CH-4 - Group theory

* **Set** : $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

e.g. $2, 3 \in \mathbb{N}$.

$2-3 = -1 \notin \mathbb{N}$.

* **Binary Operation** : $+, -, \times, \div$

Let A be a non-empty set and $*$ be any operation on A. A binary operation $*$ in a set A is a function from $A \times A$ to A.

e.g. i.e $f: A \times A \to A$ then f is said to be a binary operation on set A.

e.g. ① $2, 3 \in \mathbb{N}$ & $(\mathbb{N}, +)$.

$\Rightarrow 2+3 = 5 \in \mathbb{N}$.

$\therefore +$ is binary operation for set $\mathbb{N}$.

② $(\mathbb{N}, -) \Rightarrow 2-3 = -1 \notin \mathbb{N}$

$\therefore -$ is not binary operation for set $\mathbb{N}$.

③ $(\mathbb{N}, \div) \Rightarrow 2 \div 3 = 2/3 \notin \mathbb{N}$

$\Rightarrow \div$ is not binary operation for set $\mathbb{N}$

④ $(\mathbb{N}, \times) \Rightarrow 2 \times 3 = 6 \in \mathbb{N}$

$\therefore \times$ is binary operation on set $\mathbb{N}$.

* **Properties of binary operation** :

① closure Property

② Associative Property

(3) Identity Property
(4) Inverse Property
(5) Commutative Property
(6) Idempotent

If the operation following

(1) closure = Algebraic structure

(2) closure + Associative = Semigroup.

(3) closure + Asso. + Identity = Monoids

(4) closure + Asso. + Identity + Inverse = Group.

(5) closure + Asso. + Identity + Inverse + Commutative = Abelian Group.

Algebraic Structure:

A non-empty set G has with one or more binary operation is called an algebraic structure.

- Suppose, * is a binary operation on G. Then (G, *) is an Algebraic Structure.

e.g. $(N, +)$, $(N, \cdot)$, $(I, +)$, $(I, \cdot)$, $(Q, +)$, $(Q, \div)$, $(N, +, \cdot)$ etc. are example of Algebraic structure.

- But $(N, -)$, $(N, \div)$ are not Algebraic Structure.

* **Group** : Let G be a non-empty set with a binary operation. We say G is a Group under this operation if the following four properties are satisfied.

(1) **closer** :
For all $a, b \in G \Rightarrow a * b \in G$.

(2) **Associative** : For all $a, b, c \in G$
$\Rightarrow (a * b) * c = a * (b * c)$.

(3) **Identity** : There is an element e (called the identity) in G, such that $a * e = e * a = a$, for all $a \in G$.

(4) **Inverse** : For each element a in G, there is an element b in G (called an inverse of a) such that $a * b = b * a = e$.
or Then b is called inverse of a and we write $b = a^{-1}$.
i.e. $a * a^{-1} = a^{-1} * a = e$.

* **Semi Group** : A non-empty set G with binary operation $*$ is known as semi-Group if the binary operation satistics the following properties.

(1) closure : $\forall\ a, b \in G \Rightarrow a * b \in G$

(2) Associative : $\forall\ a, b, c \in G$

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

Ex-1 Show that the set of integers forms an Group under

Ex-1 Q.(-1) G is the set of Rationals except -1. binary operation * is defined by $a * b = a + b + ab$. Show that it is a Group.

$\Rightarrow$ (1) closure : Let $a, b \in G$.

$\Rightarrow a * b = a + b + ab \in G$

$\therefore$ closure is satisfied.

(2) Associative : Let $a, b, c \in G$.

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

$\Rightarrow$ LHS $= b * c$

$= b + c + bc = x$

$\Rightarrow a * x = a + x + ax$.

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

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

$\Rightarrow$ RHS $= (a + b + ab) * c$.

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

$\therefore$ LHS = RHS

$\therefore$ Asso. Property is satisfied.

(3) Identity : Let $a \in G$.

$\Rightarrow a * e = e * a = a$

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

$\Rightarrow e + ae = 0$

$\Rightarrow e(1 + a) = 0. \Rightarrow e = 0$ &

(4) Inverse : let $a \in G$, & a^{-1} is inverse of a.

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

$\Rightarrow a * a^{-1} = e \Rightarrow a + a^{-1} + a \cdot a^{-1} = e$

$\Rightarrow a + a^{-1}(1+a) = 0$.

