UNIT-3
Algebraic Structures

Algebraic Systems with One Binary Operation
Binary Operation

Let S be a non-empty set. If $f : S \times S \to S$ 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.

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

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

Properties of Binary Operations

Commutative: $*$ is a binary operation in a set S. If for $a, b \in S$, $a * b = b * a$, then $*$ is said to be commutative in S. This is called commutative law.

Associative: $*$ is a binary operation in a set S. If for $a, b, c \in S$, $(a*b)*c = a*(b*c)$, then $*$ is said to be associative in S. This is called associative law.

Distributive: $\circ$, $*$ are binary operations in S. If for $a, b, c \in S$, (i) $a \circ (b * c) = (a \circ b) * (a \circ c)$, (ii) $(b * c) \circ a = (b \circ a) * (c \circ a)$, then $\circ$ is said to be distributive w.r.t the operation $*$.

Example: N is the set of natural numbers.

(i) $+, \cdot$ are binary operations in N, since for $a, b \in N$, $a + b \in N$ and $a \cdot b \in N$. In other words N is said to be closed w.r.t the operations $+$ and $\cdot$.

(ii) $+, \cdot$ are commutative in N, since for $a, b \in N$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

(iii) $+, \cdot$ are associative in N, since for $a, b, c \in N$,
$$a + (b + c) = (a + b) + c \text{ and } a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(iv) is distributive w.r.t the operation $+$ in N, since for $a, b, c \in N$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

(v) The operations subtraction $(-)$ and division $(\div)$ are not binary operations in N, since for $3, 5 \in N$ does not imply $3 - 5 \in N$ and $\frac{3}{5} \in N$.

Example: A is the set of even integers.

(i) $+, \cdot$ are binary operations in A, since for $a, b \in A$, $a + b \in A$ and $a \cdot b \in A$.

(i) $+, \cdot$ are commutative in A, since for $a, b \in A$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

(ii) $+, \cdot$ are associative in A, since for $a, b, c \in A$,
$$a + (b + c) = (a + b) + c \text{ and } a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(iv) $\cdot$ is distributive w.r.t the operation $+$ in A, since for $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Example: Let S be a non-empty set and $\circ$ be an operation on S defined by $a \circ b = a$ for $a, b \in S$. Determine whether $\circ$ is commutative and associative in S.

Solution: Since $a \circ b = a$ for $a, b \in S$ and $b \circ a = b$ for $a, b \in S$.

$$\Rightarrow a \circ b \neq b \circ a.$$

$\therefore \circ$ is not commutative in S.

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

$a \circ (b \circ c) = a \circ b = a$ for $a, b, c \in S$.

$\therefore \circ$ is associative in S.

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

Solution: If $a, b \in Z$, we have $a + b \in Z$, $ab \in Z$ and $a + b - ab \in Z$.

$$\Rightarrow a \circ b = a + b - ab \in Z.$$

$\therefore \circ$ is a binary operation in Z.

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

$\therefore \circ$ is commutative in Z.

Now

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

and

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

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

$\circ$ is associative in Z.

Example: Fill in blanks in the following composition table so that $\circ$ 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				

Solution: $d \circ a = (c \circ b) \circ a$ [$\because c \circ b = d$]

$= c \circ (b \circ a)$ [$\because \circ$ is associative]

$= c \circ b$

$= d$

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

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

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

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

$= c \circ c \circ b$

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

$= c \circ d$

$= d$

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

Example: Let $P(S)$ be the power set of a non-empty set S. Let $\cap$ be an operation in $P(S)$. Prove that associative law and commutative law are true for the operation in $P(S)$.

Solution: P(S)= Set of all possible subsets of S.
Let $A, B \in P(S)$.
Since $A \subseteq S$, $B \subseteq S \Rightarrow A \cap B \subseteq S \Rightarrow A \cap B \in P(S)$.

$\therefore \cap$ is a binary operation in $P(S)$.

Also $A \cap B = B \cap A$

$\therefore \cap$ is commutative in $P(S)$.

Again $A \cap B$, $B \cap C$, $(A \cap B) \cap C$ and $A \cap (B \cap C)$ are subsets of S.

$\therefore (A \cap B) \cap C, A \cap (B \cap C) \in P(S)$.

Since $(A \cap B) \cap C = A \cap (B \cap C)$

$\therefore \cap$ is associative in $P(S)$.

Algebraic Structures

Definition: A non-empty set G equipped with one or more binary operations is called an *algebraic structure* or an *algebraic system*.
If $\circ$ is a binary operation on G, then the algebraic structure is written as $(G, \circ)$.
Example: $(N, +)$, $(Q, -)$, $(R, +)$ are algebraic structures.

Semi Group

Definition: An algebraic structure $(S, \circ)$ is called a *semi group* if the binary oper-ation $\circ$ is associative in S.
That is, $(S, \circ)$ is said to be a semi group if

(i) $a, b \in S \Rightarrow a \circ b \in S$ for all $a, b \in S$

(ii) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$.

Example:

1. $(N, +)$ is a semi group. For $a, b \in N \Rightarrow a + b \in N$ and $a, b, c \in N \Rightarrow (a + b) + c = a + (b + c)$.

2. $(Q, -)$ is not a semi group. For $5, 3/2, 1 \in Q$ does not imply $(5 - 3/2) - 1 = 5 - (3/2 - 1)$.

3. $(R, +)$ is a semi group. For $a, b \in R \Rightarrow a + b \in R$ and $a, b, c \in R \Rightarrow (a + b) + c = a + (b + c)$.