Algebraic Structure

Algebraic Structure: A non-empty set which is equipped with some operations and some properties is known as algebraic structure.

$$\boxed{(S, *)}$$

- Groupoid ✓
- Semi-group ✓
- Monoid ✓
- Group ✓
- Abelian Group ✓

Some Properties:

I. Closure: Let 'S' be the given algebraic structure, '*' is the binary operation and a, b are any two elements in S,

If a * b ∈ S then we can say (S, *) follows closure property.

$$\boxed{\forall\, a, b \in S, \quad a * b \in S}$$

$\mathbb{Z} = S = \{ \dots -3, -2, -1, 0, 1, 2, \dots \}$

Binary operation "+"

$2+3 = 5 \in \mathbb{Z}$

$-2+5 = 3 \in \mathbb{Z}$

$0+(-7) = -7 \in \mathbb{Z}$

"+" closed

II. Associative:

$$\forall\, a, b, c \in S, \quad \boxed{a * (b * c) = (a * b) * c}$$

$2+(3+4) = (2+3)+4$

$2+(7) = (5)+4$

$9 = 9$

III. Identity:

$$\forall\, a \in S, \quad \boxed{\exists\, e \in S,} \ni$$

$$\boxed{a * e = e * a = a}$$

For every $a \in S$, There Exists some $e \in S$ such that

$a * e = a$

$2 + 0 = 2$

$3 + 0 = 3$

$4 + 0 = 4$

$\boxed{e = 0}$

IV. Inverse:

$\forall\, a \in S, \quad \exists\, b \in S, \quad \ni$

$$\boxed{a * b = b * a = e}$$

$a * b = e$

$-2 + (2) = 0$

$-5 + (5) = 0$

$9 + (-9) = 0$

$0 + 0 = 0$

$\boxed{e^{-1} = e}$

V. Commutative:

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

$$\boxed{a * b = b * a}$$

$2+3 = 3+2$

$$\boxed{\begin{array}{c}(Z, +) \subseteq (R, +) \\ Z \subseteq R\end{array}}$$

$(H, *) \subseteq (G, *)$

Classification of Algebraic Structure

Groupoid (1)	Semi-group (2)	Monoid (3)	Group * (4)	Sub-Group (4)	Abelian (5)
1) Closure	1) Closure	1) Closure	1) Closure	1) Closure	1) Closure
	2) Associative	2) Associative	2) Associative	2) Associative	2) Associative
		3) Identity	3) Identity	3) Identity	3) Identity
			4) Inverse	4) Inverse	4) Inverse
					5) Commutative
					commutative

Sub-Group:

Let (G, *) be a group, H is a subset of 'G' and (H, *) is also group then we can say (H, *) is a subgroup of (G, *)

$$(H, *) \subseteq (G, *)$$

$$Z \subseteq R$$

$$(Z, +) \subseteq (R, +)$$

Q. Check the properties of commutative and associative on binary operation '*' is defined by $a * b = a^b$, $\forall$ a, b $\in$ N

Given binary operation $*$ defined by

$$\boxed{a*b = a^b}$$

Commutative:

Take x, y (or) $2, 3$

consider $2*3 = 2^3 = 8$

$3*2 = 3^2 = 9$

$2*3 \neq 3*2$

'$*$' is NOT commutative

Associative:

Take 2, 3, 4.

$2*(3*4) = 2*(3^4)$

$= 2*(81) = 2^{81}$

$(2*3)*4 = (2^3)*4$

$= 8*4$

$= 8^4 = 2^{12}$

$\therefore 2*(3*4) \neq (2*3)*4$

NOT associative

Q. Show that the set of all rational number Q – {0} forms an abelian group under composition '*' defined by $a * b = \frac{ab}{2}$

Sol Given set $= Q - \{0\} = S$ (say)

Binary operation $\boxed{a * b = \frac{ab}{2}}$

I. closure: x, y.

$x * y = \frac{xy}{2} \in S$

$(S, *)$ is closed

II. Associative : x, y, z.

$x * (y * z) = x * \frac{(yz)}{2}$

$= \frac{x\left(\frac{yz}{2}\right)}{2} = \frac{xyz}{4}$

$(x * y) * z = \left(\frac{xy}{2}\right) * z$

$= \frac{xyz}{4}$

$\therefore (S, *)$ is associative

III. Identity: Let $e \in S$ such that

$a * e = a$

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

$\boxed{e = 2}$

IV Inverse : Let us suppose there is some $b \in S$ such that

$$a * b = e$$

$$\frac{ab}{2} = 2$$

$$\boxed{b = \frac{4}{a}}$$

Inverse of 'a' $= \frac{4}{a}$.

