Groups :-

Introduction

A set of objects with mathematical operation ⊛ operation defined on it and the properties associated with it form an form an "algebraic systems".

Mathematical operations

Mathematical operations such as addition and multiplication of numbers. union and intersection of sets, as well as composition of functions.

ie) $a+b=C$

$a \cdot b = C$ $\quad A \cap B = C$ etc.

$A \cup B = C$

Deffinition :-

An operation, f on a set A is a function of the cartesian product $A \times A$ into A, that is $f: A \times A \to A$, such that each element $f(a,b) \in A$ is associated with each ordered pair $(a,b) \in A \times A$.

Binary operations :-

An operation that specifies the way in which two objects are combined to yield a third object belonging to the same collection of objects is called a binary operation.

Definition :- Let A be a non-empty set. Then $A \times A = \{(a,b) : a \in A, b \in A\}$. If $f : A \times A \to A$, then f is said to ~~the same collection of objects is called a binary operation~~. be a binary operation on the set A.

A binary operation obviously must satisfy following conditions!

(i) It must be defined for each ordered pair of elements of A.

(ii) only one element of A is assigned to each ordered pair of its elements

Properties of Binary operations

Commutative. A binary operation $*$ on a set A is said to be commutative if for every $a, b \in A$

$$a * b = b * a$$

For example:

(i) Addition and mutiplication of real numbers are commutative operations.

ie) $a+b = b+a$ and $a \cdot b = b \cdot a$

(ii) The union and intersection in the power set of a set are both commutative. i.e)

$$A \cup B = B \cup A \text{ and } A \cap B = B \cap A$$

Associative: A binary operation $*$ on a set A is said to be associate if for every $a, b, c \in A$.

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

For example:-

(i) Addition and multiplication of real number are associative operations.

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

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

Identity element:- The set A is said to have an identity element for the operation $*$ on itself if there exists an element $e \in A$ such that.

$$e * a = a = a * e, \quad \forall \ a \in A.$$

Inverse element: let there exists an identity element e in the set A for the operation $*$. if

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

then a is called the inverse of the element a and vice versa.

Distributive law :-

If $+$ and $*$ are two operations defined on the set A such that

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

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

Groups :-

A group is the mathematical structure consisting of a set together with binary operation defined on it such that the elements of the given set have some relationships among themselves.

Definition :- Let G be a non-empty set together with a binary operation $*$ defined on it. Then the algebraic structure $(G, *)$ is said to be a group, if the binary operation satisfies the following properties.

1. Closure property

$a, b \in G \Rightarrow (a * b) \in G$

2. Associative property

(For any 3 elements $a, b, c \in G$)

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

3. Existence of identity.

$a * e = a = e * a \quad \forall \; a \in G$.

4. Existence of inverse

(For each element $a \in G$, there exists an element $b \in G$ such that)

$b * a = e = a * b$

(Here b is called an inverse of a and is denoted by $b = a^{-1}$. Thus $a^{-1} \in G$ such that

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

Abelian (or commutative) Group

A group G is said to be an abelian group if in addition to the above 4 properties the following property is also satisfied.

5.] commutative property

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

NOTE: commutative property is not the necessary property for G being a group.

Finite and Infinite Groups

A group $(G, *)$ is called a finite group if the set G contains a finite number of distinct elements, otherwise an infinite group.

The number of elements in a finite group is called the order of the group and is denoted by $|G|$.

Definition (Semi group):- A system $(G, *)$ where G is a non-empty set and $*$ is a binary operation on G, is called a semi group if it satisfies the following axiom.

(i) Associative law: $a*(b*c) = (a*b)*c$

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

Definition (order of a group):-

The number of elements in a group G is called the order of the group and denoted by $O(G)$.

Problem - 1

(1) Show that the set of integers is a group under the operation of addition.

∴ **Soln:** (i) closure property

Since sum of 2 integers is an integer,

∴ I is closed with respect to addition.

(ii) Associative property.

If a, b, c are any arbitrary elemats in I, then

$(a+b)+c = a+(b+c)$ is true.

iii) Existence of identity.

The number $0 \in I$, such that

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

Thus the integer 0 is the additive identity.

iv) Existence of inverse.

If $a \in I$, then $-a \in I$ such that

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

Thus every element in I has its additive inverse.

∴ I is a group with respect to addition.

Again, it is noted that addition of integers is commutative.

ie) $a+b = b+a$, $\forall\ a, b \in I$

Hence $(I, +)$ is an abelian group of infinite order.

Show that the set I of all integers is abelian group under usual addition.

2] Show that the set, N of natural numbers is not a group under the operation of addition.

Soln: In the set of natural numbers there exists no natural number 'e' called the additive Identity such that $a+e = a = e+a$, $\forall\ a \in N$

Hence $(N, +)$ is not a group.

3] Show that the set, $G\{1, \omega, \omega^2\}$ where $1, \omega, \omega^2$ are cube roots of unity, form an abelian group under the operation of ordinary multiplication.

(08) Cube

Show that roots of unity is abelian group.

Soln:- We prepare a composition table as follows

$\omega = \frac{-1+i\sqrt{3}}{2}$

$\omega^2 = 1/\omega$

$\omega^3 = 1$

x	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

The following properties can be verified from the composition table.

(i) closure property.

Since all the entries in the composition table are also elements of the set G.

∴ it is closed for multiplication

(ii) Associative property.

