

Eg: Show that  $\mathbb{Z}_5 = (G, \oplus_5) = \{0, 1, 2, 3, 4\}$  forms a group under addition modulo 5.

$$G \oplus_n = \{0, 1, \dots, n-1\}$$



$\oplus_5$	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

$$1 \oplus_5 4 = \frac{5}{5}$$

$$R=0$$

$$2 \oplus_5 3 = \frac{5}{5}$$

$$R=0$$

$$2 \oplus_5 4 = \frac{6}{5}$$

$$R=1$$

$$(3 \oplus_5 0) \oplus_5 2$$

→ In this table, all the elements are in  $G$   
i.e.  $a \oplus_5 b \in G, \forall a, b \in G$

→ closure satisfies.

→  $|||^{1y}$  associative law satisfies.

$$\text{i.e., } \forall a, b, c \in G, (a \oplus_5 b) \oplus_5 c = a \oplus_5 (b \oplus_5 c)$$

→ Identity element is '0'

→ Inverse law,  $\bar{0}' = 0, \bar{1}' = 4$

$$\bar{2}' = 3, \bar{3}' = 2$$

$$\bar{4}' = 1$$

∴ Therefore  $(G, \oplus_5)$  is a group



P.T the set  $G = \{1, 2, 3, 4, 5, 6\}$  is abelian group of order 6 w.r.to multiplication modulo 7

$$\begin{bmatrix} \otimes_7 \\ 0_7 \end{bmatrix}$$

$\otimes_7 \rightarrow$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$$2 \otimes_7 4 = \frac{8}{7}$$

$$R=1$$

$$2 \otimes_7 5 = \frac{10}{7}$$

$$R=3$$

→ From the table,  $a \otimes_7 b \in G$ ,  $\forall a, b \in G$

→  $\forall$  associative holds.  
i.e.,  $(a \otimes_7 b) \otimes_7 c = a \otimes_7 (b \otimes_7 c)$   
 $\forall a, b, c \in G$

→ Identity element is 1.

→ Inverse:  $1^{-1} = 1$ ,  $2^{-1} = 4$ ,  $3^{-1} = 5$   
 $4^{-1} = 2$ ,  $5^{-1} = 3$   
 $6^{-1} = 6$

→ Here  $a \otimes_7 b = b \otimes_7 a$   $\forall a, b \in G$

$$\text{i.e., } 2 \otimes_7 5 = 3$$

$$5 \otimes_7 2 = 3$$

$\therefore G$  is abelian



Q: A non-empty subset  $H$  of a group  $(G, *)$  is a subgroup of  $G$  iff the following are satisfied:

✓ (i)  $a * b \in H$  ,  $\forall a, b \in H$

✓ (ii)  $a^{-1} \in H$  ,  $\forall a \in H$

Ans: Let  $H$  be a non-empty subset of  $G$ .

$(\Rightarrow)$  Suppose  $H$  is a subgroup of  $G$ , then

(i) and (ii) follows by definition

$(\Leftarrow)$  Suppose (i) and (ii) holds in  $H$

We must prove that  $H$  is a subgroup of  $G$ .

— Closure property follows from (i)

— Inverse property follows from (ii)

— Elements of  $H$  are also elements of  $G$  ( $H \subseteq G$ )

$\therefore$  associative follows from  $G$ .

Since  $H \neq \emptyset$ , there is an element  $a \in H$

By hypothesis  $a^{-1} \in H$  (by (ii))

By (i),  $a * a^{-1} \in H$

$a * b \in H$

$e \in H$ , identity axiom satisfied.

$\Rightarrow H$  is a subgroup of  $G$ .



Q: A nonempty subset  $H$  of a group  $(G, *)$  is a subgroup of  $G$  iff  $a * b^{-1} \in H$ ,  $\forall a, b \in H$ .

Ans: Let  $H$  be a non-empty subset of  $G$ .

$(\Rightarrow)$  Let  $H$  be a subgroup of  $G$   
 $\forall a, b \in H$ ,  $a * b \in H$  (closure)

Also,  $a \in H$ ,  $b^{-1} \in H$

$\therefore a * b^{-1} \in H$  (closure)

$\Leftarrow$  Let  $a * b^{-1} \in H$ ,  $\forall a, b \in H$  — (1)

To prove that  $H$  is a subgroup of  $G$ .

Since  $H \neq \emptyset$ , there is an element  $a \in H$

$a \in H$ ,  $a \in H \Rightarrow a * a^{-1} \in H$  (by (1))  
 $e \in H$

$\therefore$  identity axiom holds

$\forall a \in H$ , we know that  $e \in H$

$e * a^{-1} \in H$  by (1)

$a^{-1} \in H$

$\therefore$  inverse axiom holds.

Since  $H$  is a subset of  $G$ , associative follows.

Let  $a, b \in H$ , as  $b \in H$ ,  $b^{-1} \in H$

we have,  $a * (b^{-1})^{-1} \in H$  by (1)

$a * b \in H$  (closure law holds)

$\therefore (H, *)$  forms a group

$\Rightarrow H$  is a subgroup of  $(G, *)$ .