V Commutative :

Take $x * y = \frac{xy}{2}$

$$= \frac{yx}{2}$$

$$= y * x$$

$(S, *)$ is commutative

$(S, *)$ is an abelian group

S.T. set of rational numbers and some conditions with binary operation '$*$' defined by $\boxed{a*b = a+b-ab}$ is an abelian group

Closure :

Associative :

Identity : $e \in S$

$$a*e = a$$

$$\cancel{a}+e-ae = \cancel{a}$$

$$e(1-a) = 0$$

$$\boxed{e = 0}$$

Inverse:

$$a*b = e$$

$$a+b-ab = 0$$

$$a+b(1-a) = 0$$

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

commutative: $a*b = a+b-ab$

$$= b+a-ba$$

$$= b*a$$

Q. Show that $[G, +_6]$ is a group where $G = \{0, 1, 2, 3, 4, 5\}$

Composition Table

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

$e =$

$4 * 2 = 0$

All the entries of composition table belongs to G

$\therefore (G, +_6)$ is closed

Associative:

2, 3, 4

$2 +_6 (3 +_6 4) = 2 +_6 (1)$

$= 3$

$(2 +_6 3) +_6 4 = 5 +_6 4$

$= 3$

$3 +_6 7 = 6\overline{)10}(1$

$\underline{6}$

$\boxed{4}$

$5 +_6 7 = 0$

Identity

$0 +_6 0 = 0$

$1 +_6 0 = 1$

$2 +_6 0 = 2$

$3 +_6 0 = 3$

$4 +_6 0 = 4$

$5 +_6 0 = 5$

$\therefore$ Identity Exists

Inverse

$a * b = e$

$1 +_6 5 = 0$

$2 +_6 4 = 0$

$3 +_6 3 = 0$

$4 +_6 2 = 0$

$5 +_6 1 = 0$

$0 +_6 0 = 0$

element	Inverse
$1 \longrightarrow$	5 ✓
$2 \longrightarrow$	4
$3 \longrightarrow$	3
$4 \longrightarrow$	2
$5 \longrightarrow$	1 ✓
$0 \longrightarrow$	0

$(G, +_6)$ follows Inverse.

Commutative: $a * b = b * a \quad \forall a, b$

$$2 +_6 3 = 3 +_6 2$$

All entries of a row are identically equals to corresponding columns.

$(G, +_6)$ is commutative

$(G, +_6)$ Abelian group

Order of Group (Vs) Order of element:

* The number of the elements (Cardinality) of a given group is known as order of group, O(G)

* Let (G, *) be a group and an element $a \in G$,

If $\boxed{a^n = e}$ (where n is a least positive integer). Then 'n' is called order of the element 'a'

$G = \{0, 1, 2, 3, 4, 5\}$ $+_6$

$O(G) = 6$

element 2:

$2^2 = 2 * 2 = 2 +_6 2 = 4$

$2^3 = 2^2 +_6 2 = 4 +_6 2 = 0 = e$

$\boxed{ord(2) = 3}$

element 4:

$4^1 = 4$

$4^2 = 4 +_6 4 = 2$

$4^3 = 4^2 +_6 4 = 2 +_6 4 = 0 = e$

$\boxed{ord(4) = 3}$

$4^3 = 4^6 = 4^9 = 0$

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

element '0': $0^1 = 0\ (e)$

element '1': $1^1 = 1$ ✓

$1^2 = 1 +_6 1 = 2$ ✓

$1^3 = 1^2 +_6 1 = 2 +_6 1 = 3$ ✓

$1^4 = 1^3 +_6 1 = 3 +_6 1 = 4$ ✓

$1^5 = 1^4 +_6 1 = 4 +_6 1 = 5$ ✓

$1^6 = 1^5 +_6 1 = 5 +_6 1 = 0$ ✓ (e)

$\boxed{ord(1) = 6}$

element '3': $3^1 = 3$

$3^2 = 3 +_6 3 = 0\ (e)$

$\boxed{ord(3) = 2}$

element '5':

