RING THEORY

After studying group theory we have observed that it was a set and a binary composition on that set. Whereas here we'll have one set and two binary compositions on that. For example-

Ring: Let R be a non-empty set $(R,+,\cdot)$ is said to be ring if

(a) $(R,+)$**is Commutative group**

(i) $\forall a \in R, \forall b \in R \Rightarrow a+b \in R$

(ii) $a+(b+c)=(a+b)+c, \forall a,b,c \in R$

(iii) $\forall a \in R\ \exists 0 \in R$ s.t $a+0=0+a=a$

(iv) For each a $\exists$ (unique) - a such that $a+(-a)=-a+a$

(v) $a+b=b+a, \forall a,b \in R$

Note- The set is an abelian group w.r.t the **first** binary composition.

(b) $(R,\cdot)$ **is Semi-group**

(i) $\forall a \in R, \forall b \in R \Rightarrow a \cdot b \in R$

(ii) $a \cdot (b \cdot c)=(a \cdot b) \cdot c, \forall a,b,c \in R$

Note- The set is a semi group w.r.t the **second** binary composition.

(c) Left and Right Distributive Law

(i) $a \cdot (b+c)=a \cdot b+a \cdot c,\ \forall a,b,c \in R$

(ii) $(a+b) \cdot c=a \cdot c+b \cdot c,\ \forall a,b,c \in R$

Note- The **second** binary composition is distributive over **first** binary composition.

Q. $(Z,+,\cdot)$ is Ring?

Ans. (a) $(Z,+)$ is cyclic group then $(Z,+)$ is commutative group

(b) $(Z,\square)$ is semi-group

(i) $\forall a \in Z, \forall b \in Z \Rightarrow ab \in Z$

(ii) $a \cdot (bc)=(ab) \cdot c,\ \forall a,b,c \in Z$

(c) Left and Right Distributive Law

(i) $a.(b+c)=a \cdot b+a \cdot c,\ \forall a,b,c \in Z$

(ii) $(a+b) \cdot c=a \cdot c+b \cdot c,\ \forall a,b,c \in Z$

Therefore $(Z,+,\cdot)$ is Ring.

Similarly,

$(Q,+,\square),(\mathbf{R},+,\square),(\mathbf{C},+,\square)$ are also Rings.

Commutative Ring: A ring $(R,+,\square)$ is said to be commutative ring if $ab=ba, \forall a,b \in R$

Q. $(Z,+,\square),(Q,+,\square),(\mathbf{R},+,\square),(\mathbf{C},+,\square)$ are commutative rings?

Ans. (i) $(\mathbf{R},+,\square)$ is ring and $a \cdot b=b \cdot a,\ \forall a,b \in R$ then $(\mathbf{R},+,\square)$ is Commutative Ring.

Since $Q \subseteq \mathbf{R}$ and $(\mathbf{R},+,\square)$ is commutative ring then $(Q,+,\square)$ is commutative ring.

Similarly, $(Z,+,\square)$ is commutative ring and also $(\mathbf{C},+,\square)$ is commutative ring.

Mindset Makers

Ring with Unity: A ring $(R,+,\square)$ is said to be ring with unity if $\exists\ \ 0\neq b\in R$ such that $a\cdot b=b\cdot a=a,\ \forall a\in R$

Q. $(Z,+,\square)$ is commutative ring with unity?

Ans. $1\in Z$ s.t $1\cdot a=a\cdot 1=a,\ \forall a\in Z$ and $(Z,+,\square)$ is commutative ring then $(Z,+,\square)$ is commutative ring with unity.

Similarly, $(Q,+,\square)$, $(\mathbf{R},+,\square)$, $(\mathbf{C},+,\square)$ are commutative ring with unity 1.

Q. $R=\{0\}$ is commutative ring with unity?

Solution: $R=\{0\}$, $(\mathbf{R},+,\square)$ is commutative ring but not unity.

Gaussian Integer:

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

Q. Show that $(Z[i],+,\cdot)$ is ring.

Solution: Gaussian Integer: $Z[i]=\{a+ib\,|\,a,b\in Z\}$ ....(1)

(A) $(Z[i],+)$ is commutative group

(i) $x=a_1+ib_1\in Z[i], y=a_2+ib_2\in Z[i]$ where, $a_1,a_2,b_1,b_2\in$

$x+y=(a_1+ib_1)+(a_2+ib_2)$

$=(a_1+a_2)+i(b_1+b_2)$

$=c_1+ic_2$, where $c_1=a_2+a_2$

$c_2=b_1+b_2$

$a_1\in Z, a_2\in Z\Rightarrow c_1=a_1+a_2\in Z$

$b_1\in Z, b_2\in Z\Rightarrow c_2=b_1+b_2\in Z$

$\Rightarrow c_1+ic_2\in Z[i]\Rightarrow x+y\in z[i]$

(ii) $z=a_3+ib_3\in Z[i]$

$x+(y+z)=(a_1+ib_1)+((a_2+ib_2)+(a_3+ik))=(a_1+a_2+a_3)+i(b_1+b_2+b_3)$

R.H.S. $=(x+y)+z=((a_1+ib_1)+(a_2+ib_2))+(a_3+ib_3)=(a_1+a_2+a_3)+i(b_1+b_2+b_3)$

L.H.S. = R.H.S.; then $x+(y+z)=(x+y)+z$

(iii) $x=a_1+ib_1\in Z[i]$ then $\exists 0=0+i0\in Z[i]$

s.t $x+0=(a_1+ib_1)+(0+i0)=(a_1+0)+i(b_1+0)=a_1+ib_1\in Z[i]$

(iv) $x=a_1+ib_1\in Z[i], a_1,b_1\in Z$

$a_1\in Z\Rightarrow -a_1\in Z$ [because Z is group]

$b_1\in Z\Rightarrow -b_1\in Z$

$\Rightarrow -a_1+i(-b_1)\in Z[i]\Rightarrow -x=a_1+i(-b_1)\in Z[i]$ s.t $x+(-x)=-x+x=0=0+i0$

(v) $x=a_1+ib_1\in Z[i], y=a_2+ib_2\in Z[i]$

$x+y=(a_1+ib_2)+(a_2+ib_2)=(a_1+a_2)+i(b_1+b_2)=(a_2+a_1)+i(b_2+b_1)$

$=(a_2+ib_2)+(a_1+ib_1)=y+x\Rightarrow x+y=y+x,\forall x,y\in Z[i]$

Mindset Makers

(a) $(Z[i],\cdot)$ is semi-group.

(i) $x=a_1+ib_1\in Z[i], y=a_2+ib_2\in Z[i]$

$x\cdot y=(a_1+ib_1)(a_2+ib_2)=(a_1a_2-b_1b_2)+i(a_1b_2+b_1a_2)\in Z[i]$

$\Rightarrow xy\in Z[i]$ [$\because a_1a_2-b_1b_2\in Z$, $a_2b_2+b_1a_2\in Z$] $\therefore xy\in Z[i]\ \forall x,y$

(ii) $x\cdot(y\cdot z)=(x\cdot y)\cdot z,\ \forall x,y,z\in Z[i]$

(c) Left and Right Distributive Law

(i) $x(y+z)=x\cdot y+x\cdot z$

(ii) $(x+y)\cdot z=x\cdot z+y\cdot z,\ \forall x,y,z\in Z[i]$ then $(Z[i],+,\cdot)$ is Ring.

Q. $(Z[i],+,\cdot)$ is commutative Ring?

Ans. Yes

Q. $(Z[i],+,\cdot)$ is commutative ring with unity?

Solution: Yes, $x=1=1+0i\in Z[i]$ is unity of $Z[i]$

Q. $(Z_n,+,\cdot)$ is ring. Show?

Solution: (A) $(Z_n,+)$ is commutative group because Z_n is cyclic group.

(B) $(Z_n,\cdot)$ is semi-group

(i) $\forall a\in Z_n, b\in Z_n\Rightarrow ab\in Z_n$

(ii) $a\cdot(b\cdot c)=(a\cdot b)\cdot c,\forall a,b$

(c) Left and Right Distributive law

(i) $a\cdot(b+c)=a\cdot b+a\cdot c$

(ii) $(a+b)\cdot c=a\cdot c+b\cdot c,\forall a,b,c\in Z_n$ then $(Z_n,+,\cdot)$ is a ring.

Q. $(Z_n,+,\cdot)$ is commutative ring?

Solution:

$\forall a\in Z_n,\forall b\in Z_n\Rightarrow ab=ba$ then $(Z_n,+,\cdot)$ is commutative ring.

Q. $(Z_n,+,\cdot)$ is commutative ring with unity?

Solution: Need not be commutative ring with unity.

Note:

(i) If $n=1$ then $(Z_n,+,\cdot)$ is commutative ring but not unity.

(ii) If $n\geq 1$ then $(Z_n,+,\cdot)$ is commutative ring with unity say unity = 1

Q. (i) Show that $M_n(\mathbf{R})=\left\{A=\left[a_{ij}\right]_{n\times m}\middle| a_{ij}\in\mathbf{R}\right\}$ is ring i.e. $(M_n(\mathbf{R}),+,\cdot)$ is Ring.

(ii) $R=Z_m\times Z_n$ is Ring?

Solution: (i) $M_n(\mathbf{R})$ is not commutative for $n\geq 1$

Note:

(i) $M_n(\mathbf{R}), n\geq 1$ is Ring with unity but not commutative.

(ii) If $n=1$ then $M_n(\mathbf{R})=\mathbf{R},(\mathbf{R},+,\cdot)$ is commutative then $M_n(\mathbf{R})$ is commutative ring with unity.

Mindset Makers

$R = Z_m \times Z_n$ is ring
$R = Z \times Z$ is ring
$R = Z \times Q$ is ring
$R = Q \times Q$ is ring
$R = \mathbf{R} \times \mathbf{R}$ is ring
$R = \mathbf{C} \times \mathbf{C}$ is ring
$R = Z[i] \times Z[i]$ is ring

Now, (A) $(Z_m \times Z_n, +)$ is commutative group.

(i) $x = (a_1, b_1) \in Z_m \times Z_n$

$y = (a_2, b_2) \in Z_m \times Z_n$

$x + y = (a_1, b_1) + (a_2, b_2) = ((a_1 + a_2), (b_1 + b_2))$

$a_1 \in Z_m, a_2 \in Z_m \Rightarrow a_1 + a_2 \in Z_m$

$b_1 \in Z_n, b_n \in Z_n \Rightarrow b_1 + b_2 \in Z_n$

$\Rightarrow ((a_1 + a_2), (b_1 + b_2)) \in Z_m \times Z_n$

(ii) $x + (y + z) = (x + y) + z, \ \forall x, y, z \in Z_m \times Z_n$

(iii) $\forall x = (a_1, b_1) \in Z_m \times Z_n, \ \exists\, e = (0,0) \in Z_m \times Z_n$ such that

$(a_1, b_1) + (0,0) = (a_1 + 0, b_1 + 0) = (a_1, b_1)$

(iv) For each $x = (a_1, b_1) \in Z_m \times Z_n$

$\exists - x = (m - a_1, n - b_1) \in Z_m \times Z_n$

s.t $x + (-x) = (-x) + x = (a_1, b_1) + (m - a_1, n - b_1) = (m, n) = (0,0)$ under modulo

(v) $x = (a_1, b_1) \in Z_m \times Z_n, \ y = (a_2, b_2) \in Z_m \times Z_n$

$x + y = (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) = (a_2 + a_1, b_2 + b_1) = y + x$

$\Rightarrow x + y = y + x, \ \forall x, y \in Z_m \times Z_n \ (Z_m \times Z_n, +)$ is abelian group

(B) $(Z_m \times Z_n, \cdot)$ is semi-group

(i) $x = (a_1, b_1) \in Z_m \times Z_n$

$y = (a_1, b_2) \in Z_m \times Z_n$

$x \cdot y = (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2) \in Z_m \times Z_n \Rightarrow xy \in Z_m \times Z_n$

(ii) $x \cdot (y \cdot z) = (x \cdot y) z, \ \forall x, y, z \in Z_m \times Z_n$

(c) Left and Right Distributive

(i) $x \cdot (y + z) = x \cdot y + x \cdot z, \ \forall x, y, z \in Z_m \times Z_n$

(ii) $(x + y) \cdot z = x \cdot z + y \cdot z, \ \forall x, y, z \in Z_m \times Z_n$

$\therefore Z_m \times Z_n$ is ring.

Similarly, $Z \times Z, \mathbf{R} \times Q, Z[i] \times Z[i]$ is ring.

Q. $Z_m \times Z_n$ is commutative ring?

Solution: Yes, $x = (a_1, b_1) \in Z_m \times Z_n$

Mindset Makers

$y=(a_2,b_2)\in Z_m\times Z_n$

$x\cdot y=(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,b_1b_2)=(a_2a_1,b_2b_1)=y\cdot x,\ \forall x,y\in Z_m\times Z_n$

$\therefore xy=y\cdot x,\ \forall x\cdot y\in Z_m\times Z_n$ then $Z_m\times Z_n$ is commutative.

Q. $R=Q\times Q$ is commutative ring with unity?

Solution:

$x=(a_1,b_1)\in Q\times Q$

$y=(a_2,b_2)\in Q\times Q$

$xy=yx$, then $Q\times Q$ is commutative ring

Now,

$x=(a_1,b_1)\in Q\times Q$

$y=(1,1)\in Q\times Q$

$x\cdot y=(a_1,b_1)(1,1)=(a_1\cdot 1,b_2\cdot 1)=(a_1,b_1)=x$

It is commutative ring with unity.

Q. $R=Q\times\{0\}$ is commutative ring with unity?

Solution: Yes, $R=Q\times\{0\}$

$(1,0)\in Q\times\{0\}$ s.t $(1,0),(a,0)=(a,0)$

$(1,0),(a,0)=(a,0)$ s.t

$(1,0)(a,0)=(a,0)$

$R=Q\times\{0\}$ is commutative ring with unity $(1,0)$

similarly, (i) $Z[i]\times\{0\}\rightarrow$ unity $(1,0)$

(ii) $\{0\}\times\mathbf{R}\times\mathbf{C}$ are commutative ring with unity $(0,1,1)$.

Integral Domain- before studying this we need to have an understanding about zero divisors in a ring.

Zero Divisors- A ring is said to have zero divisors if on composing it's any arbitrary two non-zero elements w.r.t the second binary composition the result comes out as zero element. Here zero element is the identity element of ring w.r.t the first binary composition. For example: In Z_6 we have proper zero divisors. Since 2.3=6=0 in Z_6. Similar results we can find in Matrices w.r.t multiplication.

ZERO DIVISOR

Definition: Let $(R,+,\cdot)$ is commutative ring A non-zero element, $0\neq a\in R$ is said to be zero divisor if $\exists 0\neq b\in$ such that $a\cdot b=0$

Note: If R is not commutative then

$A=\begin{bmatrix}0&1\\0&0\end{bmatrix}\in M_2(\mathbf{R}),\ B=\begin{bmatrix}1&0\\0&0\end{bmatrix}\in M_2(\mathbf{R});\ AB=\begin{bmatrix}0&1\\0&0\end{bmatrix}\begin{bmatrix}1&0\\0&0\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}\rightarrow$ represent A is zero divisor

But $BA=\begin{bmatrix}1&0\\0&0\end{bmatrix}\begin{bmatrix}0&1\\0&0\end{bmatrix}=\begin{bmatrix}0&1\\0&0\end{bmatrix}\neq\begin{bmatrix}0&0\\0&0\end{bmatrix}\therefore$ A is not zero divisor.

Mindset Makers

INTEGRAL DOMAIN

A commutative ring with unity $(R,+,\cdot)$ is called Integral domain if

$0 \neq a \in R,\ 0 \neq b \in R \Rightarrow ab \neq 0$

i.e. $a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$

Q. $(Z,+,\cdot)$ is an Integral Domain?

Solution: $a \in Z, b \in Z$ and $ab = 0 \Rightarrow a = 0$ or $b = 0$ then Z is an Integral Domain.

Similarly, Note: $(Q,+,\cdot),(R,+,\cdot),(\mathbf{C},+,\cdot),(Z[i],+,\cdot)$ are Integral Domain.

Q. $Z_{12} = \{0,1,2,....11\}$ is an Integral domain?

Solution: $0 \neq 4 \in Z_{12},\ 0 \neq 3 \in Z_{12}$, but $4 \cdot 3 = 0$ then Z_{12} is not integral domain.

Q. Z_{21} is an Integral domain?

Solution: $0 \neq 7 \in Z_{21},\ 0 \neq 3 \in Z_{21}$ but $7 \cdot 3 = 0$ then Z_{21} is not integral domain.

Note: Z_n is an integral domain iff $n = p$ where p is prime.

* $Z_3[i] \times Z_3[i]$ and $Z_7 \times Z_7$ is not an Integral Domain because $(1,0)(0,1) = (0,0)$.

Q. Z_1 is an Integral Domain?

Ans. No, because Z_1 is not commutative ring with unity.

Q. $R = Z \times Q$ is an integral domain?

Ans. $(0,0) \neq (1,0) \in Z \times Q$, $(0,0) \neq (0,1) \in Z \times Q$

But, $(1,0)(0,1) = (1.0, 0.1) = (0,0)$ then $Z \times Q$ is not an integral domain.

Q. $R = Z \times Q \times Z[i]$ is an integral domain?

Ans. No

Q. $R = Z \times Q \times Z[i] \times Z_3 \times \mathbf{R} \times \mathbf{C} \times Z_6$ is integral domain.

Ans. No

Q. $R = \mathbf{R} \times \{0\}$ is an integral domain?

Solution: $x \in \mathbf{R} \times \{0\}$ then $x = (a,0)$, $y \in \mathbf{R} \times \{0\}$ then $y = (b,0)$

$x \cdot y = 0 \Rightarrow (a,0)(b,0) = 0 = (0,0)$

$(a,0)(b,0) = (a \cdot b, 0) \Rightarrow (ab,0) = (0,0)$

$\Rightarrow ab = 0, a, b \in \mathbf{R}, \mathbf{R}$ is integral domain if either $a = 0$ or $b = 0$.

if $a = 0$ then $x = (0,0)$

$b = 0$ then $y = (0,0)$

$xy = 0 \Rightarrow x = 0$, or $y = 0$

Gaussian Integer Modulo *n*

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

$Z_1[i] = \{a + ib \mid a, b \in Z_1\} = \{0\}$, $Z_2[i] = \{a + ib \mid a, b \in Z_2\} = \{0,1,i,1+i\}; Z_2 = \{0,1\}$

$Z_3[i] = \{a + ib \mid a, b \in Z_3\} = \{0,1,2,i,2i,1+i,1+2i,2+i,2+2i\}$

Exam Point: $O(Z_n[i]) = n^2$

Mindset Makers

Q. Show that $(Z_n[i],+,\cdot)$ is commutative ring.

Note: If $n\geq 1$ then $(Z_n[i],+,\cdot)$ is commutative ring with unity 1.

Q. $Z_2[i]$ is an integral domain?

Solution:

$Z_2[i]=\{a+ib|a,b\in Z_2\}$ is commutative ring with unity $1+0i$

$Z_2[i]=\{0,1,i,1+i\}$

$0\neq(1+i)\in Z_2[i],\ 0\neq(1+i)\in Z_2[i]$

$(1+i)(1+i)=2i=0$ (modulo 2)

is not an integral domain.

Note: $Z_3[i]=O[Z_3[i]]=9$

$(0,1,2)(0,1,2)$

$=(0,0)\ (0,1)\ (0,0)\ (1,0)\ (1,1)\ (1,2)\ (2,0)\ (2,1)\ (2,2)$

" " " " " " " " "

$0\quad i\quad 2i\quad 1\quad 1+i\quad 1+2i\quad 2\quad 2+i\quad 2+2i$

Q. $Z_3[i]$ is an integral domain?

Solution: $Z_3[i]=\{a+ib|a,b\in Z_3\}=\{0,1,2,i,2i,1+i,1+2i,2+i,2+2i\}$

Construct multiplication table of non-zero element (mod 3 applied)

	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	2	$1+2i$	$2+2i$	$1+2i$
$1+i$	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	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	$2i$

$0\neq a\in Z_3[i]$ then $Z_3[i]$ is an integral domain.

$0\neq b\in Z_3[i];\ a\cdot b\neq 0$

Q. $R=Z_4[i]$ is an integral domain?

Ans. No, $0\neq 2\in Z_4[i]$

$0\neq 2\in Z_4[i]$

$2\cdot 2=4=0$ (mod 4)

then $Z_4[i]$ is not an integral domain.

Q. $R=Z_5[i]$ is an integral domain?

Solution:

$0\neq(2+i)\in Z_5[i]$

$0\neq(2+4i)\in Z_5[i]$

Mindset Makers

But $(2+i)(2+4i)=0$ then $Z_5[i]$ is not integer domain.

$=4+8i+2i+4i^2$

$=\cancel{4}+10i-\cancel{4}=0 \pmod 5$

Exam point: $Z_p[i]$ is an integral domain if 4 divides *p-3*, Where *p* is prime.

e.g. (i) 4 does not divide (13-3) $\Rightarrow Z_{13}[i]$ is not an integral domain.

(ii) 4 does not divide (13-3) $\Rightarrow Z_{17}[i]$ is not an integral domain.

Q. $Z\times Z, Z\times\mathbf{R}, Z_3[i]\times Z_7[i], Q\times\mathbf{R}\times\mathbf{C}$

$Q\times Z_7\times Z_{13}[i]\times\mathbf{R}, Q\times Q, \mathbf{R}\times\mathbf{R}, \mathbf{C}\times\mathbf{C}$

$Q\times\mathbf{C}$ are not integral domain.

Q. Show that $Z\times\mathbf{R}$ is not integral domain.

Solution:

$(0,0)\neq(1,0)\in Z\times\mathbf{R}$

$(0,0)\neq(0,1)\in Z\times\mathbf{R}$

$(1,0)(0,1)=(0,0)$ then $Z\times\mathbf{R}$ is not integral domain.

Q. $Z\times Q\times\mathbf{R}$ is an integral domain?

Solution: No, $(0,0,0)\neq(1,0,0)\in Z\times Q\times\mathbf{R}$

$(0,0,0)\neq(0,0,1)\in Z\times Q\times\mathbf{R}$ But $(1,0,0)(0,0,1)=(0,0,0)$

then $Z\times Q\times\mathbf{R}$ is not integral domain.

Q. $\mathbf{C}\times\mathbf{C}$ is an integral domain?

Solution: $(0,0)\neq(1,0)\in\mathbf{C}\times\mathbf{C}$

$(0,0)\neq(0,1)\in\mathbf{C}\times\mathbf{C}$

$(1,0)(0,1)=(0,0)$ then

$R=\mathbf{C}\times\mathbf{C}$ is not an integral domain.

Q. $R=\mathbf{C}\times\{0\}$ is an integral domain?

Solution: Yes, it is an integral domain.

Note: (Any Integral Domain) $\times\ \{0\}$ is an integral domain.

Q. Show that $Z_5[i]\times\{0\}$ is not an integral domain.

Solution:

$Z_5[i]\times\{0\}=\{(a\cdot 0)|(a,0)\in Z_5[i]\times\{0\}\}$

$(0,0)\neq(2+i,0)\in Z_5[i]\times\{0\}$

$(0,0)\neq(2+4i,0)\in Z_5[i]\times\{0\}$

but

$(2+i,0)(2+4i,0)=((2+i)(2+4i),0\cdot 0)=(0,0)$

then $Z_5[i]\times\{0\}$ is not an integral domain.

Q. $R=\{0\}\times\{0\}$ is an integral domain?

Solution: R is not commutative ring with unity then R is not an integral domain.

Mindset Makers

Note:

List of integral domains:

(i) Z (ii) Q (iii) **R** (iv) **C** (v) Z_p (vi) $Z_p[i]$ if $4 \mid p-3$, where p is prime. (vii) $Z[i]$

Note: $Q[i]=\{a+ib \mid a,b \in Q\}$, $\mathbf{R}[i]=\{a+ib \mid a,b \in \mathbf{R}\}$ are also integral domain.

Field: An integral domain $(\mathbf{F},+,\cdot)$ is field if each non-zero element of **F** has multiplicative inverse.

Example: $R=(Q,+,\cdot)$ is field?

Solution: Yes, $(Q,+,\cdot)$ is an integral domain $U(Q)=Q-\{0\}$ it means each non-zero elements of Q has multiplicative inverse then $(Q,+,\cdot)$ is a field.

Similarly, $(\mathbf{R},+,\cdot),(\mathbf{C},+,\cdot)$ are also field.

Q. $Z_5=\{0,1,2,3,4\}$ is field?

Solution: Z_5 is an integral domain and each non-zero element of Z_5 has multiplicative inverse

$1^{-1}=1,\ 2^{-1}=3,\ 3^{-1}=2,\ 4^{-1}=4$ then $(Z_5,+,\cdot)$ is field.

Note: If **F** is field then **F** is an integral domain but converse need not be true.

e.g. Z is an integral domain but not field because $3 \in Z$ but $3^{-1} \notin Z$ s.t $3 \cdot 3^{-1}=1$

Exam Point: If **F** is finite integral domain then **F** is field.

Q. $Z_7=\{0,1,2,3,4,5,6\}$, Z_7 is finite integral domain and we know that every finite integral domain is field then Z_7 is field.

Exam point: Z_n is field if and only if $n=p$

Q. $Z_3[i]$ is field?

Solution: $Z_3[i]$ is an integral domain and $Z_3[i]$ is finite then $Z_3[i]$ is field.

Note: $Z_p[i]$ is field if $4 \mid p-3$

Q. $Z_{13}[i]$ is field?

Solution: $4 \times 13-3$ then $Z_{13}[i]$ is not an integral domain then $Z_{13}[i]$ is not a field.

Q. $Z_{23}[i]$ is field?

Solution: $4 \mid 23-3$, then $Z_{23}[i]$ is finite integral domain, $Z_{23}[i]$ is field.

Polynomial Ring

Definition: Let $(R,+,\cdot)$ be a commutative ring. The set $R[x]=\{a_0+a_1x+a_2x^2+....+a_nx^n \mid a_i \in R\}$ is called Polynomial ring with indeterminant x.

Note:

(1) $f(x)=a_0+a_1x+a_2x^2+....+a_nx^n \in R[x], a_i \in R$

$g(x)=b_0+b_1x+b_2x^2+....+b_nx^n \in R[x],\ b_j \in R$

Mindset Makers

$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+....+(a_n+b_n)x^n$

$=c_0+c_1x+c_2x^2+....+c_nx^n\in R[x]=f(x)+g(x)\in R[x]$

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

$f(x)=x+1\in R[x], g(x)=x^2+2\in R[x]$

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

Degree of Polynomial: $f(x)=a_0+a_1x+a_2x^2+....+a_n\ x^n$ of degree n if $a_n\neq 0$. The degree of $f(x)$ is denoted by $\deg(f(x))$.

Q. $f(x)=x^3+x^2+x+1\in Z[x]$

$g(x)=x^3-x^2+x-1\in Z[x]$, find $\gcd(f(x),g(x))$ and L.C.M. $(f(x),g(x))$?

Solution: $f(x)=x^3+x^2+x+1,\ g(x)=x^3-x^2+x-1$

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

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

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

L.C.M. $(f(x),g(x))=(x^2+1)(x-1)(x+1)=(x^2+1)(x^2-1)=x^4-1$.

Discussion about $(Q\sqrt{2},+,.)$

(A) $(Q\sqrt{2},+)$ is Abelian group

(1) $x=a_1+b_1\sqrt{2}\in Q\sqrt{2},\ y=a_2+b_2\sqrt{2}\in Q\sqrt{2}$

$\Rightarrow x+y=(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})=(a_1+a_2)+(b_1+b_2)\sqrt{2}$

$=C_1+C_2\sqrt{2}\in Q\sqrt{2}$ where $C_1=a_1+a_2\in Q,\ C_2=b_1+b_2\in Q\Rightarrow x+y\in Q\sqrt{2}$

(2) $x+(y+z)=(x+y)+z,\ \forall x,y,z\in Q\sqrt{2}$

(3) $\forall x\in Q\sqrt{2}\ \exists\ 0=0+0\sqrt{2}\in Q\sqrt{2}$ s.t. $x+0=0+x=x$

(4) For each $x=a_1+b_1\sqrt{2}\in Q\sqrt{2}\ \exists -x=-a_1-b_1\sqrt{2}\in Q$ such that $x+(-x)=(-x)+x=0$

(5) $x+y=(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})=(a_1+a_2)+(b_1+b_2)\sqrt{2}=(a_2+a_1)+(b_2+b_1)\sqrt{2}=y+x$

(B) $(Q\sqrt{2},\cdot)$ semi-group

(1) $x=(a_1+a_2\sqrt{2})\in Q[\sqrt{2}],\ y=(b_1+b_2\sqrt{2})\in Q[\sqrt{2}]$

$x\cdot y=(a_1+a_2\sqrt{2})(b_1+b_2\sqrt{2})=(a_1b_1+2a_2b_2)+(a_1b_2+a_2b_1)\sqrt{2}=C_1+C_2\sqrt{2}\in Q[\sqrt{2}]$

$\Rightarrow xy=yx\in Q[\sqrt{2}]$

(2) $x\cdot(y\cdot z)=(x\cdot y)\cdot z,\ \forall x,y,z\in Q[\sqrt{2}]$

(c) Left and Right Distributive law

(1) $x\cdot(y+z)=xy+xz$

Mindset Makers

(2) $(x+y)\cdot z = x\cdot y + y\cdot z,\ \forall x,y,z \in Q\sqrt{2}$

$\left(Q\sqrt{2},+,\cdot\right)$ is ring.

Q. $\left(Q\sqrt{2},+,\cdot\right)$ is commutative ring with unity.

Solution: $x = a_1 + b_1\sqrt{2}$

$y = a_2 + b_2\sqrt{2}$

$x\cdot y = \left(a_1 + b_1\sqrt{2}\right)\left(a_2 + b_2\sqrt{2}\right) = \left(a_1a_2 + 2b_1b_2\right) + \left(a_1b_2 + b_1a_2\right)\sqrt{2}$

$= \left(a_2a_1 + 2b_2b_1\right) + \left(b_2a_1 + a_2b_1\right)\sqrt{2}$

$= yx$. then $\left(Q\sqrt{2},+,\cdot\right)$ is commutative ring.

$1 = 1 + 0\sqrt{2} \in Q\sqrt{2}$ such that $1\cdot x = x\cdot 1 = x\ \forall x \in Q\sqrt{2}$ then $\left(Q\left[\sqrt{2}\right]\right)$ is commutative ring with unity.

Q. Show that $\left(Q\sqrt{2},+,\cdot\right)$ is field.

Solution: Let $0 \neq x = a_1 + b_1\sqrt{2} \in Q\left[\sqrt{2}\right] \Rightarrow x^{-1} = \frac{1}{x} = \frac{1}{a_1 + b_1\sqrt{2}} = \frac{a_1 - b_1\sqrt{2}}{\left(a_1 + b_1\sqrt{2}\right)\left(a_1 - b_1\sqrt{2}\right)}$

$= \frac{a_1}{\left(a_1^2 - 2b_1^2\right)}\left(\frac{b_1}{\left(a_1^2 - 2b_1^2\right)}\right)\sqrt{2} \in Q\sqrt{2}$ s.t $xx^{-1} = x^{-1}x = 1$ then $\left(Q\sqrt{2},+,\cdot\right)$ is field.

Note: Similarly $Q\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \mid a,b \in Q\right\}, d > 0$ and d is not perfect square then $Q\left[\sqrt{d}\right]$ is field.

Q. $\mathbf{R}[2]$ is field?

Ans. Yes. Note: $\mathbf{R}\left[\sqrt{d}\right] = \mathbf{R}, d > 0$ and d is not perfect square then it is field.

Q. Construct $Z\left[\sqrt{d}\right]$?

Solution: $Z\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \mid a,b \in Z\right\}$ is integral domain but not field because $3 \in \left[\sqrt{d}\right]$ but $3^{-1} = \frac{1}{3} \notin Z\left[\sqrt{d}\right]$ then $Z\left[\sqrt{d}\right]$ is not field.

Q. $Z\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a,b \in Z\right\}$, how many unit in $Z\left[\sqrt{2}\right]$?

Solution: $\left(\sqrt{2}-1\right) \in Z\left[\sqrt{2}\right]$, $\left(\sqrt{2}+1\right) \in Z\left[\sqrt{2}\right]$

such that $\left(\sqrt{2}-1\right)\left(\sqrt{2}+1\right) = 1$ then $\sqrt{2}-1$ is unit similarly $\sqrt{2}+1$ is unit.

squaring equation (1)

$\left(\sqrt{2}-1\right)^2\left(\sqrt{2}+1\right)^2 = 1^2$

$\left(3-2\sqrt{2}\right)\left(3+2\sqrt{2}\right) = 1 \Rightarrow 3-2\sqrt{2}$ and $3+2\sqrt{2}$ is also unit

$\therefore Z\left[\sqrt{2}\right]$ has infinite units.

Mindset Makers

Q. $Z\left[\sqrt{3}\right]=\left\{a+b\sqrt{3}\mid a,b\in Z\right\}$, how many units?

Solution: $\left(2+\sqrt{3}\right)\in Z\left[\sqrt{3}\right]$, $\left(2-\sqrt{3}\right)\in Z\left[\sqrt{3}\right]$

$\left(2+\sqrt{3}\right)\left(2-\sqrt{3}\right)=1$ ....(1)

Here $2+\sqrt{3}$ and $2-\sqrt{3}$ are units

Again, squaring equation (1); $\left(2+\sqrt{3}\right)^2\left(2-\sqrt{3}\right)^2=1$

$Z\left[\sqrt{3}\right]$ has infinite units.

Q. $R=Z\left[\sqrt{5}\right]$, how many units?

Ans. Infinite

CHAPTER-2

Idempotent Element: Let $(R,+,\cdot)$ be a ring then an element $a\in R$ is said to be idempotent element of R if $a^2=a$. Special point to notice here that square doesn't mean multiplication, it means composition two times. So we must take care of it.

Q. $R=Z$, how many idempotent elements in R?

Solution: $Z=\{0,\pm1,\pm2\pm....\}$

$0\in Z$ s.t $0^2=0$, $1\in Z$ s.t $1^2=1$

so there are only 2 idempotent elements in R i.e. 0 and 1.

Q. How many idempotent elements in $Q,\mathbf{R},\mathbf{C},Z_{11}\left[i\right]$?

Q. $R=Z_6$, how many idempotent elements?

Solution: $R=Z_6=\{0,1,2,3,4,5\}$

$0\in Z_6$ s.t $0^2=0$, $1\in Z_6$ s.t $1^2=1$, $3\times Z_6$ s.t $3^2=9=3 \pmod 6$, $4\in Z_6$ s.t $4^2=16=4 \pmod 6$

then 0,1,3,4 are Idempotent elements in R i.e. exactly four Idempotent elements.

Q. How many Idempotent element in Z_{256}?

Solution: $n=256$, no of Prime divisors of $n=1$ i.e. 2 then

No. of Idempotent elements in $Z_{256}=2^1=2$ they are 0 and 1 only.

Q. How many Idempotent elements in Z_{30}?

Mindset Makers

Solution: $Z_{30}=\{0,1,2,....29\}$

$0\in Z_{30}$ s.t $0^2=0, 1\in Z_{30}$ s.t $1^2=1, 6\in Z_{30}$ s.t $6^2=36=6 \pmod{30}$

$10\in Z_{30}$ s.t $10^2=100=10 \pmod{30}, 15\in Z_{30}$ s.t $15^2=225=15 \pmod{30}$

$16\in Z_{30}$ s.t $16^2=296=16 \pmod{30}, 21\in Z_{30}$ s.t $21^2=441=21 \pmod{30}$

$25\in Z_{30}$ s.t $25^2=625=25 \pmod{30}$

Hence, 0,1,6,10,15,16,21 and 25 are Idempotent elements in Z_{30} i.e. 8 Idempotent elements exactly.

Note: Matrix concept is used if A is idempotent then I-A is also idempotent where A be any square matrix or order *n*.

Q. How many idempotent elements in Z_{20}?

Solution: $0^2=0, 1^2=1, 5^2=5, 16^2=16$

hence, 0,1,5 and 16 are Idempotent elements in Z_{20} i.e. exactly 4 idempotent elements.

Exam Point: No. of Idempotent elements in $Z_n=2^d$ where *d* is the number of Prime divisors of *n*.

e.g. $R=Z_{30}$, then how many Idempotent elements.

Prime divisor of 30 are 2, 3 and 5

Number of Idempotent element in $Z_{30}=2^3=8$

Q. $R=Z_8$, how many Idempotent elements in Z_8.

Solution: $n=8$, No. of Prime divisor of $n=1$ say (2) then

Number of Idempotent elements in $Z_8=2^1=2$

Q. Show that if a is idempotent element in R then $1-a$ is also Idempotent.

Solution: Let $(R,+,\cdot)$ is a ring and $a\in R$ is Idempotent element then $a^2=a$ ....(1)

Now, $(1-a)^2=1^2+a^2-2a=1+a-2a \ (\because a^2=a)=1-a \therefore (1-a)^2=(1-a)$

$\Rightarrow 1-a$ is also an Idempotent element in R.

Q. If R is Integral domain then R has exactly two idempotent elements.

Solution: Let $(R,+,\cdot)$ be an Integral domain if

$a\cdot b=0\Rightarrow a=0$ or $b=0 \ \ a,b\in R$ ....(1)

Let $x\in R$ is an idempotent element of R then $x^2=x$

$\Rightarrow x^2-x=0\Rightarrow x(x-1)=0\Rightarrow x=0$ or $x-1=0\Rightarrow$ If $x=0$ then 0 is Idempotent element in R

If $x-1=0$ then $x=1$ is Idempotent element in R.

Since R is an Integral domain then 0 and 1 both are Idempotent elements.

Q. How many Idempotent elements in $Z, Q, \mathbf{R}, \mathbf{C}, Z_p\left(Z_p[i] \text{where } 4\mid p-3\right)$, $Q\times\{0\}, \mathbf{R}\times\{0\}, \mathbf{C}\times\{0\}$.

Solution: All of these has exactly two idempotent elements.

Q. How many Idempotent elements in $Z_{23}[i]$?

Solution: Here $Z_{23}[i]$ and $4\mid 23-3$, then exactly 2 Idempotent elements.

Q. How many Idempotent elements in $Z_2\times Z_4$?

Mindset Makers

Solution: $Z_2 \times Z_4 = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3)\}$

$(0,0) \in Z_2 \times Z_4$ s.t $(0,0)^2 = (0,0)$, $(0,1) \in Z_2 \times Z_4$ s.t $(0,1)^2 = (0,1)$

$(1,0) \in Z_2 \times Z_4$ s.t $(1,0)^2 = (1,0)$, $(1,1) \in Z_2 \times Z_4$ s.t $(1,1)^2 = (1,1)$

Q1. How many Idempotent elements in $Z_{10} \times Z_6$?

Q2. How many Idempotent elements in $Z_3[i] \times Z_7[i]$?

Solution:

(1) $R = Z_{10} \times Z_6$

Now, Idempotent element in $Z_{10} = \{0,1\} = 2^2$

Idempotent element in $Z_6 = \{0,1\} = 2^2$

Idempotent element in $Z_{10} \times Z_6 = 2^2 \times 2^2 = 16$

(2) Idempotent elements in $Z_3[i] \times Z_7[i] = 2 \times 2 = 4$

BOOLEAN RING

A ring $(R,+,\cdot)$ is said to be Boolean ring if $x^2 = x,\ \forall x \in R$

Q. $R = Z_2$ is Boolean Ring?

Solution: $Z_2 = \{0,1\}$, here $0 \in Z_2$ s.t $0^2 = 0$, $1 \in Z_2$ s.t $1^2 = 1$

Q. Give example of Boolean ring of order 4 and ∞.

Ans. Boolean Ring of order 4:

$R = Z_2 \times Z_2 = \{(0,0),(0,1),(1,0),(1,1)\}$

$(0,0) \in Z_2 \times Z_2$ s.t $(0,0)^2 = (0,0)$

$(0,1) \in Z_2 \times Z_2$ s.t $(0,1)^2 = (0,1)$

$(1,0) \in Z_2 \times Z_2$ s.t $(1,0)^2 = (1,0)$

$(1,1) \in Z_2 \times Z_2$ s.t $(1,1)^2 = (1,1)$

Boolean Ring of order ∞; $R = Z_2 \times Z_2 \times Z_2 \times Z_2 \times .....\infty$ is Boolean Ring of order ∞

NILPOTENT ELEMENTS

An element $a \in R$ is Nilpotent element of R if $a^n = 0$ for some n.

Q. How many Nilpotent elements in Z?

Solution: $Z = \{0, \pm 1, \pm 2, ...\}$

$0 \in Z$ such that $0^1 = 0$

$0 \neq a \in Z$ then a is not nilpotent element of Z then Z has exactly one element.

Similarly $Q, \mathbf{R}, \mathbf{C}, Z_p$ has exactly one Nilpotent element.

Q. How many nilpotent elements in Z_6?

Solution: $Z_6 = \{0,1,2,3,4,5\}$, $0 \in Z_6$ such that $0^1 = 0$

then 0 is the only Nilpotent element of Z_6

$5 \in Z_6 \Rightarrow 5^2 = 25 = 1, 5^3 = 5, 5^4 = 1$

Q. How many Nilpotent element in Z_8?

Mindset Makers

Solution: $Z_8 = \{0,1,2,3,4,5,6,7\}$

$0 \in Z_6$ s.t $0^1 = 0$, $2 \in Z_6$ s.t $2^3 = 8 = 0 \pmod 8$

$4 \in Z_6$ s.t $4^2 = 16 = 0 \pmod 8$, $6^3 \in Z_6$ s.t $6^3 = 216 = 0 \pmod 8$

exactly 4 nilpotent elements they are 0,2,4 and 6 in Z_8.

Q. How many Nilpotent element in Z_{512}?

Solution: $R = Z_{512}$, $n = 2^9 = 512$

number of Nilpotent elements in $Z_{512} = 2^{9-1} = 2^8 = 256$

Note: If $n = p_1^{r_1} \times p_2^{r_2} \ldots\ldots \times p_k^{r_k}$, then number of Nilpotent elements in $Z_n = p_1^{r_1-1} \times p_2^{r_2-1} \ldots\ldots \times p_k^{r_k-1}$, p is prime.