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

ordinary multication is always associative.

(iii) Identity element

From the above table.

$1 \cdot 1 = 1 \quad . \quad 1 \cdot \omega = \omega = \omega \cdot 1$

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

iv) Inverse element:

$1 \cdot 1 = 1$ and $\omega^2 \cdot \omega = \omega \cdot \omega^2 = \omega^3 = 1$

$\therefore$ inverse of $1, \omega, \omega^2$ are $1, \omega^2, \omega$ respectively.

v) commutative.

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

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

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

4] Prove that the four roots of unity $1, -1, i, -i$, where $i = \sqrt{-1}$ form an abelian multiplation group.

(or)

Show that fourth roots of unity is an abelian group.

Soln:- Preparing the composition table for the set $G = \{1, -1, i, -i\}$

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(i) Closure property.

Since all the elements in the composition table are also elements of G.

ie) $1, -1, i, -i \in G$.

. Identity element.

1 is identity element

$1 \cdot 1 = 1$

$1 \cdot (-1) = -1$

$1 \cdot (i) = i$

$1 \cdot (-i) = -i$

i.e) $1 \cdot a = a$, for all $a \in G$

(iii) Associativity

ordinary multiplication is always associative.

iv) Inverse law.

$1 \cdot 1 = 1$

$-1 \cdot (-1) = +1$

$(-1) \cdot (-i) = i$

$i \cdot (-1) = -i$

ie) inverse of $1, -1, i$ & $-i$ are $1, -1, -i, i$ respectively.

v) Acc to the law $a \times b = b \times a$ (rows are identical to columns) $a, b \in G$ holds.

Hence G is an abelian group under multiplication.

Hence, G is an abelian group under multiplication.

5] Determine whether the set $G = \{(a,b) : a,b \in R, a \neq 0\}$ under the operation defined as
$(a,b)\cdot(c,d) = (ac, bc+d)$, $\forall (a,b),(c,d) \in G$
is an abelian group.

Soln:- verifying the following properties with respect to the given operation defined on the set A.

(i) Associativity:
Let (a,b), (c,d) and (e,f) be any three elements of A. Then

$$[(a,b)\cdot(c,d)]\cdot(e,f) = (ac, bc+d)\cdot(e,f)$$
$$= [(ac)\cdot e, (bc+d)\cdot e + f]$$
$$= [ace, bce + de + f] \quad \text{---} (1)$$

Also $(a,b)\cdot[(c,d)\cdot(e,f)] = (a,b)\cdot[ce, de+f]$
$$= [a\cdot(ce), b\cdot(ce) + (de+f)]$$
$$= [ace, bce + de + f] \rightarrow (2)$$

From eqn. (1) & (2) we conclude that multiplication is associative.

(ii) Identity element.
Now if (x,y) is an element of A such that.
$$(a,b)\cdot(x,y) = (a,b) \in A$$

Then, $(xa, ya+b) = (a,b)$.

$\therefore xa = a$ and $ya + b = b$

$\Rightarrow x = 1$ & $y = 0$

Hence $(1,0)$ is the identity element.

(iii) Inverse.

Let for each $(a,b) \in A$ there exist an element $(x,y) \in A$ such that

$(x,y) \cdot (a,b) = (1,0)$

$\Rightarrow (xa, ya+b) = (1,0)$

Then $xa = 1$ and $ya + b = 0$, which gives

$x = 1/a$ and $y = -b/a$

Since $a \neq 0$, x, y, are real numbers

$\therefore (1/a, -b/a)$ is the inverse of (a,b).

Hence A is a group. Now

$(a,b) \cdot (c,d) = (ac, bc+d)$

and $(c,d) \cdot (a,b) = (ca, da+b)$

In general $(a,b) \cdot (c,d) \neq (c,d) \cdot (a,b)$

Hence, A is non-abelian group.

6] Prove that the set, I of integers an abelian group with respect to the operation, * defined on it as:

$$a * b = a + b + 1.$$

Soln: Verifying the following properties with respect to the given operation defined on the set I:

(i) Closure law

Since a, b are the elements of I,

$$\therefore a * b = a + b + 1$$

(ii) Associativity. If $a, b, c \in I$, then.

$$(a * b) * c = (a + b + 1) * c$$
$$= (a + b + 1) + c + 1$$
$$= a + b + c + 2$$

Also $a * (b * c) = a * (b + c + 1)$

$$= a + b + c + 2$$

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

(iii) Identity element.

Let e be an element of I such that

$$e * a = a = a * e.$$

$$e * a = e + a + 1$$

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

Now $-1 \in I$ and any $a \in I$.

$$(-1) * a = -1 + a + 1 = a.$$

It follows -1 is the identity element.

iv] **Inverse :-**

For each $a \in I$ there exists an element $b \in I$ such that $b * a = -1$

i.e) $(b + a + 1) = -1$

$\Rightarrow b = -2 - a$

$\therefore$ if $a \in I$, then $-2 - a \in I$

Also $(-2 - a) * a = (-2 - a) + a + 1 = -1$

Hence $-2 - a$ is the left inverse of a

v] **commutative** $a * b = a + b + 1$

$= b + a + 1$

$= b * a$

Hence, the set I of integers is an abelian group for the given operation.

