Chapter 4

PERMUTATION GROUP

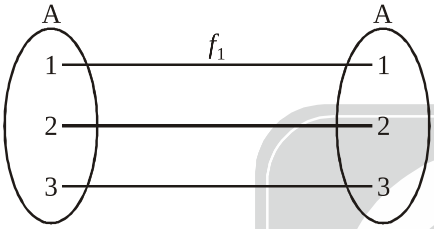
Permutation of *A*, Permutation Group of *A* :

A permutation of a set *A* is a function from *A* to *A* that is both one to one and onto.

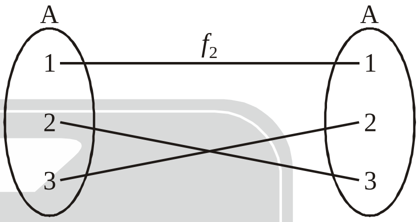
A permutation group of a set is a set of permutations of *A* that forms a group under function composition.

Ex. Let $A = \{1, 2, 3\}$. Then if we define all one-one onto functions from *A* to *A*. There will be total 6 possibilities as

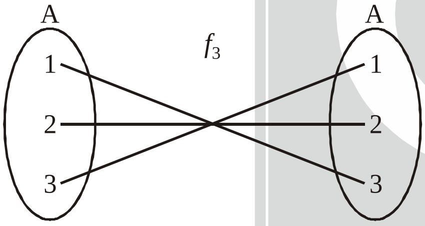
(1)



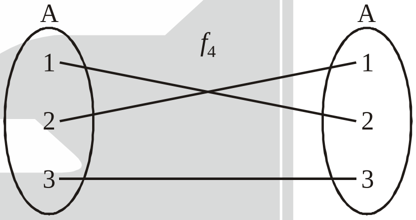
(2)



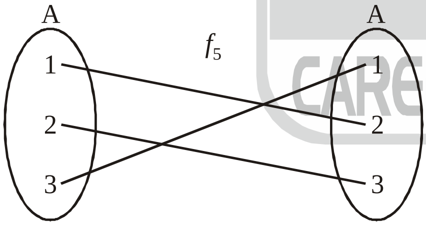
(3)



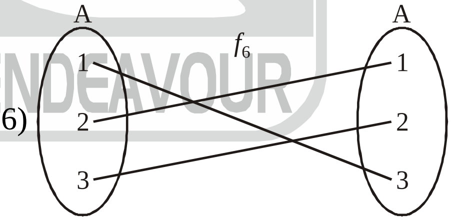
(4)



(5)



(6)



So, there are total 6 one-to-one onto homomorphism from *A* to *A*.

For example, we define a permutation α of the set {1, 2, 3, 4} by specifying

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

A more convenient way to express this correspondence is to write α in array form as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

Here $\alpha(j)$ is placed directly below *j* for each *j*. Similarly, the permutation β of the set $\{1, 2, 3, 4, 5, 6\}$ given by

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

is expressed in array form as $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$

2. **Equality of two permutations:** Two permutations *f* and *g* of degree *n* are said to be equal if we have $f(a) = g(a)\,\forall\, a \in S$.

For example, if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ are two permutations of degree 4, then we have $f = g$. Here we see that both *f* and *g* replace 1 by 2, 2 by 3, 3 by 4 and 4 by 1.

If $f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_n \\ b_1 & b_2 & b_3 \ldots & b_n \end{pmatrix}$ is a permutation of degree *n*, we can write it in several ways. The interchange of columns will not change the permutation. Thus we can write.

$$f = \begin{pmatrix} a_2 & a_1 & a_3 \ldots & a_n \\ b_2 & b_1 & b_3 \ldots & b_n \end{pmatrix} = \begin{pmatrix} a_n & a_1 \ldots & a_2 \\ b_n & b_1 \ldots & b_2 \end{pmatrix} = \begin{pmatrix} a_n & a_{n-1} \ldots a_2 & a_1 \\ b_n & b_{n-1} \ldots b_2 & b_1 \end{pmatrix} \text{ etc.}$$

For example, if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ are two permutations of degree 4, then by interchanging columns we can write $g = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

3. **Total number of distinct permutations of degree *n*.** If *S* is a finite set having *n* distinct elements, then we shall have *n*! distinct arrangements of the elements of *S*. Therefore there will be *n*! distinct permutations of degree *n*. If S_n be the set consisting of all permutations of degree *n*, then the set S_n will have *n*! distinct elements. This set S_n is called the symmetric set of permutations of degree *n*. Thus

$S_n = \{f : f \text{ is a permutation of degree } n\}$.

The set S_3 of all permutations of degree 3 will have 3! i.e., 6 elements. Obviously

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

4. **Identity Permutation:** If *I* is a permutation of degree *n* such that *I* replaces each element by the element itself, *I* is called the identity permutation of degree *n*.

