irreducible over Z_p (upto three degree)

(ii) If $f(a)=0$ for some $a\in Z_p$ then $f(x)$ is Reducible over Z_p (degree of $f(x)>1$)

Example:- $f(x)=x^2+x+1$ is irreducible over Z_2?

Soln $Z_2 = \{0,1\}$

$f(0) = 0+0+1 = 1$

$f(1) = 1+1+1 = 1$

$f(a)\neq 0$ $\forall$ $a\in Z_2$ then $f(x)$ is irreducible over Z_2.

(ii) $f(x) = 1+x^2$ is irreducible over Z_2?

Soln $Z_2 = \{0,1\}$

$f(0) = 1+0 = 1,\ f(1) = 1^2+1 = 2 = 0$

then $f(x) = x^2+1$ is not irreducible over Z_2.

Q. $f(x) = x^2+x+5$ over Z_{11}

Soln $Z_{11} = \{0,1,2,3,\ldots,10\}$

$f(0) = 5$ $\quad f(2) = 2^2+2+5 = 11 = 0$

$f(1) = 7$

$f(x) = x^2+x+5$ is not irreducible.

Scanned with CamScanner

Q. $f(x) = x^2+1$ is irreducible over Z_7

Soln $Z_7 = \{0,1,2,3,\cdots 6\}$

$f(0)=1$, $f(1)=2$, $f(3)=10=3$, $f(4)=17=3$, $f(5)=5$, $f(6)=2$

$f(a)\neq 0$ $\forall$ $a\in Z_7$ then $f(x)=x^2+1$ is irreducible over Z_7.

Q. $f(x)=1+x+x^2+x^3$ is irreducible over Z_3?

Soln $f(2)=1+2+4+8=0$

$\Rightarrow f(2)=0$ then $f(x)=1+x+x^2+x^3$ is not irreducible.

H.W.

Q. Show that $f(x)=x^2+1$ is irreducible over Z_3.

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

$f(0)=1$, $f(1)=2$, $f(2)=5$, $f(a)\neq 0$ $\forall$ $a\in Z_3$

Hence $f(x)=x^2+1$ is irreducible over Z_3.

Q. $f(x)=x^3+312312x+123123$ is irreducible over Z_3?

Soln $f(0)=123123=0$

Hence $f(0)=0$ then $f(x)$ is not irreducible.

C.S.I.R Imp.

Q. $f(x)=x^4+x^2+1$ is irreducible over Z_2?

Soln $f(x)=x^4+x^2+1$ and $Z_2=\{0,1\}$

$f(0)=1$, $f(1)=1$ $\quad f(a)\neq 0$ $\forall$ $a\in Z_2$

$x^4+x^2+1 = (x^2+x+1)^2 = (x^2+x+1)(x^2+x+1)$

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

where $g(x)=x^2+x+1 \in Z_2[x]$

& $h(x)=x^2+x+1 \in Z_2[x]$

But neither $g(x)$ is unit $h(x)$ is unit in $Z_2[x]$

then $f(x)=x^4+x^2+1$ is not irreducible.

Note :- $f(x)=x^2+1$ is always not irreducible over any Z_p

Scanned with CamScanner

H.W. $f(x) = x^3+1$ is irreducible over Z_5 ?

Soln:- $Z_5 = \{0, 1, 2, 3, 4\}$

$f(0) = 1$, $f(1) = 2$, $f(2) = 9 = 4$, $f(3) = 28 = 3$

$f(4) = 0$, $4 \in Z_5$

Hence $f(x) = x^3+1$ is not irreducible over Z_5.

Galois Field:- if F is finite Field of order p and $f(x) \in F[x]$ is irreducible polynomial of degree n over F then $\frac{F[x]}{\langle f(x) \rangle}$ is field of order p^n.

It is denoted by $GF(p^n)$

i.e. $GF(p^n) = \frac{Z_p[x]}{\langle f(x) \rangle} = \{a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n + f(x) / a_i \in Z_p\}$

where $f(x)$ is irreducible polynomial of degree over F.

Construction of Galois Field of order 2.

$$GF(2^1) = \frac{Z_2[x]}{\langle f(x) \rangle} = \{a_0 + \langle f(x) \rangle \mid a_0 \in Z_2\}$$

where $f(x)$ is irreducible polynomial over Z_2 of degree 1.

Soln let $f[x] = x+1 \in Z_2[x]$ is irreducible polynomial over Z_2.

$$GF(2^1) = \frac{Z_2[x]}{\langle x+1 \rangle} = \{a_0 + \langle x+1 \rangle \mid a_0 \in Z_2\}$$

$$= \{0 + \langle x+1 \rangle, 1 + \langle x+1 \rangle\} \text{ is Field of order 2.}$$

Construction of Galois Field of order 4:-

$$GF(4) = GF(2^2) = \frac{Z_2[x]}{\langle 1+x+x^2 \rangle} = \{a_0 + a_1 x + \langle 1+x+x^2 \rangle \mid a_0, a_1 \in Z_2\} \quad \text{---(1)}$$

$$= \{0 + \langle 1+x+x^2 \rangle, 1 + \langle 1+x+x^2 \rangle, x + \langle 1+x+x^2 \rangle, 1+x + \langle 1+x+x^2 \rangle\}$$

Scanned with CamScanner

Inverse of each non zero element of $\frac{Z_2[x]}{\langle 1+x+x^2\rangle}$

Now $1+x+x^2+\langle 1+x+x^2\rangle = 0+\langle 1+x+x^2\rangle$

$\Rightarrow 1+x+x^2 = 0$ —— (ii)

$1+\langle 1+x+x^2\rangle \in \frac{Z_2[x]}{\langle 1+x+x^2\rangle}$ is unity

then $\left(1+\langle 1+x+x^2\rangle\right)^{-1} = 1+\langle 1+x+x^2\rangle$

Inverse of $x+\langle 1+x+x^2\rangle$

$= \left(x+\langle 1+x+x^2\rangle\right)\left(1+x+\langle 1+x+x^2\rangle\right)$

$= x+x^2+\langle 1+x+x^2\rangle$

$\Rightarrow -1+\langle 1+x+x^2\rangle$

$= 1+\langle 1+x+x^2\rangle$

Inverse of $x+\langle 1+x+x^2\rangle = 1+\langle 1+x+x^2\rangle$

then each non zero element of $\frac{Z_2[x]}{\langle 1+x+x^2\rangle}$ has multiplicative inverse.

Construction of Galois Field of Order 8

$$GF(8) = GF(2^3) = \frac{Z_2[x]}{\langle 1+x+x^3\rangle} = \left\{ a_0+a_1x+a_2x^2+\langle 1+x+x^3\rangle \;\middle|\; a_i \in Z_2 \right\}$$

$$= \left\{ \begin{array}{l} 0+\langle 1+x+x^3\rangle,\ 1+\langle 1+x+x^3\rangle,\ x+\langle 1+x+x^3\rangle,\ 1+x+\langle 1+x+x^3\rangle, \\ x^2+\langle 1+x+x^3\rangle,\ 1+x^2+\langle 1+x+x^3\rangle,\ x+x^2+\langle 1+x+x^3\rangle, \\ 1+x+x^2+\langle 1+x+x^3\rangle \end{array} \right\}$$

($1+x^2=0 \Rightarrow x=\pm 1$
Replace x by 1

Construct Galois Field of Order 9 :-

$$GF(9) = GF(3^2) = \frac{Z_3[x]}{\langle 1+x^2\rangle} = \left\{ \begin{array}{l} a_0+a_1x+\langle 1+x^2\rangle, \\ a_0, a_1 \in Z_3 \end{array} \right.$$

$$= \left\{ \begin{array}{l} 0+\langle 1+x^2\rangle,\ 1+\langle 1+x^2\rangle,\ 2+\langle 1+x^2\rangle,\ x+\langle 1+x^2\rangle, \\ 2x+\langle 1+x^2\rangle,\ 1+x+\langle 1+x^2\rangle,\ 1+2x+\langle 1+x^2\rangle, \\ 2+x+\langle 1+x^2\rangle,\ 2+2x+\langle 1+x^2\rangle \end{array} \right.$$

Q. Show that $\frac{Z_3[x]}{\langle 1+x^2\rangle} \approx Z_3[i]$

Soln:-

$$\frac{Z_3[x]}{\langle 1+x^2\rangle} = \left\{ a_0 + a_1 x + \langle 1+x^2\rangle \,\middle|\, a_0, a_1 \in Z_3 \right\} \quad \text{---(I)}$$

Now $1+x^2+\langle 1+x^2\rangle = 0+\langle 1+x^2\rangle$

$x^2+1=0 \Rightarrow x = \pm i$ ---(II)

from eqn (I) and (II) we get

$$\frac{Z_3[x]}{\langle 1+x^2\rangle} = \left\{ a_0 + ia_1 + \langle 1+x^2\rangle \,\middle|\, a_0, a_1 \in Z_3 \right\}$$

$$= \{ 0+\langle 1+x^2\rangle, 1+\langle 1+x^2\rangle, 2+\langle 1+x^2\rangle, 1+\langle 1+x^2\rangle, 2i+\langle 1+x^2\rangle, 1+i+\langle 1+x^2\rangle, 1+2i+\langle x^2+1\rangle, 2+i+\langle 1+x^2\rangle, 2+2i+\langle 1+x^2\rangle \} \approx Z_3[i]$$

Q. Construct $\frac{Q(x)}{\langle x^2-2\rangle}$

Soln:-

$$\frac{Q[x]}{\langle x^2-2\rangle} = \left\{ a_0 + a_1 x + \langle x^2-2\rangle \,\middle|\, a_0, a_1 \in Q \right\} \quad \text{---(I)}$$

Now $x^2-2+\langle x^2-2\rangle = 0+\langle x^2-2\rangle$

$\Rightarrow x^2-2=0 \Rightarrow x = \pm\sqrt{2}$

$$= \left\{ a_0 + a_1\sqrt{2} + \langle x^2-2\rangle \,\middle|\, a_0, a_1 \in Q \right\} \approx Q[\sqrt{2}]$$

Q. Construct field $Q(\sqrt{2}, \sqrt{3})$

Soln:- $R = Q(\sqrt{2})(x)$ and $f(x) = x^2-3$ is irreducible Polynomial over $Q[\sqrt{2}]$.

$$\frac{Q(\sqrt{2})[x]}{\langle x^2-3\rangle} = \left\{ a_0 + a_1 x + \langle x^2-3\rangle \,\middle|\, a_0, a_1 \in Q[\sqrt{2}] \right\} \quad \text{---(I)}$$

Now $x^2-3+\langle x^2-3\rangle = 0+\langle x^2-3\rangle$

$\Rightarrow x^2-3=0 \Rightarrow x = \pm\sqrt{3}$ ---(II)

From (I) & (II) we get

$$\frac{Q[\sqrt{2}][x]}{\langle x^2-3\rangle} = \left\{ a_0 + a_1\sqrt{3} + \langle x^2-3\rangle \,\middle|\, a_0, a_1 \in Q[\sqrt{2}] \right\}$$

$$\approx Q[\sqrt{2}, \sqrt{3}]$$

Q. Show that $I = \langle x^2+1 \rangle$ is prime ideal but not maximal ideal in $\mathbb{Z}[x]$.

Soln $\frac{\mathbb{Z}[x]}{\langle x^2+1\rangle} = \left\{ a_0 + a_1 x + \langle x^2+1\rangle \;\middle|\; a_0, a_1 \in \mathbb{Z} \right\}$ — (i)

$x^2+1 + \langle x^2+1\rangle = 0 + \langle x^2+1\rangle$

$x^2+1 = 0 \Rightarrow x = \pm i$ — (ii)

from (i) and (ii) we get

$$\frac{\mathbb{Z}[x]}{\langle x^2+1\rangle} = \left\{ a_0 + ia_1 + \langle x^2+1\rangle \;\middle|\; a_0, a_1 \in \mathbb{Z} \right\} \approx \mathbb{Z}[i]$$

$\mathbb{Z}[i]$ is an integral domain but not field then $I = \langle x^2+1\rangle$ is prime ideal but not maximal.

Q. Show that $I = \langle x^2+1\rangle$ is maximal and prime ideal in $\mathbb{Q}[x]$.

Soln $\frac{\mathbb{Q}[x]}{\langle x^2+1\rangle} = \left\{ a_0 + a_1 x + \langle x^2+1\rangle \;\middle|\; a_0, a_1 \in \mathbb{Q} \right\} \approx \mathbb{Q}[i]$

$\mathbb{Q}[i]$ is field then $I = \langle x^2+1\rangle$ is maximal & prime ideal.

Q. $I = \langle x^3+x^2+x+1\rangle$ is maximal ideal in $\mathbb{Q}[x]$?

Soln $I = \langle x^3+x^2+x+1\rangle = (x^3+x^2+x+1)\mathbb{Q}[x]$

$$= \left\{ (x^3+x^2+x+1)\cdot g(x) \;\middle|\; g(x) \in \mathbb{Q}[x] \right\}$$

Now $\boxed{x^3+x^2+x+1 = (x^2+1)(x+1)}$ — (*)

let $(x^2+1) \in \mathbb{Q}[x]$ and $(x+1) \in \mathbb{Q}[x]$ s.t.