Q. $R = Z_8$, how many nilpotent elements?

Solution: $R = Z_8$ $n = 8 = 2^3$. number of nilpotent elements in $Z_8 = 2^{3-1} = 2^2 = 4$

Q. $R = Z_{12}$, how many nilpotent elements?

Solution: $R = Z_{12}$, $n = 12 = 2^2 \times 3$. Number of nilpotent elements in $Z_{12} = 2^{2-1} \times 3^{1-1} = 2 \times 1 = 2$

Q. $R = Z_{30}$, how many nilpotent elements in R?

Solution: $R = Z_{30}$, $n = 30 = 2 \times 3 \times 5$

Number of Nilpotent elements in $Z_{30} = 2^{1-1} \times 3^{1-1} \times 5^{1-1} = 1 \times 1 \times 1 = 1$

then 0 is the only Nilpotent elements.

Exam Point: If $n = p_1^{r_1} \cdot p_2^{r_2} \ldots\ldots p_k^{r_k}$ then Nilpotent elements $= \langle p_1 \times p_2 \ldots\ldots \times p_k \rangle$

e.g. (i) Nilpotent elements in $Z_{48} = Z_{2^4 \times 3} = \langle 6 \rangle = \{0,6,12,18,24,30,36,42\}$

(ii) Nilpotent elements in $Z_{16} = Z_{2^4 = \langle 2 \rangle} = \{0,2,4,6,8,10,12,14\}$ generated by $\langle 2 \rangle$.

Q. If R is an Integral domain the R has exactly one nilpotent element.

Solution: Let $(R, +, \cdot)$ be integral domain and $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$ ....(1)

Let $x \in R$ and x is nilpotent then

$x^n = 0$ for some $n \Rightarrow x \cdot x^{n-1} = 0$

$\Rightarrow x = 0$ or $x^{n-1} = 0$ [By definition of Integral Domain]

If $x = 0$ then only 0 is the Nilpotent element

If $x \neq 0$ then $x^{n-1} = 0$ i.e. $\Rightarrow x \cdot x^{n-2} = 0 \Rightarrow x = 0$ or $x^{n-2} = 0$

If $x = 0$ then 0 is the nilpotent element

If $x \neq 0$ then $x^{n-2} = 0$ and we continue the above process until we get $x = 0$.

Then, R has exactly one nilpotent element i.e. 0

Example:

$R = Z, Q, \mathbf{R}, \mathbf{C}, Z[i], Z_p, Z_p[i]_{4|p-3}$ $Q \times \{0\}, Z \times \{0\}, \mathbf{R} \times \{0\}, \times \mathbf{C} \times \{0\}, Z_p \times \{0\}$ $Z_3[i] \times \{0\}$ has exactly one nilpotent element.

Units: An element $a \in R$ is said to be Unit element of R if 'a' has multiplicative inverse in R. The set of all units of R is denoted by $U(R)$.

Example: (i) $R = Z$, then find $U(Z)$?

$Z = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$. $U(Z) = \{1, -1\}$

Mindset Makers

(ii) $R=Q$ then find $U(Q)$?. $U(Q)=Q-\{0\}=Q^*$

(iii) $R=\mathbf{R}$, find $U(\mathbf{R})$?. $U(\mathbf{R})=\mathbf{R}-\{0\}=R^*$

(iv) $R=Z[i]$, find $U(Z[i])$? . $U(Z[i])=\{\pm 1,\pm i\}$

(v) $U(\mathbf{C})=\mathbf{C}-\{0\}=\mathbf{C}^*$

(vi) $U(\mathbf{R}[i])=\mathbf{C}^*$

(vii) $U(Q[i])=Q[i]-\{0\}=Q[i]^*$

(viii) $U(Q\times\{0\})=Q\times\{0\}-\{(0,0)\}=(Q\times\{0\})^*$

$U(\mathbf{R}\times\{0\})=\mathbf{R}\times\{0\}-\{(0,0)\}=(\mathbf{R}\times\{0\})^*$

$U(\mathbf{C}\times\{0\})=\mathbf{C}\times\{0\}-(0,0)=(\mathbf{C}\times\{0\})^*$

Q. Find $U(Q\times Q)$?

Solution: $U(Q\times Q)=Q^*\times Q^*=U(Q)\times U(Q)$

Q. $R=Z_{15}$, find $U(Z_{15})$?

Solution:

$U(Z_{15})=\{1,2,4,7,8,11,13,14\}$

all the elements of Z_{15} which are relatively prime with 15 i.e. in $Z_{15}=(Z_{15})^*=U(15)$

Q. $R=Z_{10}$, find $U(Z_{10})$?

Solution: $U(Z_{10})=\{1,3,7,9\}$

Note: No. of Units in $Z_n=\phi(n)$

Q. Find $U(Z_3[i])$?

Solution: $Z_3[i]=\{0,1,2,i,2i,1+i,1+2i,2+i,2+2i\}$

$U(Z_3[i])=\{1,2,i,2i,1+i,1+2i,2+i,2+2i\}=Z_3[i]-\{0\}=(Z_3[i])^*$

Note: $R=Z_p[i]$, $4\mid p-3$ then $U(Z_p[i])=Z_p[i]-\{0\}=(Z_p[i])$

Q. $U(Z_3[i]\times Z_7[i])=?$

Q. $U(Z_5\times Z_{10})=U(Z_5)\times U(Z_{10})=Z_5^*\times Z_{10}^*$

Note: If each R_i is commutative ring with unity

$U(R_1\times R_2\times R_3\times....\times R_n)=U(R_1)\times U(R_2)\times....\times U(R_n)$

Q. $R=Z_3[i]=\{a+ib\mid a,b\in Z_3\}=\{0,1,2,i,2i,1+i,1+2i,2+i,2+2i\}$

$(Z_3[i]^*,\cdot)$ is a group?

Now, $Z_3[i]^*=Z_3[i]-\{0\}=\{1,2,i,2i,1+i,1+2i,2+i,2+2i\}$

Solution:(1) Closure Property: $\forall a\in Z_3[i]-\{0\}=Z_3[i]^*$

$\forall b\in Z_3[i]-\{0\}=Z_3[i]^*\Rightarrow a\cdot b\in Z_3[i]-\{0\}=Z_3[i]^*$

(2) Associative: $a\cdot(b\cdot c)=(a\cdot b)\cdot c,\forall a,b\in Z_3[i]^*$

Mindset Makers

(3) Identity: $\forall a \in Z_3[i]^* \exists 1 \in Z_3[i]^*$ s.t. $a \cdot 1 = 1 \cdot a = a$

(4) Inverse of each element of $Z_3[i]^*$

$1^{-1} = 1, 2^{-1} = 2, i^{-1} = 2i, 2i^{-1} = i$

$(1+i)^{-1} = 2+i$, $(1+2i)^{-1} = 2+2i$, $(2+i)^{-1} = (1+i)$, $(2+2i)^{-1} = (1+2i)$

$\therefore \left(Z_3[i]^*, \cdot\right)$ is a group of order 8.

If

$O(G) = 8$ $\begin{cases} Z_8 \\ Z_2 \times Z_4 \\ Z_2 \times Z_2 \times Z_2 \\ D_4 \times \\ Q_4 \times \end{cases}$

which mean Integral domain.

$Z_3[i]$ is commutative ring with unity, i.e. $ab = ba, \forall a, b \in Z$ and $Z_3[i]^* \subseteq Z_3[i]$ and since $Z_3[i]$ is abelian so its subset is also abelian hence $Z_3[i]^*$ must be abelian.

Now,

$O(Z_3[i]^*) = 8$ $\begin{cases} Z_8 \surd \\ Z_2 \times Z_4 \times \\ Z_2 \times Z_2 \times Z_2 \times \\ D_4 \times \\ Q_4 \times \end{cases}$

$Z_3[i]^* \not\approx D_4$ or Q_4 because $Z_3[i]^*$ is an integral domain.

Now,

$(1+i) \in Z_3[i]^*$ s.t $0(1+i) = ?$

$(1+i)^2 = (1+i)(1+i) = 2i$

$(1+i)^4 = 2i \times 2i = -4 = -1 \pmod 3$

$(1+i)^8 = -1 \times -1 = 1 \Rightarrow 0(1+i) = 8$

hence $\boxed{Z_3[i]^* \approx Z_8}$

Q. $(Z_3[i], +)$ is group?

Solution: $Z_3[i]$ is an Integral domain then $(Z_3[i], +)$ is commutative group of order 9.

Now $Z_3[i] = \{0, 1, 2, 1+i, 1+2i, 2+i, 2+2i, i, 2i\}$

$0(Z_3[i]) = 9$ $\begin{cases} Z_9 \\ Z_3 \times Z_3 \end{cases}$ here we work under addition

$o(0) = 1, o(1) = 3, o(2) = 3, o(i) = 3 \Rightarrow 3i \pmod 3 = 0i = 0$

Mindset Makers

$0(2i)=(2i+2i+2i=6i=0(\text{mod}\,3))=3$

therefore,

$O(0)=1, O(1)=3, O(2)=3, O(i)=3$

$O(2i)=3, O(1+i)=3, O(1+2i)=3, O(2+i)=3\ O(2+2i)=3$

$Z_3[i]$ has no elements of order 9 then $\therefore \boxed{Z_3[i]\approx Z_3\times Z_3}$

Q. $(Z_5[i]-\{0\},\cdot)$ is a group?

Solution: $(2+i)\in Z_5[i]-\{0\}$

$(2+4i)\in Z_5[i]-\{0\}$ But $(2+i)(2+4i)=0$ and $0\notin Z_5[i]-\{0\}$

Hence, $(Z_5[i]-\{0\},\cdot)$ is not a group.

Note: $(Z_p[i]-\{0\},\cdot)$ is group if $4\mid p-3$ where p is prime and of order p^2-1.

Q. $R=Z_7$ is an Integral domain then $(Z_7-\{0\},\cdot)$ is group?

Solution: $Z_7-\{0\}=Z_7{}^*=\{1,2,3,4,5,6\}=U(7)\approx Z_6$

modulo 7 applied here

$1\in Z_7^*, O(1)=1, 2\in Z_7^*, Q(2)=3, 3\in Z_7^*, O(3)=6$ then $(Z_7-\{0\},\cdot)=Z_7^*\approx Z_6$

Q. $R=Z_7[i]$ is an Integral domain

(i) $(Z_7[i]^*,\cdot)\approx ?$

(ii) $(Z_7[i],+)\approx ?$

<u>Subring</u>: Let $\phi\neq S\subseteq R, (S,+,\cdot)$ is subring of $(R,+,\cdot)$ if

(i) $\forall a\in S, \forall b\in S\Rightarrow a-b\in S$ [condition of subgroup S is subgroup]

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

Q. $(Z,+,\cdot)$ is subring of $(Q,+,\cdot)$?

Solution: $\phi\neq Z\subseteq Q$ and $(Z,+,\cdot)$ is ring then $(Z,+,\cdot)$ is subring of $(Q,+,\cdot)$.

Similarly, Z is subring of $\mathbf{R},\mathbf{C}$, Q- is subgroup of $\mathbf{R},\mathbf{C}$, $\mathbf{R}$ is subring of $\mathbf{C}$.

Q. Show that $S=\{0\}$ and $S=R$ always subring of R.

Solution: Let $(R,+,\cdot)$ be a ring

Case I: $S=\{0\}$ is subring of R then

(i) $\forall a\in S, \forall b\in S\Rightarrow a-b\in S$; $(0-0=\in\{0\}=S)$

(ii) $\forall a\in S, \forall b\in S\Rightarrow a\cdot b\in S(0\cdot 0=0\in\{0\}=S)$

Case II: If $S=R$

(i) $\forall a\in S, \forall b\in S\Rightarrow a-b\in R=S\Rightarrow a-b\in S$

(ii) $\forall a\in S, \forall b\in S\Rightarrow a\cdot b\in R=S\Rightarrow a\cdot b\in S$

From care I and II

$S=\{0\}$ and $S=R$ are always subring of R. [Proved]

Mindset Makers

Q. $S = 2Z$ is subring of Z?

Solution: $Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$, $2Z = \{0, \pm 2, \pm 4, \pm 6, ...\}$

$\phi \neq 2Z \subseteq Z$; $(2Z, +, \cdot)$ is subring of $(Z, +, \cdot)$ because 2Z itself is a ring.

(i) $\forall a \in 2Z, \forall b \in 2Z \Rightarrow a - b \in 2Z$ (2Z is subgroup of Z)

(ii) $\forall a \in 2Z, \forall \in 2Z \Rightarrow a \cdot b \in 2Z$

Q. mZ is subring of Z?

Solution: mZ is subring of Z because

(i) $\forall a \in mZ, \forall b \in mZ \Rightarrow a - bmZ$

(ii) $\forall a \in mZ, \forall b \in mZ \Rightarrow a \cdot b \in mZ$

hence, mZ is subring of Z.

Q. Find subring of Z_6 ?

Solution: $Z_6 = \{0, 1, 2, 3, 4, 5\}$

Subgroup of Z_6: $S_1 = \{0\}, S_2 = Z_6, S_3 = \{0, 2, 4\}$, $S_4 = \{0, 3\}$

$S_1 = \{0\}$ and $S_2 = Z_6$ are always subring of Z_6 by the theorem.

$S_3 = \{0, 2, 4\}$

(i) Since S_3 is a subgroup of Z_6, i.e.

$\forall a \in S_3, \forall b \in S_3 \Rightarrow a - b \in S_3$

(ii)

	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

From table, $\forall a \in S_3, \forall b \in S_3 \Rightarrow a \cdot b \in S_3$ then S_3 is also a subring of Z_6.

$S_4 = \{0, 3\}$

(i) Since S_4 is a subgroup of Z_6 i.e.

$\forall a \in S_4, \forall b \in S_4 \Rightarrow a - b \in S_4$

(ii)

	0	3
0	0	0
3	0	3

From table, $\forall a \in S_4, \forall b \in S_4 \Rightarrow a \cdot b \in S_4$

Thus, S_4 is also a subring of Z_6

Hence, Z_6 has exactly 4 subrings.

Q. $R = Z_{20}$, how many subrings in R?

Exam Point: Number of subrings in $Z_n = \tau(n)$

Q. $R = M_2(\mathbf{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbf{R} \right\}$ is a_n integral domain?

Mindset Makers

Solution: No, $M_2(\mathbf{R})$ is not commutative ring, then $M_2(\mathbf{R})$ not integral domain.

If $n=1$ then it is commutative ring with unity hence an integral domain.

Note: (i) $M_2(\mathbf{R})$ is a ring with unity but not commutative hence not Integral domain.

(ii) $2Z$ is commutative ring but not unity hence not an integral domain.

(iii) $R=\{0\}$ is also commutative ring without unity so not an integral domain.

Q. $R=M_2(\mathbf{R})=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}\middle| a,b,c,d\in\mathbf{R}\right\}$ and $S=\left\{\begin{bmatrix}a & 0\\ c & 0\end{bmatrix}\middle| a,c\in\mathbf{R}\right\}$, S is subring of $M_2(\mathbf{R})$?

Solution: $\phi\neq S\subset M_2(\mathbf{R})$

(i) $\forall\ A=\begin{bmatrix}a_1 & 0\\ c_1 & 0\end{bmatrix}\in S, \forall B=\begin{bmatrix}a_2 & 0\\ c_2 & 0\end{bmatrix}\in S \Rightarrow A-B=\begin{bmatrix}a_1 & 0\\ c_1 & 0\end{bmatrix}\begin{bmatrix}a_2 & 0\\ c_2 & 0\end{bmatrix}$

$\Rightarrow A-B=\begin{bmatrix}a_1-a_2 & 0\\ c_1-c_2 & 0\end{bmatrix}\in S\ [\because a_1\in\mathbf{R}, c_1\in\mathbf{R}, a_1-a_2\in\mathbf{R}]$

(ii) $\forall A=\begin{bmatrix}a_1 & 0\\ c_1 & 0\end{bmatrix}\in S,\ B=\begin{bmatrix}a_2 & 0\\ c_2 & 0\end{bmatrix}\in S$

$A\cdot B=\begin{bmatrix}a_1 & 0\\ c_1 & 0\end{bmatrix}\begin{bmatrix}a_2 & 0\\ c_2 & 0\end{bmatrix}=\begin{bmatrix}a_1a_2 & 0\\ c_1a_2 & 0\end{bmatrix}\in S$

$S=\left\{\begin{bmatrix}a & 0\\ c & 0\end{bmatrix}\middle| a,c\in\mathbf{R}\right\}$ is a subring of $M_2(\mathbf{R})$.

Q. $R=M_2(\mathbf{R})=\left\{\begin{bmatrix}a & b\\ c & a\end{bmatrix}\middle| a,b,c,d\in\mathbf{R}\right\}$ and $S=\left\{\begin{bmatrix}0 & b\\ 0 & 0\end{bmatrix}\middle| b\in\mathbf{R}\right\}$ is a subring of $M_2(\mathbf{R})$

Solution: $\phi\neq S\subseteq R$

(i) Let $A=\begin{bmatrix}0 & b_1\\ 0 & 0\end{bmatrix}\in S,\ B=\begin{bmatrix}0 & b_2\\ 0 & 0\end{bmatrix}\in S,\ A-B=\begin{bmatrix}0 & b_1-b_2\\ 0 & 0\end{bmatrix}\in S$

And (ii) $A\cdot B=\begin{bmatrix}0 & b_1\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & b^2\\ 0 & 0\end{bmatrix}\Rightarrow A\cdot B=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\in S$

$\therefore S$ is subring of R. i.e. $S=\left\{\begin{bmatrix}0 & b\\ 0 & 0\end{bmatrix}\middle| b\in\mathbf{R}\right\}$ is subring or $M_2(\mathbf{R})$.

Sum of two subrings: Let A and B are two subrings of R then the sum of A and B is defined by

$A+B=\{a+b\mid a\in A, b\in B\}$

Q. (i) Intersection of two subrings of R is a subring of R?

(ii) Union of two subring of R is a subring of R?

(iii) Sum of two subrings of R is a subring of R?

Solution:(iii) $A=\begin{bmatrix}a & 0\\ c & 0\end{bmatrix}$ is subring of $M_2(\mathbf{R})$ and $B=\begin{bmatrix}0 & b\\ 0 & 0\end{bmatrix}$ is subring of $M_2(\mathbf{R})$

Mindset Makers

then $A+B=\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$

Now, $A_1=\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\in A+B, B_1=\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}\in A+B.\ A_1B_1=\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}=\begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix}\notin A+B$

Hence Sum of two subrings need not be a subring.

Q. $4\,|\,2$ in Z_6?

Solution: If $a\,|\,b$ then $\exists x$ such that $b=ax$

If $4\,|\,2$ then $\exists x\in Z_6$ s.t $2=4x$ i.e. $4x\equiv 2(\mathrm{mod}\,6)$ ....(1)

$\gcd(4,6)=2$ and 2|2 then $4x\equiv 2(\mathrm{mod}\,6)$ then it has 2 solutions.

$$ca\equiv cb(\mathrm{mod}\,n)\Rightarrow a\equiv b\left(\mathrm{mod}\,\frac{n}{\gcd(c,n)}\right)$$

Put $x=2$, then ; $4\cdot 2\equiv 8\equiv 2(\mathrm{mod}\,6)$

Put $x=5$, then ; $4\cdot 5\equiv 20\equiv 2(\mathrm{mod}\,6)$

$x=2$ and $x=5$ are solutions of $4x\equiv 2(\mathrm{mod}\,6)$

Q. 7|3 in Z_8?

Solution: Yes, 7|3 in Z_8

$7x\equiv 3(\mathrm{mod}8),\ x\equiv 7^{-1}3(\mathrm{mod}8)\Rightarrow x\equiv 7.3(\mathrm{mod}8)\Rightarrow x\equiv 21(\mathrm{mod}8)\Rightarrow x\equiv 5(\mathrm{mod}8)$

then $x=5$ is solution of $7x\equiv 3(\mathrm{mod}8)$.

Ideal:

(i) Left Ideal: Let $\phi\neq I\subset R$ then $(I,+,\cdot)$ is called Left Ideal of R if

(1) $\forall a\in I,\forall b\in I\Rightarrow a-b\in I$

(2) $\forall a\in I,\forall r\in R\Rightarrow ra\in I$

(ii) Right Ideal: Let $\phi\neq I\subset R$ then $(I,+,\cdot)$ is said to be right ideal of R if

(1) $\forall a\in I,\ \forall b\in I\Rightarrow a-b\in I$

(2) $\forall a\in I,\ \forall r\in R\Rightarrow ar\in I$

Ideal: Let $\phi\neq I\subset R,(I,+,\cdot)$ is an Ideal of R if

(1) $\forall a\in I,\forall b\in I\Rightarrow a-b\in I$

(2) $\forall a\in I,\forall r\in R\Rightarrow ra\in I$ and $ar\in I$

Q. Z is an ideal of Q?

Solution: No. $2\in Z,\ \frac{1}{3}\in Q$ but $\frac{2}{3}\notin Z$ then Z is not ideal of Q.

Q. Q is an ideal in $\mathbf{R}$?

Solution: No, $2\in Q,\ \sqrt{2}\in\mathbf{R}$ but $2\sqrt{2}\notin Q$

Q. $\mathbf{R}$ is an ideal in $\mathbf{C}$?

Solution: $2\in\mathbf{R}, i\in\mathbf{C}$, then $\mathbf{R}$ is not an ideal of $\mathbf{C}$.

Q. Show that $I=\{0\}$ and $I=R$ are always Ideal of R.

Mindset Makers

Solution:(i) Let $I=\{0\}$

(i) $\forall a\in I,\forall b\in I\Rightarrow a-b\in I$

(ii) $\forall a\in I,\forall r\in R\Rightarrow a\cdot r=0=r\cdot a\in I$ then $I=\{0\}$ is an ideal of R

(2) Let $I=R$

(i) $\forall a\in I,\forall b\in I\Rightarrow a-b\in R=I$

(ii) $\forall a\in I,\forall r\in R\Rightarrow ra\in R=I$ and $a\cdot r\in R=I$.

Hence $I=R$ is an ideal of R.

Q. $I=2Z$ is an ideal of Z?

Solution: $\phi\neq 2Z\subset Z$

(i) $\forall a\in 2Z,\forall b\in 2Z\Rightarrow a-b\in 2Z$

(ii) $\forall a\in 2Z,\forall r\in Z\Rightarrow ra=ar\in 2Z$

then $2Z$ is an ideal of Z.

Exam point- Similarly, mZ is an ideal of Z.

Q. Show that every ideal of R is subring of R but converse need not be true?

Solution: Let I be an Ideal of R then

(i) $\forall a\in I,\forall b\in I\Rightarrow a-b\in I$

(ii) $\forall a\in I,\forall r\in R\Rightarrow ra\in I$ and $ar\in I$

Now,

(i) $\forall a\in I,\forall b\in I\Rightarrow a-b\in I$ ($\because I$ is an ideal)

(ii) $\forall a\in I,\forall b\in I\subseteq R\Rightarrow a\cdot b\in I$ and $b\cdot a\in I$ then, I is subring of R.

Converse need not be true

Z is a subring of $\mathbf{R}$ but not ideal of $\mathbf{R}$ because $3\in Z,\sqrt{5}\in\mathbf{R}$ but $3\sqrt{5}\notin Z$

Q. Z is an ideal of $Z[i]$?

Solution: No, $3\in Z,i\in Z[i]$ but $3i\notin Z$ then Z is not ideal in $Z[i]$

Q. $Z[i]$ is an ideal of $\mathbf{C}$

Solution :No, $2\in Z[i],\frac{1}{3}\in\mathbf{C}$ but $\frac{2}{3}\notin Z[i]$ then $Z[i]$ is not ideal in $\mathbf{C}$

Q. If I is an ideal of R and $1\in I$ then $I=R$

Solution: Let I is an ideal of R then $I\subseteq R$ ....(1)

Now, $1\in I,r\in R\Rightarrow r\cdot 1\in I$ because I is ideal $\Rightarrow r\in I$

$\Rightarrow R\subset I$ ....(2)

From equation (1) and (2), $I=R$

Q. $R=Z_8$, find Ideal of Z_8 ?

Solution: $Z_8=\{0,1,2,3,4,5,6,7\}$

Subring of Z_8 are

$I_1=\{0\},I_2=Z_8,I_3=\{0,2,4,6\}=\langle 2\rangle$, $I_4=\{0,4\}=\langle 4\rangle$

here $I_1=\{0\}$ and $I_2=Z_8$ are always Ideal of R

Now, $I_3=\{0,2,4,6\}$ is an Ideal because

(i) $a\in I_3,\forall b\in I_3\Rightarrow a-b\in I_3$

Mindset Makers

(ii) $\forall a \in I_3, \forall r \in Z_8 \Rightarrow ra = ar \in I_3$

then I_3 is an Ideal in Z_8. Similarly, I_4 is also an ideal in Z_8. Hence, Z_8 has exactly 4 ideals.

Q. $R = Z_{10}$ how many ideal?

Solution: No. of ideals in $Z_{10} = \tau(10) = (1+1)(1+1) = 4$

Exam Point: No. of Ideal in $Z_n = \tau(n)$

Q. (i) $S = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \middle| a,b \in \mathbf{R} \right\}$ is a subring of $M_2(\mathbf{R})$?

(ii) $S = \left\{ \begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \middle| a,b \in \mathbf{R} \right\}$ is a subring of $M_2(\mathbf{R})$

Give the example of a subset of ring that is subgroup under addition but not subring.

Solution: (i) and (iii)

$$S = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \middle| a,b \in \mathbf{R} \right\} \subseteq M_2(\mathbf{R})$$

(1) Let $A = \begin{bmatrix} a_1 & a_1+b_1 \\ a_1+b_1 & b_1 \end{bmatrix} \in S$, $B = \begin{bmatrix} a_2 & a_2+b_2 \\ a_2+b_2 & b_2 \end{bmatrix} \in S$

$$A-B = \begin{bmatrix} a_1 & a_1+b_1 \\ a_1+b_1 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & a_2+b_2 \\ a_2+b_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1-a_2 & (a_1+b_1)-(a_2+b_2) \\ (a_1+b_1)-(a_2+b_2) & b_1-b_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1-a_2 & (a_1-a_2)+(b_1-b_2) \\ (a_1-a_2)+(b_1-b_2) & b_1-b_2 \end{bmatrix} \Rightarrow A-B \in S$$ then S is subgroup of $M_2(\mathbf{R})$ under addition.

(2) Let $A = \begin{bmatrix} 1 & 1+0 \\ 1+0 & 0 \end{bmatrix} \in S$, $B = \begin{bmatrix} 2 & 2+0 \\ 2+0 & 0 \end{bmatrix}$; $A \cdot B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} \Rightarrow A \cdot B = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \notin S$

Hence S is not subring of $M_2(\mathbf{R})$ as the (2) condition not satisfied.

Q. $R = Z \times Z \times Z$ and $S = \{(a,b,c) \mid a+b = c, a,b,c \in z\}$. S is subring of R? S is ideal of R?

Solution: $a = (1,0,1) \in S$, $b = (0,1,1) \in S$; $a \cdot b = (1,0,1)(0,1,1) = (0,0,1) \notin S$

S is not subring of $Z \times Z \times Z$ then S is not Ideal of $Z \times Z \times Z$.

Q. $R = (Z_{100}, +, \cdot)$, how many ideal in R?

Solution: No. of Ideals in $Z_{100} = \tau(100) = 2^2 \times 5^2 = (2+1)(2+1) = 3 \times 3 = 9$

Q. If $\mathbf{F}$ is field then $\mathbf{F}$ has exactly two ideals.

Solution: Let $\mathbf{F}$ be a field then each non-zero element of $\mathbf{F}$ has multiplicative iverse.

Let $I = \{0\}$ is an ideal of $\mathbf{F}$ [Because $\{0\}$ and itself is always ideal of R]

Now, consider I is an ideal of $\mathbf{F}$ and $I \neq \{0\}$

Then, $\exists\, 0 \neq a \in I$ if $a \in I$ then $a \in \mathbf{F} \Rightarrow a^{-1}$ also exists because a is non-zero member of $\mathbf{F}$ i.e. $0 \neq a \in \mathbf{F}$

$0 \neq a \in I, a^{-1} \in \mathbf{F} \Rightarrow aa^{-1} \in I$ [because I is an ideal of $\mathbf{F}$] $\Rightarrow 1 \in I$

Now, $1 \in I$ and I is a an ideal of $\mathbf{F}$ then $I = \mathbf{F}$

Mindset Makers

Q. How many ideals in Q?

Solution: $(Q,+,\cdot)$ field and field has exactly 2 ideals say $I=\{0\}$ and $I=\mathbf{F}$ then Q has exactly 2 ideals say $I=\{0\}$ and $I=Q$

Q. How many ideals in $\mathbf{R}$?

Solution: $(\mathbf{R},+,0)$ is field and field has exactly 2 ideals say $I=\{0\}$ and $I=\mathbf{F}$ then $\mathbf{R}$ has exactly ideals say $I=\{0\}$ and $I=\mathbf{R}$.

Q. How many ideals in $\mathbf{R}[i]$?

Solution: $(\mathbf{R}[i],+,\cdot)$ is field and field has exactly 2 ideals say $I=\{0\}$ and $I=\mathbf{F}$ then $\mathbf{R}[i]$ has 2 ideals they are $I=\{0\}$ and $I=\mathbf{R}[i]$.

Q. How many ideal in $Z_{11}[i]$?

Solution: $Z_{11}[i]$ is field then $Z_{11}[i]$ has exactly 2 two ideals say $I=\{0\}$ and $I=Z_{11}[i]$.

Q. $I=\{0,1,2,1+i,2+i\}$ is an ideal of $Z_3[i]$?

Solution: $Z_3[i]$ is field then $Z_3[i]$ has exactly 2 ideals say $I_1=\{0\}$ and $I_2=Z_3[i]$ then $I\neq I_1$ and $I\neq I_1$ then I is not ideal of $Z_3[i]$

Q. (i) How many ideals in $Z_4\times Z_5$?

(ii)How many ideals in $Q\times\mathbf{R}$?

(iii) How many ideals in $\mathbf{R}\times Q\times Z_7$?

Solution: (ii) $R=Q\times\mathbf{R}$ ....(1)

Since Q is field then Q has exactly 2 ideals say $I_1=\{0\}$ and $I_2=Q$

Since $\mathbf{R}$ is field then $\mathbf{R}$ has exactly 2 ideals say $I_3=\{0\}$ and $I_4=\mathbf{R}$

$R=Q\times\mathbf{R}$

$\{0\},Q \quad \{0\},\mathbf{R}$

Possible Ideal of $Q\times\mathbf{R}$

(i) $\{0\}\times\{0\}$ (ii) $\{0\}\times\mathbf{R}$ (iii) $Q\times\{0\}$ (iv) $Q\times\mathbf{R}$

Number of ideals in $Q\times\mathbf{R}=4$

Q. How many ideals in $Q\times Q\times Q$?

Solution: Q is field then Q has exactly 2 ideals say

$I=\{0\}$ and $I=Q$

Ideals of $R=Q\times Q\times Q$

$\{0\}\quad Q \quad \{0\},Q \quad \{0\},Q$

$I_1=\{0\}\times\{0\}\times\{0\},\ I_2=\{0\}\times\{0\}\times Q,\ I_3=\{0\}\times Q\times\{0\},I_4=Q\times\{0\}\times\{0\}$

$I_5=\{0\}\times Q\times Q, I_6=Q\times\{0\}\times Q, I_7=Q\times Q\times\{0\}, I_8=Q\times Q\times Q$; exactly 8 ideals

Q. How many ideals in $Z_6\times Z_5$?

Solution: $Z_6=\{0,1,2,3,4,5\}$

Mindset Makers

and $Z_5=\{0,1,2,3,4\}$

then number of ideals in $Z_6=\tau(6)=(1+1)(1+1)=4$

say $I_1=\{0\}, I_2=Z_6, I_3=\langle 2\rangle=\{0,2,4\}, I_4=\langle 3\rangle=\{0,3\}$

Now, number of ideals in $Z_5=\tau(5)=(1+1)=2$

say $I_5=\{0\}, I_6=Z_5$

Then, Ideals in $Z_6\times Z_5$:

(i) $\{0\}\times\{0\}$ (ii) $\{0\}\times Z_5$ (iii) $Z_6\times\{0\}$ (iv) $Z_6\times Z_5$

(v) $\langle 2\rangle\times\{0\}$ (vi) $\langle 2\rangle\times Z_5$ (vii) $\langle 3\rangle\times\{0\}$ (viii) $\langle 3\rangle\times Z_5$

Q. Find ideals in $Q\times\mathbf{R}\times\mathbf{C}\times Z_7\times Z_{11}[i]$.

Solution: Since Q is field then it has exactly 2 ideals say $I_1=\{0\}, I_2=Q$

Since $\mathbf{R}$ is field then it has exactly 2 ideals say $I_1=\{0\}$, $I_2=\mathbf{R}$

Since $\mathbf{C}$ is field then it has exactly 2 ideals say $I_1'=\{0\}$, $I_2'=Q$

Since Z_7 is field then it has exactly 2 ideals say $I_1''=\{0\}, I_2=Z_7$

Since $Z_{11}[i]$ is finite field then it has exactly 2 ideals say $I_1'''=\{0\}$, $I_2'''=Z_{11}[i]$

# of ideals in $Q\times\mathbf{R}\times\mathbf{C}\times Z_7\times Z_{11}[i]=2\times2\times2\times2\times2=32$

Maximal Ideal: Let R be a commutative ring An ideal $A\neq R$ is said to be maximal ideal of R if $\exists$ an ideal, $B\in R$ such that $A\subseteq B\subseteq R$ then either $A=B$ or $B=R$

Q. Find Maximal ideal in Z_4?

Solution: $Z_4=\{0,1,2,3\}$

Ideals of $R=Z_4$: $I_1=\{0\}, I_2=\langle 2\rangle=\{0,2\}, I_3=Z_4, I_3=Z_4$ is not maximal by definition

$I_1=\{0\}\subseteq I_2\subseteq Z_4$ but $I_1\neq I_2$ and $I_2\neq Z_4$ then I_1 is not maximal ideal $I_2=\{0,2\}$ is maximal ideal of Z_4 because of no ideal of Z_4 exist between I_2 and Z_4

Then exactly one maximal ideal in Z_4.

Q. How many maximal ideal in Z_{10}?

Solution: $Z_{10}=\{0,1,2,3,4,5,6,7,8,9\}$

Ideals of Z_{10} are: $I_1=\{0\}, I_2=\langle 2\rangle=\{0,2,4,6,8\}, I_3=\langle 5\rangle=\{0,5\}, I_4=Z_{10}$

$I_4=Z_{10}$ is not maximal ideal by definition

$I_1=\{0\}\subseteq I_2\subseteq Z_{10}$ but $I_1\neq I_2$ and $I_2\neq Z_{10}$

I_2 is not maximal ideal, I_2 and I_3 are maximal ideals of Z_{10}.

Exam point: Number of maximal ideal in Z_n = number of prime divisor of *n*.

Q. Find maximal ideal in Z_{12}?

Solution: $Z_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

Ideals of Z_{12} are: $I_1=\{0\}$ $\times$, $I_2=\langle 2\rangle=\{0,2,4,6,8,10\}$ $\surd$, $I_3=\langle 3\rangle=\{0,3,6,9\}$ $\surd$

$I_4=\langle 4\rangle=\{0,4,8\}$ $\times$, $I_5=\langle 6\rangle=\{0,6\}$ $\times$, $I_6=Z_{12}: I_6=Z_{12}$ is not maximal idea by definition.

Mindset Makers

I_2 and I_3 are maximal ideal in Z_{12}

Q. How many maximal ideal in Z_{27} ?

Solution: No. of maximal ideal in Z_{27} = number of Prime divisor of 27 = 1 i.e. 3

$I_1 = \{0,3,6,9,12,15,18,21,24\}$ = Maximal Ideal in Z_{27}

Q. How many maximal ideal in Q?

Solution: $R = Q$ is field then Q has exactly two ideals

$I_2 = Q$ is not maximal by definition then $I_1 = \{0\}$ is only maximal ideal.

Note: If **F** is field then **F** has exactly one maximal ideal.

Solution: If **F** is field then **F** has exactly 2 ideals say

$I_1 = \{0\}$ and $I_2 = \mathbf{F}$

$I_2 = \mathbf{F}$ is not maximal ideal by definition then $I_1 = \{0\}$ is only maximal ideal of **F**.

Q. Find maximal ideal in **R**, **C**, Z_p ?

Solution: Since **R**, **C**, Z_p are field then they have exactly one maximal ideal.

Q. How many maximal ideal in $Q \times Z_3[i]$.

Solution: Since Q is field then it has exactly 2 ideals also $Z_3[i]$ has exactly 2 ideals as it is also field.

$R = Q \times Z_3[i]$, ideals of R are

(i) $I_1 = \{0\} \times \{0\}$,(ii) $I_2 = \{0\} \times Z_3[i]$,(iii) $I_3 = Q \times \{0\}$,(iv) $I_4 = Q \times Z_3[i]$

$I_4 = Q_3 \times Z_3[i]$ is not maximal ideal by definition.

$I_1 \subseteq I_2 \subseteq Q \times Z_3[i]$ but $I_1 \neq I_2$ and $I_2 \neq Q \times Z_3[i]$. Then I_2 and I_3 are maximal ideal of $Q \times Z_3[i]$.

Q. How many maximal ideal in $Q \times Z_7[i] \times Z_{11}$?

Solution: Ideals of $Q \times Z_7[i] \times Z_{11}$:

$I_1 = \{0\} \times \{0\} \times \{0\}$ $\times, I_2 = \{0\} \times \{0\} \times Z_{11}$ $\times, I_3 = \{0\} \times Z_7[i] \times \{0\}$ $\times, I_4 = Q \times \{0\} \times \{0\}$ $\times$

$I_5 = Q \times Z_7[i] \times \{0\}$ $\surd, I_6 = Q \times \{0\} \times Z_{11}$ $\surd, I_7 = \{0\} \times Z_7[i] \times Z_{11}$, $I_8 = Q \times Z_7 \times Z_{11}$

$I_8 = Q \times Z_7 \times Z_{11}$ is not maximal ideal by definition $I_1 \subseteq I_5 \subseteq Q \times Z_7[i] \times Z_{11}$ but $I_1 \neq I_5$ and $I_5 \neq Q \times Z_7[i] \times Z_{11}$ then I_1 is not maximal

$I_2 \{0\} \times \{0\} \times Z_{11} \subseteq I_6 \subseteq Q \times Z_7[i] \times Z_{11}$

but $I_2 \neq I_6$ and $I_6 \neq Q \times Z_7[i] \times Z_{11}$

I_2 is not maximal ideal.

$I_3 = \{0\} \times Z_7[i] \times \{0\} \subseteq I_7 \subseteq Q \times Z_7[i] \times Z_{11}$ but $I_3 \neq I_7$ and $I_7 \neq Q \times Z_7[i] \times Z_{11}$

I_3 is not maximal ideal

$I_4 = Q \times \{0\} \times \{0\} \subseteq I_6 \subseteq Q \times Z_7[i] \times Z_{11}$ but $I_4 \neq I_6$ and $I_6 \neq Q \times Z_7[i] \times Z_{11}$

I_4 is not maximal ideal

$I_5 = Q \times Z_7[i] \times \{0\}$, $I_6 = Q \times \{0\} \times Z_{11}$, $I_7 = \{0\} \times Z_7[i] \times Z_{11}$ are Maximal ideals.

Mindset Makers

then $Q\times Z_7[i]\times Z_{11}$ has exactly three maximal ideals.

Q. $R=Z_8\times Z_{30}$, how many maximal ideals?

Solution: Maximal ideals of $Z_8=\langle 2\rangle=2Z_8$

Maximal ideals of Z_{30}:

(i) $\langle 2\rangle=2Z_{30}$, (ii) $\langle 3\rangle=3Z_{30}$, (iii) $\langle 5\rangle=5Z_{30}$

Maximal Ideals of $Z_8\times Z_{30}: I_1=2Z_8\times Z_{30},\ I_2=Z_8\times 2Z_{30}, I_3=Z_8\times 3Z_{30}, I_4=Z_8\times 5Z_{30}$

Note: $R=R_1\times R_2$, maximal ideals of R are (maximal ideals of R_1) $\times R_2$ and $R_1\times$(maximal ideal of R_2)

Q. Maximal ideals in $Z_4\times Z_{11}$?

Solution: Maximal Ideals of $Z_4\times Z_{11}$ are $I_1=\langle 2\rangle\times Z_{11},\ I_2=Z_4\times\{0\}$

I_1 = Maximal Ideal of $Z_4\times Z_{11}$, $I_2=Z_4\times$Maximal ideal of Z_{11}

Q. How many maximal ideal in $Q\times\mathbf{R}\times\mathbf{C}\times Z_{23}$?

Solution: Since $Q,\mathbf{R},\mathbf{C}$ and Z_{23} are field so each has exactly 1 maximal ideal.

$\therefore Q\times\mathbf{R}\times\mathbf{C}\times Z_{23}$ has $1+1+1+1=4$, maximal ideals.

Q. $I=\{0\}$ is maximal ideal in Z?

Solution: $I_1=\langle 2\rangle=2Z$ is ideal of Z and $I=\{0\}\subseteq I_1\subseteq Z$ But $I\neq I_1$ and $I_1\neq Z$

then $I=\{0\}$ is not maximal ideal in Z.

Q. $\langle 2\rangle=2Z$ is maximal ideal in Z?

Solution: $2Z=\{0,\pm 2,\pm 4,\pm 6,....\}$, $Z=\{0,\pm 1,\pm 2,\pm 3,....\}$

$2Z$ is maximal ideal in Z because no ideal exist between $2Z$ and Z s.t. $2Z\subseteq I\subseteq Z$

Q. $4Z$ is maximal ideal in Z?

Solution: $4Z\subseteq 2Z\subseteq Z$ but $4Z\neq 2Z$ and $2Z\neq Z$ then $4Z$ is not maximal ideal.

Note: Maximal ideal of Z are pZ, where p is Prime i.e. $\langle p\rangle$.

Prime Ideal

Let R be a commutative ring an ideal $P\neq R$ is called Prime ideal if $a\cdot b\in P$ where $a\in R, b\in R$

$\Rightarrow$ either $a\in P$ or $b\in P$.

Q. $R=Z_{15}$, $I=\{0\}$ is an ideal of Z_{15} $I=\{0\}$ is Prime Ideal in Z_{15}?

Solution: $R=Z_{15}$, $I=\{0\}$. $3\in R, 5\in R$; $3.5=0\in I=\{0\}$ but $3\notin I$ and $5\notin I$ then

$I=\{0\}$ is not Prime Ideal in Z_{15}

Q. How many Prime Ideal in Z_{15}?

Solution: $R=Z_{15}$, $Z_{15}=\{0,1,2,3,4,5,6,7,8,9,10,11,12\}$

Ideals of $R=Z_{15}, I_1=\{0\}, I_2=\langle 3\rangle=\{0,3,6,9,12\}, I_3=\langle 5\rangle=\{0,5,10\}, I_4=Z_{15}$

$I_4=Z_{15}$ is not Prime ideal by definition

I_1 is also not Prime ideal because $3.5=0\in I_1$ but $3\notin I_1$ and $5\notin I_1$

Now, $I_2=\{0,3,6,9,12\}$, $I_3=\{0,5,10\}$

$a \cdot b \in I_2$, $a \in I_1$ or $b \in I_2$. I_2 and I_3 are Prime ideal of Z_{15}.

