GROUPS

Algebraic Structure :- A non-empty set equipped with one or more binary operations is called an algebraic structure. There are many algebraic structures with one binary operation. eg : $(N,+)$, $(R,+,\cdot)$, $(I,+)$, $(I,-)$, etc.

Binary Operation: Let S be a non-empty set. A mapping $S \times S \to S$ is called a binary operation on S. The image of $(s,t) \in S \times S$ under the operation $*$ is written as $s * t$. If $*$ is a binary operation on a set S, then S is closed w.r.t. $*$.

Hence, A system consisting of a non-empty set G together with a binary operation $*$ defined on G is denoted by $(G,*)$.

Binary operation on a set G is also known as binary composition in the set G.

Groupoid :- A groupoid is a system consisting a set G and an associative binary composition in G.

Semi-group :- An algebraic structure $(G,*)$ is called a semi-group if the binary operation $*$ is associative in G.

i.e $\forall\ a,b,c \in G$, $(a*b)*c = a*(b*c)$.

Set of natural numbers N is a semi-group w.r.t. addition. Similarly, $(N,\cdot)$, $(I,+)$ & $(R,+)$ are semi-groups.

Monoid :- A monoid is a system consisting of a set G and an associative binary composition with identity.

Group :- Let G be a non-empty set equipped with a binary operation denoted by $a*b$. Then, the algebraic structure $(G,*)$ or $(G,\cdot)$ is said to be a group iff it satisfies following properties.

1). Closure Property :- $\forall\ a, b \in G$

$\Rightarrow\ a * b \in G$.

2). Associative Property :- $\forall\ a, b, c \in G$

$\Rightarrow\ (a * b) * c = a * (b * c)$.

3). Existence of Identity :- $\forall\ a \in G$, $\exists$ an element $e \in G$ s.t. $e * a = a = a * e$. Then the element 'e' is known as Identity element.

4). Existence of Inverse Identity :- $\forall\ a \in G$, $\exists$ an element $b \in G$ s.t. $a * b = e = b * e$. where 'b' is known as Inverse Identity element & $b = \frac{1}{a}$ or a^{-1}.

Abelian group :- A group $(G, *)$ is said to be abelian or Commutative group if (in addition to above properties) it satisfied following properties. under given binary Composition $*$.

1). Closure Property.
2). Associative property.
3). Existence of Identity.
4). Existence of Inverse Identity.
5). Commutative Property :- $\forall\ a, b \in G$,

$\Rightarrow\ a * b = b * a$

Note :- 1). Group $\Rightarrow$ Monoid $\Rightarrow$ Semi-group $\Rightarrow$ Groupoid.

Group $\not\Leftrightarrow$ Monoid $\not\Leftarrow$ Semi-group $\not\Leftarrow$ Groupoid

2. In case of addition as binary composition $(*)$, $\forall a \in G$, $e = 0$ & $b = -a$

In case of multiplication as binary composition $(*)$, $\forall a \in G$, $e = 1$ & $b = 1/a$.

Finite Group :- Let G be a group of finite number of distinct elements, then the group is said to be finite group.

Infinite Group :- Let G be a group of infinite number of elements, then the group is said to be infinite group.

Order of Group :- The number of elements in a finite group is called order of group. It is denoted by $O(G)$.

The smallest group for a given composition is the set $\{e\}$ & is of order 1.

Ques :- Show that the set N of all natural numbers 1, 2, 3, 4, 5, ... does not form a group with addition or multiplication but it forms a semi-group w.r.t. addition as well as multiplication.

Soln: 1). **Closure Property :-** W.K.T. the set N is closed under addition as well as under multiplication.
∴ both addition & multiplication are binary operations on N.

2). eg :- a) $2 + 3 = 3 + 2 \in N$

b) $2 \cdot 3 = 6 \in N$

2). **Associative Property :-** Addition & Multiplication of natural numbers is associative.
∴ both the algebraic structures $(N, +)$ & $(N, \cdot)$ are semi-groups.

3) eg : a) $1 + (2 + 3) = 6 = (1 + 2) + 3$

b) $1 \cdot (2 \cdot 3) = 6 = (1 \cdot 2) \cdot 3$

3). Identity Element :- In natural numbers, ∃ no number number $e \in N$ s.t. $a+e=a=e+a \ \forall a \in N$.

$\therefore (N,+)$ is not a group $(\because 0 \notin N)$

In case of multiplication, only $1 = e \in N$ s.t.

$a.e = a = e.a$ but ∃ no other natural number except 1 which satisfies the above axiom.

$\therefore (N,\cdot)$ is not a group

Q: Show that the set I of all integers $\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ is a group w.r.t. the operation of addition of integers.

Soln: 1) Closure Property :- $\forall a, b \in I$

$\Rightarrow a+b \in I$

$\therefore$ I is closed under addition.

2). Associative Property :- $\forall a, b, c \in I$.

$\Rightarrow (a+b)+c = a+(b+c)$

$\therefore$ I is ~~closed under~~ associative under addition.

3). Existence of Identity Element :- $\forall a \in I$,

$\exists \ e \in I$ s.t. $a+e=a=e+a$ where $e = 0 \in I$.

$\therefore$ '0' is the Identity element.

4). Existence of Inverse Identity Element :-

$\forall a \in I$, $\exists -a \in I$ s.t.

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

$\therefore$ Every integer possesses additive inverse.

Hence, I is a group under addition.

Cor: Prove that it is abelian group of infinite order.

Sol^n: $\forall\ a, b \in I \Rightarrow a+b = b+a$

$\therefore$ I is commutative under addition.

Also, I contains infinite numbers of elements.

$\therefore$ I is an abelian group of infinite order.

Q: Show that the set of all positive rational numbers forms an abelian group under the composition defined by $a * b = \frac{ab}{2}$.

Sol^n: Let Q_+ be a set of all positive rational numbers.

$\therefore$ we have to prove that $\{Q_+, *\}$ is a group.

1). Closure Property :- $\forall\ a, b \in Q_+$,

$\Rightarrow a * b = \frac{ab}{2} \in Q_+ \quad (\because ab \in Q_+)$

$\therefore$ Q_+ is closed under operation $*$.

2). Associative Property :- $\forall\ a, b, c \in Q_+$, then

$$(a*b)*c = \left(\frac{ab}{2}\right)*c = \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{abc}{4}$$

& $$a*(b*c) = a*\left(\frac{bc}{2}\right) = \frac{a\left(\frac{bc}{2}\right)}{2} = \frac{abc}{4}$$

$\Rightarrow \therefore$ $\boxed{(a*b)*c = a*(b*c)}$

$\therefore$ Q_+ is associative under operation $*$.

3). Existence of Identity Element :- $\forall\ a \in Q_+$, $\exists\ e \in Q_+$ s.t. $a * e = \frac{ae}{2} = a$

$\Rightarrow ae = 2a \Rightarrow a(e-2) = 0$

$\Rightarrow a \neq 0,\ e = 2 \in Q_+$

& $e * a = a$

$\Rightarrow \frac{ea}{2} = a \Rightarrow ea = 2a$

$\Rightarrow ea - 2a = 0$

$\Rightarrow a(e-2) = 0$

$\Rightarrow a \neq 0 ; e = 2 \in Q_+$

$\therefore e = 2 \in Q_+$ is the Identity element under $*$.

4). Existence of Identity Inverse :- $\forall a \in Q_+, \exists b \in Q_+$ s.t. ~~ab~~ $a * b = e = b * a$

$\Rightarrow a * b = e$

$\Rightarrow \frac{ab}{2} = 2 \quad (\because e = 2)$

$\Rightarrow ab = 4$

$\Rightarrow b = \frac{4}{a} \in Q_+$

& $b * a = e$

$\frac{ba}{2} = e$

$ba = 4$

$b = \frac{4}{a} \in Q_+$

$\therefore \left(\frac{4}{a}\right) \in Q_+$ is the Inverse Identity element under $*$.

5). Commutative Property :- $\forall a, b \in Q_+$,

$a * b = b * a$

L.H.S. $= a * b = \frac{ab}{2} \in Q_+$, $\left(\because \forall a, b \in Q_+ \Rightarrow ab \in Q_+ \text{ & } \frac{ab}{2} \in Q_+\right)$

R.H.S. $= b * a = \frac{ba}{2} \in Q_+$

$\Rightarrow Q_+$ is Commutative under operation $*$.