$\Rightarrow a^{-1} = \frac{-a}{1+a}, \quad a \neq -1. \in \mathbb{Q}$

$\therefore$ Inverse Property exist.

$\therefore (G, *)$ is Group.

Ex-2 Show that the set of all positive rational number $\mathbb{Q}^+$ form a group under composition operation define by $a * b = ab/2$.

$\Rightarrow$ Given that, $G = \mathbb{Q}^+ =$ set of all Positive rational number.

(1) closure : let $a, b \in G = \mathbb{Q}^+$.

$\Rightarrow a * b = \frac{ab}{2} \in G \in \mathbb{Q}^+$.

b'coz if a & b are positive rational number then $ab/2$ is also posi. rati. number.

$\therefore$ closure property satisfied.

(2) Asso. : let $a, b \in G = \mathbb{Q}^+$.

$\Rightarrow a * b = ab/2$

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

$\Rightarrow$ LHS $= (a*b) * c$

$= (ab/2) * c$

$= \frac{(ab/2) \cdot c}{2} = \frac{abc}{4}$.

$\Rightarrow$ RHS $= a * (b * c)$

$= a * (bc/2) = \dfrac{a \cdot (bc/2)}{2} = \dfrac{abc}{4}$

$\therefore$ LHS = RHS

$\therefore$ Asso. Satisfied.

(3) Identity : Let $a \in G = \mathbb{Q}^+$

$\Rightarrow a * e = e * a = a$

$\Rightarrow a * e = a$

$\Rightarrow \dfrac{ae}{2} = a \Rightarrow ae = 2a$

$\Rightarrow e = 2 \in \mathbb{Q}^+$

$\therefore$ we get $e = 2$ in G such that $a * e = e * a = a$.

$\therefore$ Identity Satisfied

(4) Inverse : Let $a \in G = \mathbb{Q}^+$ & a^{-1} is Inverse of a.

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

$\Rightarrow a * a^{-1} = e \Rightarrow \dfrac{a \cdot a^{-1}}{2} = e$

$\Rightarrow a \cdot a^{-1} = 4$

$\Rightarrow a^{-1} = 4/a \in \mathbb{Q}^+$

$\therefore$ we get Inverse element $a^{-1} = 4/a$ such that $a * a^{-1} = a^{-1} * a = e$

$\therefore$ Inverse Satisfied

$\therefore$ $G = \mathbb{Q}^+$ is group under binary operation $a * b = ab/2$

H.W.
Et-3

Let $G = \mathbb{R} - \{1\}$. Prove that $(G, *)$ is a group where $*$ is defined by $a * b = a + b - ab$, $\forall a, b \in G$.

$\Rightarrow$ $a * b = a + b - ab$

(1) Let $a \in G = \mathbb{R}$.

$\Rightarrow a * b = a + b - ab \in G = \mathbb{R}$.

(2) Let $a, b \in \mathbb{R}$

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

$\Rightarrow$ LHS $= (a * b) * c$

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

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

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

$\Rightarrow$ RHS $= a * (b * c)$

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

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

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

$\therefore$ LHS = RHS.

(3) Let $a \in G$. $\Rightarrow a * e = e * a = a$

$\Rightarrow a * e = a$.

$\Rightarrow a + e - ae = a$.

$\Rightarrow e(1 - a) = 0$.

$\Rightarrow e = 0$, $a \neq 1$.

$\therefore \underline{e = 0}$.

(4) Let $a \in G$ & a^{-1} is Inverse of a

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

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

$\Rightarrow a + a^{-1} - a \cdot a^{-1} = 0$.

$\Rightarrow a + a^{-1}(1 - a) = 0$

$\Rightarrow a^{-1} = \underline{\frac{-a}{1-a}}$ & $a = 1 \notin G$.

Ex-4

Show that fourth roots of unity form a group under multiplication.

$\Rightarrow x^4 = 1$

$\Rightarrow x^4 - 1 = 0$.

$\Rightarrow x = 1, -1, i, -i$.

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

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

(1) closure : Here $\forall\ a, b \in G \Rightarrow a * b \in G$.

$\therefore$ closure satisfied.

(2) Asso : $\forall\ a, b \in G$. $\Rightarrow (a*b)*c = a*(b*c)$.

$\therefore$ Asso. satisfied

(3) Identity : Here Identity of Group G is 1.

$\therefore a * 1 = 1 * a = a$.

$\therefore$ Identity satisfied

(4) Inverse : From the table,

Inverse of 1 is 1

" " -1 " -1

" " i is -i

" " -i is i.

