7.1 Chapitre 1

Démonstration de la prop. 1.10. Soient σ et τ deux telles permutations. Notons $A = \mathrm{Supp}(\sigma)$ et $B = \mathrm{Supp}(\tau)$ et notons $A' = \{1, \ldots, n\} \smallsetminus A$ et $B' = \{1, \ldots, n\} \smallsetminus B$. Par hypothèse $A \cap B = \emptyset$ donc $A \subseteq B'$ et $B \subseteq A'$.
De plus pour $i \in A', \sigma(i) = i$ et de même pour $i \in B', \tau(i) = i$.
Soit $i \in \{1, \ldots, n\}$. Supposons $i \in A$ alors $i \in B'$ et $\tau(i) = i$ ce qui entraine $\sigma(\tau(i)) = \sigma(i)$.
D'autre part, $\sigma(i) \in A$. En effet, par l'absurde, supposons que $\sigma(i) \in A'$. Alors $\sigma(\sigma(i)) = \sigma(i)$ d'où (en appliquant σ^{-1}) $\sigma(i) = i$ ce qui signifie $i \in A'$. Absurde. Par conséquent $\sigma(i) \in B'$ d'où $\tau(\sigma(i)) = \sigma(i)$.
En conclusion, $\sigma(\tau(i)) = \tau(\sigma(i))$.
Il reste le cas où $i \in A'$. Dans ce cas $\sigma(i) = i$ et donc $\tau(\sigma(i)) = \tau(i)$. D'autre part, $\tau(i) \in B$ si $i \in B$ (c'est la même démonstration par l'absurde que précédemment) et $\tau(i) = i \in A'$ sinon. Dans les deux cas $\tau(i) \in A'$ ce qui entraine $\sigma(\tau(i)) = \tau(i)$ d'où $\tau(\sigma(i)) = \sigma(\tau(i))$. □

Démonstration du Théorème 1.11. Montrons d'abord l'existence par récurrence sur le cardinal du support. Soit $\sigma \in S_n$. Si $\mathrm{Supp}(\sigma) = \emptyset$ alors $\sigma = \mathrm{id}$. Sinon soit i_1 tel que $\sigma(i_1) \neq i_1$. Notons alors $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$, etc. Par finitude de $\{1, \ldots, n\}$ la suite des i_k est finie. Soit alors k le plus petit entier pour lequel $\sigma(i_k) \in \{i_1, \ldots, i_k\}$.
En fait, $\sigma(i_k) = i_1$. En effet si on avait $\sigma(i_k) = i_j$ avec $2 \leq j \leq k$ alors $\sigma(i_k) = \sigma(i_{j-1})$ mais σ étant bijective cela entrainerait $i_k = i_{j-1}$ et comme les éléments de $\{i_1, \ldots, i_k\}$ sont distincts deux à deux, cela entrainerait $k = j - 1 < k$ ce qui serait absurde. On a donc bien $\sigma(i_k) = i_1$.
Notons alors $\sigma_1 = (i_1 \ \cdots \ i_k)$ et définissons $\sigma' = \sigma_1^{-1} \circ \sigma$.
Notons $S = \mathrm{Supp}(\sigma)$, $S' = \mathrm{Supp}(\sigma')$ et $S_1 = \mathrm{Supp}(\sigma_1) = \{\mathrm{i}_1, \ldots, \mathrm{i}_\mathrm{k}\}$. Pour $i \in S \smallsetminus S_1$, $\sigma(i) \notin S_1$ (par injectivité de σ) d'où $\sigma'(i) = \sigma_1^{-1}(\sigma(i)) = \sigma(i) \neq i$. D'autre part, pour $i \in S_1$, $\sigma'(i) = i$. Enfin, pour $i \notin S$, $\sigma'(i) = i$. Par conséquent $S' = S \smallsetminus S_1$. En particulier, le support de σ' est strictement inclus dans celui de σ. En appliquant l'hypothèse de récurrence à σ' on l'écrit sous la forme $\sigma' = \sigma_2 \circ \cdots \circ \sigma_p$ avec des cycles à supports disjoints. On a alors $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_p$. De plus, le support de σ_1 est disjoint de ceux des autres σ_i qui sont inclus dans S'.
Montrons l'unicité d'une telle décomposition.
Supposons qu'on ait $\sigma = \sigma_1 \circ \cdots \circ \sigma_p = \sigma'_1 \circ \cdots \circ \sigma'_q$ (avec des cycles à supports disjoints).
Soit $i \in \mathrm{Supp}(\sigma_1)$ et quitte à renuméroter on peut supposer que $i \in \mathrm{Supp}(\sigma'_1)$. Pour $k > 1$, $\sigma_k(i) = \sigma'_k(i) = i$ donc pour tout $j \in \mathbb{N}$, $\sigma^j(i) = \sigma_1^j(i) = (\sigma'_1)^j(i)$ d'où $\sigma_1 = \sigma'_1$. En composant par σ_1^{-1}, on obtient $\sigma_2 \circ \cdots \circ \sigma_p = \sigma'_2 \circ \cdots \circ \sigma'_q$ et on recommence avec $i \in \mathrm{supp}(\sigma_2)$. □

Démonstration de la prop. 1.22. Soit $\sigma = (i_1 \ i_2)$ avec $i_1 < i_2$. On forme le produit des $\frac{\sigma(j)-\sigma(i)}{j-i}$ avec $j > i$.
Si $i \neq i_1$ et $j \neq i_2$ alors ça donne $\frac{\sigma(j)-\sigma(i)}{j-i} = \frac{j-i}{j-i} = 1$.
Il reste les paires du type $\{i_1, j\}$ avec $j \neq i_2$, celles du type $\{j, i_2\}$ avec $j \neq i_1$ et enfin la paire $\{i_1, i_2\}$.

- Pour celles du type $\{i_1, j\}$ (avec $j > i_1$ et $j \neq i_2$), on a $\frac{\sigma(j)-\sigma(i_1)}{j-i_1} = \frac{j-i_2}{j-i_1}$. Parmi elles, celles qui donnent un signe $-$ sont telles que $i_1 < j < i_2$.
- Pour celles du type $\{j, i_2\}$ (avec $j < i_2$ et $j \neq i_1$), on a $\frac{\sigma(i_2)-\sigma(j)}{i_2-j} = \frac{i_1-j}{i_2-j}$. Parmi elles, celles qui donnent un signe $-$ sont telles que $i_1 < j < i_2$.
- La dernière paire $\{i_1, i_2\}$ donne un signe $-$.

Si on fait le bilan du nombre de signes $-$, on en a un nombre impair ce qui donne $\varepsilon(\sigma) = -1$. □