$(x^2+1)(x+1) = x^3+x^2+x+1 \in I$

but $x^2+1 \notin I$ and $x+1 \notin I$.

then I is not prime ideal.

$\Rightarrow \frac{\mathbb{Q}[x]}{I}$ is not integral domain

$\Rightarrow \frac{\mathbb{Q}[x]}{I}$ is not field.

$\Rightarrow$ I is not maximal

Note: If $f(x)$ is irreducible polynomial over field F then ideal generated by $f(x)$ i.e. $\langle f(x) \rangle$ is maximal ideal.

20/08/16
Saturday

Q.No. Show that $I = \langle x \rangle$ is maximal and prime ideal in $\mathbb{Q}[x] \mid \mathbb{R}[x] \mid \mathbb{C}[x] \mid \mathbb{Q}[i][x]$.

Soln:

$$\frac{\mathbb{Q}[i][x]}{\langle x \rangle} = \left\{ a_0 + \langle x \rangle \;\middle|\; a_0 \in \mathbb{Q}[i] \right\} \approx \mathbb{Q}[i]$$

$\Rightarrow \frac{\mathbb{Q}[i][x]}{\langle x \rangle} \approx \mathbb{Q}[i]$ and $\mathbb{Q}[i]$ is field then $I = \langle x \rangle$ is maximal and prime ideal of $\mathbb{Q}[i][x]$.

Part C

Q.No. Show that. $I = \langle x^2 - 2 \rangle$ is an ideal of $\mathbb{Q}[x]$ and $\langle (x^2-2) \rangle \subseteq \langle f(x) \rangle \subseteq \mathbb{Q}[x]$ then

(i) $\langle f(x) \rangle = \langle (x^2-2) \rangle$

(ii) $\langle f(x) \rangle = \mathbb{Q}[x]$

(iii) $\langle f(x) \rangle \neq \langle x^2-2 \rangle$ and $\mathbb{Q}[x]$

(iv) $\langle f(x) \subseteq \langle (x^2-2) \rangle$

Soln: $\frac{\mathbb{Q}[x]}{\langle (x^2-2) \rangle} \approx \mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}]$ is field then $I = \langle (x^2-2) \rangle$ is maximal ideal of $\mathbb{Q}[x]$.

given $\langle (x^2-2) \rangle \subseteq \langle f(x) \rangle \subseteq \mathbb{Q}[x]$

Since $\langle (x^2-2) \rangle$ is maximal then $\langle f(x) \rangle = \langle (x^2-2) \rangle$

or $\langle f(x) \rangle = \mathbb{Q}[x]$

Q.No. Show that $I = \langle x^2+2 \rangle$ is maximal ideal in $\mathbb{R}[x]$ but in $\mathbb{C}[x]$.

Soln $\frac{\mathbb{R}[x]}{\langle x^2+2\rangle} = \{a_0+a_1x+\langle x^2+2\rangle \mid a_0,a_1\in\mathbb{R}\}$,

$= \{a_0+a_1\sqrt{2}\,i+\langle x^2+2\rangle \mid a_0,a_1\in\mathbb{R}\}$

$= \{a_0+bi+\langle x^2+2\rangle \mid a_0,b\in\mathbb{R}\}$ $\quad[\because \mathbb{R}[\sqrt{2}\,i]=\mathbb{R}[i]$

$= \mathbb{R}[i]$ where $b=a_1\sqrt{2}\in\mathbb{R}$

$= \mathbb{C}$

$\mathbb{C}$ is field then $I=\langle x^2+2\rangle$ is maximal and prime ideal in $\mathbb{R}[x]$.

Next, $f(x)=x^2+2$ is not irreducible over $\mathbb{C}$ then

$\frac{\mathbb{C}[x]}{\langle x^2+2\rangle}$ is not integral domain

$\Rightarrow \frac{\mathbb{C}[x]}{\langle x^2+2\rangle}$ is not field

then $I=\langle x^2+2\rangle$ is not maximal ideal.

then $I=\langle x^2+2\rangle$ is not prime ideal in $\mathbb{C}[x]$.

$[\because f(x)=x^2+2 = (x+\sqrt{2}\,i)(x-\sqrt{2}\,i)$
Now $(x+\sqrt{2}\,i)\in\mathbb{C}[x]$
$(x-\sqrt{2}\,i)\in\mathbb{C}[x]$
S.t. $(x+\sqrt{2}\,i)(x-\sqrt{2}\,i)\in\langle x^2+2\rangle$
But $(x+\sqrt{2}\,i)\notin\langle x^2+2\rangle$
and $(x-\sqrt{2}\,i)\notin\langle x^2+2\rangle$

Q.No. Show that $I=\langle x\rangle$ is prime ideal but not maximal ideal in $\mathbb{Z}'[x]$ | $\mathbb{Z}'[i][x]$

Soln $R=\mathbb{Z}'[x]$

and $I=\langle x\rangle$ is an ideal of $\mathbb{Z}'[x]$

Now, $f(x)=x$ is irreducible over $\mathbb{Z}'$

$\frac{\mathbb{Z}'[x]}{\langle x\rangle} = \{a_0+\langle x\rangle \mid a_0\in\mathbb{Z}'\} \cong \mathbb{Z}'$

$\mathbb{Z}'$ is an integral domain but not field then $I=\langle x\rangle$ is prime ideal but not maximal.

Q.No. Show that $I=\langle 2,x\rangle$ is an ideal of $\mathbb{Z}'[x]$

Soln $\mathbb{Z}'[x] = \{a_0+a_1x+a_2x^2+\cdots+a_nx^n \mid a_i\in\mathbb{Z}'\}$

$I=\langle 2,x\rangle = \{2\cdot f(x)+x\cdot g(x) \mid f(x)\in\mathbb{Z}'[x], g(x)\in\mathbb{Z}'[x]\}$

$\langle 2\rangle = \{2\cdot f(x) \mid f(x)\in\mathbb{Z}'[x]\}$
$\langle x\rangle = \{x\cdot f(x) \mid f(x)\in\mathbb{Z}'[x]\}$

Scanned with CamScanner

(i) let $I_1(x) \in I$ then $I_1(x) = 2f_1(x) + xg_1(x)$, $f_1(x), g_1(x) \in \mathbb{Z}[x]$
and $I_2(x) \in I$ then $I_2(x) = 2f_2(x) + xg_2(x)$, $f_2(x), g_2(x) \in \mathbb{Z}[x]$
s.t. $I_1(x) - I_2(x) = 2(f_1(x) - f_2(x) + x(g_1(x) - g_2(x))$
$= 2f'(x) + xg'(x) \in I(x)$
where $f'(x) = f_1(x) - f_2(x) \in \mathbb{Z}[x]$
$g'(x) = g_1(x) - g_2(x) \in \mathbb{Z}[x]$
$\Rightarrow I_1(x) - I_2(x) \in I(x)$

(ii) let $I_1(x) \in I \Rightarrow I_1(x) = 2f(x) + xg(x)$, $f(x) \in \mathbb{Z}[x]$ and $g(x) \in \mathbb{Z}[x]$
and $\gamma(x) \in \mathbb{Z}[x]$
s.t. $I_1(x).\gamma(x) = [2.f(x) + xg(x)]\gamma(x)$
$= 2f(x)\gamma(x) + x.g(x)\gamma(x)$
$= 2f'(x) + xg'(x)$ where $f'(x) = f(x)\gamma(x) \in \mathbb{Z}[x]$, $g'(x) = g(x)\gamma(x)$
$\Rightarrow I_1(x)\gamma(x) \in I(x) = I$
then $I = I(x) = \langle 2, x \rangle$ is an ideal of $\mathbb{Z}[x]$.

Q.No. Show that $I = \langle m, x \rangle$ is an ideal of $\mathbb{Z}[x]$

Soln :- Similarly, for $I = \langle 2, x \rangle$
$= \{2.f(x) + x.g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$
$= \{2.\frac{1}{2} + x.0\} = \{1\}$
$\Rightarrow I = \mathbb{Z}[x]$.

Q.No. $I = \langle x \rangle$ is not maximal ideal of $\mathbb{Z}[x]$ then $\exists\ I'(x) \in \mathbb{Z}[x]$ s.t. $\langle x \rangle \subseteq I'(x) \subseteq \mathbb{Z}[x]$, find $I'(x)$.

$\langle x \rangle \subseteq \langle 2, x \rangle \subseteq \mathbb{Z}[x]$
But $\langle x \rangle \neq \langle 2, x \rangle$ and $\langle 2, x \rangle \neq \mathbb{Z}[x]$
$2 \in \langle 2, x \rangle$

Scanned with CamScanner

and $1 \in \mathbb{Z}[x]$ But $I \notin \langle 2, x \rangle$

Pau B.

Q. No. $\langle 2, x \rangle \subseteq I(x) \subseteq \mathbb{Z}[x]$ and $I(x) \neq \mathbb{Z}[x]$ then find $I(x) = ?$

(i) $I(x) \subseteq \langle 2, x \rangle$

(ii) $I(x) \subseteq \langle 2, x \rangle$

(ii) $\langle 2, x \rangle \subseteq I(x)$

(iii) $I(x) = \langle 2, x \rangle$

(iv) None

Soln $\mathbb{Z}[x]$ is commutative Ring with unity and $I = \langle 2, x \rangle$ is an ideal of $\mathbb{Z}[x]$

Now $\frac{\mathbb{Z}[x]}{\langle 2, x \rangle} = \left\{ f(x) + \langle 2, x \rangle \mid f(x) \in \mathbb{Z}[x] \right\}$ — (1)

$2 \cdot f(x) + x g(x) + \langle 2, x \rangle = 0 + \langle 2, x \rangle$

$\Rightarrow 2 = 0$ and $x = 0$ — (2)

From eqn (1) & (2)

$$\frac{\mathbb{Z}[x]}{\langle 2, x \rangle} = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \langle 2, x \rangle \mid a_i \in \mathbb{Z} \right\}$$

$$= \left\{ a_0 + a_1 x + \cdots + a_n x^n + \langle 2, x \rangle \mid a_i = 0 \text{ or } 1 \right\}$$

$\Rightarrow \frac{\mathbb{Z}[x]}{\langle 2, x \rangle} = \left\{ a_0 + \langle 2, x \rangle \mid a_0 = 0 \text{ or } 1 \right\}$ [$2 = 0$ in eqn (1)]

$= \left\{ 0 + \langle 2, x \rangle, 1 + \langle 2, x \rangle \right\}$

$\approx \mathbb{Z}_2$

$\mathbb{Z}_2$ is field then $I = \langle 2, x \rangle$ is maximal and prime ideal.

Note:- $\frac{\mathbb{Z}[x]}{\langle m, x \rangle} \approx \mathbb{Z}_m$, $m \geq 1$

if $m = 1$ $\frac{\mathbb{Z}[x]}{\langle 1, x \rangle} = \frac{\mathbb{Z}[x]}{\mathbb{Z}[x]} \approx \{0\}$

(iii) If $m = 0$

$\frac{\mathbb{Z}[x]}{\langle 0, x \rangle} = \frac{\mathbb{Z}[x]}{\langle x \rangle} \approx \mathbb{Z}$

Scanned with CamScanner

M is Maximal ideal iff M is Prime.

Q.No. Show that $I = \langle p, x \rangle$ is maximal and prime ideal in $Z[x]$.

Soln $\frac{Z[x]}{\langle p, x \rangle} \approx Z_p$ and Z_p is field then

$I = \langle p, x \rangle$ is maximal and prime ideal in $Z[x]$

Q.No. which of the following is an integral domain.

Soln (i) $\frac{Q[x,y]}{\langle x, y \rangle}$ (ii) $Z_6[x]$ (iii) $Z \times Z$ (iv) $M_2(Z)$

(ii) $2 \cdot 3 = 0$ in $Z_6[x]$

But $2 \neq 0$, $3 \neq 0$ then $Z_6[x]$ is not integral domain.

(iii) $(1,0) \cdot (0,1) = (0,0)$ but $(1,0) \neq (0,0)$ and $(0,1) \neq (0,0)$ then $Z \times Z$ is not integral domain.

(iv) $M_2(Z)$ is non commutative ring then $M_2(Z)$ is not integral domain.

**** **Note**

$$Z[x,y] = \{a_0 + a_1 x + a_2 y + a_3 xy + a_4 x^2 y + a_5 y^2 + \cdots + a' x^n y^n \mid a_0, a_1 \cdots a' \in Z\}$$

then $$\frac{Z[x,y]}{\langle x, y \rangle} = \{f(x,y) + \langle x, y \rangle \mid f(x,y) \in Z[x,y]\}$$

$$= \{a_0 + \langle x, y \rangle \mid a_0 \in Z\}$$

$$\approx Z$$

Q.No. Show that $I = \langle x, y \rangle$ is prime ideal but not maximal

$$\frac{Z[x,y]}{\langle x, y \rangle} \approx Z$$

Z is an integral domain but not field then $I = \langle x, y \rangle$ is prime ideal but not maximal.

