Permutation and Symmetric group of order 3

A one-one, onto mapping of a finite set onto itself is called permutation and the number of elements in the set is called the degree of permutation.

Consider a set $S=\{a,b,c\}$ of three distinct elements. Let f be a one-one onto mapping from S onto itself. Then f is called a permutation.

Suppose $f(a)=b$, $f(b)=a$, $f(c)=c$. This permutation is denoted by two line notation. In this notation we write the elements of S in the first row and under each element of the first row, we put down its images under the mapping f. Thus f is denoted by $f=\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$

Let $S=\{1,2,3\}$. There are $3!$ different ways of arranging the elements of S. Thus the total number of distinct one-one and onto functions which can be defined on S is $3!=6$. That is the total number of distinct permutations of order 3 is 6.

All the 6 distinct permutations of order 3 for the set $S=\{1,2,3\}$ are as follows.

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

Note: The permutations $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ is same as the permutation $\begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}$ because the mapping is same in both the cases.

Equality of two permutations

Two permutations f and g of degree 3 on the set $S=\{1,2,3\}$ are said to be equal if $f(x)=g(x)\ \forall\ x\in S$.

$f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ and $g=\begin{pmatrix}2&1&3\\1&3&2\end{pmatrix}$ are equal as $f(1)=g(1)=3$, $f(2)=g(2)=1$, $f(3)=g(3)=2$.

Identity permutation

The identity mapping I on the set $S=\{1,2,3\}$ onto itself is called the identity permutation of degree 3. ie, $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ is the identity permutation of order 3.

Product or Composition of two permutations

Given two permutations of same order, they can be combined by means of composition of two functions. This is called the product of two permutations.

Let $f=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ be two permutations of degree 3. fog is the product of permutations f and g such that

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

$fog(2)=f(g(2))=f(1)=2$ Thus $fog=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

$fog(3)=f(g(3))=f(2)=3$.

i.e., $f=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

Also fog can be found as: $g:\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $f:\ 3\ 1\ 2$ $\therefore fog=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

Similarly gof can be found as: $f:\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $g:\ 2\ 3\ 1$ $\therefore gof=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

Observe that $fog\neq gof$.

Inverse of a permutation

Consider a permutation $f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ of degree 3 on the set $S=\{1,2,3\}$.

Since f is a one-one onto mapping from the set S onto S, the inverse of f exists and it is

$$f^{-1}=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix} \text{ or } = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

Further f^{-1} is a permutation of degree 3.

The inverse permutation f^{-1} is written by interchanging the rows and writing in an order.

Further, $f\circ f^{-1}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=I$, the identity permutation

Also $f^{-1}\circ f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=I$.

S_3 – the set of all permutations of degree 3.

Let $S=\{1,2,3\}$. The number of permutations of degree 3 are 6 and these are:

$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $f=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $g=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $h=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $i=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $j=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

Thus $S_3=\{e,f,g,h,i,j\}$

Theorem: The set S_3 of all permutations of degree 3, is a finite non-abelian group of order 6, under the product of permutations.

Symmetric group of degree 3

The group S_3 of all permutations of degree 3 is called the symmetric group of degree 3.

Examples.

1. If $f=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ are two elements of S_3, find fog^{-1}, gof^{-1}.

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

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

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

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

2. If $f=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $g=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ and $h=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, in S_3 find $fogoh$ and $hogof$.

Soln Given

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

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

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

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

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

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

Exercise.

1. If $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ is an element of S_3 find g^{-1}.

2. If $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ are in S_3, find (i) $f \circ f$ and (ii) $g \circ g$.

3. In the symmetric group of S_3 of $S = \{a, b, c\}$, $f^{-1} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, $g = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$.

Find (i) $f \circ g$, (ii) $g \circ f$, (iii) $f \circ g^{-1}$.

Integral powers of an element of a group.

Let a be an element of a group G. Then for every integer n, by the element a^n, we mean,

(i) $a^n = a.a.a.\ldots.a$, n times, if n is positive integer.

(ii) $a^{-n} = (a^n)^{-1}$, i.e., a^{-n} is the inverse of a^n.

(iii) $a^0 = e$, the identity element of G.

