Endomorphismes semi-simples

Lionel Chaussade

03/10/07

Un endomorphisme semi-simple est un endomorphisme dont tous les sous-espaces stables possèdent un supplémentaire stable. Le théorème principal donne un critère sur le polynôme minimal d'un endomorphisme pour qu'il soit semi-simple. Ce résultat peut faire office de développement dans plusieurs leçons.

L'étude des endomorphismes semi-simples permet de revoir de nombreux outils d'algèbre linéaire : lemme des noyaux, critères de diagonalisabilité, polynômes d'endomorphismes, décomposition de Dunford.

Un paragraphe sur les endomorphismes semi-simples peut être inséré dans de nombreux plans de leçons :

- 118-Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 122-Matrices équivalentes. Matrices semblables.
- 125-Réduction d'un endomorphisme en dimension finie. Applications.
- 126-Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.
- 127-Endomorphismes diagonalisables.
- 129-Endomorphismes nilpotents.
- 130-Polynômes d'endomorphismes.

La démonstration du théorème principal est donnée en utilisant la notion de modules, mais si cette vision simplifie la démonstration, elle n'est pas nécessaire : on trouvera une démonstration dans [1] p. 219 qui n'utilise pas ce biais.

La démonstration présentée ici est issue principalement de l'exercice 6.8 de [2].

Pour approfondir la notion très générale de semi-simplicité, le lecteur pourra se rapporter au chapitre 17 de [3].

1 Définitions et premiers exemples

Dans la suite K désignera un corps que l'on précisera le cas échéant, E un K-espace vectoriel de dimension finie et u un endomorphisme de E.

Définition 1. *On dit que u est semi-simple si tout sous-espace stable par u admet un supplémentaire stable par u.*

Exemples et remarques :

• Lorsque F est un sous-espace stable de u, cela a un sens de considérer l'endomorphisme u restreint à F que l'on peut voir comme un élément de $\mathcal{L}(F)$.

• Soit u une rotation de $\mathbb{R}^2$ d'angle θ, si $\theta \neq 0$ $[\pi]$ alors u ne possède pas de sous-espaces stables non triviaux, u est donc semi-simple. Si $\theta = 0$ $[\pi]$, toutes les droites sont stables par u, la caractérisation de la semi-simplicité est donc vérifiée automatiquement.

Pour avoir une intuition de la notion de semi-simplicité, voyons d'abord un cas particulier où les choses se simplifient, il s'agit du cas où le corps K est algébriquement clos.

Proposition 1. *Si K est algébriquement clos, alors u est semi-simple si et seulement si u est diagonalisable.*

Sur $\mathbb{C}$, la notion de semi-simplicité n'apporte donc rien de nouveau par rapport à la diagonalisabilité. On verra que sur $\mathbb{R}$, par exemple, il en est autrement.

dém : $\Rightarrow$ on suppose u semi-simple, montrons que E est somme directe des sous-espaces propres de u ce qui impliquera que u est diagonalisable. Soit $F = \bigoplus_{\lambda \in Spec(u)} E_\lambda$

où $E_\lambda = \mathrm{Ker}(u - \lambda \mathrm{id})$, on veut montrer que $F = E$. F est stable par u puisque chacun des sous-espaces propres de u est stable par u. F admet donc un supplémentaire stable par u : G.

Supposons par l'absurde que $G \neq \{0\}$ alors u restreint à G est un endomorphisme. Comme K est algébriquement clos, cet endomorphisme admet un vecteur propre $x \neq 0$ (en effet le polynôme minimal de $u_{|F}$ a une racine qui est donc une valeur propre). Mais alors x est dans l'un des sous-espaces propres de u, il devrait donc appartenir à F. C'est absurde car $F \cap G = \{0\}$. Donc $G = \{0\}$ et $F = E$.

$\Leftarrow$ Réciproquement on suppose que u est diagonalisable, montrons que u est semi-simple. Soit F un sous-espace stable par u, trouvons-lui un supplémentaire stable par u. L'idée va être de fractionner le problème et de le résoudre sur chaque sous-espace propre de u.