Scanned with CamScanner

Q.No. $\frac{Q[x,y]}{\langle x,y\rangle} \approx Q$ and Q is field then $I = \langle x,y\rangle$ is maximal and prime ideal of $[x,y]$.

Q.No. $\frac{Z[x,y,z]}{\langle 2,x,y,z\rangle} \approx Z_2$

Soln Z_2 is field then $I = \langle 2,x,y,z\rangle$ is prime and Maximal ideal in $Z[x,y,z]$.

Q.No. $\frac{Z[x]}{\langle 2\rangle} \approx ?$

$$\frac{Z[x]}{\langle 2\rangle} = \{ f(x) + \langle 2\rangle \mid f(x) \in Z[x] \}$$

$$= \{ a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \langle 2\rangle \mid a_i \in Z \} \quad \text{---(1)}$$

Now: $2 + \langle 2\rangle = 0 + \langle 2\rangle$

$\Rightarrow 2 = 0$ ——— (11)

$$\frac{Z[x]}{\langle 2\rangle} = \{ a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \langle 2\rangle \mid a_i = 0 \text{ or } 1 \}$$

$$\approx Z_2[x]$$

Note:-

(i) $\frac{Z[x]}{\langle m\rangle} \approx Z_m[x]$

(ii) if $m=0$ then $\frac{Z[x]}{\langle 0\rangle} = \frac{Z[x]}{\{0\}} \approx Z[x]$

(iii) if $m=1$ then $\frac{Z[x]}{\langle 1\rangle} = \frac{Z[x]}{Z[x]} \approx \{0\}$

gmp

Thm: If R is commutative Ring with unity and I is an ideal of R.

then $\frac{R[x]}{I[x]} \approx \left[\frac{R}{I}\right][x]$

Scanned with CamScanner

For Example:-

(i) $\frac{\mathbb{Z}_2[x]}{\langle 2 \rangle} = \frac{\mathbb{Z}[x]}{\langle 2, x \rangle}$

$$\frac{\mathbb{Z}[x]}{\langle 2, x \rangle} = \left[\frac{\mathbb{Z}}{\langle 2 \rangle}\right][x]$$

$$= \mathbb{Z}_2[x]$$

(ii) $\frac{\mathbb{Z}[x]}{\langle m \rangle} = \frac{\mathbb{Z}[x]}{\langle m, x \rangle} \approx \frac{\mathbb{Z}}{\langle m \rangle}[x]$

$$\Rightarrow \frac{\mathbb{Z}[x]}{\langle m \rangle} \approx \mathbb{Z}_m[x]$$

Note:- $\mathbb{Z}_p[x]$ is infinite vector space over finite field and $\text{char}(\mathbb{Z}_p[x]) = p$ but $\mathbb{Z}_p[x]$ is not field.

Q.No. If F is field then $F^* = F - \{0\}$ is abelian group w.r.t. Multiplication.

(ii) If F is finite then $F^* = F - \{0\}$ is cyclic group w.r.t. Multiplication and $F^* \approx \mathbb{Z}_{o(F)-1}$.

(i) Soln Let F is field $F^* = F - \{0\}$ — ①

① let $a \in F^*$ then $0 \neq a \in F$

and $b \in F^*$ then $0 \neq b \in F$

Since F is field then $0 \neq a \cdot b \in F$

$\Rightarrow a \cdot b \in F^*$

(ii) $F^* \subseteq F$ and $(F, +, \cdot)$ is field then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\forall\ a, b, c \in F^*$

(iii) $1 \in F$ and $1 \neq 0$ then $1 \in F^*$ s.t. $a \cdot 1 = 1 \cdot a = a$, $\forall\ a \in F^*$

(iv) Let $a \in F^*$ then $0 \neq a \in F$ and F is field then $\bar{a}^1 \in F$ s.t. $a\bar{a}^1 = \bar{a}^1 a = 1$

Scanned with CamScanner

$\Rightarrow a^{-1} \neq 0$ $[\because a \neq 0$ and $a a^{-1} = 1]$

$\Rightarrow a^{-1} \in F^*$

then inverse of each element of F^* in F^*

then $(F^*, \cdot)$ is group

Now show that $(F^*, \cdot)$ is abelian

Since F is field then F is commutative ring with unity

$a \cdot b = b \cdot a$, $\forall\ a, b \in F$

Now $F^* \subseteq F$ and $x, y \in F^*$ then $x, y \in F$ s.t.

$x \cdot y = y \cdot x$ $[\because$ F is commutative$]$

then $(F^*, \cdot)$ is abelian group.

For Example:-

$F = Q$ is field then $F^* = Q^* = Q - \{0\}$ is abelian group w.r.t. Multiplication.

(ii) $F = Q[i]$ is field then $F^* = Q[i]^* = Q[i] - \{0\}$ is abelian gp. w.r.t. Multiplication.

(iii) $F = Z_{11}$ is field then $F^* = Z_{11}^* = U(11) \approx Z_{10}$ is abelian group w.r.t. Multiplication.

Q. No. (i) $F = GF(2^3)$ then $(F^*, \cdot) \approx$?

(ii) $F = GF(3^2)$ then $(F^*, \cdot) \approx$?

Soln (i) $GF(2^3)$ is finite field then

$o(GF(2^3))^* = o(GF(2^3)) - 1$

$= 8 - 1 = 7$

$\Rightarrow GF(2^3) \approx 7$

(iii) $(GF(3^2))^*$ is cyclic gp. of order

$o(GF(3^2)) - 1 = 9 - 1 = 8$

then $(GF(3^2))^* \approx Z_8$

Scanned with CamScanner

(ii) $F = GF(3^2)$ is finite field then $(GF(3^2)^*, \cdot)$ is cyclic group of order $o(GF(3^2)) - 1 = 9 - 1 = 8$

then $(GF(3^2)^*, \cdot) \approx Z_8$

C.S.I.R. 2014

Q.No. If F is field of order 9 then

(i) $(F, +) \approx Z_9$

(ii) $(F, +) \approx Z_3 \times Z_3$

(iii) $(F^*, \cdot) \approx Z_2 \times Z_4$

(iv) $(F^*, \cdot) \approx Z_8$

Soln Let F is field of order 9

$$F \simeq GF(3^2) = \frac{Z_3[x]}{\langle f(x) \rangle}$$

$$\text{char}(GF(3^2)) = \text{char}\left(\frac{Z_3[x]}{\langle f(x) \rangle}\right) = 3$$

$\Rightarrow 3 \cdot a = 0, \forall\ a \in GF(3^2)$ ——— (*)

$o(GF(3^2), +) = 9 \Big\langle \begin{matrix} Z_9 \\ Z_3 \times Z_3 \end{matrix}$

if $(GF(3^2), +) \approx Z_9$

then $(GF(3^2), +)$ has elements of order 9 But $(GF(3^2), +)$ has no elements of order 3

then $(GF(3^2), +) \approx Z_9$

$\Rightarrow (GF(3^2), +) \approx Z_3 \times Z_3$

Now $(GF(3^2)^*, \cdot) \approx Z_8$

Q.No. If F is field of order 16 then $(F, +) \approx ?$ and $(F, \cdot) \approx ?$

Soln $o(F) = 16$

$$F = GF(2^4) = \frac{Z_2[x]}{\langle f(x) \rangle}$$

Scanned with CamScanner

$(F,+)$ is always abelian group of order 16

$(F,+)$ $\begin{cases} Z_{16} \\ Z_2 \times Z_8 \\ Z_2 \times Z_2 \times Z_4 \\ Z_4 \times Z_4 \\ Z_2 \times Z_2 \times Z_2 \times Z_2 \end{cases}$ ✓

$\text{char}(GF(2^4)) = 2$ then $2 \cdot a = 0$, $\forall\, a \in GF(2^4)$

then $(GF(2^4), +)$ has no element of order > 2

then $(F, +) \approx Z_2 \times Z_2 \times Z_2 \times Z_2$

and $(F^*, \cdot) \approx Z_{O(F)-1} = Z_{15}$

Note: (I) $(GF(p^n), +) \approx \underbrace{Z_p \times Z_p \times Z_p \cdots Z_p}_{n\text{-times}}$

(II) $(GF(p^n)^*, \cdot) \approx Z_{p^n-1}$

(III) If F is finite field of order p^n then $F \approx GF(p^n)$

2016, Net Booklet
Q.No. 8

Let P is prime no. Pick each correct statement from below upto isomorphism.

(I) there are exactly two abelian groups of order p^2

(II) " " " two groups of order p^2

(III) " " " " commutative ring of order p^2

(IV) " " " one integral domain of order p^2.

Soln

$O(G) = p^2$ $\begin{cases} Z_{p^2} \\ Z_p \times Z_p \end{cases}$

$O(R) = p^2$ and R is an integral domain

$\Rightarrow$ R is field

$\Rightarrow R \approx GF(p^2) \approx \frac{Z_p[x]}{\langle f(x) \rangle}$ is field.

Scanned with CamScanner

21/04/11

Q.No. If F is field of order 8 and $x \in F$ s.t. $x^7 = 1$ But $x^k \neq 1$ if $k < 7$ then how many elements in F satisfied the given condn.

Soln let F is field of order 8

i.e. $O(F) = 8$ then $F \approx GF(2^3)$, $x^7 = 1$

~~But $x^k \neq 1$ if $k < 7$~~

$(F^*, \cdot) \approx Z_7$

# of elements of order 7 in $Z_7 = \phi(7) = 6$

then F^* has 6 element of order 7

$\Rightarrow (F, +, \cdot)$ has 6 element s.t. $x^7 = 1$ But $x^k \neq 1$ if $k < 7$

Q.No. If $O(F) = 9$ then how many elements in F s.t. $x^4 = 1$, $x \in F$.

Soln $O(F) = 9$ and F is field then $F \approx GF(9) = GF(3^2)$

then $O(GF(3^2)^*, \cdot) = 8$

$\Rightarrow GF(3^2)^* \approx Z_8$

# of elements of order 4 in $Z_8 = \phi(4) = 2$

" " " 2 " $= \phi(2) = 1$

" " " 1 " $= \phi(1) = 1$

Total No. of elements $= 2 + 1 + 1 = 4$.

Hence F has 9 elements s.t. $x^4 = 1$, $x \in F$

Note: If F is field of order p^n then # of subfield in $F = \tau(n)$

i.e. $GF(p^m)$ is subfield of $GF(p^n)$ iff $m | n$

Q. How many subfield of F when $O(F) = 16$

Soln $O(F) = 16 \Rightarrow F \approx GF(2^4)$,

Scanned with CamScanner

# of subfield = $\tau(4)=3$
Say 1, 2 and 4 are positive divisor.
$\Rightarrow$ (i) $GF(2^1)$ is subfield of $GF(2^4)$
(ii) $GF(2^2)$ " " " $GF(2^4)$
(iii) $GF(2^4)$ " " " $GF(2^4)$

Q.No. $O(F)=32$ then how many subfield in F.

Soln:- $O(F)=32=2^5$
No. of subfield $=\tau(5)=2$
Positive divisor of of 5 are 1 and 5
then $GF(2^1)$ and $GF(2^5)$ are subfield of $GF(2^5)$.

[$GF(2^5)=\frac{Z_2[x]}{\langle f(x)\rangle}$ ↓ irreducible poly.]

Subfield:- $\phi \neq S \subseteq F$ is said to be subfield of F if $(S,+,\cdot)$ is itself field.

OR
(i) $\forall\, a\in S, \forall\, b\in S \Rightarrow a-b\in S$
(ii) $\forall\, a\in S, \forall\, b\in S \Rightarrow a\cdot b\in S$

e.g: (i) $\phi\neq\mathbb{Q}\subseteq\mathbb{R}$ and $(\mathbb{Q},+,\cdot)$ is subfield of $(\mathbb{R},+,\cdot)$
(ii) $\phi\neq\mathbb{Q}[\sqrt{2},\sqrt{3}]\subseteq\mathbb{R}$ and $(\mathbb{Q}(\sqrt{2},\sqrt{3}),+,\cdot)$ is subfield of $(\mathbb{R},+,\cdot)$

Chinese Remainder thm for ideals:-

Note:- If R is commutative Ring with unity and $I=I_1, I_2, \dots I_n$ are ideal generated by I then

$$\frac{R}{\langle I\rangle}=\frac{R}{\langle I_1,I_2,\dots I_n\rangle}\approx\frac{R}{\langle I_1\rangle}\times\frac{R}{\langle I_2\rangle}\times\cdots\frac{R}{\langle I_n\rangle}$$

when $\gcd(I_i,I_j)=1$ if $i\neq j$

Scanned with CamScanner

e.g. $\frac{\mathbb{Z}}{\langle 6\rangle} = \frac{\mathbb{Z}}{\langle 2\cdot 3\rangle} \approx \frac{\mathbb{Z}}{\langle 2\rangle} \times \frac{\mathbb{Z}}{\langle 3\rangle}$

$\Rightarrow \mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$

(ii) $\frac{\mathbb{Z}}{\langle 15\rangle} = \frac{\mathbb{Z}}{\langle 3\cdot 5\rangle} \approx \frac{\mathbb{Z}}{\langle 3\rangle} \times \frac{\mathbb{Z}}{\langle 5\rangle}$

$\Rightarrow \boxed{\mathbb{Z}_{15} \approx \mathbb{Z}_3 \times \mathbb{Z}_5}$

Q.No. Find maximal and prime Ideal in $\frac{\mathbb{Q}[x]}{\langle (x^2-1)\rangle}$

Soln $f(x) = x^2 - 1 = (x+1)(x-1)$ and $\gcd((x+1),(x-1)) = 1$

then $\frac{\mathbb{Q}[x]}{\langle (x^2-1)\rangle} \approx \frac{\mathbb{Q}[x]}{\langle (x-1)\rangle} \times \frac{\mathbb{Q}[x]}{\langle (x+1)\rangle}$

$\approx \mathbb{Q} \times \mathbb{Q}$

and $\mathbb{Q} \times \mathbb{Q}$ has exactly two maximal and prime ideal then $\frac{\mathbb{Q}[x]}{\langle (x^2-1)\rangle}$ has exactly two maximal & prime ideal.

