PERMUTATIONS

In crude sense, permutations are arrangements of objects in various orders and forms. In terms of sets and functions, permutations are bijective mappings on non-empty sets. The main interest of the mathematical society is to deal with the permutations on finite sets as those are more effectively employed to deal with the problems related to finite dimensional objects and their transformations as well as their properties. Studies of symmetries of geometrical objects may be particularly cited in this case. Here we first give the formal definition of a permutation on finite sets and then we will discuss on various important and relevant topics related to it. Finally we establish that the set of all the permutations on a finite set forms a group under the operation of composition of mappings.

Groups containing permutations are known as permutation groups. These groups are very useful in the study of finite groups. This is because of the fact that every finite group is isomorphic (structurally same) to a permutation group. So, the study of permutations and permutation groups invites more attention of the mathematicians dealing with finite group theory.

*Definition* 1. If S is a non-empty finite set having *n* elements, then a bijective or a one-one and onto mapping $f: \mathrm{S} \to \mathrm{S}$ is called a permutation of degree *n* on S.

**Remarks**:

1. The degree of permutation is nothing but the number of elements in the underlined finite set, known as the set of symbols or symbol set, on which the permutations are defined.
2. We have a total number of $n^n$ functions on a set S having *n* distinct elements. Out of these $n^n$functions, only the bijective mappings on S are the permutations on S.

**Notation for a permutation**

Let $\mathrm{S} = \{a_1, a_2, a_3, a_4, \dots \dots, a_n\}$ is a finite set having *n*-distinct elements and $f: \mathrm{S} \to \mathrm{S}$ is a bijective mapping on S such that $f(a_i) = b_i, i = 1, 2, \dots, n$, where $b_i'^s \in \mathrm{S} = \{a_1, a_2, \dots, a_n\}$. Then, by definition, $f: \mathrm{S} \to \mathrm{S}$ is a permutation of degree *n* on S. This permutation is generally denoted by the symbol

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

In the above convention of two row notation for a permutation, we observe that each element in the second row is the f-image of the element in the first row just lying directly above it.

For example, by the permutation$g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, we generally understand the one-one and onto function $g: \{1, 2, 3\} \to \{1, 2, 3\}$ such that $g(1) = 3, g(2) = 1, g(3) = 2$.

**Remarks**: A permutation represented in a two-row symbolism may be written in many different ways. For, if we interchange the positions of two columns in a particular permutation without changing their entries, those interchanges don't affect in the rule of the bijective mapping giving the permutation. Therefore, the permutation and the permutation obtained after interchanges of columns will represent the same permutation. Thus, though the appearances of the permutations given below seem different, they represent the same permutation as they are representing the same functional rule: $1 \to 3, 2 \to 1, 3 \to 2$ only.

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

**Equality of permutations**

*Definition* 2. Two permutations $f$ and $g$ of degree *n* on the same symbol set S are said to be equal if we have that $f(x) = g(x), \forall x \in$ S. That is, two permutations $f$ and $g$ on the same symbol set S are equal if they are equal as functions on S. In this case we usually write $f = g$.

For example, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 3 & 5 & 4 & 1 & 2 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ are two equal permutations of degree 5. Further the six permutations mentioned in the above remark are all equal.

**Note**: The only difference, if there exists, there may arise between two equal permutations is the difference in the column positions.

**Identity permutation**

*Definition* 3**.** If a permutation *I* of degree *n* on S is such that *I* replaces each element of S by the element itself, then *I* is called the identity permutation of degree *n*. That is, the identity permutation of degree *n* on S is the identity mapping on S.

In other words, if both the rows of a permutation are identical, then the permutation is an identity permutation.

For example, $I = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ a_1 & a_2 & a_3 \dots & a_n \end{pmatrix}$ or $\begin{pmatrix} b_1 & b_2 & b_3 \dots & b_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 \dots & n \\ 1 & 2 & 3 \dots & n \end{pmatrix}$ are identity permutations of degree *n*.

**Total number of distinct permutations of degree** *n*

Let S $= \{a_1, a_2, a_3, a_4, \dots \dots., a_n\}$ and $f = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix}$ be a permutation of degree *n* on S. It is easy to see that by fixing the elements in the first row of *f* and arranging the elements in the second row by changing their orders, we get different permutations. The *n* distinct elements in the second row can be arranged in *n*! distinct ways and hence we get *n*! distinct permutations on the set S. Thus from a set having 2 distinct elements we will get 2!=2 and from a set having 3 distinct elements we will get 3!=6 distinct permutations etc.

**The symmetric set of permutations**

The set of all the $n!$ distinct permutations of degree $n$ on a finite set S having $n$ distinct elements is denoted by $P_n$ or by $S_n$ and is called the symmetric set of permutations of degree $n$. Thus $S_3$ denotes the symmetric set of all the permutations of degree 3. Clearly $S_3$ contains $3!= 6$ distinct elements. Similarly $S_4$ is the symmetric set of permutations of degree 4 having $4!= 24$ elements.

