Date ....
Page No. ....

Binary Composition (BC)

Let A be a non-empty set. A Binary Composition on set A is a mapping $f : A \times A \to A$, is generally denoted by $\circ$. For a pair of elements a, b in A, the image of pair (a, b) under the binary composition '$\circ$' is denoted by $a \circ b$

Eg - on the set $\mathbb{Z}$ let '$\circ$' stand for the binary composition 'addition'. If we write $2 \circ 3 = 5$,

$6 \circ 4 = 10$

If binary composition '$\circ$' represent 'multiplication'.

$2 \circ 3 = 6$

$6 \circ 4 = 24$

- 'Subtraction' is not a binary composition on the set N.

- A Binary Composition $\circ$ is said to be defined on a non-empty set A if $a \circ b \in A \ \forall a, b \in A$.

- In this case, the set A is said to be closed under the binary composition '$\circ$'.

- Let '$\circ$' be the Binary composition on a set A. '$\circ$' is said to be commutative if $a \circ b = b \circ a \ \forall a, b \in A$. It is said to be associative if $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall a, b, c \in A$.

1. $a \circ b = b \circ a$, $\forall a, b \in A$. (Commutative)
2. $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall a, b, c \in A$ (Associative).

Groupoid

Let G be a non-empty set

Groupoid

Let G be a non-empty set on which a Binary composition 'o' is defined some algebraic structure is imposed on G by the composition o. Then (G, o) becomes a algebraic system. This (G, o) is said to be groupoid.

- (Z, +), (Z, -) are examples on groupoid
- (Q, ÷), $r = \frac{p}{q}$, $q \neq 0$

(*) A groupoid (G, o) is said to be commutative groupoid if the Binary composition 'o' is commutative.

(*) An element 'e' in set G is said to an identity element in the groupoid (G, o) if $\boxed{a \circ e = e \circ a = a \; ; \; a \in G}$

(*) An element e in G is said to be a right identity element in the groupoid (G, o) if $a \circ e = a, \forall a \in G$

Eg - (Z, -) → 0 is a right-identity element, $a - 0 = a$.

(*) An element e in G is said to be a left identity element in the groupoid (G, o) if $e \circ a = a, \forall a \in G$

~~Eg -~~

Theorem - If a groupoid (G, o) contains an identity element then that element is unique.

Proof - If possible let there be two identity elements e and f in groupoid (G, o)

Then $a \circ e = e \circ a = a$ and

$a \circ f = f \circ a = a, \forall a \in G$

Now, $e \circ f = e$ [by property of f]

$e \circ f = f$ [by property of e]

$e = f$

Theorem - If a groupoid contains a left identity as well as a right-identity then they are equal and the element is the identity element.

(*) Let e be the left identity and f be the right identity in the groupoid (G, o) then,

$$e \circ a = a \text{ (by property of } e)$$
$$a \circ f = a \text{ (by property of } f)$$

Now, $e \circ f = f$ (by property of e)

$e \circ f = e$ (by property of f)

$\boxed{\Rightarrow e = f}$

This proves that 'e' or 'f' are the same and the unique identity element in the groupoid G.

- Let (G, o) be a groupoid containing the identity element e. An element 'a' in G $(a \in G)$ is said to be invertible if there exists an element 'a'' in G such that $a' \circ a = a \circ a' = e$ (a' is the inverse of a).

∃ Eg - $(Z, +)$; $e = 0$.

$\underbrace{5 + (-5) = 0}_{\text{inverse}}$; $a = 5$, $a' = -5$.

(*) An element $a \in G$ is said to be left-invertible if there exists an element $b \in G$ such that $b \circ a = e$

(*) If e be just a left identity in the groupoid $(G, \circ)$, then an element a in G is said to be left e-invertible if there exists an element b in G $b \circ a = e$ and a is said to be right e-invertible if there exist and element c in G such that $a \circ c = e$. Here b is said to be a left e-inverse of 'a' and 'c' is said to be a right e-inverse of a.

