Groups

Date : .....

Defn: If G is a non empty set and $*$ is a binary operation on G, then $(G, *)$ is called a group if the following conditions are satisfied:

(1) $\forall a, b \in G$, $a * b \in G$. (G is closed under $*$)

(2) $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$ (Associative property)

(3) $\exists\, e \in G$ with $a * e = a = e * a$, $\forall\, a \in G$ (The existence of an identity)

(4) For each $a \in G$, $\exists\, a' \in G$ such that $a * a' = e = a' * a$ (Existence of inverse)

Here, e is called an identity element under $*$, a' is called an inverse of a under $*$ and is usually denoted by a^{-1}.

Further, group $(G, *)$ is said to be commutative or abelian if $ab = ba$, $\forall a, b \in G$.

For every group G, the number of elements in G is called order of G and is denoted by $|G|$ or $o(G)$.

Date : .....

For simplicity, we use the notation ab for $a * b$ and a^2 for $a * a$.

Problems:

1) Let G be the set of all non-zero real numbers and let $a * b = \frac{1}{2}ab$. Show that $(G, *)$ is an abelian group.

Soln: Closure property:

$\forall\, a, b \in G$, $\frac{1}{2}ab \in G$

$\Rightarrow a * b \in G$

$\therefore$ Therefore, G is closed under $*$.

Associative property:

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

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

$= \frac{1}{4}abc$

and $(a * b) * c = \frac{1}{2}(a * b)c = \frac{1}{2}ab$

$= \frac{1}{2}\left(\frac{1}{2}ab\right)c = \frac{1}{4}abc$

i.e., $a * (b * c) = (a * b) * c$

$\therefore$ $*$ is associative.

Date : .....

Identity property:

Let e be an identity element in G,

for $a \in G$, $a * e = a$

$\frac{1}{2}ae = a \Rightarrow e = 2$

Further, $a * 2 = 2 * a = \frac{1}{2}(2a) = a$, $\forall a \in G$.

$\therefore$ $e = 2$ is the identity element in G w.r.t. $*$.

Inverse property:

Let a' be the inverse of a w.r.t. $*$.

i.e., $a * a' = 2 \Rightarrow \frac{1}{2}(aa') = 2 \Rightarrow a' = \frac{4}{a}$

Further, $a * \frac{4}{a} = \frac{4}{a} * a = \frac{1}{2}\left(a\frac{4}{a}\right) = 2$

Thus, for every $a \in G$, $a' = \frac{4}{a}$ is inverse in G under $*$.

Commutative property

For $a, b \in G$,

$a * b = \frac{1}{2}(ab) = \frac{1}{2}(ba) = b * a$

$\therefore$ $(G, *)$ is an abelian group.

Date : .....

2) Let G be the set of all real numbers not equal to -1 and $*$ be defined by $a*b = a+b+ab$. Prove that $(G,*)$ is an abelian group.

Sol: for $a \neq -1$ & $b \neq -1 \in G$,

$a+b+ab \neq -1 \in G$.

$\therefore$ G is closed under $*$

Associative property:

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

Consider $a*(b*c) = a*(b+c+bc)$

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

$= a+b+c+bc+ab+ac+abc$

and $(a*b)*c = (a+b+ab)*c$

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

$= a+b+ab+c+ac+bc+abc$

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

$\therefore$ $*$ is associative.

Identity property:

Let e be the identity element in G.

for $a \in G$, $a*e = a$

$a+e+ae = a$

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

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

So, for every $a \in G$,

$a*0 = 0*a = 0$

$\therefore$ $e = 0$ is the identity element.

Inverse property:

Let a' be inverse of a.

$a*a' = e$

$\Rightarrow a+a'+aa' = 0$

$\Rightarrow a'(1+a) = -a \Rightarrow a' = -\frac{a}{1+a}$

So, $\forall\ a \in G$, $\exists\ a' = -\frac{a}{1+a}$ such that

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

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

$\therefore$ $a' = -\frac{a}{1+a}$ is inverse for every $a \in G$.

Commutative property:

$\forall\ a,b \in G$, $a*b = a+b+ab$

$= b+a+ba$

$= b*a$

$\therefore$ $(G,*)$ is an abelian group.

Date : .....

Theorem 1: In a group, there exists only one identity element (66)

The identity element in a group is unique.

Pf: let e_1 and e_2 are identity elements in a group G.

e_1 is identity $\Rightarrow a * e_1 = a = e_1 * a, \forall a \in G$

Since $e_2 \in G$, $e_2 * e_1 = e_2 = e_1 * e_2$

but e_2 is also identity

$\Rightarrow e_2 * e_1 = e_1 = e_1 * e_2$

i.e., $e_1 = e_1 * e_2 = e_2 * e_1 = e_2$

$\Rightarrow$ e_1 and e_2 are not ~~identical~~ different

This means G has unique identity element.

Theorem 2: In a group G, every element has only one inverse. (i.e., every element has a unique inverse in G).

Pf: let e be identity element in G.

suppose a' and a'' are inverses of an element $a \in G$.

$\Rightarrow a'a = e = aa'$

& $a''a = e = aa''$

Date : .....

we have $a' = a'e$ ($\because$ e is identity)

$= a'(aa'')$ ($\because$ a'' is inverse of a)

$= (a'a)a''$ ($\because$ associative property)

$= e\,a''$ ($\because$ a' is inverse of a)

$= a''$ ($\because$ e is identity).

i.e., a' and a'' cannot be different.

Theorem 3: For any elements a, b in a group G, we have

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

Pf: (i) let $a^{-1} = x$ (x is inverse of a)

$\Rightarrow ax = e = xa$

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

$\Rightarrow a$ is inverse of x.