7] Prove that the set Q of rational number other than 1 forms an abelian group with respect to the operation $*$ defined as: $a * b = a + b - ab$

(or)

Show that $(A, *)$ is an abelian group where $A = \{a \in Q \mid a \neq 1\}$ and for any $a, b \in A$, $a * b = a + b - ab$.

Soln: Verifying the following properties with respect to the given operation defined on the set Q.

(i) Closure $\quad a \in Q \neq b \in Q$

$\Rightarrow a \neq b$ are rational numbers other than 1

Now $a * b = a+b-ab$ which is also a rational number and it cannot be equal to 1.

Since $a+b-ab = 1$

$\therefore a+b-ab-1 = 0 \Leftrightarrow (a-1)(1-b)$

i.e) $a = 1, b = 1$

which is not true.

$\therefore a * b \in Q, \forall a, b \in Q$.

(ii) Associativity If $a, b, c \in Q$, then

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

Also $a*(b*c) = a*(b+c-bc)$

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

Hence $(a*b)*c = a*(b*c)$ $\forall a, b, c \in Q$.

(iii) Identity let $e \in Q$ be the identity element such that.

$$e * a = a = a * e \; ; \; a \in Q$$

$$e * a = e + a - ea = a$$

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

ie) $e = 0$. since $a \neq 1$

Thus $0 \in Q$, is the identity element.

(iv) Inverse For each $a \in Q$, there exists an element, $b \in Q$ such that.

$$a * b = 0 = b * a$$

Now, $a * b = 0$

$$a + b - ab = 0$$

$$b(1-a) + a = 0$$

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

Thus $\frac{a}{a-1}$ is the inverse of a $(a \neq 1)$ because

$$a * \left(\frac{a}{a-1}\right) = \left(\frac{a}{a-1}\right) + a - \left(\frac{a}{a-1}\right) a$$

$$= \frac{a + a^2 - a - a^2}{a-1} = \frac{0}{a-1} = 0$$

v) Commutative:

If $a, b \in Q$, then $a * b = b * a$. Now

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

Hence, mathematical structure $(Q, *)$ is an abelian group.

① 8] Prove that the set Q of rational numbers other than -1 forms an abelian group for the operation $*$ defined as:

$$a*b = a+b+ab$$

Show that $(A, \cdot)$ is an abelian group where $A = \{a \in Q \mid a \neq -1\}$ and for any $a, b \in A$, $a \cdot b = a+b+ab$

9] Prove that the set Q_+ of positive rational numbers forms an abelian group with respect to the operation $*$ defined as: $a*b = ab/2$.

Soln:- a) Closure. If $a, b \in Q_+$. then $ab/2$ is also in Q_+

b) Associativity. If $a, b, c \in Q_+$, then

$$(a*b)*c = \frac{ab}{2} * c = \frac{1}{2}\left[\frac{abc}{2}\right]$$

$$= \frac{1}{4}[(a \cdot b) \cdot c] = \frac{1}{4}[a \cdot (b \cdot c)]$$

$$= \frac{1}{2}\left[a \cdot \frac{bc}{2}\right] = \frac{1}{2}[a \cdot (b*c)]$$

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

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

c) Identity. The number e serves as an identity element provided $e \in Q$ and $e*a = a = a*e$. for all $a \in Q_+$

Now $e*a = a \Rightarrow \frac{ea}{2} = a$ i.e) $e = 2$

Thus, $2 \in Q_+$ serves as an identity element, because.

$$2 * a = \frac{2a}{2} = a * 2, \quad \forall a \in Q_+$$

d) Inverse :-

Any element, $b \in Q_+$ is said to be the inverse of $a \in Q_+$, if $b * a = 2 = a * b$ [since $e = 2$]

Now $b * a = 2 \Rightarrow \frac{ab}{2} = 2$ ⓪ $b = 4/a$

Thus $a \in Q_+ \Rightarrow \frac{4}{a} \in Q_+$

$$\Rightarrow \frac{4}{a} * a = \frac{1}{2}\left(\frac{4}{a}\right) \cdot a = \frac{4a}{2a} = 2.$$

Hence $4/a$ is the inverse of a.

e) Commutative.

If $a, b \in Q_+$ then $a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$

Hence $(Q_+, *)$ is an abelian group.

Properties of a Group :-

① Concellation law :

Let G be a group and $a, b, c \in G$.

Then $a \cdot b = a \cdot c \Rightarrow b = c$

Since $a^{-1} \in G$, then

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

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

$$\Rightarrow e \cdot b = e \cdot c$$

$$\Rightarrow b = c \quad \text{(left concellation law)}$$

illy Right cancellation law

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

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

$= b * a$

$$b \cdot e = c \cdot e$$

$$b = c$$

(02)

Let G be a group and and let a, b, c be elements of G. Then

(i) $a \cdot b = a \cdot c$ implies $b = c$ (left)

(ii) $b \cdot a = c \cdot a$ implies $b = c$ (Right)

2. The left Identity is also the Right Identity.

ie) $e.a = a = a.e$, for $a \in G$

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

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

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

$$\therefore a^{-1}(a.e) = (a^{-1}.a).e \Rightarrow a.e = a$$

Hence e is also the right identity element in group G.

