Théorème de réduction de Frobénius - Applications :

Voici les notes que j'ai réalisées lors de mon année de préparation à l'agrégation. Au delà de la démonstration du théorème, y figurent des applications/compléments.

Table des matières

Dans tout ce document, E désigne un espace vectoriel sur un corps $\mathbb{K}$ quelconque.

1 Théorème de réduction de Frobénius

Définition 1

Soit E un espace vectoriel de dimension finie n, et $u \in \mathcal{L}(E)$. On rappelle que u est dit cyclique s'il existe un vecteur $x \in E$ tel que $E = Vect(u^i(x), i \in \mathbb{N})$. Un tel vecteur est dit vecteur cyclique.

1.1 Un lemme fondamental

Lemme 1

Soient E un espace vectoriel de dimension finie, et $u \in \mathcal{L}(E)$, une application linéaire. Alors, il existe $x \in E$ tel que $\pi_u = \pi_{u,x}$.

La démonstration de ce lemme repose sur les deux propriétés suivantes :

Proposition 1

Soient E un espace vectoriel de dimension finie, et $u \in \mathcal{L}(E)$. On considère $(x, y) \in E^2$ tels que $\pi_{u,x} \wedge \pi_{u,y} = 1$. Alors, $\pi_{u,x+y} = \pi_{u,x}\pi_{u,y}$.

Démonstration : En effet, remarquons que : $(\pi_{u,x}\pi_{u,y})(u)(x+y) = \pi_{u,y}(u) \circ \pi_{u,x}(u)(x) + \pi_{u,x}(u) \circ \pi_{u,y}(u)(y) = 0$. On en déduit que :

$$\pi_{u,x+y} | \pi_{u,x}\pi_{u,y}.$$

Réciproquement, on a, par définition,

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

Ainsi,

$$(\pi_{u,y}\pi_{u,x+y})(u)(x) = -\pi_{u,x+y}(u) \circ \pi_{u,y}(u)(y) = 0.$$

Par suite, $\pi_{u,x} | \pi_{u,y}\pi_{u,x+y}$. Par hypothèse de primalité, on déduit du lemme de Gauss que $\pi_{u,x} | \pi_{u,x+y}$. De manière similaire, $\pi_{u,y} | \pi_{u,x+y}$. Ainsi,

$$\pi_{u,x}\pi_{u,y} = \pi_{u,x} \vee \pi_{u,y} | \pi_{u,x+y}.$$

Les polynômes sont donc associés, et puisqu'ils sont unitaires, ils sont égaux. ■

Proposition 2

Soient $P \in \mathbb{K}[X]$ un polynôme irréductible, $A \in \mathbb{K}[X]$, et $\alpha \in \mathbb{N}^*$ tel que $P \wedge A = 1$. Supposons que $\pi_u = P^\alpha A$. Alors, il existe $x \in E$, tel que $\pi_{u,x} = P^\alpha$.

Démonstration : Le lemme des noyaux fournit

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

Si, pour tout $x \in \ker(P^\alpha(u))$, $\pi_{u,x} | P^{\alpha-1}$, alors, $P^{\alpha-1}A$ annule u sur $\ker(P^\alpha(u))$ et sur $\ker(A(u))$ donc sur E. Ainsi, $P^{\alpha-1} \in (\pi_u)$ et $\pi_u | P^{\alpha-1}A$. Impossible, donc, il existe $x \in \ker(P^\alpha(u))$ tel que $\pi_{u,x} \nmid P^{\alpha-1}$. Or, $\pi_{u,x} | P^\alpha$, donc par irréductibilité de P, $\pi_{u,x} = P^\alpha$. ■

Nous pouvons alors passer à la démonstration du lemme :

Démonstration : On décompose π_u en produit de facteurs irréductibles sur $\mathbb{K}$, $\pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$. Par la proposition 2, pour $i \in [\![1, r]\!]$, il existe $x_i \in E$ tel que $\pi_{u,x_i} = P_i^{\alpha_i}$. Puisque $P_i \wedge \left(\prod_{\substack{j=1,\\ j\neq i}}^{r} P_j^{\alpha_j} \right)$, la proposition 1 donne $\pi_{u,x} = \prod_{i=1}^{r} P_i^{\alpha_i} = \pi_u$ pour $x = \sum_{i=1}^{r} x_i$. ■

Remarque 1. *On déduit de ce résultat la caractérisation suivante des endomorphismes cycliques : pour $u \in \mathcal{L}(E)$, les propositions suivantes sont équivalentes :*

1. *u est cyclique.*
2. *il existe $x \in E$ tel que $\mathcal{B} = (x, u(x), \cdots, u^{n-1}(x))$ base de E.*
3. *il existe une base $\mathcal{B}$ de E pour laquelle $Mat_{\mathcal{B}}(u)$ est une matrice compagnon.*
4. *$\pi_u = \chi_u$.*

