Ring

Definition :-

Suppose R is a non empty set equipped with two binary operations called addition & multiplication & denoted by '+' & '.' respectively.

ie for all $a, b \in R$ we have $a+b \in R$ & $a.b \in R$. Then this algebraic structure $(R, +, \cdot)$ is called a Ring, if the following postulates are satisfied

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

(ii) $(R, \cdot)$ is a semigroup. ($\cdot$ is associative)

(iii) Multiplication is distributive with respect to addition.

ie for all a, b, c in R,

(i) $a \cdot (b+c) = a \cdot b + a \cdot c$ [left distributive law]

& (ii) $(b+c) \cdot a = b \cdot a + c \cdot a$ [Right " "]

(i) Addition is closed :-

$a+b \in R \quad \forall\, a, b \in R$.

(ii) Addition is associative :-

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

(iii) There exists an element denoted by 0 in R such that

$0+a = a = a+0 \quad \forall\, a \in R$.

(iv) To each element a in R there exists an element $-a$ in R such that

$(-a)+a = 0$.

(v) Multiplication is associative.

i.e. $a.(b.c) = (a.b).c \quad \forall\, a, b, c \in R$.

(vi) Multiplication is closed

$a.b \in R \quad \forall\, a, b \in R$.

(vii) Addition is commutative :-

i.e. $a+b = b+a \quad \forall\, a, b \in R$.

(viii) Multiplication is distributive with respect to addition.

i.e. for all $a, b, c \in R$

$a.(b+c) = a.b + a.c$ (Left distributive law)

$(b+c).a = b.a + c.a$ (Right ")

the element $0 \in R$ will be the additive identity. It is called the zero element of the ring.

Note :-

The equation $a+x=b$ will have a unique solution in R & it will be $x = b-a$ obiously $a+(b-a)$

$$= a+[b+(-a)]$$
$$= a+[(-a)+b]$$
$$= [a+(-a)]+b = [(-a)+a]+b$$
$$= 0+b = b.$$

IIIly the equation $y+a=b$ will have a unique solution in R & it will be $y = b-a$.

Eg :- Examples of Ring are the

(i) set of integers Z is a ring w.r.t addition & Multiplication.

(ii) Set of even integer $2I$ is a ring "

(iii) Set of Real numbers R is a ring "

(iv) set of Rational numbers Q

(v) set of complex number C is a ring "

(VI) The set M of $n \times n$ matrices with their elements as real numbers (rational, complex & integers) is a ring with respect to addition & multiplication of matrices as the two ring compositions.

(VII) Set of $Z_n = \{0, 1, 2, \ldots (n-1)\}$ form a ring w.r.t $+_n$, $\cdot_n$.

Commutative Ring :-

If in a Ring R, the multiplication composition is also commutative.

ie if we have $a \cdot b = b \cdot a \quad \forall a, b \in R$.

then R is called a commutative Ring.

Ring with unity :-

If in a ring R, there exists an element denoted by 1 such that

$1 \cdot a = a = a \cdot 1 \quad \forall a \in R$. then R is called a ring with unit element.

The element $1 \in R$ is called the unit element of the ring. Obviously 1 is the multiplicative identity of R. Thus if a ring possesses multiplicative identity, then it is ring with unity.

Ring with Zero divisors :-

In any Ring R, if 0 is the additive identity is the zero element of the ring, then $0 \cdot a = a \cdot 0 = 0$ $\forall a \in R$.

However there are rings in which it is possible that $a \cdot b = 0$ when neither $a = 0$ nor $b = 0$. Such elements are called Zero divisors.

(OR)

If R is a commutative ring, i.e. $a \neq 0$ then a non zero element 'a' of a ring R is called a zero divisor or a divisor of zero if there exists an element $b \neq 0 \in R$

Such that either $a.b=0$ or $b.a$

(OR)

A ring R is said to be ring with zero divisor, if there exists an element $a, b \in R$ such that

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

Rings without zero divisors :-

A ring R is said to be ring without zero divisors if the product of no two non zero elements of R is zero,

ie if $a.b=0 \Rightarrow$ either $a=0$ or $b=0$.

$ab \neq 0 \Rightarrow a \neq 0, b \neq 0.$

Integral domain :-

A ring is called an integral domain if it (i) is commutative, (ii) has unit element (iii) is without zero divisors.

(OR)

A commutative ring R with unit element having no zero divisors is called an integral domain.

(OR)

~~Field~~ :-

An integral domain is a commutative ring with unity having atleast two element which is without zero divisors.

Field :-

A ring R with atleast two elements is called a field if it,

(i) is commutative (ii) has unity

(iii) is such that each non-zero element possesses multiplicative inverse.

(OR)

A field is a commutative ring with unity having atleast two elements in which the multiplicative inverse of each non-zero element exists.

