RINGS

Def^n: An algebraic structure $(R, +, \cdot)$ where R is a non-zero empty set and $(+)$ & $(\cdot)$ are two binary operation on R is called a ring if it satisfies the following properties:

(I) $(R, +)$ is an abelian group.

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

(ii) **Associative property:-** $\forall\ a, b, c \in R \Rightarrow (a+b)+c = a+(b+c)$

(iii) **Existence of Identity:-** $\exists\ 0 \in R$ s.t $a+0 = 0+a = a\ \forall\ a \in R$.

then '0' is the identity ell. in R.

(iv) **Existence of Inverse:-** For each $a \in R$, $\exists\ -a \in R$ s.t $a+(-a) = (-a)+(a) = 0$

then $(-a)$ is called inverse of a in R.

(v) **Commutative prop:-** $\forall\ a, b \in R \Rightarrow a+b = b+a$.

(II) $(R, \times)$ is a **semi-group:-**

(i) **Closure prop:-** $\forall\ a, b \in R \Rightarrow a, b \in R$

(ii) **Associative prop:-** $\forall\ a, b, \in R \Rightarrow (ab)c = a(bc)$

(III) **Distributive laws:-** $\forall\ a, b, c \in R$

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

(ii) $(b+c) \cdot a = b \cdot a + c \cdot a$ (RDL)

(*) **Ring with unity:-** A ring R which contains the multiplicative identity (called unity) i.e. called a ring with unity i.e. if $1 \in R$ s.t $a \cdot 1 = 1 \cdot a = a\ \forall a \in R$. then, the ring R is called a ring with unity.

(*) **Ring without unity:-** A ring R which does not contain multiplicative identity is called a ring without unity.

(*) Commutative ring :- If in a ring R, the commu property w.r.t multiplication is satisfied then the ring R is called commutative ring.

i.e. $\forall\ a, b \in R \Rightarrow a \cdot b = b \cdot a$

then, the ring R is called a commutative ring.

(*) Division Ring or Skew Field :- If in a ring R, the non-zero elts. form a group w.r.t multiplication a ring R is called a Division Ring.

(or)

A ring R is a division ring if

(i) R has atleast two elements.

(ii) R has unity.

(iii) Each non-zero element of R has multiplicative inverse

(*) Zero Divisor of a Ring :- Let $(R, +, \cdot)$ be a ring If there exist $a, b \in R$, where $a \neq 0$, $b \neq 0$, and $ab = 0$, then, R is called ring with zero divisors.

(or) a, b are called zero divisors.

Here, 'a' is called the left zero divisor and 'b' is called the right-zero divisors.

(Or)

A non-zero elt. of a ring R is called a zero divisor (or) a divisor of zero if $\exists$ an elt. $b \neq 0\ (\in R)$ s.t either $ab = 0$ or $ba = 0$.

(*) Ring without zero Divisors :- A ring which is not with zero divisors is called ring without zero divisor ie. if $a \neq 0$, $b \neq 0$, then $ab \neq 0$.

or

R is said to have no zero divisors if ⑤
R and $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Examples (1.) The ring of integers $(\mathbb{Z}, +, \cdot)$ has no zero divisors.
For, $a, b \in \mathbb{Z}$ and $ab = 0 \Rightarrow a = 0$ or $b = 0$.

(2.) The ring $(R, +, \cdot)$ where R = set of 2×2 matrices whose elts. are real no's. has zero divisors.
Since, $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq 0$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \neq 0 \in R$

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

④ **Integral Domain:-** A commutative ring with unity and without zero divisors is called an I.D.
i.e. A ring R is an Integral Domain.
if (i) R is commutative
(ii) R has unity.
(iii) R is without zero divisors.

⑤ **Field:-** A commutative division ring is called a field. (i.e. abelian gp. w.r.t multiplication)
i.e. A ring R is said to be a field if it has atleast two elements and (i) is commutative
(ii) has unity
(iii) every non-zero elt of R is invertible w.r.t $(\cdot)$.

Some Elementary properties of Rings:-
If R is a ring and $0, a, b \in R$, then
(i) $0 \cdot a = a0 = 0$.
(ii) $a(-b) = (-a)b = -(ab)$
(iii) $(-a)(-b) = ab$ and
(iv) $a(b - c) = ab - ac$.

Examples:-

(1) Let $R = \{0\}$ and $+, \cdot$ be the binary operations by $0+0 = 0$ and $0 \cdot 0 = 0$, then $(R, +, \cdot)$ is clearly a ring, called the null ring or zero ring.

(2) I = set of integers

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

$\therefore$ closure property is satisfied.

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

$\therefore$ Associative prop. is satisfied.

(iii) $\forall\, a \in I \;\; \exists\, -a \in I$ s.t $a+(-a) = (-a)+a = 0$.

