Algebric Structure

* A non empty set "S" is called an algebric structure w.r.t binary operation "*" if $(a*b) \in S$ $\forall a, b \in S$ ie '*' is closure operation on 'S'

ex: 1 $S = \{1, -1\}$

$* \rightarrow *$

$(S, *)$

$1 * -1 = -1$
$1 * 1 = 1$
$-1 * -1 = 1$
} all belongs to set S.

It is Algebric structure as the set S is closed under this operation.

ex 2: $S = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

$* \rightarrow \cup$

$(S, \cup) \rightarrow$ check whether it is algebric structure.

yes $\{\phi\} \cup \{a\} = \{a\}$

ex 3: $A = \{1, 2, 3\}$

$R = \{$ Reflexive Relation $\}$

$(R, \cup)$ ✓

$(R, \cap)$ ✓ set of all Reflexive relation are closed under $\cap$

R = set of Infinite Ref Relation.

$(R, +)$

$(N, *)$ N = set of Natural No.

ex1. $S = \{1, 2, 3\}$

$(S, *)$? A.S → No $\quad 2*3 = 6$ (∉ fail)

sup / huge -5

ex: $(Z, /)$ Z-set of all Integers. (2/3 fail)

↳ Not an A.S.

$(N, -)$

↳ Not an A.S $\quad (1, -2 = -1)$ fails

Semi Group: An algebraic structure $(S, *)$ is called a Semi-Group if $(a*b)*c = a*(b*c)$ $\forall\ a, b, c \in S$ ie associative on 'S'

ex: $(N, +)$? A.S ✓ $(a+b)+c = a+(b+c)$? SG

$(N, *)$? AS ✓ $(a*b)*c = a*(b*c)$? SG ✓

$(Z, -)$? AS ✓ $(a-b)-c = a-(b-c)$; $-1-3 = 1-(-1)$; $-4 = 2$ } SG X

Rational No — $(Q^*, +)$? $a+(-a)=0$ → 0 is not a Rational No.

AS X, SG X

$(Q^*, *)$? AS ✓ SG ✓

$(P(A), \cup)$? AS ✓ SG ✓

$(P(A), \cap)$? AS ✓ SG ✓

OUP Let $(G, *)$ be an algebraic structure where $*$ is binary operation then $(G, *)$ is called Group if following conditions.

C① CLOSURE LAW:

if $a \in G$, $b \in G$ then $a * b \in G$ $\forall a, b \in G$

C② : Associative Law:

if $a, b, c \in G$ then $a * (b * c) = (a * b) * c$ $\forall a, b, c \in G$

C③ : Existence of Identity : there exists $e \in G$ such that $a * e = e * a = a$ $\forall a \in G$

The element 'e' of is called Identity of Group.

C④ Existence of Inverse - Every element of G has an inverse ie for every $a \in G$ there exists $b \in G$ such that $a * b = b * a = e$ is b called as inverse of a & b is written as $(a^{-1}) = b$

C1 – Groupoid

C1 C2 – Semi Group

C1 C2 C3 → Monoid

C1 C2 C3 C4 → Group

C1 C2 C3 C4 C5 → Abelian group.

* A group G is said to be abelian group if it satisfy commutative property

C5 → $a * b = b * a$ $\forall a, b \in G$.

Monoid: A semi-Group $(S, *)$ is called a monoid if there exists an element $e \in S$ such that

$(a * e) = (e * a) = a \quad \forall a \in S$

The element e is called identity element of S with

ex: $(N, *)$? AS ✓, SG, mv $a*e = a$ monoid ✓

$(e = 1)$ ✓

$(N, +)$? AS ✓ SG ✓, mx $a+e = a$ $(e = 0)$ [0 is not present in Natural No. set

Integer set $(Z, +)$? ASv, SGv, mv $a+e = a$ [0 is present in integer

$(P(A), \cup)$? AS ✓ SG ✓, mv $A \cup e = A$ $e = \emptyset$

set set

Group

$(Z, +)$? Group ✓ $a + (-a) = 0$. [Inverse is there]

$(Q, \cdot)$? ✗Group $a \cdot b = 1$ $\left(b = \frac{1}{a}\right)$ for every element a Inverse is possible.

$(Q^*, \cdot)$? → Group. ✓ $0, \frac{1}{0}$ [Since for 0 inverse not possible.]

$(P(A), \cup)$? → Identity element = $\emptyset$ ✓ but Inverse not possible.
✗Group.

→ set of all Rational no. without containing zero.

