IMS™
(INSTITUTE OF MATHEMATICAL SCIENCES)
IAS/IFoS MATHEMATICS by K. Venkanna

Set-II

Permutation groups

→ We construct some finite groups whose elements, called permutations, act on finite sets.

- These groups will provide us with examples of finite non-abelian groups.
- The notion of a permutation of a set as a rearrangement of the elements of the set.

Now for the set $\{1,2,3,4,5\}$.

a rearrangement of the elements could be given below schematically as:

(i)	(ii)
$1 \to 4$	$1 \to 3$
$2 \to 2$	$2 \to 2$
$3 \to 5$	$3 \to 4$
$4 \to 3$	$4 \to 5$
$5 \to 1$	$5 \to 3$

Let us think of the diagram (i) as a function mapping of each element listed in the left coloumn in a single (not necessarily different) element from the same set listed at the right.

Furthermore, to be a permutation of the set, this mapping must be such that each element appearing in the right coloumn once and only once.

The diagram in fig (ii) doesnot give a permutation, for 3 appears twice while 1 doesnot appear at all in the right coloumn.

We now define a permutation to be such a mapping.

Defn: A permutation of a set A is a function $\phi : A \to A$ that is both one-one and onto.

(or)

Suppose A is a finite set having 'n' distinct elements. Then a 1-1 mapping of A onto itself is called a permutation of degree 'n'.

→ The number of elements in the finite set A is known as the degree of permutation.

Symbols for permutations:

Let $A = \{a_1, a_2, \ldots a_n\}$ be a finite set.

If $\phi : A \to A$ is 1-1 and onto then ϕ is a permutation of degree 'n'.

I. Let $\phi(a_1) = b_1$, $\phi(a_2) = b_2 \ldots\ldots \phi(a_n) = b_n$

where $\{b_1, b_2, \ldots b_n\} = \{a_1, a_2, \ldots a_n\}$

i.e, $b_1, b_2, \ldots b_n$ is some arrangement of n elements $a_1, a_2, \ldots a_n$.

II. we can introduce a two-line notation.

i.e, $\phi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$

i.e, each element in the second row is the ϕ image of the element the first row lying directly above it.

Ex: Let $A = \{1, 2, 3, 4\}$

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

Here the elements 1, 2, 3, 4 have been replaced by 2, 4, 1, 3 respectively.

$\phi(1) = 2$, $\phi(2) = 4$, $\phi(3) = 1$ & $\phi(4) = 3$

Equality of two permutations:

Two permutations f and g of degree 'n' are said to be equal if $f(a) = g(a)\ \forall a \in S$. where S is a finite set of 'n' distinct elements.

Ex: If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

Here $f = g$.

∵ In both cases 1 is replaced by 2, 2 by 3, 3 by 4 and 4 by 1) (35)

Note: The interchange of coloumns doesnot change the permutation.

Ex: If $f = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$

then $f = \begin{pmatrix} a_2 & a_1 & a_3 \\ b_2 & b_1 & b_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_3 & a_2 \\ b_1 & b_3 & b_2 \end{pmatrix}$ etc.

Total no. of distinct permutations of degree 'n':

If S is a finite set having 'n' distinct elements, then we have $n!$ distinct arrangements of the elements of S. Therefore there will be $n!$ distinct permutations of degree 'n'.

— If P_n be the set consisting of all permutations of degree 'n', then the P_n will have $n!$ distinct elements.

This set P_n is called the symmetric set of permutations of degree 'n'.

sometimes it is denoted by S_n.

i.e $P_n = \{f : f$ is a permutation of degree $n\}$.

Ex: The set P_3 of all permutations of degree 3 will have $3!$ (i.e, 6) elements.

i.e, $P_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$.

Identity permutation:

Identity permutation on $S = \{a_1, a_2, \ldots a_n\}$ in S_n is denoted by I.

where $I = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ (or) $\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$.

$b_1, b_2, \ldots b_n$ are nothing but the elements $a_1, a_2, \ldots a_n$ of S in some order.

If $S = \{1, 2, 3, 4, 5\}$ then Identity permutation on S is $I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 1 & 5 & 2 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ etc.

Product of permutations (or) Multiplication of permutations (or) Composition of permutations in S_n:

Let S_n be the set of all permutations of degree 'n'.

