(A) $a+b = a^b \ \forall\, a,b \in \mathbb{Z}$. Is $(\mathbb{Z}, *)$ binary opperation.

- $(\mathbb{Z}, *)$ is not closure.

Ex:- $2, -1 \in \mathbb{Z}$, if $a=2, b=-1$

$$2 \oplus (-1) = 2^{-1} = \frac{1}{2} \notin \mathbb{Z}.$$

(B) $(\text{Symm}(A), \circ)$ is group.

Proof:- $\text{Symm}(A) = \{ f : A \to A \text{ is 1-1 and onto} \}$
i.e. f is bijective.

(1) Closure: let $f_1, f_2 \in \text{Symm}(A)$, f_4, f_2 bij.

$$f_4 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$= f_5 \in \text{symm}(A)$$

(2) Associative: $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$

(3) Identity: $I_A : A \to A$ is bijective

$$f \circ I_A = I_A \circ f = f \text{ s.t } f = \{f_1, f_2, \dots, f_6\}.$$

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

④ $\forall f \in \text{Symm}(A)$. f is bijective, then f^{-1} is bijective

$$f \circ f^{-1} = f^{-1} \circ f = I_A.$$

$$f_4 \circ f_4^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

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

Ⓒ Is $3 \equiv 1 \pmod 3$.

Solve: $3 - 1 = 2 \neq 3 * k$.

$\therefore 3 \not\equiv 1 \pmod 3$.

Ⓓ Show that $(Z_4, +4)$ is a commutative group.

Solve: $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$+4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Commutative.

(E) Theorem :- Let $(G, *)$ be a group. Then

① $e^{-1} = e$.

Proof :- Let $X = e^{-1}$

If X is element and G is a group, then

$$X * e = e * X = X \quad \text{---- ①}$$

If X is inverse, then

$$e * X = X * e = e \quad \text{------ ②}$$

$\therefore X = e$

$\therefore e^{-1} = e$.

② If $a = a^{-1}$, then G is Commutative group.

Proof : Let $a, b \in G \Rightarrow a * b \in G$ (by closure properties)

$a = a^{-1}$ & $b = b^{-1}$

$a * b \in G$.

$\therefore (a * b) = (a * b)^{-1}$ (as element).

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

$= b * a \Longrightarrow a * b = b * a$

$\therefore G$ is Commutative.

The inverse is not true.

Ex: Let $(G=\{1,-1,i,-i\},\cdot)$ is Commutative group

if $a=i$, $a^{-1}=-i \Rightarrow a \neq a^{-1}$

Ex If $(G,\cdot)$ is agroup such that $(G=\{1,-1,i,-i\})$. Find $o(G)$, $o(a)$

If $a=1,-1,i,-i$.

Solve: $o(G)=4$ (The number of element).

$a^n=e$ with binary operation$(\cdot)$ and (n) Least positive integer.

i.e $Z^+=\{1,2,3,\ldots\ldots$

$(-1)^2=1 \quad \therefore o(-1)=2$

$(1)^1=1 \quad \therefore o(1)=1$

$(i)^4=i^4=i^2.i^2=-1.-1=1 \quad \therefore o(i)=4$

$(-i)^2=-i^2=-(-1)=1 \quad \therefore o(-i)=2$

Theorem (1.19) :▷ In a group $(G, *)$, the equation $a * x = b$ and $y * a = b$ have unique solutions.

Proof :▷ First, $x = a^{-1} * b$ satisfies the group equation $a * x = b$,

Since $a * (a^{-1} * b) = (a * a^{-1}) * b$

$= e * b$

$= b$

This show that $\exists$ at Least one solution on G.

To show that the solution is unique,

let $\bar{x} \in G$ s.t $a * \bar{x} = b$.

$$a * \bar{x} = a * (a^{-1} * b)$$

by cancellation Law.

$$\bar{x} = a^{-1} * b$$

$\therefore \bar{x} = x$

by the same way $y * a = b$, have unique solution

* Is $(Z_n, +_n)$ group ?

