- Algebraic system :- A set together with no. of binary operations (defined) on itself is called an algebraic system or algebraic structure.

Eg:- $(\mathbb{Z}, +)$ is a ~~A-S~~ algebraic system

$(\mathbb{R}, +, \cdot)$ is a " "

Properties of binary operations

Let $(G, *)$ is an algebraic system for any elements $a, b, c \in G$

i) Closure :- ~~$\forall$~~ $a, b \in G$

$a * b \in G$

ii) Association :- $\forall\ a, b, c \in G$

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

iii) Identity :- for any $a \in G$ there exist $e \in G$ such that $a * e = e * a = a$.

iv) Inverse :- for any $a \in G$ there exist $b \in G$ such that $a * b = b * a = e$

then b is the inverse of a.

Abilian or Commutative :-

~~for all~~ $\forall a, b \in G$

$a * b = b * a$

Groupoid :- A set G with the binary operation * satisfy only closure property then it is called groupoid.

Eg:-

$D(N, +)$ is a groupoid

Let $1, 2 \in N$ $\quad N = \{1, 2, 3, \ldots\}$

$1 + 2 \in N$

$\therefore (N, +)$ is a groupoid.

$+$ is closed in N.

semigroup

Let S is any ~~set~~ non Empty set with ✓ and ~~circle~~ $\circ$ is binary operation defined on S if $\circ$ satisfies closure & associative property then $(S, \circ)$ is called semi group.

Eg:-

$(N, +)$ is semi group.

Let $1, 2, 3 \in N$

$(1 + 2) + 3 = 1 + (2 + 3)$

$\circ$ satisfy associate

$\therefore (N, +)$ is a semigroup.

Monoid :- Let M be a non empty set and * is a binary operation defined on M then, if (M, *) satisfies closure, Associative and identity properties then (M, *) is called monoid

Group :- An algebraic structure (G, *) is a group if * satisfies the following properties

i) closure
ii) Associative
iii) Identity
iv) Inverse.

Eg:- (Z, +) is a Group

Abilian or Combitative :- A Group (G, *) is said to be abilian group if a*b = b*a

Finite group :- A Group (G, *) is said to be finite group if G contains finite no. of distinct elements otherwise G is infinite group

(8) Let $\mathbb{Z}$ be the set of integers and $\circ$ is the operation defined by $a \circ b = a+b+ab \ \forall a,b \in \mathbb{Z}$ show that $(\mathbb{Z}, \circ)$ is a semi group

closure: $\forall a,b \in \mathbb{Z}$

$a+b \in \mathbb{Z}$

$ab \in \mathbb{Z}$

$a+b+ab \in \mathbb{Z}$

$\therefore a \circ b \in \mathbb{Z}$

$\therefore \circ$ is closed in $\mathbb{Z}$

associate :-

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

L.H.S $(a \circ b) \circ c = \underbrace{(a+b+ab)}_{a} \circ \underset{b}{c}$

$\Rightarrow (a+b+ab)+c+(a+b+ab)c$

$\Rightarrow a+b+c+ab+ac+bc+abc$

R.H.S $= a \circ (b \circ c) = \underset{a}{a} \circ \underbrace{(b+c+bc)}_{b}$

$\Rightarrow a+(b+c+bc)+a(b+c+bc)$

$\Rightarrow a+b+c+abc+ab+ac+abc$

L.H.S = R.H.S

$\circ$ satisfied associate

$\therefore (\mathbb{Z}, \circ)$ is semi group.

8) Show that the set of rational No's under the binary operation o defined as $a \circ b = \frac{a+b}{2}$ is not a semi group.

Q_1 = set of rational no = $\{p/q$ where $q \neq 0\}$

$a \circ b = \frac{a+b}{2}$

closure :- $\forall a, b \in Q$

$a \circ b = \frac{a+b}{2} \in Q$

o is closed.

associative :- to prove $a \circ (b \circ c) = (a \circ b) \circ c$

L.H.S = $a \circ (b \circ c) = a \circ \left(\frac{b+c}{2}\right)$

$\Rightarrow \frac{a + \frac{b+c}{2}}{2} = \frac{2a+b+c}{4}$

R.H.S :- $(a \circ b) \circ c = \frac{a+b}{2} \circ c$

$\Rightarrow \frac{\frac{a+b}{2} + c}{2}$

$\Rightarrow \frac{a+b+2c}{4}$

Since L.H.S $\neq$ R.H.S

o is not associate in Q_1.

30) show that $* x*y = x^y$ is not associate where $x, y \in R$.