**Product of permutations**

We have seen that every permutation is a bijective mapping. We also know that the composition of two bijective mappings on S is again a bijective mapping. So, it immediately follows that the composition of two permutations of degree $n$ on S is again a permutation of degree $n$ on S. Therefore, with the help of composition of mappings we can naturally define the product of two permutations $f$ and $g$ of the same degree n, denoted as $fg$, by $fg = gof$.

In other words, the product $fg$ of two permutations $f$ and $g$ of the same degree $n$ is obtained by first carrying out the operation defined by $f$ and then by $g$.

For example, if $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$, then by definition

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$$

And $$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$$

Here we notice that $fg \neq gf$.

**Remarks**:

1. If we have to find the product $fg$, then it is customary to express the permutation $g$ in such a way that its first row coincides with the second row of $f$ so that one can immediately and easily find the images under $fg$. After expressing the second permutation in this way, without following other mechanical ways one can easily write the product $fg$ by taking the first row of $f$ as the first row of $fg$ and the second row of $g$ as the second row of $fg$.

   Thus $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$

   $$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}\begin{pmatrix} 3 & 1 & 4 & 5 & 2 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$$

2. Product or multiplication of permutations is not necessarily commutative. That is, it is not necessary that $fg = gf$.

**Inverse of a permutation**

If $f$ is a permutation of degree *n* on a set of symbols S, then $f$ is a bijective mapping on S. We know that a bijective mapping always possesses a unique inverse mapping and that the inverse is also a bijective mapping. So, if $f^{-1}$ is the inverse of the permutation $f$ of degree *n* on S, then $f^{-1}$ is also a bijective mapping on S and hence is a permutation of degree *n* on S. This inverse mapping $f^{-1}$ of $f$ is defined as the inverse of the permutation $f$.

Thus if $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, then its inverse is $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$.

**Note**: One can very easily find the inverse of a permutation just by interchanging its rows. That is, in general, the inverse of the permutation $\begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix}$ is $\begin{pmatrix} b_1 & b_2 & b_3 \ldots & b_n \\ a_1 & a_2 & a_3 \ldots & a_n \end{pmatrix}$.
Thus the inverse of $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$ is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.

**The Symmetric groups of permutations**

***Theorem*1**: The symmetric set $\mathrm{S_n}$ of all permutations on n symbols is a finite group of order *n*! with respect to composition of mappings as the binary operation. For $n \leq 2$, this group is Abelian and for $n \geq 3$, the group is always non-Abelian.

**Proof**: Let $\mathrm{S} = \{a_1, a_2, a_3, a_4, \ldots \ldots, a_n\}$ be a finite set having *n*-distinct elements and

$$\mathrm{S_n} = \{f \mid f : \mathrm{S} \to \mathrm{S} \text{ and f is bijective}\}.$$

Here we notice that to have bijective mappings from S onto itself, we can associate the elements $a_1$ through $a_n$ in $n, n-1, n-2, \ldots \ldots, 1$ ways respectively and hence by fundamental principle of counting, we will have $n(n-1)(n-2) \ldots \ldots .2.1 = n!$ distinct bijective mappings from S onto itself, i.e., $n!$ distinct permutations of degree *n* on S. Thus, the symmetric set $\mathrm{S_n}$ contains n! distinct elements.

Now we show that $\mathrm{S_n}$ is a group under the composition of mappings as the binary operation.

**Closure property**:

We have,

$$f, g \in \mathrm{S}_n \Longrightarrow f : \mathrm{S} \to \mathrm{S} \text{ and } g : \mathrm{S} \to \mathrm{S} \text{ are bijective mappings}$$

$$\Longrightarrow gof : \mathrm{S} \to \mathrm{S} \text{ is a bijective mapping}$$

$$\Longrightarrow gof = fg \in \mathrm{S}_n$$

Therefore $S_n$ is closed under the operation of composition of mappings.

**Associativity:**

We know that composition of mappings is always an associative operation. Therefore,

$$(hog)of = ho(gof), \quad \forall f, g, h \in S_n$$

Now $(hog)of = ho(gof) \Longrightarrow (gh)of = ho(fg)$, [$\because$ by definition $hog = gh, gof = fg$ ]

$$\Longrightarrow f(gh) = (fg)h, \forall f, g, h \in S_n$$

Associativity can also be established alternatively as follows:

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix}$, $g = \begin{pmatrix} b_1 & b_2 & b_3 \dots & b_n \\ c_1 & c_2 & c_3 \dots & c_n \end{pmatrix}$, $h = \begin{pmatrix} c_1 & c_2 & c_3 \dots & c_n \\ d_1 & d_2 & d_3 \dots & d_n \end{pmatrix} \in S_n$

