Remarks on Linear Algebra II, Sheet 1, Hilary Term, 2012

First some notation:

–For a cycle γ, denote by $l(\gamma)$ its length. Note that

$$l(\gamma) = |\mathrm{Supp}(\gamma)|.$$

–For a permutation ρ, denote by $c(\rho)$ the number of distinct cycles in a cycle decomposition of ρ. Here, when we refer to a cycle decomposition, we include the cycles of length one. Thus, for example, in Sym(4), a cycle decomposition of (12) is

$$(12) = (12)(3)(4).$$

Note that since the cycles in a cycle decomposition have disjoint supports, one can change the order of the cycles that occur.

Problem 7 (i) asks the following: Given a permutation $\rho \in \mathrm{Sym}(n)$ with cycle decomposition

$$\rho = \gamma_1\gamma_2\cdots\gamma_k,$$

define the *index* of ρ by

$$\mathrm{Ind}(\rho) = \sum_i [l(\gamma_i) - 1].$$

Using the fact that

$$(a_1a_2\cdots a_s) = (a_1a_2)(a_1a_3)\cdots(a_1a_s),$$

(which involves $s-1$ transpositions) we see right away that ρ can be written as a product of $\mathrm{Ind}(\rho)$ transpositions. But we are aksed to show that $\mathrm{Ind}(\rho)$ is the *minimum* m such that ρ can be written as a product of m transpositions. This fact is rather tricky even for a single cycle γ. It's clear that γ can be broken into $l(\gamma)-1$ transpositions. How do we know there is no shorter expression?
Here is another form of the statement we wish to prove:

If

$$\rho = \tau_1\tau_2\cdots\tau_m \qquad (*)$$

for transpositions τ_i, then $m \geq \mathrm{Ind}(\rho)$.

In this form, one can attempt an induction on m. In any case, the assertion concerns a rather subtle relation between the two standard ways of decomposiing a permutation, in terms of disjoint cycles, and in term of transpositions.

At this point, before we proceed with the induction, let us write down one other convenient expression for the index. When

$$\rho = \gamma_1\gamma_2\cdots\gamma_k$$

is a cycle decomposition, we know that $\sum_i l(\gamma_i) = n$. So

$$\mathrm{Ind}(\rho) = n - k = n - c(\rho),$$

and the assertion we wish to prove for any m as in $(*)$ is

$$m \geq n - c(\rho).$$

Let $m = 1$, so that ρ is a single transposition. Then $\mathrm{Ind}(\rho) = 1$, so clearly, $m \geq \mathrm{Ind}(\rho)$. Now assume the statement true for some $m \geq 1$ and let

$$\rho = \tau_1\cdots\tau_{m+1}.$$

Then

$$\rho = \sigma\tau_{m+1}$$

where

$$\sigma = \tau_1 \cdots \tau_m.$$

Let

$$\sigma = \gamma_1 \cdots \gamma_k$$

be a cycle decomposition of σ. We are assuming that

$$m \geq n - k.$$

We have

$$\rho = \gamma_1 \cdots \gamma_k \tau_{m+1}.$$

We will use this expression to give a lower bound for $c(\rho)$. We consider the two possibilities for the interaction between the support of τ_{m+1} and that of the γ_i. We might have

$$\mathrm{Supp}(\tau_{m+1}) \subset \mathrm{Supp}(\gamma_j)$$

for some j. In this case, since the γ_i commute with each, we may as well assume that

$$\mathrm{Supp}(\tau_{m+1}) \subset \mathrm{Supp}(\gamma_k).$$

Write

$$\rho = (\gamma_1 \cdots \gamma_{k-1})(\gamma_k \tau_{m+1})$$

and

$$\gamma_k \tau_{m+1} = c_1 \cdots c_t$$

for the cycle decomposition of $\gamma_k \tau_{m+1}$. Then

$$\mathrm{Supp}(c_i) \subset \mathrm{Supp}(\gamma_k \tau_{m+1}) = \mathrm{Supp}(\gamma_k).$$

So the support of the c_i are disjoint from $\mathrm{Supp}(\gamma_i)$ for $i < k$. Therefore,

$$\rho = \gamma_1 \cdots \gamma_{k-1} c_1 \cdots c_t$$

is a cycle decomposition of ρ and $c(\rho) \geq k$.
Now suppose $\mathrm{Supp}(\tau_{m+1})$ meets the support of two of the γ_i. Once again, by commuting them through to the end, we can assume they are γ_{k-1} and γ_k. So we have

$$\rho = \gamma_1 \cdots \gamma_{k-2}(\gamma_{k-1}\gamma_k\tau_{m+1}).$$

By the same argument as in the previous paragraph, we then see that

$$c(\rho) \geq k - 1.$$

Therefore, in either case,

$$n - c(\rho) \leq n - k + 1 \leq m + 1,$$

and we are done.

Exercise: Write down an explicit form of a cycle decomposition for $\gamma_k\tau_{m+1}$ and $\gamma_{k-1}\gamma_k\tau_{m+1}$ in the two cases towards the end of the proof above.