Note: If the group operation is denoted by $+$, then we write (i) $a+a+\ldots+a$ by na instead of a^n (n is positive integer)

(ii) $(-n)a = -na$

(iii) $0.a = 0$, the identity element of a group.

Eg: In $(Z_5^*, \times_5)$, where $Z_5^* = \{1,2,3,4\}$

$3^4 = 3 \times_5 3 \times_5 3 \times_5 3 = 1$.

In $(Z_4, +_4)$, where $Z_4 = \{0,1,2,3\}$

$6(3) = 3 +_4 3 +_4 3 +_4 3 +_4 3 +_4 3 = 2$,

here $3 \in Z_4$ and 6 is the integer by which times the element 3 is composed with itself.

Order of an element

The order of an element a of a group G, is the least positive integer m such that $a^m = e$. If there exists no such integer for which $a^m = e$, we say the element a is of infinite order.

The order of an element a is denoted by $O(a)$, read as order of a.

Note: 1. For any group, the identity element is the only element of order 1.

2. If for $a \in G$, where G is a group, $a^m = e$, for some positive integer n, then $O(a) \leq n$.

3. If $O(a) \geq n$, then $a^m \neq e$ for $0 < m < n$.

Examples

1. Find the orders of the elements of the multiplicative group $G = \{1, -1, i, -i\}$ of fourth root of unity

Sol^n. Since 1 is the identity element, $O(1) = 1$.

$(-1)^2 = 1 \quad \therefore O(-1) = 2$.

$i^4 = 1 \quad \therefore O(i) = 4$

$-i^4 = 1 \quad \therefore O(-i) = 4$

2. Find the orders of the elements of the multiplicative group $G = \{1, \omega, \omega^2\}$ of cube roots of unity. [where $\omega = (-1 + i\sqrt{3})/2$]

Sol^n Since 1 is the identity element $O(1) = 1$.

$\omega^3 = 1 \quad \therefore O(\omega) = 3$

$(\omega^2)^3 = 1 \quad \therefore O(\omega^2) = 3$

3. Find the orders of the elements of the group.

$G = \langle Z_4, +_4 \rangle$.

Sol^n $Z_4 = \{0, 1, 2, 3\}$.

since 0 is the identity element $O(0) = 1$

$4(1) = 1 +_4 1 +_4 1 +_4 1 = 0 \quad \therefore O(1) = 4$

$2(2) = 2 +_4 2 = 0 \quad \therefore O(2) = 2$

$4(3) = 3 +_4 3 +_4 3 +_4 3 = 0 \quad \therefore O(3) = 4$

Note:

1. In the group $\langle Z, + \rangle$ of integers, every element except identity 0, is of infinite order.
2. In the multiplicative group of positive rational numbers, every element except the identity element 1, is of the infinite order.

Properties related to order of an element of a group

1. In a group G, $O(a) = O(a^{-1})$, for every $a \in G$.
2. If a is an element of the group G, is of order n, then $a^m = e$, for any integer m, if and only if n dives m.
3. If a and x be any two elements of the group G, then $O(a) = O(xax^{-1})$.
4. In a group G, $O(ab) = O(ba)$, $\forall\ a, b \in G$.
5. In a group G, the order of any element a cannot exceed that of the group. That is $O(a) \leq O(G)$.
6. Let G be a group and $a \in G$. If $O(a) = n$ and $(m, n) = 1$, then $O(a^m) = n$.
7. The order of any power of an element of a group cannot exceed the order of the element. ie, $O(a^k) \leq O(a)$.
8. If $O(a) = n$, where a is an element of the group G and $d = (n, m)$ then $O(a^m) = \frac{n}{d}$.

Examples

1. Give an example of a group to show that $O(ab)$ need not be equal to $O(a).O(b)$.

Sol: Consider the group $G = \{1, -1, i, -i\}$ of fourth roots of unity under multiplication.

$\because (-1)^2 = 1 \Rightarrow O(-1) = 2$ and $\because (-i)^4 = 1 \Rightarrow O(-i) = 4$.

Now $(-1).(-i) = i$ and $\because i^4 = 1 \Rightarrow O[(-1)(-i)] = 4$.

But $O(-1).O(-i) = 2 \cdot 4 = 8$

Thus $O[(-1)(-i)] \neq O(-1).O(-i)$.

