

Discrete Structures and Theory of Logic

Lecture-39

Dr. Dharmendra Kumar

(Associate Professor)

United College of Engineering and Research, Prayagraj

October 2, 2023

Ring

An algebraic structure $(R, +, \cdot)$, where R is a set and $+$ and \cdot 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, \cdot) is a semigroup.
- (3)** Distributive property must hold i.e. $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$, $\forall a, b, c \in R$.

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 \cdot 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 \mathbb{Z} of integers under addition and multiplication is commutative ring with unity.

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

Closure property: We know that the addition of any two integers is also an integers. So, \mathbb{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, $a + (b + c) = (a + b) + c, \forall a, b, c \in \mathbb{Z}$.

Therefore, \mathbb{Z} satisfies associative property.

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

Existence of inverse property: Let $a \in \mathbb{Z}$. Clearly, $-a \in \mathbb{Z}$ 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, $a+b = b+a$, $\forall a, b \in \mathbb{Z}$. So, \mathbb{Z} satisfies commutative property with respect to addition operation. Therefore, $(\mathbb{Z}, +)$ is an abelian group.

Now, we have to show that (\mathbb{Z}, \cdot) is a semigroup.

Closure property: We know that the multiplication of any two integers is also an integers. So, \mathbb{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, $a.(b.c) = (a.b).c, \forall a,b,c \in \mathbb{Z}$.

Therefore, \mathbb{Z} satisfies associative property.

Therefore, (\mathbb{Z}, \cdot) 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 $(\mathbb{Z}, +, \cdot)$.

Therefore, $(\mathbb{Z}, +, \cdot)$ is a ring.

Example: The set $Z_n = \{0,1,2,3,\dots,n-1\}$ 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.

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 $a, b, c \in Z_n$; 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.

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. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$ and $(b - c) \cdot a = b \cdot a - c \cdot a$

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

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

$$\text{Therefore, } (-a).b = -(a.b)$$

$$\text{Therefore, } a.(-b) = (-a).b = -(a.b)$$

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

$$\begin{aligned}(4) \quad a.(b-c) &= a.(b+(-c)) \\ &= a.b + a.(-c) \\ &= a.b - a.c\end{aligned}$$

$$\begin{aligned}\text{Similarly, } (b-c).a &= (b+(-c)).a \\ &= b.a + (-c).a \\ &= b.a - c.a\end{aligned}$$

Example: If R is a ring such that $a^2 = a$, $\forall a \in R$, 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:

$$(1) (a+a)^2 = a+a$$

$$\Rightarrow a^2 + a^2 + a^2 + a^2 = a+a$$

$$\Rightarrow a+a+a+a = a+a$$

$$\Rightarrow a+a = 0 \text{ using cancellation law}$$

It is proved.

$$\begin{aligned} (2) \quad a+b &= 0 \Rightarrow a+b = a+a \text{ (using part (1))} \\ &\Rightarrow b = a \text{ (using cancellation law)} \end{aligned}$$

It is proved.

$$\begin{aligned} (3) \quad (a+b)^2 &= a+b \\ \Rightarrow a^2 + ab + ba + b^2 &= a+b \\ \Rightarrow a + ab + ba + b &= a + b \\ \Rightarrow ab + ba &= 0 \text{ (using cancellation law)} \\ \Rightarrow ab &= ba \text{ (using part (2))} \end{aligned}$$

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