Let $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ and $g = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$ be any two permutations of S_n.

Here $b_1, b_2, \ldots b_n$ or $c_1, c_2, \ldots c_n$ are nothing but the elements $a_1, a_2, \ldots a_n$ of S in some order.

Now $f(a_1) = b_1$, $g(b_1) = c_1$; $f(a_2) = b_2$, $g(b_2) = c_2$ etc.

By defn, we have

$$c_1 = g(b_1) = g(f(a_1)) = (gf)(a_1)$$

i.e, $(gf)(a_1) = c_1$

Similarly $(gf)(a_2) = c_2, \ldots (gf)(a_n) = c_n$.

$$\therefore gf = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

$\therefore gf$ is also a permutation of degree 'n' on S and hence $gf \in S_n$ for $g, f \in S_n$.

→ **Ex:** If $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ then $AB = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$(\because (AB)(1) = A(B(1)) = A(3) = 1$ etc.

and $BA = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $(\because (BA)(1) = B(A(1)) = B(2) = 1$ etc$)$

→ If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$

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

$\therefore fg \neq gf$.

$\therefore$ Multiplication of permutations is not commutative

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

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

Similarly $If = f$.

Note: Some times we may have $fg = gf$.

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

then $fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = gf$.

Multiplication of permutations is associative:

If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$

then $(fg)h = f(gh)$.

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

$(fg)h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$ and $f(gh) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$

Inverse of a permutation:

Inverse of a permutation is also a permutation (bijection).

If $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ then its inverse, denoted by

f^{-1} is $\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ $\left(\because f(a_1) = b_1,\ f^{-1}(b_1) = a_1 \text{ etc}\right)$

Also $f^{-1}f = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} = I$$

Similarly $ff^{-1} = I$.

Note: 1. The set S_n of all permutations on n symbols is a finite group of order $n!$ w.r.t multiplication of permutations.
for $n \leq 2$, the group is abelian and for $n \geq 3$ the group is non-abelian.

2. To write the inverse of a permutation, write the 2^{nd} row as 1^{st} row and 1^{st} row as 2^{nd} row.

3. The group S_n of all permutations of degree 'n' is called the symmetric group of degree 'n' or the symmetric group of order $n!$.

problem → Show that the set P_3 (or S_3) of all permutations on three symbols 1, 2, 3 is a finite non-abelian group of order 6 w.r.t Permutation multiplication as composition.

Soln: we have

$$P_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

where

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ and } f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Now Construct the composition table:

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

$f_1 f_1 = f_1$, $f_1 f_2 = f_2 f_1 = f_1$, $f_1 f_3 = f_3 f_1 = f_3$,
$f_1 f_4 = f_4 f_1 = f_4$, $f_1 f_5 = f_5 f_1 = f_5$, $f_1 f_6 = f_6 f_1 = f_6$.

$f_2 f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$

$f_2 f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5$

$f_2 f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_6$

$f_2 f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_3$

$f_2 f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4.$

$f_3 f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_6$

$f_3 f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$

$f_3 f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5$

$f_3 f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4$

$f_3 f_6 = f_2.$

$f_4 f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5$

$f_4 f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_6$

$f_4 f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$

$f_4 f_5 = f_2$ and $f_4 f_6 = f_3.$

$f_5 f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4$ and so on.

(i) Since all the entries in the composition table are elements of P_3.

$\therefore P_3$ is closed w.r.t multiplication of permutations

(ii) multiplication of permutations is an associative

(iii) From the composition table the first row coincides with the top row.

Here identity permutation f_1 is the identity element.

Since $f_1 f_1 = f_1$, $\underset{=f_2 f_1}{f_1 f_2 = f_2}$, $\underset{=f_3 f_1}{f_1 f_3 = f_3}$, $f_1 f_4 = f_4 = f_1 f_4$ and so on.

(iv) In the composition table, every row and every coloumn contains the identity element.

Here $f_1 f_1 = f_1$, $f_2 f_2 = f_1$, $f_3 f_3 = f_1$, $f_4 f_4 = f_1$, $f_5 f_6 = 1 = f_6 f_5$.

(v) The composition is not commutative.

Since $f_4 f_2 = f_5$ & $f_2 f_4 = f_6$.

$\therefore f_4 f_2 \neq f_2 f_4$.