→ $a \cdot b = 1$ $b = \frac{1}{a}$

Abelian Group: (Commutative Group)

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

ex: $(Z, +)$ Abel ✓ $a + b = b + a$

$(R^*, \cdot)$ Abel ✓ $a * b = b * a$

$(M, *)$ Abel ✗ $A \times B \neq B \times A$.

→ Set of Real No except 0.

$(AB)C = A(BC)$ ✓ Associative (AS)

I → Identity (SG)

Inverse ✓ (M)

so (G).

Which of the following is are true?

① In a group $(G, *)$ with identity element 'e' if $a*a = a$ then $a = e$.

② _____ if $x^{-1} = x \ \forall x \in G$ then G is abelian group.

③ _____ if $(a*b)^2 = a^2 * b^2 \ \forall a, b \in G$ then it is Abelian group.

Ans ① $a * a = a$

$a * a = a * e$

$a * a = a * e$

$a = e$ True

Ans ② $(a*b)^{-1} = b^{-1} * a^{-1}$

$a * b = b * a$

commutative group.

True

Ans ③ a^2, $a * a$

$(P(A), \cup)$ x^2 $x \cup x$

x^3 $x \cup x \cup x$

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

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

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

$b*a = a*b$

Q) $A = \{1, 3, 5, 7, \ldots \infty\}$ and $B = \{2, 4, 6, 8 \ldots \infty\}$ which of the following is a semi-group?

a) $(A, +)$ ✗ $1+3=4$ closure fail

b) $(A, \cdot)$ ✓ (odd * odd = odd) closure is satisfied ✓ Ass ✓

c) $(B, +)$ ✓ even + even = even Cl ✓ A ✓

d) $(B, \cdot)$ ✓ even * even = even closure C ✓ Ass ✓ Associative

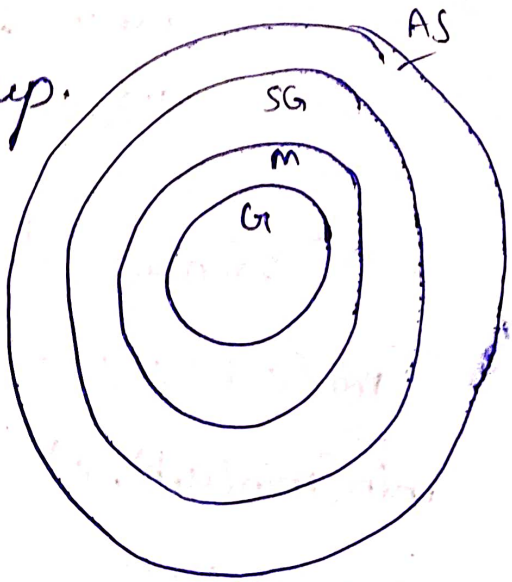
Q) Let $A = \{1, 2, 3, 4 \ldots \infty\}$ and a binary operation $*$ is defined by $a * b = a^b \ \forall a, b \in A$ which of the following is true?

a) $(A, *)$ is semigroup but not monoid

b) $(A, *)$ is a monoid but not group.

c) $(A, *)$ is a group

d) $(A, *)$ is not a semi-group



$a^b \in A \rightarrow$ closure hold

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

LHS $(a^b) * c$ RHS $a * (b^c)$

$(a^b)^c \Rightarrow a^{bc}$

$= a^{bc}$

Associativity fails

$2 \ 3 \ 4$
$a \ b \ c$

2^{3^4} $\quad 2^{3^4}$

$2^{12} \neq 2^{81}$

Q) Let $A = \{x / 0 < x \leq 1\}$ and x is 'A' w.r.t multiplication is

$\{0, 0.1, 0.2 \ldots\}$ real no} then

↳ {all real no which are possible b/w 0 & 1 but not including 0 & including 1 $(0, 1]$

a) A Semigroup but not monoid

b) A monoid but not a group

c) group

d) Not a semigroup.

a	inverse a^{-1}
0.1	$\frac{1}{0.1}$

fails

$(A, \cdot)$ C-AS ✓
A-SG ✓
I-M ✓
Invers

} M

Q) Let A is set of all integers and a binary operation "$*$" is defined by $(a*b) = \min(a,b)$ then $(A,*)$ is

Ans

$1*2 = 1$

$-1*10 = (-1)$

$11*20 = 11$

AS → C
SG → A
} SG only

$(a*b)*c \overset{?}{=} a*(b*c)$

$\min(a,b)*c = a*\min(b*c)$

$\min(\min(a,b),c) \quad \min(a,\min(b,c))$

$\min(a,b,c) \quad \min(a,b,c)$ Associativity Holds

Identity $a*e = a = e*a$ we can't find a number which acts as an identity, $99*100 = 99$ ✓

$101*100 = 100$ ✗

$a*e = a$

so Identity fails Hence only Semi Group

Q) Which of the following is not a group?

a) $\{0, \pm2, \pm4, \pm6, \ldots \infty\}$ w.r.t $+$ Ab G ✓

b) $\{0, \pm k, \pm 2k, +3k, \ldots \infty\}$ w.r.t $+$ Ab. G ✓

c) $\{2^n / n$ is an integer$\}$ w.r.t multiplication.

d) Set of all complex no. w.r.t multiplication.

