Idempotents de $\mathbb{K}[u]$, Dunford et Exponentielle de matrices

Introduction

Ce développement est constitué de beaucoup de choses :

— un beau diagramme commutatif reliant le lemme chinois et le lemme des noyaux

— ... qui donne une preuve rapide et élégante de la description des idempotents de $\mathbb{K}[u]$

— ... d'où une preuve rapide de la décomposition de Dunford.

— la surjectivité de l'exponentielle de matrices sur $\mathbb{C}$ (qui ici requiert le travail précédent puisqu'il faut se servir du fait que les composantes de la décomposition de Dunford sont des polynômes en u),

— ... si bien présentée qu'on pourra en déduire très rapidement l'image de l'exponentielle de matrices sur $\mathbb{R}$.

La divsersité des sujets abordés donne un bon recasage à ce développement. Cependant, il est en soi bien trop long pour être présenté entièrement. Dans la section 1, il est bon d'aller assez vite car les constructions effectuées sont très naturelles. Pour gagner du temps, certains bouts de démonstration peuvent être omis et simplement mentionnés à l'oral tellement ils sont naturels (par exemple, le calcul du polynôme minimal de u_{C_i} où C_i est un sous-espace caractéristique de u peut être annoncé comme un corollaire immédiat de ce qui précède. En regardant le jury droit dans les yeux, vous saurez le convaincre du fait que pour vous c'est clair et que vous pouvez donc passer à la suite lol).

Selon les recasages, il est plus ou moins nécessaire de tout prouver. Par exemple, dans une leçon où le côté « exponentielle de matrices » est plus important, il faudra présenter correctement sa surjectivité sur $\mathbb{C}$ et son image sur $\mathbb{R}$. Pour cela, il faut aller vite sur la partie « algèbre », enlever les corollaires inutiles (comme la desciption complète des idempotents de $\mathbb{K}[u]$: seul le fait que les projecteurs sont des polynômes en u compte pour prouver l'existence de Dunford, dont on pourrait d'ailleurs se passer de l'unicité).

Pour une leçon où le côté « algèbre » est plus important, on pourra faire un peu moins d'exponentielle de matrices.

I. Théorème des restes chinois versus lemme des noyaux

1. Généralités

Soit E un $\mathbb{K}$-espace vectoriel (de dimension quelconque). Si u en est un endomorphisme et si V en est un sous-espace stable, on notera par abus $u_{|V} = u_{|V}^{|V}$. On note $\mathrm{res}_V : \mathbb{K}[u] \to \mathbb{K}\big[u_{|V}\big]$ le morphisme de restriction et corestriction bien défini puisqu'il envoie un élément de la forme $P(u)$ vers un élément de la forme $P\big[u_{|V}\big]$.

Si E est un $\mathbb{K}$-espace vectoriel et $f_i : E \to F_i$ est une collection de morphismes, alors on note $(f_i)_i : E \to \prod_i F_i$ le morphisme naturellement induit. De même, si $f_i : E_i \to F_i$ est une collection de morphismes, on notera sans ambiguïté avec le cas précédent : $(f_i)_i : \prod_i E_i \to \prod_i F_i$ le morphisme induit.

2. Quatre morphismes magiques

Soit u un endomorphisme de E, fixé. On suppose que u admet un polynôme annulateur dans $\mathbb{K}[X]$ (par exemple si E est de dimension finie), et on note π_u le polynôme minimal annulateur.

On note $\pi_u = \prod_{i=1}^{r} P_i^{n_i}$ où P_i sont dans $\mathbb{K}[X]$, irréductibles et unitaires. Le théorème chinois fournit un isomorphisme qu'on note $c : \mathbb{K}[X]/(\pi_u) \to \prod_{i=1}^{r} \mathbb{K}[X]/(P_i^{n_i})$. On note $C_i = C_{P_i}(u) = \mathrm{Ker}(P_i^{n_i}(u))$ l'espace caractéristique de u associé au polynôme irréductible P_i. On pose $u_i = u_{|C_{P_i}(u)}$.

