Algebraic Structures

Binary operations:

Let 'G' be a non-empty set. Then $G \times G = \{(a, a) : a \in G, b \in G\}$

If $f: G \times G \to G$, then 'f' is said to be binary operation on G.

Thus a binary operation on 'G' is a function that each ordered pair of elements of 'G' is a unique element of G.

The symbols $(+, \cdot, 0, *)$ etc are used to denoted binary operations on a set.

Thus '+' will be binary operation on G if & only if

$a + b \in G \quad \forall \; a, b \in G$

$a + b$ is unique

My, '*' will be a binary operation on G if & only if $a * b \in G \quad \forall \; a, b \in G$

$a * b$ is unique.

Algebraic System:

A system consisting of a set & one (or) more operations on the set is called an algraic system. It is denoted by $(S, f_1, f_2 \ldots)$ where 'S' is a non-empty set & f_1, f_2 are operations on S.

The operations & relations on the set 'S' defined a structure on the elements of set S, an algebraic system is called

algebraic structure.

Algebraic structure: A Non-empty set together with one (or) more than one binary operations is called algebraic structure.

Ex: $(N, +)$, $(Z, +)$, $(R, +, \cdot)$ are all algebraic structures.

Addition & multiplication are both binary operations on the set R of real numbers.

Therefore $(R, +, *)$ is an algebraic structure.

** Group: Let $(G, *)$ be an algebraic structure where $*$ is a binary operation then $(G, *)$ is called a group if the following 4-conditions are satisfied.

(1) closure property (3) Identity element
(2) Associative law (4) Inverse element.

1. closure property:

The binary operation $*$ is a closed operation. i.e $a * b \in G$

$a * b \in G$ for all $a, b \in G$.

2. Associated property:

The binary operation $*$ is an associative Operation i.e $a * (b * c) = (a * b) * c$ $\forall$ $a, b, c \in G$.

3. Identity property:

There Exist an identity Element

for Every $a \in G$ there Exist an unique element $e \in G$ such that

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

Inverse property: for Each a in G there Exist an Element a^{-1} (inverse)

such that $a * a' = a' * a = e$.

Abelian group: A group 'G' is said to be Abelian if the commutative property holds i.e $a * b = b * a \ \forall \ a, b \in G$.

(or)

Group - 4 properties with commutative property satisfies then it is known as abelian group.

→ A group with addition binary operation is known as additive group. and that with multiplication binary operation is known as multiplicative group.

Note :-

1. A set 'G' with a binary composition is said to be a groupoid.
2. A set 'G' with a binary composition which is associative is said to be a semigroup
3. A set 'G' with a binary composition which is associative and identity element exists is said to be a monoid.

Order of a group (finite & infinite groups):-

If the number of elements in the set 'G' forming a group be finite then it is called a finite group and the number of elements in it is called the order of this finite group. otherwise it is called an infinite group and it is said to be of infinite order (or) zero order.

Prove that the fourth root of unity 1, -1, i, -i form an abelian multiplicative group

(OR)

Prove that $G = \{-1, 1, i, -i\}$ is an abelian group under multiplication.

Sol: Let $G = \{1, -1, i, -i\}$

Composition table:

×	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

(i) closure:

$a, b \in G$

$a * b = b * a$

from above table all the elements of G. Hence 'G' is closed w.r.t multiplication.

(ii) Associative:

$a, b, c \in G$

$a * (b * c) = (a * b) * c$

$1(-1)(i) = -i$

$i(-1)(1) = -i$

∴ 'G' Associative

(iii) Identity:

let $1 \in G \Rightarrow 1 \cdot a = a \cdot 1 = a$

(iv) Inverse:

$1 \times 1 = i(-i)$ ∵ $i^2 = -1$

$1 = -i^2 = -(-1)$

$= 1$

$(-1) \times (-1) = 1$

Inverse of $1, -1, i, -i$ are $1, -1, -i$

(v) commutative: $a, b \in G \Rightarrow ab = ba$

$\forall a, b \in G$

$1(-1) = (-1)(1) = -1$

∴ multiplication of complex numbers is always commutative.
Hence it follows that G' is an abelian multiplicative group.

