5 Décomposition de Frobenius

Leçons 150, 153, 154(, 122, 151, 159)

Ref : [Gourdon Analyse] B.2 Th1

Le théorème suivant donne une manière de réduire les endomorphisme dans n'importe quel cadre, sans avoir besoin de se placer sur un corps où les polynômes ont des racines. On peut notamment en déduire le théorème de réduction de Jordan si l'on ajoute l'hypothèse de clôture algébrique sur le corps.

On se donne donc un corps $\mathbb{K}$ et un espace vectoriel E de dimension n.

Théorème 1 (Réduction de Frobenius) Soit $u \in L(E)$. Il existe un unique entier $r \geq 1$, et des sous-espaces $F_1, \cdots, F_r$ de E stables par u, tels que

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

(ii) pour $i \in [\![1, r]\!]$, la restriction $u_i := u_{|F_i}$ est un endomorphisme cyclique sur F_i,

(iii) en notant μ_i le polynôme minimal de u_i, $\mu_{i+1}|\mu_i$, et les polynômes $\mu_1, \cdots, \mu_r$ ne dépendent que de u, et pas des sous-espaces F_i.

On dit que les μ_i sont les *invariants de similitude* de u.

Démonstration.

Étape 1. Supplémentaire du plus grand espace sur lequel u est cyclique.

On note $k > 0$ le degré du polynôme minimal μ de u, et on se donne $x \in E$ tel que $\mu_{u,x} = \mu$. Alors le sous-espace $F := E_{u,x} = \{P(u)(x),\ P \in \mathbb{K}[X]\}$ est de dimension k, et est bien sûr stable par u. De plus, la famille $(e_1, \cdots, e_k) = (x, u(x), \cdots, u^{k-1}(x))$ forme une base de F. On complète cette famille en une base $(e_1, \cdots, e_n)$ de E, et on note $(e_1^*, \cdots, e_n^*)$ sa base duale. On définit la partie $\Gamma := \left\{{}^t u^i(e_k^*),\ i \in \mathbb{N}\right\}$, et on fixe le sous-espace $G = \Gamma^0$ de E. C'est l'ensemble des vecteurs tels que la k-ième coordonnée de $u^i(x)$ (dans la base $(e_j)_{1 \leq j \leq n}$) est nulle pour tout i. En particulier, c'est un sous-espace stable par u.

Montrons que G est un supplémentaire de F dans E. Soit $y = \sum_{i=1}^{p} a_i e_i$ un vecteur de $F \cap G$, en ayant choisi p de manière à ce que ce soit le plus grand parmis les indices des coefficients non nuls de y dans la base $(e_j)_{1 \leq j \leq n}$. Comme $y \in F$, $p \leq k$. On a de plus

$$0 = {}^t u^{k-p}(e_k^*)(y) = e_k^*(a_1 e_{k-p+1} + \cdots + a_p e_k) = a_p,$$

où la première égalité est due au fait que $y \in G$. Ceci est bien sûr absurde si $y \neq 0$. Donc F et G sont en somme directe. De plus, on a

$$\dim(G) = \dim(E) - \dim(\mathrm{Vect}(\Gamma)).$$

On doit donc montrer que $\mathrm{Vect}\,\Gamma$ est de dimension k. On considère pour cela l'application

$$\varphi : \left| \begin{array}{ccc} \mathbb{K}[u] & \longrightarrow & \mathrm{Vect}(\Gamma) \\ v & \longmapsto & {}^t v(e_k^*) \end{array} \right.$$

Par défition de $\mathrm{Vect}(\Gamma)$, φ est surjective. Soit $v = \sum_{i=1}^{p} a_i u^i \in \mathbb{K}[u]$, avec $p \leq k$ et maximal parmi les indices dont le coefficient a_i est non nul, tel que $\varphi(g) = 0$. Alors

$$0 = \varphi(v)(u^{k-p}(x)) = e_k^*(a_1 e_{k-p+1} + \cdots + a_p e_k) = a_p,$$

ce qui est une nouvelle fois absurde si $v \neq 0$. Donc φ est injective. Donc $\mathrm{Vect}(\Gamma)$ est de même dimension que $\mathbb{K}[u]$, c'est-à-dire k. Finalement, F et G sont tous les deux stables par u et sont supplémentaires l'un de l'autre.

Étape 2. Existence des invariants de similitude par récurrence finie.

