Ques:- Prove that the set of Integers is an abelian group under Addition

Sol^n Let I be the set of Integers.

$I = \{0, \pm 1, \pm 2, \ldots\}$

Abelian group → Groupoid, Semigroup, Monoid group, Group } satisfy

① Closure Property :-
The sum of two integers is always an integer. e.g.:- $a, b \in I$ then

$a + b \in I$

② Associative Property :- If $a, b, c \in I$

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

③ Identity of set I under Addition

If $a \in I$ then

$a + 0 = 0 + a = a \quad \forall\, a \in I$ & $0 \in I$

Hence, 0 is identity element

④ The inverse of a is $-a$ for

$a + (-a) = (-a) + a = 0 \quad \forall\, a \in I$

⑤ Commutative Property $a + b = b + a \quad a, b \in I$

Addition in I is always commutative.

Hence, All ⑤ Properties are satisfied then the set of Integers is an abti abelian group under addition

..... Show that the set of all integers I forms a

Ques:- Show that the identity element in a group is unique.

Proof:- Let us assume that there exists two identity elements of G i.e., e and e'.

Since, $e \in G$ and e' is an identity

We have $e'e = ee' = e$

Also, $e' \in G$ and e is an identity we have $e'e = ee' = e'$

$\therefore \quad e = e'$

Hence, identity in a group is unique.

Theorem:- Show that inverse of an element a in the group is unique.

Proof:- Let us assume that $a \in G$ be an element. Also, assume that a_1^{-1} and a_2^{-1} be two inverse elements of a.

Then we have

$$a_1^{-1} a = a a_1^{-1} = e \quad \text{and} \quad a_2^{-1} a = a a_2^{-1} = e$$

Now, $$a_1^{-1} = a_1^{-1} e = a_1^{-1} (a a_2^{-1}) = (a_1^{-1} a) a_2^{-1} = e a_2^{-1} = a_2^{-1}$$

Thus, the inverse of an element is unique.

Theorem:- Show that $(a^{-1})^{-1} = a$ for all $a \in G$ where G is a group a^{-1} is an inverse of a.

Proof:- Given that a^{-1} is an inverse of a. Then we have

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

This implies that a is also an inverse of a^{-1}.

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

Ques:- The inverse of the product of two elements of a group is the product of the inverse taken in the reverse order.

OR

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

Soln Let G be a group and also let a, b be the elements of G i.e; $a, b \in G$ then we have to prove that

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

Since $a, b \in G$, then a^{-1} and b^{-1} are the inverse of a and b.

$$\therefore \quad a a^{-1} = e = a^{-1} a \quad \& \quad \text{—— (1)}$$

$$b b^{-1} = e \quad b^{-1} b \quad \text{—— (2)}$$

e is the identity element.

Now Consider

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

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

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

$$= e \quad \text{— (3)}$$

Similarly $(b^{-1} a^{-1})(ab) = b^{-1} [a^{-1} (ab)]$

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

$$= b^{-1} [e b]$$

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

$$= e \quad \text{— (4)}$$

from (3) & (4), we have

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

Ques:- Show that the set of all integers I forms a group w.r.t the binary operation '*' defined by the rule $a*b = a+b+1 \quad \forall\ a,b \in I$.
Determine (I, *) is a group.

Sol^n The algebraic structure (I, *) forms a group, if it satisfies the following properties:-

$a*b$ →
- Closure Property
- Associative
- Existence of Identity
- Existence of inverse

} satisfies ↓ Group.

① **Closure Property:-** If $a,b \in I$, then $a \in I, b \in I \Rightarrow$

$a+b+1 \in I$

② **Associativity:-** If $a,b,c \in I$, then

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

L.H.S $(a*b)*c = (a+b+1)*c = a+b+1+c+1$

$= a+b+c+2$

R.H.S $a*(b*c) = a*(b+c+1) = a+b+c+1+1$

$= a+b+c+2$

L.H.S = R.H.S

③ **Existence of Identity:-** An element $e \in I$ will be the identity, if $e*a = a*e = a \quad \forall\ a \in I$

$e*a = e+a+1$

$\therefore\ e+a+1 = a \Rightarrow e = -1$

Since $-1 \in I$, hence identity element is -1

④ **Existence of Inverse:-** If $a \in I$ and b is the inverse of a then by definition, we have

$a*b = b*a = e = -1$

i.e; $a+b+1 = -1 \Rightarrow b = -2-a$

Since $a \in I$, $-2 \in I$, hence $(-2-a) \in I$

$\therefore (-2,-a)$ is the inverse group $(I, *)$

Since, the algebraic system $(I, *)$ satisfy all the properties of a group. Hence $(I, *)$ is a group.

