Discrete Structures and Theory of Logic

Lecture-13

Dharmendra Kumar

July 22, 2020

Definition of Group

An algebraic structure (G,o), where G is a set and o is a binary operator defined on the set G, is called a group if it satisfies following properties:-

(1) Closure property:

For all a,b $\in$ G, aob $\in$ G.

(2) Associative property:

For all a,b,c $\in$ G, ao(boc) = (aob)oc.

(3) Existence of identity property:

For all a $\in$ G, $\exists$ e $\in$ G, such that aoe = eoa = a.

Element e is said to be identity element of the group G.

(4) Existence of inverse property:

For all a $\in$ G, $\exists$ b $\in$ G, such that aob = e = boa.

Element b is said to be inverse of an element a.

Abelian group

A group (G,o) is said to be an abelian group if it satisfies the following property:-

$$aob = boa, \forall\ a,b \in G.$$

Note: If aob = boa, $\forall$ a,b $\in$ G, then this is known as commutative property.

Group

Groupoid

An algebraic structure (G,o) is said to be groupoid if it satisfies only closure property.

Semigroup

An algebraic structure (G,o) is said to be semigroup if it satisfies closure and associative property.

Monoid

An algebraic structure (G,o) is said to be monoid if it satisfies closure, associative and existence of identity property.

Group

Example: Is (R,+) a group, where R is a set of real numbers?

Solution: (R,+) will be a group if it satisfies all the four properties of the group.

Closure property

Consider any two real numbers a and b. Clearly a+b will also be a real number. Therefore, (R,+) satisfies closure property.

Associative property

Consider three real numbers 10, 15, 2/3.

$10+(20+(2/3)) = 10+(62/3) = 92/3.$

$(10+20)+2/3 = 30+2/3 = 92/3.$

Clearly, $10+(20+(2/3)) = (10+20)+2/3.$

Therefore, $a+(b+c) = (a+b)+c$, for all $a,b,c \in R$.

Therefore, (R,+) satisfies associative property.

Group

Identity property

Clearly, 0 is a real number such that $0+a = a$, $\forall\ a \in R$.

Therefore, 0 is the identity element. Therefore, (R,+) satisfies identity property.

Inverse property

Consider an element $a \in R$. Clearly, $a+(-a) = 0$, therefore inverse of a is -a. Similarly, for any real number a, -a will be its inverse.

Therefore, (R,+) satisfies inverse property.

Since (R,+) satisfies all the four properties of the group, therefore (R,+) is a group.

Group

Example: Is (R',*) a group, where R' = R-{0} ?

Solution:

Closure property

Consider any two non-zero real numbers a and b. Clearly a*b will also be a real number. Therefore, (R',*) satisfies closure property.

Associative property

Consider three real numbers 10, 0.5, 2.

10*(0.5*2) = 10*1 = 10.

(10*0.5)*2 = 5*2 = 10. Clearly, 10*(0.5*2) = (10*0.5)*2 .

Therefore, a*(b*c) = (a*b)*c, for all a,b,c $\in$ R'.

Therefore, (R',*) satisfies associative property.

Group

Identity property

Clearly, 1 is a real number such that 1*a = a, $\forall$ a $\in$ R'.

Therefore, 1 is the identity element. Therefore, (R',*) satisfies identity property.

Inverse property

Consider an element a $\in$ R'. Clearly, there exists a non-zero real number 1/a such that a*(1/a) = 1, therefore inverse of a is 1/a. Similarly, for any real number a, 1/a will be its inverse. Therefore, (R',*) satisfies inverse property.

Since (R',*) satisfies all the four properties of the group, therefore (R',*) is a group.

Group

Example: Is $(Z^+,+)$ a group, where Z^+ denotes set of positive integers?

Solution: Solution:

Since the sum of any two positive integers is also a positive integers, therefore it satisfies closure property.

Similarly, the sum of any three positive integers in any way will be same. therefore it satisfies associative property.

Since the operation is addition, therefore identity element is 0. Clearly $0 \in Z^+$, therefore it satisfies identity property.

But the inverse of any positive integer a will be -a. and -a $\notin Z^+$. Therefore, inverse property is not satisfied. Hence, $(Z^+,+)$ is not a group.

Group

Example: Prove that the four roots of unity 1, -1, i, , -i form an abelian multiplicative group.

Solution: First we construct composition table of it. The composition table of it is the following:-

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Group

From table, all entries in this table are belong into the given set. Therefore, closure property is satisfied.

Clearly, associative operation is also satisfied, because the operation is multiplication.

In the table, row 1 indicate that element 1 is identity element.

Clearly, $(1)^{-1} = 1$, $(-1)^{-1} =$ -1, $(i)^{-1} =$ -i, $(-i)^{-1} =$ i. Since each element has inverse, therefore inverse property is satisfied.

Clearly, a*b = b*a, therefore commutative property is also satisfied.

Since all the five properties of abelian group is satisfied, therefore this is a multiplicative group.

Example: Show that the set of all positive rational numbers form an abelian group under the operation defined by aob = (ab)/2.

Solution:

Closure property

Consider any two positive rational numbers a and b.

Since aob = (ab)/2. Clearly (ab)/2 will be a positive rational number. Therefore, it satisfies closure property.

Associative property

Consider three positive rational numbers a, b, c.

ao(boc) = ao(bc/2) = (abc)/4

(aob)oc = ((ab)/2)oc = (abc)/4

Clearly, ao(boc) = (aob)oc, for all a,b,c $\in$ R. Therefore, it satisfies associative property.

Group

Identity property

Let e the identity element. Therefore, aoe = a $\Rightarrow$ (ae)/2 = a $\Rightarrow$ e = 2. Therefore, 2 is an identity element. Therefore, (it satisfies identity property.

Inverse property

Consider, a is positive rational number. Let b is an inverse of a. Therefore, aob = e = 2 $\Rightarrow$ (ab)/2 = 2 $\Rightarrow$ b = 4/a. Therefore inverse of a is 4/a. Therefore, it satisfies inverse property.

Now, aob = (ab)/2 = (ba)/2 = boa. Therefore, it satisfies commutative property.

Since it satisfies all the five properties of an abelian group, therefore it is an abelian group.