C.S.I.R. Q: $R = \frac{\mathbb{Q}[x]}{\langle (x^4-1)\rangle}$ how many maximal and prime ideal in R ?

Soln $\frac{\mathbb{Q}[x]}{\langle (x^4-1)\rangle} = \frac{\mathbb{Q}[x]}{\langle (x^2+1)(x^2-1)\rangle} \approx \frac{\mathbb{Q}[x]}{\langle (x^2-1)\rangle} \times \frac{\mathbb{Q}[x]}{\langle (x^2+1)\rangle}$

$= \frac{\mathbb{Q}[x]}{\langle x-1\rangle} \times \frac{\mathbb{Q}[x]}{\langle x+1\rangle} \times \frac{\mathbb{Q}[x]}{\langle (x^2+1)\rangle}$

$= \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}[i]$

$\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}[i]$ has three maximal and prime ideal

then $\frac{\mathbb{Q}[x]}{\langle (x^4-1)\rangle}$ " " " " "

Q.No. $\frac{\mathbb{Q}[x]}{\langle (x^5-1)\rangle} = \frac{\mathbb{Q}[x]}{\langle (x-1)(x^4+x^3+x^2+x+1)\rangle}$? How many maximal & prime ideal.

Scanned with CamScanner

Sol:-

$$\frac{Q[x]}{\langle (x^5-1)\rangle} \approx \frac{Q[x]}{\langle (x-1)\rangle} \times \frac{Q[x]}{\langle (x^4+x^3+x^2+x+1)\rangle}$$

$$\approx Q \times ff, \text{ where } ff \text{ is field}$$

$Q \times ff$ has two maximal and prime ideal.

$\Rightarrow \frac{Q[x]}{\langle (x^5-1)\rangle}$ " " " " " " .

Note:- (i) if $f(x)$ is irreducible over Z_p (for some p) and degree of $f(x)$ over Z_p is same as degree of $f(x)$ over Q then $f(x)$ is irreducible over Q.

For Example:-

(i) $f(x) = x^2+x+1$ is irreducible over Z_2 and degree of $f(x)$ over Z_2 is same as degree of $f(x)$ over Q then $f(x) = x^2+x+1$ is irreducible over Q.

(ii) $f(x) = x^3+2x+1$ is irreducible over Z_3 ($f(x) \neq 0 \ \forall \ x \in Z_3$) and degree of $f(x)$ over Z_3 is same as degree of $f(x)$ over Q then $f(x)$ is irreducible over Q.

Note:- (ii) if $f(x)$ is irreducible over Q and $f(x) \neq a \cdot g(x)$, $a \neq 1, -1$ then $f(x)$ is irreducible over Z.

For Example:-

(i) $f(x) = x^3+2x+1$ is irreducible over Q and $f(x) \neq a \cdot g(x)$ then $f(x)$ is irreducible over Z.

(ii) $f(x) = x^4+x^3+x^2+x+1$ is irreducible over Q and $f(x) \neq a \cdot g(x)$ then

...ible over Z

Scanned with CamScanner

Q.No. $f(x) = 1+(x+1)+(x+1)^2+(x+1)^3+(x+1)^4$ is irreducible over $\mathbb{Z}$?

Put $x = x-1$, -1 is the unity of $\mathbb{Z}$

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

Note: [for only $\mathbb{Z}[x]$ if $f(x) \in \mathbb{Z}[x]$ and $f(x)$ is irreducible over $\mathbb{Z}$ then $f(x)$ is irreducible over $\mathbb{Q}$.]

Principle Ideal:-

Ideal generated by single element is called principle ideal.

e.g. $I = \langle 2 \rangle = 2\mathbb{Z}$, is generated by single element 2 of $\mathbb{Z}$. then $I = \langle 2 \rangle$ is called principle ideal.

Q.No. Show that every Ideal of $\mathbb{Z}$ is principle ideal of $\mathbb{Z}$.

Soln: Ideal of $\mathbb{Z}$ generated by single element m

i.e. $I = \langle m \rangle$, $m \geq 0$

then $I = \langle m \rangle$ is principle ideal.

Q.No. How many principle ideal in $\mathbb{Q}$.

Soln If $\mathbb{Q}$ is field then $\mathbb{Q}$ has exactly two ideal

$I_1 = \{0\} = \langle 0 \rangle = \{0.a \mid a \in \mathbb{Q}\}$

$I_2 = \mathbb{Q} = \langle 1 \rangle = \{1.a \mid a \in \mathbb{Q}\}$

then $\mathbb{Q}$ has exactly two principle ideals.

Q.No. if F is field then F has exactly two Principle ideals.

Soln if F is field, then F has exactly 2 ideals.

$\{0, a \mid a \in F\}$

then F has exactly 2 Principleideal.

H.P.

Principle Ideal Domain :- (P.I.D.)

An integral domain $(R, +, \cdot)$ is said to be P.I.D. if every Ideal of R is principle Ideal.

Q.No. Show that Z is P.I.D?

Soln $(Z, +, \cdot)$ is an integral domain and every ideal of Z is Principle Ideal then $(Z, +, \cdot)$ is P.I.D.

Q.No. If F is field then F is P.I.D., but converse need not be true.

Soln if F is field then F has exactly two ideals say

$I_1 = \{0\} = \langle 0 \rangle$

$I_2 = F = \langle 1 \rangle$

which are principle ideal then F is P.I.D.

But converse need not be true

$Z[i]$ is P.I.D. but $Z[i]$ is not field

The ideal of $Z[i]$ is generated by $a \in Z[i]$

i.e. $I = \langle a \rangle$

Q.No. $R = Z[x]$ is P.I.D. ?

Soln $I = \langle 2, x \rangle$ is not Principle ideal of $Z[x]$ then $Z[x]$ is not P.I.D.

Q.No. $Z[i][x]$ is P.I.D ?

Soln No, $I = \langle 2, x \rangle$ is not principle ideal of $Z[i][x]$

Scanned with CamScanner

then $Z[i][x]$ is not P.I.D.

Note:- if R is P.I.D. then R[x] need not be P.I.D.
if R[x] is P.I.D then R is always P.I.D. (field)

Q which of the following is/are order of P.I.D?
(i) 15 (ii) 25 (iii) 35 (iv) 6

Soln we know that if R is P.I.D. then R is an integral domain and every finite integral domain is field and order of finite integral domain $= p^n$
$\Rightarrow O(PID) = p^n$

Q. $R = Q \times R$ is P.I.D?
Soln $Q \times R$ is not integral domain then
$Q \times R$ is not P.I.D.

Q. which of the following is P.I.D?
(i) $\frac{Q[x,y]}{\langle x \rangle}$ (ii) $Z[x]$ → ($I = \langle 3, x \rangle$ is not principle ideal then $Z[x]$ is not P.I.D.)
(iii) $Z \times Z$ (iv) $M_2(Z)$ → ($M_2(Z)$ is not commutative ring then it is not P.I.D.)
↓
(it is not integral domain then $Z \times Z$ is not P.I.D.)

Q.No. $R = \frac{Z_2[x]}{\langle (1+x+x^3) \rangle}$ is P.I.D.?

Soln $f(x) = (1+x+x^3)$ is irreducible over Z_2 then $\frac{Z_2[x]}{\langle (1+x+x^3) \rangle}$ is field then it is P.I.D.

Q Imp $\frac{Q[x]}{\langle x^3+1 \rangle}$ is P.I.D?

(ii) $\frac{\mathbb{R}[x]}{\langle x^5+3x^4+x^2+x+1 \rangle}$ is P.I.D?

Soln x^3+1 is not irreducible then $I = \langle x^3+1 \rangle$ is not prime ideal

$\Rightarrow \frac{Q[x]}{\langle x^3+1 \rangle}$ is not integral domain $\Rightarrow$ not P.I.D.

(ii) $x^5+3x^4+x^2+x+1$ is not irreducible over $\mathbb{R}$ ($\because$ degree >2)

So $\frac{Q[x]}{\langle x^5+3x^4+x^2+x+1 \rangle}$ is not ID

$\Rightarrow \frac{Q[x]}{\langle f(x) \rangle}$ is not PID

Q (i) $\frac{Z_1[x]}{\langle 5, x \rangle}$ is P.I.D?

(ii) $\frac{Z_1[x]}{\langle 6, x \rangle}$ is P.I.D?

Soln (i) $\frac{Z_1[x]}{\langle 5, x \rangle} \cong Z_5$ then $\frac{Z_1[x]}{\langle 5, x \rangle}$ is field $\Rightarrow \frac{Z_1[x]}{\langle 5, x \rangle}$ is P.I.D.

(ii) $\frac{Z_1[x]}{\langle 6, x \rangle} \cong Z_6$ then it is not integral domain

$\Rightarrow \frac{Z_1[x]}{\langle 6, x \rangle}$ is not P.I.D.

Q (i) $R = Q \times \{0\}$ is P.I.D ? Field

(ii) $R = Z_{11}[i]$ is P.I.D ? Field

(iii) $R = Z_{13}[i]$ is P.I.D ? Not integral domain

(iv) $R = \frac{Z_7[i][x]}{\langle x \rangle}$ is P.I.D. Field

$\frac{Z_7[i][x]}{\langle x \rangle} \cong Z_7[i]$ is field $\Rightarrow$ PID

Scanned with CamScanner

ED ⇒ PID ⇒ UFD

negation ← ¬UFD ⇒ ¬PID ⇒ ¬ED

Irreducible Element :-

Defn :- let R be an integral domain. A non zero non unit element $a \in R$, is said to be irreducible element of R if $a = b \cdot c$, $b \in R$, $c \in R$ then either b is unit or c is unit in R.

For Example :- (1) $a = 11$ is irreducible element of $\mathbb{Z}$

$11 = 11 \times 1$ or $(-11) \times (-1)$

then 1 is unit in $\mathbb{Z}$ or -1 is unit in $\mathbb{Z}$.

then $a = 11$ is irreducible element in $\mathbb{Z}$.

Similarly, $a = p$ and $a = -p$ are irreducible element of $\mathbb{Z}$.

Q. $a = 10$ is irreducible element in $\mathbb{Z}$?

Soln $a = 10 = 2 \times 5$

$= b \cdot c$ where $b = 2 \in \mathbb{Z}$, $c = 5 \in \mathbb{Z}$

But neither 2 is unit nor 5 is unit in $\mathbb{Z}$.

then $a = 10$ is not irreducible element.

Q.No. $a = 1+i$ is irreducible element of $\mathbb{Z}[i]$?

Soln let $1+i = (a+ib)(c+id)$, $a, b, c, d \in \mathbb{Z}$ ——— ①

Taking conjugate on both side

$1-i = (a-ib)(c-id)$ ——— ②

① × ② then we get

$(1+i)(1-i) = (a+ib)(c+id) \times (a-ib)(c-id)$

$2 = (a^2+b^2)(c^2+d^2)$ ——— ③

Scanned with CamScanner

Case 1 if $a^2+b^2=2$ then $c^2+d^2=1 \Rightarrow (c+id)(c-id)=1$

$\Rightarrow (c+id)$ is unit in $Z[i]$

(its means c+id has Multiplicative inverse

Case 2 if $c^2+d^2=2$ then $a^2+b^2=1$

$\Rightarrow (a+ib)$ is unit in $Z[i]$

From case ① and ②

either $c+id$ is unit or $a+ib$ is unit

then $\alpha = 1+i$ is irreducible element of $Z[i]$

H.W.

Q Show that $\alpha = 1-i$ is irreducible element of $Z[i]$

Soln $1-i = (a+ib)(c+id) \Rightarrow 1+1 = (a^2+b^2)(c^2+d^2)$

$\Rightarrow 1+i = (a-ib)(c-id) \Rightarrow 2 = (a^2+b^2)(c^2+d^2)$

Case 1 :- if $a^2+b^2=2$, $c^2+d^2=1 \Rightarrow (c+id)(c-id)=1$

$\Rightarrow c+id$ is unit in $Z[i]$

Case 2 if $c^2+d^2=2$, then $a^2+b^2=1$

$\Rightarrow a+ib$ is unit in $Z[i]$

From case ① and ②, either $c+id$ unit or $a+ib$

So, $1-i$ is irred. element of $Z[i]$

H.P.

