DÉCOMPOSITION D'UNE PERMUTATION EN UN PRODUIT DE CYCLES À SUPPORTS DISJOINTS

Théorème 1. *Soit $\sigma \in \mathcal{S}_n$ ($n \geq 2$). Alors σ se décompose en*

$$\sigma = c_1 \circ c_2 \circ \cdots c_m,$$

où $c_1, \ldots, c_m$ sont des cycles à supports deux à deux disjoints. Si de plus on exclut les cycles (triviaux) de longueur 1 alors cette décomposition est unique à l'ordre près.

Proposition 2. *Les orbites des éléments de $\{1, \ldots, n\}$ forment une partition de $\{1, \ldots, n\}$. De plus, si $i \in \{1, \ldots, n\}$ alors en posant $l = \min\{k \in \mathbb{N}^* \,;\, \sigma^k(i) = i\}$ on a $X_i = \{\sigma^k(i) \,;\, 0 \leq k \leq l-1\}$ et si $0 \leq k < k' \leq l-1$ alors $\sigma^k(i) \neq \sigma^{k'}(i)$.*

Démonstration. Clairement comme pour tout i dans $\{1, \ldots, n\}$, $i \in X_i$, l'ensemble des orbites recouvrent l'ensemble $\{1, \ldots, n\}$. Pour montrer que deux orbites sont égales ou bien disjointes il suffit de montrer (par exemple) que si $j \in X_i$ alors $X_j = X_i$. Soient i et j ($i \neq j$) tel que $j \in X_i$ et soit $k \geq 1$ tel que $\sigma^k(i) = j$. Comme $j \in X_i$ il est clair par définition de l'orbite de l'élément i que $X_j \subset X_i$. Comme le groupe monogène engendré par σ est fini ($\mathcal{S}_n$ est lui-même fini), soit $p \in \mathbb{N}^*$ tel que $\sigma^p(i) = i$. En décomposant à l'aide de la division euclidienne $k = qp + r$ on obtient $j = \sigma^r(i)$ puis $\sigma^{p-r}(j) = i$ d'où $i \in X_j$ soit $X_i \subset X_j$. On a démontré que $X_i = X_j$.

Pour la deuxième propriété (qui se démontre indépendamment de la première) l est bien défini car le groupe monogène engendré par σ est cyclique. Par la division euclidienne de k par l on a $k = ql + r$ avec $0 \leq r < l-1$ d'où $\sigma^k(i) = \sigma^{ql+r}(i) = \sigma^r(\sigma^{ql}(i)) = \sigma^r(i)$ d'où $X_i = \{\sigma^k(i) \,;\, 0 \leq k \leq l-1\}$. Si k et k' sont tels $0 \leq k < k' \leq l-1$ et $\sigma^k(i) = \sigma^{k'}(i)$ le fait que σ soit une bijection entraîne que $\sigma^{k'-k}(i) = i$, or $0 < k' - k \leq l-1$, ce qui contredit la minimalité de l. □

Démonstration du théorème 1.

– Existence. D'après la proposition 2, soient $X_{i_1}, X_{i_2}, \ldots, X_{i_p}$ les p orbites formant une partition de $\{1, \ldots, n\}$.

Considérons l'orbite X_{i_k} et construisons le cycle associé à cette partition. Nous avons aussi $X_{i_k} = \{\sigma^q(i_k) \,;\, 0 \leq q \leq l_k - 1\}$ avec $l_k = \min\{r \in \mathbb{N}^* \,;\, \sigma^r(i_k) = i_k\}$. Posons alors

$$c_k(j) = \begin{cases} j & \text{si } j \notin X_{i_k} \\ \sigma(j) & \text{si } j \in X_{i_k} \end{cases}.$$

L'application c_k ainsi défini est bien un cycle $\mathcal{S}_n$ de longueur l_k et avec les notations du cours $c_k = (i_k, \sigma(i_k), \sigma^2(i_k), \ldots, \sigma^{l_k-1}(i_k))$.

Ainsi on a construit p cycles à supports disjoints ; $c_1, \ldots, c_n$. Montrons que $\sigma = c_1 \circ \cdots \circ c_p$. Si i est un élément de $\{1, \ldots, n\}$ celui-ci appartient nécessairement à une et une seule orbite X_{i_k}. Comme les supports des cycles $c_1, \ldots, c_p$ sont disjoints on a, par construction des c_j,

$$c_1 \circ \cdots \circ c_p(i) = c_k(i) = \sigma(i),$$

D'où le résultat.

– Unicité. On suppose que l'on a

$$\sigma = c_1 \circ c_2 \cdots \circ c_p = \gamma_1 \circ \gamma_2 \cdots \circ \gamma_q \tag{1}$$

où $c_1, \ldots, c_p$ sont des cycles à support disjoint de longueur ≥ 2 et de même concernant $\gamma_1, \ldots, \gamma_q$. La propriété sur la composition de permutations à supports disjoints nous donne

$$\operatorname{supp}(\sigma) = \bigcup_i^p \operatorname{supp}(c_i) = \bigcup_i^p \operatorname{supp}(\gamma_i). \tag{2}$$

Soit X_i une orbite non réduite à un singleton. Comme dans (2) nous avons une réunion d'ensembles disjoints, il y a un unique k tel que $i \in \operatorname{supp}(c_k)$ et un unique k' tel que $i \in \operatorname{supp}(\gamma_k)$. On peut toujours supposer, à une renumérotation près que $k = k' = 1$, c'est-à-dire que $i \in \operatorname{supp}(c_1)$ et $i \in \operatorname{supp}(\gamma_1)$. Ainsi $\sigma(i) = c_1(i) = \gamma_1(i)$ et pour tout $k \in \mathbb{N}$ on a $\sigma^k(i) = c_1^k(i) = \gamma_1^k(i)$. Donc γ_1 et c_1 ont pour support X_1 et sont égales (la restriction de c_1 et γ_1 sur $\{1, \ldots, n\} \setminus X_1$ sont l'identité).

De proche en proche on montre alors, à une renumérotation près, que nécessairement $p = q$ et $c_i = \gamma_i$ pour $1 \leq i \leq p$. □

Proposition 3. *La signature d'une transposition vaut -1.*

Démonstration. Soient $a < b$ et $t_{a,b}$ la transposition associée (qui s'écrit aussi comme le cycle $(a,\ b)$). Un couple (i, j) avec $i < j$ réalise une inversion (i.e. $t_{a,b}(i) > t_{a,b}(j)$) si et seulement si ($a \leq i < b$ et $j = b$) ou bien ($i = a$ et $a < j < b$). En regardant les couples qui réalisent une inversion il apparaît que (a, i) est une inversion si et seulement (i, b) en est une aussi, ce qui donne un nombre pair d'inversions du type (i, j) avec ($i = a$ et $j \neq b$) ou ($i \neq a$ et $j = b$). Il reste à ajouter l'inversion (a, b) et au total il y a un nombre impair d'inversions, soit encore $\varepsilon(t_{a,b}) = -1$. □