Page No:
Date: / /

Module 5

Introduction to Group theory

The concept of Groups was introduced by Evariste Galois in the early 19^{th} century.
He developed this concept to describe the solvability of polynomial equations by the operations involving addition, subtraction, multiplication, division & extraction of roots.

Groups are important for computer science because (applications)

1. used in cryptographic algorithms (eg. RSA algorithm) to secure communication.
2. used in error detection and correction algorithms in data transmission.
3. used in computer graphics & vision to describe and recognize symmetries and patterns.

Definition: Group.

a b
$a+b$ $a\times b$

Let G be a non empty set and $*$ be a binary operation on G.
G is called a Group if the following conditions holds

(1) $a*b \in G$ for all $a, b \in G$ (G is closed under $*$)

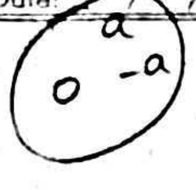
(2) $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$ (The associative property)

(3) There exists $e \in G$ with $a*e = e*a = a$ for all $a \in G$ (existence of identity)

e 1 0

$e \to$ identity element additive

(4) For each $a \in G$ there is an element $a' \in G$ such that $a * a' = a' * a = e$ of (existence of Inverse)



$a + (-a) = 0$

Note :- Group is denoted as G or $(G, *)$,

If $ab = ba$ for all $a, b \in G$ then G is called Commutative or abelian group.

(1) Show that fourth root of unity is an abelian group.

Soln:- let $W_4 = \{1, -1, i, -i\}$ be the set of all fourth root of unity.

The operation ~~table~~ $\times$ for the usual multiplication on W_4 is shown below

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

W_4

1 is identity for $\times$
0 is identity for $+$

From the table it is clear that W_4 is closed under $\times$. (i.e $\forall a, b \in W_4$, $a \times b \in W_4$)

Since $\times$ is associative in the set of complex numbers, it is associative in W_4. (i.e $\forall a, b, c \in W_4$, $(a \times b) \times c = a \times (b \times c)$)

1 is W_4 and is the identity element under $\times$.

Also every element of W_4 has an inverse under $\times$.

i.e Inverse of 1 is 1, $1^{-1} = 1$, $-1^{-1} = -1$, $i^{-1} = -i$, $-i^{-1} = i$

Lastly, we find that $\forall a, b \in W_4$, $ab = ba$

Hence W_4 is an abelian group under $\times$.

(2) 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 :- For any two non zero real numbers a, b we note that $\frac{1}{2}(ab)$ is also a non zero real number.

$\Rightarrow$ for any $a, b \in G$, $a*b \in G$ (G is closed under $*$)

For any $a, b, c \in G$, we have

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

$\because a*b = \frac{1}{2}ab$, $b*c = \frac{1}{2}bc$

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

Thus $*$ is associative.

For any $a \in G$, we have $a*2 = 2*a = \frac{1}{2}(2a) = a$

$\therefore$ 2 is the identity element under $*$, $2 \in G$.

For any $a \in G$, we set $a' = 4/a$ then $a' \in G$

$$\Rightarrow \quad a*a' = \frac{1}{2}(aa') = \frac{1}{2}\cdot 4 = 2 = \text{identity}$$
$$a'*a = \frac{1}{2}(a'a) = \frac{1}{2}\cdot 4 = 2 = \text{identity}$$

Thus very a in G has $a' = 4/a$ as the inverse in G

$\therefore$ The above facts show that $(G, *)$ is a group.

Further for any $a, b \in G$

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

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

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

Soln :- First, suppose that G is abelian, then for $a, b \in G$,

$$a^{-1} b^{-1} = b^{-1} a^{-1} \quad (\because ab = ba)$$

$$= (ab)^{-1} \quad \left| \because b^{-1}a^{-1} = (ab)^{-1} \text{ in a group} \right.$$

Conversely suppose that

$(ab)^{-1} = a^{-1} b^{-1}$ for any $a, b \in G$ then for any $x, y \in G$

$$xy = (x^{-1})^{-1} (y^{-1})^{-1} \quad \left| \because x = (x^{-1})^{-1},\ y = (y^{-1})^{-1} \right.$$

$$= (y^{-1} x^{-1})^{-1}$$

$$= (y^{-1})^{-1} (x^{-1})^{-1} \quad \left| \because a^{-1} b^{-1} = (ba)^{-1} \right.$$

$$xy = yx$$

$\therefore$ G is abelian group.