3. The left Inverse of an Element is also the Right Inverse.

ie) $a^{-1}.a = e = a.a^{-1}$ for $a \in G$

let a^{-1} is the inverse of a, then

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

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

Thus $a^{-1}(a.a^{-1}) = a^{-1}.e \Rightarrow a.a^{-1} = e$

4. The identity element of a group is Unique (Imp)

Suppose if possible e and e' be two elements of the group G then

(i) $a.e = a = e.a$

(ii) $a.e' = a = e'.a$, $\forall\ a \in G$

Now $a = e'$ in (i) and $a = e$ (ii)

$\Rightarrow e.e' = e'$ $\Rightarrow e.e' = e$

But $e.e' = e'$ and $e.e' = e \Rightarrow e = e'$

Hence, the identity element is unique.

5] The inverse of an element of a group is unique. [Imp]

Soln:- let e be the identy element and a be an element of the group $(G, *)$

If possible let b and c be 2 inverses of $a \in G$

Since b is an inverse of a

$$a*b = b*a = e \quad \text{—①}$$

Again c is an inverse of a

$$a*c = c*a = e \quad \text{—②}$$

$$\Rightarrow b = b*e$$

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

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

$$b = e*c$$

$$\Rightarrow \boxed{b = c}$$

] If a, b are 2 elements of a group G. then the Equations $ax = b$ and $ay = b$ have unique solution in G.

Soln:- Consider the equation $a*x = b$

$$ax = b$$

For an element $a \in G \Rightarrow a^{-1} \in G$

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

$$a^{-1}.(a.x) = a^{-1}.b$$

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

$$\Rightarrow e.x = a^{-1}.b$$

$$\Rightarrow x = a^{-1}.b$$

To establish the uniqueness of the solution, we shall assume that there are 2 soln. say x_1 and x_2

i.e) $ax_1 = b$ and $ax_2 = b$

$\Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$ (left cancellation law)

Hence the soln is unique.

Again consider the equation $ay = b$

$a^{-1}.(a.y) = b.a^{-1}$

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

$\Rightarrow e.y = b.a^{-1}$

$\Rightarrow y = b.a^{-1} \Rightarrow y = a^{-1}.b$

Thus the solution of $a.y = b$ is $y = b.a^{-1}$

we shall assume that there are 2 solutions say y_1 and y_2

i.e) $ay_1 = b$ and $ay_2 = b$

$\Rightarrow ay_1 = ay_2$

$\Rightarrow y_1 = y_2$

Hence, the solution is unique.

7] Inverse of an Inverse of the Element of a Group is the Element

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

By definition of inverse.

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

Pre-multiplying both sides by $(a^{-1})^{-1}$

$\Rightarrow (a^{-1})^{-1}[a^{-1}a] = (a^{-1})^{-1}e$

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

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

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

8] Inverse of the product of 2 elements of a group is the product of their Inverses taken in the reverse order

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

Let $a, b \in G$ and a^{-1}, b^{-1} are inverses of 'a' and 'b' respectively such that

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

and $bb^{-1} = e = b^{-1}b$

where e is the identity element of the group G.

Now, Let $x = b^{-1} * a^{-1}$ and

$y = a * b$

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

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

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

$x * y = \therefore b^{-1} * b$

$x * y = e$ ——— (1)

Again consider,

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

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

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

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

$y * x = e$ ——— (2)

from (1) & (2) x is a inverse of y

$\Rightarrow x = y^{-1}$

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

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

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

Some particular group

(1) The klein 4- group :-

Definition :-

⇒ The klein four-group is an abelian group with four elements, in which each element is self-inverse and in which composing any two of the 3 non-identity elements produces the third one.

Problem 8 :-

If $A = \{e, a, b, c\}$ then show that this is a klein-4 group.

Soln :-

Set $A = \{e, a, b, c\}$, $*$ be the binary operation defined on A as per the table shown below.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

① ~~cts~~ closure law:
each row and each column contains all the elements of the set.

② Associative property.

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

$c * c = a * a$

$e = e.$

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

③ Identity element:

$a * e = a = e * a$

$b * e = b = e * b$

$c * e = c = e * e$

Hence 'e' is the Identity element.

④ Inverse.

$a * a = e$

$b * b = e$

$c * e = e$

So, each element is its own inverse.

⑤ commutative law :-

$a * b = b * a$

$c = c$

$b * c = c * b$

$a = a$

$a * e = e * a$

$b = b$

we conclude A is an abelian group.

→ Klein-4 group.

(2) Define klein-4 group.
verify $A = \{1, 3, 5, 7\}$ is a klein 4 group.

Soln:

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

(1) Closure law:
each row & each column contains all the elements of the set ∴ its closure

(2) Associativity: $[(a*b)*c = a*(b*c)]$

$(3*5)*7 = 3*(5*7)$

$7*7 = 3*3$

$1 = 1$

(3) Identity element. $[a*e = a = e*a]$

$3*1 = 3 = 1*3$

$5*1 = 5 = 1*5$

$7*1 = 7 = 1*7$

Hence '1' is an Identity element.

(4) Inverse law :- [a*b=e=b*a]

$1 * 1 = 1$

$3 * 3 = 1$

$5 * 5 = 1$

$7 * 7 = 1$

So, each each element is its own inverse.

(5) commutative law. [a*b = b*a]

$5 * 3 = 3 * 5$

$7 = 7$

Illy $3 * 7 = 7 * 3 = 5$

$5 * 7 = 7 * 5 = 3$ //

we ~~conc~~ conclude A is an abelian as klein-4 group.