$\therefore$ Inverse satisfied

Hence $G = \{-1, 1, i, -i\}$ is Group under multiplication.

* **Abelian Group** : A Group with commutative property is known as abelian group or commutative Group.

Ex. Let Q^+ be the set of all positive rational numbers and $*$ be a binary operation on Q^+ defined by $a*b = ab/3$. is abelian Group.

(1) closure property :

$\forall\ a, b \in Q^+ = G$

$\Rightarrow a * b = \frac{ab}{3} \in Q^+ = G.$

$\therefore Q^+$ is closed with '$*$' operation.

(2) Asso.

$\forall\ a, b, c \in Q^+ = G.$

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

$\Rightarrow$ LHS $= (a*b)*c$

$= (ab/3)*c$

$= \frac{(ab/3).c}{3} = \frac{abc}{9}$

$\Rightarrow$ RHS $= a*(b*c)$

$= a*(bc/3)$

$= \frac{a.(bc/3)}{3} = \frac{abc}{9}$

$\therefore$ LHS = RHS.

$\therefore$ $*$ is Asso. ~~under~~ on Q^+.

(3) Identity : $\forall\ a \in Q^+.$

$\Rightarrow a*e = e*a = a$

$\Rightarrow a*e = a$

$\Rightarrow a.e/3 = a$

$\Rightarrow e = 3a/a = 3. \in Q^+ = G.$

$\therefore$ 3 is Identity element for $*$ and also $3 \in Q^+$.

(4) Inverse : $\forall a \in G^+$ & a^{-1} is Inverse of $a \in G^+$ =

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

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

$\Rightarrow a \cdot a^{-1}/3 = 3$.

$\Rightarrow a \cdot a^{-1} = 9 \Rightarrow a^{-1} = 9/a \in G^+$

$\therefore$ Hence, Inverse property satisfy

(5) Commutative :

$\forall$ ~~if~~ $a, b \in G^+$.

$\Rightarrow a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$.

Hence, ~~if~~ $(G^+, *)$ is abelian group

Ex. $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in R \right\}$. Show that G is an abelian group under the Matrix addition.

$\Rightarrow$ Here given set $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in R \right\}$

$\Rightarrow$ Let $A, B, C \in G$. where, $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$,

$B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ and $C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$.

(1) closure : Let $A, B \in G$.

$\Rightarrow A + B = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

$= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \in G$.

Hence, $A, B \in G \Rightarrow A + B \in G$

(2) Associative : We know that matrix addition is always associative under the given operation.

$\therefore (A+B)+C = A+(B+C)$; $\forall A, B, C \in G$.

(3) Identity : Let $e = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}$ be the Identity

Now, $A + e = A$.

$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$.

$\Rightarrow \begin{bmatrix} a_1+e_1 & b_1+e_2 \\ c_1+e_3 & d_1+e_4 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$.

$\Rightarrow a_1+e_1 = a_1$, $b_1+e_2 = b_1$

$c_1+e_3 = c_1$, $d_1+e_4 = d_1$.

$\therefore e_1 = 0$, $e_2 = 0$, $e_3 = 0$, $e_4 = 0$.

$\therefore e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G$.

& $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is Identity element of G.

(4) Inverse : Let $I = \begin{bmatrix} i_1 & i_2 \\ i_3 & i_4 \end{bmatrix}$ be the Inverse of A.

$\Rightarrow A + I = e$

$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} i_1 & i_2 \\ i_3 & i_4 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}$.

$\Rightarrow \begin{bmatrix} a_1+i_1 & b_1+i_2 \\ c_1+i_3 & d_1+i_4 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\Rightarrow a_1+i_1 = 0$ $b_1+i_2 = 0$ $\Rightarrow I = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix}$

$c_1+i_3 = 0$ $d_1+i_4 = 0$.

$\in G$

non-negative Integer $a +_m b$ Integer

$a +_m b = r$

r is the reminder when $a+b$ is divided by m.

M T W T F S S — YOUVA

q $I = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix}$ be the inverse element of A.

(5) Commutative : $\forall\ A, B \in G$.

we have $A + B = B + A$.

$\therefore$ G is abelian Group under matrix Addition.

Ex. (H.W.) Show that the set of all Positive rational number Q^+ form a group under the operation define by $a * b = ab/5$.

* Congruence :

Let m be a positive Integer. Then two Integer a and b are said to be Congruent modulo m, in symbol $a \equiv b \pmod m$, if m divides $a-b$.