Hence Q_+ is an abelian group under the binary operation $*$.

Prove that $\langle Q^+, * \rangle$, where Q^+ is the set of positive rational numbers, is an abelian group under binary operation $*$ defined as $a * b = \frac{ab}{3} \quad \forall\ a, b \in Q^+$

Solu:- (i) **Closure Property:-**

Let $a, b \in Q^+$

$\Rightarrow ab \in Q^+$ [Product of two +ive rat. is a rat.]

$\Rightarrow \frac{ab}{3} \in Q^+$

$\Rightarrow a * b \in Q^+$

$\therefore Q^+$ is closed under $*$

(ii) **Associative law:-**

Let $a, b, c \in Q^+$

$$(a * b) * c = \left(\frac{ab}{3}\right) * c$$

$$= \frac{\frac{abc}{3}}{3}$$

$$= \frac{abc}{9}$$

$$a * (b * c) = a * \left(\frac{bc}{3}\right)$$

$$= \frac{\frac{abc}{3}}{3}$$

$$= \frac{abc}{9}$$

$\therefore (a * b) * c = a * (b * c) \quad \forall\ a, b, c \in Q^+$

(iii) Existence of Identity :-

To show for each $a \in Q^+$ $\exists$ $e \in Q^+$ such that

$a * e = a = e * a$

$a * e = a$

$\Rightarrow \frac{ae}{3} = a$

$\Rightarrow \frac{ae}{3} - a = 0$

$\Rightarrow \frac{a}{3}(e-3) = 0$ $\quad \{a \neq 0 \text{ as } a \in Q^+\}$

$\Rightarrow e - 3 = 0$

$\Rightarrow \boxed{e = 3} \in Q^+$

$e * a = a$

$\Rightarrow \frac{ea}{3} = a$

$\Rightarrow \frac{ea}{3} - a = 0$

$\Rightarrow a\left(\frac{e}{3} - 1\right) = 0$

$\Rightarrow \frac{a}{3}(e-3) = 0$ $\quad \{a \neq 0 \text{ as } a \in Q^+\}$

$\Rightarrow e - 3 = 0$

$\boxed{e = 3} \in Q^+$

$\therefore 3 \in Q^+ \Rightarrow e \in Q^+$ s.t $a * e = a = e * a$.

$\therefore$ 3 is an identity element which belongs to Q^+

(iv) Existence of Inverse :-

To show for each $a \in Q^+$ $\exists\ x \in Q^+$ such that

$a * x = 3 = x * a$

$a * x = 3$

$\Rightarrow \frac{ax}{3} = 3$

$\Rightarrow \boxed{x = \frac{9}{a}}$

$x * a = 3$

$\Rightarrow \frac{xa}{3} = 3$

$\Rightarrow \boxed{x = \frac{9}{a}}$

$\therefore$ for $a \in Q^+$ $\exists\ \frac{9}{a} \in Q^+$ s.t $a * \frac{9}{a} = 3 = \frac{9}{a} * a$

$\therefore \frac{9}{a}$ is an inv. element which belongs to Q^+

(v) Commutative Law :-

Let $a, b \in Q^+$

then $a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$ $\{\because ab = ba\}$

Hence $\langle Q^+, * \rangle$ is an abelian group.

Prove that $\langle Q, * \rangle$ where Q is the set of all rationals except 1, is an abelian group under binary operation $*$ defined as $a*b = a+b-ab$.

Soln:- **Closure Property:-**

Let $a, b \in Q$ then

$a+b \in Q$ and $ab \in Q$

$\Rightarrow a+b \in Q$ and $-ab \in Q$

$\Rightarrow a+b-ab \in Q$

$\Rightarrow a*b \in Q$

$\therefore Q$ is closed under $*$

Associative law:-

Let $a, b, c \in Q$

$$(a*b)*c = (a+b-ab)*c$$
$$= a+b-ab+c-(a+b-ab)c$$
$$= a+b-ab+c-ac-bc+abc$$
$$= a+b+c-ab-bc-ac+abc.$$

$$a*(b*c) = a*(b+c-bc)$$
$$= a+b+c-bc-a(b+c-bc)$$
$$= a+b+c-bc-ab-ac+abc$$
$$= a+b+c-ab-bc-ac+abc.$$

$\therefore (a*b)*c = a*(b*c)$

Existence of Identity :-

To show for each $a \in \mathbb{Q}$ $\exists\ e \in \mathbb{Q}$ s.t

$a * e = a = e * a$

$a * e = a$

$\Rightarrow a + e - ae = a$

$\Rightarrow a + e - ae - a = 0$

$\Rightarrow e - ae = 0$

$\Rightarrow e(1-a) = 0$

$\Rightarrow \boxed{e = 0}$ $\{1 - a \neq 0,\ a \neq 1\}$

Illy, $e * a = a$

$\Rightarrow e + a - ea = a$

$\Rightarrow e + a - ea - a = 0$

$\Rightarrow e - ea = 0$

$\Rightarrow e(1-a) = 0$

$\Rightarrow \boxed{e = 0}$ $\{1 - a \neq 0$ but $a \neq 1\}$

$\therefore e = 0 \in \mathbb{Q}$

$\exists\ e \in \mathbb{Q}$ s.t $a * e = a = e * a$ $\forall\ a \in \mathbb{Q}$.

Existence of Inverse :-

To show for each $a \in \mathbb{Q}$ $\exists\ x \in \mathbb{Q}$ s.t

$a * x = 0 = x * a$

$a * x = 0$

$\Rightarrow a + x - ax = 0$

$\Rightarrow a + (1-a)x = 0$

$\Rightarrow x(1-a) = -a$

$\Rightarrow x = \frac{-a}{1-a}$

$\Rightarrow \boxed{x = \frac{a}{a-1}}$

$\therefore a^{-1} = \frac{a}{a-1}$

Illy, $x * a = 0$

$\Rightarrow x + a - xa = 0$

$\Rightarrow x(1-a) + a = 0$

$\Rightarrow x(1-a) = -a$

$\Rightarrow x = \frac{-a}{1-a}$

$\Rightarrow \boxed{x = \frac{a}{a-1}}$

Commutative Law :-

Let $a, b \in Q$

$$a * b = a + b - ab$$
$$= b + a - ba$$
$$= b * a$$

Hence, $\langle Q, * \rangle$ is an abelian gp.

Let $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \text{ where } a \neq 0, \text{ be a real no.} \right\}$. Prove G is an abelian gp. under matrix multiplication.

Soln:- Closure Property :-

Let $A, B \in G$

where $A = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix}$ where $a_1, a_2 \neq 0$

Now,

$$AB = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 + 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{bmatrix} \in G \quad \text{where } a_1 a_2 \neq 0$$

$$|AB| = \begin{vmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{vmatrix}$$

$\therefore AB \in G$ $\therefore G$ is closed under mult.

Associative Law :-

Let $A, B, C \in G$

where $A = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix}$, $C = \begin{bmatrix} a_3 & 0 \\ 0 & 0 \end{bmatrix}$

$$(AB)C = \left\{ \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix} \right\} \begin{bmatrix} a_3 & 0 \\ 0 & 0 \end{bmatrix}$$

$$= \left\{ \begin{bmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{bmatrix} \right\} \begin{bmatrix} a_3 & 0 \\ 0 & 0 \end{bmatrix}$$

$$= \left\{ \begin{bmatrix} a_1 a_2 a_3 & 0 \\ 0 & 0 \end{bmatrix} \right\}$$

$$= \begin{bmatrix} a_1 a_2 a_3 & 0 \\ 0 & 0 \end{bmatrix}$$

$$A(BC) = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}\left\{\begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a_3 & 0 \\ 0 & 0 \end{bmatrix}\right\}$$

$$= \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}\left\{\begin{bmatrix} a_2a_3 & 0 \\ 0 & 0 \end{bmatrix}\right\}$$

$$= \begin{bmatrix} a_1a_2a_3 & 0 \\ 0 & 0 \end{bmatrix}$$

$(AB)C = A(BC)$

$\therefore$ Associative law holds under matrix multiplication.