Now, $f(gh) = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} \left[ \begin{pmatrix} b_1 & b_2 & b_3 \dots & b_n \\ c_1 & c_2 & c_3 \dots & c_n \end{pmatrix} . \begin{pmatrix} c_1 & c_2 & c_3 \dots & c_n \\ d_1 & d_2 & d_3 \dots & d_n \end{pmatrix} \right]$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 \dots & b_n \\ d_1 & d_2 & d_3 \dots & d_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ d_1 & d_2 & d_3 \dots & d_n \end{pmatrix}$$

And $(fg)h = \left[ \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 \dots & b_n \\ c_1 & c_2 & c_3 \dots & c_n \end{pmatrix} \right] . \begin{pmatrix} c_1 & c_2 & c_3 \dots & c_n \\ d_1 & d_2 & d_3 \dots & d_n \end{pmatrix}$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ c_1 & c_2 & c_3 \dots & c_n \end{pmatrix} . \begin{pmatrix} c_1 & c_2 & c_3 \dots & c_n \\ d_1 & d_2 & d_3 \dots & d_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ d_1 & d_2 & d_3 \dots & d_n \end{pmatrix} = f(gh)$$

Therefore the composition is associative.

**Existence of Identity**:

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} \in S_n$ be arbitrary.

Now we have the identity permutation $I = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ a_1 & a_2 & a_3 \dots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & b_3 \dots & b_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} \in S_n$

Again $fI = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 \dots & b_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} = f$

And $If = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ a_1 & a_2 & a_3 \dots & a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{pmatrix} = f$

Thus $If = f = fI, \forall f \in \mathrm{S}_n$ .

Hence $I = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ a_1 & a_2 & a_3 \ldots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & b_3 \ldots & b_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix} \in \mathrm{S}_n$ is the identity element.

**Existence of Inverse**:

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix} \in \mathrm{S}_n$ be arbitrary. Then, $f^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 \ldots & b_n \\ a_1 & a_2 & a_3 \ldots & a_n \end{pmatrix} \in \mathrm{S}_n$ and

$$ff^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix}\begin{pmatrix} b_1 & b_2 & b_3 \ldots & b_n \\ a_1 & a_2 & a_3 \ldots & a_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ a_1 & a_2 & a_3 \ldots & a_n \end{pmatrix} = I$$

Further $f^{-1}f = \begin{pmatrix} b_1 & b_2 & b_3 \ldots & b_n \\ a_1 & a_2 & a_3 \ldots & a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & b_3 \ldots & b_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix} = I$

Hence $\begin{pmatrix} b_1 & b_2 & b_3 \ldots & b_n \\ a_1 & a_2 & a_3 \ldots & a_n \end{pmatrix} \in \mathrm{S}_n$ is the inverse of $\begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix} \in \mathrm{S}_n$

Thus $\mathrm{S}_n$ is a group of order n! under the composition of mappings as the binary operation.

Finally, for $n = 1, 2$, this symmetric group is of orders 1 and 2 respectively. Since groups of order 1 and 2 are always Abelian, so $\mathrm{S}_1$ and $\mathrm{S}_2$ are Abelian.

We now prove that $\mathrm{S}_n$ is non-Abelian for $n > 2$.

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_2 & a_3 & a_4 & a_5 & \ldots & a_1 \end{pmatrix}, g = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_2 & a_1 & a_3 & a_4 & \ldots & a_n \end{pmatrix} \in \mathrm{S}_n$

Then, $fg = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_1 & a_3 & a_4 & a_5 & \ldots & a_1 \end{pmatrix} \neq gf = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_3 & a_2 & a_4 & a_5 & \ldots & a_1 \end{pmatrix}$

So, $\mathrm{S}_n$ is non-Abelian for $n > 2$.

**Note**: The structure of a symmetric set $\mathrm{S}_n$ and number of elements in it depend only on the number of elements in the symbol set S. So, it is immaterial whatever symbol we use to form permutations. The only important thing is the number of symbols in the symbol set. Thus we may use $1, 2, 3, 4, \ldots \ldots, n$ or $a_1, a_2, a_3, a_4, \ldots \ldots, a_n$ or any $n$-distinct symbols to form $\mathrm{S}_n$.

**Cyclic Permutations**

*Definition* 4. Let $f$ be a permutation of degree $n$ on a set S having $n$ distinct symbols. If it is possible to arrange $m(\leq n)$ elements of the set S in a row in such a way that the $f$-image of each element in the row, except the last element, is the element which follows it, the $f$-image of the last element in the row is the first element and the remaining $(n - m)$ elements of the set which are not appearing in the row are left unchanged by $f$, then $f$ is called a *cyclic permutation* or a *cycle of length m* or simply an *m-cycle*.