2. Addition modulo m :-

Let 'm' be a fixed positive integer and 'a' and 'b' be any two integers. The binary composition called addition modulo m, denoted and defined as.

$a +_m b$ = least non-negative remainder obtained by dividing the usual sum a+b by m.

For example :-

Under addition modulo 7, we have

$4 +_7 6 = 3$ ∵ the usual sum $4+6=10$ leaves 3 as remainder when divided by 7

Illy $4 +_4 5 = 1$

$3 +_7 7 = 0$

$2 +_7 7 = 4$

3. Multiplication modulo m :-

Let 'm' be a fixed positive integer and 'a' and 'b' be any 2 integers. The binary composition called multiplication modulo m.

⇒ $a \times_m b$ = least non-negative remainder obtained by dividing the usual product $a \cdot b$ by m.

Examples- Under multiplication modulo 6, we have $4 \times_6 6 = 0$ ∵ the usual product $4 \cdot 6 = 24$ leaves 0 as remainder when divided by 6.

Illy $4 \times_3 5 = 2$, $3 \times_3 7 = 0$

$2 \times_5 7 = 4$ etc.

Problems

① Show that $(Z_6, +_6)$, where $Z_6 = \{0, 1, 2, 3, 4, 5\}$ is a abelian group.

$+_6$	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 law:
each row & each column contains all the elements of set ∴ its closure.

(2) Associativity
consider $3 +_6 (4 +_6 2) = (3 +_6 4) +_6 2$

$3 +_6 0 = 1 +_6 2$

$3 = 3$

Illy, with any other 3 elements of Z_6
Thus, $+_6$ is associative in Z_6

3] Existance of identity:
From addition table 0 is the Identity element of the given operation

(4) Existence of Inverse:-

From the table, we see that the Inverses of 0, 1, 2, 3, 4 and 5 are 0, 5, 4, 3, 2 and 1 respectively.

For example:-

$5 +_6 1 = 0 = 1 +_6 5$

$2 +_6 4 = 0 = 4 +_6 2$

$3 +_6 3 = 0 = 3 +_6 3$

(5) Commutative law.

If $a, b \in G$, then $a +_6 b = b +_6 a$

Example. $5 +_6 4 = 3 = 4 +_6 5$.

Hence, G is an abelian group.

2] Show that $G = \{1, 2, 3, 4\}$ is an abelian group under multiplication modulo 5.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(1) Closure law. :-

For any $a, b \in G$.

$a \times_5 b \in G$

Example:

$4 \times_5 3 = 2$

i.e. $2 \in G$

② Associativity :-

For any $a, b, c \in G$.

$$a \times_5 (b \times_5 c) = (a \times_5 b) \times_5 c$$

For example:-

$$3 \times_5 (4 \times_5 2) = (3 \times_5 4) \times_5 2$$

$$3 \times_5 3 = 2 \times_5 2$$

$$4 = 4$$

Illy For any other 3 elements of G.

③ Identity :-

From the table it follows that 1 acts as the identity element $[a \times_6 e = a]$

For example:-

$$2 \times_6 1 = 2$$
$$3 \times_6 1 = 3$$
$$4 \times_6 1 = 4$$

④ Existence of inverse :-

For every element $a \in G$, there exists an element $b \in G$ such that $a \times_5 b = 1 = b \times_5 a$

example:- $2 \times_5 3 = 1 = 3 \times_5 2$

$1 \times_5 1 = 1 = 1 \times_5 1$

$4 \times_5 4 = 1 = 4 \times_5 4$.

⑤ Commutative :-

For any $a, b \in G$

$$\Rightarrow a \times_5 b = b \times_5 a$$
$$2 \times_5 3 = 3 \times_5 2$$

Hence $(G, \times_5)$ is an abelian Group.

Subgroup

A non-empty subset $(H, *)$ of a group $(G, *)$ is said to be a subgroup of G if $(H, *)$ is also a group by itself.

condition:- for $a, b \in H$, $a * b^{-1} \in H$

$e \in H$

for any $a \in H$, $a^{-1} \in H$.

Example:-

The group $(Q, +)$ of rational numbers under usual addition, is a subgroup of the group $(R, +)$ of real numbers, under usual addition.

(1) A non empty subset H of a group $(G, *)$ is a subgroup of G if and only if

i) $a, b \in H \Rightarrow a * b \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$

Soln:-

[a] Let H be a subgroup of G

we shall show that condition (i) & (ii) are true

By data H is a sub group of $(G, *)$.

Thus H is a group by itself under the binary operation $*$

$\therefore$ H is closed under the binary operation $*$.

ie) $\forall a, b \in H$

$a * b \in H$

Again H is group under $*$

thus, by the existence of inverse axiom. we have.

$a \in H \Rightarrow a^{-1}$ exists and $a^{-1} \in H$

Hence (i) and (ii) are true.

b) let H be a subset of G such that (i) and (ii) are true. we shall show that H is a group by itself under the binary operation $*$.

By data $(a, b \in H \Rightarrow a * b \in H)$

$\Rightarrow$ H is closed under the binary operation $*$.

Since the associative law is true in G

$\Rightarrow$ it is also true in $H \subset G$

Again by data, $a \in H \Rightarrow a^{-1} \in H$

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

$\Rightarrow e \in H$

Thus, the identity element of $e \in H$.