$\therefore P_3$ is a finite non-abelian group of order 6 w.r.t permutation multiplication.

Orbits and cycles of a permutation:

Defn: Consider a set $S = \{a_1, a_2, \ldots a_n\}$ and a permutation f on S. If for $a \in S$, there exists a smallest positive integer 'l' depending on 'a' such that $f^l(a) = a$ then the set $\{a_1, f^1(a), f^2(a), \ldots f^{l-1}(a)\}$ is called the orbit of 'a' under the permutation f. The ordered set $\{a, f^1(a), f^2(a), \ldots f^{l-1}(a)\}$ is called a cycle of f.

Ex: Consider $S = \{1, 2, 3, 4, 5, 6\}$ and a permutation on S be $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$

Now we have $f^1(1) = 2$, $f^2(1) = f(2) = 1$

$\therefore$ orbit of 1 under $f = \{1, f(1)\} = \{1, 2\}$

we have $f^1(2) = 1$, $f^2(2) = f(1) = 2$

$\therefore$ orbit of 2 under $f = \{2, f(2)\} = \{2, 1\}$

we have $f(3) = 3$

$\therefore$ orbit of 3 under $f = \{3\}$

we have $f^1(4) = 5$, $f^2(4) = f(5) = 6$, $f^3(4) = f(6) = 4$.

$\therefore$ orbit of 4 under $f = \{4, 5, 6\}$

we have $f(5) = 6$, $f^2(5) = f(6) = 4$, $f^3(5) = f(4) = 5$.

$\therefore$ orbit of 5 under $f = \{5, 6, 4\}$.

we have $f^1(6) = 4$, $f^2(6) = 5$, $f^3(6) = 6$.

$\therefore$ Orbit of 6 under $f = \{6, 4, 5\}$

Hence the cycles of f are $(1, 2)$, (3), $(4, 5, 6)$

Cyclic permutations:

Defn: Consider a set $S = \{a_1 a_2 \ldots a_n\}$ and a permutation $f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_k & a_{k+1} & \ldots & a_n \\ a_2 & a_3 & a_4 & \ldots & a_1 & a_{k+1} & \ldots & a_n \end{pmatrix}$ on S.

i.e, $f(a_1) = a_2,\ f(a_2) = a_3, \ldots\ldots f(a_k) = a_1,\ f(a_{k+1}) = a_{k+1}, \ldots\ldots f(a_n) = a_n$.

This type of permutation f is called a cyclic permutation of length k and degree n.

It is represented by $(a_1, a_2, \ldots a_k)$ or $(a_1\, a_2 \ldots a_k)$ which is a cycle of length k or k-cycle.

→ Also we can write the cycle $(a_1\, a_2 \ldots a_k)$ as $(a_2\, a_3 \ldots a_k\, a_1)$ or $(a_3\, a_4 \ldots a_k\, a_1\, a_2)$ etc.

Ex:

① $S = \{1, 2, 3, 4, 5, 6\}$ then a permutation of f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 5 & 2 \end{pmatrix}$

It can be written as $(1\,3\,4\,6\,2)$.

Since $f(1) = 3,\ f(3) = 4,\ f(4) = 6,\ f(6) = 2,\ f(2) = 1$ and $f(5) = 5$.

f is a cycle of length 5.

f can also be written as $(3\ 4\ 6\ 2\ 1)$ or $(4\ 6\ 2\ 1\ 3)$ etc.

following the cycle order.

Ex② If $S = \{1, 2, 3, 4, 5, 6, 7\}$ then a permutation f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix}$. It can be written as $(1\ 3\ 5\ 7)$

$\therefore f$ is cycle of length 4.

f can be written as $(3\ 5\ 7\ 1)$ or $(5\ 7\ 1\ 3)$ or $(7\ 1\ 3\ 5)$

Ex③ If $S = \{1, 2, 3, 4, 5, 6\}$ then the permutation f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}$.

f is not cyclic permutation

Since $f(1) = 4,\ f(4) = 1,\ f(2) = 3,\ f(3) = 5,\ f(5) = 2,\ f(6) = 6$.

Note: [1]. A cyclic permutation doesnot change by changing the places of its elements provided their cyclic order, is not changed.

[2]. A cycle of length 1 is the identity permutation since $f(a_1)=a_1$, $f(a_2)=a_2$, ---- $f(a_n)=a_n$.