For example, consider the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 5 & 6 \end{pmatrix}$ of degree 6. This permutation can be represented by the cycle $(1\ \ 3\ \ 2\ \ 4)$. For, from the 4-cycle $(1\ \ 3\ \ 2\ \ 4)$, by the definition of a cyclic permutation, the permutation *f* can easily be written by the rule that the $f$-image of 1 is 3, the $f$-image of 3 is 2, the $f$-image of 2 is 4, the $f$-image of 4 is 1 and the remaining 2 symbols 5 and 6 are left unchanged by *f*.

Similarly, the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$ can be represented by the cycle $(1\ 2\ \ 3\ \ 4\ \ 5)$. But the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}$ cannot be represented by a cycle or not cyclic.

**Disjoint cycles**

Two cyclic permutations or cycles are said to be disjoint if they have no symbol in common.

For example, (1 2 4 3) and (5 7 6) are disjoint cycles while (1 3 4 5) and (4 7 6 2) are not disjoint cycles.

**An important note**: If two cycles of same length containing the same symbols are such that they look different as rows, but they maintain the same cyclic order, then they represent the same cycle. For example $(1\ 2\ \ 3\ \ 4\ \ 5), (\ 3\ \ 4\ \ 5\ \ 1\ 2)$ and $(\ \ 4\ \ 5\ \ 1\ 2\ \ 3)$ represent the same cycle. This is evident if we represent them as permutations of two-rowed symbols.

**Multiplication or product of cycles**

As a cycle represents a permutation, the product of two cycles is nothing but the product of the permutations represented by the cycles.

For example, the product of the cycles $(1\ \ 3\ \ 5\ \ \ 4)$ *and* $(6\ \ 2\ \ 4)$ is

$$(1\ \ 3\ \ 5\ \ \ 4)\ (6\ \ 2\ \ 4\ ) = \begin{pmatrix} 1 & 3 & 5 & 4 & 2 & 6 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{pmatrix} \begin{pmatrix} 6 & 2 & 4 & 1 & 3 & 5 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{pmatrix}$$

And

$$(6\ \ 2\ \ 4\ )(1\ \ 3\ \ 5\ \ \ 4) = \begin{pmatrix} 6 & 2 & 4 & 1 & 3 & 5 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 & 5 & 4 & 2 & 6 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 6 & 4 & 2 \end{pmatrix}$$

**Remarks**: One can easily find the product of two cycles without expressing the cycles into two-rowed form. For this purpose we first consider the first element of the first cycle. By definition of cycles its image is the second element in the first cycle. Now we find the image of this second element in the second cycle. The image found in this way is the image of the first element of the first cycle. Then we find the image of the image of first element in the same process and proceeding in the same way we get the product of the cycles easily.

For example, consider the product$(6\ \ 2\ \ 4\ \ \ 3)(1\ \ 3\ \ 5\ \ \ 2\ \ \ 4)$. Here the image of 6 in first cycle is 2 and that of 2 in the second cycle is 4. Hence the image of 6 in the product is 4. Now we find the image of 4 in the product. Here, the image of 4 in the first cycle is 3 and that of 3 in the second cycle is 5. Therefore, the image of 4 in the product is 5. Then we see that the symbol 5 is absent in the first cycle. So, its image in the first cycle is 5 by the convention of a cycle. Again the image of 5 in the second cycle is 2 and hence the image of 5 in the product is 2. Proceeding in this way we will easily find that the image of 2 is1, the image of 1 is 3 and the image of 3 is 6 in the product. Thus we get the product as$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 5 & 2 & 4 \end{pmatrix} = (1\ \ 3\ \ 6\ \ \ 4\ \ \ 5\ \ \ 2)$.

**Note**: For the product of disjoint cycles we have the following important theorem.

**Theorem 2**: *If $f$ and $g$ are two disjoint cycles, then$fg = gf$* i.e., *the product of disjoint cycles is commutative.*

**Proof**: We have,

$$f \text{ and } g \text{ are disjoint cycles} \Longrightarrow f \text{ and } g \text{ have no symbol in common}$$

So, it follows that the symbols permuted by *f* are left unchanged by *g* and also the symbols permuted by *g* are left unchanged by *f*. Hence $fg = gf$.

For example, consider the cycles $f = (3\quad 2\quad 5)$and $g = (1\quad 4\quad 6)$

Here $fg = (3\quad 2\quad 5)(1\quad 4\quad 6) = \begin{pmatrix} 1 & 2 & 5 & 3 & 4 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix} \begin{pmatrix} 1 & 4 & 3 & 2 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}$$

And $fg = (1\quad 4\quad 6)(3\quad 2\quad 5) = \begin{pmatrix} 1 & 4 & 3 & 2 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 5 & 3 & 4 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} = gf$$

**Inverse of a cyclic permutation**

We have seen that a cyclic permutation is nothing but a simple expression of a permutation of two-rowed form. So, a cyclic permutation must have its inverse. We can find the inverse of the cyclic permutation by first converting it to two-rowed expression and then exchanging its rows in general. But this is somewhat lengthy to some extent and hence time consuming. We can find the inverse of the cyclic permutation very easily in just one step using a simple rule which has been obtained from the following important theorem.

**Theorem 3:** *The inverse of a cyclic permutation is the cyclic permutation obtained by writing the elements in the cycle in reverse order*.

**Proof**: Let $(a_1\ \ a_2\ \ a_3\ \ a_4\ \ \ldots\ldots a_n)$ be a cycle of length n.

We need to show that $(a_1\ \ a_2\ \ a_3\ \ a_4\ \ \ldots\ldots a_n)^{-1} = (a_n\ \ a_{n-1}\ \ a_{n-2}\ \ \ \ldots\ldots a_1)$

We have, $\quad (a_1\ \ a_2\ \ a_3\ \ a_4\ \ \ldots\ldots a_n)(a_n\ \ a_{n-1}\ \ a_{n-2}\ \ \ \ldots\ldots a_1)$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_2 & a_3 & a_4 & a_5 & \ldots & a_1 \end{pmatrix} \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & a_2 & a_1 \\ a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_1 & a_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_1 & a_2 & a_3 & a_4 & \ldots & a_n \end{pmatrix} = I$$

Similarly, $(a_n\ \ a_{n-1}\ \ a_{n-2}\ \ \ \ldots\ldots a_1)\ (a_1\ \ a_2\ \ a_3\ \ a_4\ \ \ldots\ldots a_n)$

$$= \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & a_2 & a_1 \\ a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_1 & a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_2 & a_3 & a_4 & a_5 & \ldots & a_1 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_n \\ a_1 & a_2 & a_3 & a_4 & \ldots & a_n \end{pmatrix} = I$$

So, it is clear that $(a_1\ \ a_2\ \ a_3\ \ a_4\ \ \ldots\ldots a_n)^{-1} = (a_n\ \ a_{n-1}\ \ a_{n-2}\ \ \ \ldots\ldots a_1)$.

**Inverse of the product of cyclic permutations**

We have already seen that the symmetric set $S_n$ of all permutations of degree n is a group under composition of mappings. Also, by property of groups, we have that

$$(fg)^{-1} = g^{-1}f^{-1}, \forall\ f, g \in S_n.$$

Also, from the above theorem we have found that the inverse of a cyclic permutation is the cyclic permutation obtained by writing the elements in the cycle in reverse order. So, we can easily find $g^{-1}$ and $f^{-1}$ and thereby $(fg)^{-1} = g^{-1}f^{-1}$.

**Important Note**: For two disjoint cycles $f, g \in S_n$, it can be verified that $(fg)^{-1} = f^{-1}g^{-1}$. This result is obtained by using the fact that product of disjoint cycles is always commutative.

**Transpositions**

A cycle of length 2 or a 2-cycle is called a transposition. For example, (1 2), (3 5), (2 4) are all transpositions.

**Note**:

1. The concept of transpositions leads us to define even and odd permutations and also to introduce the concept of alternating groups.

2. The inverse of a transposition is the transposition itself. For example, consider the transposition (2 6). Here (2 6)(2 6) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix}$ = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = I$. Hence $(2\ 6)^{-1} = (2\ 6)$.

**Some Important Results on the Product of permutations**

Below we give some important results related to product of permutations in the form of theorems without proofs but with proper verifications:

**Theorem 1**: *Every permutation can be expressed as a product of disjoint cycles.*

**Verification**:

Consider the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 7 & 1 & 6 & 2 & 8 \end{pmatrix}$.

We can easily check that $f = (1 \quad 3 \quad 5)(2 \quad 4 \quad 7) =$ product of disjoint cycles

**Theorem 2**: *Every cycle can be expressed as a product of transpositions in infinitely many ways.*

**Verification:** Consider the cycle $f = (2 \quad 3 \quad 5 \quad 4 \quad 6)$

By actual multiplication, we can check that

$$f = (2 \quad 3 \quad 5 \quad 4 \quad 6) = (2 \quad 3)(2 \quad 5)(2 \quad 4)(2 \quad 6)$$

Since the inverse of a transposition is the transposition itself, so for a transposition, say $(2 \quad 3)$, we have,

$$(2 \quad 3)(2 \quad 3) = I, (2 \quad 3)(2 \quad 3)(2 \quad 3)(2 \quad 3) = I, \ldots\ldots\ldots$$

That is, the product of even number of $(2 \quad 3)'^s$ will give us the identity permutation only. So, the insertion of any even number of a particular transposition between any two transpositions or at both the ends of the cycle *f* doesn't change it. This insertion can be done in infinitely many ways. Therefore, f can be expressed as a product of transpositions in infinitely many ways.

**Theorem 3**: *Every permutation can be expressed as a product of transpositions in infinitely many ways.*

This theorem is an outcome of combining the results in Theorem1 and Theorem2.

**Theorem4**: *If a permutation is expressed as a product of transpositions, then the number of transpositions is either always even or always odd.*

**Note**: The proof of this theorem is beyond the scope of this book. But due to the fact of this theorem now we are at a position to define even and odd permutations.

**Even and Odd permutations**

*Definition*. A permutation is said to be an even permutation if it can be expressed as a product of an even number of transpositions and otherwise it is said to be an odd permutation.

**Corollaries on the above theorems**

**Cor.1**: A cycle of length *n* can be expressed as a product of *n*-1 transpositions. Therefore a cycle of length *n* is an even or odd permutation according as *n* is odd or even respectively.

**Cor.2**: The identity permutation is an even permutation.

**Cor.3**: The product of two even permutations and two odd permutations are even permutations.

**Cor.4**: The product of an even permutation and an odd permutation is an odd permutation.

**Cor.5**: The inverse of an even permutation is an even permutation and that of an odd permutation is an odd permutation.

**Total number of even permutations of degree n**

**Theorem 5**: *Of the* $n!$ *permutations of* $S_n$, *there are* $\frac{1}{2}n!$ *number of even and* $\frac{1}{2}n!$ *number of odd permutations*.

**Proof**:

Let there be exactly *k* numbers of odd permutations and *m* numbers of even permutations in $S_n$ so that $k + m = n!$. Further let the *k* distinct odd permutations in $S_n$ be $O_1, O_2, O_3, O_4, \dots \dots, O_k$ and the *m* distinct even permutations in $S_n$ be $E_1, E_2, E_3, E_4, \dots \dots, E_m$.

Now if $t \in S_n$ be a transposition, then by closure property in the symmetric group $S_n$, we have, $tO_1, tO_2, tO_3, \dots, tO_k, tE_1, tE_2, tE_3, \dots, tE_m$ are all elements of $S_n$.

Clearly every member of the set $\{tO_1, tO_2, tO_3, \dots, tO_k\}$ is an even permutation and also every member in $\{tE_1, tE_2, tE_3, \dots, tE_m\}$ is an odd permutation. So, it follows that

$$\{tO_1, tO_2, tO_3, \dots, tO_k\} \subseteq \{E_1, E_2, E_3, E_4, \dots \dots, E_m\}$$

And $$\{tE_1, tE_2, tE_3, \dots, tE_m\} \subseteq \{O_1, O_2, O_3, O_4, \dots \dots, O_k\}$$

From the above facts, we have, $k \le m$ and $m \le k$.

Now $k \le m$ *and* $m \le k \Longrightarrow m = k$

Further $m = k, k + m = n! \Longrightarrow m = k = \frac{n!}{2}$

**Alternating set of permutations**

The set of all the $\frac{n!}{2}$ even permutations in the symmetric group $\mathrm{S}_n$ is denoted by $\mathrm{A}_n$ and is called an alternating set of permutations of degree *n*.

**The Alternating group of all even permutations of degree *n***

**Theorem*:*** *The set* $\mathrm{A}_n$ *of all even permutations of degree n is a finite group of order* $\frac{n!}{2}$ *with respect to product of permutations.*

**Proof**: **Closure Property**:

We have,

$$E_1, E_2 \in A_n \Longrightarrow E_1 \text{ and } E_2 \text{ are even permutations.}$$

So, $E_1$ and $E_2$ can be expressed as products of even number of transpositions. Hence their product is also expressible as a product of even number of transpositions. That is, $E_1E_2$ is an even permutation. Therefore, $E_1E_2 \in A_n$.

**Associativity**: We know that product of permutations is associative. Since, $A_n \subseteq \mathrm{S}_n$, so it is also associative in $A_n$.

**Existence of identity**:

If $t = (a\ b) \in \mathrm{S}_n$ be any transposition, then $t^2 = (a\ b)(a\ b) = I$ . This implies that the identity permutation *I* is expressible as a product of even number of transpositions and hence is an even permutation.

Further, $If = f = fI,\ \forall f \in A_n$.

Therefore $I \in A_n$ is the identity element.

**Existence of inverse**:

Let $f \in A_n$ be arbitrary. Then, $f$ is an even permutation.

Let $f = (a_1 \quad b_1)(a_2 \quad b_2)(a_3 \quad b_3)(a_4 \quad b_4) \dots \dots \dots \dots (a_{2n-1} \quad b_{2n-1})(a_{2n} \quad b_{2n})$

Then by socks-shoe property,

$$f^{-1} = [(a_1 \quad b_1)(a_2 \quad b_2)(a_3 \quad b_3) \dots \dots \dots \dots (a_{2n-1} \quad b_{2n-1})(a_{2n} \quad b_{2n})]^{-1}$$

$$= [(a_{2n} \quad b_{2n})]^{-1}[(a_{2n-1} \quad b_{2n-1})]^{-1} \dots \dots \dots \dots [(a_2 \quad b_2)]^{-1}[(a_1 \quad b_1)]^{-1}$$

$$= (a_{2n} \quad b_{2n})(a_{2n-1} \quad b_{2n-1}) \dots \dots \dots \dots (a_3 \quad b_3)(a_2 \quad b_2)(a_1 \quad b_1)$$

$= (a_{2n} \quad b_{2n})(a_{2n-1} \quad b_{2n-1}) \ldots\ldots\ldots\ldots(a_3 \quad b_3)(a_2 \quad b_2)(a_1 \quad b_1)$

$=$ a product of even number of transpositions

= an even permutation

Therefore, $f^{-1} \in A_n$ and clearly, $ff^{-1} = I = f^{-1}f$.

Thus every element in $A_n$ possesses its inverse in $A_n$.

Hence $A_n$ is a group itself and as a subset of $S_n$ , it is a subgroup of $S_n$.

**Order of a permutation**:

If $f \in S_n$, then there always exists positive integers $n \in N$ such that $f^n = I$. The smallest of all such positive integers is the order of the permutation$f \in S_n$.

Here we give the following two important results (without proof) for the easy calculation of orders of any permutation.

**Theorem1**: *The order of a cyclic permutation of length m is m.*

**Verification**:

Let us consider the cycle $f = (2 \quad 4 \quad 1 \quad 6 \quad 5)$. This is a cycle of length 5. According to the above theorem we must have that$o(f) = 5$ . We verify this in the following lines.

We have

$$f^2 = (2 \quad 4 \quad 1 \quad 6 \quad 5)(2 \quad 4 \quad 1 \quad 6 \quad 5)$$

$$= \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 4 & 1 & 6 & 5 & 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 4 & 1 & 6 & 5 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 1 & 6 & 5 & 2 & 4 & 3 \end{pmatrix}$$

$$f^3 = f.f^2 = \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 4 & 1 & 6 & 5 & 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 1 & 6 & 5 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 6 & 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

$$f^4 = f.f^3 = \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 4 & 1 & 6 & 5 & 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 6 & 5 & 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 5 & 2 & 4 & 1 & 6 & 3 \end{pmatrix}$$

$$f^5 = f.f^4 = \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 4 & 1 & 6 & 5 & 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 5 & 2 & 4 & 1 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 6 & 5 & 3 \\ 2 & 4 & 1 & 6 & 5 & 3 \end{pmatrix} = I$$

Hence $o(f) = 5$

**Theorem2**: *The order of a permutation, when expressed as a product of disjoint cycles, is the LCM of the lengths of the disjoint cycles.*

**Verification**:

Let us consider the permutation$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}$. This can be expressed as a product of two disjoint cycles as$f = (1 \quad 4)(2 \quad 3 \quad 5)$. Now the LCM of the lengths 2 and 3 of the disjoint cycles is 6. So, according to the above theorem we must have that $o(f) = 6$.

We verify this result in the following lines.

$$f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}$$

$$f^4 = f^2.f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix}$$

$$f^6 = f^2.f^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = I$$

Thus $o(f) = 6 = \text{LCM of the lengths of } (1 \quad 4) \text{ and } (2 \quad 3 \quad 5)$.

This can alternatively be done as follows:

$$f^2 = (1 \quad 4)(2 \quad 3 \quad 5)(1 \quad 4)(2 \quad 3 \quad 5)$$

$$= (1 \quad 4)(1 \quad 4)(2 \quad 3 \quad 5)(2 \quad 3 \quad 5) \quad [\because \text{ disjoint cycles commute}]$$

$$= I(2 \quad 3 \quad 5)(2 \quad 3 \quad 5) \quad [\because \text{a transposition is its own inverse }]$$

$$= (2 \quad 5 \quad 3)$$

$$f^4 = f^2.f^2 = (2 \quad 5 \quad 3)\,(2 \quad 5 \quad 3) = (2 \quad 3 \quad 5)$$

$$f^6 = f^2.f^4 = (2 \quad 5 \quad 3)\,(2 \quad 3 \quad 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = I$$

**Some Solved Examples**

**Example1:** If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$, then find $f^2$, $f^{-1}$, $fg$ and $gf$.

**Solution**: Here,$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$

Now $f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}\begin{pmatrix} 4 & 1 & 2 & 3 & 6 & 5 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix}$$

$$f^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 & 6 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$$

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}\begin{pmatrix} 4 & 1 & 2 & 3 & 6 & 5 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}\begin{pmatrix} 2 & 4 & 5 & 1 & 3 & 6 \\ 1 & 3 & 6 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 2 & 5 \end{pmatrix}$$

**Example2:** If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$, then express $f$, $f^{-1}$, and $g$ as products of disjoint cycles. Also find their orders.

