Non existence et non unicité de la décomposition « semi-simple+nilpotent » sur un corps non parfait

par Romain Bondil, professeur en MPSI au lycée Joffre, Montpellier, Charles Boubel, Agrégé préparateur à l'ENS Lyon.

RÉSUMÉ. *Pour tout endomorphisme f d'un espace vectoriel de dimension finie sur un corps algébriquement clos K, on connaît l'écriture de Jordan-Dunford $f = d + n$. Pour généraliser cette écriture au cas où le corps K n'est pas algébriquement clos, on fait intervenir la notion d'endomorphisme semi-simple : s est* semi-simple *si, et seulement si, tout sous-espace vectoriel stable par s admet un supplémentaire stable par s.*
Sur un corps parfait*, semi-simple équivaut à* diagonalisable dans la clôture algébrique $\widehat{K}$*, et on obtient encore pour tout endomorphisme f une unique décomposition $f = s+n$ en semi-simple plus nilpotent, commutant entre eux.*
On sait moins que sur un corps non parfait, la propriété d'être diagonalisable dans la clôture algébrique est plus forte que semi-simple *: les endomorphismes vérifiant cette propriété sont dits* absolument semi-simples.
On rappelle ici, suivant Bourbaki, la condition nécessaire et suffisante sur le polynôme minimal de f pour l'obtention d'une décomposition absolument semi-simple + nilpotent*, qui est la version la plus générale du théorème de Jordan ci-dessus. Pour autant, la condition d'être semi-simple (pas absolument) est aussi intéressante géométriquement ; se pose alors la question d'une éventuelle décomposition* semi-simple + nilpotent *pour tout f sur un corps non parfait et on donne deux contre-exemples : l'un pour l'unicité, tiré de Bourbaki, et le second pour l'existence.*

MOTS-CLÉS : *Semi-simple, absolument semi-simple, nilpotent, décomposition de Jordan-Dunford, diagonalisable, corps parfait, clôture algébrique*

1. Décomposition de Jordan-Dunford classique

Le résultat suivant est bien connu, quoique hors-programme en spéciales : il est souvent cité improprement sous le nom de décomposition de Dunford, mais il s'agit d'un théorème de Jordan, cité comme tel dans Bourbaki. Le résultat de N. Dunford (cf. [4]) porte sur une généralisation de la décomposition qui suit pour les opérateurs *spectraux* dans les espaces de Banach.

Théorème 1 (Jordan) *(i) Si $f \in \mathcal{L}(E)$ a son polynôme caractéristique χ_f scindé dans $K[X]$ alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$, avec d diagonalisable et n nilpotent tel qu'on ait simultanément :*

- $f = d + n$,
- $d \circ n = n \circ d$.

De plus d et n sont des polynômes en f.

(ii) Si K est algébriquement clos, la décomposition du (i) s'applique donc pour tout $f \in \mathcal{L}(E)$.

(La preuve est une application facile du théorème de décomposition des noyaux.)

2. Endomorphisme semi-simple

2.1. *Définition et problème du passage à la clôture algébrique*

Pour généraliser le théorème 1 au cas où K n'est plus algébriquement clos, il est nécessaire d'introduire la notion d'endomorphisme *semi-simple*, que nous rappelons ici.

Définition 1 *Si K est un corps quelconque, et E un K-ev de dimension finie, un endomorphisme $f \in \mathcal{L}(E)$ est* semi-simple *si, et seulement si, tout sous-espace vectoriel F de E stable par f admet un supplémentaire stable par f.*

Sur un corps algébriquement clos, le lien avec la notion d'endomorphisme diagonalisable est évident :

Remarque 1 *Si K est algébriquement clos, f est semi-simple si, et seulement si, f est diagonalisable.*

Si K n'est pas algébriquement clos, il est naturel de « passer » à sa clôture algébrique $\widehat{K}$ ou, de manière plus économe, à un corps de décomposition L du polynôme minimal μ_f.

Pour économiser l'écriture des produits tensoriels $E \otimes_K L$, on fixe un base $\mathcal{B}$ de E sur K et considère désormais la matrice A de f dans $\mathcal{B}$.