Existence of Identity :-

For each $A \in G$ $\exists$ an identity matrix I of order 2 such that

$$AI = A = IA$$

ie $$\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$IA = A$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$$

Hence, identity matrix is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Existence of Inverse :-

For each $A \in G$, $\exists\, B = A^{-1} \in G$ such that

$$AA^{-1} = I = A^{-1}A.$$

i.e. $AA^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = A^{-1}A$

*

Show that set $G_1 = \{a+b\sqrt{2} ; a,b \in Q\}$ where Q is the set of rationals is a group / (is an infinite abelian group) under addition.

Solu:- Let $x = a+b\sqrt{2}$
$y = c+d\sqrt{2} \in G_1$ where $a, b, c, d \in Q$.

(i) Closure Property :-

$x+y = (a+b\sqrt{2}) + (c+d\sqrt{2})$
$= (a+c) + \sqrt{2}(b+d)$ [$\because a,b,c,d \in Q \Rightarrow a+b, c+d \in Q$]
$\in G_1$

$\therefore G_1$ is closed under addition.

(ii) Associative Law :-

Let $x, y, z \in G_1$ where $x = a+b\sqrt{2}$
$y = c+d\sqrt{2}$
$z = e+f\sqrt{2}$

$x+(y+z) = (a+b\sqrt{2}) + [(c+d\sqrt{2}) + (e+f\sqrt{2})]$
$= (a+b\sqrt{2}) + [(c+e) + (d+f)\sqrt{2}]$
$= [a+(c+e)] + \sqrt{2}[b+(d+f)]$
$= [(a+c)+e] + \sqrt{2}[(b+d)+f]$
$= [(a+c)+\sqrt{2}(b+d)] + [e+\sqrt{2}f]$
$= [(a+\sqrt{2}b) + (c+\sqrt{2}d)] + [e+\sqrt{2}f]$
$= (x+y)+z$.

$\therefore x+(y+z) = (x+y)+z \quad \forall x, y, z \in G_1$.

$\therefore$ Associative law holds under addition.

(iii) Existence of Identity Element :-

$\forall\ x = a+b\sqrt{2} \in G_1 \quad \exists\ 0+0\sqrt{2} \in G_1$ s.t.
$(a+b\sqrt{2}) + (0+0\sqrt{2}) = a+b\sqrt{2} = (0+0\sqrt{2}) + (a+b\sqrt{2})$
i.e. $(a+0) + \sqrt{2}(b+0) = a+b\sqrt{2} = (0+a) + \sqrt{2}(0+b)$

$\therefore$ 0 is an identity element of G_1.

(iv) Existence of Inverse element :-

$\forall\ x = a+b\sqrt{2} \in G_1\ \exists\ -a-b\sqrt{2} \in G_1$ such that

$(a+b\sqrt{2})+(-a-b\sqrt{2}) = 0+\sqrt{2}0 = (-a-b\sqrt{2})+(a+b\sqrt{2})$

i.e $[a+(-a)]+\sqrt{2}[b+(-b)] = 0+\sqrt{2}\cdot 0 = [(-a)+a]+\sqrt{2}[(-b)+(b)]$

$0+\sqrt{2}(0) = 0+\sqrt{2}\cdot 0 = 0+\sqrt{2}\cdot 0$

$\therefore$ $-a-b\sqrt{2}$ is an inverse of $a+b\sqrt{2}$.

(V) Commutative Law :- Let $x = a+b\sqrt{2} \in G_1$.

$y = c+d\sqrt{2}$

$a, b, c, d \in \mathbb{Q}$.

$x+y = (a+b\sqrt{2})+(c+d\sqrt{2})$

$= (a+c)+(b+d)\sqrt{2}$

$= (c+a)+(d+b)\sqrt{2}$

$= (c+d\sqrt{2})+(a+b\sqrt{2})$

$= y+x \quad \forall\ x, y \in G_1$

$\therefore\ x+y = y+x$

Hence, $\langle G_1, + \rangle$ is a group.

Show that the set of matrices $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} ; a \neq 0, b \neq 0, a, b \in R \right\}$ is an abelian group under matrix multiplication.

Soln:- Closure Property:-

Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ be any two elements of G where $a \neq 0, b \neq 0, c \neq 0, d \neq 0$.

Then

$$AB = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

$$= \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in G.$$

$ac \neq 0$, $bd \neq 0$ and $ac, bd \in R$

$\therefore$ closure property holds in G.

Associative law:- Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$, $C = \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$ be any three elements of G where $a, b, c, d, e, f \neq 0$.

Then

$$A(BC) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \left\{ \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} \right\}$$

$$= \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \left\{ \begin{bmatrix} ce & 0 \\ 0 & df \end{bmatrix} \right\}$$

$$= \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} ce & 0 \\ 0 & df \end{bmatrix}$$

$$= \begin{bmatrix} ace & 0 \\ 0 & bdf \end{bmatrix}$$

$$(AB)C = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \right\} \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$= \left\{ \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \right\} \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$= \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$= \begin{bmatrix} ace & 0 \\ 0 & bdf \end{bmatrix}$$

$\therefore A(BC) = (AB)C \quad \forall A, B, C \in G.$

(iii) Existence of Identity Element :- $\forall A \in G \; \exists I \in G$ such that $AI = A = IA$.

$\therefore I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an identity element of G.

* $AI = A$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

$A = IA$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

$\therefore AI = A = IA$

(iv) Existence of Inverse Element :- $\forall A \in G$, we have to find $B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in G$ such that

$AB = I = BA$.

$$AB = I$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\Rightarrow ac = 1, \quad bd = 1$

$\Rightarrow \boxed{c = \frac{1}{a}}, \boxed{d = \frac{1}{b}}$

Also $c \neq 0, d \neq 0$ as $a \neq 0, b \neq 0$

$\therefore B = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{bmatrix}$

Now, $BA = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$

$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$= I$

$\therefore B = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{bmatrix}$ is the inverse of $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$

Commutative law :- Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in G_1$.

Then, $AB = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$

$= \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}$

$= \begin{bmatrix} ca & 0 \\ 0 & db \end{bmatrix}$

$= BA$

$\Rightarrow AB = BA$

Hence G_1 is an abelian group under matrix multiplication.

Show that the set $G_1 = \{1, \omega, \omega^2\}$ of cube roots of unity forms a finite abelian group of order 3 under multiplication of complex numbers.

Solu:- Here $G_1 = \{1, \omega, \omega^2\}$

Since G_1 is finite, we form the composition table, using $\omega^3 = 1$.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Closure Property:- Since all the elements in composition table are elements of G_1, so G_1 is closed under multiplication.

Associative Law:- Since all the elements of G_1 are complex numbers and multiplication of complex numbers is associative.

$\therefore a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \forall\ a, b, c \in G_1$.

Existence of Identity Element:- From composition table,

$1\cdot 1 = 1 = 1\cdot 1$

$\omega\cdot 1 = \omega = 1\cdot\omega$

$\omega^2\cdot 1 = \omega^2 = 1\cdot\omega^2$

i.e $a\cdot 1 = a = 1\cdot a \quad \forall\ a \in G_1$.

Existence of Inverse Element:- From the composition table,

$1\cdot 1 = 1 = 1\cdot 1 \Rightarrow 1^{-1} = 1$

$\omega\cdot\omega^2 = \omega^3 = \omega^2\cdot\omega$

$\Rightarrow \omega\cdot\omega^2 = 1 = \omega^2\cdot\omega$

Now $\omega\cdot\omega^2 = 1$

$\omega^2 = \frac{1}{\omega}$

$\omega^2 = \omega^{-1}$

i.e $\boxed{\omega^{-1} = \omega^2}$

Also, $1 = \omega^2\cdot\omega$

$\frac{1}{\omega^2} = \omega$

$\boxed{(\omega^2)^{-1} = \omega}$

$\therefore$ Inverse of each element exists in G_1.

Commutative Law:- Since all the elements of G_1 are complex numbers and multiplication of complex numbers is commutative.

$\therefore\ a\cdot b = b\cdot a \quad \forall\ a, b \in G_1$.

Hence, G_1 is a finite abelian group under multiplication of order 3.

Q: Prove that the set Q_0 of all non-zero rational numbers forms a group under the operation of multiplication of rational numbers.

Soln: 1). Closure Property :- $\forall\ a, b \in Q_0$,

then, $a \times b \in Q_0$ (∵ Product of two non-zero rational nos is a non-zero rational number)

∴ Q_0 is closed under multiplication.