On a $E = \bigoplus_{\lambda \in \mathrm{Spec}(u)} E_\lambda$ car u est diagonalisable et

$$F = F \cap E = \bigoplus_{\lambda \in \mathrm{Spec(u)}} F \cap E_\lambda.$$

Pour voir cela on peut appliquer le lemme des noyaux à $u_{|F}$. Rappelons son énoncé :

Théorème 1. *Soit E un K-espace vectoriel, $u \in \mathcal{L}(E)$ et P un polynôme annulateur de u, si $P = Q_1 Q_2 ... Q_n$ où les Q_i sont premiers entre eux 2 à 2, alors $E = \bigoplus_{i=1}^{n} Ker\ Q_i(u)$.*

Le polynôme $P = \prod_{\lambda \in \mathrm{Spec(u)}} (X - \lambda)$ annule u donc annule également $u_{|F}$; d'après le lemme des noyaux (qui s'applique car les $X - \lambda$ sont premiers entre eux) on a :

$$\mathrm{Ker}(P(u_{|F})) = \bigoplus_{\lambda \in \mathrm{Spec}(u)} \mathrm{Ker}(u_{|F} - \lambda \mathrm{id}).$$

or $\mathrm{Ker}(P(u_{|F})) = F$ et $\mathrm{Ker}(u_{|F} - \lambda \mathrm{id}) = F \cap E_\lambda$. Soit G_λ un supplémentaire de $F \cap E_\lambda$ dans E_λ, G_λ est stable par u car inclus dans un sous-espace propre. Alors $G = \bigoplus_{\lambda \in \mathrm{Spec(u)}} G_\lambda$ est bien un supplémentaire de F stable par u.

Remarques :

- Attention en général $E = \bigoplus_i F_i$ n'implique pas que $F \cap E = \bigoplus F \cap F_i$. Par exemple $\mathbb{R}^2 = \mathbb{R}(1,0) \oplus \mathbb{R}(0,1)$ mais $F = \mathbb{R}(1,1)$ fournit un contre-exemple.

- On remarquera que le sens u diagonalisable implique u semi-simple est toujours vrai sans supposer que K est algébriquement clos.

2 Semi-simplicité et polynôme minimal

2.1 Le théorème

Nous allons voir la caractérisation d'un endomorphisme semi-simple :

Théorème 2. *Un endomorphisme u est semi-simple si et seulement si son polynôme minimal, π_u est sans facteurs carrés, c'est à dire que $\pi_u = Q_1 ... Q_r$ où les Q_i sont irréductibles unitaires et distincts.*

Remarque : Si K est algébriquement clos, on retrouve la proposition précédente car les polynômes irréductibles d'un corps algébriquement clos sont de degré 1, et dire que π_u est produit de polynômes de degré 1 distincts signifie exactement que π_u est scindé à racines simples et donc que u est diagonalisable.

Exemple : Un endomorphisme nilpotent est semi-simple si et seulement si il est nul. En effet le polynôme minimal d'un endomorphisme nilpotent est de la forme $\pi_u = X^r$, si u est semi-simple ce polynôme ne peut avoir de facteurs carrés donc $r = 1$ et u est nul. Intuitivement les endomorphismes semi-simples sont vraiment à l'opposé des nilpotents, presque en "somme directe", en effet la décomposition de Dunford que l'on verra au chapitre 4 renforce cette idée.

Il y a deux manières de démontrer ce théorème : l'une utilisant les modules (voir exercice 6.8 de [2]), l'autre plus élémentaire mais plus longue ([1] p. 219). Enfin une troisième démonstration sera proposée en annexe, elle utilise les modules sans en faire mention explicitement.

La démonstration qui va suivre peut constituer un développement dans les leçons suivantes :

- 118-Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 126-Sous espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.
- 130-Polynômes d'endomorphismes. Polynômes annulateurs. Applications.

Mais avant de commencer la démonstration proprement dite, mettons en place les outils nécessaires en faisant quelques rappels sur les modules.

2.2 Endomorphismes et $K[X]$-modules

Rappelons tout d'abord quelques définitions :

Définition 2. *Soit A un anneau, $(M, +, .)$ est un A-module si $(M, +)$ est un groupe abélien et si . est une loi externe de $A \times M \to M$ telle que :*

- $\forall a \in A,\ \forall (m_1, m_2) \in M^2,\ a.(m_1 + m_2) = a.m_1 + a.m_2,$
- $\forall (a_1, a_2) \in A^2,\ \forall m \in M,\ (a_1 + a_2).m = a_1.m + a_2.m,$
- $\forall (a_1, a_2) \in A^2,\ \forall m \in M,\ (a_1 a_2).m = a_1.(a_2.m),$
- $\forall m \in M,\ 1_A.m = m.$

On remarque que ce sont les mêmes axiomes que dans la définition d'un espace vectoriel (cas où A est un corps).