On note $r : \mathbb{K}[u] \to \prod_{i=1}^{r} \mathbb{K}[u_{|C_i(u)}]$ le morphisme $r = \left(\mathrm{res}_{C_i(u)}\right)_{i=1,\dots,r}$ (qui à un polynôme en u associe la liste chaque restriction à chaque sous-espace caractéristique de u). Le lemme des noyaux nous apprend que la somme des C_i vaut E donc ce morphisme r est injectif.

Puisque le noyau du morphisme d'évaluation en u $\mathrm{ev}_u : \mathbb{K}[X] \to \mathbb{K}[u]$ est (π_u) et puisque ce morphisme est surjectif, le premier théorème d'isomorphisme donne un isomorphisme $\mathrm{ev}_u : \mathbb{K}[X]/(\pi_u) \to \mathbb{K}[u]$.

Puisque u_i est annulé par $P_i^{n_i}$, on a un morphisme $\mathbb{K}[X]/(P_i^{n_i}) \to \mathbb{K}[u_i]$, qui est clairement surjectif. Attention, on n'a pas encore montré que c'est son polynôme annulateur, donc on ne sait pas encore que c'est un isomorphisme. On a donc un morphisme $(\mathrm{ev}_{u_i})_i : \prod_{i=1}^{r} \mathbb{K}[X]/(P_i^{n_i}) \to \prod_{i=1}^{r} \mathbb{K}[u_i]$. Il est cependant clair qu'il est surjectif.

3. Le diagramme magique

Théorème I.3.1.
Le diagramme suivant est commutatif :

$$\begin{tikzcd}
\mathbb{K}[X]/(\pi_u) \arrow[r, "c"'] \arrow[d, "\mathrm{ev}_u"'] & \prod_{i=1}^{r} \mathbb{K}[X]/(P_i^{n_i}) \arrow[d, "(\mathrm{ev}_{u_i})_i"] \\
\mathbb{K}[u] \arrow[r, "r"] & \prod_{i=1}^{r} \mathbb{K}[u_i]
\end{tikzcd}$$

De plus, ces quatre flèches sont des isomorphismes.

Preuve. On va montrer que $r \circ \mathrm{ev}_u = (\mathrm{ev}_{u_i})_i \circ c$. Soit $P \in \mathbb{K}[X]$. Si $Q \in \mathbb{K}[X]$, note $P \bmod Q$ la classe de P dans $\mathbb{K}[X]/(Q)$. D'une part :

$$\begin{aligned}
(\mathrm{ev}_{u_i})_i \circ c(P \bmod \pi_u) &= (\mathrm{ev}_{u_i})_i((P \bmod P_i^{n_i})_i) \\
&= (\mathrm{ev}_{u_i}\,(P \bmod P_i^{n_i}))_i = (P(u_i))_i.
\end{aligned}$$

D'autre part :

$$r \circ \mathrm{ev}_u(P \bmod \pi_u) = r(P(u)) = (\mathrm{res}_{C_{P_i}(u)}\,(P(u)))_i = (P(u_i))_i.$$

Le diagramme est donc bien commutatif. res_u est un isomorphisme et r est injectif donc $r \circ \mathrm{res}_u$ est injectif donc $(ev_{u_i})_i\circ$ est injectif. Mais c est un isomorphisme donc $(ev_{u_i})_i$ est injective aussi.

D'ailleurs, puisque chaque ev_{u_i} est surjectif, le produit $(ev_{u_i})_i$ l'est également. Donc puisque c est un isomorphisme, $(ev_{u_i})_i \circ c$ est surjective donc r doit être surjective.

Mais res_u est un isomorphisme donc $r \circ \mathrm{res}_u$ est surjective donc $(ev_{u_i})_i$ est surjective. Donc $(ev_{u_i})_i$ est un isomorphisme donc finalement r aussi. Magique, non ? □

Corollaire I.3.2.
Le polynôme minimal de u_i est bien $P_i^{n_i}$.