2. Let a, b be two elements of a group G such that $ab = ba$. If $O(a)$ and $O(b)$ are relatively prime, show that $O(ab) = O(a).O(b)$.

Sol^n Let $O(a) = n$ and $O(b) = m$

Thus $a^n = e$ and $b^m = e$.

Also $(m, n) = 1$.

Now, $(ab)^{mn} = (ba)^{mn}$ $[\because ab = ba]$

$= a^{mn} . b^{mn}$

$= (a^n)^m . (b^m)^n$

$= e^m . e^n$

$= e$

$\Rightarrow O(ab)$ is finite and $\leq mn$.

Let $O(ab) = l$. Then $l \leq mn$ and $l \mid mn$ — (1)

Now $(ab)^l = e \Rightarrow (ba)^l = e$ $[\because ab = ba]$

$\Rightarrow a^l b^l = e$

$\Rightarrow a^l = b^{-l}$.

Now $a^{lm} = (a^l)^m = (b^{-l})^m = (b^m)^{-l} = e^{-l} = e \Rightarrow n \mid lm$

Now $(m, n) = 1$ and $n \mid lm \Rightarrow n \mid l$.

Similarly $m \mid l$. Thus $mn \mid l$ — (2)

From (1) & (2) $l = mn$

$\therefore O(ab) = O(a).O(b)$.

Cyclic Groups

If G is a group and $a \in G$, the subset $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is known as the cyclic subgroup of G generated by the element a. In this subgroup for every element $b \in H$, there exists an integer $m \in \mathbb{Z}$, such that $b = a^m$.

That is every element of H can be expressed as an integral power of a. For this reason, H is called the "subgroup generated by a".

If this property of expressing every element as an integral power of a single element, say a, holds good for the whole group, then such group is called a cyclic group generated by the element a.

A group G is said to be a cyclic group generated by the element $a \in G$ if $G = \{a^n \mid n \in \mathbb{Z}\}$ and is denoted by $G = \langle a \rangle$.

Note:

1. If the binary operation for the cyclic group $G = \langle a \rangle$ is $+$, then every element of G is of the form na for some $n \in \mathbb{Z}$.
2. A cyclic group may have more than one generator.
3. A cyclic group is said to be finite cyclic group, if the group is finite, otherwise it is said to be infinite cyclic group.

Examples

1. Show that the multiplicative group of fourth roots of unity is a cyclic group.

Sol^n $G_1 = \{1, -1, i, -i\}$

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

Therefore i is a generator of G_1.

Thus G_1 is a cyclic group generated by the element i.

The element $-i$ is another generator of G_1.

2. Show that the group $\langle Z_5, +_5 \rangle$ is a cyclic group and every non zero element of Z_5 is a generator.

Sol^n $Z_5 = \{0, 1, 2, 3, 4\}$.

Consider $4 \in Z_5$ $\quad 4 = 1.4$

$$4 +_5 4 = 3 \Rightarrow 3 = 2.4$$

$$4 +_5 4 +_5 4 = 2 \Rightarrow 2 = 3.4$$

$$4 +_5 4 +_5 4 +_5 4 = 1 \Rightarrow 1 = 4.4$$

$$4 +_5 4 +_5 4 +_5 4 +_5 4 = 0 \Rightarrow 0 = 0.4$$

Thus every element of Z_5 can be expressed as some integral multiple of the element $4 \in Z_5$.

Therefore Z_5 is a cyclic group with 4 as a generator.

Similarly, one can verify other non zero element of Z_5 is also a generator.

Note

1. $\langle Z, + \rangle$ is an infinite cyclic group with 1 as a generator.
2. $\langle Z_n, +_n \rangle$ is a finite cyclic group with 1 as a generator.
3. $\langle Q, + \rangle$ is not a cyclic group.

[Let $\langle Q, + \rangle$ be a cyclic group generated by $m \in Q$.

Then $m = \frac{p}{q}$, $p, q \in Z$, $q \neq 0$.

Let $\frac{1}{2q} \in Q \Rightarrow \frac{1}{2q} = n.m$, $n \in Z \Rightarrow \frac{1}{2q} = n.\frac{p}{q} \Rightarrow \frac{1}{2} = n.p$.

It is impossible as the product of two integers is not equal to a fraction. Thus $\langle Q, + \rangle$ is not cyclic].

