DÉVELOPPEMENT 29

ENDOMORPHISMES SEMI-SIMPLES

Définition. — Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.

(*i*) On dit que $f \in \mathcal{L}(E)$ est *semi-simple* si pour tout sous-espace F de E stable par f, il existe un supplémentaire S de F stable par f.

(*ii*) On dit que $M \in \mathcal{M}_n(\mathbb{K})$ est semi-simple si l'endomorphisme $x \mapsto Mx$ est semi-simple.

Lemme. — *Soit $f \in \mathcal{L}(E)$ est tel que μ_f soit irréductible alors f est semi-simple.*

Démonstration. — Soit F un sous-espace strict de E stable par f et soit $x_1 \in E \setminus F$ alors le sous-espace $E_{x_1} = \{P(f)(x_1)\ ;\ P \in \mathbb{K}[X]\}$ est stable par f et $I_{x_1} = \{P \in \mathbb{K}[X]\ ;\ P(f)(x_1) = 0\}$ est un idéal non nul de $\mathbb{K}[X]$ (puisque $\mu_f(f)(x_1) = 0$) donc il existe $\pi_1 \in \mathbb{K}[X]$ unitaire tel que $I_{x_1} = \pi_1\mathbb{K}[X]$. De plus, $x_1 \neq 0$ donc id $\notin I_{x_1}$ *i.e.* π_1 n'est pas constant. Puisque μ_f est irréductible et divisible par π_1, on a en fait $\mu_f = \pi_1$ d'où (d'après l'hypothèse) π_1 irréductible.

Supposons qu'il existe $y \in E_{x_1} \cap F$ non nul, on écrit $y = P(f)(x_1)$ avec $P \in \mathbb{K}[X]$; alors π_1 est irréductible et ne divise pas P donc π_1 et P sont premiers entre eux et il existe donc $U, V \in \mathbb{K}[X]$ tels que $UP + V\pi_1 = 1$ d'où

$$x_1 = U(f) \circ P(f)(x_1) + V(f) \circ \pi_1(f)(x_1) = U(f) \circ P(f)(x_1) = U(f)(y)$$

mais $y \in F$ et F est stable par f donc $U(f)(y) \in F$ ce qui est impossible par choix de x_1. On a donc $E_{x_1} \cap F = \{0\}$ *i.e.* E_{x_1} et F sont en somme directe. Si $F \oplus E_{x_1} = E$, c'est fini, sinon on considère $x_2 \in E \setminus F \oplus E_{x_1}$. Puisque E est de dimension finie, on obtient une décomposition de la forme

$$E = F \oplus E_{x_1} \oplus \cdots \oplus E_{x_r}$$

avec chaque E_{x_i} stable par f ; on pose donc $S = E_{x_1} \oplus \cdots \oplus E_{x_r}$. □

Proposition. — *Si $f \in \mathcal{L}(E)$ alors on a équivalence entre*

(*i*) *f est semi-simple*

(*ii*) *μ_f est un produit de polynôme irréductibles unitaires deux à deux distincts.*

Démonstration. — $\boxed{(i) \Rightarrow (ii)}$ Si μ_f a un facteur carré *i.e.* si $\mu_f = M^2N$, alors $F = \ker M(f)$ est stable par f donc il existe un supplémentaire S de F stable par f. Soit $x \in S$ alors $M(f) \circ MN(f)(x) = \mu_f(f)(x) = 0$ *i.e.* $MN(f)(x) \in F$ et, d'autre part, S est stable par f donc $MN(f)(x) \in S$; on a donc $MN(f)(x) \in F \cap S = \{0\}$ *i.e.* $MN(f)$ s'annule sur S. Si $x \in F$ alors $MN(f)(x) = N(f)(M(f)(x)) = 0$ *i.e.* $MN(f)$ s'annule sur F. Il s'ensuit que $MN(f)$ est nul alors que $\deg MN < \deg \mu_f$ ce qui contredit la définition du polynôme minimal.