Ans (c)

$\{\infty, \ldots 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, \ldots \infty\}$

$2^a \times 2^b = 2^{a+b}$ Closure ✓ AS ✓ A SG ✓

for Associative

$(2^a * 2^b) * 2^c = 2^a \times (2^b \times 2^c)$

Identity (1) is present as 2^0 is present.

Inverse $2^a \times I = 1$

$I = \frac{1}{2^a} = 2^{-a}$ ✓

Inverse also present.

Ans (d) $a + ib$ ← Real No

$C1 * C2 =$ complex ✓ C ✓ AS ✓ A SG ✓ Identity ✓

* – $I = 1$

if $a = 1, b = 0$ then we get 1.

$(a+ib) * I = 1$

$I = (a+ib)^{-1}$ or $\frac{1}{a+ib}$

0 is complex no whose inverse is not possible.

so fail for group.

Subgroup: Let $(G, *)$ be a group.

A subset 'H' of G is called a subgroup of G if $(H, *)$ is a group.

~~ex: Let $(G, *)$ be a group with identity elements~~

ex: $G = \{1, -1, i, -i\ *\}$ then

$H = \{1, -1\}, *)$ is subgroup.

Th ①: Let 'H' be ~~a~~ a non-empty subset of group $(G, *)$. H is subgroup of G iff $a * b^{-1} \in H \quad \forall a, b \in H$.

Th ②: Let H be a non-empty finite subset of a group $(G, *)$ H is a sub-group of G iff $(a * b) \in H, \forall a, b \in H$

Th ③: Lagrange Theorem:

If H is a subgroup of finite group $(G, *)$ then $O(H)$ is the divisor of $O(G)$.

The converse of the above theorem need not to be true.

Q) Show that the set $\{1,2,3,4,5\}$ is not a group under addition & multiplication modulo 6.

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

(0 → fail to closure fail)

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Lagrange

$O(G) = m$

$O(H) = n$

ex: ① $O(G) = 10$

$O(H) = 3$ (NO)

so H can't be subgroup of G

ex ② $O(G) = 10$

$O(H) = 5$ (may or may not)

Since 5 divides 10 there is a chance.

Q) Let $G = (\{0,1,2,3,4,5\}, \oplus_6)$ is group. Which of the following is subgroup of G?

a) $H_1 = \{1,3\}$

b) $H_2 = \{1,5\}$

c) $H_3 = \{0,3\}$.

d) $H_4 = \{0,2,4\}$

e) $H_5 = \{0,2,3,5\}$ [No → 6 is not divisible by 4]

a)

	1	3
1	2	(9)
3	1	

does not belongs to H_1.

so H_1 is not closed.

b)

	1	5
1	(2)	0
5		

2 is not present in H_3

c)

	0	3
0	0	3
3	3	0

Can be subgroup

d)

	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Q) $G = \{1, 2, 3, 4, 5, 6\}, \circledast_7$ Which of the following are subgroup of G?

a) $H_1 = \{1, 6\}$

b) $H_2 = \{1, 2, 4\}$

c) $H_3 = \{1, 3, 5\}$

d) $H_4 = \{1, 2, 3, 5\}$

	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

	1	3	5
1	1	3	5
3	3	2	×
5			

Lagrange theorem

The order of each sub-group of a finite group G is a divisor of order of the group G.

Let H be any sub group of order m of a group G of order n.

Cyclic Group: A group $(G, *)$ is called a cyclic group if there exists an element $a \in G$ such that every element of G can be written as a^n for some integer n. Then 'a' is called generating element/generator.