$[a] = [a]_m = \{a + mq \mid q \in \mathbb{Z}\}$.

i.e $[0], [1], [2], \ldots, [m-1]$ are all the congruence classes modulo m.

* Addition Modulo (m) :

Let a and b any two integers and m is a fixed positive integer. The addition modulo m of a and b written as $a +_m b$ defined by

$a +_m b = r$; $0 \le r < m$.

where r is the least non-negative reminder when the ordinary Product $a+b$ is divided by m.

e.g $15 +_3 8 = (23, +_3) = 2$ | $11 +_4 6 = 1$ $(17, +_4)$ | $9 +_3 8 = (17, +_3) = 2$ $-20 +_5$ $= (-14, +_5) = -4 +_5$

$-3 +_5 5 = 2$

* **Multiplication modulo (m):**

Let a and b be any two integers. and m is a fixed Positive integer. The multiplication modulo m of a and b written as $a \times_m b$ defined by

$$a \times_m b = r \; ; \; 0 \le r < m.$$

e.g: $7 \times_3 5 = (35, \times_3) = 2$ | $28 \times_3 8 = (16, \times_3) = 1$

$15 \times_8 7 = (105, \times_8) = 1.$

Remark: The set Z_m contain elements are $Z_m = \{0, 1, 2, \ldots, m-1\}$.

Ex Prove that the set $G = \{0, 1, 2, 3, 4\}$ is abelian Group under addition modulo 5.

⇒ $G = \{0, 1, 2, 3, 4\}$.

$+_5$	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.

1) From the table, we have $a +_5 b \in G$ for all $a, b \in G$.

2) From the table we have,
$(a +_5 b) +_5 c = a +_5 (b +_5 c)$.
For all $a, b, c \in G$.

3) From the table, the Identity element of Group G is 0.

i.e. $a +_5 0 = 0 +_5 a = a$; $\forall a \in G$

4) From the above table,
Inverse of 0 is 0.
" " 1 is 4.
" " 2 is 3
" " 3 is 2
" " 4 is 1

5) For $a, b \in G$ we have,
$a +_5 b = b +_5 a$
∴ Given $(G, +_5)$ is abelian group

Ex. Prove that $G = \{1, 2, 3, 4\}$ is an abelian group under multiplication modulo 5.

⇒ $G = \{1, 2, 3, 4\}$.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1) From the table we have, $a \times_5 b \in G$ for all $a, b \in G$.

2) From the table, $\forall a, b, c \in G$, we have
$(a \times_5 b) \times_5 c = a \times_5 (b \times_5 c)$

3) From the table, the Identity element of G is 1.
i.e. $a \times_5 1 = 1 \times_5 a = a$; $\forall a \in G$.

4). From the table we have,
Inverse of 1 is 1.
2 is 3
3 is 2
4 is 1.

(5). For any two elements $a, b \in G$.
we have $a * b = b * a$.
∴ Given set G is Abelian grp.

H.W.
Ex.1) Prove that the set $G = \{0, 1, 2, 3, 4, 5\}$ is an abelian group under addition modulo 6.

(2) $G = \{0, 1, 2, \ldots, 7\}$ is abelian group under addition modulo 8.

(3) Show that $\{Z_6, +_6\}$ is abelian group.

* Permutations Group OR Symmetric Group

Let S be a set of n element A one-one-onto mapping from S to S is called Permutation on S.

The set of all Permutation is denoted by S_n.

* Representation of Permutation :

$S = \{a_1, a_2, \ldots a_n\}$.
let $f \in S_n$ and $f(a_1) = b_1$, $f(a_2) = b_2$, $\ldots f(a_n) = b_n$.

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$$

* **Total number of Permutation :**
Let P be a set having n distinct elements. Then the elements of P can be Permuted in n! (Ln) distinct ways. i.e $O(S_n) = Ln = n!$

eg $P = \{1, 2, 3\}$.
no. of Permutation $= 3! = 6$.

$\Rightarrow P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

* **Identity Permutation :**

$$I = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

$I(a_1) = a_1$, $I(a_2) = a_2$ ——, $I(a_n) = a_n$

Eg $S = \{1, 2, 3, 4\}$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

* **Equality of two Permutation :**

$\Rightarrow f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

then $f = g$.

* Product of two Permutation :

⇒ Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

then $f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

$g \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

i.e. $f \cdot g \neq g \cdot f$.