On parlera de *matrice semi-simple* pour dire que l'endomorphisme de K^n canoniquement associé est semi-simple. On considère alors la :

Question 1 *Si $A \in M_n(K)$ est semi-simple, et $\widehat{K}$ est la clôture algébrique de K, est-il vrai A est diagonalisable dans $M_n(\widehat{K})$?*

Vu la remarque 1, cette question est un cas particulier de la question de savoir si « semi-simple » est *une propriété stable par extension de corps* :

Question 2 *Si $K \subset L$ sont deux corps et $A \in M_n(K)$ est semi-simple, A est-elle semi-simple dans $M_n(L)$?*

On va voir que la réponse à ces deux questions est négative en général.

2.2. *Caractérisation en termes de polynôme minimal*

On rappelle d'abord la :

Définition 2 *Un polynôme $P \in K[X]$ est dit* sans facteur multiple[1] *dans $K[X]$ si, et seulement si, il s'écrit comme produit $P = P_1 \dots P_r$ de polynômes P_i irréductibles dans $K[X]$, deux à deux non proportionnels.*

La caractérisation suivante est bien connue (cf. p.ex. [6] § 5.6 ou [1] VI. 8) :

Proposition 1 *Soient K un corps quelconque et $A \in M_n(K)$. Se valent :*

(i) *A est semi-simple dans $M_n(K)$,*

(ii) *le polynôme minimal μ_A de A est sans facteur multiple dans $K[X]$.*

Eléments de la preuve – Nous mentionnons ici les arguments de la preuve dont nous aurons besoin par la suite, en renvoyant aux références ci-dessus pour ce qui manque.

On note $E = K^n$ et $f \in \mathcal{L}(E)$ l'endomorphisme canoniquement associé à A.

On vérifie d'abord le :

Lemme 1 *Si on note $\mu_f = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition de μ_f en irréductibles, et si $E_i =$ Ker $P_i^{\alpha_i}(f)$ de sorte que $E = E_1 \oplus \cdots \oplus E_r$, alors f est semi-simple si, et seulement si $f_{|E_i}$ est semi-simple pour tout $i \in [\![1, r]\!]$.*

---

1. en géométrie algébrique, on dit aussi *réduit*

En remplaçant f par sa restriction à chaque E_i, il suffit alors de montrer :

Lemme 2 *Si $f \in \mathcal{L}(E)$ a un polynôme minimal* primaire *i.e. de la forme P^α où P est irréductible, alors se valent :*

1. *f est semi-simple,*
2. *$\alpha = 1$, i.e. μ_f est irréductible.*

Preuve de $(2. \Rightarrow 1.)$

Comme μ_f est irréductible, $K[f]$, isomorphe à $K[X]/(\mu_f)$, est un corps.

On munit alors E d'une structure de $K[f]$-espace vectoriel, en posant que $\forall\, Q(f) \in K[f],\ \forall v \in E$, $Q(f).v := Q(f)(v)$.

Alors un K-sous-espace vectoriel F de E est *stable par f* si, et seulement si, c'est un sous-espace vectoriel de E *pour cette structure $K[f]$-e.v.*

Or, par propriété générale des espaces vectoriels, tout $K[f]$-sous-espace vectoriel de E admet un supplémentaire, et donc f est bien semi-simple. $\square$

2.3. *Semi-simple ne signifie pas diagonalisable dans $\hat{K}$*

Compte-tenu, de ce qui précède, et pour répondre aux deux questions du § 2.1, on est encouragé par le résultat important et bien connu suivant :

Théorème 2 *Soit $K \subset L$ deux corps et $A \in M_n(K)$. On note $\mu_{A,K}$ (resp. $\mu_{A,L}$) le polynôme minimal de A vue dans $M_n(K)$ (resp. vue dans $M_n(L)$).*

Alors $\mu_{A,K} = \mu_{A,L}$, et on notera simplement μ_A.

