Chapter-1
Introduction to Rings, Integral Domains and Fields

Long Type Question:

Q.1. Define a ring and given an example of a commutative ring with identity. **2004,15**

Sol^n: Definition of Ring : A non empty of R with two binary opprations '+' and '•' called addition and multiplication is said to be a ring if it satisfied follwoing axioms:

1. **<R, +> form an abelian group. i.e. R satisfied:**

(i) **Closure property :** $a,b,\in,R \Rightarrow a+b\in R$

(ii) **Associative property :** a, b, c, $\in$,R

$\Rightarrow$ a+((b+c) = (a+b)+c

(iii) **Existance of Identity :** $\exists O\in R$ s.t. a+O = O+a =a

$\forall$ a $\in$ R

(iv) **Existance of Inversse :** $\forall$ a $\in$ R $\exists -a\in R$

s.t. a + (–a) = – a (+a) = O $\forall$ R

(v) **Commutative law :** a, b $\in$ R

we have a + b = b + a

2. **<R.· > is sami group : i.e.**

i) R is clossed with respect to (.) a, b$\in$R $\Rightarrow$ a.b$\in$R

ii) R is associative w.r. to (.)

a, b, c $\in$R

a (b.c) = (a.b) .c

Multiplication is distributive over addition : i.e.

i) Multiplication is left distributive over addition -

$\forall$ a, b, c $\in$ R

a. (b+c) = a.b + a.c

ii) Multiplictiion is right distributive over addition.

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

ommutative Ring : A ring <R,+, .> is said to the com-utative ring if satisfied the commutative law with re-pect to (.)

2. The set $\mathbf{Q\sqrt{p}} = \{a + b\sqrt{p}, a, b, \in Q\}$ **form a ring un-**

der p is prime usual addition and multiplic tion.

Sol^n: To proof that $< Q\sqrt{p}, +, \cdot >$ is a ring we have to sho $Q\sqrt{p}$ satisfied following condition :

1. $< Q\sqrt{p} + >$ **form an abelive group :**

(i) Closure property : Let $x, y \in Q\sqrt{p}$ then x and can be expressed as

$$\left.\begin{aligned} x &= a_1 + b_1\sqrt{p} \\ y &= a_2 + b_2\sqrt{p} \end{aligned}\right\} \forall a\ b_1, a_2, b_2 \in Q$$

$$\text{Now } x + y = \left(a_1 + b_1\sqrt{p}\right) + \left(a_2 + b_2\sqrt{p}\right)$$

$$= \left(a_1 + a_2\right) + \left(b_1 + b_2\right)\sqrt{p}. \in Q\sqrt{p}$$

Hence, closure property hold.

2. Associative property : Let $x, y, z \in Q\sqrt{p}$ then

$$\left.\begin{aligned} x &= a_1 + b_1\sqrt{p} \\ y &= a_2 + b_2\sqrt{p} \\ z &= a_3 + b_3\sqrt{p} \end{aligned}\right\} \forall a_1, b_1, a_2, b_2, a_3, b_3 \in Q$$

Now, $x + (y + z) = (x + y) + z$

$$a_1 + b_1\sqrt{p} + \left(a_2 + b_2\sqrt{p} + a_3 + b_3\sqrt{p}\right)$$

$$= \left(a_1 + b_1\sqrt{p} + a_2 + b_2\sqrt{p}\right) + \left(a_3 + b_3\sqrt{p}\right)$$

$$\Rightarrow \quad \left(a_1 + a_2 + a_3\right) + \left(b_1 + b_2 + b_3\right)\sqrt{p}$$

$$= \left(a_1 + a_2 + a_3\right) + \left(a_1 + b_2 + b_3\right)\sqrt{p}$$

L.H.S.=R.H.S.

Hence Associative property holds.

