Mémoire de M2 - Préparation à l'agrégation
Université de Rennes 1 - ENS Rennes

153 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

Gurvan Mével
encadré par Lionel Fourquaux

Table des matières

Introduction

Réduire un endomorphisme, c'est chercher une base de l'espace vectoriel dans laquelle il s'exprime simplement. Cela permet de l'étudier plus efficacement : son comportement, ses éléments propres, les sous-espaces qu'il laisse stables,... L'intérêt est aussi pratique : les calculs se font plus simplement avec une matrice diagonale ou avec une forme de Jordan qu'en toutes généralités.

La question se pose alors : sous quelles conditions peut-on réduire un endomorphisme, et de quelles réductions disposons-nous ? Nous verrons ici plusieurs outils pour répondre à ces problèmes.

Les polynômes d'endomorphismes, tout d'abord, sont un élément central dans notre étude. L'étude de l'algèbre des polynômes en un endomorphisme u permet de dégager des polynômes annulateurs, parmi lesquels le polynôme minimal. Celui-ci est porteur d'informations sur u, et est l'objet d'un premier critère de diagonalisation. La manipulation des polynômes minimaux permet également d'aboutir à la réduction de Frobenius, qui classifie complètement les classes de similitudes des endomorphismes.

D'autres outils apparaissent avec les éléments propres. Définis à partir du polynôme caractéristique de u, qui par ailleurs est un polynôme annulateur, ils conduisent également à des critères de diagonalisation et trigonalisation. La réduction de Jordan met en évidence des propriétés des valeurs propres et de leurs multiplicités.

Il est également possible de réduire simultanément des endomorphismes, sous couvert de commutativité. Les éléments propres jouent un rôle dans la démonstration de ces résultats. Une généralisation est donnée par le théorème de Lie-Kolchin, qui établit un lien entre sous-groupes résolubles de $\mathrm{GL}_n(\mathbb{C})$ et sous-groupes cotrigonalisables.

Nous évoquons pour finir la décomposition de Dunford. Ce n'est pas à proprement parler une réduction, mais elle permet néanmoins d'obtenir des résultats. Son intérêt réside également dans le fait qu'elle fait apparaître des polynômes en l'endomorphisme qu'on étudie.

Le plan repris ici est celui présenté devant la classe, agrémenté d'exemples supplémentaires et de plus de détails. Des remarques ont également été ajoutées, tirées de l'échange qui a suivi la présentation de la leçon.

Notations

On désigne par $\mathbb{K}$ un corps et par E un $\mathbb{K}$-espace vectoriel de dimension finie n. On note $\mathcal{L}(E)$ l'ensemble des applications linéaires de E dans E. Quand ce n'est pas précisé, u désigne un élément de $\mathcal{L}(E)$.

1 Polynômes d'endomorphismes

1.1 L'algèbre $\mathbb{K}[u]$

Étant donné u un endomorphisme de E, on note $u^2 = u \circ u$ et, plus généralement, pour $n \in \mathbb{N}^*$ on note $u^n = u \circ ... \circ u$ où le symbole $\circ$ apparaît $n-1$ fois. Pour un polynôme $P = \sum_{k=0}^{n} a_k X^k$, on note donc

$$P(u) = \sum_{k=0}^{n} a_k u^k \in \mathcal{L}(E).$$

Définition 1.1. L'application $\mathrm{ev}_u \left| \begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{L}(E) \\ P & \mapsto & P(u) \end{array} \right.$ s'appelle le morphisme d'évaluation en u. Son image est notée $\mathbb{K}[u]$ et s'appelle l'algèbre des polynômes en l'endomorphisme u.

Proposition 1.2. $(\mathbb{K}[u], +, \cdot, \circ)$ est une $\mathbb{K}$-algèbre commutative.

Puisque $\mathbb{K}[X]$ est de dimension infinie alors que $\mathcal{L}(E)$ est de dimension finie n^2, l'application ev_u ne peut pas être injective. Son noyau est donc un idéal non-nul de $\mathbb{K}[X]$. Or, l'anneau $\mathbb{K}[X]$ est principal. Ainsi, $\ker(\mathrm{ev}_u)$ admet un unique générateur unitaire.

Définition 1.3. Le polynôme minimal π_u de u est l'unique générateur unitaire de $\ker(\mathrm{ev}_u)$. On a donc $\ker(\mathrm{ev}_u) = \langle \pi_u \rangle$.

Exemple.
- ▷ Si u est une homothétie de rapport $\lambda \in \mathbb{K}$, alors $\pi_u = X - \lambda$. Réciproquement, si $\deg(\pi_u) = 1$, alors u est une homothétie.
- ▷ Si u est nilpotent, alors il existe $\mathbb{K} \in \mathbb{N}$ tel que $\pi_u = X^k$. Réciproquement, si π_u a cette forme, alors u est nilpotent.

Remarque. Tout endomorphisme de E (avec E de dimension finie) admet un polynôme minimal. C'est faux en dimension infinie.

Contre-exemple. La dérivation des polynômes $D \left| \begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{R}[X] \\ P & \mapsto & P' \end{array} \right.$ n'a pas de polynôme minimal. En effet, supposons qu'elle en admette un, notons le π_D. Soit $n = \deg(\pi_D)$ et notons $\pi_D = X^n + \sum_{k=0}^{n-1} a_k X^k$. Alors pour tout polynôme P, $P^{(n)} + \sum_{k=0}^{n-1} a_k P^{(k)} = 0$. Pour $P = X^n$, cela donne $n! = 0$, ce qui est absurde.

En revanche, la restriction $D_n : \mathbb{R}_n[X] \to \mathbb{R}_{n-1}[X]$ admet X^{n+1} comme polynôme minimal : en effet, elle est nilpotente d'indice $n+1$.

Nous décrivons maintenant quelques propriétés de $\mathbb{K}[u]$ vu en tant qu'algèbre, espace vectoriel ou anneau.

Proposition 1.4. On a un isomorphisme de $\mathbb{K}$-algèbres $\mathbb{K}[u] \simeq \mathbb{K}[X]/\langle \pi_u \rangle$. En particulier, la dimension en tant que $\mathbb{K}$-espace vectoriel de $\mathbb{K}[u]$ est $\dim(\mathbb{K}[u]) = \deg(\pi_u)$.

Proposition 1.5. L'anneau $\mathbb{K}[u]$ vérifie les propriétés suivantes.

1. Les inversibles de $\mathbb{K}[u]$ sont les $P(u)$ avec $P \wedge \pi_u = 1$.
2. $\mathbb{K}[u]$ est un corps $\Leftrightarrow$ $\mathbb{K}[u]$ est un intègre $\Leftrightarrow$ π_u est irréductible.
3. Les idéaux de $\mathbb{K}[u]$ sont de la forme $\langle P(u) \rangle$ où P divise π_u.
4. Les nilpotents de $\mathbb{K}[u]$ sont les $P(u)$ tels qu'il existe $m \in \mathbb{N}$ tel que π_u divise P^m, c'est-à-dire tels que les facteurs irréductibles de π_u (sans compter les multiplicités) sont des facteurs irréductibles de P.
5. Les idempotents de $\mathbb{K}[u]$ sont les $P(u)$ tels que π_u divise $P^2 - P$, c'est-à-dire tels que les facteurs irréductibles de π_u (avec multiplicités) sont des facteurs irréductibles de P ou de $P - 1$ (avec des multiplicités supérieures).

Démonstration.

1. Soit P premier avec π_u. Il existe une relation de Bézout $AP + B\pi_u = 1$. Puisque $\pi_u(u) = 0$, ceci donne $A(u) \circ P(u) = \mathrm{id}$, de sorte que $P(u)$ est inversible. Réciproquement, si $P(u)$ est inversible, alors il existe un polynôme A tel que $A(u) \circ P(u) = \mathrm{id}$ dans $\mathbb{K}[u]$. Par l'isomorphisme $\mathbb{K}[u] \simeq \mathbb{K}[X]/\langle \pi_u \rangle$, cela signifie qu'il existe un polynôme B tel que $AP = 1 + B\pi_u$, et donc que P et π_u sont premiers entre eux par théorème de Bézout.
2. Puisque $\mathbb{K}[u] \simeq \mathbb{K}[X]/\langle \pi_u \rangle$, alors $\mathbb{K}[u]$ est un corps (respectivement intègre) si et seulement si $\langle \pi_u \rangle$ est maximal (respectivement premier) si et seulement si π_u est irréductible.
3. Puisque $\mathbb{K}[u] \simeq \mathbb{K}[X]/\langle \pi_u \rangle$, il y a une correspondance bijective entre les idéaux de $\mathbb{K}[u]$ et ceux de $\mathbb{K}[X]$ contenant π_u. De plus, $\langle P \rangle$ contient π_u si et seulement si P divise π_u, d'où le résultat.
4. $P(u)$ est nilpotent si et seulement s'il existe m entier tel que $P(u)^m = 0$ si et seulement s'il existe m entier tel que π_u divise P^m.
5. $P(u)^2 = P(u)$ si et seulement si $(P(P-1))(u) = 0$ si et seulement si π_u divise $P(P-1)$, d'où le résultat car P et $P - 1$ sont premiers entre eux.

