UNIT-4

ALGEBRAIC STRUCTURES

DEFINITIONS:

Set:

Set is a collection of well-defined objects

CLOSURE:

Let S be a non-empty set.

If $a, b \in S$, then $a * b \in S$

S is said to be closure under $*$

or $(S, *)$ is closure.

eg: $(N, +)$ is closure,

$a, b \in N \Rightarrow a+b \in N$

$(N, -)$ is not closure, $1, 2 \in N$ $\quad 1 * 2 = 1-2 = -1 \notin$

ASSOCIATIVE:

If S is a non-empty set then for every $a, b, c \in S$

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

eg: $(N, \times)$ is a Associative

$\forall a, b, c \in N$,

$$\begin{aligned} a * (b * c) &= a * (bc) \\ &= a(bc) \\ &= (ab)c \\ &= (a * b) * c \end{aligned}$$ //

$(Z, -1)$ is not a Associative.

Let $-1, -2, +3 \in Z$

$$(-1 * -2) * 3 = (-1-2) * 3$$

$$= -3-3 = -6 //$$

$$-1 * (-2 * 3) = -1 * (-2-3)$$

$$= -1 * (-5)$$

$$= -1+5$$

$$= 4 //$$

$$(-1 * -2) * 3 \neq -1 * (-2 * 3)$$

EXISTENCE OF IDENTITY ELEMENT:

Let S be a non-empty set and $a \in S$,

If $e \in S$

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

the e is said to be identity element of S.

eg: 0 is the identity element for addition
1 is the identity element for multiplication

EXISTENCE OF INVERSE ELEMENT:

Let S be a non-empty set & $a \in S$

if $\exists\ a^{-1} \in S$ such that

$$a * a^{-1} = a^{-1} * a = e.$$

COMMUTATIVE:

Let S be a non-empty set.

If $a, b \in S$
$\Rightarrow a * b = b * a$ then $(S, *)$ follow commutative

SEMI-GROUP:

Let G be a non-empty set and it said to be semi-Group $(G, *)$ is semi group if its satisfying then two properties.

i) Closure
ii) Associative

MONOID:

Let G be a non-empty set and $(G, *)$ is said to be if its satisfying the following properties.

i) Closure
ii) Associative
iii) $e \in G$ (e is the Identity element)

GROUP:

Let G be a non-empty set its said to be group under the operation of $*$ if satisfying the properties.

i) closure
ii) Associative
iii) $e \in G$ (e is the Identity element)

iv) $a^{-1} \in G$ (a^{-1} is the inverse element of a, $\forall a \in G$)

E

ABELIAN GROUP:

If G is non-empty set its said to be Abelian group under the operator of if satisfying the following properties.

i) Closure $(G,*)$ is close

ii) $(G,*)$ is Associative

iii) $(G,*)$ $e \in G$ (e is the Identity element)

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

v) $(G,*)$ $a * b = b * a$ $\forall a, b \in G$

1) Let 'G' be a set of real number and set of N number and the * is defined by $a * b = a+b-ab$ verify $(G,*)$ is group or not?

Ans: Let $a, b \in G$

Then $a * b = a+b-ab \in G$

$(G,*)$ is closure

let $a, b, c \in G$

Then $a * (b * c) = a * (b+c-bc)$

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

$= LHS //$

$= a+b+c-bc-ab-ca+abc$

$= a+b+c-ab-bc-ca+abc \rightarrow (1)$

RHS

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

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

$= a+b+c-ab-bc-ca+abc.$

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

Then $(G,*)$ is Associative

iii) Let $a \in G$

$a * e = a$

$a + e - ae = a$

$e(1-a) = 0$

$e = 0 \in G$ $\therefore (G,*)$ has Identity $0 \in G$

iv) Let $a \in G$

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

$a + a^{-1} - aa^{-1} = 0$

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

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

$a^{-1} = a/a-1$. $\therefore a^{-1}$ exist except for $a = 1$

we can't find the inverse of $1 \in G$ //

Let G be a set of $R - \{-1\}$
$\forall a, b.\ a * b = a + b + ab$

i) let $a, b \in G$
Then $a * b = a + b + ab \in G$
$(G, *)$ is closure

ii) let $a, b, c \in G$
Then $a * (b * c) = a * (b + c + bc)$
LHS $= a + (b + c + bc) + a(b + c + bc)$
$= a + b + c + ab + bc + ac + abc$

$= a + b + c + ab + ac + bc + abc \rightarrow (1)$

RHS $(a * b) * c = (a + b + ab) * c$
$= (a + b + ab) + c + (a + b + ab)c$
$= a + b + c + ab + ac + bc + abc + abc$

$= a + b + c + ab + ac + bc + abc \rightarrow (2)$

$(1) = (2)$
$a * (b * c) = (a * b) * c$
$(G, *)$ is Associative

iii) Let $a \in G$
$a * e = a$
$a + e + ae = a \rightarrow e(1 + a) = a$
$e(1 + a) = 0$
$e = 0 \in G$
$(G, *)$ has Identity element $0 \in G$

iv) Let $a \in G$
$a * a^{-1} = e$
$a + a^{-1} = e \rightarrow a + a^{-1} + aa^{-1} = 0$
$a^{-1}(1 + a) = -a$
$a^{-1} = -a/1 + a$
$e^{-1} = \frac{a}{-a-1}$ //.