Note :- In a ring every element possesses additive inverse. ∴ the question of an element being inversible or not arises only with respect to multiplication.

If R is a ring with unity, then an element $a \in R$ is called inversible, if there exists $b \in R$ such that $ab = 1 = ba$. Also then we write $b = a^{-1}$.

Division Ring or Skew field :-

A ring R with at least two elements is called a division ring or a skew field if it (i) has unity (ii) is such that each non zero element possesses multiplicative inverse.

Commutative Division Ring is a field.

Note :-

Note :-

Every field is also a division ring. But a division ring is a field if it is also commutative.

Eg :- Commutative ring :-

(i) Set of all Even integers is a commutative ring without unity. the addition & multiplication of integers being the two ring composition.

(ii) Set of all rational numbers is a commutative ring with unity. the addition & multiplication of rational numbers being the two ring compositions.

(iii) set- of all real numbers is a commutative ring with unity.

(iv) Set of all complex numbers is a commutative ring with unity

(v) The set M of all $n \times n$ matrices with their elements as real numbers (rational numbers complex numbers, integers) is a non-commutative ring with unity w.r.t $+$ & $\cdot$.

$\therefore$ matrix multiplication is not commutative

$\therefore$ the ring is a non-commutative ring.

∴ I be the unit matrix of the type $n \times n$, then $I \in M$ & we have

$I \cdot A = A = A \cdot I \quad \forall A \in M$. Therefore the matrix I is the multiplicative identity.

Thus the ring is with unity & the matrix I is the unity element of the ring i.e. $I = 1$.

(VI) The set $R = \{0, 1, 2, 3, 4, 5, +_6, \cdot_6\}$ is a commutative ring with unity.

∴ $\times_6$ is a commutative composition on R as is clear from the composition table also, ∴ R is a commutative ring. Also 1 is the identity element for the composition $\times_6$. ∴ R is a ring with unity 0 is the zero element of the ring.

Eg:- Ring with zero divisors :-

Suppose M is a ring of all 2×2 matrices with their elements as integers, the addition & multiplication of matrices being the two ring compositions. Then M is a ring with zero divisors.

Proof :-

The null matrix $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element (additive identity) of this ring. Now $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are two non-zero elements of this ring.

ie $A \neq 0$, $B \neq 0$ we have

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$= 0.$$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring. $\therefore$ M is a ring with zero divisors.

Also it is interesting to note that

$$BA = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus in a ring R it is possible that

$ab = 0$ but $ba \neq 0$.

2) The ring $\{0,1,2,3,4,5, +_6, \cdot_6\}$ is a ring with zero divisors.

We have $2 \times_6 3 = 0$ $3 \times_6 4 = 0$ i.e product of two non-zero elements is equal to the zero element of the ring.

3. The ring of Integers is a ring without zero divisors.

The product of two non-zero integers cannot be equal to the zero integers.

Integral domain :-

Ex Ring of integers is an integral domain

set of all integers is a commutative ring with unity. Also I does not possess zero divisors. We know that if a, b are integers s.t $ab = 0$ then either a or b must be zero.

$(C, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$ are all integral domains.

Set of all modulo 5 w.r.t $+_5$ & $\cdot_5$ is the ring $\{0, 1, 2, 3, 4, +_5, \times_5\}$ is a finite integral domain.

Field :-

Eg :- The ring of rational numbers $(Q, +, \cdot)$ is a field.

Since it is commutative ring with unity & each non zero element is invertible.

The rings of real numbers & complex numbers are also Field.

The ring Z of integers $(Z, +, \cdot)$ is an integral domain.

For any two integers $a \neq b$ $ab \neq 0$
$a \neq 0, b \neq 0$.

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

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

$1 \otimes_5 2 = 2$
$2 \otimes_5 3 = 1$
$3 \otimes_5 4 = 2$
$4 \otimes_5 1 = 4$

Here $a \neq 0, b \neq 0$
$\Rightarrow ab \neq 0$
Z_6 - an integral domain

Subrings :-

Let R be a ring. A non-empty subset S of the set R is said to be a subring of R if S is closed with respect to the operations of addition & multiplication in R & S itself is a ring for these operations.

condition for a subring :-

The necessary & sufficient 3 conditions for a non-empty subset S of a ring R to be a subring of R are

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

(ii) $a \in S, b \in S \Rightarrow ab \in S$.

* S is closed under subtraction & Multiplication

[A subset S of a ring R is a subring of R if S is itself a ring with the operations of R)

Ex:- $\{0, 2, 4\}$ is a subring of the ring Z_6, the integers modulo 6.