2). Associative Property :- $\forall\ a, b, c \in Q_0$,

$$(a \times b) \times c = a \times (b \times c)$$

∵ Product of two non-zero rational number is associative

∴ Q_0 is associative under multiplication.

3). Existence of Identity :- $\forall\ a \in Q_0$, $\exists\ e = 1 \in Q_0$

s.t $a.1 = a = 1.a$

∴ $1 \in Q_0$ is the multiplicative Identity element.

4). Existence of Inverse Identity :- $\forall\ a \in Q_0$, $\exists\ b \in Q_0$

s.t. $a \times b = e = 1$

$\Rightarrow a \times b = 1$

$\Rightarrow b = \frac{1}{a}$

$\Rightarrow a \times \frac{1}{a} = 1 = \frac{1}{a} \times a$

∴ $b = \frac{1}{a} \in Q_0$ is the Inverse Identity element under multiplication.

5). Commutative Property :- $\forall\ a, b \in Q_0$

$\Rightarrow \quad a \times b = b \times a$

$\because$ Product of two non-zero rational numbers is commutative

$\Rightarrow$ Q_0 is commutative under multiplication.

Hence Q_0 is an abelian group under multiplication.

Properties of Groups :-

Theorem : 1: Uniqueness of Inverse

"The inverse of each element of a group is unique.

Proof: Let G be any group (non-empty set) with binary composition as multiplicatively.

$\therefore \quad \forall\ a \in G, \exists\ e \in G.$

Also let b & c be the inverse elements of a

$\therefore \quad ba = e = ab \quad$ & $\quad ca = e = ac$ (Identity Property)

Now; $\quad b(ac) = b(e) = b$

& $\quad (ba)c = (e)c = c$

But if G is a group then it should satisfy associative property i.e. $b(ac) = (ba)c$

$\Rightarrow \quad b = c$

Hence, Inverse element of each element of a group is unique.

Note :- Identity element is its own inverse.

Theorem: 2:

"If the inverse of a is a^{-1}, then inverse of a^{-1} is a.

i.e. T.Prove $(a^{-1})^{-1} = a$.

Proof:- Let G be a group under multiplication.

$\forall\ a \in G$, $\exists\ e$ & $a^{-1} \in G$ s.t.

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

$$(a^{-1})^{-1}(a^{-1}a) = (a^{-1})^{-1}.e \qquad \text{(Pre multiplying both sides by } (a^{-1})^{-1}\text{)}$$

$$[(a^{-1})^{-1}.a^{-1}].a = (a^{-1})^{-1}$$

$$e.a = (a^{-1})^{-1} \qquad \text{(Using property, } aa^{-1} = e\text{)}$$

$$\Rightarrow \boxed{a = (a^{-1})^{-1}} \text{ or } \boxed{(a^{-1})^{-1} = a}$$

Hence, proved.

Theorem: 3: **Uniqueness of Identity:-**

"The Identity element in a group is unique."

Proof:- Let G be a group under binary composition of multiplication.

Let us suppose e & e' are two identity elements of G.

$\therefore\ ee' = e$ (if e' is Identity element)

& $ee' = e'$ (if e is Identity element)

But ee' is unique element

$$\Rightarrow e = ee' = e'$$

$$\Rightarrow e = e'$$

Hence, Identity element is unique.

Theorem: 4: "Cancellation law holds good in a group".

i.e. If $a, b, c \in G$, then

$ab = ac \Rightarrow b = c$ (Left cancellation law)

& $ba = ca \Rightarrow b = c$ (Right cancellation law)

Proof:- Let G be group under multiplication.

$\forall a \in G, \exists\ a^{-1} \in G$ s.t. $a a^{-1} = e = a^{-1}.a$

where 'e' is the Identity element of G.

Now, $ab = ac$

Premultiplying both sides by a^{-1}.

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

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

$\Rightarrow eb = ec$

$\Rightarrow \boxed{b = c}$

Also, $ba = ca$

Post multiplying both sides by a^{-1}.

$(ba)a^{-1} = (ca)a^{-1}$.

$b(aa^{-1}) = c(aa^{-1})$

$be = ce$

$\boxed{b = c}$

Hence, proved.

In case of addition,

$a + b = a + c$

$-a + a + b = -a + a + c$

$b = c$

Hence, proved.

$b + a = c + a$

$b + a + (-a) = c + a + (-a)$

$b = c$

Theorem:- 6:- If a & b are any two elements of a group G, then the equation $ax = b$ & $ya = b$ have unique solution in G.

Theorem: 7:- Prove that $(ab)^{-1} = b^{-1}a^{-1}$ $\forall\, a, b \in G$.

i.e. the inverse of the product of two elements of a group GT is the product of the inverses taken in the inverse order.

Ques: Show that the set of all complex numbers of the form $\cos\theta + i\sin\theta$, where θ is any

Soln: ~~Closure Property~~ :-

Let $G = \{z : z = \cos\theta + i\sin\theta,\ \theta \in R\}$; R denotes reals.

1) **Closure Property:-** $\forall\ z_1, z_2 \in G$,

where $z_1 = \cos\theta_1 + i\sin\theta_1$ & $z_2 = \cos\theta_2 + i\sin\theta_2$,

$$\Rightarrow z_1 z_2 = (\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)$$
$$= \cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2) \quad \in G$$

$\because\ \theta_1, \theta_2 \in R \Rightarrow \theta_1 + \theta_2 \in R.$

$\therefore$ G is closed under multiplication.

2) **Associative Property:-** Let $z_1, z_2, z_3 \in G$, then

$$z_1 \cdot (z_2 \cdot z_3) = \text{cis}\,\theta_1 \cdot (\text{cis}\,\theta_2 \cdot \text{cis}\,\theta_3)$$
$$= \text{cis}\,\theta_1 \cdot \text{cis}\,(\theta_2+\theta_3)$$
$$= \text{cis}\,(\theta_1+\theta_2+\theta_3)$$

& $(z_1 \cdot z_2)\cdot z_3 = (\text{cis}\,\theta_1\ \text{cis}\,\theta_2)\cdot \text{cis}\,\theta_3$
$$= \text{cis}\,(\theta_1+\theta_2)\cdot \text{cis}\,\theta_3$$
$$= \text{cis}\,(\theta_1+\theta_2+\theta_3)$$

$\Rightarrow$ $\boxed{(z_1 \cdot z_2)\cdot z_3 = z_1 \cdot (z_2 \cdot z_3)}$

$\therefore$ G is associative under multiplication

3) Existence of multiplicative identity (Identity Inverse) :- $\forall z \in G, \exists 1 \in G$

s.t. $z.1 = z = 1.z$.

Ie $z.1 = (\cos\theta + i\sin\theta).(\cos 0 + i\sin 0)$

$= \cos(\theta+0) + i\sin(\theta+0)$

$= \cos\theta + i\sin\theta = z$

& $1.z = (\cos 0 + i\sin 0).(\cos\theta + i\sin\theta)$

$= \cos(0+\theta) + i\sin(0+\theta)$

$= \cos\theta + i\sin\theta = z$

$\Rightarrow$ $\boxed{z.1 = z = 1.z}$

$\therefore$ '1' $= \cos 0 + i\sin 0$ is the multiplicative identity of G.

4). Existence of Inverse Identity :- Let $z \in G$

then $\exists\ z^{-1} \in G$ where $z^{-1} = (\cos\theta + i\sin\theta)^{-1}$

$= \cos\theta - i\sin\theta$

s.t. $zz^{-1} = 1 = z^{-1}.z$.

Now; $zz^{-1} = (\cos\theta + i\sin\theta)(\cos\theta - i\sin\theta)$

$= \cos^2\theta + \sin^2\theta = 1$

& $z^{-1}z = (\cos\theta - i\sin\theta)(\cos\theta + i\sin\theta)$

$= \cos^2\theta + \sin^2\theta = 1$

Hence, $\boxed{zz^{-1} = 1 = z^{-1}z}$

$\therefore$ G is a group for multiplication of complex numbers.

Composition Table for finite sets :-

A binary composition in a finite set can be shown in a tabular form known as composition Table.

Note: Composition table for a finite group contains each element exactly once in each of its rows & columns.

Example ①: Show that the set $G = \{1, \omega, \omega^2\}$; where ω is a imaginary cube root of unity is a group with respect to multiplication.

