(3) To prove, $a^{-n} = (a^{-1})^n = (a^n)^{-1}$, $\forall\, n \in Z^+$

If $n = 1 \Longrightarrow p(1) : (a^{-1})^1 = a^{-1} = (a^1)^{-1}$

Suppose that if $n = k$ is true $\Longrightarrow p(k) = (a^{-1})^k = (a^k)^{-1}$

We must prove p (k+1) is true

$P(k+1) : (a^{-1})^{k+1} = (a^{k+1})^{-1}$?

$(a^{-1})^{k+1} = (a^{-1})^k * (a^{-1})^1 = (a^k)^{-1} * (a^1)^{-1} = (a^{k+1})^{-1}$

$\therefore$ p (k +1) is true

By the principle of math. ind. $\Longrightarrow$ p (n)is true , $\forall\, n \in Z^+$.

(4) ($\Longrightarrow$) If $n = 2 \Longrightarrow (a * b)^2 = a^2 * b^2$, To prove, is comm. Group.

$(a * b) * (a * b) = a * a * b * b$ (by def . of power int.)

$a * (b * a) * b = a * (a * b) * b$ (by asso .)

$(b * a) * b = (a * b) * b$ (by cancellation law)

$b * a = a * b$ (by cancellation law)

$\therefore$ G is comm . group.

($\Longleftarrow$) Let G be comm . group .

To prove, $(a * b)^n = (a^n * b^n)$, $\forall\, n \in Z$.

Let $p(n) : (a * b)^n = a^n * b^n$

If $n = 1 \Longrightarrow (a * b)^1 = a^1 * b^1$ is true

Suppose that p (k) is true with $k \in Z^+$ and $k \leq n$

s.t . $(a * b)^k = a^k * b^k$

We must prove P (k +1) is true

$P(k+1) : (a * b)^{k+1} = (a * b)^k * (a * b)^1$

$= a^k * b^k * a^1 * b^1$

$= (a^k * b^k) * (b * a)$ (G is comm .)

$= a^k * (b^k * b) * a$ (by asso .)

$= a^k * b^{k+1} * a$

$= a^k * a * b^{k+1}$

$= a^{k+1} * b^{k+1}$

$\therefore$ p(k + 1) is true , $\forall\, n \in Z^+$

Definition 1.33: ((**Order of a Group**))

The number of elements of a group G is called the order of G and is denoted by | G | or o (G).

G is called a finite group if | G | $< \infty$ and infinite group otherwise .

Definition 1.34: (**The Order of an Element**)

The order of an element a , $a \in$ G is the least positive integer n such that $a^n = e$, where e is the identity element of G. We denoted to order a by | a | or o(a).

(i.e.) | a | $= n$ if $a^n = e$, $n \in Z^+$

Example 1.35: (Z , +) is an infinite group .

Example 1.36: In a trivial group G = { 0 }

| G | = 1 , G is the only group of order 1.

Example 1.37: find the order of G and the order of each element of (G, .). Such that G = { 1, -1 , i, -i}.

Solution:

| G | = 4 and

| a | = ??

If a = 1, and $(1)^1 = 1$, $\Longrightarrow$ | a | = | 1 | = 1 (since e = 1)

If a = -1, and $(-1)^2 = 1$ $\Longrightarrow$ | -1 | = 2

If a = i, and $i^2 = -1$, $i^4 = 1 \Longrightarrow$ | i | = 4

If a = -i, and $-i^2 = -1$, $-i^3 = i$, $-i^4 = 1 \Longrightarrow$ | -i | = 4

The Group of Integers Modulo *n* **زمرة الاعداد الصحيحة مقياس *n***

Definition 1.38:

Let a , $b \in$, Z , $n > 0$. Then a is congruent to b modulo n if $a - b = nk$, $k \in$ Z and denoted by $a \equiv b$ or $a \equiv b$ (mod n)

Example 1.39:

(1) $17 \equiv 5$ (mod 6) , sine 17 – 5 = 12 = (6) (2)

(2) $8 \equiv 4$ (mod 2) , since 8 – 4 = 4= (2) (2)

(3) $-12 \equiv 3$ (mod 3) , since -12 -3 = -15 = (3) (-5)

(4) $5 \not\equiv 2$ (mod 2), since $5 - 2 = 3 \neq (2)(k)$, $\forall$ $k \in$ Z

Theorem 1.40: The congruence module *n* is an equivalence relation on the set of integers.

Proof: Let $a , b , c \in Z , n > 0$

(1) $a - a = 0 = (n)(0)$

$\therefore a \equiv a \pmod{n}$ **Reflexive is true**

(2) If $a \equiv b \pmod{n}$, To prove, $b \equiv a \pmod{n}$

Since $a \equiv b \pmod{n} \Longrightarrow a - b = nk , k \in Z$

so , $b - a = -nk = (n)(-k) , -k \in Z$

$\therefore b \equiv a \pmod{n} \Longrightarrow$ **Symmetric is true**

(3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. To prove, $a \equiv c \pmod{n}$

Since $a \equiv b \pmod{n}$, then $a-b = nk$

And $b \equiv c \pmod{n}$, then $b - c = nk'$

By adding these two eqs . $\Longrightarrow a - c = n (k + k') , k + k' \in Z$

$\therefore a \equiv c \pmod{n} \Longrightarrow$ **Transitive is true**

$\therefore$ The congruence modulo *n* is an equivalence relation .

Definition 1.41: Let $a \in Z , n > o$. The congruence class of a modulo *n*, denoted by [a] is the set of all integers that are congruent to a modulo *n* .

(i.e.) $[a] = \{z \in Z : z \equiv a \pmod{n}\}$

$= \{z \in Z : z = a + k n , k \in Z\}$

Example 1.42:

If $n = 2$, find [0] , [1]

$[0] = \{ z \in Z : z \equiv 0 \pmod{2} \}$

$= \{ z \in Z : z = 0 + 2k , k \in Z \}$

$= \{ 0 , \mp 2 , \mp 4 , \ldots\ldots\ldots \}$

$[1] = \{ z \in Z : z \equiv 1 \pmod{2} \}$

$= \{ z \in Z : z = 1 + 2k , k \in Z \}$

$= \{ \mp 1 , \mp 3 , \mp 5 , \ldots . \}$.

Example 1.43:

If $n = 3$, find [1] , [7]

$[1] = \{ z \in Z : z \equiv 1 \pmod{3} \}$

$= \{ 1 , 1 \mp 3, 1 \mp 6 \ldots . \}$

$= \{1 , -2 , 4 , 7 , -5 , \ldots . \}$.

[7] **(Home Work).**