Preuve – Si l'on est assez savant, c'est une conséquence directe de l'obtention des *invariants de similitude* de A (cf. p. ex. [6] § 4.2) mais rappelons une preuve élémentaire : dire que le polynôme minimal $\mu_{A,K}$ est de degré d implique que $I, A, \ldots, A^{d-1}$ sont K-linéairement indépendantes. Or des vecteurs indépendants d'un K-ev sont encore L-linéairement indépendants en voyant l'indépendance linéaire comme une condition sur des mineurs. Donc $I, A, \ldots, A^{d-1}$ sont encore L-linéairement indépendantes et deg$(\mu_{A,L}) \geqslant d$ ce qui donne le sens non évident. $\square$

Si donc le polynôme minimal se comporte bien par extension de corps, *cela n'est pas le cas de la propriété d'être sans facteur multiple*, ce qui va nous donner la réponse négative aux questions du § 2.1 :

Contre-exemple 1 *Soient p un nombre premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $K = \mathbb{F}_p(T)$ le corps des fractions rationnelles sur $\mathbb{F}_p$ en l'indéterminée T. Si $P = X^p - T$ alors P est irréductible dans $K[X]$ mais si L est un corps de décomposition de P, $L = K(\tau)$ avec $\tau^p = T$ dans L et*

$P = X^p - \tau^p = (X-\tau)^p$. *Ainsi* P *est* sans facteur multiple *dans* $K[X]$ *et est* une puissance *dans* $L[X]$.

Preuve : pour ce qui est de l'écriture $P = (X-\tau)^p$, rappelons qu'en caractéristique p, la formule du binôme se réduit à :

$$(x+y)^p = x^p + y^p, \tag{1}$$

l'application $\square^p$ est donc un morphisme additif, appelé *morphisme de Frobenius*.

Pour voir que $P \in K[X]$ est irréductible on peut voir qu'un facteur irréductible dans $K[X]$ serait de la forme $(X-\tau)^k \in K[X]$ avec $1 \leqslant k < p$ donc k premier avec p, et l'écriture $1 = ku + pv$ donnerait $X - \tau \in K[X]$. $\square$

Traduit en termes matriciels via les matrices « compagnons », ce contre-exemple devient :

Contre-exemple 2 *Avec les notations du contre-exemple 1, soit l'endomorphisme* m_τ *de multiplication par* τ *dans* L *vu comme* K*-ev et* A *sa matrice dans la base* $(1, \tau, \ldots, \tau^{p-1})$ *(dite* matrice compagnon *de* P*).*

Alors A *admet* $P = X^p - T$ *comme polynôme minimal et donc* A *est semi-simple dans* $M_n(K)$ *mais n'est plus semi-simple dans* $M_n(L)$ *(ce qui voudrait dire diagonalisable, cf. rem.1).*

Ainsi la réponse aux deux questions du § 2.1 est non.

2.4. *Version* absolue *de la propriété*

Ainsi, la notion de polynôme sans facteur multiple ne se comportant pas bien par changement de corps, mieux vaut lui substituer la notion suivante :

Définition 3 *Un polynôme* $P \in K[X]$ *est dit* séparable *si, et seulement si, il est premier avec son polynôme dérivé si, et seulement si, il a toutes ses racines simples dans son corps de décomposition.*

L'équivalence des deux propriétés de la définition précédente est directe en notant qu'en toute caractéristique, on peut écrire une formule de Taylor à l'ordre 1 pour les polynômes i.e. $P(X) = P(a) + P'(a)(X-a) + (X-a)^2 Q(X)$.

Rappelons encore la définition suivante :

Définition 4 *Un corps* K *est* parfait *si, et seulement si, tout polynôme* P irréductible *dans* $K[X]$ *est séparable.*

Les corps de caractéristique nulle sont bien sûr parfaits.

Pour un corps de caractéristique p, un polynôme irréductible P est non séparable si, et seulement si $P' = 0$ si, et seulement si, $P = P_1(X^p)$.

On montre que les corps finis sont parfaits[2] et le corps $K = \mathbb{F}_p(X)$ est donc le plus petit exemple raisonnable de corps non parfait, avec comme polynôme non séparable celui du contre-exemple 1 !

