Algebra: Chapter – 3

Permutations:

Let $S = \{a_1, a_2, \dots, a_n\}$ – a non-empty finite set. A bijective mapping on S, $i.e.\ f: S \to S$ is called a permutation.

Total number of such permutations is $n!$

[a_1 can be mapped to any one of $a_1,\ a_2, \dots,\ a_n$, $i.e.\ n$ ways; a_2 can be mapped to any one of $a_1,\ a_2, \dots,\ a_n$, except the one which a_1 is mapped to, $i.e.\ n-1$ ways; …… and so on]

Example: A permutation can be expressed as, $f = \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ f(a_1) & f(a_2) \dots . & \dots f(a_n) \end{pmatrix}$.

Example: Identity Permutation is written as, $i = \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ a_1 & a_2 \dots & \dots a_n \end{pmatrix}$.

Multiplication of permutations:

Let us assume,

$f = \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ f(a_1) & f(a_2) \dots . & \dots f(a_n) \end{pmatrix}$, $g = \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ g(a_1) & g(a_2) \dots . & \dots g(a_n) \end{pmatrix}$, $h = \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ h(a_1) & h(a_2) \dots . & \dots h(a_n) \end{pmatrix}$

Then,

$$\left.\begin{aligned} f.g &= \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ f[g(a_1)] & f[g(a_2)] \dots . & \dots f[g(a_n)] \end{pmatrix} \\ g.f &= \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ g[f(a_1)] & g[f(a_2)] \dots . & \dots g[f(a_n)] \end{pmatrix} \end{aligned}\right\} f.g \neq g.f$$

i.e. multiplication is not Commutative.

Also,

$$f.(g.h) = \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ f(a_1) & f(a_2) \dots . & \dots f(a_n) \end{pmatrix} . \begin{pmatrix} a_1 & a_2 & \dots & \dots & a_n \\ g[h(a_1)] & g[h(a_2)] & \dots & \dots & g[h(a_n)] \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \dots & \dots & a_n \\ f\{g[h(a_1)]\} & f\{g[h(a_2)]\} & \dots & \dots & f\{g[h(a_n)]\} \end{pmatrix} = (f.g).h$$

i.e. multiplication is Associative.

Given, $f = \begin{pmatrix} a_1 & a_2 \dots & \dots a_n \\ f(a_1) & f(a_2) \dots . & \dots f(a_n) \end{pmatrix}$, f^{-1} is calculated as: $f^{-1}.f = i$

$i.e.\ f^{-1}$ is obtained from relations : $f^{-1}[f(a_1)] = a_1,\ f^{-1}[f(a_2)] = a_2, \dots, f^{-1}[f(a_n)] = a_n$

Example:

Let, $S = \{1,2,3,4\}$, $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ & $h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$

$f.g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$; $g.f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \Rightarrow f.g \neq g.f$

Multiplication of permutation is not commutative.

$$\left.\begin{aligned} f.(g.h) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} . \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\ (f.g).h &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} . \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \end{aligned}\right\} \Rightarrow f.(g.h) = (f.g).h$$

Multiplication of permutation is associative.

Let, $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ t & x & y & z \end{pmatrix} \Rightarrow f^{-1}.f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ t & y & z & x \end{pmatrix} = i \Rightarrow t = 1; y = 2; z = 3\ \&\ x = 4$

Then, $f^{-1} = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix}$; Similarly, $g^{-1} = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$ & $h^{-1} = \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix}$

Also,

$$\left.\begin{aligned}(f.g)^{-1} &= \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 1 & 2\end{pmatrix}\\ g^{-1}.f^{-1} &= \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}.\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 1 & 2\end{pmatrix}\end{aligned}\right\} \Rightarrow (f.g)^{-1} = g^{-1}.f^{-1}$$

Cycles:

Let $S = \{a_1, a_2, \dots, a_n\}$ – a non-empty finite set. A permutation f is such that $\exists r$ elements $a_{i_1}, a_{i_2}, \dots, a_{i_r} \in S$ so that, $f(a_{i_1}) = a_{i_2}$, $f(a_{i_2}) = a_{i_3}, \dots$, $f(a_{i_{r-1}}) = f(a_{i_r})$, $f(a_{i_r}) = a_{i_1}$ & $f(a_j) = a_j$, $where\ j \neq i_1, i_2, \dots, i_r$; then f is a $r - cycle$ of length r, denoted by $(a_{i_1}, a_{i_2}, \dots, a_{i_r})$ or $(a_{i_2}, a_{i_3}, \dots, a_{i_r}, a_{i_1})$ or in any other cyclic order.

