Endomorphismes semi-simples

Références : Beck, Malick, Peyré, *Objectif Agrégation*, (Application 4.32 p. 160, exercice 4.23 p. 229 et exercice 6.8 p. 324), Francinou, Gianella, Nicolas, *Oraux X-ENS : Algèbre, Tome 2*, Gourdon, *Algèbre*.

Soit E un espace vectoriel sur un corps k, de dimension finie n. On dit qu'un endomorphisme $u \in \mathrm{L}(E)$ est *semi-simple* si et seulement si tout sous-espace u-stable $F \subset E$ possède un supplémentaire u-stable. Nous utiliserons cette notion surtout lorsque le corps de base k est *parfait*, ce qui veut dire par définition que k est soit de caractéristique 0, soit de caractéristique $p > 0$ avec un endomorphisme de Frobenius surjectif.

Exemples de corps parfaits : les corps de caractéristique 0, les corps finis, les corps algébriquement clos.

Exemples de corps non parfaits : corps de fractions rationnelles en une ou plusieurs indéterminées sur un corps de carcactéristique $p > 0$, typiquement, $\mathbb{F}_p(X)$.

Théorème : *Soient les conditions :*

(i) *u est semi-simple.*

(ii) *le polynôme minimal de u est produit de polynômes irréductibles distincts.*

(iii) *u est diagonalisable sur une clôture algébrique de k.*

Alors (i) $\iff$ (ii) $\Leftarrow$ (iii), et si k est parfait les trois conditions sont équivalentes.

Lemme : *Soit u un endomorphisme et $\mu_u = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition de son polynôme minimal en facteurs irréductibles. Soit $E_i = \ker(P_i^{\alpha_i}(u))$. Pour tout sous-espace vectoriel $F \subset E$ qui est u-stable, on a $F = \oplus F \cap E_i$.*

Preuve : Il est clair que les espaces $F \cap E_i$ sont en somme directe. Il suffit de voir qu'ils engendrent F. Or pour $x \in F$, on peut écrire $x = x_1 + \dots + x_r$ avec $x_i \in E_i$. On utilise le fait que les projecteurs $\pi_i \colon E \to E_i$, $x \mapsto x_i$, sont des polynômes en u. Alors si F est stable par u, il est stable par π_i, donc $x_i = \pi_i(x) \in F$ et c'est gagné. □

Preuve du théorème :

i ⇒ ii Soit u semi-simple. Supposons que la décomposition du polynôme minimal μ_u contient un facteur carré : $\mu_u = P^2 Q$. On va montrer que $(PQ)(u) = 0$ ce qui contredira le fait que le polynôme minimal de u est P^2Q. Soit $F = \ker(P(u))$ et S un supplémentaire u-stable de F. Soit $a = (PQ)(u)$, alors :

- a est nul sur F puisque $a = (QP)(u) = Q(u) \circ P(u)$.
- a est nul sur S. En effet si $y \in S$, on a $a(y) \in F$ puisque $P(u)[a(y)] = (P^2Q)(u)(y) = 0$ et $a(y) \in S$ puisque S est stable par u, donc par a qui est un polynôme en u. Donc $a(y) \in F \cap S$, donc $a(y) = 0$ car $F \cap S = 0$, cqfd.

En conclusion $a = 0$, d'où la contradiction cherchée, donc il n'y pas de facteur carré dans μ_u.

ii $\Leftarrow$ i Réciproquement supposons que $\mu_u = P_1 \dots P_r$ avec tous les P_i irréductibles distincts. Soit F un sous-espace stable, on va lui construire un supplémentaire stable. Soit $E_i = \ker(P_i(u))$. D'après le lemme on a $F = \oplus F \cap E_i$ de sorte que si pour chaque i on construit un supplémentaire stable pour $F \cap E_i$ dans E_i, par somme on aura un supplémentaire pour F dans E. Comme $\mu_{u_{|E_i}} = P_i$, on se ramène ainsi au cas où $\mu_u = P$ est irréductible.