Démonstration : *L'equivalence entre les points 1 et 2 est claire, en effet : (2) $\Rightarrow$ (1) est évident.*

Pour (1) $\Rightarrow$ (2), soit $y \in E$, il existe $m \in \mathbb{N}$ et $\lambda_0, \cdots, \lambda_m \in \mathbb{K}$ tel que $y = \sum_{j=0}^{m} \lambda_j u^j(x) = A(x)$ pour $A = \sum_{j=0}^{m} \lambda_j X^j$. Par division euclidienne, il existe un unique couple $Q, R \in \mathbb{K}[X]$ tels que $A = Q\chi_u + R$, et $\deg(R) < \deg(\chi_u) = n$. Par suite, $y = R(x) \in Vect(x, u(x), \cdots, u^{n-1}(x))$. La famille est génératrice, ayant le bon cardinal, c'est une base.

(2) $\Leftrightarrow$ (3) est claire.

Montrons (1) $\Rightarrow$ (4). Par (2), la famille $(x, u(x), \cdots, u^{n-1}(x))$ est libre. Ainsi, $\deg(\pi_{u,x}) \geq n$. Puisque $\pi_{u,x} | \pi_u | \chi_u$, $\deg(\pi_{u,x}) \leq \deg(\chi_u) = n$. Ceci conclut car, $\pi_u | \chi_u$, et les polynômes sont unitaires, de même degré.

Réciproquement, il existe $x \in E$ tel que $\chi_u = \pi_u = \pi_{u,x}$. Ainsi, $n = \deg(\chi_u) = \deg(\pi_{u,x})$. Par suite, la famille $(x, u(x), \cdots, u^{n-1}(x))$ est libre (sinon, on contredit la minimalité de $\pi_{u,x}$). Ceci conclut. ■

1.2 Démonstration du théorème de réduction

Lors de la présentation du développement, je démontrais le lemme ainsi que l'existence, mais pas l'unicité à cause du manque de temps.

Theorème 1

Soient E un espace vectoriel de dimension n, et $u \in \mathcal{L}(E)$. Alors il existe une décomposition de $E = \bigoplus_{i=1}^{r} E_i$ en sous-espaces stables et $(P_1, \cdots, P_r) \in \mathbb{K}[X]^r$ tels que

- $u_{|E_i}$ *est un endomorphisme cyclique, de polynôme* P_i.
- $P_r|\cdots|P_2|P_1 = \pi_u$.

De plus, $(P_1, \cdots, P_r)$ *ne dépend que de* u.

Démonstration : Existence : On raisonne par récurrence forte sur $n = \dim(E)$. Si $n = 1$, l'endomorphisme est nécessairement cyclique et il n'y a rien à montrer. On suppose le résultat acquis pour des espaces de dimension $k \in \{0, \cdots, n-1\}$. Soit E un espace vectoriel de dimension n et $u \in \mathcal{L}(E)$. On considère $x \in E$ tel que $\pi_u = \pi_{u,x}$. On note $d := \deg(\pi_{u,x}) \geq 1$. La famille $(x, u(x), \cdots, u^{d-1}(x))$ est libre. On note $F = \text{Vect}(x, u(x), \cdots, u^{d-1}(x))$, sous-espace vectoriel de E de dimension d, stable par u (par division euclidienne par le polyôme minimal). De plus $u_{|F}$ est un endomorphisme cyclique.

But : montrer que F admet un sous-espace vectoriel supplémentaire dans E, stable par u. On pourra alors lui appliquer l'hypothèse de récurrence. Remarquons que si $d = n$, alors l'endomorphisme est cyclique, et on a terminé. Sinon, on procède comme suit :

Pour $i \in [\![1, d]\!]$, on note $e_i = u^{i-1}(x)$ et on complète $(e_i)_{i\in[\![1,d]\!]}$ en une base de E, $\mathcal{B} = (e_i)_{i\in[\![1,n]\!]}$. On note $\mathcal{B}^*$ la base duale de $\mathcal{B}$. On note enfin $\varphi = e_d^*$. On introduit :

$$G = \text{Vect}(\varphi, {}^tu \circ \varphi, \ldots, {}^tu^{d-1} \circ \varphi).$$

Montrons que G est de dimension d :
Soient $\lambda_0, \cdots, \lambda_{d-1}$ tels que $\displaystyle\sum_{i=0}^{d-1} \lambda_i {}^tu^i \circ \varphi = 0$, *i.e.* $\displaystyle\sum_{i=0}^{d-1} \lambda_i \varphi \circ u^i = 0$. En évaluant en x, on obtient $\lambda_{d-1} = 0$. En appliquant en cascade ${}^tu$ à l'égalité, on obtient le résultat.