Existance of Indentity : Let $x \in Q\sqrt{p}$

$$x + e = e + x = x$$

$$\left(a_1 + b_1\sqrt{p}\right) + \left(O + O\sqrt{p}\right) = \left(a_1 + b_1\sqrt{p}\right) = x,\ O \in Q$$

Hence $O + \sqrt{p}$ is identity eleument of $Q\sqrt{p}$

Existance of Inverse : Let $x \in Q\sqrt{p}$

Then $\exists y \in Q\sqrt{p}$

$$x + y = O + O\sqrt{p}$$

$$x = a_1 + b_1\sqrt{p}$$

$$y = \left(-a_1\right) + \left(-b_1\right)\sqrt{p}$$

$$x + y = \left(a_1 + b_1\sqrt{p}\right) + \left[\left(-a_1\right) + \left(-b_1\right)\sqrt{p}\right]$$

$$= \left\{a_1 + \left(-a_1\right)\right\} + \left\{b_1 + \left(-b_1\right)\right\}\sqrt{p}$$

$$= O + O\sqrt{p}$$

Which is Identy element of $Q\sqrt{p}$

Commutative law : We show that $x + y = y + x$

Let $x, y \in Q\sqrt{p}$

L.H.S. $$= \left(a_1 + b_1\sqrt{p}\right) + \left(a_2 + b_2\sqrt{p}\right)$$

$$= \left(a_1 + a_2\right) + \left(b_1 + b_2\right)\sqrt{p}$$

$$= \left(a_2 + a_1\right) + \left(b_2 + b_1\right)\sqrt{p}$$

$$= \left(a_2 + b_2\sqrt{p}\right) + \left(a_1 + b_1\sqrt{p}\right)$$

$$= y + x$$

Since commatative law hold is Q.

Hence $Q\sqrt{p}$ is an abelim group.

(2) $\langle Q\sqrt{p}, \cdot \rangle$ **is semi group :**

For this we heve to show following condition

(i) Closure Property :

$$\text{Let } \{a_1 + b_1\sqrt{p}\}\{a_2 + b_2\sqrt{p}\} \in Q\sqrt{p}$$

$$\Rightarrow \{a_1 + b_1\sqrt{p}\}.\{a_2 + b_2\sqrt{p}\}$$

$$= a_1a_2 + a_1b_2\sqrt{p} + b_1\sqrt{p}\ a_2 + b_1\sqrt{p}\ b_2\sqrt{p}$$

$$= a_1a_2 + a_1b_2\sqrt{p} + b_1\sqrt{p}\ a_2 + b_1\ b_2p$$

$$= (a_1a_2 + b_1b_2p) + (a_1b_2 + b_1a_2)\sqrt{p} \in Q\sqrt{p}$$

(ii) Associative property : let

$$\{a_1 + b_1\sqrt{p}\}\{a_2 + b_2\sqrt{p}\}\{a_3 + b_3\sqrt{p}\} \in Q\sqrt{p}$$

$$\text{Now } = \left[\{a_1 + b_1\sqrt{p}\}\{a_2 + b_2\sqrt{p}\}\right](a_3 + b_3\sqrt{p})$$

$$= a_3(a_1a_2 + b_1b_2p) + (a_3b_2a_1 + b_1a_3a_2)\sqrt{p}$$

$$+ (a_1a_2b_3\sqrt{p} + b_1b_2b_3\sqrt{p}) + b_3(a_1b_2 + b_1a_2)p$$

$$\forall x, y, z \Leftarrow Q\sqrt{p}$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \text{ i.e.}$$

Multiplication is associative

3. Multiplication is distributive over addition

(i) Left Distribution : Let $x,y,z \in Q\sqrt{p}$

$$x.(y + z) = x.y + x:z$$

$$\left.\begin{aligned} x &= a_1 + b_1\sqrt{p} \\ y &= a_2 + b_2\sqrt{p} \\ z &= a_3 + b_3\sqrt{p} \end{aligned}\right\}$$

$$\Rightarrow \left(a_1 + b_1\sqrt{p}\right).\left[\left(a_2 + b_2\sqrt{p}\right) + \left(a_3 + b_3\sqrt{p}\right)\right]$$

$$\Rightarrow a_1\left(a_2 + a_3\right) + a_1\left(b_2 + b_3\right)\sqrt{p} + b_1\sqrt{p}\left(a_2 + a_3\right) + b_1\sqrt{p}\left(b_2 + b_3\right)\sqrt{p}$$

