Definition 1.44:

The set of all congruence classes modulo n is denoted by Z_n (which is read Z mod n). Thus

$Z_n = \{ [\,0\,] , [\,1\,] , [\,2\,] , \ldots\ldots , [\,n-1\,] \}$, or

$Z_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$

Z_n has n elements.

Example 1.45:

$Z_1 = \{\overline{0}\}$, $Z_2 = \{\overline{0}, \overline{1}\}$, $Z_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

Now, **we define addition on Z_n** (write $+_n$) by the following :

$$[a] +_n [b] = [\, a +_n b\,], \quad \forall\, [a] , [b] \in Z_n$$

Similarly, **we define multiplication on Z_n** (write "$\cdot_n$" by the following :

$$[a] \cdot_n [b] = [a \cdot_n b] , \quad \forall\, [a] , [b] \in Z_n$$

It is easy to see that :

[1] $(Z_n , +_n)$ is an abelian group with identity $[\,0\,]$ and for every $[\,a\,] \in Z_n$, $[a]^{-1} = [\, n - a\,]$. **This group is called the Additive Group of Integers Modulo n .**

[2] Also, $(Z_n , \cdot_n)$ is abelian semi group with identity $[\,1\,]$. **It is called the Multiplicative Semi Group of Integers modulo n.**

Example 1.46: $(Z_4, +_4)$, $Z_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

(1) Closure is true

(2) Asso. is true

(3) $\overline{0}$ is an identity element

(4) Inverse:

$\overline{1}^{-1} = \overline{4} - \overline{1} = \overline{3}$

$\overline{2}^{-1} = \overline{4} - \overline{2} = \overline{2}$

$\overline{3}^{-1} = \overline{4} - \overline{3} = \overline{1}$

(5) Comm :

$\overline{1} + \overline{2} = \overline{3} = \overline{2} + \overline{1}$

$\overline{1} + \overline{3} = \overline{0} = \overline{3} + \overline{1}$

$+_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
1	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	3	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\therefore (Z_4, +_4)$ is a Comm.group.

Example 1.47: $(Z_4, \cdot_4)$, $Z_4 = \{\ \bar{0}\ ,\ \bar{1}\ ,\ \bar{2}\ ,\ \bar{3}\ \}$

$\cdot_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
1	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

It is clear that we cannot have a group.
Since the number $\bar{1}$ is identity,
but the numbers $\bar{0}$ and $\bar{2}$ have no inverse.
It follows that $(Z_4,\ \cdot_4)$ is not a group,
but it is semi group.

Example 1.48: Find the order of G and the order of each element of (G, *), such that (G, *) = (Z_8, $+_8$).

Solution:

$Z_8 = \{\ \bar{0}\ ,\ \bar{1}\ ,\ \bar{2}\ ,\ \bar{3}\ ,\ \bar{4}\ ,\ \bar{5}\ ,\ \bar{6}\ ,\ \bar{7}\ \}$, e = $\bar{0}$

$o(Z_8) = 8$ since (The number of elements of a group $Z_8 = 8$)

The order of an element a, $a \in Z_8$ is the least positive integer n such that $a^n = \bar{0}$, where $\bar{0}$ is the identity element of Z_8.

$o(\bar{0}) = 1$ since $(\bar{0})^1 = \bar{0} = e$

$o(\bar{1}) = 8$ since $(\bar{1})^8 = \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} + \overline{1\ + 1} = \bar{8} = \bar{0} = e$

$o(\bar{2}) = 4$ since $(\bar{2})^2 = \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8} = \bar{0} = e$

$o(\bar{3}) = 8$ since $(\bar{3})^8 = \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} = \overline{24}$

$= \bar{8} + \bar{8} + \bar{8} = \bar{0} + \bar{0} + \bar{0} = \bar{0} = e$

$o(\bar{4}) = 2$ since $(\bar{4})^2 = \bar{4} + \bar{4} = \bar{8} = \bar{0} = e$

$o(\bar{5}) = 8$ since $(\bar{5})^8 = \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} = \overline{40}$

$= (\bar{8})^5 = \overline{(0)}^5 = \bar{0} = e$

$o(\bar{6}) = 4$ since $(\bar{6})^8 = \bar{6} + \bar{6} + \bar{6} + \bar{6} = \overline{24} = \bar{0} = e$

$o(\bar{7}) = 8$ since $(\bar{7})^8 = \overline{56} = \bar{0} = e$

Exercises (4): **(Home Work 4).**

1. Find the order of Z_6 and the order of each element of (Z_6, $+_6$).
2. Find the order of Z_9 and the order of each element of (Z_8, $+_8$).
3. Find the order of Z_6 and the order of each element of (Z_9, $+_9$).

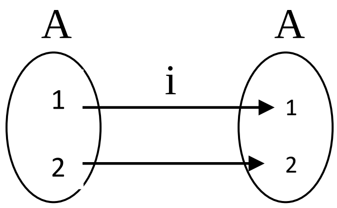
The Permutations : (التباديل)

Definition 1.49: A Permutation or symmetric of a set A is a function from A in to A that is both one to one and on to.

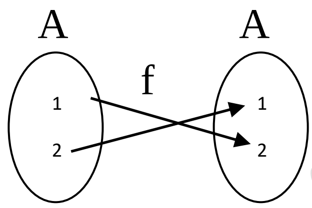
$$f: A \xrightarrow{1-1, onto} A$$

Symm (A) = $\{f |\ f: A \xrightarrow{1-1, onto} A\}$ the set of all permutation on A.
If A is the finite set {1, 2, …, n}, then the set of all permutation of A is denoted by S_n or P_n and $o(S_n) = n!$, where $n! = n\,(n-1) \ldots (3)(2)(1)$

Example 1.50: Let A = {1, 2} . Write all permutation on A.



,



Symm(A) = {i, f } = $\left\{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}$.

Example 1.51: Let A = {1, 2, 3}. Write all permutation on A.

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

$P_3 = Symm(A) = \{f_1, f_2, f_3, f_4, f_5, f_6\}$
o(P_3)= 3 ! = (3) (2) = 6

Theorem 1.52: If $A \neq \varphi$, then the set of all permutation on A Forms agroup with composition of Mapps.
(i.e.) Let $A \neq \varphi$, then (Symm(A) , o) is a group.

Proof:

Symm (A) = $\{f |\ f: A \xrightarrow{1-1, onto} A \ \ is\ a\ mapp.\}$,
To prove, (Symm(A) ,o) is a group.
since $\exists\ i_A: A \xrightarrow{1-1, onto} A$ a perm. on A
$\therefore i_A \in$ Symm(A) $\Longrightarrow$ Symm$(A) \neq \varphi$.