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 $[n] := \{1, \dots, n\}$.

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.

$1 \mapsto 4$, $2 \mapsto 2$, $3 \mapsto 1$, $4 \mapsto 3$, $5 \mapsto 5$.

(b) Write out the product of cycles $(1\,3\,5)(2\,5)$ explicitly as a function by listing the input and output values.

$1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 5$, $4 \mapsto 4$, $5 \mapsto 2$.

(c) Which of the following expressions yield the same permutation:

- $(1\,5\,3\,4)$
- $(1\,4\,3\,5)$
- $(3\,4\,1\,5)$

The first and the last.

(d) What is the inverse of $(1\,5\,3\,4)$? How would you find the inverse of a cycle in general?

$(1\,4\,3\,5)$. The inverse of a cycle is the reverse cycle.

(e) What is the *order*[1] of $(1\,5\,3\,4)$? How would you find the order of a cycle in general?

The order of $(1\,5\,3\,4)$ is four. The order of an n-cycle is n.

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

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

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.

[1]Recall that the **order** of an element g in a group G is the least integer $n > 0$ such that $g^n = e$ if some such n exists, else ∞.

[2]Hint: To show that two functions are the same, show they have the same values. Compute what each side does to i_j, and what it does to an element of $[n]$ that is not an i_j.

(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 $i \in [n]$ that hasn't appeared, and repeat with i in place of 1.
- Throw away the 1-cycles at the end.

(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	1	5

$(1\,6)(2\,7\,5\,3)$

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

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

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

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

$2, 2$ for the first; 3 for the second.

(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) Prove part (1) of Theorem 1.
(d) Prove[3] part (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**[4] 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 $\mathrm{sign}(\sigma) = 1$; in the second case, we say that σ is an **odd** permutation and define $\mathrm{sign}(\sigma) = -1$.

[3] Hint: Let $\sigma = \tau_1 \cdots \tau_m$ with τ_i disjoint cycles, and $j \in [n]$. Then j appears in at most one τ_i. Show that, for such i, $\sigma^k(j) = \tau_i^k(j)$ and use this to solve for τ_i.

(5) Signs of permutations:

(a) What is the sign of a transposition? Of a 3-cycle? Of a p-cycle? (Hint: Use the Lemma.)

A transposition has sign -1 by definition. A 3-cycle can be written as a product of two transpositions, so its sign is 1. By the Lemma, a p-cycle can be written as a product of $p-1$ tranpositions, so its sign is $(-1)^{p-1}$.

(b) If the cycle type of σ is $m_1, m_2, \ldots, m_t$, then what is the sign of σ?

Using the previous part, the sign is $(-1)^{(m_1-1)+(m_2-1)+\cdots+(m_t-1)}$.

(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) By way of contradiction, suppose that there exists

$$(a_1\, b_1)(a_2\, b_2)\cdots(a_m\, b_m) = e \qquad \text{with } m \text{ odd.} \tag{$\dagger$}$$

(Here $a_i \neq b_i$ but $a_i = a_j$ or $a_i = b_j$ is allowed.) Explain why, if an example of (†) exists, then there is a (†) with

- the smallest value of m, among all (†)'s
- among all (†)'s where m is minimal, the number t of times that a_1 appears is minimal.

(e) Show that $t = 1$ is impossible, and that[5] if $t \geq 2$, one can find another expression with the same value of m and t and also $a_1 = a_2$. Complete the proof.

[4] 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.

[5] Hint: Use the identities $(cd)(ab) = (ab)(cd)$ and $(bc)(ab) = (ac)(bc)$.