8. Binary Operation :-

Operation are classified according to the number of elements of the set that are involve in it, as unary, binary, ternary..., n-ary and so on.

Extraction of square root is a unary operation in arithmetic. as, one element of the number system is operated upon.

An operation '$\circ$' (or '$*$') which, when applied to two two elements of a set S gives a unique element, also of the same set, is called a binary operation or binary Composition.

Let '$\circ$' be a binary composition on A, by defination, '$\circ$' is a mapping of $A \times A$ into A ie $(a,b) \in A \times A$, $\circ(a,b) \in A$.

* A non-empty set, together with one or more binary operations is called algebric structure. e.g $(N,+)$, $(Z,+,-)$, $(R,+,\cdot)$ are algebric structure.

§. Groupoid :-

Let, S be a non-empty set. 'o' is a binary operation defined on it.
i.e if, $a, b \in S$ then $a \circ b \in S$.
then, (S, o) is called a groupoid.

e.g i) $(N, +)$ is a groupoid.
ii) If $S = \{-2, -1, 0, 1, 2\}$; S is not a groupoid under addition composition.
Since, $2 + 1 = 3 \notin S$

§. Left Identity :-

If $a \circ x = x \ \forall \ x \in S$, then $a \in S$ is called left identity element of the groupoid.
similarly, $a \in S$ is a right identity element of the groupoid, if $x \circ a = x \ \forall \ x \in S$.

(*) The groupoid $(Z, -)$ has no left identity element but zero is a right identity element of it.

§. Semi-group :-

A system consisting of a non-empty set S and an associative binary composition 'o' in S is called a semi-group.

§. Groupoid :-

Let, S be a non-empty set. 'o' is a bina operation defined on it.
i.e if, $a, b \in S$ then $a \circ b \in S$.
then, (S, o) is called a groupoid.

e.g i) $(N, +)$ is a groupoid.
(ii) If $S = \{-2, -1, 0, 1, 2\}$; S is no a groupoid under addition Composition.
Since, $2 + 1 = 3 \notin S$

§. Left Identity :-

If $a \circ x = x \ \forall \ x \in S$, then $a \in S$ is call left identity element of the groupoid.
Similarly, $a \in S$ is a right identity elem of the groupoid, if $x \circ a = x \ \forall \ x \in S$.

(*) The groupoid $(Z, -)$ has no left identity element but zero is a right identity element of it.

§. Semi-group :-

A system Consisting of a non-empty se S and an associative binary Composition 'o' in S is called a semi-group.

e.g $a, b, c \in Z$, the set of all integers.
then we have, $(a+b)+c = a+(b+c)$ and also $(a.b).c = a.(b.c)$.
$(Z,+)$ and $(Z,\cdot)$ are semi-groups as those two Compositions are also associative in Z.

* The system $(Z,-)$ is not a semi-group. since subtraction does not satisfy the associative law.

§. Monoid :-

A system Consisting of a non-empty sets and an associative binary Composition with identity is called a ~~pri~~ monoid.

e.g $(Z,+)$ is a monoid with identity element '0' and $(Z,\cdot)$ is a monoid with identity element '1'.

§. Left inverse :-

For each $a \in S$, the equation $x * a = e$, has a solution in S. The solution x is called ~~inverse~~ left inverse of a. 'e' being identity of S.

* A monoid having inverse of each element forms a group.

Defn:- Group

A non-empty set S of element a, b, c ... forms a group with respect to a binary operation $*$, if the following Properties hold.