□

Application 1.6. ▷ Si u est inversible, alors $\pi_u(0) \neq 0$. En effet, on aurait autrement $\pi_u(X) = XP(X)$ donc $u \circ P(u) = 0$ puis $P(u) = 0$ car u est inversible, ce qui contredit la minimalité du degré de π_u. Ainsi, en notant $\pi_u = X^d + \sum_{k=0}^{d-1} a_k X^k$ avec $a_0 \neq 0$, on a

$$u \circ \left(\frac{-1}{a_0} \left(u^{d-1} + \sum_{k=1}^{d-1} a_k u^{k-1} \right) \right) = \mathrm{id}$$

donc $u^{-1} = \frac{-1}{a_0} \left(u^{d-1} + \sum_{k=1}^{d-1} a_k u^{k-1} \right)$ est un polynôme en u.

▷ Une récurrence montre que pour tout $m \geqslant \deg(\pi_u)$, u^m est un polynôme en u. On se sert de ceci pour montrer que $\exp(u)$ est aussi un polynôme en u.

Remarque. Pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, on définit $\mathbb{K}[A]$ et π_A de la même façon. Les propositions et applications précédentes sont encore vraies en remplaçant u par A.

Exemple. Soit $P = X^n - \sum_{k=0}^{n-1} a_k X^k$ et

$$C_P = \begin{pmatrix} 0 & & & a_0 \\ 1 & & (0) & \vdots \\ & \ddots & & \vdots \\ (0) & & 1 & a_{n-1} \end{pmatrix}$$

sa matrice compagnon. En notant $(e_1, ..., e_n)$ la base canonique de $\mathbb{K}^n$, on a donc

$$\forall k \in [\![1, n-1]\!],\ C_P e_k = e_{k+1},\ \text{et } C_P e_n = \sum_{k=0}^{n-1} a_k e_{k+1},$$

donc

$$\forall k \in [\![1, n]\!],\ e_k = C_P^{k-1} e_1 \text{ et } P(C_P)e_k = (X^{k-1}P)(C_P)e_1 = 0.$$

Ainsi, $P(C_P)$ annule les vecteurs d'une base donc $P(C_P) = 0$ et π_{C_P} divise P. On a donc $\deg(\pi_{C_P}) \leqslant \deg(P) = n$. Soit $Q \neq 0$ un polynôme annulateur de C_P. Si $\deg(Q) \leqslant n-1$, alors la relation $Q(C_P)e_1 = 0$ fournit une relation de dépendance linéaire non-triviale entre les $(e_1, ..., e_n)$, ce qui est absurde. Donc $\deg(Q) \geqslant n$, et en appliquant ceci à $Q = \pi_u$ il s'ensuit que $\deg(\pi_{C_P}) = n$. Puisque P est unitaire de degré n et annule C_P, alors on obtient

$$\pi_{C_P} = P.$$

Proposition 1.7. Soit $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E. Soit $A = \mathrm{Mat}_{\mathcal{B}}(u)$ et $A' = \mathrm{Mat}_{\mathcal{B}'}(u)$. Alors

$$\pi_A = \pi_{A'} = \pi_u.$$

Autrement dit, deux matrices semblables ont même polynôme minimal, et c'est le polynôme minimal de l'endomorphisme qu'elles représentent dans des bases différentes.

Contre-exemple. Deux matrices ayant le même polynôme minimal ne sont pas forcément semblables. Par exemple, $\begin{pmatrix} 1 & & \\ & 1 & \\ & & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & & \\ & 2 & \\ & & 2 \end{pmatrix}$ ont $(X-1)(X-2)$ comme polynôme minimal commun mais ne sont pas semblables, car elles n'ont pas le même déterminant.

1.2 Lemme des noyaux et réduction

Lemme 1.8 (Lemme des noyaux). Soit $P_1, ..., P_r \in \mathbb{K}[X]$ des polynômes premiers entre eux deux à deux, et $P = P_1...P_r$. Alors

$$\ker(P(u)) = \bigoplus_{k=1}^{r} \ker(P_k(u)).$$

Démonstration. Raisonnons par récurrence sur $r \geqslant 2$.

▷ Si $r = 2$, on dispose d'une relation de Bézout $A_1P_1 + A_2P_2 = 1$. Soit $x \in \ker(P_1(u)) \cap \ker(P_2(u))$. On a

$$0 = (A_1P_1 + A_2P_2)(u)(x) = x$$

donc $\ker(P_1(u)) \cap \ker(P_2(u)) = \{0\}$. Soit maintenant $x \in \ker(P(u))$. On écrit

$$x = (A_1P_1)(u)(x) + (A_2P_2)(u)(x),$$

et on note que $(A_1P_1)(u)(x) \in \ker(P_2(u))$ car $P_2A_1P_1 = A_1P$ et $P(u)(x) = 0$, et de même $(A_2P_2)(u)(x) \in \ker(P_1(u))$. Donc $\ker(P(u)) \subset \ker(P_1(u))+\ker(P_2(u))$. L'inclusion réciproque étant évidente, et l'intersection étant triviale, on a bien

$$\ker(P(u)) = \ker(P_1(u)) \oplus \ker(P_2(u)).$$

▷ Supposons le résultat vrai pour au plus r polynômes. Soit $P_1, ..., P_{r+1} \in \mathbb{K}[X]$ premiers entre eux deux à deux, et $Q = P_1...P_r$. Alors Q et P_{r+1} sont premiers entre eux donc le cas $r = 2$ donne

$$\ker((QP_{r+1})(u)) = \ker(Q(u)) \oplus \ker(P_{r+1}(u)).$$

De plus, l'hypothèse de récurrence donne

$$\ker(Q(u)) = \bigoplus_{k=1}^{r} \ker(P_k(u)),$$

d'où le résultat.

□

Si P est un polynôme annulateur de u, le lemme des noyaux donne une décomposition de E en somme directe de sous-espaces stables par u. Dans une base adaptée à cette décomposition, la matrice de u est diagonale par blocs. C'est là que résident l'intérêt des polynômes annulateurs et l'importance du lemme des noyaux dans la réduction. Ceci est illustré par la proposition suivante.

Proposition 1.9. Un endomorphisme u est diagonalisable si et seulement s'il admet un polynôme annulateur simplement scindé si et seulement si π_u est simplement scindé.

Démonstration. ▷ Supposons u diagonalisable. Il existe une base $\mathcal{B}$ de E telle que

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix}.$$

On note $\Lambda = \{\lambda_1, ..., \lambda_n\}$. Alors le polynôme $\prod_{\lambda \in \Lambda} (X - \lambda)$ est simplement scindé et annule u.

▷ Supposons que u admette un polynôme annulateur P simplement scindé. Puisque π_u divise P, alors π_u est nécessairement simplement scindé.

▷ Supposons π_u simplement scindé et écrivons $\pi_u = \prod_{k=1}^{r} (X - \lambda_k)$, où les λ_k sont tous distincts. D'après le lemme des noyaux, on a une décomposition

$$E = \bigoplus_{k=1}^{r} \ker(u - \lambda_k \mathrm{id}).$$

Soit $\mathcal{B}$ une base adaptée à cette décomposition. Comme les $\ker(u - \lambda_k \mathrm{id})$ sont stables par u, la matrice de u dans cette base est diagonale par blocs :

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} A_1 & & (0) \\ & \ddots & \\ (0) & & A_r \end{pmatrix}.$$

Or, u agit sur chacun des $\ker(u - \lambda_k \mathrm{id})$ comme une homothétie de rapport λ_k, de sorte que A_k est diagonale. Ainsi, u est diagonalisable.

□

Exemple. ▷ Une symétrie est diagonalisable, car annulée par $X^2 - 1 = (X-1)(X+1)$. Par exemple, la transposition des matrices est un endomorphisme de $\mathcal{M}_n(\mathbb{K})$ diagonalisable, et l'application qui à un polynôme $P \in \mathbb{R}_n[X]$ associe son polynôme réciproque $\tilde{P} = X^n P(\frac{1}{X})$ est un endomorphisme de $\mathbb{R}_n[X]$ diagonalisable.

▷ Un projecteur est diagonalisable, car annulé par $X^2 - X = X(X-1)$.

▷ Un endomorphisme nilpotent non-nul n'est pas diagonalisable, car son polynôme minimal est de la forme X^k avec $k \geqslant 2$. Autrement dit, un endomorphisme nilpotent diagonalisable est nul. Par exemple, la dérivation des polynômes de $\mathbb{R}_n[X]$ n'est pas diagonalisable.

