Invariants de similitude

Leçons : 150, 153, 154, 159

S Soit K corps quelconque et E, un $\mathbb{K}$-espace vectoriel de dimension n. Génériquement, u désignera un endomorphisme dans $\mathscr{L}(E)$ dont le polynôme minimal est noté Π_u et le polynôme caractéristique χ_u.

Définition 1

Soit $u \in \mathscr{L}(E)$ et soit $x \in E$. On appelle polynôme minimal de u en x l'unique générateur unitaire de l'idéal

$$\{P \in \mathbb{K}[X],\ P(u)(x) = 0\}.$$

On le note $\Pi_{u,x}$. On a $\Pi_{u,x} | \Pi_u$.

Proposition 2

Il existe $x \in E$ tel que $\Pi_u = \Pi_{u,x}$.

Démonstration. On écrit $\Pi_u = \prod_{i=1}^r P_i^{m_i}$ où P_i sont des irréductibles distincts. On note $K_i = \ker P_i^{m_i}(u)$ et $u_i = u|_{K_i}$. Par le lemme des noyaux, $E = \oplus_i K_i$.

Montrons le résultat sur chaque sous-espace K_i. Par l'absurde, si le résultat ne tenait pas, alors pour tout $x_i \in K_i$, Π_{u_i,x_i} diviserait strictement $\Pi_{u_i} = P_i^{m_i}$ donc diviserait $P_i^{m_i-1}$ par irréductibilité. Mais alors $P_i^{m_i-1}(u_i)$ serait nul sur tout K_i, ce qui est impossible par minimalité de Π_{u_i}. On dispose donc d'éléments x_i comme dans l'énoncé sur chaque sous-espace K_i. Montrons que $x = x_1 + \ldots + x_r$ convient. On a :

$$0 = \Pi_{u,x}(u)(x) = \sum_i \Pi_{u,x}(x_i)$$

donc $\Pi_{u,x}(u)(x_i) = 0$ puisque les K_i sont en somme directe. Ainsi, $P_i^{m_i} = \Pi_{u_i,x_i} | \Pi_{u,x}$ pour tout i. Puisque les $P_i^{m_i}$ sont premiers entre eux, leur produit qui est égal à Π_u divise aussi $\Pi_{u,x}$, ce qui conclut. □

Théorème 3

Soit $u \in \mathscr{L}(E)$. Il existe une unique famille $P_1, \ldots, P_r$ de polynômes unitaires et une famille $E_1, \ldots, E_r$ de sous-espaces de E vérifiant :

1. $P_r | \ldots | P_1$
2. $E = E_1 \oplus \ldots \oplus E_r$
3. *Pour tout $i \in \{1, \ldots, r\}$, E_i est stable par u et $u_{|E_i}$ est cyclique de polynôme P_i.*

Les polynômes $P_1, \ldots . P_r$ sont appelés les invariants de similitudes de u.

Démonstration. Existence. Montrons le résultat par récurrence sur $\dim E$. Il est trivial pour $\dim E = 1$, supposons donc $\dim E > 2$.

Soit $d = \deg(\Pi_u)$ et soit $x \in E$ tel que $\Pi_{u,x} = \Pi_u$. On note $F = \mathrm{Vect}(x, u(x), \ldots, u^{d-1}(x))$. Clairement, F est stable par u et $u|_F$ est cyclique. On va montrer par dualité que F admet un supplémentaire stable par u. Soit $\varphi \in E^*$ tel que :

$$\varphi(x) = \varphi(u(x)) = \ldots = \varphi\left(u^{d-2}(x)\right) = 0 \ \text{ et } \ \varphi\left(u^{d-1}(x)\right) = 1.$$

La famille $(\varphi, \varphi\circ u, \dots, \varphi\circ u^{d-1})$ est une famille libre de E^* et on note Φ le sous-espace vectoriel de E^* engendré par cette famille. On pose alors $G := \Phi^\circ = \{y \in E,\ \forall \psi \in \Phi,\ \psi(y) = 0\}$ et on montre que c'est un supplémentaire de F stable par u.

