المادة :- جبر زمر   المرحلة الثانية   م.م. ماجد وليد عمران

Definition :- Binary operation $\quad * : G \times G \to G$

let G be a set. A binary operation on G is a function that send each ordered pair (a,b) of elements of G to an element of G.

Definition :- let $A \subseteq G$, and Let $*$ be a binary operation on G. then A is said to be closed with respect to $*$ if $a*b \in A \; ; \; \forall \; a,b \in A$

example: the set of natural number $\mathbb{N}$ is closed with respect to "addition" :-

$$a+b \in \mathbb{N} \, , \forall \; a,b \in \mathbb{N}$$

but this set not closed under subtraction because $1,2 \in \mathbb{N}$, but $1-2=-1 \notin \mathbb{N}$

Definition :- Group

let G be anonempty set together with a binary operation $*$ We Say that G is a group under this operation if the following properties are satisfied :-

1. $a*b \in G \quad \forall \; a,b \in G$.
2. Associativity: $(ab)c = a(bc)$ for all $a,b,c \in G$.
3. Identity, ther is an element e (called the identity) in G, such that $ae = ea = a$ for all a in G
4. Inverse: For each element a in G, there is an element b in G (called an inverse of a) such that $ab = ba = e \; ; \; a^{-1} = b$

- example:- the set of integers number $\mathbb{Z}$ under addition is a group $(\mathbb{Z},+)$

① $a+b \in \mathbb{Z} \;,\; \forall\, a,b \in \mathbb{Z}$

② $(a+b)+c = a+(b+c) \;,\; \forall\, a,b,c \in \mathbb{Z}$

③ there exist $0 \in \mathbb{Z}$ such that

$a+0 = 0+a = a \;;\; \forall\, a \in \mathbb{Z}$

④ ther exist $-a \in \mathbb{Z}$ for all $a \in \mathbb{Z}$ such that

$a+(-a) = (-a)+a = 0 .$

$\therefore\ (\mathbb{Z},+)$ is a group.

example:- let X is nonempty, then $(P(X),\cup)$ is semi-group with Identity $\emptyset$.

$P(X) = \{A : A \subseteq X\}$

① let $A,B \in P(X)$

$A \subseteq X ,\ B \subseteq X$

$A \cup B \subseteq X$

$A \cup B \in P(X)$

② let $A,B,C \in P(X)$

$(A \cup B)\cup C = A \cup (B \cup C)$ حسب خواص الجبرية

③ $\emptyset \subseteq X \Rightarrow \emptyset \in P(X)$

$A \cup \emptyset = \emptyset \cup A = A \quad \forall\, A \in P(X)$

$\therefore\ \emptyset$ is the Identity

④ let $A \in P(X)$ there is no A^{-1} such that

$A \cup A^{-1} = A^{-1} \cup A = \emptyset$

$\therefore\ (P(X),\cup)$ is not group but semi-group with $\emptyset$ identity.

Definition:- Let $(G, *)$ is a group, then $(G, *)$ is said to be Commutative group iff:-

$$a*b = b*a \quad \forall\ a,b \in G$$

example:- $(\mathbb{Z}, +)$ is Commutative group.

Theorem:- let $(G,*)$ is a group then:

① there is only one Identity element.

② there is a unique element b in G such that $ab = ba = e$, for each a in G

③ $(a^{-1})^{-1} = a$, $\forall\ a \in G$

Proof: ① Let e_1, e_2 are two Identity elements in G

$\therefore\ a * e_1 = a$

and $a * e_2 = a \qquad \forall\ a \in G$

$\therefore\ a * e_1 = a * e_2$

$\Rightarrow\ a^{-1} * (a * e_1) = a^{-1} * (a * e_2)$

$(a^{-1} * a) * e_1 = (a^{-1} * a) * e_2$

$e_1 * e_1 = e_2 * e_2$

$e_1 = e_2 \qquad$ C!

