Permutation Group

28 September 2020 09:12

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 $\alpha\beta = \beta\alpha$.

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

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

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

$\alpha\beta = \beta\alpha.$

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

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

Proof: Let α and β be 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 $\alpha\beta = \beta\alpha$.

For this we need to show $\alpha\beta(x) = \beta\alpha(x) \quad \forall\, x \in S$.

Let $x = a_i$ be a fixed element of S and a_i is an entry in α.
where $1 \leq i \leq m$.

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

(Here we interpret $a_{i+1} = a_1$ if $i = m$)

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

$\alpha = (a_1, a_2, \dots, a_m)$

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

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

Now, let $x = b_j$ be a fixed element of S and b_j is an entry in β, where $1 \le j \le n$

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

{Here we interpret $b_{j+1} = b_1$, if $j = n$}

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

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

Let $x = c_r$ be a fixed element of S and c_r's are the members of S left by both α and β, where $1 \le r \le k$.

Now, $\alpha\beta(c_r) = \alpha\{\beta(c_r)\} = \alpha(c_r) = c_r$

$\beta\alpha(c_r) = \beta\{\alpha(c_r)\} = \beta(c_r) = c_r$

$\therefore \alpha\beta(c_r) = \beta\alpha(c_r) \quad \forall\ c_r,\ 1 \le r \le k.$

Thus, $\alpha\beta(x) = \beta\alpha(x) \quad \forall\ x \in S$

$\Rightarrow \boxed{\alpha\beta = \beta\alpha}$

Order of a Permutation

$A = \{1, 2, 3\} \longrightarrow S_3$ contains $3! = 6$ elements

$(12) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \qquad o\{(12)\} = 2 =$ length of cycle.

$|a| \rightarrow$ smallest +ve integer n such that $a^n = e$.

$(12)^2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = I$

$\Rightarrow o\{(1\,2)\} = 2.$

$o\{(a_1 a_2 \ldots a_n)\} = n.$

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.

$A = \{1\,2\,3\,4\,5\,6\}$

$$\alpha = \begin{bmatrix} & & & & & \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix} = (1\,2)(3\,4\,6)(5)$$
$$\Rightarrow |\alpha| = LCM\{2, 3, 1\} = 6$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{bmatrix} = (1\,2)(3\,4)(5\,6)$$
$$\Rightarrow |\beta| = LCM\{2, 2, 2\} = 2$$

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 6 & 1 \end{bmatrix} = (1\,3\,2\,4\,5\,6)$$
$$\Rightarrow |\gamma| = LCM\{6\} = 6.$$

Proof: Clearly, a cycle of length n has order n.

If permutation α is a cycle of length n then $|\alpha| = n = LCM\{n\}$.

Now, suppose that permutation α is a product of two disjoint cycles α_1 and α_2 of length m and n respectively.

TS $|\alpha| = LCM\{|\alpha_1|, |\alpha_2|\} = LCM\{m, n\}$.

Let k be the LCM of m and n.

$\Rightarrow m \mid k$ and $n \mid k$ —— (1)

Now, $|\alpha_1| = m \Rightarrow \alpha_1^m = I \Rightarrow \alpha_1^k = I$

and $|\alpha_2| = n \Rightarrow \alpha_2^n = I \Rightarrow \alpha_2^k = I$

Now, since α_1 and α_2 are disjoint cycles,
therefore $\alpha_1 \alpha_2 = \alpha_2 \alpha_1$

$$\therefore (\alpha_1 \alpha_2)^k = \alpha_1^k \alpha_2^k = I.I = I$$

$\Rightarrow |\alpha_1 \alpha_2|$ divides k

$\boxed{a^k = e \Rightarrow |a| \text{ divides } k.}$

Let $r = |\alpha_1 \alpha_2|$

$\Rightarrow r$ divides k —— ②

Now, $|\alpha_1 \alpha_2| = r$.

$$\Rightarrow (\alpha_1 \alpha_2)^r = I$$

$$\Rightarrow \alpha_1^r \alpha_2^r = I$$

$$\Rightarrow \alpha_1^r \alpha_2^r \alpha_2^{-r} = I \alpha_2^{-r}$$

$$\Rightarrow \alpha_1^r = \alpha_2^{-r} \text{ —— ③}$$

Now, α_1 and α_2 are disjoint cycles.
$\therefore$ they have no common symbol, the same must be true for α_1^r and α_2^{-r} because raising a cycles to a power can not introduce new symbols.

But from eqn (3), $\alpha_1^{l} = \alpha_2^{-l}$.

It can be possible only when α_1^{l} and α_2^{-l} both are identity.

$$\therefore \alpha_1^{l} = \alpha_2^{-l} = I \quad \text{——— (4)}$$

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

$\alpha = \beta = I$

α & β have no entries in common.

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

$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I$, $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = I$.