Preuve. Les $ev_{u_i} : \mathbb{K}[X]/(P_i^{n_i}) \to \mathbb{K}[u_i]$ sont des isomorphismes par ce qui précède. Si π_{u_i} est le polynôme minimal de u_i, alors son image est nulle par ev_{u_i}. Donc $\pi_{u_i} \bmod P_i^{n_i} = 0 \bmod P_i^{n_i}$ donc $P_i^{n_i} \mid \pi_{u_i}$. Mais $P_i^{n_i}$ annule u_i donc, par minimalité de π_{u_i}, on a la divisibilité réciproque. □

Corollaire I.3.3.
Les projecteurs $p_i : E \to E$ sur les C_i parallèlement à $\oplus_{j\neq i} C_j$ sont des polynômes en u qu'on note $P_i(u)$. Les éléments idempotents de $\mathbb{K}[u]$ sont exactement les $\sum_i \varepsilon_i p_i$ où $\varepsilon_i \in \{0,1\}$.

Preuve. Soit $i \in [\![1,r]\!]$. On remarque que l'élément $(a_j)_j \in \prod_{j=1}^{r} \mathbb{K}[u_j]$ défini par $a_j = 0_{C_j}$ si $j \neq i$ et $a_i = \mathrm{id}_{C_i}$ est idempotent (de carré égal à lui-même) donc admet un antécédent idempotent par l'isomorphisme r. On note cet antécédent $P_i(u)$ avec $P_i \in \mathbb{K}[X]$. $P_i(u)$ est donc un projecteur, il est nul sur $\oplus_{j\neq i} C_j$ et vaut l'identité sur C_i, c'est le projecteur cherché.

Soit $v = V(u)$ un idempotent de $\mathbb{K}[u]$. Alors si on regarde $r(v)$, ses coordonnées, v_i, sont des idempotents des algèbres $\mathbb{K}[u_i]$. Donc $v_i = V(u_i)$ est un endomorphisme de $C_{P_i}(u)$ qui est un projecteur. Donc $V(V-1)$ est nul dans $\mathbb{K}[X]/(P_i^{n_i})$. Donc $P_i^{n_i} \mid V(V-1)$ mais $V \wedge V-1 = 1$, par conséquent, P_i divise V ou $1-V$. Donc soit c'est $V(u_i) = 0$, soit $V(u_i) = \mathrm{id}_{C_{P_i}(u)}$. Cela signifie que v vaut 0 ou l'identité sur chacun des $C_{P_i}(u)$ donc est une somme de p_i. □

II. Application : la décomposition de Dunford

Théorème II.0.1. Décomposition de Dunford
Soit u un endomorphisme du $\mathbb{K}$-espace vectoriel E supposé de dimension finie [a]*. Alors il existe un unique couple d, n d'endomorphismes de E qui commutent, où d est diagonalisable et n est nilpotent tels que $u = d + n$. De plus :*

- *d et n sont des polynômes en u.*
- *La partie diagonalisable de u, d, a le même polynôme caractéristique que u.* [b] *En particulier, ils ont le même spectre. En particulier, d est inversible si et seulement si u est inversible.*
- *(vraiment facultatif) Il existe une base de E adaptée aux sous-espaces caractéristiques de E telle que la matrice de d soit diagonale et que celle de n soit sa forme de Jordan.*

a. Sans cette hypothèse, le théorème marche encore mais le mot « diagonalisable » serait à redéfinir.
b. pas le même polynôme annulateur !! d est annulée par $\prod_i (X - \lambda_i)$ alors que u pas forcément

Preuve. On remarque que $(u_i - \lambda_i \mathrm{id}_{C_i})^{n_i} = 0$ donc si on écrit $n_i = u_i - \lambda_i \mathrm{id}_{C_i}$, alors n_i est un endomorphisme nilpotent de C_i. On remarque que $\sum_i p_i = \mathrm{id}_E$. Donc, si $x \in E$, alors $u(x) = \sum_i u(p_i(x)) = \left(\sum_i \lambda_i p_i\right)(x) + \left(\sum_i n_i \circ p_i\right)(x) := d(x) + n(x)$.