$\therefore$ '$-a$' is the inverse of 'a' in I.

Inverse property is satisfied.

(iv) $\forall\, a, b \in I \Rightarrow a+b = b+a$.

$\therefore$ Commutative property is satisfied.

$\therefore$ $(I, +)$ is an abelian gp.

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

$\therefore$ closure prop. is satisfied.

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

$\therefore$ $(I, \cdot)$ is a semi-group.

(III) $\forall\, a, b, c \in I$

(i) $a \cdot (b+c) = ab + ac$ (LDL)

(ii) $(b+c) \cdot a = ba + ca$ (RDL)

$\therefore$ Distributive laws are satisfied.

$\therefore$ $(I, +, \cdot)$ is a ring.

(IV) $\exists\, 1 \in I$ s.t $a \cdot 1 = 1 \cdot a \;\; \forall\, a \in I$

$\therefore$ Identity elt = ~~I~~ $1 \in I$

$\therefore$ $(I, +, \cdot)$ is a ring with unity.

$a, b \in I \Rightarrow ab = ba$

Commutative property is satisfied.

$(I, +, \cdot)$ is a commutative ring with unity.

I. $\forall\ a, b \in I$

$ab = 0 \Rightarrow a = 0$ or $b = 0$

$\therefore$ I does not contain zero divisors.

$\therefore (I, +, \cdot)$ is an integral domain.

VII. $\forall\ a \neq 0 \in I$, $\nexists\ \frac{1}{a} \notin I$ s.t $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

$\therefore$ Inverse property is not satisfied w.r.t $(\cdot)$.

so $(I, +, \cdot)$ is not a field.

(8) The set M of all $n \times n$ matrices with their elts as real no's. (rational no's, complex no's, integers) is a non-commutative ring with unity w.r.t $(+)$ and $(\cdot)$.

i.e. $M = \{A = [a_{ij}]_{n \times n} ;\ a_{ij} \in R\}$

Soln I. (i) $\forall\ A, B \in M$

$\Rightarrow A + B \in M$

$\therefore$ closure prop. is satisfied.

(ii) $\forall\ A, B, C \in M$

$(A+B) + C = A + (B+C)$

so, Associative prop. is satisfied.

(iii) $\exists\ B = O_{n \times n} \in M$ s.t

$A + B = B + A = A \quad \forall\ A \in M$

$\therefore$ Identity element $= O_{n \times n} \in A$

$\therefore$ Identity prop. is satisfied.

(iv) $\forall\ A \in M$ $\exists\ -A \in M$

s.t $A + (-A) = (-A) + A = O$

$\therefore$ Inverse of A is $-A$

$\therefore$ Inverse prop. is also satisfied.

II. (i) $\forall A, B \in M \Rightarrow A \cdot B \in M$

$\therefore$ closure prop. is satisfied.

(ii) $\forall A, B, C \in M$

$\Rightarrow (A \cdot B)C = A(BC)$

$\therefore$ Associative prop. is satisfied.

III. $\forall A, B, C \in M$

(i) $A \cdot (B+C) = AB + AC$

(ii) $(B+C) \cdot A = BA + CA$

Distributive prop. is satisfied.

$\therefore (M, +, \cdot)$ is a ring.

IV. $\exists B \in M$ I (unit Matrix)

s.t $A \cdot B = B \cdot A = A \quad \forall A \in M$

$\therefore$ Identity elt = I (Identity matrix)

$\therefore (M, +, \cdot)$ is a ring with unity.

V. $\forall A, B \in M$

$\Rightarrow A \cdot B \neq B \cdot A$

$\therefore$ Commutative prop. is not satisfied w.r.t $(\cdot)$.

$\therefore (M, +, \cdot)$ is non-commutative ring with unity.

(4) $F = \{ b\sqrt{2} : b \text{ is a rational no.} \}$

Soln let $a, \sqrt{2}, b\sqrt{2} \in F$ where $a, b \in Q$.

$\Rightarrow a\sqrt{2} + b\sqrt{2} = (a+b)\sqrt{2} \in F$

$(\because a, b \in Q \Rightarrow a+b \in Q)$

$\therefore$ Closure prop. is satisfied w.r.t '+'.

(ii) let $a\sqrt{2}, b\sqrt{2} \in F$; $a, b \in Q$

$\Rightarrow a\sqrt{2} \cdot b\sqrt{2} = ab(2) \notin F$

so, multiplication ie $(\cdot)$ is not a binary operation on F.

$\mathbb{Q}[\sqrt{2}] = \{ a+b\sqrt{2} \mid a,b \in \mathbb{Q} \} \subseteq R$

$(+)$ & $(\cdot)$ are binary operations on $\mathbb{Q}\sqrt{2}$.

