Math 113. Details on Proof II of Theorem 9.15

This handout provides a few more details on the proof of the following theorem from the textbook:

**Theorem 9.15.** No permutation in $S_n \ (n \in \mathbb{N})$ can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

**Proof 2 (counting orbits).** We start with the following claim.

Let $\sigma \in S_n$ and let $\tau$ be a transposition in $S_n$, so $\tau = (a, b)$ with $a \neq b$ in $\{1, 2, \ldots, n\}$. Then the number of orbits of $\sigma$ and of $\sigma\tau$ differ by 1.

**Case I.** Suppose $a$ and $b$ are in different orbits of $\sigma$. Write $\sigma$ as a product of disjoint orbits. We may assume that the last two orbits of $\sigma$ are the orbits containing $a$ and $b$, respectively. Then we have

$$\sigma = (\text{other orbits})(x_1, x_2, \ldots, x_r, a)(y_1, y_2, \ldots, y_s, b).$$

Note that $a, b, x_1, \ldots, x_r, y_1, \ldots, y_s$ are all different. Also, either or both of $r$ and $s$ may be zero.

We will use the identity

$$(x_1, x_2, \ldots, x_r, a)(y_1, y_2, \ldots, y_s, b)(a, b) = (x_1, x_2, \ldots, x_r, a, y_1, y_2, \ldots, y_s, b). \quad (1)$$

You should verify for yourselves that this is true, even if $r = 0$ or $s = 0$ or both. From this, we obtain

$$\sigma\tau = (\text{other orbits})(x_1, x_2, \ldots, x_r, a, y_1, y_2, \ldots, y_s, b),$$

where the “other orbits” are the same as in the above expression for $\sigma$. Then $\sigma\tau$ has exactly one fewer orbit than $\sigma$.

**Case II.** If $a$ and $b$ are in the same orbit of $\sigma$, then we can write

$$\sigma = (\text{other orbits})(x_1, x_2, \ldots, x_r, a, y_1, y_2, \ldots, y_s, b),$$

and use the identity

$$(x_1, x_2, \ldots, x_r, a, y_1, y_2, \ldots, y_s, b)(a, b) = (x_1, x_2, \ldots, x_r, a)(y_1, y_2, \ldots, y_s, b) \quad (2)$$

to obtain

$$\sigma\tau = (\text{other orbits})(x_1, x_2, \ldots, x_r, a)(y_1, y_2, \ldots, y_s, b).$$

Here again the “other orbits” are the same for $\sigma$ and for $\sigma\tau$, and (2) can be verified either directly or by multiplying both sides of (1) by $\tau$ and noting that $(a, b)$ has order two.

Then $\sigma\tau$ has exactly one more orbit than $\sigma$.

This proves the claim, because the two cases cover all possibilities.
Next we show that if $\sigma$ is a product of $m$ transpositions, then

$$m \equiv n - (\text{number of orbits of } \sigma) \pmod{2}. \quad (3)$$

This is proved by induction on $m$. If $m = 0$, then $\sigma$ is the identity element of $S_n$, which has $n$ orbits (every element of the set being permuted is in its own orbit). Therefore the congruence holds because both sides are zero.

To show the inductive step, assume that it holds for all products of $m$ transpositions, and let $\rho$ be a product of $m + 1$ transpositions. Let $\sigma$ be the product of the first $m$ of these transpositions and let $\tau$ be this last transposition, so that $\rho = \sigma \tau$. By the inductive hypothesis, (3) holds for $\sigma$, and we want to show that it holds also for $\rho$. By the claim, the inductive hypothesis, and the fact that both 1 and $-1$ are congruent to 1 modulo 2, we have

$$n - (\text{number of orbits of } \rho) = n - (\text{number of orbits of } \sigma) \pm 1$$

$$\equiv m \pm 1 \pmod{2}$$

$$\equiv m + 1 \pmod{2}.$$

This shows that (3) is also true for $\rho$. Therefore, by induction, it holds for all elements of $S_n$ and all $m$.

Now if $\sigma$ can be written both as a product of an even number $m$ of transpositions and an odd number $m'$, then we have

$$m \equiv n - (\text{number of orbits of } \sigma) \equiv m' \pmod{2}$$

(note that the quantity in the middle depends only on $\sigma$, not on how it’s written as a product of transpositions). But this implies that $m \equiv m' \pmod{2}$, which contradicts the fact that $m$ is even and $m'$ is odd.

Thus, the theorem is proved. \hfill \Box