▷ La matrice $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ admet X^2+1 comme polynôme annulateur. Comme elle ne correspond pas à une homothétie, son polynôme minimal est au moins de degré 2, donc est $X^2 + 1$. Ainsi, cette matrice est diagonalisable sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

Exemple. Soit $A \in \mathrm{GL}_n(\mathbb{C})$ telle qu'il existe $m \in \mathbb{N}^*$ tel que A^m soit diagonalisable. Alors A est diagonalisable.

Proposition 1.10. Si $\mathbb{K} = \mathbb{F}_q$ est un corps fini, alors u est diagonalisable si et seulement si $u^q = u$.

1.3 Endomorphismes cycliques et réduction de Frobenius

Définition 1.11. L'endomorphisme u est cyclique s'il existe un vecteur $x \in E$ tel que $(x, u(x), ..., u^{n-1}(x))$ soit une base de E.

Proposition 1.12. L'endomorphisme u est cyclique si et seulement s'il existe une base de E dans laquelle la matrice de u est une matrice compagnon.

Soit u un endomorphisme cyclique. Soit $\mathcal{B}$ une base de E et P un polynôme (de degré n) tels que $\mathrm{Mat}_{\mathcal{B}}(u) = C_P$. On sait qu'alors $\pi_u = P$. En particulier, $\deg(\pi_u) = n$.

Théorème 1.13 (Invariants de similitude). Soit $u \in \mathcal{L}(E)$. Il existe $F_1, ..., F_r$ des sous-espaces vectoriels de E stables par u tels que :

(*i*) $E = \bigoplus_{k=1}^{r} F_k$,

(*ii*) pour tout $1 \leqslant k \leqslant r$, $u_k = u_{|F_k}$ est cyclique,

(*iii*) en notant $P_k = \pi_{u_k}$ pour $1 \leqslant k \leqslant r$, on a P_k divise P_{k+1} pour $1 \leqslant k \leqslant r-1$.

De plus, la suite $(P_k)_{1 \leqslant k \leqslant r}$ est unique : elle ne dépend que de u et pas de la décomposition choisie. On l'appelle suite des invariants de similitude de u.

Théorème 1.14 (Frobenius). Soit $(P_k)_{1 \leqslant k \leqslant r}$ les invariants de similitude de u. Alors il existe une base $\mathcal{B}$ de E telle que

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} C_{P_1} & & (0) \\ & \ddots & \\ (0) & & C_{P_r} \end{pmatrix}$$

où C_{P_k} est la matrice compagnon de P_k.

Corollaire 1.15. Deux endomorphismes sont semblables si et seulement s'ils ont les mêmes invariants de similitude.

Remarque. Avec les notations des théorèmes, on a $P_\ell(u_k) = 0$ pour tout $\ell \geqslant k$, car P_k divise P_ℓ. En particulier, P_r annule tous les u_k pour $1 \leqslant k \leqslant r$. Ainsi, $P_r(C_{P_k}) = 0$ pour tout $1 \leqslant k \leqslant r$ donc $P_r(\mathrm{Mat}_{\mathcal{B}}(u)) = 0$. Ainsi, π_u divise P_r, et en particulier $\deg(\pi_u) \leqslant \deg(P_r) \leqslant n$.

De plus, si $\deg(\pi_u) = n$, alors on a nécessairement $\deg(P_r) = n$ et $r = 1$. Il en résulte que u est cyclique. Comme on sait déjà que la réciproque est vraie, alors on obtient

$$u \text{ est cyclique } \Leftrightarrow \deg(\pi_u) = n.$$

Application 1.16. Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. Si $A, B \in \mathcal{M}_n(\mathbb{K})$ sont semblables dans $\mathcal{M}_n(\mathbb{L})$, alors elles sont semblables dans $\mathcal{M}_n(\mathbb{K})$.

Application 1.17. On peut dénombrer les classes de similitude dans les corps finis. Il y a par exemple 8 classes de similitudes dans $\mathrm{GL}_2(\mathbb{F}_3)$. En effet, nous allons dénombrer les suites d'invariants de similitude possibles. Ici, $n = 2$ donc la suite des invariants contient $r = 1$ ou $r = 2$ termes.

- ▷ Si $r = 1$, il s'agit de compter des polynômes de degré 2 sur $\mathbb{F}_3$. Ces polynômes doivent être unitaires (ce sont des polynômes minimaux) et avoir un cœfficient constant non-nul (ce sont des polynômes minimaux d'endomorphismes inversibles). Il y a deux 2 choix pour le cœfficient constant et 3 choix pour le cœfficient de degré 1. Cela fait 6 possibilités.

  En termes matriciels, une matrice $A \in \mathrm{GL}_2(\mathbb{F}_3)$ ayant un seul invariant de similitude est semblable à $\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$. Comme le déterminant $-a$ est non-nul, il y a 2 choix pour a, et 3 choix pour b. On retrouve bien 6 possibilités.
- ▷ Si $r = 2$, on a deux invariants de similitude P_1 et P_2 unitaires de degré 1, chacun étant déterminé par son cœfficient constant qui est non-nul comme précédemment. Or, la condition P_1 divise P_2 implique $P_1 = P_2$. Ainsi, seul le cœfficient constant de P_1 est à choisir, et il y a 2 possibilités.

  En termes matriciels, une matrice $A \in \mathrm{GL}_2(\mathbb{F}_3)$ ayant deux invariants de similitude est semblable à $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. La condition de divisibilité donne $a = b$, et puisque le déterminant est non-nul alors $a \neq 0$. On retrouve bien 2 possibilités.

Il y a donc bien $6 + 2 = 8$ classes de similitude dans $\mathrm{GL}_2(\mathbb{F}_3)$.

2 Éléments propres

2.1 Polynôme caractéristique et spectre

Définition 2.1. Le polynôme caractéristique de u est $\chi_u(X) = \det(X\mathrm{id} - u)$.

Exemple.
- ▷ Si u est nilpotent, alors $\chi_u = X^n$. On remarque qu'alors $\chi_u(u) = 0$.
- ▷ Soit $P \in \mathbb{K}[X]$ et C_P sa matrice compagnon. En développant le déterminant par rapport à la dernière colonne, on obtient $\chi_{C_P} = P$, c'est-à-dire $\chi_{C_P} = \pi_{C_P}$. En particulier, $\chi_{C_P}(C_P) = 0$.

Remarque. Soit u en endomorphisme tel que $\chi_u = \pi_u$. Alors $\deg(\pi_u) = \deg(\chi_u) = n$, et donc u est cyclique d'après une remarque précédente. Combiné à l'exemple précédent, ceci montre

$$u \text{ est cylique } \Leftrightarrow \pi_u = \chi_u \Leftrightarrow \deg(\pi_u) = n.$$

Application 2.2 (Borne de Cauchy). Soit $P = X^n - \sum_{k=0}^{n-1} a_k X^k \in \mathbb{C}[X]$, et $\lambda \in \mathbb{C}$ une racine de P. Alors

$$|\lambda| \leqslant \max(|a_0|, 1 + |a_1|, ..., 1 + |a_{n-1}|).$$

Dans l'exemple précédent, on avait $\chi_u(u) = 0$ et $\chi_{C_P}(C_P) = 0$: les polynômes caractéristiques dans ces cas particuliers sont des polynômes annulateurs. Ceci est en réalité vrai pour tout endomorphisme.

Théorème 2.3 (Cayley-Hamilton). χ_u est un polynôme annulateur de u, c'est-à-dire π_u divise χ_u.

Démonstration. Soit $x \in E \setminus \{0\}$. Il existe un entier $p > 0$ tel que $(x, u(x), ..., u^{p-1}(x))$ soit libre et $(x, u(x), ..., u^p(x))$ liée. On dispose donc d'une relation

$$u^p(x) = \sum_{k=0}^{p-1} a_k u^k(x).$$

Complétons $(x, u(x), ..., u^{p-1}(x))$ en une base $\mathcal{B}$ de E. On a

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \text{ où } A = \begin{pmatrix} 0 & & & a_0 \\ 1 & & (0) & \vdots \\ & \ddots & & \vdots \\ (0) & & 1 & a_{p-1} \end{pmatrix}.$$

Ainsi, $\chi_u = \chi_A \chi_C$ avec $\chi_A = X^p - \sum_{k=0}^{p-1} a_k X^k$. Puisque A est la matrice compagnon associée au polynôme de dépendance linéaire entre les $(u^k(x))_{0 \leqslant k \leqslant p}$, alors $\chi_A(u)(x) = 0$. Donc

$$\chi_u(u)(x) = \chi_C(u) \circ \chi_A(u)(x) = 0.$$

Donc pour tout $x \in E \setminus \{0\}$ on a $\chi_u(u)(x) = 0$. Ceci étant évidemment vrai aussi pour $x = 0$, on en déduit que $\chi_u(u) = 0$. □

Remarque. On peut raisonner de façon plus concise en s'appuyant sur la réduction de Frobenius. Soit u un endomorphisme quelconque et $(P_k)_{1 \leqslant k \leqslant r}$ ses invariants de similitude. Par théorème de Frobenius, il existe une base $\mathcal{B}$ de E telle que $\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} C_{P_1} & & (0) \\ & \ddots & \\ (0) & & C_{P_r} \end{pmatrix}$. On obtient alors $\chi_u = P_1 ... P_r$. Or, on a vu que π_u divise P_r. Finalement, π_u divise χ_u et le théorème de Cayley-Hamilton est démontré.

