2.7 Invariants de similitude (réduction de Frobenius)

Références : X. Gourdon, *Les maths en tête, Algèbre*, Ellipses, 2009
P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométrie, Tome premier*, Calvage & Mounet, 2013.

Leçons concernées : 150, 151, 153, 154, 157, 159.

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

Définition 1. Pour $f \in \mathcal{L}(E)$, on définit $\pi_{f,x}$ l'unique polynôme unitaire qui engendre l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ et $E_x = \{P(f)(x) \mid P \in \mathbb{K}[X]\}$ qui est alors de dimension $\deg \pi_{f,x} = k$ et dont une base est $(x, f(x), \ldots, f^{k-1}(x))$.

Proposition 2. *Il existe $x \in E$ tel que $\pi_{f,x} = \pi_f$.*

Démonstration. On note $\pi_f = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ la décomposition de π_f en produit de facteurs irréductibles, $N_i = \ker P_i^{\alpha_i}(f)$ et $f_i = f_{|N_i}$. On remarque que $\pi_{f_i} = P_i^{\alpha_i}$. Par le lemme des noyaux, on a $E = N_1 \oplus \cdots \oplus N_r$. On montre d'abord la proposition sur les sous-espaces N_i : supposons par l'absurde que pour tout $x_i \in N_i$, π_{f_i,x_i} est différent de π_{f_i}. Soit $x_i \in N_i$, on a $\pi_{f_i,x_i} \mid \pi_{f_i} = P_i^{\alpha_i}$ et donc, puisque P_i est irréductible, $\pi_{f_i,x_i} \mid P_i^{\alpha_i - 1}$ et alors $P_i^{\alpha_i-1}(f_i)(x_i) = 0$. Ainsi $P_i^{\alpha_i-1}(f_i) = 0$ ce qui est absurde.

On montre alors que $x := x_1 + \cdots + x_r$ convient. On sait que $\pi_{f,x} \mid \pi_f$ et on montre donc que $\pi_f \mid \pi_{f,x}$. On a $\pi_{f,x}(f)(x) = 0 = \pi_{f,x}(f)(x_1) + \cdots + \pi_{f,x}(f)(x_r)$ et donc pour tout i, $\pi_{f,x}(f)(x_i) = 0$. Or $\pi_{f,x}(f)(x_i) = \pi_{f,x}(f_i)(x_i)$ puisque $x_i \in N_i$, et donc $\pi_{f_i,x_i} = \pi_{f_i} = P_i^{\alpha_i} \mid \pi_{f,x}$ et ainsi $\pi_f = P_1^{\alpha_1} \cdots P_r^{\alpha_r} \mid \pi_{f,x}$ ce qui conclut la preuve. □

Définition 3. On dit que $f \in \mathcal{L}(E)$ est cyclique si il existe $x \in E$ tel que $E_x = E$, c'est-à-dire, d'après la proposition précédente, si $\deg \pi_f = \dim E = n$, ou encore si $\pi_f = \chi_f$.

Remarque. Si f est cyclique, alors dans une certaine base, la matrice de f est la matrice compagnon associée à π_f. Il suffit de considérer pour cela $x \in E$ tel que $E_x = E$ et la base $(x, f(x), \ldots, f^{n-1}(x))$.

Théorème 4. *Soit $f \in \mathcal{L}(E)$. Il existe une suite $(P_1, \ldots, P_r)$ de polynômes unitaires et une suite $(F_1, \ldots, F_r)$ de sous-espaces de E stables par f tels que*

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

(ii) Pour tout $1 \leqslant i \leqslant r$, $f_i = f_{|F_i}$ soit cyclique de polynôme minimal P_i

(iii) $P_r \mid \cdots \mid P_1$.

La suite $(P_i)_i$ est unique, ses éléments sont appelés invariants de similitude *de f.*

Démonstration. Existence : on procède par récurrence sur $\dim E = n$. Pour $n = 1$, le théorème est trivial. On suppose alors le résultat vrai pour les espaces vectoriels G de dimension $\dim G \leqslant n-1$. On note $d = \deg \pi_f$. Soit $x \in E$ tel que $\pi_{f,x} = \pi_f$, que l'on note $P_1 = \pi_f$. On note également $F_1 = E_x = \mathrm{Vect}(x, f(x), \dots, f^{d-1}(x))$ qui est stable par f. Alors $f_{|F_1}$ est cyclique et son polynôme minimal est de degré d (par la définition 3) et divise $\pi_f = P_1$ car celui-ci est un polynôme annulateur, il est ainsi égal à P_1.

Étape 1 : on cherche un supplémentaire f-stable à F_1. La famille

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

forme une base de F_1 que l'on complète en une base $(e_i)_i$ de E. On considère alors la base duale $(e_i^*)_i$ de E^* et on note $\varphi := e_d^*$ qui vérifie alors

$$\varphi(e_1) = \cdots = \varphi(e_{d-1}) = 0 \quad \text{et} \quad \varphi(e_d) = 1.$$

On vérifie facilement que la famille $(\varphi, \varphi \circ f, \dots, \varphi \circ f^{d-1})$ est une famille libre de E^*. On considère alors $\Phi = \mathrm{Vect}(\varphi, \varphi \circ f, \dots, \varphi \circ f^{d-1})$ qui est donc de dimension d et on pose $G = \Phi^0 = \{x \in E \mid \varphi(x) = 0\ \forall \varphi \in \Phi\}$ qui est alors de dimension $n-d$. Montrons que G convient.

