101e année (1990-1991) Décembre 1990 - Mensuel n° 4

Revue de Mathématiques Spéciales

Un résultat et deux questions sur le groupe des automorphismes d'une algèbre de matrices

par Patrick TELLER, Lycée Turgot.

INTRODUCTION.

Un résultat classique, le théorème de Skolem-Noether, montre que les automorphismes de l'algèbre $M_n(K)$, où K est un corps, sont tous intérieurs, c'est-à-dire que tout automorphisme de $M_n(K)$ est de la forme $\sigma_P : A \mapsto P^{-1}AP$ où $P \in GL_n(K)$ [2].

On peut trouver des algèbres de matrices dont les automorphismes ne sont pas tous intérieurs (par exemple [1]). Cependant, dans ce résultat, les automorphismes mis en évidence sont malgré tout induits par la conjugaison, c'est-à-dire sont de la forme $A \mapsto P^{-1}AP$, pour des matrices de permutation particulières qui, bien entendu, n'appartiennent pas à l'algèbre considérée car, si c'était le cas, il s'agirait à nouveau d'automorphismes intérieurs.

On peut donc se demander si les automorphismes d'une algèbre de matrices M incluse dans $M_n(K)$ sont tous induits par la conjugaison, c'est-à-dire finalement ont tous le sens d'un changement de base dans l'espace vectoriel K^n sur lequel M opère naturellement ; on peut poser une autre question : soit M une algèbre de matrices, quels sont les invariants conservés par les automorphismes de M ? On conçoit que ceux-ci soient algébriques et relatifs aux propriétés de M. On se demande s'il est naturel que ceux-ci aient une interprétation géométrique, c'est-à-dire liée non aux propriétés d'algèbre de M mais à celles de l'action de M sur K^n.

Nous allons nous intéresser aux automorphismes de l'algèbre C[A] engendrée par une matrice complexe A (de façon à pouvoir utiliser la décomposition de Jordan) ; dans ce cas, comme il s'agit d'une algèbre commutative, il n'y a pas d'automorphismes intérieurs non triviaux.

On montrera que le groupe des automorphismes de C[A] contient naturellement des automorphismes induits sur C[A] par les automorphismes intérieurs de $M_n(C)$ mais, à la différence des cas cités plus haut, on verra qu'il peut exister aussi des automorphismes non induits par les automorphismes intérieurs de $M_n(C)$.

Une caractérisation des matrices A pour lesquelles cette propriété est vraie sera donnée ainsi que la détermination exacte des automorphismes de C[A].

Pour étudier des automorphismes, on peut remarquer qu'une manière de définir un endomorphisme de C[A] consiste à considérer une application f telle que

i) $f(I) = I$,

ii) $f(A)$ appartient à C[A],

iii) f est un morphisme d'algèbres.

I. — GÉNÉRALITÉS DE TYPE ALGÉBRIQUE.

On conçoit aisément que si σ est automorphisme d'une sous-algèbre M de $M_n(K)$, alors $\forall A \in M_n(K)$, $\mathrm{Min}(A) = \mathrm{Min}(\sigma(A))$ où Min(A) désignera le polynôme minimal de la matrice A et donc nécessairement A et $\sigma(A)$ ont même spectre.

Pour toute valeur propre μ de A, désignons par $n_i(A, \mu)_{i=0,\ldots,n}$ la dimension de $\mathrm{Ker}((A - \mu I)^i)$; si $\sigma(A)$ est conjuguée avec A alors $n_i(A, \mu) = n_i(\sigma(A), \mu)$ pour tout i, mais sinon il n'est pas du tout sûr que ces entiers soient égaux. Nous montrerons que dans le cas de C[A] il existe des indicateurs numériques invariants par σ.

Dans le cas de matrices à coefficients dans C, on peut utiliser la décomposition de Jordan.

Rappelons d'abord des résultats liés à la décomposition de Jordan : si u est un endomorphisme de C^n il existe une décomposition $C^n = \bigoplus V_j$, telle que, quel que soit $j \in 1, \ldots, q$, la restriction de u à V_j est de la forme $h + n$, où h est une homothétie et n est nilpotent d'indice égal à la dimension de V_j (de plus, h et n sont des polynômes en u et, par suite, tout sous-espace stable par u est stable par h et n).

Nous appellerons ces sous-espaces V_j « cellules » associées à u ; la décomposition de C^n en somme directe des V_j est unique.

Définition 1. — Caractéristique de Segre d'une matrice.