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

(ii) need to show inverse of $ab = b^{-1}a^{-1}$

consider

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ ($\because$ associative)

$= a(e)(a^{-1})$ ($\because$ Inverse)

$= (ae)a^{-1}$ ($\because$ Associative)

$= a a^{-1}$ ($\because$ Identity)

$= e$ ($\because$ Inverse)

Date : .....

and $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b$ ($\because$ Associative)
$= b^{-1}(e)b$ ($\because$ Inverse)
$= (b^{-1}e)b$ ($\because$ Associative)
$= b^{-1}b$ ($\because$ Identity)
$= e$ ($\because$ Inverse)

$\Rightarrow$ $b^{-1}a^{-1}$ is inverse of ab

$\therefore$ $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem 4: Let G be a group and let a, b, x be elements of G. Then

(i) $xa = xb \Rightarrow a = b$ (left cancellation property)

(ii) $ax = bx \Rightarrow a = b$ (right cancellation property)

Pf: (i) Consider $xa = xb$
$\Rightarrow x^{-1}(xa) = x^{-1}(xb)$ (operate x^{-1} from left)
$\Rightarrow (x^{-1}x)a = (x^{-1}x)b$ ($\because$ Associative property)
$\Rightarrow ea = eb$ ($\because$ Inverse property)
$\Rightarrow a = b$ ($\because$ Identity property)

(ii) $ax = bx$
$\Rightarrow (ax)x^{-1} = (bx)x^{-1}$ (operate x^{-1} from right)
$\Rightarrow a(xx^{-1}) = b(xx^{-1})$ ($\because$ Associative)
$\Rightarrow ae = be$ ($\because$ Inverse)
$\Rightarrow a = b$ ($\because$ Identity)

Date : .....

Theorem 5: Let G be a group, and $a, b \in G$. Then

(i) The equation $ax = b$ has a unique soln in G.

(ii) The equation $ya = b$ has a unique soln in G.

Soln (i) Consider $ax = b$
$\Rightarrow a^{-1}(ax) = a^{-1}b$ (operating a^{-1} from left)
$\Rightarrow (a^{-1}a)x = a^{-1}b$ ($\because$ associative property)
$\Rightarrow ex = a^{-1}b$ ($\because$ Inverse property)
$\Rightarrow x = a^{-1}b$ ($\because$ Identity property.

since $a \in G$, $a^{-1} \in G \Rightarrow x = a^{-1}b \in G$ is soln of $ax = b$.

Suppose x_1 and x_2 are solns of the equation $ax = b$
$\Rightarrow ax_1 = b$ and $ax_2 = b$
$\Rightarrow ax_1 = ax_2$
$\Rightarrow x_1 = x_2$ (left Cancellation property)

Thus, the 2 solns of $ax = b$ are not different.

(ii) We can prove the above result similar to above.

Date : .....

Problems:

1) Prove that a group G in which every element is its own inverse is abelian.

Sol: let $a, b \in G \Rightarrow ab \in G$ (closure property)

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

and $(ab)^{-1} = ab$.

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

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

$= ba$

$\therefore G$ is abelian group.

2) In a group G having more than one element, if $x^2 = x \ \forall x \in G$, prove that G is abelian.

Sol: let $a, b \in G \Rightarrow ab \in G$

$\Rightarrow a^2 = a$, $b^2 = b$ and $(ab)^2 = ab$

consider $a(ab)b = (aa)(bb)$

$= a^2 b^2$

$= ab$

$= (ab)^2$

$= (ab)(ab)$

$a(ab)b = a(ba)b$

$\Rightarrow ab = ba$ (using cancellation property)

$\therefore G$ is abelian group.

Date : .....

3) Prove that a group G is abelian if and only if $(ab)^2 = a^2 b^2$ for all $a, b \in G$.

Proof: Given: G is abelian

To prove that: $(ab)^2 = a^2 b^2, \ \forall a, b \in G$.

$(ab)^2 = (ab)(ab)$

$= a(ba)b$ ($\because$ associative property)

$= a(ab)b$ ($\because G$ is abelian)

$= (aa)(bb)$ ($\because$ associative)

$= a^2 b^2$

Conversely:

Given: $(ab)^2 = a^2 b^2, \ \forall a, b \in G$.

T.P.T.: G is abelian.

Consider $(ab)^2 = a^2 b^2$

$(ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ ($\because$ associativity)

$\Rightarrow ba = ab$ (on using cancellation property)

$\therefore G$ is abelian.

Date : .....

4) Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ $\forall$ $a, b \in G$.

∴ Given: G is abelian

T.P.T: $(ab)^{-1} = a^{-1}b^{-1}$

We have $a^{-1}b^{-1} = b^{-1}a^{-1}$ ($\because$ G is abelian)

$= (ab)^{-1}$ ($\because (ab)^{-1} = b^{-1}a^{-1}$ in a group)

Converse: Given $(ab)^{-1} = a^{-1}b^{-1}$

Given $(ab)^{-1} = a^{-1}b^{-1}$ for $a, b \in G$.

T.P.T: G is abelian.

Consider $ab = (a^{-1})^{-1}(b^{-1})^{-1}$ ($\because (x^{-1})^{-1} = x$)

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

$= (b^{-1})^{-1}(a^{-1})^{-1}$ ($\because (xy)^{-1} = y^{-1}x^{-1}, \forall x, y \in G$)

$= ba$ ($\because (x^{-1})^{-1} = x$)

$\therefore$ G is abelian.

5) If o is an operation on Z defined by $x o y = x + y + 1$, prove that (Z, o) is an abelian group.

∴ Closure property:

for $x, y \in G = Z$, $x + y + 1 \in Z$

$\Rightarrow x o y \in Z$

$\therefore$ Z is closed under o.

Date : .....

