Discrete Structures and Theory of Logic

Lecture-21

Dharmendra Kumar

July 24, 2020

Ring

An algebraic structure (R, +, .), where R is a set and + and . are two binary operators defined on set R, is said to be ring if it satisfies following properties:-

(1) (R, +) is an abelian group.

(2) (R, .) is a semigroup.

(3) Distributive property must hold i.e. $a.(b+c) = a.b + a.c$ and $(b+c).a = b.a + c.a$, $\forall$ a,b,c $\in$ R.

Commutative ring

A ring R is said to be commutative ring if it satisfies commutative property with respect second operation i.e.
$a.b = b.a$, $\forall$ a,b $\in$ R.

Ring with unity

A ring R is said to be ring with unity if it contains identity element with respect to second operation that is . operation.
Note: We will denote here identity element with respect to first operation by 0 and identity element with respect to second operation by 1.

Example: Show that the set Z of integers under addition and multiplication is commutative ring with unity.

Solution: (Z, +, .) is a ring if it satisfies all the properties of ring. First we have to show that (Z,+) is an abelian group.

Closure property: We know that the addition of any two integers is also an integers. So, Z is closed under addition operation.

Associative property: We know that the addition of any three integers in any way is equal, therefore we can say, $a+(b+c) = (a+b)+c, \forall a,b,c \in Z$.

Therefore, Z satisfies associative property.

Existence of identity property: Let a $\in$ Z. Clearly, 0 $\in$ Z such that a+0 = a = 0+a. Therefore, 0 is an identity element. So, it satisfies identity property.
Existence of inverse property: Let a $\in$ Z. Clearly, -a $\in$ Z such that a+(-a) = 0. Therefore, -a is an additive inverse of any element a. So, it satisfies inverse property under addition operation.
Commutative property: Clearly, a+b = b+a, $\forall$ a,b $\in$ Z. So, Z satisfies commutative property with respect to addition operation.
Therefore, (Z,+) is an abelian group.

Ring

Now, we have to show that (Z, .) is a semigroup.

Closure property: We know that the multiplication of any two integers is also an integers. So, Z is closed under multiplication operation.

Associative property: We know that the multiplication of any three integers in any way is equal, therefore we can say, $a.(b.c) = (a.b).c, \forall\ a,b,c \in Z$.

Therefore, Z satisfies associative property.

Therefore, (Z, .) is a semigroup.

Now, we have to show **distributive property** is satisfied.

Clearly, for any three integers a,b,c; followings are satisfied:-

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

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

Therefore, distributive property is satisfied in $(Z, +, .)$.

Therefore, $(Z, +, .)$ is a ring.

Ring

Example: The set $Z_n = \{0,1,2,3,.........,n\text{-}1\}$ under addition and multiplication modulo n is a commutative ring with unity.
Solution: $(Z_n, +_n, \times_n)$ is a ring if it satisfies all the properties of ring.
First we have to show that $(Z_, +_n)$ is an abelian group.
Closure property: Consider a,b $\in Z_n$. Clearly, a$+_n$b = c $\in Z_n$. Therefore, Z_n is closed under addition modulo n operation.
Associative property: Clearly, if we compute $a +_n (b +_n c)$ and $(a +_n b) +_n c)$ then both value will be same. Therefore we can say, $a +_n (b +_n c) = (a +_n b) +_n c)$, $\forall$ a,b,c $\in Z_n$).
Therefore, Z_n satisfies associative property.

Ring

Existence of identity property: Let a $\in Z_n$. Clearly, 0 $\in Z_n$ such that a$+_n$0 = a = 0$+_n$a. Therefore, 0 is an identity element. So, it satisfies identity property.

Existence of inverse property: Let a $\in Z_n$. Clearly, n-a $\in Z_n$ such that a$+_n$(n-a) = 0. Therefore, n-a is an additive modulo n inverse of any element a. So, it satisfies inverse property under addition operation.

Commutative property: Clearly, a$+_n$b = b$+_n$a, $\forall$ a,b $\in Z_n$. So, Z_n satisfies commutative property with respect to addition modulo n operation.