(i) For every pair a and $b \in S$, $a*b \in S$ [closure law]

(ii) For any three element $a, b, c \in S$
$a*(b*c) = (a*b)*c$ [associative law]

(iii) $\exists$ in S an element e, called identity element such that;
$e*a = a = a*e$

(iv) For each a in S, $\exists$ an element b in S such that,
$b*a = e = a*b$

(A) { If $(S, *)$ is commutative, then the group is called Commutative group or abelian group.

d. Let $S = \{1, -1, i, -i\}$ PT $(S, \cdot)$ forms a group (3)

e. Show that if every element of a group $(G, \circ)$ be its own inverse, then it is an abelian group.

f. Show that the set Z of all integers forms a group under the binary operation $*$ defined by $a * b = a + b + 1 \; \forall \; a, b \in Z$

Q1. $a^{-1} = a \; ; \; b^{-1} = a.$

$\therefore (a \circ b)^{-1} = (a \circ b)$

$b^{-1} \circ a^{-1} = a \circ b.$

$\therefore b \circ a = a \circ b.$

Properties of group:-

1. Let a, b, c be arbitrary elements of a group $(G, *)$. If $a * b = a * c$ then, $b = c$.

→ Given, $a * b = a * c.$

1. $a \in G$, Let a' is the inverse of a in G

$\therefore a' * (a * b) = a' * (a * c)$

ie, $(a' * a) * b = (a' * a) * c. \; ;$ | associative law.

ie, $e * b = e * c \; ;$ | e be the identity element.

ie, $b = c. \; ;$ | $\because e * b = b.$

this law is known as left cancellation law.

2) In a group $(G, *)$.

(i) The inverse of the inverse of an element is equal to the element. ie, $(a^{-1})^{-1} = a$.

(iii) $(a*b)^{-1} = b^{-1} * a^{-1}$

→ (i) Let, 'e' be the identity element in G, then, $a * a^{-1} = e$. where $a^{-1} \in G$.

also, $(a^{-1}) * a^{-1} = e$.

Now, $(a^{-1})^{-1} * a^{-1} = a * a^{-1}$.

Then by right cancellation law,

$(a^{-1})^{-1} = a$.

8. Right Cancellation law:-

Let, a, b, c be three arbitrary elements of a group $(G, *)$. If, $a*c = b*c$ then

2)(ii) If $a, b \in G$ then $(a*b) \in G$ since G is a group, so, G is closed under the binary operation '*'.

Now, $(a*b)^{-1}$ is the inverse of $a*b$.

$\therefore (a*b)^{-1} * (a*b) = e$; 'e' being id

Again, $(b^{-1} * a^{-1}) * (a*b) = b^{-1} * (a^{-1} * a) * b$

$= b^{-1} * e * b$

$= b^{-1} * b = e$. — (ii)

by (i)

$(a*b)$

$\therefore (a*b$

Q. In a

Prove tha

→ Given

ie,

ie

Now.

ie, e

ie (bo

ie (bo

ie,

$\therefore G$

by (i) and (ii)

$(a*b)^{-1} * (a*b) = (b^{-1}*a^{-1}) * (a*b)$

$\therefore (a*b)^{-1} = (b^{-1}*a^{-1})$; [by left Cancellation law.

Q. In a group $(G, \circ)$, $(a\circ b)^2 = a^2 \circ b^2$ $\forall a, b \in G$. Prove that the group is abelian.

→ Given, $(a\circ b)^2 = a^2 \circ b^2$

ie, $(a\circ b)\circ(a\circ b) = a\circ a\circ b\circ b$.

ie, $a\circ(b\circ a)\circ b = a\circ a\circ b\circ b$; [by

Now, $\bar{a}^1 \circ a \circ (b\circ a)\circ b = \bar{a}^1 \circ a\circ a\circ b\circ b$..

[∵ operating $\bar{a}^1$ in both side.

ie, $e\circ(b\circ a)\circ b = e\circ a\circ b\circ b$. ; [∵ $e \in e_G$.

ie, $(b\circ a)\circ b\circ b^{-1} = a\circ b\circ b\circ b^{-1}$.

ie, $(b\circ a)\circ e = (a\circ b)\circ e$.

ie, $(b\circ a) = (a\circ b)$

$\therefore$ G is abelian.

(11) Examine if the following systems are groups.

(a) $(Z, \circ)$ where $a \circ b = a+b+ab$.

(b) $(R, \circ)$ " $a \circ b = 2(a+b)$.

