# ALGÈBRE. - Un résultat extrémal en théorie des permutations.

Alain Jacques, Claude Lenormand, André Lentin, Jean-François Perrot

ALGÈBRE. — *Un résultat extrémal en théorie des permutations.* Note (*) de MM. **Alain Jacques**, **Claude Lenormand**, **André Lentin** et **Jean-François Perrot**, présentée par M. Jean Leray.

On calcule un Max-min et un min-Max sur l'ensemble des décompositions d'une permutation donnée en un produit de deux permutations.

Soit $\sigma \in \mathfrak{S}_n$ une permutation de $n$ objets [1]; désignons par $z(\sigma)$ le nombre des cycles disjoints de $\sigma$, y compris les cycles de longueur 1. Le but de cette Note est d'établir le

Théorème 1 :

(i) $\mathrm{Max}\{\min\{z(\tau),\ z(\theta)\};\ \tau,\ \theta \in \mathfrak{S}_n,\ \ \sigma = \tau\theta\} = [(n + z(\sigma))/2]$, *où* $[a/b]$ *note la partie entière de* $a/b$;

(ii) $\min\{\mathrm{Max}\{z(\tau),\ z(\theta)\};\ \tau,\ \theta \in \mathfrak{S}_n;\ \sigma = \tau\theta\} = 1$ *ou* 2 *selon que* $\sigma$ *est paire ou impaire.*

L'énoncé (i) se rencontre naturellement dans la théorie des équations dans les monoïdes libres. (ii) se déduit du résultat suivant, qui précise le théorème 1 de Ore [2] :

Théorème 2. — *Toute permutation paire de n objets est le commutateur d'un cycle de longueur n et d'une involution.*

Les démonstrations font appel aux propriétés suivantes :

A. Définition. — Une décomposition $\sigma = \alpha\beta\,(\sigma,\ \alpha,\ \beta \in \mathfrak{S}_n)$ sera dite *normale* si elle satisfait les trois conditions :

(*a*) $\alpha$ et $\beta$ sont des involutions, i. e. $\alpha^2 = \beta^2 = 1$;

(*b*) $|z(\alpha) - z(\beta)| \leq 1$;

(*c*) si $k = z(\sigma)$ et $\gamma_1,\ \gamma_2,\ \ldots,\ \gamma_k$ sont les cycles de $\sigma$, alors $\alpha = \alpha_1\alpha_2\ldots\alpha_k$ et $\beta = \beta_1\beta_2\ldots\beta_k$ avec pour $r = 1,\ 2,\ \ldots,\ k$, $\gamma_r = \alpha_r\beta_r$ décomposition normale de $\gamma_r$. En particulier, $\sigma i = i$ entraîne $\alpha i = \beta i = i$.

Proposition 1. — *Tout cycle* $\gamma \in \mathfrak{S}_n$ *de longueur n admet exactement n décompositions normales* $\gamma = \alpha\beta$. *Si n est impair,* $\alpha$ *et* $\beta$ *ont toujours chacune un seul point fixe. Si n est pair, dans la moitié des cas* $\alpha$ *a deux points fixes et* $\beta$ *n'en a aucun, dans les autres cas c'est l'inverse qui se produit.*

En effet, si $\gamma = \alpha\beta$ est une décomposition normale, on déduit de (*a*) que $\alpha$ et $\beta$ vérifient $\alpha\gamma\alpha^{-1} = \gamma^{-1}$ et $\beta = \alpha\gamma$. Par suite, si $\gamma = \alpha'\beta'$ est une autre décomposition normale de $\gamma$, on a $\alpha' = \alpha\xi$ et $\beta' = \beta\xi$ où $\xi$ commute avec $\gamma$, donc $\xi = \gamma^k$ : il n'y a donc pas plus de $n$ décompositions normales différentes de $\gamma$. Considérons alors $\gamma = (1,\ 2,\ \ldots,\ n)$ et, pour $n = 2p + 1$,

$$(1)\quad \alpha = (2,\ 2p+1)\,(3,\ 2p)\ldots(p+1,\ p+2),\qquad \beta = (1,\ 2p+1)\,(2,\ 2p)\ldots(p,\ p+2),$$

