RING

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

(A) $(R,+)$ commutative group

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

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

(iii) $\forall\, a\in R\ \exists\, 0\in R$ such that $a+0 = 0+a = a$

or $\forall\, a\in R\ \exists!\, b\in R$ such that $a+b = b+a = a$

(iv) for each $a\ \exists!\ -a$ such that $a+(-a) = (-a)+a = 0$

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

(B) $(R,\cdot)$ Semigroup

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

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

(C) Left and Right distributive law

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

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

$\forall\, a\in R\ \exists\, 0\in R$ such that

Ques: $(Z,+,\cdot)$ is Ring?

Sol:- (A) $(Z,+)$ is cyclic group then $(Z,+)$ is Commutative group.

(B) $(Z,\cdot)$ is semi group

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

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

L.H.S $a\cdot(b\cdot c) = a\cdot b\cdot c$

R.H.S $(a\cdot b)\cdot c = a\cdot b\cdot c$

Scanned with CamScanner

(c) Left and right distribution
(i) $a\cdot(b+c) = a\cdot b + a\cdot c \quad , \forall\ a,b,c \in Z$
(ii) $(a+b)\cdot c = a\cdot c + b\cdot c \quad , \forall\ a,b,c \in Z$

then $(Z,+,\cdot)$ is ring.

Illy $(Q,+,\cdot)$ $(R,+,\cdot)$ $(C,+,\cdot)$ are ring.

Commutative Ring:- A ring $(R,+,\cdot)$ is said to be commutative ring if $a\cdot b = b\cdot a \quad \forall\ a,b \in R$

Ques: $(Z,+,\cdot)$, $(Q,+,\cdot)$, $(R,+,\cdot)$, $(C,+,\cdot)$ are commutative ring.

Sol: $\because$ $(R,+,\cdot)$ is ring and $a\cdot b = b\cdot a \quad \forall\ a,b \in R$
then
$(R,+,\cdot)$ is commutative ring.

Since $Q \subseteq R$ and $(R,+,\cdot)$ is commutative ring
then $(Q,+,\cdot)$ is commutative ring

Illy $(Z,+,\cdot)$ is commutative ring.

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

finite integral Domain is field so $F - \{0\}$ is field

additive identity
~~identity~~
multiplicative identity

In field minimum element will be two

Scanned with CamScanner

Ques:- $(Z,+,\cdot)$ is commutative ring with unity.

Sol:- $1 \in Z$ such that $1\cdot a = a\cdot 1 = a \quad \forall\, a \in Z$

and $(Z,+,\cdot)$ is commutative ring then

$(Z,+,\cdot)$ is commutative ring with unity

Similarly $(Q,+,\cdot)$, $(R,+,\cdot)$, $(C,+,\cdot)$ are commutative ring with unity 1.

Ques: $R=\{0\}$ is commutative ring with unity?

Sol: $R=\{0\}$ $(R,+,\cdot)$ is commutative ring but not unity.

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

Sol:- Gaussian integer

$$Z[i] = \{a+ib \mid a,b \in Z\} \quad -(1)$$

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

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

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

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

$= c_1+ic_2$ where $c_1 = a_1+a_2$, $c_2 = b_1+b_2$

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

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

then $c_1+ic_2 \in Z[i]$

$\Rightarrow x+y \in Z[i]$

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

$x+(y+z) = (x+y)+z\ ?$

L.H.S. $x+(y+z) = (a_1+ib_1)+((a_2+ib_2)+(a_3+ib_3))$

$= (a_1+a_2+a_3)+i(b_1+b_2+b_3)$

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

Scanned with CamScanner

$= ((a_1+a_2)+i(b_1+b_2)) + a_3+ib_3)$

$= (a_1+a_2+a_3) + i(b_1+b_2+b_3)$

L.H.S = R.H.S

then $x+(y+z) = (x+y)+z$

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

such that

$x+0 = (a_1+ib_1)+(0+i0) = (a_1+0) + i(b_1+0)$

$= a_1+ib_1$

$= x$

(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)

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

$\Rightarrow -a_1+i(-b_1) \in Z[i]$

$\Rightarrow -x = -a_1+i(-b_1) \in Z[i]$

such that

$x+(-x) = (-x)+x = 0 = 0+i0$

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

$x+y = (a_1+ib_1) + (a_2+ib_2) = (a_1+a_2)+i(b_1+b_2)$

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

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

$= y+x$

$\Rightarrow x+y = y+x \quad \forall x,y \in Z[i]$

(B) $Z[i]$ is semi group

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

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

$= (a_1a_2-b_1b_2) + i(a_1b_2+b_1a_2) \in Z[i]$

Scanned with CamScanner

Now: $x = (a_1, b_1) \in Q \times Q$
$y = (1,1) \in Q \times Q$
$x \cdot y = (a_1, b_1)(1,1) = (a_1 \cdot 1, b_1 \cdot 1) = (a_1, b_1) = x$

then $Q \times Q$ is commutative ring with unity $(1,1)$.

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

Sol: Yes, $(1,0) \in Q \times \{0\}$ such that
$(1,0)(a,0) = (a,0)$

IIIly
(i) $Z[i] \times \{0\} \rightarrow$ unity $(1,0)$
(ii) $\{0\} \times R \times C$ are commutative ring with ~~unity~~ unity.

unity of $\{0\} \times R \times C \rightarrow (0,1,1)$

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

Ques: $R = Z_2$ is Boolean ring?

Sol: $Z_2 = \{0,1\}$
$0 \in Z_2$ such that $0^2 = 0$
$1 \in Z_2$ " " $1^2 = 1$
then Z_2 is Boolean ring.

Ques: Give the example of Boolean ring of order 4 and infinite.

Sol: Boolean ring of order 4

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

$(0,0) \in Z_2 \times Z_2$ such that $(0,0)^2 = (0,0)$

Scanned with CamScanner

$(1,0) \in Z_2 \times Z_2$ " $(1,0)^2 = (1,0)$
$(1,1) \in Z_2 \times Z_2$ " $(1\,1)^2 = (1,1)$

Boolean ring of order ∞

$$R = Z_2 \times Z_2 \times Z_2 \times Z_2 \times \cdots$$ up to infinity and so on

is Boolean ring of order ∞.