(1) $G = (\{1, -1\}, *) \to (-1)^1 = (-1)^2 = 1$

(2) $G = (\{1, \omega, \omega^2\}, *) \longrightarrow (\omega)^1 = \omega, \ \omega^2 = \omega^2, \ \omega^3 = 1$
$(\omega^2)^1 = \omega^2 \quad (\omega^2)^2 = \omega \quad (\omega^2)^3 = 1$

(3) $G = (\{1, -1, i, -i\}, *) \longrightarrow (i)^1 = i, \ (i)^3 = -i$
$(i)^2 = -1 \quad (i)^4 = +1$

(4) $G = (\{0, 1, 2, 3\}, \oplus_4)$

$1^1 = 1$, $1^2 = 2$, $1^3 = 3$, $1^4 = 0$

$3^1 = 3$, $3^2 = 2$, $3^3 = 1$, $3^4 = 0$

$3+3 = \frac{6}{4} = 2$

$3+3+3 = 9 \equiv 1 \Rightarrow 1$

(*) If $(G, *)$ is a cyclic group with generator a then:

1) a^{-1} is also generator.
2) the order of the generator $= O(G)$

(5) $(\{1, 2, 3, 4\}, \otimes)$

$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3 \quad 2^4 = 1$

$2 \otimes 2 \quad 2 \otimes 2 \otimes 2$

Theorem: Let $(G, *)$ be a cyclic group of order 'n' with generator 'a' then.

(1) The number of generators in $G = \phi(n)$

(2) a^m is also generator of G if $G(m,n) = 1$

Sol

$\phi(3) = 2$ — 1, 2

$\phi(7) = 6$ — 1

$\phi(6) = 2$ — 1, 5

[Relative prime- these is no common factor other than 1.

Ex: (1) Let $(G, *)$ be a cyclic group of order 8 with generator 'a'

(1) No. of Generators in $G = ?$

(2) Which of the following is not generator of G?

✓a) a^2 b) a^3 c) a^5 d) a^7.

$\phi 8$

$S_8 = \{1, 3, 5, 7\}$ $\{a, a^3, a^5, a^7\}$ all will be generator.

$\phi_8 = 4$

Q (2) $\phi(9)$

$S_9 = \{1, 2, 4, 5, 7, 8\}$

$o(9) = 6$

$\phi(77) = \phi(7 \times 11) = \phi(7) \cdot \phi(11)$

$= 6 \cdot 10 = 60$ Ans

Ans (1)

$\phi(35) = \phi(7) \times \phi(5) =$

$6 \times 4 = 24$ Ans → No of Generators.

Exception

$\phi(25) = \phi(5^2)$ $\left[\phi(p^n) = p^n - p^{n-1}\right]$

$\Rightarrow 5^2 - 5^1$

20 Ans

$\phi(125) = \phi(5^3)$

$= 5^3 - 5^2$

$\Rightarrow 125 - 25 = 100$ Ans

$\phi(84) = 2^2 \times 3 \times 7$

$= \phi(2^2) \times \phi(3) \times \phi(7)$

$(2^2 - 2) \times 2 \times 6$

$2 \times 2 \times 6 = 24$ Ans

Q (1) $G(\{1, 2, 3, 4, 5, 6\} \otimes_7)$

(2) $G(\{0, 1, 2, 3, 4\}, +_5)$

(3) $G(\{1, 3, 5, 7\}, \otimes_8)$

$\phi(6) = 2$

Ans ① $S_6 = \{1, 5\}$

$2^1 = 2$
$2^2 = 4$
$2^3 = 1$
$2^4 = 2^3 \cdot 2^1 = 2$
$2^5 = 2^3 \cdot 2^2 = 4$
$2^6 = 2^3 \cdot 2^3 = 1$

[2 can't be a generator]

$3^1 = 3$
$3^2 = 2$
$3^3 = 3^2 \cdot 3$
2×3
$= 6$
$3^4 = 3^2 \cdot 3^2$
$= 2 \times 2 = 4$
$3^5 = 3^2 \cdot 3^3$
$= 2 \times 6$
$= 5$

$3^6 = 3^3 \cdot 3^3$
$= 6 \times 6$
$= 1$

[order of 3 is order of group]

3 is generator

Now as 3 is generator so
3^1 & 3^5 are generator.
so $3^5 = 5$ so 2 generators are 3 & 5 Ans

Ans 2 $\phi(5) = 4$ → [4 generators if cyclic]
$S_5 = \{1, 2, 3, 4\}$

$1^1 = 1$
$1^2 = 2$
$1^3 = 3$
$1^4 = 4$
$1^5 = 0$

so 1 is generator

so $1, 1, 2, 3, 4$ are generator ⇒ 1, 2, 3, 4 Ans

Ans 3 $\phi(4) = 2$

S_4 $\langle 1, 3 \rangle$

$3^1 = 3$

$3^2 = 1$

So 3 is not generator.

$3^3 = 3$

$3^4 = 1$

$5^1 = 5$

$5^2 = 1$

5 is not generate

$7^1 = 7$

$7^2 = 1$

No generate.

No generator for this group.

Hence Not a cyclic group.