→ Groupoid :-
Let $(S, *)$ be an algebraic structure in which 'S' is a non-empty set and '*' is a binary operation on S.
Thus 'S' is closed with the operation *.
Such a structure consisting of a non-empty set S and binary operation defined on S is called a groupoid.

→ Semi-group :-
An algebraic structure $(S, *)$ is called a semigroup if the following conditions are satisfied.
i) the binary operation * is a closed operation
i.e $a * b \in S \quad \forall\ a, b \in S$
ii) the binary operation * is an associative operation.
i.e, $a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in S$.

→ Monoid :-
An algebraic structure $(S, *)$ is called a monoid if the following conditions are satisfied.
i) the binary operation * is closure law
ii) the binary operation * is an associative law.
iii) there ~~exists~~ an identity element.
i.e for some $e \in S$, $e * a = a * e = a \quad \forall\ a \in S$.

A monoid is a semi-group $(S, *)$ it has an identity element.

Sub group:

Let $(G, *)$ be a group and H is a non-empty subset of G. $(H, *)$ is said to be subgroup of G. if $(H, *)$ is also group by itself.

i.e, 'H' satisfies all the properties of a group for the induceed composition. $a, b \in H \Rightarrow ab^{-1} \in H$.

b^{-1} is the inverse of b in G.

Note:

Every set is a subset of itself.

If G is a group, then G itself is a subgroup of G. also if 'e' is the identity element of G. then the subset of G containing only identity element is also a subgroup of G.

These two subgroups $(G, *)$ & $(\{e\}, *)$ of the group $(G, *)$ are called improper (or) trivial subgroups others are called proper (or) non trivial subgroups.

Cosets:

Let H be a subgroup of a group G. & let $a \in G$. then the set $\{a * h : h \in H\}$ is called the left coset generated by a & H.

it is denoted by aH.

Similarly the set $Ha = \{h * a : h \in H\}$ is called the right coset.

it is denoted by Ha.

The element a is called a representative of aH & Ha.

Properties of cosets:
Let H be a subgroup of G. & $a \& b$ belong to G. then

1) $a \in aH$
2) $aH = H$ if & only if $a \in H$.
3) $aH = bH$ (or) $aH \cap bH = \phi$
4) $aH = bH$ if & only if $a^{-1}b \in H$.

** Theorem:
Statement: the intersection of any two sub-groups of a group $(G, *)$ is again a subgroup of $(G, *)$.
(or)
Let G_1 & G_2 be subgroups of a group G.
(i) show that $G_1 \cap G_2$ is also a subgroup of G.
(ii) Is $G_1 \cup G_2$ is always a subgroup of G.

Proof: Let H_1 & H_2 form any two subgroups of $(G, *)$.
we have $H_1 \cap H_2 \neq \phi$
since atleast the identity element is comman to both H_1 & H_2.
let $a \in H_1 \cap H_2$ & $b \in H_1 \cap H_2$
Now $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ & $a \in H_2$
$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ & $b \in H_2$.
since H_1 & H_2 form subgroups under the group $(G, *)$.
we have $a \in H_1, b \in H_1 \Rightarrow a * b^{-1} \in H_1$
$a \in H_2, b \in H_2 \Rightarrow a * b^{-1} \in H_2$
$a * b^{-1} \in H_1, a * b^{-1} \in H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$
We have $a \in H_1 \cap H_2, b \in H_1 \cap H_2$
$\Rightarrow a * b^{-1} \in H_1 \cap H_2$.
$\therefore H_1 \cap H_2$ forms a subgroup under $(G, *)$.
Note: the union of two subgroups is not

not necessarily es a subgroup.