Q. $Z_6 = \{0,1,2,3,4,5\}$

Solution: Ideals of Z_6 are

$I_1 = \{0\}, I_2 = \langle 2 \rangle = \{0,2,4\}, I_3 = \langle 3 \rangle = \{0,3\}, I_4 = Z_6, I_4 = Z_6$ is not prime ideal by definition

$I_1 = \{0\}$ is also not prime ideal because $2 \cdot 3 = 0 \in I_1 = \{0\}$ but $2 \notin I_1$ and $3 \notin I_1$.

$I_2 = \{0,2,4\}$

	1	3	5
1	1	3	5
3	3	3	3
5	5	3	1

$I_2 = \{0,2,4\}$ is also prime ideal in Z_6 Similarly, $I_3 = \{0,3\}$

	1	2	4	5
1	1	2	4	5
2	2	4	2	4
4	4	2	4	2
5	5	4	2	1

Now, for whole Z_6

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

hence, similarly $I_3 = \{0,3\}$ is prime ideal in Z_6.

Exam Point: Number of Prime Ideals in Z_n = No. of Prime Divisor of *n*.

Q. How many Prime Ideals in Z_{12} ?

Solution: Total number of Prime ideal in $Z_{12} = 2$

$I_1 = \langle 2 \rangle = \{0,2,4,6,8,10\}$, $I_2 = \langle 3 \rangle = \{0,3,6,9\}$

Q. How many Prime ideal in Zp^2q ?

Q. $4Z$ is maximal ideal in $2Z$.

Solution: $2Z = \{0, \pm 2, \pm 4, \pm 6, ...\}, 4Z = \{0, \pm 4, \pm 8, \pm 12, ...\}$ then $4Z$ is maximal ideal in $2Z$.

Q. $I = \{0\}$ is Prime Ideal in Z?

Solution: Let $a, b \in Z$ and $a \cdot b \in I = \{0\}$

$a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$ because Z is an Integral domain

If $a = 0$ then $a \in I$ and if $b = 0$ then $b \in I$. $I = \{0\}$ is Prime Ideal of Z.

Q. How many Prime ideal in Q?

Solution: $R = Q$ and Q is field then Q has exactly 2 ideals say $I_1 = \{0\}$ and $I_2 = Q$

But $I_2 = Q$ is not Prime ideal by definition

$\therefore I_1 = \{0\}$ is Prime ideal of Q because $a \in Q, b \in Q$ and $a \cdot b \in I = \{0\} \Rightarrow$ either $a = 0$ or $b = 0$ because Q is an integral domain.

Mindset Makers

Then, Q has exactly one Prime ideal.

Note: If **F** is field then **F** has exactly one Prime ideal say $I=\{0\}$.

Q. How many Prime ideals in $Q\times\mathbf{R}$.

Solution: Ideals of $Q\times\mathbf{R}$ are

(1) $I_1=\{0\}\times\{0\}$, (2) $I_2=\{0\}\times\mathbf{R}$, (3) $I_3=Q\times\{0\}$,(4) $I_4=Q\times\mathbf{R}$

$I_4=Q\times\mathbf{R}$ is not Prime ideal by the definition.

$I_1=\{0\}\times\{0\}$ is not Prime ideal because $(1,0)\in Q\times\mathbf{R}$ and $(0,1)\in Q\times\mathbf{R}$

$(1,0)(0,1)=(0,0)\in I_1=\{0\}\times\{0\}$ but $(1,0)\notin I_1$ and $(0,1)\notin I_1$.

*Show that $I_2=\{0\}\times\mathbf{R}$ is Prime ideal of $Q\times\mathbf{R}$

Let $(a,b)\in Q\times\mathbf{R}$ and $(c,d)\in Q\times\mathbf{R}$ and

$(a,b)(c,d)\in I_2=\{0\}\times\mathbf{R}$, $(ac,bd)\in I_2\Rightarrow ac=0$

$\Rightarrow$ either $a=0$ or $c=0$ [$\because$ Q is integral domain $a\in Q,c\in Q$]

If $a=0$ then $(a,b)=(0,b)\in I_2$, If $c=0$ then $(c,d)=(0,d)\in I_2$

then I_2 is Prime ideal of $Q\times\mathbf{R}$. Similarly, $I_3=Q\times\{0\}$ is also Prime ideal of $Q\times\mathbf{R}$.

Then $Q\times\mathbf{R}$ has exactly 2 Prime Ideals.

Q. Find Prime Ideals in $Q\times Z_3[i]\times\mathbf{R}$?

Solution: Ideals of $Q\times Z_3[i]\times\mathbf{R}$

$I_1=\{0\}\times\{0\}\times\{0\}$, $I_2=\{0\}\times\{0\}\times\mathbf{R}$, $I_3=\{0\}\times Z_3[i]\times\{0\}$, $I_4=Q\times\{0\}\times\{0\}$

$I_5=Q\times Z_3[i]\times\{0\}$, $I_6=Q\times\{0\}\times\mathbf{R}$, $I_7=\{0\}\times Z_3[i]\times\mathbf{R}$, $I_8=Q\times Z_3[i]\times\mathbf{R}$

$I_8=Q\times Z_3[i]\times\mathbf{R}$ is not Prime ideal by definition.

$I_1=\{0\}\times\{0\}\times\{0\}$ is not Prime ideal because

$(1,1,0)\in Q\times Z_3[i]\times\mathbf{R}$, $(0,0,1)\in Q\times Z_3[i]\times\mathbf{R}$. $(1,1,0)(0,0,1)=(0,0,0)$

$(0,0,0)\in I_1$ but $(1,1,0)\notin I_1$ and $(0,0,1)\notin I_1$ so I_1 is not Prime ideal of $Q\times Z_3[i]\times\mathbf{R}$

$I_2=\{0\}\times\{0\}\times\mathbf{R}$ is not Prime ideal because $(1,0,1)\in Q\times Z_3[i]\times\mathbf{R}$ and $(0,1,1)\in Q\times Z_3[i]\times\mathbf{R}$

$(1,0,1)(0,1,1)\subset(0,0,1)\in I_2$ but $(1,0,1)\notin I_2$, so $I_2=\{0\}\times\{0\}\times\mathbf{R}$ is not Prime ideal.

Similarly I_3 and I_4 also not Prime ideals.

Hence, I_5,I_6 and I_7 are Prime ideals of $Q\times Z_3[i]\times\mathbf{R}$

$I_5=Q\times Z_3[i]\times\{0\}$

$(a,b,c)\in Q\times Z_3[i]\times\mathbf{R}$

$(d,e,f)\in Q\times Z_3[i]\times\mathbf{R}$ and $(a,b,c)(d,e,f)\in I_5=Q\times Z_3[i]\times\mathbf{R}$

$\Rightarrow(ad,be,cf)\in I_5\Rightarrow cf=0\Rightarrow$ either $c=0$ or $f=0$ [$\because\mathbf{R}$ is integral domain]

If $c=0$ then $(a,b,0)\in I_5$,If $f=0$ then $(d,e,0)\in I_5$

Q. How many Prime ideal in Z?

Solution: It has infinite number of Prime ideals say $I=\{0\}$ and $I=pz$, where p is prime.

e.g. $2Z,3Z,5Z,7Z,11Z,....$ are Prime ideal in Z.

Mindset Makers

Q. Show that $6Z$ is not Prime ideal in Z.

Solution: $6Z=\{0,\pm6,\pm12,.....\}$

$2\in Z,\ 3\in Z,\ 2\cdot3=6\in6Z$ but $2\notin6Z$ and $3\notin6Z$ then $6Z$ is not Prime ideal.

Q. (i) Union of two maximal ideal of R is maximal ideal of R?

(ii) Intersection of two maximal ideal of R is maximal ideal of R?

Solution: (i) Need not e.g. $2Z$ is maximal ideal of Z and $3Z$ is maximal ideal of Z.

$2Z\bigcup3Z$ is not ideal of Z. $2\in2Z\bigcup3Z,\ 3\in2Z\bigcup3Z;2+3=5\notin2Z\bigcup3Z$ then $2Z\bigcup3Z$ is not ring.

(ii) Need not, e.g. $2Z$ is maximal ideal in Z

$2Z\bigcap3Z=6Z$ and $6Z$ is not maximal ideal in Z.

Q. Intersection of two Prime ideal in Prime ideal?

Solution: Need not: $2Z$ is Prime ideal of Z

$3Z$ is Prime ideal of Z. $2Z\bigcap3Z=6Z$, but $6Z$ is not Prime ideal of Z.

Exam Point: $mZ\bigcap nZ=kZ$, where $k=\text{L.C.M.}(m,n)$

Q. (i) Every Maximal ideal is Prime ideal?

Ans. Need not: e.g. $4Z$ is maximal ideal of $2Z$ but not Prime ideal because

$2\in2Z,\ 2\cdot2=4\in4Z$ but $2\notin4Z$.

(ii) Every Prime ideal is maximal ideal?

Solution: Need not. e.g. $\{0\}$ is Prime ideal in Z but $\{0\}$ is not maximal ideal in Z.

Exam Point: (i) If R is commutative ring with unity then every maximal ideal is Prime ideal.

(ii) If R is finite commutative ring with unity then every prime ideal is maximal ideal.

Q. $I=Z\times Z\times\{0\}$ is maximal ideal in $Z\times Z\times Z$?

Solution:

$I=Z\times Z\times\{0\}$ is not maximal ideal in $Z\times Z\times Z$ because

$Z\times Z\times\{0\}\subseteq Z\times Z\times2Z\subseteq Z\times Z\times Z$

but $Z\times Z\times\{0\}\neq Z\times Z\times Z$ and $Z\times Z\times2Z\neq Z\times Z\times Z$

Q. $I=Z\times Z\times\{0\}$ is Prime ideal is $Z\times Z\times Z$?

Solution:

Yes, $Z\times Z\times\{0\}$ is Prime ideal in $Z\times Z\times Z$. As $\dfrac{Z\times Z\times Z}{Z\times Z\times\{0\}}\approx$ Z is an integral domain then $Z\times Z\times\{0\}$ is Prime.

Principal Ideal: Ideal generated by single element is called Principal Ideal.

Example: $I=\langle3\rangle$ in Z, I is Principal Ideal?

Solution: Yes, because I is generated by single element $\langle3\rangle$ then $I=\langle3\rangle$ is Principal Ideal in $Z[i]$.

Q. $I=\langle m\rangle$ is Principal Ideal in Z?

Solution: Yes. Note: Every Ideal of Z is Principal Ideal Since its ideals are generated by $\langle m\rangle$.

Q. $I=\langle2,x\rangle$ is Principal Ideal is $Z[x]$.

Solution: No, because I is not generated by single elements.

Mindset Makers

Q. $R = Q$ ideals of Q are Principal ideal?

Solution: Q is field then Q has exactly two ideals

say $I_1 = \{0\} = \langle 0 \rangle, I_2 = Q = \langle 1 \rangle = \{1 \cdot a \mid a \in Q\}$. I_1 and I_2 are both Principal Ideal.

Note: If **F** is field then all ideals are Principal Ideal.

Q. How many Principal ideal in $Z_{11}[i]$?

Solution:

$Z_{11}[i]$ is field then $Z_{11}[i]$ has exactly 2 ideals

$I_1 = \{0\} = \langle 0 \rangle \quad I_2 = Z_{11}[i] = \langle i \rangle$

then both are Principal Ideals.

Factor Ring

Let R be a ring and A is an ideal of R. Then $\frac{R}{A} = \{a + A \mid a \in R\}$ is factor ring with operation

(i) $(a_1 + A) + (a_2 + A) = a_1 + a_2 + A$ (ii) $(a_1 + A)(a_2 + A) = a_1 a_2 + A$

Example: $R = Z, I = 3Z$; $\frac{R}{I} = \frac{Z}{3Z} = \{a + 3z \mid a \in Z\}$; $\frac{Z}{3Z} = \{0 + 3z, 1 + 3z, 2 + 3z\}$

Composition table of $\frac{Z}{3Z}$

(i) Under Addition

	$0+3Z$	$1+3Z$	$2+3Z$
$0+3Z$	$0+3Z$	$1+3Z$	$2+3Z$
$1+3Z$	$1+3Z$	$2+3Z$	$0+3Z$
$2+3Z$	$2+3Z$	$0+3Z$	$1+3Z$

$[(1+3Z)+(2+3Z) = 3+3Z = 0+3Z]$

(ii) Under Multiplication

	$0+3Z$	$1+3Z$	$2+3Z$
$0+3Z$	$0+3Z$	$0+3Z$	$0+3Z$
$1+3Z$	$0+3Z$	$1+3Z$	$2+3Z$
$2+3Z$	$0+3Z$	$2+3Z$	$1+3Z$

From Table, $\frac{Z}{3Z}$ is Commutative ring with Unity $1+3Z$; $\boxed{\frac{Z}{3Z} \approx Z_3}$

Q. $\frac{3Z}{9Z} = ?$

Solution: $\frac{3Z}{9Z} = \{a + 9Z \mid a \in 3Z\}$; $\frac{3Z}{9Z} = \{0 + 9Z, 3 + 9Z, 6 + 9Z\}$

$0 + 9Z \neq (3 + 9Z) \in \frac{3Z}{9Z}, 0 + 9Z \neq (6 + 9Z) \in \frac{3Z}{9Z}; (3 + 9Z)(6 + 9Z) = 18 + 9Z = 0 + 9Z$

then $\frac{3Z}{9Z}$ is not an integral domain and Z_3 is field then $\frac{3Z}{9Z} \neq Z_3$.

Q. $\frac{2Z}{4Z} \approx Z_2$?

Mindset Makers

Solution: $\frac{2Z}{4Z}=\{a+9Z \mid a\in 2Z\}=\{0+4Z,2+4Z\}$

$0\neq 2+4Z\in\frac{2Z}{4Z}$ and $(2+4Z)(2+4Z)=4+4Z=0+1$

$\Rightarrow\frac{2Z}{4Z}$ is not integral domain then $\frac{2Z}{4Z}\not\approx Z_2$, because Z_2 is field. i.e. $\frac{2Z}{4Z}\approx$ Ring but not integral domain.

Q. $\frac{Z}{6Z}\approx ?$

Solution: $\frac{Z}{6Z}=\{a+az \mid a\in Z\}=\{0+6Z,1+6Z,2+6Z,3+6Z,4+6Z,5+6Z\}$

$0+6Z\neq(2+6Z)\in\frac{Z}{6Z}$, $0+6Z\neq(3+6Z)\in\frac{Z}{6Z}$

$(2+6Z)(3+6Z)=6+6Z=0+6Z$ then $\frac{Z}{6Z}$ is not integral domain of order 6; $\boxed{\frac{Z}{6Z}\approx Z_6}$

$\because Z_6$ is not an Integral Domain.

Q. Find Factor ring of Q?

Solution:Q is field then Q has exactly two ideals say $I_1=\{0\}$ and $I_2=Q$

(1) $\frac{Q}{I_1}=\frac{Q}{\{0\}}=\{a+\{0\} \mid a\in Q\}\ \therefore\ \frac{Q}{I_1}\approx Q$

(2) $\frac{Q}{I_2}=\frac{Q}{Q}=\{a+Q \mid a\in Q\}=\{0+Q\};\ \frac{Q}{I_2}\approx\{0\}$

Exam Point: If **F** is field then **F** has exactly two factor rings

(i) $\frac{\mathbf{F}}{\{0\}}\approx\mathbf{F}$ (ii) $\frac{\mathbf{F}}{\mathbf{F}}\approx\{0\}$

Q. Construct $\frac{Q}{Z}=?$

Solution: Does not exist because Z is not ideal of Q.

Q. Construct factor ring of $Z_{23}[i]$?

Solution: Since $Z_{23}[i]$ is field then $Z_{23}[i]$ has exactly two ideals say $I_1=\{0\}$ and $I_2=Z_{23}[i]$

Then, factor ring,

(i) $\frac{Z_{23}[i]}{I_1}=\frac{Z_{23}[i]}{\{0\}}\approx Z_{23}[i]$ (ii) $\frac{Z_{23}[i]}{I_2}=\frac{Z_{23}[i]}{Z_{23}[i]}\approx\{0\}$

Q. $I=\langle(1-i)\rangle$ is an ideal of $Z[i]$, construct $\frac{Z[i]}{\langle 1-i\rangle}\approx ?$

Solution: $\frac{Z[i]}{\langle(1-i)\rangle}=\{a+ib+\langle 1-i\rangle \mid a+ib\in Z[i]\}$

$=\{a+ib+\langle 1-i\rangle \mid a,b\in Z\}$ ....(1)

$1-i+\langle 1-i\rangle=0+\langle 1-i\rangle\Rightarrow 1-i=0\Rightarrow i=1$ ....(2)

Mindset Makers

$\Rightarrow i^2 = 1^2 \Rightarrow -1 = 1 \Rightarrow 2 = 0$ ....(3)

$\frac{Z[i]}{\langle 1-i \rangle} = \{a+ib+\langle 1-i \rangle \mid a,b \in Z\} \Rightarrow \frac{Z[i]}{\langle 1-i \rangle} = \{0+\langle 1-i \rangle, 1+\langle 1-i \rangle\}$; $\boxed{\frac{Z[i]}{\langle 1-i \rangle} \approx Z_2}$

Q. $\frac{Z[i]}{\langle 3-i \rangle} = \{a+ib+\langle 3-i \rangle \mid a+ib \in Z[i]\} = \{a+ib+\langle 3-i \rangle \mid a,b \in Z\}$

Solution: $3-i+\langle 3-i \rangle = 0+\langle 3-i \rangle \Rightarrow 3-i=0 \Rightarrow 3=i \Rightarrow 3^2 = i^2$

$\Rightarrow 9 = -1$ ....(1)

$\Rightarrow 10 = 0$ ....(2)

Given into about modulo we are using

$\frac{Z[i]}{\langle 3-i \rangle} = \{0+\langle 3-i \rangle, 1+\langle 3-i \rangle, 2+\langle 3-i \rangle, 3+\langle 3-i \rangle, 4+\langle 3-i \rangle, 5+\langle 3-i \rangle, 6+\langle 3-i \rangle, 7+\langle 3-i \rangle, 8\langle 3-i \rangle, 9+\langle 3-i \rangle\}$

$\frac{Z[i]}{\langle 3-i \rangle} \approx Z_{10}$, $0+i+\langle 3-i \rangle = 0+3+\langle 3-i \rangle$

$1+i+\langle 3-i \rangle = 1+3+\langle 3-i \rangle = 4+\langle 3-i \rangle$

Exam Point: $\frac{Z[i]}{\langle a+ib \rangle} \approx Z_{a^2+b^2}$, if $\gcd(a,b)=1$

Exam Point: $\frac{Z[i]}{\langle a+ib \rangle} \approx$ not integral domain if $\gcd(a,b) \neq 1$ and $a \neq 0$, $b \neq 0$

Q. $\frac{Z[i]}{\langle 2 \rangle} = ?$

Solution: $\frac{Z[i]}{\langle 2 \rangle} = \{a+ib+\langle 2 \rangle \mid a,b \in Z\} = \{0+\langle 2 \rangle, 1+\langle 2 \rangle, i+\langle 2 \rangle, (1+i)+\langle 2 \rangle\}$

$2+\langle 2 \rangle = 0+\langle 2 \rangle \Rightarrow 2=0$ ....(2) Using Modulo 2

No, relation found for *i*.; Meaning of $\langle 2 \rangle$ is $2Z[i]$.; $\frac{Z[i]}{\langle 2 \rangle} \approx Z_2[i]$

Note:

(i) $\frac{Z[i]}{\langle 2+2i \rangle} \approx Z_2[i] \times Z_2$, (ii) $\frac{Z[i]}{\langle 3+6i \rangle} \approx Z_3[i] \times Z_5$, (iii) $\frac{Z[i]}{\langle 3+9i \rangle} \approx Z_3[i] \times Z_{10}$

$\frac{Z[i]}{\langle 2+2i \rangle} \approx Z_2[i] \times Z_2$

$4+4=8=4\times 2$

On squaring $\langle 2+2i \rangle$ repeatedly.

Q. $\frac{Z[i]}{\langle 4i \rangle}$?

Solution: $\frac{Z[i]}{\langle 4i \rangle} = \frac{Z[i]}{\langle 4 \rangle}$

Mindset Makers

$\langle 4\rangle = 4Z[i],\ \langle 4i\rangle = 4iZ[i]$

$\frac{Z[i]}{\langle 4\rangle} = \{a+ib+\langle 4\rangle \mid a,b\in Z\}$ ....(1)

$4+\langle 4\rangle = 0+\langle 4\rangle \Rightarrow 4=0$ ....(2)

Now,

$$\frac{Z[i]}{\langle 4\rangle} = \begin{Bmatrix} 0+\langle 4\rangle, 1+\langle 4\rangle, i+\langle 4\rangle, 1+i+\langle 4\rangle, 2+\langle 4\rangle, 2i+\langle 4\rangle, 2+2i+\langle 4\rangle \\ 1+2i+\langle 4\rangle, 2+i\langle 4\rangle, 3+\langle 4\rangle, 3i+\langle 4\rangle, 1+3i+\langle 4\rangle, 2+3i+\langle 4\rangle \\ 3+3i+\langle 4\rangle, 3+i+\langle 4\rangle, 3+2i+\langle 4\rangle \end{Bmatrix}$$

$\frac{Z[i]}{\langle 4\rangle} \approx Z_4[i]$

Note: $\langle 4i\rangle = 4iZ[i] = 4(iZ[i]) = 4Z[i] = \langle 4\rangle \ \therefore \langle 4i\rangle = \langle 4\rangle$

Exam Point: $\frac{Z[i]}{\langle n\rangle} \approx Z_n[i]$

Theorem 1: Let R be a commutative ring with unity and A is an ideal of R. $\frac{R}{A}$ is an integral domain iff A is Prime Ideal.

Theorem 2: Let R be a commutative ring with unity and A is an ideal of R. $\frac{R}{A}$ is field iff A is maximal ideal.

Q. Show that if R is commutative ring with unity then every maximal ideal of R is prime ideal.

Solution: Let R is commutative ring with unity and A is maximal ideal of R. Then $\frac{R}{A}$ is field

$\Rightarrow \frac{R}{A}$ is integral domain $\Rightarrow A$ is Prime ideal.

Q. Show that if R is finite commutative ring with unity then every Prime ideal of R is maximal ideal.

Solution:

Let R is finite commutative ring with unity and A is prime ideal of R.

If A is prime ideal of R then $\frac{R}{A}$ is an integral domain and $\frac{R}{A}$ is finite because R is finite.

$\Rightarrow \frac{R}{A}$ is finite integral domain $\Rightarrow \frac{R}{A}$ is field $\Rightarrow A$ is maximal ideal.

Q. $I = \langle p\rangle = pZ$ is maximal ideal is Z.

Solution: $\frac{Z}{\langle p\rangle} = \frac{Z}{pz} \approx Z_p \rightarrow$ is field then $\frac{Z}{\langle p\rangle}$ is field

$\Rightarrow \langle p\rangle$ is maximal ideal = pz is maximal ideal in Z

Q. Show that $I = \{0\}$ is Prime Ideal but not maximal.

Mindset Makers

Solution: $R = Z$ is commutative ring with unity $I = \{0\}$; $\frac{R}{I} = \frac{Z}{\{0\}} \approx Z$

Z(R.H.S.) is an integral domain but not field then $\frac{Z}{\{0\}}$ is an integral domain but not field.

$\Rightarrow \{0\}$ is Prime ideal but not maximal ideal in Z.

Q. $\langle 11 \rangle$ is maximal ideal in $Z[i]$?

Solution: $\frac{Z[i]}{\langle 11 \rangle} \approx Z_{11}[i]$

$Z_{11}[i]$ is field then $I = \langle 11 \rangle$ is maximal ideal also $Z_{11}[i]$ is an integral domain hence $\langle 11 \rangle$ is prime ideal in $Z[i]$.

Q. pz is maximal ideal in Z?

Solution:

$\frac{Z}{pz} \approx Z_p$, Z_p is field $\Rightarrow \frac{Z}{pz}$ is field $\Rightarrow pz$ is maximal ideal

Q. $I = \{0\}$ is maximal and Prime ideal of $\mathbf{F}$ where $\mathbf{F}$ is field.

Solution: $\frac{\mathbf{F}}{\{0\}} \approx \mathbf{F}$, $\mathbf{F}$ is field then $\frac{\mathbf{F}}{\{0\}}$ is field then $I = \{0\}$ is maximal ideal similarly, $\frac{\mathbf{F}}{\{0\}}$ is integral domain then $I = \{0\}$ is Prime ideal.

Q. $R = Q \times R$, find maximal ideals and prime ideals of R.

Solution: $R = Q \times \mathbf{R}$, ideals of $R = Q \times \mathbf{R}$ are $I_1 = \{0\} \times \{0\}$, $I_2 = \{0\} \times \mathbf{R}$, $I_3 = Q \times \{0\}$, $I_4 = Q \times \mathbf{R}$

(1) $\frac{Q \times \mathbf{R}}{I_1} = \frac{Q \times \mathbf{R}}{\{0\} \times \{0\}} \approx Q \times \mathbf{R}$, then $Q \times \mathbf{R}$ is not integral domain then $\frac{Q \times \mathbf{R}}{\{0\} \times \{0\}}$ is not integral domain then $I_1 = \{0\} \times \{0\}$ is not Prime ideal and maximal ideal.

(2) $\frac{Q \times \mathbf{R}}{\{0\} \times \{\mathbf{R}\}} = \frac{Q \times \mathbf{R}}{\{0\} \times \{\mathbf{R}\}} \approx Q \times \{0\} \approx Q$, Q is field then $\frac{Q \times \mathbf{R}}{\{0\} \times \{\mathbf{R}\}}$ is field $I = \{0\} \times \mathbf{R}$ is maximal and Prime ideal.

(3) $\frac{Q \times \mathbf{R}}{I_3} = \frac{Q \times \mathbf{R}}{\{0\} \times \{\mathbf{R}\}} \approx \{0\} \times \mathbf{R} \approx \mathbf{R}$

Since $\mathbf{R}$ is field then $\frac{Q \times \mathbf{R}}{\{0\} \times \{\mathbf{R}\}}$ is field then $I = Q \times \{0\}$ is maximal and Prime.

(4) $\frac{Q \times \mathbf{R}}{Q \times \mathbf{R}} \approx \{0\} \times \{0\} \approx \{0\}$. Since $\{0\}$ is not integral domain then $I_4 = Q \times \mathbf{R}$ is not Prime and maximal.

Q. $R = Q \times \mathbf{R} \times Z_{19}$

Solution: $I_1 = Q \times \mathbf{R} \times \{0\}$, $I_2 = Q \times \{0\} \times Z_{19}$, $I_3 = \{0\} \times \mathbf{R} \times Z_{19}$ maximal ideal of $Q \times \mathbf{R} \times Z_{19}$.

Mindset Makers

(1) $\frac{Q\times\mathbf{R}\times Z_{19}}{Q\times\mathbf{R}\times\{0\}}\approx\{0\}\times\{0\}\times Z_{19}\approx Z_{19}$

Z_{19} is field then $\frac{Q\times\mathbf{R}\times Z_{19}}{Q\times\mathbf{R}\times\{0\}}$ is field then $I_1=Q\times\mathbf{R}\times\{0\}$ is maximal and prime.

(2) $\frac{Q\times\mathbf{R}\times Z_{19}}{Q\times\mathbf{R}\times\{0\}}\approx\{0\}\times\mathbf{R}\times\{0\}$

Q. Show that $I=Q\times\{0\}\times\{0\}$ is not maximal and prime ideal in $Q\times\mathbf{R}\times Z_{19}$.

Solution:

$\frac{Q\times\mathbf{R}\times Z_{19}}{Q\times\{0\}\times\{0\}}\approx\{0\}\times\mathbf{R}\times Z_{19}\approx\mathbf{R}\times Z_{19}$

$\mathbf{R}\times Z_{19}$ is not integral domain then $I=Q\times\{0\}\times\{0\}$ is not maximal and prime ideal.

Q. $I=\langle 2\rangle$ is maximal and prime in Z_8 ?

Solution: $\frac{Z_8}{\langle 2\rangle}=\{0+\langle 2\rangle,1+\langle 2\rangle\}\approx Z_2.Z_2$ is field then $\frac{Z_8}{\langle 2\rangle}$ is field then $I=\langle 2\rangle$ is maximal and prime.

Q. How many maximal ideal in $\frac{Z[i]}{\langle 3+i\rangle}$?

Solution: $\frac{Z[i]}{\langle 3+i\rangle}=\{a+ib+\langle 3+i\rangle\,|\,a+ib\in Z[i]\}\approx Z_{3^2+1^2}\approx Z_{10}$ i.e. $\frac{Z[i]}{\langle 3+i\rangle}\approx Z_{10}$, and Z_{10} has exactly?

maximal ideal then $\frac{Z[i]}{\langle 3+i\rangle}$ has exactly 2 maximal ideal. They are

$\left.\begin{aligned}I_1&=\langle 2+\langle 3+i\rangle\rangle\\ I_2&=\langle 5+\langle 3+i\rangle\rangle\end{aligned}\right\}$ are maximal ideals of $\frac{Z[i]}{\langle 3+i\rangle}$

Q. $I=\langle 2+2i\rangle$ is Prime ideal in $Z[i]$

Solution: $\frac{Z[i]}{\langle 2+2i\rangle}\approx$ Not integral domain,

$I=\langle 2+2i\rangle$ is not Prime ideal

$2\in Z[i], 1+i\in Z[i]$

Another way, $2(1+i)=2+2i\in I$ but $2\notin I$ and $1+i\notin I$ then $I=\langle 2+2i\rangle$ is nor Prime ideal.

Q. Find maximal ideal in $\frac{Z[i]}{\langle 1+i\rangle}\times\frac{Z[i]}{\langle -7i\rangle}\times\frac{Z}{5Z}$?

Solution: $\frac{Z[i]}{\langle 1+i\rangle}\times\frac{Z[i]}{\langle -7i\rangle}\times\frac{Z}{5Z}\approx Z_{2^2+1^2}\times Z_7[i]\times Z_5\approx Z_2\times Z_7[i]\times Z_5$

$Z_2\times Z_7\times Z_5$ has exactly three maximal ideal then R has exactly three maximal ideal.

Mindset Makers

Q. $R=\frac{Z[i]}{\langle 1+i\rangle}\times\frac{Z[i]}{\langle -7i\rangle}\times\frac{Z}{10Z}$, how many maximal ideal of R?

Solution: Maximal ideal of R, $R=Z_2\times Z_7[i]\times Z_{10}$, are

$I_1=Z_2\times Z_7[i]\times 2Z_{10}, I_2=Z_2\times Z_7[i]\times 5Z_{10}, I_3=Z_2\times\{0\}\times Z_{10}, I_4=\{0\}\times Z_7[i]\times Z_{10}$

There are 4 maximal ideal in R.

Q1. $R=\frac{Z[i]}{\langle 1+5i\rangle}$, how many idempotent element?

Ans. 4 idempotent elements as it is $\approx Z$

Q2. $\langle 13i\rangle$ is maximal ideal in $Z[i]$?

Q3. $\langle 3+6i\rangle$ is Prime ideal in $Z[i]$?

Characteristic of Ring: Characteristic of Ring $(R,+,\cdot)$ is the least positive integer n such that $n\cdot a=0\ \forall a\in R$. It is denoted by $\text{char}(R)$. If such n does not exist then $\text{char}(R)=0$.

Example: $Z_4=\{0,1,2,3\}$. Find $\text{char}(Z_4)$ = ?

Solution: $n=4$ such that ; $4\cdot 0=0, 4\cdot 1=0, 4\cdot 2=0, 4\cdot 3=0$ then $\text{char}(Z_4)=4$.

Q. Char (Z_1) = ?

Solution: $n=1$ such that $1\cdot 0=0$ then char $(Z_1)=1$.

Exam Point: $\text{char}(Z_n)=n$

Q. $R=Z$ find $\text{char}(Z)$ = ?

Solution: char (Z) = 0 because n does not exist such that $n\cdot a=0,\ \forall a\in Z$ since Z is an integral domain.

Similarly, Note: Char $(\mathbf{R})$ = Char $(\mathbf{C})$ = Char $(Q)=0$

Q. Char $\frac{Z[i]}{\langle 2+3i\rangle}$ = ?

Solution: $\frac{Z[i]}{\langle 2+3i\rangle}\approx Z_{13}$. $\text{char}(Z_{13})=13$ and as $\frac{Z[i]}{\langle 2+3i\rangle}\approx Z_{13}$ therefore $\text{char}\left(\frac{Z[i]}{\langle 2+3i\rangle}\right)=13$

Q. Char $(Z_3[i])$ = ?

Solution: $Z_3[i]=\{0,1,2,i,2i,1+i,1+2i,2+i,2+2i\}$ $n=3$ s.t $3\cdot a=0,\ \forall a\in Z_3[i]$. $\text{char}(Z_3[i])=3$

Q. (i) $\text{char}(Z\times Z_3[i])$ = ? (ii) char $(Z_2\times Z_4)$ = ?

Solution: (ii) $Z_2\times Z_4=\{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3)\}$

$n=4$ such that $4(a,b)=(0,0),\ \forall(a,b)\in Z_2\times Z_4$

Note: $\text{Char}(R\times S)=\begin{cases}0, \text{if } \text{char}(R)=0 \text{ or } \text{char}(S)=0\\ K; K=\text{LCM}(\text{char}(R),\text{Char}(S))\end{cases}$

Mindset Makers

Q. Char $\left(Z \times Q \times Z_2 \times Z_3[i] \times \frac{Z[i]}{\langle 3+i \rangle} \times \mathbf{R} \right)$

Solution: Zero, because char $(Z) = 0$

Q. Char $(Z[i]) = ?$

Solution: Zero . Q. $Q\sqrt{2}$ is not cyclic because $Q \subseteq Q\sqrt{2}$ and Q is not cyclic.

$Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$ is field.

Q. How many maximal ideal, prime ideal, ideal, idempotent nilpotent and unit in $Q[\sqrt{2}]$?

Solution: 2 ideals, 2 Idempotent elements, 1 Nilpotent elements, ∞ units 1 maximal ideal, 1 Prime Ideal.

Note: Similarly $Q[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in Q\}, d > 0$ and d is not perfect square then $Q[\sqrt{d}]$ is field.

Q. $I = Z \times Z \times \{0\}$ is maximal/Prime ideal in $Z \times Z \times Z$.

Ans. Yes, $\frac{Z \times Z \times Z}{Z \times Z \times \{0\}} \approx Z$ is an integral domain

$\therefore$ It $Z \times Z \times \{0\}$ is Prime Ideal.

Mindset Makers

CHAPTER-3: Ring Homomorphism

Ring Homomorphism: Let $(R, +, \square)$ and $(S, +, \square)$ are two rings. A mapping $f : (R, +, \square) \to (S, +, \square)$ is said to be ring homomorphism if

(1) $f(x+y)=f(x)+f(y)$ (2) $f(x\cdot y)=f(x)\cdot f(y)$

Q. $f:Z\to Z,\ f(x)=0\cdot x$ is Ring homomorphism?

Solution: $f(x)=0\cdot x$

(1) $f(x+y)=0(x+y)=0\cdot x+0\cdot y=f(x)+f(y)$

(2) $f(x\cdot y)=0(x\cdot y)=(0\cdot x)\cdot(0\cdot y)=f(x)\cdot f(y)$

then $f(x)=0\cdot x$ is ring homomorphism.

Definition: $f:R\to R,\ f(x)=0\cdot x$ is called trivial ring homomorphism.

Q. $f:Z\to Z, f(x)=1\cdot x$ is ring homomorphism?

Solution: $f(x)=1\cdot x$

(i) $f(x+y)=1(x+y)=1\cdot x+1\cdot y=f(x)+f(y)$

(ii) $f(x\cdot y)=(1\cdot x)\cdot(1\cdot y)=f(x)\cdot f(y)$

then $f(x)=1\cdot x$ is Ring homomorphism.

Q. $f:Z\to Z,\ f(x)=2x$, is ring homomorphism?

Solution: $f(x)=2x$

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

(2) $f(x\cdot y)=2(x\cdot y)\neq 2x\cdot 2y\neq f(x)\cdot f(y)$

$\therefore f(x)=2x$ is not ring homomorphism.

Exam Point: $f:Z\to Z$ has exactly 2 ring homomorphism say $f(x)=0\cdot x$ and $f(x)=1\cdot x$.

Q. $f:Z_4\to Z_{10}$

$f(x)=5x$, is ring homomorphism?

Solution: $f(x)=5x$

(1) $f(x+y)=5x+5y=f(x)+f(y)$

(2) $f(x\cdot y)=5(x\cdot y)=25xy$ $(25\equiv 5 \bmod 10)$ [25 is idempotent element] $=5x\cdot 5y=f(x)\cdot f(y)$

then $f(x)=5x$ is ring homomorphism for $Z_4\to Z_{10}$.

Q. $f:Z_4\to Z_{10},\ f(x)=6x$ is ring homomorphism?

Solution:(1) $f(x+y)=f(x)+f(y);\ f(x+y)=6(x+y)=6x+6y=f(x)+f(y)$

(2) $f(1+3)=f(0)=6\cdot 0=0;\ f(1)+f(3)=6\cdot 1+6\cdot 3=6+18=24$ (mod 10 applied)= 4

$f(1+3)\neq f(1)+f(3)$ So, $f(x)=6x$ is not ring homomorphism.

Q. $f:Z_4\to Z_{10}$, how many ring homomorphism?

Solution: Idempotent elements of Z_{10} are 0,1,5 and 6

$f(x)=0\cdot x\ \surd,\ f(x)=1\cdot x\ \times,\ f(x)=5\cdot x\ \surd, f(x)=6\cdot x\ \surd$

$f(x)=0\cdot x$ and $f(x)=5\cdot x$ are ring homomorphisms.

Mindset Makers

Here order of 0 in Z_{10} is 1, order of 1 is 10 order of 5 is 2, and order of 6 is 5 which is not possible in Z_4.

Q. $f:Z_5\to Z_{10}, f(x)=5x$ is ring homomorphism.

Solution: 5 is an idempotent element of Z_{10} but $O(5)$ is $Z_{10}=2$ but Z_5 has no element of order 2 then $f(x)=5x$ is not ring homomorphism.

Q. How many ring homomorphism in $f:Z_5\to Z_{10}$.

Solution: 0,1,5 and 6 are idempotent elements of Z_{10}

$f(x)=0\cdot x$ √, $f(x)=1\cdot x$ ×, $f(x)=5\cdot x$ ×, $f(x)=6\cdot x$ √

and $f(x)=6\cdot x$ are only ring homomorphism.

Q. How many ring homomorphism $f:Z_{30}\to Z_{30}$?

Solution: Z_{30} has exactly 8 idempotent elements then $f:Z_{30}\to Z_{30}$ has atmost 8 ring homomorphism 0,1,6,10,15,16,21 and 25.

then $f(x)=0\cdot x$, $f(x)=1\cdot x$, $f(x)=6\cdot x$, $f(x)=10\cdot x$, $f(x)=15\cdot x$, $f(x)=16\cdot x$

$f(x)=21\cdot x$, $f(x)=25\cdot x$ are ring homomorphisms.

Exactly 8-ring homomorphisms.

Exam Point: $f:Z_m\to Z_m$;Number of Ring Homomorphisms = No. of Idempotent Elements in Z_m

Q. How many ring homomorphism in $f:Z_p\to Z_p$?

Solution: Z_p is field then Z_p has exactly two idempotent elements say 0 and 1

$\left.\begin{matrix}f(x)=0\cdot x\\ f(x)=1\cdot x\end{matrix}\right\}$ exactly 2 ring homomorphism

Example: $f:Z_{11}\to Z_{11}$; $\left.\begin{matrix}f(x)=0\cdot x\\ f(x)=1\cdot x\end{matrix}\right\}$ are ring homomorphism

Q. $f:Z_3\to Z_9$, how many ring homomorphism?

Solution: $f(x)=0\cdot x$ $\therefore Z_9$ has exactly 2 idempotent elements

$f(x)=1\cdot x$. this has exactly one ring homomorphism say $f(x)=0\cdot x$

Q. $f:Z_p\to Z_{p^m}$, $m>1$ has exactly one ring homomorphism.

Solution: Explanation: $f:Z_p\to Z_{p^m}$

Z_{p^m} has exactly 2 idempotent elements say 0 and 1.

$f(x)=0\cdot x$ is ring homomorphism

$f(x)=1\cdot x, O(1)$ in $Z_{p^m}=p^m$ and Z_p has no elements of order p^m if $m>1$ then

$f(x)=1\cdot x$ is not ring homomorphism.

Note:

(1) $f:Z_p\to Z_p$, then it has exactly 2 ring homomorphism.

Mindset Makers

(2) $f: Z_p \to Z_{p^m}, m>1$ then it has exactly 1 ring homomorphism.

Q. $f: Z_n \to Z_m$, if $m \mid n$ then how many ring homomorphism?

Solution:

If $m \mid n$, then number of ring homomorphism from $Z_n \to Z_m$ is equal to number of idempotent element is Z_m.

Exam Point: If $f: Z_n \to Z_m$, and $m \mid n$ then No. of Ring homeomorphisms from $Z_n \to Z_m$ = No. of Idempotent elements in Z_m.

Q. $f: Z_8 \to Z_4$, how many ring homomorphism?

Solution: Z_4 has exactly two idempotent elements say 0 and 1.

$f(x)=0\cdot x \to O(0)$ in $Z_4=1$ and Z_8 ahs elements of order 1 then $f(x)=0\cdot x$ is ring homomorphism.

$f(x)=1\cdot x \Rightarrow O(1)$ in Z_4 is 4 and Z_8 has elements of order 4 then $f(x)=1$ is ring homomorphism.

Then, it has exactly 2 ring homomorphism.

Q. $\left.\begin{matrix} f: Z \to Z \\ f: Q \to Q \\ f: \mathbf{R} \to \mathbf{R} \end{matrix}\right\}$ has exactly two idempotent elements say 0 and 1

$\left.\begin{matrix} f(x)=0\cdot x \\ f(x)=1\cdot x \end{matrix}\right\}$ exactly 2 ring homomorphism.