1 is the unity in Z_6, 4 is the unity in $\{0, 2, 4\}$

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

·	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

16

2

6 ⟌16

12

4

Some Elementary properties of a Ring :-

1. The additive identity or the zero element of a ring $(R, +, \cdot)$ is unique.
2. The additive inverse of every element of the ring is unique.
3. The multiplicative identity of a ring, if it exists, is unique.
4. If the ring has multiplicative identity, then the multiplicative inverse of any non zero element of the ring is unique.

Soln Let $0, 0'$ be two additive identities of $(R, +, \cdot)$

Then $0' + 0 = 0 + 0' = 0'$ $\because 0' \in R$ & 0 is a zero element. — (1)

$0 + 0' = 0' + 0 = 0$ $\because 0 \in R$ & $0'$ is a zero element. — (2)

$\therefore$ From (1) & (2) we have.

$0' = 0 + 0' = 0' + 0 = 0$

$\therefore 0 = 0'$

$\therefore$ 0 element of a ring is unique.

iv) Let $a \neq 0$, let b, c be multiplicative inverses of a (if it exists)

Then

$$a \cdot b = b \cdot a = 1 \quad \text{— (1)}$$

$$a \cdot c = c \cdot a = 1 \quad \text{— (2)}$$

$$b = b \cdot 1 = b \cdot (a \cdot c) \quad \text{by (2)}$$

$$= (b \cdot a) \cdot c \quad \text{(associativity)}$$

$$= 1 \cdot c \quad \text{(by (1))}$$

$$= c$$

$\therefore$ Multiplicative inverse of any non zero element (if it exists) is unique.

Property 2 :-

The cancellation laws of addition.

For all $a, b, c \in R$,

(i) If $a+b = a+c$ then $b = c$ (left cancellation)

(ii) If $b+a = c+a$ then $b = c$ (right cancellation)

Proof :-

$$a+b = a+c$$

$\therefore (-a) + a + b = (-a) + a + c$ where $-a$ is the additive inverse of a

$$(-a+a) + b = (-a+a) + c \quad \text{(by associativity)}$$

$$0 + b = 0 + c$$

$$\Rightarrow b = c$$

III^by. (b) part may be proved.

Property 3 :-

If $(R, +, \cdot)$ is a ring & $a \in R$ then $a \cdot 0 = 0 \cdot a = 0$ where 0 is the zero (additive identity) element of R.

Proof :- $a \cdot 0 = a \cdot (0+0)$ since $0+0=0$

$= a \cdot 0 + a \cdot 0$ — (1) ($\cdot$ is distributive over $+$)

$\therefore 0 + a \cdot 0 = a \cdot 0$

$= a \cdot 0 + a \cdot 0$ by (1)

$\therefore$ By the cancellation laws,

$a \cdot 0 = 0$

III^by we can prove that $0 \cdot a = 0$.

Property 4 :-

If $(R, +, \cdot)$ is a ring, then for any $a, b, c \in R$.

(i) $-(-a) = a$

(ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(iii) $(-a) \cdot (-b) = a \cdot b$

III^by. (b) part may be proved.

Property 3 :-

If $(R, +, \cdot)$ is a ring & $a \in R$ then $a \cdot 0 = 0 \cdot a = 0$ where 0 is the zero (additive identity) element of R.

Proof :- $a \cdot 0 = a \cdot (0+0)$ since $0+0=0$

$= a \cdot 0 + a \cdot 0$ ($\cdot$ is distributive over $+$)

— (1)

$\therefore 0 + a \cdot 0 = a \cdot 0$

$= a \cdot 0 + a \cdot 0$ by (1)

$\therefore$ By the cancellation law,

$a \cdot 0 = 0$

III^ly we can prove that $0 \cdot a = 0$.

Property 4 :-

If $(R, +, \cdot)$ is a ring, then for any $a, b, c \in R$.

(i) $-(-a) = a$

(ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(iii) $(-a) \cdot (-b) = a \cdot b$

(iv) $a \cdot (b-c) = a \cdot b - a \cdot c$

(v) $(a-b) \cdot c = a \cdot c - b \cdot c$

Proof :-

$(-a) + a = a + (-a) = 0$

$\therefore$ a is the additive inverse of $(-a)$

Also the additive inverse of $(-a)$ is unique.

$\therefore -(-a) = a$.

(ii) ~~$a \cdot (-b) = a \cdot (-b+b)$~~

We have $a \cdot [(-b)+b] = a \cdot 0$ $\quad \because -b+b = 0$

$a \cdot (-b) + a \cdot b = 0$ [by using left distributive law & the result (i)]

$\Rightarrow a \cdot (-b) = -(a \cdot b)$

↳ since in a ring $a+b=0$, $a = -b$

(iii) By we have

$(-a+a) \cdot b = 0 \cdot b$.