* Partially ordered sets (or) (POSETS)

A relation R in a set 'S' es called a partial order relation. (or) a partial ordering in S. if & only if R es reflexive, antisymmetric & transitive.

i.e 1) Reflexive : $aRa \ \forall \ a \in S$

2) antisymmetric : $aRb \ \& \ bRa \Rightarrow a=b$

3) Transitive : $aRb \ \& \ bRC \Rightarrow aRC \ \forall \ a,b,c \in S$.

A set 'S' together with a partial order relation R es called a partially ordering (or) ordered set (or) poset.

It es denoted by (S, R).

- the partial ordering (or) relation R es often denoted by the symbol $\leq$ (or) $\preceq$.

Hence poset denoted by $(S, \preceq)$ (or) $(S, \leq)$.

In a poset $(S, \leq)$ for two elements a & b, $a \leq b$ means 'a' precedes 'b' & 'b' succeed 'a'. & $a < b$ means 'a' strictly precedes b & 'b' strictly succeed 'a'.

Illustration - 1 :

Show that the relation $\geq$ es a partial order on the set of integers, Z.

Sol: Since

(1) $a \geq a$ for every $a \in Z$, $\geq$ es reflexive.

(2) $a \geq b$ & $b \geq a \Rightarrow a = b$, $\geq$ es antisymmetric.

(3) $a \geq b$ & $b \geq c \Rightarrow a \geq c$, $\geq$ es transitive.

It follows that $\geq$ es a partial order on the set of integers & $(Z, \geq)$ es a poset.

Illustration :-2 :

Consider $P(S)$ as the power set. ie, the set of all subsets of a given set S. Show that the inclusion relation $\subseteq$ is a partial order on the power set $P(S)$.

Sol:- Since

(1) $A \subseteq A \ \forall \ A \in P(S)$, $\subseteq$ is reflexive.

(2) $A \subseteq B$ & $B \subseteq A \Rightarrow A = B$ $\subseteq$ is antisymmetric.

(3) $A \subseteq B$ & $B \subseteq C \Rightarrow A \subseteq C$, $\subseteq$ is transitive.

It follow that $\subseteq$ is a partial order on $P(S)$ & $(P(S), \subseteq)$ is a poset.

Illustration - 3:

Show that the set Z^+ of all positive integers under divisibility relation forms a poset.

Sol:- Since

(1) $n/n \ \forall \ n \in Z^+$, / is reflexive

(2) n/m & $m/n \Rightarrow n = m$, / is antisymmetric.

(3) n/m & $m/p \Rightarrow n/p$, / is transitive.

It follows that / is a partial order on Z^+. & $(Z^+, /)$ is a poset.

Note:

(i) on the set of all integers, the relation division (/) is not a partial order as a & $(-a)$ both divide each other but $a = -a$ ie the relation is not antisymmetric.

(ii) A relation $(<)$ on Z^+ is not a partial order as the relation is not reflexive.

Definition: Let $(S, \leq)$ be a partially ordered set if for every $a, b \in S$. we have either $a \leq b$ (or) $b \leq a$, then $\leq$ is called a simple ordering (or) linear ordering on S, & $(S, \leq)$ is called a total ordered (or) simply ordered set (or) a chain.

Comparability:
The elements a & b of a poset $(S, \leq)$ are called comparable. if either $a \leq b$ (or) $b \leq a$ when a & b are elements of S. such that neither $a \leq b$ nor $b \leq a$.
i.e $a \not\leq b$ are not related.
$a \not\leq b$ are called non-comparable (or) incomparable.

eg: In the poset $(Z^+, /)$ the integers $2 \not\leq 4$ are comparable, since $2/4$ but $3 \not\leq 5$ are incomparable; because neither $3/5$ (nor) 5 divides 3.

Well-ordered set:
A total order $\leq$ on a set 'A' is a well-order if every non-empty subset B of A contains a least element.

Note: Every well-ordered set is totally ordered and a finite totally ordered set is also well-ordered.