Étape 2 : soit $y \in G$, vérifions que $f(y) \in G$. On a, par définition de G, pour $1 \leqslant k \leqslant d-2$, $\varphi \circ f^k(f(y)) = 0$ et d'autre part $\varphi \circ f^{d-1}(f(y)) = 0$ puisque, π_f étant de degré d, $f^d(y)$ s'exprime comme une combinaison linéaire de $(y, f(y), \dots, f^{d-1}(y))$. Ainsi, G est stable par f.

Soit $y = \lambda_1 x + \cdots + \lambda_d f^{d-1}(x) \in F_1 \cap G$. On applique alors $\varphi \circ f^i$ à y pour i allant de 0 à $d-1$ pour obtenir $\lambda_1 = \cdots = \lambda_d = 0$ et donc $F_1 \cap G = \{0\}$.

Étape 3 : par dimension, on a ainsi montré que G est un supplémentaire f-stable à F_1. On applique alors l'hypothèse de récurrence à G et $f_{|G}$, et on trouve une suite $(P_2, \dots, P_r)$ de polynômes unitaires et une suite $(F_2, \dots, F_r)$ de sous-espaces de G (donc de E) stables par $f_{|G}$ (donc par f) tels que

(i) $G = F_2 \oplus \cdots \oplus F_r$, et ainsi $E = F_1 \oplus \cdots \oplus F_r$

(ii) Pour tout $2 \leqslant i \leqslant r$, $f_i = (f_{|G})_{|F_i} = f_{|F_i}$ soit cyclique de polynôme minimal P_i, et le résultat est vrai pour $i = 1$ d'après le début de la preuve

(iii) $P_r \mid \cdots \mid P_2$.

On conclut en remarquant que puisque $P_1 = \pi_f$ est un polynôme annulateur de $f_{|G}$, $\pi_{f_{|G}} = P_2 \mid P_1$.

Unicité : soit $(Q_1, \dots, Q_s)$ et $(G_1, \dots, G_s)$ deux autres suites satisfaisant le théorème. On remarque que $P_1 = \pi_f = Q_1$. Supposons par l'absurde que la liste $(Q_1, \dots, Q_s)$ soit différente de la liste $(P_1, \dots, P_r)$. Soit alors j le premier indice i tel que $P_i \neq Q_i$, qui existe même si $s \neq r$ puisque $\sum_{i=1}^r \deg P_i = n = \sum_{i=1}^s \deg Q_i$. On a, par (i), le fait que les F_i soient stables par f, et puisque pour $i \geqslant j$, $\pi_{f_{|F_i}} = P_i \mid P_j$ par (ii) et (iii),

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

D'autre part, en utilisant $E = G_1 \oplus \cdots \oplus G_s$ qui est une décomposition en sous-espaces stables par f, on a

$$P_j(f)(E) = P_j(f)(G_1) \oplus \cdots \oplus P_j(f)(G_s). \tag{2}$$

Or, pour $1 \leqslant i \leqslant j-1$, d'après la remarque qui précède le théorème, il existe une base de F_i dans laquelle la matrice de $f_{|F_i}$ soit $\mathcal{C}(\pi_{f_{|F_i}}) = \mathcal{C}(P_i)$ et une base de G_i dans laquelle la matrice de $f_{|G_i}$ soit $\mathcal{C}(\pi_{f_{|G_i}}) = \mathcal{C}(Q_i) = \mathcal{C}(P_i)$ par hypothèse sur j et donc $\dim P_j(f)(F_i) = \dim P_j(f)(G_i)$. Ainsi, si on prend la dimension dans (1) et (2), on obtient

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

et donc

$$P_j(f)(G_j) = \cdots = P_j(f)(G_s) = \{0\}$$

ainsi, $Q_j \mid P_j$. Par symétrie on obtient $P_j \mid Q_j$ et donc $Q_j = P_j$ ce qui est absurde. $\square$

Corollaire 5 (Réduction de Frobenius)**.** *Soit $f \in \mathcal{L}(E)$ et $(P_1, \ldots, P_r)$ la suite des invariants de similitude de f. Il existe une base dans laquelle la matrice de f est la matrice par blocs*

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

où $\mathcal{C}(P_i)$ désigne la matrice compagnon associée au polynôme P_i. Deux endomorphismes f et g sont semblables si et seulement si ils ont les mêmes invariants de similitude. Enfin, le polynôme minimal de f est P_1 et son polynôme caractéristique $P_1 \cdots P_r$.

Démonstration. Pour obtenir la matrice par blocs annoncée, il suffit de considérer une base adaptée à la décomposition $E = F_1 \oplus \cdots \oplus F_r$ et de voir que pour tout i il existe une base de F_i telle que la matrice de f_i dans cette base soit $\mathcal{C}(P_i)$.

Si f et g sont semblables d'invariants de similitudes respectifs $(P_i)_i$, $(Q_j)_j$, alors puisque la relation de similitude est transitive, les $(Q_j)_j$ sont aussi des invariants de similitude de f et on conclut par unicité. La réciproque s'obtient en remarquant que si f et g ont les mêmes invariants de similitude, alors ils sont semblables à la même matrice compagnon par blocs et sont donc semblables. $\square$

Commentaire : on montre seulement le théorème 4 et éventuellement le corollaire 5, mais la preuve de la proposition 2 est à connaitre puisqu'elle est souvent demandée.