Définition 2.4. Soit $\lambda \in \mathbb{K}$. On dit que λ est valeur propre de u si $u - \lambda \mathrm{id}$ n'est pas injectif. On appelle spectre de u, noté $\mathrm{Sp}(u)$, l'ensemble des valeurs propres de u.

Soit $\lambda \in \mathrm{Sp}(u)$. Le sous-espace propre de u associé à λ est $E_\lambda = \ker(u - \lambda \mathrm{id})$. Ses éléments non-nuls sont appelés vecteurs propres de u pour λ.

Le lien entre les valeurs propres d'un endomorphisme et ses polynômes annulateurs est le suivant.

Proposition 2.5. Le spectre $\mathrm{Sp}(u)$ de u est exactement l'ensemble des racines de χ_u, et c'est aussi l'ensemble des racines de π_u.

Application 2.6. Soit $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ les suites données par

$$\left\{\begin{array}{rcl} u_0 &=& 2 \\ v_0 &=& 1 \end{array}\right. \text{ et } \left\{\begin{array}{rcl} u_{n+1} &=& u_n - v_n \\ v_{n+1} &=& 2u_n + 4v_n \end{array}\right. .$$

En posant $X_n = \left(\begin{smallmatrix} u_n \\ v_n \end{smallmatrix}\right)$ et $A = \left(\begin{smallmatrix} 1 & -1 \\ 2 & 4 \end{smallmatrix}\right)$, cela se récrit

$$X_0 = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \text{ et } X_{n+1} = AX_n$$

et on a donc pour tout $n \in \mathbb{N}$: $X_n = A^n X_0$. Or, on calcule $\chi_A = (X-2)(X-3)$. Ainsi, A possède un polynôme annulateur simplement scindé donc est diagonalisable : il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que

$$A = P \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} P^{-1} \text{ et donc } A^n = P \begin{pmatrix} 2^n & 0 \\ 0 & 3^n \end{pmatrix} P^{-1}.$$

Les calculs des vecteurs propres associés à 2 et 3 donnent $P = \left(\begin{smallmatrix} 1 & 1 \\ -1 & -2 \end{smallmatrix}\right)$. Ainsi :

$$\left\{\begin{array}{rcl} u_n &=& 5 \times 2^n - 3 \times 3^n \\ v_n &=& -5 \times 2^n + 6 \times 3^n \end{array}\right. .$$

Remarque. Ainsi, les valeurs propres de u sont racines de tout polynôme annulateur de u.

Définition 2.7. Soit $\lambda \in \mathrm{Sp}(u)$. On appelle multiplicité :

- ▷ algébrique, notée $m_a(\lambda)$, la multiplicité de λ comme racine de χ_u,
- ▷ géométrique, notée $m_g(\lambda)$, la dimension de E_λ,
- ▷ minimale, notée $m_m(\lambda)$, la multiplicité de λ comme racine de π_u.

Proposition 2.8. Pour tout $\lambda \in \mathrm{Sp}(u)$, on a $m_g(\lambda) \leqslant m_a(\lambda)$, et $m_m(\lambda) \leqslant m_a(\lambda)$.

Application 2.9. Si $\chi_u = \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$, alors le lemme des noyaux et le théorème de Cayley-Hamilton donnent

$$E = \bigoplus_{k=1}^{r} \ker((u - \lambda_k \mathrm{id})^{m_k}).$$

L'ensemble $\ker((u - \lambda_k \mathrm{id})^{m_k})$ s'appelle le sous-espace caractéristique de u associé à λ_k.

Proposition 2.10. Soit $u, v \in \mathcal{L}(E)$ tels que u et v commutent. Alors $\ker(u)$, $\mathrm{im}(u)$, les sous-espaces propres et caractéristiques de u sont stables par v.

2.2 Critères de réduction

Proposition 2.11. Les assertions suivantes sont équivalentes :

(i) l'endomorphisme u est diagonalisable,

(ii) χ_u est scindé et $\forall \lambda \in \mathrm{Sp}(u),\ m_a(\lambda) = m_g(\lambda)$,

(iii) $E = \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda$.

Dans ce cas, en notant p_λ la projection sur E_λ parallèlement à $\bigoplus_{\mu \neq \lambda} E_\mu$, on a $u = \sum_{\lambda \in \mathrm{Sp}(u)} \lambda p_\lambda$.

Exemple. Soit $A = \begin{pmatrix} & & & 1 \\ & & -1 & \\ & 1 & & \\ -1 & & & \end{pmatrix} \in \mathcal{M}_4(\mathbb{C})$. On calcule $\chi_A = (X-i)^2(X+i)^2$, donc χ_A est scindé. Cherchons les dimensions $m_g(i)$ et $m_g(-i)$ des sous-espaces propres.

▷ On a
$$A - iI_4 = \begin{pmatrix} -i & & & 1 \\ & -i & -1 & \\ & 1 & -i & \\ -1 & & & -i \end{pmatrix} = (C_1|...|C_4).$$
Puisque $C_1 + iC_4 = C_2 - iC_3 = 0$, alors $\begin{pmatrix} 1 \\ 0 \\ 0 \\ i \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -i \\ 0 \end{pmatrix} \in \ker(A - iI_4)$. Ces deux vecteurs étant indépendants, et puisque $m_g(i) \leqslant m_a(i) = 2$, alors on a $m_g(i) = m_a(i) = 2$.

▷ On montre de la même façon que $m_g(-i) = m_a(-i) = 2$

Ainsi, A est diagonalisable.

Proposition 2.12.
▷ Si $\mathbb{K} = \mathbb{C}$, alors u est diagonalisable si et seulement si u^2 est diagonalisable et $\ker(u) = \ker(u^2)$.

▷ Si $\mathbb{K} = \mathbb{R}$, alors u est diagonalisable si et seulement si u^2 est diagonalisable, $\ker(u) = \ker(u^2)$ et $\mathrm{Sp}(u^2) \subset \mathbb{R}_+$.

Proposition 2.13. L'endomorphisme u est trigonalisable si et seulement si χ_u est scindé.

Remarque. Sur un corps algébriquement clos tout endormorphisme est trigonalisable.

Exemple. Soit $A \in \mathcal{M}_n(\mathbb{C})$, alors $\det(\exp(A)) = \exp(\mathrm{tr}(A)) \in \mathbb{C}^\times$.

Application 2.14 (Applications topologiques de la trigonalisation). Dans $\mathcal{M}_n(\mathbb{C})$:

▷ les matrices diagonalisables sont denses dans $\mathcal{M}_n(\mathbb{C})$,

▷ A est diagonalisable si et seulement si sa classe de similitude est fermée dans $\mathcal{M}_n(\mathbb{C})$.

Remarque. La densité des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{C})$ et la continuité du déterminant permettent de redémontrer le théorème de Cayley-Hamilton si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

2.3 Réduction de Jordan

Soit $\lambda \in \mathbb{K}$ et $k \in \mathbb{N}^*$. On note

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & & (0) \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ (0) & & & \lambda \end{pmatrix} \in \mathcal{M}_k(\mathbb{K})$$

le bloc de Jordan de taille k associé à λ. On note $J_k = J_k(0)$. C'est une matrice nilpotente, d'indice de nilpotence égal à k.

Théorème 2.15 (Jordan nilpotent). Soit u un endomorphisme nilpotent. Il existe une base $\mathcal{B}$ de E et des entiers $n_1 \geqslant ... \geqslant n_r$ tels que

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} J_{n_1} & & (0) \\ & \ddots & \\ (0) & & J_{n_r} \end{pmatrix}.$$

Remarque. L'indice de nilpotence de u est n_1, et u est nilpotent d'indice maximal n si et seulement si $r = 1$ et $n_1 = n$.

Le théorème précédent permet de montrer la généralisation suivante, et la proposition qui suit précise le rôle joué par les différentes multiplicités des valeurs propres.

