Group —

Let $(G, *)$ be an algebric structure, where $*$ is a binary operation, then $(G, *)$ is called a group under this operation if the following conditions are satisfied. ①

1. Closure Law:

   The binary operation $*$ is closed operation

   i.e, $a * b \in G$ ~~for~~ for all $a, b \in G$

2. Associative Law:

   The binary operation $*$ is an associate operation

   i.e, $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$

3. Identity Element:

   There exists an identity element i.e, for some $e \in G$, $e * a = a * e = a$, $a \in G$

4. Inverse Element:

   For each a in G, there exists an element a' (the inverse of a) in G such that $a * a' = a' * a = e$

Note -

1. A group G is said to be Abelian if the commutative law holds i.e, $a * b = b * a$ for all $a, b \in G$

2. A group with addition binary operation is known as additive group and that with multiplication binary operation is known as multiplicative group.

Example -

1. The set R of real number, for the binary operation of addition, is a group, with 0 as identity element and $(-a)$ as the inverse of a. (Similarly $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$)
2. The set R^* of non-zero real number, for the binary operation of multiplication is group with 1 as identity element and $1/a$ as the inverse of a. (Similary $(\mathbb{Q}^*, \cdot)$ $(\mathbb{C}^*, \cdot)$)
3. The set Z^+ of positive integer with operation + is not a group. There is no identity element for + in Z^+. The set Z^+ with operation multiplication is not a group. There is an identity element 1, but no inverse of 3.

Example Prove that the fourth roots of unity 1, -1, i, -i form an abelian multiplicative group.

Soln Let $G = \{1, -1, i, -i\}$. We form the composite table as.

×	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

1. Closure property - Since all the entries in the table are the element of G and hence G is closed with respect to multiplication.
2. Associative Law: $a(bc) = (ab)c$ for all value of a, b, c in G.
   for example $1[(-1)i] = [1 \times (-1)]i$
   $-i = -i$

Commutative Law: $ab = ba \quad \forall\ a, b \in G$

From the composition table it is clear that elements in each row are the same as elements in the corresponding column so that $ab = ba$.

Identity Element:

$1 \in G$ is identity element as $1 \cdot a = a \cdot 1 = a$.

Inverse Element:

As $1 \cdot 1 = i \cdot (-i) = (-1)(-1) = 1$, the inverse of $1, -1, i, -i$ are $1, -1, -i, i$ respectively. ~~and~~ and all those belong to G.

Hence, it follows that G is an abelian multiplicative group.

Example – Show that the set of all positive rational numbers ~~We have to show that $(Q^+, *)$ is a group under the~~ forms an abelian group under the composition defined by $a * b = (ab)/2$.

Sln Let Q^+ denote the set of all positive rational numbers. We have to show that $(Q^+, *)$ is a group under the composition $a * b = (ab)/2$

1. Closure Property –

Since for every element $a, b \in Q^+$, $(ab)/2$ is also in Q^+, therefore Q^+ is closed with respect to operation $*$.

2. Associative Law: For $a, b \in \mathbb{Q}^+$, we have

$$(a*b)*c = (ab)/2 * c \Rightarrow (ab/2)\,c/2$$
$$= \frac{a}{2}(b\cdot c)/2$$
$$= a * (b\cdot c)/2$$
$$= a*(b*c)$$

3. Commutative Law: For $a, b \in \mathbb{Q}^+$, we have.

$$a*b = (ab)/2 = (ba)/2 = b*a$$

4. Identity Element:

Let e be the identity element in $\mathbb{Q}^+$, such that

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

Now, $e*a = a \Rightarrow ea/2 = a$

$$\Rightarrow \frac{a}{2}(e-2) = 0$$

$\Rightarrow e = 2$, since $a \in \mathbb{Q}^+ \Rightarrow a > 0$

But $2 \in \mathbb{Q}^+$ and we have $2*a = (2a)/2 = a = a*2$

$\forall a, \in \mathbb{Q}^+$

5. Inverse Element:

Let a be any element of $\mathbb{Q}^+$. If the number b is to be the inverse of a, then we must have.

$$b*a = e = 2 \Rightarrow (ba)/2 = 2$$
$$\Rightarrow b = \frac{4}{a} \in \mathbb{Q}^+$$

We have $(4/a)*a = 4a/2a = 2 = a*(4/a)$

Therefore, $4/a$ is the inverse of a. Thus each element of $\mathbb{Q}^+$ is invertible.

Hence, $(\mathbb{Q}^+, *)$ is an abelian group.

