

Développement : Décomposition d'une permutation en produit de cycles

Référence : Mathématiques pour l'agrégation, Algèbre et géométrie, Romabaldi, pages 42-43

Leçon : 101, 104, 105 et 108.

Théorème :

Toutes permutation $\sigma \in S(E) \setminus \{Id_E\}$ se décompose en produit de cycles deux à deux disjoints.
Cette décomposition est unique à l'ordre près.

Démonstration. **Existence :**

Soit $\sigma \in S(E) \setminus \{Id_E\}$.

Soit $O_1, \dots, O_p, \dots, O_r$ les σ -orbites deux à deux distinctes avec $r_k = \text{card}(O_k) \geq 2$ pour $k = 1, \dots, p$ et $\text{card}(O_k) = 1$ pour $k = p+1, \dots, r$ (s'il en existe).

On a alors la partition

$$E = \bigsqcup_{k=1}^r O_k$$

Pour tout k compris entre 1 et r , on désigne par u_k la permutation de E définie par

$$\forall x \in E, u_k(x) = \begin{cases} \sigma(x) & \text{si } x \in O_k \\ x & \text{si } x \notin O_k \end{cases}$$

Remarque : u_k est bien une permutation de E car la restriction de σ à une orbite O_k est une permutation de O_k .

On a deux cas :

1. Si O_k est réduit à un point, alors $u_k = Id_E$.
2. Sinon O_k est non réduit à un point et dans ce cas u_k est un r_k -cycle. En effet, pour $x \notin O_k$, on a $u_k(x) = x$ et donc $Orb_{u_k}(x) = \{x\}$ et pour $x \in O_k$, on a

$$\begin{aligned} Orb_{u_k}(x) &= \{u_k^j(x) \mid j \in \mathbb{Z}\} \\ &= \{\sigma^j(x) \mid j \in \mathbb{Z}\} \\ &= Orb_{\sigma}(x) \\ &= O_k \end{aligned}$$

Donc u_k a bien une seule orbite non réduite à un point donc u_k est un r_k -cycle.

Montrons que

$$\sigma = \prod_{j=1}^r u_j = \prod_{j=1}^p u_j$$

Soit $x \in E$, il existe un unique indice k compris entre 1 et r tel que $x \in O_k$ et on a $u_k(x) = \sigma(x)$, $u_j(x) = x$ pour tout $j \neq k$ (car $x \notin O_j$).

De plus, les u_k commutent car leurs supports sont deux à deux disjoints (par définition), on en déduit que :

$$\begin{aligned} \left(\prod_{j=1}^r u_j \right) (x) &= \left(u_k \prod_{j=1, j \neq k}^r u_j \right) (x) \\ &= u_k(x) \\ &= \sigma(x) \end{aligned}$$

Unicité :

Soit

$$\sigma = \prod_{k=1}^{p'} u'_k$$

une autre décomposition en cycles deux à deux disjoint de σ .

Posons $O'_1, \dots, O'_{p'}$ les supports des cycles.

On a pour $k \in \{1, \dots, p'\}$ et $x \in O'_k$ que $\sigma(x) = u'_k(x)$, donc, $O'_k = Orb_{u'_k}(x) = Orb_{\sigma}(x)$

Par conséquent les orbites O'_k sont les orbites non réduits à un point de σ (car $u_k \neq Id_E$ par hypothèse se sont des cycles) et $p = p'$.

On a donc $O'_k = O_j$ pour un unique j compris entre 1 et p .

Pour $x \in O'_k$, on a $u'_k(x) = \sigma(x) = u_j(x)$ et pour $x \notin O'_k$, $u'_k(x) = x = u_j(x)$ ce qui donne $u'_k = u_j$ et l'unicité de la décomposition à l'ordre près. $\square$