Théorème 2.16 (Jordan). Soit $u \in \mathcal{L}(E)$ tel que $\chi_u = \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$ soit scindé sur $\mathbb{K}$. Alors il existe une base $\mathcal{B}$ de E et des entiers $n_{k,1} \geqslant ... \geqslant n_{k,d_k}$ pour tout $1 \leqslant k \leqslant r$ tels que

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} A_1 & & (0) \\ & \ddots & \\ (0) & & A_r \end{pmatrix} \text{ avec } A_k = \begin{pmatrix} J_{n_{k,1}}(\lambda_k) & & (0) \\ & \ddots & \\ (0) & & J_{n_{k,d_k}}(\lambda_k) \end{pmatrix}.$$

Proposition 2.17. Sous les hypothèses et avec les notations du théorème précédent, on a pour tout $1 \leqslant k \leqslant r$:

- ▷ $m_a(\lambda_k)$ est la taille de la matrice A_k,
- ▷ $m_g(\lambda_k) = d_k$ est le nombre de blocs de Jordan associés à λ_k,
- ▷ $m_m(\lambda_k)$ est la taille du plus grand bloc de Jordan associé à λ_k.

Remarque.
- ▷ On retrouve le fait que si χ_u est scindé et $m_g(\lambda) = m_a(\lambda)$ pour tout $\lambda \in \mathrm{Sp}(u)$, alors u est diagonalisable. En effet, la matrice A_k alors de taille $m_a(\lambda_k)$ et formée de $m_g(\lambda_k) = m_a(\lambda_k)$ blocs. Nécessairement, ces blocs sont donc de taille 1 donc les A_k sont diagonales.
- ▷ De même, on retrouve le fait que si π_u est simplement scindé, alors u est diagonalisable. En effet, les blocs associés à une valeur propre sont alors tous de taille 1.

Un des intérêts calculatoires de la forme de Jordan est le suivant.

Proposition 2.18. Soit $\lambda \in \mathbb{K}$ et $k \in \mathbb{N}^*$. Alors

$$\exp(tJ_k(\lambda)) = e^{t\lambda} \begin{pmatrix} 1 & t & \cdots & \frac{t^{k-1}}{(k-1)!} \\ & \ddots & \ddots & \vdots \\ & & \ddots & t \\ (0) & & & 1 \end{pmatrix}.$$

Application 2.19. Soit $A \in \mathcal{M}_n(\mathbb{C})$. On note $\pi_A = \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$. Alors les solutions du système différentiel $Y' = AY$ sont de la forme

$$t \mapsto \sum_{k=1}^{r} P_k(t) e^{\lambda_k t}$$

avec $P_k \in \mathbb{C}[X]$ de degré au plus $m_k - 1$.

Exemple. Soit $A = \begin{pmatrix} 5 & 1 & -1 \\ 1 & 3 & -1 \\ 2 & 0 & -2 \end{pmatrix}$. On calcule $\chi_A = (X-2)(X-4)^2$, et on vérifie que $\pi_A = \chi_A$. Ainsi, la matrice A est semblable à la matrice réduite de Jordan $\begin{pmatrix} 2 & & \\ & 4 & 1 \\ & & 4 \end{pmatrix}$, donc les solutions du système différentiel $Y' = AY$ sont des combinaisons linéaires de e^{2t}, e^{4t} et te^{4t}.

Remarque. La connaissance de la réduction de Frobenius d'un endomorphisme u, c'est-à-dire la connaissance de ses invariants de similitude, permet d'obtenir la réduction de Jordan de u. Par exemple, si les invariants de similitude de u sont $P_1 = X - 3$ et $P_2 = (X-3)^2(X+2)^2$,

alors la forme de Jordan associée est

$$\begin{pmatrix} 3 & & & & \\ & 3 & 1 & & \\ & & 3 & & \\ & & & -2 & 1 \\ & & & & -2 \end{pmatrix}.$$

3 D'autres façons de réduire

3.1 Réduction simultanée

Proposition 3.1. Soit $(u_i)_{i\in I}$ des endomorphismes de E. Si les u_i sont diagonalisables et commutent deux à deux, alors ils sont codiagonalisables.

Exemple. Les matrices circulantes sont des polynômes en la matrice

$$J = \begin{pmatrix} & 1 & & (0) \\ & & \ddots & \\ & (0) & & 1 \\ 1 & & & \end{pmatrix} = \begin{pmatrix} 0 & I_{n-1} \\ I_1 & 0 \end{pmatrix}$$

donc elles commutent entre elles. De plus, puisque pour tout $k \in \mathbb{N}$ on a

$$J^k = \begin{pmatrix} 0 & I_{n-k} \\ I_k & 0 \end{pmatrix},$$

alors $\deg(\pi_J) \geqslant n$ et $X^n - 1$ annule J, d'où $\pi_J = X^n - 1$. Ainsi, π_J est simplement scindé sur $\mathbb{C}$ donc J est diagonalisable. Il en résulte que les matrices circulantes le sont également. Ainsi, les matrices circulantes sont codiagonalisables.

Application 3.2. Si $\mathrm{car}(\mathbb{K}) \neq 2$, les groupes $\mathrm{GL}_n(\mathbb{K})$ et $\mathrm{GL}_m(\mathbb{K})$ sont isomorphes si et seulement si $n = m$.

Application 3.3.

- ▷ Soit $\mathbb{K}$ algébriquement clos et G un sous-groupe commutatif fini de $\mathrm{GL}_n(\mathbb{K})$. Si $|G|$ et $\mathrm{car}(\mathbb{K})$ sont premiers entre eux, ou si $\mathrm{car}(\mathbb{K}) = 0$, alors G est codiagonalisable.

  En effet, soit $n = |G|$. Les éléments de G sont tous annulés par $P = X^n - 1$. On a $P' = nX^{n-1}$ et donc $P' \neq 0$ sous les hypothèses. Ainsi, 0 est la seule racine de P' mais n'est pas racine de P. Comme $\mathbb{K}$ est algébriquement clos, il en résulte que P est simplement scindé, et donc les éléments de G sont tous diagonalisables. Comme ils commutent, ils sont codiagonalisables.

- ▷ En particulier, les représentations complexes irréductibles d'un groupe abélien fini sont de degré 1.

  En effet, soit G un groupe abélien fini et $\rho : G \to \mathrm{GL}(V)$ une représentation complexe irréductible de G de dimension d. Puisque G est abélien, l'ensemble $\rho(G)$ est un sous-groupe abélien de $\mathrm{GL}(V) \simeq \mathrm{GL}_d(\mathbb{C})$. Il est donc codiagonalisable. Ainsi, il existe une

base $(e_1, ..., e_d)$ de V telle que les $\rho(g)$ pour $g \in G$ aient tous une matrice diagonale. Mais alors, chacun des sous-espaces $\text{vect}(e_k)$ est stable par G et forme donc une sous-représentation de V, ce qui est absurde sauf si $d = 1$ et $V = \text{vect}(e_1)$.

Proposition 3.4. Soit $(u_i)_{i\in I}$ des endomorphismes de E. Si les u_i sont trigonalisables et commutent deux à deux, alors ils sont cotrigonalisables.

Exemple. Tout sous-groupe abélien de $\mathrm{GL}_n(\mathbb{C})$ est cotrigonalisable.

Théorème 3.5 (Lie-Kolchin). Soit G un sous-groupe connexe résoluble de $\mathrm{GL}_n(\mathbb{C})$. Alors G est cotrigonalisable.

Démonstration. Comme G est résoluble, on dispose d'une suite

$$\{1\} = D^\ell(G) \triangleleft D^{\ell-1}(G) \triangleleft ... \triangleleft D(G) \triangleleft G$$

où l'entier $\ell \geqslant 1$ est minimal, et où chacun des quotients $D^k(G)/D^{k+1}(G)$ est abélien. Le cas où G est abélien étant traité par la proposition précédente, on suppose G non-abélien, et donc $\ell \geqslant 2$.

Étape 1. Montrons que les groupes dérivés $D^k(G)$ sont connexes.

L'application $\left\{ \begin{array}{ccc} G \times G & \to & G \\ (g,h) & \mapsto & [g,h] \end{array} \right.$ est continue pour la topologie induite par celle de $\mathcal{M}_n(\mathbb{C})$. Son image, notée X, est donc connexe car $G \times G$ l'est. De plus,

$$D(G) = \bigcup_{n\in\mathbb{N}^*} X_n, \text{ où } X_n = \{x_1...x_n,\ (x_1, ..., x_n) \in X^n\}.$$

L'ensemble X_n est l'image de l'application $\left\{ \begin{array}{ccc} X^n & \to & X_n \\ (x_1, ..., x_n) & \mapsto & x_1...x_n \end{array} \right.$, qui est continue, donc est connexe car X^n l'est. Puisque pour tout $n \in \mathbb{N}^*$, $\mathrm{id} \in X_n$, alors $D(G)$ est connexe comme union de connexes ayant une intersection non-nulle.

On a ainsi montré que si G est connexe, alors $D(G)$ est connexe. En appliquant ceci récursivement, on obtient que pour tout $k \in \mathbb{N}$, $D^k(G)$ est connexe.