$5^1 = 5$ ✓

$5^2 = 5 +_6 5 = 4$ ✓

$5^3 = 4 +_6 5 = 3$ ✓

$5^4 = 3 +_6 5 = 2$ ✓

$5^5 = 2 +_6 5 = 1$ ✓

$5^6 = 1 +_6 5 = 0$ ✓ (e)

$\boxed{ord(5) = 6.}$

element		order
1	$\longrightarrow$	6
2	$\longrightarrow$	3
3	$\longrightarrow$	2
4	$\longrightarrow$	3
5	$\longrightarrow$	6
0	$\longrightarrow$	1

divides

$\boxed{\text{ord}(G) \;\; 6}$

$a \in G,$

ord of element divides order of G

Generators & Cyclic Group:

Let (G, *) be a group and a ∈ G, If every element of (G, *) can be expressed as integral power of 'a' then 'a' is called generator of 'G' and group (G, *) is known as cyclic group.

$G = \langle a \rangle$

$G = \{0, 1, 2, 3, 4, 5\}$

$G = \{1^6, 1^1, 1^2, 1^3, 1^4, 1^5\}$

$\boxed{G = \langle 1 \rangle}$

$1, 5 \xrightarrow[\text{co-primes}]{} 6$

$1^1, 1^5$

$G = \{0, 1, 2, 3, 4, 5\}$

$G = \{5^6, 5^5, 5^4, 5^3, 5^2, 5^1\}$

$G = \langle 5 \rangle$

$1 * 5 = e$

$1 +_6 5 = 0$

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

* Every cyclic group is an abelian group.

* If 'a' is the generator of group (G, *) then a^{-1} is also be generator.

* Every group of order ≤ 6 is an abelian.

* Every group of prime order is cyclic

Q. Analyse (G, x) where G = {1, -1, i, -i}

Composition

x	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

e

all entries $\in G$,

(G, x) is closed

Take 1, -1, i

$i^2 = -1$

$-i^2 = 1$

we can prove

$1 \times (-1 \times i) = (1 \times -1) \times i$

(G, x) is Associative.

From C.T. $\boxed{e = 1}$

Inverse:

$1 \longrightarrow 1$

$-1 \longrightarrow -1$

$i \longrightarrow -i$

$-i \longrightarrow i$

(G, x) is commutative

$G = \{1, -1, i, -i\}$, $(G, \times)$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\text{ord}(G) = 4$

Divisors of $4 = 1, 2, 4$

ord of ele $= 1, 2, 4$

element 1 : $1^1 = 1$ $\quad$ $\text{ord}(1) = 1$

element -1 : $(-1)^1 = -1$

$(-1)^2 = -1 * -1 = -1 \times -1 = 1 \ (e)$ $\quad$ $\text{ord}(-1) = 2$

element i : $i^1 = i$

$i^2 = -1$

$i^3 = i^2 \times i = -1 \times i = -i$

$i^4 = i^3 \times i = -i \times i = -i^2 = 1 \ (e)$ $\quad$ $\text{ord}(i) = 4$

element -i : $(-i)^1 = -i$

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

$(-i)^3 = (-i)^2 \times (-i) = -1 \times -i = i$

$(-i)^4 = (-i)^3 \times (-i) = i \times -i = -i^2 = -1$

$\text{ord}(-i) = 4$

Lagrange's theorem

Element	order
1	1
-1	2
i	4
$-i$	4

divides

$\boxed{\begin{matrix} \text{ord}(G) \\ 4 \end{matrix}}$

Cyclic & Generators:

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

$G = \{i^4, i^2, i^1, i^3\}$

$G = \{(-i)^4, (-i)^2, (-i)^3, (-i)\}$

$G = \langle i \rangle$

$G = \langle -i \rangle$

Co-primes :

Two numbers a, b are said to co-primes $\Longleftrightarrow gcd(a,b)=1$

(or)

a,b are Relative primes $\Longleftrightarrow HCF(a,b)=1$

examples co-primes : $(8,15)$,

$(9,16)$

$(3,7)$

$(5,6)$

$(4,9)$

Q. How many generators are there for a cyclic group of order '8'?

ord of group $G = o(G) = 8$

$G = \{-, -, -, -, -, -, -, -\}$

Let us consider generator of $G = a$

$G = \langle a \rangle$

$G = \{\underline{a^1}, a^2, \underline{a^3}, a^4, \underline{a^5}, a^6, \underline{a^7}, a^8\}$

$\downarrow$

e

a^1, a^3, a^5, a^7 are 4 generators

ord(a) = 8

Co-primes of 8 = 1, ~~2~~, 3, ~~4~~, 5, ~~6~~, 7

No. of generators = 4

Euler Function

Q: How many generators are there for a cyclic group of order '9'?