Si $F = E$ on a un supplémentaire stable $G = 0$ est c'est fini. Sinon, il existe $x \in E - F$. Considérons le morphisme de k-algèbres $\varphi\colon k[X] \to E$ défini par

$$Q \mapsto Q(u)(x)$$

On note $G_x = \{Q(u)(x),\, Q \in k[X]\}$ son image, et P_x le polynôme unitaire générateur de son noyau. On va montrer que $F \cap G_x = 0$. Ceci fait, en itérant on construira $G_{x'}, G_{x''}$,... et le supplémentaire cherché sera $G_x \oplus G_{x'} \oplus G_{x''} \dots$.

Par définition de $\mu_u = P$ on a $P_x | P$ donc ils sont égaux puisque P est irréductible. Soit $y \in F \cap G_x$, que l'on peut écrire sous la forme $y = Q(u)(x)$. J'affirme que $P | Q$ de sorte que $y = 0$, ce qui conclura à $F \cap G_x = 0$. En effet, si P ne divise pas Q alors ces polynômes sont premiers entre eux, choisissons une relation de Bézout $UP + VQ = 1$. L'image par φ de cette relation de Bézout donne, dans E :

$$U(u)[\underbrace{P(u)(x)}_{=0}] + V(u)[\underbrace{Q(u)(x)}_{y}] = x$$

Or $V(u)(y) \in F$ car F est stable sous u. Ceci contredit le choix de $x \in E - F$.

iii $\Leftarrow$ ii Le polynôme minimal est inchangé par extension du corps de base, donc si u est diagonalisable sur une clôture algébrique $\overline{k}$ de k, alors μ_u est scindé dans $\overline{k}$ à racines simples et distinctes. A fortiori, comme polynôme à coefficients dans k, il est sans facteur carré.

ii $\Leftarrow$ iii lorsque k est parfait. Montrons d'abord que le polynôme dérivé μ' est non nul. Dans le cas contraire, ceci veut dire que c'est un polynôme en X^p i.e. $\mu_u(X) = F(X^p)$. Comme k est parfait, tous les coefficients de P sont des puissances p-èmes et donc $F(X^p) = (G(X))^p$. Ceci contredit le fait que μ_u est sans facteur carré. Il en résulte que $\mu'_u \neq 0$, et donc le pgcd de μ_u et μ'_u comme polynômes à coefficients dans $\overline{k}$ est égal à 1. Le pgcd est inchangé par extension du corps de base (ce fait est, par exemple, un corollaire du calcul du pgcd par l'algorithme d'Euclide), donc finalement μ_u est sans facteur carré, c'est-à-dire produit de polynômes irréductibles distincts de $k[X]$. □

Contre-exemple 1 : Soit le corps non parfait $k = \mathbb{F}_2(T)$, corps des fractions rationnelles en l'indéterminée T sur $\mathbb{F}_2$. Considérons l'espace vectoriel $E = k^2$ et l'endomorphisme

$$u = \begin{pmatrix} 1 & T+1 \\ 1 & 1 \end{pmatrix}.$$

Le polynôme caractéristique de u est $\chi_u(X) = X^2 + T$ (attention : $1 = -1$ dans k). Ce polynôme est irréductible, car T n'est pas un carré dans k, donc u est un endomorphisme semi-simple. Supposons que u est diagonalisable sur une clôture algébrique $\overline{k}$ de k. Soit α une racine de χ_u dans $\overline{k}$, on a $\chi_u(X) = (X + \alpha)^2$. Donc u est semblable dans $\overline{k}$ à l'homothétie $\alpha\,\mathrm{Id}$, et domme les homothéties commutent à toutes les matrices, il s'ensuit qu'en fait $u = \alpha\,\mathrm{Id}$. Ceci n'est pas le cas, donc u n'est pas diagonalisable sur $\overline{k}$. □

Contre-exemple 2 : Voici une métode plus facile, et plus conceptuelle aussi, pour donner un contre-exemple. Soit A une algèbre unitaire et associative sur un corps k, et $\mathrm{End}_k(A)$ l'anneau des endomorphismes de k-espace vectoriel. Pour tout $a \in A$, on note $G_a : A \to A$ l'endomorphisme de multiplication à gauche par a, tel que $G_a(x) = ax$. On vérifie alors facilement qu'en associant à a le morphisme G_a on définit un morphisme injectif de k-algèbres $A \hookrightarrow \mathrm{End}_k(A)$. Si A est de dimension finie n, l'algèbre $\mathrm{End}_k(A)$ est isomorphe à l'algèbre des matrices carrées (n, n).