Soit $\mu_1, \ldots, \mu_r$ le spectre de A, pour chaque valeur propre μ_i de A notons $K(i, 1), \ldots, K(i, l_i)$ la suite décroissante des dimensions des cellules de Jordan associées à la valeur propre μ_i.

Nous appellerons caractéristique de Segre complète de A le tableau suivant :

μ_1 ; $K(1, 1),\ K(1, 2), \ldots, K(1, l_1)$.
μ_2 ; $K(2, 1),\ K(2, 2), \ldots, K(2, l_2)$.
...
μ_r ; $K(r, 1),\ K(r, 2), \ldots, K(r, l_r)$.

Ce tableau diffère de la caractéristique de Segre [3] par le fait que nous ne nous intéressons pas seulement aux entiers $K(i, j)$ mais aussi aux valeurs des valeurs propres, μ_i.

Pour des raisons de commodité, nous appellerons caractéristique de Segre complète le tableau incluant les valeurs propres et caractéristique de Segre le tableau classique ne comprenant que les entiers.

On désignera les termes $K(i, 1)$ par le nom de « têtes de lignes », en précisant éventuellement la valeur propre associée.

Enfin, précisons que l'on peut supposer le spectre de A ordonné, c'est-à-dire que les valeurs propres sont rangées dans un ordre qui sera dit « croissant ».

Exemple :

Soit la matrice

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Sa caractéristique de Segre sera donc :

2, 1, 1.
2.

et sa caractéristique de Segre complète sera :

0 ; 2, 1, 1.
1 ; 2.

Définition 2. — Matrice à caractéristique équilibrée.

Une matrice A de $M_n(C)$ sera dite à caractéristique équilibrée si sa caractéristique de Segre possède la propriété suivante :

Deux lignes dont les têtes de lignes sont égales sont identiques.

On notera cette propriété C.E. (caractéristique équilibrée). Une matrice qui n'est pas à caractéristique équilibrée sera dite C.N.E. (caractéristique non équilibrée).

Exemple. — Soit les matrices A de l'exemple précédent et B, définie par

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A est à C.N.E., tandis que B est à C.E.

II. — Quelques groupes liés a une matrice.

Soit A une matrice de $M_n(C)$, on peut définir les groupes suivants :

- Le commutant de A, C(A), groupe des matrices P de $Gl_n(C)$ telles que PA = AP.
- Le groupe que nous désignerons par $\mu(A)$, formé par les matrices P de $Gl_n(C)$ telles que $P^{-1}AP$ peut s'exprimer comme un polynôme en A (exercice : vérifier que $\mu(A)$ est un groupe). Il est clair que C(A) est inclus dans $\mu(A)$.
- Définissons G(A), le groupe des automorphismes de l'algèbre C[A].

A tout élément P de $\mu(A)$ on peut associer $s(P)$ l'automorphisme de C[A] défini par $A \mapsto P^{-1}AP$. On obtient alors la suite exacte :

$$1 \to C(A) \to \mu(A) \xrightarrow{s} G(A).$$

Dans les cas de $M_n(K)$ et de l'article de Barker [1], s est toujours surjective, mais nous allons montrer que dans le cas considéré ici, celui de C[A], ce n'est pas vrai ; il est donc naturel de définir le quotient $G(A)/s[\mu(A)]$, ce groupe sera désigné par la suite par S(A) ; c'est lui qui mesure si tous les automorphismes de l'algèbre sont induits par la conjugaison par certaines matrices de $M_n(K)$ ou pas...

III. — Étude de S(A).

Rappelons-le

Lemme 3. — Une formule de Taylor.

Soit A une matrice de $M_n(C)$ de la forme $aI + N$ où N est nilpotente d'ordre n, si P est un polynôme de C[X], alors

$$P(A) = P(a)I + P'(a)N + P''(a)N/2! + \cdots + P^{(n-1)}(a)N^{n-1}/(n-1)!$$

Démonstration : immédiate.

Proposition 4. — **Construction de G(A).**

Soit A *une matrice de* $M_n(C)$ *dont le spectre ordonné est* $\mu_1, \ldots, \mu_r$.

i) *Tout endormorphisme de* C[A] *est induit par* $A \mapsto P(A)$ *où* $P \in C[X]$.

ii) *Il existe une permutation* θ *de* $\{1, \ldots, r\}$ *telle que, quel que soit* i :

- *la multiplicité de* $\mu_{\theta(i)}$ *dans le polynôme minimal de* A = *multiplicité de* μ_i *et* $P(\mu_{\theta(i)}) = \mu_i$.

