1) $*$ is associative
2) there exist the identity element e in S
3) for every $a \in S$, the inverse of a, ie a^{-1} exists in S.

12/02/18

» $a \times b \pmod{n} = c$ Remainder when ab is divided by n.

$\Rightarrow n \mid ab - c$

» $a + b \pmod{n} = d$

$\Rightarrow n \mid (a+b) - d$

» $a \pmod{n} = r$

$\Rightarrow n \mid a - r$

$n = 5$

$[0] / \bar{0} = \{ \ldots -15, -10, -5, 0, 5, 10, \ldots \}$
$\bar{1} = \{ \ldots -14, -9, -4, 1, 6, 11, \ldots \}$
$\bar{2} = \{ \ldots -13, -8, -3, 2, 7, 12, \ldots \}$
$\bar{3} = \{ \ldots -12, -7, -2, 3, 8, 13, \ldots \}$
$\bar{4} = \{ \ldots -11, -6, -1, 4, 9, 14, \ldots \}$

$\mathbb{Z}_5 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$
$\mathbb{Z}_5 = \{ 0, 1, 2, 3, 4 \}$

Groups	Non-groups
$\langle \mathbb{Z}, + \rangle$	$\langle \mathbb{N}, - \rangle$, $\langle M_{n \times n}, \times \rangle$
$\langle \mathbb{R} - \{0\}, \times \rangle$	
$\langle M_{m \times n}, + \rangle$	
$\langle \mathbb{C}, + \rangle$	
$\langle \mathbb{Q} - \{0\}, \times \rangle$	

$\mathbb{Q}$ → rational no.

⇒ Verify that the roots of the eqn $x^n = 1, n \in$
forms a multiplicative group.

⇒ $\langle \mathbb{Z}_5, +_5 \rangle$

$\langle \{0, 1, 2, 3, 4\}, +_5 \rangle$

⇒ Show that, $\langle \mathbb{Z}_n^*, +_n \rangle$ forms a group.

$+_5$	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

$\times_5$	0	1	2	3	4
~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

⇒ $\langle \mathbb{Z}_5 - \{0\}, \times_5 \rangle$

3

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

⇒ $\langle \mathbb{Z}_6 - \{0\}, \times_6 \rangle$

$\times_7$	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			
5						
6						

$\langle \mathbb{Z}_7 - \{0\}, \times_7 \rangle$

$\Rightarrow$ satisfies group properties.

$\times_8$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5							
6							
7							

Proposition :

Let $a \in \mathbb{Z}_n$, then $\gcd(a, n) = 1$ iff a has a multiplicative inverse b, i.e. $ab \equiv 1 \pmod n$.

$a \times b$ $\quad a = 3$

Proof :

Let $\gcd(a, n) = 1$ then,

$\exists$ $r, s \in \mathbb{Z}$ s.t.

$ar + ns = 1$

$\Rightarrow ar = 1 - ns$

$\Rightarrow -(ar - 1) = ns$

$\Rightarrow n \mid (ar - 1)$ $\Rightarrow ar \equiv 1 \pmod n$.

If $r \in \{0, 1, 2, \ldots, (n-1)\}$ then $b = r$;

else $b = r \pmod{n}$.

Conversely, let a has a multiplicative inverse b

i.e $ab \equiv 1 \pmod{n}$

Let $c = \gcd(a, n)$.

Now, $ab \equiv 1 \pmod{n}$

$\Rightarrow n \mid (ab - 1)$

$\Rightarrow (ab - 1) = n.k$, for some $k \in \mathbb{N}$

$\Rightarrow ab - nk = 1$.

$c = \gcd(a, n)$ means $c \mid a$ & $c \mid n$

$\Rightarrow ab = c$ $nk = c$

$\therefore c \mid (ab - nk)$

$\Rightarrow c \mid 1$ $\Rightarrow$ this is possible when $c = 1$.

(Proved)

S.t

$\Rightarrow$ • Proposition :-

$\langle Z_n^*, \times \rangle$ is a group when n is prime.

$\Rightarrow$ A group is said to be abelian (commutative) if the binary operation is commutative.

$\Rightarrow$ Find a group (or give example) which is not commutative.