Fundamental Theorem of Symmetric Groups

Fundamental Theorem of Symmetric Groups. Every element $\alpha \in S_X$ has a complete factorization, unique up to reordering.

Example 1. If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 3 & 1 & 4 & 6 & 2 \end{pmatrix}$, then $\alpha = (154)(27)(3)(6)$ and $\{1,2,3,4,5,6,7\} = \{1,4,5\} \sqcup \{2,7\} \sqcup \{3\} \sqcup \{6\}$.

Let $X$ be a finite set and $\alpha : X \to X$ a bijection.

Definition 2. $Y \subset X$ is $\alpha$-invariant if $\alpha(Y) \subset Y$ and $Y$ is nonempty.

Lemma 3. If $Y$ is $\alpha$-invariant, then

1. $\alpha(Y) = Y$
2. $\alpha(Y') \subset Y'$.
3. $\alpha(Y') = Y'$.

Proof. 1. Pigeonhole Principle:
$\alpha : Y \to Y$ injective $\implies$ $\alpha$ bijective.
2. By contradiction. If $\exists b \in Y'$ with $\alpha(b) \in Y$, then by 1. $\exists a \in Y$ so that $\alpha(b) = \alpha(a)$. But $\alpha$ is injective. #.
3. Follows from 2. and 1.

Notation:

- If $Y$ is $\alpha$-invariant, define the restriction $\alpha|_Y \in S_Y$ by $\alpha|_Y(i) = \alpha(i)$ for $i \in Y$. 


If $Y \subset X$, $\beta \in S_Y$ and $\gamma \in S_{Y'}$ then define $\beta \gamma \in S_X$ by
\[
\beta \gamma(i) = \begin{cases} 
\beta(i) & i \in Y \\
\gamma(i) & i \in Y'
\end{cases}
\]

**Definition 4.** $Y$ is an $\alpha$-cycle if $Y = \{i_1, i_2, \ldots, i_r\}$ and $\alpha|_Y = (i_1 i_2 \ldots i_r)$.

**Definition 5.** $Y$ is a *minimal $\alpha$-invariant set* if it is $\alpha$-invariant and has no proper subsets which are $\alpha$-invariant.

**Lemma 6.**
1. Any $i_1 \in X$ is contained in an $\alpha$-cycle.
2. An $\alpha$-cycle is a minimal $\alpha$-invariant set.
3. A minimal $\alpha$-invariant set is an $\alpha$-cycle.

**Proof.**
1. Inductively define $i_{j+1} = \alpha(i_j)$. Let $r$ be the smallest positive integer so that $\alpha(i_r) = i_{r+1} \in \{i_1, \ldots, i_r\}$. Then $\alpha(i_r) = \alpha(i_j)$ for some $j$ and since $\alpha$ is injective, $j = 1$ (or else $\alpha(i_r) = \alpha(i_{j-1})$).
2. Clear.
3. If $Y$ is a minimal $\alpha$-invariant set, and $i_1 \in Y$, then there exists a $\alpha$-cycle $Z$ so that $i_1 \in Z \subset Y$. Then $Y = Z$ by minimality.

**Definition 7.** A *partition of a set* $X$ is a collection of subsets $Y_1, Y_2, \ldots, Y_l$ so that every element of $X$ is a member of exactly one of the $Y_i$’s. In this case we write
\[
X = Y_1 \sqcup Y_2 \sqcup \cdots \sqcup Y_l
\]
where the symbol $\sqcup$ is called *disjoint union*.

**Lemma 8.** The minimal $\alpha$-invariant sets partition $X$.

**Proof.** Two different $\alpha$-invariant sets are disjoint by minimality. Lemma 6 shows that every element is contained in a minimal $\alpha$-invariant set.

**Proof of the Fundamental Theorem.** Let $X = Y_1 \sqcup Y_2 \sqcup \cdots \sqcup Y_l$ be a partition of $X$ into minimal $\alpha$-invariant sets. This is unique, up to reordering. By Lemma 6, $\alpha|_{Y_i}$ is an $\alpha$-cycle for each $i$ and thus $\alpha = \alpha|_{Y_1} \sqcup \alpha|_{Y_2} \sqcup \cdots \sqcup \alpha|_{Y_l}$ is a complete factorization. Conversely, a complete factorization gives a partition of $X$ into minimal $\alpha$-invariant sets, and the uniqueness of the partition gives a unique complete factorization.