Transpositions

Defn: A *transposition* is a cycle $(a\ b) \in S_X$.

Ex:
- $(1\ 3) \in S_7$ is a transposition
- $(1\ 3\ 5) \in S_7$ is NOT a transposition!

(NB: a more formal way to define a transposition:
$\tau \in S_X$ is a transposition when $|\{x \in X : \tau(x) \neq x\}| = 2$)

Lem: Every cycle can be expressed as a product of transpositions

pf: We prove by induction on the length of the cycle that

$$(x_1\ x_2\ \cdots\ x_n) = (x_1\ x_n)(x_1\ x_{n-1}) \cdots (x_1\ x_2).$$

Base Case: If $n=2$ then $(x_1\ x_2) = (x_1\ x_2)$.

Inductive Step: Suppose every length n cycle can be expressed as above. Now consider a cycle $\sigma = (x_1\ x_2\ \cdots\ x_n\ x_{n+1})$.

First we show $\boxed{\sigma = (x_1\ x_{n+1})(x_1\ x_2\ \cdots\ x_n)}$. Indeed

$$\sigma(y) = \begin{cases} y & \text{if } y \neq x_i \text{ for all } i \\ x_{i+1} & \text{if } y = x_i \text{ for some } 1 \leq i \leq n \\ x_1 & \text{if } y = x_{n+1} \end{cases}$$

Now we can compute the values for the right-hand side

- $[(x_1\ x_{n+1})(x_1\ x_2\ \cdots\ x_n)](y) = y$ if $y \neq x_i$ for all i,
- $[(x_1\ x_{n+1})(x_1\ x_2\ \cdots\ x_n)](x_i) = [(x_1\ x_{n+1})](x_{i+1}) = x_{i+1}$ if $1 \leq i < n$,
  $[(x_1\ x_{n+1})(x_1 x_2\ \cdots\ x_n)](x_n) = [(x_1\ x_{n+1})](x_1) = x_{n+1}$, and
- $[(x_1\ x_{n+1})(x_1\ x_2\ \cdots\ x_n)](x_{n+1}) = [(x_1\ x_{n+1})](x_{n+1}) = x_1$.

Hence the left and right sides agree pointwise.

Applying the inductive hypothesis yields $\sigma = (x_1\ x_{n+1})(x_1\ x_n) \cdots (x_1\ x_2)$. $\boxtimes$

$(x_1\ x_1\ \cdots\ x_n)$

<u>Cor:</u> Every $\sigma \in S_X$ (for X finite) can be expressed as a product of transpositions.

<u>pf:</u> Let $\boxed{\sigma \in S_X}$ be arbitrary. If $\sigma = \varepsilon$, then σ is the empty product of transpositions. Otherwise, $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ for some disjoint cycles $\sigma_1, \sigma_2, \ldots, \sigma_k \in S_X$.

Apply the lemma to each σ_i to obtain σ_i as a product of transpositions $\boxed{\sigma_i = \tau_{i,1} \tau_{i,2} \cdots \tau_{i,m_i}}$. Replace each σ_i by this product to obtain the result. ☐

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$$
$$= \tau_{1,1} \tau_{1,2} \cdots \tau_{1,m_1} \tau_{2,1} \tau_{2,2} \cdots \tau_{2,m_2} \cdots \tau_{k,1} \tau_{k,2} \cdots \tau_{k,m_k}$$

Transpositions

Lem: If $\varepsilon = \tau_1\tau_2\cdots\tau_k$ for transpositions τ_i, then k is even.

Idea of proof: We use induction and three basic properties.

→ ① Transpositions are self-inverse: $(a\ b)(a\ b) = \varepsilon$

→ ② Disjoint transpositions commute: $(a\ b)(c\ d) = (c\ d)(a\ b)$

→ ③ overlapping transpositions are "entangled": $(a\ b)(a\ c) = (b\ c)(a\ b)$

The three properties will allow us to eliminate all occurances of one element of $X = \{1, 2, \cdots, n\}$ from the τ_i's. The result, if we do this to eliminate all n's, can be used to express ε as a product of transpositions in S_{n-1} (cue induction).

pf: Suppose $\varepsilon = \tau_1\tau_2\cdots\tau_k$ for $\tau_i \in S_n$. We induct on n.
transposition

Base Cases: If $n=0$ or $n=1$, there are no transpositions in S_n, so $k=0$ and the statement holds.

If $n=2$, then note $S_2 = \{\varepsilon, (1\ 2)\}$. Thus $\tau_i = (1\ 2)$ for all i. Hence $\varepsilon = \underbrace{(1\ 2)(1\ 2)\cdots(1\ 2)}_{k \text{ times}}$. If k were odd, then $k = 2m+1$ for some $m \in \mathbb{N}$, and we may express

$$\varepsilon = \underbrace{((1\ 2)(1\ 2))((1\ 2)(1\ 2))\cdots((1\ 2)(1\ 2))}_{m \text{ times}}(1\ 2) = \underbrace{\varepsilon\cdot\varepsilon\cdots\varepsilon}_{m \text{ times}}(1\ 2) = (1\ 2),$$ ABSURD!

Hence k is necessarily even when $n=2$.

Inductive Step: Suppose $n \geq 3$ and the statement holds for $n-1$.