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

$$a \cdot b = 0$$

Note: If R is not commutative then

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{R})$$

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{R})$$

$$A \cdot B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$ represent A is zero divisor

But

$$B \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

A is not zero divisor

Integral Domain: A commutative ring with unity $(R + \cdot)$ is called integral domain if $0 \neq a \in R$, $0 \neq b \in R \Rightarrow a \cdot b \neq 0$
and $a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$

Que $(Z + \cdot)$, is an integral domain

Sol: $a \in Z$, $b \in Z$ and $a \cdot b = 0$
$\Rightarrow a = 0$ or $b = 0$ then Z is an integral

Scanned with CamScanner

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

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

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

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

$a_1 \in Z_m \;,\; a_2 \in Z_m \Rightarrow a_1 + a_2 \in Z_m$ {because Z_m is group}

$b_1 \in Z_n \;,\; b_2 \in Z_n$

$\Rightarrow b_1 + b_2 \in Z_n$ {because Z_n is group}

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

$\Rightarrow x + y \in Z_m \times Z_n$

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

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

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

such that

$x + (-x) = (a_1, b_1) + (m - a_1, n - b_1)$

$= (a_1 + m - a_1, b_1 + n - b_1)$

$= (m, n)$

$= (0, 0)$

$Z_5 \quad 2 \in Z_5$

$2^{-1} = 3$

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

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

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

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

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

$= y + x$

$x + y = y + x \quad \forall \; x, y \in Z_m \times Z_n$

$\because a_1, a_2 \in Z_m$, $a_1 + a_2 \in Z_m$, Z_m is cyclic, so abelian so $a_1 + a_2 = a_2 + a_1$

$(Z_m \times Z_n, +)$ is abelian group.

Scanned with CamScanner

commutative ring

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

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

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

$\Rightarrow x \cdot y \in Z_m \times Z_n$

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

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

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

$Z_m \times Z_n$ is ring.

IIly

$Z \times Z$, $R \times Q$, $Z[i] \times Z[i]$, $Z \times Q$, $Q \times Q$, $R \times R$, $C \times C$ are ring.

Ques: $Z_m \times Z_n$ is commutative ring?

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

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

$$
\begin{aligned}
x \cdot y &= (a_1, b_1)(a_2, b_2) \\
&= (a_1 a_2, \; b_1 b_2) \\
&= (a_2 a_1, \; b_2 b_1) \quad \{\because Z_m, Z_n \text{ are ring}\} \\
&= (a_2, b_2)(a_1, b_1) \\
&= yx
\end{aligned}
$$

$xy = yx$

then $Z_m \times Z_n$ is commutative

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

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

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

$x \cdot y = y \cdot x$, then $Q \times Q$ is commutative ring.

Scanned with CamScanner

Scanned with CamScanner

Now: $x = (a_1, b_1) \in Q \times Q$
$y = (1,1) \in Q \times Q$
$x \cdot y = (a_1, b_1)(1,1) = (a_1 \cdot 1, b_1 \cdot 1) = (a_1, b_1) = x$

then $Q \times Q$ is commutative ring with unity $(1,1)$.

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

Sol: Yes, $(1,0) \in Q \times \{0\}$ such that
$(1,0)(a,0) = (a,0)$

IIly
(i) $Z[i] \times \{0\} \rightarrow$ unity $(1,0)$
(ii) $\{0\} \times R \times C$ are commutative ring with ~~unity~~ unity.

unity of $\{0\} \times R \times C \rightarrow (0,1,1)$

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

Ques: $R = Z_2$ is Boolean ring?

Sol:- $Z_2 = \{0,1\}$
$0 \in Z_2$ such that $0^2 = 0$
$1 \in Z_2$ " " $1^2 = 1$
then Z_2 is Boolean ring.

Ques: Give the example of Boolean ring of order 4 and infinite.

Sol: Boolean ring of order 4

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

$(0,0) \in Z_2 \times Z_2$ such that $(0,0)^2 = (0,$

Scanned with CamScanner

$(0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $(0,1)^2 = (0,1)$

$(1,0) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ " $(1,0)^2 = (1,0)$

$(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ " $(1,1)^2 = (1,1)$

Boolean ring of order ∞

$R = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$ up to infinity and so on

is Boolean ring of order ∞.

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

$$a \cdot b = 0$$

Note: If R is not commutative then

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{R})$$

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{R})$$

$$A \cdot B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$ represent A is zero divisor

But

$$B \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

A is not zero divisor

Integral Domain:- A commutative ring with unity $(R, +, \cdot)$ is called integral domain if $0 \neq a \in R$, $0 \neq b \in R \Rightarrow a \cdot b \neq 0$

and $a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$

Que: $(\mathbb{Z}, +, \cdot)$, is an integral domain

Sol: $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ and $a \cdot b = 0$

$\Rightarrow a = 0$ or $b = 0$ then $\mathbb{Z}$ is an integral

Scanned with CamScanner

Illy $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ $(\mathbb{C}, +, \cdot)$ $(\mathbb{Z}[i], +, \cdot)$ are integral domain.

Ques: $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$ is an integral domain.

Sol: No, because let $0 \neq 3 \in \mathbb{Z}_{12}$, $0 \neq 4 \in \mathbb{Z}_{12}$

$3 \cdot 4 = 12 = 0$ over $\mathbb{Z}_{12}$

then $\mathbb{Z}_{12}$ is not integral domain.

Ques: $\mathbb{Z}_{21}$ is an integral domain.

Sol: $0 \neq 7 \in \mathbb{Z}_{21}$ But $7 \cdot 3 = 21 = 0$

$0 \neq 3 \in \mathbb{Z}_{21}$

Note:- $\boxed{\mathbb{Z}_n \text{ is an integral domain iff } n = p.}$

Ques: $\mathbb{Z}_1$ is integral domain.

Sol: No, $\mathbb{Z}_1$ is not commutative ring with unity.

Ques: $R = \mathbb{Z} \times \mathbb{Q}$ is an integral domain?