Associative property: for $x, y, z \in Z$,

Consider $x o (y o z) = x + (y o z) + 1$

$= x + (y + z + 1) + 1$

$= x + y + z + 2$

and $(x o y) o z = (x o y) + z + 1$

$= (x + y + 1) + z + 1$

$= x + y + z + 2$

$\therefore$ o is associative in Z.

Identity property:

let e be the identity element in Z

for $x \in Z$, $x o e = x$

$\Rightarrow x + e + 1 = x \Rightarrow e + 1 = 0 \Rightarrow e = -1$.

and $x o e = x$

and $x o (-1) = x + (-1) + 1 = (-1) + x + 1 = (-1) o x$

$\therefore$ $e = -1$ is identity element exist in Z.

Inverse property:

let x' be inverse of x in G.

$\Rightarrow x' o x = e = (-1) \Rightarrow x' + x + 1 = -1$

$\Rightarrow x' = -2 - x$

and $x o (-2 - x) = x + (-2 - x) + 1 = -1$

$(-2 - x) o x = (-2 - x) + x + 1 = -1$

$\therefore$ $\forall x \in Z$, $x' = -2 - x$ is inverse exists in Z.

Date : .....

Commutative property:

for $x, y \in \mathbb{Z}$, Consider

$$x \circ y = x + y + 1$$
$$= y + x + 1$$
$$= y \circ x$$

$\therefore$ G is abelian group under $\circ$.

6) Show that fourth roots of unity is an abelian group.

Soln (or)

Show that the set $G = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$ is an abelian group with respect to multiplication as a binary operation.

By:

x	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

From the above table, it is clear that $\forall a, b \in G$, $a \times b \in G$

$\therefore$ G is closed under $\times$.

Date : .....

Associative property:

From the table we can check that

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

$\therefore$ $\times$ is associative in G.

Identity property:

From the table, it is clear that 1 is the identity element in G

i.e., $\forall a \in G$, $a \times 1 = a = 1 \times a$.

Inverse property:

From table,

inverse of 1 is 1,

inverse of -1 is -1

inverse of i is -i

inverse of -i is i

i.e., inverse of every element in G exists.

Commutative property:

From the table, it is evident that

$\forall a, b \in G$, $a \times b = b \times a$.

$\therefore$ $(G, \times)$ is abelian group.

Date : .....

7) Prove that $G = \{1, \omega, \omega^2\}$ is a group w.r.t. multiplication whose $1, \omega, \omega^2$ are cube roots of unity.

Sol:

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

[Here, $\omega^3 = 1$, $\omega^4 = \omega$]

From above table, it is clear that

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

$\therefore$ G is closed under $\cdot$.

Associative property:

From the table, we can check

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

$\therefore$ $\cdot$ is associative in G.

Identity property:

From the above table, it is clear that

1 is the identity element in G

i.e., $\forall\ a \in G$, $a \cdot 1 = a = 1 \cdot a$.

Date : .....

Inverse property:

From the table,

inverse of 1 is 1

inverse of ω is ω^2

inverse of ω^2 is ω.

i.e., inverse of every element in G exists.

Commutative property:

Table is symmetrical about principal diagonal.

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

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

Klein-4 group:

It has four elements, say $V_4 = \{e, a, b, c\}$ satisfying following properties.

(1) e is the identity element

(2) each element is its own inverse, meaning $a^2 = b^2 = c^2 = e$;

(3) the product of any two non-identity elements is the third non-identity element; $ab = c$, $bc = a$, and $ca = b$.

Date : .....

So, the Klein-4 group

So, the cayley table for the Klein-4 group is as follows:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This table shows that $xy = yx, \forall x, y \in V_4$.

i.e., Klein-4 group is abelian.

Note : * $[x]$ → equivalence class of x.

* Z_n → set of all congruence classes modulo n,

i.e., $Z_n = \{[0], [1], [2], \ldots, [n-1]\}$

$\Rightarrow o(Z_n) = n$

* $Z_p^* = \{[1], [2], \ldots [p-1]\}$

$\Rightarrow o(Z_p^*) = p-1$, where p is prime.

* $\oplus_n$ → addition modulo n

* $\otimes_p$ → multiplication modulo p.

Date : .....

Problem

① Show that Z_6 is abelian group under $\oplus_6$

(or)

Show that $(Z_6, \oplus_6)$ is abelian group

(or)

Show that $(Z_6, +)$ is abelian group.

Let us consider the cayley table for $(Z_6, +)$.

+	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

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

Every entry in the table belongs to Z_6. Hence Z_6 is closed under $+$.

$\forall a, b, c \in Z_6$, $a + (b+c) = (a+b) + c$

$\therefore$ $+$ is associative.

Date : .....

0 is the identity element in Z_6 w.r.t. +.

Inverse of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.

i.e., inverse exists for every element.

$\therefore (Z_6, +)$ is group.

Further, table is symmetrical about principal diagonal

i.e., $(Z_6, +)$ is abelian group.

i.e., + is commutative

Hence, $(Z_6, +)$ is abelian group.

2) Show that $(Z_7^*, \cdot)$ is an abelian group

(or)

Show that $(Z_7^*, \otimes_6)$ is an abelian group

(or)

Show that Z_7^* is an abelian group under multiplication modulo 7.

Date : .....

Let us construct the Cayley's table

We know $Z_7^* = \{1, 2, 3, 4, 5, 6\}$.

·	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	1	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Every entry in the table belongs to Z_7^*

Hence Z_7^* is closed under ·.

From the table, we can check

$\forall a, b, c \in Z_7^*$

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

$\therefore$ · is associative.

1 is the identity element in Z_7^* w.r.t. ·.

Inverse of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3, 6, respectively.

i.e., inverse exists for every element in Z_7^*.

Date : .....