Let, $x, y, z \in R$

to prove $x*(y*z) = (x*y)*z$

L.H.S $= x*(y*z) = x*y^z$

$\Rightarrow x^{y^z}$

R.H.S $= (x*y)*z = x^y*z$

$\Rightarrow (x^y)^z$

$\Rightarrow x^{yz}$

$\therefore$ L.H.S $\neq$ R.H.S

$\therefore$ is not associate

Composition table

***

1) prepare composition tables for cube root of unity with $A = \{1, \omega, \omega^2\}$ & show that $(A, \times)$ is a group.

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

i) closure :- since all the entries of the composition table are the elements of A.

$\therefore$ ~~multiplication~~ $\times$ is closed

ii) Associative :- ~~since~~ since $\times$ is always associative on the set of complex numbers $(a, \times)$ is associative

iii) Identity :- from the composition table it is clear that I is the multiplicative identity with

$1 \times 1 = 1$

~~$1 \times 1 = 1$~~

$1 \times \omega = \omega$

$1 \times \omega^2 = \omega^2$

iv) Inverse :- from the composition table it is clear that

$1 \times 1 = 1$

$\omega \times \omega^2 = 1$

$\omega^2 \times \omega = 1$

i.e, $\{1, \omega, \omega^2\}$ possess inverses which are

$1^{-1} = 1$

$\omega^{-1} = \omega^2$

$(\omega^2)^{-1} = \omega$

→ 1 is the self inverse, ω & ω^2 are the mutual inverses.

∴ Each element belongs to set A posses inverses

Hence, (A, ×) is a group.

2) Construct composition table of the roots of the equal $x^4 = 1$ and show that it is a group with respect to general multiplication (×)

$$x^4 = 1$$

$$(x^2)^2 - 1^2 = 0$$

$$(x^2+1)(x^2-1) = 0$$

$$x^2 - 1 = 0, \quad x^2 + 1 = 0$$

$$x = \pm 1 \qquad x^2 = -1$$

$$x = \pm i$$

roots of $x^4 = 1$ A $\Rightarrow \{1, -1, i, -i\}$

×	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 :- Since all the entities of the composition table are the elements of A

∴ × is closed

ii) Associative:- since $*$ is always associative on the set of real & complex no.

$\therefore (A, \times)$ is associative

iii) Identity :- 1 is the multiplicative identity with

~~$1 \times 1 = 1$~~

~~$1 \times 1 = 1$~~

$1 \times 1 = 1$

$-1 \times 1 = -1$

$i \times 1 = i$

$-i \times 1 = -i$

iv) Inverse :-

$1 \times 1 = 1 \Rightarrow 1^{-1} = 1$

$-1 \times -1 = 1 \Rightarrow (-1)^{-1} = -1$

$i \times -i = 1 \Rightarrow i^{-1} = -i$

$-i \times i = 1 \Rightarrow (-i)^{-1} = i$

1 & -1 are self inverses & -i & i are mutual inverses

$\therefore$ Each element in A posses inverses

$\therefore (A, \times)$ is a group.

Addition modulo m

Let m be the positive integer ≥ 2, addition modulo of a & b is denoted by $a +_m b$ and it is defined by the remined of $a+b$ which is divisible by m.

Eg:- 1) $2 +_2 4 = 0$ ⟶ $2\overline{)6}\ \underline{6}\ 0$

2) $3 +_2 4 = 1$ ⟶ $2\overline{)7}\ \underline{6}\ 1$

Multiplication modulo P

Let P be a fixed positive integer the multiplicative modulo P of a & b is denoted by $a \times_p b$ and it is defined by the remainder of $a \times b$ which is divisible by P.

Eg:- 1) $3 \times_4 5 = 3$ $4\overline{)15}\ \underline{12}\ 3$

2) $2 \times_3 7 = 2$ $3\overline{)14}\ \underline{12}\ 2$

10) Prove that $G = \{0, 1, 2, 3, 4\}$ is a group with respect to $+_5$.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

closure:- Since all entries are the elements of G.

∴ $+_5$ is closed in G

associative:-

Addition is always associative

∴ $+_5$ is associative

identity:-

from the composition table it is clear that 0 (zero) is the identity element

$0+0=0$

$1+0=1$

$2+0=2$

$3+0=3$

5) 5C0

$4 + 0 = 4$

Inverse :- from composition table - every element passes in reverse

$0 +_5 0 = 0 \Rightarrow 0^{-1} = 0$

$1 +_5 4 = 0 \Rightarrow 1^{-1} = 4$

$2 +_5 3 = 0 \Rightarrow 2^{-1} = 3$

$3 +_5 2 = 0 \Rightarrow 3^{-1} = 2$

$4 +_5 1 = 0 \Rightarrow 4^{-1} = 1$

$\therefore$ 0 is self inverse & 1, 4 & 2, 3 are mutual inverses.