Sol: $(0,0) \neq (1,0) \in \mathbb{Z} \times \mathbb{Q}$

$(0,0) \neq (0,1) \in \mathbb{Z} \times \mathbb{Q}$.

But $(1,0)(0,1) = (1 \cdot 0, 0 \cdot 1) = (0,0)$

then

$\mathbb{Z} \times \mathbb{Q}$ is not integral domain

Ques: $R = \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}[i]$ is an integral domain?

Sol $(0,0,0) \neq (1, 0, 0+0i) \in \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}[i]$ but $(1, 0, 0+0i)(0,1,0)$ [illegible]

$(0,0,0) \neq (0,1,0) \in \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}[i]$ [illegible] $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}[i]$ [illegible]

Ques: $R = \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}[i] \times \mathbb{Z}_3 \times \mathbb{R} \times \mathbb{C} \times \mathbb{Z}_6$ is integral domain?

Sol:

Scanned with CamScanner

Ques: $R = \mathbb{R} \times \{0\}$ is an integral domain?

Sol: $x \in \mathbb{R} \times \{0\}$ then $x = (a, 0)$

$y \in \mathbb{R} \times \{0\}$ then $y = (b, 0)$

$x \cdot y = 0$

$(a, 0)(b, 0) = 0 = (0, 0)$

$\Rightarrow (ab, 0) = (0, 0)$

$\Rightarrow ab = 0$, $a, b \in \mathbb{R}$, $\mathbb{R}$ is integral domain $\Rightarrow a = 0$ or $b = 0$

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

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

$x \cdot y = 0 \Rightarrow x = 0$ or $y = 0$.

Gaussian Integer Modulo n:

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

$$\mathbb{Z}_1[i] = \{a + ib \mid a, b \in \mathbb{Z}_1\} = \{0\}$$

$$\mathbb{Z}_2[i] = \{a + ib \mid a, b \in \mathbb{Z}_2\} = \{0, 1, i, 1+i\}$$

$$\mathbb{Z}_3[i] = \{a + ib \mid a, b \in \mathbb{Z}_3\}$$

$$= \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\}$$

Note: $O(\mathbb{Z}_n[i]) = n^2$

Show that $(\mathbb{Z}_n[i], +, \cdot)$ is commutative ring.

T: If $n > 1$ then $(\mathbb{Z}_n[i], +, \cdot)$ is commutative ring with unity 1.

Scanned with CamScanner

Ques: $Z_2[i]$ is an integral domain?

Sol: $Z_2[i] = \{a+ib \mid a, b \in Z_2\}$ is commutative ring with unity

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

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

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

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

$Z_2[i]$ is Not integral domain.

Ques:

$Z_3[i]$ is an integral domain.

Sol:

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

$= \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\}$

from Composition Table

$\forall\ 0 \neq a \in Z_3[i]$

$\forall\ 0 \neq b \in Z_3[i]$

$a \cdot b \neq 0$

$Z_3[i]$ is an integral domain.

~~X 2 i 2i 1+i 1+2i~~

$\cdot$	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	[illegible]	$2i$	i	$2+2i$	$2+i$	$1+2i$	$1+i$
i	1	$2i$	$2i$	1	$i+2$	$i+1$	$2i+2$	$2i+1$
$2i$	$2i$	i	1	2	$2i+1$	$2i+2$	$i+1$	$i+2$
$1+i$	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	2	1	i
$1+2i$	$1+2i$	$2+i$	$1+i$	$2+2i$	2	i	$2i$	1
$2+i$	$2+i$	$1+2i$	$2+i$	$1+i$	[illegible]	$2i$	1	2
$2+2i$	$2+2i$	$1+i$	$2i+1$	2	1	2	2	$2i$

Ques: $Z_4[i]$ is an integral domain?

Sol: No, $0 \neq 2 \in Z_4[i]$

Scanned with CamScanner

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

$2 \cdot 2 = 4 = 0$

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

{ Composite number give always integral d...

Que: $R = Z_5[i]$ is an integral domain.

Sol: $Z_5[i] = \{a+ib \mid a, b \in Z_5\}$

$\{0, i, 2i, 3i, 4i, 1, 2, 3, 4, 1+i, 2+2i, 3+3i, 4+4i, \}$

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

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

But $(2+i)(2+4i) = 0$

then $Z_5[i]$ is not integral domain.

26/10/2014

Note: $Z_p[i]$ is an integral domain iff $4/p-3$ here p is prime no. always

e.g. $Z_2[i]$ $4 \nmid 2-3$

$\therefore$ $Z_2[i]$ is not integral domain

$Z_{13}[i] = 4 \nmid 13-3$

$Z_{13}[i]$ is not integral domain.

$Z_{17}[i] = 4 \nmid 17-3$

$Z_{17}[i]$ is not "

$Z \times Z$, $Z \times \mathbb{R}$, $Z_3[i] \times Z_7[i]$, $Q \times \mathbb{R} \times \mathbb{C}$, $Q \times Z_7 \times Z_{13}[i] \times \mathbb{R}$, $Q \times Q$, $\mathbb{R} \times \mathbb{R}$, $\mathbb{C} \times \mathbb{C}$, $Q \times \mathbb{C}$ is not integral domain.

Que: Show that $Z \times \mathbb{R}$ is not integral domain

Sol: $(0,0) \neq (1,0) \in Z \times \mathbb{R}$

Scanned with CamScanner

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

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

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

Ques: $Z \times Q \times \mathbb{R}$ is an integral domain?

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

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

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

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

Ques: $R = \mathbb{C} \times \mathbb{C}$ is an integral domain?

Sol: $(0,0) \neq (1,0) \in \mathbb{C} \times \mathbb{C}$ But $(1,0)(0,1) = (0,0)$

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

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

Ques: $R = \mathbb{C} \times \{0\}$ is an integral domain?

$Z_3[i] \times \{0\}$ is an integral domain

Ques: Show that $Z_5[i] \times \{0\}$ is not integral domain

Sol: $Z_5[i] \times \{0\} = \{(a,0) \mid (a,0) \in Z_5[i] \times \{0\}\}$

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

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

But $(2+i, 0)\ (2+4i, 0)$

$= ((2+i)(2+4i), 0.0)$

$= (0,0)$

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

Scanned with CamScanner

Ques: $R = \{0\} \times \{0\}$ is integral domain?