Dans le cas parfait, tout va bien sûr mieux :

Proposition 2 *Si K est un corps parfait, un polynôme $P \in K[X]$ est* sans facteur multiple *(déf. 2) si et seulement si il est* séparable *(déf. 3).*

Preuve – Si P est sans facteur multiple, il s'écrit $P = P_1 \dots P_r$ avec les P_i irréductibles dans $K[X]$ comme à la déf. 2. Par l'hypothèse K parfait, chaque P_i a toutes ses racines simples dans L et les P_i étant deux à deux premiers entre eux, P a toutes ses racines simples dans L. La réciproque est directe, vraie dans tout corps, parfait ou non. $\square$

Comme la propriété d'être séparable est définie indépendamment du corps de base, on obtient comme résultat positif :

Théorème 3 *Soit K un corps, $A \in \mathrm{M}_n(K)$ et L un corps de décomposition de μ_A.*

(i) Se valent : (i.a) A est diagonalisable dans $\mathrm{M}_n(L)$, (i.b) A est semi-simple dans $\mathrm{M}_n(L')$ pour toute extension L' de K, (i.c) μ_A est séparable.

(ii) Si K est parfait, A est semi-simple si et seulement si les propriétés du (i) sont vérifiées.

Preuve – (i) Par théorème 2, μ_A est aussi le polynôme minimal de A dans $M_n(L)$, et donc μ_A séparable et scindé sur L équivaut à A diagonalisable sur L i.e. (i.a) $\Leftrightarrow$ (i.c). Par ailleurs (i.b) appliqué à L donne (i.a) et si μ_A est séparable, il est sans facteur multiple sur toute extension L' de K d'où (i.c) $\Rightarrow$ (i.b).

Le (ii) est l'application de la prop. 2 et du (i). $\square$

Définition 5 *Si une matrice A vérifie les conditions du théorème 3 (i), on dit que A est* absolument semi-simple.[3].

Si K est parfait, absolument semi-simple *équivaut donc à* semi-simple.

3. Décomposition *absolument semi-simple + nilpotent*

Le théorème suivant, qui généralise le théorème 1 et se trouve encore dans [3] § 5, No. 9 sous le nom de *théorème de Jordan*, caractérise exactement les endomorphismes ayant une décomposition *absolument semi-simple* + *nilpotent* et montre en particulier que, dans le cas parfait, on obtient toujours la décomposition *semi-simple* + *nilpotent*.

---

2. exercice : passer, pour P non séparable, de la forme $P_1(X^p)$ à $(Q_1(X))^p$, en utilisant la *surjectivité* du morphisme de Frobenius dans les corps finis, ou voir [7] II. 4.
3. suivant l'usage qui qualifie d'*absolue* une propriété « permanente » quand on change de corps de base (cf. [3], § 8)

Théorème 4

(i) Soient K un corps quelconque, E un K-espace vectoriel de dimension finie et $f \in \mathcal{L}(E)$. Se valent :

1. *il existe un couple $(s, n) \in \mathcal{L}(E)^2$ avec s* absolument semi-simple *(cf. déf. 5) et n nilpotent, tels que $f = s + n$ et $s \circ n = n \circ s$.*
2. *le polynôme mimimal μ_f s'écrit : $\mu_f = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ avec chaque P_i* irréduc-tible*,* séparable.

Dans ce cas, le couple (s, n) est déterminé de façon unique et s et n sont des polynômes en f.

(ii) Si K est parfait, la décomposition du (i) 1. est obtenue pour tout $f \in \mathcal{L}(E)$.

(iii) Mieux, K est parfait si, et seulement si, pour tout K-ev de dimension finie E, tout $f \in \mathcal{L}(E)$ admet une telle décomposition.

Preuve partielle – Mentionnons l'argument donnant l'existence *i.e. 2 $\Rightarrow$ 1* : on fixe L corps de décomposition de μ_f sur K. L'extension L/K est alors galoisienne par *2*. On note G le groupe de Galois des K-automorphismes du corps L.