$(G, +_5)$ is a group.

abelian :- 1, 2, 3, 4, 5 rows are containing same elements to their respected columns

$\therefore +_5$ is combitative.

Hence, $(G, +_5)$ is an abelian group.

$a*b = a+b-ab \quad \forall\, a, b \in Q_1$

$Q_1 = Q - \{1\}$

$a * b = a+b-ab$

closure $\forall\, a, b \in Q_1$

$a+b \in Q_1 \;,\; ab \in Q_1$

$a+b-ab \in Q_1$

$a * b \in Q_1$

$*$ is closed Q_1

associative :- to prove

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

L.H.S :- $a*(b*c) = a*(b+c-bc)$

$\Rightarrow a+(b+c-bc) - a(b+c-bc)$

$\Rightarrow a+b+c-bc-ab-ac+abc$

R.H.S :- $(a*b)*c = (a+b-ab)*c$

($a+b-ab$ = a, c = b)

$\Rightarrow (a+b-ab)+c-(a+b-ab)c$

$\Rightarrow a+b+c-ab-ac-bc+abc$

Identity :-

Consider $a * e = a$

$a + e - ae = a$

$e(1-a) = 0$

$e = 0$

Inverse :-

$a * b = e$

$a + b - ab = 0$

$b(1-a) = -a$

$b = \frac{-a}{1-a} = \frac{a}{a-1}$

abelian :-

$a * b = a + b - ab$

$\Rightarrow b + a - ba$

$\Rightarrow b * a$

$(0, *)$ is an abelian group.

Show that a set of all 2×2 non singular matrices under the general multiplication is monoid

Let A, B, C are non singular matrices

i) Closure :-

Since A, B are non singular matrices if its product AB is also a non singular matrix

ii) associative :-

Since matrix multiplication is always associative

$A(BC) = (AB)C$

where A, B, C are non singular matrices.

iii) Identity :-

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identify matrix which satisfies $AI = IA = A$

∴ Set of non singular matrices with general multiplication is the monoid

Commitative

Let A, B are two non-singular matrices

But $AB \neq BA$

∴ set of non singular matrices with 'x' is a non commutative monoid.

Q) Show that the matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where $\alpha \in R$ forms a group w.r with respect to ~~multi~~ '$\times$'.

Let $G = \{A_\alpha, A_\beta, A_\gamma, \dots\}$

$$A_\beta = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

to prove $(G, \times)$ is a group.

Closure:- $A_\alpha, A_\beta \in G$

$$A_\alpha \times A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta}$$

$A_\alpha, A_\beta \in G$

$A_{\alpha+\beta} \in G$

$\therefore \times$ is closed in G

→ ~~(i)~~ Associative :-

Matrix multiplication is always associative

i.e $A_\alpha \times (A_\beta \times A_\delta) = (A_\alpha \times A_\beta) \times A_\delta$

Identity :-

$$I_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$A_\alpha \times I = I \times A_\alpha = A_\alpha$

∴ × is satisfied Identity property.

Inverse :-

$A_\alpha^{-1} \in G$

to prove $A_\alpha \times A_\alpha^{-1} = I$

$$A_\alpha^{-1} = \frac{\text{adj } A_\alpha}{|A_\alpha|}$$

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

$|A_\alpha| = \cos^2\alpha + \sin^2\alpha = 1$

$$\text{adj } A_\alpha = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$$

$$A_\alpha^{-1} = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$$

$$\therefore A_\alpha \times A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore A_\alpha \times A_\alpha^{-1} = I$

Hence, $(G, \times)$ is a group

Q) If G is a set of all positive rational No. then prove that G is an abilian group under the composition 'o' defined by $a \circ b = \frac{ab}{3}$ $\forall a, b \in Q^+$

closure

If $a, b \in Q^+$ → $a = \frac{1}{2}$ $b = \frac{1}{3}$

$a \circ b = \frac{ab}{3} \in Q^+$ $\quad \frac{\frac{1}{2} \times \frac{1}{3}}{3} \in Q^+$

Hence o is closed in Q^+

Associative:-

to Prove

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

C.H.S:- $a \circ (b \circ c) = a \circ \left(\frac{bc}{3}\right)$

$$\Rightarrow \frac{a\left(\frac{bc}{3}\right)}{3} = \frac{abc}{9}$$

R.H.S $(a \circ b) \circ c = \frac{ab}{3} \circ c$

$$\frac{\left(\frac{ab}{3}\right)c}{3}$$

$$\Rightarrow \frac{abc}{9}$$

$\therefore$ LHS = RHS

Hence $\odot$ satisfies associative property.

