Mémoire de M2 Agreg
Endomorphismes diagonalisables en dimension finie

Salim Rostam

Année 2013–2014

Table des matières

Introduction

Motivations. Les matrices les plus simples à étudier sont les matrices diagonales ; en effet, la k-algèbre des matrices diagonales de taille n sur un corps k est canoniquement isomorphe à la k-algèbre commutative k^n. Ainsi, un endomorphisme qui admet dans une base une matrice diagonale sera plus simple à étudier, en particulier on pourra plus facilement comprendre son action sur les vecteurs.

Quelques notations et conventions. Dans la suite, on considère un espace vectoriel E de dimension *finie* $n \in \mathbb{N}^*$ sur un corps k quelconque ; on procède à l'identification $\mathcal{M}_n(k) \simeq \mathcal{L}(k^n)$ via la base canonique de k^n, en particulier les définitions données pour des éléments de $\mathcal{L}(E)$ se transposent pour des éléments de $\mathcal{M}_n(k)$.

Pour $M \in \mathcal{M}_n(k)$, on note M^{T} la transposée de la matrice M. Enfin, si rien n'est précisé u désigne un élément de $\mathcal{L}(E)$.

1 Définitions

1.1 Éléments propres

Définition 1.1. On dit que $\lambda \in k$ est une *valeur propre* de u s'il existe $x \in E \setminus \{0\}$ tel que $u(x) = \lambda x$; on dit que x est un *vecteur propre* de u associé à la valeur propre λ.

Remarque 1.2. On insiste sur le fait que par définition, un vecteur propre est *non nul*.

Exemple 1.3. Soit $M := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{Q})$; on a $M \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 \\ 2 \end{smallmatrix}\right)$ donc $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ est un vecteur propre de M associé à la valeur propre 2.

Définition 1.4. Le *spectre* de u, noté $\mathrm{Sp}(u)$, est l'ensemble de ses valeurs propres.

Remarque 1.5. Pour un élément $M \in \mathcal{M}_n(k)$, la notation $\mathrm{Sp}(M)$ désigne donc les valeurs propres de M dans le corps k. Si K est un sur-corps de k, on notera $\mathrm{Sp}_K(M)$ l'ensemble des valeurs propres de M vu comme élément de $\mathcal{M}_n(K)$, *i.e.* $\mathrm{Sp}_K(M) := \{\lambda \in K : \exists x \in K^n \setminus \{0\}, Mx = \lambda x\}$.

Définition 1.6. Pour $\lambda \in \mathrm{Sp}(u)$, on dit que $E_\lambda(u) := \{x \in E : u(x) = \lambda x\}$ est le *sous-espace propre* de u associé à la valeur propre λ.

Remarque 1.7. Les éléments de $E_\lambda(u)$ sont exactement les vecteurs propres de u associés à la valeur propre λ ainsi que le vecteur nul.

Propriété 1.8. *Si $\lambda \in \mathrm{Sp}(u)$ alors $E_\lambda(u) = \ker(u - \lambda \mathrm{id}_E)$, en particulier $E_\lambda(u)$ est un sous-espace vectoriel de E stable par u.*

Proposition 1.9. *Les sous-espaces propres de u sont en somme directe.*

À propos de la démonstration. Remarquons que l'on ne sait pas encore qu'il n'y a qu'un nombre fini de sous-espaces propres. En fait, par définition de la somme directe il suffit de montrer que toute somme *finie* de sous-espaces propres est directe, ce que l'on montre par exemple par récurrence sur le nombre de sous-espaces propres intervenant dans la somme. □

Corollaire 1.10. *L'endomorphisme u possède au plus n valeurs propres.*

1.2 Diagonalisabilité

Définition 1.11. On dit que l'endomorphisme u est *diagonalisable* s'il existe une base de E formée de vecteurs propres de u.

Remarque 1.12. Dans une telle base, la matrice de u est diagonale. En particulier, une matrice $M \in \mathcal{M}_n(k)$ est diagonalisable ssi il existe $D \in \mathcal{M}_n(k)$ diagonale et $P \in \mathrm{GL}_n(k)$ telles que $M = PDP^{-1}$.

Exemple 1.13. Reprenons notre matrice $M := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{Q})$ de l'exemple 1.3 : on sait déjà que $v_2 := \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ est un vecteur propre de M, associé à la valeur propre 2. On remarque également que $v_0 := \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)$ est un vecteur propre de M associé à la valeur propre 0. Les sous-espaces $E_2(M)$ et $E_0(M)$ étant en somme directe, la famille (v_2, v_0) est une base de $\mathbb{Q}^2$; comme v_2 et v_0 sont des vecteurs propres de M, la matrice M est diagonalisable et avec $P := \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ on a $P \in \mathrm{GL}_2(\mathbb{Q})$ et $M = P \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) P^{-1}$.

On voit que montrer qu'un endomorphisme est diagonalisable est assez laborieux. Dans la section suivante, on va donner des méthodes pour déterminer (plus ou moins rapidement) si un endomorphisme est diagonalisable ou non.

2 Critères de diagonalisabilité

Remarquons que, d'après la proposition 1.9, on a déjà ce résultat.

Proposition 2.1. *Si u possède n valeurs propres distinctes alors u est diagonalisable.*

Cette situation n'étant bien entendu pas générale, on va dans ce qui suit trouver d'autres critères de diagonalisabilité, en introduisant tout d'abord un outil aussi pratique que puissant : le polynôme caractéristique.

2.1 Polynôme caractéristique

Définition 2.2. Soit $M \in \mathcal{M}_n(k)$. Le *polynôme caractéristique* de M est défini par

$$\chi_M(X) := \det(M - XI_n).$$

Le polynôme caractéristique est le déterminant d'un élément de $\mathcal{M}_n(k[X])$. Ainsi, si $P \in \mathrm{GL}_n(k)$, alors $P \in \mathrm{GL}_n(k[X])$ donc $\det(M - XI_n) = \det(PMP^{-1} - XI_n)$. On peut donc énoncer la définition suivante.

Définition 2.3. Le polynôme caractéristique de u est défini comme étant le polynôme caractéristique de la matrice de u dans une base (quelconque) de E.

Voici maintenant la proposition fondamentale qui lie le polynôme caractéristique aux valeurs propres, suivie de ses conséquences.

Proposition 2.4. *Soit $\lambda \in k$; alors $\lambda \in \mathrm{Sp}(u)$ ssi $\chi_u(\lambda) = 0$.*

Démonstration. On a $\lambda \in \mathrm{Sp}(u)$ ssi $u - \lambda \,\mathrm{id}_E$ non injectif ssi $\chi_u(\lambda) = 0$. □

Remarque 2.5. On retrouve le fait que $\mathrm{Sp}(u)$ possède au plus $\deg \chi_u = n$ éléments.

Proposition 2.6. *Si $M \in \mathcal{M}_n(k)$ alors $\mathrm{Sp}_K(M) = \{\lambda \in K : \chi_M(\lambda) = 0\}$ pour tout sur-corps K de k.*

Exemple 2.7. Toujours avec la matrice $M := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{Q})$, on a $\chi_M(X) = X^2 - \mathrm{tr}(M)X + \det(M) = X^2 - 2X = X(X-2)$ donc $\mathrm{Sp}(M) = \{0, 2\}$. Remarquons que dans l'exemple 1.13, on pouvait dans un premier temps seulement conclure que $\mathrm{Sp}(M) \supseteq \{0, 2\}$ (on pouvait en fait déjà en déduire l'égalité d'après le corollaire 1.10).

Application 2.8 (calcul de la puissance p-ième d'une matrice). Soit $M := \left(\begin{smallmatrix} 3 & -2 \\ 1 & 0 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{Q})$; on a $\chi_M = X^2 - 3X + 2 = (X-1)(X-2)$ donc $\mathrm{Sp}(M) = \{1, 2\}$. On remarque que le vecteur $v_1 := \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ est un vecteur propre associé à la valeur propre 1 et que le vecteur $v_2 := \left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right)$ est un vecteur propre associé à la valeur propre 2 (note [1]). D'après la proposition 1.9 les vecteurs v_1 et v_2 forment une base de $\mathbb{Q}^2$ donc M est diagonalisable ; avec $D := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ et $P := \left(\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right)$ on a $M = PDP^{-1}$. Pour $p \in \mathbb{N}$, la puissance p-ième de M s'obtient alors simplement par $M^p = PD^pP^{-1}$ (et même pour $p \in \mathbb{Z}$ car M est inversible) ; comme $D^p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2^p \end{smallmatrix}\right)$ on a $M^p = \left(\begin{smallmatrix} 2^{p+1}-1 & 2-2^{p+1} \\ 2^p-1 & 2-2^p \end{smallmatrix}\right)$.

Remarque 2.9. On pouvait aussi procéder par interpolation : si $Q_p \in \mathbb{Q}[X]$ désigne un polynôme envoyant 1 sur 1 et 2 sur 2^p (par exemple $Q_p(X) := \frac{X-2}{1-2} + 2^p \frac{X-1}{2-1}$) on a $D^p = Q_p(D)$ donc $M^p = PD^pP^{-1} = PQ_p(D)P^{-1} = Q_p(M)$. Cette méthode a l'avantage de ne pas nécessiter le calcul de la matrice de passage P et de son inverse, mais elle peut engendrer plus de multiplications de matrices (considérer une matrice avec n valeurs propres distinctes) ; finalement, cette méthode s'applique *a priori* uniquement quand la matrice M est diagonalisable.

Dans cette application, on a bien atteint l'objectif énoncé dans les motivations : on exploite le fait que les calculs sur les matrices diagonales sont plus faciles !

Proposition 2.10. *Si k est algébriquement clos alors $\mathrm{Sp}(u) \neq \emptyset$.*

Exemple 2.11. Avec $M := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R})$, on a $\chi_M(X) = X^2 + 1$ donc $\mathrm{Sp}_{\mathbb{R}}(M) = \emptyset$ mais $\mathrm{Sp}_{\mathbb{C}}(M) = \{-i, +i\} \neq \emptyset$.