Définition 3. *$N \subset M$ est un sous-module si N est un sous-groupe de M et $\forall (a, x) \in A \times N,\ a.x \in N$.*

Proposition 2. *Si I est un idéal de A qui annule M (c'est-à-dire $\forall i \in I,\ \forall x \in M,\ i.x = 0$), alors M a une structure de A/I-module.*

Dém : La loi interne de M est la même, il suffit de vérifier que la loi externe passe au quotient. Si x et y sont dans A tels que $\bar{x} = \bar{y}$ dans A/I alors $y = x + i$ avec $i \in I$. On définit la loi externe par $\bar{x}.m = x.m$, cette loi est clairement définie vu qu'elle ne dépend pas du représentant choisi puisque $y.m = (x + i).m = x.m$.

La donnée de $u \in \mathcal{L}(E)$ permet de définir une structure de $K[X]$-module sur E. La loi interne de E est l'addition de E. La loi externe est la suivante :

$$\forall P \in K[X],\ \forall x \in E,\ P.x = P(u)(x).$$

Réciproquement toute structure de $K[X]$-module sur E est donnée de cette manière-là, on retrouve l'endomorphisme u car $X.x = u(x)$.

Donc se donner un espace vectoriel et un endomorphisme revient au même que se donner une structure de $K[X]$-module sur E.

Proposition 3. *1) Soit F un sous-espace vectoriel de E, F est stable par u si et seulement si F est un sous-$K[X]$-module de E.*

2) u est semi-simple si et seulement si tout sous-$K[X]$-module de E admet un sous-module supplémentaire.

3) Si P est un polynôme annulateur de u alors E a une structure de $K[X]/(P)$-module.

Dém :

1) Si F est stable par u alors $\forall x \in F$, $P.x = P(u)(x) \in F$ donc F est bien un sous-module. Il est clair que c'est équivalent.

2) Un sous-module F est aussi un sous-espace vectoriel stable par u, il admet donc un supplémentaire stable par u qui est donc un sous-module. Ces notions étant équivalentes, la réciproque se fait de la même manière.

3) On utilise la proposition précédente, en remarquant que l'idéal (P) annule E car $\forall x \in E,\ P(u)(x) = 0$.

2.3 Démonstration du théorème 2

Elle va se faire en trois étapes :

1) Si u est semi-simple alors π_u est sans facteurs carrés.

2) Si π_u est irréductible alors u est semi-simple (cette partie utilisera les modules, une version alternative est en annexe).

3) Si π_u est sans facteurs carrés alors u est semi-simple.

1) Supposons par l'absurde que $\pi_u = P^2Q$ avec P un polynôme unitaire non constant. Soit $F = \mathrm{Ker}(P(u))$. F est stable par u, en effet si $x \in F$ alors $P(u)(u(x)) = u(P(u)(x)) = 0$ (les polynômes en u commutent). Comme u est semi-simple, F admet donc un supplémentaire stable par u, notons-le G. On va montrer que PQ est un polynôme annulateur de u ce qui sera contradictoire.

Pour cela montrons que $PQ(u)$ s'annule sur F et G et comme ils sont supplémentaires, on pourra alors conclure. On a $P(u) \circ PQ(u)(G) = \{0\}$ donc $PQ(u)(G) \subset F$. Mais comme G est stable par u, on a aussi $PQ(u)(G) \subset G$ donc $PQ(u)(G) \subset F \cap G = \{0\}$. D'autre part $PQ(u)(F) = QP(u)(F) = \{0\}$ puisque $F = \mathrm{Ker}(P(u))$. Donc $PQ(u)(F + G) = \{0\}$. C'est absurde.

2) On suppose π_u irréductible, montrons que u est semi-simple. D'après la proposition 3, E est un $L = K[X]/(\pi_u)$-module. Mais comme π_u est irréductible, E est un L-espace vectoriel.

Soit F un sous-espace stable par u, c'est donc un sous-L-espace vectoriel de E toujours d'après la proposition 3. Il admet donc un supplémentaire G qui est un sous-L-espace vectoriel, il est donc stable par u. Donc u est semi-simple.

