

Ring: A ring $(R, +, \cdot)$ is a set R together with two binary operations $+$ (addition) and \cdot (multiplication) defined on R such that the following axioms are satisfied:-

- (R₁) $(a+b)+c = a+(b+c) \quad \forall a, b, c \in R$
- (R₂) $a+b = b+a \quad \forall a, b \in R$
- (R₃) There exist an element $0 \in R$ such that $0+a = a \quad \forall a \in R$
- (R₄) $\forall a \in R$ there exist an element $-a \in R$ such that $a+(-a)=0$.
- (R₅) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$
- (R₆) $a \cdot (b+c) = (a \cdot b) + (a \cdot c) \quad \forall a, b, c \in R$ (Left distributive law)
- (R₇) $(b+c) \cdot a = (b \cdot a) + (c \cdot a) \quad \forall a, b, c \in R$ (Right distributive law)

We call 0 , the zero element of the ring $(R, +, \cdot)$.

That is, an algebraic system $(R, +, \cdot)$ is called a ring if

- (i) $(R, +)$ is an abelian group
- (ii) (R, \cdot) is a semigroup i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$
- (iii) The operation \cdot is distributive over the operation $+$.

* A ring R is called commutative if $a \cdot b = b \cdot a \quad \forall a, b \in R$

* In a ring, an element $e \in R$ is called a unity (identity) element if $ea = ae = a \quad \forall a \in R$. An unity element of a ring R (if it exists) is an element of the semigroup (R, \cdot) . The unity of ring (if it exists) is generally denoted by 1 . A ring R is called a ring with unity if it has an unity element.

Examples: ① $(\mathbb{Z}, +, \cdot)$
Unity 1

② $(2\mathbb{Z}, +, \cdot)$
Unity not belongs.

(3) The set $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$ under addition and multiplication modulo n is a commutative ring with unity 1.

(4) The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer elements is a non-commutative ring with unity.

Some elementary properties of Ring:-

- Let $a, b, c \in R$ Then
- (1) $a \cdot 0 = 0 \cdot a = 0$
 - (2) $a \cdot (-b) = (-a)b = -(a \cdot b)$
 - (3) $(-a) \cdot (-b) = a \cdot b$
 - (4) $a \cdot (b - c) = a \cdot b - a \cdot c$ and $(b - c) \cdot a = b \cdot a - c \cdot a$.

Ring with zero divisor:- If a and b are two non-zero elements of a ring R such that $ab=0$, then a and b are divisors of 0 (or 0 divisors). In particular, a is left divisor of 0 and b is right divisor.

In a commutative ring, every left divisor of 0 is also a right divisor of 0 and conversely.

* The ring of integers do not have zero divisors.

* Suppose M is ring of all 2×2 matrices with their elements as integers, the addition and multiplication of matrices being the two ring composition, then M is a ring with zero divisors.

Null matrix $= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$ is the zero elements of this ring.

Now $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix}$ are two non-zero elements of this ring.

$$\text{we have } AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = BA$$

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.

Ex: $\mathbb{Z}_4 = \{0, 1, 2, 3, +_4, \times_4\}$

$2 \cdot 2 = 0$, Ring with zero divisor.

Integral domain: A ring containing at least two elements is called an integral domain if it

- (1) is commutative (ii) has unity element (iii) no zero divisors.

Thus, in an integral domain a product is 0 only when one of the factors is 0, that is $ab=0$ only, when $a=0$ or $b=0$.

Ex $(\mathbb{Z}, +, \cdot) = I.D$

$(\mathbb{R}, +, \cdot) = I.D$

$(\mathbb{Q}, +, \cdot) = \times$ (unity 1)

$M_2(\mathbb{Z}) = \times$ [not commutative, also has zero divisors]

Field:-

A ring containing at least two elements is called a field if it

- (1) is commutative
(2) has unity
(3) is such that every non-zero element has multiplicative inverse in R

That is to say, a system $(R, +, \cdot)$ is a field if

- (1) $(R, +)$ is an abelian group
(2) (R', \cdot) is an abelian group where $R' = R - \{0\}$
(3) the distributive laws

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

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