Définition 2.12. Pour $\lambda \in \mathrm{Sp}(u)$, on note m_λ sa multiplicité en tant que racine de χ_u.

Proposition 2.13. *Pour $\lambda \in \mathrm{Sp}(u)$ on a $1 \leqslant \dim E_\lambda(u) \leqslant m_\lambda$.*

Idée de démonstration. Tout d'abord, on a bien $\dim E_\lambda(u) \geqslant 1$ car $E_\lambda(u) \supsetneq \{0\}$ (on a en fait déjà utilisé ce résultat dans le corollaire 1.10). On a vu que l'espace $E_\lambda(u)$ est stable par u ; soit $\tilde{u}$ l'endomorphisme induit. On a $\tilde{u} = \lambda \,\mathrm{id}_{E_\lambda(u)}$ donc $\chi_{\tilde{u}} = (\lambda - X)^{\dim E_\lambda(u)}$. En écrivant la matrice de u dans une base adaptée à une décomposition $E = E_\lambda(u) \oplus F$, on trouve que $\chi_{\tilde{u}} | \chi_u$; on conclut par définition de m_λ. □

Exemple 2.14. Avec les notations de l'exemple 1.13 on a donc $E_2(M) = \mathrm{vect}(v_2)$ et $E_0(M) = \mathrm{vect}(v_0)$. Encore une fois, on pouvait bien sûr retrouver ces résultats en résolvant les systèmes linéaires $Mx = 2x$ et $Mx = 0$.

Application 2.15. Si u est de rang r alors par le théorème du rang on a $\dim \ker u = n - r$ donc 0 est valeur propre de u et $m_0 \geqslant n - r$. En particulier, si $r = 1$ alors $\chi_u = (-1)^n(X - \lambda)X^{n-1}$ pour un $\lambda \in k$ (éventuellement nul).

1. On peut bien sûr résoudre les systèmes linéaires $Mx = x$ et $Mx = 2x$ en la variable $x \in \mathbb{Q}^2$.

2.2 Caractérisations avec les éléments propres

Fort des résultats du paragraphe précédent, on peut désormais énoncer un théorème très important.

Proposition 2.16. *Les propositions suivantes sont équivalentes :*

(*i*) *u est diagonalisable ;*

(*ii*) $E = \oplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u)$;

(*iii*) $n = \sum_{\lambda \in \mathrm{Sp}(u)} \dim E_\lambda(u)$;

(*iv*) *χ_u est scindé sur k et* $\forall \lambda \in \mathrm{Sp}(u), \dim E_\lambda(u) = m_\lambda$.

Idée de démonstration. On montre les implications en remontant.

(*iv*) $\Rightarrow$ (*iii*) χ_u est scindé sur k donc d'après la proposition 2.4 les racines de χ_u sont exactement les éléments de $\mathrm{Sp}(u)$. Ainsi, $\chi_u = \prod_{\lambda \in \mathrm{Sp}(u)} (\lambda - X)^{m_\lambda}$ donc comme χ_u est de degré n on a $\sum_{\lambda \in \mathrm{Sp}(u)} m_\lambda = n$. D'après la deuxième hypothèse on a donc $\sum_{\lambda \in \mathrm{Sp}(u)} \dim E_\lambda(u) = n$.

(*iii*) $\Rightarrow$ (*ii*) On sait déjà par la proposition 1.9 que les $E_\lambda(u)$ pour $\lambda \in \mathrm{Sp}(u)$ sont en somme directe. Ainsi, $E \supseteq \oplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u)$ et on conclut par égalité des dimensions.

(*ii*) $\Rightarrow$ (*i*) On peut trouver une base de E constituée de vecteurs propres de u.

(*i*) $\Rightarrow$ (*iv*) Il existe une base de E formée de vecteurs propres de u. En écrivant la matrice de u dans une telle base, on trouve que χ_u est scindé sur k et que $\dim E_\lambda(u) \geqslant m_\lambda$ $\forall \lambda \in \mathrm{Sp}(u)$. On conclut par la proposition 2.13.

□

Voici deux corollaires très utiles.

Corollaire 2.17 (déja vu)**.** *Si u possède n valeurs propres distinctes alors u est diagonalisable.*

Corollaire 2.18. *Si χ_u est scindé sur k à racines simples alors u est diagonalisable.*

Remarque 2.19. Bien que ces deux corollaires soient équivalents, le deuxième va être généralisé par le théorème 2.22 et le corollaire 3.4.

2.3 Caractérisations avec des polynômes annulateurs

Lemme 2.20 (lemme de décomposition des noyaux)**.** *Si P et Q sont deux polynômes de $k[X]$ premiers entre eux, on a* $\ker(PQ)(u) = \ker P(u) \oplus \ker Q(u)$.

Remarque 2.21. Par une récurrence immédiate, le lemme s'étend à N polynômes deux à deux premiers entre eux.

Vient alors un théorème très important et très utile.

Théorème 2.22. *L'endomorphisme u est diagonalisable* ssi *u est annulé par un polynôme (non nul) de $k[X]$ scindé sur k à racines simples.*

Idée de démonstration. On applique le fait que (*i*) $\Leftrightarrow$ (*ii*) dans la proposition 2.16 ainsi que le lemme des noyaux. □

On en déduit un résultat non trivial si l'on part de la définition de la diagonalisabilité.

Corollaire 2.23. *Si u est diagonalisable et si F est un sous-espace vectoriel de E stable par u alors l'endomorphisme induit par u sur F est diagonalisable.*

Présentons à présent quelques applications directes du théorème précédent : on va ainsi donner deux premières classes d'endomorphismes diagonalisables.

Exemple 2.24. Si u est un projecteur alors $u^2 = u$ donc u est annulé par le polynôme $X(X-1)$ qui est scindé sur k à racines simples donc u est diagonalisable.

Exemple 2.25. Si u est une symétrie, alors u est annulé par le polynôme $X^2-1 = (X-1)(X+1)$. Ainsi, si k est de caractéristique différente de 2 alors u est diagonalisable. Par exemple, la matrice $M := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ vérifie $M^2 = I_2$ donc c'est une symétrie. En tant qu'élément de $\mathcal{M}_2(\mathbb{Q})$ elle est donc diagonalisable, mais en tant qu'élément de $\mathcal{M}_2(\mathbb{F}_2)$ on va voir qu'elle n'est pas diagonalisable. En effet, $\chi_M = X^2 - 1$ donc étant dans $\mathbb{F}_2$ on a $\chi_M = (X-1)^2$; ainsi, $\mathrm{Sp}(M) = \{1\}$ donc si $M \in \mathcal{M}_2(\mathbb{F}_2)$ était diagonalisable on aurait $M = I_2$.

Remarque 2.26. Si k est un corps fini la proposition précédente implique que u est diagonalisable ssi $u^q = u$ où $q := \mathrm{card}(k)$; cela résulte simplement du fait que $X^q - X = \prod_{x \in k}(X - x)$. C'est un critère remarquable du point de vue théorique mais un peu moins du point de vue pratique : en effet, le nombre d'opérations nécessaires peut être exagérément élevé (par exemple pour montrer que la matrice nulle est diagonalisable).

La remarque précédente contient quelque chose d'intéressant : on sait quel polynôme tester pour savoir si u est diagonalisable. Ce qui suit généralise en quelque sorte cela.

Définition 2.27. Le *polynôme minimal* de u, noté μ_u, est le générateur unitaire de l'idéal $\{P \in k[X] : P(u) = 0\}$ de $k[X]$.

Remarque 2.28. La définition est légitime car $k[X]$ est principal (car k est un corps) et car u admet un polynôme annulateur non nul (car l'algèbre $\mathcal{L}(E)$ est de dimension finie).

Exemple 2.29. On considère les trois matrices suivantes (à coefficients dans k) : $J_0 := \left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$, $J_1 := \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ et $J_2 := \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right)$. On a $J_i^3 = 0\ \forall i$ donc $\mu_{J_i} | X^3$ et on trouve $\mu_{J_0} = X$, $\mu_{J_1} = X^2$ et $\mu_{J_2} = X^3$. Remarquons que l'on a $\forall i, \chi_{J_i} = -X^3$ donc $\mu_{J_i} | \chi_{J_i}\ \forall i$.

Voici la proposition annoncée.

Proposition 2.30. *L'endomorphisme u est diagonalisable ssi μ_u est scindé sur k à racines simples. De plus, dans ce cas on a $\mu_u = \prod_{\lambda \in \mathrm{Sp}(u)}(X - \lambda)$.*

Remarque 2.31. On retrouve bien que, avec les notations de l'exemple précédent, seule J_0 est diagonalisable.

Corollaire 2.32. *Si χ_u est scindé sur k à racines simples alors (u est diagonalisable et) $\mu_u = (-1)^n \chi_u$.*

On connaît à présent plusieurs façons de montrer qu'un endomorphisme est diagonalisable. De plus, on a pu déterminer deux classes d'endomorphismes diagonalisables, en démontrant ce fait à partir d'un théorème général. Le but de la prochaine section est de déterminer et d'étudier d'autres familles d'endomorphismes diagonalisables, et ainsi d'établir d'autres théorèmes de diagonalisabilité.

3 Familles d'endomorphismes diagonalisables

3.1 Topologie des matrices diagonalisables

Les espaces de dimension finie sur $\mathbb{R}$ ou $\mathbb{C}$ intervenant dans cette section sont munis de leur topologie d'espace vectoriel de dimension finie.

On a vu lors de la proposition 2.1 que les matrices de taille n à n valeurs propres distinctes sont diagonalisables ; la proposition suivante dit que cette situation n'est pas si rare que cela puisse en avoir l'air.