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

---

① $\boxed{\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{Z}_p,\ \mathbb{Z}_p[i] \text{ if } 4 \mid p-3 \text{ are integral domain.}}$

$\mathbb{Z}_7$ is integral domain but $\mathbb{Z}_7 \times \mathbb{Z}_7$ is not integral domain. Also $\mathbb{Z}_7 \times \mathbb{Z}_7$ is not integral domain but $\mathbb{Z}_7 \times \{0\}$ is integral domain.

Note:

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

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

$$\mathbb{Q}[i] \subseteq \mathbb{R}[i]$$

Idempotent elements:- Let $(R, +, \cdot)$ be a ring. An element $a \in R$ is said to be idempotent element of R if $a^2 = a$

Ques: $R = \mathbb{Z}$, How many idempotent elements in R?

Sol: $\mathbb{Z} = \{0, \pm 1, \pm 2 \ldots\}$

$0 \in \mathbb{Z}$ such that $0^2 = 0$

$1 \in \mathbb{Z}$ " " $(1)^2 = 1$

then only 0 & 1 are idempotent element in $\mathbb{Z}$.

Ques: How many idempotent elements in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_4[i]$.

In $\mathbb{Q}$ idempotent $\{0, 1\}$ $1^2 = 1$

" $\mathbb{R}$ " $\{0, 1\}$

Scanned with CamScanner

Ques:- $R = Z_6$ How many idempotent elements.

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

$0 \in Z_6$ such that $0^2 = 0$

$1 \in Z_6$ " " $1^2 = 1$

$3 \in Z_6$ " " $3^2 = 9 = 3$

$4 \in Z_6$ " " $4^2 = 16 = 4$

then $0, 1, 3, 4$ are idempotent elements in Z_6

$\Rightarrow$ Z_6 has exactly 4 idempotent elements.

Ques: How many idempotent elements in Z_{256}

Sol: # of prime divisor of $256 = 1$

# of idempotent element in $Z_{256} = 2^1 = 2$

Ques: How many idempotent elements in Z_{30}

Sol: $Z_{30} = \{0, 1, \ldots, 29\}$

$0^2 = 0$	$10^2 = 10$
$1^2 = 1$	$21^2 = 21$
$6^2 = 6$	$15^2 = 15$
$25^2 = 25$	$16^2 = 16$

$0, 1, 6, 25, 10, 21, 15, 16$ are idempotent.

or $0, 1, 6, 10, 15, 16, 21, 25$ " "

Ques: How many idempotent elements in Z_{20}

Sol:

$0^2 = 0$

$1^2 = 1$

$5^2 = 5$

$16^2 = 16$

exactly 4 elements.

Note: $\boxed{\text{\# of idempotent elements in } Z_n = 2^d \text{ where } d \text{ is the number of prime divisor of } n}$

Scanned with CamScanner

Example: $R = Z_{30}$

$n = 30$

# of prime divisor of $30 = 3$ (say $2, 3, 5$)

# of idempotent element in $Z_{30} = 2^3 = 8$.

Ques: $R = Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, How many idempotent element in Z_8.

Sol: $n = 8$

# of prime divisor of $n = 1$

# of idempotent element in $Z_8 = 2^1 = 2$

Ques: If a is idempotent element of R then $1-a$ is also idempotent.

Sol: Let $(R, +, \cdot)$ be a ring and $a \in R$ is idempotent element then $a^2 = a$ —(1)

Now

$$(1-a)^2 = 1^2 + a^2 - 2a$$
$$= 1 + a - 2a \quad (\because a^2 = a)$$
$$= 1 - a$$

$\therefore (1-a)^2 = (1-a)$

$\Rightarrow (1-a)$ is also idempotent element in R.

Ques: If R is integral domain then R has exactly two idempotent element.

Sol: Let $(R, +, \cdot)$ ring be an integral domain, then $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

$a, b \in R$ —(1)

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

$\Rightarrow x^2 - x = 0$

$\Rightarrow x(x-1) = 0$

$\Rightarrow x = 0$ ~~one~~ or $(x-1) = 0$

~~If $x = 0$ then 0 is idempotent ele~~ ~~R~~

If $x - 1 = 0$ then $x = 1$ then 1 is idempotent.

Since R is an integral domain then 0 & 1 both are idempotent elements.

~~Ques~~:- How ~~many~~ Note: Idempotent elements in $Z, Q, R, C, Z_p, Z_p[i]$ $(4 \mid p-3)$, $Q \times \{0\}$, $R \times \{0\}$, $C \times \{0\}$ has exactly two idempotent elements.

Ques: How many idempotent elements in $Z_{23}[i]$

Sol $\because Z_{23}[i]$ is integral domain (where $4 \mid p-3$) So $Z_{23}[i]$ has exactly two idempotent elements.

Ques: How many idempotent elements in $Z_2 \times Z_4$

Sol. $Z_2 \times Z_4 = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}$

$(0,0) \in Z_2 \times Z_4$ such that $(0,0)^2 = (0,0)$

$(0,1) \in Z_2 \times Z_4$ " " $(0,1)^2 = (0,1)$

$(1,0) \in Z_2 \times Z_4$ " " $(1,0)^2 = (1,0)$

$(1,1) \in Z_2 \times Z_4$ " " $(1,1)^2 = (1,1)$

Ques: $R = Z_{10} \times Z_6$, How many idempotent elements $= 16$

$Z_{10}: 0, 1, 2, 5, 6$

$Z_6: 0, 1, 3, 4$

No. of idempt. $(0,0)$, $(0,1)$, $(0,3)$, $(0,4)$

$(1,0)$, $(1,1)$, $(1,3)$, $(1,4)$

~~$(2,0)$ $(2,1)$ $(2,3)$ $(2,4)$~~

$(5,0)$ $(5,1)$ $(5,3)$ $(5,4)$

$(6,0)$ $(6,1)$ $(6,3)$ $(6,4)$

Scanned with CamScanner

$R = \langle 3 \rangle \times \langle 7 \rangle$. How many idempotent in R.