* Inverse of a Permutation :

If $f \cdot g = I$ then f and g are called inverse to each other

eg: $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ & $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ x & y & 2 & w \end{pmatrix}$

⇒ $f \cdot g = I$

⇒ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ x & y & 2 & w \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

⇒ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ y & x & w & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

i.e $y = 1$, $x = 2$, $w = 3$, $z = 4$.

$\therefore g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

* order of an element of Group :

Let G be a multiplicative group and $a \in G$ is any element of G. then

non-negative smallest integer n is said to be order of element ob 'a' if
$a^n = e$; e is Identity element of G.

* Cyclic Group :
A Group (multiplicative) G is said to be cyclic if its all elements can be generated by single element

$G = \{ x \mid x = a^n \}$ where $a \in G$ and n is any Positive integer

Ex $A = \{1, 2, 3, 4, 5, 6\} \times_7$

$3^1 = 3$
$3^2 = 3 \times_7 3 = 9 = 2$
$3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6$
$3^4 = 6 \times_7 3 = 18 \times_7 = 4$
$3^5 = 4 \times_7 3 = 12 \times_7 = 5$
$3^6 = 5 \times_7 3 = 15 \times_7 = 1$

i.e 3 is Generated set A
i.e This group is cyclic Group.

* Subgroup :
Let (A, *) be a group. and B be a subset of A, (B, *) is said to be subgroup of A if (B, *) is also a group by itself.

i.e A is Group.
B is subset of A
And B is also Group itself
then B is subgroup of Group A

e.g $A = \{1, 2, 3, 4\}$.
$B = \{2, 3\}$.
$\Rightarrow$ B is subset of A
$\Rightarrow$

Ex: $G = \{1, \omega, \omega^2\}$.

$\Rightarrow 1^1 = 1 \Rightarrow o(1) = 1$

$\omega^1 = 1 \Rightarrow o(\omega) = 1$

$\omega^2 = 2$

Ex: $G = \{1, -1, i, -i\}$ is multiplicative group. Find $O(G)$.

$(1)^1 = 1$. $\Rightarrow 1$ is Identity

$(-1)^2 = 1 \Rightarrow o(1) = 1$

$(i)^4 = 1 \quad o(-1) = 1$

$(-i)^4 = 1 \quad o(i) = 4$

$o(-i) = 4$

* **Proper Subgroup:** The subgroup A is called a proper subgroup if it is neither the singelton set $\{e\}$ nor the entire group G.

$A < G$.

e.g. $G = \{1, 2, 3, 4\}$.

$A = \{2, 3\}$. $\Rightarrow A < G$

* **Coset:**

Coset

Right Coset — Left Coset

Let H be a subgroup of a group $(G, *)$. for $a \in G$.

then $Ha = \{h * a \mid h \in H\}$ then Ha is called a right coset of H in G.

$aH = \{a * h \mid h \in H\}$. then aH is left coset of H in G.

* **Normal Subgroup:**

A subgroup H of G is said to be a normal subgroup of G if for every $a \in G$, $aH = Ha$.

Examples:

① Show that the multiplicative group $G = \{1, -1, i, -i\}$ is cyclic

$\Rightarrow (i)^1 = i$, $(i)^2 = -1$, $i^3 = -i$, $i^4 = 1$.

i.e. i is a generator of G.

$\therefore$ G is cyclic group.

$\Rightarrow$ Here, $-i$ is also a ~~cyclic group~~ generator of G.

$1 +_6 1 = 2$, $1 +_6 1 +_6 1 = 3$, $1 +_6 1 +_6 1 +_6 1 = 4$

Ex-2 Show that $A = (\{0, 1, 2, 3, 4, 5\}, +_6)$ is cyclic. Find all generators.

$1 \in G$.

⇒ For element 1, $(1)^1 = 1$, $(1)^2 = 1 +_6 1 = 2$
$(1)^3 = 3$, $(1)^4 = 4$, $(1)^5 = 5$, $(1)^6 = 0$.

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

∴ 1 is generator of A.

⇒ A is cyclic Group.

$2 \in G$.

⇒ $(2)^1 = 2$, $(2)^2 = 2 +_6 2 = 4$, $(2)^3 = 2 +_6 2 +_6 2 = 0$
$(2)^4 = 2$, ~~$(2)^5 = 1$~~

∴ 2 is not generator of A

- Simi, 3 & 4 are not generators of A

$5 \in G$.