→ (a) $(a \circ b) \circ c = (a+b+ab) \circ c$

$= a+b+ab+c+ac+bc+abc$

$= a+b+c+ab+bc+ac+abc$

$a \circ e = a \Rightarrow a+e+ae = a$

$e(1+a) = 0$

$e = 0$

$a \circ b = 0 \Rightarrow a+b+ab = 0$.

$3+b+3b = 0$

$4b = -3$

$b = -\frac{3}{4}$

i.e. $b(1+a) = -a$

i.e. $b = \frac{-a}{1+a} \notin Z$.

3. Prove that the set H forms a Commutative group with respect to matrix multiplication

(i) $H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a \in R, b \in R \text{ and } a^2+b^2=1 \right\}$

For next day

1) The inverse of $-i$ in the multiplicative group, $\{1, -1, i, -i\}$ is —

a) 1 b) -1 c) i d) $-i$

2) In a group $(G, \circ)$ each element is its own inverse, then, G is a/an
(a) Commutative semi group (b) Abelian group.
(c) non-abelian group. (d) None.

Before this 2. ⇒ Finite group.

$S = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$. Then, S is a abelian group with respect to multiplication

§ Order of an element :-

Let $(G, \circ)$ be a group and let 'a' an element of G. 'a' is said to be of finite order, if ∃ a (+)ve integer 'n' such that $a^n = G$. Then, order of a is said to be n and is denoted by $o(a)$.

If order of 'a' is not finite, then, 'a' is said to be of infinite order or of order Zero.

Note:- 1) Order of an identity element is 1
2) $o(a) = o(a^{-1})$
3) If $o(a) = n$ then, and $a^m = e$.

then, n is a divisor of m.

4) If $o(a) = n$, then, for a +ve integer 'm', $o(a^m) = \frac{n}{gcd(m,n)}$

Q. In a group $(G, \circ)$, a is an element of order 30. Find the order of a^{18}.

→ $o(a) = 30$, $o(a^{18}) = \frac{30}{gcd(30,18)}$

$= \frac{30}{6} = 5$.

Q. In the group $S = \{1, -1, i, -i\}$ find the order of the elements.

→ $(1)^1 = 1$; $o(1) = 1$.; order of identity is 1.

$(-1)^2 = 1$ $o(-1) = -1$.

$(i)^4 = i^2 \cdot i^2 = (-1)(-1) = 1$ $o(i) = 4$.

$(-i)^4 = (-i)^2(-i)^2 = 1 \cdot 1 = 1$. $(-i)^4 = 4$.

Q. $S = \{1, \omega, \omega^2\}$

$\omega^3 = 1$ $o(\omega) = 3$.

$(\omega^2)^3 = 1$ $o(\omega^2) = 3$.

Group Theory (GE-4)

Q. Let, $(G, *)$ be a group with identity element e. If $a^2 = e \ \forall \ a \in G$, show that G is commutative. (2009)

→ Given, $(G, *)$ is a group.
and $a^2 = e$. ie, $a = a^{-1}$.
Then, for any arbitrary element 'b'
$b = b^{-1}$.

Now, Since G is a group then, $a, b \in G$ implies $(ab) \in G$ $\therefore ab = (ab)^{-1}$ by condition

Now, $ab = (ab)^{-1}$
$= b^{-1}a^{-1}$; | by group property
$= ba$.

So, $\forall \ a, b \in G$, $ab = ba$.
$\therefore (G, *)$ is a Commutative group.

Q. Does the set of all integers form a group under usual multiplication? Give reasons in support of your answer. (2

→ Z be the set of all integers.
$(Z, \cdot)$ does not form a group. ~~under~~

As 1 is the identity element in Z.

As. for any integer $a \in Z$, $1 \in Z$.

$a.1 = a = 1.a$

Let, $b \in Z$ and 'b' be a inverse of 'a' in Z. ;

Then, $b.a = 1 \therefore b = 1/a \notin Z$.