On vérifie aisément que d est diagonalisable (prendre une base adaptée à la décomposition de E comme somme des C_i) et que le second est nilpotent (si $x = \sum_i x_i$, alors $n^l(x) = \sum_i n^l(x_i) = \sum_i n_i^l(x_i)$, tout est donc nul pour l assez grand puisque les n_i sont déjà nilpotents). Le premier terme, que l'on nomme d, est une combinaison linéaire de polynômes en u donc en est un. Comme $n = u - d$, c'est aussi le cas de n. Cela démontre l'existence et l'appartenance à $\mathbb{K}[u]$ de d et n.

Supposons que $d + n = d' + n'$ où (d', n') est un autre couple. On sait que (d, n) sont des polynômes en u. Comme n' et d' commutent avec u, on a que d commute avec d' et que n commute avec n'. Donc $d - d'$ est diagonalisable (codiagonaliser) et $n - n'$ est nilpotent (binôme de Newton). On a de plus :

$d - d' = n' - n$. On constate qu'alors $d - d'$ est à la fois diagonalisable et nilpotent donc nul. Donc $(d, n) = (d', n')$.

Regardons pourquoi $\chi_u = \chi_d$. Chaque u_i a son polynôme minimal scindé donc est trigonalisable. Il en suit donc par recollement une base de E dans laquelle u est triangulaire, et d a pour matrice la diagonale de celle de u. Et dans ce cas-là, χ_u et χ_d ne dépendent que ce cette même diagonale donc sont égaux.

(pour la partie facultative) Décomposer u en forme de Jordan. Alors une partie diagonalisable et une partie nilpotente apparaissent automatiquement. Par unicité, c'est exactement la décomposition de Dunford de u. □

III. Application à l'exponentielle de matrices

Si $A = D + N$, alors $e^A = e^D + e^D(e^N - 1)$ est la décomposition de Dunford de e^A. Cela va nous permettre de caractériser l'image de l'exponentielle de matrices.

Lemme III.0.1.
Soit $\mathbb{K}$ quelconque. Si $M \in \mathcal{M}_n(\mathbb{K})$ est nilpotente, alors $M^n = 0$

Lemme III.0.2.
Soit $n \in \mathbb{N}^*$. Soit $P = \sum_{k=0}^{n} \frac{X^k}{k!}$ et $Q = \sum_{k=1}^{n} (-1)^{k-1} \frac{X^k}{k}$. Alors $P \circ Q \equiv 1 + X[X^n]$.

Preuve. Prouvons la première formule. Si $x > -1$, alors $\exp(\ln(1+x)) = 1 + x$. Or, le développement limité de $\ln(1+x)$ en 0 à l'ordre n est $Q(x)$, et celui de $\exp(x)$ en 0 est $P(x)$. Comme $\ln(1+x)$ est nulle en 0, le développement limité de $\exp(\ln(1+x))$ en 0 à l'ordre n est donné par $P = \circ Q$, modulo les monômes de degrés $> n$. Mais ce développement limité est égal à celui de $1 + x$. Donc $P \circ Q \equiv 1 + X[X^n]$ dans $\mathbb{R}[X]$. □

Lemme III.0.3.
Soit $\mathbb{K}$ le corps $\mathbb{R}$ ou $\mathbb{C}$. Alors la fonction $M \mapsto e^M - I_n$, où M parcourt l'ensemble des matrices nilpotentes de $\mathcal{M}_n(\mathbb{K})$, atteint toutes les matrices nilpotentes de $\mathcal{M}_n(\mathbb{K})$. De plus, il existe un polynôme qui à N nilpotent associe un antécédent nilpotent par l'exponentielle.