où $\alpha 1 = 1$ et $\beta(p+1) = p+1$; et pour $n = 2p$,

$$(2)\quad \alpha = (1,\ 2p)\,(2,\ 2p-1)\ldots(p,\ p+1),\qquad \beta = (1,\ 2p-1)\,(2,\ 2p-2)\ldots(p-1,\ p+1)$$

et

$$(2') \quad \begin{cases} \alpha = (1, 2p-1)(2, 2p-2)\ldots(p-1, p+1), \\ \beta = (2p-1, 2p)(1, 2p-2)(2, 2p-3)\ldots(p-1, p), \end{cases}$$

avec dans (2), $\beta(2p) = 2p$, $\beta p = p$ et dans (2′), $\alpha(2p) = 2p$, $\alpha p = p$. En remarquant que si $\gamma = \alpha\beta$ est une décomposition normale, $\gamma = \gamma^k\alpha\gamma^{-k}\gamma^k\beta\gamma^{-k}$ en est encore une, on voit que, pour $n = 2p+1$, (1) donne naissance à $n$ décompositions normales distinctes de $\gamma$ et que, pour $n = 2p$, (2) et (2′) en donnent $p$ chacune, ce qui achève de prouver la proposition.

Proposition 2. — *Toute permutation $\sigma \in \mathfrak{S}_n$ admet au moins une décomposition normale, et toute décomposition normale $\sigma = \alpha\beta$ de $\sigma$ vérifie*

$$z(\alpha) + z(\beta) = n + z(\sigma).$$

Remarquons d'abord qu'en vertu de (c) il suffit de vérifier la proposition pour les cycles et les produits de deux cycles disjoints de longueur paire : en effet, si $\sigma$ est paire, on a nécessairement $z(\alpha) = z(\beta)$ d'après (b), et toute permutation impaire $\sigma$ s'écrit $\sigma = \sigma'\gamma$ où $\sigma'$ est paire et $\gamma$ est un cycle de longueur paire.

Pour les cycles, le résultat découle de la proposition 1 et de (c). Pour $\sigma = \gamma'\gamma''$ il suffit d'écrire $\gamma' = \alpha'\beta'$, décomposition normale du type (2) et $\gamma'' = \alpha''\beta''$ du type (2′), de constater que la décomposition $\sigma = \alpha\beta$ où $\alpha = \alpha'\alpha''$ et $\beta = \beta'\beta''$ possède les propriétés requises et de s'assurer que, d'après (c), toute décomposition normale de $\sigma$ est obtenue par ce procédé.

B. Notation. — Soit $i$ un des $n$ objets sur lesquels opère $\mathfrak{S}_n$; définissons pour $\sigma \in \mathfrak{S}_n$, $r_i\sigma = (i, \sigma i)\sigma = \sigma(i, \sigma^{-1} i)$ : on peut considérer $r_i$ comme un opérateur projetant $\mathfrak{S}_n$ sur son sous-groupe de degré $n-1$ laissant fixe $i$, et l'on vérifie immédiatement la

Proposition 3 :

— *Pour tout $\sigma \in \mathfrak{S}_n$, $n \geq 2$, $r_i(\sigma^{-1}) = (r_i\sigma)^{-1}$;*

— *Soit $\sigma = \tau\theta$ : on a $r_i\sigma = r_i\tau\, r_i\theta$ si et seulement si $i$ est point fixe de l'une au moins des trois permutations $\sigma$, $\tau$, $\theta$.*

Dans la suite, pour $i$ donné (resp. pour $i$ et $j$ donnés, $i \neq j$) $f_i$ (resp. $f_{ij}$) notera un isomorphisme du sous-groupe de $\mathfrak{S}_n$ laissant $i$ fixe (resp. $i$ et $j$ fixes) sur $\mathfrak{S}_{n-1}$ (resp. $\mathfrak{S}_{n-2}$); il est clair que $z(f_i r_i \sigma) = z(\sigma) - 1$ ou $z(\sigma)$ selon que $i$ est point fixe de $\sigma$ ou non.

*Démonstration du théorème* 1. — Désignons par $M(\sigma)$ le premier membre de (i) : d'après la proposition 2 et en vertu de (b), on a $M(\sigma) \geq [(n + z(\sigma))/2]$. On vérifie directement que pour $n = 1$ et $n = 2$ on a l'égalité.