~~for example, $1/5 \in Z$.~~

$\therefore$ inverse of the element does not belong to Z under multiplication.

2. Prove that the set D of all odd integers forms a Commutative group with respect to the Composition '*' defined by $a*b = a+b-1$ $\forall a, b \in D$. (2014)

→ Let $a = 2k+1$, $b = 2p+1$, $k, p \in Z$.

$\therefore a, b \in D$. Now, $a*b = (2k+1)+(2p+1) - 1$

$= 2(k+p)+1$

$\in D$; $\because k+p \in Z$.

So, for any $a, b \in D$. $a*b \in D$.

$\therefore$ D is closed under the binary operation *.

Now for any three element $a, b, c \in D$.

$(a*b)*c = (a+b-1)*c$

$= (a+b-1)+c-1$

$= a+b+c-2$.

and $a*(b*c) = a*(b+c-1)$

$= a+(b+c-1)-1$

$= a+b+c-2$.

$\therefore (a*b)*c = a*(b*c)$.

So, '$*$' is associative in D.

Again let, 'e' be the identity element of D. Then, for any $a \in D$.

$e*a = a$ i.e. $e+a-1 = a$.

$\therefore e = 1 \in D$.

Again let, 'b' be the inverse of 'a' in D.

Then, $b*a = e$.

i.e. $b+a-1 = 1$.

i.e. $b* = (2-a)$.

if $a = 2k+1$ then, $b = 2-2k-1$

$= 1-2k$.

$= -(2k-1)$;

for any integer value of k.;

b is an odd integer. $\therefore b \in D$.

So, since 'a' be any arbitrary element of D. Each element of D has inverse in D.

$\therefore (D, *)$ forms a group.

Q. Define a Commutative group. Show that a group $(G, *)$ is commutative if and only if $(a*b)^2 = a^2 * b^2 \ \forall\ a, b \in G$ (2012)

→ Commutative Group:-

A group $(G, *)$ is said to be commutative if '$*$' is commutative in G. ie if $\forall\ a, b \in G$. $(a*b) = (b*a)$.

2nd part: Given, $a, b \in G$, Commute.

ie $a*b = b*a$. —(i)

$$(a*b)^2 = (a*b)*(a*b)$$
$$= a*(b*a)*b \quad ; \text{ by associative law.}$$
$$= a*(a*b)*b \quad ; \text{ by (i)}$$
$$= (a*a)*(b*b)$$
$$= a^2 * b^2$$

$\therefore (a*b)^2 = a^2 * b^2$.

Conversely, Given,

$$(a*b)^2 = a^2 * b^2$$

ie $(a*b)*(a*b) = (a*a)*(b*b)$

ie $a*(b*a)*b = a*(a*b)*b$; by ax

ie, $(\bar{a}^1 * a)*(b*a)*b = (\bar{a}^1 * a)*(a*b)*b$

ie $e*(b*a)*b = e*(a*b)*b$; 'e' being identity

ie $(b*a)*(b*b^{-1}) = (a*b)*(b*b^{-1})$

ie $(b*a)*e = (a*b)*e$.

$\therefore (b*a) = (a*b)$.

$\therefore$ '$*$' is commutative in G.

8. Subgroup :- Let, $(G, \circ)$ be a group and H be a non-empty subset of G. $(H, \circ)$ is called a subgroup, if it forms a group under the same binary operation.

Example :- $(\mathbb{Q}, +)$ is a group. $\mathbb{Z}$ is a non-empty subset of $\mathbb{Q}$. then, $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.

Note:-

Theorem, Let $(H,\circ)$ be a subgroup of $(G,\circ)$. Then, (i) the identity element $(H,\circ)$ is the identity element of $(G,\circ)$.
(ii) If $a \in H$. then the inverse of a in $(H,\circ)$ is same as the inverse of a in $(G,\circ)$.

§ Theorem, Let $(G,\circ)$ be a group. A non-empty subset H of G forms a subgroup of $(G,\circ)$ if and only if
(i) $a \in H, b \in H \Rightarrow a \circ b \in H$ (ii) $a \in H \Rightarrow \bar{a}^1 \in H$.