On note μ_1 le polynôme minimal de $u_{|F}$, et P_1 le polynôme minimal de $u_{|G}$. Tout d'abord, $\mu_1 = \mu_{u,x}$ par construction, et donc en fait c'est le polynôme minimal de u. De plus, comme G est u-stable, $u_{|G} \in L(G)$ et les polynômes en $u_{|G}$ sont bien définis ; on observe alors que $\mu_1(u_{|G}) = 0$, et donc $P_1|\mu_1$. On itère alors l'algorithme, en appliquant le raisonnement précédent à $u_{|G}$ sur G. Comme G est de dimension strictement inférieure à celle de E, l'algorithme se termine en au plus n étapes. À ce moment-là, le polynôme minimal est égal au polynôme caractéristique, et $u_{|F_r}$ est cyclique. Ainsi, E est somme directe de tous les F_i. Par construction, u est cyclique sur chaque F_i. De plus, le polynôme P_i construit à l'étape i est le polynôme minimal de $u_{|F_{i+1}}$ par construction, donc on a en fait $P_i = \mu_{i+1}$, ce qui donne (iii).

Étape 3. Unicité des invariants de similitude.

On suppose l'existence de deux familles de sous-espaces $(F_1, \cdots, F_r)$ et $(G_1, \cdots, G_s)$ vérifiant les points de l'énoncé. On note cette fois μ'_j les polynômes correspondants à la famille (G_j). Les axiomes impliquent que le premier polynôme des deux familles est le polynôme minimal de u : en effet, si P est un polynôme annulateur de u, en particulier P annule u_1, donc μ_1 et μ'_1 divisent P ; de plus, si $i \in [\![1, r]\!]$ (resp $j \in [\![1, s]\!]$), μ_i divise μ_1 (resp. μ'_j divise μ'_1) donc μ_1 (resp. μ'_1) annule $u_{|F_i}$ (resp. $u_{|G_j}$). Donc $\mu_1 = \mu = \mu'_1$.

Supposons maintenant que les familles $(\mu_i)_{1\leq i\leq r}$ et $(\mu'_j)_{1\leq j\leq s}$ sont distinctes. Alors, comme par (i) et (ii), on a

$$\sum_{i=1}^{r} \deg(\mu_i) = n = \sum_{j=1}^{s} \deg(\mu'_j),$$

il existe des indices $i > 1$ tels que $\mu_i \neq \mu'_i$, et on choisit le plus petit d'entre eux. Comme μ_j divise μ_i pour $j \geq i$, on a par (ii)

$$\mu_i(u)(E) = \mu_i(u)(F_1) \oplus \cdots \oplus \mu_i(u)(F_{i-1}).$$

On a aussi

$$\mu_i(u)(E) = \mu_i(u)(G_1) \oplus \cdots \oplus \mu_i(u)(G_s).$$

On se donne, pour $j \leq i$, des bases B_j et B'_j adaptées à la cyclicité de $u_{|F_j}$ et $u_{|G_j}$, et on en déduit que ces deux endomorphismes sont semblables. Donc $\mu_i(u_{|F_j})$ et $\mu_i(u_{|G_j})$ sont semblables, et on en déduit que $\mu_i(u)(F_j)$ et $\mu_i(u)(G_j)$ sont de même dimension. En passant à la dimension dans les deux expressions de $\mu_i(u)(E)$, on en déduit que $\mu_i(u)(G_j)$ est réduit à $\{0\}$ pour $j \in [\![i, s]\!]$, et donc en particulier, en prenant $j = i$, on obtient que $\mu'_i|\mu_i$. Par symétrie de rôle, on obtient aussi que $\mu_i|\mu'_i$. Mais comme ces deux polynômes sont unitaires, on en déduit qu'ils sont égaux, ce qui est absurde. Finalement les deux familles sont bien les mêmes. □

Le forme de Frobenius de u est alors la matrice de u dans une base adaptée à la cyclicité de u sur chacun des F_i, formée de matrices compagnons pour les P_i.

Si le temps le permet, il peut être intéressant d'ajouter la démonstration de lemme suivant.

Lemme 2 Il existe $x \in E$ tel que $\mu = \mu_{u,x}$.

Démonstration.

Étape 1. Propriétés des espaces $E_{u,x}$ et des polynômes $\mu_{u,x}$.

On montre deux résultats sur les espaces $E_{u,x} := \{P(u)(x),\ P \in \mathbb{K}[X]\}$. On se donne pour cela $x, y \in E$.