$$= a_1.a_2 + a_1b_2\sqrt{p} + b_1a_2\sqrt{p} + b_1b_2p$$

$$= \left(a_1 + b_1\sqrt{p}\right)\left(a_2 + b_2\sqrt{p}\right)$$

Now $x(y+z) = x.y + xz$

$$= \left(a_1 + b_1\sqrt{p}\right)\left\{\left(a_2 + b_2\sqrt{p}\right) + \left(a_3 + b_3\sqrt{p}\right)\right\}$$

$$= \left(a_1 + b_1\sqrt{p}\right)\left\{\left(a_2 + a_3\right) + \left(b_2 + b_3\right)\sqrt{p}\right\}$$

$$= a_1\left(a_2 + a_3\right) + a_1\left(b_1 + b_3\right)\sqrt{p} + b_1\sqrt{p}\left(a_2 + a_3\right) + b_1\left(b_2 + b_3\right)p$$

$$= a_1a_3 + a_1b_3\sqrt{p} + a_3b_1\sqrt{p} + b_1b_3\sqrt{p}\sqrt{p}$$

$$= \left(a_1 + b_1\sqrt{p}\right).\left(a_3 + b_3\sqrt{p}\right)$$

$$= x.\ z$$

(ii) Right distribution : Let $x, y, z \in Q\sqrt{p}$

$$(y+z).x = y.x + zx$$

$$= \left[\left(a_2 + b_2\sqrt{p}\right) + \left(a_3 + b_3\sqrt{p}\right)\right].\left(b_1 + b_1\sqrt{p}\right)$$

$$= \left[\left(a_2 + a_3\right) + \left(b_2 + b_3\right)\sqrt{p}\right].\left(a_1 + b_1\sqrt{p}\right)$$

$$= a_1\left(a_2 + a_3\right) + a_1\left(b_2 + b_3\right)\sqrt{p} + b_1\sqrt{p}\left(a_2 + a_3\right) + b_1\left(b_2 + b_3\right)p$$

$$= a_2a_1 + a_2b_1\sqrt{p} + b_2\sqrt{p}\ a_1 + b_2b_1p$$

$$= \left(a_2 + a_2\sqrt{p}\right).\ \left(a_1 + b_1\sqrt{p}\right)$$

$$= y.\ x$$

Now, $= \left[\left(a_2 + b_2\sqrt{p}\right) + \left(a_3 + b_3\sqrt{p}\right)\right]\left(a_1 + b_1\sqrt{p}\right)$

$= \left[\left(a_2 + a_3\right) + \left(b_2 + b_3\right)\sqrt{p}\right]\left(a_1 + b_1\sqrt{p}\right)$

$= a_1\left(a_2 + a_3\right) + a_1\left(b_2 + b_3\right)\sqrt{p} + b_1\sqrt{p}\left(a_2 + a_3\right) + b_1\sqrt{p}\left(b_2 + b_3\right)\sqrt{p}$

$= a_3a_1 + a_3b_1\sqrt{p} + b_3\sqrt{p}\ a_1 + b_3b_1p$

$= \left(a_3 + b_3\sqrt{p}\right).\ \left(a_1 + b_1\sqrt{p}\right)$

$= z.\ x$

Hence is $(Q\sqrt{p}, +, .)$ a ring

(iii) Commutative Law :

Let $x, y \in Q\sqrt{p}$

s.t. $x = a_1 + b_1 Q\sqrt{p}$

$y = a_2 + b_2 Q\sqrt{p}$

Now $x + y = \left(a_1 + b_1\sqrt{p}\right) + \left(a_2 + b_2\sqrt{p}\right)$

$= \left(a_1 + a_2\right) + \left(b_1 + b_2\right)\sqrt{p}$

$= \left(a_2 + a_1\right) + \left(b_2 + b_1\right)\sqrt{p}$

$= \left(a_2 + b_2\sqrt{p}\right) + \left(a_1 + b_1\sqrt{p}\right)$

$\Rightarrow x + y = y + x$

$= \left(Q\sqrt{p}, +, \bullet\right)$ is a commutative Ring

Q.3. Define the characteristics of ring and give an example of if and prove that characteristic of I.D. is either O or prime No. **2005, 07**

Solⁿ: Characteristics of a ring : Let <R, +, •> be a ring. Then the characteristics of a ring n is the least +ve Integers s.t.

