

DÉCOMPOSITION D'UNE PERMUTATION EN CYCLES

Toute permutation $\sigma \in S_n \setminus Id$ s'écrit de façon unique (à l'ordre près des facteurs) $\sigma = c_1 c_2 \dots c_p$ où les c_i sont des cycles à supports disjoints (deux à deux).

Démonstration :

L'idée générale est que l'ensemble des σ -orbites est une partition de S_n et que chaque σ -orbite (non triviale) définit un cycle.

Formalisons :

Soit $\sigma \in S_n \setminus Id$.

Existence :

Notons A_1, A_2, \dots, A_r les σ -orbites. On a donc :

$$\llbracket 1, n \rrbracket = A_1 \cup A_2 \cup \dots \cup A_r \text{ (union disjointe)}$$

Pour tout $i \in \llbracket 1, r \rrbracket$, définissons c_i par :

$$c_i(x) = \begin{cases} \sigma(x) & \text{si } x \in A_i \\ x & \text{si } x \notin A_i \end{cases}$$

Alors c_i est soit l'identité, soit un cycle car :

$$x \notin A_i \Rightarrow \text{Orb}_{\langle c_i \rangle}(x) = \{x\} \text{ (car } x \text{ est fixe par } c_i)$$

$$x \in A_i \Rightarrow \text{Orb}_{\langle c_i \rangle}(x) = \{c_i^k(x), k \in \mathbb{Z}\} = \{\sigma^k(x), k \in \mathbb{Z}\} = \text{Orb}_{\langle \sigma \rangle}(x) = A_i$$

(Car, si $x \in A_i$ alors $\sigma(x) \in A_i$, donc $c_i^2(x) = c_i(\sigma(x)) = \sigma^2(x)$, donc par récurrence facile : $c_i^k(x) = \sigma^k(x)$)

Donc il y a au plus une c_i -orbite non réduite à un élément, ce qui prouve bien que c_i est l'identité ou un cycle.

Enfin, posons :

$$s = c_1 c_2 \dots c_r$$

Montrons que $s = \sigma$. Soit $x \in \llbracket 1, n \rrbracket$. Notons i l'unique indice tel que $x \in A_i$.

On a alors :

$$\forall j \neq i, c_j(x) = x \text{ et } c_i(x) = \sigma(x)$$

En outre :

$$\forall j \neq i, c_j(\sigma(x)) = \sigma(x) \text{ car } \sigma(x) \in A_i$$

D'où

$$s(x) = \sigma(x)$$

C'est-à-dire :

$$s = \sigma$$

Enfin, on retire du produit les éventuels c_i qui sont l'identité pour obtenir après réindexation :

$$\sigma = c_1 \dots c_p$$

Unicité :

Supposons que d_1, \dots, d_q sont des cycles à supports disjoints tels que :

$$\sigma = d_1 \dots d_q$$

Soit $j \in \llbracket 1, q \rrbracket$. Soit x un élément du support B_j de d_j .

Comme les supports de d_1, \dots, d_q sont disjoints deux à deux, seul d_j a un effet sur x :

$$\sigma(x) = d_j(x)$$

Donc, par récurrence :

$$\forall k \in \mathbb{Z}, \sigma^k(x) = d_j^k(x)$$

C'est-à-dire :

$$\text{Orb}_{\langle \sigma \rangle}(x) = \text{Orb}_{\langle d_j \rangle}(x) = B_j$$

Donc B_1, \dots, B_q sont les σ -orbites, donc $q = p$ et pour tout $i \in \llbracket 1, p \rrbracket$ on a, via une réindexation :

$$B_i = A_i$$

Donc :

$$d_i = c_i$$

Ce qui prouve l'unicité.

Exemple :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (1, 2)(3, 4, 5)$$