

Endomorphismes cycliques, invariants de similitude et réduction de Frobenius

2012-2013

Référence : Xavier Gourdon, *Algèbre (2^e édition)*, Ellipses, 2009, p.290.

Théorème 1.

Soit E un \mathbb{K} -espace vectoriel de dimension finie n .

Soit $f \in \mathcal{L}(E)$.

Alors il existe une suite F_1, \dots, F_r de sous-espaces vectoriels de E stables par f telle que :

(i) $E = F_1 \oplus \dots \oplus F_r$

(ii) $\forall i \in \{1, \dots, r\}, f_i := f|_{F_i}$ est un endomorphisme cyclique

(iii) si P_i désigne le polynôme minimal de f_i , on a :

$$\forall i \in \{1, \dots, r-1\}, P_{i+1} \mid P_i$$

La suite de polynômes P_1, \dots, P_r ne dépend que de f . On l'appelle suite des invariants de similitude de f .

Théorème 2 (Réduction de Frobenius).

Soit $f \in \mathcal{L}(E)$.

Soit P_1, \dots, P_r la suite des invariants de similitude de f .

Alors il existe une base \mathcal{B} de E telle que :

$$\text{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}$$

où $C(P_i)$ désigne la matrice compagnon de P_i .

On a $P_1 = \pi_f$ et $P_1 \dots P_r = \chi_f$.

Lemme.

Soit $f \in \mathcal{L}(E)$ un endomorphisme cyclique.

Alors il existe une base de E dans laquelle la matrice de f est égale à $C(\pi_f)$.

Démonstration. Il existe $x \in E$ tel que $(x, f(x), \dots, f^{n-1}(x))$ soit une base de E .

Si $\pi_f = X^n + a_{n-1}X^{n-1} + \dots + a_0$, alors $f^n(x) = -a_{n-1}f^{n-1}(x) - \dots - a_0x$ car π_f annule f . \square

Démonstration du théorème 1.

– Existence : soit $k = \deg(\pi_f)$, soit $x \in E$.

On note P_x le polynôme unitaire engendrant l'idéal :

$$\{P \in \mathbb{K}[X] / P(f)(x) = 0\}$$

et

$$E_x := \{P(f)(x) / P \in \mathbb{K}[X]\}$$

Soit $x \in E$ tel que $P_x = \pi_f$ (une preuve de l'existence d'un tel x est donnée en fin de document).

Le sous-espace vectoriel $F := E_x$ est de dimension k et est stable par f .

On pose :

$$e_1 = x, e_2 = f(x), \dots, e_k = f^{k-1}(x)$$

Alors (e_1, \dots, e_k) forme une base de F car $\deg(P_x) = k$ (plus de détails sont donnés en fin de document).

On la complète en une base (e_1, \dots, e_n) de E et on note (e_1^*, \dots, e_n^*) la base duale associée.

On note $G = \Gamma^\circ$ où $\Gamma = \{e_k^* \circ f^i, i \in \mathbb{N}\}$ (orthogonal vis-à-vis du dual).

i.e. G est l'ensemble des x tels que la k -ième coordonnée de $f^i(x)$ dans (e_1, \dots, e_n) soit nulle pour tout i .

G est un sev de E stable par f .

Montrons $F \oplus G = E$:

– $F \cap G = \{0\}$:

soit $y \in F \cap G$, si $y \neq 0$ on peut écrire $y = a_1e_1 + \dots + a_pe_p$ avec $a_p \neq 0$ et $p \leq k$.

En composant par $e_k^* \circ f^{k-p}$, on a :

$$0 = e_k^*(a_1e_{k-p+1} + \dots + a_pe_k) = a_p$$

donc $F \cap G = \{0\}$.

– $\dim F + \dim G = n$:

$G = (\text{Vect } \Gamma)^\circ$ donc prouvons $\dim(\text{Vect } \Gamma) = k$.

On considère :

$$\begin{aligned} \varphi : \mathcal{L}_f &:= \{P(f) / P \in \mathbb{K}[X]\} \rightarrow \text{Vect } \Gamma \\ &g \mapsto e_k^* \circ g \end{aligned}$$

φ est surjective par définition.

Si $e_k^* \circ g = 0$ avec $g \neq 0$, on peut écrire :

$$g = a_1 \text{Id}_E + \dots + a_p f^{p-1}$$

avec $p \leq k$ et $a_p \neq 0$ car $(\text{Id}_E, \dots, f_{p-1})$ est une base de \mathcal{L}_f (détails supplémentaires en fin de document).

$$\begin{aligned} 0 &= e_k^* \circ g(f^{k-p}(x)) \\ &= e_k^*(a_1 f^{k-p}(x) + \dots + a_p f^{k-1}(x)) = a_p \end{aligned}$$

Donc $g = 0$ et φ est injective.

Donc $\dim(\text{Vect } \Gamma) = \dim \mathcal{L}_f = k$.

On note P_1 le polynôme minimal de $f|_F$ ($\pi_f = P_x = P_1$) et P_2 le polynôme minimal de $f|_G$.

G est stable par f donc $P_2 \mid P_1$.

Puis on recommence sur $f|_G$.

– Unicité : soient F_1, \dots, F_r et G_1, \dots, G_s vérifiant les hypothèses du théorème.

On note $P_i = \pi_{f|_{F_i}}$ et $Q_j = \pi_{f|_{G_j}}$.