Étape 2. Étude des valeurs et vecteurs propres des éléments de $D^{\ell-1}(G)$.

Posons $A = D^{\ell-1}(G)$ et $V = \{v \in \mathbb{C}^n \mid Av \subset \mathbb{C}v\}$ l'ensemble des vecteurs propres communs à tous les éléments de A. Par choix de ℓ, $A \neq \{1\}$ et A est abélien. Puisque les éléments de A sont trigonalisables, car $\mathbb{C}$ est algébriquement clos, alors A est en fait cotrigonalisable. Il existe donc une base $(e_1, ..., e_n)$ de $\mathbb{C}^n$ telle que les matrices des endomorphismes associés aux éléments de A soient triangulaires supérieures. Alors $e_1 \in V$, et donc V n'est pas trivial.

Soit $v \in V$ et $a \in A$. On note $\lambda_v(a) \in \mathbb{C}$ la valeur propre de a associée à v : $a(v) = \lambda_v(a)v$. Soit $g \in G$. Puisque A est distingué dans G, on a $g^{-1}ag \in A$ et

$$a(g(v)) = g((g^{-1}ag)(v)) = g(\lambda_v(g^{-1}ag)v) = \lambda_v(g^{-1}ag)g(v)$$

donc $g(v) \in V$ et $\lambda_{g(v)}(a) = \lambda_v(g^{-1}ag)$.

Soit maintenant $a \in A$ et v un vecteur propre de a associé à la valeur propre $\lambda_v(a)$. Pour $g \in G$, on a $g(v) \neq 0$ car $v \neq 0$. De plus, l'application $\left\{ \begin{array}{ccc} G & \to & \mathbb{C} \\ g & \mapsto & \lambda_v(g^{-1}ag) \end{array} \right.$ est continue comme composée des applications continues $g \mapsto g^{-1}ag$ et $\lambda_v : b \in A \mapsto \lambda_v(b) = \frac{\langle b(v), v\rangle}{\|v\|^2}$, où $\langle \cdot, \cdot \rangle$ est le produit hermitien canonique sur $\mathbb{C}^n$. Ainsi, son image est connexe car G est connexe. Comme $\lambda_v(g^{-1}ag) = \lambda_{g(v)}(a)$, cette image est incluse dans l'ensemble discret $\mathrm{Sp}(a)$. C'est donc un singleton : pour tout $g \in G$,

$$\lambda_{g(v)}(a) = \lambda_{\mathrm{id}(v)}(a) = \lambda_v(a),$$

donc $g(v)$ est un vecteur propre de a associé à la même valeur propre que v.

Étape 3. Construction d'un sous-espace strict stable par G.

Soit $v \in V \setminus \{0\}$ et $W = \mathrm{vect}(g(v),\ g \in G)$. Alors W est stable par G car sa partie génératrice l'est. De plus, $v \in W$ donc $\dim(W) \geqslant 1$. Supposons par l'absurde que $\dim(W) = n$, c'est-à-dire $W = \mathbb{C}^n$. Soit $a \in A$. Tous les $g(v)$ sont vecteurs propres de a pour la même valeur propre $\lambda = \lambda_v(a)$, de sorte que $W \subset \ker(a - \lambda \mathrm{id})$, et donc $\mathbb{C}^n = \ker(a - \lambda \mathrm{id})$. Ainsi, les éléments a de A sont tous des homothéties : $a = \lambda_v(a)\mathrm{id}$. Comme $A = D^{\ell-1}(G)$ et $\ell \geqslant 2$, alors A est un groupe dérivé (A n'est pas G tout entier), donc ses éléments sont de déterminant 1. Donc pour tout $a \in A$ on a $\lambda_v(a)^n = 1$, c'est-à-dire l'application $\lambda_v \left| \begin{array}{ccc} A & \to & \mathbb{C} \\ a & \mapsto & \lambda_v(a) \end{array} \right.$ est à valeurs dans l'ensemble discret des racines n-ème de l'unité. Or, cette application est continue et A est connexe. On en déduit que λ_v est constante, et puisque $\lambda_v(\mathrm{id}) = 1$ alors pour tout $a \in A$ on a $\lambda_v(a) = 1$, et donc $a = \mathrm{id}$. Ceci est absurde par choix de ℓ. Donc $\dim(W) \leqslant n - 1$.

Étape 4. Conclusion par récurrence sur n.

Si $n = 1$, il n'y a rien à faire. Supposons que tout sous-groupe connexe résoluble de $\mathrm{GL}_k(\mathbb{C})$, pour tout $1 \leqslant k \leqslant n$, soit cotrigonalisable. Soit G un sous-groupe connexe résoluble de $\mathrm{GL}_{n+1}(\mathbb{C})$. Les étapes précédentes permettent de construire W un sous-espace strict non-trivial de $\mathbb{C}^{n+1}$ stable par G. Soit $k = \dim(W)$. En notant W' un supplémentaire de W et $\mathcal{B}$ une base adaptée à la décomposition $\mathbb{C}^{n+1} = W \oplus W'$, alors pour tout $g \in G$, on a

$$\mathrm{Mat}_{\mathcal{B}}(g) = \begin{pmatrix} \alpha(g) & \star \\ 0 & \beta(g) \end{pmatrix}$$

où les applications α et β sont des morphismes de groupes continus. Comme G est connexe, alors $\alpha(G)$ et $\beta(G)$ sont connexes. Comme G est résoluble, alors $\alpha(G)$ et $\beta(G)$ sont résolubles. Donc $\alpha(G)$ et $\beta(G)$ sont des sous-groupes connexes résolubles de $\mathrm{GL}_k(\mathbb{C})$ et $\mathrm{GL}_{n+1-k}(\mathbb{C})$ respectivement. Par hypothèse de récurrence, il existe des bases $\mathcal{B}_W$ et $\mathcal{B}_{W'}$ de W et W' respectivement qui trigonalisent les endomorphismes associés aux éléments de $\alpha(G)$ et $\beta(G)$ respectivement. Alors la base $\mathcal{B}_W \cup \mathcal{B}_{W'}$ de $\mathbb{C}^{n+1}$ trigonalise les endomorphismes associés aux éléments de G. □

Remarque. ▷ C'est une généralisation de la proposition précédente. En effet, la notion de résolubilité est une généralisation du caractère abélien.

▷ Ce théorème dit que les sous-groupes de $\mathrm{GL}_n(\mathbb{C})$ formés de matrices triangulaires supérieures sont, à une hypothèse de connexité près, les seuls sous-groupes résolubles de $\mathrm{GL}_n(\mathbb{C})$.

3.2 Décomposition de Dunford

La décomposition de Dunford n'est pas un théorème de réduction à proprement parler : elle ne donne pas l'expression de la matrice d'un endomorphisme dans une certaine base. Néanmoins, elle a des intérêts pratiques similaires à ceux de la réduction.

Théorème 3.6 (Dunford). Soit $u \in \mathcal{L}(E)$. Il existe un unique couple (d, n) d'endomorphismes de E tels que

(*i*) d est diagonalisable dans une extension $\mathbb{L}/\mathbb{K}$ et n est nilpotent,

(*ii*) $u = d + n$,

(*iii*) d et n commutent.

De plus, on a $d, n \in \mathbb{K}[u]$.

Remarque. Soit $u = d + n$ la décomposition de Dunford de u. Alors $\exp(u) = \exp(d)\exp(n)$.

Proposition 3.7 (Méthode de Newton). On suppose $\mathrm{car}(\mathbb{K}) = 0$. Soit $A \in \mathcal{M}_n(\mathbb{K})$ et $P = \frac{\chi_A}{\chi_A \wedge \chi_A'}$. On pose

$$A_0 = A \text{ et } A_{r+1} = A_r - P(A_r)P'(A_r)^{-1}.$$

Alors la suite $(A_r)_{r\in\mathbb{N}}$ est bien définie et est stationnaire à D, où $A = D + N$ est la décomposition de Dunford de A.

Démonstration. Étape 1. Étudions P.

D'une part, puisque $\mathrm{car}(\mathbb{K}) = 0$, alors $\chi_A' \neq 0$ donc P est bien défini. De plus, les racines de P sont aussi racines de χ_A car P divise χ_A. Enfin, si λ est racine de χ_A de multiplicité m, alors λ est racine de χ_A' de multiplicité $m-1$ puisque $\mathrm{car}(\mathbb{K}) = 0$. Ainsi, λ est racine simple de P. Donc P a les mêmes racines que χ_A, mais elles sont toutes simples.

Étape 2. Montrons par récurrence sur $r \geqslant 0$ les trois assertions suivantes :

(*i*) $P(A_r)$ est nilpotente, d'indice de nilpotence $n_r \leqslant 1 + \frac{n-1}{2^r}$,

(*ii*) $P'(A_r)$ est inversible,

(*iii*) A_{r+1} est bien définie, et $A_{r+1} \in \mathbb{K}[A]$.

