

## Algebraic Structures

### Binary Operation

Let  $S$  be a non-empty set. If  $f: S \times S \rightarrow S$  is a mapping then  $f$  is called a binary operation or binary composition in  $S$ .

The Symbols  $+$ ,  $\cdot$ ,  $*$ ,  $\oplus$  etc are used to denote binary operations on a set.

- $\rightarrow$  for  $a, b \in S \Rightarrow a + b \in S \Rightarrow +$  is a binary operation in  $S$ .
- $\rightarrow$  for  $a, b \in S \Rightarrow a \cdot b \in S \Rightarrow \cdot$  is a binary operation in  $S$ .
- $\rightarrow$  for  $a, b \in S \Rightarrow a * b \in S \Rightarrow *$  is a binary operation in  $S$ .
- $\rightarrow$  for  $a, b \in S \Rightarrow a \circ b \in S \Rightarrow \circ$  is a binary operation in  $S$ .

This is said to the closure property of binary operation and the set  $S$  is said to be closed with respect to binary operation.

Ex ' $\circ$ ' is operation defined on  $\mathbb{Z}$  such that  $a \circ b = a + b - ab$  for  $a, b \in \mathbb{Z}$ . Is the operation ' $\circ$ ' a binary operation in  $\mathbb{Z}$ ? If so, is it associative and commutative in  $\mathbb{Z}$ ?

Sol?: If  $a, b \in \mathbb{Z}$ , we have  $a + b \in \mathbb{Z}$ ,  $ab \in \mathbb{Z}$  and  $a + b - ab \in \mathbb{Z}$

$$\Rightarrow a \circ b = a + b - ab \in \mathbb{Z}$$

$\therefore$  ' $\circ$ ' is a binary operation in  $\mathbb{Z}$

$$\Rightarrow a \circ b = b \circ a$$

$\therefore$  ' $\circ$ ' is commutative in  $\mathbb{Z}$

$$\begin{aligned}\text{Now, } (a \circ b) \circ c &= (a \circ b) + c - (a \circ b)c \\ &= a + b - ab + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + ab\end{aligned}$$

and

$$\begin{aligned} a \circ (b \circ c) &= a + (b \circ c) - a(b \circ c) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \end{aligned}$$

$$\Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$$

$\therefore$  'o' is associative in Z.

Q Fill in the blanks in the following composition table so that 'o' is associative in  $S = \{a, b, c, d\}$

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

Sol<sup>n</sup> (i)  $d \circ a = (c \circ b) \circ a$  [ $\because c \circ b = d$ ]

$$= c \circ (b \circ a) \text{ [associative law]}$$

$$= c \circ b$$

$$= d$$

$$(ii) d \circ b = (c \circ b) \circ b = c \circ (b \circ b) = c \circ a = c$$

$$(iii) d \circ c = (c \circ b) \circ c = c \circ (b \circ c) = c \circ c = c$$

$$(iv) d \circ d = (c \circ b) \circ (c \circ b) = c \circ (b \circ c) \circ b$$

$$= c \circ c \circ b$$

$$= c \circ (c \circ b)$$

$$= c \circ d$$

$$= d.$$

Hence, the required composition table is

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d	d	c	c	d

Theorem - The identity elements of a binary operation  $*$  in a set  $A$ , if it exists and is unique.

Proof - If possible, let  $e'$  and  $e''$  be two identity element in  $A$  with respect to binary operation  $*$   $e'$  is an identity element in  $A$

$$\Rightarrow e' * e'' = e'' * e' = e''$$

and  $e''$  is an identity element in  $A$

$$\Rightarrow e' * e'' = e'' * e' = e'$$

Which together show that  $e' = e''$

Theorem. If  $*$  is an associative binary operation in  $A$ , then the inverse of every invertible element is unique.

proof - Let  $a \in A$ , be an invertible element with respect to  $*$ , If possible let  $b$  and  $c$  be two distinct inverses of the element  $a$  in  $A$ .

Let  $e$  be identity elements in  $A$  with respect to  $*$

Then we have

$$b * a = a * b = e$$

$$\text{and, } c * a = a * c = e$$

now  $(b * a) * c = b * (a * c)$  ( $\because *$  is associative in  $A$ )

$$\Rightarrow e * c = b * e$$

$$c = b$$

This completes the proof of the theorem.