SYMMETRIC GROUPS

Recall that the symmetric group $S_n$ of $n$ letters is the set of all bijections $\{1, 2, \ldots, n\} \rightarrow \{1, 2, \ldots, n\}$ with the law of composition to be composition of maps.

Notations. One way to represent an element $\sigma \in S_n$ is to list the image of each number:

$$
\begin{pmatrix}
1 & 2 & \cdots & n \\
\sigma(1) & \sigma(2) & \cdots & \sigma(n)
\end{pmatrix}
$$

For example, if $\sigma \in S_3$ permutes 1 and 2, and fixes 3, we can write $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

This notation is clear, but sometimes takes lots of time to write down.

If $a_1, a_2, \ldots, a_k$ are distinct numbers from $\{1, 2, \ldots, n\}$, define the $k$-cycle $(a_1 \ a_2 \ \cdots \ a_k)$ to be the element in $S_n$ that sends $a_1$ to $a_2$,$a_2$ to $a_3$,$\quad \vdots$ $a_{k-1}$ to $a_k$, $a_k$ to $a_1$, and fixes all the other numbers.

For example, if $\sigma = (1 \ 2 \ 3) \in S_4$, then $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$, $\sigma(4) = 4$. 

40
In general, cycles do not commute. For example, $(12)(13) = (132)$ while $(13)(12) = (123)$.

**Definition.** Two cycles $(a_1 \ldots a_k)$ and $(b_1 \ldots b_l)$ are disjoint if \[ \{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset. \]

**Lemma.** Two disjoint cycles commute with each other.

**Proof.** We can let $(a_1 \ldots a_k), (b_1 \ldots b_l)$ and $(b_1 \ldots b_l)(a_1 \ldots a_k)$ act on any number in \(\{1, 2, \ldots, n\}\), we'll find the images are always equal.

**Remark.** One cycle may have more than one expressions. Indeed, there are \(k\) equivalent expressions for each cycle. For example, \((1 2 3) = (2 3 1) = (3 1 2) \in S_3\).

- When we compute the composition of cycles, we regard each cycle as a function, so the right side one acts on \(\{1, \ldots, n\}\) first, then the left side one.

**Theorem.** Each element in \(S_n\) can be written as a product of disjoint cycles in a unique way, up to reordering of the cycles.

**Proof.** Let \(f \in S_n\). Define an equivalence relation on \(\{1, 2, \ldots, n\}\) by \(i \sim j\) if \(\exists t \in \mathbb{Z}\) such that \(f^t(i) = j\). It's not hard to check this defines an equivalence relation on \(\{1, 2, \ldots, n\}\), so we leave it as an exercise. This equivalence relation brings a partition of \(\{1, 2, \ldots, n\}\) into equivalence classes. We take a representative from each class: \(a_1, a_2, \ldots, a_k\).
Suppose $m_i = \min\{m > 0 \mid \sigma^m(a_i) = a_i\}$.

The equivalence class represented by $m_i$ can be written as $\{a_i, \sigma(a_i), \ldots, \sigma^{m_i-1}(a_i)\}$, and we see $\sigma$ permutes these elements in a cyclic way.

So we can write

$\sigma = (a_1 \sigma(a_1) \ldots \sigma^{m_1-1}(a_1)) \ldots (a_K \sigma(a_K) \ldots \sigma^{m_K-1}(a_K))$

which is a product of disjoint cycles.

If $\sigma$ is written as a product of disjoint cycles, then for any $k \in \{1, \ldots, n\}$, the number after $k$ in the cycle that contains $k$ has to be $\sigma(k)$, since other cycles all keep $k$ and $\sigma(k)$ fixed, so the uniqueness follows.

**Definition.** Write $\sigma \in S_n$ as a product of disjoint cycles, we list the lengths of the cycles in an increasing order:

$1 \leq n_1 < n_2 \leq \cdots \leq n_r$ so that $n_1 + n_2 + \cdots + n_r = n$.

We define the cycle type of $\sigma$ to be $(n_1, n_2, \ldots, n_r)$ or write as $n_1 + n_2 + \cdots + n_r$.

**Remark.** When we write an element in $S_n$ as a product of disjoint cycles, we usually omit the cycles of length one. For example, we write $(1 \ 2 \ 3)$ instead of $(1 \ 2 \ 3)(4)$. But when writing the cycle type, we need to write down the cycles of length 1, so $(1 \ 2 \ 3) \in S_4$ has cycle type $1^3$.

We are interested in cycle types because of the following theorem:
Theorem. Two elements in $S_n$ are conjugate to each other if and only if they have the same cycle type.

Proof. First, for a cycle $(a_1 \ldots a_k) \in S_n$
we can show that $\forall \tau \in S_n : \tau (a_1 \ldots a_k) \tau^{-1} = (\tau(a_1) \ldots \tau(a_k))$
which will be left as an exercise.
Next, since each $\sigma \in S_n$ can be written as a product of disjoint cycles, so if we apply the first step to each cycle, we see $\sigma$ and $\tau \circ \sigma \circ \tau^{-1}$ have the same cycle type.
Conversely, if two elements $\sigma_1$ and $\sigma_2$ have the same cycle type, then by the formula $
\tau (a_1 \ldots a_k) \tau^{-1} = (\tau(a_1) \ldots \tau(a_k)) \n$we can find an $\tau \in S_n$ such that $\sigma_1 = \tau \sigma_2 \tau^{-1}$.

Example. Find $\tau \in S_6$ such that $\tau (1 3 5) \tau^{-1} = (2 4 6)$
By the formula $\tau (a_1 \ldots a_k) \tau^{-1} = (\tau(a_1) \ldots \tau(a_k))$
we can let $\tau(1) = 2$, $\tau(2) = 4$, $\tau(3) = 6$.
We also need to assign values to $\tau(4)$, $\tau(5)$, $\tau(6)$, but there are no restrictions, as long as
$
\{\tau(4), \tau(5), \tau(6)\} = \{1, 3, 5\} \n$so we may let $\tau(4) = 1$, $\tau(5) = 3$, $\tau(6) = 5$.
$\tau = (1 2 4)(3 6 5)$

Example. Find $\tau \in S_7$ such that $\tau (1 2)(3 4 5) \tau^{-1} = (1 3)(5 6 7)$
$\tau (1 2)(3 4 5) \tau^{-1} = (\tau(1) \ \tau(2)) (\tau(3) \ \tau(4) \ \tau(5)) \n$so we can let $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 5$, $\tau(4) = 6$, $\tau(5) = 7$.
and $\tau(6) = 2$, $\tau(7) = 4$.