Principle of duality: Any statement about lattices involving the operations $\wedge$ and $\vee$

relations $\leq$ and $\geq$ remains true. if $\wedge$ is replaced by $\vee$, $\vee$ by $\wedge$. if $\leq$ by $\geq$ and $\geq$ by $\leq$.

Lattice: A poset $(P, \leq)$ is called a lattice if every 2-element subset of P has both a least upper bound and a greatest lower bound.
i.e lub (x, y) & glb (x, y) exist for every x & y in P.
In otherwords, a lattice as a partially ordered set. $(L, \leq)$ in which every pair of elements $x, y \in L$ has a greatest lower bound & least upper bound.
The greatest lower bound of a subset $(x, y) \leq L$. It is denoted by $x * y$ (or) $x \wedge y$ and the least upper bound by $x \oplus y$ (or) $x \vee y$.

Here, $x \oplus y = x \vee y = \text{lub}\{x, y\}$
$x * y = x \wedge y = \text{glb}\{x, y\}$

Note: Every chain is a lattice.

Properties of lattices:

If 'L' be a lattice, then for every a & b in L, following are true.

(i) $a \vee b = b$ if & only if if $a \leq b$
(ii) $a \wedge b = a$ if & only if if $a \leq b$
(iii) $a \wedge b = a$ if & only if if $a \vee b = b$.

Lattice as Algebraic System:

A lattice is an algebraic structure $(L, \vee, \wedge)$ with two binary operations $\vee$ and $\wedge$ which possesses the idempotent, commutative, associative & absorption properties.

$lub(a,b) = a \vee b$ & $glb(a,b) = a \wedge b$.

Complete lattice: A lattice is called complete if each of its non-empty subsets has a least upper bound & greatest lower bound.

Algebraic System:

A system consisting of a set (or) more operations on the set is called an algebraic system.

It is denoted by $(S, f_1, f_2 \ldots)$ where 'S' is a non-empty set & f_1, f_2 are operations on S.

Algebraic structure:

A non-empty set together with one (or) more than one binary operations is called algebraic structure.

Eg: $(N, +)$, $(Z, +)$, $(R, +, \cdot)$ are all algebraic structures.

Obviously addition & multiplication are both binary operations on the set R of real numbers.

Therefore, $(R, +, *)$ is an algebraic structure Equipped with two operations.

Similarly, $(\mathbb{Z}, +, *)$, $(P(S), \cup, \cap)$ are also algebraic structures.

→ **Boolean Algebra:**

A non-empty set B with two binary operations + and ·, a unary operation ', and two distinct element 0 & 1 is called boolean algebra. It is denoted by $(B, +, \cdot, ', 0, 1)$ if & only if the following properties are satisfied.

Axioms of Boolean Algebra:

If $a, b, c \in B$, then

1. commutative laws:
   (a) $a + b = b + a$
   (b) $a \cdot b = b \cdot a$
2. Distributive law:
   (a) $a + (b \cdot c) = (a + b)(a + c)$
   (b) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
3. Identity laws:
   (a) $a + 0 = a$
   (b) $a \cdot 1 = a$
4. Complement laws:
   (a) $a + a' = 1$
   (b) $a \cdot a' = 0$.

Basic theorems (or Basic laws):

let $a, b, c \in B$ then

1. Idempotent laws:
   (a) $a + a = a$
   (b) $a \cdot a = a$
2. Boundedness laws:
   (a) $a + 1$
   (b) $a \cdot 0 = 0$

3. Absorption laws :

(a) $a + (a \cdot b) = a$ (b) $a \cdot (a + b) = a$

4. Associative laws :

(a) $(a + b) + c = a + (b + c)$ (b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

5. Uniqueness of complement : If $a + x = 1$ & $a \cdot x = 0$, then $x = a'$

6. Involution law : $(a')' = a$

7. (a) $0' = 1$ (b) $1' = 0$

8. De-morgan's law

(a) $(a + b)' = a' \cdot b'$ (b) $(a \cdot b)' = a' + b'$