(4) Show that i) the identity element of G is unique.
ii) the inverse of each element of G is unique.

Sol: (i) Suppose e_1 and e_2 are identity elements in a group G.

Since e_1 is an identity element of G $\Rightarrow$ $ae_1 = e_1 a = a$, $\forall a \in G$

This is true for $a = e_2$ because $e_2 \in G$.

i.e $e_2 e_1 = e_1 e_2 = e_2$

Similarly, e_2 is an identity element of G, it shows that
$$e_1 e_2 = e_2 e_1 = e_1$$

Thus $e_1 = e_1 e_2 = e_2 e_1 = e_2$

This shows that e_1 & e_2 are same. So, G has only one identity element.

(ii)
Let e be the identity element in G. Suppose a' and a'' are inverses of an element $a \in G$.

Then
$$
\begin{aligned}
a' &= a'e && (\because x = xe \text{ for } \forall x \in G) \\
&= a'(aa'') && (\because a'' \text{ is an inverse of } a) \\
&= (a'a)a'' && (\text{associativity}) \\
&= e a'' && (\because a' \text{ is an inverse of } a)
\end{aligned}
$$
$$a' = a''$$

Thus a' & a'' are same.

$\therefore$ Every element has a unique inverse in G

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

Soln: when $a \neq -1$ and $b \neq -1$, we note that $a + b + ab \neq -1$

Therefore, $\cdot$ is a binary operation on G.

$\because a \cdot b = a+b+ab$

For any $a, b, c \in G$, we have

$$a*(b*c) = a*(b+c+bc)$$
$$= \{a+(b+c+bc)\} + a(b+c+bc)$$
$$= a+b+c+bc+ab+ac+abc$$
$$= (a+b+ab) + c + bc+ac+abc$$
$$= (a+b+ab) + c + (a+b+ab)c$$
$$a \cdot (b \cdot c) = (a*b) \cdot c \qquad \therefore \cdot \text{ is associative}$$

For any $a \in G$, we have $a*0 = a+0 + a\times 0$
$$= a$$
$$= 0+a+0\times a$$
$$a \cdot 0 = 0 \cdot a$$

Thus, 0 is the identity in G under.

For any $a \in G$, if we put $a' = \frac{-a}{1+a}$ then $a' \in G$

$$a*a' = a+a'+aa'$$
$$= a - \frac{a}{1+a} - \frac{a^2}{1+a}$$
$$= \frac{\cancel{a}+\cancel{a^2}-\cancel{a}-\cancel{a^2}}{1+a} = 0 = a' * a$$

Thus, $a' = \frac{-a}{1+a} \in G$ is the inverse of 'a' under.

Also $ab = a+b+ab = ba$

$\therefore \cdot$ is commutative.

$\therefore (G, \cdot)$ is abelian Group.

Cyclic Group

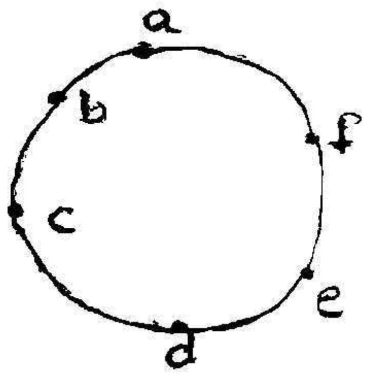
A cyclic group is a group that can be generated by a single element, called the generator.
Denoted by $\langle g \rangle$. Every element of a in G is of the form g^n for some integer n.
If g is a generator of a cyclic group G, we say that g generates G.

eg: The group $(W_4, \cdot)$ and $W_4 = \{1, -1, i, -i\}$. In this group we notice that $1 = i^0$, $-1 = i^2$, $i = i^1$, $-i = i^3$

Thus, every element of the group is an integral power of the element i.
Hence this group W_4 is cyclic & i is a generator.
i.e $(W_4, \cdot) \equiv \langle i \rangle$

(1) Show that $(G, *)$ whose multiplication 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



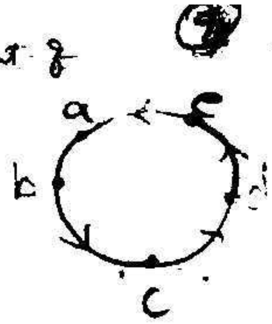
Soln: From the table, we note that
For all $a, b \in G$, $a * b \in A$ $\therefore$ G is closed under $*$.
For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$
$\therefore$ $*$ is associative in G.
The identity element a is in G.
Every element of G has an inverse under $*$.
$b^{-1} = f$, $c^{-1} = e$, $d^{-1} = d$ $e^{-1} = c$, $f^{-1} = b$