$(-a) \cdot b + a \cdot b = 0$

$(-a) \cdot b = -(a \cdot b)$

since in a ring $a+b=0$, $a=-b$

$\therefore a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(iii) we have

$$(-a)\cdot(-b) = -[(-a)\cdot b]$$

$\because a\cdot(-b) = -(a\cdot b)$

$$= -[-(a\cdot b)]$$

$\because (-a)\cdot b = -(a\cdot b)$

$$= a\cdot b$$

since R is a group w.r.t addition & in a group we have $a = -(-a)$

$$a\cdot(b-c) = a\cdot[b+(-c)]$$

by distributivity

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

by (i) $\because a\cdot(-c) = -(a\cdot c)$

$$= a\cdot b + [-(a\cdot c)]$$

$$= a\cdot b - (a\cdot c)$$

$$(a-b)\cdot c = [a+(-b)]\cdot c$$

by distributivity

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

$$= a\cdot c + -[(b\cdot c)]$$

$$= a\cdot c - (b\cdot c)$$

Property 5 :-

A commutative ring with unity is an integral domain iff it satisfies cancellation law of multiplication.

Proof :-

Let $(R, +, \cdot)$ be an integral domain.

Let $a \neq 0 \in R$ & let $a \cdot b = a \cdot c$ — (1)

i.e. $a \cdot (b - c) = 0$

Since R is an integral domain,

$a = 0$ or $(b - c) = 0$.

But $a \neq 0$. $\therefore$ $b - c = 0$

or $b = c$ — (2).

From (1) & (2) we see that left cancellation holds.

As R is commutative, right cancellation also holds.

converse :-

Let $(R, +, \cdot)$ be a commutative ring with identity & let cancellation laws hold with multiplication.

(ii) NE Laws

To prove that R is an integral domain
ie To prove R has no zero divisors.

Let $a, b \in R$ where $a \neq 0$.

If $a \cdot b = 0$

$a \cdot b = a \cdot 0$

$\Rightarrow b = 0$ by left cancellation law as $a \neq 0$.

Thus if $a \cdot b = 0$ then $a = 0$ or $b = 0$.

$\therefore$ R has no zero divisors.

$\therefore$ R is an integral domain.

Illy if $b \neq 0$ then $a = 0$.

Thus if $a \cdot b = 0$ then $a = 0$ or $b = 0$.

$\therefore$ R has no zero divisors.

property 6 :-

Every field is an integral domain.

proof :-

since a field F is a commutative ring with unity. It is enough we prove that F has no zero divisors to show that it is an integral domain.

Let a, b be elements of F with $a \neq 0$ such that $a \cdot b = 0$ ——— (1)

Since $a \neq 0$, a^{-1} exists & we have

from (1), $a \cdot b = a$

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

i.e. $$(a^{-1} \cdot a) \cdot b = 0$$

i.e. $$1 \cdot b = 0 \qquad \because a^{-1} \cdot a = 1$$

i.e. $$b = 0 \qquad \because 1 \cdot b = b.$$

(ii) By Let $a \cdot b = 0$ & $b \neq 0$.

Since $b \neq 0$, b^{-1} exists & we have

$$a \cdot b = 0$$

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

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

$$a \cdot 1 = 0$$

$$a = 0$$

Thus, in a field $a \cdot b = 0$ where $a, b \in F$ then either $a = 0$ or $b = 0$

$\therefore$ the field has no zero divisors.

$\therefore$ F is an Integral domain.

But the converse is not true.
ie Every integral domain is not a field.

For Ex: The ring of integers is an integral domain & it is not a field.
The only invertible elements of the ring of integers are 1 & -1.

For a field unity & zero are distinct elements ie $1 \neq 0$.
Let 'a' be any non zero element of a field. Then a^{-1} exists & is also non zero. For $a^{-1} = 0$

$$\Rightarrow a \cdot a^{-1} = a \cdot 0$$
$$\text{ie } 1 = 0$$
$$\text{ie } a \cdot 1 = a \cdot 0$$
$$\text{ie } a = 0$$

which is a contradiction. Now a field has no zero divisors $\therefore 1 = a^{-1}a \neq 0$.

A finite commutative ring without zero divisors is a field

(or)

Every finite integral domain is a field.

Proof :-

Let $(D, +, \cdot)$ be a finite Commutative ring without zero divisors having n elements $a_1, a_2 \cdots a_n$. In order to prove that D is a field, we must produce an element $1 \in D$ s.t $1 \cdot a = a \ \forall a \in D$ Also we should show that for every element $a \neq 0 \in D$ there exists an element $b \in D$ s.t $a \cdot b = 1$.

