Factorization of Permutations into Transpositions

**Theorem:** Every permutation is a product of transpositions (2-cycles).

**Proof.** It suffices to show that every $k$-cycle can be expressed as the product of $k - 1$ transpositions. We have

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1})(a_1, a_{k-2}) \cdots (a_1, a_2).$$

Our goal now is to show that the set of permutations which can be expressed as a product of an even number of transpositions is a normal subgroup of index 2 in $S_n$.

**Lemma:** Fix $k \geq 1$.

1. $(i, k)(j, k) = (i, k, j) = (k, j)(i, j)$ where $i$, $j$, and $k$ are distinct.
2. $(x, y)(j, k) = (j, k)(x, y)$ where $j$, $k$, $x$, and $y$ are distinct.

**Corollary:** Fix $k \geq 1$. Any product of two distinct transpositions $\alpha \beta$ where $k$ appears in $\beta$ is equal to another product of two distinct transpositions $\gamma \delta$ where $k$ does not appear in $\delta$ and it does appear in $\gamma$.

**Theorem:** Any product of $n \geq 3$ transpositions which equals the identity permutation can be transformed into a product of $n - 2$ transpositions which equals the identity permutation.

**Proof.** Suppose

$$\tau_1 \tau_2 \cdots \tau_n = e.$$

If $\tau_{n-1} = \tau_n$ then $\tau_{n-1} \tau_n = e$ and we have

$$\tau_1 \tau_2 \cdots \tau_{n-2} = e.$$

Now assume $\tau_{n-1} \neq \tau_n$. Say that $k$ appears in $\tau_n$. Then we can transform $\tau_{n-1} \tau_n$ into $\tau'_{n-1} \tau'_n$ so that $k$ does not appear in $\tau'_{n}$ but it does appear in $\tau'_{n-1}$. We now have

$$\tau_1 \cdots \tau_{n-2} \tau'_{n-1} \tau'_n = e.$$

If $\tau_{n-2} = \tau'_{n-1}$ then $\tau_{n-2} \tau'_{n-1} = e$, and eliminating them we have

$$\tau_1 \cdots \tau_{n-3} \tau'_n = e.$$
But if \( \tau_{n-2} \neq \tau'_{n-1} \) then we can transform \( \tau_{n-2}\tau'_{n-1} \) into \( \tau'_{n-2}\tau''_{n-1} \) so that \( k \) does not appear in \( \tau''_{n-1} \) but it does appear in \( \tau'_{n-2} \). We now have

\[
\tau_1 \cdots \tau_{n-3}\tau'_{n-2}\tau''_{n-1}\tau'_n = e,
\]

where \( k \) appears in \( \tau'_{n-2} \) but not in \( \tau''_{n-1} \) or \( \tau'_n \). Keep on going. We either obtain a product of \( n - 2 \) transpositions which equals \( e \), or we obtain a product of \( n \) transpositions

\[
\sigma_1 \cdots \sigma_n = e
\]
such that \( k \) appears in \( \sigma_2 \) but not in \( \sigma_3 \) through \( \sigma_n \). If \( \sigma_1 \neq \sigma_2 \) then we can convert this to

\[
\sigma'_1\sigma'_2 \cdots \sigma_n = e
\]

where \( k \) only appears in \( \sigma'_1 \). This is impossible, because \( e \) fixes \( k \) while

\[
\sigma'_1\sigma'_2 \cdots \sigma_n
\]
do not fix \( k \). Therefore we must have \( \sigma_1 = \sigma_2 \), which leaves us with

\[
\sigma_3 \cdots \sigma_n = e.
\]

So ultimately we do reduce the product from \( n \) to \( n - 2 \) transpositions.

**Corollary:** If

\[
\tau_1 \cdots \tau_n = e
\]
is a product of transpositions, then \( n \) is an even number.

**Proof.** Suppose it is possible for the product of an odd number of transpositions to equal the identity permutation. Then there is a smallest odd number \( n \) for which this is true. We must have \( n \geq 3 \) because no transposition is equal to the identity. By the theorem above, it must therefore be possible that a product of \( n - 2 \) transpositions is equal to the identity permutation. However, this is a smaller odd number. Contradiction. Therefore no product of an odd number of transpositions can be equal to the identity permutation.

**Theorem:** No permutation can be expressed in one way as the product of an even number of transpositions and in another way as the product of an odd number of transpositions.
Proof. If this were possible then we would have

$$\alpha_1 \cdots \alpha_m = \beta_1 \cdots \beta_n,$$

where all terms are transpositions and $m$ is even and $n$ is odd. Multiplying both sides by the inverse of $\beta_1 \cdots \beta_n$, we obtain

$$\alpha_1 \cdots \alpha_m \beta_n \cdots \beta_1 = e.$$

This implies that $m + n$ is even, which is false. Therefore there is no such example.

Definition: Let $\sigma$ be a permutation. $\sigma$ is even if it can be expressed as the product of an even number of transpositions. $\sigma$ is odd if it can be expressed as the product of an odd number of transpositions.