Thm

Disjoint Cycles Commute

If the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Proof:

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

$\alpha = (1\,2)$, $\beta = (3\,4)$, $A = \{1,2,3,4,5,6\}$

$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$ — permutation

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

$\alpha = (1\,2)$

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

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

$\alpha\beta = \beta\alpha$

Proof: Let α and β are permutations of the set $S = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_k\}$

To prove $\alpha\beta = \beta\alpha$

we need to show that $\alpha\beta(x) = \beta\alpha(x)$ $\forall x \in S$.

Let $x = a_i$ be the fixed element of S, where $1 \le i \le m$.

$$(\alpha\beta)(a_i) = \alpha\{\beta(a_i)\}$$
$$= \alpha(a_i) = a_{i+1},$$

Here $a_{i+1} = a_1$ if $i = m$.

$\beta = (b_1, b_2, \ldots, b_n)$

$\beta(a_i) = a_i$

Now, $(\beta\alpha)(a_i) = \beta\{\alpha(a_i)\} = \beta(a_{i+1})$
$$= a_{i+1}.$$

$\therefore$ $(\alpha\beta)(a_i) = (\beta\alpha)(a_i)$ $\forall a_i$, $1 \le i \le m$.

Now let $x = b_j$ be the fixed element of S.
where $1 \le j \le n$.

$$(\alpha\beta)(b_j) = \alpha\{\beta(b_j)\} = \alpha(b_{j+1}) = b_{j+1}$$

(Here $b_{j+1} = b_1$ if $j = n$.)

Now $$(\beta\alpha)(b_j) = \beta\{\alpha(b_j)\} = \beta\{b_j\} = b_{j+1}$$

$$\therefore (\alpha\beta)(b_j) = (\beta\alpha)b_j \quad \forall\, b_j,\ 1 \le j \le n.$$

Finally, suppose that $x = c_l$ is a fixed element of S.
where $1 \le l \le k$.

$$(\alpha\beta)(c_l) = \alpha\{\beta(c_l)\} = \alpha(c_l) = c_l.$$

Now $$(\beta\alpha)(c_l) = \beta\{\alpha(c_l)\} = \beta(c_l) = c_l$$

$$\therefore (\alpha\beta)(c_l) = (\beta\alpha)(c_l) \quad \forall\, c_l,\ 1 \le l \le k.$$

This completes the proof.

Order of a Permutation

Thm

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:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix} = \underbrace{(1\,2)}_{T_2}\ \underbrace{(3\ 4\ 6)}_{T_3}\ \underbrace{(5)}_{T_1}$$

$O(\alpha) = LCM\{2, 3, 1\} = 6$

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (12)(34)$$

$O(\alpha) = LCM\{2, 2\} = 2.$

Clearly, the cycle of a length n has order n.

Now suppose that α and β are two disjoint cycles of lengths m and n and let k be the LCM of m and n.

$O(\alpha) = m \Rightarrow \alpha^m = e = I \rightarrow$ Identity permutation

$O(\beta) = n \Rightarrow \beta^n = e = I$

$\because k = LCM\{m, n\} \Rightarrow \alpha^k = I$ and $\beta^k = I$ ——— (1)

Now, α and β are disjoint cycles, α and β will commute.

then, $(\alpha\beta)^k = \alpha^k \beta^k = I$ ——— (2) (using eq (1))

$\Rightarrow O(\alpha\beta)$ will divides k

$a^k = e$
$\Rightarrow |a|$ divides k

let $O(\alpha\beta) = l$,

It means l divides k. ——— (3)

$\because O(\alpha\beta) = l \Rightarrow (\alpha\beta)^l = I$

$\Rightarrow \alpha^{l} \beta^{l} = I$

$\Rightarrow \alpha^{l} = \beta^{-l}$ —— ④

$\because \alpha$ and β are disjoint cycles

$\Rightarrow \alpha^{l}$ and β^{-l} must be disjoint and they shouldn't have any entry in common.

But from eqn ④, $\alpha^{l} = \beta^{-l}$

$\Rightarrow$ they both must be the identity.

$\Rightarrow \alpha^{l} = I$ & $\beta^{-l} = I$.

$A = \{1,2,3,4\}$

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

$I = (1)$, $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$, $I = (2)$, $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$, $I = (3)$ $I = (4)$

I I.

$\Rightarrow \alpha^{l} = I$ & $\beta^{-l} = I$

$\Rightarrow |\alpha|$ will divides l & $|\beta|$ will divide l.

$\Rightarrow m$ divides l & n divides l

$\Rightarrow LCM(m,n)$ divides l.

$\Rightarrow k$ divides l —— ⑤

from eqn ③ & ⑤

$l = k$

$l | k$ & $k | l$

$\Rightarrow l = k$

$\Rightarrow |\alpha\beta| = LCM(m,n)$

$\Rightarrow |\alpha\beta| = LCM(|\alpha|, |\beta|)$

Similarly, $|\alpha\beta\gamma| = LCM(|\alpha|, |\beta|, |\gamma|)$.

$\because$ any permutation of a finite set can be written as a cycle or product of disjoint cycles

$\therefore$ the order of a permutation of a finite set written in disjoint cycle form is the LCM of the lengths of the cycles.