Lema. Sea $g \in S_X$ y sea $t = (\alpha\ \beta)$ una transposición. Entonces

a. $c(tg) = c(g) + 1$ si α y β están en la misma $\langle g \rangle$-orbita

b. $c(tg) = c(g) - 1$ si α y β están en distintas $\langle g \rangle$-orbitas.

Dem:

Sup. que α y β están en la misma $\langle g \rangle$-orbita Λ. Entonces podemos escribir $g_\Lambda = (\alpha_1\ \alpha_2 \cdots \alpha_m)$ con $\alpha_1 = \alpha$ y $\alpha_k = \beta$ con $1 < k \leq m$. Calculamos

$$tg_\Lambda = (\alpha\ \beta)(\alpha_1\ \alpha_2 \cdots \alpha_m) = (\alpha_1\ \alpha_2 \cdots \alpha_{k-1})(\alpha_k \cdots \alpha_m).$$

Como g y tg_Λ actuan identicamente en las otras $\langle g \rangle$-orbitas distintas de Λ, entonces tambien son $\langle tg_\Lambda \rangle$-orbitas. En Λ, sin embargo, tg y tg_Λ actuan igual y descomponen a Λ en dos $\langle tg \rangle$-orbitas. Por lo tanto $c(tg) = c(g) + 1$.

Ahora supongamos que tenemos dos $\langle g\rangle$-orbitas $\Lambda \neq \Delta$ con $\alpha \in \Lambda$ y $\beta \in \Delta$

Podemos escribir $g_\Lambda = (\alpha_1 \alpha_2 \cdots \alpha_m)$ y $\beta = (\beta_1 \beta_2 \cdots \beta_n)$ con $\alpha_1 = \alpha$ y $\beta_1 = \beta$.

Entonces $t g_\Delta g_\Lambda = (\alpha \beta)(\beta_1 \beta_2 \cdots \beta_n)(\alpha_1 \alpha_2 \cdots \alpha_m) = (\alpha_1 \alpha_2 \cdots \alpha_m \beta_1 \beta_2 \cdots \beta_n)$.

Entonces g y tg actuan igual en todas $\langle g\rangle$-orbitas que no son Λ y Δ.

En $\Lambda \cup \Delta$ la acción de tg es la misma que la de $t g_\Delta g_\Lambda$ así que $\Lambda \cup \Delta$ es una $\langle tg\rangle$-orbita y $c(tg) = c(g) - 1$.

Teorema.

Ningún elemento de S_X puede escribirse como al mismo tiempo como un producto de un número par y de un número impar de transposiciones.

Dem:

Por el lema anterior $c(tg) \equiv c(g) + 1 \mod 2$ para cada transposición t.

Repitiendo esto para transposiciones $t_1, t_2, \dots, t_m$ tenemos que $C(t_m t_{m-1} \cdots t_1) \equiv C(Id) + m = |X| + m \mod 2$. Se sigue que $g \in S_X$ es par si $C(g) \equiv |X| \mod 2$ y es impar si $C(g) \equiv |X| + 1 \mod 2$, y no es posible tener las dos congruencias al mismo tiempo.

Cor. Sea $|X| > 1$. Entonces el conjunto de permutaciones pares en S_X forma un subgrupo normal de índice 2.

Dem:

Es claro que el producto de dos permutaciones pares es par. Ahora si $g = t_1 t_2 \cdots t_m$ es una permutacion par, entonces $g^{-1} = t_m \cdots t_2 t_1$ también es par. Por lo tanto, si A es conjunto de permutaciones pares, ent $A \leq S_X$. Como $h \in S_X$ tiene la misma paridad que h^{-1}, se sigue que $h^{-1} g h \in A$ $\forall g \in A$ $\forall h \in S_X$. Por lo tanto $A \trianglelefteq S_X$.

Sea $t \in S_X$ una transposición. Si $g \in S_X$ es impar $tg \in A$ y así $tg \in tA$.

Así que $S_X = A \cup tA$ y como $t \notin A$, $[S_X : A] = 2$.

Def: Al subgrupo de S_X formado por todas las permutaciones pares se le llama el grupo alternante en X. Si $X = \{1, \ldots, n\}$, lo denotamos A_n.

Prop. El grupo alternante A_n con $n \geq 3$ está generado por los 3-ciclos.

Dem:

Solo notemos lo siguiente: Sean $(i\ j), (k\ \ell)$ dos transposiciones. Si $i = k$, entonces $(i\ j)(i\ \ell) = (i\ \ell\ j)$ y si i, j, k, ℓ son todos distintos entonces $(i\ j)(k\ \ell) = (i\ j)(i\ k)(k\ i)(k\ \ell) = (i\ k\ j)(k\ \ell\ i)$.

Cor. Sea $g \in S_X$ un m-ciclo y supongamos que $g = t_1 t_2 \cdots t_k$ con t_i transposición. Entonces $k \geq m-1$.