Permutation Groups

Definition: Given a set X, the **permuatation group** on X is the set $\mathrm{Perm}(X)$ of bijective functions on X. This is a group with composition of functions as the operation. The **symmetric group** S_n is the permuation group on the set $[n] := \{1, \ldots, n\}$.

A **cycle** is a particular type of permutation. By way of example, in S_7:

- $\alpha = (2\ 4\ 5)$ is a 3-cycle. It is the permutation given by $\alpha(2) = 4$, $\alpha(4) = 5$, $\alpha(5) = 2$, and $\alpha(i) = i$ for $i \neq 2, 4, 5$.
- $\beta = (1\ 6\ 5\ 4)$ is a 4-cycle. It is the permutation given by $\alpha(1) = 6$, $\alpha(6) = 5$, $\alpha(5) = 4$, $\alpha(4) = 1$, and $\alpha(i) = i$ for $i \neq 1, 6, 5, 4$.

We will not consider 1-cycles. A 2-cycle is also called a **transposition**.

(1) Warming up with cycles: Consider the symmetric group S_5.

- **(a)** Write out the cycle $(1\,4\,3)$ explicitly as a function by listing the input and output values.
- **(b)** Write out the product of cycles $(1\,3\,5)(2\,5)$ explicitly as a function by listing the input and output values.
- **(c)** Which of the following expressions yield the same permutation:
  - $(1\,5\,3\,4)$
  - $(1\,4\,3\,5)$
  - $(3\,4\,1\,5)$
- **(d)** What is the inverse of $(1\,5\,3\,4)$? How would you find the inverse of a cycle in general?
- **(e)** What is the *order*[1] of $(1\,5\,3\,4)$? How would you find the order of a cycle in general?

(2) Show the following Lemma: For any distinct $i_1, \ldots, i_p \in [n]$,

$$(i_1\ i_2\ \cdots\ i_p) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{p-1}\ i_p).$$

We say that two cycles $\sigma = (i_1\, i_2\ \cdots\ i_n)$ and $\tau = (j_1\, j_2\ \cdots\ j_m)$ are **disjoint** if $i_a \neq j_b$ for all a, b.

Theorem 1: Let $n \geq 1$ be an integer, and consider the symmetric group S_n.

1. Every permutation $\sigma \in S_n$ is equal to a product of disjoint cycles.
2. Disjoint cycles commute: if σ, τ are disjoint cycles, then $\sigma\tau = \tau\sigma$.
3. The expression of a permutation σ as a product of disjoint cycles is unique up to permuting factors.

The **cycle type** of a permutation is the list of the lengths of the cycles in its expression as a product of disjoint cycles.

(3) Theorem 1(1) in action: To write $\sigma \in S_n$ as a product of disjoint cycles,

- Start with $1 \in [n]$,
- Look at $\sigma(1), \sigma^2(1), \ldots$ until we get back to $1 = \sigma^m(1)$. Make a cycle out of these:

$$(1\ \sigma(1)\ \sigma^2(1)\ \cdots\ \sigma^{m-1}(1)).$$

- Look at the smallest element of $[n]$ that hasn't appeared, and repeat.
- Throw away the 1-cycles at the end.

[1] Recall that the **order** of an element g in a group G is the smallest integer $n > 0$ such that $g^n = e$.

(a) Write the following permutation in S_7 as a product of disjoint cycles:

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

(b) Write the following product of nondisjoint cycles in S_7 as a product of disjoint cycles:

$$(1\,3\,5\,7)(2\,3\,4\,5).$$

(c) What is the cycle type of $(1\,2)(3\,4)$? What is the cycle type of $(1\,2)(2\,3)$?

(4) Proof of Theorem 1:
- (a) What is the key idea to prove part (1) of Theorem 1?
- (b) Prove part (2) of Theorem 1.
- (c) Complete the proofs of parts (1) and (3) of Theorem 1.

THEOREM 2: Let $n \geq 1$ be an integer, and consider the symmetric group S_n.
- (1) Every permutation $\sigma \in S_n$ is equal to a product of transpositions; thus, S_n is **generated**[2] by transpositions.
- (2) For a fixed $\sigma \in S_n$, either
  - every expression of σ as a product of transpositions involves an *even* number of transpositions, or
  - every expression of σ as a product of transpositions involves an *odd* number of transpositions.

In the first case, we say that σ is an **even** permutation and define $\operatorname{sign}(\sigma) = 1$; in the second case, we say that σ is an **odd** permutation and define $\operatorname{sign}(\sigma) = -1$.

(5) Signs of permutations:
- **(a)** What is the sign of a transposition? Of a 3-cycle? Of a p-cycle? (Hint: Use the Lemma.)
- **(b)** If the cycle type of σ is $m_1, m_2, \ldots, m_t$, then what is the sign of σ?

(6) Proving Theorem 2:
- (a) Prove the Lemma.
- (b) Explain how part (1) of Theorem 2 follows from the Lemma and Theorem 1.
- (c) Explain why part (2) of Theorem 2 reduces to the following claim: if $\tau_1, \ldots, \tau_m$ are transpositions and $\tau_1 \cdots \tau_m = e$, then m is even.
- (d) Reconsider the claim above in the equivalent form: if $\tau_1, \ldots, \tau_m$ are transpositions and m is odd, then $\tau_1 \cdots \tau_m \neq e$. Proceed by induction on m odd. Resolve the base case.
- (e) Show[3] the inductive step, and complete the proof.

[2] Recall that a group G is **generated** by a set S if every element of G can be written as a product of elements of S and their inverses.

[3] Hint: You might find it useful to show that

$$(cd)(ab) = (ab)(cd) \qquad \text{and} \qquad (bc)(ab) = (ac)(bc)$$

for all distinct a, b, c, d in $[n]$.