3) L'idée va être comme dans la démonstration du théorème 1 de fragmenter l'espace vectoriel pour simplifier le problème puis de recoller les solutions. On suppose que π_u est sans facteurs carrés, c'est-à-dire que $\pi_u = \prod_{i=1}^{r} Q_i$ où les Q_i sont irréductibles unitaires. D'après le lemme des noyaux, $E = \bigoplus_{i=1}^{r} F_i$ où $F_i = \mathrm{Ker}(Q_i(u))$. De la même manière que dans la proposition 1, si F est un sous espace stable par u alors $F = \bigoplus_{i=1}^{r} F \cap F_i$. A présent, $u_{|F_i}$ est semi-simple d'après 2) car son polynôme minimal est Q_i qui est irréductible. Donc $F \cap F_i$ admet un supplémentaire stable par $u_{|F_i}$, notons le G_i. Alors $G = \bigoplus_{i=1}^{r} G_i$ est un supplémentaire de F stable par u. Donc u est semi-simple.

Remarque : En application du théorème, on peut voir que si u est semi-simple et F est stable par u alors $u_{|F}$ est semi-simple.

3 Semi-simplicité et extension de corps

On va montrer que la semi-simplicité ne dépend pas du corps sur lequel on voit l'endomorphisme, plus précisément :

Proposition 4. *Soient $K \subset L$ deux corps de caractéristique nulle. Soit $U \in M_n(K)$ alors U est semi-simple en tant que matrice à coefficients dans K si et seulement si U est semi-simple en tant que matrice à coefficients dans L.*

La démonstration utilise le lemme suivant :

Lemme 1. *Le polynôme minimal de U sur K, $\pi_{U,K}$ et le polynôme minimal de U sur L, $\pi_{U,L}$ sont égaux.*

Admettons un instant le lemme et démontrons la proposition 4 :
Dém :
D'après le lemme $\pi_{U,K} = \pi_{U,L}$ donc il suffit de montrer, d'après le théorème 2 que $\pi_{U,K}$ est sans facteurs carrés sur K si et seulement si il est sans facteurs carrés sur L.

Or, on sait que P est sans facteurs carrés si et seulement si $\mathrm{pgcd}(P, P') = 1$ (ici on utilise le fait que la caractéristique est nulle).

Le calcul du pgcd de deux polynômes ne dépend pas du corps sur lequel on voit les polynômes, en effet l'algorithme d'Euclide qui permet de calculer le pgcd reste le même (unicité de la division euclidienne sur L). Le fait que $\pi_{U,K}$ et $\pi'_{U,K}$ soient premiers entre eux ne dépend pas non plus du corps de base.

Dém du lemme : Il y a plusieurs démonstrations du lemme, l'une utilisant les invariants de similitude (corollaire 6.97 de [2]), l'autre plus élémentaire.

On a $\pi_{U,K} \in K[X] \subset L[X]$ donc comme $\pi_{U,K}(U) = 0$ on a $\pi_{U,L} | \pi_{U,K}$; les polynômes étant unitaires, il suffit donc de vérifier qu'ils ont le même degré.

Pour n'importe quel corps T, le degré du polynôme de $U \in M_n(T)$ est le rang, r, de la famille $(\mathrm{id}, U, U^2, ..., U^{n^2-1})$. On convertit les matrices U^j en vecteurs colonnes de taille n^2. Le rang r est égal au rang de cette famille de vecteurs colonnes.

Si l'on concatène ces vecteurs en une matrice de taille $n^2 \times n^2$, r est également le rang de cette matrice. Or le rang d'une matrice ne dépend pas du corps dans lequel il est calculé car le rang se calcule à l'aide de déterminants extraits (une matrice A est de rang r lorsque tous ses déterminants extraits de taille $r+1$ sont nuls et qu'il existe un déterminant extrait de taille r non nul).

En conclusion le degré du polynôme minimal d'un endomorphisme se calcule grâce au rang d'une matrice plus grande, ce rang ne dépendant pas du corps de base, on a donc $\deg(\pi_{U,K}) = \deg(\pi_{U,L})$. Donc les deux polynômes minimaux sont égaux.

La proposition précédente permet de parler d'endomorphisme semi-simple sans préciser dans quel corps on voit l'endomorphisme, de plus on a le résultat :

Proposition 5. *Soit K un corps de caractéristique 0. Soit $U \in M_n(K)$, alors U est semi-simple si et seulement si U est diagonalisable dans une extension de K.*

Dém : Supposons U semi-simple et considérons une extension de K dans laquelle π_U est scindé, L (par exemple une clôture algébrique de K). U est également semi-simple dans L d'après la proposition précédente donc π_U est scindé et tous ses facteurs irréductibles sont simples, donc π_U est scindé à racines simples et U est diagonalisable dans L.

Réciproquement si U est diagonalisable dans L alors U est semi-simple dans L (première proposition) donc dans K aussi.