Example:

Let, $S = \{1,2,3,4\}$, $f = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$, $g = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}$, $h = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix}$ & $k = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{pmatrix}$

Then, $f = (2,3,4)$; $g = (1,2,3,4)$; $h = (1,4,3)$; $k = (2,3)$

The cycle f can also be written as, $f = (3,4,2) = (4,2,3)$ i.e. by rotating its arguments in a cyclic fashion.

Integral powers:

Let, f be a permutation on S;

Define:

1. $f^n = f.f.f \dots . f$ $[upto\ n\ terms]$
2. $f^{-n} = f^{-1}.f^{-1} \dots . f^{-1}$ $[upto\ n\ terms]$
3. $f^0 = i\ (identity\ permutation)$

Example: Let, $S = \{1,2,3,4\}$, $f = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$; to find f^3, f^{-2}

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

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

Result: Every permutation on a finite set is either a cycle or can be expressed as a product of disjoint cycles.

Let $S = \{a_1, a_2, \dots, a_n\}$ – a non-empty finite set and f be a permutation on S.

The set $a_1, f(a_1), f^2(a_1), \dots \dots \in S$; all these cannot be distinct as S is finite;
let, r be the least positive integer such that $f^r(a_1) = a_1 \Rightarrow a_1, f(a_1), f^2(a_1), \dots, f^{r-1}(a_1)$ are all distinct;

Otherwise if, $f^p(a_1) = f^q(a_1)$, $0 < p < q < r \Rightarrow f^{q-p}(a_1) = a_1$ [Contradiction, $\because q - p < r$]

Let, $p_1 = \{a_1, f(a_1), f^2(a_1), \dots, f^{r-1}(a_1)\}$ be a cycle of length r;

If $r = n \Rightarrow f = p_1$ is a cycle.

If $r < n$, then let a_m be the first element $\in S$ that does not belong to p_1;

consider $a_m, f(a_m), f^2(a_m)$, …. None of which belongs to p_1

otherwise if, $f^i(a_1) = f^j(a_m),\ (i > j) \Rightarrow f^{i-j}(a_1) = a_m \in p_1$ [Contradiction]

let, $p_2 = \{a_m, f(a_m), f^2(a_m), \ldots.\}$ be another disjoint cycle of length s(say);

if $r + s = n \Rightarrow f$ is a product of cycles p_1, p_2;

if $r + s < n$, then , let a_k be the first element $\in S$ that does not belong to either p_1 or p_2;

proceeding as before, since S is finite, after a finite number of steps,
a finite decomposition of f is obtained as $f = p_1.p_2 \ldots.p_t$.

Hence the result:

Transposition: A cycle of length 2 is called a transposition.

A 1-cycle is the identity, can be expressed as product of transpositions (a_r, a_s) and (a_r, a_s).

A 3-cycle (a_1, a_2, a_3) can be expressed as $(a_1, a_3).(a_1, a_2)$.

An r-cycle $(a_1, a_2, \ldots, a_r)$ can be expressed as $(a_1, a_r).(a_1, a_{r-1}) \ldots (a_1, a_2)$.

Every cycle can be expressed as a product of transpositions

⇒ ***Every permutation on a finite set can be expressed as a product of transpositions***

Even & Odd permutations:

A permutation is said to be **even** if it can be expressed as the **product of an even number** of transpositions.

Similarly, A permutation is said to be **odd** if it can be expressed as the **product of an odd number** of transpositions.