Let $a \neq 0 \in D$ consider the n products $a \cdot a_1, a \cdot a_2, \cdots a \cdot a_n \in D$

$\therefore$ D is closed under multiplication All there are elements of D. Also they are all distinct

But i.e. :-

For suppose that if
$a \cdot a_i = a \cdot a_j$ for $i \neq j$

then $a \cdot (a_i - a_j) = 0$ — (1)

Since D is without zero divisors & $a \neq 0$, therefore (1) implies

$a_i - a_j = 0$

$\Rightarrow a_i = a_j$ which is not true

since $a_1, a_2, \ldots a_n$ are all the n distinct elements of D placed in some order. So $\therefore a \cdot a_1, a \cdot a_2 \ldots a \cdot a_n$ one of these elements will be equal to a. Thus there exists an element say $1 \in D$ such that

$a \cdot 1 = a = 1 \cdot a$ $\therefore$ D is commutative

we shall show that this element 1 is the multiplicative identity of D. Let y be any element of D.

Then From the above discussion for some $x \in D$, we shall have

$$a \cdot x = y = x \cdot a$$

Now $1 \cdot y = 1 \cdot (a \cdot x)$ $\because a \cdot x = y$

$= (1 \cdot a) \cdot x$

$= a \cdot x$ $\because 1 \cdot a = a$

$= y$ $\because a \cdot x = y$

$= y \cdot 1$ $\because D$ is commutative

Thus $1 \cdot y = y = y \cdot 1 \quad \forall\, y \in D$.

$\therefore$ 1 is the unit element of the ring D.

Now $1 \in D$, Therefore from the above discussion one of the n products $a \cdot a_1, a \cdot a_2, \ldots\ldots a \cdot a_n$ will be equal to 1. Thus there exists an element say $b \in D$ such that

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

$\therefore$ b is the multiplicative inverse of the non zero element $a \in D$. Thus

every non zero element of D is invertible.

Hence D is a field.

Problems :-

① If $a, b \in R$ where $(R, +, \cdot)$ is a ring. Show that

$$(a+b)^2 = a^2 + a \cdot b + b \cdot a + b^2$$

Soln We have

$$(a+b)^2 = (a+b) \cdot (a+b)$$

$$= a \cdot (a+b) + b \cdot (a+b) \quad [\text{by Right distributive law}]$$

$$= a \cdot a + a \cdot b + b \cdot a + b \cdot b \quad [\text{by left distributive law}]$$

$$= a^2 + a \cdot b + b \cdot a + b^2$$

② Prove that the set M of 2×2 matrices over the field of real numbers is a ring with respect to matrix addition & multiplication. Is it a commutative ring with unity element ? Find the zero element.

Does this ring possess zero divisors?

Soln Let $A, B \in M$ Then $A+B \in M$ & $AB \in M$

$\therefore$ M is closed with respect to addition & multiplication of matrices.

(ii) Both addition & multiplication of matrices are associative compositions.

$\therefore$ $A+(B+C) = (A+B)+C \quad \forall A, B, C \in M$

& $A \cdot (B \cdot C) = (A \cdot B) \cdot C \quad \forall A, B, C \in M$.

Addition of matrices is a commutative composition. $\therefore$ for all $A, B \in M$ we have $A+B = B+A$.

If O be the null matrix of the type 2×2 then $O \in M$ & $O+A = A \quad \forall A \in M$.

Further multiplication of matrices is distributive with respect to addition.

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

& $(B+C)\cdot A = B\cdot A + C\cdot A$ $\forall A, B, C \in$

$\therefore$ M is a ring with respect to the given compositions.

Multiplication of matrices is not in general a commutative composition.

For example,

if $A = \begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. then

$$AB = \begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 8 \\ 3 & 11 \end{pmatrix}$$

$$BA = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 8 & 14 \\ 3 & 5 \end{pmatrix}$$

Thus $AB \neq BA$ & so the ring is a non-commutative ring.

If I be the unit matrix of the type 2×2 ie if $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ then $I \in M$.

Also we have $A \cdot I = A = I \cdot A \quad \forall A \in M$

$\therefore$ I is the multiplicative identity.

Thus the ring possesses the unit element & we have $I = 1$

(the unit element of the ring)

The null matrix $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the additive identity & is therefore the zero element of the ring.

i.e $O = 0$ (the zero element of the ring)

The ring possesses Zero divisors.

For example if

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix}$$

then $AB = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Thus the product of two non-zero element of the ring is equal to the zero element of the ring.

(3) Show that the set of numbers of the form $a+b\sqrt{2}$ with $a+b$ as rational numbers is a field.

Soln Let $R = \{a+b\sqrt{2} \; ; \; a, b \in Q\}$

Let $a_1+b_1\sqrt{2} \in R$, $a_2+b_2\sqrt{2} \in R$

Then $a_1, b_1, a_2, b_2 \in Q$

we have $(a_1+b_1\sqrt{2}) + (a_2+b_2\sqrt{2}) = (a_1+a_2) + \sqrt{2}(b_1+b_2) \in R$

$\because a_1+a_2, b_1+b_2 \in Q$.