Proposition 3.1. *L'ensemble des matrices à n valeurs propres distinctes est un ouvert dense de $\mathcal{M}_n(\mathbb{C})$.*

Idée de démonstration. Notons $\mathcal{D} \subseteq \mathcal{M}_n(\mathbb{C})$ l'ensemble des matrices à n valeurs propres distinctes. On a $\mathcal{D} = f^{-1}(\mathbb{C}^*)$ où $f : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}$ est l'application qui à une matrice M associe le nombre complexe $f(M) := \operatorname{res}(\chi_M, \chi'_M)$ (note [2]) ; f étant continue, $\mathcal{D}$ est ouvert. Pour montrer que $\mathcal{D}$ est dense dans $\mathcal{M}_n(\mathbb{C})$, on utilise un argument de réduction qui nous permet de trigonaliser M (car son polynôme minimal est scindé), c'est-à-dire d'écrire $M = PTP^{-1}$ avec $P \in \mathrm{GL}_n(\mathbb{C})$ et $T \in \mathcal{M}_n(\mathbb{C})$ triangulaire supérieure. Il suffit alors de perturber les coefficients diagonaux de T pour obtenir n valeurs propres distinctes tout en restant proche de M. □

Corollaire 3.2. *L'ensemble des matrices diagonalisables est dense dans $\mathcal{M}_n(\mathbb{C})$.*

Remarque 3.3. Ce résultat est faux sur $\mathbb{R}$ dès que $n \geqslant 2$ (note [3]). Démontrons le pour $n = 2$: le polynôme caractéristique de la matrice $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R})$ est $\chi = X^2+1$, qui a pour discriminant $\Delta(\chi) = -4 < 0$. Par continuité de l'application $\mathcal{M}_2(\mathbb{R}) \ni M \mapsto \Delta(\chi_M)$ (on l'a en fait déjà évoquée ci-avant), on en déduit que M n'est pas limite de matrices diagonalisables : en effet, si $N \in \mathcal{M}_2(\mathbb{R})$ est diagonalisable alors $\chi_N \in \mathbb{R}[X]$ a ses racines réelles donc $\Delta(\chi_N) \geqslant 0$.

Développement 1. Sur $\mathcal{M}_n(\mathbb{F}_q)$, on peut compter le nombre de matrices diagonalisables ; se référer à l'annexe A.

Corollaire 3.4 (théorème de Cayley–Hamilton)**.** *On suppose que k est un sous-corps de $\mathbb{C}$. Alors $\mu_u | \chi_u$, i.e. $\chi_u(u) = 0$.*

Idée de démonstration. Soit M la matrice de u dans une base de E ; le polynôme caractéristique ne dépendant pas du corps de base, il suffit de montrer que $\chi_M(M) = 0$ en considérant M comme un élément de $\mathcal{M}_n(\mathbb{C})$. Le théorème est vrai pour les matrices diagonales et on le déduit pour les matrices diagonalisables. On conclut par densité en invoquant le fait que l'application $\mathcal{M}_n(\mathbb{C}) \ni N \mapsto \chi_N(N) \in \mathcal{M}_n(\mathbb{C})$ est continue (les coefficients sont polynomiaux). □

Remarque 3.5. Comme $\deg \chi_u = n$, on a donc la majoration $\deg \mu_u \leqslant n$; *a priori*, on avait seulement $\deg \mu_u \leqslant n^2$ puisque la k-algèbre $\mathcal{L}(E)$ est de dimension n^2.

Remarque 3.6. Le théorème de Cayley–Hamilton reste vrai pour un corps k quelconque.

2. res désigne le résultant ; $f(M)$ est en fait (à un facteur multiplicatif près) le discriminant de χ_M. En particulier, $f(M) = 0$ ssi χ_M possède une racine multiple.

3. L'adhérence des matrices diagonalisables de $\mathcal{M}_n(\mathbb{R})$ est en fait l'ensemble des matrices trigonalisables, comme on peut le pressentir dans l'idée de preuve précédente.

3.2 Endomorphismes normaux

On va maintenant présenter une classe générale d'endomorphismes diagonalisables. Pour cela, on se place dans $k = \mathbb{R}$ ou $\mathbb{C}$ et l'on suppose que E est muni d'un produit scalaire $\langle \cdot | \cdot \rangle$.

Proposition 3.7. *Il existe un unique $u^* \in \mathcal{L}(E)$ tel que $\forall x, y \in E, \langle u(x)|y\rangle = \langle x|u^*(y)\rangle$.*

Définition 3.8. L'endomorphisme u^* de la proposition précédente s'appelle l'*adjoint* de u.

Proposition 3.9. *Si $\mathcal{B}$ est une base orthonormale de E alors* $\mathrm{mat}_{\mathcal{B}}(u^*) = \overline{\mathrm{mat}_{\mathcal{B}}(u)}^{\mathrm{T}}$.

Cela nous conduit à la définition suivante.

Définition 3.10. Pour $M \in \mathcal{M}_n(k)$, on définit sa matrice *adjointe* (ou *transconjuguée*) par $M^* := \overline{M}^{\mathrm{T}}$.

Définition 3.11. On dit que u est *normal* si $u^*u = uu^*$.

Théorème 3.12 (théorème spectral)**.** *On suppose que $k = \mathbb{C}$. Alors u est normal* ssi *u se diagonalise dans une base orthonormée de E.*

Idée de démonstration. Soit M la matrice de u dans une base *orthonormée* de E ; par la proposition 3.9 on a u normal ssi M normale. Comme M est à coefficients complexes, la matrice M est unitairement semblable à une matrice triangulaire : $M = UTU^*$ avec $T \in \mathcal{M}_n(\mathbb{C})$ triangulaire et $U \in \mathcal{U}_n(\mathbb{C})$ (*i.e.* $UU^* = I_n$). La matrice T hérite du fait que M est normale et en examinant les coefficients diagonaux de $TT^* = T^*T$ on remarque que T est diagonale. □

Si $M \in \mathcal{M}_n(\mathbb{R})$ est une matrice normale, alors par le théorème spectral on a que M est $\mathbb{C}$-diagonalisable ; cependant, elle n'est *a priori* pas $\mathbb{R}$-diagonalisable. Par exemple, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ est normale mais on a vu que son spectre sur $\mathbb{R}$ est vide. Pour pallier ce manque, on va raffiner un peu la classe des endomorphismes normaux.

Définition 3.13. On dit que u est *autoadjoint* si $u^* = u$.

Remarque 3.14. Comme annoncé ci-avant, les endomorphismes autoadjoints sont des cas particuliers d'endomorphismes normaux.

Remarque 3.15. Une matrice réelle autoadjointe est dite *symétrique* et une matrice complexe autoadjointe est dite *hermitienne*.

Théorème 3.16 (théorème spectral)**.** *L'endomorphisme u est autoadjoint* ssi *u se diagonalise dans une base orthonormée de E et* $\mathrm{Sp}_{\mathbb{C}}(u) \subseteq \mathbb{R}$.

Remarque 3.17. La notation $\mathrm{Sp}_{\mathbb{C}}(u)$ désigne $\mathrm{Sp}_{\mathbb{C}}(M)$ où M est la matrice de u dans une base de E.

Application 3.18 (décomposition polaire). Pour $M \in \mathrm{GL}_n(\mathbb{R})$, on a la décomposition suivante : $\exists!(O, S) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}), M = OS$. Il suffit de constater que la matrice $M^{\mathrm{T}}M$ est symétrique définie positive ; ainsi, d'après le théorème spectral on peut écrire $M^{\mathrm{T}}M = P\,\mathrm{diag}(\lambda_i)P^{\mathrm{T}}$ où $P \in \mathcal{O}_n(\mathbb{R})$ et $\lambda_i \in \mathbb{R}_+^*$. On pose alors $S := P\,\mathrm{diag}(\sqrt{\lambda_i})P^{\mathrm{T}} \in \mathcal{S}_n^{++}(\mathbb{R})$ et $O := MS^{-1}$.

Remarque 3.19. On démontre de la même façon que toute matrice $M \in \mathrm{GL}_n(\mathbb{R})$ s'écrit de façon unique sous la forme $M = S'O'$ avec $(O', S') \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$, ce couple étant *a priori* différent de celui donné par la décomposition polaire (on a en fait égalité si et seulement si M est normale).

Remarque 3.20. On peut étendre ces deux décompositions à $\mathcal{M}_n(\mathbb{R})$ tout entier en utilisant la densité de $\mathrm{GL}_n(\mathbb{R})$ et le fait que $\mathcal{O}_n(\mathbb{R})$ est compact ; on perd cependant l'unicité de la matrice orthogonale.

Remarque 3.21. Le théorème spectral nous permet également de parler de décomposition polaire dans $\mathrm{GL}_n(\mathbb{C})$, en remplaçant « orthogonal » par « unitaire » et « symétrique » par « hermitien ». Cela généralise alors l'écriture sous forme polaire des nombres complexes : pour $z \in \mathbb{C}^*$, on peut en effet écrire de façon unique $z = ur$ avec $u \in \mathcal{U}_1(\mathbb{C}) = \{a \in \mathbb{C} : a\bar{a} = 1\} = \{e^{i\theta} : \theta \in \mathbb{R}\}$ et $r \in \mathcal{H}_1^{++}(\mathbb{C}) = \mathbb{R}_+^*$ (on remarquera que l'habitude est d'utiliser la décomposition polaire « inversée » introduite précédemment).

3.3 Codiagonalisabilité

(k désigne à nouveau un corps quelconque.) La plupart des théorèmes précédents donnent des conditions pour qu'un endomorphisme soit diagonalisable, sans parler de base de diagonalisation : ainsi, on n'a pas d'information sur une telle base. Malgré cela, on va quand même réussir à diagonaliser simultanément (sous certaines conditions) une famille d'endomorphismes.

Définition 3.22. Soit I un ensemble d'indices et soit $(u_i)_{i\in I}$ une famille d'endomorphismes de E. On dit que la famille $(u_i)_{i\in I}$ est *codiagonalisable* si les u_i possèdent une base de diagonalisation commune.

Remarque 3.23. En particulier, si (u_i) est codiagonalisable alors chaque u_i est diagonalisable.

Énonçons tout d'abord un résultat pour une paire d'endomorphismes.