Example Show that the set $\{1, 2, 3, 4, 5\}$ is not a group under addition and multiplication modulo 6. (5)

Soln Let $G = \{1, 2, 3, 4, 5\}$. The operation addition modulo 6 is denoted by $+_6$.

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

Since all the entries in the composition table do not belong to G, in particular $0 \notin G$. Hence G is not closed w.r.t $+_6$. Consequently $(G, +_6)$ is not a group.

(ii) The operation multiplication modulo 6 is denoted by $\times_6$.

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

From the composition table, it is clear that all the entries in the composition table do not belong to G, in particular $0 \notin G$. Hence G is not closed w.r.t $\times_6$.

Consequently $(G, \times_6)$ is not a group.

Properties of Groups -

1. If $(G, *)$ is a group and a, b, c are in G then
   (i) $a*b = a*c \Rightarrow b = c$ (left cancellation law)
   (ii) $b*a = c*a \Rightarrow b = c$ (right cancellation law)

2. In a group $(G, *)$
   (i) The equation $a*x = b$ has a unique solution $x = a^{-1}*b$
   (ii) The equation $y*a = b$ has a unique solution $y = b*a^{-1}$
   where, $a, b \in G$.

3. In a group $(G, *)$
   (i) $(a^{-1})^{-1} = a$
   (ii) $(ab)^{-1} = b^{-1}a^{-1}$

Example - Prove that if $a^2 = a$, then $a = e$, a being an element of a group.

Soln Let a be an element of a group G such that $a^2 = a$.
To prove that $a = e$.

$$a^2 = a \Rightarrow a.a = a \Rightarrow (a.a).a^{-1} = a.a^{-1}$$
$$\Rightarrow a.(a.a^{-1}) = e$$
$$\Rightarrow a.e = e$$
$$\Rightarrow a = e$$

Example - Show that if a, b are arbitary elements of a group G, then $(ab)^2 = a^2b^2$ iff G is abelian.

Soln Let a and b be arbitrary elements of a group G.
Suppose $(ab)^2 = a^2b^2$ ∴

To prove G is abelian, we have to show that

$ab = ba$

$(ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ by associative laws

$\Rightarrow a^{-1}a(ba)b = a^{-1}a(ab)b$ by left ~~left~~ a

$\Rightarrow (ba)b = (ab)b$ by left cancellation law

$\Rightarrow (ba)b.b^{-1} = (ab)b.b^{-1}$

$\Rightarrow ba = ab$ by right cancellation law

Again, Suppose G is abelian so that

$ab = ba \quad \forall\ a, b \in G$

To prove that $(ab)^2 = a^2b^2$

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

$= a(ba)b$

$= a(ab)b$

$= (aa)(bb)$

$= a^2b^2$

Order of Elements –

→ The order of an element g in a group G is the smallest positive integer n such that $g^n = e$.

→ If no such ~~order~~ integer exists, we say g has infinite order.

→ The order of an element g is denoted by $O(g)$

Example Let $G = \{1, -1, i, -i\}$ be a multiplicative group. Find the order of every elements.

Soln 1 is identity of Element in G

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

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

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

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

Example- In a group (G, o), a is an element of order 30. Find the order of a^5

Soln

Given $O(a) = 30$, so $a^{30} = e$, the identity element.

Let $O(a^5) = n$. so, $(a^5)^n = e$ i.e, $a^{5n} = e$

where n is the least positive integer.

Hence 30 is a divisor of $5n$ $\therefore n = 6$. Hence $O(a^5) = 6$.

Semigroup –

An algebric structure $(S, *)$ is called a semigroup if the following conditions are satisfied:

1. The binary operation $*$ is closed operation i.e, $a * b \in S$ for all $a, b \in S$ (closure law).
2. The binary operation $*$ is an associative operation i.e, $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$ (associative law)

Monoid –

An algebric structure $(S, *)$ is called a monoid if the following conditions are satisfied:

1. The binary operation $*$ is a closed operation. (closure law)
2. The binary operation $*$ is an associative operation (Associative law).
3. There exists an identity element i.e, for some $e \in S$, $e * a = a * e = a$ for

For example –

1. If Z be a set of all integers, then $(Z, +)$ and $(Z, \cdot)$ are semigroup as these two operations are closed and associative in Z.
2. The structure $(Z, +)$ is a monoid with identity element 0 and $(Z, \cdot)$ is a monoid with 1 as identity element.

Subgroup –

Let $(G, *)$ be a group and H is a subset of G. $(H, *)$ is said to be subgroup of G if $(H, *)$ is also group by itself.

Note –

If G is a group, then G is a subgroup of G. Also if e is the identity element of G. Then the subset of G containing only identity element is also a subgroup of G.

Improper Subgroup –

The two subgroups $(G, *)$ and $(\{e\}, *)$ of the group $(G, *)$ are called improper or trivial subgroup, others are called proper or non-trivial subgroups.

Example –

1. The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$
2. The additive group of even integers is a subgroup of the additive group of all integers.
3. The set Q^+ of all non-zero positive rational number is a subgroup of the multiplicative group Q^* of all non-zero rational number.

The necessary and sufficient Condition-

The necessary and sufficient condition for a non-empty sub-set H of a group $(G, *)$ to be a subgroup is

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

where b^{-1} is the inverse of b in G.

Example-

1. Let G be the additive group of all integers and H be the subset of G consisting of all positive integers. Then H is closed with respect to addition i.e, the composition in G. But H is not a subgroup of G since the identity $0 \notin H$.

2. Let $G = \{\cdots 3^{-2}, 3^{-1}, 1, 3, 3^2, \cdots\}$ be the multiplicative group consisting of all integral powers of 3. Let $H = \{1, 3, 3^2, \cdots\}$. Then $H \subset G$ and H is closed with respect to multiplication, but H is not subgroup of G since the inverse of 3 i.e, 3^{-1} does not belong to H.

Q The intersection of any two sub-groups of a group $(G, *)$ is again a sub-group of $(G, *)$

Proof - Let H_1 and H_2 form any two subgroup of $(G, *)$

We have $H_1 \cap H_2 \neq \phi$; since at least the identity element is common to both H_1 and H_2

Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$

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 $b \in H_2$

Since, H_1 and H_2 form sub-groups under the group $(G, *)$ we have

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

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

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

Thus we see

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

Therefore, $H_1 \cap H_2$ forms a subgroup under $(G, *)$

Note -

The union of two subgroups is not necessarily a subgroup.

For example - Let G be the additive group of integers.

Then, $H_1 = \{\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$H_2 = \{\ldots -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$

are both subgroup of G.

Now, $H_1 \cup H_2 = \{\ldots -4, -3, -2, 0, 2, 3, 4, 6, \ldots\}$

Obviously, $H_1 \cup H_2$ is not closed with respect to addition as ~~$2 \in H_1$~~

$2 \in H_1 \cup H_2$, $3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$.

Therefore, $H_1 \cup H_2$ is not a subgroup of G_2.

Results

1. The identity element of a subgroup is the same as that of the group.
2. The inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

have no common element.

Q. Consider the group $(\mathbb{Z}, +)$. Let $H = \{3n : n \in \mathbb{Z}\}$. Then H is a subgroup of $\mathbb{Z}$?

Soln

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

Suppose $a = 3p$ and $b = 3q$

Then $a + b^{-1} \in H$

$3p + (3q)^{-1} \in H$

$3p - 3q \Rightarrow 3(p-q)$ where $p - q \in \mathbb{Z}$

Thus $3(p-q) \in H$

Hence, H is a subgroup of $\mathbb{Z}$.

Cosets

Let H be a subgroup of a group G and let $a \in G$. Then the set $\{a * h : h \in H\}$ is called the left coset generated by 'a' and H and is denoted by aH.

Similarly the set $Ha = \{h * a : h \in H\}$ is called the right coset and is denoted by Ha.

→ If the group operation be addition, then the right coset of H in G generated by a is defined as

$$H + a = \{h + a : h \in H\}$$

Similarly, the left coset $a + h = \{a + h : h \in H\}$

Properties of Coset -

Let H be a subgroups of G, and 'a' and 'b' belong to G. Then,

1. $a \in aH$
2. $aH = H$ iff $a \in H$
3. $aH = bH$ or $aH \cap bH = \phi$
4. $aH = bH$ iff $a^{-1}b \in H$

Index of a subgroup in a group –

If H is a subgroup of a group G, the number of distinict right (left) cosets of H in G ~~are~~ is called the index of H in G and is denoted by $[G:H]$ or by $i_G(H)$.

Example –

Let G be the additive group of integers i.e,

$$G = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$$

Let H be the subgroup of G obtained on multiplying each element of G by 3. Then

$$H = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

Soln

Since, the group G is abelian any right cost will be equal to the corresponding left coset.

~~Hence~~ We have $0 \in G$

$$H = H+0 = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

Again $1 \in G$

$$H+1 = \{\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\}$$

Then $2 \in G$

$$H+2 = \{\ldots -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Now $3 \in G$ $H+3 = \{\ldots -6, -3, 0, 3, 6, 9, 12, \ldots\}$

We see that the right coset H, H+1 and H+2 are all distinct and moreover these are disjoint i.e, have no common element.

Thus, there exist three disjoint right cosets namely $H, H+1, H+2$.

$G = H \cup (H+1) \cup (H+2)$

The index of H in G is 3.

Normal Subgroup —

A subgroup H of a group G is said to be normal subgroup of G if $Ha = aH$ for all $a \in G$.

Note

Every subgroup of an abelian group is a normal subgroup.

Lagrange's Theorem –

The order of each subgroup of a finite group divides the order of the group.

Proof –

Let G be a finite group of order n so that G may be written as $G = \{a_1, a_2, \ldots a_n\}$

Let $H = \{h_1, h_2, \ldots h_m\}$ be a subgroup of G, so that $O(H) = m$. Start with any one element a_i of G and form to coset.

$$Ha_i = \{h_1 a_i, h_2 a_i, \ldots h_m a_i\}$$

All elements $h_1 a_i, h_2 a_i, \ldots h_m a_i$ of Ha_i listed above are distinct (by right cancellation law), and they are as many in number as the element in H.

Now, if $Ha_i = G$, then $m = n$ and hence $O(H) \geq O(G)$

So, that $O(H) \mid O(G)$.

If $Ha_i \neq G$, then G has an element a_j such that $a_j \notin Ha_i$. Form the coset

$$Ha_j = \{h_1 a_j, h_2 a_j, \ldots h_m a_j\}$$

The Ha_i and Ha_j are either disjoint or identical (by using coset properties). Hence

$$Ha_i \cap Ha_j = \phi$$

Now, if $Ha_i \cup Ha_j = G$, then $2m = n$ so that $m \mid n$, and hence $o(H) \mid o(G)$.

~~In general, since~~

Since G is finite, the number of ~~coset~~ distinct right coset will also be finite, say k. Hence, total number of elements of all cosets is km which is equal to the total no. of elements of G.

Hence ~~xx cancel nn~~ $km = n$, which shows that $m \mid n$ or that $o(H) \mid o(G)$.

Remarks –

The converse of Lagrange's theorem is not true. In other words, it is not necessary that if a positive integer $m \mid n$, n being the order of some group G, then G should have a subgroup of order m.

eg Au the group of all even permutations on four symbols. Now. $o(A_4) = 12$ and $6 \mid 12$. But A_4 has no subgroup of order 6.

$f = g$ for all $x \in \{1, 2, 3, 4\}$ which implies $f = g$.

Normal Subgroup –

A subgroup H of a group G is said to be a normal subgroup of G if for every $x \in G$ and for every $h \in H$, $xhx^{-1} \in H$.

[Note] –

From this definition we can immediately conclude that H is a normal subgroup of G iff $xHx^{-1} \subseteq H \quad \forall x \in G$.

Theorem –

A subgroup H of a group G is normal iff $xHx^{-1} = H \quad \forall x \in G$.

Proof –

Let $xHx^{-1} = H \quad \forall x \in G$. Then $xHx^{-1} \subseteq H \quad \forall x \in G$

Therefore, H is a normal subgroup of G.

Converse –

Let H be a normal subgroup of G.

Then $xHx^{-1} \subseteq H \quad \forall x \in G$ — (1)

Also, $x \in G \Rightarrow x^{-1} \in G$. Therefore, we have

$$x^{-1}H(x^{-1})^{-1} \subseteq H \quad \forall x \in G$$

$$\Rightarrow x^{-1}Hx \subseteq H \quad \forall x \in G$$

$$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1} \quad \forall x \in G$$

$$\Rightarrow H \subseteq xHx^{-1} \quad \forall x \in G \quad \text{— (2)}$$

From (1) and (2), we conclude that $xHx^{-1} = H$ for all $x \in G$.

$f(x) = g(x)$ for all $x \in \{1, 2, 3, 4\}$ which implies $f = g$.

Theorem- The intersection of any two normal subgroup of a group is a normal subgroup.

Proof - Let H and K be two normal subgroups of a group G. Since H and K are subgroups of G, therefore $H \cap K$ is also a subgroup of G. Now to prove that $H \cap K$ is a normal subgroup of G.

Let x be any element of G and y be any element of $H \cap K$.

We have

$$y \in H \cap K \Rightarrow y \in H \; ; \; y \in K$$

Since, H is a normal subgroup of G, therefore $x \in G, \; y \in H \Rightarrow xyx^{-1} \in H$

Similarly, $xyx^{-1} \in K$

Now $xyx^{-1} \in H$, $xyx^{-1} \in K \Rightarrow xyx^{-1} \in H \cap K$

Thus, we have $x \in G$, $y \in H \cap K \Rightarrow xyx^{-1} \in H \cap K$

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

Quotient Group –

If G is a group and H is a normal subgroup of G, then the set G/H of all cosets of H in G is a group with respect to multiplication of cosets. It is called the quotient group or factor group of G by H.