Q. $f: Z \to 2Z$, how many ring homomorphism?

Solution: Exactly one ring homomorphism, say

$f(x)=0\cdot x$

Exam Point: $mz \neq nz$ if m and n are different because we won't get one-one and onto mapping.

Q. $f: Z\times Z \to Z$, how many ring homomorphism?

Solution:

$f: Z\times Z \to Z;\ \left.\begin{matrix} f(x,y)=0 \\ f(x,y)=x \\ f(x,y)=y \end{matrix}\right\}$ are ring homomorphism

Q. $f: Z \to Z\times Z$, how many ring homorphism.

Solution:

$\left.\begin{matrix} f(x)=(0,0)x \\ f(x)=(1,0)x \\ f(x)=(0,1)x \\ f(x)=(1,1)x \end{matrix}\right\}$ are ring homomorphisms.

Here $(0,0),(0,1),(1,0)$ and $(1,1)$ are idempotent elements of $Z\times Z$.

Q. $\mathbf{C}$ is ring isomorphic to $\mathbf{R}$ $(\mathbf{C} \approx \mathbf{R}?)$.

Mindset Makers

Solution: **C** is not ring isomorphic to **R** because $x^4=1$ has 4 solutions in **C** say $(x=1,-1,i,-i)$ but $x^4=1$ has only 2 solutions in **R** say $(x=1,-1)$.

Q. $Q[i]\approx Q$? i.e. $Q[i]$ is ring isomorphic to Q?

Ans. No, reason is same as above.

Q. $Q[i]$ is ring isomorphic to $Q\left[\sqrt{2}\right]$?

Solution: No, because $x^4=1$ has 4 solutions in $Q[i]$ but in $Q\left[\sqrt{2}\right], x^4=1$ has 2 solutions also in $Q\left[\sqrt{2}\right]$, $x^2-2=0$ has solution but $Q[i]$ don't have solution for $x^2-2=0$.

Q. $Q\left[\sqrt{2}\right]\approx Q\left[\sqrt{5}\right]$, is field isomorphic?

Solution: No, it is not field isomorphic because $x^2-2=0$ has solution in $Q\left[\sqrt{2}\right]$ but $x^2-2=0$ has no solution in $Q\left[\sqrt{5}\right]$ i.e. does not exist in $Q\left[\sqrt{5}\right]$.

Q. $f:Z_2\to Z_2$, defined by $f(x)=x^2-x$ is ring homomorphism?

Solution: $f:Z_2\to Z_2;\ f(x)=x^2-x$

(1) $f(x+y)=(x+y)^2-(x+y)=x^2+y^2+2xy-x-y=(x^2-x)+(y^2-y)+2xy$

$=(x^2-x)+(y^2-y)+0 \qquad (\because 2xy=0)\ =f(x)+f(y)$

(2) $f(x\cdot y)=(xy)^2-x=x^2y^2-x^2y-xy^2+xy+x^2y+xy^2=(x^2-x)(y^2-y)+xy(x+y)$

$f(x\cdot y)=(x^2-x)(y^2-y)+xy(x+y)=f(x)f(y)+xy(x+y)$ ....(1)

From (1), $xy(x+y)=0,\ \forall x,y\in Z_2$

Case - I: If $x=0,y=0$, then $xy(x+y)=0\cdot 0(0+0)=0$

Case - II: If $x=0,y=1$ then $xy(x+y)=0\cdot 1(0+1)=0$

Case - III: If $x=1,y=0$ then $xy(x+y)=0$

Case - IV: If $x=1,y=1$ then $xy(x+y)=1\cdot 1(1+1)=1\cdot 2=2=0$

then from all 4 cases, $xy(x+y)=0,\ \forall x,y\in Z_2$

From equation (1) $f(x\cdot y)=f(x)\cdot f(y)+0=f(x)\cdot f(y),\ \forall x,y\in Z_2$

then $f(x)=x^2-x$, is ring homomorphism.

Q. $f:Z_{12}\to Z_{28}$, how many ring homomorphism?

Solution: $f(x)=0\cdot x$ √, $f(x)=1\cdot x$ ×, $f(x)=8\cdot x$ ×, $f(x)=21\cdot x$

√, $f(x)=0\cdot x,\ f(x)=21\cdot x$ are ring-homomorphism. Non-Trivial Ring homomorphism $=2-1=1$.

Mindset Makers

CHAPTER-4
Irreducible Element

Definition: Let $(R,+,\square)$ is an integral domain. A non-zero non-unit element $a \in R$ is said to be irreducible element if $a = bc, b \in R, c \in R$ then either b is unit or c is unit in R.

Example: $a = 6 \in Z$ is irreducible element of Z?

Solution: $6 = 2 \cdot 3$ and $2 \in Z, 3 \in Z$ but neither 2 nor 3 is unit in Z then 6 is not irreducible element of Z.

Q. $a = 11 \in Z$ is irreducible element in Z?

Solution: $11 = 11 \cdot 1 = b \square c \,.\, b = 11 \in Z, c = 1 \in Z$ and 1 is unit in Z then 11 is irreducible element in Z.

Q. –11 is irreducible over Z?

Solution: $-11 = 11 \times (-1) = b \cdot c,\ b = 11 \in Z,\ c = -1 \in Z$

and –1 is unit in Z then -11 is irreducible element over Z.

Q. 2 is irreducible over $Z[i]$?

Solution: No, $2 = (1+i)(1-i) = b \square c,\ b \in Z[i], c \in z[i]$

but neither $b = (1+i)$ nor $c = (1-i)$ is unit in $Z[i]$ therefore 2 is not irreducible over $Z[i]$.

Q. $a = 2 \in Z$ is irreducible over Z?

Solution: Yes, because. $2 = 2 \times 1 = b \cdot c,\ b \in Z, c \in Z$ .1 is unit in Z then 2 is irreducible element over Z.

Q. 3 is irreducible over $Z[i]$?

Solution: 3 is irreducible element in $Z[i]$

Q. Show that $1+i$ is irreducible over $Z[i]$

Solution:Let $1+i = (1+ib)(c+id)$ ....(1)

taking conjugate of equation (1)

$1-i = (a-ib)(c-id)$ ....(2)

Multiplying side by side of equation (1) and (2),

$(1+i)(1-i) = (a^2+b^2)(c^2+d^2) \Rightarrow 2 - (a^2+b^2)(c^2+d^2)$ ....(3)

Case I: If $a^2+b^2 = 2$ then $c^2+d^2 = 1 \Rightarrow (c+id)(c-id) = 1 \Rightarrow c+id$ is unit in $Z[i]$

Case II: If $c^2+d^2 = 2$ then $a^2+b^2 = 1 \Rightarrow (a+ib)(a-ib) = 1 \Rightarrow a+ib$ is unit in $Z[i]$

From case I and II, we conclude either $c+id$ is unit or $a+ib$ is unit of $Z[i]$ then $1+i$ is irreducible over $Z[i]$.

Q. Show that $1-i$ is irreducible over $Z[i]$?

Mindset Makers

Q. Show that 3 is irreducible element in $Z[i]$?

Solution: Let $a=3\in Z[i]$ and

$3=(a+ib)(c+id)$ ....(1)

Taking conjugate,

$3=(a-ib)(c-id)$ ....(2)

From (1) and (2), multiplying side by side

$9=(a^2+b^2)(c^2+d^2)$ ....(3)

Case I : If $a^2+b^2=9$ then $c^2+d^2=1\Rightarrow(c+id)(c-id)=1\Rightarrow(c+id)$ is unit in $Z[i]$

Case II: If $c^2+d^2=9$ then $a^2+b^2=1\Rightarrow(a+ib)(a-ib)=1\Rightarrow a+ib$ is unit in $Z[i]$

Case II: If $a^2+b^2=3$ then $c^2+d^2=3$ no, a,b,c and d exists in Z such that $a^2+b^2=3$ and $c^2+d^2=3$ then case III not possible.

Hence, from case I and II, we conclude that either $a+ib$ or $c+id$ is unit then 3 is irreducible element in $Z[i]$.

Q. 5 is not irreducible element in $Z[i]$

Solution: $5=(2+i)(2-i)$, but neither $2+i$ nor $2-i$ is unit in $Z[i]$ then 5 is not irreducible over $Z[i]$.

Q. $3+\sqrt{-5}$ irreducible over $Z\left[\sqrt{-5}\right]$?

Solution: $Z\left[\sqrt{-5}\right]=\left\{a+b\sqrt{-5}\mid a,b\in Z\right\}=\left\{a+ib\sqrt{5}\mid a,b\in Z\right\}$

$\alpha=3+\sqrt{-5}=3+\sqrt{5}i\in Z\left[\sqrt{-5}\right]$

Let $3+\sqrt{5}i=\left(a+ib\sqrt{5}\right)\left(c+id\sqrt{5}\right)$ ....(1)

taking conjugate of equation (1)

$3-\sqrt{5}i=\left(a-ib\right)\left(c-id\sqrt{5}\right)$ ....(2)

From (1) and (2), multiplying side by side

$9-i^2 5=\left(a-i^2 5b^2\right)\left(c^2-i^2 5d^2\right)\Rightarrow 14=\left(a^2+5b^2\right)\left(c^2+5d^2\right)$ ....(3)

Case I: If $a^2+5b^2=14$ then $c^2+5d^2=1\Rightarrow\left(c+id\sqrt{5}\right)$ is unit

Case II: If $c^2+5d^2=14$ then $a^2+5d^2=1\Rightarrow a+ib\sqrt{5}$ is unit.

Case III: If $a^2+5b^2=7$ then $c^2+5d^2=2$, so, this is not possible because a,b,c and $d\in Z$.

From case I, and II, we conclude that either $a+ib\sqrt{5}$ is unit or $c+id\sqrt{5}$ is unit then $3+\sqrt{-5}$ is irreducible element in $Z\sqrt{-5}$.

Q. $\alpha=3+i$, is irreducible over $Z[i]$?

Solution: $3+i=(2-i)(1+i)$ but neither $2-i$ is unit in $Z[i]$ nor $(1+i)$ is unit in $Z[i]$.Then it is reducible over $Z[i]$.

Q. Show that $I=\langle 2,x\rangle$ is ideal of $Z[x]$.

Solution: Let $Z[x]=\left\{a_0+a_1x+...+a_nx^n\mid a_i\in Z\right\}$

Mindset Makers

$I=\langle 2,x\rangle=\{2f(x)+xg(x)\mid f(x),g(x)\in Z[x]\}$ ..(1)

$h(x)\in I\Rightarrow h(x)=2f_1(x)+xg_1(x), k(x)\in I\Rightarrow k(x)=2f_2x_1+xg_2(x)$

$h(x)-k(x)=2(f_1(x)-f_2(x))+x(g_1(x)-g_2(x))=2f_3(x)+xg_3(x),\ f_3(x)\in Z[x],$

$g_3(x)\in Z[x]\Rightarrow 2f_3(x)+xg_3(x)\in I\Rightarrow h(x)-kx\in I=\langle 2,x\rangle \ldots(2)$

$h(x)\in I\Rightarrow h(x)=2f_1(x)+xg(x)$

$r(x)\in Z[x]\Rightarrow h(x)r(x)=2f_1(x)r(x)+xg(x)r(x)$

$=2f'(x)+xg'(x),\ f'(x)\in Z[x],\ g'(x)\in Z[x]\Rightarrow h(x)r(x)\in I=\langle 2,x\rangle$

then $I=\langle 2,x\rangle$ is an ideal of $Z[x].\Rightarrow \boxed{\frac{Z[x]}{\langle 3,x\rangle}\approx Z_3}$

Prime Element: Let $(R,+,\square)$ is an integral domain A non-zero, non-unit element $a\in R$ is said to be Prime element if $a\mid bc, b\in R, c\in R\Rightarrow$ either $a\mid b$ or $a\mid c$.

Example: $a=7$ in Z , $a=7$ is Prime element in Z.

Solution: Yes $7=7\square 1$, then; $7\mid 7\Rightarrow 7\mid 7$, 7 is Prime

Q. $a=6$ in Z, $a=6$ is Prime in Z?

Solution: $6\mid 6=2\square 3$ i.e. $6\mid\!=2\square 3$ but 6×2 and 6×3 then 6 is not Prime.

Q. $a=30$, is Prime?

Solution: $30\mid 30$ i.e. $30\mid 10\cdot 3$ but 30×10 and 30×3 then 30 is not Prime.

Q. 5 is Prime in $Z[i]$?

Solution: $5\mid 5\Rightarrow 5\mid(2+i)(2-i)$ but $5\times 2+i$ and $5\times 2-i$ then 5 is not Prime.

Q. 2 is Prime in $Z[i]$?

Solution: $2\mid 2$ i.e. $2\}(1+i)(1-i)$ but $2\times(1+i)$ and $2\times(1-i)$ then 2 is not prime in $Z[i]$.

Q. If 'a' is Prime element then 'a' is irreducible element.

Solution: Let $(R,+,\square)$ is an Integral domain and let $a\in R$ is Prime element and

$a=bc$ ....(1)

Since 'a' is prime then $a\mid a\Rightarrow a\mid bc\Rightarrow a\mid b$ or $a\mid c$

If $a\mid b$ then $\exists$ some $t\in R$ s.t. $b=at$ ....(2)

From (1) and (2); $b=bct\Rightarrow b-bct=0\Rightarrow b(1-ct)=0$

$\Rightarrow 1-ct=0;\ b\neq 0$ [$\because$ b cannot be zero since a is prime i.e. b is nonzero multiplicative inverse of c is t]

$\Rightarrow 1=ct\Rightarrow ct=1\Rightarrow c$ is unit in R. Similarly, $a\mid c$ then b is unit in R.

$a=bc$ then either b is unit or c is unit then a is irreducible elements. Then, every prime is irreducible.

Q. 3 is prime in $Z[i]$?

Solution:Yes, if $3\mid bc$ then $3\mid b$ or $3\mid c$, where $b\in Z[i], c\in Z[i]$

Note:

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

(ii) $x=a+i0$ and $|x|=p$, $4\mid p-3$ then x is prime in $Z[i]$

Mindset Makers

(iii) $x=a+ib$ and $|x|=p$, $4 \mid p-3$ then x is prime is $Z[i]$

Prime element in $Z[i]$ is known as Gaussian Prime.

Q. $\alpha=3+\sqrt{-5}$ is prime in $Z\left[\sqrt{-5}\right]$?

Solution: $\alpha=3+\sqrt{-5}=3+\sqrt{5}i$

$3+\sqrt{-5} \mid \left(3+\sqrt{5}i\right)\left(3-\sqrt{5}i\right)$, $3+\sqrt{-5} \mid 14$, $3+\sqrt{-5} \mid 7\square 2$

but $3+\sqrt{-5}\times 7$ and $3+\sqrt{-5}\times 2$ the $3+\sqrt{-5}$ is not prime in $Z\left[\sqrt{-5}\right]$.;

$\left(3+\sqrt{5}i\right)\left(3-\sqrt{5}i\right)=14$

Q. 13 is prime in $Z[i]$?

Solution: $13 \mid 13$, $13 \mid (2+3i)(2-3i)$ but $13\times(2+3i)$ and $13\times(2-3i)$ then 13 is not prime in $Z[i]$

Q. $3+i$ is prime in $Z[i]$

Solution: $3+i \mid (2-i)(2+i)$ but $3+i\times(2-i)$ and $3+i\times 1+i$

or $3+i \mid (3+i)(3-i)$; $3+i \mid 10=5\times 2$

but $3+i\times 5$ and $3+i\times 2$ then $3+i$ is not prime in $Z[i]$.

Associate: Let $(R,+,\cdot)$ be an integral domain An element $a\in R$ is said to be associate to $b\in R$ if $\exists$ unit $U\in R$ s.t $a=Ub$

Q. -1 is associate to 1 in Z

Solution: Yes $a=Ub$. $-1=(-1)1$. -1 is unit in Z.

Q. i and $-i$ are associate in $Z[i]$

Solution: $i=(-1)(-i)$ and -1 is unit in $Z[i]$

Q. $2+3i$ and $2i-3$ are associate in $Z[i]$?

Solution: Yes $2i-3=i(2+3i)$. $a=U\square b$. $i\in Z[i]$ s.t i is unit in $Z[i]$

Irreducible Polynomial:

Note: (1) R is commutative ring then $R[x]$ is also commutative ring.

(2) If R is commutative ring with Unity then $R[x]$ is commutative ring with unity.

Explanation:

Suppose 1 is unity of R then

$f(x)=1+0.x+0.x^2+....+0.x^n\in R[x]$

s.t $f(x).g(x)=g(x)$, $\forall g(x)\in R[x]$

(3) If R is an integral domain then $R[x]$ is also integral domain.

Explanation:

$0\neq f(x)\in R[x]$

$0\neq g(x)\in R[x]$

$f(x).g(x)\neq 0$, if R is integral domain.

Mindset Makers

(4) If R is field then $R[x]$ is an integral domain ($R[x]$ is not field because $x \in R[x]$ but $x^{-1} \notin R[x]$ s.t $xx^{-1} = x^{-1}x = 1$).

Irreducible Polynomial: Let $(R,+,\square)$ be an integral domain. A non-zero, non-unit polynomial $f(x) \in R[x]$ is said to be Irreducible Polynomial if $f(x) = g(x).h(x)$ where $g(x) \in R[x]$ and $h(x) \in R[x]$ thin either $g(x)$ is unit or $h(x)$ is unit in $R[x]$.

Example: $f(x) = 2x^2 + 6$ is irreducible over Q?

Solution: $f(x) = 2x^2 + 6 = 2(x^2 + 3) = g(x).h(x)$, where $g(x) = 2$ and $h(x) = x^2 + 3$

$g(x) \in Q[x]$ and $h(x) = x^2 + 3 \in Q[x]$. $g(x) = 2$ is unit in $Q[x]$ then $f(x) = 2x^2 + 6$ is irreducible over Q.

Q. $f(x) = 2x^2 + 6$, is irreducible over z?

Solution:

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

$= g(x).h(x)$, where $g(x) = 2 \in z[x]$, $h(x) = x^2 + 3 \in Z[x]$

but neither $g(x)$ is unit nor $h(x)$ in unit in $Z[x]$ then $f(x) = 2x^2 + 6$ is reducible over Z.

Q. $f(x) = 2x^2 - 4$ is irreducible over Q?

Solution:

$f(x) = 2x^2 - 4 = 2(x^2 - 2) = g(x).h(x)$, where $g(x) = 2 \in Q[x]$, $h(x) = (x^2 - 2) \in Q[x]$

$g(x) = 2$ is unit in $Q[x]$ then $f(x) = 2x^2 - 4$ is irreducible over Q.

Q. $f(x) = 2x^2 - 8$, is irreducible over Q?

Solution: $f(x) = 2x^2 - 8 = 2(x^2 - 4) = g(x).h(x)$ ....(1)

where $g(x) = 2 \in Q[x]$ and $h(x) = x^2 - 4 \in Q[x]$

$g(x) = 2$ is unit in $Q[x]$ but $f(x)$ is not irreducible because $h(x)$ is not irreducible.

From equation (1)

$f(x) = g(x).h(x) = g(x).(x^2 - 4) = g(x)(x-2)(x+2)$

then $f(x) = g(x)(x-2)(x+2) = g(x)h_1(x)h_2(x)$

$h(x) = h_1(x).h_2(x)$

$h_1(x) = (x-2) \in Q[x]$

$h_2(x) = (x+2) \in Q[x]$, but neither $h_1(x)$ nor $h_2(x)$ is unit in $Q[x]$.

Then, $h(x)$ is reducible over Q. $\Rightarrow f(x) = g(x).h(x)$ is reducible over Q.

Note: If $f(x) = g(x).h(x)$ and $g(x)$ s unit then the behaviour of $f(x)$ is depending on $h(x)$, i.e. $h(x)$ is irreducible then $f(x)$ is irreducible and if $h(x)$ is reducible then $f(x)$ is reducible.

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

Mindset Makers

Solution: $f(x)=x^2+1=(x+i)(x-i)=g(x).h(x)$, where $g(x)=(x+i)\in \mathbf{C}[x]$ and $h(x)=(x-i)\in C[x]$ but neither $g(x)$ nor $h(x)$ is unit in $\mathbf{C}$.

$\mathbf{C}[x]$ then $f(x)$ is reducible over $\mathbf{C}$.

Q. $f(x)=x^2+1$, is irreducible over $\mathbf{R}$ and Q?

Solution: $f(x)=x^2+1$ is irreducible over $\mathbf{R}$ and Q.

Einestein's Irreducible Criteria

Let $f(x)=a_0+a_1x+....+a_nx^n\in Z[x]$. If there exist prime p such that $p\mid a_0, p\mid a_1 .... p\mid a_{n-1}$ but p does not divide a_n and $p^2 notdivide a_0$ then $f(x)$ is irreducible over Q.

Q. $f(x)=3+6x+12x^2+x^3\in Z[x]$ is irreducible over Q?

Solution:

$f(x)=3+6x+12x^2+x^3$

$p=3$, such that $3\mid 3, 3\mid 6, 3\mid 12$ but $3\nmid 1$ and $3^2\nmid 3$ then $f(x)$ is irreducible over Q.

Q. $f(x)=12+6x+18x^3+x^4$, is irreducible over Q?

Solution:

Given, $f(x)=12+6x+18x^3+x^4$

i.e., $f(x)=12+6x+0.x^2+18x^3+x^4$

$\exists\ p=3$ such that $3\mid 12,\ 3\mid 0,\ 3\mid 18$, but $3\nmid 1$ and $3^2\nmid 12$ then $f(x)$ is irreducible over Q.

Q. $f(x)=x^2+1\in Z[x]$ is irreducible over Q?

Solution:

$f(x)=x^2+1\in Z[x]$ does not satisfies E.I.C. but $f(x)$ is irreducible over Q.

Note:
Let $\mathbf{F}$ is field and $0\neq a\in \mathbf{F}$
(i) If $f(ax)$ is irreducible $\mathbf{F}$ then $f(x)$ is irreducible over $\mathbf{F}$.
(ii) If $a.f(x)$ is irreducible over $\mathbf{F}$ then $f(x)$ is irreducible $\mathbf{F}$.
(iii) If $f(x+a)$ is irreducible over $\mathbf{F}$ then $f(x)$ is irreducible over $\mathbf{F}$.

Q. Show that $f(x)=x^2+1$ is irreducible over Q by E.I.C.?

Solution: $f(x)=x^2+1$ ....(1)

$0\neq a=1\in Q$

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

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

From equation (2)

$p=2$ such that $2\mid 2,\ 2\mid 2$, but $2\nmid 1$ and $2^2\nmid 2$ then $f(x+1)$ is irreducible over Q.

$\Rightarrow f(x)$ is irreducible over Q.

Q. $f(x)=x$ is irreducible over Q by E.I.C.?

Mindset Makers

Solution: $f(x)=x$ ....(1)

Put $x=x+2$

$f(x+2)=x+2=2+x$ ....(2)

From equation (2)

$p=2$, s.t $2|2$, $2\nmid 1$ and $2^2\nmid 2$ then $f(x+2)$ is irreducible over Q.

$\Rightarrow f(x)=x$ is irreducible over Q.

Q1. Show that $f(x)=1+x+x^2+.....+x^{p-1}$ is irreducible over Q.

Solution: $f(x)=1+x+x^2+....+x^{p-1}$ ....(1)

$f(x)=\dfrac{x^p-1}{x-1}$ ....(2)

This is G.P. then $\dfrac{a^r-1}{a-1}$

$0\neq 1\in Q$ such that

$$f(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=\frac{1}{x}\left[(x+1)^p-1\right]=\frac{1}{x}\left[\left(1+px+p\frac{(p-1)x^2}{2!}+....+x^p\right)-1\right]$$

$$=\frac{1}{x}\left[px+\frac{p(p-1)x^2}{2!}+....+x^p\right]$$

$$f(x+1)=p+\frac{p(p-1)}{2!}x+....+x^{p-1}$$ ....(3)

$\exists\ p$ such that $p\mid p, p\mid p\dfrac{(p-1)}{2!}....p\mid p$ but $p\nmid 1$ and $p^2\nmid p$ then $f(x+1)$ is irreducible over Q then $f(x)$ is irreducible over Q.

Q2. $f(x)=1-x+x^2-x^3+....+x^{p-1}$ is irreducible over Q?

Solution: $f(x)=1-x+x^2-x^3+....+x^{p-1}$

$0\neq -1\in Q$ such that $f(-1x)=f(-x)=1+x+x^2+....+x^{p-1}$

$f(-x)$ is irreducible over Q then $f(x)$ is irreducible over Q. (By above question).

Q3. $f(x)=-1-x-x^2-x^3....x^{p-1}$, is irreducible over Q.

Solution: $f(x)=-1-x-x^2-x^3....x^{p-1}$ ....(1)

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

$(-1)f(x)$ is irreducible over Q then by above question (1), $f(x)$ is irreducible over Q.

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

Solution: Let $f(x)=x^2+1=(x+a)(x+b)$ ....(1)

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

From equation (2)

$a+b=0$ ....(3)

$ab=1$ ....(4)

Mindset Makers

Choose a and b from Z_7 s.t $a+b=0$,

	a	b	$a+b=0$	
(i)	0	0	$0+0=0$	Mod 7 applied
(ii)	1	6	1+6 = 0	
(iii)	2	5	2+5 = 0	
(iv)	3	4	3+4 = 0	

No, such pair exit in Z_7 such that $a+b=0$ and $a.b=1$ then $f(x)=x^2+1\neq(x+a)(x+b)$ then $f(x)$ is irreducible over Z_7.

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

Solution: Let $f(x)=x^2+x+5=(x+a)(x+b)$ ....(1)

$x^2+x+5=x^2+(a+b)x+ab$ ....(2)

then

$a+b=1$ ....(3)

$ab=5$ ....(4)

Choose a and b in Z_{11} s.t $a+b=1$

a	b	$a+b=1$	
1	0	1+0=1	Mod 11 is applied
2	10	2+10=1	
3	9	3+9=1	
4	8	4+8=1	
5	7	5+7=1	
6	6	6+6=1	

satisfied $a+b=1$ and $a.b=5$

$a=3$

$b=9$

s.t. $a.b=5\Rightarrow 3.9=5 \pmod{11}$

From (1),

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

Note: (1) $f(x)\in Z_p[x]$ if $f(x)\neq 0,\ \forall x\in Z_p$ then $f(x)$ is irreducible over Z_p.

(2) If **F** is field and $f(x)$ is single degree polynomial then $f(x)$ is irreducible over **F**.

* If **F** is not field then above result (2) need not be true

e.g. $f(x)=6x$ is single degree polynomial but not irreducible over Z.

$f(x)=6x=g(x).h(x),\ g(x)=6\in Z[x],\ h(x)=x\in Z[x]$

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

Then $f(x)$ is not irreducible over Z.

Note:

3. If $f(x)\in Z[x]$ and if degree of $f(x)>1$ then $f(x)$ is always reducible over **C**.

4. If $f(x)\in Z[x]$ and degree of $f(x)>2$ then $f(x)$ is always reducible over **R**.

Mindset Makers

Explanation: Let $f(x)\in Z[x]$ and degree of $f(x)=4$ and $f(x)$ has no real roots then $f(x)$ has imaginary roots say, $a\pm ib$ and $c\pm id$ such that

$$f(x)=\Big(x-(a+ib)\Big(x-(a-ib)\Big(x-(c+id)\Big(x-(c-id)\Big)\Big)\Big)\Big)$$

$$=\Big((x-a)-ib\Big)\Big((x-a)+ib\Big)\Big((x-c)-id\Big)\Big((x-c)+id\Big)$$

$$=\Big((x-a)^2+b^2\Big)\Big((x-c)^2+d^2\Big)$$

$$=g(x).h(x)$$

where $g(x)=\Big((x-a)^2+b^2\Big)\in\mathbf{R}[x]$ and $h(x)\Big((x-c)^2+d^2\Big)\in\mathbf{R}[x]$

but neither $g(x)$ is unit in $\mathbf{R}[x]$ nor $h(x)$ is unit in $\mathbf{R}[x]$ then $f(x)$ is reducible over $\mathbf{R}$.

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

Solution:

$x^2+1\in Z_7[x]$

$Z_7=\{0,1,2,3,4,5,6\}$

$f(0)=1,\ f(1)=2,\ f(2)=5,\ f(3)=10=3\ (\text{mod})$

$f(4)=3,\ f(5)=5,\ f(6)=2$

$f(x)\neq 0,\ \forall x\in Z_7$, thus $f(x)$ is irreducible over Z_7.

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

Solution: $f(x)=1+x^2$, $Z_2=\{0,1\}$

then $f(0)=1,\ f(1)=2=0\ (\text{mod } 2)$

here $f(x)=0\quad f(1)=0$ therefore $f(x)$ is not irreducible over Z_2 i.e. it is reducible over Z_2.

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

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

$f(0)=123123=0\ (\text{mod } 3)$

then $f(x)$ is reducible over Z_3 i.e. not irreducible.

Q. $f(x)=x^3+312312x+123123$, is irreducible over $Z_7\,|\,Z_{13}$?

Solution: No, it is reducible over Z_7 and Z_{13}.

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

Solution: $f(x)=x^3+312312x+123123\in Z[x]$

$\exists\ p=3$ such that $3|123123, 3|312312, 310$, but 3×1 and $3^2\times 123123$ then $f(x)=x^3+312312x+123123$ is irreducible over Q.

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

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

Mindset Makers

$Z_2 = \{0,1\}$. $f(0)=1, f(1)=1$

$f(x) \neq 0, \forall x \in Z_2$ then $f(x) = 1+x+x^2$ is irreducible over Z_2.

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

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

$Z_3 = \{0,1,2\}$. $f(0)=1, f(1)=1, f(2)=1$

$f(x) \neq 0, \forall x \in Z_3$ then $f(x)$ is irreducible over Z.

Galois Field

Definition: If **F** is **finite** field of **order p** and $f(x) \in \mathbf{F}[x]$ is **irreducible** polynomial over **F** of degree *n*. Then $\dfrac{\mathbf{F}[x]}{\langle f(x) \rangle}$ is field of order p^n. It is denoted by $G\mathbf{F}(p^n)$ where p is prime.

$$G\mathbf{F}(p^n) = \frac{\mathbf{F}[x]}{\langle f(x) \rangle} = \{a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + < f(x) > | \, a_i \in \mathbf{F}\}$$

i.e.

$$G\mathbf{F}(p^n) = \frac{Z_p[x]}{\langle f(x) \rangle} = \{a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + \langle f(x) \rangle | \, a_i \in z_p\}$$

where **F** is field of order p and $f(x)$ is irreducible polynomial over **F** of degree '*n*'.

Q. Construct Galois Field of order 2?

Solution:

$$G\mathbf{F}(2^1) = \frac{Z_2[x]}{\langle x \rangle} = \{a_0 + \langle x \rangle | \, a_0 \in Z_2$$

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

$$\approx Z_2$$

Q. Construct Galois Field of order 3.

Q. Construct Galois field of order 4.

Solution:

$$G\mathbf{F}(4) = G\mathbf{F}(2^2) = \frac{Z_2[x]}{\langle f(x) \rangle} = \{a_0 + a_1x + \langle f(x) \rangle | \, a_i \in Z_2$$

where $f(x)$ is irreducible polynomial of degree 2 over Z_2.

$$G\mathbf{F}(2^2) = \frac{Z_2[x]}{\langle 1+x+x^2 \rangle} = \{a_0 + a_1x + \langle 1+x+x^2 \rangle | \, a_0, a_1 \in Z_2\} \quad ....(1)$$

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

each non-zero elements of $\dfrac{Z_2[x]}{\langle 1+x+x^2 \rangle}$ has multiplicative inverse.

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

$$\Rightarrow 1+x+x^2 = 0 \quad ....(2)$$

Mindset Makers

$1+\langle 1+x+x^2\rangle \in \dfrac{Z_2[x]}{\langle 1+x+x^2\rangle}$ such that

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

$x+\langle 1+x+x^2\rangle \in \dfrac{Z_2[x]}{\langle 1+x+x^2\rangle}$ s.t.

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

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

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

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

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

$= 1+\langle 1+x+x^2\rangle$; under modulo 2

From equation (2) $1+x+x^2=0$

$\Rightarrow x+x^2=-1$

Q. Construct Galois Field of order 8

Solution:

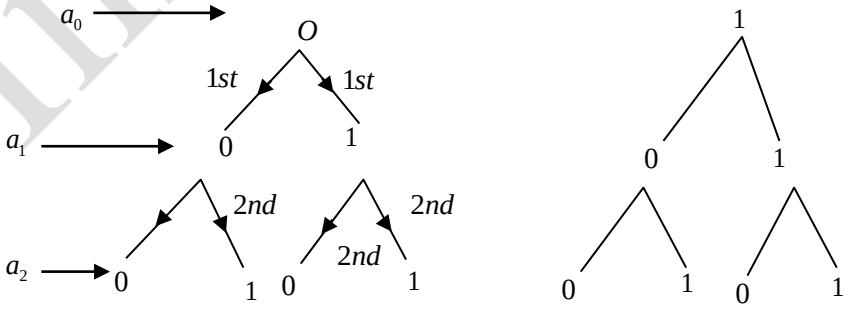
$$GF(8)=GF(2^3)=\frac{Z_2[x]}{\langle f(x)\rangle}$$

$$=\left\{a_0+a_1x+a_2x^2+\langle f(x)\rangle \mid a_0,a_1,a\in Z\right\}$$

where $f(x)$ is irreducible polynomial of degree 3 $f(x)=1+x+x^3$ is irreducible polynomial over Z_2 or degree 3.

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

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



Q. How many elements in $\dfrac{Z_2[x]}{\langle 1+x+x^3\rangle}$ such that $x^7=1$ but $x^k\neq 1, k<7$

Solution:

Mindset Makers

$x+\langle 1+x+x^3\rangle \in \dfrac{Z_2[x]}{\langle 1+x+x^3\rangle}$ such that

$\left(x+\langle 1+x+x^3\rangle\right)^2 = x^2+\langle 1+x+x^3\rangle$

$\left(x+\langle 1+x+x^3\rangle\right)^3 = x^3+\langle 1+x+x^3\rangle$

$= -1-x+\langle 1+x+x^3\rangle$

$= 1+x+\langle 1+x+x^3\rangle$ [After using modulo 2]

$\left(x+\langle 1+x+x^3\rangle\right)^4 = \left(x+\langle 1+x+x^3\rangle\right)\left(1+x+\langle 1+x+x^3\rangle\right)$

$= x+x^2+\langle 1+x+x^3\rangle$

$\left(x+\langle 1+x+x^3\rangle\right)^5 = \left(x+x^2+\langle 1+x+x^3\rangle\right)\left(x+\langle 1+x+x^3\rangle\right)$

$= x^2+x^3+\langle 1+x+x^3\rangle$

$= x^2-1-x+\langle 1+x+x^3\rangle$

$= 1+x+x^2+\langle 1+x+x^3\rangle$

$\left(x+\langle 1+x+x^3\rangle\right)^6 = x\left(1+x+x^2\right)+\langle 1+x+x^3\rangle$

$= x+x^2+x^3+\langle 1+x+x^3\rangle$

$= -1+x^2+\langle 1+x+x^3\rangle$

$= 1+x^2+\langle 1+x+x^3\rangle$

$\left(x+\langle 1+x+x^3\rangle\right)^7 = x\left(1+x^2\right)+\langle 1+x+x^3\rangle$

$= x+x^3+\langle 1+x+x^3\rangle$

$= -1+\langle 1+x+x^3\rangle$

$= 1+\langle 1+x+x^3\rangle$

$0+\langle 1+x+x^3\rangle$ will give $0+\langle 1+x+x^3\rangle$ at any power and $1+\langle 1+x+x^3\rangle$ is unity will be as it is at any power.

$\therefore$ No. of elements are = 6

Q. Construct Galois field of order 9.

Solution:

$$GF\left(3^2\right) = \frac{Z_3[x]}{\langle 1+x^2\rangle} = \left\{a_0+a_1x+\langle 1+x^2\rangle \mid a_i \in Z_3\right.$$

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

$\approx Z_3 \times Z_3$

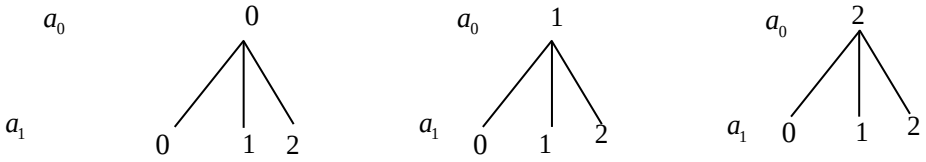
$f(x) = 1+x^2,\ Z_3 = \{0,1,2\}$

$f(0) = 1$

Mindset Makers

$f(1)=2$

$f(2)=5=2$ then $f(x)$ is irreducible over Z_3.



Q. How many elements in $\frac{Z_3[x]}{\langle 1+x^2\rangle}$ such that $x^8=1$ but $x^k\neq 1$ if $k<8$.

Q. Construct Galois Field of order 27

Solution:

$$GF(27)=GF(3^3)=\frac{Z_3[x]}{\langle 1+2x+x^3\rangle}$$

$$=\{a_0+a_1x+a_2x^2+\langle 1+2x+x^3\rangle\}$$

Q. $I=\langle 1+x+x^2\rangle$ is maximal ideal in $Z_2[x]$?

Solution:

$I=\langle 1+x+x^2\rangle$ ....(1)

$f(x)=1+x+x^2$ is irreducible polynomial then $\frac{Z_2[x]}{\langle 1+x+x^2\rangle}$ is field then

$I=\langle 1+x+x^2\rangle$ is maximal ideal.

Q. How many ideal in $\frac{Z_3[x]}{\langle 1+2x^2+x^3\rangle}$

Solution:

$I=\langle 1+2x^2+x^3\rangle$

$f(x)=1+2x^2+x^3$ is irreducible over Z_3 then $\frac{Z_3[x]}{\langle 1+2x^2+x^3\rangle}$ is field of order 27 then

$\frac{Z_3[x]}{\langle 1+2x^2+x^3\rangle}$ has exactly two ideal say,

$I_1=\{0+\langle 1+2x^2+x^3\rangle\}$, $I_2=\frac{Z_3[x]}{\langle 1+2x^2+x^3\rangle}$

$\downarrow$ Maximal ideal

Q. How many ideal in $Q\times\frac{Z_3[x]}{\langle 1+x^2\rangle}$?

Solution:

$$R=Q\times\frac{Z_3[x]}{\langle 1+x^2\rangle}=Q\times GF(3^2)$$

Ideal of $Q\times GF(3^2)$ are

Mindset Makers

$I_1 = \{0\} \times \{0\}$

$I_2 = \{0\} \times G\mathbf{F}\{3^2\}$

$I_3 = Q \times \{0\}$

$I_4 = Q \times G\mathbf{F}(3^2)$

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

Solution:

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

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

$\Rightarrow 1 + x^2 = 0$

$\Rightarrow x = \pm i$ ....(2)

From equation (1) and (2), we get

$$\frac{Q[x]}{\langle 1+x^2 \rangle} = \{a_0 + a_{1i} + \langle 1 + x^2 \rangle \mid a_i \in Q\}$$

$\approx Q[i]$

$Q[i]$ is field then $\frac{Q[x]}{\langle 1+x^2 \rangle}$ is field then ideal $\langle 1 + x^2 \rangle$ is Maximal and prime.

Q. Show that $\langle 1 + x^2 \rangle$ is maximal /prime ideal in $\mathbf{R}[x]$

Solution:

$$\frac{\mathbf{R}[x]}{\langle 1+x^2 \rangle} = \{a_0 + a_1 x + \langle 1 + x^2 \rangle \mid a_i \in \mathbf{R}\}$$

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

$$\frac{\mathbf{R}[x]}{\langle 1+x^2 \rangle} = \{a_0 + a_1 x + \langle 1 + x^2 \rangle \mid a_i \in \mathbf{R}\}$$

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

$\Rightarrow 1 + x^2 = 0$

$\Rightarrow x = \pm i$

$$\frac{\mathbf{R}[x]}{\langle 1+x^2 \rangle} = \{a_0 + a_1 i + \langle 1 + x^2 \rangle \mid a_i \in \mathbf{R}\}$$

$\approx \mathbf{R}[i] = 0$

ϕ is field then $\frac{\mathbf{R}[x]}{\langle 1+x^2 \rangle}$ is field then $I = \langle 1 + x^2 \rangle$ is maximal ideal and prime ideal.

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

Solution:

Mindset Makers

$$\frac{\mathbf{R}[x]}{\langle 3+x^2\rangle}=\{a_0+a_2x+\langle 3+x^2\rangle \mid a_i\in \mathbf{R}\}$$

$3+x^2=0$

$x=\pm\sqrt{3}i$ ....(2)

From (1) and (2)

$$\frac{\mathbf{R}[x]}{\langle 3+x^2\rangle}=\{a_0+a_2\sqrt{3}i+\langle 3+x^2\rangle \mid a_i\in \mathbf{R}\}$$

$$=\{a_0+a_2i+\langle 3+x^2\rangle \mid a_i\in \mathbf{R}\}$$

$\approx \mathbf{R}[i]$

$\mathbf{R}[i]$ is field then $I=\langle 3+x^2\rangle$ is maximal ideal.

Q. $I=\langle x\rangle$ is Prime ideal but not maximal ideal in $Z[x]$

Solution:

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

$\approx Z$

Z is on integral domain but not field hence $I=\langle x\rangle$ is Prime ideal but not maximal ideal.

Q. $I=\langle x^2+1\rangle$ is Prime ideal but not maximal in $Z[x]$.

Solution:

$$\frac{Z[x]}{\langle x^2+1\rangle}=\{a_0+a_1x+\langle 1+x^2\rangle \mid a_i\in Z\}$$ ....(1)

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

$\Rightarrow 1+x^2=0$

$\Rightarrow x=\pm i$ ....(2)

$$\frac{Z[x]}{\langle x^2+1\rangle}=\{a_0+a_{1i}+\langle 1+x^2\rangle \mid a_i\in Z\}$$

$\approx Z[i]$

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

Q. Show that $I=\langle x\rangle$ is maximal ideal and prime ideal in $Q[x]$.

Solution:

$$\frac{Q[x]}{\langle x\rangle}=\{a_0+\langle x\rangle \mid a_0\in Q\}$$

$\approx Q$

Q is field then $I=\langle x\rangle$ is maximal and prime.

Q.(i) $I=\langle x^2-2\rangle$ is maximal ideal in $Q[x]$ but not $R[x]$.

