SUR DES MATRICES DE PERMUTATIONS CONJUGUÉES

Daniel Ferrand et Jean-Claude Raoult
le 15 décembre 2004

Voici trois démonstrations d'un théorème de R. Brauer. Elles sont tout-à-fait dans le programme et dans l'esprit de l'agrégation, et peuvent être proposées comme développement dans plusieurs leçons, en particulier dans :
— dénombrements,
— groupe opérant sur un ensemble,
— groupe symétrique,
— sous-groupes du groupe linéaire,
— matrices semblables,
— déterminant.

THÉORÈME . — *Soit* K *un corps. Pour toute permutation* $\sigma \in \mathbf{S}_n$ *on note* $P(\sigma) \in \mathbf{GL}_n(K)$ *la matrice associée à la permutation de la base canonique de* K^n. *Pour que deux permutations* σ *et* τ *soient conjuguées dans le groupe symétrique* $\mathbf{S}_n$ *il faut et il suffit que* $P(\sigma)$ *et* $P(\tau)$ *soient conjuguées dans le groupe linéaire* $\mathbf{GL}_n(K)$, *c'est-à-dire que ces matrices soient semblables (sur* K*).*

Les deux premières démonstrations utilisent des égalités entre des invariants linéaires (trace, déterminant), lesquels sont des éléments du corps de base ; elles ne permettent pas de conclure en caractéristique positive. La dernière, un peu plus détournée, utilise la *dimension* de sous-espaces invariants ; elle est valable en toute caractéristique.

Remarques : 1) Soit k le sous-corps premier de K (ce corps est donc égal à $\mathbf{Q}$ ou à $\mathbf{F}_p$). Si on considère la matrice de permutation $P(\sigma)$ comme un élément de $\mathbf{GL}_n(K)$, ce dernier est en fait dans le sous-groupe $\mathbf{GL}_n(k)$; par suite ses invariants de similitudes sont des polynômes à coefficients dans $k[X]$. Ainsi, la similitude de $P(\sigma)$ et de $P(\tau)$ dans $\mathbf{GL}_n(K)$ équivaut à leur similitude dans $\mathbf{GL}_n(k)$, puisque l'égalité dans $K[X]$ de polynômes de $k[X]$, entraîne leur égalité dans $k[X]$.

2) La matrice M de changement de base qui assure $P(\tau) = M^{-1}P(\sigma)M$ peut très bien ne pas être une matrice de permutation (c'est le but du théorème d'assurer qu'on peut la choisir telle), même si $K = \mathbf{F}_2 = \{0, 1\}$. Si par exemple on note $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ la matrice de la transposition dans $\mathbf{F}_2^2$ et I la matrice de l'identité, on peut vérifier que dans $\mathbf{GL}_4(\mathbf{F}_2)$ on a

$$\begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} = \begin{pmatrix} T & T \\ 0 & T \end{pmatrix} \begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} \begin{pmatrix} T & T \\ 0 & T \end{pmatrix}.$$

Ou dans $\mathbf{GL}_3(\mathbf{Q})$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

La condition est clairement nécessaire. Réciproquement, on suppose qu'il existe une matrice $M \in \mathbf{GL}_n(K)$ telle que

$$P(\tau) = M^{-1}P(\sigma)M . \tag{1}$$

Pour que deux permutations soient conjuguées, il faut et il suffit que leurs décompositions en produits de cycles à supports disjoints comportent le même nombre de cycles de chaque longueur : en notant $\sigma = (a_1, a_2, \dots, a_k)$ et $\tau = (b_1, b_2, \dots, b_k)$ deux cycles de longueur k, toute permutation ρ telle que $\rho(b_i) = a_i$ vérifie $\tau = \rho^{-1}\sigma\rho$.

Notant $c_k(\sigma)$ le nombre de cycles de longueur k dans la décomposition de σ, on se ramène ainsi à montrer que pour tout entier $k \geq 1$ on a

$$c_k(\sigma) = c_k(\tau)\ . \tag{2}$$

Il suffit évidemment de considérer les k inférieurs ou égaux à n. Les trois démonstrations suivantes établissent en fait l'égalité de combinaisons linéaires des c_k, à coefficients dans K pour les deux premières et dans **Q** (et même dans **Z**) pour la dernière. L'inversibilité de la matrice des coefficients permet alors de conclure.