Ques: Show that the set of matrices

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

where α is the real number, form a group under matrix multiplication

Sol^n Let G be the set of matrices A_α, where

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}, \alpha \in R$$, then G formed a group if

① **Closure Property:-** Let $A_\alpha, A_\beta \in G$, then

$$A_\alpha \cdot A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \cdot \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta} \in G$$

Hence, Closure Property satisfied.

② **Associativity Property:-** We know that for all 2×2 matrix, multiplication satisfies associative law.

③ **Existence of Identity:-** Since $0 \in R$, hence, therefore

$$A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = G$$

Now $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the unit matrix of order 2,

$\therefore A_0 A_\alpha = A_\alpha A_0 = A_\alpha \quad \forall \quad A_\alpha \in G$

$\therefore A_0$ is the identity element of G

④ Existence of Inverse:-

Let $A_\alpha \in G$. Then

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}, \alpha \in R$$

$$\therefore |A_\alpha| = \cos^2\alpha + \sin^2\alpha = 1 \neq 0$$

$\therefore$ The matrix is non-singular and so its inverse exist. Now we have

$$\text{Adj } |A_\alpha| = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

$$\therefore A_\alpha^{-1} = \frac{\text{Adj } A}{|A_\alpha|} = \begin{bmatrix} \cos\alpha & +\sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \in G$$

Hence each element of G has inverse.

$\therefore$ It forms a group under matrix multiplication.

Qus:- Show that the set of cube roots of unity is an abelian group w.r.t the multiplication.

OR

Show that the set $\{1, \omega, \omega^2\}$ forms an abelian group under multiplication, where $\omega^3 = 1$

Soln The given set $G = \{1, \omega, \omega^2\}$ and binary operation is multiplication. Now we form a composition table as:

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

① Closure Property :- Since all entries in the composition table are the elements of G, thus G is closed under multiplication.

② Associativity :- Since the elements of G are all complex number and we know that multiplication of complex number is associative because

$(1 * \omega) * \omega^2 = 1 \cdot (\omega \cdot \omega^2)$ etc.

③ Existence of Identity :- from the composition table, we see that $1 * 1 = 1$, $1(\omega) = \omega$, $1 * (\omega^2) = \omega^2$

$\therefore$ 1 is the identity element of G.

④ Existence of inverse :- from the Composition Table, we find that

$1 * 1 = 1$ identity)

$\omega * \omega^2 = \omega^2 * \omega = 1$

$\omega^2 * \omega = 1$

Hence Existence of inverse is also preserved

⑤ Commutative $1 * \omega = \omega * 1 = \omega$

Hence, it follows the rule of commutative law, hence G is an abelian group.

Ques: Let $A = \{a, b, c, d\}$ be a group under operation $*$ defined in the table given below. Find identity element of the group and find the inverse of each element in the group.

*	a	b	c	d
a	(c)	d	a	b
b	d	a	b	(c)
c	a	b	(c)	d → same as Row
d	b	(c)	d	a → same as Column

Soln

① Identity Element → Unique in a group.

② Inverse " → Inverse of each element in a group exist.

element * Identity = element (it self)

$x * e$ (Identitity) $= x$

$a * c = a$

c → Identity element → (Unique)

Exist in each Row

Inverse

I^st Row → Inverse of a is a

" " b is d

" " c is c

" " d is b

Ques: Find the identity and inverse element in given table for each element

*	a	b	c	d
a				
b				
c				
d				

*	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	d	c	b	a
d	b	d	a	c

Sol^n

*	a	b	c	d
a	c	a	d	(b)
b	a	(b)	c	d
c	d	c	(b)	a
d	(b)	d	a	c

→ same as Row

↓ same as Column.

Rest find yourself

Que:- If $a * b = a+b+ab$ where $a, b \in R$ find identity and inverse element.

Sol^n ① $a * e = a$

$a + e + ae = a$

$e(1+a) = 0 \Rightarrow \boxed{e = 0}$ → identity element

② Inverse Let $y = a^{-1} \Rightarrow \therefore a * y = 0$

$a * y \Rightarrow a + y + ay = 0$

$y(1+a) = -a$

$y = \frac{-a}{1+a}$

↓

$a^{-1} = \frac{-a}{1+a}$, $a \neq -1$

Ques:- Prove that if G is an abelian group, then
$(ab)^n = a^n b^n \quad \forall\ a, b \in G$ & $\forall\ n \in I$.