On a $P_1 = \pi_f = Q_1$.

Supposons $(P_1, \dots, P_r) \neq (Q_1, \dots, Q_s)$.

On note $j = \inf\{i, P_i \neq Q_i\}$, j existe car $\sum_i \deg(P_i) = n = \sum_j \deg(Q_j)$.

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

car $E = F_1 \oplus \dots \oplus F_r$ et $P_j(f)(F_k) = 0$ pour $k \geq j$ et les F_i sont stables par f .

Or

$$P_j(f)(E) = P_j(f)(G_1) \oplus \dots \oplus P_j(f)(G_s)$$

et

$$\dim P_j(f)(F_i) = \dim P_j(f)(G_i) \text{ pour } 1 \leq i \leq j-1$$

car d'après le lemme, il existe \mathcal{B}_i et \mathcal{B}'_i telles que $\text{Mat}_{\mathcal{B}_i}(f|_{F_i}) = \text{Mat}_{\mathcal{B}'_i}(f|_{G_i})$.

D'où :

$$0 = \dim P_j(f)(G_j) = \dots = \dim P_j(f)(G_s)$$

D'où $Q_j \mid P_j$, donc $Q_j = P_j$ par symétrie. □

Démonstration du théorème 2. Soit \mathcal{B}_i base de F_i telle que $\text{Mat}_{\mathcal{B}_i}(f|_{F_i}) = C(P_i)$. La matrice de f dans la base $(\mathcal{B}_1, \dots, \mathcal{B}_r)$ est bien de la forme voulue. □

Détails supplémentaires

Proposition.

Si $k = \deg(\pi_f)$, \mathcal{L}_f est un sev de $\mathcal{L}(E)$ de dimension k , dont une base est $(Id_E, f, \dots, f^{k-1})$.

Si $l = \deg(P_x)$, E_x est un sev de E de dimension l , dont une base est $(x, \dots, f^{l-1}(x))$.

Démonstration.

$$\varphi : \mathbb{K}[X] \rightarrow \mathcal{L}(E)$$

$$P \mapsto P(f)$$

est linéaire, $\text{Im } \varphi = \mathcal{L}_f$.

$$\ker \varphi = \{P \in \mathbb{K}[X] \mid P(f) = 0\} = (\pi_f)$$

Donc

$$\mathcal{L}_f \cong \mathbb{K}[X]/(\pi_f)$$

dont une base est $(1, X, \dots, X^{k-1})$

Idem avec

$$\varphi : \mathbb{K}[X] \rightarrow E$$

$$P \mapsto P(f)(x)$$

□

Proposition.

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

Démonstration. Soit $\pi_f = Q_1^{\alpha_1} \dots Q_l^{\alpha_l}$ avec Q_i irréductible unitaire, $\alpha_i > 0$.

– soit $i \in \{1, \dots, l\}$, soit R tel que $\pi_f = Q_i^{\alpha_i} R$.

$$0 = \pi_f(f) = Q_i^{\alpha_i}(f) \circ R(f)$$

Donc

$$\text{Im } R(f) \subseteq \ker Q_i^{\alpha_i}(f)$$

Si

$$\text{Im } R(f) \subseteq \ker Q_i^{\alpha_i-1}(f)$$

alors

$$Q_i^{\alpha_i-1}(f) \circ R(f) = 0$$

donc $\pi_f \mid Q_i^{\alpha_i-1} R$, or $\deg Q_i^{\alpha_i-1} R < \deg \pi_f$, donc il existe $a_i \in \text{Im } R(f)$ tel que $Q_i^{\alpha_i-1}(f)(a_i) \neq 0$.

Mais $Q_i^{\alpha_i}(f)(a_i) = 0$ donc $P_{a_i} \mid Q_i^{\alpha_i}$, donc $P_{a_i} = Q_i^{\alpha_i}$ car $P_{a_i} \nmid Q_i^{\alpha_i-1}$ et Q_i est irréductible.

En résumé, pour $1 \leq i \leq l$, il existe $a_i \in E$ tel que $P_{a_i} = Q_i^{\alpha_i}$.

– Montrons que :

$$P_x \wedge P_y = 1 \implies P_{x+y} = P_x P_y$$

On a

$$P_x P_y(f)(x+y) = P_x P_y(f)(x) + P_x P_y(f)(y) = 0$$

Donc $P_{x+y} \mid P_x P_y$.

D'autre part,

$$P_{x+y}(f)(y) = -P_{x+y}(f)(x)$$

Donc

$$P_x P_{x+y}(f)(y) = -P_x P_{x+y}(f)(x) = 0$$

Donc $P_y \mid P_x P_{x+y}$ et $P_x \wedge P_y = 1$ donc $P_y \mid P_{x+y}$.

De même, $P_x \mid P_{x+y}$ donc $P_x P_y \mid P_{x+y}$ car $P_x \wedge P_y = 1$.

D'où $P_x P_y = P_{x+y}$.

– Alors pour $1 \leq i \leq l$, il existe a_i tel que $P_{a_i} = Q_i^{\alpha_i}$ et $Q_i^{\alpha_i} \wedge Q_j^{\alpha_j} = 1$ pour $i \neq j$, donc :

$$P_{\sum_{i=1}^l a_i} = \prod_{i=1}^l P_{a_i} = \pi_f$$

□