19/03/18

Permutation

$\Rightarrow$ Let S be a non-empty finite set. A bijective mapping f from $S \to S$ is said to be a permutation on S.

$$S = \{a_1, a_2, a_3, \ldots, a_n\}$$

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ f(a_1) & f(a_2) & f(a_3) & \cdots & f(a_n) \end{pmatrix}$$

Eg :- $S = \{1, 2, 3\}$

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

S_n contains all the permutations defined on S. $(= n!)$

- **Product / Composition :**

Let $f, g \in S_n$, then

$f \circ g$ / fg is defined as $\rightarrow$

$$f \circ g(x) \,/\, fg(x) = f(g(x))$$

$S = \{1, 2, 3\}$

$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $g \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$fg(1) = f(g(1)) = f(2) = 1$

$fg(2) = f(g(2)) = f(1) = 3$

$fg(3) = f(g(3)) = f(3) = 2$

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

$\boxed{\langle S_n, \circ \rangle}$ → finite but non-abelian.

$\circ$ → composition

→ permutation/ symmetric group.

$gf(1) = g(f(1)) = g(3) = 3$

$g(f(2)) = g(1) = 2$

$g(f(3)) = g(2) = 1$

- **Inverse of permutation :**

Let f is a set of permutation, $f \in S_n$ and $f : a_i \to a_j$, then the inverse of f denoted as f^{-1} is defined as →

$$f^{-1} : a_j \to a_i.$$

$fg = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $ff^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

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

$S = \{a_1, a_2, \dots, a_n\}$

$p \in S_n$

$p(a_1) = a_2$, $p(a_2) = a_3$, $p(a_3) = a_4 \dots$, $p(a_n) = a_1$

$p = (a_1, a_2, a_3, \dots, a_n)$ $\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}$

Let $S = \{a_1, a_2, \ldots, a_n\}$. A permutation row $p \in S_n$ is said to be a cycle of length of 'r' or an 'r'-cycle if there are 'r' elements denoted as →

$\{a_{i_1}, a_{i_2}, a_{i_3}, \ldots, a_{i_r}\}$, $p(a_{i_1}) = a_{i_2}$,

$p(a_{i_2}) = a_{i_3}$ ..... $p(a_{i_r}) = a_{i_1}$

and $p(a_j) = a_j$ $\forall\, j \notin \{i_1, i_2, \ldots, i_r\}$

Eg: $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$ → 2-cycle.

$P = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ ⟶ 1 cycle. (1)
(2)
is either a cycle or (3)

⇒ **Proposition**: Every permutation can be expressed as a product of disjoint cycles.

Proof: Let $S = \{a_1, a_2, a_3, \ldots, a_n\}$ be a permutation on S. Let p be a permutation on S. Let us consider the elements a_1, $P_1(a_1)$, $P_1^2(a_1)$, ...

All these can't distinct since all of them $\in S$ and S is a finite set. Let r = least +ve integer : $P_1^r(a_1) = a_1$. Then ⟶ $P_1(a_1)$, $P_1^2(a_1)$, ... $P_1^r(a_1)$ are distinct. Otherwise for some p, q such that $0 < q < p < r$ ⟶ $p^p(a_1) = p^q(a_1)$.

⇒ $P_1^{p-q}(a_1) = a_1$

This is a contradiction that r is the least element.

Therefore we get an 'r'-cycle P_1 which can be written as, $P_1 \equiv (a_1, P_1(a_1), P_1^2(a_1), \ldots P_1^{r-1}(a_1))$

If $r = n$, then the theorem is proved, otherwise, Let $a_m \in S$ such that it does not belong to $\{a_1, P_1(a_1), P_1^2(a_1), \ldots, P_1^{p-1}(a_1)\}$

and find $P(a_m), P^2(a_m)$.

$$\left[\begin{array}{l} P\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \\ P(1, 2\ 3) \end{array}\right.$$

Let us consider elements $P_m, P^2(m) \ldots$

Now. non of these elements $\in$ set P_1, because

if, $P^i(a_m) = P^j(a_1)$

$\Rightarrow P^{j-i}(a_1) = a_m$

which is a contradiction, since $a_m \notin P_1$.

and certainly the process of finding $P(a_m)$, $P^2(a_m) \ldots$ will stop and yield a_m at some time, since S = finite set, giving us another cycle (say) of length s. Let us name the cycle as P_2. If $p+s = m$, then the theorem is proved & $P = P_1 \cdot P_2$, Otherwise we can repeat the process for finite no. of times and obtain disjoint cycles, $\rightarrow P_1, P_2, \ldots P_m$.

$$P = P_1 \circ P_2 \circ P_3 \circ \ldots \circ P_m$$

- A cycle of length - 2 is called <u>Transposition</u>.

$$P = (a_1, a_2, a_3)$$

$$P_1 = (a_1, a_3) = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix}.$$

$$P_2 = (a_1, a_2) = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}$$

$$P_1 \circ P_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}.$$

$$\underline{P = (a_1\ a_2\ a_3)}$$

- Every permutation can be written as product of transposition: If the no. of such transpositions are even, then the permutations are called even permutation else odd-permutation.

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

$(1\ 3)\ (4\ 5\ 6\ 8)$

$$= \underbrace{(1\ 3)\ (4\ 8)\ (4\ 5)\ (4\ 6)}_{\text{Even permutation.}} \quad = 4$$

- Identity permutation can be written as

$(a_p\ a_s)\ (a_p\ a_s)$

$S = \{1, 2, 3, 4, 5, 6, 7, 8\}$

$i = (1\ 2)\ (1\ 2)$ or $(6\ 7)\ (6\ 7)$

pick up any 2 elements.