Also $(a_1+b_1\sqrt{2}) \cdot (a_2+b_2\sqrt{2})$

$= a_1 \cdot (a_2+b_2\sqrt{2}) + b_1\sqrt{2} \cdot (a_2+b_2\sqrt{2})$

$= a_1 \cdot a_2 + a_1 \cdot b_2\sqrt{2} + b_1\sqrt{2} \cdot a_2 + b_1 \cdot b_2 2$

$= a_1 \cdot a_2 + 2b_1 \cdot b_2 + \sqrt{2}(a_1 \cdot b_2 + b_1 \cdot a_2)$

$\in R$ $\because a_1 \cdot a_2 + 2b_1b_2, a_1b_2 + a_2b_1 \in Q$.

Thus R is closed with respect to addition & Multiplication.

Again $1+0\sqrt{2} \in R$ & we have

$$(1+0\sqrt{2})\cdot(a+b\sqrt{2}) = a+b\sqrt{2}$$

$$= (a+b\sqrt{2})\cdot(1+0\sqrt{2})$$

$\therefore 1+0\sqrt{2}$ is the multiplicative identity.

Thus R is a commutative ring with unity. The zero element of the ring is $0+0\sqrt{2}$ & the unit element is $1+0\sqrt{2}$

Now R will be a field if each non zero element of R possesses multiplicative inverse.

Let $a+b\sqrt{2}$ be any non zero element of this ring, ie at least one of a & b is not zero.

Then $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}$

rationalizing the denominators.

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

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

Now if a & b are rational numbers then we can have $a^2 = 2b^2$ only if $a=0$, $b=0$

Since here at least one of the rational numbers a & b is not 0, therefore we cannot have $a^2 = 2b^2$.

i.e. $a^2 - 2b^2 \neq 0$.

$\therefore \frac{a}{a^2-2b^2}$ & $\frac{-b}{a^2-2b^2}$ are both rational numbers and at least one of them is not zero.

$\therefore \frac{a}{a^2-2b^2} + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$ is a non zero element of R & is the multiplicative inverse of $a+b\sqrt{2}$.

Hence the given system is a field.

(4) Show that $(Z_6, +_6, \times_6)$ is a commutative ring.

(OR)

The set $R = \{0, 1, 2, 3, 4, 5\}$ is a commutative ring with respect to $+_6$ & $\times_6$ as the two ring compositions.

Soln

(i) All the entries in the composition table are elements of the set R. ∴ R is closed with respect to addition modulo 6. ie $+_6$.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(ii) $+_6$ is associative. :-

If a, b, c are any three elements of G, then

$$a +_6 (b +_6 c) = a +_6 (b+c)$$

$$= \text{least non negative remainder when } a+(b+c) \text{ is divided by } 6.$$

$$= \text{least non-negative remainder when } (a+b)+c \text{ is divided by } 6.$$

$\because b +_6 c \equiv b+c \pmod 6$

$= (a+b) +_6 c \quad = (a +_6 b) +_6 c$

$\because a+b = a +_6 b \pmod 6$

Existence of identity :-

We have $0 \in G$. If a is any element of G, then from the composition table we see that

$$0 +_6 a = a = a +_6 0$$

Therefore 0 is the identity element.

Existence of Inverse :-

From the table we see that the inverses of $0, 1, 2, 3, 4, 5$ are $0, 5, 4, 3, 2, 1$ resp.

For example $4 +_6 2 = 0 = 2 +_6 4$. implies 4 is the inverse of 2.

The composition is commutative as the corresponding rows & columns in the composition table are identical.

The number of elements in the set R_6 is 6.

$\therefore (R_6, +_6)$ is a finite abelian group of order 6.

(i) From the table we see that R is closed w.r.t $\times_6$.

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(ii) Also we know that $\times_6$ is an associative composition in R.

i.e $a \times_6 (b \times_6 c)$
$= (a \times_6 b) \times_6 c$
$\forall a, b, c \in R$.

Further $\times_6$ is distributive in R w.r.t $+_6$

If a, b, c are any elements of R,

then $a \times_6 (b +_6 c)$

$= a \times_6 (b+c)$ $\because b +_6 c \equiv b+c \pmod 6$

= least non negative remainder when $a(b+c)$ is divided by 6

= least non-negative remainder when $ab+ac$ is divided by 6.

$= ab +_6 ac$

$= (a \times_6 b) +_6 ac$ $\because a \times_6 b = ab \pmod 6$

$= (a \times_6 b) +_6 (a \times_6 c)$ $\because a \times_6 c \equiv ac \pmod 6$

IIIly we can prove that

$(b +_6 c) \times_6 a = (b \times_6 a) +_6 (c \times_6 a)$

$\therefore$ R is a ring with respect to the given compositions. Since $\times_6$ is a commutative composition in R as is clear from the composition table also, $\therefore$ R is a commutative ring.