In addition to this, we have every element of G is of the form b^n for $n = 1, 2, 3, 4, 5, 6$

i.e. $b^2 = b * b = c$, $b^3 = b^2 * b = c * b = d$

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

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



b is the generator of G.

similarly f is also generator of G

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

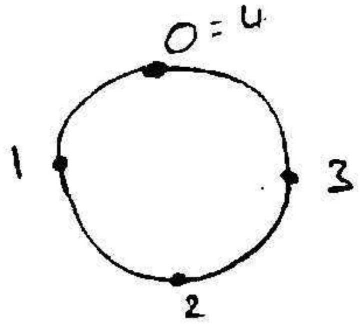
---

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

Soln :- $(Z_4, +)$ is "addition modulo 4".

Elements of Z_4 are $0 = 4, 1, 2, 3$.

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



From the table it is clear that Z_4 is closed under +.

i.e for $\forall$, $a, b \in Z_4$, $a + b \in Z_4$

we note that $\forall\, a, b, c \in Z_4$, $(a+b)+c = a+(b+c)$

$\therefore$ + is associative in Z_4

In Z_4, 0 is the identity element under the operation +.

Also, we note that inverse of 1 is 3 i.e $1^{-1} = 3$, $2^{-1} = 2$, $3^{-1} = 2$

Every element of Z_4 has an inverse under +.

$\therefore$ $(Z_4, +)$ is a group.

Every element of Z_4 is an integral power of 1

i.e $1 = 1$, $2 = 1+1 = [1]^2$ $3 = 1+1+1 = [1]^3$

$4 = 0 = 1+1+1+1 = [1]^4$. 1 is a generator.

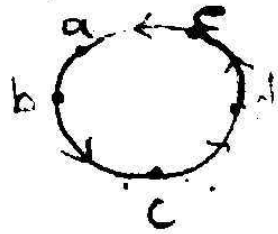
$\therefore$ $(Z_4, +)$ is cyclic.

In addition to this, we have every element of G is of the form b^n for $n = 1, 2, 3, 4, 5, 6$

i.e $b^2 = b * b = c$, $b^3 = b^2 * b = c * b = d$

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

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



b is the generator of G.

similarly f is also generator of G

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

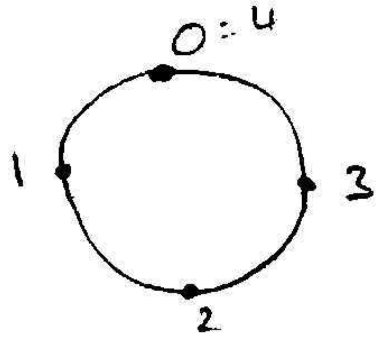
---

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

Soln: $(Z_4, +)$ is "addition modulo 4".

Elements of Z_4 are $0 = 4, 1, 2, 3$.

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



From the table it is clear that Z_4 is closed under $+$.

i.e for $\forall\, a, b \in Z_4$, $a + b \in Z_4$

we note that $\forall\, a, b, c \in Z_4$, $(a+b)+c = a+(b+c)$

$\therefore$ $+$ is associative in Z_4

In Z_4, 0 is the identity element under the operation $+$.

Also, we note that inverse of 1 is 3 i.e $1^{-1} = 3$, $2^{-1} = 2$, $3^{-1} = 2$

Every element of Z_4 has an inverse under $+$.

$\therefore (Z_4, +)$ is a group.

Every element of Z_4 is an integral power of 1

i.e $1 = 1$, $2 = 1+1 = [1]^2$ $3 = 1+1+1 = [1]^3$

$4 = 0 = 1+1+1+1 = [1]^4$. 1 is a generator.

$\therefore (Z_4, +)$ is cyclic.

$\langle 1 \rangle = \{1, 2, 3, 0\}$ | $1+1=2,\ 2+1=3,\ 3+1=4=0$ (9)
$4+1=5=1$

Page No
Date

$\langle 2 \rangle = \{2, 0\}$ | $2+2=4=0$

$\langle 3 \rangle = \{3, 2, 1, 0\}$ | $3+3=6=2,\ 6+3=9=1,\ 9+3=12=0$

$\langle 0 \rangle = \langle 4 \rangle = \{0\}$

$\therefore \langle 1 \rangle$ & $\langle 3 \rangle$ are generator's of group $(Z_4, +)$

i.e 1 & 3 generates all the elements of $(Z_4, +)$.