– Supposons que $E_{u,x} \cap E_{u,y} = \{0\}$. Comme $\mu_{u,x+y}(u)(x + y) = 0$, on a

$$\mu_{u,x+y}(u)(x) = -\mu_{u,x+y}(u)(y).$$

Ces deux éléments sont respectivement dans $E_{u,x}$ et $E_{u,y}$, donc nuls. Donc $\mu_{u,x}$ et $\mu_{u,y}$ divisent $\mu_{u,x+y}$. Comme on a aussi

$$\mathrm{ppcm}(\mu_{u,x}, \mu_{u,y})(u)(x + y) = \mathrm{ppcm}(\mu_{u,x}, \mu_{u,y})(u)(x) + \mathrm{ppcm}(\mu_{u,x}, \mu_{u,y})(u)(y) = 0,$$

on en déduit que $\mu_{u,x+y} = \mathrm{ppcm}(\mu_{u,x}, \mu_{u,y})$.

– Supposons que $\mu_{u,x}$ et $\mu_{u,y}$ sont premiers entre eux. On se donne $z \in E_{u,x} \cap E_{u,y}$. Alors $z = P(u)(x) = Q(u)(y)$, avec $P, Q \in \mathbb{K}[X]$. On a alors

$$0 = P(u) \circ \mu_{u,x}(u)(x) = \mu_{u,x}(u) \circ P(u)(x) = \mu_{u,x}(u)(z) = (\mu_{u,x}Q)(u)(y).$$

Donc $\mu_{u,y}|\mu_{u,x}Q$, et donc d'après le lemme de Gauß, $\mu_{u,y}|Q$. On en déduit que z est nul, donc $E_{u,x}$ et $E_{u,y}$ sont en somme directe. De plus, on en déduit aussi que $\mu_{u,x+y} = \mu_{u,x}\mu_{u,y}$, et donc

$$\dim(E_{u,x+y}) = \deg(\mu_{u,x+y}) = \deg(\mu_{u,x}) + \deg(\mu_{u,y}) = \dim(E_{u,x}) + \dim(E_{u,y}).$$

De plus, si $U\mu_{u,x} + V\mu_{u,y} = 1$, on a pour tout $z = P(u)(x + y) \in E_{u,x+y}$

$$z = (PU\mu_{u,x})(u)(x + y) + (PV\mu_{u,y})(u)(x + y) = (PU\mu_{u,x})(u)(y) + (PV\mu_{u,y})(u)(x) \in E_{u,x} + E_{u,y}.$$

On a finalement montré que $E_{u,x+y} \subset E_{u,x} \oplus E_{u,y}$, et donc par égalité de dimension $E_{u,x+y} = E_{u,x} \oplus E_{u,y}$.

Étape 2. Cas des facteurs du polynôme minimal.

Soit P un facteur irréductible de μ et α sa multiplicité : $\mu = P^\alpha Q$, avec Q premier avec P et donc P^α. Grâce au lemme des noyaux, on a donc

$$E = \ker(P^\alpha(u)) \oplus \ker(Q(u)).$$

Soit $x \in \ker(P^\alpha(u))$. Alors $\mu_{u,x} | P^\alpha$, donc (comme P est irréductible) il existe $\beta_x \leq \alpha$ tel que $\mu_{u,x} = P^{\beta_x}$. On cherche $x \in \ker(P^\alpha(u))$ tel que $\beta_x = \alpha$. Supposons qu'un tel x n'existe pas, et donc que pour tout $x \in \ker(P^\alpha(u))$, $P^{\alpha-1}(u)(x) = 0$, c'est-à-dire que $\ker(P^{\alpha-1}(u)) = \ker(P^\alpha(u))$. Alors en appliquant le lemme des noyaux dans l'autre sens, on obtient que $P^{\alpha-1}Q$ annule u, ce qui contredit la minimalité de μ. Donc il existe $x \in \ker(P^\alpha(u))$ tel que $\mu_{u,x} = P^\alpha$.

On note maintenant $\mu = \prod_{i=1}^{k} P_i^{\alpha_i}$ la décomposition de μ en produit d'irréductibles, et x_i un vecteur de $\ker(P_i^{\alpha_i}(u))$ tel que $\mu_{u,x_i} = P_i^{\alpha_i}$. Alors en appliquant $k-1$ fois la première étape, on en déduit que $E_{u,x_1+\cdots+x_k} = E_{u,x_1} \oplus \cdots \oplus E_{u,x_k} =$ et donc

$$\mu_{u,x_1+\cdots+x_k} = \prod_{i=1}^{k} P_i^{\alpha_i} = \mu.$$

□