Ques:

potent element: An element $a \in R$ is nilpotent element of ~~R $a^n = 0$ for some n.~~

Ques: How many Nilpotent elements in Z?

Sol: $Z = \{0, \pm 1, \pm 2 \ldots\}$

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

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

Ques: How many nilpotent elements in $\mathbb{Q}, \mathbb{R}, \mathbb{C}, Z_p$.

exactly one $\{0\}$

Ques: How many nilpotent element in Z_6.

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

$0^1 = 0$

$0 \in Z_6$ such that $0^1 = 0$ then 0 is only nilpotent element of Z_6.

Ques: How many elements in Z_8.

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

$0^1 = 0$

$2^3 = 0$

$4^2 = 0$

$6^3 = 0$ Nilpotent elements of Z_8 are $0, 2, 4$ and 6.

Ques: How many Nilpotent elements in Z_{512}

4 f Z_{512}

$2^9 = 512 = 0$

$4^5 = (2^2)^5 = 2^{10} = 1024 = 0$

$6^9 = (2 \times 3)^9 = 2^9 \times 3^9 = 0$

Scanned with CamScanner

Note: If $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, then # of nilpotent in Z_n : $p_1^{\lambda_1-1} p_2^{\lambda_2-1} \cdots p_k^{\lambda_k-1}$

Example: $R = Z_8$, $n = 8 = 2^3$

# of nilpotent in $Z_8 = 2^{3-1} = 2^2 = 4$

e.g. $R = Z_{12}$, # of nilpotent elements?

$12 = 2^2 \times 3^1$

# of Nilpotent element in $Z_{12} = 2^{2-1} \times 3^{1-1}$
$= 2^1$
$= 2$

Ques: $R = Z_{30}$, How many nilpotent elements in Z_{30}?

Sol: $n = 30 = 2^1 \times 3^1 \times 5^1$

# of nilpotent elements in $Z_{30} = 2^{1-1} \times 3^{1-1} \times 5^{1-1}$
$= 2^0 \times 3^0 \times 5^0$
$= 1$

Note: If $n = p_1^{\lambda_1} \times p_2^{\lambda_2} \cdots \times p_k^{\lambda_k}$, then Nilpotent element $= \langle p_1 \cdot p_2 \cdots p_k \rangle$

Ques: Nilpotent elements in Z_{48} = ?

Sol: Nilpotent elements in $Z_{48} = Z_{2^4 \times 3}$
$= \{0, 6, 12, 18, 24, 30, 36, 42\}$
$= \langle 6 \rangle$

(#) Nilpotent element in $Z_{16} = Z_{2^4}$
$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14\}$

Scanned with CamScanner

Que: If R is an integral element then R has exactly one nilpotent element.

Sol: Let $(R, +, \cdot)$ be an 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 element is nilpotent element

If $x \neq 0$ then $x^{n-1} = 0$

$\Rightarrow x \cdot x^{n-2} = 0$

If $x = 0$

then only zero element is nilpotent

If $x \neq 0$ then $x^{n-2} = 0$

Similarly

$x = 0$

then R has exactly one nilpotent element.

Example: $R = Z, Q, \mathbb{R}, \mathbb{C}, Z[i], Z_p, Z_p[i]$ $4 \mid p-3$
$Q \times \{0\}, Z \times \{0\}, \mathbb{R} \times \{0\}, \mathbb{C} \times \{0\}, Z_p \times \{0\}$
$Z_3[i]$ 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 $U(R)$

$a \cdot \frac{1}{a}$ multiplicative inverse of a
e.g.

$R = Z$, find $U(Z) = ?$

$Z = \{0, \pm 1, \pm 2, \pm 3, \pm \ldots\}$

$U(\mathbb{Z}) = \{1, -1\} = \mathbb{Z}^*$

Ques: $R = \mathbb{Q}$, find $U(\mathbb{Q}) = ?$

Sol: $U(\mathbb{Q}) = \mathbb{Q} - \{0\} = \mathbb{Q}^*$

Ques: $U(\mathbb{R}) = ?$

$U(\mathbb{Z}[i]) = ?$, $U(\mathbb{C}) = ?$

Sol: $U(\mathbb{R}) = \mathbb{R} - \{0\} = \mathbb{R}^*$

$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

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

\# $U(\mathbb{R}[i]) = \mathbb{C}^*$, $U(\mathbb{Q}[i]) = (\mathbb{Q}[i]) - \{0\} = (\mathbb{Q}[i])^*$

\# $U(\mathbb{Q} \times \{0\}) = \mathbb{Q}^* (1, 0)$ $(1, 0) = (1, 0)$

$U(\mathbb{R} \times \{0\}) = \mathbb{R}^*$

$U(\mathbb{C} \times \{0\}) = \mathbb{C}^*$

$\{U(\mathbb{Q}$ $\}$

H.W. $U(\mathbb{Q} \times \mathbb{Q}) = ?$

$U(\mathbb{Q} \times \mathbb{Q}) = \mathbb{Q}^* \times \mathbb{Q}^* = U(\mathbb{Q}) \times U(\mathbb{Q})$

Ques: \# $U(\mathbb{Q} \times \{0\}) = \mathbb{Q} \times \{0\} - (0, 0)$

$= (\mathbb{Q} \times \{0\})^*$ or $\mathbb{Q}^* \times \{0\}$

\# $U(\mathbb{R} \times \{0\}) = \mathbb{R} \times \{0\} - \{(0, 0)\}$

$= (\mathbb{R} \times \{0\})^*$

\# $U(\mathbb{C} \times \{0\}) = \mathbb{C} \times \{0\} - (0, 0)$

$= (\mathbb{C} \times \{0\})^*$

Ques: $R = \mathbb{Z}_{15}$

$U(\mathbb{Z}_{15}) = ?$

Sol: $U(\mathbb{Z}_{15}) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$= \mathbb{Z}_{15}^*$