Example:

Let, $S = \{1,2,3,4\}$, $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ & $k = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$

Then, $f = (2,3,4) = (2,4)(2,3) = even$; $g = (1,2,3,4) = (1,4)(1,3)(1,2) = odd$;
$h = (1,4,3) = (1,3)(1,4) = even$; $k = (2,3) = odd$

Note:

An r-cycle $(a_1, a_2, \ldots, a_r)$ can be expressed as $(a_1, a_r).(a_1, a_{r-1}) \ldots (a_1, a_2)$
⇒ An r-cycle is even if r is odd & odd if r is even.

An identity permutation i can be expressed as the product of 2 transpositions
⇒ Identity permutation i is an even permutation.

Product of two even permutations is even. Product of two odd permutations is even.

Product of an even and an odd permutation is odd.

The inverse of an even permutation is even and the inverse of an odd permutation is odd.

Result: The number of even permutations on a finite set (containing at least two elements) is equal to the number of odd permutations on it.

Let, $S = \{a_1, a_2, \dots, a_n\}, n \geq 2$

Let, A =set of all even permutations on $S \Rightarrow A \neq \phi$ [$\because i \in A$].

Let, B =set of all odd permutations on $S \Rightarrow B \neq \phi$ [$\because (a_1, a_2) \in B$].

Let, $t = (a_1, a_2)$; let, $\phi: A \to B \ \ s.t. \ \ \phi(f) = tf$.

since, $f \in A \Rightarrow f$ is even $\Rightarrow tf$ is odd $\Rightarrow tf \in B$.

let, $f_1, f_2 \in A \Rightarrow tf_1, tf_2 \in B$; $tf_1 = tf_2 \Rightarrow t^{-1}(tf_1) = t^{-1}(tf_2) \Rightarrow f_1 = f_2 \Rightarrow \phi$ is one-to-one.

let, $g \in B$ be any odd permutation $\Rightarrow tg$ is even $\Rightarrow tg \in A$.

$\phi(tg) = t^2.g = i.g = g \Rightarrow tg$ is the pre-image of $g \Rightarrow \phi$ is onto$\Rightarrow \phi$ is bijective.

Since both A, B are finite sets $\Rightarrow A, B$ must have same number of elements. Hence the result.

Result: The set of all permutations over a non-empty set forms a group under multiplication of permutations.

Let A be a non-empty set and, $S_A = \{f: f \ is \ a \ permutation \ on \ A\}$

$S_A \neq \phi$ as $i \in S_A$

Let $f, g \in S_A \Rightarrow f.g \in S_A$, since composition of two permutations on A is also a permutation on A.

Now, multiplication of permutations is associative as multiplication of functions is associative.

The identity permutation i is such that, $f.i = i.f = f, \ \forall f \in S_A$.

Also, $f \in S_A \Rightarrow f$ is a bijective mapping$\Rightarrow f^{-1}$ exists and is also bijective$\Rightarrow f^{-1} \in S_A$.

Hence S_A forms a group under multiplication of permutations.

Definition:

Let $A = \{1,2, \dots, n\}$. The group of all permutations on A is called the **symmetric group of degree n**, denoted by $\boldsymbol{S_n}$.

Result: The set of all even permutations form a subgroup of S_n.

Let A_n be the set of all even permutations in S_n.

$A_n \neq \phi$ as $i \in A_n$

Let $f, g \in A_n \Rightarrow f.g \in S_n$ [since composition of two even permutations is also an even permutation]

Also, if $f \in A_n \Rightarrow f^{-1} \in A_n$ [$\because$ inverse of an even permutation is also even]

Hence A_n is a subgroup of S_n.

Definition:

The subgroup of all even permutations in the **symmetric group $\boldsymbol{S_n}$** is called the **alternating group**, denoted by $\boldsymbol{A_n}$.

Note: Since every permutation can be expressed as a product of disjoint cycles, L.C.M. of the lengths of these cycles gives the order of the permutation.