Soln: Composition table is

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

($\because$ $\omega^3 = 1$
$\omega^4 = \omega^3 \cdot \omega = 1 \cdot \omega = \omega$

1). Asso **Closure:-** Since all the entries in the composition table are the elements of set G.
$\therefore$ G is closed w.r.t. multiplication.

2). **Associative:-** The elements of G are complex numbers (as cube root of unity are complex numbers). We know that Complex numbers are associative in nature.

3). **Existence of Identity Element :-**
From the table we see that
$1(1) = 1$; $1(\omega) = \omega$ & $1(\omega^2) = \omega^2$
$\therefore$ '1' is the multiplicative identity of G.

4). **Existence of Inverse Identity Element :-**
The inverse of $1, \omega$ & ω^2 are ω 1, ω^2 & ω resp.

5). **Commutative:-** The multiplication of complex numbers is commutative.

Also, No. of elements in G is 3.
$\therefore$ $O(G) = 3$.

Q2: Show that the four fourth roots of unity namely $1, -1, i, -i$ form a group w.r.t. multiplication.

Soln: Let $G = \{1, -1, i, -i\}$.

The Composition Table is

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

1). Closure Property :- Since all the elements of the Composition Table are the elements of set G. $\therefore$ G is closed under multiplication.

2). Associative Property :- The elements of G are Complex numbers and Complex numbers are associative. $\therefore$ G is associative under multiplication.

3). Existence of Identity Element :-
From the Composition Table, we see that

$1(1) = 1$, $1(-1) = -1$; $1(i) = i$; $1(-i) = -i$

$\therefore$ '1' is the Identity element of G.

4) Existence of Inverse Identity Element :-
We know that the Identity element is its own inverse.

$\therefore$ $1.1 = 1$; $-i.i = 1$

$-1.-1 = 1$; $i.-i = 1$

In 1.1, '1' is the Inverse Identity element of 1.
In $-i.i$, '$-i$' is " " " " of i
In $-1.-1$; '-1' " " " " of -1
In $i, -i$; 'i' " " " " of $-i$

Also G contains 4 elements.
$\therefore$ G is a group of order 4.

Q: Show that the set of six transformations $f_1, f_2, f_3, f_4, f_5, f_6$ on the set of Complex numbers defined by

$f_1(z) = z$, $f_2(z) = \frac{1}{z}$, $f_3(z) = 1 - z$, $f_4(z) = \frac{z}{z-1}$, $f_5(z) = \frac{1}{1-z}$, $f_6(z) = \frac{z-1}{z}$ forms a finite non-abelian group of order six w.r.t. the composition known as composite of two functions or product of two functions.

Soln: If $f: A \to B$ & $g: B \to C$, then by definition

$gf: A \to C$ s.t. $(gf)(x) = g[f(x)]$ $\forall x \in A$.

Then the function gf is called the composite of the functions g & f.

Now: $f_1 f_1 = f_1$; $f_1 f_2 = f_2 = f_2 f_1$, $f_1 f_3 = f_3 = f_3 f_1$, & so on

Also, $(f_1 f_2)z = f_1(f_2(z)) = f_1\left(\frac{1}{z}\right) = \frac{1}{z} = f_2(z)$

$(f_2 \cdot f_2)z = f_2(f_2(z)) = f_2\left(\frac{1}{z}\right) = \frac{1}{1/z} = z = f_1(z)$

$(f_2 \cdot f_3)z = f_2(1-z) = \frac{1}{1-z} = f_5$

$(f_2 \cdot f_4)z = f_2(f_4(z)) = f_2\left(\frac{z}{z-1}\right) = \frac{z-1}{z} = f_6$

$(f_2 \cdot f_5)z = f_2(f_5(z)) = f_2\left(\frac{1}{1-z}\right) = 1 - z = f_3(z)$.

$(f_2 \cdot f_6)z = f_2(f_6(z)) = f_2\left(\frac{z-1}{z}\right) = \frac{z}{z-1} = f_4$

$(f_3 \cdot f_2)z = f_3(f_2(z)) = f_3\left(\frac{1}{z}\right) = \frac{1}{1-1/z} = f_5 = \frac{z-1}{z} = f_6$

$(f_3 \cdot f_3)z = f_3(f_3(z)) = f_3(1-z) = 1-(1-z) = 1-1+z = z = f_1$

$(f_4 \cdot f_4)z = f_4(f_4(z)) = f_4\left(\frac{z}{z-1}\right) = \frac{\frac{z}{z-1}}{\frac{z}{z-1}-1} = \frac{\frac{z}{z-1}}{\frac{z-z+1}{z-1}} = \frac{z}{1} = z = f_1$

$(f_5 \cdot f_5)z = f_5(f_5(z)) = f_5\left(\frac{1}{1-z}\right)$

$= \frac{1}{1-\frac{1}{(1-z)}} = \frac{1-z}{z-z-1} = \frac{1-z}{-z} = \frac{z-1}{z} = f_6$

·	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_5	a_6	a_3	a_4
a_3	a_3	a_6	a_1	a_5	a_4	a_2
a_4	a_4	a_5	a_6	a_1	a_2	a_3
a_5	a_5	a_4	a_2	a_3	a_6	a_1
a_6	a_6	a_3				a_5

$a_6 \cdot a_6 = a_6\left(\frac{z-1}{z}\right) = \frac{\left(\frac{z-1}{z}\right)-1}{\frac{z-1}{z}} = \frac{z-1-z}{z} \times \frac{z}{z-1} = \frac{-1}{z-1} = \frac{1}{1-z} = a_5$

$a_4 \cdot a_3 = a_4\left(a_3(z)\right) = a_4\left(\frac{1}{1-z}\right) = \frac{\frac{1}{1-z}}{\left(\frac{1}{1-z}\right)-1} = \frac{1}{1-z-1+z} = \frac{1}{-z} = \frac{z-1}{z} = a_6$

$a_3 \cdot a_4 = a_3\left(\frac{z}{z-1}\right) = \frac{1}{1-\frac{z}{z-1}} = \frac{z-1}{z-1-z} = \frac{-1}{-1} = 1 = a_5$

Lagrange's Theorem :- If G is a finite gp. and H is a subgp. of G, then $O(H) \mid O(G)$.

Proof:- Let G be a finite group and H be a subgroup of G.

$\therefore$ H is also finite

$\therefore$ Let $H = \{h_1, h_2, \dots h_n\}$ where each h_i is distinct.

Consider $Ha = \{h_1a, h_2a, \dots h_na\}$.

We claim all h_ia's are distinct. For if,

$h_ia = h_ja$

$\Rightarrow h_i = h_j$ (Right cancellation law)

a contradiction, since each h_i's are distinct.

Hence Ha has distinct elements.

Now, G is finite. $\therefore$ number of distinct right cosets of H in G is also finite, say k.

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k = \bigcup_{i=1}^{k} Ha_i.$$

$O(G)$ = No. of elements in Ha_1 + No. of elt. in Ha_2 + $\dots$ + No. of elt. in Ha_k.

$= n + n + \dots$ k times

$= nk$.

$\therefore O(G) = n|2$

$O(G) = O(H) \cdot k$

$\Rightarrow n \mid O(G)$

$\Rightarrow O(H) \mid O(G)$

Index of a Subgroup:- Let G be a group and H be a subgroup of G. Then number of rt (lft) cosets of H in G is called index of H in G. It is denoted by $[G:H]$.

Theorem:- If G is a finite group and H is a subgroup of G. Then $[G:H] = \frac{O(G)}{O(H)}$.

Proof:- $O(G) = nk$, where k is no. of distinct rt cosets of H in G.

$$\therefore k = \frac{O(G)}{n} = \frac{O(G)}{O(H)}$$

$$\Rightarrow [G:H] = \frac{O(G)}{O(H)}.$$

Normal Subgroup:- A subgp. H of gp. G is called Normal subgp. of G if for every $g \in G$, $h \in H$
$\Rightarrow ghg^{-1} \in H$

Ques:- Let G be gp. of 2 by 2 invertible matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$; $ad - bc \neq 0$. Let $H = \left[\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} ; a \neq 0 \right]$. Then H is a normal subgp. of G.

Solu:- Let us show that H is a subgp. of G.