I (i) Closure prop: let $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Q}\sqrt{2}$ s.t $a,b,c,d \in \mathbb{Q}$

then $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in \mathbb{Q}\sqrt{2}$

$(\because a+c, b+d \in \mathbb{Q})$.

$\therefore$ closure property is satisfied.

(ii) Associative property:- let $x,y,z \in \mathbb{Q}\sqrt{2}$

Choosing $x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$, $z = e+f\sqrt{2}$

where $a,b,c,d,e,f \in \mathbb{Q}$.

$\therefore (x+y)+z = x+(y+z)$ (by Associative prop on R)

$\therefore$ Associative prop. is also satisfied.

(iii) Existence of left identity:- $\forall\ x = a+b\sqrt{2} \in \mathbb{Q}\sqrt{2}$ s.t $a,b \in \mathbb{Q}$

$\exists\ y = 0+0\sqrt{2}$; $0 \in \mathbb{Q}$

s.t $y+x = (0+0\sqrt{2}) + (a+b\sqrt{2})$

$= (0+a) + (0+b)\sqrt{2}$

$= a+b\sqrt{2}$

$= x$

$\therefore$ Identity elt $= 0+0\sqrt{2} = 0 \in \mathbb{Q}\sqrt{2}$.

(iv) Existence of left inverse:- $\forall\ a+b\sqrt{2} \in \mathbb{Q}\sqrt{2}\ (a,b \in \mathbb{Q})$

$\exists\ -a-b\sqrt{2} \in \mathbb{Q}$ $(-a, -b \in \mathbb{Q})$

s.t $(-a-b\sqrt{2}) + (a+b\sqrt{2}) = (-a+a) + (-b+b)\sqrt{2}$

$= 0+0\sqrt{2} = 0$

$(\because -a+a = 0,\ -b+b = 0)$

$\therefore$ Inverse of $a+b\sqrt{2} = -a-b\sqrt{2} \in \mathbb{Q}\sqrt{2}$.

(v) Commutative property:- $\forall\ x,y \in \mathbb{Q}\sqrt{2}$

$\Rightarrow x+y = y+x$ (by commutative prop of R)

$\therefore$ Commutative prop. is satisfied.

$\therefore$ $(\mathbb{Q}\sqrt{2}, +)$ is an abelian gp.

$\therefore x \cdot y = y \cdot x$ (by commutative prop. of R)

$\therefore$ Commutative prop. is satisfied in $\mathbb{Q}\sqrt{2}$.

So, $(\mathbb{Q}\sqrt{2}, +, \cdot)$ is a commutative

II (i) Closure prop:- let $x = a+b\sqrt{2}$, $y = c+d\sqrt{2} \in \mathbb{Q}$
s.t $a, b, c, d \in \mathbb{Q}$.

then $x \cdot y = (a+b\sqrt{2})(c+d\sqrt{2})$
$= (ac+2bd) + (ad+bc)$
$\in \mathbb{Q}\sqrt{2}$ ($\because ac+2bd, ad+bc \in \mathbb{Q}$)

$\therefore$ Closure prop. is satisfied.

(ii) Let $x, y, z \in \mathbb{Q}\sqrt{2} \subseteq R$
Choosing $x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$, $z = e+f\sqrt{2}$;
$a, b, c, d, e, f \in \mathbb{Q}$

s.t $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (By Associative prop. of R)

$\therefore (F, \cdot)$ is a semi-group.

III. Let $x, y, z \in \mathbb{Q}\sqrt{2} \subseteq R$
$x \cdot (y+z) = x \cdot y + y z$ (by LD)
$(y+z) \cdot x = y \cdot x + z \cdot x$ (by RD)

$\therefore$ Distributive laws are satisfied.

$\therefore (\mathbb{Q}\sqrt{2}, +, \cdot)$ is a ring.

IV. Identity property:- $\exists\ 1+0\sqrt{2} = 1 \in \mathbb{Q}\sqrt{2}$, $0, 1 \in \mathbb{Q}$
s.t $(1+0\sqrt{2})(a+b\sqrt{2}) = a+b\sqrt{2}$
$\forall\ a+b\sqrt{2} \in \mathbb{Q}\sqrt{2}$
& $a, b \in \mathbb{Q}$

$\therefore$ Identity elt w.r.t $(\cdot)$ is $1 = 1+0\sqrt{2}$

So, Identity property is satisfied.

(i) $\therefore (\mathbb{Q}\sqrt{2}, +, \cdot)$ is a ring with unity.

V Commutative prop:- Let $x, y \in \mathbb{Q}\sqrt{2} \subseteq R$
Choosing $x = a+b\sqrt{2}$ & $y = c+d\sqrt{2}$; $a, b, c, d \in \mathbb{Q}$.

