Ring Theory 1

08 September 2023 09:27

In group theory we dealed one binary operation
" ring " " " two " "

Definition:-

A ring R is a set together with two binary operation + and X
(we will call them addition and multiplication) satisfying :

a) $(R,+)$ is an abelian group
b) $\times$ is associative : $(a\times b)\times c = a\times(b\times c)$ $\forall a,b,c\in R$
c) the distributive law is followed :
$$(a+b)\times c = a\times c + b\times c$$
and
$$c\times(a+b) = c\times a + c\times b$$

- Ring R is commutative when multiplication is commutative
- Ring R is said to have an identity (or contain 1) if there is an element $1\in R$ with $1\times a = a\times 1 = a$ $\forall a\in$ Ring R
(may be there or may not)

Notations:- Whenever I write ab this means $a\times b$ $\forall a,b\in R$

Additive identity of R is denoted by 0
$$a+0 = 0+a = a \quad \forall a\in R$$
Additive inverse of $a\in R$ is denoted by $-a$ (will be)

As R is a group under addition $\Rightarrow$ $b+a = a+b$ $\forall a,b\in R$
So R is necessarily commutative under addition

Definition (Division Ring). –

A ring R with identity 1 where $1 \neq 0$, is called a division ring (skew field) if every non-zero element has a multiplicative inverse, i.e, $\exists\, b \in R$ such that $ab = ba = 1$. A commutative division ring is called a field

---

- $(\mathbb{Z}, +, \times)$ is ring or not? → Yes
  - ↳ It follows basic axioms

  $\mathbb{Z} - \{0\}$ with unit 1 is not a group $\Rightarrow \{\mathbb{Z}_1^{-\{0\}}, +, \times\}$ is not a ring

- $(\mathbb{Q}, +, \times)$ is ring or not? → Yes
- $(\mathbb{R}, +, \times)$ " " " " ? → Yes
- $(\mathbb{C}, +, \times)$ " " " " ? → Yes

Propositions:– Let R be a ring.

(1) $0a = a0 = 0 \;\forall\, a \in R$

(2) $(-a)b = a(-b) = -(ab) \;\forall\, a, b \in R$

(3) $(-a)(-b) = ab \;\forall\, a, b \in R$

(4) If R has an identity 1, then the identity is unique and $-a = (-1)a$

Proof:– (1), (2), (3) are easy to prove (we had done it in session)

(4) Suppose 1 and $1'$ are two identities in R.

$\Rightarrow 1a = a1 = a$ & $1'a = a1' = a \quad \forall\, a \in R$

$\Rightarrow 1a - 1'a = a - a$

$\Rightarrow (1-1')a = a + (-a) = 0 \Rightarrow (1-1')a = 0 \;\forall\, a \in R$

$\Rightarrow 1 - 1' = 0$

$\Rightarrow 1 + (-1') = 0$

$\Rightarrow \quad 1 = 1' \quad \Rightarrow\Leftarrow$

So identity in R is unique

- Unlike integers, however, general rings may posses many elements that have multiplicative inverses or may have non-zero elements a and b whose product is zero.

Def:- Let R be a ring.

1) A non-zero element a of R is called a zero divisor (ZD) if $\exists$ a non-zero element $b \in R$ such that $ab = ba = 0$

2) R has an identity $1 \neq 0$ and an element $e \in R$ is unit in R if $\exists$ some $v \in R$ such that $ev = ve = 1$. This set of units (U) is denoted by $R^{\times}$.

$\mathbb{Z}/6\mathbb{Z}$ has zero divisors as $\{2, 3, 4\}$ and units as $\{1, 5\}$

$ZD = \{2, 3, 4\}$, $U = \{1, 5\}$

$|ZD| \cup |U| \leq |R|$ for R is finite where $|\cdot|$ is the cardinality

---

Def:- (Integral Domain):- It is A commutative ring with identity $1 \neq 0$ if it has no zero divisors

" " " " " " " if $ab = 0$ if and only if $a = 0$ or $b = 0$ $\forall a, b \in R$

- $ab = ac$, $a, b, c \in$ Integral Domain and a is not a zero-divisor or 0

$\Rightarrow b = c \quad \forall a, b, c \in$ Integral Domain

---

1) Show that $(-1)^2 = 1$ in R = ring with 1 $\quad \Rightarrow (-1)^2 = (-1)(-1) = 1$

Ans:- $1 \in R \Rightarrow -1 \in R$. So, $(-1)(-1) \in R \Rightarrow 1 \in R$

1) Show ... $(-1)(-1) \in R \Rightarrow 1 \in R \Rightarrow ...$

Ans:- $1 \in R \Rightarrow -1 \in R$. So, $(-1)(-1) \in R$

2) Prove that if u is an unit in R then so is $-u$

Ans:- $u \in U(R) \Rightarrow -u \in R$

$u = (u^{-1})^{-1}$, $uu^{-1} = 1$, $(u^{-1})^{-1} u^{-1} = 1 \Rightarrow u^{-1} \in U(R)$

$-u^{-1} \in R \quad -u(-u^{-1}) = 1 \Rightarrow -u \in U(R)$

<u>Definition (Subring)</u>:- A subgroup S of R which is closed under multiplication is called a subring of R

S is a subgroup $\Rightarrow$ It is closed under addition

•) So to prove a subset S of R is a subring we must show that S is not empty and is closed under addition (rather substraction) and multiplication

•) Examples:- Subring $\mathbb{Z}$ is $n\mathbb{Z}$, $n \in \mathbb{N}$

" " " $\mathbb{Q}$

$\mathbb{Z}/n\mathbb{Z}$ is a subring of $\mathbb{Z}$ or not? $\rightarrow$ No for $n \geq 2$

$\mathbb{Z}/n\mathbb{Z}$ is the set $\{0, 1, \ldots, n-1\} \subseteq \mathbb{Z}$

In $\mathbb{Z}/n\mathbb{Z}$, $1 + (n-1) = 0 \in \mathbb{Z}/n\mathbb{Z} \neq n$ as it is not in $\mathbb{Z}/n\mathbb{Z}$

Thus $\mathbb{Z}/n\mathbb{Z}$ is not a subgroup of $\mathbb{Z} \Rightarrow$ not a subring

---

Q) Prove that the intersection of any non empty collection of subrings of a ring is also a subring

Ans:- S_1 and S_2 be subrings of R $\quad |S_1 \cap S_2| \neq 0$ as 0 is there

$x, y \in S_1 \cap S_2 \Rightarrow x, y \in S_1$ and $x, y \in S_2$

$x - y \in S_1$, $xy \in S_1$, $x - y \in S_2$, $xy \in S_2$

$\Rightarrow x - y, xy \in S_1 \cap S_2$

$\Rightarrow S_1 \cap S_2$ is subring of R

$\Rightarrow x-y,\ xy \in S_1 \cap S_2$

$\Rightarrow S_1 \cap S_2$ is subring of R