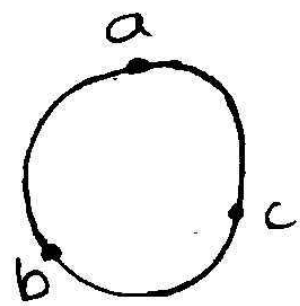
The Klein 4-Group

The group G is said to be Klein 4-group if G is abelian and each element of G has self inverse. It contains three elements and an identity element e.

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

Soln: Consider $A = \{e, a, b, c\}$. On this set, we define a binary operation as follows. (Here e is identity element).

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



From the table, we note that

For all $a, b \in A$, $a \cdot b \in A$ $\therefore$ A is closed under $\cdot$

For all $a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$\therefore \cdot$ is associative in A

The identity element e is in A.
Also every element of A has an inverse under.
i.e Inverse of a is a, $a^{-1}=a$, $b^{-1}=b$, $c^{-1}=c$.

we find that $\forall\, a,b \in A$, $ab=ba$

Hence A is an abelian group under the operation.
we observe that e is the identity element in the group and every element is its own inverse.

$\therefore (A,\cdot)$ is a klein 4 group.

Note :- (1) Additive group of modulo n is denoted by $(Z_n \oplus_n)$

eg: For $n=6$, $[3]\oplus_6[2]=[3+2]=[5]$
$[5]\oplus_6[3]=[5+3]=[8]=[2]$
$[8]\oplus_6[4]=[8+4]=[12]=[0]$

The operation table $(Z_6,+)$

+	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

(2) Multiplicative group of Integers mod p is denoted by $(Z_p^*, \otimes_p)$

eg: For $n=7$, $[2]\otimes_7[3]=[2\times3]=[6]$
$[4]\otimes_7[3]=[4\times3]=[12]=[5]$
$[5]\otimes_7[3]=[5\times3]=[15]=[1]$
$[5]\otimes_7[6]=[5\times6]=[30]=[2]$

The operation table $(Z_7^*, \cdot)$ or $(Z_7^*, \times)$

$\cdot$	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

Permutation groups

Consider a set $A = \{1, 2, 3\}$. The elements can be permuted (rearranged) in $3!$ ways. i.e $3! = 6$

123, 231, 312, 132, 321, 213.

The six permutations of the set $A = \{1, 2, 3\}$ are represented as shown below:

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Subgroups

A nonempty subset H of a group G is called a subgroup of G whenever H itself is a group under the binary operation in G. Denoted by $H \leq G$.

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

Note: Every group is subgroup of itself.

Page No.
Date: / /

Coset decomposition of a group

Let $(G, *)$ be a group and $(H; *)$ be a subgroup of G.

For any $a \in G$, let $a * H = \{a*h \mid h \in H\}$

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

Then $a*H$ is called Left coset of H wrt a.

$H*a$ is called Right coset of H wrt a.

(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 (left coset) decomposition of G.

Soln:- $Z_{12} = \{[0]\ [1]\ [2] \ldots [11]\}$

Left cosets of H wrt $a \in Z_{12}$ is

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

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

For $[a] = [0]\ [1]\ [2]\ [3] \ldots [11]$, left cosets of H are

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

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

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

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

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

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

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

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

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

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

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

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

we note that out of 12 left cosets listed above, only four are mutually disjoint, they are [0] [1] [2] [3]. others are identical with these.

$\therefore$ The Left coset decomposition of $(Z_{12}, +)$ wrt H is $(Z_{12}, +) = ([0]+H) \cup ([1]+H) \cup ([2]+H) \cup ([3]+H)$

Note: ① The Symmetric group that consists of all permutations of set of n elements, denoted by S_n.

② suppose $H \subseteq G$ and if $|G| = 4! = 24$ and $|H| = 4$ then there are $\frac{24}{4} = 6$ left cosets of H in G.

② 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 leftcosets of H in G.

Sol: Given $G = S_4$, a symmetric group of order 4

$$\langle \alpha \rangle = H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Since $H \subseteq G = S_4$ & $|G| = 4! = 24$ and $|H| = 4$ then there are $\frac{24}{4} = 6$ left cosets of H in G.