- *G est stable par u* : soit $y \in G$. Par construction, on a déjà $\forall k \in [\![0, d-2]\!], \varphi \circ u^k\big(u(y)\big) = 0$.. Comme le polynôme minimal de u est de degré d, on a $u^d(y) \in \mathrm{Vect}\big(y, u(y), \dots, u^{d-1}(y)\big)$ et donc $\varphi \circ u^{d-1}\big(u(y)) = \varphi\big(u^d(y)\big) = 0$ par ce qui précède.
- $F \cap G = \{0\}$. Soit $y \in F \cap G$, alors on peut écrire $y = a_0 x + \dots a_{d-1} u^{d-1}(x)$ et en appliquant $\varphi \circ u^i$ pour i allant de 0 à $d-1$, on trouve que tous les a_k sont nuls.
- $\dim F + \dim G = n$. C'est une propriété générale de l'orthogonal au sens de la dualité : $\dim \Phi + \dim \Phi^\circ = n$.

De plus, $\Pi_{u_{|G}} | \Pi_u$ puisque Π_u annule $u_{|G}$. En appliquant l'hypothèse de récurrence à $u_{|G}$, on obtient le résultat voulu.

Unicité. On suppose l'existence d'une autre famille de polynôme $Q_1, \dots, Q_s$ donnant lieu à une autre décomposition $F_1 \oplus \dots \oplus F_s$ comme dans l'énoncé. On a déjà $P_1 = Q_i = \Pi_u$. Soit $j > 1$ l'indice minimal tel que $P_j \neq Q_j$. Alors, on a d'une part :

$$P_j(u)(E) = P_j(u)(E_1) \oplus \dots \oplus P_j(u)(E_{j-1}),$$

et d'autre part :

$$P_j(u)(E) = P_j(u)(F_1) \oplus \dots \oplus P_j(u)(F_{j-1}) \oplus P_j(u)(F_j) \oplus \dots \oplus P_j(u)(F_s).$$

Mais pour $i < j$, on a $\dim P_j(u)(E_i) = \dim P_j(u)(F_i)$ donc $0 = \dim P_j(u)(F_j) = \dots = \dim P_j(u)(G_s)$, ce qui prouve que $Q_j | P_j$ et par symétrie $P_j | Q_j$. C'est absurde car $P_j \neq Q_j$. Finalement $r = s$ et $P_i = Q_i$ pour tout i. □

Corollaire 4 (*Décomposition de Frobenius*)

Soit $u \in \mathscr{L}(E)$. Il existe une base dans laquelle la matrice de u est de la forme

$$\begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix}$$

où C_{P_i} est la matrice compagnon associée au polynôme P_i avec $P_r | \dots | P_1$. De plus, on a

$$\chi_u = P_1 \dots P_r.$$

Corollaire 5

Deux endomorphismes u et v sont semblables si et seulement s'ils ont les mêmes invariants de similitude.

Démonstration (idée)**.** Supposons u et v semblables. On considère E_i les sous-espaces cycliques associés à u et φ tel que $\varphi \circ u = v \circ \varphi$. Alors si $F_i = \varphi(E_i)$, les F_i sont les sous-espaces cycliques associés à F. □

Corollaire 6

Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors A est semblable à sa transposée.

Démonstration. Il suffit de le montrer pour A matrice compagnon de la forme $C_P = M_{(e_1,\dots,e_n)}(u)$ où $P = X^n + \sum_{i=0}^{n-1} a_i X^i$. Le changement de base $e'_i = a_1 e_1 + \dots + a_{n-i} e_{n-i} + e_{n-i+1}$ conduit au résultat. □

Remarque.
- On retrouve en particulier la décomposition de Jordan des endomorphismes nilpotents puisque dans ce cas $\chi_u = X^n$: les invariants de similitudes sont donc de la forme X^{n_i} pour $n_i \leqslant n$.
- Les invariants de similitude ne dépendent pas du corps de base.
- La théorie des $\mathbb{K}[X]$-modules donne une façon simple pour calculer les invariants de similitude : Si U est la matrice de $u \in \mathscr{L}(E)$ dans une certaine base, alors les invariants de similitude de u sont les facteurs invariants non inversibles de la matrice $U - XI_n \in \mathscr{M}_n(\mathbb{K}[X])$.

  En effet, on montre par des opérations élémentaires sur les lignes et les colonnes qu'une matrice de la forme $C_P - XI$ est équivalente à

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & P \end{pmatrix}$$

  et on utilise la décomposition de Frobenius pour conclure.

Référence : Xavier Gourdon (2009). *Les maths en tête : algèbre*. 2e éd. Ellipses, pp. 289-291.

Merci à Antoine Diez pour ce développement.