

Group:-

Example:-

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$G = \langle \mathbb{Z}_n, + \rangle$$

$$G = \langle \mathbb{Z}_n, * \rangle$$

Additive:-

(i) closure:-

$$a=3, b=5$$

$$\begin{aligned} c &= (a+b) \bmod n \\ &= (3+5) \bmod 6 \\ &= 8 \bmod 6 \end{aligned}$$

$$\boxed{c = 2}$$

Not applicable

$$\begin{aligned} c &= (3 * 5) \bmod 6 \\ &= 15 \bmod 6 \\ &= 3 \end{aligned}$$

$$\boxed{c = 3}$$

(ii) Associative:-

$$((a+b)+c) \bmod n = (a+(b+c)) \bmod n$$

$$((3+5)+2) \bmod 6 = (3+(5+2)) \bmod 6$$

$$(8 \bmod 6 + 2) \bmod 6 = (3 + (7 \bmod 6)) \bmod 6$$

$$(2+2) \bmod 6 = (3+1) \bmod 6$$

$$4 \bmod 6 = 4 \bmod 6$$

$$\boxed{4 = 4}$$

(iii) Identity:-

Add any number with 0,

$$(3+0) \bmod 6 = 3 \bmod 6 = 3$$

$$(3*1) \bmod 6 = 3 \bmod 6 = 3$$

$$a+0 = 0+a = a \quad \forall a \in \mathbb{Z}_n$$
$$a*1 = 1*a = a$$

is also element
in \mathbb{Z}_6 .

(iv) Inverse:-

$$(4+(-4)) \bmod 6 = 0$$

$$(4+(-4 \bmod 6)) \bmod 6 = 0$$

$$(4+2) \bmod 6 = 0$$

Inverse is 2

\mathbb{Z}_n	closure	Associative	identity	inverse	Commutative
+	✓	✓	✓	✓	✓
*					

(v) Commutative:

$$(a+b) \bmod n = (b+a) \bmod n$$

$$(3+5) \bmod 6 = (5+3) \bmod 6$$

$$8 \bmod 6 = 8 \bmod 6$$

$$2 = 2$$

(or)

$$(3+2) \bmod 6 = (2+3) \bmod 6$$

$$5 \bmod 6 = 5 \bmod 6$$

Multiplicative:-

(i) closure:-

$$c = (3 * 5) \bmod 6$$

$$= 15 \bmod 6$$

$$\boxed{c = 3}$$

(ii) Associative:

$$((3 * 5) * 2) \bmod 6 = (3 * (5 * 2)) \bmod 6$$

$$(15 \bmod 6) * 2 \bmod 6 = (3 * (10 \bmod 6)) \bmod 6$$

$$(3 * 2) \bmod 6 = (3 * 4) \bmod 6$$

$$6 \bmod 6 = 12 \bmod 6$$

$$\boxed{0 = 0}$$

(iii) Distributive:

$$(3 * 1) \bmod 6 = 3$$

$4 * 1 = 1 \bmod 6$
 $n = 0, 1, 2, \dots$
 No Inverse

(iv) Inverse:

$$(4 * (4^{-1})) \bmod 6 = 1$$

$$\gcd(6, 4) = 2 \neq 1 \quad \text{No Inverse}$$

(v) Commutative:-

$$\cancel{((a * b) * c) \bmod 6 = (a * (b * c)) \bmod 6}$$

$$(a * b) \bmod 6 = (b * a) \bmod 6$$

$$(3 * 5) \bmod 6 = (5 * 3) \bmod 6$$

$$15 \bmod 6 = 15 \bmod 6$$

$$\boxed{3 = 3}$$