Problems on Chapter 3:

1. Let, $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 7 & 5 & 2 & 3 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 6 & 7 & 3 & 5 & 2 \end{pmatrix}$ be elements of S_7.
   Examine if (i) b is an even permutation; (ii) a^{-1} is an odd permutation.
2. Find all 3-cycle permutations in S_4. How many of them are distinct?
3. Construct the composition table for the symmetric group S_3.
4. Let, $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$. Find $o(a)$ in S_6.
5. Show that the order of an $r - cycle$ is r.

Hints & Solutions:

1. Here, $a = (1,6,3,7)(2,4,5) = (1,7)(1,3)(1,6)(2,5)(2,4) \Rightarrow a$ is an odd permutation
   similarly, $b = (2,4,7)(3,6,5) = (2,7)(2,4)(3,5)(3,6) \Rightarrow b$ is an even permutation
   Again, since inverse of an odd permutation is odd $\Rightarrow a^{-1}$ is an odd permutation

2. Here, $S = \{1,2,3,4\}$; all 3-cycle permutations on S are given by ${}^4p_3 = 4! = 24$, they areas follows:
   $(1,2,3), (2,3,1), (3,1,2)$
   $(1,2,4), (2,4,1), (4,1,2)$
   $(1,3,4), (3,4,1), (4,1,3)$
   $(2,3,4), (3,4,2), (4,2,3)$
   $(2,4,3), (4,3,2), (3,2,4)$
   $(4,2,1), (2,1,4), (1,4,2)$
   $(3,2,4), (2,4,3), (4,3,2)$
   $(3,1,4), (1,4,3), (4,3,1)$
   Here all the cycles on the same row are equivalent; hence number of distinct permutations are 8.
3. Here $S = \{1,2,3\}$
   Let, $\rho_0 = i;\ \rho_1 = (1,2,3);\ \rho_2 = (1,3,2);\ \rho_3 = (2,3);\ \rho_4 = (1,3); \rho_5 = (1,2)$
   Hence, the composition table is given as:

$\cdot$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_1	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_2	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_1	ρ_2	ρ_0

4. Here, $a = (1,3,2)(5,6)$; thus a is expressed as a product of two disjoint cycles of length 3 & 2 respectively. So the order of $a = k = LCM\{3,2\} = 6$.
5. Let, $f = (a_1, \dots, a_r)$ be an r-cycle on a finite set $S = \{a_1, \dots., a_n\}$
   Then, $f(a_1) = a_2, f(a_2) = a_3, \dots, f(a_{r-1}) = a_r, f(a_r) = a_1$ and $f(a_i) = a_i, r+1 \leq i \leq n$
   Hence, $f^2(a_1) = f(a_2) = a_3 \Rightarrow f^3(a_1) = f(a_3) = a_4 \dots\dots$
   $\Rightarrow f^{r-1}(a_1) = f(a_{r-1}) = a_r$
   $\Rightarrow f^r(a_1) = f(a_r) = a_1$
   Similarly, we can show that, $f^r(a_2) = a_2$; $f^r(a_3) = a_3$; $\dots\dots$; $f^r(a_r) = a_r$
   Also, $f^r(a_i) = a_i, r+1 \leq i \leq n$
   Hence, we get, $f^r(a_i) = a_i, \forall i = 1,2,..,n$
   this implies that $f^r = i$, the identity permutation.
   Again, if $f^m = i, m < r$, then $f^m(a_1) = a_1$, contradicting the fact that f is a cycle of length r.
   Hence, order of f is r.

Assignments on Chapter 3:

1. Examine if the symmetric group S_3 is cyclic.
2. Examine if the alternating group A_3 is cyclic.
3. In S_3, give an example to show that if $x.y \neq y.x$, then, $o(xy) \neq o(x).o(y)$.
4. Prove that $S_n, n \geq 3$, is a non-abelian group.
5. Let, $(G,\circ)$ be a group and $a \in G$. Let the mapping $f_a: G \to G$ be defined by, $f_a(x) = a \circ x, \forall x \in G$.
   Show that f_a is a permutation on G.
   Let, $S = \{f_a: a \in G\}$ and let a binary composition $*$ be defined on S as $f_a * f_b = f_{a \circ b}, \forall f_a, f_b \in S$.
   Show that $(S,*)$ is a group.