Def.:- let S be a non-empty set and let $*$ be any binary operation defined on S. Then the ordered pair $(S,*)$ is said to be semigroup if :

1. $\forall a,b \in S,\ a*b \in S$ (closed)

2. $(a*b)*c = a*(b*c)\ \forall a,b,c \in S$.

Ex.:- 1. $(Z,+)$.

2. $(Z,\cdot)$.

3. $(P(x),\cup)$, $(P(x),\cap)$

4. $(N,-)$ not semigroup, $3,5 \in N$ but $3-5=-2 \notin N$

Def.:- A semigroup $(S,*)$ is said to be a semigroup with identity if there exists $e \in S$ such that $a*e = e*a = a$ for all $a \in S$.

Ex.:- 1. $(Z,+)$, $e=0$

2. $(Z,\cdot)$, $e=1$

3. $(P(x),\cup)$, $e=\emptyset$

4. $(P(x),\cap)$, $e=X$

Def.:- A group is a pair $(G, *)$ consisting of a nonempty set G and a binary operation $*$ defined on G, satisfying the four requirements:-

1. $a * b \in G$ (closed) for all $a \in G$.
2. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
3. for all $a \in G$, $a * e = e * a = a$ for some $e \in G$
4. for all $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

Def.:- A group $(G, *)$ is said to be a commutative if for all $a, b \in G$, $a * b = b * a$.

* A group $(G, *)$ is said to be finite group if G is finite set.

* A group $(G, *)$ is said to be infinite group if G is infinite set.

Ex.:- $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{R}-\{0\},\cdot)$ — infinite commutative group.

$(\mathbb{Z}-\{0\},\cdot)$, infinite, commutative, not group.

Ex.:- Show that $(P(X),\cup)$ is not group. $X=\{1,2\}$

Sol.:- $X=\{1,2\}$, $P(X)=\{\emptyset, X, \{1\}, \{2\}\}$

ملاحظة:- اذا كانت المجموعة منتهية لبرهان زمرة نستخدم

$\cup$	$\emptyset$	X	$\{1\}$	$\{2\}$
$\emptyset$	$\emptyset$	X	$\{1\}$	$\{2\}$
X	X	X	X	X
$\{1\}$	$\{1\}$	X	$\{1\}$	X
$\{2\}$	$\{2\}$	X	X	$\{2\}$

$\cap$	$\emptyset$	X	$\{1\}$	$\{2\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
X	$\emptyset$	X	$\{1\}$	$\{2\}$
$\{1\}$	$\emptyset$	$\{1\}$	$\{1\}$	$\emptyset$
$\{2\}$	$\emptyset$	$\{2\}$	$\emptyset$	$\{2\}$

1. $\cup$ is closed
2. $\cup$ is asso.
3. $\emptyset = e$
4. A^{-1} not exists

$\{1\} \cup ? \neq \emptyset$

$(P(X),\cup)$ not group

1. $\cap$ is closed
2. $\cap$ is asso.
3. $X = e$
4. A^{-1} not exists

$\{1\} \cap \{1,2\} = \{1\} \neq e = X$

$(P(X),\cap)$ not group

Q₁) Show that $(Z_4, +)$, $(Z_5 - \{0\}, \cdot)$ is group?

$Z_4 = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$e = 0$

$1^{-1} = 3$

$2^{-1} = 2$

$3^{-1} = 1$

$Z_5 = \{0, 1, 2, 3, 4\}$

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$e = 1$

$1^{-1} = 1$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 4$

Q₂) Show that $(Z_6 - \{0\}, \cdot)$ is not group

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

·	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

مغلقة

تجميعية

$e = 1$

$1^{-1} = 1$

$2^{-1} \nexists$ لايوجد

$3^{-1} \nexists$ 〃

$4^{-1} \nexists$ 〃

$5^{-1} = 5$

Note:-

1. $(Z_n, +)$ is group

2. $(Z_n - \{0\}, \cdot)$ is group if n is prime number

3. إذا كانت G مجموعة منتهية وزمرة فان العناصر في الجدول لا تتكرر اكثر من مرة في الصف والعمود

Q) $G = \{e, a, b, c\}$, $(G, \cdot)$ is a group

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Q $G = \{1, -1, i, -i\}$, $(G, \cdot)$ H.W

Show that $(G, \cdot)$ group?

