Recall: A **permutation** of a set X is a bijection

$$\sigma : X \to X.$$

Under composition, the set S_X of all permutations of X forms a group. We denote by S_n the group of permutations of $X_n = \{1, \dots, n\}$ and call this the **symmetric group on n letters**. Any subgroup of S_n is called a **permutation group**.

Ex. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_5$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \in S_5$

$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ & $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$

Better: cycle notation.

A cycle of length k is a permutation $\sigma \in S_n$ s.t. $\exists$ distinct $1 \le a_1, \dots, a_k \le n$ with

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \dots,\ \sigma(a_{k-1}) = a_k$$

and $\sigma(a_k) = a$ and $\sigma(i) = i$ for all other integers $1 \le i \le n$.

In this case we can express σ as

$$\sigma = (a_1\, a_2 \cdots a_{k-1}\, a_k). \qquad (a_1, a_2, \dots, a_k)$$

Ex $(1357) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix}$

Call two cycles disjoint if their supports (as functions) are disjoint — that is, if they permute disjoint subsets of $\{1, \dots, n\}$.

e.g.,
$(135) \nmid (24)$ are disjoint
$(135) \nmid (34)$ are not

Thm. Every permutation in S_n can be written as a product of disjoint cycles.

Ex. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (13)(245) = (13)(25)(24)$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} = (13)(45)$

(Proof) Let $X_1 = \{1, \sigma(1), \sigma^2(1), \dots\} \subset X = \{1, \dots, n\}$.
Let i be the smallest integer in $X - X_1$ and set

$$X_2 = \{i, \sigma(i), \sigma^2(i), \dots\}.$$

Notice that $X_1 \cap X_2 \neq \emptyset$. Let j be the smallest element of $X - (X_1 \cup X_2)$, and so on until we have

$$X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_r.$$

Set $\sigma_i(x) := \begin{cases} \sigma(x), & x \in X_i \\ x, & x \notin X_i \end{cases}$.

Then $\sigma_1, \dots, \sigma_r$ are disjoint cycles and one can check that $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$.

Ex. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ $X_1 = \{1, 3\}$, $X_2 = \{2\}$, $X_3 = \{4, 5\}$

$$\sigma_1(x) = \begin{cases} \sigma(x), & x \in X_1 \\ x, & x \notin X_1 \end{cases} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = (13)$$

$$\sigma_2(x) = \begin{cases} \sigma(x), & x \in X_2 \\ x, & x \notin X_2 \end{cases} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = id$$

$$\sigma_3(x) = \begin{cases} \sigma(x), & x \in X_3 \\ x, & x \notin X_3 \end{cases} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (45)$$

Thm. If σ and τ are disjoint cycles, then $\sigma\tau = \tau\sigma$.

A cycle of length 2 is called a transposition.

Thm. For any $n \geq 2$, every $\sigma \in S_n$ can be as a product of transpositions.

(Proof.) We just NTS that any cycle of length k can be written as a product of transpositions. Indeed:

$$(a_1 a_2 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2).$$

Unlike disjoint cycle decompositions, transposition decompositions are not unique: $(123) = (13)(12)$
$= (12)(23)$.

$= (45)(12)(23)(45)$

Nonetheless, the parity of the number of transp. is unique.

Thm. Suppose $\sigma_1\sigma_2\cdots\sigma_m = \tau_1\tau_2\cdots\tau_n$, where each σ_i and τ_j is a transposition. Then m and n are either both even or both odd.

(Proof.)

Lemma. If (1) is written as a product of r transpositions, then r is even.

(Proof probably in book.)

Now consider $\sigma_1\sigma_2\cdots\sigma_m = \tau_1\tau_2\cdots\tau_n$.

$\rightarrow \sigma_1(\sigma_1\sigma_2\cdots\sigma_m) = \sigma_1(\tau_1\tau_2\cdots\tau_n)$

$\rightarrow \sigma_2\cdots\sigma_m = \sigma_1\tau_1\tau_2\cdots\tau_n.$

$\rightarrow \cdots \rightarrow$

$\rightarrow \sigma_m = \sigma_{m-1}\sigma_{m-2}\cdots\sigma_1\tau_1\tau_2\cdots\tau_n.$

$\rightarrow (1) = \sigma_m\sigma_{m-1}\cdots\sigma_1\tau_1\tau_2\cdots\tau_n.$

So $m+n$ is even. ← id ∎

We call a permutation **even** if it's a product of an even number of transpositions and **odd** otherwise.

Let A_n denote the collection of even permutations in S_n.

Thm. A_n is a subgroup of S_n.

(Proof.)

- Since (1) is even (by Lemma in previous proof), A_n is nonempty.

- Pick $\sigma, \tau \in A_n$. Write

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_m$$
$$\tau = \tau_1 \tau_2 \cdots \tau_k$$

as products of transpositions.

Then m and k are even.

Now $\tau^{-1} = \tau_k \cdots \tau_2 \tau_1$, so

$\sigma \tau^{-1} = \sigma_1 \sigma_2 \cdots \sigma_m \tau_k \cdots \tau_2 \tau_1$.

Since $m+k$ is even, $\sigma \tau^{-1} \in A_n$. ∎

We call A_n the alternating group on n letters.