$a + a + a + \ldots\ldots\ldots$ n times $= 0$

or $\boxed{n.a = O}$ (Where zero is the additive Identity)

If no such least +ve Integeus n does not exists then we say that ring has characteristics zero or infinite.

Ex. Let $<z, +, .>$ be the ring of Integers then no such +ve element, exist in z. s.t. n.a = 0 $\forall$ $a \in z$. Hence ring of integes is of characteristics zero or infinite.

Let D be an integral domain

If a non zero element of D is of the order zero. then the characteristic of D is zero.

Let the order of the non zero element a be finite & equal to m then $ma = 0$

Suppose b is any arbitary non zero element of D we have $ma = 0$

$\Rightarrow (ma)b = 0$

$\Rightarrow (am)b = 0$

$\Rightarrow a(mb) = 0$

$\Rightarrow mb = 0$ (D is without zero divisions. Hence each non zero element has order m But order of a is $m \Rightarrow m$ is the least +ve integers such that $ma=0$. Also we have $mo=0$ thus m is the least +ve integer s.t. $mx = 0$ $\forall$ $x \in D$ hence D is of characteristic m.

Hence, characteristics of an Integral Domain is either O or prime no. **Proved.**

Q.4. Show that $R' = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix}, a, b \in R \right\}$ **is a commutative ring with identity under usual operation.**
2008

Sol^n: Let $A = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}, C = \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix}$

be any three elements of R'

R–1 $\quad A + B = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$

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

$$= \begin{bmatrix} u & -v \\ v & u \end{bmatrix}$$ where $u = a_1 + a_2$

$v = b_1 + b_2$

and $u, v \in R$ as $a_1, a_2, b_1, b_2 \in R$

i.e. $A+B \in R'$ i.e. the set R' is closed w.r. to add[n] of matrices.

(II) $$A+(B+C) = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} + \left(\begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} + \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 + a_3 & -(b_2 + b_3) \\ b_2 + b_3 & a_2 + a_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + (a_2 + a_3) & -b_1 - (b_2 + b_3) \\ b_1 + (b_2 + b_3) & a_1 + (a_2 + a_3) \end{bmatrix}$$

$$= \begin{bmatrix} (a_1 + a_3) + a_2 & -(b_1 + b_2) - b_3 \\ (b_1 + b_2) + b_3 & (a_1 + a_2) + a_3 \end{bmatrix}$$

[addition of real no. is ass.]

$$= \begin{bmatrix} a_1 + a_2 & -(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix} + \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix}$$

$$= \left(\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \right) + \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix}$$

$= (A+B)+C$

i.e. addition of matrices in R' obey associative law.

III. $\exists$ null matrix $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ st.

$0+A=A=A+0 \ \forall \ A \in R'$

So the null matrix 0 is additive identity

IV. $\exists$ additive inverse $\begin{bmatrix} -a & b \\ -b & -a \end{bmatrix} \in R'$ of each matrix

$\begin{bmatrix} a & -b \\ b & -a \end{bmatrix} \in R'$ since

$$\begin{bmatrix} -a & b \\ -b & -a \end{bmatrix} + \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} -a+a & b-b \\ -b+a & -a+a \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

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

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

[add of real no. is commutative]

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

i.e. addition of matrices in R' obeys commutative law.