Properties of Cyclic Groups.

Theorem 1:

Every cyclic group is abelian.

Proof: Let G be a cyclic group with a as a generator.

Thus $G = \langle a \rangle = \{a^n / n \in Z\}$.

Let $x, y \in G$ be arbitrary.

Then there exists two integers m and n, such that

$$x = a^m \text{ and } y = a^n.$$

Consider $x \cdot y = a^m \cdot a^n$

$\Rightarrow x \cdot y = a^{m+n}$

$\Rightarrow x \cdot y = a^{n+m}$

$\Rightarrow x \cdot y = a^n \cdot a^m$

$\Rightarrow x \cdot y = y \cdot x$

Hence G is abelian.

Note: The converse of the above theorem is not true. That is every abelian group is not necessarily cyclic.

Consider $G = \{v_1, v_2, v_3, v_4\}$ and the associative binary composition $*$, given by the following table.

$*$	v_1	v_2	v_3	v_4
v_1	v_1	v_2	v_3	v_4
v_2	v_2	v_1	v_4	v_3
v_3	v_3	v_4	v_1	v_2
v_4	v_4	v_3	v_2	v_1

(i) v_1 is the identity element, since $v_1 * v_i = v_i = v_i * v_1 \quad \forall v_i \in G$.

(ii) $v_1^{-1} = v_1$, $v_2^{-1} = v_2$, $v_3^{-1} = v_3$, $v_4^{-1} = v_4$. Each element is inverse of itself.

(iii) The table is symmetric, Hence G is commutative.

Hence G is an abelian group.

This group $\langle G, * \rangle$ is known as the Klein's 4 group.

Here: $\langle v_1 \rangle = \{v_1\}$, $\langle v_2 \rangle = \{v_1, v_2\}$, $\langle v_3 \rangle = \{v_1, v_3\}$, $\langle v_4 \rangle = \{v_1, v_4\}$

Thus no element of G, generates the whole group G.

Hence G is not cyclic.

Theorem 2:
If a is a generator of a cyclic group G, then a^{-1} is also a generator.

Theorem 3:
If a is a generator of a cyclic group G, then $O(a) = O(G)$.

Theorem 4:
If G is a finite group of order n, containing an element of order n, then G is cyclic.

Theorem 5:
Let G be a cyclic group of order k and a be a generator. If $a^m = a^n (m \neq n)$, then $m \equiv n \pmod{k}$ and conversely.

Theorem 6:
Let G be a cyclic group of order d and a be a generator. The element $a^k (k < d)$ is also a generator of G, if and only if $(k, d) = 1$.

Theorem 7:
Every ~~cyclic~~ subgroup of a cyclic group is cyclic.

* Let d be any positive integer. The number of positive integers less than d and prime to d, is denoted by $\phi(d)$.
Any integer n can be decomposed into product of prime factors. i.e., $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, where $p_1, p_2 \ldots$ are prime factors
Then $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

Theorem 8:
A cyclic group of order d has $\phi(d)$ generators.

Examples

1. Find the number of generators of the cyclic group of order 60.

Sol^n: Given $O(G)=60$

and $60 = 2^2 \times 3 \times 5$

$\therefore \varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16$.

Thus G has 16 generators.

2. How many generators are there for the cyclic group of order 10. If a is a generator, what are the other generators?

Sol^n $10 = 2\times 5 \Rightarrow \varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 4$.

Thus there are 4 generators.

By data a is a generator. The other generators are of the form a^k, with $(k,10)=1$.

Hence $k=1,3,7,9$. Thus the generators are a, a^3, a^7, a^9.

Note:

If the group operation is in addition form, and a is one of the generator, then other generators are of the form $k\cdot 1$ with $(k,n)=1$, where $O(G)=n$.

3. Find the number of generators of the cyclic group $(Z_{18}, +_{18})$. Write all the generators.

Sol^n $O(Z_{18})=18$ and $18 = 2\times 3^2 \Rightarrow \varphi(18) = 18\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=6$

Thus there are 6 generators.

We know that 1 is a generators.

$(k,18)=1 \Rightarrow k=1,5,7,11,13,17$.

Thus the generators are 1, 5, 7, 11, 13 and 17.

Coset Decomposition of a group.