$= U(15)$

Scanned with CamScanner

{1, 3, 7, 9}

$\boxed{\text{units in } Z_n : \phi(n)}$

$]) : ?$

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

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

$= Z_3[i] - \{0\}$

$= (Z_3[i])^*$

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

$= (Z_p[i])^*$

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

27/09/2014

Que: $U(Z_5 \times Z_{10}) = \cancel{U(Z_5) \times U(Z_{10})}\ Z_5^* \times Z_{10}^*$

* If each R_i is commutative ring with unity then

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

integral domain

Que: $R = Z_3[i] = \{a+ib \mid a, b \in Z_3\}$

$= \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\}$

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

Now,

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

1. $\forall\ a \in Z_3[i] - \{0\} = Z_3[i]^*$

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

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

Scanned with CamScanner

2. $a\cdot(b\cdot c) = (a\cdot b)\cdot c$, $\forall\ a,b,c \in Z_3[i]$

3. $\forall\ a \in Z_3[i]^*\ \exists\ 1 \in Z_3[i]^*$ such that

$$a\cdot 1 = 1\cdot a = a$$

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

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

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

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

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

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

If $O(G) = 8 \to Z_8,\ Z_2\times Z_4,\ Z_2\times Z_2\times Z_2,\ D_4 \times,\ Q_4 \times$

$Z_3[i]^*$ is integral domain (is commutative with unity) $a\cdot b = b\cdot a\ \forall a,b$

$O(Z_3[i]^*) = 8 \to Z_8,\ Z_2\times Z_4,\ Z_2\times Z_2\times Z_2,\ D_4,\ Q_4$

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

$1+i \in Z_3[i]^*$ such that $O(1+i) = ?$

$$(1+i)^2 = (1+i)(1+i) = 2i$$
$$(1+i)^4 = (1+i)^2(1+i)^2 = 2i\times 2i = -1$$
$$(1+i)^8 = (1+i)^4(1+i)^4 = (-1)\times(-1) = 1$$

$\Rightarrow O(1+i) = 8$ then $Z_3[i]^* \approx Z_8$.

Que: $(Z_3[i], +)$ is group?

Sol: $Z_3[i]$ is an integral domain then

Scanned with CamScanner

$(Z_3[i], +)$ is commutative group

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

$$O(Z_3[i]) = 9 \quad \begin{cases} Z_9 \times \\ Z_3 \times Z_3 \checkmark \end{cases}$$

$O(0) = 1 \qquad O(2i) = 3$

$O(1) = 3 \qquad O(1+i) = 3$

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

$O(i) = 3 \qquad O(2+i) = 3$

$\{\because i+i+i = 3i = 0\} \quad O(2+2i) = 3$

$Z_3[i]$ has no elements of order 9 then $Z_3[i] \approx Z_3 \times Z_3$.

Que: $(Z_5[i] - \{0\}, \cdot)$ is group?

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

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

But

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

$(Z_5[i] - \{0\}, \cdot)$ is not group. because closure property is not satisfy.

Note:- $(Z_p[i] - \{0\}, \cdot)$ is group if $4 \mid p-3$

Que: $R = Z_7$ is an integral

$(Z_7 - \{0\})$ is group?

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

$\because Z_6$ is group so

$Z_7 - \{0\}$ is group.

$3^1 = 3$
$3^2 = 9 = 2$
$3^3 = 6 = -1$
$3^6 = (-1)^2 = 1$

$\because Z_6$ has element of order 6.

Scanned with CamScanner

Scanned with CamScanner

Ques $R = Z_7[i]$ is an integral domain

(i) $(Z_7[i]^*, \cdot) \simeq ?$ Z_{48}

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

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)

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

Ques: $(Z, +, \cdot)$ is a subring of $(Q, +, \cdot)$

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

Illy

Z	is subring	of	$\mathbb{R}$, $\mathbb{C}$
Q	" "	"	$\mathbb{R}$, $\mathbb{C}$
$\mathbb{R}$	" "	"	$\mathbb{C}$

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

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

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

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

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

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 Case I and Case II $S = \{0\}$ and $S = R$ always subring of R

Scanned with CamScanner

Ques: $S = 2Z$ is subring of Z?

Sol: $Z = \{0, \pm 1, \pm 2, \cdots\}$

$2Z = \{0, \pm 2, \pm 4, \cdots\}$

$\phi \neq 2Z \subseteq Z$

$(2Z, +, \cdot)$ is subring of $(Z, +, \cdot)$ because

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

(2Z is subgroup of Z)

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

Ques: mZ is subring of Z?

Ques: find subring of Z_6

{subring must more than subgroup}

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

subgroups 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 theo.

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

(i) Since S_3 is subgroup of Z_6, then $\forall a \in S_3$ $\forall b \in S_3$

$\Rightarrow a - b \in S_3$

(ii) Table

$\cdot$	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

from table $\forall a \in S_3$, $\forall b \in S$ $\Rightarrow a \cdot b \in S_3$

Z_6 are always subring of Z_6.

Illy

$S_4 = \{0, 3\}$ is also subring of Z_6

Scanned with CamScanner

(i) Since S_4 is subgroup of Z_6 then ... $\exists$ $a-b \in S_4$

(ii) Table.

	0	3
0	0	0
3	0	3

from table $\forall a \in S_4$, $\forall b \in S_4$ $\exists$ $a \cdot b \in S_4$

then S_4 is also subring of Z_6.

<u>Ques:</u> $R = Z_{20}$. How many subring in R?

<u>Note:</u> $\boxed{\text{Number of subring in } Z_n = \tau(n)}$

<u>Ques:</u> $R = M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, a, b, c, d \in \mathbb{R} \right\}$ is an integral domain?

<u>Soll:</u> No, $M_2(\mathbb{R})$ is not commutative ring, then $M_2(\mathbb{R})$ not integral domain.

<u>Note:</u> (i) $M_2(\mathbb{R})$ is a ring with unity but not commutative
(ii) $2Z$ is commutative ring but not unity.

<u>Ques:</u> $R = M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \, a, b, c, d \in R \right\}$ and $S = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \middle| \, a, c \in R \right\}$ S is subring of $M_2(\mathbb{R})$?