Proof :▷ Let $Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

1- $\forall \bar{a}, \bar{b} \in Z_n \Rightarrow \bar{a} + \bar{b} = \overline{a+b} \in Z_n$ (closure)

2- Associative, $\forall \bar{a}, \bar{b}, \bar{c} \in Z_n$, then

$$\bar{a} \oplus (\bar{b} \oplus \bar{c}) = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$$

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} \oplus \overline{(b+c)} = \overline{a+(b+c)}$$

$$= \overline{(a+b)+c} = \overline{(a+b)} \oplus \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$$

3- Identity, $e = \bar{0}$ s.t

$$\forall \bar{a} \in Z_n : \bar{a} \oplus \bar{0} = \bar{0} + \bar{a} = \bar{a} .$$

4- Inverse :▷ $\forall \bar{a} \in Z_n$ implies that $[\overline{n-a}]$.

s.t $\forall \bar{a} \in Z_n \Rightarrow \bar{a} \oplus \overline{n-a} = \overline{\cancel{a+n-a}}$

$$= \bar{n} = \bar{0} \quad \text{or}$$

$$\overline{n-a} \oplus \bar{a} = \overline{n-\cancel{a}+\cancel{a}} = \bar{n} = \bar{0}$$

$\therefore \bar{a}^{-1} = \overline{n-a} \Rightarrow (Z_n, \oplus)$ is group.

* Let G be a group, then $(\bar{a}^{-1})^{-1} = a \ \forall a \in G$.

proof: $\because (\bar{a}^{-1})^{-1}$ inverse element of $\bar{a}^{-1}$, then

$$(\bar{a}^{-1})^{-1} * \bar{a}^{-1} = e = \bar{a}^{-1} * (\bar{a}^{-1})^{-1}$$

$$\therefore (\bar{a}^{-1})^{-1} * \bar{a}^{-1} = \bar{a}^{-1} * (\bar{a}^{-1})^{-1}$$

$\because G$ group $\Longrightarrow \forall a \in G$, then $\bar{a}^{-1} \in G$.

$$\Longrightarrow a * \left((\bar{a}^{-1})^{-1} * \bar{a}^{-1}\right) = a * \left(\bar{a}^{-1} * (\bar{a}^{-1})^{-1}\right)$$

$$a * \left((\bar{a}^{-1})^{-1} * \bar{a}^{-1}\right) = (a * \bar{a}^{-1}) * (\bar{a}^{-1})^{-1}$$

$$\therefore a * \quad e \quad = \quad e \quad * (\bar{a}^{-1})^{-1}$$

$$\therefore a = (\bar{a}^{-1})^{-1}$$

* prove that $(Z_4, +)$ is group.

proof: $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Identity $e = \bar{0}$

Inverse $\bar{1} + \bar{3} = \bar{4} = \bar{0}$

$\bar{2} + \bar{2} = \bar{4} = \bar{0}$

$\bar{3} + \bar{1} = \bar{4} = \bar{0}$

closure $\forall a, b \in G = Z_4$

$a + b \in Z_4$.

Associative $\forall a, b, c \in Z_4$.

$a + (b + c) = (a + b) + c$

العناصر متماثلة

* $(Z_n^* - \{0\}, \times_n)$ is group if n is prime number.

$(Z_p^*, \otimes)$ where $Z_p^* = Z_p - \{\bar{0}\}$.

Ex!. $(Z_7^*, \otimes)$

$Z_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

T.P. $(Z_7^*, \otimes)$ is group.

$\otimes$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

① closure

② associative.

③ Identity $e = \bar{1}$

④ Inverse

$\bar{1} \otimes \bar{1} = \bar{1}$

$\bar{2} \otimes \bar{4} = \bar{1}$

$\bar{3} \otimes \bar{5} = \bar{1}$

$\bar{4} \otimes \bar{2} = \bar{1}$

$\bar{5} \otimes \bar{3} = \bar{1}$

$\bar{6} \otimes \bar{6} = \bar{1}$

$\therefore (Z_7^*, \otimes)$ group.

* $(Z_n^* - \{0\}, \times_n)$ is group if n is prime number.

$(Z_p^*, \otimes)$ where $Z_p^* = Z_p - \{\bar{0}\}$.

Ex!. $(Z_7^*, \otimes)$

$Z_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

T.P. $(Z_7^*, \otimes)$ is group.

$\otimes$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

① closure

② associative.

③ Identity $e = \bar{1}$

④ Inverse

$\bar{1} \otimes \bar{1} = \bar{1}$

$\bar{2} \otimes \bar{4} = \bar{1}$

$\bar{3} \otimes \bar{5} = \bar{1}$

$\bar{4} \otimes \bar{2} = \bar{1}$

$\bar{5} \otimes \bar{3} = \bar{1}$

$\bar{6} \otimes \bar{6} = \bar{1}$

$\therefore (Z_7^*, \otimes)$ group.