Let $\langle G, * \rangle$ be a group and H be a subgroup of G. For $a, b \in G$ "a is said to be congruent to b modulo H" or aRb, if and only if $a.b^{-1} \in H$.

If a is congruent to b mod H, then we write $a \equiv b (\text{mod } H)$

The relation $a \equiv b (\text{mod } H)$ is an equivalence relation. Hence this relation gives a partition of G, into disjoint classes. Each member in the partition is a non-empty subset of G and any two distinct members of the the partition are disjoint.

If $a \in G$, we denote the equivalent class generated by a by $[a]$. i.e., $[a] = \{x \in G \mid x \equiv a (\text{mod } H)\}$

$= \{x \in G \mid x a^{-1} \in H\}$

Cosets of a subgroup H in a group G

Let H be a subgroup of a group $\langle G, * \rangle$ and a be any element of G.

The set Ha defined by $Ha = \{ha \mid h \in H\}$ is called the right coset of H in G w.r.t. a.

The set aH defined by $aH = \{ah \mid h \in H\}$ is called the left coset of H in G w.r.t. a.

Note

1. $Ha \neq \phi$ [$\because e \in H$ and $e.a = a \in Ha$]

   $aH \neq \phi$ [$\because e \in H$ and $a.e = a \in aH$]

2. $He = \{he \mid h \in H\} = \{h \mid h \in H\} = H$

   Similarly $eH = H$, and $He = H$.

   Thus every subgroup H itself is a right coset and as well left coset of H in G.

3. If G is abelian, then every right coset Ha is equal to corresponding left coset aH.

   i.e., if G is abelian $Ha = aH$. But in general $Ha \neq aH$

Results related to Cosets.

1. If H is a subgroup of a group G, then for all $a \in G$, $[a] = Ha$.

2. From the above theorem, we have $\forall a \in G$, $Ha = [a]$. Thus any two distinct cosets of H in G are disjoint and the union of all the right cosets of H is whole of G. In other words the collection of all distinct right cosets of H in G form a partition of the group G. This decomposition of the group G is called the "right coset decomposition" of the group G, w.r.t. the subgroup H.

   Similarly if one defines a relation called "congruence modulo H" on G by $a \equiv b \pmod H$ if and only if $b^{-1}a \in H$. It can be shown that $[a] = aH$ and hence the collection of all distinct left cosets of H in G form a partition of the group G. This decomposition of the group G is called the "left coset decomposition" of the group w.r.t. the subgroup H.

3. If H is a subgroup of G, then there exists a one-to-one correspondence between any two right (left) cosets of H in G.

4. There is one-to-one correspondence between the set of all right cosets and the set of all left cosets of a subgroup of a group.

Index of a subgroup:

The number of distinct right (left) cosets of a subgroup H of a group G is called the index of the subgroup H in G and is denoted by $[G : H]$ and read as "the index of H in G".

Lagrange's Theorem

If G is any finite group and H is any subgroup of G, then $O(H)$ divides $O(G)$.

Proof: Let $O(G) = n$ and $O(H) = m$.

We shall show that $m \mid n$ i.e., $n = km$, for some $k \in Z$

Since the group G is finite, there are finite number of right (left) cosets of H in G.

Let G have k distinct right (left) cosets of H and these are $Ha_1, Ha_2, \ldots, Ha_k \Rightarrow [G:H] = k$.

We know that any two right (left) cosets of H have the same number of elements.

In particular H itself is a right (left) coset of H in G.

Since $O(H) = m$, each right (left) coset of H will have m elements.

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

$\therefore O(G) = O(Ha_1) + O(Ha_2) + \ldots + O(Ha_k)$

$\Rightarrow n = O(H) + O(H) + \ldots + O(H)$ (k cosets)

$\Rightarrow n = m + m + \ldots + m$ (k times)

$\Rightarrow n = km$

or $m \mid n$ i.e, $O(H) \mid O(G)$.

