

Th 2: Toute permutation de $\{1, \dots, n\}$ est décomposable en **produit de cycles à supports disjoints**, et cette décomposition est unique à l'ordre des cycles près.

I. Développement

A. Existence.

On raisonne par récurrence sur n par paquets que :

$\forall n \geq 2$, pour toute permutation σ de $\{1, \dots, n\}$, il existe un produit de cycles à supports disjoints égaux à σ .

- Si $n = 2$, σ est au bon l'identité, dont on a convenu que c'est un produit vide de cycles, soit la transposition $(1, 2)$, qui est un 2-cycle. Donc la propriété est vérifiée pour $n = 2$.

- Soit $n \geq 2$, et supposons que la propriété est vérifiée pour n . (HR) Pour $n+1$, il vient :

▷ 1° cas : $\sigma(n+1) = n+1$

Alors comme σ est bijective, $\{1, \dots, n\}$ est stable par σ .

$\sigma' = \sigma|_{\{1, \dots, n\}}$ est donc une permutation de $\{1, \dots, n\}$,

et d'après HR il existe $r \in \mathbb{N}^*$ et des cycles $\alpha_1, \dots, \alpha_r$ à supports disjoints deux à deux tels que $\sigma' = \alpha_1 \circ \dots \circ \alpha_r$.

Notant, pour tout $i \in \{1, \dots, r\}$, $c_i : \{1, \dots, n+1\} \rightarrow \{1, \dots, n+1\}$.

$$k \longmapsto \begin{cases} c_i(k) & \text{si } k \in \{1, \dots, n\} \\ n+1 & \text{si } k = n+1 \end{cases}$$

Il vient que $\sigma = c_1 \circ \dots \circ c_r$, où les c_i , $i \in \{1, \dots, r\}$ sont des cycles à supports deux à deux disjoints de $\{1, \dots, n+1\}$, donc la propriété est vraie pour $n+1$.

▷ 2° cas : $\sigma(n+1) \neq n+1$.

Alors les entiers $\sigma(n+1), \sigma^2(n+1), \dots, \sigma^{m-1}(n+1)$ sont au nombre de $m \geq 2$, et sont des éléments de $\{1, \dots, n+1\}$.

Donc il existe k, l distincts dans $\{0, \dots, m-1\}$, par exemple $k < l$, tels que $\sigma^k(n+1) = \sigma^l(n+1)$.

Soient de tels k, l . On note $m = l - k$ et on a : $m \in \{1, \dots, m-1\}$

et $\sigma^m(n+1) = \sigma^{l-k}(n+1)$, or $\sigma^l(n+1) = \sigma^k(n+1)$,

donc $\sigma^{l-k}(n+1) = n+1$, et $\sigma^m(n+1) = n+1$.

Donc l'ensemble $\{q \in \{1, \dots, mn\} \mid \sigma^q(mn) = mn\}$ est une partie non vide de $\mathbb{N}^*$, et admet par conséquent un plus petit élément.

Soit p ce plus petit élément. On a $\sigma^p(mn) = mn$.

D'autre part, les p entiers $mn, \sigma(mn), \dots, \sigma^{p-1}(mn)$ sont deux à deux distincts. (peux le démontrer).

En effet, s'il existait $k, l \in \{0, \dots, p-1\}$ tq $k < l$ et $\sigma^k(mn) = \sigma^l(mn)$, alors en posant $q = l - k$, on aurait $q \in \{1, \dots, mn\}$ et $\sigma^q(mn) = mn$, avec $q < p$, contredit la définition de p comme plus petit élément.

On note donc c le p -cycle $c = (mn, \sigma(mn), \dots, \sigma^{p-1}(mn))$, et on note $p = c^{-1} \circ \sigma$, de sorte que $p(mn) = c^{-1}(\sigma(mn)) = mn$.

p vérifiant $p(mn) = mn$, on peut utiliser l'étude faite par le 1° cas, d'où l'on déduit qu'il existe $v \in \mathbb{N}$ et des cycles $c_1, \dots, c_v$ de $\{1, \dots, mn\}$ à supports disjoints tels que $p = c_1 \circ \dots \circ c_v$.

Comme $p(mn) = mn$; $p(\sigma(mn)) = \sigma(mn)$; $\dots$; $p(\sigma^{p-1}(mn)) = \sigma^{p-1}(mn)$, les supports des cycles $c_1, \dots, c_v$ ne contiennent aucun des éléments $mn, \sigma(mn), \dots, \sigma^{p-1}(mn)$.

Finalement: $\sigma = c \circ c_1 \circ \dots \circ c_v$, où $c, c_1, \dots, c_v$ sont des cycles de $\{1, \dots, mn\}$ à supports disjoints, et la propriété est vérifiée pour $n+1$.

B. Unicité.

Par l'absurde. Soient $\sigma = c_1 \circ \dots \circ c_v = d_1 \circ \dots \circ d_u$ deux décompositions de σ en cycles à supports disjoints.

Comme les c_i , $i \in \{1, \dots, v\}$ sont à supports disjoints, ils commutent entre eux deux à deux. De même pour les d_j , $j \in \{1, \dots, u\}$. Comme l'identité est un produit vide de cycles, l'unicité est acquise. Supposons $\sigma \neq \text{Id}$.

$\exists i \in \{1, \dots, m\}$ tq $\sigma(i) \neq i$, et $\exists a \in \{1, \dots, v\}$, $\exists a' \in \{1, \dots, u\}$ tels que i appartienne au support de c_a et à celui de $d_{a'}$.

En reprenant le raisonnement du 2° cas de l'existence,
 $\exists p \in \mathbb{N}^* \text{ tq : } (i, \sigma(i), \dots, \sigma^{p-1}(i)) \text{ sont deux à deux distincts}$
 $\left\{ \begin{array}{l} \sigma^p(i) = i. \end{array} \right.$

On a alors $\alpha = d_{\alpha'} = (i, \sigma(i), \dots, \sigma^{p-1}(i))$

En répétant le raisonnement pour tous les $i \in \{1, \dots, n\}$ tels que $\sigma(i) \neq i$, on obtient que $n = n'$ et $\{\alpha, \dots, \alpha_n\} = \{\alpha', \dots, \alpha_{n'}\}$.