$\boxed{(ii) \Rightarrow (i)}$ On décompose $\mu_f = P_1 \cdots P_r$ et on note $F_i = \ker P_i(f)$. Soit F stable par f alors on a $E = F_1 \oplus \cdots \oplus F_r$ et $F = (F \cap F_1) \oplus \cdots \oplus (F \cap F_r)$. Chaque F_i est stable par f et on peut considérer la restriction $f_i \in \mathcal{L}(F_i)$ de f à F_i. Pour tout i, on a $P_i(f_i) = 0$ avec P_i irréductible donc $P_i = \mu_{f_i}$ et, d'après le lemme, f_i est semi-simple *i.e.* il existe S_i stable par f_i tel que $F_i = (F \cap F_i) \oplus S_i$. Il suffit alors de poser $S = S_1 \oplus \cdots \oplus S_r$. □

Corollaire. — *Si $\mathbb{K}$ est algébriquement clos alors $f \in \mathcal{L}(E)$ est semi-simple si et seulement si f est diagonalisable.*

Démonstration. — Si $\mathbb{K}$ est algébriquement clos alors les polynômes irréductibles sur $\mathbb{K}$ sont ceux de degré 1 donc μ_f est sans facteur carré si et seulement si μ_f est scindé à racines simples. □

Proposition. — *Soit $M \in \mathcal{M}_n(\mathbb{R})$.*

(*i*) *M est semi-simple si et seulement si M est diagonalisable dans $\mathcal{M}_n(\mathbb{C})$.*

(*ii*) *Si $M \in \mathcal{M}_n(\mathbb{R})$ est semi-simple alors M est semblable dans $\mathcal{M}_n(\mathbb{R})$ à une matrice de la forme $\begin{bmatrix} D & 0 \\ 0 & B \end{bmatrix}$ avec D diagonale et B constituée de blocs de la forme $\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ centrés sur sa diagonale principale.*

Démonstration. — (*i*) Si M est semi-simple alors $\mu_M = P_1 \cdots P_r$ avec les P_i irréductibles unitaires deux à deux non associés. Soit $\alpha \in \mathbb{C}$ une racine de μ_M alors α est une racine de l'un des P_i, par exemple P_1, or P_1 est irréductible sur $\mathbb{R}$ donc α est racine simple de P_1. Pour $i > 1$, on a P_i et P_1 premiers entre eux *i.e.* $UP_i + VP_1 = 1$ avec $U, V \in \mathbb{R}[X]$ donc $UP_i(\alpha) = 1$ *i.e.* α n'est pas racine des autres P_i donc μ_M est à racines simples et il s'ensuit que M est diagonalisable sur $\mathbb{C}$. Réciproquement, si M est diagonalisable sur $\mathbb{C}$ alors $\mu_M \in \mathbb{R}[X]$ est scindé à racines simples dans $\mathbb{C}$ donc μ_M est sans facteur carré dans $\mathbb{C}[X]$ et *a fortiori* dans $\mathbb{R}[X]$.

(*ii*) On raisonne par récurrence sur n, le cas $n = 1$ étant trivial. Si μ_M est scindé sur $\mathbb{R}$ alors, d'après le première proposition et puisque M est semi-simple, μ_M est un produit de polynômes irréductibles distincts donc est à racines simples et il s'ensuit que M est diagonalisable sur $\mathbb{R}$. On peut donc supposer que $\mu_M = [(X-\alpha)^2 + \beta^2]Q$ avec $\alpha \in \mathbb{R}$, $\beta > 0$ et $Q \in \mathbb{R}[X]$ et on pose $E = \ker[(M-\alpha)^2 + \beta^2\mathrm{I}]$. Puisque Q divise strictement μ_M, on a $Q(M) \neq 0$ donc $[(X-\alpha)^2 + \beta^2]$ n'est pas inversible et il s'ensuit que $E \neq \{0\}$, on considère $e_1 \in E$ non nul. Si $Me_1 = \lambda e_1$ alors

$$0 = [(M-\alpha)^2 + \beta^2\mathrm{I}](e_1) = [(\lambda-\alpha)^2 + \beta^2]e_1$$

ce qui est impossible puisque $\beta > 0$ donc e_1 et Me_1 sont indépendants et il en est donc de même de e_1 et $e_2 = \frac{1}{\beta}[Me_1 - \alpha e_1]$. De plus, on a $Me_1 = \alpha e_1 + \beta e_2$ et

$$Me_2 = (M - \alpha\mathrm{I})e_2 + \alpha\mathrm{I}e_2 = \frac{1}{\beta}(M - \alpha\mathrm{I})^2 e_1 + \alpha e_2 = -\beta e_1 + \alpha e_2$$

donc $F = \mathrm{Vect}(e_1, e_2)$ est stable par M et on a $M_{|F} = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$. Puisque M est semi-simple, il existe un supplémentaire G de F stable par M et il suffit d'appliquer l'hypothèse de récurrence à la matrice $M_{|G}$. □