Solution:

Mindset Makers

$I=\langle x^2-2\rangle$

$\frac{Q[x]}{\langle x^2-2\rangle}=\{a_0+a_1x+\langle x^2-2\rangle \mid a_i\in Q\}$

$f(x)=x^2-2$ is irreducible polynomial over Q then $\frac{Q[x]}{\langle x^2-2\rangle}$ is field

$\frac{Q[x]}{\langle x^2-2\rangle}=\{a_0+a_1\sqrt{2}+\langle x^2-2\rangle \mid a_i\in Q\}$

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

$Q[\sqrt{2}]$ is field then $I=\langle x^2-2\rangle$ is maximal in $Q[x]$.

(ii) $I=\langle x^2-2\rangle$ is not irreducible over $\mathbf{R}$.

Solution:

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

$I_1=(x-\sqrt{2})\in \mathbf{R}[x]$

$I_2=(x+\sqrt{2})\in \mathbf{R}[x]$

$I_1 I_2=x^2-2\in\langle x^2-2\rangle$

But neither I_1 is member of $\langle x^2-2\rangle$ nor I_2 is member of $\langle x^2-2\rangle$ then $\langle x^2-2\rangle$ nor I_2 is member of $\langle x^2-2\rangle$ then $\langle x^2-2\rangle$ is not prime ideal.

$\Rightarrow \frac{\mathbf{R}[x]}{\langle x^2-2\rangle}$ is not integral domain

$\Rightarrow \frac{\mathbf{R}[x]}{\langle x^2-2\rangle}$ is not field

$\Rightarrow I=\langle x^2-2\rangle$ is not maximal.

Q. $(G\mathbf{F}(2^3),+)\approx ?$, where $G\mathbf{F}(2^3)$ is Galois field of order 8.

(1) Z_8 ×

(2) $Z_4\times Z_2$ ×

(3) $Z_2\times Z_2\times Z_2$ √

(4) D_4 ×

(5) Q_4 ×

Solution:

$G\mathbf{F}(2^3)=\frac{Z_2[x]}{\langle f(x)\rangle}$, where $f(x)$ is irreducible polynomial over Z_2.

Here, no element has order greater than 2.

Mindset Makers

$\therefore \left(G\mathbf{F}\left(2^3\right),+\right) \approx Z_2 \times Z_2 \times Z_2$

Note: $\left(G\mathbf{F}\left(p^n\right),+\right) \approx Z_p \times Z_p \times Z_p ..... \times Z_p$

Note: $\mathbf{F} = G\mathbf{F}\left(p^n\right)$ then $\text{char}\left(\mathbf{F}\right) = P$

Q. Let $\mathbf{F}$ is field of order 27, then $\text{char}\left(\mathbf{F}\right)$?

Solution:

$$G\mathbf{F}\left(p^n\right) = \frac{Z_p[x]}{\langle f(x)\rangle} = \left\{a_0 + a_1 x + ... + a_{n-1}x^{n-1} + < f \mid a_i \in Z_p[x]\right\}$$

where $f(x)$ is irreducible polynomial of degree 'n' then $\forall\ a \in \frac{Z_p[x]}{\langle f(x)\rangle}$ such that $pa = 0$

then $\text{char}\left(\frac{Z_p[x]}{\langle f(x)\rangle}\right) = P$

$\Rightarrow \text{char}\left(G\mathbf{F}\left(p^n\right)\right) = P$

Note: If $\mathbf{F}$ is field of order p^n then $\mathbf{F} \approx G\mathbf{F}\left(p^n\right)$

Note: If $\mathbf{F}$ is field then char ($\mathbf{F}$) = 0, field is infinite
= p, finite field
i.e. char ($\mathbf{F}$) = 0 or p (For infinite and finite field respectively)

Q. $I = \langle x^2 + 1\rangle$ is prime / maximal in $\phi[x]$?

Solution:

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

$f(x) = x^2 + 1$ is not irreducible over ϕ because

$f(x) = (x - i)(x + i)$ ....(1)

$= g(x) \cdot h(x)$ where $g(x) = x - i \in \phi[x],\ h(x) = x + i \in \phi[x]$

but neither $g(x)$ nor $h(x)$ is unit in $\phi[x]$

$I_1(x) = (x - i) \in \phi[x]$

$I_2(x) = (x + i) \in \phi[x]$

$I_1(x) \cdot I_2(x) = (x - i)(x + i) = (x^2 + 1) \in I = \langle x^2 + 1\rangle$ but neither $(x - i) \notin I = \langle x^2 + 1\rangle$ nor $(x + i) \notin I = \langle x^2 + 1\rangle$ then $I = \langle x^2 + 1\rangle$ is not Prime ideal in $\phi[x]$.

Now, $\frac{\phi[x]}{\langle x^2 + 1\rangle}$ = not integral domain

$\Rightarrow \frac{\phi[x]}{\langle x^2 + 1\rangle}$ is not field

$\Rightarrow \frac{\phi[x]}{\langle x^2 + 1\rangle}$ is not field then $I = \langle x^2 + 1\rangle$ is not maximal.

Mindset Makers

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

Note: Let R be a commutative ring with unity and $I_1, I_2, I_3, ...I_r$ are ideals of R and $\gcd(I_i, I_j)=1, i\neq j$. Then, $\frac{R}{\langle I_1, I_2, ...I_x\rangle}\approx \frac{R}{\langle I_1\rangle}\times\frac{R}{\langle I_2\rangle}$

Q. Find number of ideals in $\frac{Q[x]}{\langle x^2-1\rangle}$

Solution:

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

$$\approx Q\times Q$$

$$\Rightarrow \frac{Q[x]}{\langle x^2-1\rangle}\approx Q\times Q$$

No. of ideals in $Q\times Q=4$

Then,

$\frac{Q[x]}{\langle x^2-1\rangle}$ has exactly 4 ideals.

Q. How many Prime ideal in $\frac{Q[x]}{\langle x^4-1\rangle}$?

Solution:

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

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

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

$$\approx Q\times Q\times Q[i]$$

Prime ideals is $Q\times Q\times Q[i]$ are:

$I_1=\{0\}\times Q\times Q[i]$, $I_2=Q\times\{0\}\times Q[i]$

$I_3=Q\times Q\times\{0\}$

then $\frac{Q[x]}{\langle x^4-1\rangle}$ has exactly 3 Prime ideals.

Q. How many Prime ideal in $\frac{Q[x]}{\langle x^5-1\rangle}$

Solution:

Mindset Makers

$$\frac{Q[x]}{\langle x^5-1\rangle}$$

$$\Rightarrow \frac{Q[x]}{\langle x^5-1\rangle}=\frac{Q[x]}{\langle (x-1)(x^4+x^3+x^2+x+1)\rangle}$$ By Eirentoin's Irreducibility Criteria

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

$\approx Q\times \mathbf{F}$, where $\mathbf{F}=\dfrac{Q[x]}{\langle x^4+x^3+x^2+x+1\rangle}$ is field.

$Q\times\mathbf{F}$ has exactly two prime ideals then $\dfrac{Q[x]}{\langle x^5-1\rangle}$ has exactly two prime ideals.

Q. $\dfrac{Z_5[x]}{\langle x\rangle}\approx ?$

Solution:

$$\frac{Z_5[x]}{\langle x\rangle}=\{a_0+\langle x\rangle \mid a_0\in Z_5\}$$

$$\approx Z_5$$

Q. Construct $Q\left[\sqrt{2},\sqrt{3}\right]$.

Solution:

$$\frac{Q[x]}{\langle x^2-2\rangle}\approx Q\left[\sqrt{2}\right]$$

Now,

$$\frac{Q\left[\sqrt{2}\right][x]}{\langle x^2-3\rangle}=\{a_0+a_1x+\langle x^2-3\rangle \mid a_i\in Q\left[\sqrt{2}\right]\} \quad \text{....(1)}$$

$$x^2-3=0$$

$$\Rightarrow x=\pm\sqrt{3} \quad \text{....(2)}$$

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

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

Q. Construct $Q\left[\sqrt{2},\sqrt{3},\sqrt{5}\right]$

Solution:

$$\frac{Q[x]}{\langle x^2-2\rangle}\approx Q\left[\sqrt{2}\right]$$

Mindset Makers

$$\frac{Q\left[\sqrt{2}\right][x]}{\left\langle x^2-3\right\rangle} \approx Q\left[\sqrt{2},\sqrt{3}\right]$$

$$\frac{Q\left[\sqrt{2},\sqrt{3}\right][x]}{\left\langle x^2-5\right\rangle} \approx \left[\sqrt{2},\sqrt{3},\sqrt{5}\right]$$

Note: $Q\left[\sqrt{2},\sqrt{3}\right]$ can also be written as $Q\left[\sqrt{2}+\sqrt{3}\right]$ or $Q\left[\sqrt{3}+\sqrt{2}\right]$.

$Q\left[\sqrt{2},\sqrt{3},\sqrt{5}\right]=Q\left[\sqrt{2}+\sqrt{3}+\sqrt{5}\right]$

$\because$ Dimension $\left[Q\sqrt{2}\sqrt{3}\sqrt{5}:Q\sqrt{2}\right]=4$

Dim $\left[Q\sqrt{2}:Q\sqrt{2}\right]=1$

Q. $Q\left[\sqrt{2},i\right]$, construct.

Solution: $\frac{Q[x]}{\left\langle x^2-2\right\rangle}=\left\{a_0+a_1x+\left\langle x^2-2\right\rangle \mid a_i \in Q\right\}$

$\approx Q\sqrt{2}$

$$\frac{Q\left[\sqrt{2}\right][x]}{\left\langle x^2+1\right\rangle}=\left\{a_0+a_1x+\left\langle x^2+1\right\rangle \mid a_i \in Q\sqrt{2}\right\}$$

$$=\left\{a_0+a_1i+\left\langle x^2+1\right\rangle \mid a_i \in Q\sqrt{2}\right\}$$

$$\frac{Q\left[\sqrt{2}\right][x]}{\left\langle x^2+1\right\rangle} \approx Q\left[\sqrt{2}\right][i]=Q\left[\sqrt{2},i\right]$$

Q. Which of the following polynomial is irreducible over $R=\frac{Q[x]}{\left\langle x^2+1\right\rangle}$.

(a) $1-y^2$

(b) $1+y^2$

(c) $1+y+y^2$

(d) y^3-y^2+y-1

Ans.(c)

Solution: $R=\frac{Q[x]}{\left\langle x^2+1\right\rangle}=Q[i]$

(a) If $f(y)=1-y^2=(1-y)(1+y)=g(y)\cdot h(y)$

$g(y)=(1-y)\in Q[i][y]$

$h(y)=(1+y)\in Q[i][y]$

but neither $g(y)$ nor $h(y)$ is unit in $Q[i][y]$ then $f(y)=1-y^2$ is reducible over $Q[i]$.

(b) $f(y)=1+y^2=(y+i)(y-i)=g(y)\cdot h(y)$

Mindset Makers

$g(y)=(y+i)\in Q[i][y]$

$h(y)=(y-i)\in Q[i][y]$

but neither $g(y)$ nor $h(y)$ is unit in $Q[i][y]$ $f(y)=1+y^2$ is reducible over $Q[i]$.

(c) $ax^2+bx+c=0$

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

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

$$y=\frac{-1\pm\sqrt{1^2-4\times1\times1}}{2\times1}$$

$$y=\frac{-1\pm\sqrt{3}i}{2}$$

$$1+y+y^2=\left(y-\left(\frac{-1+\sqrt{3}i}{2}\right)\left(y-\left(\frac{-1-\sqrt{3}i}{2}\right)\right)\right)$$

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

but $g(y)\notin Q[i][y]$ and $h(y)\notin Q[i][y]$ then $f(y)=1+y+y^2$ is irreducible over $Q[i]$.

(d) $f(y)=y^3-y^2+y-1=y^2(y-1)+1(y-1)$

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

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

$g(y)=(y^2+1)\in Q[i][y]$

$h(y)=(y-1)\in Q[i][y]$ but neither $g(y)$ nor $h(y)$ is unit in $Q[i][y]$ then

$f(y)=y^3-y^2+y-1$ is reducible over $Q[i]$.

Hence, $1+y+y^2$ is only irreducible polynomial. i.e. (c) is correct option.

Q. $\dfrac{Z[x]}{I=\langle 2,x\rangle}=\{a+\langle 2,x\rangle \mid a\in Z[x]\}$

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

$\approx Z_2$

$$\frac{Z[x]}{\langle 2,x\rangle}\approx\frac{Z}{\langle 2\rangle}\approx Z_2$$

$$\Rightarrow\frac{Z}{\langle 2,x\rangle}\approx Z_2$$

Note: $\dfrac{Z[x]}{\langle p,x\rangle}=\{a+\langle p,x\rangle \mid a\in Z[x]\}$

$\approx Z_p$

Q. Show that $I=\langle 3,x\rangle$ is maximal in $Z[x]$.

Mindset Makers

Solution:

$\frac{Z[x]}{\langle 3,x\rangle} \approx Z_3$

and Z_3 is field then $I=\langle 3,x\rangle$ is maximal ideal.

Q. $\frac{Z[x,y]}{\langle x,y\rangle} \approx \{a+\langle x,y\rangle \mid a \in Z[x,y]\}$

where $Z[x,y]=\{a_0+a_1x+a_2y+a_3xy+a_4x^2+....\mid a_i \in Z_j\}$

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

Q. Show that $I=\langle x,y\rangle$ is maximal and prime ideal in $Q[x,y]$.

Solution:

$\frac{Q[x,y]}{\langle x,y\rangle} = \{a+\langle x,y\rangle \mid a \in Q[x,y]\}$

$\approx Q$

$\frac{Q[x,y]}{\langle x,y\rangle} \approx Q$ and Q is field then $I=\langle x,y\rangle$ is maximal and prime ideal in $Q[x,y]$.

Q. Show that $I=\langle 2,x,y\rangle$ is maximal and prime ideal in $Z[x,y]$.

Solution:

$\frac{Z[x,y]}{\langle 2,x,y\rangle} = \{a+\langle 2x,y\rangle \mid a \in Z[x,y]\}$

$\approx Z_2$ is field then

$I=\langle 2,x,y\rangle$ is maximal and prime ideal in $Z[x,y]$.

Q. Show that $I=\langle x,y\rangle$ is Prime ideal but not maximal in $Z[x,y]$.

Q. $\frac{Z[x]}{\langle 2\rangle} = ?$

Solution: $\frac{Z[x]}{\langle 2\rangle} = \{a+\langle 2\rangle \mid a \in Z[x]\}$

Note: $\frac{Z[x]}{\langle m\rangle} = \{a+\langle m\rangle \mid a \in Z[x]\}$

* $Z_p[x]$ is infinite vector space over finite field.

$Z_p[x]=\{a_0+a_1x+a_2x^2+....\mid a_i \in Z_p\}$

Subfield: Let $(\mathbf{F},+,\cdot)$ is field are $\phi \neq S \subseteq \mathbf{F}$ $(S,+,\cdot)$ is called subfield of $(\mathbf{F},+,\cdot)$ if

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

(ii) $\forall a \in S,\ 0 \neq b \in S \Rightarrow ab^{-1} \in S$

Example: $(Q,+,\cdot)$ is subfield of $(\mathbf{R},+,\cdot)$

Mindset Makers

Solution: $\phi \neq Q \subseteq \mathbf{R}$ and $(Q,+,\cdot)$ is field then $(Q,+,\cdot)$ is subfield of $(\mathbf{R},+,\cdot)$

Similarly,(i) $(\mathbf{R},+,\square)$ is subfield of $(\mathbf{D},+,\square)$, (ii) $(\mathrm{Q},+,\square)$ is subfield of $\left(Q\sqrt{2},+,\square\right)$

Q. Let $\mathbf{F}$ be a finite field of p^n then no. of subfield of $\mathbf{F} = \tau(n)$, no. of positive divisor of *n*.

Suppose $K_1, K_2, ...K_r$ positive factor of *n* then subfield of $\mathbf{F}$ of order

(i) $O(\mathbf{F}_1) = p^{k_1}$ (ii) $O(\mathbf{F}_2) = p^{k_2}$ (iii) $O(\mathbf{F}_r) = p^{kr}$

Q. Let $\mathbf{F}$ be field of order 2^4, find # of subfield in $\mathbf{F}$.

Solution: $\mathbf{F} = G\mathbf{F}(2^4) = \dfrac{Z_2[x]}{\langle f(x)\rangle}$, where $f(x)$ is irreducible polymeric over Z_2 of degree 4.

$\dim\left(G\mathbf{F}(2^4) : Z_2\right) = 4$ i.e. $\dim\left(G\mathbf{F}(2^4) : G\mathbf{F}(p')\right) = 4$

Subfield of $G\mathbf{F}(2^4)$ are : $G\mathbf{F}(p^1) = G\mathbf{F}(2^1), G\mathbf{F}(p^2) = G\mathbf{F}(2^2), G\mathbf{F}(p^4) = G\mathbf{F}(2^4)$

then $\mathbf{F}$ has exactly 3 subfields.

Q. How many subfields in $\mathbf{F}$ where $O(\mathbf{F}) = 3^{100}$?

Solution: number of subfield in $\mathbf{F} = \tau(100) = 2^2 \times 5^2 = (2+1)(2+1) = 3\times 3 = 9$

Theorem:

(i) If $\mathbf{F}$ is field then $(\mathbf{F}^*,\square)$ is abelian group of order $O(\mathbf{F})-1$.

(ii) If $\mathbf{F}$ is finite field then $(\mathbf{F}^*,\square)$ is cyclic of order $O(\mathbf{F})-1$

i.e. $F^* \approx Z_{0(\mathbf{F})-1}$

Now, automorphism,

$f : (\mathbf{F},*,\square) \to (\mathbf{F}^*,\cdot) \approx f : Z_{26} \to Z_{26}$

Aut $(\mathbf{F}^*)$ = Aut $(Z_{26}) \approx U(26) \approx Z_{12}$. So Aut $(\mathbf{F}^*) \approx Z_{12}$

Since Z_{12} is cyclic then Aut $(\mathbf{F}^*)$ is cyclic group of order 12.

Q. Let $\mathbf{F}$ be finite field of order 9, how many elements in $\mathbf{F}$ such that $x^4 = 1, x \in \mathbf{F}$

Solution: $O(\mathbf{F}) = 9 = 3^2$. $(\mathbf{F},*,\square) \approx Z_8$

number of elements of order 1 in $Z_8 = 1$

number of elements of order 2 in $Z_8 = \phi(2) = 1$

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

Total number of elements = 1+1+2 = 4. then $\mathbf{F}$ has exactly 4 elements satisfied x^4 -1

Mindset Makers

CHAPTER-5

Principal Ideal Domain: An integral domain $(R,+,\square)$ is said to be Principal Ideal domain if every ideal of R is Principal ideal.

Q. $R=Z$ is Principal Ideal Domain?

Solution: Every ideal of Z is Principal ideal $(\langle m\rangle)$ then Z is Principal ideal domain.

Q. $R=Q$ is Principal ideal domain?

Solution: Q is field then Q has exactly two ideal

say, $I_1=\{0\}=\langle 0\rangle, I_2=Q=\langle 1\rangle$ Principal Ideal then Q is P.I.D.

Note: If $\mathbf{F}$ is field then $\mathbf{F}$ is P.I.D.

Q. $R=Z\times Q$ is P.I.D.

Solution: $Z\times Q$ is not integral domain then it is not P.I.D.

Q. $M_2(\mathbf{R})=\left\{\begin{bmatrix} a & b \\ c & d\end{bmatrix}\middle| a,b,c,d\in\mathbf{R}\right\}$ is P.I.D.?

Solution: $M_2(\mathbf{R})$ is not integral domain hence it is not P.I.D.

Q. $R=G\mathbf{F}\left(3^{100}\right)$ is P.I.D.?

Solution: $R=G\mathbf{F}\left(3^{100}\right)$ is field it is PID

Q. $R=Z[x]$ is P.I.D.?

Solution: $I=\langle 2,x\rangle$ is not Principal ideal in $Z[x]$ then $Z[x]$ is not P.I.D.

Q. Which of the following is/are true.

(1) $R=\dfrac{Q[x]}{\langle x\rangle}$ is P.I.D? (2) $R=\dfrac{[x,y]}{\langle 2\rangle\langle y\rangle}$ is P.I.D.? (3) $R=\dfrac{Z[x]}{\langle 4,x\rangle}$ is P.I.D.?

(4) $R=\dfrac{Q\times\mathbf{R}}{\mathrm{Q}\times\{0\}}$ is P.I.D.

Mindset Makers

Solution:(1) $\frac{Q[x]}{\langle x\rangle}\approx Q$ is field then $\frac{Q[x]}{\langle x\rangle}$ is field then $\frac{Q[x]}{\langle x\rangle}$ is P.I.D.

(2) $\frac{Z_2[x,y]}{\langle 2,x,y\rangle}\approx Z_2$ then $\frac{Z_2[x,y]}{\langle 2,x,y\rangle}$ is P.I.D.

(3) $\frac{Z[x]}{\langle 4,x\rangle}\approx Z_4$, Z_4 is not integral domain then $\frac{Z[x]}{\langle 4,x\rangle}$ is not integral then $\frac{Z[x]}{\langle 4,x\rangle}$ is not P.I.D.

(4) $\frac{Q\times\mathbf{R}}{\mathrm{Q}\times\{0\}}\approx\mathbf{R}$, then $\frac{Q\times\mathbf{R}}{\mathrm{Q}\times\{0\}}$ is field then $\frac{Q\times\mathbf{R}}{\mathrm{Q}\times\{0\}}$ is P.I.D.

Q. Which of the following is not order or P.I.D.?
(1) 25 (2) 35 (3) 49 (4) 11

Solution: We know that if $\mathbf{F}$ is finite field then $O(\mathbf{F})=p^n=G\mathbf{F}(p^n)$

Since, every field is on integral domain then order of finite integral domain is also p^n.

(1) $25=5^2=p^n$, then it is possible for order or P.I.D.

(2) $35=5\times7\neq p^n$, then it is not possible for order of finite integral domain then it is not possible order of P.I.D.

(3) $49=7^2=p^n$, then it is possible order of P.I.D.

(4) $11=11^1=p^n$, then it is possible order of P.I.D.

Euclidean Domain

Definition: An integral domain $(D,+,\bullet)$ is said to be Euclidean Domain if $\exists$ a function d from non-zero elements of D to non-negative integer such that

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

(2) If $a\in D,0\neq b\in D$ then $\exists$ q order in D s.t. (q is not necessarily prime)

$a=bq+r$ where $r=0$ or $d(r)<d(b)$.

Q. Show that $(Z,+,\square)$ is Euclidean domain

Solution: $D=(Z,+,\square)$ is an integral domain

Let $d(a)=|a|,\ \forall 0\neq a\in Z$

(1) Let $0\neq a\in D,\ 0\neq b\in D;\ d(a)=|a|\le|ab|=d(a,b)\Rightarrow d(a)\le d(a,b)$

(2) If $a\in Z,\ 0\neq b\in Z$ then $\exists$ Unique q and r such that

$a=bq+r$, where $r=0$ or $r<b\Rightarrow r=0,\ r=|r|<|b|\Rightarrow d(r)<d(b)\Rightarrow r=0$ or $d(r)<d(b)$

then $(Z,+,\cdot)$ is E.D.

Q. If $\mathbf{F}$ is field then $\mathbf{F}$ is Euclidean Domain

Solution: Let $(\mathbf{F},+,\cdot)$ is field and let

$d(a)=1,\ \forall 0\neq a\in\mathbf{F}$ (1) $0\neq a\in\mathbf{F},\ 0\neq b\in\mathbf{F};\ d(a)=1=d(a,b)$

$[\,0\neq a\in\mathbf{F},0\neq b\in\mathbf{F}\Rightarrow 0\neq a\cdot b\in\mathbf{F}$ then $d(a,b)=0\,]$

(2) If $a\in\mathbf{F},\ 0\neq b\in\mathbf{F}$ s.t $a=a\cdot1+0=ab^{-1}b+0=(ab^{-1})b+0$

$a=(ab^{-1})b+0=q\cdot b+r$, where $q=ab^{-1}$ and $r=0$; $a=bq+r$, where $r=0$

Mindset Makers

then if $\mathbf{F}$ is field then it is Euclidean Domain.

Q. If $\mathbf{F}$ is field then $\mathbf{F}[x]$ is Euclidean Domain.

Solution: Let $\mathbf{F}$ is field then $\mathbf{F}[x]$ is an integral domain.

Suppose, $d(f(x))$ = degree $(f(x))$, $\forall 0 \neq f(x) \in \mathbf{F}[x]$

(1) Let $0 \neq f(x) \in \mathbf{F}[x]$, $0 \neq g(x) \in \mathbf{F}[x]$

$d(f(x))$ = degree $(f(x)) \leq$ degree $(f(x))$ + degree $(g(x))$

= degree $(f(x)\square g(x)) = d(f(x)\square g(x)) \Rightarrow d(f(x)) \leq d(f(x)\cdot g(x))$

(2) If $f(x) \in \mathbf{F}[x]$, $0 \neq g(x) \in \mathbf{F}[x]$ then $\exists\, q(x)$ and $r(x) \in \mathbf{F}[x]$ such that

$f(x) = g(x)\square q(x) + r(x)$ where $r(x) = 0$ or

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

then $\mathbf{F}[x]$ is Euclidean Domain.

Q. Show that $Z[i] = \{a + ib \mid a, b \in Z\}$ is Euclidean Domain.

Solution: $0 \neq x = a + ib \in Z[i]$ such that

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

(1) Let $0 \neq x = a_1 + ib_1 \in Z[i]$

$0 \neq y = a_2 + ib_1 \in Z[i]$ such that $d(x) = a_1^2 + b_1^2$ ....(1)

Now, $d(x, y) = d(a_1 + ib_1)(a_2 + ib_2) = d((a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2))$

$= (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2 = a_1^2a_2^2 + b_1^2b_2^2 - 2a_1a_2 \cancel{b_1}\cancel{b_2} + a_1^2b_2^2 + b_1^2a_2^2 + 2a_1b_2 \cancel{b_1}\cancel{a_2}$

$= a_1^2(a_2^2 + b_2^2) + b_1^2(a_2^2 + b_2^2) \Rightarrow d(x, y) = (a_1^2 + b_1^2)(a_2^2 + b_2^2)$ ....(2)

$d(x) = (a_1^2 + b_1^2) \leq (a_1^2 + b_1^2)(a_2^2 + b_2^2) = d(xy)$ then $d(x) \leq d(x, y)$

(2) If $x = a_1 + ib_1 \in Z[i]$, $0 \neq y = a_2 + ib_2 \in Z[i]$

$\frac{x}{y} = \frac{a_1 + ib_1}{a_2 + ib_2} = \frac{(a_1 + ib_1)}{(a_2 + ib_2)} = \frac{(a_1 - ib_1)}{(a_2 - ib_2)} = \frac{a_1^2}{a_2^2 + 1} \Rightarrow x = yq + r,\ r = 0$ or $d(r) < d(y)$

Hence, $Z[i]$ is P.I.D.

Q. $Q[x]$ is Euclidean Domain?

Solution: Since Q is field then $Q[x]$ is Euclidean Domain.

Q. $Z_{11}[x]$ is Euclidean Domain?

Solution: Z_{11} is field then $Z_{11}[x]$ is Euclidean Domain.

Q. $Z_5[i][x]$ is E.D.?

Solution: $Z_5[i]$ is not an integral domain then $Z_5[i][x]$ is not Euclidean Domain.

Q. $G\mathbf{F}(3^5)$ is E.D.?

Solution: Yes, $G\mathbf{F}(3^5)$ is field and we know that every field is E.D. then $G\mathbf{F}(3^5)$ is E.D.

Mindset Makers

Unique Factorization Domain

Definition: An integral domain $(D,+,\cdot)$ is said to be Unique Factorization Domain if

(i) Every non-zero, non-unit element of D can be written as product of Irreducible element of D and

(ii) The factorization is Unique upto associate.

i.e. Let a is non-zero, non-unit element of D and $a = a_1 a_2 ....a_r$ where $a_1 a_2 ....a_r$ are irreducible element of D.

If $a = b_1 b_2 ....b_3$, where $b_1 b_2 ...b_s$

$a_1 a_2 ....a_r = b_1 b_2 ...b_3$ then $r = S$ and a_i is associate to b_j (only one b_j)

Example: $(Z,+,\bullet)$ is U.F.D.

Solution: $a = 10 \in Z$; $-2 \times -5 = 10 = 2 \times 5$; -2 is associate to 2 and -5 is associate to 5. Then, the factor of 10 is Unique upto associate. $\forall a \in Z$, s.t. factorization 'a' is unique upto associate then Z is Unique Factorization Domain.

Q. $Z\left[\sqrt{-5}\right]$ is U.F.D.?

Solution: $Z\left[\sqrt{-5}\right] = \left\{a + ib \mid a,b \in Z\right\} \Rightarrow Z\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a,b \in Z\right\}$

$\Rightarrow Z\left[\sqrt{-5}\right] = \left\{a + i\sqrt{5} \mid a,b \in Z\right\}$ ....(1)

$14 \in Z\left[\sqrt{-5}\right]$; $\left(3 + i\sqrt{5}\right)\left(3 - i\sqrt{5}\right) = 14 = 7 \times 2$

But $\left(3 + i\sqrt{5}\right)$ is not associate to 7 or 2. and $\left(3 - i\sqrt{5}\right)$ is not associate to 7 or 2.

then factorization of 14 is not Unique upto associate.. Then, $Z\left[\sqrt{-5}\right]$ is not Unique Factorization Domain.

Q. $Z\left[\sqrt{-3}\right]$ is U.F.D?

Solution: $Z\left[\sqrt{-3}\right] = \left\{a + ib\sqrt{3} \mid a,b \in Z\right\}$; $\left(1 + \sqrt{3}i\right)\left(1 - \sqrt{3}i\right) = 4 = 2 \times 2$

here, $\left(1 + \sqrt{3}i\right)$ is not associate to 2 and $\left(1 - \sqrt{3}i\right)$ is not associate to 2

then factorization of 4 is not Unique upto associate then $Z\left[\sqrt{-3}\right]$ is not U.F.D.

Note: (1) $Z\left[\sqrt{-d}\right] = \left\{a + ib\sqrt{d} \mid a,b \in Z\right\}$ is not Unique Factorization Domain if $d > 2$

Note: $Z\left[\sqrt{-d}\right], d = 1,2$ is Euclidean Domain

Note: Relation Field $\Rightarrow$E.D. $\Rightarrow$ PID $\Rightarrow$ U.F.D $\Rightarrow$Integral Domain

Q. Which of the following is true

(1) $U.F.D \subseteq PID \subseteq E.D.$,(2) $E.D \subseteq PID \subseteq U.F.D$

(3) $PID \subseteq E.D \subseteq U.F.D$,(4) $E.D \subseteq U.F.D \subseteq P.I.D$

Q. $Q\sqrt{2}$ is U.F.D., PID?

Solution: $Q\left[\sqrt{2}\right]$ is field then $Q\sqrt{2}$ is E.D. $\Rightarrow Q\left[\sqrt{2}\right]$ is P.I.D. $\Rightarrow Q\left[\sqrt{2}\right]$ is U.F.D.

Q. $Z[x]$ is E.D?

Solution: $Z[x]$ is not P.I.D. then $Z[x]$ is not E.D.

Mindset Makers

Q. $\frac{Q[x,y]}{\langle x\rangle}$ is PID, UFD?

Solution: $\frac{Q[x,y]}{\langle x\rangle}\approx Q[y]$, since Q is field then $Q[y]$ is E.D. $\Rightarrow Q[y]$ is P.I.D. $\Rightarrow Q[y]$ is U.F.D.

Q. $Q[x,y]$ is Euclidean Domain?

Solution: $I=\langle x,y\rangle$ is an ideal of $Q[x,y]$ and I is not Principal Ideal then $Q[x,y]$ is not P.I.D.

$\Rightarrow Q[x,y]$ is not E.D.

Q. $\frac{Z[x,y]}{\langle 2,x,y\rangle}$ is E.D., PID, UFD?

Solution: $\frac{Z[x,y]}{\langle 2,x,y\rangle}\approx Z_2$

since Z_2 is field then $\frac{Z[x,y]}{\langle 2,x,y\rangle}$ is field then $\frac{Z[x,y]}{\langle 2,x,y\rangle}$ is E.D. , PID and UFD.

Q. $Z\left[\sqrt{-3}\right]=\left\{a+b\sqrt{-3}\mid a,b\in Z\right\}$ is E.D., PID and UFD?

Solution: $Z\left[\sqrt{-3}\right]$ is not U.F.D. $\Rightarrow Z\left[\sqrt{-3}\right]$ is not P.I.D. $\Rightarrow Z\left[\sqrt{-3}\right]$ is not E.D.

Q. $Z\left[\sqrt{-1}\right]$ is U.F.D, PID and E.D.?

Solution: $Z\left[\sqrt{-1}\right]=Z[i]$ is E.d. $\Rightarrow Z[i]$ is P.I.D. $\Rightarrow Z[i]$ is U.F.D.

Q. $Z\left[\sqrt{-6}\right]=\left\{a+i\sqrt{6}b\mid a,b\in Z\right\}$ is E.D.?

Solution: $\left(3+i\sqrt{6}\right)\left(3-i\sqrt{6}\right)=15=5\times 3$ and $15\in Z\left[\sqrt{-6}\right]$

but $\left(3+i\sqrt{6}\right)$ is not associate to 5 or 3 and $\left(3-i\sqrt{6}\right)$ is not associate to 5 or 3

then $Z\left[\sqrt{-6}\right]$ is not E.D. $\Rightarrow Z\left[\sqrt{-6}\right]$ is not PID $\Rightarrow Z\left[\sqrt{-6}\right]$ is not U.F.D.

Q. $f(x)=x^4+3x^3-9x^2+7x+27$ then

(a) $f(x)$ is irreducible over Z_2 (b) $f(x)$ is irreducible over Q

(c) $f(x)$ is irreducible over Z_3 (d) $f(x)$ is irreducible over Z.

Solution: If any polynomial $f(x)$ is irreducible in Z_p then it is always irreducible over Q but it should not be so for n $a\cdot f(x)$ i.e. we will check the irreducibility over Z_p first if $f(p)\neq 1$ then it is not reducible i.e. irreducible over Z_p.

Condition:

Note: (i) If degree of $f(x)$ over Q and degree of $f(x)$ over Z_p are same and $f(x)$ is irreducible over Z_p (for some *p*) then $f(x)$ is irreducible over Q.

Note: (i) If $f(x) \neq a \cdot g(x)$, $a \neq 1$ or -1 (a is not unit) and $f(x)$ is irreducible over Q then $f(x)$ is irreducible over Z.

Example: $f(x) = 2x^2 + 2$ is irreducible over Q but not irreducible over Z because $f(x) = a \cdot g(x) = 2(x^2 + 1)$

Q. $f(x) = x^3 + 2x^2 + x - 1$, $f(x)$ is irreducible over field K.

(a) $f(x)$ is irreducible over $K = Q$ √ (b) $f(x)$ is irreducible over $K = \mathbf{R}$ ×

(c) $f(x)$ is irreducible over $K = Z_2$ √ (d) $f(x)$ is irreducible over $K = Z_3$ ×

Solution: (b) $f(x)$ is reducible over $\mathbf{R}$ since the degree of polynomial is 3.

$f(x)$ is irreducible over Z_2 because $f(x) \neq 0 \ \forall x \in Z_2$ and degree of $f(x)$ over Z_2 and degree of $f(x)$ over Q both are same then $f(x)$ is irreducible over Q.

CHAPTER-6

Extension Field

Let H is subfield of K. The field is called extension field of $\mathbf{F}$.

Q. Q is subfield of $Q[\sqrt{2}]$ then $Q\sqrt{2}$ is called extension field of Q.

Ans. It has 2 extensions since $Q \subseteq Q[\sqrt{2}]$ and $Q[\sqrt{2}] \subseteq Q[\sqrt{2}]$

Q. How many subfields of $Q[\sqrt{2}]$

Solution:

Q and $Q[\sqrt{2}]$ are two subfields of $Q[\sqrt{2}]$ then exactly two subfields.

Similarly, $Q[\sqrt{3}]$ has two subfields Q and $Q[\sqrt{3}]$.

Q. How many subfields in $Q(\sqrt{2}, \sqrt{3})$?

Solution:

$Q, Q(\sqrt{2}), Q(\sqrt{3})$ and $Q(\sqrt{2}, \sqrt{3})$ exactly 4 subfields.

Note: If L is extension field of K and K is extension field of $\mathbf{F}$ then L is extension field of $\mathbf{F}$ i.e. $[L:K][K:\mathbf{F}] = [L:\mathbf{F}]$

Imp: Extension of field is not symmetric hence it is not an equivalence relation. Then $\dim[L:\mathbf{F}] = \dim[L:K] \times \dim[K:\mathbf{F}]$

Q. Find dimension of $Q[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ over Q.

Solution:

$\dim[Q[\sqrt{2}, \sqrt{3}, \sqrt{5}] : Q]$

$[Q\sqrt{2}, \sqrt{3}, \sqrt{5} : Q] = [Q\sqrt{2}, \sqrt{3}, \sqrt{5} : Q\sqrt{2}, \sqrt{3}][Q\sqrt{2}, \sqrt{3} : Q\sqrt{2}][Q\sqrt{2} : Q]$

Mindset Makers

$\dim\left[Q\sqrt{2},\sqrt{3},\sqrt{5}:Q\right]=\dim\left[Q\sqrt{2},\sqrt{3},\sqrt{5}:Q\sqrt{2},\sqrt{3}\right]\left[Q\sqrt{2},\sqrt{3}:Q\sqrt{2}\right]\dim\left[Q\sqrt{2}:Q\right]$

$=2\times2\times2=8$

Q. Find $\dim\left[Q\sqrt{2}+\sqrt[3]{2}\right]$

Solution:

$\left[Q\sqrt{2}+\sqrt[3]{5}:Q\sqrt{2}\right]=\left[Q\sqrt{2},(5)^{1/3}:Q\sqrt{2}\right]$

then $\dim Q\left[\sqrt{2}+\sqrt[3]{5}:Q\sqrt{2}\right]=3$

Q. $\dim\left[Q(2)^{1/4},(3)^{1/3},(5)^{1/7}:Q(3)^{1/3}\right]=?$

Solution:

$\dim\left[Q(2)^{1/4},(3)^{1/3},(5)^{1/7}:Q(3)^{1/3}\right]=4\times7=28$

Note: $\dfrac{Z[x]}{\langle m\rangle}=\dfrac{Z[x]}{mZ[x]}=\left[\dfrac{Z}{mZ}\right][x]=Zm[x]$

$\left(\dfrac{R[x]}{I[x]}\approx\left[\dfrac{R}{I}\right][x]\right)$

Q. $\dfrac{Z[x]}{\langle 2\rangle}=\dfrac{Z[x]}{2Z[x]}=\left[\dfrac{Z}{2Z}\right][x]$

$\approx Z_2[x]$

Note: Aut $(K\,|\,\mathbf{F})\approx Z_m$, where K is extension field of $\mathbf{F}$ with dimension m and $\mathbf{F}$ is finite field.

Example: K is field of order 3^{100}

Aut $(\mathrm{K}|\mathbf{F})\approx Z_{100}$ = Galon Group

Aut $\left(G\mathbf{F}\left(3^{100}\right)|G\mathbf{F}(3')\right)\approx Z_{100}$

Aut $\left(G\mathbf{F}\left(3^{100}\right)|G\mathbf{F}(3')\right)\approx Z_{100}$

$G\mathbf{F}\left(3^{100}\right)=\dfrac{Z_3[x]}{\langle f(x)\rangle}$

$\dim\left[G\mathbf{F}\left(3^{100}\right):G\mathbf{F}(3')\right]=100$

then Aut $\left(G\mathbf{F}\left(3^{100}\right)|G\mathbf{F}(3')\right)\approx Z_{100}$

Q. How many subgroups in Aut $(\mathbf{F})$ where $\mathrm{O}(\mathbf{F})=2^8$

Solution:

$O(\mathbf{F})=2^8=G\mathbf{F}\left(2^8\right)$

Aut $\left(G\mathbf{F}\left(2^8\right)|G\mathbf{F}\left(2^1\right)\right)$=?

$\dim\left[G\mathbf{F}\left(2^8\right):G\mathbf{F}\left(2^1\right)\right]=8$ then

Aut $\left(G\mathbf{F}\left(2^8\right)|G\mathbf{F}\left(2^1\right)\right)=Z_8$

Mindset Makers

# of subgroups in $Z_8 = T(8) = 2^3 = (3+1) = 4$

Q. Let G be a Galois group of the splitting field of $x^5 - 2$ over Q.

Splitting Field: Let K is an extension field of **F** and $f(x) \in \mathbf{F}[x]$ A field K of **F** is called splitting field over $f(x)$ is

(i) $f(x)$ can be written as product of linear factors over K.

For example:

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

$Q[i]$ is splitting field of Q over $f(x) = x^2 + 1$

(ii) $f(x) = x^2 - 3 \in Q[x]$

$Q[\sqrt{3}]$ is splitting field of Q over $f(x) = x^2 - 3$

$\left(\frac{Q[x]}{\langle x^2 - 3 \rangle} \approx Q[\sqrt{3}] \right)$

Q. $Q(\sqrt{2}, i)$ is splitting field of Q over $x^2 + 2$

Solution:

$\frac{Q[x]}{\langle x^2 + 2 \rangle} \approx Q[\sqrt{2}, i]$

Q. Let G be a Galois group of the splitting field of $x^5 - 1$ over Q.

Solution:

$f(x) = x^5 - 1 \in Q[x]$ but $f(x)$ is not irreducible

$f(x) = x^5 - 1 = 0$

$\Rightarrow x^5 = 1$

$\Rightarrow x = (1)^{1/5}$, let $(1)^{1/5} = \omega$

$f(\omega) = 1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$

$f(\omega) = 1 + \omega + \omega^2 + \omega^3 + \omega^4$

$f(\omega) = 1 + \omega + \omega^2 + \omega^3 + \omega^4$ is irreducible polynomial over Q of degree 4 then order of Galois Group = 4, because degree of extension is 4.

Then, Galois Group = Aut $(K \mid Q) = \{A^i \mid A^4 = e\}$

$\approx Z_4$

Note: $f(x) - x^n - 1$ over Q then Aut$(K \mid Q)$ = Galois Group $\approx U(n)$.

Q. $f(x) = x^7 - 1$ over Q then Galois group is isomorphic to?

Solution:

Aut$(K \mid Q)$ = Galois group $\approx U(7) \approx Z_6$

Q. Let G be a Galois Group over

$f(x) = x^5 - 2$ over Q. Find $O(G)$?