$y = y \cdot x$ (by commutative prop. of R)
commutative prop. is satisfied. in $\mathbb{Q}\sqrt{2}$.
$(\mathbb{Q}\sqrt{2}, +, \cdot)$ is a commutative ring with unity.

I. Let $x, y \in \mathbb{Q}\sqrt{2} \subseteq R$
choosing $x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$; $a, b, c, d \in \mathbb{Q}$
$\therefore x \cdot y = 0 \Rightarrow x = 0$ or $y = 0$.
$\therefore \mathbb{Q}\sqrt{2}$ does not contain zero divisors.
$\therefore (\mathbb{Q}\sqrt{2}, +, \cdot)$ is an integeal domain.

VII. let $a+b\sqrt{2} \neq 0 \in \mathbb{Q}\sqrt{2}$ ($\because a \neq 0, b \neq 0 \in \mathbb{Q}$)
s.t $(c+d\sqrt{2})(a+b\sqrt{2}) = 1$

$$\Rightarrow c+d\sqrt{2} = \frac{1}{a+b\sqrt{2}}$$

$$= \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

$$= \frac{a}{a^2-2b^2} + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in \mathbb{Q}\sqrt{2}$$

$$\left(\because \frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q} \text{ & } a^2-2b^2 \neq 0\right)$$

$\therefore \exists \frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}\sqrt{2} \subseteq R$.

s.t $\left(\frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2}\right)(a+b\sqrt{2}) = 1$
$\forall\ a+b\sqrt{2} \in F$.

$\therefore$ Inverse of $a+b\sqrt{2}$ is $\frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}\sqrt{2}$.

$\therefore$ Every non-zero elt. of $\mathbb{Q}\sqrt{2}$ has inverse w.r.t $(\cdot)$.

$\therefore$ Inverse prop. is satisfied.

$\therefore (\mathbb{Q}\sqrt{2}, +, \cdot)$ is a field.

(6) $F = I[i]$ = the set of gaussian integers
$= \{ a+bi \mid a, b \in I \} \subseteq C$
prove that $(F, +, \cdot)$ is an ID but not a field

(7) Show that the set of integers w.r.t two binary operations '$*$' & '$\circ$' defined by $a * b = a + b - 1$
$a \circ b = a + b - ab$
$\forall\ a, b \in I$
is a Commutative ring.

Soln: $\forall\ a, b \in I$,
$a * b = a + b - 1 \rightarrow (1)$
and $a \circ b = a + b - ab \rightarrow (2)$

I. from (1)
(i) we have $a * b = a + b - 1 \in I$
$\therefore$ '$*$' is closed in I.

(ii) $\forall\ a, b, c \in I$
$(a * b) * c = a * (b * c)$.
since, $(a * b) * c = (a + b - 1) * c$
$= (a + b - 1) + c - 1$
$= a + b + c - 2$
$a * (b * c) = a * (b + c - 1)$
$= a + (b + c - 1) - 1$
$= a + b + c - 2$
$\therefore$ Associative prop. is satisfied.

(iii) Existence of left identity:- $\forall\ a \in I$
$\exists\ b \in I$
s.t $b * a = a$
$b + a - 1 = a$
$\Rightarrow b = 1$
$\therefore \forall\ a \in I, \exists\ 1 \in I$ s.t $1 * a = a$
$\therefore$ 1 is the identity in I w.r.t $*$.

Existence of left inverse :- $\forall\ a \in I$, $\exists\ b \in I$

s.t $b * a = 1$

$\Rightarrow b + a - 1 = 1$

$\Rightarrow b = 2 - a \in I$

$\therefore \forall\ a \in I$, $\exists\ b = 2 - a \in I$

s.t $(b - a) * a = 1$

$\therefore b = 2 - a$ is the inverse of 'a' in I w.r.t $(*)$

(vi) Commutative property :- $\forall\ a, b \in I$, $a * b = b * a$

Since, $a * b = a + b - 1$

$= b + a - 1$

$= b * a$

$\therefore$ $(*)$ is commutative in I.

$\therefore (I, *)$ is abelian gp.

II. From (2), (i) Closure prop :- $\forall\ a, b \in I$

$a \circ b = a + b - ab \in I$

'$\circ$' is closed in I

(ii) $\forall\ a, b, c \in I$

$a \circ (b \circ c) = (a \circ b) \circ c$

Since, $(a \circ b) \circ c = (a + b - ab) \circ c$

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

$= a + b + c - ab - ac - bc + abc$

& $a \circ (b \circ c) = a \circ (b + c - bc)$

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

$= a + b + c - ab - bc - ac + abc$

$\therefore$ '$\circ$' is associative in I.

$\therefore (I, \circ)$ is a semi-group.