Matriciellement, si $\mathcal{B}$ base de E sur K et $A = \mathrm{Mat}_{\mathcal{B}}(f)$, on décompose A dans $M_n(L)$ en $A = D + N$ (via le théorème 1).

En faisant agir G sur $M_n(L)$, pour tout $\sigma \in G$, $(\sigma D, \sigma N)$ donnent encore une décomposition de Dunford-Jordan de A, et l'unicité dans le théorème 1 permet de conclure que D et N sont fixes par G, et donc, comme L/K est galoisienne, sont dans $M_n(K)$.

On renvoie à loc. cit. pour les autres arguments, plus élémentaires, du (i).

Pour le (iii) : si K n'est pas parfait, il suffit de considérer un polynôme P irréductible non séparable et f un endomorphisme cyclique représenté par la matrice compagnon de P. $\square$

4. Décomposition dans le cas non parfait

4.1. *Semi-simple plutôt qu'absolument semi-simple ?*

Sur un corps non parfait, on a donc des endomorphismes n'admettant pas la décomposition du théorème 4 (cf. (iii) de ce théorème). On peut alors s'intéresser aux endomorphismes semi-simples non absolument semi-simples, suivant la définition 1, qui est une condition géométrique. Se pose alors la :

Question – Si K est un corps non parfait et $f \in \mathcal{L}(E)$ (quelconque, *i.e.* ne vérifiant pas les conditions du théorème 4), existe-t-il une décomposition $f = s + n$ avec s seulement *semi-simple* et pas nécessairement *absolument semi-simple* et si oui, est-elle unique ? (Question soulevée par [2]).

4.2. *Non unicité*

La réponse négative au problème de l'unicité dans la *Question* du § 4.1 est donnée encore dans Bourbaki ([3] § 5, Exercice 14).

Cet exemple fait intervenir un produit tensoriel. Pour ne pas rebuter le lecteur non familier avec cette notion, on le reformule en termes d'algèbre d'endomorphismes, formulation ici équivalente, puis on fait le lien avec la présentation de [3].

Avant cela, à cause de la méthode d'obtention de la composante absolument semi-simple dans le théorème 4, on peut préciser où chercher la non-unicité :

Remarque – Si f admet déjà une décomposition $f = s + n$ avec s absolument semi-simple comme dans le théorème 4, alors toute décomposition semblable $f = s' + n'$ avec s' seulement semi-simple coïncidera en fait avec la première. Les contre-exemples à l'unicité sont donc à chercher parmi les endomorphismes ne vérifiant pas la propriété du théorème 4.

4.2.1. *Le contre-exemple, en termes d'algèbre d'endomorphismes*

On reprend les notations du contre-exemple 1 : soient les corps $K = \mathbb{F}_p(T)$ et $L = K(\tau)$ corps de rupture de $P = X^p - T$, avec $\tau^p = T$. La multiplication m_τ par τ dans L est dans $\mathcal{L}_K(L)$ i.e. est un endomorphisme de L pour sa structure de K-espace vectoriel.

Contre-exemple 3 (Cf. [3] § 5, Exercice 14) *Soit $E = \mathcal{L}_K(L)$ vu comme K-algèbre : on parlera de* la multiplication dans *E pour désigner la loi $\circ$ de composition des endomorphismes. Soient l_τ (resp. r_τ) les endomorphismes K-linéaires de E définis par la multiplication à gauche (resp. à droite) par m_τ dans E (si cela vous paraît compliqué, voir § 4.2.2). Alors :*

(i) l_τ et r_τ sont semi-simples, et commutent entre eux,

(ii) $n := l_\tau - r_\tau$ est nilpotent, non nul, d'indice p,

de sorte que l'écriture $l_\tau = n + r_\tau$ contredit l'unicité d'une décomposition « semi-simple+ nilpotent », commutant entre eux.