- $(5)^1 = 5$, $5^2 = 5 +_6 5 = 4$, $5^3 = 4 +_6 5 = 3$
$(5)^4 = 2$, $(5)^5 = 1$, $(5)^6 = 0$.

∴ 5 is also generator of A

i.e 1 and 5 are generator of A.

Ex-1 Find all the generators of the cyclic Group $G = (\{1, 2, 3, 4\} \times_5)$

⇒ Here $O(H) = 4$.

i.e. Its generator is the element of G whose order is 4.

- we have $1 \in G$.
$1^2 = 1$, $1^3 = 1$, $1^4 = 1$, $1^5 = 1$.
∴ $O(1) = 1$.

$2 \in G$.

- $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$.
∴ $O(2) = 4$

$3 \in G$.

- $3^1 = 3$, $3^2 = 4$, $3^3 = 2$, $3^4 = 1$.
∴ $O(3) = 4$

$4 \in G$.

- $4^1 = 4$, $4^2 = 16 \times_5 = 1$, $4^3 = 4$
∴ $O(4) = 2$

∴ 2 and 3 are generators of Group G

↑ cyclic

Ex Show that $H = \{0, 2, 4\}$ is a subgroup of the group that $G = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6.

⇒ clearly $H = \{0, 2, 4\} \subset G$. — (1).

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

(1) All the entire in the table are the element of H.
∴ closure is satisfied

(2) ~~∀ a, b ∈ H, we have, a+~~
Consider $(0 +_6 2) +_6 4 = 2 +_6 4 = 0$.
& $0 +_6 (2 +_6 4) = 0 +_6 6 = 0$.
∴ Associative satisfied

(3) Identity : 0 is Identity element of Addition modulo 6.
i.e, $a +_6 0 = 0 +_6 a = a$.
$2 +_6 0 = 0 +_6 2 = 2$

(4) Inverse : From the table
$0^{-1} = 0$, $2^{-1} = 4$, $4^{-1} = 2$.
So, every element has inverse in the set H.
∴ $(H, +_6)$ is ~~group~~ group.
∴ H is subgroup of G.

Ex $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$. Find order of each element. where G is multi. group

⇒ $e = a^6$
$(a)^6 = e \Rightarrow o(a) = 6$
$(a^2)^3 = a^6 = e \Rightarrow o(a^2) = 3$
$\Rightarrow o(a^3) = 2$
$\Rightarrow o(a^4) = 3$

$o(a^5) = 6$
$o(a^6) = 1$.

Ex Let G be the additive group of integer. $G = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ and $H = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$ be a subgroup of G. then find all left and Right coset of H in G.

→ Right coset:

⇒ Here $0 \in G$.

$H = H+0 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.

$1 \in G$.

$H+1 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$2 \in G$.

$H+2 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

$3 \in G$.

$H+3 = \{\ldots, -3, 0, 3, 6, 9, \ldots\}$.

$4 \in G$.

$H+4 = \{\ldots, -2, -1, 4, 7, 10, \ldots\}$.

since $H+3 = H+0$.

$H+4 = H+1$

$H+5 = H+2$.

∴ Right coset are $\{H+0, H+1, H+2\}$, $i_G(H) = 3$

⇒ left coset:

$0+H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.

$1 \in G$

$1+H = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$.

$2 \in G$

$2+H = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

$3 \in G$

$3+H$ ——

⇒ $0+H = 3+H$, $5+H = 2+H$,

$4+H = 1+H$

∴ left coset are $\{0+H, 1+H, 2+H\}$, $i_G(H) = 3$.

Ex-2 Consider a group $(Z, +)$. it's subgroup $H = (4Z, +)$. Find all right and left coset.

⇒ $G = Z = \{ \ldots -3, -2, -1, 0, 1, 2, 3, \ldots \}$

$H = 4Z = \{ \ldots -12, -8, -4, 0, 4, 8, \ldots \}$

⇒ Right coset : $\{H, H+1, H+2, H+3\}$

$\therefore i_G(H) = 4.$

Left coset : $\{H, 1+H, 2+H, 3+H\}$.

$\therefore i_G(H) = 4.$

Ex Find the generators of $(Z_7 - \{0\}, \times_7)$.

⇒ $Z_7 = \{[1], [2], [3], [4], [5], [6]\}$.