Proposition 3.24. *Soient $u, v \in \mathcal{L}(E)$ deux endomorphismes qui commutent. Alors :*
- *les sous-espaces propres de u sont stables par v ;*
- *si u et v sont diagonalisables alors u et v sont codiagonalisables ;*
- *si u possède n valeurs propres distinctes alors v est un polynôme en u, en particulier u et v sont codiagonalisables.*

Idée de démonstration. Le premier point ne pose pas de problème ; pour le deuxième, on utilise le premier point et le corollaire 2.23 (et la proposition 2.16). Finalement, pour démontrer le troisième point il suffit d'utiliser le deuxième point et de considérer un polynôme interpolateur envoyant les valeurs propres de u sur celles de v. □

Place enfin à la proposition centrale de cette section.

Proposition 3.25. *Soit $(u_i)_{i\in I}$ une famille d'endomorphismes diagonalisables de E. Alors $(u_i)_{i\in I}$ est codiagonalisable* ssi *les u_i pour $i \in I$ commutent deux à deux.*

Idée de démonstration. Remarquons tout d'abord que la condition est nécessaire. Pour montrer qu'elle est suffisante, on raisonne par récurrence sur la dimension de E et on utilise le premier point de la proposition précédente en supposant qu'au moins l'un des u_i n'est pas une homothétie pour pouvoir utiliser l'hypothèse de récurrence sur ses sous-espaces propres. □

Exemple 3.26. Les matrices $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ de $\mathcal{M}_2(\mathbb{Q})$ ont leur polynôme caractéristique scindé sur $\mathbb{Q}$ à racines simples donc elles sont diagonalisables ; elles ne commutent pas donc elles ne sont pas codiagonalisables.

On peut déduire de la proposition précédente quelques corollaires intéressants.

Corollaire 3.27. *Toute représentation linéaire irréductible d'un groupe abélien fini est de dimension* 1*.*

Idée de démonstration. Soit G un groupe abélien fini de cardinal n et soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible avec V un $\mathbb{C}$-espace vectoriel de dimension finie $d \in \mathbb{N}^*$. Les éléments de $\rho(G) := \{\rho(g) : g \in G\}$ commutent deux à deux (car G est abélien) et sont diagonalisables (ils sont annulés par $X^n - 1$ qui est scindé à racines simples sur $\mathbb{C}$) donc la famille $\rho(G)$ est codiagonalisable. Si x est un vecteur propre commun alors le sous-espace $\mathbb{C}x$ est stable par tous les $\rho(g)$ donc comme V est irréductible on a $V = \mathbb{C}x$ *i.e.* $d = 1$. □

Corollaire 3.28. *On suppose que k est de caractéristique différente de* 2*. Si $m \in \mathbb{N}^*$ est tel que $\mathrm{GL}_m(k) \simeq \mathrm{GL}_n(k)$ (isomorphisme de groupes) alors $m = n$.*

Démonstration. Notons G_n^2 l'ensemble des sous-groupes finis (abéliens) de $\mathrm{GL}_n(k)$ pour lesquels chaque élément est d'ordre au plus 2. Bien sûr $G_n^2 \neq \emptyset$ puisque $\{I_n\} \in G_n^2$; soit $G \in G_n^2$. Le groupe G est abélien d'ordre fini donc comme dans la démonstration précédente, les éléments de G sont codiagonalisables. Ainsi, il existe $P \in \mathrm{GL}_n(k)$ telle que $\forall M \in G, PMP^{-1} = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ avec $\lambda_i \in k$. Comme $M^2 = I_n$ on a $\lambda_i^2 = 1$ $\forall i$, *i.e.* $\lambda_i = \pm 1$; ainsi, $\mathrm{card}(G) \leqslant 2^n$. Remarquons finalement qu'il existe $G \in G_n^2$ de cardinal 2^n : il suffit par exemple de considérer l'ensemble des matrices de la forme $\mathrm{diag}(\varepsilon_1, \dots, \varepsilon_n)$ avec les ε_i qui décrivent $\{-1, 1\}$ (remarquons que $1 \neq -1$ car k est supposé de caractéristique différente de 2). Ainsi, $n = \log_2(\max\{\mathrm{card}(G) : G \in G_n^2\})$.

Finalement, si $m \in \mathbb{N}^*$ est tel qu'il y a un isomorphisme de groupes Φ entre $\mathrm{GL}_m(k)$ et $\mathrm{GL}_n(k)$, on peut construire une bijection $\widetilde{\Phi} : G_m^2 \to G_n^2$ donnée par $\forall G \in G_m^2, \widetilde{\Phi}(G) := \Phi(G)$. On a évidemment $\forall G \in G_m^2, \mathrm{card}(\widetilde{\Phi}(G)) = \mathrm{card}(G)$ donc par la formule précédente $m = n$. □

Développement 2. Toute sous-algèbre réduite de $\mathcal{M}_n(\mathbb{C})$ est codiagonalisable ; se référer à l'annexe B.

4 Décomposition de Dunford

On suppose momentanément que $k = \mathbb{C}$. On a déjà mentionné que toute matrice à coefficients complexes est trigonalisable, c'est-à-dire semblable à une matrice triangulaire supérieure. La décomposition de Dunford va donner un premier raffinement de cette trigonalisation [4], qui va faire intervenir des matrices diagonalisables ; on exploitera alors le fait que les calculs sur les matrices diagonalisables sont facilités.

Dans toute cette section, on se place dans le cas où k est un sous-corps de $\mathbb{C}$ (note [5]). De plus, n ne désigne plus un entier naturel (sauf mention du contraire), en particulier ce n'est plus la dimension de E.

4. Un deuxième raffinement étant, dans la continuité de la décomposition de Dunford, la réduction de Jordan.

5. La plupart des énoncés présents dans cette section peuvent être généralisés.

Théorème 4.1 (décomposition de Dunford, version 1)**.** *Si χ_u est scindé sur k, il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que :*
- *d est diagonalisable ;*
- *n est nilpotent ;*
- *$u = d + n$;*
- *d et n commutent.*

Remarque 4.2. La dernière condition est essentielle pour l'intérêt de la décomposition.

Idée de démonstration. Pour $\lambda \in \mathrm{Sp}(u)$ on note $N_\lambda(u) := \ker[(u-\lambda\,\mathrm{id}_E)^{m_\lambda}]$. De la même façon que dans la proposition 3.24, on montre que si $v \in \mathcal{L}(E)$ commute avec u alors $N_\lambda(u)$ est stable par v. Le polynôme χ_u est scindé sur k qui est un sous-corps de $\mathbb{C}$ donc d'après le théorème de Cayley-Hamilton et le lemme de décomposition des noyaux on a $E = \oplus_{\lambda\in\mathrm{Sp}(u)} N_\lambda(u)$. Pour $\lambda \in \mathrm{Sp}(u)$, on note p_λ la projection sur $N_\lambda(u)$ parallèlement à $\oplus_{\mu\neq\lambda} N_\mu(u)$. On a vu dans l'exemple 2.24 que chaque p_λ est diagonalisable ; de plus, si $\lambda \neq \mu$ on a $p_\lambda \circ p_\mu = 0$ donc d'après la proposition 3.25 les p_λ pour $\lambda \in \mathrm{Sp}(u)$ sont codiagonalisables. Ainsi, $d := \sum_{\lambda\in\mathrm{Sp}(u)} \lambda p_\lambda$ est diagonalisable, laisse stable chaque $N_\lambda(u)$ et $d|_{N_\lambda(u)} = \mathrm{id}_{N_\lambda(u)}$. On pose alors $n := u - d$ et on montre que n est nilpotent (n laisse chaque $N_\lambda(u)$ stable et est nilpotent sur chacun de ces sous-espaces). Finalement, pour montrer que d et n commutent, il suffit de remarquer que d et n commutent sur chaque $N_\lambda(u)$ et que d et n laissent stables chacun de ces sous-espaces.

Pour l'unicité, soit $(d',n') \in \mathcal{L}(E)^2$ un autre couple qui vérifie les mêmes conditions que (d,n). On montre (de la même façon que pour d et n) que d et d' commutent, puis que n et n' commutent. Finalement, $d - d' = n' - n$ est diagonalisable (par la proposition 3.24) et nilpotent [6] donc est nul. □

Remarque 4.3. En fait, on peut montrer que chaque p_λ est un polynôme (que l'on peut déterminer, cf. application 4.12) en u ; ainsi, d et donc n sont des polynômes en u.

On va maintenant présenter des applications de la décomposition de Dunford. Avant cela, on munit $\mathcal{L}(E)$ d'une norme d'algèbre.

Définition 4.4. On définit l'*exponentielle* de u par $\exp(u) := \sum_{i=0}^{+\infty} \frac{1}{i!} u^i \in \mathcal{L}(E)$.

Le lemme suivant sera à la source de chaque application que l'on va donner.

Lemme 4.5. *Si $u, v \in \mathcal{L}(E)$ commutent alors $\exp(u+v) = \exp(u)\exp(v)$.*

Lemme 4.6. *On a $\det(\exp(u)) = \exp(\mathrm{tr}(u))$, en particulier $\exp(u)$ est inversible.*

Proposition 4.7. *L'endomorphisme u est diagonalisable* ssi *$\exp(u)$ est diagonalisable.*

Idée de démonstration. Seule la réciproque présente une difficulté. Supposons $\exp(u)$ diagonalisable et soit (d,n) la décomposition de Dunford de u ; on montre alors que la décomposition de Dunford de $\exp(u)$ est $(\exp(d), \exp(d)[\exp(n) - \mathrm{id}_E])$. Ainsi, comme $\exp(u)$ est diagonalisable, par unicité on en déduit que $\exp(d)(\exp(n) - \mathrm{id}_E) = 0$. Comme $\exp(d)$ est inversible (lemme 4.6) on a $\exp(n) - \mathrm{id}_E = 0$. L'exponentielle n'est pas injective en général (voir remarque 4.11), mais dans notre cas si $n \neq 0$ on obtient une contradiction en considérant l'indice de nilpotence de n. Finalement $n = 0$ ce qui signifie que $u = d$ est diagonalisable ! □

6. C'est un résultat classique qu'une somme de deux endomorphismes nilpotents qui commutent est nilpotente.

Pour la prochaine application, n désigne de nouveau un entier naturel non nul.