Again by data $a \in H \Rightarrow a^{-1} \in H$

Thus, the inverse of a exists in H

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

Thus, H is a group by itself and hence, it is a subgroup of G.

2] A non empty subset H of a group (G, *) is a subgroup of G if and only if $\forall a, b \in H, a * b^{-1} \in H$ [Imp]

Proof

a] Let H be a sub group of (G, *)

we shall show that

$\forall a, b \in H \quad a * b^{-1} \in H$

By data H is a subgroup of G and

$\therefore$ H is a group by itself. Thus

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

and $a, b \in H, \quad a * b \in H.$

$a \in H, \; b \in H \Rightarrow a \in H$

$, b^{-1} \in H \Rightarrow a * b^{-1} \in H.$

Hence, (1) is true.

b] let H be a non empty subset of G such that $\forall a, b \in H \Rightarrow a * b^{-1} \in H$

we shall show that H is a group under *

Now let $a \in H \Rightarrow a * a^{-1} \in H \Rightarrow e \in H$

Thus H contains the identity element.

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

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

Thus inverse of a exists in H.

Now $\forall a, b \in H. \Rightarrow a, b^{-1} \in H$

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

is closed under *

The Associative law holds in H, as it holds in G.

Thus, H is a group by itself and hence, it is a subgroup of the group $(G, *)$.

3] The intersection of any two subgroups of a group is also a subgroup of G. [IMP]

let H_1 and H_2 be any two subgroups of G.

Then $H_1 \cap H_2 \neq \phi$

Since atleast identity element e is common to both H_1 and H_2

To prove $H_1 \cap H_2$ is a subgroup.

$a \in H_1 \cap H_2$, $b \in H_1 \cap H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

Now, $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

But H_1, H_2 are subgroups, so

$a \in H_1, b \in H_1 \Rightarrow ab^{-1} \in H_1$

and

$a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2$

$\therefore ab^{-1} \in H_1 \cap H_2$

Thus, we have shown that.

$a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} H_1 \cap H_2$

Hence, $H_1 \cap H_2$ is a subgroup of G.

(4) If H and K are two subgroups of G, then $H \cap K$ is also a subgroup of G.

Proof:- Let e be an identity of G.

Then e will also be the identity element in H as well as K.

i.e) $e \in H \cap K$

Thus $e \in H \cap K$ and $H \cap K \neq \phi$

If $a, b \in H$, then $a * b^{-1} \in H$

Illy if $a, b \in K$ and $a * b^{-1} \in K$

then $a * b^{-1} \in H \cap K$

Hence, $H \cap K$ is subgroup of G.

5] Show that $H = \{0, 2, 4\}$ is a subgroup of the group $(G, +_6)$ where $G = \{0, 1, 2, 3, 4, 5\}$

Soln Clearly $H \subset G$.

We shall show that H is a group by itself under Addition modulo 6.

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Clearly H is closed under addition modulo 6.

Associative law:- $H \subset G$

$(0 +_6 2) +_6 4 = 0 +_6 (2 +_6 4)$

$2 +_6 4 = 0 +_6 0$

$0 = 0$.

Existence of identity:

The element '0' acts as the identity elemt.

example $0 +_6 2 = 2 = 2 +_6 0$

$4 +_6 0 = 4 = 0 +_6 4.$

Existence of inverse:-

The inverse of 0 is 0, inverse 2 is 4 and inverse of 4 is 2

ie) $0 +_6 0 = 0$

$2 +_6 4 = 0$

$4 +_6 2 = 0.$

Thus $(H, +_6)$ is a group by itself and hence a subgroup of G.

Permutation group

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

(or)

A bijuctive mapping of a non-empty set 'S' to 'S' ie) $S \to S$ is called permutation of S.

The set G of all permutations on a non-empty set 'S' under the binary operation * of right composition of Permutation is a group (G, *) called permutation group.

If $S = \{1, 2, 3, 4, \ldots n\}$ the Permutation group is also called the Symmetric group of degree n. and denoted by S_n. possible permutations of S_n is n!

(1) Verify $(S_3, *)$: where $S = \{1, 2, 3\}$ is a group under the operation of right composition.

Given: $S = \{1, 2, 3\}$

There are 3! permutations possible of S

let $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Cayley's table:-

*	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_1	P_4	P_3	P_6	P_5
P_3	P_3	P_6	P_5	P_2	P_1	P_4
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_4	P_1	P_6	P_3	P_2
P_6	P_6	P_3	P_2	P_5	P_4	P_1

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

P_2 P_2 P_1

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

P_2 P_3 P_4

Using the above table, all the axioms of group can be obtained from the group.

① Closure :-

$P_1, P_2 \in S_3 \Rightarrow P_1 * P_2 \in S_3$

Hly all the permutations on the table are in the set S_3.

② Associativity :-

$(P_2 * P_4) * P_6 = P_2 * (P_4 * P_6)$

$P_3 * P_6 = P_2 * P_3$

$P_4 = P_4$

Always Associativity true for ordinary multiplication.

③ Existance of identity :-

We have

$P_1 * P_i = P_i$ for all $i = 1, 2, 3, 4, 5, 6$

$\therefore P_1$ is the identity element.