III. Left Distributive law :- $\forall\ a, b, c \in I$

$\Rightarrow a \circ (b * c) = a \circ (b + c - 1)$

$= a + (b + c - 1) - a(b + c - 1)$

$= a + b + c - 1 - ab - ac + a$

$= (a + b - ab) + (a + c - ac - 1)$

$= (a \circ b) + (a \circ c) - 1 = (a \circ b) * (a \circ c)$

(∵ Distributive law is satisfied.
∴ $(I, *, o)$ is a ring.

IV. Commutative Prop^{n}:- $\forall\ a, b \in I$

$\Rightarrow a o b = a + b - ab$
$= b + a - ba$
$= boa$

(∵ '+' is a commutative in I.
∴ $(I, *, o)$ is a commutative.

Def^{n} Cancellation Laws in a Ring:- In a ring R, for $a, b, c \in R$ if $a \neq 0$, $ab = ac \Rightarrow b = c$ (LCL)

and $a \neq 0$, $ba = ca \Rightarrow b = c$ (RCL)

then, we say that cancellation laws hold in R.

Result 1.) If R is a ring with unit element and $x \neq 0 \in R$ and a unique element $y \in R$ exists s.t $xyx = x$. Show that $xy = yx = 1$.

Sol^{n}: $x \neq 0$ and $xyx = x$

$\Rightarrow x \neq 0$ and $(xy)x = 1 \cdot x$

$\Rightarrow xy = 1$ (By RCL)

Now, $x \neq 0$ and $xyx = x$

$\Rightarrow x \neq 0$ & $x(yx) = x \cdot 1$

$\Rightarrow yx = 1$ (By LCL)

$\therefore xy = yx = 1$.

2.) Let R be a commutative ring with unity. Then R is an I.D iff $ab = ac \Rightarrow b = c$.

where $a, b, c \in R$ and $a \neq 0$.

(OR)

A commutative ring R with unity is an ID iff the cancellation laws holds in R.

Suppose R is an ID, then we have to show the cancellation laws hold in R.

$a, b, c \in R$ and $a \neq 0$

we have $ab = ac$

$\Rightarrow a(b-c) = 0 \rightarrow (1)$

Since R is I.D

i.e. R is a Commutative ring with unity and has no zero divisors.

$\therefore$ From (1), either $a = 0$ or $b - c = 0$

but it is given that $a \neq 0$

$\therefore b - c = 0$

$\Rightarrow b = c$

Similarly, we prove that $a, b, c \in R$, $a \neq 0$,

$ba = ca$

$\Rightarrow b = c$

$\therefore$ The Cancellation laws holds in R.

Conversely: Suppose that the cancellation laws hold in R. We prove that R is an I.D.

For this, we are enough to prove that R has no zero divisors.

If possible, let R has zero divisors then

$\exists\ a, b \in R$ s.t $a \neq 0, b \neq 0$ and $ab = 0$

Now, we have $a \neq 0$, $ab = 0$

$\Rightarrow a \neq 0$, $ab = a0$

$\Rightarrow b = 0$ (By LCL)

which is contradiction.

$\therefore$ R has no zero divisors.

$\therefore$ R is an ID.

Note: The Cancellation laws may not hold in an arbitrary ring. Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ & $B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ & $C = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ be three elements in the ring M_2 of all 2×2 matrices over the integers. Then $AC = \begin{bmatrix} 2 & 0 \\ 2 & 0 \end{bmatrix} = BC$ but $A \neq B$.

Thm: A division ring has no zero divisors (i.e. without zero divisors).

Pf: Let $(R, +, \cdot)$ be a division ring
i.e. in a ring R, the non-zero elements form a group w.r.t multiplication.
Let $a, b \in R$ and $a \neq 0$.
Since, R is a division ring.
for $a \neq 0 \in R \Rightarrow a^{-1}$ exists in R.
$\therefore aa^{-1} = a^{-1}a = 1$.
Now, we have $ab = 0$

$$\Rightarrow a^{-1}(ab) = a^{-1}0$$
$$\Rightarrow (a^{-1}a)b = 0$$
$$\Rightarrow 1b = 0$$
$$\Rightarrow b = 0$$

$\therefore a, b \in R$, $a \neq 0$ and $ab = 0 \Rightarrow b = 0$.
Similarly, we can prove that $a, b \in R$, $b \neq 0$ and

$$ab = 0$$
$$\Rightarrow a = 0.$$

$\therefore a, b \in R$ and $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$
$\therefore R$ has no zero divisors.

Thm: A field has no zero divisors.
Pf: Same as the proof of the above thm.

Subrings

Defn: Let R be a ring. S be a non-empty subset of R (i.e. $S \subseteq R$), if S is a ring w.r.t binary operations defined in R, then S is called a subring of R.

Note: If $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$ then, $(S, +)$ is a subgroup of the group $(R, +)$.

