

Lecture Notes: Symmetric Groups and Parity

MAT3004

1. Recall: Symmetric/Permutation Group

The Symmetric Group on n elements is defined as:

$$S_n := \{\sigma : \{1, 2, \dots, n\} \rightarrow \{1, \dots, n\} \mid \sigma \text{ is bijective}\}$$

Example 1 ($n = 8$). Let $\sigma \in S_8$ be defined by the mapping:

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

Values explicitly:

$$\begin{aligned} \sigma(1) &= 3, & \sigma(3) &= 7, & \sigma(7) &= 5 \\ \sigma(5) &= 1, & \sigma(2) &= 6 \\ \sigma(6) &= 8, & \sigma(8) &= 2, & \sigma(4) &= 4 \end{aligned}$$

Remark: S_n describes all permutations of n identical objects.

2. Cycles

Definition 1 (k -cycle). Let $\{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$. A k -cycle is a permutation $\gamma = (i_1, i_2, \dots, i_k) \in S_n$ such that:

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \dots, \quad \sigma(i_k) = i_1$$

and $\sigma(j) = j$ for all $j \notin \{i_1, \dots, i_k\}$.

Example: In S_8 , let $\sigma = (1\ 3\ 7\ 5)$. This represents the mapping $1 \rightarrow 3 \rightarrow 7 \rightarrow 5 \rightarrow 1$. The fixed points are $\{2, 4, 6, 8\}$.

Properties of Cycles

1. **Cyclic Shift:** The representation is not unique; it can be shifted cyclically.

$$(i_1, i_2, i_3, \dots, i_k) = (i_2, i_3, \dots, i_k, i_1) = (i_3, \dots, i_k, i_1, i_2) = \dots$$

2. **Decomposition:** Not all $\gamma \in S_n$ are k -cycles. However, any $\gamma \in S_n$ can be expressed as a product (composition) of disjoint cycles.

Example (from above):

$$\sigma = (1\ 3\ 7\ 5) \circ (2\ 6\ 8) \circ (4)$$

Often written simply as: $\sigma = (1\ 3\ 7\ 5)(2\ 6\ 8)$.

3. **Order:** If $\gamma = (i_1, i_2, \dots, i_k)$ is a k -cycle, then:

$$\text{ord}(\gamma) = k$$

4. **Inverse:** For $\gamma = (i_1, i_2, \dots, i_{k-1}, i_k)$, the inverse is simply the cycle reversed:

$$\gamma^{-1} = (i_1, i_k, i_{k-1}, \dots, i_2)$$

3. Operations in S_n

Example in S_7 : Let $\sigma = (1\ 3\ 7\ 5)(2\ 6)$ and $\tau = (4\ 6\ 7)(2\ 5)$.

Then:

$$\sigma\tau = (1\ 3\ 7\ 5)(2\ 6)(4\ 6\ 7)(2\ 5) = (1\ 3\ 7\ 4\dots)$$

$$\tau\sigma = (4\ 6\ 7)(2\ 5)(1\ 3\ 7\ 5)(2\ 6) = (1\ 3\ 4\ 6\ 5)(2\ 7)$$

$\therefore \sigma\tau \neq \tau\sigma$ (in general, S_n is non-abelian).

Note:

- If σ and τ have **disjoint entries** (e.g., $\sigma = (1\ 2\ 4)$, $\tau = (3\ 6)(7\ 9)$), then they commute ($\sigma\tau = \tau\sigma$).
- General Inverse: For $\sigma = \gamma_1\gamma_2\dots\gamma_l$, then $\sigma^{-1} = \gamma_l^{-1}\dots\gamma_2^{-1}\gamma_1^{-1}$.

4. Transpositions

Definition 2. A 2-cycle $\tau = (i\ j)$ is called a **transposition**.

Lemma 1. Any $\sigma \in S_n$ can be expressed as a product of transpositions (not necessarily disjoint).

Proof. First, a k -cycle can be decomposed:

$$(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_3)(i_1, i_2)$$

Since any permutation is a product of cycles, any permutation is therefore a product of transpositions. \square

Non-uniqueness: The expression is not unique.

$$\begin{aligned} \sigma &= (1\ 2\ 3) = (1\ 3)(1\ 2) \\ &= (1\ 3)(1\ 2)(1\ 2)(1\ 2) \\ &= (2\ 3)(1\ 2)(1\ 3)(2\ 3) \end{aligned}$$

5. Parity of Permutations

Although the factorization into transpositions is not unique, the **parity** (evenness/oddness) of the number of transpositions is invariant.

Theorem 1 (Parity Theorem). *Let $\sigma \in S_n$. If*

$$\sigma = \tau_1 \dots \tau_k \quad \text{and} \quad \sigma = \tau'_1 \dots \tau'_{\ell}$$

are two expressions of σ as a product of transpositions, then:

$$k \equiv \ell \pmod{2}$$

To prove this, we first need a proposition regarding the identity element.

Proposition 1. *If the identity e is expressed as a product of transpositions $e = \tau_1 \dots \tau_k$, then $k \equiv 0 \pmod{2}$ (i.e., k is even).*

Proof of Proposition (Induction on k)

Proof. **Base Cases:**

- $k = 0$: e is product of 0 transpositions. 0 is even. ✓
- $k = 1$: $e \neq (ab)$. Impossible.

Inductive Step: Suppose the statement holds for all lengths $< k$. Consider $e = \tau_1 \dots \tau_k$. Let the last transposition be $\tau_k = (ab)$. We analyze $\tau_{k-1}\tau_k$. There are 4 cases for τ_{k-1} relative to (a, b) :

1. $\tau_{k-1} = (ab)$. Then $\tau_{k-1}\tau_k = e$. We can remove both. Length becomes $k - 2$. By induction, $k - 2$ is even $\implies k$ is even.
2. $\tau_{k-1} = (ac)$ where $c \neq b$. Then $(ac)(ab) = (ab)(bc)$.
3. $\tau_{k-1} = (bd)$ where $d \neq a$. Then $(bd)(ab) = (ad)(ab)$.
4. $\tau_{k-1} = (cd)$ disjoint from $\{a, b\}$. Then $(cd)(ab) = (ab)(cd)$.

In cases 2, 3, and 4, we rewrite $\tau_{k-1}\tau_k$ such that the index a moves to the right-hand transposition or disappears from the k -th position. By repeating this process, we either find a cancellation (Case 1) or we push an occurrence of a all the way to the left, i.e., $e = (ax)\tau'_2 \dots \tau'_k$ where a does not appear in $\tau'_2 \dots \tau'_k$.

If $e = (ax) \dots$, then $\sigma(a) = x$. But for identity, $\sigma(a)$ must be a . Thus $x = a$, which is impossible for a transposition. Therefore, cancellation MUST have occurred. Cancellation reduces length by 2. Thus k must be even. \square

Proof of Parity Theorem

Proof. Suppose $\sigma = \tau_1 \dots \tau_k = \tau'_1 \dots \tau'_{\ell}$. Then:

$$(\tau_1 \dots \tau_k)(\tau'_1 \dots \tau'_{\ell})^{-1} = e$$

Since $\tau^{-1} = \tau$:

$$\tau_1 \dots \tau_k \tau'_{\ell} \dots \tau'_1 = e$$

This is a product of $k + \ell$ transpositions equal to identity. By the Proposition above, $k + \ell$ is even.

$$k + \ell \equiv 0 \pmod{2} \implies k \equiv \ell \pmod{2}$$

□

6. Alternating Group A_n

Definition 3. The **Alternating Group** A_n is the subgroup of S_n consisting of all even permutations (permutations that can be expressed as an even number of transpositions).