Solution:

Mindset Makers

$f(x)=x^5-2$ over Q

$f(x)=x^5-2=0$

$\Rightarrow x^5-2=0$

$\Rightarrow x^5=2\cdot 1$

$\Rightarrow x=(2)^{1/5}(1)^{1/5}$ ....(1)

$1,\omega,\omega^2,\omega^3,\omega^4$

degree of $\left[Q(\omega):Q\right]=4$ ....(2)

degree of $\left[Q\left(2^{1/5}\right):Q\right]=5$ ....(3)

degree $\left(Q(2)^{1/5}\omega:Q\right)=5\times 4=2Q$

Aut$\left(Q(2)^{1/5}(\omega):Q\right)$=Galois Group of order 20

$$=\left\{\begin{matrix}A^iB^i \mid A^4=e,B^4=e,\ AB\neq BA,i=0,1,2,3\\ j=0,1,2,3,4\end{matrix}\right\}$$

$$\begin{pmatrix}A\to\omega\\ B\to r\end{pmatrix}$$

$O\left(Aut\left(Q(2)^{1/5}(\omega):Q\right)\right)=2O$

Q. Let G be the Galois group of the splitting field x^5-2 over Q then which of the following statement are true?

(a) G is cyclic

(b) G is Non-Abelian

(c) $O(G)=20$

(d) G has elements of order 4

Q. Let $\mathbf{F}\subseteq C$ be the splitting field x^7-2 over Q and $Z=\omega=e^{\frac{2\pi i}{7}}$. Let $\left[F:Q(\omega)\right]=0$ and $\left[F:Q(2)^{1/7}\right]=b$. Then

(a) $a=b=7$

(b) $a=b=6$

(c) $a>b$

(d) $a<b$

Solution:

$\mathbf{F}$ is splitting field over x^7-2

dim$[\mathbf{F}:Q]$=?

$f(x)=x^7-2$

$\Rightarrow x^7-2=0$

$\Rightarrow x^7=2\cdot 1$

$\Rightarrow x=(2)^{1/7}\cdot(1)^{1/7}$

$\Rightarrow x=(2)^{1/7}\cdot\omega,\ \omega=(1)^{1/7}$

Mindset Makers

$1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega$

$\left[F = Q(2)^{1/7} : Q\right] = 7 \times 6 = 42$ ....(1)

$\left[F = Q(2)^{1/7}\,\omega : Q\right] = \left[Q(2)^{1/7}\,\omega : Q(\omega)\right]\left[Q(\omega) : Q\right]$

$42 = a \times 6$

$\Rightarrow a = \frac{47}{6} = 7$

$\left[F = Q(2)^{1/7}\,\omega : Q\right] = \left[F = Q(2)^{1/7}\,\omega : Q(2)^{1/7}\right]\left[Q(2)^{1/7} : Q\right]$

$42 = b \times 7$

$\Rightarrow b = \frac{42}{7} = 6$

Q. Let G be a Galois group of splitting field $x^3 - 2$ over Q. Find subgroup in G?

Q. Let ω be a Complex number such that $\omega^3 = 1$ but $\omega \neq 1$. Suppose L is field $Q\left((2)^{1/3}, \omega\right)$ generated by $(2)^{1/3}$ and ω over Q field then number of subfields K such that $Q \subseteq K \subseteq L$ is

(1) 2
(2) 3
(3) 4
(4) 5

Solution:

$f(x) = x^3 - 2 = 0$

$\Rightarrow x^3 - 2 = 0$

$\Rightarrow x^3 = 2 \cdot 1$

$\Rightarrow x = (2)^{1/3}(1)^{1/3}$

$\Rightarrow x = (2)^{1/3}\,\omega$, where $\omega = (1)^{1/3}$

degree $\left[Q(2)^{1/3}\,\omega : Q\right] = 6$

Then,

Aut$\left[Q(2)^{1/3}\,\omega : Q\right]$ = Galois Group

$= \left\{A^i B^i \mid A^2 = e, B^3 = e, AB \neq BA \; i = 0,1, \; j = 0,1,2\right\}$

$A \Rightarrow \omega$

$B \Rightarrow x$

then Galois Group $\approx S_3$.

No. of subgroups in $S_3 = 6$ says,

$H_1 = \{I\}, H_2 = \{I(1,2)\}, H_3 = \{I, (13)\}$

$H_4 = \{I(23)\}, H_5 = \{I, (123)(132)\}$

$H_6 = S_3$

The subgroup H of S_3 such that $\{e\} \subseteq H \subseteq S_3$ are H_2, H_3, H_4 and H_5.

Mindset Makers

Then, S_3 has 4 subgroup s.t. $\{e\} \subseteq H \subseteq S_3$
then
$L = \left[Q(2)^{1/3} \omega : Q \right]$ has 4 subfields s.t. $Q \subseteq K \subseteq L$.

Theoretical Chapter

Theorem 1. The characteristic of a ring with unity is 0 or n > 0 according as the unity element 1 regarded as a member of the additive group of the ring has the order zero or n.

Proof. Let R be a ring with unity element 1. If 1 has order zero, then the characteristic of the ring is zero.

Suppose 1 is of finite order n so that 1 + 1 + 1 + … upto n terms = 0 i.e., n1 = 0.

Let a be any element of R. Then, we have; $na = a + a + a + \ldots$ upto n terms

$= 1a + 1a + 1a + \ldots$ upto n terms $= (1+1+1+\ldots$ upto n terms$)a$ [by dist. law]

$= (n1)a = 0a = 0$. $\therefore$ order of a is „ n.

Hence the characteristic of the ring is n.

Theorem 2. The characteristic of an integral domain is 0 or n according as the order of any non-zero element regarded as a member of the additive group of the integral domain is either 0 or n.

Proof. Let D be an integral domain. If a non-zero element of D is of order zero, then the characteristic of D is zero.

Let the order of the non-zero element a be finite and equal to n. Then na = 0.

Suppose b is any other non-zero element of D.

We have $na = 0 \Rightarrow (na)b = 0$

$\Rightarrow (a + a + a + \ldots \text{ upto } n \text{ terms})b = 0 \Rightarrow (ab + ab + ab + \ldots \text{ upto } n \text{ terms}) = 0$

$\Rightarrow a(b + b + b + \ldots \text{ upto } n \text{ terms}) = 0 \Rightarrow a(nb) = 0.$

But D is without zero divisors. Therefore $a \neq 0$ and $a(nb) = 0 \Leftrightarrow nb = 0.$

But the order of a is $n \Rightarrow n$ is the least positive integer such that na = 0. Also we have n0 =0.

Thus n is the least positive integer such that $nx = 0 \ \forall \ x \in D.$ Hence D is of characteristic n.

Theorem 3. Each non-zero element of an integral domain D, regarded as a member of the additive group of D, is of the same order

Proof. Let D be an integral domain. Suppose a is a nonzero element of D and o(a) is finite and say, equal to n. Suppose b is any other non-zero element of D and o(b) = m.

We have $o(a) = n \Rightarrow na = 0 \Rightarrow nb = 0$ [see theorem 2] $\Rightarrow o(b) \,,, n \Rightarrow m \,,, n.$

Similarly $o(b) = m \Rightarrow mb = 0 \Rightarrow a(mb) = 0 \Rightarrow a(b + b + \ldots \text{ upto } m \text{ times}) = 0$

$\Rightarrow (ab + ab + ab + \ldots \text{ upto } m \text{ times}) = 0 \Rightarrow (a + a + a \ldots \text{ upto } m \text{ times})b = 0 \Rightarrow (ma)b = 0$

$\Rightarrow ma = 0$ [$\because \ b \neq 0$ and D is without zero divisors]

$\Rightarrow o(a) ,, m \Rightarrow n ,, m$

Now $m ,, n , n ,, m \Rightarrow m = n.$ Hence $o(a) = o(b)$.

Also if o(a) is zero, then o(b) cannot be finite. Because $o(b) = m \Rightarrow ma = 0$ i.e., the order cannot be finite. Hence o(b) must also be zero. Hence the theorem.

Theorem 4. The characteristic of an integral domain is either 0 or a prime number.

Proof. Suppose D is an integral domain. Let $0 \neq a \in D.$ If o(a) is zero, then the characteristic of D is 0 . If o(a) is finite, let o(a) = p. Then the characteristic of D will be p. We are to prove that p must be prime.

Suppose p is not prime. Let p = p_1p_2 where $p_1 \neq 1, p_2 \neq 1$ and $p_1 < p$ also $p_2 < p$.

Mindset Makers

Since D is an integral domain, therefore the product of two non-zero elements of D cannot be equal to zero. $\therefore \quad aa \neq 0$ i.e., $a^2 \neq 0$.

Now in an integral domain two non-zero elements are of the same order.

$\therefore \quad o(a) = p \Rightarrow o\left(a^2\right) = p \Rightarrow pa^2 = 0 \Rightarrow \left(p_1 p_2\right) a^2 = 0 \quad [\because \quad p = p_1 p_2]$

$\Rightarrow \left(a^2 + a^2 + a^2 + \ldots \text{ upto } p_1 p_2 \text{ terms}\right) = 0 \Rightarrow \left(p_1 a\right)\left(p_2 a\right) = 0$

$\Rightarrow$ enther $p_1 a = 0$ or $p_2 a = 0$ [$\because$ D is without zero divisors]

But $p_1 < p$ and $p_2 < p$. Also p is the least positive integer such that $pa = 0$. Hence p must be prime.

Characteristic of a field. Every field is an Integral domain. Therefore the characteristic of a field F is 0 or $n > 0$ according as any non-zero element (in particular the unit element 1) of F is of order 0 or n.

Thus in order to find the characteristic of a field F, we should find the order of the unit element 1 of F when regarded as a member of the additive group of F. If the order of 1 is zero, then F is of characteristic 0 . If the order of 1 is finite, say, n then the characteristic of F is n.

The characteristic of the field of real numbers is 0. The characteristic of the finite field $\left(I_7, x_7, X_7\right)$ is 7 where $I_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

13. Imbedding of a ring into another ring.

Definition. A ring R is said to be imbedded in a ring R′ if there is a subring S′ of R′ such that R is isomorphic to S′.

Obviously a ring R can be imbedded in a ring R′ if there exists a mapping f of R into R′ such that f is one-to-one and $f(a+b) = f(a) + f(b), f(ab) = f(a) f(b) \; \forall \; a, b \in R.$

Mindset Makers

For then f(R) is a subring of R′ and f is an isomorphism of R onto f(R) making R isomorphic to f(R).

Theorem. Any ring R without a unity element can be imbedded in a ring with unity.

Proof. Let R be any ring without unity. Let Z be the ring of integers.

Let $R' = R \times Z = \{a, m) : a \in R \text{ and } m \in Z \}$.

We shall show that when been defined in $R \times Z$, then it becomes binary operations have been defined in $R \times Z$, then it becomes a ring with a unity element containing a subring, isomorphic to R.

If (a, m) and (b, n) are two elements of $R \times Z$, then we define addition in $R \times Z$ by the equation

$$(a, m) + (b, n) = (a + b, m + n) \qquad \ldots(1)$$

And multiplication in $R \times Z$ by the equation

$$(a, m)(b, n) = (ab + na + mb, mn). \qquad \ldots(2)$$

In the right hand side of (1), a + b is addition of two elements of R and m + n is addition of two integers. In the right hand of (2), ab is multiplication of two elements of R, mn is multiplication of two integers and na, mb are units of R, mn is multiplication.

Since $a + b \in R$ and $m + n \in Z$, therefore $(a + b,\ m + n)(a + b,\ m + n) \in R \times Z$. Thus $R \times Z$ is closed with respect to addition. Further $ab, na, mb \in R \Rightarrow ab + na + mb \in R.$ Also $mn \in Z.$

Therefore $(ab + na + mb, mn) \in R \times Z$ and $R \times Z$ is closed with respect to multiplication.

Now let $(a, m), (b, n), (c, p)$ be any elements of $R \times Z.$ Then we observe:

Associativity of addition. We have

$$[(a, m) + (b, n)] + (c, p) = (a + b, m + n) + (c, p) \ = ([a + b] + c, [m + n] + p) = (a + [b + c], m + [n + p])$$

$$= (a, m) + (b + c, n + p) = (a, m) + [(b, n) + [(c, p)].$$

Commutativity of addition. We have

$(a,m)+(b,n)=(a+b,m+n)\ =(b+a,n+m)$ [$\because$ addition is commutative in R and also in Z]

$=(b,n)+(a,m)$.

Existence of addition identify. We have $(0,0)\in R\times Z$. Here the first 0 is the zero element of R and the seconds 0 is the zero integer. Also $(0,0)+(a,m)=(0+a,0+m)=(a,m)$

$\therefore$ (0, 0) is the additive identity.

Existence of additive inverse. If $(a,m)\in R\times Z$, then

$(-a,-m)\in R\times Z$ and we have

$(-a,-m)+(a,m)=(-a+a,-m+m)=(0,0)$

$\therefore$ $(-a,-m)$ is the additive inverse of (a, m).

Associativity of multiplication. We have

$[(a,m)(b,n)](c,p)=(ab+na+mb,mn)(c,p)$

$=((ab+na+mb)c+p(ab+na+mb)+(mn)c,(mn)p)$

$=(abc+n(ac)+m(bc)+p(ab)+(pn)a+(pm)b+(mn)c,(mn)p).$

Also $(a,m)[(b,n)(c,p)]=(a,m)(bc+pb+nc,np)$

$=(a(bc+pb+nc)+(np)a+m(bc+pb+nc),m(np))$

$=(abc+a(pb)+a(nc)+(np)a+m(bc)+m(pb)+m(nc),(mn)p)$

$=(abc+p(ab)+n(ac)+(np)a+m(bc)+(mp)b+(mn)c,(mn)p)$

We see that $[(a,m)(b,n)](c,p)=(a,m)[(b,n)(c,p)]$

Distributive laws. We have

$(a,m)[(b,n)+(c,p)]=(a,m)(b+c,n+p)$

$=(a(b+c)+(n+p)a+m(b+c),m(n+p))\ =(ab+na+mb,mn)+(ac+pa+mc,mp)$

$=(ab+na+mb,mn)+(ac+pa+mc,mp)\ =(a,m)(b,n)+(a,m)(c,p)$.

Mindset Makers

Similarly we can show that the other distributive law also holds good.

Thus $R \times Z$ is a ring with respect to the operations defined on it.

Existence of multiplicative identity. We have

$(0,1) \in R \times Z.$ if $(a,m) \in R \times Z$, then

$(0,1)(a,m) = (0a + m0 + 1a, 1m) = (0 + 0 + a, m) = (a,m).$

Also $(a,m)(0,1) = (a0 + 1a + m0, m1) = (0 + a + 0, m) = (a,m)$

$\therefore$ (0, 1) is the multiplicative identity. So $R \times Z$ is a ring with unity element (0, 0)

Now consider the subset $S' = R \times \{0\}$ of $R \times Z$ which consists of all pairs of the form (a, 0). We shall show that $R \times \{0\}$ is a subring of $R \times Z$. Let (a, 0), (b, 0) be any two elements of $R \times \{0\}$.

Then $(a,0) - (b,0) = (a,0) + (-b,-0) = (a-b, 0-0) = (a-b,0) \in R \times \{0\}.$

Also $(a,0)(b,0) = (ab + 0a + 0b, 00) = (ab + 0 + 0, 0) = (ab,0) \in R \times \{0\}.$

$\therefore$ $R \times \{0\}$ is a subring of $R \times Z$.

Finally we shall show that R is isomorphic to $R \times \{0\}$. be a mapping from R to $R \times \{0\}$ defined as $\phi(a) = (a,0)\ \forall a \in R.$ ϕ is one-one. We have

$\phi(a) = \phi(b) \Rightarrow (a,0) = (b,0) \Rightarrow a = b \Rightarrow \phi$ is one-one.

ϕ is onto. Let (a, 0) be any element of $R \times \{0\}$. Then $a \in R$ and we have $\phi(a) = (a,0).$

Therefore ϕ is onto. ϕ preserves additions and multiplications.

If a, b be any two elements of R, then

$\phi(a+b) = (a+b,0) = (a,0) + (b,0) = \phi(a) + \phi(b).$

Also $\phi(ab) = (ab,0) = (a,0)(b,0) = \phi(a)\phi(b)$.

$\therefore$ ϕ preserves compositions.

Hence ϕ is an isomorphism of R onto $R \times \{0\}$.

This completes the proof of the theorem.

Mindset Makers

14. The field of Quotients.

Definition. A ring R can be imbedded in a ring S if S contains a subset S′ such that R is isomorphic to S′.

If D is a commutative ring without zero divisors, then we shall see that it can be imbedded in a field F i.e., there exists a field F which contains a subset D′ isomorphic to D. We shall construct a field F with the help of elements of D and this field F will contain a subset D′ such that D is isomorphic to D′. This field F is called the "field of quotients" of D, or simply the “quotient field” of D.

On account of isomorphism of D onto and D′ are abstractly identical. Therefore if we identify D′, with D, then we can say that the quotient field F of D is a field containing D. We shall also see that F is the smallest field containing D.

Motivation for the construction of the quotient field. We are all quite familiar with the ring I of integers. Also our familiar set Q of rational numbers is nothing but the set of quotients of the of the elements of I. Thus $\mathrm{Q}=\left\{\frac{p}{q}: p \in I, 0 \neq q \in I\right\}$. If we identify the rational numbers…, $\frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1}$ ….. with the integers…, $-3,-2,-1,0,1,2,3,\ldots,$ then $I \subseteq Q$.

Also if and $\frac{a}{b}$ and $\frac{c}{d} \in Q$, then we remember that

(i) $\frac{a}{b}=\frac{c}{d}$ iff $ad=bc,$ (ii) $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ (iii) $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$

Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain. We have the following theorem:

Theorem 1. A commutative ring with zero divisors can be imbedded in a field.

Every integral domain can be imbedded in a field.

Mindset Makers

From the elements of an integral domain D, it is possible to construct a field F which contains a subset D′ isomorphic to D.

Proof. Let D be a commutative ring without zero divisors. Let D_0 be the set of all non-zero elements of D. Let $S = D \times D_0$. i.e., let S be the set of all ordered pairs (a, b) where $a, b \in \bar{D}$ and $b \neq 0$. Let us define a relation $\sim$ in S. We shall say that $(a,b) \sim (c,d)$ if and only if ad = bc.

We claim that this relation is an equivalence relation in S. Reflexivity. Since D is a commutative ring, therefore ab = ba $ab = ba \forall a, b \in D.$ Therefore $(a,b) \sim (a,b) \; \forall \; (a,b) \in S.$

Symmetry. We have $(a,b) \sim (c,d)$

$\Rightarrow ad = bc \Rightarrow da = cb$ [$\because$ Multiplication is commutative in D]

$\Rightarrow cb = da \Rightarrow (c,d) \sim (a,b)$

Transitivity. Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$.

Then $ad = bc$ and $cf = de.$ $\therefore$ $adf = bcf$ and $bcf = bde.$

$\therefore$ $adf \Rightarrow bde$ [$\because D$ is a commutative ring]

$\Rightarrow$ $afd - bed = 0 \Rightarrow (af - be)d = 0 \Rightarrow$ $af - be = 0$ [$\because d \neq 0$ and D is without zero divisors]

$\Rightarrow af = be \Rightarrow (a,b) \sim (e,f).$

Thus $\sim$ is an equivalence relation in S. Therefore it will partition S into disjoint equivalence classes. We shall denote the equivalence class containing (a, b) by $\frac{a}{b}$. Other notations to denote this equivalence class are (a, b) or [a, b].

Then $\frac{a}{b} = \{(c,d) \in S : (c,d) \sim (a,b)\}$

Obviously $\frac{d}{b} = c/d$ iff $(a,b) \sim (c,d)$ i.e., iff $ad = bc.$

Mindset Makers

Also $\frac{a}{b}=\frac{ax}{bx}\ \forall\ x\in D_0$. The reason is that

$(a,b)\sim(ax,bx)$ since abx = bax.

These equivalence classes are our quotients. Let F be the set of all such quotients i.e.,

$F=\left\{\frac{a}{b}:(a,b)\in S\right\}$.

We now define addition and multiplication operations in F as follows:

$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ and $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$.

Since D is without zero divisors, therefore $b\neq 0,\ d\neq 0\Rightarrow bd\neq 0$. Therefore both

$\frac{ad+bc}{bd}$ and $\frac{ac}{bd}$ are elements of F. Thus F is closed with respect to addition and

multiplication. We shall now show that both addition and multiplication in F are well defined.

For this we are to show that if

$\frac{a}{b}=\frac{a'}{b'}$ and $\frac{c}{d}=\frac{c'}{d'}$, then $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$ and $\frac{a}{b}\frac{c}{d}=\frac{a'}{b'}\frac{c'}{d'}$

We have $\frac{a}{b}=\frac{a'}{b'}\Rightarrow ab'-ba'$ and $\frac{c}{d}=\frac{c'}{d'}\Rightarrow cd'=dc'$.

Now to show that $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d''}$ we are to show that

$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$ i.e..$(ad+bc)b'd'=bd\left(a'd'+b'c'\right)$.

Now $(ad+bc)b'd'=adb'd'+bcb'd'=ab'dd'+bb'cd'$

$=ba'dd'+bb'dc'$ $\qquad [\because\ \ ab'=ba'$ and $cd'=dc']$

$=bda'd'+bdb'c'=bd\left(a'd'+b'c'\right)$, which was desired.

Again to show that $\frac{ac}{b}\frac{a'}{d}=\frac{c'}{b'}\frac{c'}{d'}$ we are to show that

$\frac{ac}{bd} = \frac{a'c'}{b'd'}$ i.e., $acb'd' = bda'c'$.

Now $acb'd' = ab'cd' = ba'dc' = bda'c'$, which was desired.

Therefore both addition and multiplication are well defined on F. We shall now show that F is a field for these two operations.

Associativity of addition. We have $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$

Existence of additive identify We have

$\frac{0}{a} \in F$ where $a \neq 0$. If $\frac{c}{d}$ is any element of F, then

$\frac{0}{a} + \frac{c}{d} = \frac{0d+ac}{ad} = \frac{0+ac}{ad} - \frac{ac}{ad} = \frac{c}{d}$ $[\because \quad acd = adc]$

$\therefore$ $\frac{0}{a}$ is the additive identify. It should be noted that

$\frac{0}{a} = \frac{0}{b} \; \forall \; a,b \in D_0$. Also $\frac{c}{d} = \frac{0}{a}$ iff $ca = d0$ i.e., $c = 0$.

Existence of additive inverse. If $\frac{a}{b} \in F$, then $\frac{-a}{b} \in F$.

Also we have, $\frac{-a}{b} + \frac{a}{b} = \frac{(-a)b+ba}{b^2} = \frac{0}{b^2} = \frac{0}{a}$ $\left[\because \quad 0a = b^2 0\right]$

$\therefore$ $\frac{-a}{b}$ is the additive inverse of $\frac{a}{b}$.

Associativity of multiplication. We have

$$\left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f} = \frac{ac}{bd}\frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b}\frac{ce}{df} = \frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right)$$

Commutativity of multiplication. We have

$$\frac{ac}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\frac{a}{b}.$$

Existence of multiplication identify. We have

Mindset Makers

$\frac{a}{a} \in F$ where $a \neq 0$. Also if $\frac{c}{d} \in F$, then

$\frac{ac}{a}\frac{ac}{d} = \frac{ac}{ad} = \frac{c}{d}$ [$\because$ $(ac, ad) \sim (c, d)$ because $acd = adc$]

$\therefore$ $\frac{a}{a}$ is the multiplicative inverse of $\frac{a}{b}$,

Distributivity of multiplication over addition. We have

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b}\frac{cf+de}{df} = \frac{a(cf+de)}{bdf} = \frac{acf+ade}{bdf} = \frac{(acf+ade)bdf}{bdfbdf}$$

$$= \frac{acfbdf+bdfade}{bdfbdf} = \frac{acf}{bdf}+\frac{ade}{bdf} = \frac{ac}{ba}+\frac{ae}{bf} = \frac{ac}{b}\frac{c}{d}+\frac{ae}{bf}.$$

Similarly the other distributive law holds.

$\therefore$ F is a field under the addition and multiplication defined above. This field F is called the field of quotients of D.

We shall now show that the field F contains a subset D′ such that D is isomorphic to D′.

Let $D' = \left\{\frac{ax}{x} \in F : a, 0 \neq x \in D\right\}$. Then $D' \subseteq F$. If $x \neq 0$, $y \neq 0$ are elements of D, then

$\frac{ax}{x} = \frac{ay}{y}$ since $axy = xay$. Therefore if x is any fixed non-zero element of D, we can write

$D' = \left\{\frac{ax}{x} \in F : a \in D\right\}$.

We claim that the function ϕ: $D \to D'$ defined by

$\phi(a) = \frac{ax}{x}$ $\forall$ $a \in D$ is an isomorphism of D onto D′.

ϕ is one-one. We have

$$\phi(a) = \phi(b) \Rightarrow \frac{ax}{x} = \frac{bx}{x} \Rightarrow axx = xbx \Rightarrow ax^2 = bx^2 \Rightarrow (a-b)x^2 = 0$$

Mindset Makers

$\Rightarrow a-b=0,$ since $x^2 \neq 0 \Rightarrow a=b.$ $\therefore$ ϕ is one-one

ϕ is onto D′. If $\frac{ax}{x} \in D',$ then $a \in D.$ Also we have $\phi(a)=\frac{ax}{x}$.

Thus ϕ is onto D′.

Also $\phi(a+b)=\frac{(a+b)x}{x}=\frac{(a+b)x^2}{x^2}=\frac{ax^2+bx^2}{x^2}=\frac{axx+xbx}{x^2}$ $=\frac{ax}{x}+\frac{bx}{x}=\phi(a)+\phi(b)$

and $\phi(ab)=\frac{(ab)x}{x}=\frac{(ab)x^2}{x^2}=\frac{(ax)(bx)}{x^2}=\frac{ax}{x}\frac{bx}{x}=\phi(a)\phi(b)$.

$\therefore$ ϕ is an isomorphism of D and D′. Hence $D \cong D'$

Hence

If we identify D′ with D i.e., if in F we write a, b, c etc. in place of $\frac{ax}{x}, \frac{bx}{x}, \frac{cx}{x}$ etc., then we see that D is contained in F. Thus F (the field of quotients of D) is a field containing D.

In the next theorem we shall show that the quotient field F of D is the smallest field containing D. In other words if D is contained in any other field K, then F will also be contained in K.

Theorem 2. If K is any field which contains an integral domain D, then K contains a subfield isomorphic to the quotient field F of D. In other words the quotient field F of D is the smallest field containing D.

Proof. Let D be a commutative ring without zero divisors, Let $a \in D$ and $0 \neq b \in D$. Since K is a field containing D, therefore $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K$.

Let K′ be the subset of K containing the elements of the form ab^{-1} where $a,b \in D$ with $b \neq 0.$

Thus

$K' = \{ab^{-1} \in K : a, 0 \neq b \in D\}$.

Mindset Makers

We shall show that K′ is a subfield of K and K′ is isomorphic to the quotient field F of D. Let $ab^{-1} \in K', cd^{-1} \in K'$. Then $0 \neq b, 0 \neq d \in D$.

Now $ab^{-1} - cd^{-1} = add^{-1}b^{-1} - cbb^{-1}d^{-1} = (ad - bc)d^{-1}b^{-1} = (ad - bc)(bd)^{-1} \in K'$, since $ad - bc \in D$ and $0 \neq bd \in D$.

Further suppose that $0 \neq cd^{-1} \in K'$. Then $c \neq 0$ and we have $\left(ab^{-1}\right)\left(cd^{-1}\right)^{-1} = ab^{-1}dc^{-1} = ad(cb)^{-1} \in K'$, since $ad \in D$ and $0 \neq cb \in D$.

Hence K′ is a subfield of K. We shall now show that the quotient field F of D is isomorphic to K′. We have $F = \left\{\frac{a}{b} : a \in D, 0 \neq b \in D\right\}$

Consider the mapping $f : F \to K'$ defined by

$$f\left(\frac{a}{b}\right) = ab^{-1} \ \forall \ \frac{a}{b} \in F.$$

The mapping f is one-one because we have

$$f\left(\frac{a}{b}\right) = f\left(\frac{c}{d}\right) \Rightarrow ab^{-1} = cd^{-1}$$

$$\Rightarrow ab^{-1}bd = cd^{-1}bd \Rightarrow ad = cbd^{-1}d$$

$$\Rightarrow ad = bc \Rightarrow (a,b) \sim (c,d) \Rightarrow \frac{a}{b} = \frac{c}{d}.$$

Also f is onto K′. If ab^{-1} is any element of K′, then $\frac{a}{b} \in F$ and $f\left(\frac{a}{b}\right) = ab^{-1}$.

Further $f\left(\frac{a}{b} + \frac{c}{d}\right) = f\left(\frac{ad + bc}{bd}\right) = (ad + bc)(bd)^{-1}$

$$= (ad + bc)d^{-1}b^{-1} = add^{-1}b^{-1} + bcd^{-1}b^{-1}$$

$$= ab^{-1} + cd^{-1} = f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right).$$

Mindset Makers

Also $f\left(\frac{a}{b}\frac{c}{d}\right)=f\left(\frac{ac}{bd}\right)=(ac)(bd)^{-1}=(ac)d^{-1}b^{-1}=\left(ab^{-1}\right)\left(cd^{-1}\right)=f\left(\frac{a}{b}\right)f\left(\frac{c}{d}\right)$

Hence $F\cong K'$.

$=(ab^{-1})(cd^{-1})=f\left(\frac{a}{b}\right)f\left(\frac{c}{d}\right)$

Hence $F\cong K'$.

If we identify K' with F, we see that if D is contained in any filed K, then F is also contained in K. Therefore F is the smallest field containing D.

Cor. The quotient field of a finite integral domain concludes D. The quotient field F of D is also the smallest field containing D. Hence F coincides with D.

Ex. What is the quotient field of 2 Z, where Z is the ring integers?

Theorem: Any two isomorphic integral domains have isomorphic-quotient fields.

Let f be an isomorphism of D onto D'. If a, b, c, etc. are the elements of D then f (a), f (b), f(c) etc. will be the elements of D'. Also.

$F(a+b)=f(a)+f(b)$ and $f(ab)=f(a)f(b)+a,b\in D.$

Let F, F' be the quotient fields of D, D' respectively. Then F consists of the equivalence classes (quotients) of the from $\frac{a}{b}$ where a, $0\neq$ b $\in$ D and F' consists of the equivalence classes of the

$\frac{f(a)}{f(a)}$ where $f(a),0\neq f(b)\in D'$.

Consider the mapping ϕ : F $\rightarrow$ F' defined by $\phi\left(\frac{a}{b}\right)=\frac{f(a)}{f(a)}\vee\frac{a}{b}\in F.$

First we shall show that the mapping ϕ is well defined i.e., if.

$\frac{a}{b}=\frac{c}{d}$ then $\phi\left(\frac{a}{b}\right)=\phi\left(\frac{c}{d}\right)$ we have $\frac{a}{b}=\frac{c}{d}\Rightarrow ad=bc$

$\Rightarrow f(ad)=f(bc)\Rightarrow f(a)f(d)=f(b)f(c)\Rightarrow\frac{f(a)}{f(b)}=\frac{f(c)}{f(d)}\Rightarrow\phi\left(\frac{a}{b}\right)=\phi\left(\frac{c}{d}\right)$

$\therefore$ ϕ is well defined.

ϕ is one-one, we have

$\phi\left(\frac{a}{b}\right)=\phi\left(\frac{c}{d}\right)\Rightarrow\frac{f(a)}{f(b)}=\frac{f(c)}{f(d)}\Rightarrow f(a)f(d)=f(b)f(c)\Rightarrow f(ad)=f(bc)\Rightarrow ad=bc\Rightarrow\frac{a}{b}=\frac{c}{d}$

ϕ is one-one

Mindset Makers

Also ϕ is onto F'. $\frac{f(a)}{f(b)} \in F'$, then

$\frac{a}{b} \in F$ *and* $\phi\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}$. Therefore ϕ is onto F'.

Further

$$\phi\left(\frac{a}{b}+\frac{c}{d}\right) = \phi\left(\frac{ad+bc}{bd}\right) = \frac{f(ad+bc)}{f(bd)} = \frac{f(ad)+f(bc)}{f(b)f(d)}$$

$$= \frac{f(a)f(d)+f(b)f(c)}{f(b)f(d)} = \frac{f(a)}{f(b)} + \frac{f(c)}{f(d)} = \phi\left(\frac{a}{b}\right) + \phi\left(\frac{c}{d}\right) \text{ Also}$$

$$\phi\left(\frac{a}{b}\frac{c}{d}\right) = \phi\left(\frac{ac}{bd}\right) = \frac{f(ac)}{f(bd)} = \frac{f(a)f(c)}{f(b)(d)}$$

$$= \frac{f(a)}{f(b)}\frac{f(c)}{f(d)} = \phi\left(\frac{a}{b}\right)\phi\left(\frac{c}{d}\right)$$

$\therefore$ ϕ is an isomorphism of F onto F'.

$\therefore$ $F \cong F'$.

Theorem 1. Show that every prime field of characteristic 0 is isomorphic to the field of rational numbers.

Proof. Let F be a prime field of characteristic 0. For the sake of convenience let us denote the unity element (multiplicative identity) of F by e. Since F is of characteristic 0, therefore for any integer n, we have ne=0 (zero element of F) if and only if n=0.

Here ne is an integral multiple of the element e of F. We have ne$\in$F. Consider a subset F' of F defined as F= {me/ne: m, n$\in$ the set of integers I with n$\neq$0}.

Since $n \neq 0 \Rightarrow ne \neq 0$, therefore *ne* is an inversible element of F. So me/ne=(me) $(ne)^{-1}$ is definitely an element of F. We claim that F' is a subfield of F.

Let $\frac{m_1e}{n_1e}, \frac{m_2e}{n_2e} = \frac{(m_1e)(n_2e)-(n_1e)m_2e)}{(n_1e)(n_2e)} = \frac{(m_1n_2)e^2-(n_1m_2)e^2}{(n_1n_2)e^2} = \frac{(m_1n_2)e-(n_1m_2)}{(n_1n_2)e}$ $[\because e^2 = e]$

$$= \frac{(m_1n_2-n_1m_2)}{(n_1n_2)e} \in F' \text{since} 0 \neq n_1n_2 \in I.$$

Again let $\frac{m_1e}{n_1e}$ by any element of F' and $\frac{m_2e}{n_2e}$ be any non-zero element of F'. Then $m_1, n_1 \in$ I with $n_1 \neq 0$. Also $m_2, n_1 \in$ I with $m_2 \neq 0, n_2 \neq 0$. We have.

$$\frac{m_1e}{n_1e}\left(\frac{m_2e}{n_2e}\right)^{-1} = \frac{m_1e}{n_1e}\frac{n_2e}{m_2e} = \frac{(m_1e)(n_2e)}{(n_1e)(m_2e)} = \frac{(m_1n_2)e^2}{(n_1m_2)e^2} = \frac{(m_1n_2)e}{(n_1m_2)e} \in F' \text{since } 0 \neq n_1m_2 \in I.$$

Therefore F' is a subfield of F. But F can have no proper subfield because F is a prime field. Therefore we must have F' = F.

Mindset Makers

Thus F = $\{m_e/ n_e : m, n \in I \text{ with } n \neq 0\}$ if Q is the filed off rational numbers, then Q = $\{m/ n : m, n \in I \text{ with } n \neq 0\}$

Let f be a mapping from F into Q defined as

f (me/ne) = m/n : m, n $\in$ I with n $\neq$0.

f is well-defined. We

have $\frac{m_1e}{n_1e} = \frac{m_2e}{n_2e} \Rightarrow (m_1e)(n_2e) = (n_1e)(m_2e) \Rightarrow (m_1n_2)e^2 = (n_1m_2)e^2 \Rightarrow (m_1n_2)e = (n_1m_2)e$

$\Rightarrow (m_1n_2 - n_1m_2)e = 0 \Rightarrow m_1n_2 - n_1m_2 = 0$

$\Rightarrow \frac{m_1}{n_1} = \frac{m_2}{n_2} \Rightarrow f\left(\frac{m_1e}{n_1e}\right) = f\left(\frac{m_2e}{n_ee}\right)$. $\therefore$ the mapping f is well-defined.

f is one-one. We have $f\left(\frac{m_1e}{n_1e}\right) = f\left(\frac{m_2e}{n_ee}\right). \Rightarrow (m_1e)(n_2e) = (n_1e)(m_2e) \Rightarrow \frac{m_1e}{n_1e} = \frac{m_2e}{n_2e} \Rightarrow f$ is one-one.

f is onto. Let m/n be any element of Q. Then me/ne $\in$ *F* and it such that *f* (me/ne) = m/n. Therefore f is onto.

f preserves compositions. We have

$$f\left(\frac{m_1e}{n_1e} + \frac{m_2e}{n_2e}\right) = f\left[\frac{(m_1e)(n_2e) + (n_1e)(m_2e)}{(n_1e)(n_1e)}\right] = f\left[\frac{(m_1 + n_2 + n_1m_2)e}{(n_1n_2)}\right]$$

$$= \frac{m_1n_2 + n_1m_2}{n_1n_2} = \frac{m_1}{n_1} + \frac{m_2}{n_2} = f\left(\frac{m_1e}{n_1e}\right) + f\left(\frac{m_2e}{n_2e}\right)$$

Also $f\left(\frac{m_1e}{n_1e}\frac{m_2e}{n_2e}\right) = f\left[\frac{(m_1m_2)e^2}{(n_2n_2)e^2}\right] = f\left[\frac{(m_2m_2)e}{(n_1n_2)e}\right]$

$$= \frac{m_1m_2}{n_1n_1} = \frac{m_1}{n_1}\frac{m_2}{n_2} = f\left(\frac{m_1e}{n_1e}\right) f\left(\frac{m_2e}{n_2e}\right)$$

Theorem 2 Every field of characteristic 0 contains a subfield isomorphic to the field of rational Number.

Proof. Let F be any field of characteristic 0 and let e be the unity element of F. Since F is of characteristic 0, therefore for any integer n, we have ne = 0 if and only if n = 0.

Consider the subset F' of F defined as

$$F' = \{me/ne : m \in I, 0 \neq n \in I\}$$

Now prove that F' is a subfield of F and F' $\cong$ Q where Q is the field of rational numbers. Give the same proof as in theorem 1.

Theorem 3. Every prime field of finite characteristic p is isomorphic to the field I_p of the residue classes of the set of integers modulo p.

Proof. Let F be a prime field of finite characteristic p. Then p must be a prime number. The unit elemen t e of

Mindset Makers

ne = 0 if and only if p is a divisor of n.

Consider a subset F' of F defined as $F' = \{ne : n \in I \text{ where } I \text{ is the set of integers.}\}$

F' is a cyclic subgroup of the additive group of F. Since F' is generated by e whose order is p, therefore F' contains p distinct elements. We claim that F' is a subfield of F. For this we shall prove that F' is an integral domain and we know that every finite integral domain is a field.

Let me, ne be any two elements of F'. Then $me - ne = (m-n)e \in F' \text{since } m-n \in I$

Also $(me)-(ne) = (mn)e^2 = \in F' \text{ since } mn \in I$

Thus F' is a subring of F. Since F is without zero divisors, therefore F' is also without zero divisors. Therefore F' is a commutative ring without zero divisors. Therefore F' is an integral domain and so F' is a subfield of F. But F can have no proper subfield because F is a prime field. Therefore we must have

$F = F' = \{ne : n \in I\}$

Now we shall prove that $F \cong I_p$

Let f be a mapping from F into I_p defined as

F (ne) = the residue class [n], $\forall\ n \in I$

f is well defined. We have ne = me

$\Rightarrow (n-m)e = 0 \Rightarrow p$ is devisor of n – m $\Rightarrow n \equiv m (\text{mod p})$

$\Rightarrow [n] = [m] \Rightarrow f(ne) = f(me) \Rightarrow$ f is well- defined.

F is one- one. We have f(ne) = f(me)

$\Rightarrow [n] = [m] \Rightarrow n-m$ is divisible by $p \Rightarrow (n-m)e = 0$

$\Rightarrow ne = me \Rightarrow$ f is one – one.

f is onto. Let [n] by any element of I_P. Then $ne \in F$ and is such that f (ne) = [n]. Therefore f is onto.

f preserves compositions. We have

$f(me+ne) = f((m+n)e) = [m+n] = [m]+[n] = f(me)+f(ne)$

$f(me)(ne) = f((mn)e) = [mn] = [m][n] = f(me)\,f(ne)$

Hence $F \cong I_p$

Note. The ring of endomorphisms of an abelian group G is a ring with unity. If 1 denotes the identity mapping of G 1:G→G such that $1\ (a) = (a), \forall\ a \in G,$ then 1 is the unit element of this ring. Obviously 1 is an endomorphism of G and we have $1f = f = f1 \forall\ f \in R$. The ring R may not be commutative and may have zero divisors.

Theorem 2. Every ring with unity is isomorphic to a ring of endomorphisms of an abelian group.

Proof. Let R be a ring with unity element 1. The additive group of R is an abelian group. Let S denote the ring of endomorphisms of the abelian group R.

If a ∈R, let f_a denote the mapping of R into itself defined

by the rule $f_a(x) = ax \ \forall\ x \in R$

Obviously f_a is an endomorphism of the additive group of R.

For, if $x, y \in R,$ We have $f_a(x+y) = a(x+y) = ax+ay = f_a(x)+f_a(y)$

Thus is an endomorphism of the additive group of R. Let of S. First we shall show that

$f_{a+b} = f_a + f_b, f_{ab} = f_a f_b, f_{-a} = -f_a$

Now for all $x \in R$, We have $f_{a+b}(x) = (a+b)x = ax+bx = f_a(x)+f_b(x) = (f_a + f_b)(x)$

Mindset Makers

Therefore $f_{a+b} = f_a \_ f_b$

Further $f_{-a}(x) = (-a)x = -(ax) = -[f_a(x)] = -(-f_a)(x)$

Therefore $f_{-a} = -f_a$

Now let f_a, f_b be any two elements of T. We have

$f_a - f_b = f_a + (-f_b) = f_a + f_b = f_{a+(-b)} = f_{a-b}$ Since $a - b \in R$ Therefore

$f_{a-b} \in T$. *Also* $f_a f_b = f_{ab} \in T$ since $ab \in R$ *Thus* $f_a, f_b \in T$

$\Rightarrow f_a - f_b \in T$ and $f_a f_b \in T$. Therefore T is a subring of S.

Now we shall show that the ring R is isomorphic to the ring T. Let ϕ: R→T such that $\phi(a) = f_a \forall a \in R$

ϕ is one – one. If $a, b \in R$ Then

$\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \forall x \in R \Rightarrow ax = bx \ \forall \ x \in R$

$\Rightarrow a1 = b1 \quad [\because \quad 1 \in R] \quad \Rightarrow a = b$. Therefore ϕ is 1-1.