Therefore, $(Z_n, +_n)$ is an abelian group.

Ring

Now, we have to show that $(Z_n, \times_n)$ is a semigroup.

Closure property: Consider a,b $\in Z_n$. Clearly, a$\times_n$b $=$ c $\in Z_n$. Therefore, Z_n is closed under multiplication modulo n operation.

Associative property: Clearly, if we compute $a \times_n (b \times_n c)$ and $(a \times_n b) \times_n c)$ then both value will be same. Therefore we can say, $a \times_n (b \times_n c) = (a \times_n b) \times_n c)$, $\forall$ a,b,c $\in Z_n$).

Therefore, Z_n satisfies associative property.

Therefore, $(Z_n, \times_n)$ is a semigroup.

Now, we have to show **distributive property** is satisfied.

Clearly, for any three elements a,b,c Z_n; followings are satisfied:-

(i) a$\times_n$(b$+_n$c) $=$ a$\times_n$b $+_n$ a$\times_n$c

(ii) (b$+_n$c)$\times_n$a $=$ b$\times_n$a $+_n$ c$\times_n$a

Therefore, distributive property is satisfied in $(Z_n, +_n, \times_n)$.

Therefore, $(Z_n, +_n, \times_n)$ is a ring.

Ring

Now, if this ring satisfies commutative property and identity property with respect to multiplication modulo n operation, then it is said to be commutative ring with unity.

Commutative property: Clearly, a$\times_n$b = b$\times_n$a, $\forall$ a,b $\in$ Z_n. So, Z_n satisfies commutative property with respect to multiplication modulo n operation.

Existence of identity property: Let a $\in Z_n$. Clearly, 1 $\in Z_n$ such that a$\times_n$1 = a = 1$\times_n$a. Therefore, 1 is an identity element. So, it satisfies identity property with respect to multiplication modulo n operation.

Therefore, this ring $(Z_n, +_n, \times_n)$ is commutative ring with unity.

Elementary properties of a ring

Let a,b,c $\in$ R, then

1. a.0 = 0.a = 0
2. a.(-b) = (-a).b = -(a.b)
3. (-a).(-b) = a.b
4. a.(b-c) = a.b - a.c and (b-c).a = b.a - c.a

Ring

Proof: **(1)** $a.0 + a.a = a.(0+a)$

$= a.a$

$= 0 + a.a$

using right cancellation law, $a.0 = 0$

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

$= a.a$

$= 0 + a.a$

using right cancellation law, $0.a = 0$

Therefore, $a.0 = 0.a = 0$

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

$= a.0$

$= 0$

therefore, $a.(-b) = -(a.b)$

Ring

$$\text{Similarly, } (-a).b + a.b = (-a+a).b$$
$$= 0.b$$
$$= 0$$

Therefore, $(-a).b = -(a.b)$

Therefore, $a.(-b) = (-a).b = -(a.b)$

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

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

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

Example: If R is a ring such that $a^2 = \text{a}$, $\forall$ a $\in$ R, prove that
(1) a+a = 0 , $\forall$ a $\in$ R i.e. each element of R is its own additive inverse.
(2) a+b = 0 $\Rightarrow$ a = b
(3) R is a commutative ring.

Solution:

(1) $(a+a)^2 = \text{a+a}$
$\Rightarrow$ $a^2 + a^2 + a^2 + a^2 = \text{a+a}$
$\Rightarrow$ a+a+a+a = a+a
$\Rightarrow$ a+a = 0 using cancellation law
It is proved.

Ring

(2) a+b $=0 \Rightarrow$ a+b $=$ a+a (using part (1))

$\Rightarrow$ b $=$ a (using cancellation law)

It is proved.

(3) $(a+b)^2 =$ a+b

$\Rightarrow a^2 + ab + ba + b^2 =$ a+b

$\Rightarrow$ a + ab + ba + b = a + b

$\Rightarrow$ ab + ba = 0 (using cancellation law)

$\Rightarrow$ ab = ba (using part (2))

Therefore, R is commutative ring. Now, It is proved.