Ce résultat montre en particulier qu'un endomorphisme réel est semi-simple si et seulement si il est diagonalisable dans $\mathbb{C}$.

4 Application à la décomposition de Dunford

Voici le théorème classique de la décomposition de Dunford, on verra ensuite une version plus générale utilisant la semi-simplicité.

Théorème 3. *Soit $u \in \mathcal{L}(E)$, avec E un K-espace vectoriel de dimension finie, K étant un corps algébriquement clos, alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que :*
- *d diagonalisable,*
- *n nilpotent,*
- *$dn = nd$,*
- *$u = d + n$.*

Il y a par exemple une démonstration dans [1] p. 191, cela utilise principalement le lemme des noyaux et la notion de sous-espaces caractéristiques.

Remarques :

- On peut trouver dans [1] un algorithme explicite pour trouver d et n toutefois cet algorithme nécessite la connaissance préalable des valeurs propres de l'endomorphisme.
- Une méthode présentée par Daniel Ferrand dans un document disponible sur le site de la préparation à l'agrégation de Rennes présente une méthode pour obtenir la décomposition de Dunford sans connaître les valeurs propres et utilisant une variante de l'algorithme de Newton.

Applications de la décomposition de Dunford :

- Connaître une telle décomposition est utile pour le calcul d'exponentielle de matrice, car $\exp(u) = \exp(d+n) = \exp(d)\exp(n)$ (d et n commutant).
- On peut montrer en utilisant la décomposition de Dunford que u est diagonalisable si et seulement si $\exp(u)$ est diagonalisable (voir exercice 4.18 de [2]).

Théorème 4. *(Dunford version semi-simple)*
Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Alors il existe un unique couple $(s, n) \in \mathcal{L}(E)$ tel que :
- *s semi-simple,*
- *n nilpotent,*
- *$sn = ns$,*
- *$u = s + n$.*

Cette version du théorème est donc plus générale.
Dém : L'unicité provient du fait que u peut être vu comme un endomorphisme à coefficients dans $\mathbb{C}$ donc s qui peut être vu dans $\mathbb{C}$ aussi est diagonalisable, donc l'unicité provient de l'unicité du théorème précédent.
Soit $U = D + N$ la décomposition de Dunford selon le théorème 1 (on voit U comme étant à coefficients complexes) alors $\bar{U} = \bar{D} + \bar{N}$. Or $U = \bar{U}$, $\bar{N}$ est nilpotente et $\bar{D}$ est diagonalisable dans $\mathbb{C}$. Donc par unicité $D = \bar{D}$ et $N = \bar{N}$. Ce qui démontre le théorème puisque diagonalisable dans $\mathbb{C}$ signifie semi-simple.

Application : Cette généralisation sert, par exemple, à montrer que $\exp(M_n(\mathbb{R})) = \{A \in Gl_n(\mathbb{R}),\ \exists B \in M_n(\mathbb{R}),\ A = B^2\}$ voir [2] exercice 4.17.

5 Annexe

Voyons à présent une démonstration alternative de l'étape 2 du théorème 2.
Dém : On suppose que π_u est irréductible, montrons que u est semi-simple. On remarque que $L = K[X]/(\pi_u)$ est un corps puisque π_u est irrédutible. On peut alors voir E comme un L-espace vectoriel avec la multiplication externe : $P.x = P(u)(x)$. Ici il faut vérifier que la multiplication ne dépend pas du représentant choisi (cela vient du fait que π_u est un polynôme annulateur) et que les conditions pour avoir un espace vectoriel sont vérifiées. C'est fastidieux mais élémentaire.
On va interpréter les sous-K-espaces vectoriels u-stables en termes de sous L-espaces vectoriels. Si F est un sous-K-espace vectoriel u-stable alors F est également stable par tous les polynômes en u donc F est un sous L-espace vectoriel de E.
Donc F admet un sous-L-espace vectoriel supplémentaire, G, qui est donc un sous-K-espace vectoriel u-stable.
Donc u est semi-simple.
Remarque : Cette démonstration est exactement la même que celle utilisant les modules mais elle évite de parler de modules (même si la notion est sous-jacente) puisqu'en définitive on ne se sert que d'espaces vectoriels.

Références :
[1] : Gourdon : Algèbre.
[2] : Beck, Malick, Peyré : Objectif Agrégation.
[3] : Lang : Algebra.

Merci à Clément qui m'a suggéré la démonstration alternative présentée en annexe.
Merci aussi à Marie, Mathilde et Clément qui ont bien voulu relire ce document et corriger de nombreuses fautes.