Further, Cayley table is symmetrical about principal diagonal

i.e., $\forall a, b \in Z_7^*$; $a \cdot b = b \cdot a$

$\therefore \Rightarrow (Z_7^*, \cdot)$ is an abelian group.

3. Show that $G = \{1, 3, 5, 7\}$ is Klein-4 group under multiplication modulo 8.

Sol: Let us construct the Cayley's table

$\otimes_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

From the table it is clear that every entry in the table is part of G

$\therefore$ G is closed under $\times_8$.

$\forall a, b, c \in G$, we can check

$a \otimes_8 (b \otimes_8 c) = (a \otimes_8 b) \otimes_8 c$

$\therefore \otimes_8$ is associative.

Date : .....

1 is the identity element in G.

Inverse of 1, 3, 5, 7 are 1, 3, 5, 7 respectively.

i.e., inverse of every element is itself.

$\therefore (G, \otimes_8)$ is ~~abelian~~ group.

Further, Cayley's table is symmetrical about principal diagonal.

i.e., $\forall a, b \in G$, $a \otimes_8 b = b \otimes_8 a$.

$\therefore (G, \otimes_8)$ is an abelian group.

Here, $|G| = 4$ and $(G, \otimes_8)$ satisfies all properties of Klein-4 group.

So, $(G, \otimes_8)$ is Klein-4 group.

Permutations group:

Let S_3 denotes all permutations of three elements 1, 2, 3.

$S_3 = \{P_0, P_1, P_2, P_3, P_4, P_5\}$.

$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Date : .....

$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Here, the entries in the upper row denote the places and the entries in the bottom row denotes the elements that are placed in the corresponding places.

We observe that these six (3!) permutations are bijective functions from set $A = \{1, 2, 3\}$ to itself. Therefore, the composition of two permutations is a permutation. Thus, if S_3 ~~denotes the set of all~~ Since S_3 denotes set of all permutations, S_3 is closed under the composition of permutations.

Since the composition of functions is associative, the composition of

Date : .....

permutations is also associative.

The Cayley's table for the composition of permutations on S_3 is given below.

$\circ$	P_0	P_1	P_2	P_3	P_4	P_5
P_0	P_0	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_2	P_0	P_5	P_3	P_4
P_2	P_2	P_0	P_1	P_4	P_5	P_3
P_3	P_3	P_4	P_5	P_0	P_1	P_2
P_4	P_4	P_5	P_3	P_2	P_0	P_1
P_5	P_5	P_3	P_4	P_1	P_2	P_0

[Note: $P_1 \circ P_3$

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

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

$= P_5$]

Above table is obtained using rule of composition of functions.

Date : .....

From the Cayley's table it is clear that

(i) P_0 is the identity element in S_3

(ii) Inverses of $P_0, P_1, P_2, P_3, P_4, P_5$ are $P_0, P_2, P_1, P_3, P_4, P_5$ respectively. i.e., inverse exists for every element of S_3.

(iii) Table is not symmetrical about principal diagonal.

$\therefore (S_3, o)$ is non-abelian group.

Generalizing the above discussions, it can be shown that the set of all permutations on any finite set having n elements is a non-abelian group under composition of permutations. This group contains $n!$ number of permutations and is called the symmetric group of degree n; it is denoted by S_n. $o(S_n) = |S_n| = n!$

Date : .....

Problem: The symmetric group S_4 consists of all the permutations of the set $A = \{1, 2, 3, 4\}$. What is the order of S_4? What is the identity element in S_4? If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, verify that $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

Sol:- $o(S_4) = 4!$

The identity element in S_4 is the identity permutation, $P_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

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

If $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$ is inverse of α, then $\alpha^{-1}\alpha = P_0$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ b & d & c & a \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$\Rightarrow b = 1, d = 2, c = 3, a = 4$

Date : .....

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

Similarly if $\bar{\beta}^{-1}$ is inverse of β then

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ d & b & a & c \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

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

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

$$(\alpha\beta)^{-1}(\alpha\beta) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I_0$$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & d & b & c \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Date : .....

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

from (1) & (2)

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

Subgroups:

A non empty subset H of a group G is called a subgroup of G whenever H itself is a group under the binary operation in G.

Problem: Let $H = \{0, 2, 4\} \subseteq Z_6$. Prove that $(H, +)$ is a subgroup of $(Z_6, +)$.

Sol: let we construct the Cayley's table

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Every entry in the table is part of H, so H is closed under addition modulo 6.

Further, $\forall\, a, b, c \in H$,

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

Date : .....

$\therefore +$ is associative

0 is the identity element in H.

Inverses of 0, 2, 4 are 0, 4, 2 respectively.

i.e., inverse of every H exists.

$\therefore (H, +)$ is a group & $H \subseteq Z_6$

$\therefore (H, +)$ is a subgroup of $(Z_6, +)$.

Problem: Let $T = \{P_0, P_1, P_2\} \subseteq S_3$. Verify that T is a subgroup of S_3 under composition of functions.

Pf: Let us construct the Cayley's table

$\circ$	P_0	P_1	P_2
P_0	P_0	P_1	P_2
P_1	P_1	P_2	P_0
P_2	P_2	P_0	P_1

Every entry in the table belongs to T. $\therefore$ T is closed under $\circ$.

Composition of functions is associative

$\therefore \circ$ is associative.

P_0 is identity element in T.

Inverses of P_0, P_1, P_2 are P_0, P_2, P_1 respectively.

Date : .....

Inverse of every element in T exists.

$\therefore (T, \circ)$ is a group & $T \subseteq S_3$

$\therefore (T, \circ)$ is a subgroup of $(S_3, \circ)$.

Note: Similar to above example, we can show $T_1 = \{P_0, P_3\}$, $T_2 = \{P_0, P_4\}$ and $T_3 = \{P_0, P_5\}$ are also subgroups of S_3 under $\circ$.