Identity :- Let $e \in Q^+$

$$a \odot e = a$$

$$\frac{ae}{3} = a$$

$$\frac{e}{3} = 1$$

$$e = 3$$

$\therefore$ Identity element 3 $e = 3 \in Q^+$

Inverse :-

Let b is the inverse of element $a \in Q^+$

$$a \odot b = e$$

$$\frac{ab}{3} = e$$

$$\frac{ab}{3} = 3 \Rightarrow ab = 9$$

$$b = \frac{9}{a} \in Q^+$$

$\therefore b = \frac{9}{a}$ is the inverse of 'a'

~~$\therefore (Q^+, \odot)$ is a group~~

abelian :-

$$a \circ b = \frac{ab}{3}$$

$$= \frac{ba}{3}$$

$$= b \circ a$$

$\therefore \circ$ satisfies abelian property

Hence $(\mathbb{Q}^+, \circ)$ is a Abelian group

Theorems

TH 1 :- for a, b, c in a group.

i) $a \cdot b = a \cdot c \Rightarrow b = c$ (left cancelation law)

ii) $b \cdot a = c \cdot a \Rightarrow b = c$ (Right cancelation law)

Proof i) consider $a \cdot b = a \cdot c$

Pre operating with a^{-1} on both sides.

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$$

$$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c \quad \text{(associative)}$$

$$e \cdot b = e \cdot c \quad \text{(Inverse)}$$

$$b = c$$

Proof

ii) $b \cdot a = c \cdot a$

Post operating with a^{-1} on both sides

~~$a^{-1}b(bc) = a^{-1}(c \cdot a)^{-1}$~~

$(b \cdot a)a^{-1} = (c \cdot a)a^{-1}$

$(ba)a^{-1})b = (aa^{-1})c$

$eb = ec$

$b = c$

TH:-2 If G is a group

i) the identity element of G is unique

ii) $\forall a \in G$, $\exists$ (their exist) unique inverse in a

iii) $\forall a \in G$, $(a^{-1})^{-1} = a$

iv) $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

Proof

Let $(G, \cdot)$ is a ~~pro~~ group

to prove that G has unique identity elem

On contradiction let us assume that there exi two identity elements e and e' for group G.

for any $a \in G$, e is the identity element $\in G$

$a \cdot e = e \cdot a = a$ ——— ①

for any $a \in G$, $e^{-1} \in G$

$$a \cdot e^{-1} = e^{-1} \cdot a = a \quad \text{—②}$$

from ① & ②

$$a \cdot e = a \cdot e^{-1} \quad \text{(left cancelation law)}$$

$$e = e^{-1}$$ ~~(left cancel~~

∴ Identity element is unique

Our assumpting to there exist two identity elements in G is wrong.

ii) Let, $(G, \cdot)$ is a group

On contradiction let us assume that there exist two inverses a^{-1} & b for the same element a.

∴ for any $a \in G$ its inverse $b \in G$

Such that $a \cdot b = b \cdot a = e$ —①

for any $a \in G$ its inverse $a^{-1} \in G$

$$a \cdot a^{-1} = a^{-1} \cdot a = e \quad \text{—②}$$

from ① & ②

$$a \cdot b = a \cdot a^{-1} \quad \text{[left cancelation law)}$$

$$\Rightarrow b = a^{-1}$$

∴ There exist unique inverse for any element $a \in G$

iii) Let $(G, \cdot)$ is a group

$a \in G$, $a^{-1} \in G$

$a \cdot a^{-1} = a^{-1} \cdot a = e$

$a^{-1} \in G$, $(a^{-1})^{-1} \in G$

$a^{-1} \cdot (a^{-1})^{-1} = (a^{-1})^{-1} \cdot a^{-1} = e$ — (2)

from (1) & (2)

$a \cdot a^{-1} = (a^{-1})^{-1} \cdot a^{-1}$ (R.C.L)

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

iv) $\forall a, b \in G$ $(ab)^{-1} = b^{-1}a^{-1}$

Let $(G, *)$ is a group

to prove $(ab)(b^{-1}a^{-1}) = e$

consider $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ (associative)

$\Rightarrow a(e)a^{-1}$ (Inverse)

$\Rightarrow (ae)a^{-1}$ associative

$= aa^{-1}$ (Identity)

$= e$ (Inverse)

$\therefore$ Inverse of (ab) is $b^{-1}a^{-1}$

2) $(ab)^{-1} = b^{-1}a^{-1}$

Where G is abelian group

$ab = ba$

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