S be a non-empty subset of a ring R. Then S is a sub-ring of R iff $\forall a,b \in S \Rightarrow a-b \in S$ and $ab \in S$.

Necessary Cond^n: Let S be a subring of R.
By the def^n of 'S' is a ring w.r.t binary operations of R.

(i) $\forall a,b \in S \Rightarrow a \in S, -b \in S$ (inverse prop. of S)
$\Rightarrow a+(-b) \in S$ (by closure prop.)
$\Rightarrow a-b \in S$

(2) $\forall a,b \in S \Rightarrow a.b \in S$ (by closure prop.)

$\therefore \forall a,b \in S \Rightarrow a-b \in S$ & $ab \in S$.

Sufficient Cond^{n}s – Let $S \subseteq R$
$\forall a,b \in S \Rightarrow a-b \in S$ → (1) & $ab \in S$ → (2).

(i) $a, a \in S \subseteq R$
$\Rightarrow a-a \in S \subseteq R$ (By (1))
$\Rightarrow 0 \in S \subseteq R$
$\therefore \forall a \in S \subseteq R, \exists\ 0 \in S \subseteq R$ s.t $0+a = a = a+0$.
$\therefore$ 0 is the identity element in S.
$\therefore$ Identity prop. is satisfied.

(ii) $0 \in S, a \in S \Rightarrow 0-a \in S$ (By (1))
$\Rightarrow -a \in S$
$\therefore \forall a \in S, \exists\ -a \in S$ s.t $a+(-a) = (-a)+a = 0$. (By inverse of R)
$\therefore$ Inverse prop. is satisfied in S.
$\therefore$ Inverse of a is $-a$ in S.

(iii) $\forall b \in S \Rightarrow -b \in S$ (By ii)
$\therefore \forall a, -b \in S \Rightarrow a-(-b) \in S$ (hyp)
$\Rightarrow a+b \in S$
$\therefore a,b \in S \Rightarrow a+b \in S$
$\therefore$ closure prop. in S is satisfied w.r.t (+).

Def:- Let $(F,+,\cdot)$ be a field and $(S,+,\cdot)$ be a of F. If $(S,+,\cdot)$ is a field then we say that 'S' is a subfield of F.

(or)

Let F be a field and S is a non-empty subset of F. If S is a field w.r.t binary operations defined in F then S is called a sub-field of F.

Note:- (1) If $(S,+,\cdot)$ is a subfield of $(F,+,\cdot)$ then

(a) $(S,+)$ is a subgp. of $(F,+)$

(b) $(S-\{0\},\cdot)$ is a subgp. of $(F-\{0\},\cdot)$

(2) If $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ then

(a) $(S,+)$ is a subgp. of $(R,+)$

(b) $(S,\cdot)$ is a sub semi-gp of $(R,\cdot)$

and (c) distributive laws holds.

Examples:- → The set of even integers is a subring of the ring of integers under $(+)$ and $(\cdot)$.

→ $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ are subrings of the ring of real no's. $(\mathbb{R},+,\cdot)$.

Let $(\mathbb{Q},+,\cdot)$ be the ring of rational no's.

If $S=\left\{\frac{a}{2} \mid a\in\mathbb{Z}\right\}$, then S is a non-empty subset of $\mathbb{Q}$ and $(S,+)$ is a subgp. of $(\mathbb{Q},+)$.

but for $\frac{1}{2}\in S$

we have $\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}\notin S$

∴ multiplication $(\cdot)$ is not a binary operation on S.

∴ $(S,+,\cdot)$ is not a subring of $(\mathbb{Q},+,\cdot)$.

$a, b, c \in S \subseteq R$

$a+(b+c) = (a+b)+c$ (by associative prop. of R)

∴ Associative prop. in S is satisfied.

(v) $a, b \in S \subseteq R \Rightarrow a+b = b+a$ (by commutative prop of R)

∴ Commutative prop. in S is satisfied.

∴ $(S, +)$ is an abelian gp.

II. (i) $\forall\ a, b \in S \Rightarrow ab \in S$ (By ②)

∴ closure prop. is satisfied.

(ii) $\forall\ a, b, c \in S \subseteq R \Rightarrow (ab)c = a(bc)$ (By Ass. prop of R)

∴ $(\cdot)$ is associative in S.

∴ $(S, \cdot)$ is a semi-group.

III. $\forall\ a, b, c \in S \subseteq R \Rightarrow a\cdot(b+c) = a\cdot b + a\cdot c$ & $(b+c)\cdot a = ba + ca$ ['$\cdot$' is distributive in R]

Thm 6- The intersection of two subrings of a ring R is a subring of R.

Pf:- Let S_1 & S_2 are two subrings of a ring R.