Transposition:

Defn: A cycle of length '2' is called a transposition.

Ex: If $S=\{1,2,3,4,5\}$ and a permutation f on S is $\begin{pmatrix}1&2&3&4&5\\1&3&2&4&5\end{pmatrix}$ then $f=(2,3)$ is a cycle of length 2 and degree 5.

Observe that $f(2)=3$, $f(3)=2$ and the image of each element is itself (i.e, the remaining missing elements are left unchanged)

Here $f^{-1}=(3\,2)=(2\,3)$

i.e, $f^{-1}=f$.

i.e, the transposition is itself.

Disjoint cycles:

Let $S=\{a_1\,a_2\,\text{----}\,a_n\}$. If f, g be two cycles on S such that they have no common elements, then they are called disjoint cycles.

Ex: Let $S=\{1,2,3,4,5,6,7\}$

(i) If $f=(1\,3\,7)$ and $g=(2\,4\,5)$ then f, g are disjoint cycles.

(ii) If $f=(1\,3\,7)$ and $g=(2\,3\,4\,5)$ then f, g are not disjoint cycles.

→ Product of two cycles over the same set $S=\{1,2,3,4,5,6\}$.

Ex: $f=(1\,4\,3)$, $g=(2\,5)$

Now we find products gf, fg.

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

(INSTITUTE OF MATHEMATICAL SCIENCES) IMS TM

Also $gf = (2\ 5)(1\ 4\ 3)$

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

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

$\therefore fg = gf.$

Note 1. If f & g are two disjoint cycles then $fg = gf$.
i.e, the product of disjoint cycles is commutative.

2. we leave identity permutation (s) while writing the product of cycles.

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

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

$= (1\ 5\ 2)(3\ 4)$ ($\because$ (6) is the identity permutation and it need not be shown).

$= (3\ 4)(1\ 5\ 2)$

Observe that $(3\ 4)$, $(1\ 5\ 2)$ are disjoint cycles.

Ex: $f = (2\ 3\ 6)$, $g = (1\ 4\ 6)$.
Now we find products fg, gf.

$\therefore fg = (2\ 3\ 6)(1\ 4\ 6)$

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

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

and $gf = (1\ 4\ 6)(2\ 3\ 6)$

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

observe that f, g are not disjoint and $fg \neq gf$.

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

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

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

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

Ex: $(3\ 4)(3\ 5)(3\ 6) = (3\ 4)(3\ 6\ 5)$
$= (3\ 6\ 5\ 4)$

and $(3\ 4)(3\ 5)(3\ 6) = (3\ 5\ 4)(3\ 6)$
$= (3\ 6\ 5\ 4)$

Ex: If $f = (1\ 3\ 4)$, $g = (2\ 3)$, $h = (5\ 4\ 2)$
then we have $(fg)h = f(gh)$.

Inverse of a cyclic permutation:

Ex: 1) If $f = (2\ 3\ 4\ 1)$ of degree 5, then $f^{-1} = (1\ 4\ 3\ 2)$

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

2) If $f = (1\ 3\ 4\ 6)$ is a cyclic permutation on 6 symbols, its inverse $f^{-1} = (6\ 4\ 3\ 1)$
$= (4\ 3\ 1\ 6)$ etc.

3) If $f = (1\ 2\ 3\ 4\ 5\ 8\ 7\ 6)$, $g = (4\ 1\ 5\ 6\ 7\ 3\ 2\ 8)$ are cyclic permutations then show that $(fg)^{-1} = g^{-1}f^{-1}$.

Now $fg = (1\ 2\ 3\ 4\ 5\ 8\ 7\ 6)(4\ 1\ 5\ 6\ 7\ 3\ 2\ 8)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 8 & 1 & 6 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 2 & 1 & 6 & 7 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 3 & 2 & 1 & 6 & 4 & 5 \end{pmatrix}$$

and $(fg)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 3 & 7 & 8 & 6 & 2 & 1 \end{pmatrix}$

Also $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 2 & 3 & 4 & 7 & 8 & 5 \end{pmatrix}$ and $g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 8 & 1 & 5 & 6 & 2 \end{pmatrix}$

$\therefore g^{-1}f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 3 & 7 & 8 & 6 & 2 & 1 \end{pmatrix}$