The identity element of the quotient group G/H is H.

Theorem –

The set of all cosets of a normal subgroup is a group with respect to multiplication of the composition.

Proof

Let H be a normal subgroup of a group G. Since, H is normal in G, therefore each right coset will be equal to the corresponding left coset. ~~Thus~~ Therefore Let G/H be the collection of all cosets of H in G i.e

Let $G/H = \{Ha : a \in G\}$

1. Closure Property –

Let $a, b \in G$. Then $(Ha)(Hb) = H(aH)b$

$= H(Ha)b$

$= HHab$

$= Hab$

Since, $ab \in G$, therefore Hab is also a coset of H in G. So, $Hab \in G/H$. Thus G/H is closed w.r.t ~~Cosets~~ coset multiplication.

Associativity –

(4)

Let $a, b, c \in G$. Then $Ha, Hb, Hc \in G/H$. We have

$$Ha[(Hb)(Hc)] = Ha(Hbc) = Ha(bc) = H(ab)c$$

$$= (Hab)Hc = [(Ha)(Hb)]Hc$$

Thus the product in G/H satisfies the associative law.

Existence of Identity –

We have $H = He \in G/H$. Also, if Ha is any element of G/H, then

$$H(Ha) = (He)(Ha) = Hea = Ha$$

and similarly, $(Ha)H = (Ha)(He) = Hae = Ha$

Therefore the coset H is the identity element.

Existence of Inverse –

Let $Ha \in G/H$. Then $Ha^{-1} \in G/H$

We have, $(Ha)(Ha^{-1}) = Haa^{-1} = He = H$

and $(Ha^{-1})(Ha) = Ha^{-1}a = He = H$

$\therefore$ The coset Ha^{-1} is the inverse of Ha i.e., $(Ha)^{-1} = Ha^{-1}$

Thus, each element of G/H possesses inverse.

Hence, G/H is a group with respect to product of cosets.

Permutation Group –

Let A be a finite set. Then a function $f: A \to A$ is said to be a permutation of A if

(i) f is one-one

(ii) f is onto.

i.e, A bijection from A to itself is called a permutation of A.

→ The number of distinct elements in the finite set A is called the degree of permutation.

→ In general, a permutation f on the set $\{1, 2, 3, \ldots, n\}$ can be written as

$$f = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{bmatrix}$$

Equality of Two permutation –

Let f and g be two permutations on a set X. Then $f = g$ iff $f(x) = g(x)$ for all x in X.

eg Let f and g be given by

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \qquad g = \begin{bmatrix} 3 & 2 & 1 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

Here, $f(x) = g(x)$ for all $x \in \{1, 2, 3, 4\}$ which implies $f = g$.

$$\begin{bmatrix} 2 & 3 & 4 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 4 & 1 & 2 & 3 \end{bmatrix}$$

Identity Permutation –

If each element of a permutation be replaced by itself. Then it is called the identity permutation and is denoted by the symbol I. for example –

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

Product of Permutation (or Composition of Permutation)

The product of two permutations f and g of same degree is denoted by fog or fg, meaning first perform f and then perform g.

$$f = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{bmatrix}$$

$$g = \begin{bmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ c_1 & c_2 & c_3 & \cdots & c_n \end{bmatrix}$$

Then, $$fog = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ c_1 & c_2 & c_3 & \cdots & c_n \end{bmatrix}$$

Example Find the product of two permutation and show that it is not commutative.

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \text{ and } g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$$

Soln $$fg = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \text{ and } gf = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

Result -

1. Permutation is not commutative.
   i.e $fg \neq gf$
2. Permutation multiplication is associative.
   i.e $P_1(P_2 P_3) = (P_1 P_2) P_3$

Inverse Permutation -

Since a permutation is one-one onto map and hence it is inversible, i.e, every permutation on a set has a unique inverse permutation denoted by f^{-1}

i.e $f = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{bmatrix}$ then $f^{-1} = \begin{bmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{bmatrix}$.

Total number of distinct permutation of degree n.

If S is a finite set having n distinct elements, then we shall have n! distinct arrangement of the element of S. Therefore there will be n! distinct permutation of degree n. If P_n be the set containing of all permutation of degree n, then the set P_n will have n! distinct element. This set P_n is called the symmetric set of permutation of degree n. Sometime it is also denoted by S_n.