ϕ is onto. Let $f_a \in T$. Then $a \in R$ and we have $\phi(a) = f_a$. Therefore ϕ is onto.

ϕ preserves compositions in R and T. Let $a, b \in R$. Then

$\phi(a+b) = f_{a+b} = f_a + f_b = \phi(a) + \phi(b)$

And $\phi(ab) = f_{ab} = f_a f_b = \phi(a)\phi(b)$

Hence ϕ is an isomorphism of the ring R onto the ring T and therefore $R \cong T$

Theorem 4. An ideal S of a commutative ring R with unity is maximal if and only if the residue class ring R/S is a field.

Proof. Since R is a commutative ring with unity; therefore R/S is also a commutative ring with unity. The zero element of the ring R/S is S and the unity element is the coset S+1 where I is the unity element of R.

Let the ideal S be maximal. Then to prove that R/S is a field.

Let S+b be any non zero element of R/S. Then S+b≠S i.e., b ∉es. To prove that S+b is inversible.

If (b) is the principal ideal of R generated by b, then S+(b) is also an ideal of R. Since b ∉S, therefore the ideal S is properly contained in S+(b). But S is a maximal ideal of R. Hence we must have S+(b)=R.

Since I ∉R, therefore we must obtain 1 on adding an element of S to an element of (b). Therefore there exists an element a ∈∈S and x ∈R such that

$a + \alpha b = 1$ [*Note that* $(b) = \{\alpha b : \alpha \in R\}$]

$a - \alpha b = a \in S$

Consequently $S + 1 = S + \alpha b = (S + a)(S + b)$

$\therefore S + \alpha = (S + b)^{-1}$ Thus S + b is inversible .

$\therefore R/S$ is a field.

Conversely, let S be an ideal of R such that R/S is a field. We shall prove that S is a maximal ideal of R.

365

Let S' be an ideal of R properly containing S i.e., S ⊆ S and S ≠ S. Then S will be maximal if S' = R. The elements of R contained in S already belong to S' since S ⊆ S. Therefore R will be a subset of S' if every element α of R not contained in S also be-longs to S'. If $\alpha \in$ R is such that $\alpha \notin$S, then $S + \alpha \neq S$ i.e., S+α is a non-zero element of R/S. Also S' properly contains S.

There- fore there exists an element β of S' not contained in S so that S+ β is also a non-zero element of R/S. Now the non-zero elements of R/S form a group with respect to multiplication because R/S is a field. Therefore there exists a non-zero element S+y of R/S such that

$$(S+y)(S+\beta)=S+\alpha$$

[We may take $S+y=(S+\alpha)(S+\beta)^{-1}$]

$\Rightarrow S+y\beta=S+\alpha\Rightarrow y\beta-\alpha\in S\Rightarrow y\beta-\alpha\in S'$ $[\because S\subseteq S']$

Now S' is an ideal. Therefore $y\in R,\beta\in S'\Rightarrow y\beta\in S'$ Again

$y\beta\in S', y\beta-S'\Rightarrow y\beta(y\beta-\alpha)\in S'$ *i.e.* $\alpha\in S'$

Thus $R\subseteq S'$ Also $S'\subseteq R$ as S' is an ideal of R.

$\therefore$ S = R

Hence the theorem.

Theorem 1. Let R be a commutative ring and S an ideal of R. Then the ring of residue classes R/S is an integral domain if and only if S is a prime ideal.

Proof. Let R be a commutative ring and S an ideal of R.

Then $R/S=\{S+a: a\in R\}$

Let S + a, S + b be any two elements of R/S. Then $a.b\in R$

We have (S +a) (S +b) = S + ab

= S + ab [$\therefore$ R is a commutative ring]

= (S +b) (S +a)

$\therefore$ R/S is a commutative ring.

Now let S be a prime ideal of R Then we are to prove that R/S is an integral domain. For this we are to show that R/S is without zero divisors. The zero element of the ring R/S is the residue class S itself. Let S+a, S+b be any two elements of R/S.

Then (S+a) (S+b) = S (the zero element of R/S)

$\Rightarrow S+ab=S\Rightarrow ab\in S$

Either a or b is in S, since S is a prime ideal

$\Rightarrow$ either S + a = S or S + b = S [Note that $a\in S\Leftrightarrow S+a=S$]

$\Rightarrow$ either S + a or S + b is the zero element of R/S.

$\therefore$ R/S is without zero divisors.

Since R/S is a commutative ring without zero divisors, therefore R/S is an integral domain.

Conversely, let R/S be an integral domain. Then we are to prove that S is a prime ideal of R.

Let a, b be any two elements in R such that ab $\in$ S. We have

ab $\in$ S $\Rightarrow$ S+ab = S $\Rightarrow$ (S+a) (S+b) = S.

Since R/S is an integral domain, therefore it is without zero divisors. Therefore

(S+a) (S+b)=S (the zero element of R/S)

$\Rightarrow$ either S + a or S + b is zero $\Rightarrow$ either S + a = S or S + b = S

$\Rightarrow$ either $a\in S$ *or* $b\in S\Rightarrow S$ is a prime ideal.

This completes the proof of the theorem.

Note If R is a ring with unity, then R/S is also a ring with unity. The residue class S+l is the unity element of R/S. There- fore if we define an integral domain as a commutative ring with unity and without zero divisors, even then the above theorem will be true. But in that case R must be a commutative ring with "nity.

Theorem. Let R be a commutative ring with unity. Then every maximal ideal of R is a prime ideal.

Mindset Makers

Proof. R is a commutative ring with unit element. Let S be a maximal ideal of R. Then R/S is a field.

Now every field is an integral domain. Therefore R/S is also an integral domain. Hence by theorem 1, S is a prime ideal of R. This completes the proof of the theorem.

But it should be noted that the converse of the above theorem is not true i.e., every prime ideal is not necessarily a maximum ideal.

Solved Examples

Ex.1. Let R be the field of real numbers and S the set of all those polynomials $f(x) \in R[x]$ such that f (0) = 0=F (1). Prove that S is an ideal of R [x]. Is the residue class ring R [x] / S an integral domain ? give reasons for your answer.

Solution Let f (x), g (x) be any elements of S. Then

$f(0) = 0\, f(1)$ *and* $g(0) = 0 = g(1)$

Let $h(x) = f(x) - g(x)$ Then

$h(0) = f(0) - g(0) = 0 - 0 = 0$ *and* $f(1) - g(1) = 0 - 0 = 0$

Thus $h(0) = 0 = h(1)$ *Therefore* $h(x) \in S$

Thus $f(x), g(x) \in S \Rightarrow h(x) = f(x) - g(x) \in S$

Further let f (x) be any element of S and r(x) be any element of R[x]. Then f (0) = 0 = f(1), by definition of S.

Let t (x) = r (x) f (x) = f (x) r (x) [R[x] is a commutative ring]

Then t (0) = r (0) f (0) = r (0). 0 = 0

and t (1) = r (1) f (1) = r (1). 0=0.

$t(x) \in S$

Thus $r(x) \in R[x], f(x) \in S \Rightarrow r(x) f(x) \in S$

Hence S is an ideal of R[x].

Now we claim that S is not a prime ideal of R[x]. Let f (x) = x (x-1). Then f (0) = 0 (0-1) = 0, and f (1) = 1 (1-1) = 0. Thus f(x) = x (x-1) is an element of S.

Now let p (x) = x, q (x) = x-1.

We have p (1) = 1≠ 0. Therefore $p(x) \notin S$ Also q (0) = 0-1 = - 1 ≠ 0. Therefore q (x) ∉S.

Thus $x(x-1) \in S$ while neither $x \in S$ *nor* $x - 1 \in S$ Hence S is not a prime ideal of R [x].

Since S is not a prime ideal of R [x], therefore the residue class ring R[x]/S is not an integral domain.

Ex.2 Let R be the ring of all real valued continuous functions defined on the closed interval [0, 1]. Let

M={f(x) ∈ R : f (t)=0}.

Show that M is a maximal ideal of R.

Solution. First of all we observe that M is non-empty because the real valued function e(x) on [0, 1] defined by belongs to M.

e (x)=0 ∨ x ∈ [0, 1]

belongs to M.

Now let f(x), g(x) be any two elements of M. Then f(1/3) = 0, 8(1/3) = 0, by definition of M.

Let h(x) = f(x) - 8(x). Then h(1/3)=(3)-g(1/3) = 0 - 0 = 0.

Therefore h(x) ∈ M.

Thus $f(x), g(x) \in M \Rightarrow h(x) = f(x) - g(x) \in M$.

Mindset Makers

Further let f(x) be any element of M and r(x) be any element of R. Then f(1/3) = 0, by definition of M.

Let $t(x)=r(x)\,f(x)=f(x)r(x)$ [R is a commutative ring]

Then $t(1/3)=r(1/3)\,f(1/3)=r(1/3)$ Therefore t (x) $\in$ M

Thus $r(x)\in R, f(x)\in M \Rightarrow r(x)\,f(x)\in M$

Hence M is an ideal of R.

Clearly M $\neq$ R because i(x) $\in$ R given by i(x) = 1 $\forall$ $x\in[0,1]$ does not belong to M.

The ring R is with unity and the element i(x) is its unity element.

Let N be an ideal of R properly containing M i.e., M $\subseteq$ N and M $\neq$ N. Then M will be a maximal ideal of R if N=R, which will be so if the unity i(x) of R belongs to N. Since M is a proper subset of N, therefore there exists λ (x) $\notin$ N such that λ (x) $\notin$ M.

This means $\lambda(1/3)\neq 0$. Put $\lambda(1/3)$ = c where c$\neq$0.

Let us define $\beta(x)\in R$ *by* $\beta(x)=c\forall\ x\in[0,1]$ Now consider

$\mu(x)\in R$ *given by* $\mu(x)=\lambda(x)-\beta(x)$

We have $\mu(1/3)=\lambda(1/3)-\beta(1/3)=c-c=0$

Therefore μ (x) $\in$ M and so μ (x) also belongs to N because N is a super-set of M. Now N is an ideal of R and λ(x), μ (x) are in N. Therefore λ(x) - μ(x) = β (x) is also an element of N.

Now define $\gamma(x)\in R by\,\gamma(x)=1/c\forall x\in[0,1]$. Since N is an ideal of R, therefore

$\gamma(x)\in R and\,\beta(x)\in N\Rightarrow\gamma(x)\beta(x)\in N.$ We shall show that $\gamma(x)\beta(x)=ix$

For every $x\in[0,1]$ we have

$$\gamma(x)\beta(x)=(1/c)c=1$$

Therefore $\gamma(x)\beta(x)=i(x)$ by the definition of $i(x)$.

Thus the unity element t (x) of R belongs to N and consequently N = R

Hence M is a maximal ideal of R.

Ex. 3. If R is a finite commutative ring (i.e., has only a finite per of elements) with unit élement prove that every prime ideal of R is a maximal ideal of R.

Solution. Let R be a finite commutative ring with unit element. Let S be a prime ideal of R. Then to prove that S is a maximal ideal of R. Since S is a prime ideal of R, therefore the residue class ring

R/S is an integral domain. Now $R/S=\{S+a:a\in R\}$

Since R is a finite ring, therefore R/S is a finite integral do- main. But every finite integral domain is a field. Therefore R/S is a field. Since R is a commutative ring with unity and R/S is a field, therefore S is a maximal ideal of R.

CSE

Ex.4. Give an example of a ring in which some prime ideal is not a maximal ideal.

Solution. Let I [x] be the ring of polynomials over the ring of integers I. Let S be the principal ideal of I [x] generated by x i.e., let S = (x). We shall show that (x) is prime but not maximal.

We have S = (x) = {x f(x): f(x) $\in$ I [x]}.

First we shall prove that S is prime.

Let a(x), b(x) $\in$ I [x] be such that a(x) b(x) $\in$ S. Then there exists a polynomial c (x) $\in$ I [x] such that

Xc (x) = a (x) b (x) …(1)

Mindset Makers

Let a (x) $= a_0 + a_1x + a_1x^2 + ...,b(x) = b_0 + b_1x + b_1x^2 + ...$

$c(x) = (c_0 + c_1x + ...) = (a_0 + a_1x + ...)(b_0 + b_1x + ...)$ Then (1) becomes

$x(c_0 + c_1x + ...) = (a_0 + a_1x + ...)(b_0 + b_1x + ...)$

Equating the constant term on both sides, we get

$a_0b_0 = 0$

$\Rightarrow a_0 - 0$ *or* $b_0 = 0$ [$\therefore$ I is without zero divisors]

Now $a_0 = 0 \Rightarrow a(x) = a_1x + a_2x^2 + ...$

$\Rightarrow a(x) = (x)(a_1 + a_2x + ...) \Rightarrow a(x) \in (x)$

Similarly $b_0 = 0 \Rightarrow b(x) = b_1x + b_2x^2 + ...$

$\Rightarrow b(x) = (x)(b_1 + b_2x + ...) \Rightarrow b(x) \in (x)$

Thus a (x) b (x) $\in$(x) $\Rightarrow$either $a(x) \in (x)$ *or* $b(x) \in (x)$

Hence (x) is a prime ideal.

Now we shall show that (x) is not a maximal ideal of I [x]. For this we must show an ideal N of I [x] such that (x) is properly contained in N, while N itself is properly contained in I [x]. The ideal N = (x, 2) serves this purpose.

Obviously (x) $\subseteq$ (x, 2). In order to show that (x) is properly contained in (x, 2) we must show an element of (x, 2) which is not in (x). Clearly 2 $\in$ (x, 2). We shall show that 2 $\notin$(x).

Let $2 \in (x)$. Then we can write,

$2 = xf(x)$ for some $f(x) \in I[x]$

Let $f(x) = a_0 + a_1x + ...$

Then $2 = xf(x) \Rightarrow 2 = x(a_0 + a_1x + ...)$

$\Rightarrow 2 = a_0x + a_1x^2 + ...$

$\Rightarrow 2 = 0 + a_0x + a_1x^2 + ...$

$\Rightarrow 2 = 0$ [by equality of two polynemials]

But $2 \neq 0$ in the ring of integers. Hence 2 $\notin$(x). Thus (x) is properly contained in (x,2).

Now obviously $(x,2) \subseteq I[x]$. In order to show that (x,2) is properly contained in (x, 2). is properly contained in I [x] we must show an element of I [x] which is not in (x, 2). Clearly 1 $\in$I [x]. We shall show that $1 \notin (x,2)$. Let $1 \in I[x]$ Then we have a relation of the form

$1 = xf(x) + 2g(x)$ where $f(x)g(x) \in I[x]$.

Let $f(x) = a_0 + a_1x + ..., g(x) = b_0 + B_1x +$

Then $1 = xf(a_0 + a_1x + ...) + 2(b_0 + B_1x + ...)$

$\Rightarrow 1 = 2b_0$ [Equating constant term on both sides]

But there is no integer b_0 such that $1 = 2b_0$

Hence $1 \notin (x,2)$ Thus $(x,2)$ is properly contained in I [x].

Therefore (x) is not a maximal ideal of I[x]

Theorem 10 An ideal S of the Euclidean ring R is maximal iff S is generated by some prime element of R.

Proof. We know that every ideal of a Euclidean ring R is a principal ideal. Suppose S is an ideal of R generated by p so that S=(p). Now we are to prove that

(i) S is maximal if p is a prime element of R.

Mindset Makers

(ii) p is prime if S is maximal.
First we shall prove (i). Let p be a prime element of R such that (p) = S. Let T be an ideal of R such that $S \subseteq T \subseteq R$. Since T is also a principal ideal of R, so let T = (q) where $q \in R$.

Now $S \subseteq$ T-(p) $\subseteq$ (q) $\rightarrow p \in (q) \Rightarrow p = xq$ for some $x \in R \Rightarrow q / p$
Since p is prime, therefore either q should be a unit in R or q should be an associate of p.
If q is a unit in R, then T=(q)=R.
If q is an associate of p, then T=(q)=(p)=S.
Thus either T-R or T=S.
Now we shall prove (ii). Let (p) = S be a maximal ideal. We are to show that p is prime. Let us suppose that p is composite i.e., p is not prime.
Let p = mn where neither m nor n is a unit in R.
Now p = mn $\Rightarrow$ m\p $\Rightarrow (p) \subseteq (m)$
But $(m) \subseteq R$. Therefore we have $(p) \subseteq (m) \subseteq R$
But (p) is a maximal ideal, therefore we should have either
(m) = (p) or (m) = R
If R = (m) then $R \subseteq (m)$
$\therefore 1 \in R \Rightarrow 1 \in (m) \Rightarrow 1 = ym$ for some $y \in R \Rightarrow$ m is inversible $\Rightarrow$ m is a unit in R.
Thus we get a contradiction.
If (m) = (p), then $m \in (p)$. Therefore m = lp for some $I \in R$
$\therefore p = mn = lpn = p\ln \ \therefore p(1 - \ln) = 0$
$\Rightarrow 1 - \ln = 0$ [$\therefore$ p $\neq$ 0 and R is without zero divisors]
$\Rightarrow$ In = 1 $\Rightarrow$ n is inversible $\Rightarrow$ n is a unit of R.
This is again a contradiction. Hence p must be a prime element of R

Mindset Makers

Revision Document: Ring Theory

Ring: Let R be a non-empty set $(R,+,\cdot)$ is said to be ring if

(a) $(R,+)$**is Commutative group (b)** $(R,\cdot)$ **is Semi-group (c) Left and Right Distributive Law**

Note- The set is an abelian group w.r.t the **first** binary composition.

Examples: $(Z,+,\cdot)$ is Ring, $(Q,+,\square),(\mathbf{R},+,\square),(\mathbf{C},+,\square)$ are also Rings.

Commutative Ring: A ring $(R,+,\square)$ is said to be commutative ring if $ab=ba,\forall a,b\in R$

Q. $(Z,+,\square),(Q,+,\square),(\mathbf{R},+,\square),(\mathbf{C},+,\square)$ are commutative rings.

Ring with Unity: A ring $(R,+,\square)$ is said to be ring with unity if $\exists\ \ 0\neq b\in R$ such that $a\cdot b=b\cdot a=a,\ \forall a\in R$

$1\in Z$ s.t $1\cdot a=a\cdot 1=a,\ \forall a\in Z$ and $(Z,+,\square)$ is commutative ring then $(Z,+,\square)$ is commutative ring with unity. Similarly, $(Q,+,\square)$, $(\mathbf{R},+,\square)$, $(\mathbf{C},+,\square)$ are commutative ring with unity 1.

Gaussian Integer: $Z[i]=\{a+ib|a,b\in Z\}$. $(Z[i],+,\cdot)$ is commutative ring with unity.

$Z_n[i]=\{a+ib|a,b\in Z_n\}$

$Z_1[i]=\{a+ib|a,b\in Z_1\}=\{0\},\ Z_2[i]=\{a+ib|a,b\in Z_2\}=\{0,1,i,1+i\};Z_2=\{0,1\}$

$Z_3[i]=\{a+ib|a,b\in Z_3\}=\{0,1,2,i,2i,1+i,1+2i,2+i,2+2i\}$

Exam Point: $O(Z_n[i])=n^2$

$R=\{0\}$ is commutative ring with unity? $R=\{0\}$, $(\mathbf{R},+,\square)$ is commutative ring but not unity.

If $n=1$ then $(Z_n,+,\cdot)$ is commutative ring but not unity.

If $n\geq 1$ then $(Z_n,+,\cdot)$ is commutative ring with unity say unity = 1

$M_n(\mathbf{R}),n\geq 1$ is Ring with unity but not commutative.

If $n=1$ then $M_n(\mathbf{R})=\mathbf{R},(\mathbf{R},+,\cdot)$ is commutative then $M_n(\mathbf{R})$ is commutative ring with unity.

$R=Z_m\times Z_n$ is ring, $R=Z\times Z$ is ring, $R=Z\times Q$ is ring, $R=Q\times Q$ is ring

$R=\mathbf{R}\times\mathbf{R}$ is ring, $R=\mathbf{C}\times\mathbf{C}$ is ring, $R=Z[i]\times Z[i]$ is ring

$R=Q\times\{0\}$ is commutative ring with unity? Yes, $R=Q\times\{0\}$

$(1,0)\in Q\times\{0\}$; $(1,0).(a,0)=(a,0)$ s.t $(1,0)(a,0)=(a,0)$

Mindset Makers

$R = Q \times \{0\}$ is commutative ring with unity $(1,0)$. similarly, (i) $Z[i] \times \{0\} \to$ unity $(1,0)$ $\square \{0\} \times \mathbf{R} \times \mathbf{C}$ are commutative ring with unity $(0,1,1)$.

Polynomial Ring: Definition: Let $(R,+,\cdot)$ be a commutative ring. The set $R[x] = \{a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \mid a_i \in R\}$. is called Polynomial ring with indeterminant *x*.

Degree of Polynomial: $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n \ x^n$ of degree *n* if $a_n \neq 0$. The degree of $f(x)$ is denoted by $\deg(f(x))$.

Note: (1) R is commutative ring then $R[x]$ is also commutative ring.

(2) If R is commutative ring with Unity then $R[x]$ is commutative ring with unity.

ZERO DIVISOR Definition: Let $(R,+,\cdot)$ is commutative ring A non-zero element, $0 \neq a \in R$ is said to be zero divisor if $\exists 0 \neq b \in$ such that $a \cdot b = 0$

Note: If R is not commutative then

$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbf{R})$, $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbf{R})$; $AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \to$ represent A is zero divisor But $BA = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $\therefore$ A is not zero divisor.

INTEGRAL DOMAIN: A commutative ring with unity $(R,+,\cdot)$ is called Integral domain if $0 \neq a \in R,\ 0 \neq b \in R \Rightarrow ab \neq 0$ i.e. $a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

$(Z,+,\cdot)$ is an Integral Domain.

Z_n is an integral domain iff $n = p$ where *p* is prime.

$Z_p[i]$ is an integral domain if 4 divides *p-3*, Where *p* is prime.

$Z \times \mathbf{R}$ is not integral domain. $(0,0) \neq (1,0) \in Z \times \mathbf{R}$, $(0,0) \neq (0,1) \in Z \times \mathbf{R}$. $(1,0)(0,1) = (0,0)$ then $Z \times \mathbf{R}$ is not integral domain.

Q. $Z \times Q \times \mathbf{R}$ is an integral domain? No, $(0,0,0) \neq (1,0,0) \in Z \times Q \times \mathbf{R}$, $(0,0,0) \neq (0,0,1) \in Z \times Q \times \mathbf{R}$ But $(1,0,0)(0,0,1) = (0,0,0)$. then $Z \times Q \times \mathbf{R}$ is not integral domain.

Q. $\mathbf{C} \times \mathbf{C}$ is an integral domain? No $(0,0) \neq (1,0) \in \mathbf{C} \times \mathbf{C}$, $(0,0) \neq (0,1) \in \mathbf{C} \times \mathbf{C}$, $(1,0)(0,1) = (0,0)$ then $R = \mathbf{C} \times \mathbf{C}$ is not an integral domain.

Q. $R = \mathbf{C} \times \{0\}$ is an integral domain? Yes, it is an integral domain.

Note: (Any Integral Domain) $\times$ $\{0\}$ is an integral domain.

Q. Show that $Z_5[i] \times \{0\}$ is not an integral domain.; $Z_5[i] \times \{0\} = \{(a \cdot 0) \mid (a,0) \in Z_5[i] \times \{0\}\}$ $(0,0) \neq (2+i,0) \in Z_5[i] \times \{0\}$; $(0,0) \neq (2+4i,0) \in Z_5[i] \times \{0\}$ but $(2+i,0)(2+4i,0) = ((2+i)(2+4i), 0 \cdot 0) = (0,0)$. then $Z_5[i] \times \{0\}$ is not an integral domain.

Q. $R = \{0\} \times \{0\}$ is an integral domain: R is not commutative ring with unity then R is not an integral domain.

Mindset Makers

List of integral domains:

(i) Z (ii) Q (iii) **R** (iv) **C** (v) Z_p (vi) $Z_p[i]$ if $4 \mid p-3$, where p is prime. (vii) $Z[i]$

Note: $Q[i]=\{a+ib \mid a,b \in Q\}$, $\mathbf{R}[i]=\{a+ib \mid a,b \in \mathbf{R}\}$ are also integral domain.

Units: An element $a \in R$ is said to be Unit element of R if 'a' has multiplicative inverse in R. The set of all units of R is denoted by $U(R)$.

Example: (i) $R=Z$, then find $U(Z)$? $Z=\{0,\pm1,\pm2,\pm3,....\}$. $U(Z)=\{1,-1\}$

(ii) $R=Q$ then find $U(Q)$?. $U(Q)=Q-\{0\}=Q^*$, (iii) $R=\mathbf{R}$, find $U(\mathbf{R})$?. $U(\mathbf{R})=\mathbf{R}-\{0\}=R*$

(iv) $R=Z[i]$, find $U(Z[i])$? . $U(Z[i])=\{\pm1,\pm i\}$, (v) $U(\mathbf{C})=\mathbf{C}-\{0\}=\mathbf{C}*$

(vi) $U(\mathbf{R}[i])=\mathbf{C}*$, (vii) $U(Q[i])=Q[i]-\{0\}=Q[i]*$

(viii) $U(Q\times\{0\})=Q\times\{0\}-\{(0,0)\}=(Q\times\{0\})*$

$U(\mathbf{R}\times\{0\})=\mathbf{R}\times\{0\}-\{(0,0)\}=(\mathbf{R}\times\{0\})*$, $U(\mathbf{C}\times\{0\})=\mathbf{C}\times\{0\}-(0,0)=(\mathbf{C}\times\{0\})*$

Q. Find $U(Q\times Q)$? Solution: $U(Q\times Q)=Q*\times Q*=U(Q)\times U(Q)$

Field: An integral domain $(\mathbf{F},+,\cdot)$ is field if each non-zero element of **F** has multiplicative inverse.

$(Q,+,\cdot)$ is a field. Similarly, $(\mathbf{R},+,\cdot),(\mathbf{C},+,\cdot)$ are also fields. $Z_5=\{0,1,2,3,4\}$ is field. Exam point: Z_n is field if and only if $n=p$. **Exam Point**: If **F** is finite integral domain then **F** is field.

Note: $Z_p[i]$ is field if $4 \mid p-3$.

$Q[\sqrt{d}]=\{a+b\sqrt{d} \mid a,b \in Q\}, d>0$ and d is not perfect square then $Q[\sqrt{d}]$ is field.

$\mathbf{R}[\sqrt{d}]=\mathbf{R}, d>0$ and d is not perfect square then it is field.

$Z[\sqrt{d}]=\{a+b\sqrt{d} \mid a,b \in Z\}$ is integral domain but not field because $3 \in [\sqrt{d}]$ but $3^{-1}=\frac{1}{3} \notin Z[\sqrt{d}]$ then $Z[\sqrt{d}]$ is not field. Interesting question is $Z[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b \in Z\}$, how many unit in $Z[\sqrt{2}]$? $(\sqrt{2}-1)(\sqrt{2}+1)=1$ then $\sqrt{2}-1$ is unit similarly $\sqrt{2}+1$ is unit. $(3-2\sqrt{2})(3+2\sqrt{2})=1 \Rightarrow 3-2\sqrt{2}$ and $3+2\sqrt{2}$ is also unit. $\therefore Z[\sqrt{2}]$ has infinite units.

Idempotent Element: Let $(R,+,\cdot)$ be a ring then an element $a \in R$ is said to be idempotent element of R if $a^2=a$. Special point to notice here that square doesn't mean multiplication, it means composition two times. So we must take care of it. Example: there are only 2 idempotent elements in real numbers ring R i.e. 0 and 1. Note: Matrix concept is used if A is idempotent then I-A is also idempotent where A be any square matrix or order n.

Exam Point: No. of Idempotent elements in $Z_n=2^d$ where d is the number of Prime divisors of n.

Mindset Makers

If a is idempotent element in R then $1-a$ is also Idempotent. If R is Integral domain then R has exactly two idempotent elements. Q. How many Idempotent elements in $Z, Q, \mathbf{R}, \mathbf{C}, Z_p\left(Z_p[i] \text{where} 4 \mid p-3\right)$, $Q\times\{0\}, \mathbf{R}\times\{0\}, \mathbf{C}\times\{0\}$. Solution: All of these has exactly two idempotent elements.

BOOLEAN RING: A ring $(R,+,\cdot)$ is said to be Boolean ring if $x^2 = x,\ \forall x \in R$

Q. $R = Z_2$ is Boolean Ring? Solution: $Z_2 = \{0,1\}$, here $0 \in Z_2$ s.t $0^2 = 0$, $1 \in Z_2$ s.t $1^2 = 1$

Q. Give example of Boolean ring of order 4 and ∞.

Ans. Boolean Ring of order 4: $R = Z_2 \times Z_2 = \{(0,0),(0,1),(1,0),(1,1)\}$. Boolean Ring of order ∞; $R = Z_2 \times Z_2 \times Z_2 \times Z_2 \times .....\infty$ is Boolean Ring of order ∞

NILPOTENT ELEMENTS: An element $a \in R$ is Nilpotent element of R if $a^n = 0$ for some *n*.

Q. How many Nilpotent elements in Z? $Z = \{0, \pm 1, \pm 2, ...\}, 0 \in Z$ such that $0^1 = 0.0 \neq a \in Z$ then a is not nilpotent element of Z then Z has exactly one element. Similarly $Q, \mathbf{R}, \mathbf{C}, Z_p$ has exactly one Nilpotent element.

Note: If $n = p_1^{r_1} \times p_2^{r_2} .....\times p_k^{r_k}$, then number of Nilpotent elements in $Z_n = p_1^{r_1-1} \times p_2^{r_2-1} ....\times p_k^{r_k-1}$, *p* is prime.

Subring: Let $\phi \neq S \subseteq R, (S,+,\cdot)$ is subring of $(R,+,\cdot)$ if

(i) $\forall a \in S, \forall b \in S \Rightarrow a-b \in S$ [condition of subgroup S is subgroup (ii) $\forall a \in S, \forall b \in S \Rightarrow a \cdot b \in S$

$(Z,+,\cdot)$ is subring of $(Q,+,\cdot)$. $\phi \neq Z \subseteq Q$ and $(Z,+,\cdot)$ is ring then $(Z,+,\cdot)$ is subring of $(Q,+,\cdot)$.

Similarly, Z is subring of $\mathbf{R}, \mathbf{C}$, Q- is subgroup of $\mathbf{R}, \mathbf{C}$, $\mathbf{R}$ is subring of $\mathbf{C}$. $S = \{0\}$ and $S = R$ always subring of R.

mZ is subring of Z.

Exam Point: Number of subrings in $Z_n = \tau(n)$

$S = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \middle| b \in \mathbf{R} \right\}$ is subring or $M_2(\mathbf{R})$. Interesting to notice identity of subring and it's ring here. Are they different!

Sum of two subrings: Let A and B are two subrings of R then the sum of A and B is defined by

$A + B = \{a + b \mid a \in A, b \in B\}$

(i) Intersection of two subrings of R is a subring of R? (ii) Union of two subring of R is a subring of R?

(iii) Sum of two subrings of R is a subring of R? need not be.

Ideal: Let $\phi \neq I \subset R, (I,+,\cdot)$ is an Ideal of R if

(1) $\forall a \in I, \forall b \in I \Rightarrow a-b \in I$, (2) $\forall a \in I, \forall r \in R \Rightarrow ra \in I$ and $ar \in I$

Z is an ideal of Q? Solution: No. $2 \in Z, \frac{1}{3} \in Q$ but $\frac{2}{3} \notin Z$ then Z is not ideal of

Q. Q is an ideal in $\mathbf{R}$? Solution: No, $2 \in Q$, $\sqrt{2} \in \mathbf{R}$ but $2\sqrt{2} \notin Q$

Q. $\mathbf{R}$ is an ideal in $\mathbf{C}$? Solution: $2 \in \mathbf{R}, i \in \mathbf{C}$, then $\mathbf{R}$ is not an ideal of $\mathbf{C}$

Q. Show that $I = \{0\}$ and $I = R$ are always Ideal of R.

Exam point- Similarly, mZ is an ideal of Z.

Note. every ideal of R is subring of R but converse need not be true.

Exam Point: No. of Ideal in $Z_n = \tau(n)$

Q. (i) How many ideals in $Z_4 \times Z_5$? (ii)How many ideals in $Q \times \mathbf{R}$?(iii) How many ideals in $\mathbf{R} \times Q \times Z_7$?

Solution: (ii) $R = Q \times \mathbf{R}$ ....(1)

Since Q is field then Q has exactly 2 ideals say $I_1 = \{0\}$ and $I_2 = Q$ .Since $\mathbf{R}$ is field then $\mathbf{R}$ has exactly 2 ideals say $I_3 = \{0\}$ and $I_4 = \mathbf{R}$

$R = Q \times \mathbf{R}$

$\{0\}, Q \quad \{0\}, \mathbf{R}$

Possible Ideal of $Q \times \mathbf{R}$ (i) $\{0\} \times \{0\}$ (ii) $\{0\} \times \mathbf{R}$ (iii) $Q \times \{0\}$ (iv) $Q \times \mathbf{R}$. Number of ideals in $Q \times \mathbf{R} = 4$

Q. How many ideals in $Q \times Q \times Q$?

Solution: Q is field then Q has exactly 2 ideals say. $I = \{0\}$ and $I = Q$

Ideals of $\mathrm{R} = Q \times Q \times Q$

$\{0\} \quad Q \quad \{0\}, Q \quad \{0\}, Q$

$I_1 = \{0\} \times \{0\} \times \{0\}$, $I_2 = \{0\} \times \{0\} \times Q$, $I_3 = \{0\} \times Q \times \{0\}$, $I_4 = Q \times \{0\} \times \{0\}$

$I_5 = \{0\} \times Q \times Q$, $I_6 = Q \times \{0\} \times Q$, $I_7 = Q \times Q \times \{0\}$, $I_8 = Q \times Q \times Q$; exactly 8 ideals.

Exam Point. $I = \langle 2, x \rangle$ is ideal of $Z[x]$. Solution: Let $Z[x] = \{a_0 + a_1 x + ... + a_n x^n \mid a_i \in Z\}$

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

Maximal Ideal: Let R be a commutative ring An ideal $A \neq R$ is said to be maximal ideal of R if $\exists$ an ideal, $B \in R$ such that $A \subseteq B \subseteq R$ then either $A = B$ or $B = R$

Exam point: Number of maximal ideal in Z_n = number of prime divisor of *n*.

Q. How many maximal ideal in Q? Solution: $R = Q$ is field then Q has exactly two ideals. $I_2 = Q$ is not maximal by definition then $I_1 = \{0\}$ is only maximal ideal. Note: If $\mathbf{F}$ is field then $\mathbf{F}$ has exactly one maximal ideal.

Prime Ideal: Let R be a commutative ring an ideal $P \neq R$ is called Prime ideal if $a \cdot b \in P$ where $a \in R, b \in R \Rightarrow$ either $a \in P$ or $b \in P$. Example $R = Z_{15}$, $I = \{0\}$ is an ideal of Z_{15}

$I = \{0\}$ is Prime Ideal in Z_{15} ?Solution: $R = Z_{15}$, $I = \{0\}$. $3 \in R, 5 \in R$; $3.5 = 0 \in I = \{0\}$ but $3 \notin I$ and $5 \notin I$ then

Mindset Makers

$I=\{0\}$ is not Prime Ideal in Z_{15}. **Exam Point:** Number of Prime Ideals in Z_n = No. of Prime Divisor of *n*.

Q. How many Prime ideal in Q? Solution: $R=Q$ and Q is field then Q has exactly 2 ideals say $I_1=\{0\}$ and $I_2=Q$ But $I_2=Q$ is not Prime ideal by definition $\therefore I_1=\{0\}$ is Prime ideal of Q because $a\in Q, b\in Q$ and $a\cdot b\in I=\{0\}\Rightarrow$ either $a=0$ or $b=0$ because Q is an integral domain. Then, Q has exactly one Prime ideal. Note: If **F** is field then **F** has exactly one Prime ideal say $I=\{0\}$.

Q. How many Prime ideal in Z? Solution: It has infinite number of Prime ideals say $I=\{0\}$ and $I=pz$, where *p* is prime. e.g. $2Z,3Z,5Z,7Z,11Z,....$ are Prime ideal in Z. Q. Show that $6Z$ is not Prime ideal in Z. Solution: $6Z=\{0,\pm6,\pm12,.....\}: 2\in Z,\ 3\in Z,\ 2\cdot3=6\in 6Z$ but $2\notin 6Z$ and $3\notin 6Z$ then $6Z$ is not Prime ideal.

Q. (i) Union of two maximal ideal of R is maximal ideal of R? (ii) Intersection of two maximal ideal of R is maximal ideal of R? Solution: (i) Need not e.g. $2Z$ is maximal ideal of Z and $3Z$ is maximal ideal of Z. $2Z\bigcup 3Z$ is not ideal of Z.
$2\in 2Z\bigcup 3Z,\ 3\in 2Z\bigcup 3Z; 2+3=5\notin 2Z\bigcup 3Z$ then $2Z\bigcup 3Z$ is not ring. (ii) Need not, e.g. $2Z$ is maximal ideal in Z. $2Z\bigcap 3Z=6Z$ and $6Z$ is not maximal ideal in Z.

Q. Intersection of two Prime ideal in Prime ideal? Solution: Need not: $2Z$ is Prime ideal of Z $3Z$ is Prime ideal of Z. $2Z\bigcap 3Z=6Z$, but $6Z$ is not Prime ideal of Z.

Exam Point: $mZ\bigcap nZ=kZ$, where $k=\text{L.C.M.}(m,n)$.

Exam Point: (i) If R is commutative ring with unity then every maximal ideal is Prime ideal. (ii) If R is finite commutative ring with unity then every prime ideal is maximal ideal.

Principal Ideal: Ideal generated by single element is called Principal Ideal. Example: $I=\langle 3\rangle$ in Z, I is Principal Ideal.

Factor Ring: Let R be a ring and A is an ideal of R. Then $\frac{R}{A}=\{a+A\mid a\in R\}$ is factor ring with operations (i) $(a_1+A)+(a_2+A)=a_1+a_2+A$ (ii) $(a_1+A)(a_2+A)=a_1a_2+A$

Example: $R=Z, I=3Z$; $\frac{R}{I}=\frac{Z}{3Z}=\{a+3z\mid a\in Z\}$; $\frac{Z}{3Z}=\{0+3z,1+3z,2+3z\}$.

Exam Point: If **F** is field then **F** has exactly two factor rings (i) $\frac{\mathbf{F}}{\{0\}}\approx\mathbf{F}$ (ii) $\frac{\mathbf{F}}{\mathbf{F}}\approx\{0\}$

Q. Construct $\frac{Q}{Z}=?$ Solution: Does not exist because Z is not ideal of Q.

Q. Construct factor ring of $Z_{23}[i]$? Solution: Since $Z_{23}[i]$ is field then $Z_{23}[i]$ has exactly two ideals say $I_1=\{0\}$ and $I_2=Z_{23}[i]$.Then, factor ring,(i) $\frac{Z_{23}[i]}{I_1}=\frac{Z_{23}[i]}{\{0\}}\approx Z_{23}[i]$ (ii) $\frac{Z_{23}[i]}{I_2}=\frac{Z_{23}[i]}{Z_{23}[i]}\approx\{0\}$

Q. $I=\langle(1-i)\rangle$ is an ideal of $Z[i]$, construct $\frac{Z[i]}{\langle 1-i\rangle}\approx ?$

Solution: $\frac{Z[i]}{\langle(1-i)\rangle}=\{a+ib+\langle 1-i\rangle \mid a+ib\in Z[i]\}$

$=\{a+ib+\langle 1-i\rangle \mid a,b\in Z\}$ ....(1)

$1-i+\langle 1-i\rangle=0+\langle 1-i\rangle \Rightarrow 1-i=0\Rightarrow i=1$ ....(2)

$\Rightarrow i^2=1^2\Rightarrow -1=1\Rightarrow 2=0$ ....(3)

$\frac{Z[i]}{\langle 1-i\rangle}=\{a+ib+\langle 1-i\rangle \mid a,b\in Z\}\Rightarrow \frac{Z[i]}{\langle 1-i\rangle}=\{0+\langle 1-i\rangle,1+\langle 1-i\rangle\}$; $\boxed{\frac{Z[i]}{\langle 1-i\rangle}\approx Z_2}$

Q. $\frac{Z[i]}{\langle 3-i\rangle}=\{a+ib+\langle 3-i\rangle \mid a+ib\in Z[i]\}=\{a+ib+\langle 3-i\rangle \mid a,b\in Z\}$

Solution: $3-i+\langle 3-i\rangle=0+\langle 3-i\rangle \Rightarrow 3-i=0\Rightarrow 3=i\Rightarrow 3^2=i^2$

$\Rightarrow 9=-1$ ....(1)

$\Rightarrow 10=0$ ....(2)

Given into about modulo we are using

$\frac{Z[i]}{\langle 3-i\rangle}=\{0+\langle 3-i\rangle,1+\langle 3-i\rangle,2+\langle 3-i\rangle,3+\langle 3-i\rangle,4+\langle 3-i\rangle,5+\langle 3-i\rangle,6+\langle 3-i\rangle,7+\langle 3-i\rangle,8\langle 3-i\rangle,9+\langle 3-i\rangle\}$

$\frac{Z[i]}{\langle 3-i\rangle}\approx Z_{10}$, $0+i+\langle 3-i\rangle=0+3+\langle 3-i\rangle$

$1+i+\langle 3-i\rangle=1+3+\langle 3-i\rangle=4+\langle 3-i\rangle$

Exam Point: $\frac{Z[i]}{\langle a+ib\rangle}\approx Z_{a^2+b^2}$, if $\gcd(a,b)=1$.

Exam Point: $\frac{Z[i]}{\langle a+ib\rangle}\approx$ not integral domain if $\gcd(a,b)\neq 1$ and $a\neq 0$, $b\neq 0$

Exam Point: $\frac{Z[i]}{\langle n\rangle}\approx Z_n[i]$

Theorem 1: Let R be a commutative ring with unity and A is an ideal of R. $\frac{R}{A}$ is an integral domain iff A is Prime Ideal.

Theorem 2: Let R be a commutative ring with unity and A is an ideal of R. $\frac{R}{A}$ is field iff A is maximal ideal.

Q. Show that if R is commutative ring with unity then every maximal ideal of R is prime ideal.

Solution: Let R is commutative ring with unity and A is maximal ideal of R. Then $\frac{R}{A}$ is field

$\Rightarrow \frac{R}{A}$ is integral domain $\Rightarrow A$ is Prime ideal.

Q. Show that if R is finite commutative ring with unity then every Prime ideal of R is maximal ideal. Solution: Let R is finite commutative ring with unity and A is prime ideal of R.