Q.No. $\alpha=2$ is irreducible element of $Z[i]$?

Soln $2 = (1+i)(1-i)$

But neither $(1+i)$ is unit nor $(1-i)$ is unit in $Z[i]$

Q.No. $\alpha=5$ is irreducible element of $Z[i]$?

Scanned with CamScanner

Soln $5 = (2+i)(2-i)$. But $(2+i)$ & $(2-i)$ both are not unit in $Z[i]$
then 5 is not irreducible element in $Z[i]$

Q.No. $\alpha = 3$ is irreducible element in $Z[i]$?

Soln $3 = (a+ib)(c+id)$ — ①

Taking conjugate

$\Rightarrow 3 = (a-ib)(c-id)$ — ②

① × ② we get

$9 = (a^2+b^2)(c^2+d^2)$ — ③

Case I if $a^2+b^2=9$ then $c+id$ is unit
Case II if $c^2+d^2=9$ " $a+ib$ " "
Case III if $a^2+b^2=3$ then $c^2+d^2=3$

Since $a,b,c,d \in Z$ then $a^2+b^2=3$ and $c^2+d^2=3$ is not possible.

then case (III) is not possible.

From case ① and ②, we get

either $a+ib$ is unit or $c+id$ is unit.

then $\alpha=3$ is irreducible element of $Z[i]$

Note:- (i) if $x = a+ib$, $a\neq 0, b\neq 0$ and $a^2+b^2=p$ then
$x = a+ib$ is irreducible

(ii) if $x = a+ib$, either $a=0$ or $b=0$ and $|x|=p$ with $4 \mid p-3$
then x is irreducible element of $Z[i]$

e.g. $\alpha = 3+i \in Z[i]$ s.t. $3^2+1^2=10$ is not prime then
$\alpha = 3+i$ is not irreducible

(ii) $\alpha = 3i \in Z[i]$
then $|\alpha| = |3i| = 3$ and $4 \mid 3-3$ then
$\alpha = 3i$ is irreducible

(iii) $\alpha = 7 \in Z[i]$ and $|\alpha| = 7$ and $4 \mid 7-3$ then
$\alpha = 7$ is irreducible.

Scanned with CamScanner

C.S.I.R

Q.No. $\alpha = 3+\sqrt{-5}$ is irreducible element in $Z[\sqrt{-5}]$?

Soln $Z[\sqrt{-5}] = \{a+\sqrt{-5}b \mid a,b \in Z\}$
$= \{a+\sqrt{5}ib \mid a,b \in Z\}$

let $\alpha = (3+\sqrt{5}i) = (a+\sqrt{5}ib)(c+\sqrt{5}id)$ — (I)

$\Rightarrow (3-\sqrt{5}i) = (a-\sqrt{5}ib)(c-\sqrt{5}id)$ — (II)

$14 = (a^2+5b^2)(c^2+5d^2)$ — (III)

Case I If $a^2+5b^2=14$ then $(c+\sqrt{5}id)$ is unit

Case II If $c^2+5d^2 = 14$ then $(a+\sqrt{5}ib)$ is unit

case III If $a^2+5b^2=7$ then $c^2+5d^2=2$ is not possible

Then $\alpha = 3+\sqrt{-5}$ is irreducible element in $Z[\sqrt{-5}]$
(from case I & II)

Prime Element

Let R be an integral domain. A non zero non unit element $p \in R$ if $p \mid a\cdot b$ then $p \mid a$ or $p \mid b$. where $a,b \in R$

e.g. (i) $a=15$ is not prime element in Z ?

Soln $15 \mid 3\cdot 5$ But $15 \nmid 3$ & $15 \nmid 5$
Then $a=15$ is not prime element in Z.

Q.No. Show that p and $-p$ are prime ~~ideal~~ element of Z.

Soln let $-p \mid a\cdot b$ — (I)

If $-p \mid a$ then done

if $-p \nmid a$ then $\gcd(-p, a)=1$ then $-p \mid b$

Similarly $\alpha = p$ is also prime element of Z

Hence $\alpha = \pm 2, \pm 3, \pm 5$ — are prime elements.

Q. $\alpha = 2$ is prime element of $Z[i]$?

Soln

Soln $2 \mid (1+i)(1-i)$ But $2 \times (1+i)$ & $2 \times (1-i)$

then $a = 2$ is not prime element.

H.W.

Q.No. $a = 5$ is prime element of $Z[i]$?

Ans No.

$a = 5$ is not prime element of $Z[i]$.

$\therefore a = 5$, then $5 \mid (2+i)(2-i)$ but $5 \times (2+i)$ and $5 \times (2-i)$

then $a = 5$ is not prime element.

Q.No. $a = 3+\sqrt{-5}$ is prime element in $Z[\sqrt{-5}]$?

Soln $(3+\sqrt{-5}) \mid 14$

$\Rightarrow (3+\sqrt{-5}) \mid 2 \times 7$ But $(3+\sqrt{-5}) \times 2$ and $(3+\sqrt{-5}) \times 7$ then

$3+\sqrt{-5}$ is not prime element.

Q.No. Show that every prime element of R is an irreducible element of R. But converse need not be true.

Soln :- let R be an integral domain and $a \in R$ is any prime element of R

Now, let $a = b \cdot c$ —— (1)

$\Rightarrow a \mid b \cdot c$

$\Rightarrow a \mid b$ or $a \mid c$

because a is prime element of R.

if $a \mid b$ then $\exists\ x \in R$ s.t. $b = ax$

$\Rightarrow b = bcx$ (from (1))

$\Rightarrow b(1-cx) = 0$

$\Rightarrow b = 0$ or $1-cx = 0$ ($\because$ R is an integral domain)

(unity)

$b=0$ is not possible because $a=b\cdot c=0\cdot c=0$

$\Rightarrow a=0$ but a is prime ideal of R

then $a\neq 0$

$\Rightarrow 1-cx=0$

$\Rightarrow cx=1$

$\Rightarrow c$ is unit

Similarly if $a|c$ then b is unit

Hence either b is unit or e is unit in R.

then a is irreducible element of R.

But converse need not be true.

$\alpha=3+\sqrt{5}i$ is irreducible element of $Z[\sqrt{-5}]$ but not prime element of $Z[\sqrt{-5}]$

only for $Z[i]$

Note

(i) If $x=a+ib$, $a\neq 0$, $b\neq 0$ and $a^2+b^2=p$ then x is prime element of $Z[i]$.

(ii) if $x=a+ib$, either $a=0$ or $b=0$ and $|x|=p$ with $4|p-3$ then x is prime.

For Example:- (i) $\alpha=3+i$ is prime element of $Z[i]$?

Hint $(3+i)\,|\,(2+i)(1-i)$

But $(3+i)\times(2+i)$ and $(3+i)\times(1-i)$

Associate:-

Let R be an integral domain.

An element a is associate to b if $\exists$ unit $u\in R$ s.t.

$a=ub$

Note:- If a is associate to b then b is also associate to b.

Scanned with CamScanner

Hint & Note:- $a = ub \Rightarrow b = u^{-1}a$ If u is unit then u^{-1} is also unit in R.

e.g. (i) 1 and -1 are associate in $\mathbb{Z}$

$1 = (-1)(-1)$

$a = ub$

where $u = (-1)$ is unit in $\mathbb{Z}$

(ii) 1 and i are associate in $\mathbb{Z}[i]$

$1 = (-i)(i)$

$a = ub$

where $u = -i$ is unit in $\mathbb{Z}[i]$

H.W.

Q: 2 and i are associate in $\mathbb{Z}[i]$?

Ans No, because $a = ub$, whose u is unit in $\mathbb{Z}[0]$

$u = \{1, -1, i, -i\}$

$\Rightarrow 2 \neq u \cdot i$ Hence 2 and i not associate.

Q: $\alpha = 2+3i$ is associate to $\beta = 2i-3$ in $\mathbb{Z}[i]$?

Soln $2i-3 = i(2+3i)$ where i is unit in $\mathbb{Z}[i]$, then $2+3i$ & $2i-3$ are associate

Q: Show that 4 and 1 are associate in $\mathbb{Q}|\mathbb{R}| \not\subset |\mathbb{Q}[i]| \mathbb{Q}[\sqrt{2}]$

Soln $4 = 1 \cdot u$ i.e. $a = ub$

where $u = 1$ is unit in $\mathbb{Q}|\mathbb{R}| \not\subset |\mathbb{Q}[i]| \mathbb{Q}[\sqrt{2}]$

So, 1 & 4 are associate.

Scanned with CamScanner

Euclidean Domain (E.D.)

(defⁿ) An integral domain $(D, +, \cdot)$ is said to be E.D. if a function "d" from non zero element of D to non negative integer s.t.

① $d(a) \le d(a \cdot b)$ $\forall\ 0 \neq a \in D$, $\forall\ 0 \neq b \in D$

② let $a \in D$, $0 \neq b \in D$ then $\exists$ some q and r in D s.t. $a = bq + r$, where $r = 0$ or $d(r) < d(b)$

Q: Show that $\mathbb{Z}$ is an Euclidean domain.

Soln let $D = (\mathbb{Z}, +, \cdot)$

define $d(a) = |a|$, $\forall\ 0 \neq a \in \mathbb{Z}$

| ED ⇒ PID ⇒ UFD
| ¬UFD ⇒ ¬PID ⇒ ¬ED
| Unit factorisation domain

① let $0 \neq a \in \mathbb{Z}$, $0 \neq b \in \mathbb{Z}$

s.t. $d(a) = |a| \le |a \cdot b| = d(a \cdot b)$

$\Rightarrow d(a) \le d(a \cdot b)$

let $a \in \mathbb{Z}$, $0 \neq b \in \mathbb{Z}$ then $\exists!$ q and r in $\mathbb{Z}$ s.t.

$a = bq + r$, $r = 0$ or $r < |b|$ (E.A.)

$\Rightarrow r = 0$ or $|r| < |b|$

$\Rightarrow r = 0$ or $d(r) < d(b)$

then $\mathbb{Z}$ is ED

$\Rightarrow \mathbb{Z}$ is P.I.D

$\Rightarrow \mathbb{Z}$ is UFD

Q: if F is field then F is an E.D.

Soln let F is field and $d(a) = 1$, $\forall\ 0 \neq a \in F$

① let $0 \neq a \in F$ and $0 \neq b \in F$ s.t. $d(a) = 1$ —①

Scanned with CamScanner

Now $0 \neq a \in R$, $0 \neq b \in R$ and R is Field then

$0 \neq a \cdot b \in R$

$\Rightarrow d(a \cdot b) = 1$ —— (ii)

From (i) & (ii), we get

$d(a) \leq d(a \cdot b)$

(ii) let $a \in R$ and $0 \neq b \in R$

Now $a = a \cdot 1 + 0$

$= ab^{-1}b + 0$

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

$a = bq + r$ where $q = ab^{-1} \in R$ & $r = 0 \in R$

then R is E.D. $\Rightarrow$ i.e. $\mathbb{Q}$ | $\mathbb{R}$ | $\mathbb{C}$ | $\mathbb{Q}[i]$ | $\frac{\mathbb{Z}_3[x]}{\langle 1+2x+x^3 \rangle}$ | $\mathbb{Q}[\sqrt{2}]$ | $\mathbb{Z}_{11}[i]$ etc

are E.D. $\Rightarrow$ P.I.D $\Rightarrow$ UFD.

Field $\Rightarrow$ E.D. $\Rightarrow$ P.I.D $\Rightarrow$ UFD
$\neg$UFD $\Rightarrow$ $\neg$PID $\Rightarrow$ $\neg$E.D. $\Rightarrow$ $\neg$Field

Q: $D = \frac{\mathbb{Z}[i]}{\langle 3+i \rangle}$ is E.D ?

Soln $\frac{\mathbb{Z}[i]}{\langle 3+i \rangle} \approx \mathbb{Z}_{10}$, $\mathbb{Z}_{10}$ is not integral domain then $\frac{\mathbb{Z}[i]}{\langle 3+i \rangle}$ is not E.D.

$\Rightarrow \frac{\mathbb{Z}[i]}{\langle 3+i \rangle}$ " " P.I.D.

$\Rightarrow$ " " " UFD

Q: $R = \frac{GF(3^2)[x]}{\langle x \rangle}$ is E.D.? yes $\left(R = \frac{GF(3^2)[x]}{\langle x \rangle} \text{ is field.} \right)$

(ii) $R = \mathbb{Z} \times \mathbb{Z}$ is E.D ? No ($\because$ $\mathbb{Z} \times \mathbb{Z}$ is not field)

" " " integral domain

(iii) $R = \mathbb{Z}[x]$ is E.D ? → No ($\because$ $\mathbb{Z}[x]$ is not P.I.D.)

(iv) $R = \mathbb{Z}[i][x]$ is E.D ? → No ($\because$ $\mathbb{Z}[i][x]$ is not P.I.D.

" " " E.D.

Scanned with CamScanner

Q.No. If F is field then $F[x]$ is E.D.