Supposons que ce ne soit pas toujours vrai et soit N l'entier minimal pour lequel il existe trois permutations de N objets, $\sigma$, $\tau$, $\theta$ avec $\sigma = \tau\theta$ et $z(\tau)$, $z(\theta) > [(N + z(\sigma))/2]$. De $z(\sigma) \geq 1$ on déduit que $\tau$ et $\theta$ ont chacune au moins un point fixe; si elles ont un point fixe commun, soit $i$, c'est aussi un point fixe de $\sigma$ et l'on a $z(f_i\xi) = z(\xi) - 1$ pour $\xi = \sigma$, $\tau$, $\theta$, d'où, dans $\mathfrak{S}_{N-1}$, $f_i\sigma = f_i\tau f_i\theta$ avec $z(f_i\tau)$, $z(f_i\theta) > [(N - 1 + z(f_i\sigma))/2]$, ce qui contredit la minimalité de N; sinon, soient $\tau i = i$, $\theta j = j$, $i \neq j$, $i$ et $j$ ne sont pas points fixes de $\sigma$ : posons $\bar{\xi} = f_{ij} r_i r_j \xi$ pour $\xi = \sigma$, $\tau$, $\theta$, en vertu de la proposition 3, on a $\bar{\sigma} = \bar{\tau}.\bar{\theta}$ et $z(\bar{\sigma}) \leqq z(\sigma)$, $z(\bar{\tau}) = z(\tau) - 1$, $z(\bar{\theta}) = z(\theta) - 1$, donc une décomposition dans $\mathfrak{S}_{N-2}$ telle que $z(\bar{\tau})$, $z(\bar{\theta}) > [(N - 2 + z(\bar{\sigma}))/2]$, ce qui contredit encore la minimalité de N et achève de prouver l'égalité (i).

*Démonstration du théorème* 2. — Soit $\sigma \in \mathfrak{A}_n$ une permutation paire et $\sigma = \alpha\beta$ une décomposition normale de $\sigma$. Un raisonnement par récurrence sur $n$ montre qu'il existe un cycle $\gamma$ de longueur $n$ tel que $\gamma^{-1}\alpha\gamma = \beta$.

Le résultat est trivial pour $n = 1$ et $n = 2$. Soit donc $n > 2$. D'après la proposition 2, $\alpha$ et $\beta$ ont chacune $z(\sigma)$ points fixes, donc si $\sigma \neq 1$ (le cas $\sigma = 1$ est trivial) elles ont chacune au moins un point fixe qui n'est pas point fixe de $\sigma$, soient $i$ et $j$, $i = \alpha i$, $j = \beta j$ et $\sigma i \neq i$, $\sigma j \neq j$, donc $i \neq j$, $\alpha j \neq j$ et $\beta i \neq i$. Posons $\bar{\xi} = f_{ij} r_i r_j \xi$ pour $\xi = \sigma$, $\alpha$, $\beta$ : on a $\bar{\sigma} \in \mathfrak{A}_{n-2}$ et en vertu de la proposition 3, $\bar{\sigma} = \bar{\alpha}.\bar{\beta}$ est une décomposition normale, comme on le vérifie facilement. D'après l'hypothèse de récurrence, il existe dans $\mathfrak{S}_{n-2}$ $\bar{\gamma}$ cycle de longueur $n - 2$ tel que $\bar{\gamma}^{-1}\bar{\alpha}.\bar{\gamma} = \bar{\beta}$. On vérifie alors que $\gamma = (i, \alpha j) f_{ij}^{-1} \bar{\gamma}(j, \beta i)$ est un cycle de longueur $n$ et que $\beta = \gamma^{-1}\alpha\gamma$.

(ii) se déduisant immédiatement de ce résultat, le théorème 1 est complètement démontré.

(*) Séance du 5 février 1968.

(1) *Notations :* 1 désignera la permutation identique; la composition de la permutation $\theta$ par la permutation $\tau$ sera notée $\tau\theta$; les minuscules grecques désigneront, en général, des permutations.

(2) O. Ore, *Proc. Amer. Math. Soc.*, 2, 1951, p. 307-314. *Voir* aussi N. Itô, *Math. Japon*, 2, 1951, p. 59-60.

(*Institut de Programmation, Impasse d'Aubervilliers, Paris*, 19e.)