Sol^n Since n is being an integer, it can assume that +ve values, -ve values and also the zero values, therefore.

(i) Let $n = 0$, then by definition of identity element

$a^0 = e = b^0 = (ab)^0 = e$ and $a^0\, b^0 = e \cdot e = e$

$\therefore (ab)^0 = e = a^0 \cdot b^0 = e$ or

$(ab)^n = a^n b^n$ if $n = 0$

(ii) Let $n > 0$, if $n = 1$ then

$(ab)^1 = ab = a^1 \cdot b^1 = ab$

$\therefore (ab)^n = a^n b^n$ if $n = 1$

Let us suppose that it is true for $n = k$ i.e

$(ab)^k = a^k b^k$

Now $(ab)^{k+1} = (ab)^k (ab)$

$= (a^k b^k)(ab)$

$= a^k (b^k ab)$ by associative law

$= a^k (a\, b^k) b$ since G is abelian

$\therefore b^k a = a\, b^k$

$= (a^k \cdot a)(b^k \cdot b)$

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

$\therefore$ The given statement is true for $n = k+1$ if it is true for $n = k$

$\therefore$ By mathematical induction the statement is true for every positive value of n

(iii) Let $n < 0$, let $n = -m$ then

$$(ab)^n = (ab)^{-m} = [(ab)^m]^{-1}$$
$$= (a^m b^m)^{-1}$$
$$= (b^m a^m)^{-1} \quad (\text{since } G \text{ is abelian} \therefore a^m b^m = b^m a^m)$$
$$= (a^m)^{-1} (b^m)^{-1}$$
$$= a^{-m} b^{-m} \Rightarrow a^n b^n$$

$\therefore$ from (i), (ii) & (iii), we have

$(ab)^n = a^n b^n \quad \forall\ a, b \in G$ & $\forall\ n \in I$

Proved.

Ques:- Prove that if every element of a group G is its own inverse, then G is an abelian group.

Sol^n Let a and b be any two element of G, then ab is also an element of group G

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

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

$\Rightarrow b*a = a*b \quad (\because b^{-1} = b \text{ & } a^{-1} = a)$

$\Rightarrow G$ is an abelian

Hence Proved

Ques:- Show that the set $\{1, -1, i, -i\}$ forms an abelian group w.r.t multiplication.

Soln The Composition table under multiplication is

*	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 elements of G is also an element of Composition table, hence G is closed under closure Property.

② Associativity Property:- $a = 1, b = i, c = -i$

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

L.H.S $(a * b) * c$

$= (1 * i) * (-i)$

$= +1$

R.H.S $a * (b * c)$

$= 1 * (i * -i)$

$= 1 * 1$

$= 1$

L.H.S = R.H.S

Hence, it satisfies associativity Property.

③ Existence of Identity :- From compesition table we see that $1 * G$ such that

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

$1 * (i) = i$

④ Inverse:- $1 * a = 1 \Rightarrow a = 1$

$-1 * b = 1 \Rightarrow b = -1$

$i * c = 1 \Rightarrow c = -i$

$-i * d = 1 \Rightarrow d = i$

∴ inverse of i is 1, -1 is 1, i is $-i$ and $-i$ is i

(3) Commutative:- It is also satisfies the Commutative Property. Hence G is

Hence, G is abelian group.

Ques:- Show that the four matrices $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$ form a finite abelian group.

Sol^n Let $A = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, B = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, C = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ and $D = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$

Let G be a group and all these are the elements of G i.e; $G = \{A, B, C, D\}$, then

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

$$B * B = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}+1 & 0\\ 0 & 1\end{bmatrix} = BA$$

Illy $C \cdot C = D \cdot D = A$ and

$$A * B = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}-1+0 & 0+0\\ 0+0 & 0+1\end{bmatrix} = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = B$$

And $A \cdot C = C$, $A \cdot D = D$.

The Composition table is given as

*	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

① Closure Property:- Since all the entries in the composition table are the elements G, Hence G is closed.

② Associativity:- Let $A, B, C \in G$, then

$$(A * B) * C = B * C = D$$

and $$A * (B * C) = A * D = D$$

Hence $$(A * B) * C = A * (B * C$$

③ Identity:- From the composition table, we find that the row headed by element A just coincides with the top of the row of the composition table, hence matrix A is the identity element.

④ Inverse:- From the composition table, it is clear that

$$A^{-1} = A, \quad B^{-1} = B, \quad C^{-1} = C \quad \& \quad D^{-1} = D$$

This shows that in multiplication, every element is its own inverse.

⑤ Commutative:- From composition table we see that if $A, B \in G$ then $A * B = B * A = A$

Hence, it satisfies the commutative law.

∴ The given group is an abelian group.

SUBGROUPS:-

A non-empty subsets H of a group G, is said to be a subgroup of G, if the composition of G is also a composition in H, then H is itself a group.

example The multiplicative group $\{1,-1\}$ is a subgroup of the multiplicative group $\{1,-1,i,-i\}$

Theorem:-①

A non-empty subset H of a group G is a subgroup of G if and only if

(i) $a \in H$, $b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$, where a^{-1} is the inverse of a in G.

Proof:- Let H is a subgroup of G, then H itself is a group w.r.t multiplication i.e; H must be closed w.r.t multiplication

$\therefore a \in H, b \in H \Rightarrow ab \in H$

Let $a \in H$ and a^{-1} is the inverse of a in G since H itself is a group then $a^{-1} \in H$

$\therefore a \in H \Rightarrow a^{-1} \in H$.

Conversely

Let $a,b \in H \Rightarrow a,b \in H$ & $a \in H \Rightarrow a^{-1} \in H$, then we have to show that H is a group w.r.t multiplication

(a) **Closure:-** Given condition $a \in H, b \in H \Rightarrow ab \in H$

$\therefore$ closure property satisfied.

(b) **Associativity:-** The elements of H are also the elements of G and G is associative.

$\therefore$ H is must be associative.

(c) Identity:- Since $a \in H \Rightarrow a^{-1} \in H$

further $a \in H, a^{-1} \in H \Rightarrow a a^{-1} \in H$

$\therefore e$ is the identity element of H

(d) Inverse:- Since $a \in H \Rightarrow a^{-1} \in H$

$\therefore$ each element of H possesses inverse.

Since H itself is a group for the composition in G.

$\therefore H$ is a subgroup of G.

Theorem (2) If H is any subgroup of G then $H^{-1} = H$

Proof:- Let $h^{-1} \in H^{-1}$ then $h \in H$

$\therefore H^{-1} \subseteq H$ ——— (1)

Again $h \in H \Rightarrow h^{-1} \in H$

$\therefore H \subseteq H^{-1}$ ——— (2)

from (1) & (2) we have

$H = H^{-1}$

Proved.

Theorem (3):- A Necessary and sufficient condition for a non-empty subset of H of a group G to be a subgroup is that $a \in H, b \in H \Rightarrow a b^{-1} \in H$

Proof:- Let H be a subgroup of G and we have to prove that $a \in H, b \in H \Rightarrow ab^{-1} \in H$

Let $a \in H, b \in H$

Since H is a subgroup, $\therefore$ each element of H must possesses inverse

$\therefore b \in H \Rightarrow b^{-1} \in H$

Also H must be closed w.r.t multiplication

$\therefore a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$

Now let us suppose that

$a \in H, b \in H \Rightarrow ab^{-1} \in H$ and we have to prove that H is a subgroup of G. with composition multiplication

(a) Closure:- Since $b \in H \Rightarrow b^{-1} \in H$

so $a \in H, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H$

$\Rightarrow ab \in H$

(b) Associativity:- The elements of H is also elements of G and G is associative.

Hence, H is also associative.

(c) Identity:- $a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H$

$\Rightarrow e \in H$

$\therefore$ e is the identity element of H.

(d) Inverse:- $e \in H, a^{-1} \in H \Rightarrow ea^{-1} \in H$

$a^{-1} \in H$

$\therefore$ each element of H possesses inverse

$\therefore$ H is a subgroup of G.

Theorem (4):- If H and K are two subgroup of a group G, then HK is a subgroup of G if and only if $HK = KH$.

Proof:- Since H and K are two subgroup of a group G then $H^{-1} = H$ and $K^{-1} = K$

Now let HK is a subgroup, then

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

$K^{-1}H^{-1} = HK$

$KH = HK \quad (\because H^{-1} = H \text{ & } K^{-1} = K$

Conversely Let $HK = KH$, then we have to prove that HK is a subgroup of G, it is sufficient to prove that $HK(HK)^{-1} = HK$

L.H.S $= (HK)(HK)^{-1}$

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

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

$= HKH^{-1}$ (Since K is subgroup $\Rightarrow KK^{-1} = K$)

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

$= KH$ (Since H is subgroup $\Rightarrow HH^{-1} = H$)

$= HK$ ($\because KH = HK$)

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

L.H.S = R.H.S

H.P

Ques:- Let $(I, +)$ be a group, where I is the set of all integers and $(+)$ is an addition operation. Determine whether the following subsets of G are subgroup of G?

(a) The set G_1 of all odd integers,

(b) The set G_2 of all ~~positive~~ even integers,

Sol^n

(a) The set G_1 of all integers is not a subgroup of G. it does not satisfy the closure property. Since, addition of two odd integers is always even.

(b) (i) Closure Property:- The set G_2 is closed under the operation $+$, Since addition of two even integers is always even.

(ii) Associative Property:- The operation $+$ is associative since

$(a+b)+c = a+(b+c) \quad \forall\ a, b, c \in G_2$

(III) Identity The element 0 is the identity element.
Hence, $0 \in G_2$

(IV) Inverse :- The inverse of every element $a \in G_2$ is $-a \in G_2$. Hence, the inverse of every element exists.
Since the system $(G_2, +)$ satisfy all the conditions of a subgroup. Hence, $(G_2, +)$ is a subgroup.

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

(V) The operation $*$ is commutative i.e;

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

e.g:- Consider an algebraic system $(I, +)$, where I is the set of all integers and $+$ is an addition operation. The system $(I, +)$ is an abelian group because it satisfies all the properties of an group also the operation $+$ is Commutative for every $a, b \in I$.

Order of an element of Group:-

Let G be a multiplicative group and $a \in G$ is any element of G then a non-negative smallest integer 'n' is said to be order of element 'a' if

$a^n = e = 1$ (where e is the identity element of multiplication group G)

$a^n = e = 0$ (where e is the identity element of Addition group G)

e.g:- Let $G = \{1, \omega, \omega^2\}$ order of one

$1^1 = 1 \Rightarrow O(1) = 1$

$(\omega)^3 = 1 \Rightarrow O(\omega) = 3$

$(\omega^2)^3 = 1 \Rightarrow O(\omega^2) = 3$

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

$1^1 = 1 \Rightarrow O(1) = 1$

$(-1)^2 = 1 \Rightarrow O(-1) = 2$

$(i)^4 = 1 \Rightarrow O(i) = 4$

$(-i)^4 = 1 \Rightarrow O(-i) = 4$

Addition Modulo m :-

It is a new type of addition known as "addition modulo m" and it is written as

$a +_m b = r$ (non-negative integer. r → remainder.)

a, b → Integer

$0 \leq r \leq m$

where r is the least non-negative remainder, when (a+b) is divided by m

e.g:- ① $7 +_3 3 = \frac{10}{3} \Rightarrow 3(3) + (1)$ → remainder

② $8 +_3 11 = \frac{19}{3} \Rightarrow 3(6) + (1)$ → "

③ $8 +_3 10 = \frac{18}{3} \Rightarrow 3(6) + (0)$ → remainder

④ $-23 +_3 3 = 1 \Rightarrow -23 + 3 = 1$

Because $-23 + 3 = -20$

Now $-20 = -3 \times 7 + 1$ i.e; remainder is 1

Multiplication Modulo m :-

It is a new type of multiplication known as "multiplication modulo m" and it is written as

$$a \times_m b = r \qquad 0 \le r < m$$

where a & b are any integers bw m is a fixed +ve integer and r is least non-negative remainder when (a×b) is divided by m.

e.g:- ① $8 \times_5 3 = 4$ (because 24/5 then least non negative integer less than 5 is 4)

② $8 \times_5 4 = 2$ (because 32/5 then we get the least non-negative integer 2 which is <5

③ $7 \times_8 5 =$

④ $11 \times_5 4 =$

Ques:- Prove that the set $G = \{0,1,2,3,4,5\}$ is a finite abelian group of order 6 with respect to addition modulo 6.

Sol^n Give that $G = \{0,1,2,3,4,5\}$

Let us construct the composition table of addition modulo 6 as:-

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

① Closure Property:- Since all the entries in the Composition table are the elements of the set G. Hence G is closed under addition modulo 6

② Associativity:- Let $a, b, c \in G$ then

$$a +_6 (b +_6 c) = (a +_6 b) +_6 c$$

Let $a = 1, b = 2, c = 3 \in G$ then

① $1 +_6 (2 +_6 3) = 1 +_6 (5) = 0$

② $(1 +_6 2) +_6 3 = 3 +_6 3 = 6$

③ Identity :- Since $0 \in G$ then $a +_6 0 = a \ \forall \ a \in G$

$\therefore$ 0 is the identity element of G

④ Commutative:- Inverse:- From composition table, we see that the inverse of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively

⑤ Commutative Let $a, b \in G$, then $a +_6 b = b +_6 a \ \forall \ a, b \in G$. Let $a = 1$ & $b = 4$, then

$a +_6 b = 1 +_6 4 = 5$

and $b +_6 a = 4 +_6 1 = 5$

Hence it is commutative.

$\therefore$ G is an abelian group under addition modulo 6

Ques:- Prove that the set $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group of order 6 w.r.t multiplication modulo 7.

Sol^n Given that

$G = \{1, 2, 3, 4, 5, 6\}$ the binary operation is multiplication modulo 7.

Let us consider the composition table multiplication modulo 7 as :-

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Closure Property:- Since all entries in the composition table are the elements of G, hence G is closed

Associativity :- Let $a, b, c \in G$, then

$$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c$$

Let $a = 2$, $b = 3$ & $c = 5$ then

$$2 \times_7 (3 \times_7 5) = 2 \times_7 1 = 2$$

$$(2 *_7 3) \times_7 5 = 6 \times_7 5 = 2$$

$\therefore$ Associative law holds.

Identity :- Since $1 \in G$ & $1 \times_7 a = a \quad \forall \ a \in G$

Hence 1 is the identity elements of G.

Inverse :- From composition table we see that the inverse of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3, 6 respectively.

Commutative :- Let $a, b \in G$ then $a *_7 b = b *_7 a \quad \forall \ a, b \in G$

$$2 *_7 5 = 5 *_7 2$$

L.H.S $2 \times_7 5 = 3$ & R.H.S $= 5 \times_7 2 = 3$

hence it is commutative.

$\therefore$ G is an abelian group.

Cyclic Group:- A group $(G, *)$ is called cyclic, if for $a \in G$, every element $x \in G$ of the form a^n, where n is some integer. Symbolically it is written as:-

$$G = \{a^n / n \in I\}$$

Note:-

① The element a is called a generator of G

② It may be more than one generator of cyclic group.

③ If G is a cyclic group generated by a then we write $G = \{a\}$.

Ques:- The multiplication group $G = \{1, -i, i, -1\}$ is cyclic.

Sol^n:- The given group $G = \{1, -1, i, -i\}$ can be written as:-

$$G = \{i, i^2, i^3, i^4\}$$

Hence G is a cyclic group and the generator of this group is i

Note:- Also G can be written as:-

$$G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$$

Here the generator of G is $-i$ and it is also a cyclic group.

Ques:- The multiplication group of cube root of unity i.e; $\{1, \omega, \omega^2\}$ is a cyclic group of order 3. Find its all generator when $\omega^3 = 1$

Ques: Prove that every cyclic group is an abelian group.

Sol^n Let $G = \{a\}$ be a cyclic group, generated by a.
Let $x, y \in G$, then there exist integers r and s s.t

$$x = a^r \quad , \quad y = a^s .$$

$$\therefore xy = a^r \cdot a^s = a^{r+s}$$

$$= a^{s+r} = a^s \cdot a^r$$

$$\therefore xy = yx \quad \forall \; x, y \in G .$$

Hence G is an abelian group.

Ques: If a is a generator of a cyclic group G, then a^{-1} also a generator of G.

Sol^n Let $G = \{a\}$ be a cyclic group, generator rated by a and a^r be an element of G, then we can write $a^r = (a^{-1})^{-r}$

Since r is an integer.

$\therefore$ Every element of G is generated by a^{-1}

$\therefore$ a^{-1} is also generated by G

Cosets:-

Let G be a group, on which the group operation is multiplication and H be a subgroup of G.