Lemme 4.8. *Soient $M \in \mathrm{GL}_n(k)$ et $N \in \mathcal{M}_n(k)$ nilpotente deux matrices qui commutent. Alors $M+N$ est inversible.*

Proposition 4.9. *L'application $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.*

Démonstration. Le lemme 4.6 dit que l'exponentielle de $\mathcal{M}_n(\mathbb{C})$ est bien à valeurs dans $\mathrm{GL}_n(\mathbb{C})$. Soit maintenant $M \in \mathrm{GL}_n(\mathbb{C})$; écrivons $M = D + N$ sa décomposition de Dunford. Comme D et N commutent, on en déduit que M et N commutent donc par le lemme 4.8, comme $D = M - N$ la matrice D est inversible [7]. Ainsi, $M = D + N = D(I_n + D^{-1}N)$; l'objectif est maintenant d'écrire chacun de ces deux facteurs comme une exponentielle.

- Écrivons $D = P\,\mathrm{diag}(\lambda_i)P^{-1}$ avec $P \in \mathrm{GL}_n(\mathbb{C})$ et $\lambda_i \in \mathbb{C}$; comme D est inversible on a en fait $\lambda_i \in \mathbb{C}^*$. Comme $\exp : \mathbb{C} \to \mathbb{C}^*$ est surjective [8] on a donc $D = \exp(D')$ avec $D' = P\,\mathrm{diag}(\mu_i)P^{-1}$ où les $\mu_i \in \mathbb{C}$ sont tels que $\exp(\mu_i) = \lambda_i$ et $[\mu_i = \mu_j$ si $\lambda_i = \lambda_j]$. De plus, en interpolant on montre que D' est un polynôme en D
- Comme D^{-1} et N commutent et que N est nilpotente, la matrice $D^{-1}N$ est nilpotente ; soit $p \in \mathbb{N}$ tel que $(D^{-1}N)^{p+1} = 0$. Pour $t \in \mathbb{R}$, on pose $\log(I_n + tD^{-1}N) := \sum_{i=1}^{p} \frac{(-1)^{i-1}}{i}(tD^{-1}N)^i$; en montrant par exemple que $\mathbb{R} \ni t \mapsto \exp(\log(I_n + tD^{-1}N))$ vérifie la même équation différentielle que $t \mapsto I_n + tD^{-1}N$, on montre que $\exp(\log(I_n + D^{-1}N)) = I_n + D^{-1}N$.

Finalement, on a $M = \exp(D')\exp(N')$; de plus, par construction D' est un polynôme en D et N' est un polynôme en $D^{-1}N$ donc D' et N' commutent. Ainsi, $M = \exp(D' + N')$. □

Remarque 4.10. Étant donné que D et N sont des polynômes en M (cf. remarque 4.3), on a en fait montré que toute matrice $M \in \mathrm{GL}_n(\mathbb{C})$ s'écrit $M = \exp(P(M))$ avec $P \in \mathbb{C}[X]$.

Remarque 4.11. L'application $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ n'est évidemment pas injective car $\exp(2i\pi I_n) = \exp(\mathrm{diag}(2i\pi)) = \mathrm{diag}(e^{2i\pi}) = I_n = \exp(0_n)$.

Application 4.12 (résolution d'un système différentiel linéaire à coefficients constants). On cherche à résoudre le système différentiel suivant :

$$(S) : \begin{cases} x'(t) &= 2z(t) \\ y'(t) &= x(t) - 5z(t) \\ z'(t) &= y(t) + 4z(t) \end{cases}$$

pour $x, y, z \in \mathcal{C}^1(\mathbb{R}, \mathbb{R})$. En posant $X := \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $M := \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -5 \\ 0 & 1 & 4 \end{pmatrix}$, le système (S) est équivalent à $(\Sigma) : X' = MX$, et les solutions de (Σ) sont donc données par :

$$\mathbb{R} \ni t \mapsto X(t) = \exp(tM)X(0) \tag{1}$$

Tout le problème est donc de calculer $\exp(tM)$; pour cela, on va utiliser la décomposition de Dunford de M. On va illustrer sur cet exemple comment obtenir en pratique les projecteurs p_λ de la démonstration du théorème 4.1.

7. On pourrait aussi dire que par construction de D (dans la preuve de la décomposition de Dunford) on a $\mathrm{Sp}(D) = \mathrm{Sp}(M)$.

8. C'est un résultat délicat à montrer, mais en admettant que $\exp : i\mathbb{R} \to \{z \in \mathbb{C} : |z| = 1\}$ est surjective, on peut dire que si $z = \rho e^{i\theta} \in \mathbb{C}^*$ avec $\rho \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$ alors $z = \exp(\log\rho + i\theta)$.

1. On calcule le polynôme caractéristique de M ; on trouve ici $\chi_M = -(X-1)^2(X-2)$. (On peut à ce stade vérifier que M n'est pas diagonalisable puisque $(M-I_3)(M-2I_3) \neq 0$, cf. proposition 2.30.)
2. On trouve $Q_1 \in \mathbb{R}[X]$ une solution de $\left\{ \begin{smallmatrix} Q_1 \equiv 1 & [(X-1)^2] \\ Q_1 \equiv 0 & [X-2] \end{smallmatrix} \right.$: une relation de Bézout entre $(X-1)^2$ et $X-2$ étant $(X-1)^2 - X(X-2) = 1$, on peut prendre $Q_1 := -X(X-2)$.
3. De même, on considère $Q_2 := (X-1)^2 \in \mathbb{R}[X]$ solution de $\left\{ \begin{smallmatrix} Q_2 \equiv 0 & [(X-1)^2] \\ Q_2 \equiv 1 & [X-2] \end{smallmatrix} \right.$.
4. On pose $P_1 := Q_1(M)$ et $P_2 := Q_2(M)$; on a déjà vu que $\mathbb{C}^3 = \ker(M-I_3)^2 \oplus \ker(M-2I_3)$ et en regardant sur une base adaptée à cette décomposition on trouve que P_1 et P_2 sont exactement les projecteurs recherchés.

Ainsi, on a $D = P_1 + 2P_2 = \left(\begin{smallmatrix} 2 & 2 & 4 \\ -2 & -3 & -8 \\ 1 & 2 & 5 \end{smallmatrix} \right)$ et $N = M - D = \left(\begin{smallmatrix} -2 & -2 & -2 \\ 3 & 3 & 3 \\ -1 & -1 & -1 \end{smallmatrix} \right)$. Par construction de D on a $\chi_D = -(X-1)^2(X-2)$; D est diagonalisable donc $D = R\,\mathrm{diag}(1,1,2)R^{-1}$ avec R une matrice de passage et on obtient :
- $Q(D) = R\,\mathrm{diag}(Q(1), Q(1), Q(2))R^{-1}$ $\forall Q \in \mathbb{R}[X]$;
- $\exp(tD) = R\,\mathrm{diag}(e^t, e^t, e^{2t})R^{-1}$.

On considère maintenant Q_t un polynôme d'interpolation qui envoie $(1,2)$ sur (e^t, e^{2t}), par exemple $Q_t := e^t \frac{X-2}{1-2} + e^{2t}\frac{X-1}{2-1} = (e^{2t} - e^t)X + 2e^t - e^{2t}$; on a donc $\exp(tD) = Q_t(D) = (e^{2t} - e^t)D + (2e^t - e^{2t})I_3$.

Finalement, on vérifie que $N^2 = 0$ donc $\exp(tN) = I_3 + tN$; comme D et N commutent, on a $\exp(tM) = \exp(tD)\exp(tN) = Q_t(D)(I_3 + tN)$ et on déduit alors grâce à (1) les solutions de (Σ) et donc de (S).

D'après la méthode donnée ci-avant, on peut déterminer la décomposition de Dunford à condition de connaître les valeurs propres ; c'est un problème car on n'en connaît en général qu'une approximation (ce sont les racines du polynôme caractéristique). On va présenter une autre preuve de la décomposition de Dunford, qui ne possède pas cet inconvénient. On rappelle que n ne désigne plus un entier naturel, *a fortiori* la dimension de E.

Théorème 4.13 (décomposition de Dunford, version 2)**.** *Si χ_u est scindé sur k, il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que :*
- *d est diagonalisable ;*
- *n est nilpotent ;*
- *$u = d + n$;*
- *d et n commutent.*

De plus, d et n sont des polynômes en u et on peut les déterminer sans connaître les valeurs propres de u.

Développement 3. On adapte dans l'annexe C l'algorithme de Newton pour la recherche d'un zéro d'une fonction pour démontrer ce théorème.

Remarque 4.14. Par unicité, on retrouve le fait que les d et n de la première version de la décomposition de Dunford sont des polynômes en u.

Remarque 4.15. Dans les deux énoncés de la décomposition de Dunford que l'on a donnés, on pourrait croire que l'hypothèse « χ_u scindé sur k » est une assez grosse restriction. En fait, pour le cas $k = \mathbb{R}$ par exemple, si le polynôme caractéristique de $M \in \mathcal{M}_n(\mathbb{R})$ (où $n \in \mathbb{N}^*$) n'est pas scindé alors on peut quand même écrire dans $\mathcal{M}_n(\mathbb{C})$ la décomposition de Dunford $M = D + N$. En utilisant le fait que $\overline{M} = M$ ainsi que l'unicité dans la décomposition de

Dunford, on montre que $D, N \in \mathcal{M}_n(\mathbb{R})$; en particulier, D est une matrice à coefficients réels diagonalisable sur $\mathbb{C}$ (on dit que D est *semi-simple*).

Références

[1] V. Beck, J. Malick et G. Peyré, *Objectif Agrégation* (deuxième édition). H&K, 2005.