Mindset Makers

If A is prime ideal of R then $\frac{R}{A}$ is an integral domain and $\frac{R}{A}$ is finite because R is finite. $\Rightarrow \frac{R}{A}$ is finite integral domain $\Rightarrow \frac{R}{A}$ is field $\Rightarrow A$ is maximal ideal.

Q. $I=\langle p\rangle = pZ$ is maximal ideal is Z. Solution: $\frac{Z}{\langle p\rangle}=\frac{Z}{pz}\approx Z_p \rightarrow$ is field then $\frac{Z}{\langle p\rangle}$ is field $\Rightarrow \langle p\rangle$ is maximal ideal = pz is maximal ideal in Z.

Characteristic of Ring: Characteristic of Ring $(R,+,\cdot)$ is the least positive integer n such that $n\cdot a=0\ \forall a\in R$. It is denoted by $\text{char}(R)$. If such n does not exist then $\text{char}(R)=0$. Example: $Z_4=\{0,1,2,3\}$. Find $\text{char}(Z_4)$ = $n=4$ such that ; $4\cdot 0=0, 4\cdot 1=0, 4\cdot 2=0, 4\cdot 3=0$.

Exam Point: $\text{char}(Z_n)=n$

Q. $R=Z$ find $\text{char}(Z)$ = ? Solution: char (Z) = 0 because n does not exist such that $n\cdot a=0,\ \forall a\in Z$ since Z is an integral domain. Similarly, Note: Char $(\mathbf{R})$ = Char $(\mathbf{C})$ = Char $(Q)=0$

Q. Char $\frac{Z[i]}{\langle 2+3i\rangle}$ = ? Solution: $\frac{Z[i]}{\langle 2+3i\rangle}\approx Z_{13}$. $\text{char}(Z_{13})=13$ and as $\frac{Z[i]}{\langle 2+3i\rangle}\approx Z_{13}$ therefore $\text{char}\left(\frac{Z[i]}{\langle 2+3i\rangle}\right)=13$

Q. Char $(Z_3[i])$ = ?Solution: $Z_3[i]=\{0,1,2,i,2i,1+i,1+2i,2+i,2+2i\}$ $n=3$ s.t $3\cdot a=0,\ \forall a\in Z_3[i]$.$\text{char}(Z_3[i])=3$

Note: $\text{Char}(R\times S)=\begin{cases}0, \text{if } \text{char}(R)=0 \text{ or } \text{char}(S)=0\\ K; K=\text{LCM}(\text{char}(R),\text{Char}(S))\end{cases}$

Q. How many maximal ideal, prime ideal, ideal, idempotent nilpotent and unit in $Q[\sqrt{2}]$?

Solution: 2 ideals, 2 Idempotent elements, 1 Nilpotent elements, ∞ units 1 maximal ideal, 1 Prime Ideal.

Note: Similarly $Q[\sqrt{d}]=\{a+b\sqrt{d}\mid a,b\in Q\}, d>0$ and d is not perfect square then $Q[\sqrt{d}]$ is field.

Q. $I=Z\times Z\times\{0\}$ is maximal/Prime ideal in $Z\times Z\times Z$. Ans. Yes, $\frac{Z\times Z\times Z}{Z\times Z\times\{0\}}\approx Z$ is an integral domain $\therefore$ It $Z\times Z\times\{0\}$ is Prime Ideal.

Ring Homomorphism: Let $(R,+,\square)$ and $(S,+,\square)$ are two rings. A mapping $f:(R,+,\square)\rightarrow(S,+,\square)$ is said to be ring homomorphism if (1) $f(x+y)=f(x)+f(y)$ (2) $f(x\cdot y)=f(x)\cdot f(y)$

Q. $f:Z\to Z,\ f(x)=0\cdot x$ is Ring homomorphism? Solution: $f(x)=0\cdot x$. then $f(x)=0\cdot x$ is ring homomorphism. **Definition**: $f:R\to R,\ f(x)=0\cdot x$ is called trivial ring homomorphism.

(1) $f(x+y)=0(x+y)=0\cdot x+0\cdot y=f(x)+f(y)$

(2) $f(x\cdot y)=0(x\cdot y)=(0\cdot x)\cdot(0\cdot y)=f(x)\cdot f(y)$.

Q. $f:Z\to Z,\ f(x)=2x$, is ring homomorphism? Solution: $f(x)=2x$

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

(2) $f(x\cdot y)=2(x\cdot y)\neq 2x\cdot 2y\neq f(x)\cdot f(y)\therefore f(x)=2x$ is not ring homomorphism.

Exam Point: $f:Z\to Z$ has exactly 2 ring homomorphism say $f(x)=0\cdot x$ and $f(x)=1\cdot x$.

Exam Point: $f:Z_m\to Z_m$;Number of Ring Homomorphisms = No. of Idempotent Elements in Z_m

Q. How many ring homomorphism in $f:Z_p\to Z_p$? Solution: Z_p is field then Z_p has exactly two idempotent elements say 0 and 1. $\left.\begin{matrix}f(x)=0\cdot x\\ f(x)=1\cdot x\end{matrix}\right\}$ exactly 2 ring homomorphisms.

Note: (1) $f:Z_p\to Z_p$, then it has exactly 2 ring homomorphism. (2) $f:Z_p\to Z_{p^m}, m>1$ then it has exactly 1 ring homomorphism.

Q. **C** is ring isomorphic to **R** $(\mathbf{C}\approx\mathbf{R}?)$. Solution: **C** is not ring isomorphic to **R** because $x^4=1$ has 4 solutions in **C** say $(x=1,-1,i,-i)$ but $x^4=1$ has only 2 solutions in **R** say $(x=1,-1)$.

Q. $Q[i]\approx Q$? i.e. $Q[i]$ is ring isomorphic to Q? Ans. No, reason is same as above.

Irreducible Element: Definition: Let $(R,+,\square)$ is an integral domain. A non-zero non-unit element $a\in R$ is said to be irreducible element if $a=bc, b\in R, c\in R$ then either b is unit or c is unit in R.

Example: $a=6\in Z$ is irreducible element of Z? Solution: $6=2\cdot 3$ and $2\in Z, 3\in Z$ but neither 2 nor 3 is unit in Z then 6 is not irreducible element of Z.

Q. 2 is irreducible over $Z[i]$? Solution: No, $2=(1+i)(1-i)=b\square c,\ b\in Z[i], c\in z[i]$ but neither $b=(1+i)$ nor $c=(1-i)$ is unit in $Z[i]$ therefore 2 is not irreducible over $Z[i]$.

Q. $a=2\in Z$ is irreducible over Z? Solution: Yes, because. $2=2\times 1=b\cdot c,\ b\in Z, c\in Z$ .1 is unit in Z then 2 is irreducible element over Z.

Q. 3 is irreducible over $Z[i]$?Solution: 3 is irreducible element in $Z[i]$

Q. Show that $1+i$ is irreducible over $Z[i]$

Solution: Let $1+i=(1+ib)(c+id)$ ....(1)

taking conjugate of equation (1)

$1-i=(a-ib)(c-id)$ ....(2)

Multiplying side by side of equation (1) and (2),

Mindset Makers

$(1+i)(1-i)=(a^2+b^2)(c^2+d^2) \Rightarrow 2-(a^2+b^2)(c^2+d^2)$ ....(3)

Case I: If $a^2+b^2=2$ then $c^2+d^2=1 \Rightarrow (c+id)(c-id)=1 \Rightarrow c+id$ is unit in $Z[i]$

Case II: If $c^2+d^2=2$ then $a^2+b^2=1 \Rightarrow (a+ib)(a-ib)=1 \Rightarrow a+ib$ is unit in $Z[i]$

From case I and II, we conclude either $c+id$ is unit or $a+ib$ is unit of $Z[i]$ then $1+i$ is irreducible over $Z[i]$.

Prime Element: Let $(R,+,\square)$ is an integral domain A non-zero, non-unit element $a \in R$ is said to be Prime element if $a \mid bc, b \in R, c \in R \Rightarrow$ either $a \mid b$ or $a \mid c$. Example: $a=7$ in Z, $a=7$ is Prime element in Z. Solution: Yes $7=7\square 1$, then; $7 \mid 7 \Rightarrow 7 \mid 7$, 7 is Prime.

Q. $a=6$ in Z, $a=6$ is Prime in Z? Solution: $6 \mid 6=2\square 3$ i.e. $6 \mid = 2\square 3$ but 6×2 and 6×3 then 6 is not Prime.

Associate: Let $(R,+,\cdot)$ be an integral domain An element $a \in R$ is said to be associate to $b \in R$ if $\exists$ unit $U \in R$ s.t $a=Ub$. Example. -1 is associate to 1 in Z? Solution: Yes $a=Ub$. $-1=(-1)1$. -1 is unit in Z.

Q. *i* and -*i* are associate in $Z[i]$? Solution: $i=(-1)(-i)$ and -1 is unit in $Z[i]$

Q. $2+3i$ and $2i-3$ are associate in $Z[i]$? Solution: Yes $2i-3=i(2+3i)$. $a=U\square b$. $i \in Z[i]$ s.t *i* is unit in $Z[i]$.

Irreducible Polynomial: Let $(R,+,\square)$ be an integral domain. A non-zero, non-unit polynomial $f(x) \in R[x]$ is said to be Irreducible Polynomial if $f(x)=g(x).h(x)$ where $g(x) \in R[x]$ and $h(x) \in R[x]$ thin either $g(x)$ is unit or $h(x)$ is unit in $R[x]$.

Example: $f(x)=2x^2+6$ is irreducible over Q?

Solution: $f(x)=2x^2+6=2(x^2+3)=g(x).h(x)$, where $g(x)=2$ and $h(x)=x^2+3$. $g(x) \in Q[x]$ and $h(x)=x^2+3 \in Q[x]$. $g(x)=2$ is unit in $Q[x]$ then $f(x)=2x^2+6$ is irreducible over Q.

Einestein's Irreducible Criteria

Let $f(x)=a_0+a_1x+....+a_nx^n \in Z[x]$. If there exist prime p such that $p \mid a_0, p \mid a_1 .... p \mid a_{n-1}$ but p does not divide a_n and $p^2 notdivide a_0$ then $f(x)$ is irreducible over Q.

Q. $f(x)=3+6x+12x^2+x^3 \in Z[x]$ is irreducible over Q? Solution: $f(x)=3+6x+12x^2+x^3$. $p=3$, such that $3 \mid 3, 3 \mid 6, 3 \mid 12$ but $3 \nmid 1$ and $3^2 \nmid 3$ then $f(x)$ is irreducible over Q.

Note: Let **F** is field and $0 \neq a \in \mathbf{F}$

(i) If $f(ax)$ is irreducible **F** then $f(x)$ is irreducible over **F**.

(ii) If $a.f(x)$ is irreducible over **F** then $f(x)$ is irreducible **F**.

(iii) If $f(x+a)$ is irreducible over **F** then $f(x)$ is irreducible over **F**.

Galois Field

Mindset Makers

Definition: If **F** is **finite** field of **order p** and $f(x)\in \mathbf{F}[x]$ is **irreducible** polynomial over **F** of degree *n*. Then $\frac{\mathbf{F}[x]}{\langle f(x)\rangle}$ is field of order p^n. It is denoted by $G\mathbf{F}(p^n)$ where p is prime.

$$G\mathbf{F}(p^n)=\frac{\mathbf{F}[x]}{\langle f(x)\rangle}=\{a_0+a_1x+a_2x^2+....+a_{n-1}x^{n-1}+<f(x)>|\, a_i\in \mathbf{F}\}$$

i.e. $$G\mathbf{F}(p^n)=\frac{Z_p[x]}{\langle f(x)\rangle}=\{a_0+a_1x+a_2x^2+....+a_{n-1}x^{n-1}+\langle f(x)\rangle|\, a_i\in z_p\}$$

where **F** is field of order p and $f(x)$ is irreducible polynomial over **F** of degree '*n*'.

Q. Construct Galois Field of order 2?

Solution: $G\mathbf{F}(2^1)=\frac{Z_2[x]}{\langle x\rangle}=\{a_0+\langle x\rangle|\, a_0\in Z_2=\{0+\langle x\rangle,1+\langle x\rangle\}\approx Z_2$

Q. Construct Galois Field of order 3.

Q. Construct Galois field of order 4.

Solution: $G\mathbf{F}(4)=G\mathbf{F}(2^2)=\frac{Z_2[x]}{\langle f(x)\rangle}=\{a_0+a_1x+\langle f(x)\rangle|\, a_i\in Z_2$ where $f(x)$ is irreducible polynomial of degree 2 over Z_2.

$$G\mathbf{F}(2^2)=\frac{Z_2[x]}{\langle 1+x+x^2\rangle}=\{a_0+a_1x+\langle 1+x+x^2\rangle|\, a_0,a_1\in Z_2\} \quad ....(1)$$

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

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

$$1+x+x^2+\langle 1+x+x^2\rangle=0+\langle 1+x+x^2\rangle\Rightarrow 1+x+x^2=0 \quad ....(2)$$

$1+\langle 1+x+x^2\rangle\in\frac{Z_2[x]}{\langle 1+x+x^2\rangle}$ such that $(1+\langle 1+x+x^2\rangle)^{-1}=1+\langle 1+x+x^2\rangle$

$x+\langle 1+x+x^2\rangle\in\frac{Z_2[x]}{\langle 1+x+x^2\rangle}$ s.t $(x+\langle 1+x+x^2\rangle)^{-1}=1+x+\langle 1+x+x^2\rangle$

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

$=-1+\langle 1+x+x^2\rangle=1+\langle 1+x+x^2\rangle$; under modulo 2

From equation (2) $1+x+x^2=0\Rightarrow x+x^2=-1$

Subfield: Let $(\mathbf{F},+,\cdot)$ is field are $\phi\neq S\subseteq\mathbf{F}$ $(S,+,\cdot)$ is called subfield of $(\mathbf{F},+,\cdot)$ if

(i) $\forall a\in S,\ \forall b\in S\Rightarrow a-b\in S$ (ii) $\forall a\in S,\ 0\neq b\in S\Rightarrow ab^{-1}\in S$

Example: $(Q,+,\cdot)$ is subfield of $(\mathbf{R},+,\cdot)$. Solution: $\phi\neq Q\subseteq\mathbf{R}$ and $(Q,+,\cdot)$ is field then $(Q,+,\cdot)$ is subfield of $(\mathbf{R},+,\cdot)$. Similarly,(i) $(\mathbf{R},+,\square)$ is subfield of $(\mathbf{D},+,\square)$, (ii) $(\mathbf{Q},+,\square)$ is subfield of $(Q\sqrt{2},+,\square)$

Mindset Makers

Note- Let $\mathbf{F}$ be a finite field of p^n then no. of subfield of $\mathbf{F} = \tau(n)$, no. of positive divisor of n.

Principal Ideal Domain: An integral domain $(R,+,\square)$ is said to be Principal Ideal domain if every ideal of R is Principal ideal.

Q. $R = Z$ is Principal Ideal Domain? Solution: Every ideal of Z is Principal ideal $(\langle m \rangle)$ then Z is Principal ideal domain.

Q. $R = Q$ is Principal ideal domain? Solution: Q is field then Q has exactly two ideal. say, $I_1 = \{0\} = \langle 0 \rangle, I_2 = Q = \langle 1 \rangle$ Principal Ideal then Q is P.I.D. Note: If $\mathbf{F}$ is field then $\mathbf{F}$ is P.I.D.

Q. $M_2(\mathbf{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a,b,c,d \in \mathbf{R} \right\}$ is P.I.D.? Solution: $M_2(\mathbf{R})$ is not integral domain hence it is not P.I.D.

Q. $R = G\mathbf{F}(3^{100})$ is P.I.D.? Solution: $R = G\mathbf{F}(3^{100})$ is field it is PID

Q. $R = Z[x]$ is P.I.D.? Solution: $I = \langle 2, x \rangle$ is not Principal ideal in $Z[x]$ then $Z[x]$ is not P.I.D.

Q. Which of the following is/are true.

(1) $R = \dfrac{Q[x]}{\langle x \rangle}$ is P.I.D? (2) $R = \dfrac{[x,y]}{\langle 2 \rangle \langle y \rangle}$ is P.I.D.? (3) $R = \dfrac{Z[x]}{\langle 4, x \rangle}$ is P.I.D.?(4) $R = \dfrac{Q \times \mathbf{R}}{\mathrm{Q} \times \{0\}}$ is P.I.D.

Solution:(1) $\dfrac{Q[x]}{\langle x \rangle} \approx Q$ is field then $\dfrac{Q[x]}{\langle x \rangle}$ is field then $\dfrac{Q[x]}{\langle x \rangle}$ is P.I.D.

(2) $\dfrac{Z_2[x,y]}{\langle 2, x, y \rangle} \approx Z_2$ then $\dfrac{Z_2[x,y]}{\langle 2, x, y \rangle}$ is P.I.D.

(3) $\dfrac{Z[x]}{\langle 4, x \rangle} \approx Z_4$, Z_4 is not integral domain then $\dfrac{Z[x]}{\langle 4, x \rangle}$ is not integral then $\dfrac{Z[x]}{\langle 4, x \rangle}$ is not P.I.D.

(4) $\dfrac{Q \times \mathbf{R}}{\mathrm{Q} \times \{0\}} \approx \mathbf{R}$, then $\dfrac{Q \times \mathbf{R}}{\mathrm{Q} \times \{0\}}$ is field then $\dfrac{Q \times \mathbf{R}}{\mathrm{Q} \times \{0\}}$ is P.I.D.

Euclidean Domain: Definition: An integral domain $(D,+,\bullet)$ is said to be Euclidean Domain if $\exists$ a function d from non-zero elements of D to non-negative integer such that

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

(2) If $a \in D, 0 \ne b \in D$ then $\exists$ q order in D s.t. (q is not necessarily prime)

$a = bq + r$ where $r = 0$ or $d(r) < d(b)$.

$(Z,+,\square)$ is Euclidean domain. $d(a) = |a|$, $\forall 0 \ne a \in Z$.

If $\mathbf{F}$ is field then $\mathbf{F}$ is Euclidean Domain. $d(a) = 1$, $\forall 0 \ne a \in \mathbf{F}$.

If $\mathbf{F}$ is field then $\mathbf{F}[x]$ is Euclidean Domain. $d(f(x))$ = degree $(f(x))$,

$\forall 0 \ne f(x) \in \mathbf{F}[x]$ $Z[i] = \{a + ib \mid a,b \in Z\}$ is Euclidean Domain. $0 \ne x = a + ib \in Z[i]$ such that $d(x) = a^2 + b^2$.

Mindset Makers

Unique Factorization Domain

Definition: An integral domain $(D,+,\cdot)$ is said to be Unique Factorization Domain if

(i) Every non-zero, non-unit element of D can be written as product of Irreducible element of D and

(ii) The factorization is Unique upto associate.

i.e. Let a is non-zero, non-unit element of D and $a=a_1a_2....a_r$ where $a_1a_2....a_r$ are irreducible element of D.

If $a=b_1b_2....b_3$, where $b_1b_2...b_s$

$a_1a_2....a_r=b_1b_2...b_3$ then $r=S$ and a_i is associate to b_j (only one b_j)

Example: $(Z,+,\bullet)$ is U.F.D. Solution: $a=10\in Z$; $-2\times-5=10=2\times5$; -2 is associate to 2 and -5 is associate to 5.. Then, the factor of 10 is Unique upto associate. $\forall a\in Z$, s.t. factorization 'a' is unique upto associate then Z is Unique Factorization Domain.

Q. $Z\left[\sqrt{-5}\right]$ is U.F.D.? Solution:

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

$$\Rightarrow Z\left[\sqrt{-5}\right]=\left\{a+i\sqrt{5}\mid a,b\in Z\right\} \quad ....(1)$$

$14\in Z\left[\sqrt{-5}\right]$; $\left(3+i\sqrt{5}\right)\left(3-i\sqrt{5}\right)=14=7\times2$. But $\left(3+i\sqrt{5}\right)$ is not associate to 7 or 2. and $\left(3-i\sqrt{5}\right)$ is not associate to 7 or 2. Then factorization of 14 is not Unique upto associate.

Then, $Z\left[\sqrt{-5}\right]$ is not Unique Factorization Domain.

Note: Relation Field $\Rightarrow$E.D. $\Rightarrow$ PID $\Rightarrow$ U.F.D $\Rightarrow$Integral Domain .

Extension Field

Let H is subfield of K. The field is called extension field of **F**.

Q. Q is subfield of $Q\left[\sqrt{2}\right]$ then $Q\sqrt{2}$ is called extension field of Q.

Ans. It has 2 extensions since $Q\subseteq Q\left[\sqrt{2}\right]$ and $Q\left[\sqrt{2}\right]\subseteq Q\left[\sqrt{2}\right]$

Q. How many subfields of $Q\left[\sqrt{2}\right]$ Solution: Q and $Q\left[\sqrt{2}\right]$ are two subfields of $Q\left[\sqrt{2}\right]$ then exactly two subfields. Similarly, $Q\left[\sqrt{3}\right]$ has two subfields Q and $Q\left[\sqrt{3}\right]$.

Q. How many subfields in $Q\left(\sqrt{2},\sqrt{3}\right)$? Solution: $Q,Q\left(\sqrt{2}\right),Q\left(\sqrt{3}\right)$ and $Q\left(\sqrt{2},\sqrt{3}\right)$ exactly 4 subfields.

Note: If L is extension field of K and K is extension field of **F** then L is extension field of **F** i.e. $[L:K][K:\mathbf{F}]=[L:\mathbf{F}]$

Imp: Extension of field is not symmetric hence it is not an equivalence relation. Then $\dim[L:\mathbf{F}]=\dim[L:K]\times\dim[K:\mathbf{F}]$

Q. Find dimension of $Q\left[\sqrt{2},\sqrt{3},\sqrt{5}\right]$ over Q. Solution: $\dim\left[Q\left[\sqrt{2},\sqrt{3},\sqrt{5}\right]:Q\right]$

$$\left[Q\sqrt{2},\sqrt{3},\sqrt{5}:Q\right]=\left[Q\sqrt{2},\sqrt{3},\sqrt{5}:Q\sqrt{2},\sqrt{3}\right]\left[Q\sqrt{2},\sqrt{3}:Q\sqrt{2}\right]\left[Q\sqrt{2}:Q\right]$$

Mindset Makers

$\dim\left[Q\sqrt{2},\sqrt{3},\sqrt{5}:Q\right]=\dim\left[Q\sqrt{2},\sqrt{3},\sqrt{5}:Q\sqrt{2},\sqrt{3}\right]\left[Q\sqrt{2},\sqrt{3}:Q\sqrt{2}\right]\dim\left[Q\sqrt{2}:Q\right]$
$=2\times2\times2=8$

Q. Find $\dim\left[Q\sqrt{2}+\sqrt[3]{2}\right]$

Solution: $\left[Q\sqrt{2}+\sqrt[3]{5}:Q\sqrt{2}\right]=\left[Q\sqrt{2},(5)^{1/3}:Q\sqrt{2}\right]$.then $\dim Q\left[\sqrt{2}+\sqrt[3]{5}:Q\sqrt{2}\right]=3$

Q.
$\dim\left[Q(2)^{1/4},(3)^{1/3},(5)^{1/7}:Q(3)^{1/3}\right]=?$ Solution: $\dim\left[Q(2)^{1/4},(3)^{1/3},(5)^{1/7}:Q(3)^{1/3}\right]=4\times7=$ 28

Note: $\dfrac{Z[x]}{\langle m\rangle}=\dfrac{Z[x]}{mZ[x]}=\left[\dfrac{Z}{mZ}\right][x]=Zm[x]$

$\left(\dfrac{R[x]}{I[x]}\approx\left[\dfrac{R}{I}\right][x]\right)$

Q. $\dfrac{Z[x]}{\langle 2\rangle}=\dfrac{Z[x]}{2Z[x]}=\left[\dfrac{Z}{2Z}\right][x]\approx Z_2[x]$

Note: Aut $(K\,|\,\mathbf{F})\approx Z_m$, where K is extension field of $\mathbf{F}$ with dimension m and $\mathbf{F}$ is finite field.

Splitting Field: Let K is an extension field of $\mathbf{F}$ and $f(x)\in\mathbf{F}[x]$ A field K of $\mathbf{F}$ is called splitting field over $f(x)$ is (i) $f(x)$ can be written as product of linear factors over K.

For example:(i) $f(x)=x^2+1\in Q[x]$. $Q[i]$ is splitting field of Q over $f(x)=x^2+1$

(ii) $f(x)=x^2-3\in Q[x]$. $Q\left[\sqrt{3}\right]$ is splitting field of Q over $f(x)=x^2-3$

$\left(\dfrac{Q[x]}{\langle x^2-3\rangle}\approx Q\left[\sqrt{3}\right]\right)$

Theoretical Chapter

Theorem 1. The characteristic of a ring with unity is 0 or n > 0 according as the unity element 1 regarded as a member of the additive group of the ring has the order zero or n.

Theorem 2. The characteristic of an integral domain is 0 or n according as the order of any non-zero element regarded as a member of the additive group of the integral domain is either 0 or n.

Theorem 3. Each non-zero element of an integral domain D, regarded as a member of the additive group of D, is of the same order

Theorem 4. The characteristic of an integral domain is either 0 or a prime number.

Mindset Makers

Characteristic of a field. Every field is an Integral domain. Therefore the characteristic of a field F is 0 or n > 0 according as any non-zero element (in particular the unit element 1) of F is of order 0 or n.

Thus in order to find the characteristic of a field F, we should find the order of the unit element 1 of F when regarded as a member of the additive group of F. If the order of 1 is zero, then F is of characteristic 0 . If the order of 1 is finite, say, n then the characteristic of F is n.

The characteristic of the field of real numbers is 0. The characteristic of the finite field (I_7, x_7, X_7) is 7 where $I_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

Imbedding of a ring into another ring.

Definition. A ring R is said to be imbedded in a ring R′ if there is a subring S′ of R′ such that R is isomorphic to S′.Obviously a ring R can be imbedded in a ring R′ if there exists a mapping f of R into R′ such that f is one-to-one and

$$f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b)\ \forall\ a,b \in R.$$

For then f(R) is a subring of R′ and f is an isomorphism of R onto f(R) making R isomorphic to f(R).

Theorem. Any ring R without a unity element can be imbedded in a ring with unity.

14. The field of Quotients.

Definition. A ring R can be imbedded in a ring S if S contains a subset S′ such that R is isomorphic to S′.

If D is a commutative ring without zero divisors, then we shall see that it can be imbedded in a field F i.e., there exists a field F which contains a subset D′ isomorphic to D. We shall construct a field F with the help of elements of D and this field F will contain a subset D′

Mindset Makers

such that D is isomorphic to D′. This field F is called the "field of quotients" of D, or simply the “quotient field” of D.

On account of isomorphism of D onto and D′ are abstractly identical. Therefore if we identify D′, with D, then we can say that the quotient field F of D is a field containing D. We shall also see that F is the smallest field containing D.

Motivation for the construction of the quotient field. We are all quite familiar with the ring I of integers. Also our familiar set Q of rational numbers is nothing but the set of quotients of the of the elements of I. Thus $Q = \left\{ \frac{p}{q} : p \in I, 0 \neq q \in I \right\}$. If we identify the rational numbers…, $\frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1}$ ….. with the integers…, $-3, -2, -1, 0, 1, 2, 3, \ldots$, then $I \subseteq Q$.

Also if and $\frac{a}{b}$ and $\frac{c}{d} \in Q$, then we remember that

(i) $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$, (ii) $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ (iii) $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$

Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain. We have the following theorem:

Theorem 1. A commutative ring with zero divisors can be imbedded in a field.

Every integral domain can be imbedded in a field.

From the elements of an integral domain D, it is possible to construct a field F which contains a subset D′ isomorphic to D.

Theorem 2. If K is any field which contains an integral domain D, then K contains a subfield isomorphic to the quotient field F of D. In other words the quotient field F of D is the smallest field containing D.

Theorem: Any two isomorphic integral domains have isomorphic-quotient fields.

Mindset Makers

Theorem 1. Show that every prime field of characteristic 0 is isomorphic to the field of rational numbers.

Theorem 2 Every field of characteristic 0 contains a subfield isomorphic to the field of rational Number.

Theorem 3. Every prime field of finite characteristic p is isomorphic to the field I_p of the residue classes of the set of integers modulo p.

Theorem 2. Every ring with unity is isomorphic to a ring of endomorphisms of an abelian group.

Theorem 4. An ideal S of a commutative ring R with unity is maximal if and only if the residue class ring R/S is a field.

Theorem 1. Let R be a commutative ring and S an ideal of R. Then the ring of residue classes R/S is an integral domain if and only if S is a prime ideal.

Theorem 10 An ideal S of the Euclidean ring R is maximal iff S is generated by some prime element of R.

Following are some famous examples. Repeatedly asked in exams.

Q1. Let R be the field of real numbers and S the set of all those polynomials $f(x) \in R[x]$ such that f (0) = 0=F (1). Prove that S is an ideal of R [x]. Is the residue class ring R [x] / S an integral domain ? give reasons for your answer.

Q2. Let R be the ring of all real valued continuous functions defined on the closed interval [0, 1]. Let

M={f(x) $\in$ R : f (t)=0}.

Show that M is a maximal ideal of R.

Q3. If R is a finite commutative ring (i.e., has only a finite per of elements) with unit élement prove that every prime ideal of R is a maximal ideal of R.

Previous Years Questions(2008-203).

Answers of all questions are in this document. If you want quick look over those where in sequence you'll get answers then just have glimpses over revision document. In this revision document points are aligned in orders as those are done in this booklet.

CHAPTER 1. RINGS AND FIELDS

Q2. Let R be an integral domain. Then prove that ch R (characteristic of R) is 0 or a prime. **[1a 2019 IFoS]**

Q3. Find all the proper subgroups of the multiplicative group of the field $(\mathbf{Z}_{13}, +_{13}, \times_{13})$, where $+_{13}$ and $\times_{13}$ represent addition modulo 13 and multiplication modulo 13 respectively. **[3a UPSC CSE 2018]**

Q4. Give an example of a ring having identity but a subring of this having a different identity. **[1b UPSC CSE 2015]**

Q5. Do the following sets form integral domains with respect to ordinary addition and multiplication? If so, state if they are fields:

(i) The set of numbers of the form $b\sqrt{2}$ with b rational

(ii) The set of even integers

(iii) The set of positive integers. **[4a UPSC CSE 2015]**

Q6. If p is a prime number and e a positive integer, what are the elements 'a' in the ring $\mathbf{Z}_{p^e}$ of integers modulo p^e such that $a^2 = a$? Hence (or otherwise) determine the elements in $\mathbf{Z}_{35}$ such that $a^2 = a$. **[2a 2015 IFoS]**

Q7. Show that $\mathbf{Z}_7$ is a field. Then find $\left(|5|+|6|\right)^{-1}$ and $\left(-|4|\right)^{-1}$ in $\mathbf{Z}_7$. **[2a UPSC CSE 2014]**

Q8. Show that the set $\left\{a+b\omega : \omega^3 = 1\right\}$, where a and b are real numbers, is a field with respect to usual addition and multiplication. **[3a UPSC CSE 2014]**

Q9. Prove that the set $\mathbf{Q}\left(\sqrt{5}\right) = \left\{a+b\sqrt{5} : a,b \in \mathbf{Q}\right\}$ is a commutative ring with identity.

[4a UPSC CSE 2014]

Q10. Let J_n be the set of integers mod n. Then prove that J_n is a ring under the operations of addition and multiplication mod n. Under what conditions on n, J_n is a field? Justify your answer.

[2a IFoS 2014]

Q11. Show that any finite integral domain is a field. **[2a 2013 IFoS]**

Q12. Every field is an integral domain - Prove it. **[2b 2013 IFoS]**

Q13. Show that every field is without zero divisor. **[1b 2012 IFoS]**

Q14. Let Q be the set of all rotational numbers. Show that $Q\left(\sqrt{2}\right) = \left\{a+b\sqrt{2} : a,b \in Q\right\}$ is a field under the usual addition and multiplication. **[1b 2011 IFoS]**

Q15. Let $C = \left\{ f : I = [0,1] \to \mathbf{R} \mid f \text{ if continuous} \right\}$. Show C is a commutative ring with 1 under point wise addition and multiplication. Determine whether C is an integral domain. Explain.

[2b UPSC CSE 2010]

Q16. Let F be a field of order 32. Show that the only subfields of F are F itself and $\{0,1\}$.

[1b 2010 IFoS]

Q17. Show that a field is an integral domain and a non-zero finite integral domain is a field.

[4b 2009 IFoS]

Q18. Find the multiplicative inverse of the element

$$\begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$$

of the ring, M, of all matrices of order two over the integers. **[2c 2009 IFoS**

CHAPTER 2. IDEALS AND QUOTIENT RINGS

Q3. (a) Prove that $x^2+1$is an irreducible polynomial in $Z_3[x]$. Further show that the quotient ring $\frac{Z_3[x]}{<x^2+1>}$ is a field of 9 elements. **UPSC CSE 2023** **(15)**

Q1. Let K be a finite field. Show that the number of elements in K is p^n , where p is a prime, which is characteristic of K and $n \geq 1$ is an integer. Also, prove that $\frac{Z_3[x]}{\left(X^2+1\right)}$ is a field. How many elements does this field have? **[4b 2020 IFoS]**

Mindset Makers

Q1. Let R be a principal ideal domain. Show that every ideal of a quotient ring of R is principal ideal and R/P is a principal ideal domain for a prime ideal P of R. **[1b UPSC CSE 2020]**

Q2. Let R be a non-zero commutative ring with unity. Show that M is a maximal ideal in a ring R if and only if R/M is a field. **[2a 2020 IFoS]**

Q3. Show by an example that in a finite commutative ring, every maximal ideal need not be prime.

[3b 2018 IFoS]

Q4. Let A be an ideal of a commutative ring R and $B=\{x\in R: x^n\in A \text{ for some positive integer } n\}$. Is B an ideal of R? Justify your answer. **[2c 2017 IFoS]**

Q5. Let R^C = ring of all real valued continuous functions on $[0,1]$, under the operations

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

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

Let $M=\left\{f\in R^C \,\middle|\, f\left(\frac{1}{2}\right)=0\right\}$. Is M a maximal ideal of R? Justify your answer.

[3b UPSC CSE 2013]

Q6. Prove that:

(i) the intersection of two ideals is an ideal

(ii) a field has no proper ideals. **[3b 2013 IFoS]**

Q7. Is the ideal generated by 2 and X in the polynomial ring $\mathbf{Z}[x]$ of polynomials in a single variable X with coefficients in the ring of integers $\mathbf{Z}$, a principal ideal? Justify your answer.

[3a UPSC CSE 2012]

Q8. Describe the maximal ideals in the ring of Gaussian integers $\mathbf{Z}[i]=\{a+bi \,|\, a,b\in\mathbf{Z}\}$.

[4a UPSC CSE 2012]

Q9. How many elements does the quotient ring $\frac{\mathbf{Z}_5[X]}{(X^2+1)}$ have? Is it an integral domain? Justify yours answers. **[3b UPSC CSE 2009]**

Q10. How many proper, non-zero ideals does the ring Z_{12} have? Justify your answer. How many ideals does the ring $\mathbf{Z}_{12}\oplus\mathbf{Z}_{12}$ have? Why? **[2a UPSC CSE 2009]**

CHAPTER 3. HOMOMORPHISM OF RINGS UPDATED

Q1. Let F be a finite field of characteristic *p*, where *p* is a prime. Then show that there is an injective homomorphism from $\mathbf{Z}_p$ (group of integers modulo *p*) to F. Also show that number of elements in F is p^n, for some positive integer *n*. **[1a IFoS 2022]**

Q1. Let R be a finite field of characteristic $p(>0)$. Show that the mapping $f:R\to R$ defined by $f(a)=a^p$, $\forall a\in R$ is an isomorphism. **[3a UPSC CSE 2020]**

Q2. Let I and J be ideals in a ring R. Then prove that the quotient ring $(I+J)/J$ is isomorphic to the quotient ring $I/(I\cap J)$. **[2a 2019 IFoS]**

Q3. Let R be a commutative ring with unity. Prove that an ideal P of R is prime if and only if the quotient ring R/P is an integral domain. **[2d 2018 IFoS]**

Q4. If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R' prove that $\phi(1)$ is the unit element of R'. **[2a UPSC CSE 2015]**

Q5. Show that the set of matrices $S=\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} a,b\in \mathbf{R}\right\}$ is a field under the usual binary operations of matrix addition and matrix multiplication. What are the additive and multiplicative identities and what is the inverse of $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$? Consider the map $f:\mathbf{C}\to S$ defined by $f(a+ib)=\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Show that *f* is an isomorphism. (Here $\mathbf{R}$ is the set of real numbers and $\mathbf{C}$ is the set of complex numbers.) **[1a UPSC CSE 2013]**

Q6. Show that the quotient ring $\mathbf{Z}[i]/10\mathbf{Z}$ where $\mathbf{Z}[i]$ denotes the ring of Gaussian integers. **[3b UPSC CSE 2010]**

CHAPTER 4. EUCLIDEAN RINGS, PID

UPDATED

Q1(b) Express the ideal 4*Z*+6*Z* as a principal ideal in the integral domain *Z*. **UPSC CSE 2023**

Q1. Let R be a field of real numbers and S, the field of all those polynomials $f(x)\in R[x]$ such that $f(0)=0=f(1)$. Prove that S is an ideal of $R[x]$. Is the residue class ring $R[x]/S$ an integral domain? Give justification for your answer. **[4a UPSC CSE 2022]**

Q1. Let *a* be an irreducible element of the Euclidean ring R, then prove that $R/(a)$ is a field. **[3d UPSC CSE 2019]**

Q2. Prove that the ring $\mathbf{Z}[i]=\{a+ib:a,b\in\mathbf{Z},i=\sqrt{-1}\}$ of Gaussian integers is a Euclidean domain. **[2d 2017 IFoS]**

Q3. Show that in the ring $R=\{a+b\sqrt{-5}\,|\,a,b \text{ are integers}\}$, the elements $\alpha=3$ and $\beta=1+2\sqrt{-5}$ are relatively prime, but $\alpha\gamma$ and $\beta\gamma$ have no g.c.d. in R, where $\gamma=7(1+2\sqrt{-5})$. **[2c 2016 IFoS]**

Q4. Let $J=\{a+bi\,|\,a,b\in\mathbf{Z}\}$ be the ring of Gaussian integers (subring of $\mathbf{C}$). What of the following is J: Euclidean domain, principal ideal domain, unique factorization domain? Justify your answer. **[3a UPSC CSE 2013]**

Q5. Let R be a Euclidean domain with Euclidean valuation *d*. Let *n* be an integer such that $d(1)+n\geq 0$. Show that the function $d_n:R-\{0\}\to S$, where S is the set of all negative

Mindset Makers

integers defined by $d_n(a)=d(a)+n$ for all $a\in R-\{0\}$ is a Euclidean valuation. **[4a 2010 IFoS]**

Q6. Show that $d(a)<d(ab)$, where *a*, *b* be two non-zero elements of a Euclidean domain R and *b* is not a unit in R. **[4a 2009 IFoS]**

CHAPTER 5. POLYNOMIAL RINGS, UFD
UPDATED

Q1. Prove that $R[x]$ is a principal ideal domain if and only if R is a field.
[4b IFoS 2022]

Q2. Let F be a field and $f(x)\in F[x]$ a polynomial of degree > 0 over F. Show that there is a field F' and an imbedding $q:F\to F'$ s. t. the polynomial $f^q\in F'[x]$ has a root in F', where f^q is obtained by replacing each coefficient a of *f* by $q(a)$. **[2b UPSC CSE 2021]**

Q3. Show that an element *x* in a Euclidean domain is a unit if and only if $d(x)=d(1)$, where the notations have their usual meanings. [4b IFoS 2021]

Q3. Let R be a non-zero commutative ring with unity. If every ideal of R is prime, prove that R is a field.
(ii) Let R be a commutative ring with unity such that $a^2=a,\forall a\in R$. If I be any prime ideal of R, find all the elements of $\frac{R}{I}$. **[3b IFoS 2021]**

Q1. Let R be an integral domain with unit element. Show that any unit in $R[x]$ is a unit in R. **[1a UPSC CSE 2018]**

Q2. Let F be a field and $F[X]$ denote the ring of polynomials over F in a single variable X. For $f(X),g(X)\in F[X]$ with $g(X)\neq 0$, show that there exist $q(X),r(X)\in F[X]$ such that degree $(r(X))<$ degree$(g(X))$ and $f(X)=q(X)\cdot g(X)+r(X)$. **[2c UPSC CSE 2017]**

Q3. Let $\mathbf{K}$ be a field and $\mathbf{K}[X]$ be the ring of polynomials over $\mathbf{K}$ in a single variable X. For a polynomial $f\in\mathbf{K}[X]$, let (f) denote the ideal in $\mathbf{K}[X]$ generated by *f*. Show that (f) is a maximal ideal in $\mathbf{K}[X]$ if and only if *f* is an irreducible polynomial over $\mathbf{K}$. **[1a UPSC CSE 2016]**

Q4. Show that every algebraically closed field is infinite. **[4a UPSC CSE 2016]**

Mindset Makers

Q5. Let R be an integral domain with unity. Prove that the units of R and $R[x]$ are same.

[3a 2014 IFoS]

Q6. If R is an integral domain, show that the polynomial ring $R[x]$ is also an integral domain.

[3c 2012 IFoS]

Q7. Let F be the set of all real valued continuous functions defined on the closed interval $[0,1]$. Prove that $(F,+,\cdot)$ is a Commutative Ring with unity with respect to addition and multiplication of functions defined point wise as below:

and $\left.\begin{array}{l}(f+g)(x)=f(x)+g(x)\\(f\cdot g)(x)=f(x)\cdot g(x)\end{array}\right\} x\in[0,1]$ where $f,g\in F$. **[3a UPSC CSE 2011]**

Q8. Consider the polynomial ring $Q[x]$. Show $p(x)=x^3-2$ is irreducible over Q. Let I be the ideal in $Q[x]$ generated by $p(x)$. Then show that $Q[x]/I$ is a field and that each element of it is of the form $a_0+a_1t+a_2t^2$ with a_0,a_1,a_2 in Q and $t=x+I$. **[3a UPSC CSE 2010]**

Q9. Show that $Z[X]$ is a unique factorization domain that is not a principal ideal domain (**Z** is the ring of integers). Is it possible to give an example of principal ideal domain that is not a unique factorization domain? ($\mathbf{Z}[X]$ is the ring of polynomials in the variable X with integer.)

[3a UPSC CSE 2009]

(EXTENSION FIELD)

Q1. Let K be an extension of a field F. Prove that the elements 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. **[3a UPSC CSE 2016]**

Mindset Makers