Première démonstration (on suppose que K est de caractéristique nulle).
L'égalité (1) implique que les deux matrices ont le même polynôme caractéristique. La matrice $P(\sigma)$ est le tableau diagonal des matrices des cycles à supports disjoints de la décomposition de σ. Or le polynôme caractéristique d'un cycle de longueur k est $T^k - 1$. L'hypothèse se traduit donc par l'égalité suivante entre polynômes à coefficients dans K :

$$\prod_k (T^k - 1)^{c_k(\sigma)} = \prod_k (T^k - 1)^{c_k(\tau)}. \tag{3}$$

Soit ζ une racine de l'unité d'ordre m (dans une clôture algébrique de K). Comme K est de caractéristique nulle, les polynômes $T^k - 1$ sont à racines simples et, par suite, la multiplicité de ζ dans $T^k - 1$ est 1 si $\zeta^k = 1$, c'est-à-dire 1 si m divise k, et 0 sinon. L'égalité (3) entraîne donc la propriété suivante, pour tout $m \geq 1$:

$$\sum_{m|k} c_k(\sigma) = \sum_{m|k} c_k(\tau)\ . \tag{4}$$

Les égalités (2) découlent alors du lemme suivant.

LEMME 1 . — *Soient* E *un ensemble muni d'un ordre noté* $x \leq y$ *et* $f, g : \mathrm{E} \to \mathbf{Z}$ *deux applications à support fini et vérifiant la propriété suivante : pour tout* $x \in \mathrm{E}$ *on a*

$$\sum_{x \leq y} f(y) = \sum_{x \leq y} g(y)\ . \tag{5}$$

Alors $f = g$.

Comme f et g sont à support fini, l'ensemble $F \subseteq E$ des points où f et g diffèrent est fini. S'il n'était pas vide, l'ensemble F possèderait un élément maximal x (puisqu'il est fini) ; mais la condition (5) conduirait alors à une contradiction.

Une autre façon de montrer l'égalité des vecteurs colonnes $C = (c_k)_k$: noter A la matrice définie ainsi :

$$a_{ij} = \begin{cases} 1 & \text{si } j \text{ divise } i, \\ 0 & \text{sinon.} \end{cases}$$

Elle est triangulaire inférieure, parce que si $j > i$, j ne peut diviser i. De plus, on a $a_{ii} = 1$ et $A = I + N$ où N est une matrice triangulaire inférieure à diagonale nulle, donc vérifiant $N^n = 0$. La matrice A est donc de déterminant 1, et inversible d'inverse $A^{-1} = I - N + N^2 + \cdots + (-1)^{n-1}N^{n-1}$, à coefficients entiers (on peut aussi calculer A^{-1} au moyen de la formule d'inversion de Mœbius).

Or les égalités (4) ci-dessus se traduisent, pour $m = 1, \dots, n$ par

$$C(\sigma)^t \,.\, A = C(\tau)^t \,.\, A \quad \text{d'où} \quad C(\sigma) = C(\tau).$$

Deuxième démonstration (on suppose toujours K de caractéristique nulle).
L'égalité (1) entraîne que pour tout entier m on a

$$P(\tau^m) = M^{-1} P(\sigma^m) M \,, \tag{6}$$

et par suite, que

$$\mathrm{Tr}(\tau^m) = \mathrm{Tr}(\sigma^m).$$

Or la trace d'une matrice de permutation est un élément *du corps de base* égal au nombre de 1 sur la diagonale de la matrice relativement à la base permutée, i.e. au nombre d'éléments de cette base que la permutation laisse invariants. Pour le calculer, on utilise le lemme suivant.

LEMME 2 . — *Si* ρ *est un cycle de longueur* k*, alors* ρ^m *est le produit de* d *cycles à supports disjoints de longueur* k/d *où* $d = \mathrm{pgcd}(k, m)$.

La conclusion devrait être claire lorsque m est un diviseur de k. Si elle ne l'est pas, écrire ρ sous la forme $(1, 2, \dots, k)$ et constater que ρ^m est le produit des m cycles

$$(1, m+1, 2m+1, \dots, k-m+1)(2, m+2, \dots, k-m+2) \cdots (m, 2m, \dots, k).$$

Passons à m quelconque : si $d = \mathrm{pgcd}(k, m)$ les permutations ρ^m et ρ^d engendrent le même sous-groupe de $\mathbf{S}_n$. En effet, comme d divise m, $\rho^m = (\rho^d)^{m/d}$. D'autre part, l'identité de Bezout s'écrit $d = ma + kb$, donc $\rho^d = (\rho^m)^a$. Enfin les orbites, vues comme les parties stables minimales, dépendent du groupe et non du choix de ses générateurs.