Let $h_1, h_2 \in H$ s.t

$$h_1 = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \quad h_2 = \begin{bmatrix} a_1 & 0 \\ 0 & a_1 \end{bmatrix} ; \quad a \neq 0, a_1 \neq 0$$
$\because aa_1 \neq 0$

- $h_1 h_2 = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & a_1 \end{bmatrix} = \begin{bmatrix} aa_1 & 0 \\ 0 & aa_1 \end{bmatrix} \in H$

$\therefore H$ is closed under matrix multiplication.

For $A \in H$,

$$A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \quad |A| = \begin{vmatrix} a & 0 \\ 0 & a \end{vmatrix} = a^2.$$

Also, $A_{11} = a$, $A_{12} = 0$, $A_{21} = 0$, $A_{22} = a$

$$\therefore \operatorname{adj} A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}' = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

Now, $A^{-1} = \dfrac{\operatorname{adj} A}{|A|} = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{bmatrix} \in H, \ a \neq 0.$

- Thus, each elt. belonging to H has multiplicative inverse. Hence H is a subgp. of G.

Again for $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, $h = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in H$.

Let $ghg^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} a^2 & ba \\ ca & da \end{bmatrix} \begin{bmatrix} & \\ & \end{bmatrix}$$

$$= \begin{bmatrix} \frac{a^2d-bac}{ad-bc} & \frac{-a^2b+ba^2}{ad-bc} \\ \frac{cad-dac}{ad-bc} & \frac{-cab+da^2}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{a(ad-bc)}{ad-bc} & 0 \\ 0 & \frac{a(ad-bc)}{ad-bc} \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in H.$$

Hence, H is normal subgp of G under matrix multiplication.

Theorem:- The intersection of 2 normal subgps of a gp is a normal subgp.

Proof:- Let H and K be 2 normal subgps of gp G.

Since H and K are subgp of G.

$\therefore$ $H \cap K$ is also subgp of G.

T.P $H \cap K$ is normal subgp of G.

Let $g \in G$ and $h \in H \cap K$.

Now, $h \in H \cap K$.

$\Rightarrow h \in H$ and $h \in K$.

Since H is normal subgp of G.

$\therefore$ $g \in G, h \in H \Rightarrow ghg^{-1} \in H$ —(1)

Ily, K is normal subgp of G.

$\therefore$ $g \in G, h \in K \Rightarrow ghg^{-1} \in K$ —(2)

from (1) and (2)

$ghg^{-1} \in H \cap K$.

$\therefore$ $g \in G, h \in H \cap K$

$\Rightarrow ghg^{-1} \in H \cap K$.

Hence $H \cap K$ is a normal subgp of G.

Quotient Group :- Let G_1 be a group and H be a normal subgroup of G_1. Let G_1/H denotes the set of right (left) cosets of H in G_1. Then G_1/N is a group called quotient group or factor group under the coset multiplication defined by

$$(aH)(bH) = abH$$

Cyclic Group :- A group G_1 is called cyclic if for some $a \in G_1$, every element $x \in G_1$ is of form a^n for some $n \in Z$. Element a is called generator of G_1.

- ∴ If G_1 is cyclic then we write it as $G_1 = \langle a \rangle$

Eg :- If $G_1 = \{1, -1, i, -i\}$, then G_1 is a cyclic gp. generated by i.

∵ Every elt of G_1 is of form i^n for some $n \in G_1$.
Hence i is generator for cyclic gp. $\{ i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1 \}$

Theorem :- Every subgroup of a cyclic group is cyclic.

Proof :- Let G_1 be cyclic group generated by a.

i.e. $G_1 = \langle a \rangle$

Let H be subgp. of G_1.

Case-I If $H = \{e\}$, then $H = \langle e \rangle$

Case-II If $H \neq \{e\}$ then $O(H) \geq 2$ i.e. $\exists\ e \neq a \in H$

Since H is a subgp. ∴ it must be closed under inverse and ∴ it contains five powers of a.

Let m be the least five integer s.t $a^m \in H$.

T.P $b = a^m$ is generator of H.

Let $x \in H$ But $H \subseteq G_1$.

∴ $x \in G_1$

Since G_1 is a cyclic gp. with a as generator

$\therefore x = a^n$ for some $n \in \mathbb{Z}$.

By division algorithm $\exists$ integers q, r s.t

$$n = mq + r \; ; \quad 0 \le r < m$$

$$a^n = a^{mq+r}$$
$$= a^{mq} \cdot a^r$$
$$= b^q \cdot a^r \quad \{ \because a^m = b^q \}$$
$$\Rightarrow \quad a^r = b^{-q} \cdot a^n$$

Now, $a^n, b \in H$ and H is subgp.

$\therefore$, $b^{-q} a^n \in H \Rightarrow a^r \in H$.

But m was least +ve integer of a s.t $a^m \in H$ and $r < m$.

$\therefore$ we must have $r = 0$.

Hence $a^n = b^q$ for some $q \in \mathbb{Z}$

$\Rightarrow x = a^n = b^n$ ie every elt of form $x \in H$ is of form b^q for some $q \in \mathbb{Z}$.

$\therefore$ H is cyclic

$=$

Let G_1 be gp. and $g \in G_1$. Define a fn. $f: G_1 \to G_1$ by $f(x) = gxg^{-1}$. Show that g is an isomorphism of G_1 to G_1.

Solu. Given $f: G_1 \to G_1$ is fn defined by $f(x) = gxg^{-1}$ for each $x \in G_1$.

① Let $x, y \in G_1$ and Let.

$$f(xy) = g(xy)g^{-1} = g(xg^{-1}gy)g^{-1} = (gxg^{-1})(gyg^{-1}) = f(x)f(y)$$

$\therefore f$ is a homomorphism of G_1 to G_1.

② 1-1 Let $f(x) = f(y)$

$$\Rightarrow gxg^{-1} = gyg^{-1}$$
$$\Rightarrow (gxg^{-1})g = (gyg^{-1})g$$
$$\Rightarrow gx(g^{-1}g) = gy(g^{-1}g)$$
$$\Rightarrow gxe = gye$$
$$\Rightarrow gx = gy$$
$$\Rightarrow g^{-1}(gx) = g^{-1}(gy)$$
$$\Rightarrow (g^{-1}g)x = (g^{-1}g)y$$
$$\Rightarrow ex = ey$$
$$\Rightarrow x = y$$

$\therefore f$ is 1-1

③ onto:- Let $z \in G_1$ and

Let $f(g^{-1}zg) = g(g^{-1}zg)g^{-1} = (gg^{-1})z(gg^{-1}) = eze = z$

$\therefore$ for each $z \in G_1$ we have $g^{-1}zg \in G_1$ s.t $f(g^{-1}zg) = z$ $\therefore f$ is onto.

Hence $G_1 \cong G_1$

Group Isomorphism :- A homomorphism ϕ which is 1-1 and onto is called isomorphism and gp's G and G' are called Isomorphic. written as : $G \cong G'$

(*) Homomorphism which is onto → epimorphism

(*) " " " 1-1 → monomorphism.

Group Homomorphism :- A mapping f from G into G' is said to be homomorphism if

$$f(ab) = f(a)\,f(b) \quad \forall\, a, b \in G.$$

G' is said to be homomorphic image of G.

Kernel f :- If f be homomorphism of G to $\bar{G}$ then kernel f is set defined by

$$\ker f = \{ x \in G : f(x) = \bar{e} \} \text{ where } \bar{e} \in \bar{G}.$$

Image f :- The image f is set of images of elements under f.

$$\text{Img}(f) = \{ b \in G' ; f(a) = b \text{ for } a \in G \} \text{ where } f \text{ is homomorphism of } G \text{ to } G'$$

Let G_1 be a gp. and H be subgp. of G_1 then $b \in aH$ iff $aH = bH$.

(ii) If G_1 be a gp. and H be a subgp. of G_1, then $a \in Hb$ iff $Ha = Hb$.

Soln:- Since $b \in aH$ (Left coset) then $b = ah_1$ for $h_1 \in H$.

$$\Rightarrow a = bh_1^{-1}$$

Then for any $h \in H$,

$$bh = (ah_1)h = a(h_1h) \in aH$$

$$\therefore bH \subseteq aH \quad -(1)$$

Again for $h \in H$, $ah = (bh_1^{-1})h = b(h_1^{-1}h) \in bH$

$$\Rightarrow aH \subseteq bH \quad -(2)$$

from (1) & (2)

$$aH = bH.$$

Conv Let $aH = bH$.

Since $b \in bH$

$\therefore b \in aH$.

(ii) Since $a \in Hb$

$$\Rightarrow ab^{-1} \in Hbb^{-1} \quad \{\because HH = H\}$$

$$\Rightarrow ab^{-1} \in H$$

$$\Rightarrow Hab^{-1} = H$$

$$\Rightarrow Hab^{-1}b = Hb$$

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

$$\Rightarrow Ha = Hb$$

Conv, Let $Ha = Hb$.

since, $a \in Ha$

$\therefore a \in Hb$ $\{\because Ha = Hb\}$

If H and K are 2 subgp. of G, then $H \cap K$ is also subgp.

Proof:- Let H and K are 2 subgp. of G. Then $H \cap K \neq \emptyset$. Since atleast ident elt e is common to both H & K.

T.P $H \cap K$ is a subgp. It is sufficient to prove that $a, b \in H \cap K$, $b \in H \cap K$

T.P T.P.T $\Rightarrow ab^{-1} \in H \cap K$.

Let $a, b \in H \cap K$.

$a \in H \cap K \Rightarrow a \in H$ and $a \in K$.

$b \in H \cap K \Rightarrow b \in H$ and $b \in K$.

Since H is a subgp. of G and $a, b \in H$.

$\Rightarrow ab^{-1} \in H$ — (1)

Also K is a subgp. of G and $a, b \in K$.

$\Rightarrow ab^{-1} \in K$. — (2)

from (1) & (2)

$ab^{-1} \in H \cap K$.

Hence $H \cap K$ is a subgp. of G.

Abelian group :- Let us consider, an algebraic system $(G, *)$ where $*$ is a binary operation on G. Then system $(G, *)$ is said to be an abelian gp if it satisfies all properties of group plus an additional property.

(i) operation $*$ is commutative

i.e. $a * b = b * a \quad \forall a, b \in G$.

Ex :- $(\mathbb{I}, +)$

If H, K are 2 subgp's of Group G, then HK is a subgp of G iff $HK = KH$

Proof:- Let H, K are 2 subgroups of G

Let $HK = KH$

T.P HK is a subgp of G.

i.e $(HK)(HK)^{-1} = HK$

Now, $(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1})$

$= H(KK^{-1})H^{-1}$ [$\because$ K is subgp of G $\Rightarrow KK^{-1} = K$]

$= (HK)H^{-1}$ [$\because HK = KH$]

$= (KH)H^{-1}$ [$\because$ H is subgp. $\therefore HH^{-1} = H$]

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

$= KH$

$= HK$

$\therefore HK = KH \Rightarrow HK$ is subgp of G.

Conversely :- Let HK is a subgp.

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

$\Rightarrow K^{-1}H^{-1} = HK$ [$\because$ K is subgp. $\Rightarrow K^{-1} = K$ and $H^{-1} = H$]

$\Rightarrow KH = HK$

Let (G, o) be a group. Show that if (G, o) is an abelian gp, then $(a o b)^2 = a^2 o b^2 \ \forall a, b \in G$.

Soln:- Let us assume (G, o) is an abelian gp.

then $(a o b)^2 = (a o b) o (a o b)$

$= a o (b o a) o b$ [$\because$ o is comm]

$= a o (a o b) o b$

$= (a o a) o (b o b)$

$= a^2 o b^2$

Hence $(a o b)^2 = a^2 o b^2 \ \forall a, b \in G$.

Determine whether a semigp. with more than one idempotent element can be a group.

Soln:- Let $(A, *)$ be a semigp. with 2 idempotent elements a and b $(a \neq b)$.

Then

$$a * a = a \quad -(1)$$
$$b * b = b \quad -(2)$$

Let us assume that A is a group with identity element e.

Then, $a * e = a \quad -(3)$

and $b * e = b \quad -(4)$

from (1) & (3)

$a * a = a = a * e$ (Left cancellation law)

$\Rightarrow a = e$

i.e. $e = a$

from (2) and (4)

$b * b = b = b * e$ (Left can law)

$b = e$

$\Rightarrow a = e = b$ which is contradiction to $a \neq b$.

Hence, $(A, *)$ can't be gp.

Ring :- Let R be a non-empty set equipped with two binary operations addition "+" and multiplication "·". The algebraic structure $\langle R, +, \cdot \rangle$ is called a ring if the following axioms are satisfied.

I Properties of Addition :-

(i) **Closure Property :-**

$\forall\ a, b \in R \Rightarrow a+b \in R$

i.e. R is closed under addition.

(ii) **Associative Law :-**

$\forall\ a, b, c \in R,\ (a+b)+c = a+(b+c)$

(iii) **Existence of additive identity :-**

$\forall\ a \in R,\ \exists\ 0 \in R$ s.t $a+0 = a = 0+a$.

(iv) **Existence of additive inverse :-**

$\forall\ a \in R,\ \exists\ -a \in R$ s.t $a+(-a) = 0 = (-a)+a$.

(v) **Commutative Law :-**

$\forall\ a, b \in R \Rightarrow a+b = b+a$.

II Properties of Multiplication :-

(vi) **Closure Property :-**

$\forall\ a, b \in R \Rightarrow a \cdot b \in R$.

(vii) **Associative Law :-**

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

(viii) **Distributive Laws :-**

$\forall\ a, b, c \in R$

$a \cdot (b+c) = a \cdot b + a \cdot c$ {Left Distributive Law}

$(b+c) \cdot a = b \cdot a + c \cdot a$ {Right " "}

Commutative Ring :- A ring R is said to be commutative if $ab = ba \quad \forall\, a, b \in R$.

otherwise, it is called non-commutative ring.

Ring with Unity :- A ring R is said to be ring with unity if $\exists$ an elt. $1 \in R$ s.t

$$a \cdot 1 = a = 1 \cdot a \quad \forall\, a \in R$$

otherwise, it is called ring without unity.

* The unity of a ring is also called the identity element of the ring.

Prove that set $R = \{(a,b) / a, b \in R\}$ is a commutative ring under the addition and multiplication of ordered pairs defined as

$(a,b) + (c,d) = (a+c, b+d)$

$(a,b)(c,d) = (ac, bd) \; \forall \; (a,b), (c,d) \in R$.

Soln :- Given $R = \{(a,b) / a, b \in R\}$

(A) Properties of Addition :-

(i) Let $x, y \in R$ then $x = (a,b)$, $y = (c,d)$ where a, b, c, d are reals.

$\therefore x + y = (a,b) + (c,d)$

$= (a+c, b+d)$

$\in R$ $\{\because a, b, c, d \in R \Rightarrow a+c, b+d \in R\}$

$\therefore R$ is closed under addition

(ii) Associative law :- Let $x, y, z \in R$ then $x = (a,b)$, $y = (c,d)$, $z = (e,f)$ where a, b, c, d, e, f are reals.

Then,

$(x+y)+z = [(a,b) + (c,d)] + (e,f)$

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

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

$x + (y+z) = (a,b) + [(c,d) + (e,f)]$

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

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

$= [(a+c)+e, (b+d)+f]$ $\{\because a, b, c, d, e, f$ are reals and Associative Prop. holds for reals$\}$

$\therefore (x+y)+z = x+(y+z)$

$\forall x, y, z \in R$.

(iii) Existence of Identity :- For each $x = (a,b) \in R$ $\exists$ $0 = (0,0) \in R$ such that

$$x + 0 = (a,b) + (0,0)$$
$$= (a+0, b+0)$$
$$= (a,b)$$
$$= x$$

IIly, $0 + x = (0,0) + (a,b)$
$$= (0+a, 0+b)$$
$$= (a,b)$$
$$= x$$

$\therefore x + 0 = x = 0 + x$.

so, $(0,0)$ is the additive identity.

(iv) Existence of Inverse :- For each $x = (a,b) \in R$

$\exists$ $y = (-a,-b) \in R$ s.t

$$x + y = (a,b) + (-a,-b)$$
$$= [(a+(-a)), (b+(-b))] \quad \{\because a,b \in R \Rightarrow -a,-b \in R\}$$
$$= [0,0]$$
$$= 0$$

$$y + x = (-a,-b) + (a,b)$$
$$= [((-a)+a), ((-b)+b)]$$
$$= [0,0]$$
$$= 0$$

$\therefore x + y = 0 = y + x$.