Let $S = S_1 \cap S_2$

Let $a, b \in S \Rightarrow a, b \in S_1 \cap S_2$

$\Rightarrow a, b \in S_1$ and $a, b \in S_2$

$\Rightarrow a-b \in S_1$ & $a-b \in S_2$ (∵ S_1 & S_2 are two subrings of R)

$\Rightarrow a-b \in S_1 \cap S_2$

Also, $ab \in S_1$ & $ab \in S_2$

$\Rightarrow ab \in S_1 \cap S_2$

So, $a-b \in S_1 \cap S_2$, $ab \in S_1 \cap S_2$

$\Rightarrow a-b \in S$ & $ab \in S$

∴ $S = S_1 \cap S_2$ is a subring of R.

H.P

Thm:- Intersection of arbitrary no. of subrings is a subring of R.

Pf:- Let $S_1, S_2 \dots S_n \dots$ are subrings of R

Let $S = S_1 \cap S_2 \dots \cap S_n \cap \dots$

ie $S = \bigcap_{i \in N} S_i$

Let $a, b \in S \Rightarrow a, b \in S_1 \cap S_2 \cap \dots \cap S_n \cap \dots$

$\Rightarrow a, b \in S_i \ \forall \ i \in N$

$\Rightarrow a-b \in S_i$ & $ab \in S_i$ ($\because$ each S_i is a subring of R)

$\Rightarrow a-b \in \bigcap_{i \in N} S_i$, $ab \in \bigcap_{i \in N} S_i$

$\Rightarrow a-b \in S$, $ab \in S$

$\therefore S = S_1 \cap S_2 \dots \cap S_n \cap \dots$ is a subring of R

$\therefore$ Intersection of arbitrary no. of subrings is a subring.

Thm:- Union of two subrings of R need not be a subring of R.

Soln:- Let R = I (the ring of integers)

Let $S_1 = \{2n : n \in I\} = \{\dots -6, -4, -2, 0, 2, 4, 6 \dots\}$

$S_2 = \{3n : n \in I\} = \{\dots -9, -6, -3, 0, 3, 6, 9 \dots\}$

be two subrings of R.

Now, $2 \in S_1, 3 \in S_2 \Rightarrow 2, 3 \in S_1 \cup S_2$

But $2+3 = 5 \notin S_1 \cup S_2$

$\therefore S_1 \cup S_2$ is not closed under addition.

$\therefore S_1 \cup S_2$ is not a subring of R.

Thm:- If S_1 and S_2 are two subrings of a ring R then $S_1 \cup S_2$ is a subring of R iff $S_1 \subset S_2$ or $S_2 \subset S_1$.

Pf:- Let $S_1 \cup S_2$ be a subring of R.

Now, we prove that $S_1 \subset S_2$ or $S_2 \subset S_1$

If possible, suppose that $S_1 \not\subset S_2$ or $S_2 \not\subset S_2$.

$S_1 \not\subset S_2$ but $a \notin S_2$

Let $a \in S_1$

$S_2 \not\subset S_1$

So, let $b \in S_2$ but $b \notin S_2$.

Now, we have $a \in S_1$, $b \in S_2$

$\Rightarrow a, b \in S_1 \cup S_2$

$\Rightarrow a+b \in S_1 \cup S_2$ ($\because S_1 \cup S_2$ is a ring)

$\Rightarrow$ either $a+b \in S_1$ or $a+b \in S_2$

Now, we have

$a \in S_1$, $a+b \in S_1$

$\Rightarrow (a+b) - a \in S_1$ ($\because S_1$ is a subring of R).

$\Rightarrow b \in S_1$

which is a contradiction

Now, we have

$b \in S_2$, $a+b \in S_2$

$\Rightarrow (a+b) - b \in S_2$

$\Rightarrow a \in S_2$

which is a contradiction.

$\therefore$ Our supposition that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$ is wrong.

So, either $S_1 \subset S_2$ or $S_2 \subset S_1$.

Converse:- Suppose that $S_1 \subset S_2$ or $S_2 \subset S_1$.

Prove that $S_1 \cup S_2$ is a subring.

Since, $S_1 \subset S_2 \Rightarrow S_1 \cup S_2 = S_2$

& S_2 is a subring of R

$\Rightarrow S_1 \cup S_2$ is a subring of R.

Since, $S_2 \subset S_1 \Rightarrow S_1 \cup S_2 = S_1$

& S_1 is a subring of R

$\Rightarrow S_1 \cup S_2$ is a subring of R.

H.P.

Characteristics of a Ring:- A ring R is said to be of finite characteristic if there exists a positive integer 'n' s.t $na = 0 \ \forall \ a \in R$.

→ If a ring R is of finite characteristic, then the characteristic of R is defined as the smallest positive integer 'p' s.t $pa = 0 \ \forall \ a \in R$.