[2] X. Gourdon, *Les maths en tête, Algèbre* (deuxième édition). Ellipse, 2009.

[3] J. Grifone, *Algèbre linéaire* (quatrième édition). Cépaduès, 2011.

[4] D. Serre, *Matrices : théorie et pratique*. Dunod, 2001.

A Nombre de matrices diagonalisables dans $\mathcal{M}_n(\mathbb{F}_q)$

Référence : S. Francinou, H. Gianella et S. Nicolas, *Exercices des oraux X-ENS, Algèbre 1.* Exercice 1.10 (donne l'idée de la démonstration).

On rappelle que n désigne un élément de $\mathbb{N}^*$ et soit q une puissance d'un nombre premier. On note $\mathcal{D}_n(q)$ l'ensemble des matrices de $\mathcal{M}_n(q) := \mathcal{M}_n(\mathbb{F}_q)$ diagonalisables sur $\mathbb{F}_q$ (note [9]) ; on s'intéresse au cardinal de $\mathcal{D}_n(q)$. Finalement, pour simplifier les notations on va légèrement changer la définition 2.2 en imposant au polynôme caractéristique d'être unitaire, c'est-à-dire $\chi_A(X) := \det(XI_n - A)$ pour une matrice A de taille n (note [10]) ; de plus, si X est un ensemble fini on renote $|X|$ son cardinal.

Théorème A.1. *Avec la convention* $|\mathrm{GL}_0(q)| = 1$ *on a la formule suivante :*

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1,\dots,m_q \in \mathbb{N} \\ m_1+\cdots+m_q=n}} \frac{|\mathrm{GL}_n(q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(q)|}.$$

Remarquons tout de suite que l'on a une formule explicite pour le cardinal du groupe linéaire.

Lemme A.2. *Pour* $m \in \mathbb{N}$ *on a* $|\mathrm{GL}_m(q)| = \prod_{i=0}^{m-1}(q^m - q^i) = q^{\frac{m(m-1)}{2}} \prod_{i=1}^{m}(q^i - 1)$.

Venons-en à la démonstration du théorème. On va se baser sur le fait suivant :

$$\mathcal{D}_n(q) = \{PDP^{-1} : D \in \mathcal{M}_n(q) \text{ diagonale et } P \in \mathrm{GL}_n(q)\}. \tag{2}$$

Remarquons que $\mathrm{GL}_n(q)$ agit par conjugaison sur $\mathcal{D}_n(q)$; pour $M \in \mathcal{D}_n(q)$, on note $\mathrm{Orb}(M)$ son orbite et $\mathrm{Stab}(M)$ son stabilisateur pour l'action de $\mathrm{GL}_n(q)$ sur $\mathcal{D}_n(q)$.

Définition A.3. Soit χ un polynôme scindé unitaire sur $\mathbb{F}_q$ de degré n ; on écrit $\chi = \prod_{i=1}^{r}(X - \lambda_i)^{m_i}$ avec les $\lambda_i \in \mathbb{F}_q$ deux à deux distincts. On lui associe la matrice diagonale $D_\chi := \mathrm{diag}(\lambda_i I_{m_i})_{1 \leqslant i \leqslant r}$ et on note $\mathrm{Scal}_n^{\mathrm{b}}(q) := \{D_\chi : \chi \text{ polynôme scindé unitaire sur } \mathbb{F}_q \text{ de degré } n\}$.

9. On rappelle que $\mathbb{F}_q$ désigne un corps à q éléments.

10. Cela ne change en rien les résultats utilisant le polynôme caractéristique puisqu'il s'agit uniquement de le multiplier par $(-1)^n$.

Remarque A.4. En réalité, D_χ dépend de l'ordre que l'on choisit pour les racines de χ mais cela n'est pas grave : la chose importante est que deux éléments distincts de $\mathrm{Scal}_n^{\mathrm{b}}(q)$ ont leur polynôme caractéristique distinct (le polynôme caractéristique de D_χ étant bien sûr χ).

Lemme A.5. *L'ensemble* $\mathrm{Scal}_n^{\mathrm{b}}(q)$ *est un système de représentants des orbites de* $\mathcal{D}_n(q)$ *sous l'action de* $\mathrm{GL}_n(q)$*, en particulier :*

$$\mathcal{D}_n(q) = \bigsqcup_{D \in \mathrm{Scal}_n^{\mathrm{b}}(q)} \mathrm{Orb}(D).$$

Démonstration. Tout d'abord, chaque $D' \in \mathcal{D}_n(q)$ possède au moins un représentant de son orbite dans $\mathrm{Scal}_n^{\mathrm{b}}(q)$, à savoir $D_{\chi_{D'}}$. En effet, D' est semblable à une matrice diagonale et cette matrice diagonale est semblable à $D_{\chi_{D'}}$ (par une matrice de permutation par exemple : il suffit de permuter les vecteurs de la base). Finalement, si χ et ψ sont deux polynômes scindés unitaires sur $\mathbb{F}_q$ de degré n tels que $D_\chi \in \mathrm{Orb}(D_\psi)$ alors D_χ et D_ψ sont semblables ; elles ont donc le même polynôme caractéristique d'où $\chi = \psi$. □

Une conséquence immédiate de ce lemme est la chose suivante (formule des classes) :

$$|\mathcal{D}_n(q)| = \sum_{D \in \mathrm{Scal}_n^{\mathrm{b}}(q)} |\mathrm{Orb}(D)|. \tag{3}$$

Lemme A.6. *Pour* $D \in \mathrm{Scal}_n^{\mathrm{b}}(q)$ *on a* $\mathrm{Stab}(D) = \mathcal{C}(D) \cap \mathrm{GL}_n(q)$ *où* $\mathcal{C}(D) := \{M \in \mathcal{M}_n(q) : MD = DM\}$ *est le commutant de* D*.*

Démonstration. Soit $P \in \mathcal{M}_n(q)$; on a $P \in \mathrm{Stab}(D)$ ssi $P \in \mathrm{GL}_n(q)$ et $PDP^{-1} = D$ ssi $P \in \mathrm{GL}_n(q)$ et $PD = DP$ ssi $P \in \mathrm{GL}_n(q) \cap \mathcal{C}(D)$. □

D'après l'équation (3) et la relation orbite–stabilisateur, il ne reste donc plus qu'à déterminer $|\mathcal{C}(D) \cap \mathrm{GL}_n(q)|$.

Lemme A.7. *Pour* $D = \mathrm{diag}\,(\lambda_i I_{m_i})_{1 \leqslant i \leqslant r} \in \mathrm{Scal}_n^{\mathrm{b}}(q)$ *(avec les* λ_i *deux à deux distincts) on a la formule suivante :*

$$|\mathcal{C}(D) \cap \mathrm{GL}_n(q)| = \prod_{i=1}^{r} |\mathrm{GL}_{m_i}(q)|.$$

Démonstration. Soit D comme dans l'énoncé et soit $P \in \mathcal{C}(D)$. Par la proposition 3.24, les sous-espaces propres de D sont stables par P, autrement dit P est de la forme $P = \mathrm{diag}(P_i)_{1 \leqslant i \leqslant r}$ avec $P_i \in \mathcal{M}_{m_i}(q)$. Réciproquement, on vérifie que si P est de cette forme alors $P \in \mathcal{C}(D)$. Finalement, pour avoir $P \in \mathrm{GL}_n(q)$ il faut et il suffit de choisir chaque P_i dans $\mathrm{GL}_{m_i}(q)$, ce qui conclut la preuve. □

Démonstration du théorème. Par les lemmes précédents et la relation orbite–stabilisateur on obtient :

$$|\mathcal{D}_n(q)| = \sum_{D \in \mathrm{Scal}_n^{\mathrm{b}}(q)} \frac{|\mathrm{GL}_n(q)|}{\prod_{i=1}^{r} |\mathrm{GL}_{m_i}(q)|}$$

où l'on écrit les matrices $D \in \mathrm{Scal}_n^{\mathrm{b}}(q)$ sous une forme $D = \mathrm{diag}(\lambda_i I_{m_i})$ avec les $\lambda_i \in \mathbb{F}_q$ deux à deux distincts. Le but est maintenant de réindexer la somme ; en particulier, la description actuelle n'est pas la plus adaptée car les valeurs propres des matrices D n'interviennent pas. On se souvient que, par construction, $\mathrm{Scal}_n^{\mathrm{b}}(q)$ est en bijection avec l'ensemble des polynômes

unitaires scindés sur $\mathbb{F}_q$ de degré n ; or, ce dernier ensemble est lui-même en bijection avec l'ensemble des q-uplets $(m_1, \dots, m_q) \in \mathbb{N}^q$ de somme n. En effet, en écrivant $\mathbb{F}_q =: \{\mu_1, \dots, \mu_q\}$ l'application qui à un q-uplet $(m_1, \dots, m_q)$ de somme n associe le polynôme $\prod_{i=1}^q (X - \mu_i)^{m_i}$ est une bijection sur les polynômes unitaires scindés sur $\mathbb{F}_q$ de degré n. On obtient alors la forme énoncée dans le théorème. □

Remarque A.8. On peut réécrire le résultat sous la forme :

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1 \leqslant \dots \leqslant m_q \in \mathbb{N} \\ m_1 + \dots + m_q = n}} \binom{q}{\nu_0(m), \dots, \nu_n(m)} \frac{|\mathrm{GL}_n(q)|}{\prod_{i=1}^q |\mathrm{GL}_{m_i}(q)|}$$

où :
- $\nu_i(m) := |\{j \in \{1, \dots, q\} : m_j = i\}|$;
- $\binom{a}{b_0, \dots, b_n} := \frac{a!}{b_0! \cdots b_n!}$ est le coefficient multinomial.