▷ Puisque les racines de P sont celles de χ_A, alors χ_A divise P^n. Par théorème de Cayley-Hamilton, on a donc $P(A)^n = 0$, donc $P(A)$ est nilpotente. Son indice de nilpotence n_0 est au plus n, d'où (*i*).

De plus, les valeurs propres de $P'(A)$ sont les $P'(\lambda)$, pour $\lambda \in \mathrm{Sp}(A)$. Puisque les racines de P sont simples et sont exactement les valeurs propres de A, alors $P'(\lambda) \neq 0$. Donc $0 \notin \mathrm{Sp}(P'(A))$ ce qui signifie que $P'(A)$ est inversible, d'où (ii).
Enfin, on a $P'(A) \in \mathbb{K}[A]$ donc $P'(A)^{-1} \in \mathbb{K}[P'(A)] \subset \mathbb{K}[A]$, d'où (iii).

▷ Supposons les assertions démontrées pour un $r \geqslant 0$. En notant $P = \sum_{k=0}^{d} a_k X^k$, on a pour $a, h \in \mathbb{K}$:

$$\begin{aligned} P(a+h) &= \sum_{k=0}^{d} a_k (a+h)^k \\ &= \sum_{k=0}^{d} a_k \left(a^k + k a^{k-1} h + \sum_{i=0}^{k-2} \binom{k}{i} a^i h^{k-i} \right) \\ &= P(a) + hP'(a) + h^2 Q(a,h) \end{aligned}$$

où $Q \in \mathbb{K}[X,Y]$. Alors pour $R, S \in \mathbb{K}[X]$ et $x \in \mathbb{K}$, on a

$$P(R(x)+S(x)) = P(R(x)) + S(x)P'(R(x)) + S(x)^2 \tilde{Q}(x)$$

où $\tilde{Q} \in \mathbb{K}[X]$. Comme $P'(A_r) \in \mathbb{K}[A_r]$, alors $P'(A_r)^{-1} \in \mathbb{K}[A_r]$ donc il existe $T \in \mathbb{K}[X]$ tel que $P'(A_r)^{-1} = T(A_r)$. En prenant $R(X) = X$ et $S(X) = -P(X)T(X)$, on obtient :

$$\begin{aligned} P(A_{r+1}) &= P(A_r - P(A_r)P'(A_r)^{-1}) \\ &= P(A_r) - P(A_r)P'(A_r)^{-1}P'(A_r) + (P(A_r)P'(A_r)^{-1})^2 \tilde{Q}(A_r) \\ &= (P(A_r)P'(A_r)^{-1})^2 \tilde{Q}(A_r) \\ &= P(A_r)^2 P'(A_r)^{-2} \tilde{Q}(A_r) \end{aligned}$$

où on a utilisé le fait que $P(A_r)$ et $P'(A_r)^{-1}$ commutent, car ce sont des polynômes en A. Ainsi, puisque $P(A_r)$, $P'(A_r)^{-1}$ et $\tilde{Q}(A_r)$ commutent (pour la même raison), alors $P(A_{r+1})$ est nilpotente car $P(A_r)$ l'est, et son indice de nilpotence n_{r+1} vérifie

$$n_{r+1} \leqslant \frac{n_r + 1}{2} \leqslant 1 + \frac{n-1}{2^{r+1}},$$

d'où (i).
De plus, on a $P \wedge P' = 1$ donc par théorème de Bézout, il existe $U, V \in \mathbb{K}[X]$ tels que $UP + VP' = 1$. On a donc

$$B_{r+1} := V(A_{r+1})P'(A_{r+1}) = I_n - U(A_{r+1})P(A_{r+1}).$$

Or, $U(A_{r+1})P(A_{r+1})$ est nilpotente car $P(A_{r+1})$ l'est et ces matrices commutent. Ainsi, $B_{r+1} = I_n + N_{r+1}$ avec N_{r+1} nilpotente, donc $\mathrm{Sp}(B_{r+1}) = \mathrm{Sp}(I_n) = \{1\}$ et B_{r+1} est inversible. Il en résulte que $P'(A_{r+1})$ l'est aussi, d'où (ii).
Enfin, A_{r+2} est donc bien défini et est dans $\mathbb{K}[A]$ car A_{r+1}, $P(A_{r+1})$ et $P'(A_{r+1})^{-1}$ sont tous des polynômes en A, d'où (iii).

Étape 3. On en déduit la décomposition de Dunford de A.

Pour $m \geqslant \log_2(n)$, $P(A_m)$ est nilpotente d'indice au plus 1, c'est-à-dire $P(A_m) = 0$. Donc la suite $(A_r)_{r \in \mathbb{N}}$ est stationnaire à A_m, avec $m = \lfloor \log_2(n) \rfloor + 1$. Puisque P est simplement scindé et annule A_m, alors A_m est diagonalisable.

De plus, on a

$$A - A_m = \sum_{k=0}^{m-1} (A_k - A_{k+1}) = \sum_{k=0}^{m-1} P(A_k)P'(A_k)^{-1}.$$

Comme $P(A_k)$ et $P'(A_k)^{-1}$ commutent (ce sont des polynômes en A) et que $P(A_k)$ est nilpotente, alors $P(A_k)P'(A_k)^{-1}$ est nilpotente. Donc $A - A_m$ est une somme de matrices nilpotentes qui commutent (car ce sont toutes des polynômes en A). Il en résulte que $A - A_m$ est nilpotente.

Enfin, puisque A_m et $A - A_m$ sont des polynômes en A donc commutent, la décomposition de Dunford de A est bien

$$A = D + N \text{ avec } D = A_m \text{ et } N = A - A_m.$$

□

Proposition 3.8. Si $\chi_u = \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$ est scindé, soit $P \in \mathbb{K}[X]$ tel que pour tout $1 \leqslant k \leqslant r$, $P = \lambda_k \ [(X - \lambda_k)^{m_k}]$. Alors la décomposition de Dunford de u est

$$u = P(u) + (u - P(u)).$$

Exemple. Soit $M = \begin{pmatrix} 1 & 2 & 0 \\ 0 & -2 & 0 \\ 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$. Alors $\chi_M = (X-1)^2(X+2)$. On cherche un polynôme P tel que

$$\begin{cases} P &= 1 \quad [(X-1)^2] \\ P &= -2 \quad [X+2] \end{cases}$$

Pour cela, on applique l'algorithme d'Euclide étendu à $A = (X-1)^2$ et $B = X + 2$ pour obtenir une relation de Bézout. On pose

$$(R_0, R_1) = (A, B), \ (U_0, U_1) = (1, 0), \ (V_0, V_1) = (0, 1).$$

On a $R_0 = (X-4)R_1 + 9$, de sorte que $R_2 = 9$ est inversible. On a donc

$$U_2 = U_0 - (X-4)U_1 = 1 \text{ et } V_2 = V_0 - (X-4)V_1 = 4 - X.$$

On obtient comme relation de Bézout $R_0U_2 + R_1V_2 = R_2$, c'est-à-dire

$$AU + BV = 1 \text{ avec } U = \frac{U_2}{R_2} = \frac{1}{9} \text{ et } V = \frac{V_2}{R_2} = \frac{4 - X}{9}.$$

Posons alors $P = 1 \times BV + (-2) \times AU$. On a bien $P = 1 \ [A]$ et $P = -2 \ [B]$. On calcule $P = \frac{-1}{3}(X^2 - 2X - 2)$ puis

$$D = P(M) = \begin{pmatrix} 1 & 2 & 0 \\ 0 & -2 & 0 \\ 0 & \frac{1}{3} & 1 \end{pmatrix} \text{ et } N = M - D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & \frac{2}{3} & 0 \end{pmatrix}.$$

On aurait pu aller plus vite et se dispenser d'appliquer l'algorithme d'Euclide. En effet, on doit avoir $P(X) = 1 + Q(X)(X-1)^2$ et $P(-2) = -2$, c'est-à-dire $1 + Q(-2) \times 9 = -2$. Prenons donc Q constant égal à $\frac{-1}{3}$. On a alors $P = 1 - \frac{1}{3}(X-1)^2 = \frac{-1}{3}(X^2 - 2X - 2)$.

Voyons maintenant quelques applications de la décomposition de Dunford.

Application 3.9. Soit $\chi_u = \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$ et $P \in \mathbb{C}[X]$. Alors $P(u)$ est diagonalisable si et seulement si $P^{(i)}(\lambda_k) = 0$ pour tout $1 \leqslant k \leqslant r$ et $1 \leqslant i \leqslant m_k - 1$.