$\therefore$ the identity element is unique

② let a_1^{-1}, a_2^{-1} are two inverse elements to a

$\therefore\ a * a_1^{-1} = e$

and $a * a_2^{-1} = e \qquad \forall\ a \in G$

Since the Identity element is unique then

$\therefore \quad a * a_1^{-1} = a * a_2^{-1}$

$\Rightarrow \quad a^{-1} * (a * a_1^{-1}) = a^{-1} * (a * a_2^{-1})$

$\Rightarrow \quad (a^{-1} * a) * a_1^{-1} = (a^{-1} * a) * a_2^{-1}$

$\Rightarrow \quad e * a_1^{-1} = e * a_2^{-1}$

$\Rightarrow \quad a_1^{-1} = a_2^{-1}$

$\therefore$ the inverse is unique

③ $\because \quad a * a^{-1} = e \quad , \forall a \in G$

& $(a^{-1})^{-1} * a^{-1} = e \quad , \forall a^{-1} \in G$

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

$\Rightarrow \quad (a * a^{-1}) * a = ((a^{-1})^{-1} * a^{-1}) * a$

$\Rightarrow \quad a * (a^{-1} * a) = (a^{-1})^{-1} * (a^{-1} * a)$

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

$\Rightarrow \quad a = (a^{-1})^{-1}$

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

theorem 2 :— let $(G, *)$ is a group then :-

$(a * b)^{-1} = b^{-1} * a^{-1} \quad \forall a, b \in G$

Proof:- let $a, b \in G$

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

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

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

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

$\therefore$ $b^{-1} * a^{-1}$ is the inverse of ~~$(a*b)$~~ element $(a * b)$

but $(a * b)^{-1}$ is the inverse of element $(a * b)$

& since the inverse is unique.

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

theorem:- let $(G,*)$ be a group and $a*b=a*c$ then $b=c \quad \forall \quad a,b,c \in G$

Proof:- let $a,b,c \in G$

$\because \quad a*b = a*c$

$\Rightarrow \quad a^{-1}*(a*b) = a^{-1}*(a*c)$

$\Rightarrow \quad (a^{-1}*a)*b = (a^{-1}*a)*c$

$\Rightarrow \quad e*b = e*c$

$\Rightarrow \quad \therefore \quad b = c$

$\mathbb{Z}_n = \{0, 1, 2, 3, ---, n-1\}$

let $n=5$

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

Q/ Is $(\mathbb{Z}_5, +)$ is group?

+	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

③ $e = 0$

④ $(1)^{-1} = 4$

$(2)^{-1} = 3$

$(3)^{-1} = 2$

$(4)^{-1} = 1$

① $(\mathbb{Z}_5, +)$ is closed

$a+b \in \mathbb{Z}_5 \quad \forall \ a,b \in \mathbb{Z}_5$

② $a+(b+c) = (a+b)+c \quad \forall \ a,b,c \in \mathbb{Z}_5$

$\therefore$ associative hold.

$\therefore (\mathbb{Z}_5, +)$ is group Commutative note: In general $(\mathbb{Z}_n, +)$ Commutative group.

example: $(M_{2\times2}, +)$

$$M_{2\times2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

$M_{2\times2} \neq \emptyset$

Now for $A, B, C \in M_{2\times2}$

① $A + B \in M_{2\times2}$

② $(A+B)+C = A+(B+C)$

③ $e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $A \in M_{2\times2}$

$$e + A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

④ $A^{-1} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$, $A + A^{-1} = e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\therefore (M_{2\times2}, +)$ group

and $A + B = B + A$, $\forall A, B \in M_{2\times2}$

note: $(\mathbb{Z}, +)$ is group

$(\mathbb{Q}, +)$ is group

$(\mathbb{R}, +)$ is group

Note: $(\mathbb{Z}, \cdot)$ is not group

* $(\mathbb{Z}_6 - \{0\}, \cdot)$ is not group, because not closed

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

$\cdot$	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				
5	5				

Now for $(\mathbb{Z}_5 - \{0\}, \cdot)$

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

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

here $e = 1$

$1 \cdot 2 = 2$

$1 \cdot 3 = 3$

$1 \cdot 4 = 4$

$1 \cdot 1 = 1$

$2 \cdot 3 = 1$

$3 \cdot 2 = 1$

$4 \cdot 4 = 1$

$\therefore (1)^{-1} = 1, \quad (2)^{-1} = 3$

$(3)^{-1} = 2, \quad (4)^{-1} = 4$

$\therefore (\mathbb{Z}_5 - \{0\}, \cdot)$ is group and Comm. group

note: $(\mathbb{Z}_n - \{0\}, \cdot)$ is Comm. group where $n = P$

example:- Let $(\mathbb{Z}_8, +)$ group , Comm.

Sol^n $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Now $e = 0$

$(1)^{-1} = 7$, $(2)^{-1} = 6$, $(3)^{-1} = 5$

$(4)^{-1} = 4$, $(5)^{-1} = 3$, $(6)^{-1} = 2$, $(7)^{-1} = 1$

Also: $a + b \in \mathbb{Z}_8$ for each $a, b \in \mathbb{Z}_8$

and $(a+b)+c = a+(b+c) \quad \forall\ a, b, c \in \mathbb{Z}_8$

$\therefore (\mathbb{Z}_8, +)$ is group.