En effet, une fois qu'un q-uplet $m = (m_1, \dots, m_q)$ est fixé alors on peut générer directement plusieurs polynômes scindés de degré n (*i.e.* pas seulement $\prod (X - \mu_i)^{m_i}$) ; par exemple avec $q = 3$, le couple $(0, 1, 1)$ peut aussi bien représenter $X(X-1)$ que $X(X-2)$ ou encore $(X-1)(X-2)$. Le nombre de polynômes que l'on peut générer à partir d'un q-uplet m est alors $\binom{q}{\nu_0}\binom{q-\nu_0}{\nu_1} \cdots \binom{q-\nu_0-\cdots-\nu_{i-1}}{\nu_n} = \frac{q!}{\nu_0!(q-\nu_0)!} \frac{(q-\nu_0)!}{\nu_1!(q-\nu_0-\nu_1)!} \cdots \frac{(q-\nu_0-\cdots-\nu_{i-1})!}{\nu_n!0!} = \frac{q!}{\nu_0!\nu_1!\cdots\nu_n!}$ qui est bien le coefficient multinomial qui apparaît.

B Toute sous-algèbre réduite de $\mathcal{M}_n(\mathbb{C})$ est codiagonalisable

Référence : R. Mneimné, *Réduction des endomorphismes*.

Définition B.1. On dit qu'une algèbre (pas forcément unitaire) est *réduite* quand il n'y a pas d'élément non nul nilpotent.

Soit $\mathcal{A}$ une sous-algèbre réduite de $\mathcal{M}_n(\mathbb{C})$. On va montrer successivement que :
- on peut supposer que $I_n \in \mathcal{A}$;
- tous les éléments de $\mathcal{A}$ sont diagonalisables ;
- l'ensemble des projecteurs de $\mathcal{M}_n(\mathbb{C})$ qui sont dans $\mathcal{A}$ engendre $\mathcal{A}$ (en tant qu'algèbre) ;
- $\mathcal{A}$ est commutative.

On peut supposer $\mathcal{A}$ unitaire. Soit $\mathcal{B} := \mathcal{A} + \mathbb{C}I_n$; c'est bien une algèbre (remarquons que pour $A \in \mathcal{A}$ on a $AI_n = I_nA = A \in \mathcal{A}$ que I_n soit dans $\mathcal{A}$ ou non). Pour $P \in \mathrm{GL}_n(\mathbb{C})$ on a $P\mathcal{B}P^{-1} = P(\mathcal{A} + \mathbb{C}I_n)P^{-1} = P\mathcal{A}P^{-1} + \mathbb{C}I_n$ donc $\mathcal{A}$ est codiagonalisable ssi $\mathcal{B}$ est codiagonalisable. Reste donc à montrer que l'algèbre $\mathcal{B}$ est réduite ; pour cela, soit $B \in \mathcal{B}$ nilpotente. On peut écrire $B = A + \lambda I_n$ avec $A \in \mathcal{A}$ et $\lambda \in \mathbb{C}$; si $\lambda = 0$ alors $B \in \mathcal{A}$ donc $B = 0$: on suppose donc $\lambda \neq 0$.

Pour se ramener à un élément de $\mathcal{A}$, on considère $AB = A^2 + \lambda A \in \mathcal{A}$. Cette matrice est nilpotente car B est nilpotente et commute avec A, donc comme $\mathcal{A}$ est réduite on a $AB = 0$. Pour conclure que $B = 0$, il reste à dire que A est inversible : c'est le cas car $A = B - \lambda I_n$, la matrice B étant nilpotente et $\lambda \neq 0$.

On peut donc supposer que $I_n \in \mathcal{A}$, *i.e.* que l'algèbre $\mathcal{A}$ est unitaire. On obtient alors le résultat de stabilité suivant.

Lemme B.2. *Si $P \in \mathbb{C}[X]$ et $A \in \mathcal{A}$ alors $P(A) \in \mathcal{A}$.*

Démonstration. Tout d'abord, le résultat est clair si $P = 0$ puisque $P(A)$ est alors égal à $0 \in \mathcal{A}$ (puisque $\mathcal{A}$ est une algèbre). On suppose donc maintenant que $P \neq 0$ et on écrit $P = \sum_{i=0}^{d} p_i X^i$ avec $d \geqslant 0$. On a donc $P(A) = p_0 I_n + \sum_{i=1}^{d} p_i A^i$; le résultat en découle puisque comme $A \in \mathcal{A}$, chaque A^i pour $i \geqslant 1$ est dans $\mathcal{A}$ et comme $\mathcal{A}$ est unitaire on a également $I_n \in \mathcal{A}$. □

Les éléments de $\mathcal{A}$ sont diagonalisables. Soit $A \in \mathcal{A}$ et soit χ_A son polynôme caractéristique ; d'après le théorème de Cayley–Hamilton, on a $\chi_A(A) = 0$. De plus, $\chi_A \in \mathbb{C}[X]$ donc χ_A est scindé : on peut donc écrire $\chi_A = \prod_{i=1}^{r}(\lambda_i - X)^{m_i}$ avec $r \in \mathbb{N}^*, \lambda_i \in \mathbb{C}$ deux à deux distincts et $m_i \in \mathbb{N}^*$. Ainsi, en posant $\mu := \prod_{i=1}^{r}(X - \lambda_i)$, le polynôme μ est un élément de $\mathbb{C}[X]$ scindé à racines simples. De plus, avec $m := \max_{1 \leqslant i \leqslant r} m_i \in \mathbb{N}^*$ on a $\chi_A | \mu^m$. Ainsi, comme $\chi_A(A) = 0$ on récupère $\mu^m(A) = 0$ *i.e.* $\mu(A)^m = 0$. Or, par le lemme B.2 on sait que $\mu(A)$ est un élément de $\mathcal{A}$: on vient de montrer que c'est un élément nilpotent donc comme $\mathcal{A}$ est réduite on a $\mu(A) = 0$. Le polynôme μ étant scindé à racines simples, on en déduit par le théorème 2.22 que A est diagonalisable.

Les projecteurs de $\mathcal{A}$ forment une famille génératrice. Soit $A \in \mathcal{A}$. On vient de voir que A est diagonalisable, ainsi par la proposition 2.16 on a $\mathbb{C}^n = \oplus_{\lambda \in \mathrm{Sp}(A)} E_\lambda(A)$. En notant P_λ la matrice dans la base canonique du projecteur sur $E_\lambda(A)$ parallèlement à $\oplus_{\mu \neq \lambda} E_\mu(A)$, on a la relation $x = \sum_{\lambda \in \mathrm{Sp}(A)} P_\lambda x$ pour tout vecteur $x \in \mathbb{C}^n$. Ainsi, $Ax = \sum_\lambda A(P_\lambda x)$ et comme $P_\lambda x \in E_\lambda(A)$ on a $Ax = \sum_\lambda \lambda P_\lambda x$. Ainsi, on a l'égalité suivante :

$$A = \sum_{\lambda \in \mathrm{Sp}(A)} \lambda P_\lambda \tag{4}$$

On ne peut pas encore conclure car on ne sait pas que les P_λ sont dans $\mathcal{A}$! En fait, on va montrer dans ce cas particulier (cf. remarque 4.3) que les P_λ sont des polynômes en A et donc que ce sont des éléments de $\mathcal{A}$ (par le lemme B.2).

On vient de voir que pour $\lambda \in \mathrm{Sp}(A)$ on a $AP_\lambda = \lambda P_\lambda$ donc de l'égalité précédente on obtient $\forall k \in \mathbb{N}, A^k = \sum_\lambda \lambda^k P_\lambda$ d'où :

$$\forall Q \in \mathbb{C}[X], Q(A) = \sum_{\lambda \in \mathrm{Sp}(A)} Q(\lambda) P_\lambda. \tag{5}$$

Ainsi, pour $\lambda \in \mathrm{Sp}(A)$, en considérant un polynôme d'interpolation $Q_\lambda \in \mathbb{C}[X]$ qui envoie les éléments de $\mathrm{Sp}(A) \setminus \{\lambda\}$ (s'il en existe) sur 0 et λ sur 1, on obtient directement par l'équation (5) que $Q_\lambda(A) = P_\lambda$. Ainsi, les P_λ sont des polynômes en A, ce sont donc des éléments de $\mathcal{A}$ et l'égalité (4) permet de conclure.

Remarque B.3. On a en fait montré que les projecteurs engendrent $\mathcal{A}$ en tant que $\mathbb{C}$-espace vectoriel (c'est encore mieux !).

$\mathcal{A}$ est commutative. D'après ce qui précède, il suffit de montrer que chaque élément de $\mathcal{A}$ commute avec tous les projecteurs de $\mathcal{A}$. Soit donc $A \in \mathcal{A}$ et soit $P \in \mathcal{A}$ un projecteur de $\mathcal{A}$; on veut montrer que $AP = PA$, *i.e.* $AP - PA = 0$. Pour montrer cette égalité, on va utiliser le fait que l'on dispose d'un projecteur en composant à la source puis au but par P.

Montrons tout d'abord que $(AP - PA)P = 0$. On a $(AP - PA)P = AP^2 - PAP = AP - PAP$ (on a $P^2 = P$ car P est un projecteur) qui n'a pas de raison particulière d'être nul. On exploite alors le fait que $\mathcal{A}$ est réduite : $[(AP-PA)P]^2 = (AP-PAP)^2 = (AP)(AP)+(PAP)(PAP)-(AP)(PAP)-(PAP)(AP) = APAP+PAPAP-APAP-PAPAP = 0$ donc on a bien $\mathcal{A} \ni (AP - PA)P = 0$, *i.e.* $AP = PAP$. On montre de même que $P(AP - PA) = 0$ (note [11]), *i.e.* $PA = PAP$. Ainsi on a $AP = PAP = PA$, en particulier $AP = PA$.

Conclusion. Finalement, on a montré que tous les éléments de $\mathcal{A}$ sont diagonalisables et commutent donc d'après la proposition 3.25 la famille $\mathcal{A}$ est codiagonalisable.

Remarque B.4. On déduit immédiatement de ce résultat que pour $A \in \mathcal{M}_n(\mathbb{C})$, A est diagonalisable ssi $\mathbb{C}[A]$ est réduite.

