

Invariants de similitude

Nous montrons l'existence et l'unicité des invariants de similitude d'un endomorphisme d'un espace de dimension finie en utilisant la dualité.

Soit E un espace vectoriel de dimension finie $n \geq 1$ sur un corps commutatif $\mathbb{K}$. Soit $f \in \mathcal{L}(E)$.

[GOU21]
p. 398

NOTATION 1

Soit $x \in E$. On note P_x le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ (un tel polynôme existe car $\mathbb{K}[X]$ est principal et cet idéal est non réduit à $\{0\}$) et $E_x = \{P(f)(x) \mid P \in \mathbb{K}[X]\}$.

LEMME 2

- (i) Si $k = \deg(\pi_f)$, alors $\mathbb{K}[f]$ est un sous-espace vectoriel de $\mathcal{L}(E)$ de dimension k , dont une base est $(f^i)_{i \in \llbracket 0, k-1 \rrbracket}$.
- (ii) Soit $x \in E$. Si $l = \deg(P_x)$, alors E_x est un sous-espace vectoriel de E de dimension l , dont une base est $(f^i(x))_{i \in \llbracket 0, l-1 \rrbracket}$.

Démonstration. (i) Montrons que la famille $(f^i)_{i \in \llbracket 0, k-1 \rrbracket}$ est à la fois libre et génératrice.

p. 61

- Soit $P(f) \in \mathbb{K}[f]$. On fait la division euclidienne de P par π_f dans $\mathbb{K}[X]$ pour écrire $P = \pi_f Q + R$ avec $Q, R \in \mathbb{K}[X]$ et $\deg(R) < k = \deg(\pi_f)$. En évaluant en f , cela donne $P(f) = R(f) \in \text{Vect}(\text{id}_E, \dots, f^{k-1})$. Donc la famille est génératrice.
- Si $\sum_{i=0}^{k-1} \lambda_i f^i = 0$, alors le polynôme $P = \sum_{i=0}^{k-1} \lambda_i X^i$ vérifie $P(f) = 0$. Donc $\pi_f \mid P$, et comme $\deg(P) < \deg(\pi_f)$, on a $P = 0$. Donc $\lambda_0 = \dots = \lambda_{k-1} = 0$. Donc la famille est libre.

(ii) La deuxième assertion se montre sensiblement de la même manière.

□

LEMME 3

Il existe $x \in E$ tel que $P_x = \pi_f$.

p. 290

La démonstration est un peu trop longue pour être incluse ici : c'est un résultat qui demande du temps pour le démontrer (et pourrait constituer un vrai développement à part entière). Nous vous renvoyons vers [GOU21] p. 178 pour la démonstration.

THÉORÈME 4

Théorème de Frobenius.

Il existe des sous-espaces vectoriels $F_1, \dots, F_r$ de E tous stables par f tels que :

- (i) $E = \bigoplus_{i=1}^r F_i$.
- (ii) $\forall i \in \llbracket 1, r \rrbracket$, la restriction $f_i = f|_{F_i}$ est un endomorphisme cyclique de F_i .
- (iii) Si $P_i = \pi_{f_i}$ est le polynôme minimal de f_i , on a $P_{i+1} \mid P_i \forall i \in \llbracket 1, r-1 \rrbracket$.

La suite $(P_i)_{i \in \llbracket 1, r \rrbracket}$ ne dépend que de f et non du choix de la décomposition (elle est donc unique). On l'appelle **suite des invariants de f** .

Démonstration. • Existence : Soit $k = \deg(\pi_f)$. Par le Lemme 3, il existe $x \in E$ tel que $P_x = \pi_f$. Par le Lemme 2, le sous-espace $F = E_x$ est de dimension k et est stable par f et comme $\deg(P_x) = k$, la famille de vecteurs

$$\left(\underbrace{x}_{=e_1}, \dots, \underbrace{f^{k-1}(x)}_{=e_k} \right)$$

forme une base de F . Complétons cette base en une base $(e_1, \dots, e_n)$ de E . En désignant par $(e_1^*, \dots, e_n^*)$ la base duale associée et en notant $\Gamma = \{e_k^* \circ f^i \mid i \in \mathbb{N}\}$, on pose

$$\begin{aligned} G &= \Gamma^\circ \\ &= \{x \in E \mid \forall i \in \mathbb{N}, (e_k^* \circ f^i)(x) = 0\} \end{aligned}$$

Ainsi, G est l'ensemble des $x \in E$ tels que la k -ième coordonnée de $f^i(x)$ (dans la base $(e_1, \dots, e_n)$) est nulle $\forall i \in \mathbb{N}$; G est donc un sous-espace de E stable par f . Montrons que $F \oplus G = E$.