The principal of Mathematical Induction
مبدأ الاستقراء الرياضي :-

The processes (العمليات) of Mathematical Induction

let $p(m)$ be any statement such that $m \in Z^+$ and let $q \in Z^+$, to prove $p(m)$ is true, we must prove that :-

I. $1 \in p(m) \Rightarrow p(1)$ is true.

II. $p(m)$ is true statement.

III. If $m \geq q$ and $p(m)$ is true, then $p(m+1)$ is true".

Ex.:- ① show that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

proof:- I. Assume that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} = p(n)$

then when $n=1$, and hence $1 = \frac{(1)(2)(3)}{6} = R.H.S$

and $L.H.S = 1 = 1^2$ also. Hence $p(1)$ is true or
left hand side
statements.

that is $p(1)$ is true statements

II. assume that $p(m)$ is true, that is

$$p(m) = \sum_{i=1}^{m} i^2 = \frac{m(m+1)(2m+1)}{6}$$

III. to prove $p(m+1)$ is true, we have:

$$\sum_{i=1}^{m} i^2 + (m+1)^2 = \frac{m(m+1)(2m+1)}{6} + (m+1)^2$$

$$\Rightarrow \sum_{i=1}^{m+1} i^2 = \frac{m(m+1)(2m+1) + 6(m+1)^2}{6}$$

$$\Rightarrow \sum_{i=1}^{m+1} i^2 = \frac{m+1[m(2m+1) + 6(m+1)]}{6}$$

$$\Rightarrow \quad = \frac{(m+1)(2m^2 + m + 6m + 6)}{6}$$

$$= \frac{(m+1)(2m^2 + 7m + 6)}{6}$$

$$= \frac{(m+1)[(m+2)(2m+3)]}{6}$$

$$= \frac{(m+1)[(m+1)+1][2((m+1)+1)]}{6}$$

that is $p(m+1)$ is true, hence $p(n)$ is true for all $n \in Z^+$.

Ex(2):-

If $a, b \in R$, $n \in N$, then $\frac{a^n - b^n}{a-b} = \sum_{i=1}^{n} a^{n-i} b^{i-1}$

proof:- to prove by Mathematical induction

I. Assume that $\sum_{i=1}^{n} a^{n-i} b^{i-1} = \frac{a^n - b^n}{a-b} = p(n)$

then when $n=1$ and hence $1 = \sum_{i=1}^{1} a^{1-i} b^{i-1} = 1$

that is $p(1)$ is true statements.

II. suppose that $p(m)$ is true statement

then $p(m)$ $\frac{a^m - b^m}{a-b} = \sum_{i=1}^{m} a^{m-i} b^{i-1}$

Now, to prove $p(m+1)$ is true, we have:-

$$\frac{a^{m+1} - b^{m+1}}{a-b} = \frac{a^{m+1} - ab^m + ab^m - b^{m+1}}{a-b}$$

$$= a\left(\frac{a^m - b^m}{a-b}\right) + b^m$$

$\frac{a^{m+1} - ab^m}{a-b} + b^m$

$\frac{a^{m+1} - ab^m + ab^m - b^{m+1}}{a-b}$

$$= a . \sum_{i=1}^{m} a^{m-i} b^{i-1} + b^m$$

$$= a.(a^{m-1} + a^{m-2} b + \dots + b^{m-1} + b^m)$$

$$= a^m + a^{m-1} b + \dots + ab^{m-1} + b^m$$

$$= \sum_{i=1}^{m+1} a^{(m+1)-i} b^{i-1} \Longrightarrow$$

Thus $p(m+1)$ is true statement. That is $p(n)$ is true for all $n \in N$