Note

1. The index of any subgroup of a finite group is a divisor of the order of the group.
   [i.e, if $O(G) = n$, $[G:H] = k$ then $k \mid n$ [It follows from Lagrange's theorem]]
2. The converse of Lagrange's theorem need not be true. i.e, If G is a finite group of order n and m is a positive integral divisor of n, then G need not have a subgroup of order m.
3. If $O(G) = n$, $O(H) = m$, & $[G:H] = k$, then the number of right (left) cosets of H in G is equal to $\frac{O(G)}{O(H)}$

Consequences of Lagrange's Theorem

1. If G is a finite group and $a \in G$, then $O(a)$ divides $O(G)$.
2. If G is a finite group of order n then $\forall a \in G$, $a^n = e$, where e is the identity element of G.
3. A finite group of prime order is cyclic and hence abelian.
4. If G is a cyclic group of prime order then G has no proper subgroup.
5. Every finite group of composite order has proper subgroups.
6. Any group of order five or less than five is abelian.
7. If G is a finite cyclic group of order k, then for every divisor n of k, there exists a unique subgroup of G of order n.

Examples

1. Consider the multiplicative group $G = \{1, -1, i, -i\}$ of fourth roots of unity and $H = \{-1, 1\}$ be a subgroup of G. Write all the right cosets of H in G.

Sol^n Here $O(G) = 4$, $O(H) = 2$

The number of distinct right cosets of H in G is $[G:H] = \frac{O(G)}{O(H)} = \frac{4}{2} = 2$.

The right cosets are $H.1 = \{-1, 1\}$ and $H.i = \{-i, i\}$

2. Find all the left cosets of $H = \{0, 4, 8\}$ in $\langle Z_{12}, +_{12} \rangle$

Sol^n Here $O(Z_{12}) = 12$ and $O(H) = 3$.

$\therefore$ number of distinct left cosets of H in $G = \frac{12}{3} = 4$.

These are

$0 +_{12} H = \{0, 4, 8\}$

$1 +_{12} H = \{1, 5, 9\}$

$2 +_{12} H = \{2, 6, 10\}$

$3 +_{12} H = \{3, 7, 11\}$.

3. List all the subgroups of the cyclic group of fourth roots of unity.

Sol^n $G = \{1, -1, i, -i\}$.

Here $O(G) = 4$ and i is a generator.

The divisors of 4 are 1, 2 and 4.

$\therefore$ The subgroups of G are the only subgroups generated by i, $i^2 = -1$ and $i^4 = 1$.

$\therefore$ The subgroups are

$\langle i \rangle = \{1, -1, i, -i\}$, $\langle -1 \rangle = \{1, -1\}$, $\langle 1 \rangle = \{1\}$.

4. List all the subgroups of a cyclic group G of order 24 and whose generator is g.

Sol^n Here $O(G) = 24$, $O(g) = 24$.

The divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24.

$\therefore$ The subgroups of G are the only subgroups generated by $g, g^2, g^3, g^4, g^6, g^8, g^{12}$ and $g^{24} = e$.

5. Find all the subgroups of $\langle Z_{18}, +_{18} \rangle$.

Sol^n: 1 is a generator of Z_{18}.

The divisors of 18 are 1, 2, 3, 6, 9, 18.

∴ The generators of the subgroups are

$1 \cdot 1 = 1$, $1 \cdot 2 = 2$, $1 \cdot 3 = 3$, $1 \cdot 6 = 6$, $1 \cdot 9 = 9$, $1 \cdot 18 = 0$

Subgroups are $\langle 1 \rangle = Z_{18}$

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$

$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$

$\langle 6 \rangle = \{0, 6, 12\}$

$\langle 9 \rangle = \{0, 9\}$

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

Exercise.

1. Find all the right cosets of the subgroup $H = \{0, 3\}$ in the group $\langle Z_6, +_6 \rangle$.
2. Find all the right cosets of the subgroup $H = \{1, 3, 9\}$ in the group $\langle Z_{13} - \{0\}, \times_{13} \rangle$.
3. List all the subgroups of $\langle Z_9, +_9 \rangle$.
4. Find all the subgroups of $\langle Z_6, +_6 \rangle$.
5. Find the number of elements in the cyclic subgroup of $\langle Z_{12}, +_{12} \rangle$ generated by 3 and 8.

[Hint: If g is a generator of a cyclic group G of order n, then g^m generates a subgroup H of G of order $\frac{n}{d}$, where $d = (n, m)$]

6. Find all the left cosets of $H = \{0, 3, 6, 9\}$ in $\langle Z_{12}, +_{12} \rangle$ and verify Lagrange's theorem in each case.