18/09/24.

1) prove that
$a * b = a + b + 1$

i) closure
$a, b \in Z \Rightarrow a * b \in Z$
$a * b = a + b + 1 \in Z$
$\Rightarrow (Z, *)$ is closure

ii) Associative
$\forall\ a, b, c \in Z$
$a * (b * c) = (a * b) * c$

LHS $a * (b * c) = a * (b + c + 1)$
$= a + b + c + 1$
$= a + b + c + 2 \rightarrow (1)$

RHS $(a * b) * c = (a + b + 1) * c$
$= a + b + 1 + c + 1$
$= a + b + c + 2 \rightarrow (2)$

from (1) & (2) LHS = RHS
$a * (b * c) = (a * b) * c$
$(Z, *)$ is associative

iii) Existence of Identity.

$\forall a \in Z \quad \exists e \in Z$

such that $a * e = e * a = a$

$a * e = a$

$a + e + 1 = a$

$e = a - a - 1$

$e = -1 \in Z$

iv) Existence of Inverse

$\forall a \in Z \quad \exists a^{-1} \in Z$

such that, $a * a^{-1} = a^{-1} * a = e$

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

$a + a^{-1} + 1 = -1$

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

$a^{-1} = -2 - a \in Z$

v) Commutative

$a * b = b * a \quad \forall a, b \in Z$

$\Rightarrow a * b = a + b + 1$

$= b + a + 1$

$= b * a$

from the all above $(G, *)$ is abelian.

2) Show that $(Q^+, *)$ is a abelian by the star is defined by $a * b = \frac{ab}{2} \quad \forall a, b \in Q^+$

i) closure

$a, b \in Q^{-1} \Rightarrow a * b \in Q^+$

$a * b = \frac{ab}{2} \in Q^+$

$\therefore (Q^+, *)$ is closure

ii) Associative

$\forall a, b, c \in Q^+$

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

LHS

$a * (b * c) = a * \left(\frac{bc}{2}\right)$

$= \frac{a\left(\frac{bc}{2}\right)}{2} \Rightarrow \frac{abc}{4} \rightarrow (1)$

RHS $(a * b) * c = \frac{ab}{2} * c$

$= \frac{\left(\frac{ab}{2}\right)c}{2} \Rightarrow \frac{abc}{4} \rightarrow (2)$

from (1) and (2) LHS = RHS

$\therefore (Q^+, *)$ is associative

iii) Existence of Identity

$\forall a \in Q^+ \exists e \in Q^+$ such that,

$a * e = e * a = a$

$a * e = a$

$\frac{ae}{2} = a$

$e = \frac{2a}{a}$

$e = 2 \in Q^+$

iv) Existence of Inverse

$\forall a \in Q^+ \exists a^{-1} \in Q^+$ such that $a * a^{-1} = a^{-1} * a = e$

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

$\frac{aa^{-1}}{2} = 2$

$aa^{-1} = 4$

$a^{-1} = \frac{4}{a} \in Q^+$

v) commutative

$a * b = b * a \quad \forall a, b \in Q^+$

$a * b = \frac{ab}{2}$

$= \frac{ba}{2}$

$= b * a$

$\therefore (Q^+, *)$ is abelian

4) Write the caley representation of $(Z_3, +)$ (or) $(Z, +_3)$

$+_3$	0	1	2
0	0	1	2
1	1	2	3
2	2	3	4

Let $Z^*5 = \{[1]\ [2]\ [3]\ [4]\}$ be non-zero elements of $Z5$

Prove that $(Z^*5, 5)$ is an abelian group. write the caley representation table of (Z^*5)

$*_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

(i) closure :

$\forall a, b \in S \Rightarrow a * b \in S$

from the table it is clear $(Z^*5, 5)$ is closure.

ii) Associative :

$\forall a, b \in S \Rightarrow a*(b*c) = (a*b)*c$

from the table it is clear.

$(Z^*5, *5)$ is Associative.

iii) $[1] \in Z_5$ is Identity element.

iv) The inverse of [1] is [1]
The inverse of [2] is [3]
The inverse of [3] is [2]
The inverse of [4] is [4]

v) commutative

$\forall a, b \in S \quad a * b = b * a$

from the table it is clear $(Z^*5, 5)$ is commutative.