Preuve – Par construction, l_τ et r_τ commutent. Par propriété des endomorphismes de multiplication, le polynôme minimal de l_τ et r_τ coïncide avec le polynôme minimal de τ sur K, c'est-à-dire P, donc l_τ et r_τ sont semi-simples. Dans $\mathcal{L}(E)$ e.v. sur K de caractéristique p, la propriété de Frobenius (1) p. 5 donne $n^p = l_\tau^p - r_\tau^p$. Or $l_\tau^p = r_\tau^p = T.\mathrm{Id}_E$: c'est la multiplication par l'endomorphisme $m_{\tau^p} = m_T$ —à gauche ou à droite, c'est la même chose car $T \in K$. On vérifie par ailleurs que $n^q \neq 0$ pour $q < p$. □

4.2.2. *Introduction à la formulation tensorielle de [3]*

L'exemple précédent se comprend mieux en termes de produits tensoriels.

Le lecteur qui ne serait pas à l'aise avec la notion de produit tensoriel d'espaces vectoriels peut se contenter de penser que si L est un K-ev muni d'une base $(e_1, \ldots, e_p)$ alors $E = L \otimes_K L$ est un K-ev de dimension p^2 muni d'une base notée $(e_i \otimes e_j)_{(i,j)\in[1,p]^2}$, et d'une application $\otimes\ :\ L \times L \to L \otimes L$ définie comme suit : si v et w sont des éléments de L, qui s'écrivent $v = \displaystyle\sum_{i=1}^{p} \lambda_i e_i$ et $w = \displaystyle\sum_{j=1}^{p} \mu_j e_j$, on définit un élément $v \otimes w \in E = L \otimes L$ simplement par bilinéarité : $v \otimes w := \displaystyle\sum_{(i,j)\in[1,p]^2} \lambda_i \mu_j\, e_i \otimes e_j$.

L'application $\otimes$ ainsi définie est donc bilinéaire, en particulier :

$$\forall\, \lambda \in K, \forall\, (v, w) \in L^2,\ (\lambda\, v) \otimes w = v \otimes (\lambda w) = \lambda\, (v \otimes w). \qquad (\dagger)$$

On se gardera bien de croire que $\otimes$ est surjective : les éléments de l'image, de la forme $v \otimes w$ sont appelés les éléments purs ; un élément général de $L \otimes L$ est une combinaison linéaire d'éléments purs (puisque $(e_i \otimes e_j)$ est une base).

Si on considère les éléments de L comme des vecteurs-colonnes, on peut identifier $\otimes$ avec $(v, w) \mapsto v.{}^t w$ et par là $L \otimes_K L$ à $\mathcal{L}_K(L)$.[4]. Les éléments purs $v \otimes w$ s'identifient donc aux endomorphismes de rang un dans $\mathcal{L}_K(L)$.

Toute application $\varphi \in \mathcal{L}_K(L)$ permet de construire deux endomorphismes de $E = L \otimes_K L$, disons l_φ et r_φ définis dans la base ci-dessus respectivement par : $l_\varphi(e_i \otimes e_j) := (\varphi(e_i) \otimes e_j)$ et $r_\varphi(e_i \otimes e_j) := e_i \otimes \varphi(e_j)$, *i.e.* suivant qu'on fait agir φ à gauche ou à droite. On vérifie qu'ils s'identifient aux multiplications à gauche et à droite par φ dans $\mathcal{L}_K(L)$.

On introduit maintenant la structure de K-algèbre de $L \otimes L$:

Comme le K-ev L est en outre une K-algèbre, on définit sur $L \otimes L$ une structure de K-algèbre en définissant le produit des éléments purs : $\forall (v_1, w_1, v_2, w_2) \in L^4$, on pose $(v_1 \otimes w_1).(v_2 \otimes w_2) := (v_1.v_2) \otimes (w_1.w_2) \in L \otimes L$ et en étendant ce produit par bilinéarité. Cette structure s'identifie à celle de la K-algèbre $\mathcal{L}_K(L)$.

Ceci simplifie beaucoup la compréhension du contre-exemple : on définit l_τ (resp. r_τ) comme l'endomorphisme de multiplication par $\tau \otimes 1$ (resp. $1 \otimes \tau$) et on reprend en ces termes plus simples la preuve du contre-exemple 3.