Here we have multiplication $\times_7$ as operation

⇒ $[1] \in Z_7$

⇒ $(1)^1 = 1, (1)^2 = 1, \ldots (1)^6 = 1.$

$\therefore [1]$ is not a generator

⇒ $[2] \in Z_7$

$(2)^1 = [2], (2)^2 = 4, 2^3 = 1, 2^4 = 2,$

$2^5 = 4, 2^6 = 1.$

$\therefore [2]$ is not a generator

⇒ $[3] \in Z_7$

$(3)^1 = [3], (3)^2 = 2, (3)^3 = 6, (3)^4 = 4,$

$(3)^5 = 5, (3)^6 = 1$

$\therefore 3$ is generator.

⇒ $[4] \in Z_7$

4 is not generator.

⇒ $[5] \in Z_7$ —

$[6] \in Z_7$ —

* Boolean Algebra :

If Algebraic structure $\langle B, *, \oplus, 0, 1, ' \rangle$ is satisfy following four Property then it is called Boolean Algebra.

1. Lattice Property
2. Bounded Property.
   there exist 0-element and 1-ele in B such that
   (1) $a * 0 = 0$ (2) $a * 1 = a$
   (3) $a \oplus 0 = a$ (4) $a \oplus 1 = 1$.
3. Complemented Property :
   $\forall a \in B. \exists b \in B$ S.T.
   $a * b = 0$ & $a \oplus b = 1$.
4. Distributive Property : $\forall a, b, c \in B$.
   (1) $a * (b \oplus c) = (a * b) \oplus (a * c)$
   (2) $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$

Ex Check $\langle B, *, \oplus, 0, 1, ' \rangle$ is boolean Al.
$B = \{0, 1\}$

*	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	1

Element	0	1
comp. ele	1	0

(1) From table (1) & (2) we say that $\langle B, *, \oplus \rangle$ is a lattice

(2) Here glb $B = 0$ = 0 - element of B
lub $B = 1$. = 1 - " " "
∴ B is bounded lattice
∴ $\langle B, *, \oplus, 0, 1 \rangle$ is bounded lattice

(3) From table (3), we have every element of B has unique complement in B.
∴ 0 & 1 are com. of each other. $\langle B, *, \oplus, 0, 1, ' \rangle$ is com.

(4) $\langle B, \oplus, * \rangle$ is lattice with only two element
∴ $\langle B, *, \oplus \rangle$ is distributive lattice

* Def^n

* Boolean Algebra :

- ~~Bol~~ Boolean Algebra as a lattice

A lattice is said to be a B.A. if it is both distributive and complemented.

Ex Show that $\langle S_{30}, *, \oplus, 0, 1, ' \rangle$ is boolean Algebra.

⇒ $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

For boolean Algebra, first we make table of glb and lub as follow.

gcd	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	2	10	5	10
15	1	1	3	5	3	5	15	15
30	1	2	3	5	6	10	15	30

lub	1	2	3	5	6	10	15	30
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

Element	1	2	3	5	6	10	15	30
Complement	30	15	10	6	5	3	2	1

- From the above table we check the Properties of Algebra as follow

① Lattice Property :
From table 1 and 2 we say that $\langle S_{30}, *, \oplus \rangle$ is Lattice

② Bounded Property :
glb $S_{30} = 1 = 0$ - element
lub $S_{30} = 30 = 1$ - element.
∴ S_{30} is bounded lattice
∴ $\langle S_{30}, *, \oplus, 0, 1 \rangle$ is bounded Lattice

③ Complemented Property :
From Table - 3 we have every element of S_{30} has a unique Complement in S_{30}.
∴ $\langle S_{30}, *, \oplus, ', 0, 1 \rangle$ is bounded Complemented Lattice

④ Distributive Property :
From ① & ② S_{30} is Distributive
∴ $\langle S_{30}, *, \oplus \rangle$ is Distributive Lattice

∴ $\langle S_{30}, *, \oplus, 0, 1, ' \rangle$ is Boolean Algebra.

* Join Irreducible element :

If $\langle B, *, \oplus \rangle$ is lattice and $a \in B$ then a is said to be Join-Irr. if it can not be express as a Join (lub) of two distinct element of B.

* Atoms :

Let $\langle B, *, \oplus \rangle$ be a lattice and $a \in B$ then a is said to be Atom if it satisfy the following Property

(1) a is Join-Irreducible
(2) a is cover of 0.

⇒ Here, 0 means 0-element of B i.e. glb of B.

* Meet Irreducible :

Let $\langle L, *, \oplus \rangle$ be a lattice and $a \in L$ is said to be meet Irre. if it can not be expresse as meet of two element of L.

i.e. there does not exist $a_1, a_2 \in B$ such that $a = a_1 * a_2$.