Soit le corps des fractions rationnelles $k = \mathbb{F}_p(T)$, soit le corps $A = k[U]/(U^p - T)$ et u l'image de l'indéterminée U dans A. Le polynôme minimal de $u \in \mathrm{End}_k(A) \simeq \mathrm{M}_p(k)$ est $X^p - T$, qui est irréductible, donc u est semi-simple. En revanche, il n'est pas diagonalisable sur une clôture algébrique $\overline{k}$, car son polynôme minimal a une seule racine α dans $\overline{k}$ et u n'est pas une homothétie. □

La décomposition $u = d + n$ dite de Jordan-Dunford, valable pour un endomorphisme dont le polynôme caractéristique est scindé, s'étend comme suit.

Proposition : *Soit k un corps parfait et soit $u \in \mathrm{L}(E)$ un endomorphisme quelconque. Alors il existe un couple (s, n) unique avec*

(1) $u = s + n$,

(2) *s semi-simple et n nilpotent,*

(3) $sn = ns$.

Le cas particulier $k = \mathbb{R}$ est le plus important pour nous. Démontrons le résultat dans ce cas particulier très simple. On peut plonger $\mathrm{M}_n(\mathbb{R})$ dans $\mathrm{M}_n(\mathbb{C})$ et pour tout endomorphisme a, représenté par une matrice complexe dans une base fixée, notons $\overline{a}$ l'endomorphisme représenté par la matrice dont les coefficients sont les complexes conjugués. La proposition dit juste ceci : on peut écrire la décomposition $u = d + n$ dans $\mathbb{C}$. On a $\overline{u} = u$ et comme $\overline{u} = \overline{d} + \overline{n}$, par unicité de la décomposition de Dunford on a $\overline{d} = d$, $\overline{n} = n$. Donc d et n sont en fait à coefficients dans $\mathbb{R}$. Clairement d est semi-simple, on a donc la décomposition cherchée.

Preuve : La démonstration utilise un peu de théorie de Galois. Soit K le corps de décomposition du polynôme caractéristique μ_u. Comme k est parfait, c'est une extension galoisienne de k. Soit G le groupe de Galois de K sur k. Si on choisit une base de E alors $\mathrm{L}(E \otimes_k K)$ s'identifie à l'anneau des matrices (n, n) à coefficients dans K. Via cette identification, le groupe G agit sur $\mathrm{L}(E \otimes_k K)$ en agissant sur les coefficients des matrices. La théorie de Galois nous dit que $k = K^G$, et donc les éléments de $\mathrm{L}(E \otimes_k K)$ fixés par G sont les éléments de $\mathrm{L}(E)$.

Sur K, on peut écrire la décomposition $u = d + n$ où d et n sont dans $\mathrm{L}(E \otimes_k K)$. Pour tout $\sigma \in G$, on a $u^\sigma = u$ car $u \in \mathrm{L}(E)$. Or on peut écrire $u^\sigma = d^\sigma + n^\sigma$. Il est facile (immédiat !) de voir que d^σ est diagonalisable et n^σ est nilpotent, donc par unicité de la décomposition $d + n$ on doit avoir $d^\sigma = d$ et $n^\sigma = n$. Ainsi d et n sont fixes sous G, donc dans $\mathrm{L}(E)$. On pose $s = d$ qui est bien semi-simple (puisque diagonalisable lorsqu'on passe sur K). Sur k, on a la décomposition $u = s + n$ souhaitée. □

Contre-exemple 3 : Nous reprenons la méthode du contre-exemple 2. Soit $k = \mathbb{F}_p(T)$ et l'algèbre $A = k[U, V]/(U^p - T, V^p)$ qui n'est pas un corps. Soient u, v les images de U, V dans A. On vérifie que u est semi-simple de polynôme minimal irréductible $X^p - T$, $u + v$ est semi-simple de polynôme minimal $X^p - T$ également, et v est nilpotent de polynôme minimal X^p. Ainsi on a $u = (u + v) - v$ ce qui met en défaut l'unicité de la décomposition $s + n$.