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

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

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

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

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

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

(3) If H is a Subgroup of the finite group then for all $a \in G$ then prove that $aH = H$

Sol: Since $aH = \{ah / h \in H\}$ it follows that $|aH| \leq |H|$. If $|aH| = |H|$ and we have $ah_i = ah_j$ with $h_i\ h_j$ distinct elements of H. By left cancellation in G, we then get a contradiction $h_i = h_j$ so $|aH| = |H|$.

Lagrange's Theorem

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

proof : Since G is a finite group, H is also finite. $\therefore$ No. of cosets of H in G is finite.

Let $Ha_1, Ha_2 --- Ha_r$ be the distinct right cosets of H in G. Then by right coset decomposition of G we have

$$G = Ha_1 \cup Ha_2 \cup Ha_3 \cup --- \cup Ha_r$$

So that $O(G) = O(Ha_1) + O(Ha_2) + --- + O(Ha_r)$

But $o(Ha_1) = o(Ha_2) = - - - - - = o(Ha_r) = o(H)$

Therefore, $o(G) = o(H) + o(H) + o(H) + - - - + o(H)$ (r terms)

$$o(G) = r[o(H)] \Rightarrow \frac{o(G)}{o(H)} = r$$

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

(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, $|H|$ must divide $|G| = 660$ and $|K| = 66$ must divide $|H|$.

Also we have $|G| \neq |H| \neq |K|$. Therefore, $660 = |H| q_1$ for some integer $q_1 > 1$ and $|H| = 66 q_2$ for some integer $q_2 > 1$

Hence $660 = 66 q_1 q_2$ (or) $q_1 q_2 = 10$.

Thus, either $q_1 = 2$ and $q_2 = 5$ (or) $q_1 = 5$ and $q_2 = 2$

Thus $|H| = 66 \times 5 = 330$ (or) $|H| = 66 \times 2 = 132$

(2) P.T If G is a finite group of order n and $a \in G$ then $a^n = e$

Soln:- Let $o(a) = m$. Then $a^m = e$ and WKT if G is finite then $o(a)$ divides $o(G)$ $\Rightarrow$ m divides $o(G)$.

i.e $n = km$. where k is a positive integer

Hence $a^n = a^{km} = (a^m)^k = e^k = e$

(3) If H, K are Subgroups of a group G prove that $H \cap K$ is also Subgroup of G.

Is $H \cup K$ is a Subgroup of G?

Soln: Let G be a group and H, K are Subgroups of G.

Take any $a, b \in H \cap K$. Then $a, b \in H$ & $a, b \in K$.

$\therefore ab^{-1} \in H$ and $ab^{-1} \in K$. ($\because$ If $H \leq G$, $a, b \in H \Rightarrow ab \in H$ & $a^{-1} \in H$)

$\Rightarrow ab^{-1} \in H \cap K$ ($\because$ If $H, K \leq G$ & $a, b \in H, K \Rightarrow ab^{-1} \in H, K$)

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

Now consider the Symmetric group S_3 and two of its Subgroups $H = \{P_0, P_3\}$ and $K = \{P_0, P_4\}$. Then $H \cup K = \{P_0, P_3, P_4\}$.

From multiplication table for S_3, we find that $P_3 P_4 = P_1$. But $P_1 \notin H \cup K$.

$\therefore H \cup K$ is not closed under product of permutations, and consequently cannot be a group.

$\therefore H \cup K$ is not a group. (Union of two groups need not be a group)

(4) Prove that, H is a Subgroup of G if and only if for all $a, b \in H$, we have $ab^{-1} \in H$.

Soln:- Suppose, H is Subgroup of G. Then H itself is a group.

Take any $a, b \in H$ then $b^{-1} \in H$ and so $ab^{-1} \in H$.

Conversely, if $\forall a, b \in H$ then $ab^{-1} \in H$ holds.

$\Rightarrow aa^{-1} \in H$ (taking $b = a$). Thus $e \in H$. The same condition applied to e and a yields $ea^{-1} \in H$ when $a \in H$.

Thus $a^{-1} \in H$ for every $a \in H$. Since $b \in H$, we have $b^{-1} \in H$. Therefore $a(b^{-1})^{-1} \in H$ i.e. $ab \in H$. Thus H is closed under the binary operation of G. Associative law also holds for all elements of $H \subseteq G$.

$\therefore H$ is Subgroup of G.