En appliquant ce lemme, on voit que le nombre de points fixes (orbites de longueur $k/d = 1$) de ρ^m est égal à k si k divise m, et à zéro sinon. L'égalité des traces implique donc que pour tout entier $m \geq 1$ on a, dans K :

$$\sum_{k|m} k c_k(\tau) = \sum_{k|m} k c_k(\sigma) \,.$$

Le lemme 1, mais appliqué cette fois-ci à l'ordre opposé à la divisibilité, donne les égalités $kc_k(\tau) = kc_k(\sigma)$. Comme K est de caractéristique nulle, on obtient l'égalité des entiers c_k.

Autre façon de terminer la démonstration : noter $D = (kc_k)_k$ le vecteur colonne des kc_k et constater que les égalités ci-dessus, pour $m = 1, \dots, n$ s'écrivent, avec la matrice A inversible définie plus haut :

$$A\, D(\tau) = A\, D(\sigma) \quad \text{d'où} \quad D(\tau) = D(\sigma)$$

et on termine comme ci-dessus lorsque K est de caractéristique nulle.

Remarque : Sur un ensemble à p éléments avec p premier, un cycle de longueur p et l'application identique ont pour polynômes caractéristiques $T^p - 1$ et $(T-1)^p$ respectivement. Ces polynômes sont égaux en caractéristique p et ne permettent donc pas de distinguer le cycle de l'application identique.

Troisième démonstration (K quelconque)
Posons $V = K^n$. Un élément $v = (v_1, \dots, v_n) \in V$ est invariant sous une permutation $\rho \in \mathbf{S}_n$ lorsque ses coordonnées vérifient les relations $v_i = v_{\rho(i)}$ c'est-à-dire si elles sont constantes sur les orbites de ρ ; par suite, $\dim_K(V^\rho)$ est égal au nombre d'orbites de ρ, y compris celles réduites à un point (il s'agit ici d'un «vrai» entier, un élément de $\mathbf{N}$). Pour exprimer le nombre d'orbites de σ^m en fonction des

$c_k(\sigma)$, on utilise de nouveau le lemme 2 : chaque cycle de longueur k composant σ se décompose en $\mathrm{pgcd}(k,m)$ cycles dans σ^m. Par suite, le nombre d'orbites de σ^m est $\Sigma_k \mathrm{pgcd}(k,m)c_k(\sigma)$. Les égalités (6) impliquent donc, pour tout entier $m \in \mathbf{N}$,

$$\sum_k \mathrm{pgcd}(k,m)c_k(\sigma) = \sum_k \mathrm{pgcd}(k,m)c_k(\tau).$$

La conclusion suit de l'inversibilité de la matrice des pgcd. Celle-ci est classique :

LEMME (Déterminant de Smith) . — *Soit* S *la matrice* $n \times n$ *dont le terme d'indice* (i,j) *est* $\mathrm{pgcd}(i,j)$. *Alors*

$$\det(\mathrm{S}) = \varphi(1)\varphi(2)\cdots\varphi(n)$$

où φ *est la fonction indicatrice d'Euler :* $\varphi(n)$ *est le nombre d'entiers inférieurs à* n *et premiers avec lui.*

Notons Φ la matrice diagonale de termes $(\varphi(1), \varphi(2), \ldots, \varphi(n))$. En utilisant la relation $\Sigma_{d|m}\ \varphi(d) = m$, on vérifie immédiatement l'égalité suivante :

$$\mathrm{A}\Phi\mathrm{A}^t = \mathrm{S}\ ,$$

où A est encore la matrice de la divisibilité définie plus haut ; et on a déjà vu que $\det \mathrm{A} = 1$, cqfd.

Références

La première démonstration figure maintenant dans le livre de BECK, MALICK, PEYRE : *Objectif Agrégation,* H&K (2004). Elle est détaillée dans un exercice (corrigé) page 321.

La troisième démonstration se trouve dans une lettre de Kovacs à Curtis, intitulée : *The permutation lemma of Richard Brauer,* et reproduite dans le Bull. London Math. Soc., 14 (1982), 127-128.