- *Si* μ_i *possède un bloc de Jordan d'ordre supérieur strictement à* 1. $P'(\mu_i) \neq 0$.

Démonstration. — Comme le résultat est conservé par conjugaison, nous allons raisonner sur le cas d'une matrice sous forme de Jordan.

i) Considérons d'abord un endomorphisme f de C[A], il est connu dès qu'est connue la matrice $f(A) = A'$ de C[A], c'est-à-dire le polynôme P tel que $A' = P(A)$.

ii) A quelle condition sur P, l'endomorphisme $f(P)$ est-il une bijection de C[A] ?

- Dans un premier temps, considérons le cas où A est un bloc de Jordan, d'ordre supérieur à 1, associé à la valeur propre μ_i :

D'après le lemme, P(A) est une matrice triangulaire supérieure dont les termes de la diagonale sont égaux à $P(\mu_i)$; comme $A - \mu$ est nilpotente d'ordre n, si P(A) est l'image de A par un automorphisme, P(A) doit aussi avoir pour valeur propre μ_i (conservation du polynôme minimal) et, de plus vérifier la relation $P(A) - \mu_i I$ est nilpotente d'ordre n, ce qui sera le cas si, et seulement si, $P'(\mu_i) \neq 0$.

Inversement, si $P'(\mu_i) \neq 0$, nous allons montrer qu'il existe un polynôme Q de C[X], tel que $(Q \circ P)(A) = A$.

Développant P(X) et Q(X) suivant les puissances de $X - \mu_i$, ceci est équivalent à montrer que si P est un polynôme de C[X] tel que $P(0) = 0$ et $P'(0) \neq 0$, alors il existe un polynôme Q tel que $(Q \circ P)(X) = X$ modulo X^n ; c'est un résultat connu (notons qu'alors on a aussi $(P.Q)(X) = X$ modulo X^n).

- Dans le cas d'une matrice ayant plusieurs blocs de Jordan associés à une seule et unique valeur propre, le raisonnement est le même.

- Dans le cas où il y a plusieurs valeurs propres $\mu_1, \ldots, \mu_r$, les changements sont les suivants :

$P(\mu_i)$ ne doit pas nécessairement être égal à μ_i mais à une valeur propre μ_j, racine de même ordre du polynôme minimal de A.

La condition $P'(\mu_i) \neq 0$ permet comme plus haut d'assurer l'existence de l'inverse.

Théorème 5. — **Condition nécessaire et suffisante de nullité de S(A).**

Soit une matrice A *de* $M_n(C)$, *on a l'équivalence suivante :* A *est à* C.E. *si, et seulement si,* S(A) *est nul.*

Démonstration. — Soit B l'image de A par l'automorphisme g de G(A), le polynôme minimal de B est égal à celui de A, donc leurs spectres sont égaux et les dimensions des blocs de Jordan maximaux relatifs à chacune des valeurs propres sont égales. Donc, les tableaux de A et de B ont même nombre de lignes et même premier terme dans chacune des lignes ; de plus, si V_j est une cellule relative à A, il est stable par B et donc peut se décomposer en une somme directe de cellules relatives à B : W_i pour $i \in 1, \ldots, p$. Cependant, si B est l'image de A par un automorphisme, A est l'image de B par l'automorphisme inverse et, par suite, chaque W_i peut se décomposer en une somme directe de cellules relatives à A, en conclusion comme V_j était minimal, on en déduit que V_j était déjà une cellule pour B. Donc, A et B ont même polynôme minimal, même spectre et aussi mêmes cellules.

Maintenant distinguons trois cas.

1. *Les têtes de lignes sont distinctes deux à deux.*

Donc, si a est une valeur propre de A, elle l'est aussi de B, les têtes de lignes étant distinctes deux à deux, les multiplicités de a comme racine du polynôme minimal de A et de B étant les mêmes, on en déduit que si V_j désigne une cellule de dimension maximale associée à a pour A, elle est aussi une cellule de dimension maximale pour a et B. Par suite, si on considère une cellule relative à A et à la valeur propre a, elle est transformée en une cellule de B relative à la valeur propre a, donc chaque bloc est transformé sous l'action de g en un bloc semblable et A est transformée en une matrice semblable B.

2. *Les têtes de lignes ne sont plus distinctes deux à deux, mais la matrice est à C.E.*

Le raisonnement est analogue à ceci près qu'il peut y avoir plusieurs cellules associées à des têtes de lignes qui ont la même dimension et donc le raisonnement précédent permet de conclure que sur ces blocs de dimension maximale l'action de g peut être une permutation.

Donc g permute éventuellement les valeurs propres et donc les blocs, un bloc n'est pas nécessairement transformé en un bloc semblable ; mais « tout se retrouve » car les lignes associées à deux valeurs propres permutées sont égales et donc finalement une chaîne de blocs a été transformée en une chaîne semblable à une autre et réciproquement. Encore une fois, B est semblable à A. Ceci établit donc que si A est à C.E., l'application $\mu(A) \to G(A)$ est surjective donc S(A) est nul.

3. *A est à C.N.E.*

Dans ce cas, nous allons montrer qu'il existe des polynômes P et Q de C[X] tels que $(P.Q)(A) = A$ avec $P(A)$ non semblable à A. Pour cela nous allons utiliser la proposition 4 : soit deux valeurs propres μ_{i_0} et μ_{j_0} correspondant à des têtes de lignes égales mais des lignes distinctes ; définissons une permutation s de $1, \ldots, r$ telle que $s(i_0) = j_0$. Montrons qu'il existe un polynôme P de C[X] tel que, quel que soit $i \in 1, \ldots, r$, $P(\mu_i) = \mu_{s(i)}$ et $P'(\mu_i) \neq 0$.

La première condition définit P comme appartenant à un sous-espace affine E(A) de dimension $n - r$ de C[X], la deuxième condition définit P comme appartenant à l'intersection de $n - r$ ouverts denses de C[X] (avec bien entendu $r < n$). Il existe de tels polynômes P comme on peut le voir facilement et même de tels polynômes forment un ouvert dense de E(A). Le résultat est donc établi.

On remarquera donc que, dans le cas de l'algèbre C[A], les automorphismes sont différents du cas de l'algèbre étudiée par Barker [1] où, comme dans le cas de $M_n(K)$, le groupe que nous avons désigné par S est trivial, tous les automorphismes sont induits par la conjugaison par des matrices de $M_n(K)$.

Exemple. — Dans le cas de la matrice A définie plus haut, on peut construire la matrice A' qui n'est pas semblable à A, mais l'endomorphisme de C[A] défini par $A \mapsto A'$ est un automorphisme de C[A].

Il suffit de déterminer un polynôme P(X) tel que $P(0) = 1$, $P(1) = 0$, $P'(0) \neq 0$ et $P'(1) \neq 0$.

Le polynôme $P(X) = 1 + X - 6X^2 + 4X^3$ convient.

Alors la matrice P(A) est égale à :

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Corollaire. — Conservation des caractéristiques de Segre.

Si M est une sous-algèbre de $M_n(K)$ tout automorphisme de M de la forme $A \mapsto P^{-1}AP$ conserve la caractéristique de Segre complète ; dans le cas de C[A], tout automorphisme σ qui n'est pas induit par la conjugaison dans $M_n(C)$, ne conserve que la caractéristique de Segre (*mais pas la caractéristique complète*).

Théorème 6. — Description de S(A).

Soit $\mu_1, \ldots, \mu_r$ le spectre ordonné de A, S(A) est le sous-groupe de S_r engendré par les transpositions (i, j) pour les couples (i, j) tels que $K(\mu_i, 1) = K(\mu_j, 1)$ mais la i^e ligne de la caractéristique de Segre est différente de sa j^e ligne.

Démonstration. — Se reporter à la construction faite dans les questions précédentes.

Exemple.

Soit une matrice A dont la caractéristique de Segre est :

3, 2, 1, 1.
4, 2, 1.
3, 1, 1.
4, 2.
4, 2, 1.

S(A) est isomorphe au sous-groupe de S_5 engendré par les transpositions : (1, 3), (2, 4), (4, 5).

Théorème 7. — Nature de G(A).

G(A) *est le produit direct de* S(A) *et de* $s[\mu(A)]$.

Démonstration. — Tout élément f de G(A) est connu dès qu'est connu $f(A)$: d'autre part, les éléments de $\mu(A)$ agissent sur les restrictions de A aux cellules de A, tandis que les éléments de S(A) échangent certains blocs de type $K(i, p)$ (où $p = 2, \ldots$).

IV. — Le résultat dans le cas d'une algèbre de matrices triangulaires.

Dans l'article de Barker [1] cité plus haut, celui-ci montre que si M est une algèbre de matrices triangulaires engendrée par des matrices de la forme $E_{i,j}$ (où $E_{i,j}$ désigne la matrice dont tous les éléments sont nuls sauf celui qui se trouve à l'intersection de la i^e ligne et de la j^e colonne), alors le groupe des automorphismes de M est le produit semi-direct du groupe des automorphismes intérieurs de M et d'un groupe d'automorphismes induits par la conjugaison $A \mapsto P^{-1}AP$ pour des matrices P de permutation associées à cette algèbre.

V. — Une remarque et deux questions.

On avait remarqué que la conservation du spectre et du polynôme minimal est naturelle ; ce qui est curieux, c'est que dans les divers cas considérés on a pu constater que les automorphismes d'algèbre laissent invariante la caractéristique de Segre et, dans le cas du théorème de Skolem-Noether, comme dans l'article de Barker, c'est même la caractéristique complète de Segre qui est conservée, puisque l'image d'une matrice est une matrice semblable.

Ceci est *a priori* surprenant car il s'agit là d'éléments qui ne sont pas intrinsèques à l'algèbre de matrices mais liés à son action sur C^n.

D'où une première question : la situation rencontrée ici, la conservation de la caractéristique de Segre, est-elle vraie quelle que soit la sous-algèbre de $M_n(C)$?

Deuxième question : comment caractériser les sous-algèbres de $M_n(C)$ pour lesquelles la caractéristique de Segre complète est conservée, ou pour lesquelles l'image d'une matrice est une matrice semblable ?

Références :

[1] G. P. Barker, « Automorphism Groups of Algebras of Triangular Matrices », *Linear Algebra and its Applications*, 121 : 207-215 (1989).
[2] Bourbaki, *Éléments de Mathématiques*, Livre II, Algèbre, chapitre 8, « Modules et anneaux semi-simples », Hermann (1958).
[3] A. I. Mal'cev, *Foundations of Linear Algebra*, Freeman and Company (1963).

Concours commun mines, ponts et chaussées

Option M
Deuxième composition

6557. Irrationalité de π^2.

(Voir l'énoncé complet dans la Revue n° 1, page 96.)

Partie I.

1° La fonction f est clairement continue sur $\mathbb{R}\backslash\pi\mathbb{Z}$. On constate immédiatement qu'elle est également continue en 0 et que sa limite à gauche au point π (qui vaut 0) est aussi égale à sa limite à droite en ce même point (c'est-à-dire à sa limite à droite au point $-\pi$).

La fonction f est donc continue sur $\mathbb{R}$. Les restrictions de f à $[-\pi, 0]$ et $[0, \pi]$ sont bien évidemment de classe C^∞. La fonction f est donc continue et de classe C^1 par morceaux. Un théorème du cours assure que sa série de Fourier converge normalement et que sa somme est égale à f. On a donc, avec les notations classiques

$$\forall x \in \mathbb{R}, \quad f(x) = \frac{a_0(f)}{2} + \sum_{n=1}^{+\infty} (a_n(f) \cos nx + b_n(f) \sin nx).$$

Comme la fonction f est paire, on a $\forall n \geqslant 1$, $b_n(f) = 0$ et

$$a_n(f) = \frac{2}{\pi}\int_0^\pi (\pi - x)\cos nx \,\mathrm{d}x = \frac{2}{\pi}\left[(\pi - x)\frac{\sin nx}{n}\right]_0^\pi - \frac{2}{n\pi}\int_0^\pi \sin nx\,\mathrm{d}x = \frac{2}{n^2\pi}((-1)^n - 1),$$

d'où

$$a_{2p}(f) = 0 \qquad \text{et} \qquad a_{2p+1}(f) = -\frac{4}{(2p+1)^2\pi}.$$

On a d'autre part $a_0(f) = \dfrac{2}{\pi}\displaystyle\int_0^\pi (\pi - x)\,\mathrm{d}x = \pi$. On déduit donc de ces calculs que

$$\forall x \in \mathbb{R}, \quad f(x) = \frac{\pi}{2} - \frac{4}{\pi}\sum_{p=0}^{+\infty}\frac{\cos(2p+1)x}{(2p+1)^2}.$$

2° Appliquons le résultat précédent pour $x = 0$. On obtient que

$$\pi = \frac{\pi}{2} - \frac{4}{\pi}\sum_{p=0}^{+\infty}\frac{1}{(2p+1)^2},$$

soit encore

$$\sum_{p=0}^{+\infty}\frac{1}{(2p+1)^2} = \frac{\pi^2}{8}.$$