1) Let $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

show that G is a group under the operation of multiplication.

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

X	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

$$A \times A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 0+0 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A \times B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1+0 & 0+0 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$A \times C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1+0 & 0+0 \\ 0+0 & 0-1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$B \times A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1+0 & 0+0 \\ 0+0 & 0-1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$B \times B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1+0 & 0+0 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$B \times C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1+0 & 0+0 \\ 0+0 & 0+0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

i) closure :

$\forall a, b \in S \Rightarrow a * b \in S$

from the table it is clear.

$(G, *)$ is closure

ii) Associative.

$\forall a, b \in S \Rightarrow a * (b * c) = (a * b) * c$

from the table it is clear

$(G, *)$ is Associative.

(iii) Identity. $I_1 \in G_1$ is Identity element with respect to $*$.

(iv) Inverse.

The inverse of I is I

The inverse of A is A

The inverse of B is B.

The inverse of C is C.

Hence $(G_1, *)$ is group from the above table.

*	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

18/09/2024:

CYCLIC GROUP: A group $(G_1, *)$ is said to be cyclic if $\exists a \in G_1$ such that every element x in G_1 can be expressed $x = a^n$ for some integer n.

(i) Show that the group $G_1 = \{1, -1, i, -i\}$ is cyclic under usual multiplication and hence find its generators.

$G_1 = \{1, -1, i, -i\}$

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

A group $(G_1, *)$ is said to be cyclic if $\exists a \in G_1$ such that every element x in G_1 can be expressed $x = a^n$ for some integer n.

$i \in G_1$

$i^1 = i$

$i^2 = i \times i = -1$

$i^3 = i \times i \times i = -i$

$i^4 = i \times i \times i \times i = 1$

$i \in G$ can generate the entire group.
$\therefore$ G is cyclic group and $i \in G$ is the generator of G.

NOTE: If a is generator of cyclic group G then a^{-1} is also generator of G.

2) State and Prove Lagrange's Theorem:

STATEMENT:

The order of sub group of a finite group is a divisor of order of group.

[(H, *) be a group and (H, *) is a sub group of G and let order of $o(G) = n$ & $o(H) = m$.
o(H) divides o(G)]

PROVE:

STEP1 Any two co-sets of H either disjoint or identically equal.

* Let aH & bH are any two left co-sets of H.
* If aH & bH are disjoint, our statement (claim) is true
* If aH and bH are not disjoint we have to prove that they are identically equal
that is aH = bH.
* Since aH and bH are not disjoint there exists an element $c \in aH$ & $c \in bH$ this implies

$c = a * h_1$, $c = b * h_2$, $h_1, h_2 \in H$

$a * h_1 = b * h_2$

$a * h_1 * h_1^{-1} = b * h_2 * h_1^{-1}$

$a * e = b * h_2 * h_1^{-1}$

$\boxed{a = b * h_2 * h_1^{-1}} \rightarrow (1)$

Let $x \in aH$,

Then $x = a * h_3$ $h_3 \in H$

$= (b * h_2 * h_1^{-1}) * h_3$ [by eqn (1)]

$= b * (h_2 * h_1^{-1} * h_3) \in bH$

$\therefore x \in bH$ and this implies aH is subset of bH. $\Rightarrow aH \in bH \rightarrow (2)$

Similarly we can prove $bH \in aH \rightarrow (3)$

from (2) and (3)

$$aH = bH$$

STEP 2 : Every element of G belongs to exactly one co-set of H

PROOF :

Let $a \in G$ is arbitary element then clearly

$a = a * e$, $e \in H$

$\Rightarrow a \in aH$

$\Rightarrow a \notin bH$

from step (1) and step (2) we can say that the set of left co-set of H in G form a partition of G.

STEP 3 : Each co-sets has exactly the same number of elements.

PROOF : We have order of $o(H) = m$

$\Rightarrow H = \{h_1, h_2, \ldots h_m\}$: $h_i \neq h_j$

$aH = \{ah_1, ah_2, \ldots ah_m\}$

$\Rightarrow aH$ has m elements

$bH = \{bh_1, bh_2, \ldots bh_m\}$

$\Rightarrow bH$ has m elements.

$\therefore$ Every co-set of H has exactly m elements

Let p be the number of distinct co-sets of H each having m elements therefore the total number of elements is equal to mp

$\Rightarrow n = mp$

$\Rightarrow \frac{n}{m} = p$

$\Rightarrow o(H)$ divides $o(G)$

Hence Lagrange's theorem proved.

GROUP HOMOMORPHISM:

If $(G, *)$ & (G', Δ) are two groups a mapping from G to G' is called group homomorphism. If for $\forall a, b \in G$,

$$f(a * b) = f(a) \Delta f(b)$$