Also 1 is the identity element for the composition $\times_6$.

$\therefore$ R is a ring with unity.

The integer 0 is the zero element (additive identity of this ring.

We see that in this ring R neither 2 nor 3 is equal to the zero element of the ring. But $2 \times_6 3 = 0$ (zero element of the ring). Thus in a ring it is possible that the product of two non zero elements is equal to the zero element. Also the number of elements in R is finite. So it is a finite ring. ring with zero divisors.

(5) Show that the set of complex numbers $a+ib$ where a & b are integers form a ring ~~is an~~ integral domain under ordinary addition & multiplication of complex numbers. Is it an integral domain? Is it a field.

Soln Let $a+ib$ & $c+id$ be any two complex number (Gaussian integers)

Then $(a+ib)+(c+id)$

$=(a+c)+i(b+d)$

& $(a+ib)\cdot(c+id)$

$=ac+iad+ibc+i^2bd$

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

There are again complex numbers.

∴ It is closed w.r.t ordinary addition & multiplication of complex numbers.

Further in complex numbers both addition & multiplication are associative as well as commutative composition. Also multiplication distributes w.r.t respect to addition.

The complex number $0+i0$ is the additive identity. The additive inverse of $a+ib$ is $(-a)+i(-b)$. The Gaussian integer $1+i0$ is the multiplicative identity.

$(a+ib)\cdot(1+i0)$

$a+0+ib+0$

$= a+ib$

$\therefore$ the set of complex number (Gaussian integers) is a commutative ring with unity for the given composition.

Also this ring is free from zero divisors. Since the product of two non zero complex numbers cannot be zero. $\therefore$ it is an integral domain.

But this is not a field. since the multiplicative inverse of $a+ib$.

$$\frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2-(ib)^2}$$

$$= \frac{a-ib}{a^2+b^2}$$

$$= \left(\frac{a}{a^2+b^2}\right) + i\left(\frac{-b}{a^2+b^2}\right)$$

which is not always a Gaussian integers as $\frac{a}{a^2+b^2}$ & $\frac{-b}{a^2+b^2}$ are not necessarily integers.

(6) If R' is the set of all even integers & $*$ is defined by $a*b = \frac{ab}{2}$ where $a\,b \in R'$. Show that $(R', +, *)$ is a commutative ring, where $+$ stands for ordinary addition of integers.
(ii) What acts as the unit element of R'?

Soln Obviously R' is an abelian group with respect to addition.

If a & b are both even integers then $\frac{ab}{2}$ is also an even integer.

$\therefore \quad a*b = \frac{ab}{2} \in R' \quad \forall a, b \in R'$

Thus R' is closed with respect to $*$.

Also if a, b, c are any elements of R'

then $a*(b*c) = a*\left(\frac{bc}{2}\right) = \frac{a\left(\frac{bc}{2}\right)}{2}$

$= \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{\frac{ab}{2}*c}{2}$

$= (a * b) * c$

$\therefore$ $*$ is associative

Further $a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$

$\therefore$ $*$ is commutative.

Again $a * (b + c) = \frac{a(b+c)}{2} = \frac{ab}{2} + \frac{ac}{2}$

$= (a * b) + (a * c)$

III^{ly} $(b + c) * a = (b * a) + (c * a)$

$\therefore$ $*$ is distributive w.r.t. $+$.

$\therefore$ $(R', +, *)$ is a commutative ring

(ii) we have for all $a \in R'$

$2 * a = \frac{2a}{2} = a = a * 2$

$\therefore$ 2 is the unit element of R'.

(7) If M is the set of matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ where a, b are real numbers, show that M is a subring of the ring R of all 2×2 real matrices.

Soln Let $A = \begin{pmatrix} a_1 & 0 \\ b_1 & 0 \end{pmatrix}$ $B = \begin{pmatrix} a_2 & 0 \\ b_2 & 0 \end{pmatrix}$ be any two elements of M.

Then $A-B = \begin{pmatrix} a_1-a_2 & 0 \\ b_1-b_2 & 0 \end{pmatrix}$

Also $AB = \begin{pmatrix} a_1 & 0 \\ b_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ b_2 & 0 \end{pmatrix}$

$= \begin{pmatrix} a_1a_2 & 0 \\ b_1a_2 & 0 \end{pmatrix}$

Now $A-B$ & AB are both members of M. Since the second column of $A-B$ & also of AB consists of zeros only.

$\therefore$ M is a subring of R.

(8) If S is the set of ordered pairs (a,b) of real numbers & if the binary operations addition & multiplication are defined by the equation

$$(a,b) + (c,d) = (a+c, b+d)$$

$$(a,b) \cdot (c,d) = (ac-bd, bc+ad)$$

prove that $(S, +, \cdot)$ is a field.

proof :-

S is closed with respect to the two compositions. since $a+c, b+d, ac-bd$ $bc+ad$ are all real numbers.