④ Existance of Inverse :-

$P_1 * P_1 = P_1$

$P_2 * P_2 = P_1$

$P_3 * P_5 = P_1$

$P_4 * P_4 = P_1$

$P_5 * P_3 = P_1$

$P_6 * P_6 = P_1$

$\therefore$ Inverse exists for each element of S_3

Hence $(S_3, *)$ is a group.

iv) NOTE:- we have $P_3 * P_6 = P_4$

$P_6 * P_3 = P_2$

$\therefore *$ is not commutative.

Hence $(S_3, *)$ is not an abelian group.

2] In the symmetric group S_4 consisting of all the permutation of this set $S = \{1, 2, 3, 4\}$

$$\alpha = \begin{Bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{Bmatrix} \text{ and } \beta = \begin{Bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{Bmatrix}$$

Verify $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$

Soln:-

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

$$(\alpha\beta)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \quad \text{---} (1)$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

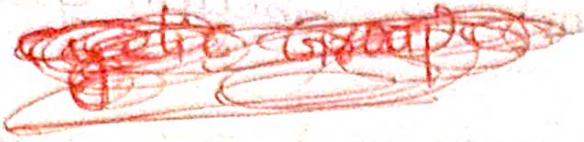
$$\beta^{-1}\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} - (2)$$

From (1) & (2)

$$(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$$

H.W

(3) Prove that $(S_2, *)$ is group where $S = \{1, 2\}$.



(4) In set $A = \{1, 2, 3\}$, let

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

Find $f \cdot g$ and $g \cdot f$.

$$\begin{cases} \text{WKT. } (g \cdot f)(x) = g[f(x)] & \forall x \in A \\ \text{and } (f \cdot g)(x) = f[g(x)] & \forall x \in A. \end{cases}$$

Soln:-

$$(g \cdot f)(1) = g[f(1)] = g(2) = 2$$
$$(g \cdot f)(2) = g[f(2)] = g(1) = 3$$
$$(g \cdot f)(3) = g[f(3)] = g(3) = 1$$

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

Again,

$$(f \cdot g)(1) = f[g(1)] = f(3) = 3$$
$$(f \cdot g)(2) = f[g(2)] = f(2) = 1$$
$$(f \cdot g)(3) = f[g(3)] = f(1) = 2$$

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

Note: $fg \neq gf$

5] In a set $G = \{a, b, c\}$. define the permutation A and B as $A = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$ and $B = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$ Find AB and BA.

Soln:

$$AB = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = I$$

and $$BA = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = I$$

$\therefore AB = BA = I$

CYCLIC GROUP

Definition :-

Let G be a group. If there exists an element $a \in G$ such that every element is expressible as $b = a^n$ for some integer n, then G is called a cyclic group and the element a is then called a generator of the cyclic group G. and it is denoted by

$$G = \{a\}$$

Symbolically, it is expressed as.

$$G = \{a^n : n \in I\} \text{ for multiplication}$$

$$G = \{na : n \in I\} \text{ for addition.}$$

Example :-

Consider the set, $A = \{1, 2, 3, 4\}$ and the $\times_5$. obviously, $(A, \times_5)$ is a group. It may be noted that

$$2^1 = 2 \pmod 5$$

$$2^2 = 4 \pmod 5$$

$$2^3 = 8 = 3 \pmod 5$$

$$2^4 = 16 = 1 \pmod 5$$

that is $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$

$\therefore$ 2 generates the elements (or) the group of 2 is the generator of the group. $\therefore A = \{2\}$

① Prove that the group $(\{1,-1,i,-i\},\times)$ is cyclic and its generator.

WKT $i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

It follows that elements of the set can be expressed as integral power of i

$\therefore$ it is a cyclic group generated by i.

② Define cyclic group and show that $(G, *)$ whose multiplication table as given below is cyclic

*	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

Soln:- From the cayley table,
G is closed w.r.t *
and Associative property can also be verified.

example :- $(a * b) * c = a * (b * c)$

$b * c = a * d$

$d = d$,

Existence of Identity:

'a' is the identity element.

ie) $b * a = b$
$c * a = c$
$d * a = d$
$e * a = e$
$f * a = e$

} from cayley table.

Existence of Inverse:-

From cayley table

$a * a = a$
$b * f = a$
$c * e = a$
$e * e = a$
$d * d = a$
$f * b = a$

} ∴ a, b, c, d, e, f inverses are a, f, e, d, e, b respectively.

Cyclic :-

$b^1 = b$

$b^2 = b * b = c$

$b^3 = b^2 * b = c * b = d$

$b^4 = b^3 * b = d * b = e$

$b^5 = b^4 * b = e * b = f$

$b^6 = b^5 * b = f * b = a$

$\therefore$ b is the generator of G

$G = \{b\}$

$\therefore (G, *)$ is a cyclic group

Cosets :-

Definition :-

If $(H, *)$ is the subgroup of a group $(G, *)$. Let $a \in G$.

Then the $H * a = \{h * a : h \in H\}$ is called a right coset of H in G generated by 'a'.

Similarly, the set $a * H = \{a * h : h \in H\}$ is called left coset of H in G generated by 'a'

Properties of cosets :-

1) $a \in aH$

2] $aH = H$ if and only if $a \in H$

3] $aH = bH$ or $aH \cap bH = \phi$

4] $aH = bH$ if and only if $a^{-1} \in H$

(1) Let $G = S_4$, the Symmetric group of order (degree) 4.

For $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, find the Subgroup $H = \langle \alpha \rangle$. Also, determine the no. of left cosets of H in G.