On pose $G^0 = \{x \in E,\ \forall f \in G,\ f(x) = 0\}$. C'est un sous-espace vectoriel de E, de dimension $n - d$. Il est clairement stable par u (car G est stable par ${}^tu$).

Montrons que $E = F \oplus G^0$. On a clairement l'inclusion $\supseteq$, et l'égalité des dimensions. Soit $y \in F \cap G^0$. Alors, $y = \displaystyle\sum_{i=0}^{d-1} \lambda_i u^i(x)$. De plus, $\forall j \in [\![0, d-1]\!]$, $0 = \varphi \circ u^j(y) = \displaystyle\sum_{i=0}^{d-1} \lambda_i \varphi \circ u^{i+j}(x) = \lambda_{d-1-j}$. Ceci conclut.

Par l'hypothèse de récurrence, il existe une décomposition de G^0 en sous-espaces vectoriels stables par $u_{|G^0}$ (donc par u), $G^0 = \displaystyle\bigoplus_{i=2}^{r} E_i$ pour lesquels $u_{|G^0|E_i} = u_{|E_i}$ est cyclique de polynôme caractéristique P_i, avec $P_r|\cdots|P_3|P_2 = \pi_{u_{|G^0}}$. Enfin, puisque $\pi_u(u_{|G^0}) = 0$, $P_2 = \pi_{u_{|G^0}} | \pi_u = P_1$.

Unicité : soient $E = \displaystyle\bigoplus_{j=1}^{r} E_j = \bigoplus_{j=1}^{s} F_j$ deux telles décompositions associées respectivement aux polynômes $(P_1, \cdots, P_r)$ et $(Q_1, \cdots, Q_s)$. On suppose que $(P_1, \cdots, P_r) \neq (Q_1, \cdots, Q_s)$, et on introduit j le plus petit indice tel que $P_j \neq Q_j$, $j \in [\![1, \min(r, s)]\!]$. C'est possible même si $r \neq s$ car $n = \displaystyle\sum_{j=1}^{r} \deg(P_j) = \sum_{j=1}^{s} \deg(Q_j)$.
On sait que pour $i \geq j$, $\pi_{u_{|E_i}} = P_i | P_j$, donc $P_j(u_{|E_i}) \underset{stabilité}{=} P_j(u)|_{E_i} = 0$. Ainsi,

$$P_j(u)(E) = P_j(u)(E_1) \oplus \cdots \oplus P_j(u)(E_{j-1}) = P_j(u)(F_1) \oplus \cdots \oplus P_j(u)(F_s).$$

De plus, pour $i \in [\![1, j-1]\!]$, $u_{|E_i}$ est cyclique, de polynôme $P_i = Q_i$, donc, $u_{|E_i} \sim u_{|F_i}$, donc $P_j(u_{|E_i}) \sim P_j(u_{|F_i})$. Ainsi, on obtient par le rang $\dim(P_j(u)(E_i)) = \dim(P_j(u)(F_i))$. Par suite on a :

$$\forall i \in [\![j, s]\!],\ P_j(u)(F_i) = 0.$$

Alors, $P_j(u_{|F_j}) = 0$ donc $Q_j | P_j$. Par symétrie, $P_j = Q_j$. Absurde. ■

2 Applications

2.1 Un corollaire immédiat : classification des invariants de similitude

Theorème 2

Deux endomorphismes (respectivement deux matrices) sont semblables ssi elles ont les mêmes invariants de similitudes.

Démonstration : Pour le sens direct, on remarque que si deux endomorphismes sont semblables, ils représentent le même endomorphisme dans deux bases différentes. Puisque les invariants de similitude sont indépendants de la base, on conclut. La réciproque est évidente. ■

2.2 Transposée

Theorème 3

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors, $A \sim {}^tA$.

Démonstration : Au vu du théorème de réduction de Frobénius, il suffit de le vérifier pour une matrice compagnon, et on pourra conclure par blocs. Soit $A = C_P$, une matrice compagnon de polynôme P. On remarque que $Q(A) = 0 \Leftrightarrow Q({}^tA) = 0$. Ainsi, $\chi_A = \chi_{{}^tA}$ et $\pi_A = \pi_{{}^tA}$. Ainsi, ${}^tA$ est cyclique, de polynôme P, donc semblable à $C_P = A$. ■

2.3 Un cas particulier

Theorème 4

Soient $M \in \mathcal{M}_n(\mathbb{K})$ et $P_1, \cdots, P_s$ ses facteurs invariants. Alors,

$$s = n \Leftrightarrow M \text{ est une homothétie.}$$

Démonstration : On sait que $M \sim \mathrm{Diag}(C_{P_1}, \cdots, C_{P_n})$. De plus, $n = \deg(\chi_M) = \sum_{j=1}^{n} \deg(P_j) \geq \sum_{j=1}^{n} 1 = n$. Donc, pour tout $i \in [\![1, n]\!]$, $\deg(P_i) = 1$, donc $P_i = X + a_i$. Enfin, comme $P_n | \cdots | P_1$, $a_1 = \cdots = a_n$, et $M \sim -a_1 I_n$ est une homothétie. La réciproque est évidente. ■

2.4 Vraisemblance et changement de corps

Theorème 5

Soit $L/\mathbb{K}$ une extension de corps, et $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$ tels que $A \underset{L}{\sim} B$. Alors, $A \underset{\mathbb{K}}{\sim} B$.