$\therefore (fg)^{-1} = g^{-1}f^{-1}$

(4) If $f=(1\,3\,4)$, $g=(2\,3)$, $h=(5\,4\,2)$ then we have (i) $(fg)^{-1}=g^{-1}f^{-1}$ and (ii) $(fgh)^{-1}=h^{-1}g^{-1}f^{-1}$. (40)

Order of a cyclic permutation:

Ex: If $A=\{1,2,3,4\}$ and $f=(2\,1\,3)$ then

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

i.e, $(2\,1\,3)(2\,1\,3)=(2\,3\,1)$

Now $f^3=f^2f$

$=(2\,3\,1)(2\,1\,3)$

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

$\therefore$ If f is a cycle of length 3 and degree 4 then $f^3=I$ and hence the order of f is 3.

Ex: If $f=(1\,2\,3\,4\,5)$ then $f^2=(1\,3\,5\,2\,4)$

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

$f^4=(1\,5\,4\,3\,2)$ and $f^5=I$.

$\therefore$ If f is a cycle of length 5 and degree 5 then $f^5=I$ and hence the order of f is 5.

→ Every permutation can be expressed as a product of disjoint cycles.

Ex: Let $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&4&8&6&9&7&5\end{pmatrix}$ be a permutation of degree 9 on the set $\{1,2,3,\ldots\ldots 9\}$.

we have $f=(1\,2\,3)(4)(5\,8\,7\,9)(6)$.

$=(1\,2\,3)(5\,8\,7\,9)$.

Ex: write down the following products as disjoint cycles.

(i) $(1\,3\,2)(5\,6\,7)(2\,6\,1)(4\,5)$

(ii) $(1\,3\,6)(1\,3\,5\,7)(6\,7)(1\,2\,3\,4)$.

Solⁿ (i) $(1\ 3\ 2)(5\ 6\ 7)(2\ 6\ 1)(4\ 5)$

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

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

Since 7 is the maximum in any cycle, we take every cycle as a permutation of a degree 7.

→ Express the product $(4\ 5)(1\ 2\ 3)(3\ 2\ 1)(5\ 4)(2\ 6)(1\ 4)$ on 6 symbols as the product of disjoint cycles

Solⁿ: $(4\ 5)\underline{(1\ 2\ 3)(3\ 2\ 1)}(5\ 4)(2\ 6)(1\ 4)$

$= (4\ 5)(5\ 4)(2\ 6)(1\ 4)$

$(\because (3\ 2\ 1)^{-1} = (1\ 2\ 3)$ and $(3\ 2\ 1)^{-1}(3\ 2\ 1) = I$

$= (2\ 6)(1\ 4)$ $\quad (\because (5\ 4)^{-1} = (4\ 5))$

→ Every cycle can be expressed as a product of transpositions.

Ex: Let $f = (2\ 4\ 3)$ of degree 4.

Then $f = (2\ 3)(2\ 4)$

$$\left(\because \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3)\right)$$

Also we have

$f = (2\ 3)(1\ 2)(2\ 1)(2\ 4)$

$f = (1\ 3)(3\ 1)(2\ 3)(2\ 4)$

$f = (1\ 3)(3\ 1)(2\ 3)(1\ 4)(4\ 1)(2\ 4)$ etc.

Also $f = (4\ 3\ 2)$

∴ we can have

$f = (4\ 2)(4\ 3)$

$f = (3\ 1)(1\ 3)(4\ 2)(1\ 2)(2\ 1)(4\ 3)$ etc.

∴ Every cycle can be expressed as a product of transpositions in many ways.

Ex: Let $f = (1\,2\,3\,4)$

we have $f = (1\,4)(1\,3)(1\,2)$

Also $f = (2\,3\,4\,1)$

we have $f = (2\,1)(2\,4)(2\,3)$ etc.

Ex: Let $f = (a_1\, a_2 \ldots\ldots a_n)$

we can have

$$f = (a_1\, a_n)(a_1\, a_{n-1}) \ldots\ldots (a_1\, a_3)(a_1\, a_2).$$

i.e, a cycle of length 'n' may be expressed as a product of $(n-1)$ transpositions.

Note:

In the case of any cycle the number of transpositions is either always odd or always even.