Soln:-

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

In S_4, the identity element.

$$P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

$$H = \langle \alpha \rangle = \{\alpha^1, \alpha^2, \alpha^3, \alpha^4 \dots \alpha^n = P^n\}$$

$$\alpha^2 = \alpha \times \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

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

$$\alpha^3 = \alpha^2 \times \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

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

$$\alpha^4 = \alpha^3 \times \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\alpha^4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = P_1$$

$$\therefore H = \left\{ \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} \right\}$$

The number of elements of the group is called order of the group and is denoted by $O(G)$ or $|G|$

Here $O(H) = 4$

$O(G) = O(S_4) = 4! = 24$

There fore, the number of distict left cosets of H in G is $[G:H] = \frac{24}{4} = 6$.

(2) Prove that the group $(U_9, \cdot)$ is cyclic

The elements of U_9 are

$\{1, 2, 3, 4, 5, 6, 7, 8\}$

and the operation in $(U_9, \cdot)$ is "multiplication modulo 9". we find that, in U_9

$[2] = [2]$

$[2]^2 = [4]$

$[2]^3 = [8]$

$[2^4] = [16] = [7]$

$[2]^5 = [32] = 5$

$[2]^6 = [64] = [1]$

Thus, every element of U_9 is an integral power $[2]$.

$\therefore (U_9, \cdot)$ is a cyclic group with $[2]$ as a generator.

(3) Prove that the group $(Z_4, +)$ is cyclic. Find all its generators.

The elements of Z_4 are the congruence classes $[0], [1], [2], [3]$ and operation $+$ in $(Z_4, +)$ is "addition modulo 4", we note that

$$[1]^1 = [1]$$
$$[2] = [1] + [1] = [1]^2$$
$$[3] = [1] + [1] + [1] = [1]^3$$
$$[0] = [4] = [1] + [1] + [1] + [1] = [1]^4$$

Thus, every element of Z_4 is an integral power of $[1]$. $\therefore$ $(Z_4, +)$ is a cyclic group with $[1]$ as a generator.

Since $[1]$ is a generator of $(Z_4, +)$,

$[1]^{-1} = [-1] = [4-1] = [3]$ is also a generator of $(Z_4, +)$.

Since $[0]$ is the identity element in $(Z_4, +)$; $[0]$ cannot be a generator of $(Z_4, +)$; because $[0]^n = n[0] = 0$ for all $n \in \mathbb{Z}$

Further, $[2]$ cannot be generator of $(Z_4, +)$ because $[2]^n \neq [1]$ in Z_4 $\forall\, n \in \mathbb{Z}$

Thus $(Z_4, +)$ is a cyclic group with $[1]$ and $[3]$. $(Z_4, +) = \langle [1] \rangle = \langle [3] \rangle$.

(4) Prove that $(Z_5, \cdot)$ is a cyclic group. Find all its generators.

The elements of the group $(Z_5, \cdot)$ are the congruence classes $[1], [2], [3], [4]$.

$(Z_5, \cdot) \Rightarrow$ multiplication modulo 5.

$[2] = [2]^1$

$[3] = [2]^3$

$[4] = [2]^2$

$[1] = [2]^4$

$(Z_5, \cdot) = \langle [2] \rangle$

$\therefore [2]^{-1} = 3$ is also a generator of $(Z_5, \cdot)$

$\therefore$ $[2]$ and $[3]$ are the generators of $(Z_5, \cdot)$.

Lagrange's Theorem

Statement :- If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Proof :- Since G is a finite group, H is finite,

$\therefore$ the number of cosets of H in G is finite. Let $a \in G$, then Ha is right coset of H in G

Let $Ha_1, Ha_2, \ldots Ha_k$ be the distinct right cosets of H in G.

Then, by the right coset decomposition of G we have.

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$$

So that

$$o(G) = o(Ha_1) + o(Ha_2) + \ldots + o(Ha_k)$$

But $o(Ha_1) = o(Ha_2) = \ldots = o(Ha_k) = o(H)$

$$\therefore o(G) = o(H) + (o(H)) + o(H) + \ldots + o(H)$$

$$= k\, o(H)$$

$$k = \frac{o(G)}{o(H)}$$

This shows that $o(H)$ divides $o(G)$

① let G be a group with subgroups H and K if $|G| = 660$ $|K| = 66$ $K \subset H \subset G$. Then find the possible value of $|H|$

Given $|G| = 660$ $|K| = 66$

$\therefore K \subset H \subset G$.

By lagrouge's theorem

$$K = \frac{O(G)}{O(H)}$$

$$O(G) = K O(H)$$

$$660 = K\, O(H) \longrightarrow (1)$$

and

$$n = \frac{O(H)}{O(K)}$$

$$\Rightarrow O(H) = n\, O(K)$$

$$O(H) = n\, 66 \longrightarrow (2)$$

from (1) & (2).

$$660 = K \times O(H)$$

$$660 = K \times n \times 66 \quad (\text{By } (2))$$

$$10 = K \times n$$

possible values of m & n such that

$mn = 10$

are $k=2$, $n=5$ (or) $m=5$, $n=2$

If $k=2$, $n=5$ (2) $\Rightarrow o(H) = 5 \times 66 = 330$

If $k=5$, $n=2$ (2) $\Rightarrow o(H) = 2 \times 66 = 132$.

$\therefore$ The possible values of $|H|$ are

132 (or) 330.