We write it as $\text{char}(R) = p$.

→ A ring R is said to be of characteristic zero or infinite if there exists no positive integer 'n' s.t $na = 0 \ \forall \ a \in R$.

Examples: $\text{Char } \mathbb{Z} = 0$, $\text{Char } \mathbb{Q} = 0$, $\text{Char } \mathbb{R} = 0$

$\text{Char } \mathbb{Z}_2 = 2$, where $\mathbb{Z}_2 = \{0, 1\}$

Since, $1 +_2 1 = 0$

$2 +_2 0 = 0$.

Thm: If R is a ring with unity element, then R has characteristic $p > 0$ iff p is the least positive integer s.t $p1 = 0$.

Pf: Let char. of ring $R = p$ $(p > 0)$

$\therefore$ By defn, $pa = 0 \ \forall \ a \in R$, where p is the least positive integer.

& In particular, $p1 = 0$.

Conversely: Suppose that p is the least positive integer such that $p1 = 0$

Now, for any $a \in R$, we have

$$pa = a + a + \cdots + a \ (p \text{ times})$$
$$= a(1 + 1 + \cdots + 1) \ (p \text{ times})$$
$$= a(p1) \quad (\because p1 = 0, \text{ where } p \text{ is the least positive integer})$$
$$= a(0)$$

$\therefore pa = 0 \ \forall \ a \in R$, where p is the least positive integer.

$\therefore$ Char. of the ring $R = p$.

Thm:- The characteristic of an integral domain is either a prime or zero.

Pf:- Let $(R,+,\cdot)$ be an I.D.

If char of $R = 0$, then, there is nothing to prove.

Let char $R = p$ $(p \neq 0)$.

then, 'p' is the least positive integer such that

$$pa = 0 \quad \forall\, a \in R \rightarrow (1)$$

Now, we prove that 'p' is prime.

If possible, suppose that p is not prime, then,

$p = mn$; $1 < m, n < p$.

Eq^n (1) implies, $pa = 0 \quad \forall\, a \in R$

$$\Rightarrow (mn)a = 0$$

$$\Rightarrow (mn)ab = ob, \quad b \in R$$

$$\Rightarrow ab + ab + \cdots + ab \ (mn \text{ times}) = 0 \quad \forall\, a, b \in R$$

$$\Rightarrow \underbrace{(a+a+\cdots+a)}_{m \text{ times}} \underbrace{(b+b+\cdots+b)}_{n \text{ times}} = 0 \quad \forall\, a, b \in R$$

$$\Rightarrow (ma)(nb) = 0 \quad \forall\, a, b \in R \rightarrow (2)$$

Since, R is an I.D

$\therefore$ R is without zero divisors.

$\therefore$ (1) implies either $ma = 0 \ \forall\, a \in R$ or $nb = 0 \ \forall\, b \in R$ where $1 < m < p$, $1 < n < p$.

$\therefore$ these two statements contradict the fact that 'p' is the least positive integer such that $pa = 0 \ \forall\, a \in R$

$\therefore$ p must be a prime no.

Thm The characteristic of a field is either zero or a prime no.

Pf: Since, every field is an I.D.

So, by above thm, the characteristic of a field is either zero or prime.

Thm The characteristic of a division ring is either zero or prime.

Pf:- The division ring has no zero divisors. so, result follows from the thm, "The characteristic of an integral domain is zero or prime."

→ If F is a field of characteristic p, p is a prime then $(a+b)^p = a^p + b^p \ \forall\ a,b \in F$.

Soln: Since, F is a field.
& char F = p; a prime
so, $px = 0 \ \forall\ x \in F$. → (1)
where 'p' is the least positive integer.

Now, we have $(a+b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{2!}a^{p-2}b^2 + \cdots + pab^{p-1} + b^p$

$= a^b + b^p$ (By (1))

Hence.

→ If R is a non-zero ring so that $a^2 = a \ \forall\ a \in R$ prove that characteristic of R = 2.

Soln: Since, $a^2 = a \ \forall\ a \in R$
so, we have $(a+a)^2 = a+a$
$\Rightarrow (a+a)(a+a) = a+a$
$\Rightarrow a(a+a) + a(a+a) = a+a$
$\Rightarrow (a^2+a^2) + (a^2+a^2) = a+a$
$\Rightarrow (a+a) + (a+a) = a+a$ ($\because a^2 = a$)
$\Rightarrow (a+a) + (a+a) = (a+a) + 0$
$\Rightarrow a+a = 0$ (By LCL)
$\Rightarrow 2a = 0$

$\therefore$ for every $a \in R$, $2a = 0$
further, $a \neq 0$, $1a = a \neq 0$ so, 2 is the least +ve int. s.t $2a = 0 \ \forall\ a \in R$.
so, char R = 2.