Note: ① For any group G, $e \in G$.

We can note $\{e\}$ and G are trivial subgroups of group G.

Criteria for a subset to be a subgroup

Theorem 1: H is a subgroup of G if and only if, $\forall a, b \in H$, we have (i) $ab \in H$ and (ii) $a^{-1} \in H$.

Pf: Given: H is subgroup of G

T.P.T.: $\forall a, b \in H$, (i) $ab \in H$ & (ii) $a^{-1} \in H$.

Date : .....

H is a group subgroup of G
⇒ H itself is a group.
⇒ ∀ a, b ∈ H, ab ∈ H (∵ closure property)
& a^{-1} ∈ H (∵ Inverse property)

Conversely: Given: (i) ∀ a, b ∈ H, ab ∈ H
(ii) ∀ a ∈ H, a^{-1} ∈ H.

T.P.T. H is a subgroup of G.

Condition (i) says closure law satisfied.

Take any a, b, c ∈ H
⇒ a, b, c ∈ G (∵ H ⊆ G)
⇒ (ab)c = a(bc)

Thus associative law holds in H.

From (ii), we can note every element in H has inverse.

Further, a^{-1} ∈ H
⇒ $a a^{-1}$ ∈ H (∵ Condition (i))
⇒ e ∈ H

∴ H is a group and H ⊆ G
⇒ H is a subgroup of G.

Date : .....

Theorem 2: H is a subgroup of G iff ∀ a, b ∈ H, we have ab^{-1} ∈ H.

Proof:

Given: H is a subgroup of G.

T.P.T: ∀ a, b ∈ H, ab^{-1} ∈ H.

H is a group ⇒ b^{-1} ∈ H, ∀ b ∈ H.

∴ ab^{-1} ∈ H, ∀ a, b ∈ H.
(∵ closure & inverse property).

Converse: Given, H ⊆ G & ∀ a, b ∈ H, ab^{-1} ∈ H.

T.P.T: H is a subgroup of G.

If b = a in given condition
⇒ $a a^{-1}$ ∈ H ⇒ e ∈ H.

Further, e ∈ H & a^{-1} ∈ H
⇒ $e a^{-1}$ ∈ H ⇒ a^{-1} ∈ H, ∀ a ∈ H.

Since b ∈ H & b^{-1} ∈ H
⇒ $a(b^{-1})^{-1}$ ∈ H (∵ given condition)
⇒ ab ∈ H
⇒ closure law satisfied.

Since associative law holds for all elements of G, this law holds for all elements of H.

∴ H is a subgroup of G.

Date : .....

Note: Above two theorems provides necessary and sufficient conditions for a subset H of a group G, to be a subgroup of the group G.

Problems:

1) Prove that the intersection of two subgroups of a group is a subgroup of the group.
Is the union of two subgroups of a group a subgroup of group?

Sol: Let G be a group and H & K are subgroups of G.

T.P.T: $H \cap K$ is subgroup of G.

Consider $a, b \in H \cap K$

$\Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow ab^{-1} \in H$ and $ab^{-1} \in K$ (∵given)

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

Thus, the intersection of a two subgroups of a group G is a subgroup of G.

Date : .....

Union of two subgroups of a group need not be a subgroup of group. To establish this, let we consider the following example.

Consider Cayley's table for Klein-4 group

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

From the above Table we can see that $T_1 = \{e, a\}$ and $T_2 = \{e, c\}$ are subgroups of Klein-4 group

Now, $T_1 \cup T_2 = \{e, a, c\}$

Here, $a * c = b \notin T_1 \cup T_2$

$\therefore T_1 \cup T_2$ is not closed under the binary operation.

$\therefore T_1 \cup T_2$ is not a subgroup of Klein-4 group.

Date : .....

2) Prove that $J = \{x \in G \mid xy = yx \text{ for } y \in G\}$ is a subgroup of G.

pf: We have $e \in G$

$\Rightarrow ey = ye \quad \forall y \in G$

$\Rightarrow e \in J$.

$\Rightarrow J$ is non-empty.

T.P.T: $\forall a, b \in J$, $ab \in J$.

Consider $(ab)y = a(by)$ ($\because a, b, y \in G$ & associative law holds)

$= a(yb)$ ($\because b \in J$)

$= (ay)b$ ($\because$ associative law)

$= (ya)b$ ($\because a \in J$)

$= y(ab)$ ($\because$ associative law)

$\Rightarrow ab \in J$.

T.P.T: $\forall a \in J$, $\bar{a}^1 \in J$.

we have for $y \in G$, $ay = ya$

$\Rightarrow \bar{a}^1(ay)\bar{a}^1 = \bar{a}^1(ya)\bar{a}^1$

$\Rightarrow (\bar{a}^1 a)(y\bar{a}^1) = (\bar{a}^1 y)(a\bar{a}^1)$

$\Rightarrow e(y\bar{a}^1) = (\bar{a}^1 y)e$ (inverse)

$\Rightarrow y\bar{a}^1 = \bar{a}^1 y$ (identity)

$\Rightarrow \bar{a}^1 \in J$

$\therefore J$ is a subgroup of G.

Date : .....

Note: J is also called the centre of G.

Integral powers of an element

Let G be a group under a binary operation $*$, with e as the identity element. For any $a \in G$, integral power is defined as follows.

$a^0 = e$, $a^1 = a$, $a^2 = a * a$, $a^3 = a^2 * a$

... $a^n = a^{n-1} * a$ for any $n \in Z^+$

$\bar{a}^1 = \bar{a}^1$ (inverse of a in G)

$\bar{a}^2 = \bar{a}^1 * \bar{a}^1$, $\bar{a}^3 = \bar{a}^2 * \bar{a}^1$, ... $\bar{a}^n = \bar{a}^{(n-1)} * \bar{a}^1$ for any $n \in Z^+$.