§ Theorem, Let, $(G,\circ)$ be a group A non-empty subset H of G forms a subgroup of $(G,\circ)$ if and only if : $a \in H, b \in H \Rightarrow a \circ b^{-1} \in H$.

§ Theorem, Let, $(G,\circ)$ be a group and H, K are subgroups of $(G,\circ)$. Then, $H \cap K$ is a subgroup of $(G,\circ)$.

→ $H \cap K$ is a non-empty subset of G Since 'e' belongs to both H and K, e being the identity element.
Let, $a, b \in H \cap K$, then $a, b \in H$ and ~~$a, b \in$~~
$a, b \in K$.

Since H is a subgroup, $a, b \in H \Rightarrow a \circ b^{-1}$

" K " " " : $a, b \in K \Rightarrow a \circ b^{-1}$

$\therefore a \in H \cap K,\ b \in H \cap K \Rightarrow a \circ b^{-1} \in H \cap K$

~~that~~ These Prove that $H \cap K$ is a Subgro of $(G, \circ)$.

Note The union of two subgroups of a group G is not necessarily a subgroup of G.

Let us Consider, the group $G = (\mathbb{Z}, +)$ and the subgroup $H = (2\mathbb{Z}, +)$. $K = (3\mathbb{Z}, +)$.

$2 \in H \cup K$, $3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$

Q. If 'a' be a fixed element of the group G, Then S.T the set,

$N(a) = \{x \in G \mid xa = ax\}$ is a Subgroup of G.

→ $x, y \in N(a)$. Then, $xa = ax$ and

$ya = ay$ — (1)

Now, $ya = ay \Rightarrow y^{-1}(ya)y^{-1} = y^{-1}(ay)y^{-1}$

$\Rightarrow (y^{-1}y)(ay^{-1}) = (y^{-1}a)(yy^{-1})$

$\Rightarrow e(ay^{-1}) = (y^{-1}a)e$

$\therefore y a y^{-1} = y^{-1} a$. ——(ii)

$\therefore y^{-1} \in N(a)$.

Again, $(xy^{-1})a = x(y^{-1}a)$; | Associative law.

$= x(ay^{-1})$; | by (ii)

$= (xa)y^{-1}$

$= (ax)y^{-1}$; | by (i).

$\therefore (xy^{-1})a = a(xy^{-1})$.

$\therefore xy^{-1} \in N(a)$. Since $x, y \in N(a)$.

$\therefore$ by Neceassary and Sufficient Condition of subgroup $N(a)$ is a subgroup.

8. Def: Ring

A set of element $a, b, c, \cdots$ forms a ring with respect to the binary Composition — addition $(+)$ and multiplication $(\cdot)$ defined on R, if,

(i) $a+b \in R$, for any two elements $a, b \in R$.

(ii) $a+(b+c) = (a+b)+c$ for any three $a, b, c \in R$

(iii) $\exists$ an element denoted by '0' in R such that $a+0 = a \;\forall\; a \in R$.

(iv) For each element $a \in R$, $\exists$ an element denoted by $(-a)$ in R such ~~that~~ that $a+(-a)=0$.

(v) $a+b = b+a$ for any two elements $a, b \in R$.

(vi) $a.b \in R$ for any two elements $a, b \in R$.

(vii) $a.(b.c) = (a.b).c$ for any three element $a, b, c \in R$.

(viii) $a.(b+c) = a.b + a.c$ and

$(b+c).a = b.a + c.a \;\forall\; a, b, c \in R$.

Then, the algebric structure $(R, +, \cdot)$ is a ring.

8. Some elementary Properties of a ring:

(a) If the system $(R, +, \cdot)$ be a ring and $a \in R$ and '0' be the additive identity of the ring R, then,

$$a.0 = 0 \quad , 0.a = 0.$$

$\rightarrow$ $a.0 + a = a$

9. Ring (Def^n): A non-empty set R is said to form a ring with respect to two binary Compositions addition (+) and multiplication (·) defined on it, if the following conditions are satisfied.