Preuve. Soit N une matrice nilpotente à coefficients dans $\mathbb{K}$. Alors avec les notations du lemme III.0.2, on a $P \circ Q(N) = 1 + N$ puisque $N^n = 0$. $Q(0) = 0$ donc $Q(N)$ est une somme de matrices nilpotentes qui commutent donc est nilpotente. Donc $P(Q(N))$ est égale à $e^{Q(N)}$. Cela signifie que $e^{Q(N)} - 1 = N$. □

Théorème III.0.4. Images de l'exponentielle

(i) L'exponentielle de matrices $\mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective. De plus, toute matrice $M \in \mathrm{GL}_n(\mathbb{C})$ admet un antécédent qui est un polynôme en M.

(ii) L'image de $\mathcal{M}_n(\mathbb{R})$ par l'exponentielle est l'ensemble $\{M^2 \mid M \in \mathrm{GL}_n(\mathbb{R})\}$. De plus, on peut demander à un antécédent de M^2 d'être un polynôme en M.

Preuve. Soit $M \in \mathrm{GL}_n(\mathbb{C})$. π_M est scindé dans $\mathbb{C}$ donc $M = D_0 + N_0$ où D_0 est diagonalisable dans $\mathbb{C}$. Si $A = D + N$, alors $e^A = e^D + e^D(e^N - I_n)$ est sa décomposition de Dunford. Donc $e^A = M$ signifie $D_0 = e^D$ et $N_0 = e^D(e^N - I_n)$. Si $D_0 = P \operatorname{diag}(\lambda_1, \ldots, \lambda_n) P^{-1}$, alors on prend, par surjectivité de l'exponentielle sur $\mathbb{C}^\times$, des μ_i tels que $\exp(\mu_i) = \lambda_i$, et on pose $D = P \operatorname{diag}(\mu_1, \ldots, \mu_n) P^{-1}$. Comme $N_0 = e^D(e^N - I_n) = (e^N - I_n)e^D$, on a $e^{-D} N_0 = e^N - I_n = N_0 e^{-D}$. Donc N_0 commute avec e^{-D}. Donc $N_0 e^D$ est nilpotente donc, par le lemme III.0.3, il existe effectivement N nilpotente telle que $e^N - I_n = e^{-D} N_0$.

On suppose pour l'instant que D est un polynôme en D_0. C'est donc un polynôme en M (polynomialité de la décomposition de Dunford). On constate alors par le lemme III.0.3 que N peut être choisie comme

étant un polynôme en $e^{-D}N_0$ donc obtenue comme polynôme en D et en N_0 donc comme un polynôme en M. Donc, dans ce cas, $A = D + N$ est un polynôme en M. On prouve maintenant que D peut effectivement être choisi comme un polynôme en D_0. On s'arrange tout d'abord pour que, lors du choix des μ_i, on ait $\lambda_i = \lambda_j \Rightarrow \mu_i = \mu_j$. Il n'y a donc qu'à prendre le polynôme d'interpolation de Lagrange qui envoie les λ_i sur les μ_i. Alors ce polynôme en D_0 vaut D. Conclusion de ce paragraphe : A peut être choisi comme un polynôme en M.

Pour la surjectivité dans $\mathbb{R}$: on a $e^A = \left(e^{A/2}\right)^2$ donc une inclusion est vraie. Pour l'inclusion réciproque, soit $M \in \mathrm{GL}_n(\mathbb{R})$, montrons que M^2 est dans l'image de l'exponentielle. Par le point précédent, il existe $A = Q(M) \in \mathcal{M}_n(\mathbb{C})$ un polynôme en M telle que $e^A = M$ mais M est réelle et l'exponentielle passe à la conjugaison donc $e^{\overline{Q}(M)} = e^{\overline{A}} = M$. Comme deux polynômes en M commutent toujours, $M^2 = e^{\overline{Q}(M)+Q(M)} = e^{(Q+\overline{Q})(M)}$ ce qui conclut la preuve. $\square$