$\because a + b = b + a \ , \forall\ a, b \in \mathbb{Z}_8$

$\therefore (\mathbb{Z}_8, +)$ is Comm. group.

example: Let $G = \{x \in \mathbb{C} : x^4 = 1\}$

Prove that $(G, \cdot)$ is group

Sol^n $\Rightarrow$ $x^4 - 1 = 0 \Rightarrow (x^2-1)(x^2+1) = 0$

$(x-1)(x+1)(x-i)(x+i) = 0$

$\therefore G = \{1, -1, i, -i\}$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

here we have $e = 1$

$(1)^{-1} = 1$

$(-1)^{-1} = -1$

$(i)^{-1} = -i$

$(-i)^{-1} = i$

also $a \cdot b \in G$, $\forall$ $a, b \in G$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall$ $a, b, c \in G$

$\therefore (G, \cdot)$ is group.

example: $G = \{(a,b) : a,b \in \mathbb{Z}_2\}$, IS $(G,+)$ group Comm group?

Solution:-

$$\mathbb{Z}_2 = \{0,1\}$$

$\therefore G = \{(0,0),(1,1),(0,1),(1,0)\}$

+	(0,0)	(1,1)	(0,1)	(1,0)
(0,0)	(0,0)	(1,1)	(0,1)	(1,0)
(1,1)	(1,1)	(0,0)	(1,0)	(0,1)
(0,1)	(0,1)	(1,0)	(0,0)	(1,1)
(1,0)	(1,0)	(0,1)	(1,1)	(0,0)

$e = (0,0)$

$(1,1)^{-1} = (1,1)$

$(0,1)^{-1} = (0,1)$

$(1,0)^{-1} = (1,0)$

$(1,1)^{-1} = (1,1)$

$(a,b) + (c,d) \in G$, $\forall\ (a,b),(c,d) \in G$

also $((a,b)+(c,d)) + (e,f) = (a,b) + ((c,d)+(e,f))$

$\therefore (G,+)$ is group.

and we have $(a,b) + (c,d) = (c,d) + (a,b)$

$\forall\ (a,b),(c,d) \in G$

$\therefore (G,+)$ is Comm. group.

example:- Let $G = \{(a,b) : a,b \in \mathbb{R} , a \neq 0\}$
and let $(a,b) * (c,d) = (ac, bc+d)$
Is $(G, *)$ group, Comm. group?

Sol^n:-

$\forall (a,b), (c,d) \in G$ we have
$(a,b) * (c,d) = (ac, bc+d) \in G$
and $\forall (a,b), (c,d), (x,y) \in G$ we have
$[(a,b) * (c,d)] * (x,y) = (ac, bc+d) * (x,y)$
$= (acx, (bc+d)x + y)$ ... ①
$(a,b) * [(c,d) * (x,y)]$
$= (a,b) * (cx, dx+y)$
$= (acx, bcx + dx + y)$ ... ②
from ① & ② we get
$[(a,b) * (c,d)] * (x,y) = (a,b) * [(c,d) * (x,y)],$
$\forall (a,b), (c,d), (x,y) \in G.$

Now to find $e = (e_1, e_2)$ in G:-
Let $(a,b) * (e_1, e_2) = (a,b)$
$\Rightarrow (ae_1, be_1 + e_2) = (a,b)$
$\therefore a e_1 = a \Rightarrow \because a \neq 0 \Rightarrow e_1 = 1$
and $be_1 + e_2 = b \Rightarrow b + e_2 = b \Rightarrow e_2 = 0$
$\therefore (e_1, e_2) = (1, 0)$

Let $(a,b)^{-1} = (x,y)$

such that $(a,b) * (x,y) = (1,0)$

$\Rightarrow (ax, bx+y) = (1,0)$

$\Rightarrow ax = 1 \quad , \quad bx + y = 0$

$\Rightarrow x = \frac{1}{a} \quad , \quad b\frac{1}{a} + y = 0 \Rightarrow y = \frac{-b}{a}$

$\therefore (a,b)^{-1} = \left(\frac{1}{a}, \frac{-b}{a}\right)$

$\therefore (G, *)$ is group

Now for $(a,b), (c,d) \in G$ we have

$(a,b) * (c,d) = (ac, bc+d)$ --- ①

$(c,d) * (a,b) = (ca, da+b)$ --- ②

from ① & 2 we get that

$(a,b) * (c,d) \neq (c,d) * (a,b)$

$\therefore (G, *)$ is not Comm. group.