→ Every permutation can be expressed as a product of transpositions in many ways.

Even and odd permutation

A permutation is said to be an even (odd) permutation if it can be expressed as a product of an even (odd) number of transpositions.

Note: $\boxed{1}$. If f is expressed as a product of 'n' transpositions then 'n' is even or 'n' is odd but not both and n is unique.

In otherwords, a permutation can be expressed as a product of an even number of transpositions or an odd number of transpositions. Hence the permutation group S_n on 'n' symbols can be split up into two disjoint sets, namely, the set of even permutations and the set of odd permutations.

→ Every transposition is an odd permutation.

- Identity permutation I is always an even permutation.

  Since I can be expressed as a product of two transpositions.

  Ex: $I = (1\ 2)(2\ 1)$
  $= (1\ 2)(2\ 1)(1\ 3)(3\ 1)$ etc.

→ A cycle of length 'n' can be expressed as a product of $(n-1)$ transpositions.

- If 'n' is odd, then the cycle can be expressed as a product of even number of transpositions.

- If 'n' is even, then the cycle can be expressed as a product of odd number of transpositions.

→ The product of two odd permutations is an even permutation.

Proof: Let f, g be two odd permutations.
Let f can be expressed as a product of r (odd) transpositions and g can be expressed as a product of s (odd) transpositions.
$\therefore gf$ can be expressed as $r+s$ i.e, even number of transpositions.
$\therefore gf$ is even.

Note: $\boxed{1}$. The product of two even permutations is an even permutation.

$\boxed{2}$. The product of an odd permutation and an even permutation is an odd permutation.

→ The inverse of an odd permutation is an odd permutation.

proof: Let f be an odd permutation and I be the identity permutation.

$\therefore f^{-1}$ is also a permutation and $f^{-1}f = ff^{-1} = I$.

Since I is even permutation and f is odd permutation.

$\therefore f^{-1}$ is must be an odd permutation.

Note: The inverse of an even permutation is an even permutation.

→ Let S_n be the permutation group on 'n' symbols. Then of the $n!$ permutations (elements) in S_n, $\frac{1}{2}n!$ are even permutations and $\frac{1}{2}n!$ are odd permutations.

proof: Let $S_n = \{e_1, e_2, \ldots e_p, o_1, o_2, \ldots o_q\}$ be the permutation group on 'n' symbols where $e_1, e_2, \ldots e_p$ are even permutations and $o_1, o_2, \ldots o_q$ are odd permutations.

($\because$ any permutation can be either even or odd but not both).

$\therefore p + q = n!$

Let $t \in S_n$ and t be a transposition.

Since permutation multiplication follows Closure law in S_n.

we have

$te_1, te_2, \ldots te_p, to_1, to_2, \ldots to_q$ as elements of S_n.

Since t is an odd permutation.

$\therefore te_1, te_2, \ldots te_p$ are all odd and $to_1, to_2, \ldots to_q$ are all even.

Here no two of the permutations $te_1, te_2, \ldots te_p$ are equal.

Because $te_i = te_j$ for $i \le p$, $j \le p$.

Since S_n is a group,
by LCL $e_i = e_j$ which is absurd.
$\therefore te_i \neq te_j$ for $i \leq p$, $j \leq 8$ and hence the 'p' permutations $\therefore te_1, te_2, \ldots te_p$ are all distinct odd permutations in S_n.

But S_n contains exactly 'q' odd permutations.

$\therefore p \leq q$ —— (1)

Similarly we can show that q even permutations $to_1, to_2, \ldots to_q$ are all distinct even permutations in S_n.

$\therefore q \leq p$ —— (2)

from (1) & (2) we have

$$p = q = \frac{n!}{2} \quad (\because p + q = n!)$$

$\therefore$ Number of even permutations in S_n
= Number of odd permutations in S_n
$= \frac{n!}{2}$

Defn: Let S_n be the permutation group on 'n' symbols. The set of all $\frac{n!}{2}$ even permutations of S_n denoted by A_n, is called the alternating set of permutations of degree 'n'.

Theorem: The set A_n of all even permutations of degree 'n' forms a group of order $\frac{n!}{2}$ w.r.t permutation multiplication.

proof: (i) Closure: Let $f, g \in A_n$.
then f, g are even permutations.
$\therefore gf$ is an even permutation.
$\therefore gf \in A_n$.