<u>Solution:</u> $\phi \neq S \subseteq M_2(\mathbb{R})$

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

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

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

Scanned with CamScanner

then $S = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \mid a, c \in \mathbb{R} \right\}$ is subring of $M_2(\mathbb{R})$

Ques: $R = M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$

$S = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in \mathbb{R} \right\}$ is subring of $M_2(\mathbb{R})$?

Sol: $\phi \neq S \subseteq M_2(\mathbb{R})$

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

$A - B = \begin{bmatrix} 0 & b_1 - b_2 \\ 0 & 0 \end{bmatrix} \in S$

(ii) $A \cdot B = \begin{bmatrix} 0 & b_1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

then

$S = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in \mathbb{R} \right\}$ is subring of $M_2(\mathbb{R})$.

Sum of two subrings:

let A and B are two subrings of R. 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 subring of R — Yes

(ii) Union of two subrings " " " " " R — Need not (Example are subgroups)

(iii) Sum of two subrings of R is subring of R.

(iii) **Sol:** $A = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}$ is subring of $M_2(\mathbb{R})$

and $B = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$ " " " $M_2(\mathbb{R})$.

$A + B = \begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$, $A_1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in A + B$

$B_1 = \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} \in A + B$

Scanned with CamScanner

$A_1 B_1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \notin A+B$

Sum of two subring need not be a subring.

Ques: $4 | 2$ in Z_6 ?

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

If $4 | 2$ in Z_6 then $\exists\, x \in Z_6$ such that

$$4x \equiv 2 \pmod 6 \quad \text{--- (1)}$$

$\gcd(4,6) = 2$ and $2 | 2$, then

$4x \equiv 2 \pmod 6$ has two solution.

Put $x = 2$ then

$$4 \cdot 2 = 8 \equiv 2 \pmod 6$$

$\left\{ \begin{array}{l} ca \equiv cb \pmod n \\ \Rightarrow a \equiv b \left(\bmod \dfrac{n}{\gcd(c,n)}\right) \end{array} \right.$

Put $x = 5$

$$4 \cdot 5 = 20 \equiv 2 \pmod 6$$

$x = 2$ and $x = 5$ are solution of $4x \equiv 2 \pmod 6$.

Ques: $7 | 3$ in Z_8 ?

Sol: Yes $7 | 3$ in Z_8

$7x \equiv 3 \pmod 8$

$x \equiv 7^{-1} 3 \pmod 8$

$\Rightarrow x \equiv 7 \cdot 3 \pmod 8$

$\Rightarrow x \equiv 21 \pmod 8$

$\Rightarrow x \equiv 5 \pmod 8$

$x = 5$ is a solution of $7x \equiv 3 \pmod 8$

HW

Ques: $4 | 1$ in Z_6 ?

$\boxed{\text{Ideal}}$

Left Ideal :- let $\phi \neq I \subseteq R$, $(I, +, \cdot)$ is called left ideal of R if

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

(ii) $\forall\, a \in I,\ \forall\, r \in R \Rightarrow r \cdot a \in I$

Right Ideal :- let $\phi \neq I \subseteq R$ $(I, +, \cdot)$ is said to be right ideal of R if

Scanned with CamScanner

(i) $\forall\ a \in I, \forall\ b \in I \Rightarrow a - b \in I$
(ii) $\forall\ a \in I, \forall\ r \in R \Rightarrow a \cdot r \in I$.

Ideal:- Let $\phi \neq I \subseteq R$, $(I, +, \cdot)$ is an ideal of R if
(i) $\forall\ a \in I, \forall\ b \in I \Rightarrow a - b \in I$
(ii) $\forall\ a \in I, \forall\ \lambda \in R \Rightarrow a \cdot \lambda \in I$ and $\lambda \cdot a \in I$.

Ques: $(Z, +, \cdot)$ is an ideal of $(Q, +, \cdot)$?
or (Z) is " " " " Q?

Sol: No,
$2 \in Z, \quad \frac{1}{3} \in Q$
But $\frac{2}{3} \notin Z$ then Z is not ideal in Q

Ques: (i) Q is an ideal in R?
(ii) R " " " " C?

(i) **Sol:** No, $2 \in Q, \ \sqrt{2} \in R$
But $2\sqrt{2} \notin Q$

(ii) **Sol:** No, $2 \in R$, $i \in C$
$2i \notin R$.

Ques Show that $I = \{0\}$ and $I = R$ are always ideal of R.

Sol: (I) Let $I = \{0\}$
(i) $\forall\ a \in I, \forall\ b \in I \Rightarrow a - b \in I$.
(ii) $\forall\ a \in I, \forall\ \lambda \in R \Rightarrow a \cdot \lambda = 0 = \lambda \cdot a \in I$
then $I = \{0\}$ is an ideal of R.

II) Let $I = R$
(i) $\forall\ a \in I, \forall\ b \in I \Rightarrow a - b \in R = I$
(ii) $\forall\ a \in I, \forall\ \lambda \in R \Rightarrow \lambda \cdot a \in R = I$ and $a \cdot r \in R = I$
then $I = R$ is an ideal of R.

Ques: $I = 2Z$ is an ideal of Z?

Scanned with CamScanner

Sol: $\phi \neq 2Z \subseteq Z$

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

(ii) $\forall a \in 2Z, \forall r \in Z \Rightarrow \underbrace{ra = ar}_{\text{because } Z \text{ is commutative.}} \in 2Z$

then $2Z$ is an ideal of Z

Ques: mZ is an ideal of Z.

Ques: Show that every ideal of R is subring of R but converse need not be true.

Sol: Let I be an ideal of R then

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

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

Now

(i) $\forall a \in I, \forall b \in I \Rightarrow a-b \in I$ (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 subring of R but not ideal of R

because $3 \in Z$, $\sqrt{5} \in R$ but $3\sqrt{5} \notin Z$.

Ques: Z is ideal of $Z[i]$?