Definition: In any group $(G,*)$, Integral power of an element $a \in G$ are defined by:

1) $a^K = a * a * * \cdots * a$ ← K-time

2) $a^0 = e$ Identity element

3) $a^{-K} = (a^{-1})^K$

$= a^{-1} * a^{-1} * \cdots * a^{-1}$ ← K-time

Theorem: let $(G,*)$ be a group $a \in G$, $n,m \in \mathbb{Z}$ the powers of a defined as following:

1) $a^m * a^n = a^{m+n} = a^n * a^m$

2) $(a^m)^n = a^{m \cdot n} = (a^n)^m$

3) $e^n = e$

4) $a^{-n} = (a^n)^{-1}$

Proof: ①

$$a^m * a^n = (\underbrace{a * a * \cdots * a}_{m\text{-time}})(\underbrace{a * a * \cdots * a}_{n\text{-time}})$$

$$= \underbrace{a * a * a \cdots * a}_{m+n\text{-time}}$$

$$= a^{m+n}$$

14

④ $a^{-n} = a^{-1} * a^{-1} * \cdots * a^{-1}$ ← n-time

$= (a)^{-1} * (a)^{-1} * \cdots * (a)^{-1}$ ← n-time

$= (a * a * a * \cdots * a)^{-1}$ ← n-time

$= (a^n)^{-1}$

example/ let $a \in \mathbb{R} - \{0\}$ and G defined by

$G = \{a^k : k \in \mathbb{Z}\}$ Prove that $(G, \cdot)$ group.

Proof:

① Let $x, y \in G$ such that

$x = a^n \quad , \quad y = a^m$ where $n, m \in \mathbb{Z}$

$\therefore x \cdot y = a^n \cdot a^m = a^{n+m} \in G \quad (\because n+m \in \mathbb{Z})$

$\therefore (\cdot)$ is closed

② Let $x = a^n \quad , y = a^m \quad , z = a^L$ where $n, m, L \in \mathbb{Z}$

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$L.H.S = (x \cdot y) \cdot z = (a^n \cdot a^m) \cdot a^L$

$= a^{n+m} \cdot a^L$

$= a^{n+m+L} \in G \; ; n+m+L \in \mathbb{Z}$

$R.H.S = x \cdot (y \cdot z)$

$= a^n \cdot (a^m \cdot a^L)$

$= a^n \cdot (a^{m+L})$

$= a^{n+m+L} \in G \; ; n+m+L \in \mathbb{Z}$

$\therefore L.H.S = R.H.S$

③ $\because 0 \in \mathbb{Z}$ and $a^k \in G \Rightarrow a^0 = 1 \in G$

$\therefore$ 1 is the identity element of G

$(\because \forall x \in G \Rightarrow x = a^n , n \in \mathbb{Z}$

$\Rightarrow x \cdot a^0 = a^n \cdot a^0 = a^{n+0} = a^n = x)$

④ Let $x \in G$ To prove that $\exists\ x^{-1} \in G$

$\because x \in G \Rightarrow x = a^n , n \in \mathbb{Z}$

$\therefore x^{-1} = a^{-n}$

$\Rightarrow x \cdot x^{-1} = a^n \cdot a^{-n}$

$= a^{n+(-n)} = a^0 = 1$

$\therefore (G, \cdot)$ is group

example:- let $(G, *)$ be a group, $a, b \in G$ such that $a*b = b*a$ then $(a*b)^k = a^k * b^k$

Proof:-

$$(a*b)^k = \underbrace{(a*b)*(a*b)*\cdots*(a*b)}_{k\text{-time}}$$

$$= a*(b*a)*(b*a)*\cdots*(b*a)*b$$

$$= a*(a*b)*(a*b)*\cdots*(a*b)*b$$

$$\vdots$$

$$= \underbrace{(a*a*a*\cdots*a)}_{k\text{-time}} * \underbrace{(b*b*\cdots*b)}_{k\text{-time}}$$

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

example: Given $a^2 = e$ for every element of group $(G, *)$, show that the group must be commutative.