Lagrange's Theorem:

Let (G, *) be a group and (H, *) be a subgroup of G then order of subgroup (H, *) is always divides of group (G, *)

Let (G, *) be a group and an element $a \in G$, then the order of element 'a' always divides order of group

$$O(H) \mid O(G) \checkmark$$

$$O(a) \mid O(G)$$

Q. The set {1, 2, 3, 5, 6, 7, 8, 9} under multiplication modulo 10 is not a group. Given below are four possible reasons. Which one of them is false? **[2006 : 1 Mark]**

a) It is not closed

b) 2 does not have an inverse

c) 3 does not have an inverse (False)

d) 8 does not have an inverse

$G = \{1, 2, 3, 5, 6, 7, 8, 9\}$

(a) closure: $\forall a, b \in S, \ a * b \in S$

$2 * 5 = 2 \times_{10} 5 = 0 \notin G$

$(G, \times_{10})$ is not closed (TRUE reason)

$\Rightarrow (G, \times_{10})$ is NOT group

(c) element '3': $a * b = e$

$3 * 7 = 3 \times_{10} 7 = 1 \ (e)$

Inverse of element $(3) = 7$

(b) Inverse: $a * b = e$

$2 * 1 = 2$

$2 * 3 = 2 \times_{10} 3 = 6$

$2 * 5 = 0$

$2 * 6 = 2$

$2 * 7 = 4$

$2 * 8 = 6$

$2 * 9 = 8$

$2 * 2 = 4$

'2' does not have inverse (TRUE)

Q. Which one of the following is NOT necessarily a property of a Group?

[2009 : 1 Mark]

a) Commutativity

b) Associativity

c) Existence of inverse for every element

d) Existence of identity

Q. For the composition table of a cyclic group shown below:

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

element 'c':

$c^1 = c$

$c^2 = c * c = b$

$c^3 = c^2 * c = b * c = d$

$c^4 = c^3 * c = d * c = a$

Which one of the following choices is correct? **[2009 : 2 Marks]**

a) a, b are generators

b) b, c are generators

c) c, d are generators

d) d, a are generators

element 'a':

$a^1 = a$

$a^2 = a * a = a$

element 'b': $b^1 = b$

$b^2 = b * b = a$

$b^3 = b^2 * b = a * b = b$

Q. A binary operation ⊕ on a set of integers is defined as $x \oplus y = x^2 + y^2$. Which one of the following statements is TRUE about ⊕?

[2013 : 1 Mark]

a) Commutative but not associative

b) Both commutative and associative

c) Associative but not commutative

d) Neither commutative nor associative

$x * y = x^2 + y^2$
$= y^2 + x^2 = y * x$
commutative

Take $x * (y * z) = x * (y^2 + z^2)$
$= x^2 + (y^2 + z^2)^2$

RHS $= (x * y) * z = (x^2 + y^2) * z$
$= (x^2 + y^2)^2 + z^2$

NOT associative

Q. Let G be a group of 15 elements. Let L be a subgroup of G. It is known that L ≠ G and that the size of L is at least 4. The size of L is ________________.

(GATE-14-Set3)

order $(G) = 15$

'L' is subgroup of G

order of subgroup of can be $1, 3, 5, 15$

possibilities $|L| = o(L) = \cancel{1}, \cancel{3}, 5, \cancel{15}$

$L \neq G, \ |L| \geq 4$

size of $L = 5$

Q. The set {1, 2, 4, 7, 8, 11, 13, 14} is a group under multiplication modulo 15. The inverse of 4 and 7 are respectively. **(GATE-05)**

a) 3 and 13

b) 2 and 11

c) 4 and 13

d) 8 and 14

Binary operation $= \times_{15}$

$G = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$(4)^{-1} = ?$

$(7)^{-1} = ?$

option - a: $4 * 3 = e$

$7 * 13 = e$

check $4 * 3 = 4 \times_{15} 3 = 12 \neq e$

(b) $4 * 2 = 4 \times_{15} 2 = 8 \neq e$

(c) $4 * 4 = 4 \times_{15} 4 = 1 = e$

$7 * 13 = 7 \times_{15} 13 = 1 = e$

$\boxed{a * b = e}$

Q. Let G be a group of 35 elements. Then the largest possible size of a subgroup of G other than G itself is ________. **(GATE-20)**