(ii) Associativity: Since a permutation is a bijection, multiplication of permutations (composition of mappings) is associative.

(iii) Existence of left identity:

Let $f \in A_n$.
Let I be the identity permutation on the 'n' symbols then $I \in A_n$.

Since I is an even permutation.

$\therefore If = f$ for $f \in A_n$.

$\therefore$ Identity exists in A_n and I is the identity in A_n.

(iv) Existence of left inverse:

Let $f \in A_n$

Since f is even permutation.

$\therefore f^{-1}$ is also even permutation on 'n' symbols

$\therefore f^{-1}f = I$ for $f \in A_n$.

$\therefore$ Every element of A_n is invertible and inverse of f is f^{-1}.

$\therefore A_n$ forms a group of order $\frac{n!}{2}$.

($\because$ the number of permutations on 'n' symbols is $\frac{n!}{2}$)

Note: 1. The group A_n is called an alternating group (or) alternating group of degree 'n' and the number of elements in A_n is $\frac{n!}{2}$

2. The product of two odd permutations is an even permutation and hence the set of odd permutations w.r.t permutation multiplication is not a group.

Ex: Examine whether the following permutations are even or odd.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$

(iii) $(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(4\ 5)$.

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

$= (1\ 7)(1\ 6)(1\ 5)(1\ 4)(1\ 3)$

(product of 5 transpositions.)

$\therefore$ The permutation is odd.

→ Express $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$ as a product of transpositions.

→ write down the inverses of the following permutations.

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

Ans: $(6\ 1\ 5\ 2)(7\ 3)$

→ write down the following permutations as products of disjoint cycles.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 4 & 8 & 2 & 6 & 5 \end{pmatrix}$ (ii) $(1\ 3\ 2\ 5)(1\ 4\ 3)(2\ 5\ 1)$

(iii) $(4\ 3\ 1\ 2\ 5)(1\ 4\ 5\ 2)$

→ Express $(1\ 2\ 3)(4\ 5\ 6)(1\ 6\ 7\ 8\ 9)$ as a product of disjoint cycles. Find its inverse.

→ write down all the permutations on four symbols 1, 2, 3, 4 which of these permutations are even?

Sol: Let $S = \{1, 2, 3, 4\}$

There will be $4!$ permutations of degree 4.

i.e, 24 permutations then

If P_4 is the set of all permutations

$P_4 = \{ (1), (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$
$(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3),$
$(2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (2\ 3)(1\ 4),$
$(3\ 1)(2\ 4), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\ (1\ 3\ 2\ 4)$
$(1\ 3\ 4\ 2)\ (1\ 4\ 2\ 3), (1\ 4\ 3\ 2) \}$

If A_4 is the set of all even permutations of degree 4 then A_4 will have $\frac{4!}{2}$ i.e, 12 elements.

IMS (INSTITUTE OF MATHEMATICAL SCIENCES)

i.e, $A_4 = \{ (1), (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4),$ (144)
$(1\,4\,3), (2\,3\,4), (2\,4\,3), (1\,2)(3\,4), (2\,3)(1\,4)$
$(3\,1)(2\,4) \}$.

→ Show that the four permutations $I, (a\,b), (c\,d), (a\,b)(c\,d)$ on four symbols a, b, c, d form a finite abelian group w.r.t the permutation multiplication.

Solⁿ: Let $I = f_1$, $(a\,b) = f_2$, $(c\,d) = f_3$ and $(a\,b)(c\,d) = f_4$.

Let $G = \{f_1, f_2, f_3, f_4\}$.

Now construct the composition table.

→ Show that the eight permutations $(a), (a\,b\,c\,d), (a\,c)(b\,d), (a\,d\,c\,b), (a\,b)(c\,d), (b\,c)(a\,d), (b\,d), (a\,c)$ on four symbols a, b, c, d form a finite non-abelian group w.r.t permutation multiplication.

→ Show that the set G of four permutations $I, (1\,2)(3\,4), (1\,3)(2\,4)$ and $(1\,4)(2\,3)$ on four symbols $1, 2, 3, 4$ is abelian group. w.r.t the permutation multiplication.