Soln let F is field and $F[x] = \{a_0 + a_1x + \cdots a_nx^n \mid a_i \in F\}$

let $0 \neq f(x) \in F[x]$ s.t. $d(f(x)) =$ degree of $f(x)$

(i) let $0 \neq f(x) \in F[x]$ and $0 \neq g(x) \in F[x]$

s.t. $d(f(x)) =$ degree of $f(x) \leq$ degree of $f(x)$ + degree of $g(x)$

$= \text{degree}\ (f(x).g(x))$

$= d(f(x).g(x))$

$\Rightarrow d(f(x)) \leq d(f(x).g(x))$

(ii) let $f(x) \in F[x]$ and $0 \neq g(x) \in F[x]$

then $\exists$ polynomial $q(x)$ and $r(x)$ in $F[x]$ s.t.

$f(x) = g(x).q(x) + r(x)$, $r(x) = 0$ (↓ remainder)

or degree $r(x) \leq$ degree $g(x)$

$\Rightarrow r(x) = 0$ or $d(r(x)) < d(g(x))$

then $F[x]$ is ED

$\Rightarrow$ " " PID

$\Rightarrow$ " " UFD

For Example:-

(i) Q is field then $Q[x]$ is ED, PID and UFD

(ii) $Q[i]$ is " " $Q[i][x]$ " " " " .

(iii) $F = Z_p \mid Z_3[i] \mid Q \times \{0\} \mid \frac{Z[i]}{\langle 2+i \rangle}$ is field

then $F[x] = Z_p[x] \mid Z_3[i][x] \mid Q \times \{0\}[x] \mid \frac{Z[i][x]}{\langle 2+i \rangle}$ is E.D, PID, UFD.

Q.No. Show that $Z[i]$ is E.D.

Soln $Z[i] = \{a+ib \mid a \in Z, b \in Z\}$

s.t. $d(x) = a^2 + b^2$, for $x = a+ib \in Z[i]$

Scanned with CamScanner

(i) let $0 \neq x = a+ib \in \mathbb{Z}[i]$ and $0 \neq y = c+id \in \mathbb{Z}[i]$

s.t. $d(x) = a^2+b^2$ — (i)

Now $x \cdot y = (a+ib)(c+id)$

$= (ac-bd)+i(bc+ad)$

$\Rightarrow d(x \cdot y) = (ac-bd)^2 + (bc+ad)^2$

$= a^2c^2+b^2d^2-2abcd + b^2c^2+a^2d^2+2abcd$

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

$= (a^2+b^2)(c^2+d^2)$ —— (ii)

From (i) $d(x) = (a^2+b^2) \leq (a^2+b^2)(c^2+d^2)$

$= d(x \cdot y)$ (from (ii))

$\Rightarrow d(x) \leq d(x \cdot y)$

(ii) let $x = a+ib \in \mathbb{Z}[i]$ & $0 \neq y = c+id \in \mathbb{Z}[i]$

$$\frac{x}{y} = \frac{(a+ib)(c-id)}{(c^2+d^2)}$$

$= yq + r$ where $r = 0$ or $d(r) < d(y)$

Then $\mathbb{Z}[i]$ is E.D $\Rightarrow$ P.I.D $\Rightarrow$ UFD

Q. $\mathbb{Z}[\sqrt{-2}] = \{a+\sqrt{2}ib \mid a,b \in \mathbb{Z}\}$ is E.D., PID and UFD

Soln **Hint** $\mathbb{Z}[\sqrt{-2}] = \{a+\sqrt{2}ib \mid a,b \in \mathbb{Z}\}$

s.t. $d(x) = a^2+2b^2$, where $0 \neq x = a+\sqrt{2}ib \in \mathbb{Z}[\sqrt{-2}]$

Q.No. $\mathbb{Z}[i][x]$ is E.D ?

$\mathbb{Z}[i][x]$ is not PID

$\Rightarrow$ " " " E.D.

H.P.

Scanned with CamScanner

Unique factorization Domain (UFD)

An Integral domain $(D, +, \cdot)$ is said to be unique factorisation domain if

(i) Each non zero non unit element of D can be written as product of irreducible element of D, and

(ii) The factorisation of element is unique upto associate.

i.e. let a is non zero non unit element of D

$a = a_1 a_2 \cdots a_r$, a_i is irreducible element of D

& $a = b_1 b_2 \cdots b_s$, b_j " " " "

then $r = s$ and a_i is associate to only one of b_j

Q.No. Show that factorisation of 6 is unique upto associate in $\mathbb{Z}$.

Soln

$6 = 2 \times 3$ — (i)

also $-2 \times -3 = 6 = 2 \times 3$ — (ii)

↓ we can written as

-2 is associate to 2

and -3 is associate to 3

then factorisation of 6 is unique upto associate in $\mathbb{Z}$.

Q.No. Show that factorisation of 30 is unique upto associate in $\mathbb{Z}$.

$-2 \times -3 \times 5 = 30 = 2 \times 3 \times 5 = -2 \times 3 \times -5 = 2 \times -3 \times -5$

-2 is associate to 2

-3 " " " 3

-5 " " " 5

then factorisation of 30 is unique upto associate in $\mathbb{Z}$.

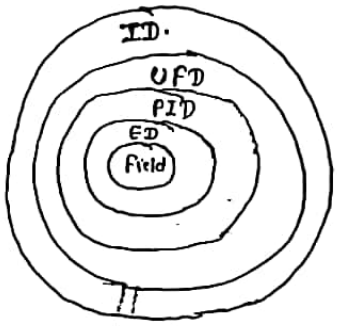
Scanned with CamScanner

Q. Show that $\mathbb{Z}$ is UFD?

Soln $\mathbb{Z}$ is ED $\Rightarrow$ PID $\Rightarrow$ UFD

$F \Rightarrow E.D \Rightarrow PID \Rightarrow UFD \Rightarrow I.D.$
$\neg I.D \Rightarrow \neg UFD \Rightarrow \neg PID \Rightarrow \neg ED \Rightarrow F$

Q. Show that $\mathbb{R} = Q[\mathbb{R}[\phi[\mathbb{Z}_p[\frac{\mathbb{Z}_3[x]}{\langle 1+x^2\rangle}$ is UFD.



Soln F is field then
F is E.D $\Rightarrow$ P.I.D $\Rightarrow$ UFD

H.W.
Q.No. Show that $\mathbb{Z}[i]$ is UFD

Soln $\mathbb{Z}[i]$ is ED $\Rightarrow$ $\mathbb{Z}[i]$ is PID
$\Rightarrow$ $\mathbb{Z}[i]$ is UFD

Q.No. Show that if F is field then F[x] is UFD

Soln If F is field then F[x] is E.D.
$\Rightarrow$ " " P.I.D
$\Rightarrow$ " " U.F.D.

Note:- If F[x] is E.D. then F is E.D. (field)

Q.No. $Q[x,y]$ is E.D?

Soln $I = \langle x, y\rangle$ is not principle ideal
then $Q[x,y]$ is not P.I.D.
$Q[x,y]$ is not ED.

H.W.
Q.No. $\mathbb{R}[x,y,z]$ is E.D?

Soln $I = \langle x, y, z\rangle$ is not principle ideal
then $\mathbb{R}[x,y,z]$ is not E.D.

Scanned with CamScanner

Q.No. $\mathbb{Z}[\sqrt{-3}]$ is ED?

Soln $4 \in \mathbb{Z}[\sqrt{-3}]$

s.t. $2 \times 2 = 4 = (1+\sqrt{3}i)(1-\sqrt{3}i)$

But 2 is not associate to $(1+\sqrt{3}i)$ & $(1-\sqrt{3}i)$

then factorisation of 4 is not unique upto associate in $\mathbb{Z}[\sqrt{-3}]$.

then $\mathbb{Z}[\sqrt{-3}]$ is not UFD

$\Rightarrow$ " " " PID

$\Rightarrow$ " " " E.D.

Q. $\mathbb{Z}[\sqrt{-5}]$ is E.D?

Soln $21 = 7 \times 3$

$(4+\sqrt{5}i)(4-5i) = 21 = 7 \times 3$

But $(4+\sqrt{5}i)$ is not associate to 7 & 3

then factorisation of 21 is not unique upto associate.

Q. $\mathbb{Z}[\sqrt{-11}]$ is E.D?

Soln $(2+\sqrt{11}i)(2-\sqrt{11}i) = 15 = 3 \times 5$, But $(2+\sqrt{11}i)$ not associate to 3 & 5

then factorisation of 15 is not unique upto associate.

then $\mathbb{Z}[\sqrt{-11}]$ is not E.D

$\Rightarrow$ " " " P.I.D

$\Rightarrow$ " " U.F.D.

Note (i) $\mathbb{Z}[\sqrt{-d}]$ is not UFD if $d > 2$

(ii) $\mathbb{Z}[\sqrt{-d}]$ is ED if $d = 1, 2$

H.W. Thm:- If R is UFD then R[x] is UFD.

Soln If R is UFD
⇒ R is ED ⇒ R is field
⇒ R[x] is UFD.
H.P.

Extension field:- If F is subfield of K then K is called extension field of F.

e.g. (i) $\mathbb{Q} \subseteq \mathbb{R}$ or $\mathbb{Q}$ is subfield of $\mathbb{R}$ then $\mathbb{R}$ is called extension field of $\mathbb{Q}$.

(ii) $\mathbb{Q}$ is subfield of $\mathbb{Q}[i]$ then $\mathbb{Q}[i]$ is an extension field of $\mathbb{Q}$.

e.g. (i) $\mathbb{Q}[\sqrt{2}]$ is subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ then $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is an extension field of $\mathbb{Q}[\sqrt{2}]$.

Q. [redacted] is an extension field of $\mathbb{Q}[i]$
$\mathbb{R}$

Soln $\mathbb{Q}[i] \not\subseteq \mathbb{R}$ then $\mathbb{R}$ is not extension field of $\mathbb{Q}[i]$

Q. $\mathbb{C}$ is an extension field of $\mathbb{Q}[i]$?

Soln $\mathbb{Q}[i] \subseteq \mathbb{C}$ and $\mathbb{C}$ is field then $\mathbb{C}$ is an extension field of $\mathbb{Q}[i]$.

Scanned with CamScanner

Q. $\dim(\phi(Q[i])) = ?$

$\dim(\phi[Q[i]]) = \infty$

Degree of Extension :-

If K is Extension field of F then the dimension of vector space K over F is called degree of extension. It is denoted by $[K:F] = \dim K(F) = \dim_F(K)$

e.g.

Q.No. Find degree of extension of $Q[\sqrt{2}, \sqrt{3}]$ over Q.

i.e. $[Q[\sqrt{2},\sqrt{3}] : Q] = ?$

Soln :-

$$Q[\sqrt{2},\sqrt{3}] = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{2}\sqrt{3} \mid a_0, a_1, a_2, a_3 \in Q\}$$

Put $a_0 = 1$, $a_1 = a_2 = a_3 = 0$ then 1

Put $a_0 = 0$, $a_1 = 1$, $a_2 = a_3 = 0$

then $\sqrt{2}$

Put $a_0 = 0$, $a_1 = a_3 = 0$, $a_2 = 1$ then $\sqrt{3}$

Put $a_0 = a_1 = a_2 = 0$, $a_3 = 1$ then $\sqrt{2}\sqrt{3}$

then $\beta = \{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$

$= \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

$\sigma(\beta) = 4$ then $\dim(Q(\sqrt{2},\sqrt{3}) : Q) = 4$

$\downarrow$ dim.

then degree of extension $= 4$

Q. Find degree of extension of $Q[\sqrt{3}]$ over Q ?

Scanned with CamScanner

Soln: $\mathbb{Q}[\sqrt{3}] = \{ a_0 + a_1\sqrt{3} \mid a_0, a_1 \in \mathbb{Q} \}$

Put $a_0 = 1$, $a_1 = 0$ then 1

Put $a_0 = 0$, $a_1 = 1$ then $\sqrt{3}$

$\beta = \{ 1, \sqrt{3} \}$

$o(\beta) = 2$, then $\dim [\mathbb{Q}\sqrt{3}] = 2 \Rightarrow \dim \left(\mathbb{Q}(\sqrt{3}) : \mathbb{Q} \right) = 2$

then degree of extension = 2

Q: Find degree of extension of $\mathbb{C}(\mathbb{C})$ and $\mathbb{C}(\mathbb{R})$

Soln: $\mathbb{C} = \{ x \mid x \in \mathbb{C} \}$

$\beta = \{1\} \Rightarrow o(\beta) = 1.$

(Basis)

then degree of extension $\mathbb{C}(\mathbb{C}) = 1$

$\mathbb{C} = \{ a + ib \mid a, b \in \mathbb{R} \}$ ($\because$ $a=0, b=i$ then i; $a=1, b=0$ " 1)

$\beta = \{1, i\}$

$\Rightarrow o(\beta) = 2$ then $\dim(\mathbb{C}(\mathbb{R})) = 2$

$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2(\mathbb{R}) = \{ (a,b) \mid a, b \in \mathbb{R} \}$

$\beta = \{ (1,0), (0,1) \}$

then $\dim(\mathbb{R}^2(\mathbb{R})) = 2$

Q.No. $\mathbb{C}^2(\mathbb{C}) = \{ (a,b) \mid a \in \mathbb{C}, b \in \mathbb{C} \}$

$\Rightarrow \beta = \{ (1,0), (0,1) \}$

then $\dim(\mathbb{C}^2(\mathbb{C})) = 2$

Q. $\dim(\mathbb{C}^2(\mathbb{R}))$

Soln: $\mathbb{C}(\mathbb{R}) = \{ x \mid x \in \mathbb{C} \} = \{ a + ib \mid a, b \in \mathbb{R} \}$

$\beta = \{1, i\}$

Scanned with CamScanner

Now $\mathbb{C}^2(\mathbb{R}) = \{(a,b) \mid a,b \in \mathbb{R}\}$

$\beta^1 = \{(1,0), (0,1)\}$

$\mathbb{C}^2 = \mathbb{C} \times \mathbb{C} = \mathbb{C}(\mathbb{R}) \times \mathbb{C}(\mathbb{R})$

$o(\beta^1) = 4$

Then $\boxed{\dim(\mathbb{C}^2(\mathbb{R})) = 4}$

H.W.