Q) Let $(Z, *)$ be a groupoid where $*$ is defined by $a * b = a + 2b$, $a, b \in Z$. Does any identity element exists in the groupoid.

A). $a * 0 = a + 2 \times 0 = a$.

$\therefore a * e = a$.

$0 * b = 0 + 2b = 2b \neq b$.

$\therefore e * b \neq b$. $(e * b = b)$ [$\because$ def^n of Left Identity].

only right identity element is present i.e 0.

Q) $5 \in Z$. $(Z, *)$, $*$ is defined by $a * b = a + 2b$, $a, b \in Z$.
↳ Is 5 left 0 invertible element?
Is 5 right 0 invertible element.

Ans) Def^n of Left 0 Invertible -

$a' * a = e$.

$a' + 2a = 0$. $\therefore$ Here $a = 5$.

$a' + (2 \times 5) = 0$.
$\Rightarrow a' = -10 \in Z$. $\therefore a = 5$ is a Left Ivertible elemen

Def^n of Right Invertible.

$a * a' = e$.
$\Rightarrow a + 2a' = 0$ $(a = 5)$
$\Rightarrow 5 + 2a' = 0$.
$\Rightarrow 2a' = -5$.
$\Rightarrow a' = -\frac{5}{2} \notin Z$ $\therefore a = 5$ is not a Right Invertible Element.

If $a = 6$, Left Invertible

$a' * a = e$.

$a' + 2a = e \quad [e = 0 \ \& \ a = 6]$
$\Rightarrow a' + 12 = 0$
$\Rightarrow a' = -12 \in Z \quad [\because a = 6$ is a Left- ~~Identity~~ Invertible Element].

Right - Identity Element.

$a * a' = e \quad [e = 0]$
$\Rightarrow a + 2a' = 0 \quad [a = 6]$
$\Rightarrow 6 + 2a' = 0$
$\Rightarrow a' = -3 \in Z \quad [\because a = 6$ is a Right Invertible Element].

Semigroup

1) Let a groupoid $(G, \circ)$ is said to a semigroup if the binary composition '$\circ$' is associative in nature.

$(Z, +)$, $(Z, *)$, $(R, +)$, $(R, *)$ are all examples of semigroup.

(*) Let $(G, \circ)$ is a semigroup and $a \in G$ then $a \circ a \in G$,
$a \circ (a \circ a) = (a \circ a) \circ a$, as $\circ$ is associative.

Dropping the parenthesis, each of them is written $a \circ a \circ a$ Thus $a \circ a \circ a \in G$, $a \circ a \circ a \in G$ . . .

The +ve integral powers of $a \in G$ are defined as follows :

$$a' = a, \quad a^2 = a \circ a, \quad a^3 = a \circ a \circ a, \ldots$$
$$a^{n+1} = a^n \circ a, \quad \forall n \in N$$
$$a^n = a^{n-1} \circ a.$$

~~Let $(S, *)$ be a groupoid~~

Let $(S, \circ)$ be a ~~(groupoid)~~ semigroup & $a \in S$. Then $a^{m+n} = a^m \circ a^n \ \forall \ m, n \in \mathbb{N}$.

$$a^{m+n} = a^m \circ a^n$$
$$= a \circ a \circ a \circ a \cdots \circ a \ (m+n \text{ times})$$

↳ (As the Binary composition is associative

$$\Rightarrow a^m \circ a^n = \underbrace{(a \circ a \circ a \circ \cdots \circ a)}_{m \text{ times}} \underbrace{(a \circ a \circ a \circ \cdots \circ a)}_{n \text{ times}}$$

$$\therefore \boxed{a^{m+n} = a^m \circ a^n}$$

Monoid

An algebraic system $(G, \circ)$ is said to be a monoid if

i) $(a \circ b) \circ c = a \circ (b \circ c)$, $\forall a, b, c \in G$ &

ii) There exist an element e in G such that $e \circ a = a \circ e = a \ \forall \ a \in G$.