Let $a \in G$ then, the set

$Ha = \{ha : h \in H\}$ → Right coset of H in G generated by a

$aH = \{ah : h \in H\}$ → Left coset of H in G generated by a

Note:-

① If group operation is addition, then the

$H+a = \{h+a : h \in H\}$ – Right coset of H in G generated by a

$a+H = \{a+h : h \in H\}$ → left coset of H in G generated by a

② If e is the identity of G, then

$He = eH = H$

③ $e \in H \Rightarrow ae \in Ha \Rightarrow a \in Ha$

Ques:- If G is an additive group of all integers and H is additive subgroup of all even integers of G, then find all the cosets of H in G.

Soln Given

$G = \{0, \pm1, \pm2, \pm3, ----\}$

$H = \{0, \pm2, \pm4, \pm6, ---\}$

Let $0, 1, 2, ---- \in G$ then

$H+0 = \{0, \pm2, \pm4, \pm6, ---\} = H$

$H+1 = \{0+1, \pm2+1, \pm4+1, \pm6+1 ---\}$

$= \{1, \pm3, -1, 5, -3, ---\}$

$H+2 = \{0+2, \pm 2+2, \pm 4+2, \ldots\}$

$= \{2, 4, 0, 6, -2 \ldots\} = H$

These are the cosets of H in G.

Theorem: If H is any subgroup of G and $h \in H$, then

$Hh = H = hH$.

Proof: Let $h \in H \subseteq G$, then we have to show that

$Hh = H$ and $hH = H$

Let us suppose that h be an arbitrary elements of H, then $h'h \in Hh$. Since H is subgroup of G.

$\therefore h' \in H, \quad h \in H \Rightarrow h'h \in H$

$\therefore h'h \in Hh \Rightarrow h'h \in H$

$\therefore h'h \in H$ & $h'h \in Hh \Rightarrow Hh \in H$ — (1)

Again $h' = h'e = h'(h^{-1}h)$ $[\because h^{-1}h = e, \; eh' = h']$

$= (h'h^{-1})h \in Hh$

Hence $h' \in H, h \in H \Rightarrow h'h^{-1} \in H \subseteq H$ is subgroup.

$\therefore h' \in H \Rightarrow h' \in Hh$

$\Rightarrow H \subseteq Hh$ — (2)

From (1) & (2) we get

$Hh = H$

Why, we can find $hH = H$

Hence $Hh = H = hH$

H.P

Theorem 2 If a & b are any two elements of a group G and H is a subgroup of G, then prove that

$$Ha = Hb \iff ab^{-1} \in H \text{ and } aH = bH \iff b^{-1}a \in H$$

Proof:

H is a subgroup of G and $a, b \in G$ s.t

$$Ha = Hb$$

If e be the identity element then

$$e \in H \Rightarrow ea \in Ha \Rightarrow a \in Ha$$

But $Ha = Hb \Rightarrow a \in Hb$

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

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

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

Conversely – let H is a subgroup of G, $a, b \in H$ s.t $ab^{-1} \in H$, then to show that $Ha = Hb$

as $ab^{-1} \in H \Rightarrow H(ab)^{-1} = H$

$$\Rightarrow H(ab)^{-1} = Hb$$

$$\Rightarrow Hae = Hb$$

$$\Rightarrow Ha = Hb$$

$$\therefore Ha = Hb \iff ab^{-1} \in H$$

and $aH = bH \iff b^{-1}a \in H$

H.P

Permutation and Symmetric Group :-

Let S be finite set consisting n elements, then the set of all one - one on to mapping from S to S form a group w.r.t composition of mapping. This group is called Permutation Group or symmetric group of n symbols of degree n and is denoted by S_n

If $S = \{a_1, a_2, \dots, a_n\}$, then we can write an element $f \in S_n$ as :-

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ f(a_1) & f(a_2) & f(a_3) & & f(a_n) \end{pmatrix}$$

where $f(a_1), f(a_2), \dots, f(a_n)$ are the pre-image of $a_1, a_2, \dots a_n$ resp. , So its permutation of n - symbols

Permutation :- A one - one mapping of a finite set S onto itself is called permutation.