1, 5, 7, 35

1, 5, 7, ~~35~~

*

7

Q. Let A be the set of all nonsingular matrices of order n × n over real numbers and let * be the matrix multiplication operator. Then **(GATE-95)**

a) A is closed under * but ⟨A, *⟩ is not a semigroup

b) ⟨A, *⟩ is a semigroup but not a monoid

c) ⟨A, *⟩ is a monoid but not a group

d) ⟨A, *⟩ is a group but not an abelian group

Non-singular = $\det A \neq 0$

$\Rightarrow$ Inverse exists

$\Rightarrow A^{-1} = \frac{\text{adj} A}{\det A}$

$A = \{ \underset{A_1}{[\ ]}, \underset{A_2}{[\ ]}, [\ ]_{n\times n}, \ldots \}$

$\underset{n\times n}{A_1} \times \underset{n\times n}{A_2} = [\ ]_{n\times n}$

$A \times B$

$(A, *)$ closed.

Associative:

$$A_1(A_2A_3) = (A_1A_2)A_3$$

Commutative

$$A \times B \neq B \times A$$

Identity: $\forall a \in S,\quad a * e = e * a = e$

$$A \times I = I \times A = A$$

$I_{n \times n}$ Identity

Inverse: $\forall a \in S,\quad a * b = b * a = e$

$$A \times B = B \times A = I$$

$$A \times A^{-1} = A^{-1} \times A = I$$

Q. The following is the incomplete operation table of a 4-element group **(GATE-04)**

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

The last row of the table is

$ord(G) = 4 \leq 6$

$\therefore G$ is an abelian group

$x * y = y * x, \quad \forall x, y$

a) c a e b

b) c b a e

c) c b e a

d) c e a b

Q. Let G be a finite group on 84 elements. The size of a largest possible proper subgroup of G is _______. **(GATE-18-CSIT)**

If H is a subgroup G and $H \neq G$ Then H is known proper subgroup of G

$$\boxed{(H,*) \subseteq (G,*)}$$

Subgroup

$$\boxed{(H,*) \subset (G,*)}$$

proper subgroup

$o(G) = 84$

$84 = 1 \times 84$ ✓
$= 2 \times \boxed{42}$ *
$= 3 \times 28$
$= 4 \times 41$

size of largest possible pro. subgroup = 42 *

Q. Let G be a group of order 6, and H be a subgroup of G such that $1 < |H| < 6$.

(GATE-21-Set1)

a) Both G and H are always cyclic

b) G is always cyclic, but H may not be cyclic

c) G may not be cyclic, but H is always cyclic

d) Both G and H may not be cyclic

$ord(G) = 6$

$\therefore$ G is an abelian group

$ord(G) = 6$

possible $o(H) = \cancel{1}, \boxed{2, 3}, \cancel{6}$

$1 < o(H) < 6$

$o(H) = 2$ or 3 (prime)

We know that every group of prime order is a cyclic. Hence H is cyclic

Q. Let S = {0,1,2,3,4,5,6,7} and $\otimes$ denote multiplication modulo 8, that is, $x \otimes y = (xy) \bmod 8$.

a) Prove that ({0,1}, $\otimes$) is not a group **(GATE-2000)**

b) Write 3 distinct groups (G, $\otimes$) where $G \subset S$ and G has 2 elements.

(a)

$\times_8$	0	1
0	0	0
1	0	1

Inverse: $a * b = e$

$1 * 1 = 1 \times_8 1 = 1 = e$

$0 * \ = e$

$(0)^{-1}$ = Doesnot exists

(b) {1,3}, {1,5}, {1,7}

$\times_8$	1	3
1	1	3
3	3	1

[{1,3}, $\times_8$] follows clos, Assoc, Ident, and inverse property.

It is group subgroup

$\boxed{a * b = e}$