Let $(a,b), (c,d) (e,f)$ be any elements of S. Then we make the following observations.

Associativity of addition, We have

$$\left[(a,b) + (c,d)\right] + (e,f)$$

$$= (a+c, b+d) + (e,f)$$

$$= ([a+c]+e, [b+d]+f)$$

$$= (a+[c+e], b+[d+f])$$

$= (a,b) + (c+e, d+f)$

$= (a,b) + [(c,d) + (e,f)]$

commutativity of addition :-

we have

$(a,b) + (c,d)$

$= (a+c, b+d)$ ~~$+ (e,f)$~~

$= ([a+c]+e, [b+d]+f)$ $= (c+a, d+b)$

$= (a+[c+e], b+[d+f])$ $= (c,d) + (a,b)$

$= (a,b) + (c+e, d+f)$

$= (a,b) + [(c,d) + (e,f)]$

Existence of additive identity :-

we have $(0,0) \in S$.

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

$= (a,b)$

$\therefore (0,0)$ is the additive identity.

Existence of additive inverse :-

If $(a,b) \in S$ then $(-a,-b) \in S$

We have

$$(-a,-b)+(a,b) = (-a+a,-b+b)$$

$$= (0,0)$$

$\therefore (-a,-a)$ is the additive inverse of (a,b)

Associativity of Multiplication :-

$$[(a,b)\cdot(c,d)]\cdot(e,f)$$

$$= (ac-bd,\ bc+ad)\cdot(e,f)$$

$$= [(ac-bd)\cdot e - (bc+ad)\cdot f,\ [bc+ad]\cdot e + [ac-bd]\cdot f)$$

$$= (a[ce-df]-b[de+cf],\ b[ce-df]+a[de+cf])$$

$$= (a,b)(ce-df,\ de+cf)$$

$$= (a,b)[(c,d)\cdot(e,f)]$$

Distributive laws :-

$$(a,b)[(c,d)+(e,f)]$$

$$= (a,b)[c+e,\ d+f]$$

$$= (a[c+e]-b[d+f],\ b[c+e]+a[d+f])$$

$$= [ac-bd]+[ae-bf],\ [bc+ad]+[be+af])$$

$= (ac-bd, bc+ad) + (ae-bf, be+af)$

$= (a,b)(c,d) + (a,b)(e,f)$.

IIIly we can show that the other distributive law also holds good.

∴ R is a ring with respect to the given compositions.

The ordered pair (0,0) is the

commutativity of Multiplication :-

we have

$(a,b) \cdot (c,d) = (ac-bd, bc+ad)$

$= (ca-db, da+cb)$

$= (ca, db)$

$= (c,d) \cdot (a,b)$

∴ R is a commutative Ring.

Existence of Multiplicative identity :-

we have $(1,0) \in R$. If $(a,b) \in R$

then $(1,0) \cdot (a,b) = (1a-0b, 0a+1b)$

$= (a,b)$

$= (a,b) \cdot (1,0)$

∴ $(1,1)$ is the multiplicative identity of the ring & is therefore the unit element of the ring.

Existence of Multiplicative identity :-

We have $(1,0) \in R$. If $(a,b) \in R$

then $(a,b)\cdot(1,0) = (a1-b0, b1+a0)$

$= (a,b)$

$= (1,0)\cdot(a,b)$

$\therefore (1,0)$ is the unity element of the ring.

Existence of Multiplicative inverse of each non-zero element of R.

Let (a,b) be any non-zero element of R. Then a & b are not both simultaneously zero. If (c,d) is the multiplicative inverse of (a,b), then we should have

$(a,b)\cdot(c,d) = (1,0)$

$(ac-bd, bc+ad) = (1,0)$.

By the definition of the equality of two ordered pairs, we have

$ac - bd = 1$ & $bc + ad = 0$

Solving these equations for c, d we get

$bac - b^2d = b$

$abc + a^2d = 0$

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

$d = -\frac{b}{a^2+b^2}$

$ac = 1 + bd$

$= 1 + \frac{b^2}{a^2+b^2} = \frac{a^2}{a^2+b^2}$

$c = \frac{a}{a^2+b^2}$

$$c = \frac{a}{a^2+b^2} \qquad d = \left(-\frac{b}{a^2+b^2}\right)$$

Now $a \neq 0$. or $b \neq 0$. $\Rightarrow a^2+b^2 \neq 0$.

$\therefore$ either c or d or both are non zero real numbers. Thus $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is the multiplicative inverse of (a,b).

Hence S is a field.

$a=1$ $c=\frac{1}{2}$
$b=-1$
$\frac{1}{2}$