Proof:- Let $a, b \in G$

we will show that $a*b = b*a$

$\because a^2 = e \Rightarrow a*a = e$ $\quad *$ by a^{-1}

$\Rightarrow a*a*a^{-1} = e*a^{-1}$

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

$a = a^{-1}$ ---(1)

and we have $b^2 = e \Rightarrow b*b = e$ $\quad *$ by b^{-1}

$\Rightarrow b*b*b^{-1} = e*b^{-1}$

$\Rightarrow b*e = b^{-1}$

$\Rightarrow b = b^{-1}$ ---(2)

Now take $(a*b) \in G$

$(a*b)^2 = e$ $\quad$ multiply by $(a*b)^{-1}$

$(a*b)^{-1} * (a*b)^2 = (a*b)^{-1} * e$

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

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

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

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

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

from (1) & (2) we get

$\therefore a*b = b*a$

Example: let $G = \{f_1, f_2, f_3, f_4\}$ where :

$f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$

Check if (G, o) group, Comm.

Solution:-

o	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

'o' Composite function

(1) $\forall f_i, f_j \in G$; $i, j = 1, 2, 3, 4$

we have $f_i o f_j \in G$

$\therefore$ G is closed with respect to 'o'

(2) $\forall f_i, f_j, f_L \in G$ $i, j, L = 1, 2, 3, 4$

we have that

$(f_i o f_j) o f_L = f_i o (f_j o f_L)$

(3) $e = f_1$

(4) $(f_2)^{-1} = f_2$, $(f_4)^{-1} = f_4$

$(f_3)^{-1} = f_3$

$\therefore$ (G, o) group

~~Now for we have~~

$\forall f_i, f_j \in G$, $i, j = 1, 2, 3, 4$

$f_i o f_j = f_j o f_i$ $\therefore$ (G, o). Comm. group ex: $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, where

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

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

Show that (S_3, o) is group, Is (S_3, o) Comm.?

Sol^n:-

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

① $\forall\ f_i, f_j \in S_3$, $i, j = 1, 2, \ldots, 6$
$f_i \circ f_j \in S_3$

② $\forall\ f_i, f_j, f_m$ $\quad i, j, m = 1, 2, \ldots, 6$
$(f_i \circ f_j) \circ f_m = f_i \circ (f_j \circ f_m)$

③ $e = f_1$

④ $(f_2)^{-1} = f_2$, $(f_3)^{-1} = f_3$, $(f_4)^{-1} = f_4$
$(f_5)^{-1} = f_6$ $\quad (f_6)^{-1} = f_5$

Definition: ① Let G be a group. The order of G is the number of elements of G. denoted by ($o|G|$, $|G|$)
② Let $a \in G$, then order of a is the smallest Possitive integer n, such that $a^n = e$ and denoted by ($o(a)$)

example: ① $G = \{1, -1, i, -i\}$ *الزمرة G تحتوي على 4 عناصر*
here $o|G| = 4$
② $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$
$|G| = 6$ *الزمرة G تحتوي على 6 عناصر*

③ $G = \{e\}$, $|G| = 1$
④ $Z_6 = \{0, 1, 2, 3, 4, 5\}$, $(Z_6, +)$
$\therefore |Z_6| = 6$

$\because 1+1+1+1+1+1 = 6 = 0$
$\therefore o(1) = 6$ or $|1| = 6$
$\because (2)^3 = 2+2+2 = 6$ in $(Z_6, +)$
$\therefore |2| = 3$
$(3)^2 = 6 = 0$ $\therefore |3| = 2$
$(4)^3 = 6 = 0$ $\therefore |4| = 3$

$(5)^6 = 6 = 0$ $\therefore |5| = 6$

Definition: Let $(G,*)$ be a group and Let $\emptyset \neq H \subseteq G$ then $(H,*)$ is said to be subgroup of G If:

① $a,b \in H \Rightarrow a*b \in H$

② $(a*b)*c = a*(b*c)$

③ $a*e = e*a = a \quad \forall\, a \in H$

④ $\forall\, a \in H \;\; \exists\; a^{-1} \in H \quad s.t \;\; a*a^{-1} = e$

For example: $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{C},+)$

$\therefore$ We have $(\mathbb{Z},+)$ subgroup of $(\mathbb{R},+)$

$(\mathbb{Q},+)$ subgroup of $(\mathbb{R},+)$

$(\mathbb{R},+)$ subgroup of $(\mathbb{C},+)$

example: Let $(\mathbb{Z}_{12},+)$ be a group

$H_1 = \{0\}$

$H_2 = \mathbb{Z}_{12}$

$H_3 = \{0,2,4,6,8,10\}$

$H_4 = \{0,3,6,9\}$

$H_5 = \{0,4,8\}$

$H_6 = \{0,6\}$

$\therefore$ $H_1, H_2, H_3, H_4, H_5, H_6$ are subgroups of $(\mathbb{Z}_{12},+)$

Note: H_1, H_2 are called trivial subgroup and H_3, H_4, H_5, H_6 are called proper subgroup