Chapter 7: Groups of Symmetry

Mphako-Banda

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG
SCHOOL OF MATHEMATICS

LEARNING OUTCOMES FOR THE LECTURE

By the end of this lecture, students will be able to:

- ♣ state and prove the cycle decomposition theorem
- ♣ compare the cyclic structure of permutations in S_n
- ♣ define a transposition
- ♣ write any permutation as a product of transpositions
- ♣ find the order of a permutation

Theorem (7.4.6 CYCLE DECOMPOSITION THEOREM)

If $\sigma \neq e$ is in S_n, then σ is the product of one or more disjoint cycles of length at least 2.

PROOF:

We prove the existence of decomposition by induction on $n \geq 2$ for $\sigma \in S_n$. (Assume the uniqueness).

It can be proved that this factorisation is unique up to the order of factors.

A If $n = 2$ then each permutation has length 2 since $S_2 = \{e, (1\ 2)\}$ and $\sigma \neq e$.

B If $n > 2$ assume result true for S_{n-1}.

case 1

C Let $\sigma \in S_n$. If σ fixes n then $\sigma(n) = n$ and so $\sigma \in S_{n-1}$. By induction hypothesis σ is the product of disjoint cycles of length at least 2.

case 2 Assume σ moves n and $\sigma(n) \neq n$. set $m = \sigma^{-1}(n)$ or $\sigma(m) = n$ with $m \neq n$.
Let $\gamma = (m \quad n)$ where $\gamma^2 = e$.
Consider $\tau = \sigma\gamma$. Thus $\tau\gamma = \sigma\gamma^2 = \sigma$.
Moreover, $\tau(n) = \sigma\gamma(n) = \sigma(m) = n$.
Therefore $\tau \in S_{n-1}$ and so τ is the product of disjoint cycles in S_{n-1} of length at least 2 by induction hypothesis.

We consider 2 cases: CASE 1, $\tau(m) = m$ and CASE 2, $\tau(m) \neq m$ $\quad \sigma = \tau\gamma$

CASE 1: $\tau(m) = m$ and $\tau(n) = n$ by above so τ fixes both m and n and τ disjoint from γ.

$\therefore \quad \sigma = \tau\gamma$ is as required.

CASE ~~1~~ 2: $\tau(m) \neq m$. Then m is moved by exactly one factor in the decomposition of τ.

say $\tau = \mu(m \quad k_1 \quad k_2 \quad \cdots \quad k_r)$ where μ is the product of cycles that do not move $m \quad k_1 \quad k_2 \quad \cdots \quad k_r$ and n

$$\begin{aligned} \sigma = \tau\gamma &= \overbrace{\mu(m \quad k_1 \quad k_2 \quad \cdots \quad k_r)}^{\tau}\overbrace{(m \quad n)}^{\gamma} \\ &= \mu(m \quad n \quad k_1 \quad k_2 \quad \cdots \quad k_r) . \end{aligned}$$

and σ has the required decomposition.

So by principle of induction, the statement is true $\forall n \in \mathbb{N}$.

Example (7.4.7)

$|S_4| = 24$. *List of elements*
e; $(1 \quad 2)$; $(1 \quad 2)(3 \quad 4)$; $(1 \quad 2 \quad 3)$;
$(1 \quad 2 \quad 3 \quad 4)$ *etc.*
These are the types of decomposition.

Cyclic Structure

Definition (7.5.1)

Two permutations have the same cyclic structure if when factored into disjoint cycles they have the same number of cycles of each length.

Definition (7.5.2)

A cycle of length 2 is called a transposition.

Note 7.5.3 (i) $m, n \in X$, $\delta = (m \quad n)$ is a transposition.
$X = \{1, 2, 3\}$ the $(1 \quad 2), \quad (1 \quad 3), \quad (2 \quad 3)$ are transpositions.
Note $\delta^2 = e$ for all δ transposition and so $\delta = \delta^{-1}$.
Note 7.5.3 (ii) Let $\sigma = (1 \quad 2)(3 \quad 4)$ then

$$\begin{aligned} \sigma^2 &= (1 \quad 2)(3 \quad 4)(1 \quad 2)(3 \quad 4) \\ &= (1 \quad 2)(1 \quad 2)(3 \quad 4)(3 \quad 4) = e. \end{aligned}$$

(by Theorem 7.4.3 if disjoint the permutations commute)
Since the transposition are disjoint and hence commute.
But σ is not a transposition.

You can start with any element, numbers must appear in the same order.

In each product we have:

(first fourth)(first third)(first second)

$$\begin{array}{cccc} \text{(first} & \text{second} & \text{third} & \text{fourth)} \\ (1 & 2 & 3 & 4) \end{array} = (1\ \ 4)(1\ \ 3)(1\ \ 2)$$

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

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

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

The decomposition above is not unique!

(fourth third)(fourth second)(fourth first) also works...

Eg. (2 1)(2 4)(2 3) = (3 4 1 2)

Theorem (7.5.4)

Every cycle of length $r > 1$ is a product of $r - 1$ transpositions.
Infact
$(k_1 \quad k_2 \quad \cdots \quad k_{r-1} \quad k_r) =$
$(k_1 \quad k_r)(k_1 \quad k_{r-1}) \quad \cdots \quad (k_1 \quad k_3)(k_1 \quad k_2).$

Lemma (7.5.5)

Let $\gamma_1 \neq \gamma_2$ be transpositions. If γ_1 moves k, transpositions δ_1 and λ_2 exist such that $\gamma_2\gamma_1 = \lambda_2\delta_1$, where δ_1 fixes k and λ_2 moves k.

Eg) (1 3)(2 3) = (2 3)(2 1)

1 moved in first factor

1 now moved in second factor

Lemma (7.5.6)

If the identity permutation e can be written as a product of $n \geq 3$ transpositions, then it can be written as a product of $n - 2$ transpositions.

Theorem (7.5.4 PARITY THEOREM)

If a permutation σ has two factorisations

$$\sigma = \gamma_n \gamma_{n-1} \cdots \gamma_2 \gamma_1 = \rho_m \rho_{m-1} \cdots \rho_2 \rho_1$$

where each γ_i and ρ_j is a transposition, then both m and n are even or both are odd.

Order of permutation

Definition (7.6.1)

1. *An element α of S_n has order $r > 0$ if $\alpha^r = e$, and no smaller positive power of α is e.*
2. *The order of a k cycle is k.*
3. *The order of the product of disjoint cycles is the lcm of the orders of the cycles.*