Thus, $I = \begin{pmatrix} 1 & 2 & 3 \ldots n \\ 1 & 2 & 3 \ldots n \end{pmatrix}$ or $\begin{pmatrix} a_1 & a_2 & a_3 \ldots a_n \\ a_1 & a_2 & a_3 \ldots a_n \end{pmatrix}$ or $\begin{pmatrix} b_1 & b_2 & b_3 \ldots b_n \\ b_1 & b_2 & b_3 \ldots b_n \end{pmatrix}$

is the identity permutation of degree *n*.

5. **Product or composite of two permutations:** The product or composition of two permutations *f* and *g* of degree *n* denoted by *fg*, is obtained by first carrying out the operation defined by *g* and then by *f*.

For example, Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$ and $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$ then

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \uparrow \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

6. **Groups of Permutations:**

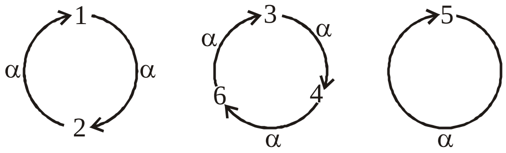
Theorem: The set S_n of all permutations on n symbol is a finite group of order $n!$ with respect to composition of mappings as the operation. For $n \le 2$, this group is abelian and for $n > 2$ it is always non-abelian.

7. **Cycle Notation:** There is another notation commonly used to specify permutations. It is called cycle notation and was first introduced by the great French mathematician Cauchy in 1815. Cycle notation has theoretical advantages in that certain important properties of the permutation can be readily determined when cyclic notation is used.

As an illustration of cycle notation, let us consider the permutation.

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

This assignment of values could be presented schematically as follows:



We can simply write $\alpha = (1\ 2)(346)(5)$. As second example, consider

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

In cycle notation, β can be written (2 3 1 5) (6 4) or (4 6) (3 1 5 2). An expression of the form $(a_1, a_2, ..., a_m)$ is called a cycle of length m or an m-cycle.

8. **Permutations represented by a cycle:** (1 3 4 2 6) is a cycle of length 5. Suppose it represents a permutation of degree 9 on a set S consisting of the elements 1, 2,...,9. Then the permutation represented will be

$$\begin{pmatrix} 1 & 3 & 4 & 2 & 6 & 5 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 1 & 5 & 7 & 8 & 9 \end{pmatrix}$$

i.e., the image of each element in the cycle (1 3 4 2 6) is the element which follows it, the image of the last element 6 is the first element 1 and the missing elements 5, 7, 8, 9 are their images themselves.

However, if the cycle (1 3 4 2 6) represents a permutation of degree 6 on six symbols 1, 2, 3, 4, 5, 6 then the corresponding permutation will be

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

Important Note: A cycle does not change by changing the places of its elements provided their cyclic order is not changed.

Thus (1 2 3 4) = (2 3 4 1) = (3 4 1 2) = (4 1 2 3)

Also (1 2) = (2 1), (2 3) = (3 2).

9. **Transpositions. Definition:** A cycle of length two is called a transposition. Thus the cycle (1 3) is a transposition. If the transposition (2, 3) is a permutation of degree 3 on three symbols 1, 2, 3 then the corresponding permutation will be

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

A cycle of length one means that the image of the element involved is the element itself and the missing elements are left unchanged. Thus all the elements are left unchanged. Therefore every cycle of length one will represent the identity permutation.

10. **Multiplication of Cycles.** We multiply cycles by multiplying the permutations represented by them. For example if the cycles (1 2 3) and (5 6 4 1) represent permutation of degree 6 on six symbols, 1, 2, 3, 4, 5, 6, then

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

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

Since, a cycle of length one represents the identity permutation, therefore (1) (2 3 4) (6) = (2 3 4).

11. **Disjoint Cycles:** Two cycles are said to be disjoint if they have no symbol in common. For example (123) and (45) are disjoint cycles

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

Proof : The cycles f and g have no symbols common. Therefore the elements permuted by f are left unchanged by g and also the elements permuted by g remain the same under f. Therefore we shall have $fg = gf$.

Now we shall give an example to illustrate this theorem. Let $f = (1\ 2\ 3)$ and $g = (4\ \ 5)$ represent two permutation on 5 symbols 1, 2,...,5.

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

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

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

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

Inverse of a cyclic permutation: To prove that $(1\ \ 2\ \ 3...n)^{-1} = (n\ \ n-1...3\ 2\ 1)$ i.e., to write the inverse of a cycle we should write its elements in the reverse order.

Proof : We have $(1\ \ 2\ \ 3...n)(n...3\ \ 2\ \ 1)$

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

Also $(n...3\ \ 2\ \ 1)\ (1\ \ 2\ \ 3...n) = I$

$\therefore\ (1\ \ 2\ \ 3...n)^{-1} = (n...3\ \ 2\ \ 1)$

In particular, every transposition is its own inverse. If (1 2) is a transposition, then $(1\ \ 2)^{-1}$ = (2 1) = (1 2).