Application 3.10. Soit $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\mathrm{Sp}(A) \subset \{\mathrm{Re}(z) < 0\}$. Alors il existe des constantes $a > 0$ et $K > 0$ telles que pour tout temps $t \geqslant 0$, $\|\exp(tA)\| \leqslant Ke^{-at}$. Ceci est utile pour étudier la stabilité des solutions d'équations différentielles.

Proposition 3.11. Soit $u = d + n$ la décomposition de Dunford de u. Alors la décomposition de Dunford de $\exp(u)$ est $\exp(u) = \exp(d) + \exp(d)(\exp(n) - \mathrm{id})$.

Application 3.12. L'endomorphisme u est diagonalisable si et seulement si $\exp(u)$ est diagonalisable.

Proposition 3.13. La fonction $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

Questions du jury et du public

Voici quelques questions qui ont été posées suite à la présentation de cette leçon devant la classe, et les réponses que nous avons essayées d'apporter avec des compléments du professeur encadrant.

Question 1. De quoi aurait-on pu parler dans cette leçon qui ne figure pas dans le plan ?

Réponse. On aurait pu parler du commutant $\mathcal{C}(u)$ d'un endomorphisme, et évoquer des résultats comme : u cyclique $\Leftrightarrow \mathcal{C}(u) = \mathbb{K}[u]$. On peut prolonger cela en introduisant également le bicommutant.

Le théorème spectral ainsi que des applications auraient également pu être mentionnés. □

Question 2. Quelles différences entre les résultats de Jordan et Dunford ?

Réponse. Le théorème de Jordan est une réduction : il fournit une matrice particulière dans la classe de similitude de la matrice considérée. Ce résultat fait intervenir un changement de base : la forme réduite de Jordan d'un endomorphisme est la matrice de cet endomorphisme dans une certaine base.

Le théorème de Dunford est une décomposition : il ne donne pas la matrice de l'endomorphisme dans une certaine base, mais met en évidence deux autres endomorphismes, l'un diagonalisable et l'autre nilpotent. □

Question 3. Peut-on obtenir la décomposition de Dunford en connaissant la réduction de Jordan ?

Réponse. A priori, non. En effet, une forme réduite de Jordan se décompose immédiatement en une somme d'une matrice diagonale et d'une matrice nilpotente. Néanmoins, ces matrices

ne sont pas forcément des polynômes en la matrice initiale et ne commutent pas forcément. Ainsi, la matrice diagonale n'est pas nécessairement semblable à la matrice diagonalisable apparaissant dans la décomposition de Dunford. □

Question 4. Peut-on obtenir la réduction de Jordan en connaissant la décomposition de Dunford ?

Réponse. Si $u = d + n$ est la décomposition de Dunford de u, alors d et n commutent. Si on est sur un corps algébriquement clos (par exemple $\mathbb{C}$), on peut donc cotrigonaliser d et n. Les sous-espaces propres de d sont stables par d et n, de sorte que dans la base de cotrigonalisation, la matrice de d est en fait diagonale ; celle de n est diagonale par blocs, chacun des blocs étant triangulaire. On peut faire le travail habituel pour obtenir la réduction de Jordan (suite des noyaux itérés) sur chacun de ces blocs. □

Question 5. Réduire un endomorphisme, c'est chercher une base dans laquelle il s'exprime simplement. Qu'est-ce que cela signifie en termes de matrices ? Et quel peut-être l'intérêt ?

Réponse. On cherche une matrice dans la classe de similitude qui soit plus simple que les autres : diagonale (par blocs), triangulaire,... On y trouve un intérêt pratique de calcul. De plus, si on peut trouver une matrice à la forme simple dans chaque classe de similitude, on peut par exemple répondre à des problèmes de dénombrement (voir l'application 1.17 à la suite de la réduction de Frobenius). □

Question 6. Application du théorème de Lie-Kolchin ?

Réponse. De façon analogue à la théorie de Galois sur la résolubilité par radicaux des équations polynomiales, il existe une théorie de la résolubilité par quadratures (c'est-à-dire uniquement à l'aide de primitives) des équations différentielles. Un résultat énonce qu'une équation différentielle est résoluble si et seulement si la composante connexe de l'élément neutre d'un groupe, s'identifiant à un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$, est résoluble. Le théorème de Lie-Kolchin est utile dans ce cadre.

Ceci dépasse toutefois largement mes connaissances et le cadre de l'agrégation. Je pense qu'on peut se contenter de présenter ce théorème comme une généralisation de la propriété de cotrigonalisation d'endomorphismes qui commutent. □

Question 7. Déterminer la décomposition de Dunford de la matrice suivante, où $a \neq b$:

$$A = \begin{pmatrix} a & x & z \\ 0 & a & y \\ 0 & 0 & b \end{pmatrix} \in \mathcal{M}_3(\mathbb{C}).$$

Réponse. On calcule $\chi_A = (X-a)^2(X-b)$. En suivant la proposition 3.8, on cherche un polynôme P tel que $P = a\ [(X-a)^2]$ et $P = b\ [X-b]$. On peut chercher P sous la forme $P(X) = a + Q(X)(X-a)^2$. La condition $P(b) = b$ suggère de prendre $Q(X) = \frac{1}{b-a}$, et donc

$$P(X) = a + \frac{(X-a)^2}{b-a}.$$

On calcule alors

$$D = P(A) = \begin{pmatrix} a & 0 & z + \frac{xy}{b-a} \\ 0 & a & y \\ 0 & 0 & b \end{pmatrix} \text{ et } N = A - D = \begin{pmatrix} 0 & x & \frac{-xy}{b-a} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

□

Question 8. Démonstration du théorème de Cayley-Hamilton.

Réponse. Plusieurs démonstrations sont possibles. Celles données dans le plan conviennent dans le cas général. Une autre démonstration générale fait intervenir la formule de la comatrice.

Comme mentionné dans le plan, si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ on peut donner une démonstration plus spécifique en utilisant la densité des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{C})$. On montre que le résultat est vrai pour les matrices diagonales, et donc pour les matrices diagonalisables, puis on approche une matrice quelconque à cœfficients réels ou complexes par une suite de matrices complexes diagonalisables. Le déterminant étant une fonction continue, on obtient le résultat souhaité. □

Question 9. Soit $A, B \in \mathcal{M}_n(\mathbb{C})$ deux matrices qui commutent, et

$$P(X, Y) = \det(YA - XB) \in \mathbb{C}[X, Y].$$

Montrer que $P(A, B) = 0$.

Réponse. Cela fait penser à des polynômes caractéristiques. On va travailler pour se ramener à l'application du théorème de Cayley-Hamilton.

Supposons d'abord A inversible. Alors

$$\begin{aligned} P(X, Y) &= \det(A) \det(YI_n - XA^{-1}B) \\ &= \det(A) X^n \det\left(\frac{Y}{X} I_n - A^{-1}B\right) \\ &= \det(A) X^n \chi_{A^{-1}B}\left(\frac{Y}{X}\right). \end{aligned}$$

Notons $Q(X, Y) = X^n \chi_{A^{-1}B}\left(\frac{Y}{X}\right)$ et $\chi_{A^{-1}B} = \sum_{k=0}^{n} a_k X^k$, de sorte que $Q(X, Y) = \sum_{k=0}^{n} a_k Y^k X^{n-k}$.
En utilisant l'inversibilité de A et le fait que A et B commutent, on a

$$\begin{aligned} Q(A, B) &= \sum_{k=0}^{n} a_k B^k A^{n-k} \\ &= A^n \sum_{k=0}^{n} a_k B^k A^{-k} \\ &= A^n \sum_{k=0}^{n} a_k (A^{-1}B)^k \\ &= A^n \chi_{A^{-1}B}(A^{-1}B) \\ &= 0. \end{aligned}$$

Donc $P(A, B) = \det(A) Q(A, B) = 0$.

Le cas général s'en déduit alors par densité de $\mathrm{GL}_n(\mathbb{C})$ dans $\mathcal{M}_n(\mathbb{C})$ et continuité du déterminant. □

Références

[BMP05] Vincent Beck, Jérôme Malick et Gabriel Peyré : *Objectif agrégation.* H&K, 2005.

[CG17] Philippe Caldero et Jérôme Germoni : *Nouvelles histoires hédonistes de groupes et de géométries - Tome 1.* Calvage & Mounet, 2017.

[CL05] Antoine Chambert-Loir : *Algèbre corporelle.* Éditions de l'École Polytechnique, 2005.

[FGN09] Serge Francinou, Hervé Gianella et Serge Nicolas : *Oraux X-ENS, algèbre 2.* Cassini, 2009.

[Gou08] Xavier Gourdon : *Algèbre.* Les maths en tête. Ellipses, 2008.

[Gri11] Joseph Grifone : *Algèbre linéaire.* Cépaduès, 2011.

[MM12] Roger Mansuy et Rached Mneimné : *Algèbre linéaire - Réduction des endomorphismes.* Vuibert, 2012.