Note :- ① The no. elements in a finite set S is known as the degree of permutation. It is denoted by

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}$$

Equal Permutation :- Let f and g are two permutations and S be a non - empty finite set then f and g are equal if

$$f(a) = g(a) \quad \forall \ a \in S$$

e.g. Let $S = \{1, 2, 3, 4\}$ and Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

$$g = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

then $f(1) = g(1) = 3$

$f(2) = g(2) = 1$ i.e; $f(a) = g(a)\ \forall\ a \in S$

$f(3) = g(3) = 2$ hence $f = g$

$f(4) = g(4) = 4$

Note: ① If there are n elements in a set S, then the total no. of permutation is $n!$ or $\lfloor n$.

e.g: Let $S = \{1, 2, 3\}$ then the total no. of permutation $= 3! = 6$ and it is given as

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

Identity Permutation:

Let S be a finite non-empty set an identity permutation on S denoted by I and is defined by:- $I(a) = a\ \forall\ a \in S$ is called identity permutation

e.g: Let ~~$S = \{1, 2, 3, 4\}$~~ $S = \{1\ \ 2\ \ 3\ \ 4\}$ then

$$S_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$ is the identity permutation

Product of or Composition of Permutations :-

Let $S = \{a_1, a_2, a_3, \ldots\ldots a_n\}$ and Let

$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ f(a_1) & f(a_2) & f(a_3) & & f(a_n) \end{pmatrix}$ & $g = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ g(a_1) & g(a_2) & g(a_3) & \cdots & g(a_n) \end{pmatrix}$

be two arbitrary permutations on S. Then the product or Composition of f and g is denoted by fg or $f \circ g$ and defined as

$$fog = fg = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(a_1) & g(a_2) & \cdots & g(a_n) \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(g(a_1)) & f(g(a_2)) & & f(g(a_n)) \end{pmatrix}$$

Note: ① Generally $fog \neq gof$

Ques: Let $S = \{1, 2, 3\}$ and

$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

be two permutations on S, then find fog & gof

Sol^n $fog = fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$gof = gf = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Here $fog \neq gof$

Inverse of Permutation :- Let f be a permutation on $S = \{a_1, a_2, \cdots a_n\}$ s.t

$$f = \begin{pmatrix} a_1 & a_2 & a_n \\ b_1 & b_2 & b_n \end{pmatrix}$$

then there exist a permutation called inverse of f denoted by f^{-1} s.t

$$fof^{-1} = f^{-1}of = I \text{ where}$$

$$f^{-1} = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Ques! If $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$,

$B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$ then find AB, BA

and A^{-1}

Soln

$$AB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$BA = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$AB \neq BA$

Now A^{-1}

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}^{-1} \Rightarrow \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Cyclic Permutation:-

Let $S = \{a_1, a_2, \ldots a_n\}$ be a finite set of n symbols. A permutation f defined on S is said to be cyclic permutation if it is defined as :-

$f(a_1) = a_2$, $f(a_2) = a_3$, $\ldots$ $f(a_{n-1}) = a_n$, $f(a_n) = a_1$.

e.g: Let $S = \{1, 2, 3, 4\}$ and

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$ is cyclic permutation.

Note: Cyclic permutation written as $f(1\,2\,3\,4)$.

Transposition:-

A cycle of length 2 is called transposition

① Let $S = \{a_1, a_2, \ldots a_n\}$, f, g, h be cyclic permutation on S. Then

(a) $(fog)^{-1} = g^{-1} o f^{-1}$ (b) $(fogoh)^{-1} = h^{-1} o g^{-1} o f^{-1}$

② In S_n is a perm permutation in S_n a $\frac{n!}{2}$ are of n symbols then, if $n!$ permutation in S_n, $\frac{n!}{2}$ are even permutation & $\frac{n!}{2}$ are odd permutations

③ The set of all even permutation degree n form a group under the composition of permutations.

④ The group of even permutation is called Alternating group.

Even And Odd Permutation :-

A permutation f is said to be an even permutation if f can be expressed as the product of even no.'s of transpositions otherwise it is called odd permutations.

① An identity permutation is consider as an even permutation.

② A transposition is always odd.

③ The product of two even permutation is even and the product of two odd permutation is also even.

④ The product of an even and odd permutation is odd.

Disjoint Cycles :-

Let $S = \{a_1, a_2, ----, a_n\}$. If f and g are two cycles on S, s.t they have no common elements then f and g are said to be disjoint cycles

e.g! Let $S = \{1,2,3,4,5,6\}$ if $f = \{1,4,5\}$ & $g = \{2,3,6\}$ Then f and g are disjoint cycles permut-ation on S.

Ques! Let $f = (1\ 2\ 3)$ and $g\ (4\ 5)$ be two permutations on 5 symbols 1,2,3,4,5 then

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Also find gf and we see that $fg = gf$