Sol: No. $3 \in Z$, and $i \in Z[i]$,

But $3i \notin Z$

Z is not ideal of $Z[i]$

Ques: $Z[i]$ is ideal of Q

Sol: $2 \in Z[i]$, $\frac{1}{3} \in Q$

$\frac{2}{3} \notin Z[i]$, then $Z[i]$ is not ideal of Q

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

Scanned with CamScanner

Scanned with CamScanner

Sol:- Let I be an ideal of R then
$I \subseteq R$ —(1)

Now.
$1 \in I$, $r \in R$ then $r \cdot 1 \in I$ (because I is ideal)
$\Rightarrow r \in I$
$\Rightarrow R \subseteq I$ —(2)

from (1) & (2)
$I = R$.

Ques: $R = Z_8$, find ideal of Z_8

Sol:- $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$
Subring of Z_8 are
$I_1 = \{0\}$
$I_2 = Z_8$
$I_3 = \{0, 2, 4, 6\}$
$I_4 = \{0, 4\}$

I_1 & I_2 always ideal of Z_8
$I_3 = \{0, 2, 4, 6\}$ is an ideal because
(i) $\forall a \in I_3, \forall b \in I_3 \Rightarrow a - b \in I_3$
(ii) $\forall a \in I_3, \forall r \in Z_8 \Rightarrow r \cdot a = a \cdot r \in I_3$
then I_3 is an Ideal.
Similarly I_4 is also ideal in Z_8
then Z_8 has exactly 4-ideals.

Ques: $R = Z_{10}$, How many ideal

Note: $\boxed{\# \text{ of ideal in } Z_n = \tau(n)}$

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

pg 233 Q-50

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

Scanned with CamScanner

Que: Give the example of a subset of M_2 which is subgroup under addition But not subring.

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

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

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

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

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

$\Rightarrow A-B \in S$ then S is subgroup of $M_2(\mathbb{R})$ under addition.

(ii) $A = \begin{bmatrix} 1 & 1+0 \\ 1+0 & 0 \end{bmatrix} \in S$, $B = \begin{bmatrix} 2 & 2+0 \\ 2+0 & 0 \end{bmatrix} \in S$

$$A \cdot B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \notin S$$

then S is not subring of $M_2(\mathbb{R})$

Que: $R = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ and $S = \{(a, b, c) \mid a+b = c;\ a, b, c \in \mathbb{Z}\}$

S is subring of R?, S is ideal of R?

Sol: $a = (1, 0, 1) \in S$
$b = (0, 1, 1) \in S$

Scanned with CamScanner

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

30/09/2024. $\boxed{\text{Infinite no. of ideals in } Z}$

Ques: $R = (Z_{100}, +, \cdot)$, How many ideals in R?

Sol: # of ideals in $Z_{100} = \tau(100) = \tau(2^2 \times 5^2)$
$= (2+1)(2+1)$
$= 3 \cdot 3$
$= 9$

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

Example: $R = (Q, +, \cdot)$ is field?
Sol: Yes. $(Q, +, \cdot)$ is an integral domain and $U(Q) = Q - \{0\}$ i.e. each nonzero element of Q has multiplicative inverse then $(Q, +, \cdot)$ is field.

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

Ques: $Z_5 = \{0, 1, 2, 3, 4\}$ is field

Sol: Z_5 is an Integral domain & each non zero element of Z_5 has multiplicative inverse

i.e. $1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$ (under multiplication)
$4^{-1} = 4$

then $(Z_5, +, \cdot)$ is field.

Scanned with CamScanner

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

for example:-

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

Note:- If F is finite integral domain then F is field.

Ques: # $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, $\mathbb{Z}_7$ is finite integral domain and we know that every finite integral domain is field then $\mathbb{Z}_7$ is field.

Note: $\boxed{\mathbb{Z}_n \text{ is field iff } n = p}$

Ques: $\mathbb{Z}_3[i]$ is field?

Sol: $\mathbb{Z}_3[i]$ is an integral domain and $\mathbb{Z}_3[i]$ is finite then $\mathbb{Z}_3[i]$ is field.

Note:- $\{\mathbb{Z}_p[i]$ is field iff $4 \mid p-3\}$

Ques: $\mathbb{Z}_{13}[i]$ is field?

Sol: $4 \nmid 13-3$ then $\mathbb{Z}_{13}[i]$ is not integral domain. then $\mathbb{Z}_{3}[i]$ is not field.

Ques: $\mathbb{Z}_{23}[i]$ is field?

Sol: $4 \mid 23-3$ then $\mathbb{Z}_{23}[i]$ is finite integral domain. then $\mathbb{Z}_{23}[i]$ is field.

Ques: If F is field then F has exactly two ideals.

Sol: Let F be a field then each non-zero element of F has multiplicative inverse.

Scanned with CamScanner

Let $I = \{0\}$, then $I = \{0\}$ is an ideal of F

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

then $\exists$ $0 \neq a \in I$, if $a \in I$ then $a \in F \Rightarrow a^{-1}$ exist

because $0 \neq a \in F$

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

$\Rightarrow 1 \in I$

Now $1 \in I$ and I is an ideal of F then $I = F$

Ques: How many ideals in Q?

Sol: $(Q, +, \cdot)$ is field and Field has exactly ~~ha~~ two ideals say $I = \{0\}$ and $I = F$

Ques: (i) How many ideals in $\mathbb{R}$?

(ii) How many ideals in $\mathbb{R}[i]$?

(iii) How many ideals in $Z_{11}[i]$?

Sol: (i) $I = \{0\}$ and $I = \mathbb{R}$

(ii) $I = \{0\}$ and $I = \mathbb{R}[i]$

(iii) $Z_{11}[i]$ is field then $Z_{11}[i]$ has exactly two ideal say $I = \{0\}$ and $I = Z_{11}[i]$.

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

Sol: $Z_3[i]$ is field then $Z_3[i]$ has exactly two ideals $I_1 = \{0\}$ and $I_2 = Z_3[i]$

$I \neq I_1$ and $I \neq I_2$

then I is not ideal of $Z_3[i]$.

Ques: (i) How many ideal in $Z_4 \times Z_5$

(ii) " " " " $Q \times \mathbb{R}$

(iii) " " " " $\mathbb{R} \times Q \times Z_7$

Scanned with CamScanner