DÉCOMPOSITION EN CYCLES

On présente ici la démonstration du théorème de décomposition d'une permutation en cycles à supports disjoints.

Dans tout ce qui suit, n désigne un entier naturel non nul.

Théorème 1

Toute permutation de $[\![1;n]\!]$ est décomposable en un produit de cycles à supports deux à deux disjoints (Id se décompose en un produit vide de cycles). Cette décomposition est unique, à l'ordre près des cycles (les cycles commutent deux à deux puisqu'ils sont à supports disjoints).

■ ▶ Existence :

Pour $n \in \mathbb{N}^*$, on note $\mathscr{P}(n)$: « tout élément de $\mathfrak{S}_n$ se décompose en un produit de cycles à supports deux à deux disjoints ».

Initialisation :
Si $n = 1$, l'ensemble des cycles de $\mathfrak{S}_1$ est vide et l'on a bien $\mathfrak{S}_1 = \{\mathrm{Id}\} = \langle\varnothing\rangle$.
Si $n = 2$, $\mathfrak{S}_2$ contient un seul cycle $c = (1,2)$ qui l'engendre car $\mathfrak{S}_2 = \{\mathrm{Id}, c\}$ et $c^2 = \mathrm{Id}$.

Hérédité :
Fixons $n \geqslant 2$ tel que $\mathscr{P}(n)$ est vraie et prouvons $\mathscr{P}(n+1)$. Soit $\sigma \in \mathfrak{S}_{n+1}$. Distinguons deux cas :

* Premier cas : $\sigma(n+1) = n+1$

  La restriction σ'de σ à $[\![1;n]\!]$ est un élément de $\mathfrak{S}_n$. D'après l'hypothèse de récurence, σ' est donc un produit de k cycles à supports disjoints de $[\![1;n]\!]$: $\sigma' = c'_k \dots c'_2 c'_1$. Chaque cycle c'_j (où $1 \leqslant j \leqslant k$) se prolonge en un cycle c_j de $[\![1;n+1]\!]$ en fixant $n+1$. On a alors $\sigma = c_k \dots c_2 c_1$ et les cycles c_j sont toujours à supports disjoints (ils ont les mêmes supports que les c'_j).

* Second cas : $\sigma(n+1) = p \neq n+1$

  On va utiliser le principe des tiroirs ! Pour cela, introduisons les $n+2$ premiers éléments de l'orbite de $n+1$ sous l'action de σ, c'est-à-dire les entiers $n+1$, $\sigma(n+1)$, …, $\sigma^{n+1}(n+1)$. Ce sont $n+2$ nombres de l'intervalle d'entiers $[\![1;n+1]\!]$ qui ne contient que $n+1$ éléments. Dès lors, le principe des tiroirs nous dit qu'il existe $0 \leqslant k < \ell \leqslant n+1$ tels que $\sigma^\ell(n+1) = \sigma^k(n+1)$.
  En notant $m = \ell - k$, on a $m \in [\![1;n+1]\!]$ et $\sigma^m(n+1) = n+1$.
  Ainsi, l'ensemble $\{q \in [\![1;n+1]\!] : \sigma^q(n+1) = n+1\}$ est une partie non vide de $\mathbb{N}^*$. Elle admet à ce titre un plus petit élément, noté p.
  On a $\sigma^p(n+1) = n+1$.
  D'autre part, les p entiers $n+1$, $\sigma(n+1)$, …, $\sigma^{p-1}(n+1)$ sont deux à deux distincts car, s'il existait deux entiers k et ℓ tels que $0 \leqslant k < \ell \leqslant p-1$ et $\sigma^\ell(n+1) = \sigma^k(n+1)$, alors on aurait $\sigma^{\ell-k}(n+1) = n+1$ avec $1 \leqslant \ell - k < p$, ce qui contredirait la minimalité de p.
  Notons c le p-cycle $c = \big(n+1, \sigma(n+1), \dots, \sigma^{p-1}(n+1)\big)$ et considérons $\rho = c^{-1}\sigma$ de sorte que $\rho(n+1) = c^{-1}\big(\sigma(n+1)\big) = n+1$.
  D'après le premier cas, ρ est donc un produit de k cycles de $[\![1;n+1]\!]$ à supports deux à deux disjoints : $\rho = c_k \dots c_2 c_1$. Alors $\sigma = c\rho = c_k \dots c_2 c_1$ est un produit de $k+1$ cycles de $[\![1;n+1]\!]$. Or les entiers $n+1$, $\sigma(n+1)$, …, $\sigma^{p-1}(n+1)$ sont fixes sous l'action de ρ donc les supports des cycles c_i (où $1 \leqslant i \leqslant k$) ne contiennent aucun des éléments $n+1$, $\sigma(n+1)$, …, $\sigma^{p-1}(n+1)$, ce qui signifie que $c, c_1, \dots, c_k$ sont des cycles de $[\![1;n+1]\!]$ à supports deux à deux disjoints.

Cela démontre que $\mathscr{P}(n+1)$ est vraie.

Conclusion :
D'après le principe de récurrence, $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}^*$, ce qui démontre l'existence de la décomposition.

▶ Unicité :

Soit $\sigma \in \mathfrak{S}_n$ tel que $\sigma \neq \mathrm{Id}$ (ce cas est évident). On considère $\sigma = c_k \dots c_2 c_1 = d_\ell \dots d_2 d_1$ deux décompositions de σ en produit de cycles à supports deux à deux disjoints.

Soit $i \in [\![1; n]\!]$ tel que $\sigma(i) \neq i$ (cet entier i existe puisque $\sigma \neq \mathrm{Id}$). Dès lors, i est dans le support de l'un des c_j, disons c_r, et dans le support de l'un des d_j, disons d_s.

En reprenant une partie du raisonnement développé pour démontrer l'existence de la décomposition, on peut affirmer qu'il existe $p \in \mathbb{N}^*$ tel que $i, \sigma(i), \dots, \sigma^{p-1}(i)$ sont deux à deux distincts et $\sigma^p(i) = i$.

On a alors $c_r = \big(i, \sigma(i), \dots, \sigma^{p-1}(i)\big)$ et $d_s = \big(i, \sigma(i), \dots, \sigma^{p-1}(i)\big)$, donc $c_r = d_s$.

En réitérant ce processus, on en déduit que $n = m$ et $\{c_1, \dots, c_k\} = \{d_1, \dots, d_\ell\}$. Cela justifie l'unicité de la décomposition, à l'ordre près des cycles. ■