* Anti-Atoms :

Let $\langle L, *, \oplus \rangle$ be a lattice and $a \in L$ is said to be anti atoms if it satisfy the following Property

(i) a is meet-Irreducible
(ii) a is cover of 1

Here 1 means 1-element of B i.e. lub of

Ex

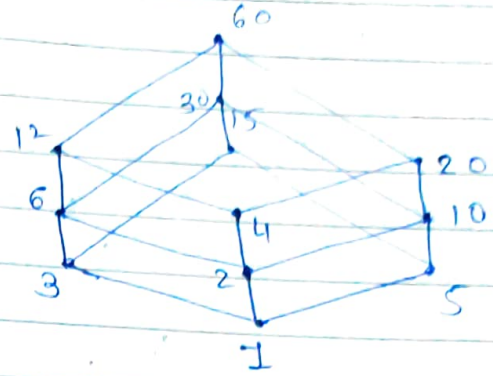
Join irreducible = 2, 3, 4

Meet = 1, 2, 3

Join
= d, g, b, a
= b, c, e, d, g

Ex Find Join-Irreducible, Meet-Irredu. Atom and Anti-Atom for the lattice $\langle S_{60}, D \rangle$, $\langle S_{90}, D \rangle$ and $\langle S_{100}, D \rangle$.

⇒ $\langle S_{60}, D \rangle$.



Join-Irreducible – 2, 3, 4, 5
Atoms – 2, 3, 5
Meet-Irr – 12, 15, 20, 30
Anti-Atoms – 12, 20, 30.

② $\langle S_{90}, D \rangle$.

Join-Irre – 2, 3, 5, 9
Atoms – 2, 3, 5
Meet-Irre – ~~10, 15, 45~~ 10, 18, 30, 45
Anti-Atoms 18, 30, 45

③ $\langle S_{150}, D \rangle$.

Join-Irre – 2, 3, 5, 25
Atoms – 2, 3, 5
Meet-Irre – 50, 75, 30, 6
Anti-Atom – 50, 75, 30.

⇒ $\langle S_{210}, D \rangle$.

Join - Irre - 2, 5, 7, 3

Atoms - 2, 3, 5, 7

Meet - Irre - 30, 42, 70, 105

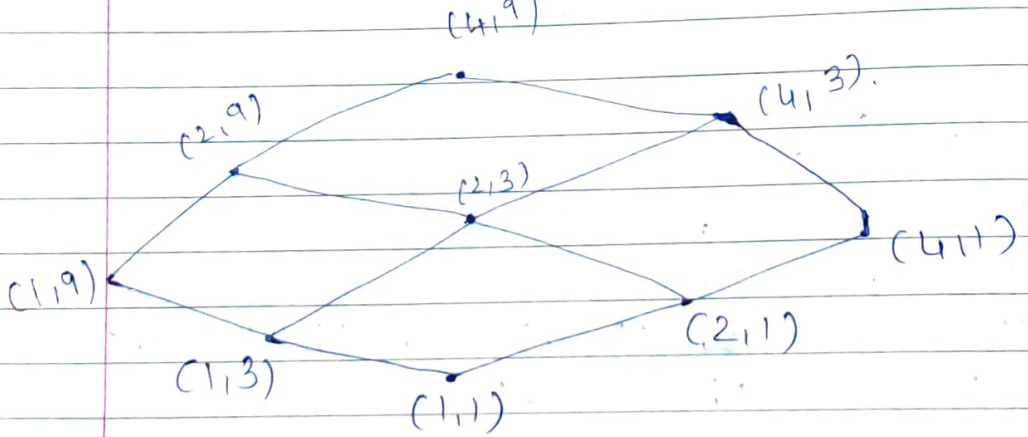
Anti - Atoms - 30, 42, 70, 105

Ex. Find Join - Irre., meet - Irre, Atoms and Anti - Atoms of lattice $\langle S_4 \times S_9, D \rangle$.

⇒ $S_4 = \{1, 2, 4\}$.

$S_9 = \{1, 3, 9\}$.

$S_4 \times S_9 = \{(1,1), (1,3), (1,9), (2,1), (2,3), (2,9), (4,1), (4,3), (4,9)\}$.



Join - Irre - (1,3), (1,9), (2,1), (4,1)

Atoms - (1,3), (2,1)

meet - Irre - (2,9), (4,3), (1,9), (4,1)

Anti - Atoms - (2,9), (4,3)