Montrons que $F \cap G = \{0\}$. Soit $y \in F \cap G$. Si $y \neq 0$, on peut écrire $y = \lambda_1 e_1 + \dots + \lambda_p e_p$ avec $\lambda_p \neq 0$ et $p \leq k$. En composant par $e_k^* \circ f^{k-p}$, on obtient

$$\begin{aligned} 0 &= e_k^* \circ f^{k-p}(y) \\ &= e_k^*(\lambda_1 f^{k-p}(e_1) + \dots + \lambda_p f^{k-p}(e_p)) \\ &= e_k^*(\lambda_1 f^{k-p}(x) + \dots + \lambda_p f^{k-p}(x)) \\ &= \lambda_p \end{aligned}$$

Ce qui est absurde.

Montrons que $\dim(F) + \dim(G) = n$. Cela revient à montrer que $\dim(G) = n - k$. On sait que $G = \Gamma^\circ = (\text{Vect}(\Gamma))^\circ$ et $\dim(\text{Vect}(\Gamma)) + \dim(\text{Vect}(\Gamma)^\circ) = n$. Montrons donc que $\dim(\text{Vect}(\Gamma)) = k$. Posons

$$\begin{aligned} \varphi: \mathbb{K}[f] &\rightarrow \text{Vect}(\Gamma) \\ g &\mapsto e_k^* \circ g \end{aligned}$$

Par définition de Γ , φ est surjective. Soit $g \in \text{Ker}(\varphi)$. On a alors $e_k^* \circ g = 0$, et comme $g \in \mathbb{K}[f]$,

$$g = \lambda_1 \text{id} + \dots + \lambda_p f^{p-1} \text{ avec } \lambda_p \neq 0 \text{ et } p \leq k$$

On a donc $0 = e_k^* \circ g(f^{k-p}(x)) = \lambda_p \neq 0$. Ainsi, $g = 0$ et φ est un isomorphisme. Donc $\dim(\text{Vect}(\Gamma)) = \dim(\mathbb{K}[f]) = k$ par le Lemme 2, ce que l'on voulait.

Soit P_1 le polynôme minimal de $f|_F$ (qui est le polynôme minimal de f car $P_1 = \pi_{f|_F} = \pi_f = \pi_{f|_E}$). Soit P_2 le polynôme minimal de $f|_G$. Comme G est stable par f , on a $P_1(f|_G) = \pi_f(f|_G) = 0$, donc $P_2 \mid P_1$. Il suffit alors de réitérer en remplaçant f par $f|_G$ et E par G pour obtenir la décomposition voulu.

• Unicité : Soient $F_1, \dots, F_r$ et $G_1, \dots, G_s$ des sous-espaces vectoriels stables par f qui vérifient le Point (i), le Point (ii) et le Point (iii). On note pour tout i , $P_i = \pi_{f|_{F_i}}$ et $Q_i = \pi_{f|_{G_i}}$. On suppose par l'absurde $(P_1, \dots, P_r) \neq (Q_1, \dots, Q_s)$. Soit $j = \min\{i \mid P_i \neq Q_i\}$. Comme $E = \bigoplus_{i=1}^r F_i$ (où $\forall i \in \llbracket 1, r \rrbracket$, F_i est stable par f et $\forall k \geq j \geq 1$, $P_j(f)(F_k) = 0$) :

$$P_j(f)(F_1) \oplus \dots \oplus P_j(f)(F_{j-1}) = P_j(f)(E) \quad (*)$$

De même,

$$P_j(f)(G_1) \oplus \cdots \oplus P_j(f)(G_{j-1}) \oplus P_j(f)(G_j) \oplus \cdots \oplus P_j(f)(G_s) = P_j(f)(E) \quad (**)$$

Notons que l'on a $\forall i \in \llbracket 1, j-1 \rrbracket$, $\dim(P_j(f)(F_i)) = \dim(P_j(f)(G_i))$. En effet, on peut trouver une base $\mathcal{B}_i$ de F_i et une base $\mathcal{B}'_i$ de G_i telles que $\text{Mat}(f|_{F_i}, \mathcal{B}_i) = \text{Mat}(f|_{G_i}, \mathcal{B}'_i)$ par cyclicité de $f|_{F_i}$ et $f|_{G_i}$. En prenant les dimensions dans (*) et (**), on en déduit :

$$0 = \dim(P_j(f)(G_j)) = \cdots = \dim(P_j(f)(G_s)) \implies Q_j \mid P_j$$

Par symétrie, on a de même $P_j \mid Q_j$. D'où $P_j = Q_j$: absurde.

□

Bibliographie

Les maths en tête

[GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3^e éd. Ellipses, 13 juill. 2021.

<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.