Démonstration : Par unicité des invariants de similitude, les invariants de $A \in \mathcal{M}_n(\mathbb{K})$ et de $A \in \mathcal{M}_n(L)$ sont les mêmes. Puisque $A \underset{L}{\sim} B$, ils ont les mêmes invariants sur L donc sur $\mathbb{K}$. Ainsi, $A \underset{\mathbb{K}}{\sim} B$. ■

2.5 Cas particulier de la dimension 2 et 3

Proposition 3

Soient $M, N \in \mathcal{M}_n(\mathbb{K})$, et $n = 2, 3$. Alors, $M \sim N$ ssi $\begin{cases} \chi_M = \chi_N \\ \pi_M = \pi_N \end{cases}$.

Démonstration : Le sens direct est évident. Réciproquement, si $n = 2$, et si M est diagonalisable, alors N l'est aussi, et ayant les mêmes valeurs propres, elles sont semblables. Sinon $M \sim C_P$, et $\chi_M = \chi_N = \pi_M = \pi_N = P$, donc, N est une matrice compagnon de même polynôme. Ceci conclut.

Si $n = 3$, alors, soit $M \sim C_P$, et on conclut de la même façon, soit $M \sim \begin{pmatrix} C_{P_1} & 0 \\ 0 & C_{P_2} \end{pmatrix}$, avec $P_2|P_1 = \pi_M$, et $P_1P_2 = \chi_M$. Les matrices M et N ont donc les mêmes invariants et sont donc semblables. Enfin, si M possède 3 invariants, c'est une homothétie. Au vu de l'égalité du polynôme minimal, il en est de même pour N. ■

2.6 Sur le commutant

Proposition 4

Pour tout $u \in \mathcal{L}(E)$, $\dim(Com(u)) \geq \dim(E)$.

Démonstration : On applique le théorème de réduction de Frobénius, et la dimension du commutant de u est la dimension du commutant de $M = \mathrm{Diag}(C_{P_1}, \cdots, C_{P_r})$. On remarque que si A_i commute avec C_{P_i}, alors $\mathrm{Diag}(0, \cdots, 0, A_i, 0, \cdots, 0)$ commute avec M. Par suite,

$$\dim(\mathrm{Com}(u)) \geq \dim\left(\{\mathrm{Diag}(0, \cdots, 0, A_i, 0, \cdots, 0),\ i \in [\![1, r]\!],\ A_i \in \mathrm{Com}(C_{P_i})\}\right).$$

Puisque C_{P_i} est cyclique, il est connu que $\mathrm{Com}(C_{P_i}) = \mathbb{K}[C_{P_i}]$. Alors,

$$\dim(\mathrm{Com}(u)) \geq \sum_{i=1}^{r} \deg(\pi_{C_{P_i}}) = \sum_{i=1}^{r} \deg(P_i) = \deg(\chi_u) = n.$$

■

Proposition 5

Pour tout $u \in \mathcal{L}(E)$, u est cyclique $\Leftrightarrow$ $Com(u) = \mathbb{K}[u]$.

Démonstration : Le sens direct est connu. Réciproquement, on applique le théorème de réduction de Frobénius à u. Le but est de montrer que u ne possède qu'un invariant de similitude. On a la décomposition $E = \bigoplus_{i=1}^{r} E_i$ en sous-espaces cycliques stables par u, et $(P_i)_{1 \leq i \leq r}$ ses invariants de similitude, avec $P_1 = \pi_u$. On considère S la projection sur $\bigoplus_{i=2}^{r} E_i$ parallèlement à E_1.

Pour tout $x \in E$, il existe une unique décomposition $(x_1, \cdots, x_r) \in E_1 \times \cdots \times E_r$ telle que $x = \sum_{j=1}^{r} x_j$. Alors, par stabilité,

$$S \circ u(x) = \sum_{j=2}^{r} u(x_j) = u\left(\sum_{j=2}^{r} x_j\right) = u \circ S(x).$$

Ainsi, il existe $P \in \mathbb{K}[X]$ tel que $S = P(u)$. Or, $S_{|E_1} = 0$. Ainsi, $\pi_{u_{|E_1}} = P_1 = \pi_u|P$. Donc, $S = P(u) = 0$. Ainsi, $\ker(S) = E_1 = E$, et $r = 1$. ■