Note: Laws of indices holds for any element 'a' in a group.

i.e., $a^m * a^n = a^{m+n} = a^{n+m}$ =

i.e., $a^m * a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m$

$(a^m)^n = a^{mn} = a^{nm} = (a^n)^m$

Date : .....

Cyclic group: A group G is said to be cyclic if there exists an element $g \in G$ such that every element a of G is an "integral power" of g. Then the element g is called a generator of the group.

If G is cyclic group generated by g then, we write $G = \langle g \rangle$.

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

Soln let $a \in G \Rightarrow a = g^n$ for some $n \in Z$

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

$\Rightarrow a$ is an integral power of g^{-1}

$\Rightarrow g^{-1}$ is also a generator of G.

2) Show that $(W_4, \cdot)$, where $W_4 = \{1, -1, i, -i\}$ is cyclic group.

Soln Here, $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.

i.e., every $a \in W_4$ can be expressed as i^n for some $n \in Z$.

$\therefore (W_4, \cdot) = \langle i \rangle$.

3) Show that the group $(G, *)$ whose multiplication table (Cayley's table) is 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 By examining the table, we note that a is identity element in G.

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

$b^4 = b^3 * b = d * b = e$, $b^5 = b^4 * b = e * b = f$

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

Thus, every element of G is "an integral power" of b.

$\therefore (G, *) = \langle b \rangle$.

Note: Here, $b * f = f * b = a$ (identity)

$\Rightarrow f = b^{-1}$, which is also a generator of G.

Date : .....

4) Prove that $(Z_4, +)$ is cyclic. Find all its generators.

Sol^n $Z_4 = \{[0], [1], [2], [3]\}$ and the operation $+$ is "addition modulo 4". Consider the following Cayley's table.

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

Here, $[0]$ is identity element in $(Z_4, +)$. So, $[0]$ cannot be generator.

$[1]^1 = [1]$

$[1]^2 = [1] + [1] = [2]$

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

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

Thus, every element of Z_4 is an integral power of $[1]$.

$\therefore (Z_4, +) = \langle [1] \rangle$.

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

Date : .....

But, $[2]^n \neq [1]$ for any $n \in Z$,

$\Rightarrow$ $[2]$ cannot be generator.

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

Sol^n $Z_5^* = \{[1], [2], [3], [4]\}$ and the operation $\cdot$ in $(Z_5^*, \cdot)$ is "multiplication modulo 5". Consider the following Cayley's table.

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

Here, $[1]$ is identity element

$\Rightarrow$ $[1]$ cannot be generator of $(Z_5^*, \cdot)$.

$[2]^1 = [2]$

$[2]^2 = [2] \cdot [2] = [4]$

$[2]^3 = [2]^2 \cdot [2] = [4] \cdot [2] = [3]$

$[2]^4 = [2]^3 \cdot [2] = [3] \cdot [2] = [1]$.

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

Date : .....

Further, $[2]^{-1} = [3]$ $\Rightarrow$ $[3]$ is also generator of $(Z_5^*, \cdot)$.

But $[4]^n \neq [2]$ for any $n \in Z$.

$\therefore$ $[4]$ is not generator of $(Z_5^*, \cdot)$

6) Prove that the Klein-4 group is not cyclic.

Sol^n: In Klein-4 group, every element is its own inverse. Thus, for any x in the group, $x^2 = e$

$\Rightarrow$ $x^n = e$ if x is even

and $x^n = ex = x$ if x is odd.

$\Rightarrow$ every integral power of x is equal to e or x.

$\Rightarrow$ no element in this group can be a generator of the group.

$\therefore$ K_4 is not cyclic.

7) Every cyclic group is abelian, but the converse is not true.

Sol^n let G be a cyclic group and g be its generator.

Date : .....

T.P.T.: $ab = ba$, $\forall\, a, b \in G$.

now $a, b \in G \Rightarrow a = g^m$ and $b = g^n$ for some $m, n \in Z$.

consider, $ab = g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m = ba$

$\Rightarrow$ G is abelian.

we noted that Klein-4 group is abelian but not cyclic.

$\Rightarrow$ ~~G is abelian~~

$\Rightarrow$ An abelian group need not be cyclic.

8) Every subgroup of a cyclic group is cyclic.

Sol^n let $G = \langle g \rangle$ and H be a subgroup of G.

$\Rightarrow$ every element of H is in G and is an integral power of g.

let m be the smallest positive integer such that $g^m \in H$.

let $a \in H \Rightarrow a = g^n$ for some $n \in Z$.

$\Rightarrow$ $a = g^{mq+r}$, where $q, r \in Z$ with $0 \leq r < m$

$\Rightarrow$ $a = (g^m)^q * g^r$

Date : .....

since $g^m \in H$, $(g^m)^q \in H$ ($\because$ H is subgroup)
Also $a \in H \Rightarrow g^r \in H$.
But m is the smallest positive integer such that $g^m \in H$ & $r < m$, $g^r \in H$ is possible only if $r = 0$.

$\Rightarrow n = qm$

$\Rightarrow a = (g^m)^q$

i.e., every element a of H is an integral power of g^m. Hence, H is a cyclic group with g^m as a generator.

9) Prove that every element of a group G generates a cyclic group which is a subgroup of G.

Soln Let G be a group and 'a' be any element of G. Consider subset A of G defined by

$A = \{x \in G \mid a^n = x \text{ for some } n \in Z\}$

Here, A is non-empty ($\because a = a^1 \in A$).

T.P.T: $\forall x, y \in A$, $xy^{-1} \in A$
& xy^{-1} is an integral power of a.

now, $x, y \in A \Rightarrow x = a^m$ & $y = a^n$ for some $m, n \in Z$.