Eg - $(\mathbb{Z}, +)$, $(\mathbb{Z}, *)$

Theorem - In a monoid $(G, \circ)$ if any element 'a' be invertible then it has an unique inverse

Proof - If possible let there be two inverses 'a'' and 'a''' $\in G$ then $a \circ a' = e = a' \circ a$

and $a \circ a'' = a'' \circ a = e$. where e being the identity element

Now, $(a' \circ a) \circ a'' = a' \circ (a \circ a'')$ [$\because$ since $\circ$ is associative]

$a' \circ (a \circ a'') = a' \circ e = a'$

$\therefore a' = a''$.

Theorem.

(*) In a monoid $(G, \circ)$ if an element a is left invertible as well as right invertible then a is invertible and has the unique inverse in the monoid.

~~In a monoid if an element~~

<u>Proof</u> - Let e be the identity element and b be a left inverse and c be a right inverse of the element a.

Then we can write,

$b \circ a = e$

$a \circ c = e$

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

Now,

$e \circ c = c$.

<u>GROUP</u> - A non-empty set G is said to form a group with respect to a binary composition if

i) G is closed used the binary composition $\circ$.

ii) Binary composition '$\circ$' is associative.

iii) There exists an element $e \in G$ such that $a \circ e = e \circ a = a$, $\forall a \in G$.

iv) For each element a in G there exists an element a' in G such that $a' \circ a = a \circ a' = e$.

<u>Theorem</u> - A group $(G, \circ)$ contains only one identity element.

<u>Proof</u> - Let there be two identity elements $e, f \in G$, where G is a group $(G, \circ)$. ($e \rightarrow RI$, $f \rightarrow LI$).

Let a be an element $\in (G, \circ)$ then,

$a \circ e = a$ (by property of e)

$f \circ a = a$ (by property of f)

then,

$f \circ e = f$ (By property of e)

$f \circ e = e$ (By property of f)

$\therefore e = f$. [$\therefore$ There is only one identity element].

Q) Prove that in a group only one unique inverse is present for given element.

consider a group (G, o) and an element $a \in G$.
Let a' and a'' be two inverses of the element a then,
By the property of inverse,

$$a' o a = a o a' = e \quad \text{and,}$$
$$a'' o a = a o a'' = e$$, where e is the identity element.

As, we know that 'o' is associative in nature in a group.

$$\therefore (a' o a) o a'' = a' o (a o a'')$$
$$\Rightarrow e o a'' = a' o e$$
$$\Rightarrow a'' = a'$$

<u>Theorem</u> - In a Group (G, o)
i) $a o b = a o c$ implies $b = c$ (left cancellation law)
ii) $b o a = c o a$ implies $b = c$ (right cancellation law)
$\forall\ a, b, c \in G$.

<u>Proof</u> - a) Let (G, o) be a group and $a, b, C \in G$.

Let $a' \in G$ be the inverse of element a

$\boxed{a o b = a o c}$ — from this we can write -

~~$e o a o b = e o$~~

~~We know~~

$$\Rightarrow (a o a') o b = (a o a') o c \quad [\because a o a' = e]$$
$$\Rightarrow e o b = e o c \quad [\because e o n = n, \text{ where } n \in G].$$
$$\Rightarrow b = c \quad [\text{Hence Proved}].$$

Date ....
Kabita Page No. ....

b) Let ~~G be~~ $(G, \circ)$ be a group and $a, b, c \in G$.

Given, $b \circ a = c \circ a$

~~$\Rightarrow (b \circ b') \circ c = c$~~

$\Rightarrow b \circ (a \circ a') = c \circ (a \circ a')$ [∵

$\Rightarrow b \circ e = c \circ e$

$\Rightarrow b = c$