(i) $(R, +)$ is a Commutative group.

(ii) $(R, \cdot)$ is a semigroup.

(iii) For any three elements $a, b, c \in R$ the left distributive laws $a.(b+c) = a.b + a.c$ and right " " $(b+c).a = b.a + c.a$ both hold.

* R is said to be a Commutative ring if the multiplication is Commutative.

§ Subring $(R,+,\cdot)$ be a ring and S be non-empty subset of R such that S is stable under '+' and '.' ie,

$a \in S, b \in S \Rightarrow a+b \in S$ and $a.b \in S$.

e.g. $(Z,+,\cdot)$ is a ring. $(2Z,+,\cdot)$ is a subring of the ring $(Z,+,\cdot)$.

§ Field :- A non-empty set F forms a field with respect to two binary operation addition (+) and multiplication (·) defined on it, if the following conditions are satisfied.

(i) $(F,+)$ is a commutative group.

(ii) $(F,\cdot)$ is a " "

(iii) ~~Addition '+'~~ Multiplication '.' is distributive over '+'.

ie, $a.(b+c) = a.b + a.c$

$(b+c).a = b.a + c.a$.

Subfield

Let F be a field. A non-empty subset K is a subfield of F iff

(i) $a, b \in K \Rightarrow a - b \in K$ and

(ii) $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K$.

Q. Show that the set of matrices of the form $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ where $a, b \in R$ forms a ring under matrix addition and multiplicat

Q. S.T in a ring $(R, +, \cdot)$ $\forall a, b, c \in R$

(i) $a.0 = 0$, where '0' is the zero element of R.

(ii) $(a-b).c = a.c - b.c$

→ $a.0 = a.(a+0)$

$= a.0 + a.0$ [left distributive law]

$-(a.0) + a.0 = -(a.0) + [a.0 + a.0]$

ie $0 = [-(a.0) + a.0] + a.0$

ie. $0 = 0 + a.0$

ie $0 = a.0$

$\therefore a.0 = 0 \quad \forall a \in R$, Hence prove.

Q. If R be a ring such that $a^2 = a \; \forall a \in R$; then Prove that $a+a = 0 \; \forall a \in R$.

$\rightarrow (a+a) = (a+a)^2 \quad \because a^2 = a \; \forall a \in R$

$= (a+a)(a+a)$.

$= a(a+a) + a(a+a)$

$= (aa + aa) + (aa + aa)$

$= (a+a) + (a+a) \quad \because a^2 = a$

$\therefore 0 + (a+a) = (a+a) + (a+a)$

$\therefore$ By the right cancellation law,

$0 = a+a$.

Q. Prove that the ring of matrices, $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in R \right\}$ is a field.

$\rightarrow$ Let, $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in R \right\}$.

$(S, +, \cdot)$ is a ring with unity, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity.

Let, $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ & $B = \begin{pmatrix} p & q \\ -q & p \end{pmatrix} \in S$

Then, $A.B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} p & q \\ -q & p \end{pmatrix}$

$= \begin{pmatrix} ap-bq & aq+bp \\ -bp-aq & -bq+ap \end{pmatrix}$

$B.A = \begin{pmatrix} p & q \\ -q & p \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

$= \begin{pmatrix} pq-qb & pb+qa \\ -qa-pb & -qb+pa \end{pmatrix}$

$\therefore AB = BA \quad \forall A, B \in S.$

$\therefore (S, +, \cdot)$ is a commutative ring with unity.

Let, $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ be a non-zero element of S. Then, $(a, b) \neq (0,0)$ and $\det A = a^2+b^2 \neq 0$.

Hence, A^{-1} exist, and $A^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in S$

$A^{-1} \in S.$

$\therefore$ Each non-zero element of the ring S has inverse in S.

Hence $(S, +, \cdot)$ is a field.