Date : .....

Consider, $xy^{-1} = a^m (a^n)^{-1} = a^m a^{-n} = a^{m-n}$

Thus A is a subgroup of G. since every element of A is an integral power of a, it follows that A is a cyclic subgroup of G.

Thus, every element a of G generates a cyclic group A which is a subgroup of G.

10) In the group $(W_4, \cdot)$, find the cyclic subgroups generated by -1 and -i.

Soln We have $W_4 = \{1, -1, i, -i\}$.

$(-1)^1 = -1$, $(-1)^2 = 1$

$\therefore \langle -1 \rangle = \{x \in W_4 \mid x = (-1)^n \text{ for } n \in Z\}$

$= \{1, -1\}$.

$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = +i$, $(-i)^4 = 1$

$\therefore \langle -i \rangle = \{x \in W_4 \mid x = (-i)^n \text{ for } n \in Z\}$

$= \{1, -1, i, -i\} = W_4$

$\therefore$ (illegible)

Date : .....

1) Find the cyclic subgroups generated by the elements [2] and [3] of the group $(Z_6, +)$.

Sol^n $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$

Here, + is "addition modulo 6".

$\langle [2] \rangle = \{x \in Z_6 \mid x = [2]^n, n \in Z\}$

$= \{x \in Z_6 \mid x = n[2], n \in Z\}$

$= \{[0], [2], [4]\}$

and $\langle [3] \rangle = \{x \in Z_6 \mid x = [3]^n, n \in Z\}$

$= \{x \in Z_6 \mid x = n[3], n \in Z\}$

$= \{[0], [3]\}$.

Left and Right coset of a group:

Let $(H, *)$ be a subgroup of the group $(G, *)$. For any $a \in H$,

$a * H = \{a * h \mid h \in H\}$

and $H * a = \{h * a \mid h \in H\}$.

Then, $a * H$ is called left coset of H w.r.t. a in G and $H * a$ is called right coset of H w.r.t. a in G.

Date : .....

Note: ① If there is no ambiguity we write aH for $a * H$ and Ha for $H * a$.

② The left cosets and right cosets of H are subsets of G.

③ $e * H = H * e = H$, where e is identity element in H.

④ $aH \neq Ha$, in general.

⑤ $aH = Ha$, if G is abelian.

Theorem 1: There exists a one-to-one correspondence between the elements of a subgroup and the elements of the left (right) coset thereof.

Pf: Let H be a subgroup of G and aH be a left coset of H w.r.t. $a \in G$. Define a function $f: H \to aH$ by

$f(h) = ah, \forall h \in H$.

For $h_1, h_2 \in H$, Consider

$f(h_1) = f(h_2)$

$\Rightarrow ah_1 = ah_2$

$\Rightarrow h_1 = h_2$ ($\because$ Cancellation laws)

Date : .....

let $y \in aH \Rightarrow y = ah_3$ for $h_3 \in H$.

$\Rightarrow y = f(h_3)$ for some $h_3 \in H$

$\therefore f$ is onto.

$\therefore f$ is 1-1 correspondence from H to aH.

Corollary: If H is a finit subgroup of G and $a \in G$, then $|H| = |aH| = |Ha|$

Theorem 2: Any two left (right) cosets of a subgroup H of a group G are either disjoint or identical.

Pf: let aH and bH be two left cosets of H in G.

T.P.T: $aH = bH$, whenever aH and bH are not disjoint.

suppose $aH \cap bH \neq \phi$

$\Rightarrow \exists$ atleast one element c such that $c \in aH$ and $c \in bH$.

so, $c = ah_1$ and $c = bh_2$ for some $h_1, h_2 \in H$.

$\Rightarrow ah_1 = bh_2$

$\Rightarrow a = (bh_2)h_1^{-1}$ (∵ cancellation law)

$= bh_2h_1^{-1}$ (∵ associative law)

Date : .....

Now consider $x \in aH$

$\Rightarrow x = ah_2$ for some $h \in H$

$\Rightarrow x = (bh_2h_1^{-1})h$

$\Rightarrow x = b(h_2h_1^{-1}h)$ (∵ associative law)

$\Rightarrow x = bh_3$, where $h_3 = h_2h_1^{-1}h \in H$

$\Rightarrow x \in bH$

$\therefore aH \subseteq bH$

Similarly, we can show $bH \subseteq aH$

$\therefore aH = bH$.

coset decomposition:

From the defn and properties of left and right cosets, we note that

(i) left (right) cosets are subsets of group

(ii) every element of the group belongs to atleast one left (right) coset.

(iii) every two left (right) cosets are either identical (or) disjoint.

Hence, every group G can be partitioned into mutually disjoint left (right)

Date : .....

cosets of subgroup H of G. This partitioning of G is called the left (right) coset decomposition of G w.r.t. H.

Note: left coset decomposition of G w.r.t. H = set of all mutually disjoint left cosets of subgroup H of G.

Problems: 1) For the group $G = (Z_{12}, +)$ and the subgroup $H = \{[0], [4], [8]\}$ of G, find all the left cosets of H in G. Also obtain the corresponding coset decomposition of G.

Sol: We have $Z_{12} = \{[0], [1], [2], \ldots [11]\}$.

left coset of given H w.r.t. $[a] \in Z_{12}$ is given by

$[a]+H = \{[a]+[h] \mid [h] \in H\}$

$= \{[a]+[0], [a]+[4], [a]+[8]\}$.

$[0]+H = \{[0]+[0], [0]+[4], [0]+[8]\}$

$= \{[0], [4], [8]\}$.

Date : .....

$[1]+H = \{[1], [5], [9]\}$.

