AUTOUR DES MATRICES DE FROBENIUS OU COMPAGNON

Hervé Carrieu, Maurice Fadel, Etienne Fieux, Patrice Lassère & Frédéric Rodriguez

12 février 2007

« When a polynomial in one variable interests you, ask about the matrices of which it is the caracteristic polynomial. »
Olga Taussky,[1]

Table des matières

1 INTRODUCTION **3**

2 RÉSULTATS FONDAMENTAUX **4**
2.1 Endomorphismes et matrices cycliques . . . 4
2.2 Théorème de décomposition de Frobenius . . . 6
2.3 Quelques propriétés topologiques . . . 8
2.4 Propriétés spectrales . . . 9

3 APPLICATIONS À L'ALGÈBRE LINÉAIRE **11**
3.1 Le Théorème de Cayley-Hamilton . . . 11
3.2 Décomposition de Jordan . . . 12
3.3 Matrices semblables . . . 14
3.4 Matrice transposée . . . 15
3.5 Commutant et bicommutant . . . 17
3.5.1 Le commutant . . . 17
3.5.2 Approche topologique de la dimension du commutant . . . 19
3.5.3 Le bicommutant . . . 20
3.5.4 Quelques précisions sur la dimension du commutant . . . 21

4 AUTRES APPLICATIONS MATHÉMATIQUES **24**
4.1 Polynômes de Sylvester . . . 24
4.2 Les formules de Newton . . . 25
4.3 Localisation des racines d'un polynôme . . . 27
4.4 Quelques dernières applications . . . 28

5 UNE APPLICATION « CONCRÈTE » **29**

6 CONCLUSION **32**

[1] « How I Became a Torchbearer for Matrix Theory », American Mathematical Monthly (1988), Vol. 95-9.

1 INTRODUCTION

Dans tout ce travail et sauf mention contraire le symbole $\mathbb{K}$ désignera le corps[2] $\mathbb{R}$ ou $\mathbb{C}$. À tout polynôme unitaire

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{K}[X]$$

on associera sa **matrice de Frobenius** ou **compagnon**[3]

$$C_P = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix} \in M_n(\mathbb{K}).$$

Un calcul élémentaire (en développant par exemple par rapport à la dernière ligne) montre que son polynôme caractéristique[4]

$$P_{C_P}(X) := \det(XI_n - C_P) = P(X),$$

Ce lien entre matrice et polynôme (illustré par l'appellation « compagnon ») permet souvent de « traduire » certains énoncés « matriciels » en des énoncés « polynomiaux » et réciproquement : c'est la source d'élégantes démonstrations souvent plus élémentaires que par les approches classiques. Nous proposons ici une étude assez détaillée de ces matrices et de leurs applications.

Notations : $\triangleright$ La matrice compagnon C_P d'un polynôme $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ sera aussi parfois appelée **matrice compagnon** C_a **du vecteur** $a = (a_0, a_1, \cdots, a_{n-1})$.

$\triangleright$ Pour un endomorphisme φ (resp. une matrice M), P_φ et π_φ (resp. P_M et π_M) désignent le **polynôme caractéristique** et le **polynôme minimal** associés.

$\triangleright$ Une matrice est **cyclique** (cf. §2.1) si, et seulement si, elle est semblable à une matrice compagnon et l'ensemble des matrices cycliques sera noté $\mathcal{C}_n$.

$\triangleright$ Il faut enfin signaler que nous userons et abuserons tout au long de cet article de l'isomorphisme canonique « matrice $\simeq$ endomorphisme ».

2 RÉSULTATS FONDAMENTAUX

2.1 Endomorphismes et matrices cycliques

Un endomorphisme φ d'un $\mathbb{K}$-espace vectoriel E (de dimension n) est **cyclique** s'il existe un vecteur x tel que $\mathcal{B} := \{\varphi^k(x),\ k = 0, \dots, n-1\}$ soit une

[2]Un grand nombre des résultats restent vrais dans le contexte d'un corps plus général, toutefois afin de faciliter la lecture il est plus raisonnable de se cantonner au cas $\mathbb{R}$ ou $\mathbb{C}$.

[3]Ou **matrice compagne** pour les automaticiens.

[4]Bien noter que le polynôme caractéristique est ici (et contrairement à la tradition) **unitaire**, nous suivons le point de vue de Fresnel [5].

base de E. Il est alors immédiat que la matrice de φ dans la base $\mathcal{B}$ sera une matrice compagnon et la réciproque est claire : si la matrice de φ est semblable à une matrice compagnon alors φ est cyclique. On dira qu'une **matrice est cyclique** si elle est la matrice d'un endomorphisme cyclique (autrement dit, s'il existe $x \in E$ tel que $\{x, Mx, \ldots, M^{n-1}x\}$ soit une base de E) ; on a donc :

Proposition 1 *Une matrice est cyclique si, et seulement si, elle est semblable à une matrice compagnon.*

Dans l'anneau des polynômes à une indéterminée $\mathbb{K}[X]$, tout idéal est engendré par un polynôme unitaire de degré minimal. Ainsi pour tout $x \in E$, l'idéal

$$I_{\varphi,x} := \left\{ P \in \mathbb{K}[X] \ : \ P(\varphi)(x) = 0 \right\}$$

est engendré par un polynôme $\pi_{\varphi,x}$. C'est le **polynôme minimal de x relativement à φ**. Le résultat qui suit est essentiel, nous l'utiliserons à plusieurs reprises dans ce travail.

Lemme fondamental *Il existe $x \in E$ tel que $\pi_{\varphi,x} = \pi_\varphi$.*

Démonstration : Il est déjà évident ($\pi_\varphi \in I_{\varphi,x}$) que $\pi_{\varphi,x}$ divise π_φ pour tout $x \in E$. Il n'existe donc, lorsque x décrit E qu'un nombre fini de tels polynômes $\pi_{\varphi,x_1}, \ldots, \pi_{\varphi,x_l}$, soit

$$E = \bigcup_{1 \leqslant i \leqslant l} \mathrm{Ker}(\pi_{\varphi,x_i})$$

et par un argument classique, $E = \mathrm{Ker}(\pi_{\varphi,x_i})$ pour un entier $i \in \{1, \ldots l\}$. Mais alors $\pi_{\varphi,x_i}(\varphi)(y) = 0$ pour tout y dans E : π_{φ,x_i} est donc annulé par φ et c'est donc un multiple du polynôme minimal π_φ. Vu ce qui précède, $\pi_\varphi = \pi_{\varphi,x_i}$ et la propriété est démontrée. ■

Nous laissons en exercice les résultats suivants, conséquences immédiates (ou presque) de ce qui précède (nous les utiliserons à maintes reprises) :

Exercice 1 *1) Tout polynôme unitaire est à la fois polynôme minimal et caractéristique de sa matrice compagnon.*
2) Une matrice est cyclique si et seulement si ses polynômes minimal et caractéristique coïncident.
3) Une matrice est cyclique si, et seulement si, tous ses sous-espaces propres sont de dimension 1.
4) Tout bloc de Jordan est semblable à une matrice de Frobenius.
5) L'ensemble des vecteurs cycliques (d'un endomorphisme φ) constitue un ouvert dense.

2.2 Théorème de décomposition de Frobenius

Pour $A \in M_n(\mathbb{C})$ la mise sous forme triangulaire et la réduite de Jordan[5] sont quelques unes des multiples réductions sous forme canonique d'une matrice[6], un autre type de réduction est celle en blocs de matrices compagnon (réduction ou décomposition de Frobenius) :

Théorème 1 (décomposition de Frobenius) *Toute matrice est semblable à un bloc diagonal de matrices compagnon. Plus précisément donnons-nous un endomorphisme $\varphi \in \mathcal{L}(E)$ (E $\mathbb{K}$-espace vectoriel sur un corps commutatif $\mathbb{K}$ de dimension finie $n \geqslant 1$) ou de manière équivalente une matrice $A \in M_n(\mathbb{K})$. Alors il existe une suite $E_1, E_2, \ldots, E_r$ de sous-espaces vectoriels de E, tous stables par φ telle que :*

▷ $E = \bigoplus_{i=1}^{r} E_i$.

▷ *Pour tout $1 \leqslant i \leqslant r$, $\varphi_i := \varphi_{/E_i}$ est un endomorphisme cyclique.*

▷ *Notons P_i le polynôme minimal de φ_i, alors pour tout $1 \leqslant i \leqslant r-1$: P_{i+1} divise P_i.*

▷ *La suite de polynômes $(P_i)_{i=1}^{r}$ ne dépend que de l'endomorphisme φ et non de la décomposition. c'est la suite des* **invariants de similitude** *de φ (ou de A).*

(★) *En particulier, il existe une base $\mathcal{B}$ de E pour laquelle la matrice de φ est de la forme*

$$M(\varphi, \mathcal{B}) = \begin{pmatrix} C_{P_1} & & & \\ & C_{P_2} & & 0 \\ & & \ddots & \\ 0 & & & C_{P_r} \end{pmatrix}$$

avec $P_1 = \pi_\varphi$ et $P_1 P_2 \ldots P_r = P_\varphi$.

Démonstration : ► Existence de la décomposition : On procède par récurrence sur la dimension de E. Si d est le degré du polynôme minimal de φ, il existe un vecteur $y \in E$ tel que $\pi_\varphi = \pi_{\varphi,y}$ et il est clair que le plus petit sous-espace stable par φ et contenant y est de dimension d et admet pour base $e_1 = y$, $e_2 = \varphi y, \ldots, e_d = \varphi^{d-1} y$, i.e. :

$$E_y := \{ P(\varphi)y,\ P \in \mathbb{K}[X]\} = \mathrm{Vect}\{e_1, \ldots, e_d\}$$

[5] La réduction de Jordan dans $M_n(\mathbb{K})$ est possible si le corps $\mathbb{K}$ est algébriquement clos, la suite des invariants de similitude à la base de la décomposition de Frobenius, elle, est valable dans tout corps $\mathbb{K}$ ([5] p.139).

[6] On pourra consulter [9].

Soit à présent $F = \{x \in E, \forall k \in \mathbb{N}, e_d^*(\varphi^k(x)) = 0\}$ et montrons que $E = E_y \oplus F$.

Par définition, F est l'ensemble des vecteurs x de E dont la d-ième coordonnée de $\varphi^i y$ dans la base $\{e_1, \ldots, e_d\}$ est nulle pour tout i et ceci a pour conséquence immédiate que F est stable par φ (puisque $e_d^*(\varphi^k(\varphi(x)) = e_d^*(\varphi^{k+1}(x)) = 0$ si $x \in F$). De plus, si $z = a_1e_1 + \ldots + a_de_d$, $e_d^*(z) = a_d$ et aussi si $z = a_1e_1 + \ldots + a_ke_k$ avec $k < d$, $e_d^*(\varphi^{d-k}(z)) = a_k$ et ceci montre que $z = a_1e_1 + \ldots + a_de_d \in F \Leftrightarrow a_1 = a_2 = \ldots = a_d = 0$, autrement dit que $E_y \cap F = \{0\}$. Il reste à montrer que F est de dimension $n - d$.

Pour cela considérons l'opérateur T défini sur $\mathbb{K}[\varphi] \subset E^* = \mathcal{L}(E, \mathbb{K})$:

$$T \ : \ g \ \mapsto \ T(g) = e_d^\star \circ g$$

T est injectif car si $e_d^\star \circ g = 0$ avec g non nul, on peut l'écrire sous la forme $g = a_1 Id_E + a_2\varphi + \cdots + a_p\varphi^{p-1}$ avec $p \leqslant d$ et a_p non nul. Or

$$0 = e_d^\star \circ g(\varphi^{d-p}) = e_d^\star(a_1e_{d-p+1} + \cdots + a_pe_d^\star) = a_p$$

ce qui est absurde. Par conséquent, $\dim \mathrm{Im}T = d$ et comme, par définition, F est l'orthogonal de $\mathrm{Im}T$ (au sens du dual), on trouve bien que $\dim F = n - \dim \mathrm{Im}T = n - d$.

Nous avons donc trouvé un sous-espace F stable par φ et tel que $E = E_y \bigoplus F$. Soit P_1 le polynôme minimal de $\varphi_{|E_y}$: $P_1 = \pi_{\varphi_{|E_y}}$ car $\varphi_{|E_y}$ est par construction un endomorphisme cyclique (cf. Exercice 1), soit encore $P_1 = \pi_{\varphi,y} = \pi_\varphi$. Soit maintenant P_2 le polynôme minimal de $\varphi_{|F}$, F est stable par φ donc P_2 divise P_1. On n'a plus qu'à reprendre la procédure avec $\varphi_{|F}$ et au bout d'un nombre fini d'étapes on obtiendra la décomposition annoncée.

► **Unicité :** Supposons l'existence de deux suites de sous-espaces $F_1, F_2, \ldots, F_r$ et $G_1, G_2, \ldots, G_s$ tous stables par φ vérifiant les trois premières propriétés. Notons $P_i = \pi_{\varphi_{|F_i}}$ et $Q_i = \pi_{\varphi_{|G_i}}$.

Il est déjà clair que $P_1 = \pi_\varphi = Q_1$ (et $\dim F_1 = \dim G_1$). Supposons les deux suites distinctes et notons $j \geqslant 2$ le premier indice tel que $P_j \neq Q_j$ (un tel indice existe toujours car $\displaystyle\sum_{i=1}^{r} \deg(P_i) = \sum_{j=1}^{s} \deg(Q_j) = \dim E$). On a alors (puisque $P_j(F_{j+k}) = 0$ si $k \geqslant 0$) :

$$(1) \qquad P_j(\varphi)(E) = P_j(\varphi)(F_1) \oplus \cdots \oplus P_j(\varphi)(F_{j-1})$$

et aussi :

$$(2) \quad P_j(\varphi)(E) = P_j(\varphi)(G_1) \oplus \cdots \oplus P_j(\varphi)(G_{j-1}) \oplus P_j(\varphi)(G_j) \cdots \oplus P_j(\varphi)(G_s)$$

Mais pour $1 \leqslant i \leqslant j-1$, puisque $P_i = Q_i$, $\varphi_{|E_i}$ est semblable à $\varphi_{|G_i}$ car ces endomorphismes sont respectivement semblables à C_{P_i} et C_{Q_i}. On en déduit $\dim P_j(\varphi)(F_i) = \dim P_j(\varphi)(G_i)$ soit, vu (2) et (1) :

$$0 = \dim P_j(\varphi)(G_j) = \cdots = \dim P_j(\varphi)(G_s)$$

qui implique que Q_j divise P_j et par symétrie P_j divise aussi Q_j soit $P_j = Q_j$ ce qui est absurde. Finalement $P_i = Q_i$ pour tout i (et $r = s$).

La forme matricielle dans l'énoncé du théorème est évidemment obtenue en considérant les bases associées à la décomposition $E = E_1 \oplus \ldots \oplus E_r$ dont on vient de démontrer l'existence. ■

Notations : Les matrices obtenues par la décomposition de Frobenius seront appelées **« réduites de Frobenius »** .

Remarques : ***Attention !*** *Alors qu'une matrice diagonale par blocs et dont chaque bloc est un bloc de Jordan est une réduite de Jordan, une matrice diagonale par blocs et dont les blocs sont des matrices de Frobenius n'est en général pas une réduite de Frobenius. Par exemple, la matrice* $M = \left(\begin{array}{ccc|cc} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$ *n'est pas une réduite de Frobenius. En effet, elle s'écrit encore* $M = \begin{pmatrix} C_{X^3-1} & 0 \\ 0 & C_{X^2} \end{pmatrix}$ *et* X^2 *ne divise pas* $X^3 - 1$*. En fait, son polynôme caractéristique* $X^5 - X^2$ *est aussi son polynôme minimal (tous ses sous-espaces propres sont de dimension* 1*) :* M *est cyclique et sa réduite de Frobenius est*

$$C_{X^5-X^2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

On peut d'ailleurs énoncer de manière plus précise :

Proposition 2 *Une matrice diagonale par blocs de Frobenius est cyclique si, et seulement si, deux blocs distincts sont sans valeur propre commune.*

Démonstration : Chaque fois qu'une valeur propre apparaît dans un bloc de Frobenius, la dimension du sous-espace propre correspondant est augmentée de 1. On utilise alors l'exercice 1.3 ■

Par exemple, la matrice blocs 4×4 : $\begin{pmatrix} C_{(X-1)(X-2)} & 0 \\ 0 & C_{(X-3)(X-4)} \end{pmatrix}$ est semblable à la matrice compagnon $C_{(X-1)(X-2)(X-3)(X-4)}$

2.3 Quelques propriétés topologiques

On s'intéresse dans ce paragraphe à la structure topologique de l'ensemble $\mathcal{C}_n$ des matrices cycliques (i.e. semblables à une matrice compagnon), $M_n(\mathbb{C})$ étant bien entendu muni de sa topologie d'espace vectoriel normé.

Proposition 3 $\mathcal{C}_n$ *est un ouvert connexe dense de* $M_n(\mathbb{C})$.

Démonstration : ▶ En effet, si $A \in \mathcal{C}_n$, il existe $x_0 \in \mathbb{C}^n$ tel que $\left(A^k x_0\right)_0^{n-1}$ soit une base de $\mathbb{C}^n$. Alors, l'application continue sur $M_n(\mathbb{C})$

$$\varphi_{x_0} \ : \ M_n(\mathbb{C}) \ni M \mapsto \varphi_{x_0}(M) := \det(x_0,\, Mx_0, \dots,\, M^{n-1}x_0)$$

vérifie donc $\varphi_{x_0}(A) \neq 0$. Par continuité de φ_{x_0} en A il existe $\delta > 0$ tel que $\varphi_{x_0}(M) \neq 0$ pour tout $M \in B(A, \delta)$ i.e. $B(A, \delta) \subset \mathcal{C}_n$ et $\mathcal{C}_n$ est bien ouvert.

▶ Pour la connexité, on aura toujours

$$A \in \mathcal{C}_n \iff \exists P \in GL_n(\mathbb{C}),\, \exists\, a = (a_0, \dots, a_{n-1}) \in \mathbb{C}^n \ : \ A = P^{-1} C_a P,$$

où C_a est la matrice compagnon associée au vecteur $a \in \mathbb{C}^n$ (cf. notations §1). Autrement dit, $\mathcal{C}_n = \psi(GL_n(\mathbb{C}) \times \mathbb{C}^n)$ avec

$$\psi \ : \ GL_n(\mathbb{C}) \times \mathbb{C}^n \ni (P, a) \mapsto \psi(P, a) := P^{-1} C_a P.$$

ψ est une application clairement continue de l'ouvert $GL_n(\mathbb{C}) \times \mathbb{C}^n$ connexe (comme produit des deux ouverts connexes $GL_n(\mathbb{C})$ et $\mathbb{C}^n$) : image continue d'un connexe, $\mathcal{C}_n$ est donc bien connexe.

▶ Il nous reste à établir la densité : mais il est bien connu (par exemple [8] page 51) que toute matrice de $M_n(\mathbb{C})$ est limite d'une suite de matrices à valeurs propres deux à deux distinctes donc semblables à des matrices de Frobenius. ■

Terminons par un petit corollaire[7] amusant :

Corollaire 1 *Si $n \geqslant 2$, l'application $\varphi \ : \ A \in M_n(\mathbb{C}) \mapsto \varphi(A) := \pi_A$ n'est pas continue.*

Démonstration : Supposons φ continue, il en sera alors de même pour

$$\psi \ : \ M_n(\mathbb{C}) \ni A \mapsto \psi(A) := p_A - \pi_A \in \mathbb{C}[X]$$

mais alors

$$\mathcal{C}_n = \{A \in M_n(\mathbb{C}) \ : \ p_A = \pi_A\} = \psi^{-1}(\{0_{\mathbb{C}[X]}\})$$

est fermé dans $M_n(\mathbb{C})$ comme image réciproque d'un fermé par une application continue. Nous avons vu plus haut que $\mathcal{C}_n$ est ouvert : c'est donc une partie à la fois ouverte, fermée, non vide du connexe $M_n(\mathbb{C})$, la seule alternative est $\mathcal{C}_n = M_n(\mathbb{C})$: égalité absurde si $n \geqslant 2$ et triviale si $n = 1$. ■

2.4 Propriétés spectrales

Étudions en détail les éléments propres d'une matrice compagnon C_P. Les valeurs propres de C_P sont bien entendu les zéros de P et la première observation que l'on peut faire est que :

[7] Consulter l'ouvrage de Rombaldi ([8] page 52) pour une preuve plus classique de ce résultat.

▶ **Les sous-espaces propres sont toujours de dimension 1** : tout cela est immédiat dès que l'on a observé que pour tout $\lambda \in \mathbb{C}$, le rang de la matrice

$$C_P - \lambda I_n = \begin{pmatrix} -\lambda & 0 & \dots & 0 & -a_0 \\ 1 & -\lambda & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & -\lambda - a_{n-1} \end{pmatrix}$$

est visiblement supérieur ou égal à $n-1$.

Remarque : *Tout ceci peut se déduire aussi du fait que pour une matrice compagnon, polynômes minimal et caractéristique coïncident exercice 1.2) mais ceci est plus savant.*

▶ Si **les racines de P sont toutes simples**, C_P est donc diagonalisable et on connait une base de vecteurs propres de sa transposée, car pour λ racine de P, si on pose

$$^t e_\lambda = (1, \lambda, \lambda^2, \dots, \lambda^{n-1})$$

on vérifie sans peine (en utilisant la relation $P(\lambda) = 0$ pour la dernière ligne) que

$$^t C_P e_\lambda = \lambda e_\lambda,$$

Ainsi $\lambda_1, \dots, \lambda_n$ désignant les n racines distinctes de P, la famille $\mathcal{B} = \{e_{\lambda_1}, \dots, e_{\lambda_n}\}$ est une base de vecteurs propres de $^t C_P$. En particulier, la matrice de passage G à la forme diagonale

$$^t C_P \ := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix} = G \operatorname{diag}(\lambda_1, \dots, \lambda_n)\, G^{-1}$$

est la transposée d'une matrice de Vandermonde :

$$^t G = V(\lambda_1, \dots, \lambda_n) = \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \dots & \lambda_2^{n-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \dots & \lambda_n^{n-1} \end{pmatrix}$$

▶ Dans le cas où **les racines de P ne sont pas toutes simples**, on peut écrire
$P(X) = \displaystyle\prod_{i=1}^{d} (X - \lambda_i)^{\alpha_i}$ (les racines $\lambda_1, \dots, \lambda_d$ étant deux à deux distinctes) avec disons $\alpha_1 \geqslant 2$. Vu ce qui précède, $\dim(E_{\lambda_1}) = \dim(\operatorname{vect}(e_{\lambda_1})) = 1 < \alpha_1$: C_P n'est donc pas diagonalisable, mais on peut toutefois en étudiant plus en détail la famille des vecteurs propres $e_{\lambda_1}, \dots, e_{\lambda_d}$ déterminer la matrice de passage pour la forme de Jordan de $^t C_P$: en effet, si

$$e(\lambda) := {}^t(1, \lambda, \lambda^2, \dots, \lambda^{n-1}),$$

il n'est pas difficile (en utilisant cette fois-ci les relations $P^{(k)}(\lambda_i) = 0,\ 0 \leqslant k \leqslant \alpha_i - 1$) de vérifier[8] que la matrice de passage de ${}^tC_P$ à sa forme de Jordan est

$$G = \left(e(\lambda_1), e'(\lambda_1), \frac{e''(\lambda_1)}{2!} \dots, \frac{e^{(\alpha_1-1)}(\lambda_1)}{(\alpha_1-1)!}, \dots, e(\lambda_d), \dots, \frac{e^{(\alpha_d-1)}(\lambda_d)}{(\alpha_d-1)!} \right)$$

En résumé nous avons

1) Les sous-espaces propres d'une matrice compagnon sont toujours de dimension 1, elle est donc diagonalisable si et seulement si ses valeurs propres sont deux à deux distinctes.
2) Dans ce cas, la matrice de passage à la forme diagonale de sa transposée est la matrice de Vandermonde associée à ces valeurs propres.
3) Dans le cas contraire on a tout de même la forme explicite de la matrice de passage de sa transposée à sa réduite de Jordan.

3 APPLICATIONS À L'ALGÈBRE LINÉAIRE

Le théorème de décomposition de Frobenius est essentiel. Il est en fait une conséquence de la théorie des invariants de similitude dans tout anneau principal factoriel. Ici, l'anneau est $\mathbb{K}[X]$ et, en particulier, ceci signifie que la réduction de Frobenius est valable pour tout corps $\mathbb{K}$ commutatif.

3.1 Le Théorème de Cayley-Hamilton

La conclusion du théorème de décomposition nous dit que $P_\varphi = P_1 P_2 ... P_r$ avec $P_1 = \pi_\varphi$; par conséquent :

Théorème 2 (Cayley-Hamilton) *Pour tout* $\varphi \in \mathrm{End(E)}$*, on a* $P_\varphi(\varphi) = 0$.

On notera également la démonstration classique et plus élémentaire (sans recourir au théorème de décomposition) du théorème de Cayley-Hamilton reposant également sur l'usage des matrices compagnons :
Démonstration : On cherche à montrer que $P_A(A)x = 0$ pour tout x. Soit donc x un vecteur non nul de $\mathbb{C}^n$ (si $x = 0$ il n'y a rien a démontrer) notons $\mathcal{E}_x$ le plus petit (au sens de l'inclusion) sous-espace stable par A de $\mathbb{C}^n$ contenant x. $\mathcal{E}_x$ est de dimension $d \in \{1, \dots, n\}$, et admet pour base $\{x, Ax, \dots, A^{d-1}x\}$: il existe $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{C}^n$ tel que

$$(\bigstar) \qquad A^d x = a_{d-1}A^{d-1}x + \cdots + a_1 Ax + a_0 x.$$

[8] L. Brand *« The Companion matrix and its properties »*, Amer.Math.Monthly (1964), 629-634. et *« Applications of the companion matrix »* ibid. (1968), 146-152.

Complétons alors la famille libre $\{x, Ax, \ldots, A^{d-1}x\}$ pour obtenir une base de $\mathbb{C}^n$ de la forme

$$\{x, Ax, \ldots, A^{d-1}x, e_{d+1}, \ldots, e_n\}$$

Dans cette base la matrice A est de la forme $\begin{pmatrix} C_P & Z \\ 0 & B \end{pmatrix}$ où $B \in M_{n-d}(\mathbb{C}), Z \in M_{d,n-d}(\mathbb{C})$ et C_P est la matrice compagnon du polynôme $P(X) = X^d - a_{d-1}X^{d-1} - \cdots - a_1X - a_0$ i.e. :

$$C_P = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & a_{n-1} \end{pmatrix}.$$

on a donc $P_A(X) = P_{C_P}(X)P_B(X)$, mais alors

$$\begin{aligned} P_A(A)x &= P_{C_P}(A)P_B(A)x \\ &= P_B(A)P_{C_P}(A)x \\ &= P_B(A)(A^dx - a_{d-1}A^{d-1}x - \cdots - a_1Ax - a_0x) = 0 \text{ vu } \quad (\bigstar) \end{aligned}$$

dans la seconde inégalité les deux endomorphismes $P_{C_P}(A)$ et $P_B(A)$ commutent comme polynômes en A. Ainsi $P_A(A)x = 0,\ \forall x \in \mathbb{C}^n$ i.e. $P_A \equiv 0$. ■

Remarque : *En suivant la même idée, on montre tout aussi élémentairement que pour une matrice cyclique, polynômes minimal et caractéristiques coïncident, le théorème de Cayley-Hamilton est déja établi pour une matrice cyclique, on achève la preuve soit en utilisant le théorème 1, soit par un argument de densité (proposition 3).*

3.2 Décomposition de Jordan

La décomposition de Jordan est bien connue ; mais on peut la voir aussi comme une conséquence de la décomposition de Frobenius :

Théorème 3 *Soit $\varphi \in \mathrm{End(E)}$ avec P_φ scindé sur $\mathbb{K}$. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u est diagonale par blocs de Jordan :*

$$M(\varphi, \mathcal{B}) = \begin{pmatrix} J(\lambda_1) & & & \mathit{0} \\ & J(\lambda_2) & & \\ & & \ddots & \\ \mathit{0} & & & J(\lambda_k) \end{pmatrix}$$

où $\lambda_1, \ldots, \lambda_m$ sont les valeurs propres (éventuellement avec répétitions) de φ.

Démonstration : Le théorème de décomposition donne **directement** la décomposition de Jordan dans le cas d'un endomorphisme **nilpotent** (modulo une permutation des vecteurs de base de la forme $(e_1, \ldots, e_k) \mapsto (e_k, e_{k-1}, \ldots, e_2, e_1)$ dans chacun des sous-espaces stables apparaissant dans la décomposition de l'endomorphisme nilpotent φ).

Dans le cas général, supposons que φ admet m valeurs propres distinctes $\lambda_1, \ldots, \lambda_m$ et que $P_\varphi(X) = (X - \lambda_1)^{l_1} \ldots (X - \lambda_m)^{l_m}$. D'après le lemme des noyaux, $E = \bigoplus_{i=1}^{m} F_i$ avec $F_i = \mathrm{Ker}\,(\varphi - \lambda_i \mathrm{Id}_E)^{l_i}$ et on peut alors appliquer le cas précédent aux restrictions de $u - \lambda_i \mathrm{Id}_E$ à F_i, pour i allant de 1 à m. On obtient ainsi la décomposition de Jordan. ■

Remarque : *La décomposition de Jordan repose sur la décomposition de l'espace total en somme de sous-espaces caractéristiques (autrement dit, elle raisonne valeur propre par valeur propre) tandis que la décomposition de Frobenius, qui repose sur les polynômes invariants, « mélange » les valeurs propres. Il s'agit d'une distinction essentielle.*

En particulier, pour une matrice M (à polynôme caractéristique scindable), le nombre de blocs Jordan (de sa réduite de Jordan) est supérieur ou égal au nombre de blocs Frobenius (de sa réduite de Frobenius). Plus précisément, ces deux nombres ne sont égaux que dans le cas où M n'admet qu'une seule valeur propre (et ils sont alors, « respectivement », de même taille). Par exemple, la décomposition de Frobenius de $\begin{pmatrix} a & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & 0 & a & 1 \\ 0 & 0 & 0 & a \end{pmatrix}$ *est* $\begin{pmatrix} 0 & 0 & 0 & -a^4 \\ 1 & 0 & 0 & 4a^3 \\ 0 & 1 & 0 & -6a^2 \\ 0 & 0 & 1 & 4a \end{pmatrix}$ *ou encore (en notant Frob(M) la réduite de Frobenius de M) :*

$$M = \left(\begin{array}{ccc|ccc|cc|c} a & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & a & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & a & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \end{array}\right)$$

et

$$\mathit{Frob}(M) = \left(\begin{array}{ccc|ccc|cc|c} 0 & 0 & a^3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -3\,a^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3\,a & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & a^3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -3\,a^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3\,a & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & -a^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2\,a & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \end{array}\right)$$

En particulier, $M = aI_n$ (où I_n est la matrice identité d'ordre n) est le cas très particulier de matrices qui sont à la fois des réduites de Jordan et de Frobenius (autrement dit, si M a ses réduites de Frobenius et de Jordan identiques alors M est un multiple (non nul) de l'identité). Par contre, dès que M possède au moins deux valeurs propres distinctes, le nombre de blocs de Jordan *(de la réduite de Jordan) est strictement supérieur au nombre de blocs Frobenius (de la réduite de Frobenius). De ce point de vue, le cas extrême est le cas où M admet n valeurs propres (M étant une matrice carrée d'ordre n) deux à deux distinctes. Dans ce cas là, la matrice diagonale (formée par les valeurs propres) est la décomposition de Jordan de M (qui est donc formée de n blocs d'ordre 1) alors que la réduite de Frobenius de M ne compte qu'un seul bloc. Par exemple, pour $n = 4$ et $M = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix}$, on obtient $frob(M) = \begin{pmatrix} 0 & 0 & 0 & -abcd \\ 1 & 0 & 1 & abc+abd+acd+bcd \\ 0 & 1 & 0 & -(ab+ac+ad+bc+bd+cd) \\ 0 & 0 & 1 & a+b+c+d \end{pmatrix}$ lorsque a, b, c et d sont deux à deux distincts (on voit naturellement apparaître dans les coefficients de $(X-a)(X-b)(X-c)(X-d)$ les polynômes symétriques sur lesquels nous reviendrons plus loin).*

De manière générale, on peut facilement voir que l'on peut connaître la réduite de Jordan d'une matrice dont on connaît la réduite de Frobenius à condition de tenir compte de la multiplicité de chacune des racines des invariants de similitude (i.e., des valeurs propres de la matrice). Réciproquement, on peut trouver les invariants de similitude (et donc la réduite de Frobenius) d'une matrice à partir de sa réduite de Jordan et des suites de Segré attachées à chaque valeur propre.

3.3 Matrices semblables

Théorème 4 *Deux endomorphismes sont semblables si, et seulement si, ils ont les mêmes invariants de similitude.*

Démonstration : Deux matrices A, B dans $\mathcal{M}_n(\mathbb{K})$ sont semblables s'il existe une matrice $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $A = P^{-1}BP$. Notons u et v les endomorphismes de $\mathbb{K}^n$ de matrices respectives A et B dans la base canonique ; on a donc $u = f^{-1} \circ v \circ f$ où f est un automorphisme de $\mathbb{K}^n$. Dans cette situation, si $P_1, \ldots, P_r$ est la suite des invariants de similitude de u ($\mathbb{K}^n = \bigoplus_{i=1}^{r} E_i$, $u_{|E_i}$ est cyclique et de polynôme minimal P_i), on a également $\mathbb{K}^n = \bigoplus_{i=1}^{r} f(E_i)$. De plus, la relation de similitude implique que pour tout Q de $\mathbb{K}[X]$, on a $f(Q(u)(x)) = Q(v)(f(x))$ et on en déduit que les $f(E_i)$ sont v-stables, que P_i est aussi le polynôme minimal de $v_{|f(E_i)}$ et que $v_{|f(E_i)}$ est cyclique. Ainsi A et B ont mêmes invariants de similitude. Réciproquement, si A et B sont deux matrices ayant mêmes invariants de similitude, le théorème de décomposition de Frobenius montre qu'elles sont semblables. ■

En « petite dimension », cela se traduit par :

Corollaire 2 *Pour $n \leqslant 3$, deux endomorphismes sont semblables si, et seulement si, ils ont mêmes polynômes minimal et caractéristique.*
Pour $n \geqslant 4$ l'implication non triviale est fausse.

Démonstration : Soient $P_1, \ldots, P_k$ les polynômes associés à la décomposition de Frobenius de notre endomorphisme. Il est alors facile de constater que pour $n \leqslant 3$ la donnée de P_1 et le produit $P_1 \ldots P_k$ (avec P_{i+1} divise P_i) détermine complétement la suite $(P_i)_1^k$. Par contre, si $n \geqslant 4$, il est possible de construire deux suites distinctes $(P_i)_1^k$ et $(Q_i)_1^l$ avec $P_1 = Q_1$ et $P_1 \ldots P_k = Q_1 \ldots Q_l$. Par exemple, les deux matrices 4×4 ci-dessous ont même polynômes caractéristique et minimal mais ne sont pas semblables au vu de l'unicité dans le théorème de décomposition (elles correspondent aux suites de polynômes X^2, X^2 et X^2, X, X) :
$\begin{pmatrix} C_{X^2} & 0 \\ 0 & C_{X^2} \end{pmatrix}$ et $\begin{pmatrix} C_{X^2} & 0 & 0 \\ 0 & C_X & 0 \\ 0 & 0 & C_X \end{pmatrix} \in M_4(\mathbb{R})$. ∎

Exercice 2 *1) Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$. Si M et N sont des matrices de $\mathcal{M}_n(\mathbb{K})$ semblables dans $\mathcal{M}_n(\mathbb{L})$, alors elles sont semblables dans $\mathcal{M}_n(\mathbb{K})$.*
2) Soit $M \in \mathcal{M}_n(\mathbb{K})$ et $\mathbb{L}$ une extension du corps $\mathbb{K}$. On a alors $\pi_{\mathbb{K},M} = \pi_{\mathbb{L},M}$.

3.4 Matrice transposée

Il est bien connu que

Théorème 5 *Toute matrice est semblable à sa transposée.*

La preuve est immédiate à partir du théorème de décomposition (les invariants de similitude étant les mêmes). On notera que la démonstration « classique » de ce résultat repose sur la réduction de Jordan (il en en effet facile de montrer que toute matrice de Jordan est semblable à sa transposée), de manière duale il est tout aussi facile de prouver qu'une matrice compagnon est semblable à sa transposée (et cela fournit une autre preuve de ce corollaire à partir de la réduction de Frobenius) : si

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}, \quad S = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} & 1 \\ a_2 & a_3 & \ldots & 1 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ a_{n-1} & 1 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix} \in GL_n(\mathbb{C}),$$

alors

$$AS = \begin{pmatrix} -a_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & a_2 & a_3 & \dots & a_{n-1} & 1 \\ 0 & a_3 & a_4 & \iddots & 1 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & a_{n-1} & 1 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

est une matrice symétrique et par conséquent $AS = {}^t\!(AS) = S({}^tA)$ i.e. $A = S({}^tA)S^{-1}$.

Il est intéressant de remarquer dans la formule ci-dessus que la matrice de passage de A à sa transposée est symétrique. Le théorème suivant clarifie ce fait

Théorème 6
1) Pour toute matrice carrée réelle, il existe une matrice de passage à sa transposée qui soit symétrique.
*2) Les matrices de passage d'une matrice $A \in M_n(\mathbb{K})$ à sa transposée sont **toutes** symétriques si, et seulement si, la matrice A est cyclique.*

Démonstration : 1) Comme toute matrice compagnon admet une matrice symétrique de passage à sa transposée, il en résulte que toute matrice de Frobenius (i.e. une matrice constituée de blocs diagonaux cycliques) F admet aussi une matrice de passage à sa transposée S symétrique réelle ($F = SAS^{-1}$). Vérifions maintenant que cette propriété se généralise à **toutes** les matrices.
Maintenant avec le théorème de décomposition de Frobenius, toute matrice $A \in M_n(\mathbb{R})$ est semblable à une matrice de Frobenius : il existe donc $P \in GL_n(\mathbb{R}), S \in \mathcal{S}_n(\mathbb{R}) \cap GL_n(\mathbb{R})$ et F matrice de Frobenius, telles que

$$A = PFP^{-1}, \quad F = S\,{}^tFS^{-1}.$$

Ainsi

$$\begin{aligned} A = P(S\,{}^tFS^{-1})P^{-1} &= (PS)({}^tP\,{}^tP^{-1})\,{}^tF({}^tP\,{}^tP^{-1})(S^{-1}P^{-1}) \\ &= (PS\,{}^tP)({}^tP^{-1}\,{}^tF\,{}^tP)({}^tP^{-1}S^{-1}P^{-1}) \\ &= (PS\,{}^tP)\,{}^tA({}^tP^{-1}S^{-1}P^{-1}) \\ &= (PS\,{}^tP)\,{}^tA(PS\,{}^tP)^{-1} = S_1\,{}^tAS_1^{-1} \end{aligned}$$

où $S_1 = PS\,{}^tP$. La matrice de passage S_1 est clairement symétrique, nous avons donc démontré que pour toute matrice $A \in M_n(\mathbb{R})$, il existe une matrice de passage symétrique S telle que $A = S\,{}^tAS^{-1}$.

2) Pour la seconde propriété, voir[9] O. Taussky & H. Zassenhaus « On the similarity tranformation between a matrix and its transpose » Pacific J. Math. (9) 1959. ■

[9]Nous remercions notre collègue J.B. Hiriart-Urruty (Université Paul Sabatier, Toulouse) pour nous avoir communiqué cette référence.

Terminons par un corollaire intéressant[10]

Corollaire 3 *Toute matrice carrée réelle est le produit de deux matrices symétriques réelles.*

Démonstration : Vu ce qui précède, on peut écrire

$$A = SS', \quad \text{où} \quad S' = {}^t\!AS^{-1}$$

et comme

$${}^t(S') = {}^t({}^t\!AS^{-1}) = {}^t\!S^{-1}A = S^{-1}S\,{}^t\!AS^{-1} = {}^t\!AS^{-1} = S'$$

S' est symétrique et le tour est joué puisque $A = SS'$ ■

3.5 Commutant et bicommutant

Soit $u \in \mathrm{End(E)}$ où E est un $\mathbb{K}$-espace vectoriel de dimension n. On rappelle que :

$$\mathrm{Com}(u) = \{v \in \mathrm{End(E)}\ :\ \mathrm{u \circ v = v \circ u}\}$$

$$\mathrm{Bicom}(u) = \{v \in \mathrm{End(E)}\ :\ \mathrm{v \circ w = w \circ v}\ ,\ \forall\, \mathrm{w \in Com(u)}\} \subset \mathrm{Com}(u)$$

sont, respectivement, le commutant et le bicommutant de u. Si M est la matrice de u (peu importe le choix de la base de E), on a bien sûr les définitions similaires de $\mathrm{Com}(M)$ et $\mathrm{Bicom}(M)$.

3.5.1 Le commutant

Théorème 7 *Soit $u \in \mathrm{End(E)}$ où E est un $\mathbb{K}$-espace vectoriel de dimension n. On a alors :*

1) $\dim \mathrm{Com}(u) \geqslant n$.

2) $\dim \mathrm{Com}(u) = n$ *si, et seulement si, u est cyclique.*

Démonstration : 1) Soit $\begin{pmatrix} C_{P1} & & & 0 \\ & C_{P_2} & & \\ & & \ddots & \\ 0 & & & C_{P_k} \end{pmatrix}$ la décomposition de Frobenius de u, $P_1P_2\ldots P_k$ est le polynôme caractéristique de u, $\deg(P_1) +$

[10] Voir aussi la « question-réponse 544 » RMS 116-2.

$\deg(P_2)+\ldots+\deg(P_k)=n$ et il est clair que l'ensemble des matrices diagonales par blocs :

$$\begin{pmatrix} {\scriptstyle 0} & & & & & & \\ & \ddots & & & & 0 & \\ & & {\scriptstyle 0} & & & & \\ & & & C_{P_i}^{i_j} & & & \\ & & & & {\scriptstyle 0} & & \\ & 0 & & & & \ddots & \\ & & & & & & {\scriptstyle 0} \end{pmatrix} \qquad \text{avec } \begin{cases} i=1,\ldots,k \\ i_j=1,\ldots,\deg(P_i)-1 \end{cases}$$

$$\text{et } \ C_P^l = \underbrace{C_P\times\ldots\times C_P}_{l \text{ fois } C_P}$$

est une famille libre $\mathcal{H}$ formée de n vecteurs appartenant à $\mathrm{Com}(u)$ et ceci prouve que $\dim \mathrm{Com}(u)\geqslant n$.

2) Supposons u cyclique et soit x un vecteur cyclique pour u (i.e. $\{x,u(x),\ldots, u^{n-1}(x)\}$ est une base de E). Alors tout v de $\mathrm{Com}(T)$ est entièrement déterminé par $v(x)$ (puisque $v(u^i(x))=u^i(v(x))$, pour tout $1\leqslant i\leqslant k$) et l'application linéaire de $\mathrm{Com}(u)$ dans E donnée par

$$u\longmapsto u(x)$$

est injective. Ceci prouve que $\dim\mathrm{Com}(u)\leqslant n$ et en tenant compte de (1), on conclut que $\dim\mathrm{Com}(u)=n$ lorsque u est cyclique.

Supposons à présent que u ne soit pas cyclique ; en reprenant les notations de la partie (1), il faut montrer que $\mathrm{Com}(M)$ contient au moins un élément qui n'est pas dans $\mathrm{Vect}(\mathcal{H})$. Sans perte de généralité, on peut supposer $k=2$ (u n'est pas cyclique) ; il existe alors une base $\mathcal{B}$ de E telle que

$$M_{\mathcal{B}}(u)=\begin{pmatrix} C_{PQ} & 0 \\ 0 & C_P \end{pmatrix}$$

où PQ et P^2Q sont respectivement les polynômes minimal et caractérsitique de u. Il est connu que E est muni naturellement d'une structure de $\mathbb{K}[u]$-module (et si $v\in\mathrm{End}_{\mathbb{K}}(E)$, dire que v commute avec u signifie que v est $\mathbb{K}[u]$-linéaire). Cela se traduit par l'existence de $x,y\in E$ tels que

$$E=\mathbb{K}[u](x)\oplus\mathbb{K}[u](y)\overset{\Phi}{\simeq}\mathbb{K}[X]/PQ\times\mathbb{K}[X]/P$$

En notant π la surjection canonique $\mathbb{K}[X]/PQ\to\mathbb{K}[X]/P$, l'application

$$\begin{array}{rccc} L: & \mathbb{K}[X]/PQ\times\mathbb{K}[X]/P & \to & \mathbb{K}[X]/PQ\times\mathbb{K}[X]/P \\ & (S,R) & \mapsto & (0,\pi(S)) \end{array}$$

induit, via l'isomorphisme Φ, une application $\mathbb{K}[X]$-linéaire $\tilde{L}\in\mathrm{End}_{\mathbb{K}}(\mathrm{E})$. Par conséquent, $\tilde{L}\in\mathrm{Com}(u)$ et sa matrice dans la base $\mathcal{B}$ est de la forme

$$M_{\mathcal{B}}(\tilde{L})=\begin{pmatrix} 0 & 0 \\ C & 0 \end{pmatrix}.$$

Visiblement $M_{\mathcal{B}}(\tilde{L}) \notin \mathrm{Vect}(\mathcal{H})$, ce qui achève la preuve du théorème. $\blacksquare$

Remarques : ***1.*** *Il est clair que* $\mathbb{K}[u] \subset \mathrm{Com}(u)$ *pour tout endomorphisme* u *et on a donc* $\mathrm{Com}(u) = \mathbb{K}(u)$ *si, et seulement si,* u *est cyclique.*

2. *On notera le principe de la preuve lorsque u n'est pas cyclique : dire que* M *n'est pas une matrice compagnon revient à dire que la décomposition de Frobenius de* M *comprend* **au moins** *deux blocs compagnon. Par exemple, si cette décomposition comprend exactement deux blocs, i.e. si elle s'écrit :* $\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$*, l'idée est de chercher une matrice de la forme* $\left(\begin{array}{c|c} 0 & 0 \\ \hline C & 0 \end{array}\right)$ *telle que :*

$$(*) \qquad \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) \left(\begin{array}{c|c} 0 & 0 \\ \hline C & 0 \end{array}\right) = \left(\begin{array}{c|c} 0 & 0 \\ \hline C & 0 \end{array}\right) \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$$

et ceci est équivalent à avoir $BC = CA$*. En particulier, la fin de la preuve du théorème montre l'existence d'une telle matrice* $\left(\begin{array}{c|c} 0 & 0 \\ \hline C & 0 \end{array}\right)$ *que l'on notera* L_C *avec de plus la propriété que* C *est de rang maximum (c'est la matrice d'une application surjective). Cette propriété supplémentaire interviendra de façon cruciale dans la preuve du théorème 8.*

3.5.2 Approche topologique de la dimension du commutant

De la structure topologique de l'ensemble des matrices cycliques et de la semi-continuité inférieure de l'application rang, il n'est pas difficile de donner une preuve plus élémentaire de la première assertion du théorème précédent.

Pour toute matrice $A \in M_n(\mathbb{C})$ *son commutant* Com*(A) est un sous-espace vectoriel de* $M_n(\mathbb{C})$ *de dimension au moins* n*.*

Démonstration : Soit $A \in M_n(\mathbb{C})$, on a l'inclusion évidente $\mathbb{C}[A] \subset \mathrm{Com}(A)$; mais, si A est cyclique $\mathbb{C}[A] = \mathrm{vect}\{ I_n, A, \dots, A^{n-1}\}$ est (lemme fondamental) de dimension n. Par ailleurs, l'ensemble des matrices cycliques $\mathcal{C}_n$ est (paragraphe 2.3) ouvert dense dans $M_n(\mathbb{C})$. Par transitivité de la densité, il sera donc suffisant de montrer que l'ensemble

$$F := \{ A \in M_n(\mathbb{C}) \ : \ \dim \mathrm{Com}(A) \geqslant n\} \supset \mathcal{C}_n$$

est fermé dans $M_n(\mathbb{C})$. Pour établir ce dernier point, considérons, si $A \in M_n(\mathbb{C})$, l'endomorphisme $\varphi_A \in \mathcal{L}(M_n(\mathbb{C}))$ défini par $\varphi_A(B) = AB - BA$. Puisque $\mathrm{Ker}(\varphi_A) = \mathrm{Com}(A)$,

$$F = \{ A \in M_n(\mathbb{C}) \ : \ \mathrm{rang}(\varphi_A) \leqslant n^2 - n\}.$$

Sous cette forme, il est n'est pas difficile de vérifier que F est fermé dans $M_n(\mathbb{C})$: soit $A \in \overline{F}$, il existe dans F une suite $(A_k)_k$ de limite A, ce qui implique aussitot : $\lim_k \varphi_{A_k} = \varphi_A$. Montrer que $A \in F$ est maintenant une conséquence immédiate de la semi-continuité inférieure de l'application rang en dimension finie, précisément :

> *Pour tout espace vectoriel E de dimension finie d et tout entier $1 \leqslant k \leqslant d$, les ensembles de niveau $\mathcal{R}_k = \{T \in \mathcal{L}(E)\ :\ rang(T) \leqslant k\}$ sont fermés dans $\mathcal{L}(E)$.*

En effet, pour $T \in \overline{\mathcal{R}_k}$, $(T_l)_l \subset \mathcal{R}_k$ de limite T : si $r = \text{rang(T)}$, la matrice T admet un mineur $\Delta_r(T)$ non nul et par continuité : $\lim_l \Delta_r(T_l) = \Delta_r(T) \neq 0$. Il existe donc l_0 tel que $l \geqslant l_0$ implique $\Delta_r(T_l) \neq 0$; autrement dit :

$$\forall l \geqslant l_0\ :\ k \geqslant \text{rang}(T_l) \geqslant r$$

i.e. $k \geqslant r \implies T \in F$. Le résultat suit avec $T = \varphi_A,\ T_l = \varphi_{A_l}$. ■

3.5.3 Le bicommutant

Théorème 8 *Soit $u \in \text{End}_{\mathbb{K}}(\text{E})$ où E est un $\mathbb{K}$-espace vectoriel de dimension n. On a alors*[11] *:*

$$\text{Bicom}(u) = \mathbb{K}[u]$$

En particulier, $\dim \text{Bicom}(u) = n$ *si, et seulement si, u est cyclique.*

Démonstration : L'inclusion $\mathbb{K}[u] \subset \text{Bicom}(u)$ est toujours vraie. Montrons l'inclusion inverse.

▷ Pour u cyclique, elle est immédiate puisque $\text{Bicom}(u) \subset \text{Com}(u) = \mathbb{K}[u]$ (cf. remarque après le théorème 7).

▷ Considérons à présent le cas où u n'est pas cyclique. Comme dans la preuve du théorème précédent, on peut supposer que $E = \mathbb{K}[u](x) \oplus \mathbb{K}[u](y)$ avec $\dim \mathbb{K}[u](x) = n_1$ (c'est le degré du polynôme minimal de u) et $\dim \mathbb{K}[u](y) = n_2$ (avec $1 \leqslant n_2 \leqslant n_1$ et $n_1 + n_2 = n$). En fait, on va démontrer le résultat (équivalent) $\text{Bicom}(M) \subset \mathbb{K}(M)$ où

$$M := M_{\mathcal{B}}(u) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) \quad \text{avec} \quad A \in \mathcal{M}_{n_1}(\mathbb{K}),\ B \in \mathcal{M}_{n_2}(\mathbb{K})$$

est la décomposition de Frobenius de u dans la base

$$\mathcal{B} = \{x, u(x), \dots, u^{n_1-1}(x), y, u(y), \dots, u^{n_2-1}(y)\}.$$

Le résultat s'ensuit alors de calculs très élémentaires. Pour tout $v \in \text{End}_{\mathbb{K}}(\text{E})$, on écrira ? ?

$$M_{\mathcal{B}}(v) = \left(\begin{array}{c|c} X & Y \\ \hline Z & W \end{array}\right)$$

avec $X \in \mathcal{M}_{n_1}(\mathbb{K})$, $W \in \mathcal{M}_{n_2}(\mathbb{K})$, $Y \in \mathcal{M}_{n_1,n_2}(\mathbb{K})$ et $Z \in \mathcal{M}_{n_2,n_1}(\mathbb{K})$.

Soit $N = \left(\begin{array}{c|c} X & Y \\ \hline Z & W \end{array}\right) \in \mathrm{Bicom}(u)$. La matrice $\left(\begin{array}{c|c} \mathrm{Id}_{n_1} & 0 \\ \hline 0 & 0 \end{array}\right)$ est dans $\mathrm{Com}(u)$ et

$$\left(\begin{array}{c|c} X & Y \\ \hline Z & W \end{array}\right)\left(\begin{array}{c|c} \mathrm{Id}_{n_1} & 0 \\ \hline 0 & 0 \end{array}\right) = \left(\begin{array}{c|c} \mathrm{Id}_{n_1} & 0 \\ \hline 0 & 0 \end{array}\right)\left(\begin{array}{c|c} X & Y \\ \hline Z & W \end{array}\right)$$

i.e.

$$\left(\begin{array}{c|c} X & 0 \\ \hline Z & 0 \end{array}\right) = \left(\begin{array}{c|c} X & Y \\ \hline 0 & 0 \end{array}\right)$$

montre que nécessairement $Z = 0$ et $Y = 0$. Par conséquent, $N = \left(\begin{array}{c|c} X & 0 \\ \hline 0 & W \end{array}\right)$ est diagonale par blocs. De plus, N commute avec M et ceci signifie que $X \in \mathrm{Com}(A)$ et $W \in \mathrm{Com}(B)$ d'après le théorème précédent, on obtient $N = \left(\begin{array}{c|c} \Pi_1(A) & 0 \\ \hline 0 & \Pi_2(B) \end{array}\right)$ où Π_1 et Π_2 sont des polynômes. A présent le calcul de NL_C et L_CN (où L_C est la matrice de la remarque qui suit le théorème 5) :

$$\left(\begin{array}{c|c} \Pi_1(A) & 0 \\ \hline 0 & \Pi_2(B) \end{array}\right)\left(\begin{array}{c|c} 0 & 0 \\ \hline C & 0 \end{array}\right) = \left(\begin{array}{c|c} 0 & 0 \\ \hline \Pi_2(B)C & 0 \end{array}\right)$$

et

$$\left(\begin{array}{c|c} 0 & 0 \\ \hline C & 0 \end{array}\right)\left(\begin{array}{c|c} \Pi_1(A) & 0 \\ \hline 0 & \Pi_2(B) \end{array}\right) = \left(\begin{array}{c|c} 0 & 0 \\ \hline C\Pi_1(A) & 0 \end{array}\right)$$

montre que $C\Pi_1(A) = \Pi_2(B)C$ puisque $N \in \mathrm{Bicom}(M)$. Par ailleurs, comme $L_C \in \mathrm{Com}(M)$, on a $BC = AC$ et on en déduit que $\Pi_1(B)C = \Pi_2(B)C$ et finalement $\Pi_1(B) = \Pi_2(B)$ car C est de rang maximum. On a ainsi montré que

$$N = \left(\begin{array}{c|c} \Pi_1(A) & 0 \\ \hline 0 & \Pi_2(B) \end{array}\right) = \Pi(M) \quad \text{avec } \Pi \in \mathbb{K}[X]$$

i.e., que $\mathrm{Bicom}(M) \subset \mathbb{K}[M]$. Ceci achève la preuve de $\mathrm{Bicom}(M) = \mathbb{K}[M]$ ou, de façon équivalente, $\mathrm{Bicom}(u) = \mathbb{K}[u]$. ■

3.5.4 Quelques précisions sur la dimension du commutant

Au vu du Théorème 7, on a pour toute matrice $A \in M_n(\mathbb{C})$ l'encadrement :

$$n \leqslant \dim \mathrm{Com}(A) \leqslant n^2$$

et la dimension vaut n si, et seulement si A est cyclique et n^2 si et seulement si A est un multiple la matrice identité. La question se pose alors de savoir si la dimension du commutant peut prendre toutes les valeurs comprises entre n et n^2.

Par exemple, pour $n = 2$, un raisonnement sur le nombre $k \in \{1, 2\}$ de blocs Frobenius dans la réduite de Frobenius d'une matrice A permet de conclure immédiatement que $\dim \mathrm{Com}(A) \in \{2, 4\}$ et que $\dim \mathrm{Com}(A) = 3$ est impossible

; en effet, si $k = 1$, A est cyclique et $\dim \mathrm{Com}(A) = 2$ (théorème 5) et si $k = 2$, $A = \lambda \mathrm{Id}$ et $\dim \mathrm{Com}(A) = 4$.

Ce raisonement sur le nombre de blocs Frobenius de la réduite de Frobenius d'une matrice se généralise au cas d'une dimension quelconque et le résultat suivant montre que la dimension du commutant ne dépend que du nombre et de la taille[12] des blocs Frobenius.

Avant d'énoncer ce résultat, fixons les notations. On prend toujours $u \in \mathrm{End}_{\mathbb{K}}(\mathrm{E})$ où E est un $\mathbb{K}$-espace vectoriel de dimension n. Soit k le nombre de blocs Frobenius de la réduite de Frobenius de u et p_1, p_2, ..., p_k les tailles respectives de ces blocs avec $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_k$. On a bien entendu :

$$p_1 + p_2 + \ldots + p_k = n$$

i.e., la suite d'entiers $\mathcal{P} = (p_1, p_2, \ldots, p_k)$ est une partition de n que l'on appellera *partition associée à u*. À une partition $\mathcal{P} = (p_1, p_2, \ldots, p_k)$ d'un entier n est associé son *diagramme de Young* : c'est simplement le dessin de k lignes, la ième ligne comprenant p_i « cases » ou « points ». Par exemple voici les diagrammes de Young : $\begin{array}{llll}\bullet&\bullet&\bullet&\bullet\\ \bullet&\bullet&&\\ \bullet&&&\end{array}$ et $\begin{array}{llll}\bullet&\bullet&\bullet&\bullet\\ \bullet&\bullet&\bullet&\end{array}$ qui correspondent respectivement aux partitions $(4, 2, 1)$ et $(4, 3)$ de 7. On définit alors la partition conjuguée (ou duale) de $\mathcal{P}$ de la manière suivante : si l'on voit le diagramme de Young de $\mathcal{P}$ comme une matrice (à k lignes et p_1 colonnes), la transposée de cette matrice définit une autre partition de n qui est, *par définition*, la partition duale $\mathcal{P}^*$ de $\mathcal{P}$. Par exemple, dans les deux exemples précédents, on obtient $\begin{array}{lll}\bullet&\bullet&\bullet\\ \bullet&\bullet&\\ \bullet&&\\ \bullet&&\end{array}$ et $\begin{array}{ll}\bullet&\bullet\\ \bullet&\bullet\\ \bullet&\bullet\\ \bullet&\end{array}$, ce qui signifie que $(4, 2, 1)^* = (3, 2, 1, 1)$ et $(4, 3)^* = (2, 2, 2, 1)$. On peut noter encore $(1, 1, \ldots, 1)^* = (n)$, la partition $(1, 1, \ldots, 1)$ correspondant à une matrice multiple de l'identité et la partition (n) correspondant à une matrice cyclique : ce sont les deux « situations extrêmes ».

On peut à présent énoncer le résultat annoncé[13].

Théorème 9 *Soit $u \in \mathrm{End}_{\mathbb{K}}(\mathrm{E})$ où E est un $\mathbb{K}$-espace vectoriel de dimension n et $\mathcal{P} = (p_1, p_2, \ldots, p_k)$ sa partition associée. Alors,* $\dim(\mathrm{Com}(u)) = q_1^2 + q_2^2 + \ldots + q_l^2$ *où $(q_1, q_2, \ldots, q_l)$ est la partition conjuguée de $\mathcal{P}$.*

On notera simplement ici (voir [3] pour une peuve détaillée) que ce résultat met en avant l'intérêt de la décomposition de Frobenius. En particulier, il existe un énoncé « équivalent » (cf. [1]) que l'on obtient à partir de la décomposition

[12] Une matrice carrée à k lignes est dite de *taille k*.

[13] Cf. Question-Réponse 338 (RMS 9/10, 1998/99) pour un énoncé partiel de ce résultat.

de Jordan mais dont l'énoncé (à partir des suites de Segré) est beaucoup plus fastidieux.

Une conséquence immédiate de ce résultat concerne la codimension du commutant[14] :

Corollaire 4 *La codimension du commutant d'un endomorphisme est paire.*

Démonstration : Avec les notations du théorème précédent, $\operatorname{codim}\operatorname{Com}(A) = n^2 - \dim\operatorname{Com}(A) = (q_1 + \cdots + q_l)^2 - q_1^2 - \cdots - q_l^2 = 2 \sum_{1\leqslant i<j\leqslant l} q_i q_j$. ■

On terminera ce paragraphe sur la dimension du commutant en évoquant un joli petit exercice déniché dans un vieux numéro de la RMS ; la question était de déterminer la structure de l'ensemble $\mathcal{E}$ des endomorphismes $\varphi \in \mathcal{L}(M_n(\mathbb{R}))$ vérifiant

$$\varphi({}^tB) = {}^t\varphi(B), \quad \forall\, B \in M_n(\mathbb{R}).$$

Si on désigne par T l'endomorphisme $M \mapsto {}^tM$ de $M_n(\mathbb{R})$, $\mathcal{E}$ n'est rien d'autre que le commutant de T et c'est donc une sous-algèbre de $\mathcal{L}(M_n(\mathbb{R}))$. Soit $\mathcal{S}_n$ (resp. $\mathcal{A}_n$) l'espace vectoriel des matrices symétriques (resp. antisymétrique). Puisque $M_n(\mathbb{R}) = \mathcal{S}_n \oplus \mathcal{A}_n$, un endomorphisme φ vérifiant $\varphi \circ T = T \circ \varphi$ doit laisser stable les deux sous-espaces propres de T que sont $\mathcal{S}_n$ et $\mathcal{A}_n$. Mais inversement, un endomorphisme laissant stable $\mathcal{S}_n$ et $\mathcal{A}_n$ satisfait (avec les notations évidentes) à

$${}^t\varphi(B) = {}^t\varphi(S+A) = {}^t\varphi(S)+{}^t\varphi(A) = \varphi(S)-\varphi(A) = \varphi(S-A) = \varphi\left({}^t(S+A)\right) = \varphi({}^tB)$$

ce qui montre que $\varphi \in \mathcal{E}$. L'algèbre $\mathcal{E}$ est donc constituée des endomorphismes de $M_n(\mathbb{R})$ qui laissent stables les sous-espaces $\mathcal{S}_n$ et $\mathcal{A}_n$. Il existe donc un isomorphisme évident

$$\mathcal{E} \longrightarrow \mathcal{L}(\mathcal{S}_n) \times \mathcal{L}(\mathcal{A}_n)$$

qui à φ associe le couple $\left(\varphi_{|\mathcal{S}_n}, \varphi_{|\mathcal{A}_n}\right)$. Il en résulte que

$$\dim\mathcal{E} = \left(\frac{n(n+1)}{2}\right)^2 + \left(\frac{n(n-1)}{2}\right)^2 = \frac{n^2(n^2+1)}{2}.$$

Cette dernière formule illustre le théorème 9 et le théorème 7, en retour, nous informe que l'opérateur de transposition n'est pas cyclique car $\dfrac{n^2(n^2+1)}{2} > n^2$ dès que $n > 1$.

[14]Pour une autre approche, consulter l'exercice 15, RMS 9/10, 2000/2001.

4 AUTRES APPLICATIONS MATHÉMATIQUES

4.1 Polynômes de Sylvester

Par **polynôme de Sylvester** on entend tout polynôme $P \in \mathbb{Z}[X]$ unitaire à racines de module inférieur où égal à 1. Nous allons voir comment les matrices compagnon permettent de prouver simplement que les racines non nulles de tout polynôme de Sylvester de degré n sont des racines n-ièmes de l'unité ; ce théorème est dû à Kronecker[15]. On pourra aussi consulter les ouvrages de J.M. Arnaudies & J. Bertin[16] ou E. Leichnam[17] pour d'autres approches.
Pour $n \in \mathbb{N}^\star$, l'ensemble des polynômes d3 & 19 ? ?e Sylvester de degré n sera noté S_n et $s_n := \#S_n$ désignera le nombre de polynômes de Sylvester de degré n.

Théorème 10 (Kronecker) *Les zéros non nuls d'un polynôme de Sylvester sont des racines de l'unité.*

Démonstration : Soit $n \in \mathbb{N}^\star$. Notons Z_n l'ensemble de tous les zéros (comptés avec leurs multiplicités) des polynômes de Sylvester de degré inférieur ou égal à n.

► Pour $n \in \mathbb{N}^\star$: s_n est fini.

Si $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 = \prod_{i=1}^{n}(z - \zeta_i) \in S_n$, par les formules de Newton si on a pour $0 \leqslant k \leqslant n-1$

$$|a_k| = \Big| \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^k \zeta_{i_1} \dots \zeta_{i_k} \Big| \leqslant \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |\zeta_{i_1} \dots \zeta_{i_k}| \leqslant C_n^k \leqslant n!,$$

mais les coefficients a_k sont dans $\mathbb{Z}$ et par conséquent s_n est fini.

► $(\ \zeta \in Z_n) \implies \left(\ \zeta^k \in Z_n,\ \forall\, k \in \mathbb{N}\right)$

Soit $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, sa matrice compagnon

$$C_p = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix} \in M_n(\mathbb{Z})$$

[15] *Zwei Sätze über Gleichungen mit ganzzahligen Coeffienten*, Crelle, Oeuvres **1** (1857) 105-108.
[16] [1], T.1, pages 127-128.
[17] E. Leichnam *« Exercices corrigés de Mathématiques, Polytechnique, ENS » (Algèbre et Géométrie)*, exercice 1-30, Ellipse, (1999)

est triangularisable dans $M_n(\mathbb{C})$, il existe $G \in GL_n(\mathbb{C})$ vérifiant $C_p = G^{-1}\begin{pmatrix} \zeta_1 & * & \dots & * \\ & \ddots & \ddots & \vdots \\ 0 & & \ddots & * \\ & & & \zeta_n \end{pmatrix} G$. Mais alors $C_p^N = G^{-1}\begin{pmatrix} \zeta_1^N & * & \dots & * \\ & \ddots & \ddots & \vdots \\ 0 & & \ddots & * \\ & & & \zeta_n^N \end{pmatrix} G \in M_n(\mathbb{Z})$, autrement dit C_p^N est une matrice à coefficients dans $\mathbb{Z}$ qui admet $\zeta_1^N, \dots \zeta_n^N$ comme valeurs propres : son polynôme caractéristique répond à la question.

► *Conclusion :* Supposons qu'il existe un polynôme $p \in S_n$ admettant au moins une racine, disons ζ_1, qui ne soit ni racine de l'unité, ni de module strictement compris entre 0 et 1, l'ensemble $\{\zeta_1^N\}_{N\in\mathbb{N}^\star}$ est alors de cardinal **infini**. D'autre part, par la seconde étape $p_{C_p^N}(\zeta_1^N) = 0,\ \forall N \in \mathbb{N}^\star$, si bien que l'ensemble infini $\{\zeta_1^N\}_{N\in\mathbb{N}^\star}$ est inclu dans Z_n de cardinal **fini** (étape 1) soit la contradiction désirée, le théorème est démontré. ■

Remarques : 1) *On peut tout aussi bien montrer qu'un polynôme de Sylvester est sans zéros de module strictement compris entre* 0 *et* 1 *de la manière suivante : soit* $p(z) = z^k \prod_{i=k+1}^{n} (z - \zeta_i) \in K_n$, *toujours avec Newton :* $1 \leqslant |a_k| = |\zeta_{k+1} \dots \zeta_n| \leqslant 1$, *soit* $|\zeta_{k+1}| = \dots = |\zeta_n| = 1$.
2) Un **entier algébrique** *est une racine d'un polynôme unitaire* $P(X) = X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0 \in \mathbb{Z}[X]$. *Avec les mêmes méthodes que dans la démonstration du théorème de Kronecker, on peut démontrer le résultat suivant :* ***Un entier algébrique est soit entier, soit irrationnel.***

4.2 Les formules de Newton

Ces célèbres formules relient les coefficients d'un polynôme aux fonctions symétriques de ses racines. Il existe de nombreuses démonstrations, celle que nous proposons ici est peu connue[18], elle repose à travers les matrices compagnon sur le calcul matriciel et le théorème de Cayley-Hamilton.
Soit $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - r_1)\dots(x - r_n) \in \mathbb{C}[x]$, et posons pour $k \in \mathbb{N}^\star$: $s_k := \sum_{j=1}^{n} r_j^k$. Les formules de Newton sont

$$(\bigstar) \qquad \begin{aligned} s_k + s_{k-1}a_{n-1} + \dots + s_{k-n}a_0 &= 0 & \quad & k > n, \\ s_k + s_{k-1}a_{n-1} + \dots + s_1 a_{n-k+1} &= -ka_{n-k} & & 1 \leqslant k \leqslant n. \end{aligned}$$

[18] www.american.edu/academic.depts/cas/mathstat/ People/kalman/pdffiles/newtonsID.pdf

Pour établir ces formules, considérons la matrice compagnon $C \in M_n(\mathbb{C})$ de P. Il est bien connu

$$\forall\, k \geqslant 1 \quad \mathrm{tr}(C^k) \,=\, s_k,$$

ainsi, pour $k > n$ les formules de Newton s'écrivent aussi sous la forme

$$\mathrm{tr}(C^k) + a_{n-1}\mathrm{tr}(C^{k-1}) + \cdots + a_0\mathrm{tr}(C^{k-n}) \,=\, 0,$$

mais, par linéarité de la trace

$$\begin{aligned}\mathrm{tr}\big(C^k + a_{n-1}C^{k-1} \cdots + a_0 C^{k-n}\big) &= \mathrm{tr}\big(C^{k-n}(C^n + a_{n-1}C^{n-1} + \cdots + a_0 I_n)\big)\\ &= \mathrm{tr}\big(C^{k-n}P(C)\big)\\ &= 0\end{aligned}$$

puisque (Cayley-Hamilton) $P(C) \,=\, 0$.

Passons maintenant au cas où $1 \leqslant k \leqslant n$, il s'agit cette fois de montrer

$$\mathrm{tr}(C^k) + a_{n-1}\mathrm{tr}(C^{k-1}) + \cdots + a_{n-k+1}\mathrm{tr}(C) \,=\, -k a_{n-k},$$

soit encore

$$\mathrm{tr}\big(C^k + a_{n-1}C^{k-1} + \cdots + a_{n-k+1}I_n\big) \,=\, (n-k)a_{n-k},$$

mais on considère la famille de polynômes $Q_{n-k}(X) \,=\, X^k + a_{n-1}X^{k-1} + \cdots + a_{n-k+1}$, $(1 \leqslant k \leqslant n)$, la formule précédente devient

$$\mathrm{tr}(Q_{n-k}(C)) \,=\, (n-k)a_{n-k},$$

et on a la relation de récurrence

$$Q_{n-k}(C) \,=\, CQ_{n-k+1}(C) + a_{n-k}I_n$$

qui ($Q_0(C) \,=\, P(C) \,=\, 0$) si $k = 0$, s'écrit $0 \,=\, CQ_1(C) + a_0 I_n$. Un petit calcul (vu la formule de récurrence) nous montre que les $Q_{n-k}(C)$ sont précisement les coefficients qui apparaissent lorsque l'on divise dans $M_n(\mathbb{C})$ $P(X)$ par $X - C$ en particulier

$$P(xI_n) \,=\, \big(xI_n - C\big)\big(x^{n-1}I_n + x^{n-2}Q_{n-1}(C) + \cdots + xQ_2(C) + Q_1(C)\big).$$

Désirant prendre la trace dans la formule précédente, commençons par éliminer le facteur $(xI_n - C)$ (la trace passe mal au produit). Pour cela, si x n'est pas valeur propre de C, la matrice $xI_n - C$ est inversible, et

$$x^{n-1}I_n + x^{n-2}Q_{n-1}(C) + \cdots + xQ_2(C) + Q_1(C) \,=\, (xI_n - C)^{-1}P(xI_n),$$

soit

$$nx^{n-1} + \mathrm{tr}\big(x^{n-2}Q_{n-1}(C) + \cdots + xQ_2(C) + Q_1(C)\big) \,=\, \mathrm{tr}\big((xI_n - C)^{-1}P(xI_n)\big)$$

et il ne reste plus qu'à remarquer que puisque $P(xI_n) = P(x)I_n$

$$\begin{aligned}\operatorname{tr}\big((xI_n - C)^{-1}P(xI_n)\big) &= P(x)\operatorname{tr}\big((xI_n - C)^{-1}\big)\\ &= P(x)\sum_{j=1}^{n}\frac{1}{x-r_j}\\ &= P'(x) \qquad \forall\, x \in \mathbb{C}\setminus \operatorname{spect}(C)\end{aligned}$$

i.e.

$$nx^{n-1} + \operatorname{tr}\big(x^{n-2}Q_{n-1}(C) + \cdots + xQ_2(C) + Q_1(C)\big) = P'(x), \qquad \forall\, z \in \mathbb{C}\setminus\operatorname{spect}(C)$$

$\mathbb{C}\setminus\operatorname{spect}(C)$ étant un ouvert connexe dense du plan complexe, cette dernière égalité s'étend à $\mathbb{C}$ tout entier. Il ne reste plus alors qu'à identifier les coefficients des deux polynômes pour terminer la démonstration. ■

4.3 Localisation des racines d'un polynôme

À toute norme $||.||$ sur $\mathbb{C}^n$ on associe de manière naturelle une norme sur $M_n(\mathbb{C})$ par $|||A||| := \sup_{||x||=1}||Ax||$. Pour une telle norme c'est un exercice élémentaire de montrer que le rayon spectral $\rho(A) := \max\{|\lambda|,\ \lambda$ valeur propre de $A\}$ de A vérifie

$$\rho(A) \leqslant |||A|||.$$

Ainsi différents choix de normes fourniront différentes estimations du rayon spectral d'une matrice, et via les matrices compagnon on pourra donc obtenir en fonction de ses coefficients une majoration du module des racines d'un polynôme. En voici quelque unes, certaines sont élémentaires pour les autres nous renvoyons à [6] §5.6 et sa bibliographie. En outre si $a_0 \neq 0$ les racines de $q(z) = \dfrac{1}{a_0}z^n p(z^{-1})$ étant les inverses de celles de p, on peut donc les minorer et localiser ainsi les racines du polynôme dans une couronne centrée à l'origine. Voici quelques exemples
Soit donc $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{C}[X]$ et $z^\star$ un zéro de p avec la norme $\|.\|_1$ on obtient l'estimation de **Cauchy**

$$\boxed{\frac{|a_0|}{|a_0| + \max\{1, |a_1|, \ldots, |a_{n-1}|\}} \leqslant |z^\star| \leqslant 1 + \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}}$$

avec la norme $\|.\|_\infty$ on obtient l'estimation de **Montel**

$$\boxed{|a_0|\,(1 + |a_0| + |a_1| + \ldots, |a_{n-1}|) \leqslant |z^\star| \leqslant \max\{1, |a_0| + |a_1| + \cdots + |a_{n-1}|\}}$$

Enfin avec la norme $\|.\|_2$ on a l'estimation de **Carmichael-Manson**

$$\boxed{\frac{|a_0|}{\{1+|a_0|^2+|a_1|^2+\dots,|a_{n-1}|^2\}^{1/2}} \leqslant |z^\star| \leqslant (1+|a_0|^2+|a_1|^2+\dots+|a_{n-1}|^2)^{1/2}}$$

4.4 Quelques dernières applications

Les applications des matrices compagnon sont nombreuses et nous pourrions continuer encore longtemps, citons en vrac quelques derniers exemples :

▶ Il est bien connu[19] que les matrices compagnon permettent de déterminer facilement la structure de l'ensemble des solutions d'une équation différentielle linéaire : nous n'insisterons donc pas plus sur ce sujet (même remarque pour les suites récurrentes).

▶ Récemment[20] Harm Derksen montre en utilisant **uniquement** des outils d'Algèbre linéaire que tout endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension paire admet au moins une valeur propre, il en résulte aussitot, via les matrices compagnon, que tout polynôme de degré pair admet au moins une racine. Le cas du degré impair étant conséquence élémentaire[21] du théorème des valeurs intermédiaires : le théorème de d'Alembert-Gauss est donc démontré.

▶ Les matrices compagnon jouent encore un rôle essentiel autour du résultant et des matrices de Barnett, une raison de plus pour consulter le remarquable ouvrage de Prasolov [7] qui sera bientot traduit en francais...

▶ Un changement de base préserve la trace, et les éléments diagonaux d'une matrice ne sont donc pas complétement arbitraires. Le théorème de Gibson ([7] page 81) assure que toute matrice A distincte de λI_n est semblable à une matrice dont les éléments diagonaux sont $(0,\dots,\mathrm{tr}(A))$. La matrice compagnon déjà de la forme requise permet donc de réduire la démonstration aux matrices à polynômes minimal et caractéristique distincts ce qui se fait sans trop de peine.

▶ Dans[22] on trouve l'étude de l'ensemble $E := \{\, A \in M_n(\mathbb{C})$ telles que $\deg(\pi_A) = n-1\}$ (on pourrait dire que ce sont des matrices *presques* cycliques) où les matrices compagnon jouent un rôle essentiel. Dans le même ouvrage l'exercice 19 page 54 présente une trés élégante approche de la continuité « coefficients-racines » via les matrices compagnon attribuée à B. Randé.

[19] C. Deschamps & A. Warusfel, *« Mathématiques* 2^e *année », ch.23, Dunod (2001)* ou J.P. Demailly, *« Analyse numérique et équations différentielles », ch.7, Grenoble Sciences, (1991).*

[20] H. Derksen *« The Fundamental Theorem of Algebra and Linear Algebra »*, Amer.Math.Monthly **110** (2003), 620-623.

[21] Quitte à considérer $z \mapsto P(z)\overline{P(\bar z)}$ on peut supposer que $P \in \mathbb{R}[X]$.

[22] R. Mneimné & F. Testard *« Introduction à la théorie des groupes de Lie classiques »*, Hermann (1986), p.40

► La lecture du remarquable ouvrage de J. Fresnel [5], est des plus conseillée, on y trouvera de nombreuses précisions et beaucoup d'exercices. La même remarque vaut pour la RMS : depuis quelques années les matrices compagnon ont fait un retour remarqué dans les épreuves écrites de certains concours et sont aussi la source (de manière plus ou moins explicite) de nombreux exercices d'oral.

5 UNE APPLICATION « CONCRÈTE »

L'approche matricielle pour l'automatisation des systèmes physiques date d'une cinquantaine d'années. Elle a été fortement induite par l'émergence de systèmes de grande dimension et à ce titre l'aéronautique et le spatial constituent des terrains d'applications par excellence. Qu'il s'agisse des premières commandes de vol électriques inaugurées sur le Concorde ou bien du pilotage des avions gros porteurs de nouvelles générations tel le A380, la définition des lois de commande requiert l'usage de représentation matricielles pour la maîtrise de l'évolution dynamique des grandeurs pilotées. C'est un formalisme particulièrement adapté au contrôle des systèmes multidimensionnels, c'est-à-dire possédant plusieurs entrées et plusieurs sorties, eut égard à la nécessité de réaliser des opérations en temps réel avec des temps de calcul compatibles avec les organes de calcul. Bon nombre de systèmes physiques, peuvent aisément se représenter sous la forme différentielle suivante[23] :

$$(\bigstar) \qquad \begin{cases} x'(t) &= A\,x(t) + B\,u(t), \\ y(t) &= C\,x(t). \end{cases}$$

Où $A, C \in M_n(\mathbb{R}),\ B \in \mathbb{R}^n,\ x, y \in \mathcal{C}^1(\mathbb{R}, \mathbb{R}^n),\ u \in \mathcal{C}(\mathbb{R}, \mathbb{R})$. Cette forme fait apparaitre la notion d'état par l'intermédiaire de $x(t)$, nommé vecteur d'état qui représente l'information minimale relative au passé afin de calculer l'évolution future. Outre la stabilité, liée à l'existence de valeurs propres pour A strictement négatives, nous pouvons caractériser ce système par deux propriétés fondamentales que sont la **commandabilité** et **l'observabilité**. Elles doivent être nécessairement vérifiées pour piloter toutes les composantes du système avec un nombre minimum de capteurs. Elles sont définies comme suit :

▷ Un état x_i est **commandable** en t_0 s'il est possible de déterminer $u(t)$ sur $[t_0, t_f]$, $(t_0 \leqslant t_f < \infty)$ amenant tout état initial $x_i(t_0)$ vers un état x_f défini à l'avance en temps borné. Si cette propriété est vraie pour tout t_0 et pour tout x_i alors le système est dit **commandable** ou **gouvernable**.

▷ Un état x_i est **observable** en t_0 s'il est possible de déterminer $x_i(t_0)$ en connaissant y sur $[t_0, t_f]$ avec $t_0 \leqslant t_f < \infty$. Si cette propriété est vraie pour tout t_0 et pour tout x_i alors le système est dit **observable**.

[23] Nous nous placons ici bien entendu dans un cas simple, c'est-à-dire linéaire ou linéarisé

R.E. Kalman a démontré que la propriété de commandabilité ne dépend que de la paire (A, B) et que la propriété d'observabilité ne dépend que de la paire (A, C) et il a formulé les critères éponymes suivants :

Critères de KALMAN : Une condition nécessaire et suffisante pour que le système (★) soit commandable (resp. observable) est que le rang de la matrice $Q_c = (B \ AB \ A^2B \ \ldots \ A^{n-1}B)$ (resp. $Q_o = (C \ CA \ CA^2 \ \ldots \ CA^{n-1})$) soit maximal c'est-à-dire égal à n ; en d'autres termes A est une matrice cyclique admettant B (resp. C) comme vecteur cyclique.

Donnons juste ([4]) une idée de la démarche dans le cas d'un système discret[24] :

$$\begin{cases} X(k+1) & = A\,X(k) + B\,u(k) \\ Y(k) & = C\,X(k) \end{cases}$$

et l'évolution du vecteur d'état sur un horizon N est donnée par

$$X(N) = A^N(X(0)) + \sum_{k=0}^{N-1} A^{N-1-k}Bu(k)$$

soit

$$X(N) = A^N(X(0)) + (B \ AB \ A^2B \ \ldots \ A^{n-1}B \ A^nB \ \ldots \ A^{N-1}B) \begin{pmatrix} u(N-1) \\ \vdots \\ u(0) \end{pmatrix}.$$

Sans perte de généralité on peut imaginer le recalage à l'origine soit $X(N) = 0$

$$(B \ \ AB \ \ A^2B \ \ \ldots \ \ A^{n-1}B \ \ A^nB \ \ \ldots \ \ A^{N-1}B) \begin{pmatrix} u(N-1) \\ \vdots \\ u(0) \end{pmatrix} = -A^N(X(0))$$

La dimension de l'état étant n, si $N < n$, il n'existe pas de solution pour U, l'horizon de commmande étant trop faible, par contre si $N > n$, il est possible d'exprimer les colonnes $A^nB, \ldots, A^{N-1}B$ en fonction des précédentes en vertu du théorème de Cayley Hamilton. Ainsi le rang maximal de $(B \ AB \ A^2B \ \ldots \ A^{n-1}B \ A^nB \ \ldots \ A^{N-1}B)$ ne peut excéder celui de Q_c et le système sera commandable si le rang de Q_c est maximal c'est-à-dire égal à n. ■

En matière de synthèse de lois de commande et d'observateurs, l'usage des formes compagnes (i.e., des matrices compagnon) s'avère d'un intérêt majeur

[24]La théorie du contrôle était le thème des Journées X-UPS en 1999, le lecteur intéressé trouvera l'intégralité des actes de ces journées sur le lien : http ://math.polytechnique.fr/xups/vol99.html

par la simplicité du calcul qui en découle. Dans un cas, il s'agit de déterminer le vecteur $K \in \mathbb{R}^n$ pour imposer les valeurs propres de $A - B\,{}^tK$ et dans l'autre cas, le vecteur $L \in \mathbb{R}^n$ pour imposer les valeurs propres de $A - LC$. Le placement des valeurs propres est quelquefois utilisé pour stabiliser un système lorsque les valeurs propres naturelles sont à parties réelles positives, mais plus souvent il est mis en place pour accélérer la dynamique d'évolution afin de réduire le temps de réponse du dispositif et plus rarement il constitue un moyen pour ralentir l'évolution des variables quand des critères de qualité l'exigent.
Dans la base canonique compagne de commande (resp. la base canonique compagne d'observation) nous obtenons les formes suivantes :

$$\widetilde{A}_c = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix} , \ \widetilde{B}_c = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

et

$$\widetilde{A}_o = \begin{pmatrix} -a_{n-1} & 1 & 0 & \dots & 0 \\ -a_{n-2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ -a_1 & 0 & \dots & 0 & 1 \\ -a_0 & 0 & \dots & 0 & 0 \end{pmatrix} , \ \widetilde{C}_o = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

Les matrices de changement de base M_c (resp. M_o) sont établies en explicitant les n relations déduites de $M_c^{-1} A M_c = \widetilde{A}_c$ (resp. $M_o^{-1} A M_o = \widetilde{A}_o$). La matrice $\widetilde{A}_c - \widetilde{B}_c\,\widetilde{{}^tK}$(resp. $\widetilde{A}_o - \widetilde{L}\widetilde{C}_c$) **reste**[25] **sous une forme compagne**. Ainsi si l'on souhaite imposer le polynôme caractéristique : $D(\lambda) = \lambda^n + \gamma_{n-1}\lambda^{n-1} + \ldots + \gamma_1\lambda + \gamma_0$, il vient les solutions simples suivantes : $\widetilde{k}_i = \gamma_i - a_i$ pour $0 \leqslant i \leqslant n-1$ (resp. $\widetilde{l}_i = \gamma_i - a_i$, $0 \leqslant i \leqslant n-1$). La solution dans la base physique est alors obtenue par ${}^tK = \widetilde{{}^tK} M_c^{-1}$(resp. $L = M_o^{-1}\widetilde{L}$).

Il est à noter que la propriété de commandabilité assure l'existence de M_c^{-1}, et que la propriété d'observabilité assure l'existence de M_o^{-1}. Le problème du placement de valeurs propres se ramène ainsi au calcul du polynôme caractéristique, d'une matrice de changement de base et de son inverse. Cette procédure simple est liée à l'utilisation des formes compagnes. Sur le plan algorithmique, cette méthode en simplifiant le calcul des matrices de bouclage L et K, constitue une solution hautement performante dans le domaine des systèmes électroniques embarqués où il est nécessaire d'allier rapidité et faible encombrement de la mémoire. A titre comparatif la procédure de calcul basée sur les formes compagnes amène un gain en temps et de stabilité de calcul par rapport à la formulation classique d'Ackermann dans un rapport n.

[25]car vu la forme du vecteur $\widetilde{B}_c$ seule la dernière ligne de la matrice $\widetilde{A}_c - \widetilde{B}_c\,\widetilde{{}^tK}$ est modifiée.

6 CONCLUSION

Ce travail prenant des proportion déraisonnables, il est plus que temps de conclure. Nous n'avons pas traité l'approche algorithmique qui est un volet essentiel de la théorie mais nous renvoyons le lecteur à l'article de Bernard Randé « Un algorithme pour la décomposition en espaces cycliques » RMS, (4) 2005.

Références

[1] J.M. Arnaudiés & J. Bertin *« Groupes, Algèbre et Géométrie »*, Ellipse, (1993) t.1 & 3.

[2] S. Barnett *« Matrices in Control Theory »*, Van Nostrand Reinhold, London 1971.

[3] H. Carrieu, E. Fieux & P. Lassère, *« Notes sur les décompositions de Frobenius et de Jordan »*, travail en cours, 2004.

[4] G.F. Franklin & J.D. Powell *« Digital Control of Dynamics Systems »* , Addison-Wesley publishing Company (1980).

[5] J. Fresnel *« Algèbre des Matrices »* Hermann University Press (1999).

[6] R.A. Horn & C.R. Johnson *« Matrix Analysis »* Cambridge (1997).

[7] V.V. Prasolov *« Problems and Theorems in Linear Algebra »* Translations of mathematical monographs vol **134**. American Mathematical Society (1994).

[8] J.E. Rombaldi *« Analyse Matricielle, Cours et Exercices Résolus »*, EDP sciences (1999).

[9] J.H. Wilkinson *« The Algebraic Eigenvalue Problem »*, Clarendon Press. Oxford (1965).

Hervé Carrieu : Lycée Camille GUÉRIN, 86000 POITIERS FRANCE. herve.carrieu@ac-poitiers.fr
Maurice Fadel : LEEI/ENSEEIHT 2 rue Charles Camichel 31071 BP 7119 Toulouse Cedex 7 FRANCE. maurice.fadel@leei.enseeiht.fr
Etienne Fieux & Lassère Patrice : Laboratoire de Mathématiques, E.Picard UMR CNRS 5580, Université Paul Sabatier, 119 route de Narbonne, 31062 TOULOUSE FRANCE. fieux@picard.ups-tlse.fr & lassere@picard.ups-tlse.fr
Frédéric Rodriguez : Laboratoire du CERS, UMR CNRS 5177, Université Toulouse II, 5, allées Antonio Machado, 31058 TOULOUSE Cedex 9. frederic.rodriguez@univ-tlse2.fr