Endomorphismes cycliques, invariants de similitude et réduction de Frobenius

2013 – 2014

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

Théorème 1.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.
Soit $u \in \mathcal{L}(E)$.
Alors il existe une suite $F_1, \dots, F_r$ de sous-espaces vectoriels de E non réduits à $\{0\}$ et stables par u telle que :

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

(ii) $\forall i \in \{1, \dots, r\}, u_i := u_{|F_i}$ *est un endomorphisme cyclique*

(iii) si P_i désigne le polynôme minimal de u_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 u. On l'appelle suite des invariants de similitude de u.

Théorème 2 (Réduction de Frobenius)**.**
Soit $u \in \mathcal{L}(E)$.
Soit $P_1, \dots, P_r$ la suite des invariants de similitude de u.
Alors il existe une base $\mathcal{B}$ de E telle que :

$$Mat_{\mathcal{B}}(u) = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}$$

où $C(P_i)$ désigne la matrice compagnon de P_i.
On a $P_1 = \pi_u$ et $P_1 \dots P_r = \chi_u$.

Lemme.
Soit $u \in \mathcal{L}(E)$ un endomorphisme cyclique.
Alors il existe une base de E dans laquelle la matrice de u est égale à $C(\pi_u)$.

Démonstration. Il existe $x \in E$ tel que $(x, u(x), \ldots, u^{n-1}(x))$ soit une base de E.
Si $\pi_u = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, alors $u^n(x) = -a_{n-1}u^{n-1}(x) - \ldots - a_0 x$ car π_u annule u. □

Démonstration du théorème 1.

– Existence : soit $k = \deg(\pi_u)$, soit $x \in E$.
On note P_x le polynôme unitaire engeandrant l'idéal :

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

et

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

Soit $x \in E$ tel que $P_x = \pi_u$ (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 u.
On pose :

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

Alors $(e_1, \ldots, e_k)$ forme une base de F car $\deg(P_x) = k$ (plus de détails sont donnés en fin de document).
En complétant $(e_1, \ldots, e_k)$ en une base $(e_1, \ldots, e_n)$ et en considérant la base duale $(e_1^*, \ldots, e_n^*)$, on montre qu'il existe $\varphi \in E^*$ telle que $\varphi(e_k) = 1$ et $\varphi(e_i) = 0$ pour $i < k$ ($\varphi = e_k^*$).

On note $G = \Gamma^\circ$ où $\Gamma = \{ {}^t u^i(\varphi), i \in \mathbb{N}\}$ (orthogonal vis-à-vis du dual).
G est un sev de E stable par u car Γ est stable par ${}^t u$.
Montrons $F \oplus G = E$:
– $F \cap G = \{0\}$:
On remarque que l'on a, pour $i + j \leq k$,

$$\begin{aligned} \langle {}^t u^i(\varphi), e_j \rangle &= \langle \varphi, u^i(e_j) \rangle \\ &= \langle \varphi, e_{i+j} \rangle \\ &= \delta_{i+j,k}. \end{aligned} \tag{1}$$

Donc si $y \in F \cap G$, $\langle {}^t u^i(\varphi), y \rangle = e_{k-i}^*(y) = 0$ pour $0 \leq i \leq k-1$, donc $y = 0$.

– $\dim F + \dim G = n$:
D'après (1), la famille $(\varphi, {}^t u(\varphi), \ldots, {}^t u^{k-1}(\varphi))$ est libre et $(\mathrm{id}, u, \ldots, u^k)$ est liée donc $(\varphi, {}^t u(\varphi), \ldots, {}^t u^k(\varphi))$ aussi, donc $\dim(\text{Vect } \Gamma) = k$.
On en déduit $\dim G = n - k$ car $G = (\text{Vect } \Gamma)^\circ$.

On note P_1 le polynôme minimal de $u_{|F}$ ($\pi_u = P_x = P_1$) et P_2 le polynôme minimal de $u_{|G}$.
G est stable par u donc $P_2 \mid P_1$.
Puis on recommence sur $u_{|G}$.

– Unicité : soient $F_1, \dots, F_r$ et $G_1, \dots, G_s$ vérifiant les hypothèses du théorème. On note $P_i = \pi_{u_{|F_i}}$ et $Q_j = \pi_{u_{|G_j}}$.

Supposons $(P_1, \dots, P_r) \neq (Q_1, \dots, Q_s)$.
On note $p = \inf\{i, P_i \neq Q_i\}$, p existe car $\sum_i \deg(P_i) = n = \sum_j \deg(Q_j)$ et $\deg(P_i), \deg(Q_j) \neq 0$.

$$P_p(u)(E) = P_p(u)(F_1) \oplus \dots \oplus P_p(u)(F_{p-1})$$

car $E = F_1 \oplus \dots \oplus F_r$ et $P_p(u)(F_k) = 0$ pour $k \geq p$ et les F_i sont stables par u.
Or

$$P_p(u)(E) = P_p(u)(G_1) \oplus \dots \oplus P_p(u)(G_s)$$

et

$$\dim P_p(u)(F_i) = \dim P_p(u)(G_i) \text{ pour } 1 \leq i \leq p-1$$

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

$$0 = \dim P_p(u)(G_p) = \dots = \dim P_p(u)(G_s)$$

D'où $Q_p \mid P_p$, donc $Q_p = P_p$ par symétrie.

□

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

Détails supplémentaires

Proposition.
Si $k = \deg(\pi_u)$, $\mathcal{L}_u$ est un sev de $\mathcal{L}(E)$ de dimension k, dont une base est $(Id_E, u, \dots, u^{k-1})$.
Si $l = \deg(P_x)$, E_x est un sev de E de dimension l, dont une base est $(x, \dots, u^{l-1}(x))$.

Démonstration.

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow \mathcal{L}(E) \\ P &\longmapsto P(u) \end{aligned}$$

est linéaire, $\mathrm{Im}\,\varphi = \mathcal{L}_u$.

$$\ker \varphi = \{P \in \mathbb{K}[X] \ / \ P(u) = 0\} = (\pi_u)$$

Donc

$$\mathcal{L}_u \cong \mathbb{K}[X]/(\pi_u)$$

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

Idem avec

$$\begin{aligned}\varphi : \mathbb{K}[X] &\longrightarrow E \\ P &\longmapsto P(u)(x)\end{aligned}$$

□

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

Démonstration. Soit $\pi_u = Q_1^{\alpha_1} \dots Q_l^{\alpha_l}$ avec Q_i irréductible unitaire, $\alpha_i > 0$.
– soit $i \in \{1, \dots, l\}$, soit R tel que $\pi_u = Q_i^{\alpha_i} R$.

$$0 = \pi_u(u) = Q_i^{\alpha_i}(u) \circ R(u)$$

Donc

$$\operatorname{Im} R(u) \subseteq \ker Q_i^{\alpha_i}(u)$$

Si

$$\operatorname{Im} R(u) \subseteq \ker Q_i^{\alpha_i - 1}(u)$$

alors

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

donc $\pi_u \mid Q_i^{\alpha_i - 1} R$, or $\deg Q_i^{\alpha_i - 1} R < \deg \pi_u$, donc il existe $a_i \in \operatorname{Im} R(u)$ tel que $Q_i^{\alpha_i - 1}(u)(a_i) \neq 0$.
Mais $Q_i^{\alpha_i}(u)(a_i) = 0$ 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 :

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

On a

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

Donc $P_{x+y} \mid P_x P_y$.
D'autre part,

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

Donc

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

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 :

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

□