Q.No. $\dim(\mathbb{C}^3(\mathbb{R})) = ?$

$\beta = \mathbb{C}^3(\mathbb{R}) = \{(a,b) \mid a,b \in \mathbb{R}\}$

$= \{(1,0,0), (i,0,0), (0,1,0), (0,i,0), (0,0,1), (0,0,i)\}$

$o(\beta) = 6$

Q.No. $[Q[\sqrt{2}, \sqrt{3}, \sqrt{5}] : Q[\sqrt{3}]] = ?$

Note:- If L is extension field of K and K is extension field of F then L is extension field of F.

$[L:K][K:F] = [L:F]$

$[Q(\sqrt{2}, \sqrt{3}, \sqrt{5}) : Q] = 2 \times 2 \times 2 = 8$

& $[Q[\sqrt{3}] : Q] = 2$

Now $[Q[\sqrt{2}, \sqrt{3}, \sqrt{5}] : Q] = Q[\sqrt{2}, \sqrt{3}, \sqrt{5}] : Q[\sqrt{3}]] \cdot [Q[\sqrt{3}] : Q]$

$8 = a \times 2$

$a = \frac{8}{2} = 4$

then $Q[(\sqrt{2}, \sqrt{3}, \sqrt{5}) : Q[\sqrt{3}]] = 4$

Scanned with CamScanner

Q.No. $[Q[2]^{1/7} : Q] = ?$

Soln $\dim[Q[2]^{1/7} / Q] = 7$

the degree of extension of $Q(2)^{1/7}$ over $Q = 7$

Q.No. $[Q(2)^{1/3}(3)^{1/5}(7)^{1/8} : Q] = ?$

$= 3 \times 5 \times 8$

$= 120$

Q.No. Find degree of extension of $[Q(2)^{1/3}, (3)^{1/5}, (7)^{1/8} : Q(7)^{1/8}]$

Soln $[Q(2)^{1/3}, (3)^{1/5}, (7)^{1/8} : Q] = [Q(2)^{1/3}(3)^{1/5}, (7)^{1/8} : Q[7]^{1/8}]$
$[Q(7)^{1/8} . Q]$

$120 = a \times 8$

$a = \frac{120}{8} = 15$

Note:-

$[Q(a_1)^{1/n_1}(a_2)^{1/n_2} \cdots (a_k)^{1/n_k} : Q] = n_1 \cdot n_2 \cdot n_3 \cdots n_k$

where $a_i \neq a_j \neq 1$

Q. $[Q(2)^{1/2}, (2)^{1/4} : Q] ? = 4$

C.S.I.R. $[Q(2)^{1/2}, (2)^{1/3} : Q[2]^{1/2}] = ?$

Soln $[Q(2)^{1/2}, (2)^{1/3} : Q(2)^{1/2}]$

let $Q(2)^{1/2} = F$

then $[F(2)^{1/3} : F] = 3$

$\Rightarrow [Q(2)^{1/2}, (2)^{1/3} : Q[2]^{1/2}] = 3$

Q.No. $[Q(2)^{1/2}, (2)^{1/4}, (2)^{1/8}, Q] = ?$

$= LCM(2\ 4\ 8) = 8$

Scanned with CamScanner

Note:- $\left[\left(\mathbb{Q}(a)^{1/n_1}(a)^{1/n_2}\cdots-(a)^{1/n_k}\right):\mathbb{Q}\right]=LCM(n_1,n_2\cdots n_k)$

H.W:

Q.No. $\left[\mathbb{Q}(3)^{1/3},(3)^{1/7},(3)^{1/6}:\mathbb{Q}\right]=?$

Soln $LCM(3\ 7\ 6)=42$

#Algebraic Elements:-

Let K is an extension field of F. An element $a\in K$ is said to be algebraic element over F if $\exists$ non zero polynomial $f(x)\in F[x]$ s.t. $f(a)=0$.

Q.No. $\alpha=\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ is an algebraic over $\mathbb{Q}$?

Soln $\alpha=\sqrt{2}\in\mathbb{Q}(\sqrt{2})$

let $f(x)=x^2-2\in\mathbb{Q}[x]$

s.t. $f(\sqrt{2})=(\sqrt{2})^2-2=0$

then $\alpha=\sqrt{2}$ is algebraic over $\mathbb{Q}$.

Q. (i) $\alpha=\pi$ is algebraic over $\mathbb{Q}$?

(ii) $\alpha=\pi$ " " " $\mathbb{R}$?

$f(x)=x-\pi\notin\mathbb{Q}[x]$

s.t. $f(\pi)=0$

then $\alpha=\pi$ is not algebraic over $\mathbb{Q}$.

(ii) $f(x)=x-\pi\in\mathbb{R}[x]$

s.t. $f(\pi)=0$ then π is algebraic over $\mathbb{R}$.

Q. $\alpha=\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ is algebraic over $\mathbb{Q}$?

Soln let $x=\sqrt{2}+\sqrt{3}$

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

Squaring on both side, we get

$x^2+2-2\sqrt{2}x=(\sqrt{3})^2$

$\Rightarrow x^2-1=2\sqrt{2}x$

Scanned with CamScanner

$(x^2-1)^2 = 8x^2$

$\Rightarrow x^4 - 10x^2 + 1 = 0$

$f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$

s.t. $f(\sqrt{2}+\sqrt{3}) = 0$

$\alpha = \sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$.

Q.No. $\alpha = (2)^{1/5} \in \mathbb{Q}[(2)^{1/5}]$ is algebraic over $\mathbb{Q}$.

$x = (2)^{1/5} \Rightarrow x^5 = 2 \Rightarrow x^5 - 2 = 0$

let $f(x) = x^5 - 2 \in \mathbb{Q}[x]$, $f(x) = 0$

i.e. $f(2^{1/5}) = 0$

$\Rightarrow \alpha = 2^{1/5}$ is algebraic over $\mathbb{Q}$.

Algebraic-Extension:-

An extension field K of F is said to be algebraic extension if every element of K is algebraic over F.

Q.No. Show that $\mathbb{Q}[\sqrt{2}]$ is an algebraic extension of $\mathbb{Q}$.

Soln $\mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$

let $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $a, b \in \mathbb{Q}$

s.t. $f(x) \in \mathbb{Q}[x]$

$\Rightarrow f(\alpha) = 0$

let $x = a + b\sqrt{2}$

$\Rightarrow x - a = b\sqrt{2}$

$\Rightarrow (x-a)^2 = 2b^2$

$\Rightarrow x^2 + a^2 - 2ax = 2b^2$

$\Rightarrow f(x) = x^2 - 2ax + a^2 - 2b^2 = 0 \in \mathbb{Q}[x]$

s.t. $f(a+b\sqrt{2}) = 0$ then $\mathbb{Q}[\sqrt{2}]$ is an algebraic extension of $\mathbb{Q}$.

Q.No. (i) $\mathbb{R}$ is an algebraic extension of $\mathbb{Q}$?
Q.No. (ii) $\mathbb{R}$ " " " " " $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Soln:
(i) $\alpha = e \in \mathbb{R}$ is not algebraic over $\mathbb{Q}$ then $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$.

(ii) $f(x) = x - e \notin \mathbb{Q}[\sqrt{2}, \sqrt{3}]$
s.t. $f(e) = 0$ then
$e \in \mathbb{R}$ is not algebraic over $\mathbb{Q}$.
then $\mathbb{R}$ is not " extension over $\mathbb{Q}$.

Q.No. Show that $\mathbb{C}$ is an algebraic extension over $\mathbb{R}$ but not $\mathbb{Q}$.

Soln:
$$\mathbb{C} = \{ a+ib \mid a, b \in \mathbb{R} \}$$
let $\alpha = a+ib \in \mathbb{C}$, $a, b \in \mathbb{R}$
Now let $x = a+ib \Rightarrow x - a = ib \Rightarrow (x-a)^2 = (ib)^2$
$\Rightarrow x^2 + a^2 - 2ax = -b^2$
$\Rightarrow x^2 + a^2 + b^2 - ax \in \mathbb{R}[x]$
$\Rightarrow f(x) = x^2 + a^2 + b^2 - ax \in \mathbb{R}[x]$
$\Rightarrow f(a+ib) = 0$
then $\mathbb{C}$ is algebraic over $\mathbb{R}$
Now $\pi \in \mathbb{C}$ But $f(x) = x - \pi \notin \mathbb{Q}[x]$ s.t. $f(\pi) = 0$
then π is not algebraic over $\mathbb{Q}$
then $\mathbb{C}$ is " " extension of $\mathbb{Q}$.

Note:
If $\dim(K/F)$ is finite then K is always Algebraic over F. But converse need not be true.
$\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots]$ is algebraic over $\mathbb{Q}$ but dim. of $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots]$ is infinite

Scanned with CamScanner

e.g. $\dim\left[\mathbb{Q}(2)^{1/7}(2)^{1/8} \mid \mathbb{Q}\right] = 56$ is finite then $\mathbb{Q}\left[(2)^{1/7}(2)^{1/8}\right]$ is algebraic over $\mathbb{Q}$.

(ii) $\dim(\mathbb{C}(\mathbb{R})) = 2$ is finite
then $\mathbb{C}$ is algebraic over $\mathbb{R}$

Splitting Field :-

An extension field K of F is said to be splitting field of $f(x) \in F[x]$ over F if

(i) $f(x)$ can be factored into linear over K, and
(ii) $f(x)$ can not be factor into linear over any subfield of K containing F.

e.g. $\mathbb{Q}[\sqrt{3}]$ is splitting field of $f(x) = x^2 - 3$ over $\mathbb{Q}$
$f(x) = x^2 - 3 = (x-\sqrt{3})(x+\sqrt{3})$ over $\mathbb{Q}[\sqrt{3}]$
and $\mathbb{Q}[\sqrt{3}]$ is smallest extension of $\mathbb{Q}$ s.t.
$f(x) = x^2 - 3 = (x-\sqrt{3})(x+\sqrt{3})$

Q. (ii) $\mathbb{C}$ is splitting field of $f(x) = x^2+1$ over $\mathbb{Q}$?
(iii) " " " " " " " $\mathbb{R}$?

e.g. (i) $f(x) = x^2+1 = (x+i)(x-i)$ in $\mathbb{C}$
But $\mathbb{Q}[i]$ is subfield of $\mathbb{C}$ s.t. $\mathbb{Q} \subseteq \mathbb{Q}[i] \subseteq \mathbb{C}$
and $f(x) = x^2+1 = (x+i)(x-i)$ in $\mathbb{Q}[i]$ then $\mathbb{C}$ is not splitting field of $\mathbb{Q}$.

(ii) $f(x) = x^2+1 = (x+i)(x-i)$ in $\mathbb{C}$ and $\mathbb{C}$ is smallest extension of $\mathbb{R}$.

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

Q. No. $f(x) = x^2 - 5x + 6 \in \mathbb{Q}[x]$ Find splitting field of $f(x)$ over $\mathbb{Q}$.

Soln $f(x) = x^2 - 5x + 6 = (x-2)(x-3)$ over $\mathbb{Q}$

then $\mathbb{Q}$ is splitting field of $f(x)$ over $\mathbb{Q}$.

Q. No. $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ find splitting field of $f(x)$ over $\mathbb{Q}$.

Ans $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Soln $f(x) = x^4 - 5x^2 + 6 = (x^2-2)(x^2-3)$ over $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$

then $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is splitting field of $f(x)$.

[**Note**:- splitting field of $f(x)$ over $\mathbb{Q}[\sqrt{2}]$

H.P.