$[2]+H = \{[2], [6], [10]\}$

$[3]+H = \{[3], [7], [11]\}$

$[4]+H = \{[4], [8], [0]\}$

$[5]+H = \{[5], [9], [1]\}$

$[6]+H = \{[6], [10], [2]\}$

$[7]+H = \{[7], [11], [3]\}$

$[8]+H = \{[8], [0], [4]\}$

$[9]+H = \{[9], [1], [5]\}$

$[10]+H = \{[10], [2], [6]\}$

$[11]+H = \{[11], [3], [7]\}$.

Here, we note that only first four are mutually disjoint.

$\therefore (Z_{12}, +) = ([0]+H) \cup ([1]+H) \cup ([2]+H) \cup ([3]+H)$.

2) Consider the group $(G, *)$ given below, compute the left cosets of all the elements of G w.r.t. the subgroup $H = \{a, c, e\}$ of G. Hence obtain a left coset decomposition of G w.r.t. H.

Date : .....

$*$	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 for $x \in G$, we know

$x*H = \{ x*h \mid h \in H \}$

$= \{ x*a, x*c, x*e \}$.

So, $a*H = \{ a*a, a*c, a*e \}$

$= \{ a, c, e \}$

$b*H = \{ b*a, b*c, b*e \} = \{ b, d, f \}$

$c*H = \{ c*a, c*c, c*e \} = \{ c, e, a \}$

$d*H = \{ d*a, d*c, d*e \} = \{ d, f, b \}$

$e*H = \{ e*a, e*c, e*e \} = \{ e, a, c \}$

$f*H = \{ f*a, f*c, f*e \} = \{ f, b, d \}$

$\therefore G = (a*H) \cup (b*H)$.

Date : .....

3) Consider the symmetric group S_3 and the subgroup $H = \{ p_0, p_5 \}$ thereof. Find all the right cosets of H in S_3 and hence obtain a right coset decomposition of S_3.

Soln $S_3 = \{ p_0, p_1, p_2, p_3, p_4, p_5 \}$.

$p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Right coset of H w.r.t. $x \in S_3$ is

$Hx = \{ hx \mid h \in H \} = \{ p_0 x, p_5 x \}$

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

$Hp_0 = H \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} = \{ p_0, p_5 \} = H$.

Date : .....

$$Hp_1 = H\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$= \left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right\} = \{p_1, p_3\}$$

$$Hp_2 = H\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$= \left\{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\} = \{p_2, p_4\}$$

$$Hp_3 = H\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$= \left\{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\} = \{p_2, p_4\}$$

$$Hp_3 = H\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$= \left\{\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\} = \{p_3, p_1\}$$

$$Hp_4 = H\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$= \left\{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\} = \{p_4, p_2\}$$

Date : .....

$$Hp_5 = H\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$= \left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\right\} = \{p_5, p_0\}$$

Here, H, Hp_1 and Hp_2 are distinct.

$\therefore S_3 = H \cup (Hp_1) \cup (Hp_2)$.

4) Let $G = S_4$, for $\alpha = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$, find the subgroup $H = \langle\alpha\rangle$. Determine the left cosets of H in G.

Sol^n:

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

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

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

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

Date : .....

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

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

$= e$, identity permutation.

$\therefore H = \{\alpha, \alpha^2, \alpha^3, \alpha^4 = e\}$.

left coset of H w.r.t. $x \in S_4$ is

$xH = \{xh \mid h \in H\}$

$= \{x\alpha, x\alpha^2, x\alpha^3, xe = x\}$.

So, ~~$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} H = H$~~.

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

We know $O(S_4) = 4! = 24$.

Here, we are listing out distinct left cosets of H in e.

Date : .....

So, $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} H = H$

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

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

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

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

Date : .....

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

Date : .....

Date : .....

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.

Pf: G is finite group.

$\Rightarrow$ H is finite.

$\Rightarrow$ Number of cosets of H in G is finite.

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

$\Rightarrow G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_r$

$\Rightarrow o(G) = o(Ha_1) + o(Ha_2) + \ldots + o(Ha_r)$

but $o(Ha_1) = o(Ha_2) = \ldots = o(Ha_r) = o(H)$

$\Rightarrow o(G) = \underbrace{o(H) + o(H) + \ldots + o(H)}_{r \text{ times}}$

$\Rightarrow o(G) = r\, o(H)$.

$\Rightarrow o(H)$ divides $o(G)$.

Problems

1) Let G be a group with subgroups H and K. If $|G| = 660$, $|K| = 66$ and $K \subset H \subset G$, what are the possible values for $|H|$?

Soln: By Lagrange's theorem, $o(H)$ divides $o(G)$ & $o(K)$ divides $o(H)$.

$\Rightarrow o(G) = o(H) q_1$ and $o(H) = o(K) q_2$ for some integer q_1, q_2.

$\Rightarrow 660 = o(H) q_1$ and $o(H) = 66 q_2$

$\Rightarrow 660 = 66 q_1 q_2$

$\Rightarrow q_1 q_2 = 10$

$\Rightarrow q_1 = 2$ and $q_2 = 5$ (or) $q_1 = 5$ and $q_2 = 2$.

Thus, $o(H) = 66 \times 5 = 330$ (or) $o(H) = 66 \times 2 = 132$.

2) Every group G of prime order is cyclic. Moreover, every $a (\neq e) \in G$ is a generator of G.

Soln: Let G be a group of order p, where p is prime number.

Since $p \geq 2$, G has atleast one element $a \neq e$.

Let $A = \langle a \rangle$.

$\Rightarrow o(A) > 1$.

Date : .....

By Lagrange's theorem, $o(A)$ must divide p.

Since p is prime, $o(A)$ must be p only.

Here, $A \subseteq G$ and $o(G) = p$,

so, $A = G$.

$\Rightarrow$ Cyclic group generated by a is G.

Thus, G is cyclic with $a \neq e$ as a generator.

Date : .....