$\alpha = (12)$, $\beta = (34)$, $\beta^2 = I$,

$\alpha^2 = (1)$, $\beta^{-2} = (3)$

$\alpha^2 = \beta^{-2} = I$

$\beta^{-2} = (\beta^2)^{-1}$

from eqn (4), $\alpha_1^{l} = I$

$\Rightarrow m$ divides l. $(\because |\alpha_1| = m)$

and $\alpha_2^{-l} = I \Rightarrow (\alpha_2^{-l})^{-1} = (I)^{-1}$

$\Rightarrow \alpha_2^{l} = I$

$\Rightarrow n$ divides l $(|\alpha_2| = n)$

$\therefore m | l$ & $n | l$.

$\Rightarrow$ LCM (m, n) divides ℓ.

$\Rightarrow$ k divides ℓ —— (5)

from eqn (2) & (5),

$\ell \mid k$ & $k \mid \ell$

$\Rightarrow$ $k = \ell$

$\Rightarrow$ $\text{LCM}\{m, n\} = |\alpha_1 \alpha_2|$

$\Rightarrow$ $|\alpha_1 \alpha_2| = \text{LCM}\{m, n\}$

$\Rightarrow$ $|\alpha| = \text{LCM}\{|\alpha_1|, |\alpha_2|\}$

Similarly, if α is a product of n disjoint cycles $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Then $|\alpha| = \text{LCM}\{|\alpha_1|, |\alpha_2|, \ldots, |\alpha_n|\}$.

Chapter 2 Problems

Q (50) $x^3 = e$ a, a^{-1}, eliminate them. $a \neq a^{-1}$

$x^5 = e$, $a \neq a^2$

a is the soln, a^2, a^3, a^4 $\quad$ $a \neq a^3$
$a \neq a^4$.

eg| a, a^2, a^3, a^4.
If $a \neq e$, is a soln of the eqn $x^5 = e$
then a^2, a^3, a^4 are also the solns.
& $a \neq a^2 \neq a^3 \neq a^4$.

no. of non identity soln of $x^5 = e$ are multiple of 4.

Q 52 $\begin{bmatrix} a & a \\ a & a \end{bmatrix}^{-1} = \begin{pmatrix} 1/4a & \frac{1}{4a} \\ 1/4a & 1/4a \end{pmatrix}$

$\because a \neq 0$, inverse exists.

The group G is different from $GL(2, R)$

Identity of $G = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ is different from $GL(2, R)$

$\therefore$ Inverse of elements of G exists whether the determinant is zero of every matrix.

Chapter (3),

Q (1), In Q, $|0| = 1$.

$|a| = \infty \quad \forall a \in \mathbb{Q}, a \neq 0.$

In $\mathbb{Q}^*$, $|1| = 1$, $|-1| = 2$.

$|a| = \infty \quad \forall a \in \mathbb{Q}^*, a \neq 1, -1.$

Q (7) $(abc)^{-1} = c^{-1} b^{-1} a^{-1}$.

$|a| = 6, |b| = 7$

$(a^4 c^{-2} b^4)^{-1} = (b^4)^{-1} (c^{-2})^{-1} (a^4)^{-1} \Rightarrow a^6 = e, \quad b^7 = e.$

$= b^{-4} c^2 a^{-4}.$ $\qquad b^7 b^{-4} = e b^{-4}$

$\Rightarrow b^3 c^2 a^2$ $\qquad b^3 = b^{-4}.$

Q. (17) let a, b be two distinct elements of order 2.

Then $(ab)^2 = a^2 b^2 = e \Rightarrow |ab| = 2$

let $c \neq a, c \neq b, c \neq ab$ be the fourth element of order 2.

ac, bc, abc have order 2.

$\therefore$ there are atleast seven elements of order 2.

Example: Q_8, D_3, D_4, S_3, S_4

~~$D_3 \to$~~ ~~$Q_8 \to$~~ $\{\pm 1, \pm i, \pm j, \pm k\}$ ± 1 order 2.
~~$S_3 \to$~~

D_4 has ____ elements of order 2

D_4 has elements of order 2 between 3 and 7.

Q. 20 $x^2 \neq e$, $x^6 = e$

Prove that $x^4 \neq e$, $x^5 \neq e$

What can you say about $|x|$.

Soln If $x^4 = e \Rightarrow (x^4)^2 = e^2$

$\Rightarrow x^8 = e \Rightarrow x^6 \cdot x^2 = e$

$\Rightarrow e \cdot x^2 = e \Rightarrow x^2 = e$ $\rightarrow\leftarrow$

$\therefore x^4 \neq e$.

If $x^5 = e \Rightarrow (x^5)^2 = e \Rightarrow x^4 = e$ $\rightarrow\leftarrow$

$x^6 = e$, $x^2 \neq e$.

$\Rightarrow x^3$ may be equal to e