Inverse of a product of cyclic permutations. If f and g are any two cycles, then we have

$(fg)^{-1} = g^{-1}f^{-1}$. Also $(fgh)^{-1} = h^{-1}g^{-1}f^{-1}$

If f and g are disjoint cycles then $(fg)^{-1} = (gf)^{-1} = f^{-1}g^{-1}$

Thus $[(1\ \ 2\ \ 3)(4\ \ 5)(7\ \ 6)]^{-1} = (7\ \ 6)^{-1}\ (4\ \ 5)^{-1}\ (1\ \ 2\ \ 3)^{-1}$

= (6 7) (5 4) (3 2 1)

Also, $[(1\ \ 3\ \ 5)(2\ \ 4)]^{-1} = (1\ \ 3\ \ 5)^{-1}\ (2\ \ 4)^{-1}$ = (5 3 1) (4 2).

We shall now give some important results on the product of permutations.

12. **Theorem: Products of Disjoint Cycles:** Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Ex. Write to the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 3 & 5 & 8 & 6 & 2 & 1 \end{pmatrix}$ **in disjoint cycles.**

Soln. $\begin{pmatrix} 1 & 4 & 5 & 8 \\ 4 & 5 & 8 & 1 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 7 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 3 \end{pmatrix} \begin{pmatrix} 6 \\ 6 \end{pmatrix} = (1 \quad 4 \quad 5 \quad 8) \; (2 \quad 7)$

Remarks :

(*i*) 1-cycles does not effect to the permutation if we do not write them in product of disjoint cycles.

(*ii*) We can express above expression in transpositions as $(1 \quad 4 \quad 5 \quad 8) = (1 \quad 4)\;(1 \quad 5)\;(1 \quad 8)$

so, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 3 & 5 & 8 & 6 & 2 & 1 \end{pmatrix} = (1 \quad 4)\;(1 \quad 5)\;(1 \quad 8)\;(2 \quad 7)$

13. **Theorem: Disjoint cycles commute:** If the pair of cycles $\alpha = (a_1, a_2, ..., a_m)$ and $\beta = (b_1, b_2, ..., b_n)$ have no entries in common then $\alpha\beta = \beta\alpha$.

14. **Theorem: Order of a Permutation (Ruffini-1799):** The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Proof: First, observe that a cycle of length *n* has order *n*. (Verify this yourself). Next, suppose that α and β are disjoint cycles of lengths *m* and *n*, and let *k* be the least common multiple of *m* and *n*. It follows from theorem that both α^k and β^k are the identity permutation *e* and, since α and β commute, $(\alpha\beta)^k = \alpha^k\beta^k$ is also the identity. Thus, we know that $a^k = e$ implies that $o(a)$ divides *k*.

$\Rightarrow$ The order of $\alpha\beta$ - let us call it '*t*' must divide *k*. But then $(\alpha\beta)^t = \alpha^t\beta^t = e$, so that $\alpha^t = \beta^{-t}$. However, it is clear that if α and β have no common symbol, the same is true for α^t and β^{-t}, since raising a cycle to a power does not introduce new symbols. But, if α^t and β^{-t} are equal and have no common symbols, they must both be the identity, because every symbol in α^t is fixed by β^{-t} and vice versa (remember that a symbol not appearing in a permutation is fixed by the permutation). It follows, then, that both *m* and *n* must divide *t*. This means that *k*, the least common multiple of *m* and *n*, divides *t* also. This shows that *k* = *t*.

Thus far, we have proved that the theorem is true in the cases where the permutation is a single cycle or a product of two disjoint cycles. The general case involving more than two cycles can be handled in an analogous way.

15. **Theorem: Product of 2-cycles:** Every permutation in $S_n, n > 1$, is a product of 2-cycles.

Proof: First, note that the identity can be expressed as (12) (12)

We know that every permutation can be written in the form $(a_1a_2...a_k)(b_1b_2...b_t)...(c_1c_2...c_s)$

Direct computation shows that this is the same as

$(a_1a_k)(a_1a_{k-1})...(a_1a_2)(b_1b_t)(b_1b_{t-1})...(b_1b_2)...(c_1c_s)(c_1c_{s-1})...(c_1c_2)$

This completes the proof.

The first decomposition in the following example demonstrates this technique. The other products in example show that the decomposition on permutation into a product of 2-cycles is not unique.

Example: (12345) = (15) (14) (13) (12)
= (45) (53) (25) (15)
= (21) (25) (24) (23)
= (54) (52) (21) (25) (23) (13)

Definition: Even and Odd Permutations: A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation.