Une application du déterminant de Smith

Léo Daures

Leçons 105, 152

1 Le théorème de Brauer

L'ensemble $\mathfrak{S}_n$ des permutations de $\{1,\dots,n\}$ s'injecte naturellement dans $\mathcal{M}_n(K)$ via $\sigma \mapsto (\delta_{j,\sigma(i)})_{1\leqslant i,j\leqslant n}$ (où K est un corps que l'on supposera ici de caractéristique nulle). On va montrer dans ce développement le propriété suivante :

Théorème 1. *Soit $n \in \mathbb{N}$. Deux matrices de permutation de taille n sont semblables si et seulement si les permutations associées sont conjuguées dans $\mathfrak{S}_n$.*

La réciproque étant facile (si $\sigma = \alpha\tau\alpha^{-1}$, il suffit de prendre la matrice de permutation associée à α comme matrice de changement de base), on ne montrera que le sens direct. C'est celui qui est intéressant, car rien ne dit *a priori* que le changement de base par lequel une matrice de permutation peut être semblable à une autre puisse être associé à une troisième permutation.

2 Preuve

Pour $\sigma \in \mathfrak{S}_n$, on note $\mathcal{C}(\sigma)$ l'ensemble des cycles apparaissant dans la décomposition de σ en cycles, et $\mathcal{C}_l(\sigma)$ la partie de cet ensemble constituée des cycles de longueur l. On notera aussi $c_l(\sigma) = |\mathcal{C}_l(\sigma)|$. Rappelons que connaître la "structure" d'une permutation σ signifie connaître les $c_l(\sigma)$ pour tout $l \in \{1,\dots n\}$.

Avant de commencer, rappelons un lemme préliminaire sur les permutations utilisé de manière centrale dans la suite :

Lemme 1. *Soit $\sigma, \sigma' \in \mathfrak{S}_n$. σ et σ' sont conjugués si et seulement si ils ont la même structure, c'est à dire si et seulement si $\forall 1 \leqslant l \leqslant n, c_l(\sigma) = c_l(\sigma')$.*

Preuve. En effet, il suffit d'observer que $\forall \alpha \in \mathfrak{S}_n$, $\alpha \circ (x_1\ x_2 \dots x_k) \circ \alpha^{-1} = (\alpha(x_1)\ \alpha(x_2) \dots \alpha(x_k))$. Donc, le conjugué d'un $k-$cycle est un $k-$cycle. Par conséquent si la décomposition de σ en cycles à supports disjoints s'écrit $\sigma = c_1 c_2 \dots c_p$ avec $c_i = (x_{i,1}\ x_{i,2}\ \dots x_{i,l_i})$, alors $\alpha\sigma\alpha^{-1} = \alpha c_1 \alpha^{-1} \alpha c_2 \alpha^{-1} \dots \alpha c_p \alpha^{-1}$ où $\alpha c_i \alpha^{-1} = (\alpha(x_{i,1})\ \alpha(x_{i,2}) \cdots \alpha(x_{i,l_i}))$. Ceci montre que σ et $\alpha\sigma\alpha^{-1}$ ont les mêmes structures

Réciproquement, si σ et σ' ont les mêmes structures, on note la décomposition de σ' en cycles à supports disjoints $\sigma' = c'_1 c'_2 \dots c'_p$ où chaque c'_i a la même longueur que c_i (hypothèse sur les structures), et on peut écrire chaque c'_i sous la forme $c'_i = (y_{i,1}\ y_{i,2}\ \dots y_{i,l_i})$. On pose pour tout $i \leqslant p$ et pour tout $k \leqslant l_i$, $\alpha(x_{i,k}) = y_{i,k}$). Cette définition est correcte car tous les $x_{i,k}$ sont distincts, et de plus α est une bijection car les $y_{i,k}$ le sont aussi. On donc bien une permutation α telle que $\alpha\sigma\alpha^{-1} = \sigma'$. □

On considère M_σ et $M_{\sigma'}$ deux matrices de permutations (associées respectivement aux permutations σ et σ'), et on suppose qu'elles sont semblables. on veut montrer qu'alors, σ et σ' sont conjuguées dans $\mathfrak{S}_n$. Le premier réflexe est alors d'utiliser le lemme précédent : pour qu'elles soient bien conjuguées il suffit qu'elles aient la même structure. Nous nous attelons donc à montrer que σ et σ' ont le même nombre de cycles de chaque longueur.

On n'a que des informations sur les matrices M_σ et $M_{\sigma'}$, mais on peut réussir à en extraire des informations sur σ et σ'. Pour commencer on peut observer M_σ dans une base adaptée à sa décomposition en cycles :

$$PM_\sigma P^{-1} = \begin{pmatrix} M_1 & & (0) \\ & \ddots & \\ (0) & & M_p \end{pmatrix}$$

où les M_i sont des matrices carrées de taille l_i de la forme $M_i = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & (0) & \\ & \ddots & \ddots & \\ (0) & & 1 & 0 \end{pmatrix}$

Compter les blocs diagonaux de $PM_\sigma P^{-1}$ revient exactement à compter les cycles de σ (c'est bien pour cela qu'on a choisi cette base en particulier !). C'est une considération qui dépend encore de la base, c'est à dire de la matrice de changement de base P, mais on peut la ramener à une considération indépendante de la base avec le lemme suivant, vrai pour toute permutation :

Lemme 2. *Pour une permutation $\tau \in \mathfrak{S}_n$ associée à la matrice M_τ, on a $|\mathcal{C}(\tau)| = \dim\ker(M_\tau - I_n)$*

En effet, si P est une matrice de changement de base, on a $\dim\ker(M_\tau - I_n) = \dim\ker(P(M_\tau - I_n)P^{-1}) = \dim\ker(PM_\tau P^{-1} - I_n)$, donc quitte à considérer $PM_\tau P^{-1}$ on suppose que M_τ est une matrice diagonale par blocs dont les blocs sont comme précédemment. Par la remarque précédente, elle a exactement $|\mathcal{C}(\tau)|$ blocs. $M_\tau - I$ est encore digaonale par blocs et ses blocs sont de la forme

$$B_i = \begin{pmatrix} -1 & & & 1 \\ 1 & \ddots & (0) & \\ & \ddots & \ddots & \\ (0) & & 1 & -1 \end{pmatrix}$$

En le développant par rapport à la première ligne, le déterminant d'un tel bloc B_i vaut $-(-1)^d_i + (-1^d_i) = 0$ (où d_i est la taille du bloc i), donc le bloc n'est pas inversible. En revanche, sa sous-matrice extraite en lui retirant la première ligne et la première colonne est inversible (triangulaire supérieure avec des 1 sur la diagonale). On en déduit que le bloc B_i est de rang $d_i - 1$. C'est vrai pour tous les blocs ! Par conséquent la matrice M_τ est de rang la somme des rangs de ses blocs, c'est-à-dire $\mathrm{rg}(M_\tau) = (d_1 - 1) + \ldots + (d_{|\mathcal{C}(\tau)|} - 1)$, d'où $\mathrm{rg}(M_\tau) = (d_1 + \ldots + d_{|\mathcal{C}(\tau)|}) - |\mathcal{C}(\tau)| = n - |\mathcal{C}(\tau)|$. Par conséquent, $|\mathcal{C}(\tau)| = \dim\ker(M_\tau - I_n)$. □

On a donc réussi à trouver une information sur le nombre de cycles d'une permutation à partir de sa matrice. Malheureusement cette information est insuffisante pour conclure sur la structure de la permutation : la formule obtenue ne donne *a priori* que le nombre de cycles de la permutation, alors qu'on a besoin de tous les $c_l(\sigma)$ et $c_l(\sigma')$.

Mais on peut contourner le problème ! Le lemme suivant donne le nombre de cycles d'une puissance de permutation en fonction de sa structure. Comme $\tau \mapsto M_\tau$ est un isomorphisme, passer τ à la puissance m revient à passer M_τ à la puissance m. En ayant des informations sur M_τ^m, on a donc des informations sur τ^m, et donc par le lemme suivant des informations sur les $c_l(\tau)$.

Lemme 3. *Pour une permutation $\tau \in \mathfrak{S}_n$ et $m \in \mathbb{N}$, on a*

$$|\mathcal{C}(\tau^m)| = \sum_{l=1}^{n} (m \wedge l) c_l(\tau)$$

Preuve. Comme les cycles de τ sont à support disjoints, ils commutent et il suffit de raisonner sur un seul cycle $c = (x_0\ x_1\ \ldots\ x_{l-1})$. On veut montrer que $\mathcal{C}(c^m)$ compte exactement $m \wedge l$ éléments.

Observons que $c^k(x_i) = x_{i+k\ (\mathrm{modl})}$ si $k \in \mathbb{N}$ et par suite que $(c^m)^k(x_i) = x_{i+km\ (\mathrm{modl})}$. Ainsi, les points de $\{x_0, x_1, \ldots, x_{l-1}\}$ atteints par $((c^m)^k(x_i))_{k\in\mathbb{N}}$ sont les points d'indices $\{i+km\ (\mathrm{mod}l),\ k \in \mathbb{Z}\}$. Autrement dit, $((c^m)^k(x_i))_{k\in\mathbb{N}}$ atteint exactement $\frac{l}{m\wedge l}$ de ces points, et le cycle de la décomposition de c^m contenant x_i est de longueur $\frac{l}{m\wedge l}$. Cela montre que tous les cycles de la décomposition de c^m sont de longueur $\frac{l}{m\wedge l}$. Finalement, il y a $l/(\frac{l}{m\wedge l}) = m \wedge l$ cycles de longueur $\frac{l}{m\wedge l}$ dans $\mathcal{C}(c^m)$.

Enfin, on peut maintenant compter le nombre d'éléments de $\mathcal{C}(\tau^m)$. τ étant un produit de cycles qui commutent, τ^m est le produit de ces mêmes cycles à la puissance m. Par ce qui précède, chacun des cycles à la puissance m donne $m \wedge l$ cycles, donc

$$|\mathcal{C}(\tau^m)| = \sum_{c \in \mathcal{C}(\tau)} |\mathcal{C}(c^m)| = \sum_{l=1}^{n} \sum_{c \in \mathcal{C}_l(\sigma)} |\mathcal{C}(c^m)| = \sum_{l=1}^{n} \sum_{c \in \mathcal{C}_l(\sigma)} (m \wedge l) = \sum_{l=1}^{n} c_l(\tau)(m \wedge l)$$

□

Soit $m \in \mathbb{N}$. Grâce à ce lemme et à la formule précédente, on obtient d'une part :

$$\dim \ker(M_\sigma^m - I_n) = \dim \ker(M_{\sigma^m} - I_n) = |\mathcal{C}(\sigma^m)| = \sum_{l=1}^{n} (m \wedge l) c_l(\sigma)$$

et d'autre part :

$$\dim \ker(M_{\sigma'}^m - I_n) = \dim \ker(M_{\sigma'^m} - I_n) = |\mathcal{C}(\sigma'^m)| = \sum_{l=1}^{n} (m \wedge l) c_l(\sigma')$$

Comme les matrices M_σ et $M_{\sigma'}$ sont semblables, les matrices $M_\sigma^m - I_n$ et $M_{\sigma'}^m - I_n$ le sont aussi. Donc $\dim \ker(M_\sigma^m - I_n) = \dim \ker(M_{\sigma'}^m - I_n)$, et on a l'égalité $\sum_{l=1}^{n} (m \wedge l) c_l(\sigma) = \sum_{l=1}^{n} (m \wedge l) c_l(\sigma')$. On a réussi, avec les deux lemmes précédents à extraire des égalités de matrices des égalités intrinsèques sur les permutations ! Pour résumer, on a :

$$\begin{cases} \sum_{l=1}^{n} (1 \wedge l)(c_l(\sigma) - c_l(\sigma')) = 0 \\ \sum_{l=1}^{n} (2 \wedge l)(c_l(\sigma) - c_l(\sigma')) = 0 \\ \quad \vdots \\ \sum_{l=1}^{n} (n \wedge l)(c_l(\sigma) - c_l(\sigma')) = 0 \end{cases}$$

En fait, il s'agit d'un système linéaire de dimension n sur les inconnues $c_l(\sigma) - c_l(\sigma')$! Pour avoir l'égalité des structures il suffit de montrer que ce système est inversible, car alors on aurait $c_l(\sigma) - c_l(\sigma') = 0$ pour tout $l \in \{1, \ldots, n\}$.

Lemme 4. *On considère $A \in \mathcal{M}_n(K)$ la matrice dont le coefficient de la i-ème ligne et de la j-ème colonne est $i \wedge j$.*

$$A = \begin{pmatrix} 1 \wedge 1 & 1 \wedge 2 & \cdots & 1 \wedge n \\ 2 \wedge 1 & 2 \wedge 2 & \cdots & 2 \wedge n \\ \vdots & \vdots & \ddots & \vdots \\ n \wedge 1 & n \wedge 2 & \cdots & n \wedge n \end{pmatrix}$$

Cette matrice est inversible dans $\mathcal{M}_n(K)$.

Preuve. On va décomposer la matrice A en un produit pour calculer son déterminant. Pour tout entier $k \in \mathbb{N}$,

$$k = \sum_{d|k} \varphi(d) = \sum_{d=1}^{k} \mathbb{1}_{\{d|k\}} \varphi(d)$$

où φ est la fonction indicatrice d'Euler. En particulier, toute l'astuce de la démonstration réside dans l'égalité suivante :

$$\forall i, j \leqslant n, \quad i \wedge j = \sum_{d=1}^{i \wedge j} \mathbb{1}_{\{d|i \wedge j\}} \varphi(d) = \sum_{d=1}^{i \wedge j} 1_{\{d|i\}} 1_{\{d|j\}} \varphi(d) \qquad (*)$$

En effet, $\mathbb{1}_{\{d|i \wedge j\}} = \mathbb{1}_{\{d|i\} \cap \{d|j\}} = 1_{\{d|i\}} 1_{\{d|j\}}$ car $d|(i \wedge j)$ si et seulement si $d|i$ et $d|j$. Pourquoi est-ce l'astuce de la démonstration ? Car on reconnaît dans $(*)$ un produit matriciel : $A = B\Phi$, où B et Φ sont des matrices carrées de taille n définies comme suit :

$$(B)_{i,j} = \mathbb{1}_{\{j|i\}} \qquad (\Phi)_{i,j} = \mathbb{1}_{\{i|j\}}\varphi(j)$$

On voit facilement que B est triangulaire inférieure avec des 1 sur sa diagonale, et φ est triangulaire supérieure avec les $\Phi(j)$ sur la diagonale. Donc,

$$\det(A) = \underbrace{\det(B)}_{=1} \times \underbrace{\det(\Phi)}_{=\prod_{j=1}^{n}\varphi(j)} = \prod_{j=1}^{n}\varphi(j) \neq 0$$

□

(On remarque que pour affirmer que $\det(A) \neq 0$, on a besoin de l'hypothèse de la caractéristique nulle, mais c'est le seul endroit où cette hypothèse intervient.)

On vient de montrer que le système linéaire dont est solution $(c_l(\sigma) - c_l(\sigma'))_{1\leqslant l\leqslant n}$ est inversible ! Donc on a, pour tout $1 \leqslant l \leqslant n$, $c_l(\sigma) = c_l(\sigma')$. Autrement dit, σ et σ' ont les mêmes structures, et par le premier lemme, elles sont conjuguées.