(This group is known as the Klein-4-group)

→ prove that the set A_3 of three permutations $(a), (a\,b\,c), (a\,c\,b)$ on three symbols a, b, c forms a finite abelian group w.r.t the permutation multiplication

Imp. **Order of an n-cycle:**

Let $f = (1\,2\,3 \ldots n)$ be a cycle of length n.

Then f^2 moves every symbol two places along. Similarly f^3 moves every symbol three places along and f^n moves every symbol n places along

i.e, $f^n = (1)(2) \ldots \ldots (n)$

i.e, identity permutation.

$\therefore$ Order of f is n.

In particular

if $f = (1\,2\,3\,4\,5)$ then $f^2 = (1\,3\,5\,2\,4)$, $f^3 = (1\,4\,2\,5\,3)$

$f^4 = (1\,5\,4\,3\,2)$, $f^5 = (1)(2)(3)(4)(5)$ = Identity permutation.

$\therefore f^5 = I$

$\therefore o(f) = 5$.

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

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

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

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

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

$= (1\,4\,2\,5\,3)$

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

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

$= (1\,5\,4\,3\,2)$

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

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

Order of the product of the disjoint cycles of lengths $m_1, m_2, \ldots\ldots m_k$:

Suppose a permutation f is the product of disjoint cycles of lengths $m_1, m_2, \ldots\ldots m_k$.

The order of f will be the L.C.M. (least common multiple) of the integers $m_1, m_2, \ldots m_k$.

Ex: find the order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$

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

$= (1)(2\,3\,4)$

$\therefore o(f) =$ L.C.M of $1, 3$

$= 3$.

→ If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$, $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$, then find σ^{100} and μ^{100}.

Sol^n: $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 3 & 4 & 2 & 6 \\ 5 & 1 & 4 & 3 & 2 & 6 \end{pmatrix}$

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

$O(\mu) = \text{L.C.M}\,[\text{lengths of } (1\,5), (3\,4), (2), (6)]$

$= \text{L.C.M}\,[2, 2, 1, 1] = 2$

$\therefore O(\mu) = 2$

$\mu^2 = I$ (By defn of an order of element)

Thus $(\mu^2)^{50} = I^{50}$

$= I$

$\therefore \mu^{100} = I$

→ Let $\sigma = (1\ 3\ 5\ 7\ 11)(2\ 4\ 6) \in S_{11}$. What is the smallest +ve integer 'n' such that $\sigma^n = \sigma^{37}$.

(a) 3 (b) 5 (c) 7 (d) 11.

Sol^n: $O(\sigma) = \text{LCM of } 5 \,\&\, 3$

$= 15$

$\therefore \sigma^{15} = I$

$\therefore \sigma^{37} = (\sigma^{15})^2 \cdot \sigma^7$

$= I \cdot \sigma^7 = \sigma^7$

$\sigma^n = \sigma^{37} = \sigma^7$

$\Rightarrow \boxed{n = 7}$

→ Consider the permutation $\alpha = (1\ 2\ 3)(1\ 4\ 5)$ on the set $\{1, 2, 3, 4, 5\}$. What is the permutation α^{99}

(a) $(5\ 4\ 1)(3\ 2\ 1)$ (b) $(5\ 4\ 1)(1\ 2\ 3)$ (c) $(3\ 2\ 1)(5\ 4\ 1)$ (d) $(1\ 3\ 2)(1\ 5\ 4)$.

Sol^n: $\alpha = (1\ 2\ 3)(1\ 4\ 5) = (1\ 3)(1\ 2)(1\ 5)(1\ 4) = (1\ 4\ 5\ 2\ 3)$

$\alpha^5 = I \Rightarrow \alpha^{99} = (\alpha^5)^{20} \alpha^{-1}$

$= I(3\ 2\ 5\ 4\ 1)$

$= (3\ 2\ 5\ 4\ 1) = (5\ 4\ 1)(3\ 2\ 1)$

→ What is the number of distinct cycles of length > 1 in the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 7 & 6 & 3 & 4 & 1 \end{pmatrix}$?

(a) 2 b) 3 (c) 4 (d) 5

Ans: $\sigma = \begin{pmatrix} 1 & 5 & 3 & 7 & 2 & 4 & 6 \\ 5 & 3 & 7 & 1 & 2 & 6 & 4 \end{pmatrix} = (1\ 5\ 3\ 7)(2)(4\ 6)$.