Leçons concernées

11 Idéaux d'un anneau commutatif unitaire. Exemples et applications

14 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

23 Réduction d'un endomorphisme en dimension finie. Applications

24 Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications

37 Endomorphismes diagonalisables

40 Polynômes d'endomorphismes. Applications

Sébastien Pellerin

Compléments

Une lemme utile. —

Lemme. — *Soit $f \in \mathcal{L}(E)$ et $\mu_f = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$. Si F est un sous-espace stable par f alors*

$$F = \bigoplus_{i=1}^{r} (F \cap \ker P_i^{\alpha_i}(f)).$$

Première démonstration. — Soit $x = x_1 + \cdots + x_r \in F$ où $x_i \in \ker P_i^{\alpha_i}(f)$ alors, pour tout $P \in \mathbb{K}[X]$, on a $P(f)(x) = P(f)(x_1) + \cdots + P(f)(x_r)$. Soit $i \in \{1, \ldots, r\}$, on écrit $\mu_f = P_i^{\alpha_i} Q_i$ avec $Q_i \in \mathbb{K}[X]$ alors $Q_i(f)(x) = Q_i(f)(x_1)$. Puisque $\ker P_i^{\alpha_i}(f)$ et $F \cap \ker P_i^{\alpha_i}(f)$ sont stables par f, ils sont stables par $Q_i(f)$ donc on peut considérer les restrictions g et h de $Q_i(f)$ à $\ker P_i^{\alpha_i}(f)$ et $F \cap \ker P_i^{\alpha_i}(f)$ respectivement. Notons que

$$\ker Q_i(f) \cap \ker P_i^{\alpha_i}(f) = \big(\bigoplus_{j \neq i} \ker P_j^{\alpha_j}(f) \big) \cap \ker P_i^{\alpha_i}(f) = \{0\}$$

i.e. g et h sont injectives d'où bijectives. Alors $y = g(x_i)$ est dans $\ker P_i^{\alpha_i}(f)$ or $y = Q_i(f)(x)$ donc y est aussi dans F ; il s'ensuit que y est dans $F \cap \ker P_i^{\alpha_i}(f)$ donc $x_i = h^{-1}(y)$ aussi *i.e.* $x_i \in F \cap \ker P_\lambda(f)$. □

Deuxième démonstration. — On pose $F_i = \ker P_i^{\alpha_i}(f)$, on a $E = F_1 \oplus \cdots \oplus F_r$ et on note p_i la projection sur F_i parallèlement à $\bigoplus_{j \neq i} F_j$, il s'agit d'un polynôme en f. Comme F est stable par f, F est aussi stable par chaque p_i *i.e.* $p_i(F) \subset F$ mais on a aussi $p_i(F) \subset p_i(E) \subset F_i$, d'où $p_i(F) \subset F \cap F_i$. Comme $p_1 + \cdots + p_r = \mathrm{id}_E$, il vient

$$F \subset p_1(F) + \cdots + p_r(F) = p_1(F) \oplus \cdots \oplus p_r(F) \subset (F \cap F_1) \oplus \cdots \oplus (F \cap F_r).$$

□

Démonstration dans le cas diagonalisable. — Si f est diagonalisable alors on a $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_r}$. Soit $x \in F$, on écrit $x = x_1 + \cdots + x_r$, où $x_i \in E_{\lambda_i}$, alors $P(f)(x) = P(\lambda_1)x_1 + \cdots + P(\lambda_r)x_r$ pour tout $P \in \mathbb{K}[X]$. Soit $1 \leq i \leq r$ et $P_i \in \mathbb{K}[X]$ tel que $P_i(\lambda_i) = 1$ et $P_i(\lambda_j) = 0$ pour $j \neq i$, alors $x_i = P_i(f)(x) \in F$. □

Le théorème de Maschke. —

Théorème. — *Soit E un $\mathbb{C}$-espace vectoriel de dimension finie $n \geq 1$, G un sous-groupe fini de $GL(E)$ et F un sous-espace de E stable par tous les éléments de G. Alors F admet un supplémentaire stable par tous les éléments de G.*

Démonstration. — On pose

$$\varphi(x, y) = \sum_{g \in G} \langle g(x), g(y) \rangle$$

ce qui définit un produit scalaire sur E invariant par G. Il suffit alors de prendre l'orthogonal $S = F^\perp$ de F pour le produit scalaire φ. □

Références

M. Alessandri, *Thèmes de géométrie. Groupes en situation géométrique*, Dunod, 1999.

S. Francinou, H. Gianella et S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2001.

X. Gourdon, *Algèbre*, Ellipses, 1994.