C La décomposition de Dunford avec la méthode de Newton

Référence : J.-J. Risler et P. Boyer, *Algèbre pour la licence 3*.

On rappelle que k est un sous-corps de $\mathbb{C}$ et que n ne désigne plus un entier naturel ; on va démontrer le théorème suivant.

Théorème C.1 (décomposition de Dunford, version 2)**.** *Si χ_u est scindé sur k, il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que :*

- *d est diagonalisable ;*
- *n est nilpotent ;*
- *$u = d + n$;*
- *d et n commutent.*

De plus, d et n sont des polynômes en u et on peut les déterminer sans connaître les valeurs propres de u.

On suppose donc que χ_u est scindé sur k, et on considère $P \in k[X]$ la partie sans facteur carré de χ_u, c'est-à-dire $P = \prod_{\lambda \in \mathrm{Sp}(u)}(X - \lambda)$. L'heuristique de la démonstration de l'existence d'une décomposition est la suivante : on va trouver une « racine » $d \in \mathcal{L}(E)$ de P (c'est-à-dire $P(d) = 0$) en adaptant la méthode de Newton que l'on connaît pour trouver un zéro d'une fonction réelle. On démontrera alors que d est l'endomorphisme diagonalisable du théorème. Ainsi, on cherche à définir la suite suivante :

$$\begin{cases} u_0 := u \\ \forall i \in \mathbb{N}, u_{i+1} := u_i - P(u_i)[P'(u_i)]^{-1} \end{cases}$$

On va montrer par récurrence que $\forall i \in \mathbb{N}$:

$(\mathcal{P}_i^0)$ u_i est bien défini ;

$(\mathcal{P}_i^1)$ u_i est un polynôme en u ;

$(\mathcal{P}_i^2)$ $P(u_i) = P(u)^{2^i} v_i$ où $v_i \in \mathcal{L}(E)$ est un polynôme en u ;

$(\mathcal{P}_i^3)$ $P'(u_i)$ est inversible.

Avant de commencer, énonçons deux petits lemmes [12].

11. En réalité, on peut même se dispenser de refaire des calculs : on sait que $\chi_{(AP-PA)P} = (-X)^n$ donc on a $\chi_{P(AP-PA)} = (-X)^n$ donc $P(AP - PA) \in \mathcal{A}$ est nilpotent donc est nul car $\mathcal{A}$ est réduite.

12. On a en fait déjà démontré le deuxième dans l'annexe B.

Lemme C.2. *Si $v \in \mathrm{GL}(E)$ alors v^{-1} est un polynôme en v.*

Lemme C.3. *L'endomorphisme $P(u)$ est nilpotent.*

Démonstration. On utilise simplement le théorème de Cayley–Hamilton et la définition de P, qui permet d'affirmer que $\chi_u | P^m$ pour $m \in \mathbb{N}$ assez grand. □

Initialisation. Tout d'abord, $u_0 = u$ est bien défini, est bien un polynôme en u et comme $\mathrm{id}_E = 1(u)$ on a bien $P(u_0) = P(u)^{2^0} v_0$ avec $v_0 = \mathrm{id}_E \in k[u]$. Comme P est sans facteur carré et que k est de caractéristique nulle, on a $P \wedge P' = 1$. Ainsi, il existe $U, V \in k[X]$ tels que $UP + VP' = 1$ et donc $U(u)P(u) + V(u)P'(u) = \mathrm{id}_E$ donc $V(u)P'(u) = \mathrm{id}_E - U(u)P(u)$. Or, par le lemme C.3 l'endomorphisme $P(u)$ est nilpotent ; ainsi, comme $U(u)$ et $P(u)$ commutent (ce sont des polynômes en u), l'endomorphisme $U(u)P(u)$ reste nilpotent. Finalement, par le lemme 4.8 on en déduit que $V(u)P'(u) = \mathrm{id}_E - U(u)P(u)$ est inversible et donc que $P'(u)$ est inversible.

Hérédité. Soit $i \in \mathbb{N}$ tel que $(\mathcal{P}_i^0)$ u_i soit bien défini, $(\mathcal{P}_i^1)$ u_i soit un polynôme en u, $(\mathcal{P}_i^2)$ $P(u_i) = P(u)^{2^i} v_i$ avec $v_i \in k[u]$ et $(\mathcal{P}_i^3)$ $P'(u_i)$ soit inversible ; en particulier, $u_{i+1} = u_i - P(u_i)[P'(u_i)]^{-1}$ est bien défini et on a donc $(\mathcal{P}_{i+1}^0)$. Par le lemme C.2, $[P'(u_i)]^{-1}$ est un polynôme en $P'(u_i)$ et ainsi $[P'(u_i)]^{-1}$ est un polynôme en u_i. Finalement, u_{i+1} est un polynôme en u_i et donc par $(\mathcal{P}_i^1)$ on conclut que u_{i+1} est un polynôme en u ce qui fournit $(\mathcal{P}_{i+1}^1)$.

En écrivant le développement de Taylor de P à l'ordre 2, on trouve Q dans $k[X, Y]$ tel que :

$$P(X + Y) = P(X) + YP'(X) + Y^2 Q(X, Y)$$

En substituant à X l'endomorphisme u_i et à Y la différence $u_{i+1} - u_i$, comme ces deux endomorphismes commutent (ce sont des polynômes en u) on obtient :

$$P(u_{i+1}) = P(u_i) + (u_{i+1} - u_i)P'(u_i) + (u_{i+1} - u_i)^2 Q(u_i, u_{i+1} - u_i)$$

Or, par définition de u_{i+1} on a $P(u_i) + (u_{i+1} - u_i)P'(u_i) = 0$; on récupère ainsi :

$$P(u_{i+1}) = (u_{i+1} - u_i)^2 Q(u_i, u_{i+1} - u_i) = (u_{i+1} - u_i)^2 \widetilde{Q}(u)$$

pour un certain $\widetilde{Q} \in k[X]$. Or, $u_{i+1} - u_i = P(u_i)[P'(u_i)]^{-1}$ donc on a :

$$P(u_{i+1}) = [P(u_i)]^2 \left([P'(u_i)]^{-1}\right)^2 \widetilde{Q}(u)$$

On sait par $(\mathcal{P}_i^2)$ que $P(u_i) = P(u)^{2^i} v_i$ avec $v_i \in k[u]$ et on a déjà vu que $[P'(u_i)]^{-1} \in k[u_i] \subseteq k[u]$ donc on obtient finalement :

$$P(u_{i+1}) = [P(u)^{2^i} v_i]^2 \widetilde{\widetilde{Q}}(u) = P(u)^{2^{i+1}} v_{i+1}$$

avec $v_{i+1} \in k[u]$, ce qui constitue $(\mathcal{P}_{i+1}^2)$. En particulier, comme $P(u)$ est nilpotent et que $P(u)$ et v_{i+1} commutent on obtient que $P(u_{i+1})$ est nilpotent. Comme lors de l'initialisation, on a $V(u_{i+1})P'(u_{i+1}) = \mathrm{id}_E - U(u_{i+1})P(u_{i+1})$ qui est donc inversible d'après le lemme 4.8. Ainsi, $P'(u_{i+1})$ est inversible ce qui montre $(\mathcal{P}_{i+1}^3)$ et achève la démonstration de l'hérédité.

Ainsi, par récurrence on a montré que la suite $(u_i)_{i \in \mathbb{N}}$ est bien définie ainsi que chaque propriété $(\mathcal{P}_i^j)$ pour $j \in \{1, 2, 3\}$ et pour chaque $i \in \mathbb{N}$.

Fin de la démonstration de l'existence. Si i_0 est un entier tel que $2^{i_0} \geqslant \dim E$ alors comme $P(u)$ est nilpotent (lemme C.3) on a $P(u)^{2^{i_0}} = 0$: en effet, par le théorème de Cayley–Hamilton on a $P(u)^{\dim E} = 0$. Ainsi, pour $i \geqslant i_0$ on a $P(u_i) = P(u)^{2^i} v_i = 0$ donc $u_{i+1} = u_i$. On a donc obtenu deux choses :

– la suite $(u_i)_{i\in\mathbb{N}}$ est stationnaire (au moins) à partir du rang i_0 ;

– u_{i_0} est annulé par le polynôme P.

Le polynôme P étant scindé à racines simples, on en déduit que $d := u_{i_0}$ est diagonalisable. Reste à montrer que $n := u - u_{i_0}$ est nilpotent !

Pour cela, on écrit que $u - u_{i_0} = \sum_{i=0}^{i_0-1}(u_i - u_{i+1})$. Or, $u_i - u_{i+1} = P(u_i)[P'(u_i)]^{-1}$ donc comme $P(u_i)$ est nilpotent (car $P(u_i) = P(u)^{2^i} v_i$) et commute avec $[P'(u_i)]^{-1}$ (d'après la propriété $(\mathcal{P}_i^1)$ on travaille dans $k[u]$ donc tout commute), $u_i - u_{i+1}$ est également nilpotent. Encore une fois, tous les u_i sont des polynômes en u donc les $u_i - u_{i+1}$ commutent donc $u - u_{i_0}$ est nilpotent, et c'est un polynôme en u car u_{i_0} est un polynôme en u d'après $(\mathcal{P}_{i_0}^1)$. Finalement, (d, n) est bien un couple qui vérifie les conditions du théorème.

Unicité. Soit (d', n') un autre couple qui vérifie les conditions du théorème. On a $u = d' + n'$ donc comme d' commute avec n', d' commute également avec u. Comme d est un polynôme en u, on en déduit que d' commute également avec d. De même, on montre que n' commute avec n. Ainsi, $d - d' = n - n'$ est un endomorphisme qui est à la fois diagonalisable et nilpotent donc il est nul, donc $d = d'$ et $n = n'$.

Remarque C.4. Il faut signaler que puisque k est de caractéristique nulle, le polynôme P (partie sans facteur carré de χ_u) s'obtient par la formule $P = \frac{\chi_u}{\chi_u \wedge \chi_u'}$.