4.3. *Non existence*

Le but de cette section est d'expliciter le contre-exemple suivant, qui répond par la négative à l'existence dans la *Question* du § 4.1 d'une décomposition $s + n$.

---

4. Cette identification, dépendant du choix d'un isomorphisme de l'espace vectoriel avec son dual, n'est pas canonique.

Contre-exemple 4 *Soient encore $K = \mathbb{F}_p(T)$ et $P = X^p - T \in K[X]$ comme au contre-exemple 1. Soit $\mathcal{A} = K[X]/(P^d)$ avec $1 < d \leqslant p$. En notant x la classe de X dans $\mathcal{A}$, soit $f = m_x$ l'endomorphisme de multiplication par x dans $\mathcal{A}$. Alors f n'admet pas de décomposition $f = s + n$ avec s semi-simple, n nilpotent, commutant entre eux.*

Pour démontrer ce résultat, on remarque d'abord :

Lemme 3 *Soit K un corps quelconque, et soit $f \in \mathcal{L}(E)$ ayant un polynôme minimal μ_f de la forme P^r où $P \in K[X]$ est irréductible et $r \in \mathbb{N}^*$ quelconque.*

Si f peut s'écrire sous la forme $f = s+n$ avec s semi-simple, n nilpotent, tels que $s \circ n = n \circ s$, alors le polynôme minimal μ_s de s est égal à P.

Preuve – Notons S, N les matrices associées à s, n dans une base de E fixée, et les polynômes caractéristiques avec des χ. Soit $\widehat{K}$ un corps de décomposition de χ_s. Comme S et N commutent, elles sont simultanément triangulables dans $\mathrm{M}_n(\widehat{K})$ i.e. s'écrivent $S = PS_1P^{-1}$ et $N = PN_1P^{-1}$ avec S_1 et N_1 triangulaires supérieures ; N_1, qui est nilpotente, est alors de diagonale nulle. Alors :

$$\begin{aligned}\chi_s &= \det(XI_n - S_1) = \det(XI_n - (S_1 + N_1)),\\ &= \det(XI_n - (S + N)) = \chi_f.\end{aligned}$$

Comme les polynômes minimal et caractéristique d'un endomorphisme ont mêmes facteurs irréductibles, $\mu_f = P^r$ donne $\chi_f = P^k$ pour un $k \geqslant r$. Ainsi, $\chi_s = P^k$ et le polynôme minimal μ_s est à son tour une puissance de P, mais s semi-simple signifie alors (Proposition 1) que $\mu_s = P$. □

On utilise un argument du même type que pour la preuve du lemme 2 page 4 :

Si f est comme donné au contre-exemple 4, et si, *par l'absurde*, f admet une décomposition $f = s + n$ comme énoncé, alors par le lemme précédent, $\mu_s = P$ et donc (cf. page 4) $K[s]$ est un corps et $\mathcal{A}$, vu comme $K[s]$ module, est donc un $K[s]$-espace vectoriel.

Comme $f \circ s = s \circ f$, f est une application $K[s]$-linéaire, et de même pour n.

Or, $\dim_K K[s] = p$ et $\dim_K \mathcal{A} = pd$ impliquent que $\dim_{K[s]} \mathcal{A} = d \quad (*)$.

Enfin, n étant un $K[s]$-endomorphisme nilpotent de $\mathcal{A}$, on obtient maintenant, avec $(*)$, que $n^d = 0$.

Ainsi $P(f) = P(s+n) = (s+n)^p - T = s^p + n^p - T = s^p - T = P(s) = 0$, puisque P est le polynôme minimal de s. C'est une *contradiction* puisque, par construction, le polynôme minimal de f est P^d avec $d > 1$. □

Appendice : généralisations diverses

Dans tout ce qui suit, on note encore $P = X^p - T \in K[X]$ où p est un nombre premier et $K = \mathbb{Z}/p\mathbb{Z}(T)$.