Scanned with CamScanner

Galois Group:- let K is an extension field of F. A group G of all automorphism of K over F is called Galois group, it is denoted by $Gal(K|F) = Aut(K|F)$ and $o(Gal(K|F)) = dim_{(K|F)}$

Note:-
(i) $Gal(F|\mathbb{R}) \approx Z_1$ or Z_2 where F is field
(ii) $Gal(F|\mathbb{C}) \approx Z_1$

Explanation:-

① let $F = \mathbb{C}$ then $Gal(\mathbb{C}|\mathbb{R}) = Aut(\mathbb{C}|\mathbb{R}) \approx Z_2$

$\Rightarrow o(Aut(\mathbb{C}|\mathbb{R})) = dim(\mathbb{C}|\mathbb{R}) = 2$

② let $F = \mathbb{R}$ then $Gal(\mathbb{R}|\mathbb{R}) \approx Z_1$ $\quad [dim(\mathbb{R}|\mathbb{R}) = 1$

② $Gal(\mathbb{F}|\mathbb{C}) = ?$
extension of $\mathbb{C}$ is only $\mathbb{C}$ then $Gal(\mathbb{C}|\mathbb{C}) = Aut(\mathbb{C}|\mathbb{C}) \approx Z_1$

③ $Gal(GF(p^n)|GF(p^1)) = Aut(GF(p^n) \approx ? \approx \frac{Z_n}{I} = Z_n$.

Q.No:- Find Galois Group of $GF(2^{50})$

Soln. $Gal(GF(2^{50})|GF(2^1)) = Aut(GF(2^{50})/GF(2))$
$\approx Z_{50}$

Q.No. If F is field of order 3^{100} then how many subgp in Automorphism of F.

Soln $o(F) = 3^{100}$ then $F \approx GF(3^{100})$
then $Gal(GF(3^{100})|GF(3^1)) = Aut(GF(3^{100})|GF(3^1)) \approx Z_{100}$
# of subgp. in $Z_{100} = \tau(100) = 9$

Scanned with CamScanner

Q.No. Find splitting field of $f(x) = x^5 - 1$ over Q.
Galois of the

Soln $f(x) = x^5 - 1$ over Q

$f(x) = x^5 - 1 = 0 \Rightarrow x = (1)^{1/5} = \alpha$

S.t. $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$ is irreducible over Q

$\Rightarrow f(x) = x^5 - 1 = (x-1)(1 + x + x^2 + x^3 + x^4)$ has irreducible poly. of degree 4.

then $o\left(Gal(Q(\alpha)|Q)\right) = o\left(Aut(Q(\alpha))|Q\right) = 4$

$\Rightarrow Gal(Q(\alpha)|Q) = \{A^i \mid A^4 = e\}$

$\approx Z_4$

Note:- If $f(x) = x^n - 1$ then
Galois group of splitting field $f(x) = x^n - 1$ over $Q \approx U(n)$
i.e. $Gal(Q(1)^{1/n}|Q) \approx U(n)$

2015 83
Q.No.10- $K = Q(\omega^2)$
$L = Q(\omega)$ where $\omega =$ 10th root of unity
$\omega = (1)^{1/10}$

$Gal(K|Q) = Gal(Q(\omega^2)|Q) = Gal(Q(1)^{1/5}|Q) \approx U(5) \approx Z_4$

Now
$Gal(L|Q) = Gal(Q(\omega)|Q) = Gal(Q(1)^{1/10}|Q) = U(10) \approx Z_4$

then $L = K$

option (3) & (4) are correct.

Q.:: Find Galois Group of the splitting field. $f(x) = x^5 - 2$

Soln:- $f(x) = x^5 - 2$ over Q
let ~~$x^5 = 2$~~ $f(x) = 0$

$x^5 - 2 = 0$

$\Rightarrow x^5 = 2$

$\Rightarrow x^5 = 2 \cdot 1$

$\Rightarrow x = (2)^{1/5}(1)^{1/5}$

(i) for 5^{th} root of unity $\alpha = (1)^{1/5}$

s.t. $1+\alpha+\alpha^2+\alpha^3+\alpha^4 = 0$

$\Rightarrow f(\alpha) = 1+\alpha+\alpha^2+\alpha^3+\alpha^4$ is irreducible poly. over $\mathbb{Q}$ s.t. $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$ — (*)

(ii) for $x = (2)^{1/5}$

$\Rightarrow f(x) = x^5 - 2$ is irreducible poly. of degree (5) over $\mathbb{Q}$.

then $[\mathbb{Q}(2)^{1/5} : \mathbb{Q}] = 5$ — (**)

from equn (*) & (**)

$[\mathbb{Q}[\alpha, (2)^{1/5}] : \mathbb{Q}] = 4 \cdot 5 = 20$

then $o(Gal(\mathbb{Q}(\alpha, 2^{1/5}) : \mathbb{Q}) = o(Aut(\mathbb{Q}(\alpha, 2^{1/5}) : \mathbb{Q}) = 20$

Now $Gal(\mathbb{Q}(\alpha, 2^{1/5}) : \mathbb{Q}) = \{ A^i B^j \mid A^4 = e,\ B^5 = e,\ AB \neq BA$ $i = 0,1,2,3$ $j = 0,1,\ldots,4 \}$

Q.No.o- Find Galois Group of Splitting of $f(x) = x^3 - 2$ over $\mathbb{Q}$.

Sol^{n} o- $f(x) = x^3 - 2$ over $\mathbb{Q}$

Now $f(x) = x^3 - 2 = 0 \Rightarrow x^3 = 2 \cdot 1$

$\Rightarrow x = (2)^{1/3}(1)^{1/3} = (2)^{1/3} \cdot \omega$

for 3^{rd} roots of unity.

$\omega = (1)^{1/3}$ s.t. $f(\omega) = 1+\omega+\omega^2$ is irreducible poly. over $\mathbb{Q}$.

then $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ — (*)

Now (ii) $x = (2)^{1/3}$

then $[\mathbb{Q}(2)^{1/3} : \mathbb{Q}] = 3$ — (**)

$[\mathbb{Q}((2)^{1/3} \cdot \omega) : \mathbb{Q}] = 2 \times 3 = 6$

then $o(Gal(\mathbb{Q}((2^{1/3}, \omega)) : \mathbb{Q}) = 6$

Scanned with CamScanner

then $Gal\left(Q((2)^{1/3}, \omega) : Q\right) = \{ A^i B^j \mid A^2 = e,\ B^3 = e,\ AB \neq BA \}$
$i = 0,1,\ j = 0,1,2$

then $Gal\left(Q((2)^{1/3}, \omega) : Q\right) \approx D_3$

Q. How many subfield in $L = Q[(2)^{1/3}, \omega]$ over Q. other than Q of L.

Soln:- $Gal\left[(Q(2)^{1/3}, \omega) : Q\right] \approx D_3$

# of subfield in $Q((2)^{1/3}, \omega)$ over Q
$= \#$ of subgp. in $Gal\left(Q(2)^{1/3}, \omega : Q\right)$
$= \#$ " " in D_3
$= 6$

then L has 6 subfield over Q.
# of subfield of L over Q other than Q of L
$= 6 - 2 = 4$

June 2019
Q.No. 39 If is splitting field of $x^7 - 2$ and $z = e^{\frac{2\pi i}{7}}$
let $(F : Q(z)) = a$ and $(F : Q(2)^{1/7}) = b$
Ans (iii) option is correct

Soln F is splitting field of $x^7 - 2$
$F = Q[(2)^{1/7}\ (1)^{1/7}] = Q[(2)^{1/7} \cdot z]$

then $[F : Q] = [Q[(2)^{1/7}, z] : Q] = 7 \cdot 6 = 42$

$[F : Q] = [F : Q(z)] \cdot [Q(z) : Q]$
$= a \cdot 6$
$\Rightarrow a = \frac{42}{6} = 7$

Now $[F : Q(2)^{1/7}]\ [Q(2)^{1/7} : Q]$
$\Rightarrow 42 = b \cdot 7$
$\Rightarrow b = 6$

Scanned with CamScanner

Scanned with CamScanner

Q.: Show that $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ is field.

Soln 1st prove that $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] \subseteq \mathbb{R}$ is a subring

$$\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] = \{ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}+e\sqrt{2}\sqrt{3}+f\sqrt{3}\sqrt{5} + g\sqrt{2}\sqrt{5}+h\sqrt{2}\sqrt{3}\sqrt{5} \mid a,b,c,d,e,f,g,h \in \mathbb{Q} \}$$

$\Rightarrow \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ is common ring and

$1 \in \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ i.e. $[\sqrt{2},\sqrt{3},\sqrt{5}]$ is a common ring with unity.

Since $\mathbb{R}$ is integral domain

Now, $x^{-1} \in \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ s.t. $x x^{-1} = 1$

So, $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ is an integral domain.

H.P.

Scanned with CamScanner

$\Rightarrow Z_4[i] \approx Z_4 \times Z_4$

Note:- $\boxed{(Z_n[i], +) \approx Z_n \times Z_n}$

Q.No. $(Z_2[i]^*, \cdot)$ is group?

Soln:-

$Z_2[i] = \{0, 1, i, 1+i\}$

$(Z_2[i])^* = \{1, i\} \approx Z_2$

Q.No. $(Z_2[i] - \{0\}, \cdot)$ is group?

$Z_2[i] - \{0\} = \{1, i, 1+i\}$

No, it is not

$\therefore (1+i) \in Z_2[i] - \{0\}$ s.t. $(1+i)(1+i) = 0 \notin Z_2[i] - \{0\}$

then $Z_2[i] - \{0\}$ is not group w.r.t. Multiplication.

Q.No. $(Z_3[i] - \{0\}, \cdot)$ is group?

Soln $Z_3[i] - \{0\} = \{1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\}$

composition table are, of $Z_3[i] - \{0\}$

	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
1	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
2	2	1	$2i$	i	$2+2i$	$2+i$	$1+2i$	$1+i$
i	i	$2i$	2	1	$2+i$	$1+i$	$2+2i$	$1+2i$
$2i$	$2i$	i	1	2	$1+2i$	$2+2i$	$1+i$	$2+i$
$1+i$	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	2	1	i
$1+2i$	$1+2i$	$2+i$	$1+i$	$2+2i$	2	i	$2i$	1
$2+i$	$2+i$	$1+2i$	$2+2i$	$1+i$	1	$2i$	i	2
$2+2i$	$2+2i$	$1+i$	$1+2i$	$2+i$	i	1	2	$2i$

Q.No: $(Z_4[i], +) \approx$

Soln $Z_4[i] = \{a+ib \mid a \in Z_4, b \in Z_4\}$

$= \{0, 1, 2, 3, i, 2i, 3i, 1+i, 1+2i, 1+2i, 1+3i, 2+i, 2+2i, 2+3i, 3+i, 3+2i, 3+3i\}$

$O(Z_4[i]) = 16$

Since $(Z_4[i], +)$ is abelian gp. then possible non isomorphic abelian gp. of order 16 are

① Z_{16}
② $Z_8 \times Z_2$
③ $Z_4 \times Z_4$
④ $Z_4 \times Z_2 \times Z_2$
⑤ $Z_2 \times Z_2 \times Z_2 \times Z_2$

then $Z_4[i]$ $\not\cong$ Z_{16}, $Z_8 \times Z_2$, $Z_4 \times Z_4$, $Z_4 \times Z_2 \times Z_2$, $Z_2 \times Z_2 \times Z_2 \times Z_2$

Since $Z_4[i]$ has no elements of order 4
then $Z_4[i] \not\cong Z_{16}$ and $Z_8 \times Z_2$
$1 \in Z_4[i]$ s.t. $O(1) = 4$
then $Z_4[i]$ has elements of order 2
$\Rightarrow Z_4[i] \not\cong Z_2 \times Z_2 \times Z_2 \times Z_2$

Now, if $Z_4[i] \approx Z_4 \times Z_2 \times Z_2$ then $Z_4[i]$ has seven element of order 2.
But $Z_4[i]$ has exactly three elements of order 2
then $Z_4[i] \not\cong Z_4 \times Z_2 \times Z_2$ say $2, 2i, 2+2i$

Scanned with CamScanner

Soln (A)

Need not.

(i) If $n=1$ then $Z_1[i] = \{0\}$

$\Rightarrow o(Z_1[i]) = 1$

$\Rightarrow Z_1[i] \approx Z_1$

Then $Z_1[i]$ is cyclic.

(ii) If $n \geq 2$ then $Z_n[i] = \{a+ib \mid a,b \in Z_n\}$ is not cyclic because

$o(Z_n[i]) = n^2$ but

$Z_n[i]$ has no element of order $> n$

If $n \neq 1$ then $n^2 > n$

For example:-

$Z_2[i] = \{0, 1, i, 1+i\}$

$o(Z_2[i]) = 2^2 = 4$

$0 \in Z_2[i]$ s.t. $o(0) = 1$

$1 \in Z_2[i]$ " $o(1) = 2$

$i \in Z_2[i]$ " $o(i) = 2$

$1+i \in Z_2[i]$ such that $o(1+i) = 2$

$o(Z_2[i]) = 4 \begin{cases} Z_4 \\ Z_2 \times Z_2 \end{cases}$

$Z_2[i]$ has no element of order > 2 then

$Z_2[i] \not\approx Z_4$

$\Rightarrow Z_2[i] \approx Z_2 \times Z_2$

Q.No. $(Z_3[i], +) \approx ? = 9 \begin{cases} Z_9 \\ Z_3 \times Z_3 \end{cases}$

$Z_3[i] = \{a+ib \mid a \in Z_3, b \in Z_3\}$

$= \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\}$

Scanned with CamScanner

$Z_3[i]$ has no element of order 73

then $Z_3(i) \neq Z_9$

$\Rightarrow Z_3(i) \approx Z_3 \times Z_3$