$\therefore y = (-a,-b)$ is an additive inverse of $x \in R$.

(v) Commutative law :- Let $x=(a,b)$, $y=(c,d)$ $\forall x, y \in R$.

$$\begin{aligned} x+y &= (a,b)+(c,d) \\ &= (a+c,\ b+d) \\ &= (c+a,\ d+b) \\ &= (c,d)+(a,b) \\ &= y+x \end{aligned}$$

[$\because$ for a,b,c,d reals, commutative law holds]

$\therefore x+y = y+x \ \forall x, y \in R$.

6.) Properties of Multiplication

Closure Property :- Let $x, y \in R$ then $x=(a,b)$, $y=(c,d) \in R$

$$\begin{aligned} \therefore xy &= (a,b)(c,d) \\ &= (ac,\ bd) \\ &\in R \end{aligned}$$

[$\because a,b,c,d \in R \Rightarrow ac, bd \in R$]

$\therefore R$ is closed under multiplication

Associative Law :- Let $x=(a,b)$, $y=(c,d)$, $z=(e,f)$ $\forall x, y, z \in R$. where a,b,c,d,e,f are reals

$$\begin{aligned} (xy)z &= [(a,b)(c,d)](e,f) \\ &= [(ac,\ bd)](e,f) \\ &= [(ac)e,\ (bd)f] \\ &= [a(ce),\ b(df)] \\ &\in R \end{aligned}$$

[$\because (ac)e = a(ce)$ & $(bd)f = b(df)$ as Ass. Prop. under mult holds in reals.]

$$\begin{aligned} x(yz) &= (a,b)[(c,d)(e,f)] \\ &= (a,b)[(ce,\ df)] \\ &= [a(ce),\ b(df)] \\ &\in R. \end{aligned}$$

$\therefore (xy)z = x(yz)$

(C) Distributive laws :-

Let $x = (a,b)$
$y = (c,d)$
$z = (e,f)$ $\forall\ x,y,z \in R$ where a,b,c,d,e,f are reals.

$$\therefore x\cdot(y+z) = (a,b)\cdot[(c,d)+(e,f)]$$
$$= (a,b)\ [(c+e,\ d+f)]$$
$$= (a,b)\ (c+e,\ d+f)$$
$$= [a(c+e),\ b(d+f)]$$
$$= (ac+ae,\ bd+bf)$$

$$x\cdot y + x\cdot z = (a,b)\cdot(c,d) + (a,b)\cdot(e,f)$$
$$= (ac,\ bd) + (ae,\ bf)$$
$$= (ac+ae,\ bd+bf)$$

$\therefore$ $\boxed{x\cdot(y+z) = x\cdot y + x\cdot z}$ $\forall x,y,z \in R$.

Ildly, $(y+z)\cdot x = [(c,d)+(e,f)]\cdot(a,b)$
$= [(c+e,\ d+f)]\ (a,b)$
$= (c+e,\ d+f)\ (a,b)$
$= (c+e)a,\ (d+f)b$
$= (ca+ea,\ db+fb)$

$$y\cdot x + z\cdot x = (c,d)(a,b) + (e,f)(a,b)$$
$$= (ca,db) + (ea,fb)$$
$$= (ca+ea,\ db+fb)$$

$\therefore$ $\boxed{(y+z)\cdot x = y\cdot x + z\cdot x}$ $\forall x,y,z \in R$.

Hence R is a ring w.r.t given operations.

Also, $xy = (a,b)(c,d)$
$= (ac,\ bd)$ $\{\because ac = ca$ & $bd = db\}$
$= (ca,\ db)$
$= (c,d)\ (a,b) = yx$

$\therefore$ R is comm. ring under given operations.

Subring :- Let $[R, +, \cdot]$ be a ring and S be subset of R. Then S is called a Subring of R iff S is itself a ring under the operation of R.

Units :- Let $(R, +, \cdot)$ be a ring with unity. An element $a \in R$ is said to be unit if for $0 \neq a \in R$, $\exists\ b \in R$ such that $a \cdot b = 1 = b \cdot a$

or An element is a unit if a has multiplicative inverse, $\bar{a}^{-1} \in R$ s.t $a\bar{a}^{-1} = 1 = \bar{a}^{-1}a$.

Consider rings $(R, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$. Every nonzero element in R (Reals) and $\mathbb{Q}$ (Rationals) has a multiplicative inverse.

Example :- $\frac{4}{3} \in R$ has multiplicative inverse $\frac{3}{4} \in R$. since $\frac{4}{3} \cdot \frac{3}{4} = 1$.

Integral Domain :-

A Commutative ring R is called an integral Domain if ~~$\exists$ a nonzero element $b \in R$ s.t a~~ for every $0 \neq a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

, a commutative ring R is called an Integral Domain if R has no zero divisor.

Find all the zero divisors of Z_{15}.

Sol:- $Z_{15} = [0, 1, 2, \cdots 14, +_{15}, \times_{15}]$.

We know that an element m, in $[Z_n, +_n, \times_n]$ is a zero divisor iff m is not relative prime to n.

Hence $n = 15$.

The elements which are not relative prime to 15 are 3, 5, 6, 9, 10, 12.

Hence 3, 5, 6, 9, 10, 12 are zero divisors.

Also, $3 \times_{15} 5 = 0$, $9 \times_{15} 10 = 0$, $5 \times_{15} 6 = 0$, $10 \times_{15} 12 = 0$.

Ring Isomorphism:- Let $(R, +, \cdot)$ and $[R', +', \cdot']$ be 2 rings. $R \cong R'$ iff $\exists$ mapping $f: R \to R'$ s.t (i) f is 1-1 and onto

(ii) $f(a+b) = f(a) +' f(b) \quad \forall\, a, b \in R$

(iii) $f(a \cdot b) = f(a) \cdot' f(b) \quad \forall\, a, b \in R.$

Subring:- Let $[R, +, \cdot]$ be a ring and $S \subseteq R$. Then S is called subring of R iff S is itself a ring under operations of R.

- **Units**:- Let R be a commutative ring with unity element 1. An elt $a \in R$ is a unit if $\exists$ an elt $b \in R$ s.t $ab = 1$.

⊛ An elt is a unit if a has multiplicative inverse, $a^{-1} \in R$ s.t $aa^{-1} = 1 = a^{-1}a$.

Integral Domain:- A nonzero element $a \in R$ is called a zero divisor if $\exists$ a nonzero elt $b \in R$ s.t $ab = 0$.

- A commutative ring R is called an Integral domain if for every $0 \neq a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Thus, a comm. ring R is called I.D. if R has no zero divisors

Field :- Let F be a non-empty set having atleast two elements with two binary operations addition "+" and multiplication "·". The algebraic structure $\langle F, +, \cdot \rangle$ is called a field if following axioms are satisfied.

I Properties of Addition

(i) **Closure Property :-** $\forall\ a, b \in F \Rightarrow a+b \in F$
i.e F is closed under addition.

(ii) **Associative Law :-** $\forall\ a, b, c \in F$,
$(a+b)+c = a+(b+c)$

(iii) **Existence of additive identity :-** $\forall\ a \in F, \exists\ 0 \in F$ s.t $a+0 = a = 0+a$.

(iv) **Existence of additive Inverse :-** $\forall\ a \in F, \exists$ $-a \in F$ s.t $a+(-a) = 0 = (-a)+a$.

(v) **Commutative Law :-** $\forall\ a, b \in F$, we have
$a+b = b+a$.

II Properties of Multiplication

(vi) **Closure Property :-** $\forall\ a, b \in F \Rightarrow a \cdot b \in F$
i.e F is closed under multiplication.

(vii) **Associative Law :-** $\forall\ a, b, c \in F$,
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(viii) **Existence of multiplicative Identity :-**
$\forall\ a \in F, \exists\ 1 \in F$ s.t $a \cdot 1 = a = 1 \cdot a$.

(ix) **Existence of multiplicative Inverse :-**
$\forall\ 0 \neq a \in F, \exists\ b \in F$ s.t $a \cdot b = 1 = b \cdot a$

(X) Commutative law :-

$\forall\ a, b \in F,\quad a \cdot b = b \cdot a$

(XI) Distributive Laws :-

$\forall\ a, b, c \in F,$

$a \cdot (b + c) = a \cdot b + a \cdot c$

and $(b + c) \cdot a = b \cdot a + c \cdot a$