R–2

$$A.B. = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - b_1a_2 \\ b_1a_2 + b_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ (a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix}$$

$$= \begin{bmatrix} u & -v \\ v & u \end{bmatrix}$$

where $u = a_1a_2 - b_1b_2 \in R$ and $v = a_1b_2 + a_2b_1 \in R$
as $a_1, a_2, b_1, b_2 \in R$
i.e. $AB \in R$ i.e. that set R' is closed w.r. to multiplication of matrics.

$$= \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2a_3 - b_2b_3 & -(a_2b_3 + b_2a_3) \\ b_2a_3 + a_2b_3 & a_2a_3 - b_2b_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1(a_2a_3 - b_2b_3) - b_1(a_2b_3 + b_2a_3) & -a_1(a_2b_3 + b_2a_3) + b_1(a_2a_3 - b_2b_3) \\ b_1(a_2a_3 - b_2b_3) + a_1(b_2b_3 + a_2b_3) & a_1(a_2a_3 - b_2b_3) - b_1(b_2a_3 + a_2b_3) \end{bmatrix}$$

$$(A.B.).C = \left(\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \right) \cdot \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix}$$

$$= \left(\begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix} \right) \cdot \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_3(a_1a_2 - b_1b_2) - b_3(a_1b_2 + a_2b_1) & -b_3(a_1a_2 - b_1b_2) - a_3(a_1b_2 + a_2b_1) \\ a_3(a_1b_2 + a_2b_1) + b_1(a_1a_2 - b_1b_2) & a_3(a_1a_2 - b_1b_2) - b_3(a_1b_2 + a_2b_1) \end{bmatrix}$$

clearly A (B.C). = (A.B.).C

as $a_1, a_2, b_1, b_2, b_3 \in R$ obey associative law of multiplication.

R–3

$$A.\ (B+C) = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} + \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2 + a_3 & -(b_2 + b_3) \\ b_2 + b_3 & a_2 + a_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1(a_2 + a_3) - b_1(b_2 + b_3) & -a_1(b_2 + b_3) - b_1(a_2 + a_3) \\ b_1(a_2 + a_3) + a_1(b_2 + b_3) & a_1(a_2 + a_3) - b_1(b_2 + b_3) \end{bmatrix}$$

$$A.B + A.C = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} + \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_3 & -b_3 \\ b_3 & a_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ b_1a_2 + b_2a_1 & a_1a_2 - b_1b_2 \end{bmatrix} + \begin{bmatrix} a_1a_3 - b_1b_3 & -(a_1b_3 + b_1a_3) \\ b_1a_3 + a_1b_3 & a_1a_3 - b_1b_3 \end{bmatrix}$$

$$\begin{bmatrix} a_1a_2 - b_1b_2 + a_1a_3 - b_1b_3 & -(a_1b_2 + a_2b_1) - (a_1b_3 + b_1a_3) \\ b_1a_2 + b_2a_1 + b_1a_3 + a_1b_3 & a_1a_2 - b_1b_2 + a_1a_3 - b_1b_3 \end{bmatrix}$$

$\therefore$ A. (B+C) = A.B+A.C.

Similarly we can show that (B+C). A = B.A.+C.A

i.e. matrix multiplication is left and right distrubuties with respect to matrix addition in R'.

R-4

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

$$= \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ b_1a_2 + b_2a_1 & a_1a_2 - b_1b_2 \end{bmatrix}$$

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

$$= \begin{bmatrix} a_2a_1 - b_2b_1 & -(a_2b_1 + b_2a_1) \\ b_2a_1 + b_1a_2 & a_2a_1 - b_1b_2 \end{bmatrix}$$

$\therefore$ A.B = B.A

commutative law w.r. to multiplication is satisfied.

R–5

$$\text{an element} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R' \text{ s.t}$$

$$= \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

$\therefore$ R' is a commutative ring with identity under usual operation.

Hence Proved.

2.6. Show that a ring R is with out zero divisor iff the restricted concellation law holds in R.

2010,2015

Proof: (i) Nesserry Conditions: Let R be with

divisor and we shall show that ristricted cancellation law holds in R.

$\Rightarrow$ $a, b \in R$.

then $a.b = 0$

either $a = 0$ or $b = 0$

$a.b = a.c$

$a.b. - a.c = 0$

$a(b - c) = 0$

$= \quad a \neq 0$

$b - c = 0$

$\Rightarrow \quad \boxed{b = c}$ similarly we can proof.

if $b.a = c.a$

$\Rightarrow \quad \boxed{b = c}, a \neq 0$

(ii) Sufficient part : In this part we suppose that restricted cancellation law holds in R and we shall show that ring with zero divisor.

i.e. $a, b \in R$.