(i) Dans le contre-exemple 4, l'hypothèse $d \leqslant p$, simplificatrice, est en fait inutile. L'endomorphisme compagnon de P^d, à savoir l'endomorphisme $f = m_x$ du contre-exemple, n'admet aucune décomposition *« semi-simple + nilpotent »*, dès qu'il n'est pas lui-même semi-simple *i.e.* que $d > 1$.

En effet, pour tout d :

$$P(f) = P(s+n) = (s+n)^p - T = s^p + n^p - T = P(s) + n^p = n^p.$$

Comme $n^d = 0$, en posant δ le plus petit entier supérieur ou égal à d/p, il vient : $P^\delta(f) = n^{p\delta} = 0$. Or, comme $d > 1$ et $p \geqslant 2$, $\delta < d$. C'est absurde, car P^d est le polynôme minimal de f.

(ii) Cependant, d'autres K-endomorphismes f de polynôme minimal P^d avec $d > 1$, en dimension finie, peuvent admettre une décomposition « $f = s + n$ ». Voici un exemple simple :

Soit E un L-espace vectoriel de dimension $p + 1$, avec $L = K[X]/(P)$, et, toujours en notant x la classe de X dans $K[X]/(P) = L$, soit $s = x\,\mathrm{Id} \in \mathcal{L}_L(E)$ et n n'importe quel L-endomorphisme nilpotent d'indice $p+1$ de E. Comme s est proportionnel sur L, à l'identité, on a $s \circ n = n \circ s$. Soit enfin $f = s + n$. Alors s, n et f sont aussi des endomorphismes de E vu comme K-espace vectoriel. Comme tels, s est semi-simple avec $\mu_s = P$ et on vérifie que $\mu_f = P^2$ (Attention, s et f n'ont pas mêmes polynômes minimaux selon qu'on les considère comme endomorphismes du K-e.v. E, ou du L-e.v. E. Il ne s'agit pas ici d'extension du corps de base). Le K-endomorphisme f admet donc la décomposition *« semi-simple + nilpotent »* $f = s + n$, avec $s \circ n = n \circ s$.

Notons que si on avait pris $1 < \dim_L E \leqslant p$, on aurait obtenu $\mu_f = P$, et donc retrouvé un contre-exemple à l'unicité très proche du contre-exemple 3.

(iii) Par ailleurs, si $\mu_f = P^d$, une décomposition *« semi-simple + nilpotent »*, même quand elle existe, n'a pas le même sens que la décomposition donnée par le théorème 4 dans le cas où $\mu_f = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ avec chaque P_i *irréductible*, *séparable*. En effet, si $\mu_f = P^d$, une telle décomposition ne sera jamais unique, comme peut le montrer une petite réflexion prolongeant le contre-exemple à l'unicité esquissé à la fin du (ii).

Pour ceux qui veulent approfondir le sujet, la surjection canonique $K[f] \cong K[X]/(P^d) \to K[X]/(P) \cong L$ n'admet pas de section, alors qu'elle en admet si f satisfait les hypothèses du théorème 4. Sur ce point de vue, et d'autres éclairages, on pourra aussi consulter la référence [5].

(iv) Le contre-exemple 4 et cet appendice restent valides en prenant pour polynôme P n'importe quel polynôme irréductible non séparable sur un corps K.

Remerciement. Nous remercions Michel Brion pour son aide qui a permis notre réflexion.

Références

[1] J.-M. ARNAUDIES, J. BERTIN, Groupes, algèbres et géométrie, T. 1, ellipses, 1993.

[2] C. BOUBEL, *Intersection of orthogonal or symplectic groups : case of two groups.* Preprint, UMPA, ENS Lyon, 2006.

[3] N. BOURBAKI, Algèbre Chap. VII, Masson, 1981.

[4] N. DUNFORD, *Spectral Operators*, Pacific Journal of Math. **4** (1954), 321–354.

[5] D. FERRAND, Une méthode effective pour la décomposition de Dunford, `http ://perso.univ-rennes1.fr/daniel.ferrand`, 2003.

[6] J. FRESNEL, Algèbre des matrices, Hermann, 1997.

[7] P. SAMUEL, Théorie algébrique des nombres, Hermann, 1971.