Group: G - Non-empty set

$*$: Binary operation $(a*b \in G,\ a,b \in G)$

$(G, *)$ is called a group if it satisfies the following properties.

(i) Associativity: $\forall\ a,b,c \in G$

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

(ii) Existence of Identity: $\exists\ e \in G$ s.t.

$$\forall a \in G,\quad a*e = a = e*a$$

e is called identity element or the zero element of $(G,*)$

(iii) Existence of Inverse: $\forall a \in G$, $\exists\ a^{-1} \in G$ s.t.

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

a^{-1} is called the inverse element of a.

Ex: 1. $(\mathbb{Z}, +)$ - Group.

$+$ ↓ Binary operation

Identity $e = 0$

Inverse of $a \in \mathbb{Z} = -a$

2. $(\mathbb{Q}, +)$ - Group.

3. $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - Groups.

4. Is $(\mathbb{Z}, -)$ a group? $\{\because$ $-$ is not associative

A group $(G,*)$ is called an abelian group if $*$ is commutative in G.

$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ - Abelian groups.

$(\mathbb{Z}, \underbrace{\times}_{\text{multiplication}})$ a group?

$0 \in \mathbb{Z}$, $\quad 0 \times 1 = 0 = 1 \times 0$

$a \in \mathbb{Z}$, $\quad \frac{1}{a} \notin \mathbb{Z}$

$(\mathbb{Z}, \times)$ is not a group.

$(\mathbb{Q}, \times)$ a group?

$\underline{0^{-1}}$ doesn't exists therefore $(\mathbb{Q}, \times)$ is not a group.

$(\mathbb{R}, \times)$ & $(\mathbb{C}, \times)$ are not groups.

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\quad (\mathbb{Q}^*, \times)$ – Group

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\quad (\mathbb{R}^*, \times)$ "

$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ $\quad (\mathbb{C}^*, \times)$ "

$U(n) = \{ x \in \mathbb{N} \mid 1 \le x \le n, \ \gcd(x, n) = 1 \}$

$(U(n), \underbrace{\times_n}_{\text{multiplication modulo } n})$ – Group.

$U(8) = \{1, 3, 5, 7\}$ $\qquad 1^{-1} = 1$

$(U(8), \times_8)$ – Group. $\qquad 3^{-1} = 3$

$5^{-1} = 5$

$7^{-1} = 7$

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$(\mathbb{Z}_n, +_n)$ – Group.

$+_n$ is assoc.

$e = 0$

$a^{-1} = (n-a)$, $\underline{a \in \mathbb{Z}_n}$

$A_n = \{1, 2, 3, \cdots, n\}$

$S_n = \{$ All one-one onto mappings from A_n to $A_n\}$

$=$ set of all permutations of A_n.

S_n with operation Composition forms a group.

<u>Ex</u> : $A_3 = \{1, 2, 3\}$

$\underline{S_3} = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}$

$= \{ [1\ 2\ 3], [2\ 1\ 3], [3\ 2\ 1], [1\ 3\ 2], [2\ 3\ 1], [3\ 1\ 2] \}$

$= \{ (1), (12), (13), (23), (123), (132) \}$

$(S_3, \circ)$ - Forms a group

$\circ \downarrow$ composition.

Identity $e = (1)$

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

$(12)^{-1} = (12)$

$(13)^{-1} = (13)$

$(23)^{-1} = (23)$

$(123)^{-1} = (132)$

$(132)^{-1} = (123)$

<u>Order of a Group</u>: $(G, *)$ - Group

Order of $(G, *)$ = $|G|$ = No. of elements in $(G, *)$

If $|G|$ is finite then $(G, *)$ is called a finite group

" " " infinite " " " " an infinite "

<u>Subgroup</u>: $(G,*)$ - Group

$H \subseteq G$

Then $(H,*)$ is called a subgroup of G if $(H,*)$ is a group.

$(\mathbb{Z},+)$

$2\mathbb{Z} = \{0, \pm 2, \pm 4, \cdots\}$

$2\mathbb{Z} \subseteq \mathbb{Z}$

$(2\mathbb{Z},+)$ a group? <u>Yes</u>.

$(2\mathbb{Z},+)$ is a subgroup of $\mathbb{Z}$

$(n\mathbb{Z},+)$ " " " " " where $n \in \mathbb{N}$.

$\mathbb{Z}_{10} = \{0, 1, 2, \cdots, 9\}$

$H = \{0, 2, 4, 6, 8\}$, $\underline{H \subseteq \mathbb{Z}_{10}}$

$(H, +_{10})$ - Group

$\therefore$ $(H, +_{10})$ is a subgroup of $(\mathbb{Z}_{10}, +_{10})$

<u>Cyclic Group</u>: $(G,*)$ - Group.

$(G,*)$ is called a cyclic group if all the elements of G can be generated by using power of an element of G.

i.e. if $\exists\, a \in G$ s.t.

$G = \{\underbrace{a*a*\cdots*a}_{n\text{-times}} \mid n \in \mathbb{N}\}$ | 'a' is called a generator of G.

<u>Ex</u>: $\mathbb{Z}_8 = \{0, 1, 2, \cdots, 7\}$, $(\mathbb{Z}_8, +_8)$ - Group.

$1 +_8 1 = 2$, $1^3 = 1 +_8 1 +_8 1 = 3$, $1^4 = 4$, $1^5 = 5$ ...

$3^1 = 3, \quad 3^2 = 6, \quad 3^3 = 1, \quad 3^4 = 4, \quad 3^5 = 7, \quad 3^6 = 2,$

$3^7 = 5, \quad 3^8 = 0,$

3 is also a generator of $(\mathbb{Z}_8, +_8)$.
5 " " " "
7 " " " "
x " " " " " if $\gcd(x, 8) = 1$.

$(\mathbb{Z}_n, +_n)$ is a cyclic group

x is a generator of $(\mathbb{Z}_n, +_n)$ if $\gcd(x, n) = 1$.

Lagrange's Theorem: G - Group, H is a subgp of G.

Order of a subgroup H divides the order of the group G.

$$|H| \mid |G|$$

Ex: $(\mathbb{Z}_{10}, +_{10}) = \{0, 1, 2, \ldots, 9\}$

divisors of 10 = $\underbrace{1, 2, 5, 10}_{\text{Possible orders of a subgp of } (\mathbb{Z}_{10}, +_{10})}$

Order of an element: $(G, *)$ - Group

Let $a \in G$ then the order of a is the least +ve integer n s.t.

$$a^n = \underbrace{a * a * \cdots * a}_{n\text{-times}} = e \quad (\text{Identity of } G)$$

$\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$

$O(0) = 1, \quad O(1) = 10, \quad O(2) = 5, \quad O(3) = 10, \quad O(4) = 5$

Note: A group $(G, +)$ supports the operations $+$ & $-$