$\Rightarrow$ $a.b = 0$ s.t. $a \neq 0, b \neq 0$

Now $a.b = 0$

$a.b. = a.0$

$\Rightarrow \quad b = 0$ {by left canc law}

Which contradicts that ring is with zero divisor and Hence, our supposition is wrong and ring is without zero divisor.

Integral Domain : A commutative ring with element(CRU) is said to be and integral domain if R without zero divisor i.e.

A ring R is said to be can integral domain if satisfied.

(i) Commutative law (ii) Unit element

(iii) R is without divisors

Q.7. Set of Integers z is the simplest example I.D. with respect to operation add, multi.

Ans.(i) we know that $<z, +, \bullet)$ is a ring to proove that an I.D. we shall show.

1. z is commutative

z has unit ellement

Q.8. The charecterstic of an integral domain is either zero or a prime numbers. 2010,2015

Sol": Proof : In the case when charecterstic ctristics of D is zero (ie) $\forall\ a \in D$

$\Rightarrow 0.a = 0$

There is following to prove an other case when charecterstic of D is n,

To prove the theorem it is enough to show n is a prime number.

To get a contradiction, let n is not a prime number.

To get a composite number. Then by definition of composite number n can be expresed as finite product

of $n = p_1\ p_2 \quad \begin{Bmatrix} p_1 < n \\ p_2 < n \end{Bmatrix}$

Since D is an I.D.

$\Rightarrow \quad \forall a \neq 0$ in D

$\therefore \quad a.a = a^2 \neq 0$ in D

cha D = n

$\Rightarrow \quad na = 0$

$\Rightarrow \quad (n.a)\ a = 0.a$ (by Ass. law)

$\Rightarrow \quad na^2 = 0$

$\Rightarrow \quad (p_1p_2)a^2 = 0$

$\Rightarrow \quad (p_1a)\ (p_2a) = 0$

Since D is an I.D. then either

$(p_1a) = 0$ or $(p_2a) = 0$

Let $(p_1a) = 0$

cha of D is p_1 {since $p_1 < n$}

Which is a prime number. Proof.

Short Questions :

Q.1. Define an integral domain and give an example of an Infinite integral domain. 2004,15

Ans. : Solution : A ring (R, +, .) is said to be an integral domain if

(i) R is commutative.

(ii) R has no zero divisor.

Q.2. Prove that set of Matrics contain zero divisor.

Soln: Let M denote the set of all 2x2 matrics and let binary operation are (+) and '(•)'.

Then of $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

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

$\Rightarrow \quad AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Hence set of Matrics has zero divisors.

Q.3. Define characteristic of a Ring (R, +, .) and give an example of it. **2007**

Soln: characteristic of a Ring : Let R be a Ring. If there exists a pasitive integer n such that

$$na = 0 \qquad \forall\ a \in R$$

then R is said to have finite characteristic n.

It such no positive integer exists then R is said to have characteristic zero or (infinity).

Example : Let us consider the ring of integers (R,+,.).

Here we have for any $a \in R$ we have no any pasitive integer n s.t:

$$na = 0$$

Hnce, <R, +, .> is of characteristics zero

Q.4. Let <R, +, .> be a ring then ∀ a, b, c, ∈R Prove that

(i) **a.o = 0.a =0**

(ii) **a.(–b) = (–a).b = –(ab)** **2009**

(iii) **(–a). (–b) = ab**

(iv) **a. (b–c) = a.b – a.c**

(v) **(b–c) .a = ba–c.a**

(i)Proof : Let $0 \in R$

$0 + 0 = 0 \in R$

$a.0 = a.(0+0)$

$a.0 = a.0 + a.0$

$(a.0 - a.0) = a.0$

$0 = a.0$

simmillerly 0.a =0

(ii) Proof : consider = a.(–b) +a.b

= a {(–b)+b}

a.(–b) + a.b = a.0 =0 by (i) proof.