$|\{x\in X : \sigma(x) \neq x\}|$

Observe $k \neq 1$, lest $\varepsilon = \tau_1$, which is absurd! We now write an algorithm to show that we can replace the expression

$$\boxed{\varepsilon = \tau_1\tau_2\cdots\tau_k} = \nu_1\nu_2\cdots\nu_m$$ for transpositions ν_j with $\nu_j(n) = n$ for all j.

viewable as a product of transpositions in S_{n-1}

If all of the τ_i's fix n, we're done. Otherwise, let i be the smallest index with $\tau_i(n) \neq n$. Thus $\boxed{\tau_i = (n\ x_i)}$.

$$\underbrace{\tau_1 \tau_2 \cdots \tau_{i-1}}_{\text{fix } n} \tau_i \tau_{i+1} \cdots \tau_k \qquad \tau_i(n) \neq n$$

Observe $\boxed{i \neq k}$, lest

"if $i = k$"

$$\boxed{x_i} = \varepsilon(x_i) = (\tau_1 \tau_2 \cdots \tau_{k-1} (n\ x_i))(x_i) = (\tau_1 \tau_2 \cdots \tau_{k-1})(n) = \boxed{n}$$

$\therefore$ we can consider τ_{i+1}. There are three cases.

<u>Case 1</u>: If $\tau_{i+1} = \tau_i$, then $\tau_i \tau_{i+1} = \varepsilon$ So...

* (we removed exactly 2)

$$* \ \varepsilon = \tau_1 \tau_2 \cdots \tau_{i-1} \tau_i \tau_{i+1} \tau_{i+2} \cdots \tau_k = \tau_1 \tau_2 \cdots \tau_{i-1} \tau_{i+2} \cdots \tau_k.$$

Thus we've reduced the number of τ_j's that move n. Return to beginning.

<u>Case 2</u>: If τ_{i+1} is disjoint with τ_i, we can commute τ_i and τ_{i+1}.

(Number fixed)

$$\varepsilon = \tau_1 \tau_2 \cdots \tau_{i-1} \tau_i \tau_{i+1} \cdots \tau_k = \tau_1 \tau_2 \cdots \tau_{i-2} \tau_{i+1} \tau_i \tau_{i+2} \cdots \tau_n.$$

Thus we have "pushed" the first τ_j (from the left) that moves n closer to the right. Return to the beginning of the procedure.

<u>Case 3</u>: If τ_{i+1} overlaps τ_i, there are two subcases.

<u>Subcase A</u>: $\tau_{i+1} = (n\ x_{i+1})$. Then

$$* \ \tau_i \tau_{i+1} = (n\ x_i)(n\ x_{i+1}) = (n\ x_{i+1}\ x_i) = (x_i\ n\ x_{i+1}) = (x_i\ x_{i+1})(n\ x_i)$$

Thus $[\varepsilon = \tau_1 \tau_2 \cdots \tau_{i-1} \tau_i \tau_{i+1} \tau_{i+2} \cdots \tau_k = \tau_1 \tau_2 \cdots \tau_{i-1} (x_i\ x_{i+1})(n\ x_i) \tau_{i+2} \cdots \tau_k]$

Thus we've "pushed" the first τ_j (from the left) that moves n closer to the right. Return to the beginning.

(number of transpos same)

<u>Subcase B</u>: $\tau_{i+1} = (x_i\ x_{i+1})$. Then

$$\tau_i \tau_{i+1} = (n\ x_i)(x_i\ x_{i+1}) = (n\ x_i\ x_{i+1}) = (x_{i+1}\ n\ x_i) = (x_i\ x_{i+1})(n\ x_{i+1})$$

Thus $\varepsilon = \tau_1 \tau_2 \cdots \tau_{i-1} \tau_i \tau_{i+1} \tau_{i+2} \cdots \tau_k = \tau_1 \tau_2 \cdots \tau_{i-1} (x_i\ x_{i+1})(n\ x_{i+1}) \tau_{i+2} \cdots \tau_k$

Thus we've "pushed" the first τ_j (from the left) that moves n closer to the right. Return to the beginning.

(number of transpos same)

Hence, in all cases we have advanced the index of the transposition to consider. As k is finite, this procedure must terminate. The only way that can happen is if $\nu_i(n) = n$ for all i. Hence we may consider the product $\varepsilon = \nu_1 \nu_2 \cdots \nu_m$ as a product in (S_{n-1}).

By induction, m is even. Finally, note that $k \equiv m \mod 2$.

Indeed, each case above either ① keeps the number of transpositions the same or ② reduces that number by 2.

Hence, k is even, as claimed. ☒

Defn: If $\sigma = \tau_1 \tau_2 \cdots \tau_k$, then σ is...

$$\left\{\begin{matrix} \text{even} \\ \text{odd} \end{matrix}\right\} \text{ if } k \text{ is } \left\{\begin{matrix} \text{even} \\ \text{odd} \end{matrix}\right\}.$$

This is the *parity* of σ.

Theorem: Permutation parity is well-defined.

pf: Suppose $\sigma \in S_n$ and $[\sigma = \tau_1 \tau_2 \cdots \tau_k = \rho_1 \rho_2 \cdots \rho_m]$ for transpositions $\tau_1, \tau_2, \ldots, \tau_k$ and $\rho_1, \rho_2, \ldots, \rho_m$.

Then $\varepsilon = \sigma^{-1}\sigma = (\tau_1 \tau_2 \cdots \tau_k)^{-1}(\rho_1 \rho_2 \cdots \rho_m) = \tau_k \tau_{k-1} \cdots \tau_2 \tau_1 \rho_1 \rho_2 \cdots \rho_m$.

Thus, we've expressed ε as a product of $m+k$ transpositions.

Hence $m + k \equiv 0 \mod 2$, which yields $m \equiv k \mod 2$. ☒