**Solution**: Here, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$

Now $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix} = (1\ \ 4\ \ 3\ \ 2)(5\ \ 6)$

$$f^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 & 6 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1\ \ 2\ \ 3\ \ 4)(5\ \ 6)$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = (1\ \ 2\ \ 4\,)(3\ \ 5)$$

Further $o(f) = o\big((1\ \ 4\ \ 3\ \ 2)(5\ \ 6)\big) = \text{LCM}\{2,4\} = 4 = o(f^{-1})$

$$o(g) = o\big((1\ \ 2\ \ 4)(3\ \ 5)\big) = \text{LCM}\{2,3\} = 6$$

**Example 3:** Determine which of the following permutations are even or odd:

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 6 & 5 & 7 \end{pmatrix}$ (ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 3 & 7 & 6 \end{pmatrix}$ (iii) $h = (1\ \ 3\ \ 5\ \ 4\ \ 6\ \ 2)$

**Solution**: We have

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 6 & 5 & 7 \end{pmatrix} = (1\ \ 4\ \ 3\ \ 2)(5\ \ 6) = (1\ \ 4)(1\ \ 3)(1\ \ 2)(5\ \ 6)$

$= \text{a product of four(even) transpositions}$

$= \text{an even permutation}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 3 & 7 & 6 \end{pmatrix} = (1\ \ 2\ \ 4)(3\ \ 5)(6\ \ 7) = (1\ \ 2)(1\ \ 4)(3\ \ 5)(6\ \ 7)$

$= \text{a product of four(even) transpositions}$

$= \text{an even permutation}$

(iii) $h = (1\ \ 3\ \ 5\ \ 4\ \ 6\ \ 2) = (1\ \ 3)(1\ \ 5)(1\ \ 4)(1\ \ 6)(1\ \ 2)$

$= \text{a product of five(odd) transpositions}$

$= \text{an odd permutation}$

**Example 4:** Determine the orders of the following cycles:

(i) $f = (1\ \ 2\ \ 5\ \ 6\ \ 4)(3\ \ 7\ \ 8)$ (ii)$g = (3\ \ 4\ \ 5)(\ 1\ \ 2\ \ 6\ \ 7)$(iii)$h = (1\ \ 3\ \ 5\ \ 4\ )(2\ \ 7\ \ 6\ \ 8)$

**Solution**: We have

(i) $o(f) = o\big((1\ \ 2\ \ 5\ \ 6\ \ 4)(3\ \ 7\ \ 8)\big) = \text{LCM of 5 and 3} = 15$

(ii) $o(g) = o((3\ \ 4\ \ 5)(\ 1\ \ 2\ \ 6\ \ 7)) = \text{LCM of 3 and 4} = 12$

(iii) $o(h) = o\big((1\ \ 3\ \ 5\ \ 4\ )(2\ \ 7\ \ 6\ \ 8)\big) = \text{LCM of 4 and 4} = 4$

**Example 5:** Write all the elements in $S_4$ and $A_4$.

**Solution**: $S_4$ has 4!=24 permutations. Here all the permutations in $S_4$ are listed below in the form of cycles or product of disjoint cycles.

(1), (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2 3), (1 3 2) , (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2).

And the 12 even permutations in $A_4$ are given below in the form of cycles or product of disjoint cycles:

(1), (1 2 3), (1 3 2) , (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3).

## Exercises

1. Find the orders of (i) the alternating group $A_6$ and (ii) the symmetric group$S_6$.
2. Is the group $S_3$ Abelian? Justify your answer.
3. Consider the following permutations in $S_6$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 2 & 5 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 4 & 6 \end{pmatrix}$$

Then,

(a) Find $\alpha\beta$, $\alpha^2\gamma$, $\beta\gamma^{-2}$, $\alpha\beta\alpha^{-1}$, $\beta^{-6}$

(b) Express α, β, γ as products of disjoint cycles and hence find their orders.

(c) Express $\alpha$, $\beta$, $\gamma$ as products of transpositions and hence determine whether they are odd or even permutations.

4. What is the order of the product of a pair of disjoint cycles of lengths 4 and 6?
5. Express each of the following permutations as a product of disjoint cycles:
   (a) (1 2 4 3) (4 2 5)
   (b) (1 3 2 5 6) (2 3) (4 6 5 1 2)
   (c) (1 2) (1 3) (2 3) (3 4 1)
6. What is the order of each of the following permutations:
   (a) (1 4 3) (2 6 5 7)
   (b) (2 3 4 5) ( 1 6 7)
   (c) (1 2 4) ( 3 5 7 8 6 9)
   (d) (1 2 3 5) (2 4 5 6 7)
   (e) (3 4 5) (2 4 5)
7. Express the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}$ as a product of transpositions and as a product of disjoint cycles. Is this an element of the alternating group $A_6$? What is the inverse and the order of $\alpha$?
8. If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 2 & 5 \end{pmatrix}$, then find $\sigma^{100}$ and $\sigma^{-105}$. Also find their orders.
9. Write all the even permutations in $S_3$. Is $S_3$ a non-Abelian group?
10. Show that a cycle containing odd number of symbols is an even permutation and a cycle containing even number of symbols is an odd permutation.