⇒ a. (–b) = – (a.b)

simmillerly (–a).b = – (a.b)

(iii) Proof : (–a). (–b) =ab

consider (–a). (–b) + {–(a.b)}

(–a). (–b) + {(–a).b} by (ii)

(–a) {(–b)+b}

(–a) . 0 = 0 from (i) proof

(–a). (–b) + {–(a.b)} =0

(–a) . (–b) = ab proof

(iv) Proof : consider

a (b–c) + a.c.

a [(b–c) + c]

a.b

∴ a(b–c) + a.c = a.b

a (b–c) = ab –ac

(v) Proof : consider

= (b–c) a +c.a

= [(b–c) +c] a

= b.a

(b–c) a × c.a = b.a

(b–c) a = b.a – c.a **proof**

Q.5. Show that every field is an Integral domain.

2010

Soln: Let <F, +, •> is a field.

Let a be any non zero element of F.

To show that F is without zero diviser we shall proof for any element b ∈F.

a. b =0

or b = 0

Now a.b. =0 since a ∈ F, a^{-1}∈F

⇒ a^{-1} (a.b) = a^{-1}.o

⇒ (a^{-1}a).b = 0

⇒ 1.b = 0

$\Rightarrow \quad \boxed{b = 0}$

Simmillerly we can show that if $b \neq 0 \in F$ then

$a.\ b = 0$

$\Rightarrow \quad a = 0$

i.e. Field has no zero diviser.

$\therefore$ every field is an Integral domain.

Q.6. Prove that division ring is a ring but connerse is no true. **2010**

Sol^n: let (R,+,.) be a divisor ring. Then by definition of division ring we have,

(i) R is a ring with unity.

(ii) Every non zero element of R have multiplicative inverse. i.e. division ring must be a ring first and then satisfies above given conditions (i) and (ii)

The converse of above statement is not rue i.e. A ring need not be a divisior ring.

For example let us suppose the ring of integer (z, +,.>. It is not a division ring as it does not have multiplicative inverse.

Q.7. In a ring (R,+,.> Prove that

(a) a (b–c) = a.b.–a.c

(b) (a–b)c = a.c. –b.c **2011**

Proof.: (i) $a.\ (b-c) = a.\ [b+(-c)]$

$= a.b + a.(-c)$

by righ distribution law

$= a.b + (-ac)$

$= ab - ac$

(ii) $(b-c).a = [b+(-c)].a$

$= b.c + (-c).a$

by left distribution law

$(b-c).a = b.c - c.a$

Q.8. Define Field. **2005**

Sol^n.: If every dement $a \neq 0$ of anintegral domain has a multiplicative inverse a^{-1} in the integral domain, then it is called a field and is denoted by F.

A ring F whose non-zero elements form an

multiplication group is known as a field.

Show that the set of all residue classes modulo p is an integral domain iff p is a prime.

2015

If I be an given ring the we have follwoing two cases:

Case I : If p is prime and $\bar{a}, \bar{b} \in I(\rho)$ such that $\bar{a}.\bar{b} = \bar{0}$,

then $ab \equiv 0 \pmod{\rho} \Rightarrow ab$ is divisible by p

$\therefore$ Either a is divisible by p or b.

because p is prime either

$$a \equiv 0 \pmod{\rho}$$

or $$b \equiv 0 \pmod{\rho}$$

Therefore $\bar{a} = \bar{0}$, or $\bar{b} = \bar{0}$

$\therefore$ I (p) is an integral domain

Case-II : If p is not prime and $p = r_1 r_2$

where $1 < r_1 < p$ & $1 < r_2 < p$

then in I (p), we have

$$\bar{r}.\bar{r_2} = \overline{r_1 r_2} \equiv 0 (\text{mod } p)$$

where $\bar{r_1} \neq \bar{0}$, $\bar{r_2} \neq \bar{0}$

Then I (p) is not an integral domain. Hence I (p) is an integral domain. If p is prime.

****