P. Maurer

ENS Rennes

Recasages : *150, (151), 153, 154, 159*

Référence : Gourdon, Algèbre

Réduction de Frobenius

On se donne un espace vectoriel E de dimension finie $n\in\mathbb{N}^*$ sur $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, et $f\in\mathcal{L}(E)$. On commence par des rappels sur les endomorphismes cycliques.

Notation 1. *On note π_f le polynôme minimal de f, et $\mathcal{L}_f$ l'ensemble $\{P(f)\ :\ P\in\mathbb{K}[X]\}$.*

Si $x\in E$, on note P_x le polynôme unitaire engendrant l'idéal $\{P\in\mathbb{K}[X]\ :\ P(f)(x)=0\}$, et E_x l'ensemble $\{P(f)(x)\ :\ P\in\mathbb{K}[X]\}$.

Dans la suite, on notera k le degré de π_f et ℓ_x le degré de P_x pour $x\in E$.

Proposition 2. *L'ensemble $\mathcal{L}_f$ est un sous espace vectoriel de $\mathcal{L}(E)$ de dimension k, dont une base est $(\mathrm{Id}_E, f,\dots,f^{k-1})$. L'ensemble E_x est un sous-espace vectoriel de E de dimension ℓ_x, dont une base est $(x,\dots,f^{\ell_x-1}(x))$.*

Démonstration. L'application linéaire $\varphi\colon\left\{\begin{array}{lcl}\mathbb{K}[X] & \to & \mathcal{L}(E)\\ P & \mapsto & P(f)\end{array}\right.$ a pour image $\mathcal{L}_f$, qui est donc un sous-espace vectoriel. Son noyau est $\{P\in\mathbb{K}[X]\ :\ P(f)=0\}=(\pi_f)$, donc le premier théorème d'isomorphisme donne $\mathcal{L}_f\simeq\mathbb{K}[X]/(\pi_f)$. Par ailleurs, on a $\mathbb{K}[X]/(\pi_f)=\mathrm{Vect}(\overline{1},\overline{X},\dots,\overline{X}^{k-1})$ par division euclidienne, et cette famille est libre sur $\mathbb{K}[X]/(\pi_f)$, donc c'est une base de $\mathbb{K}[X]/(f)$.

En particulier, $\mathcal{L}_f$ est de dimension k et une base de $\mathcal{L}_f$ est donnée par $(\mathrm{Id}_E, f,\dots,f^{k-1})$ au vu de l'isomorphisme de factorisation $\tilde{\varphi}\colon\left\{\begin{array}{lcl}\mathbb{K}[X]/(\pi_f) & \to & \mathcal{L}(E)\\ \overline{P} & \mapsto & \overline{P}(f)\end{array}\right.$.

En considérant $\psi\colon\left\{\begin{array}{lcl}\mathbb{K}[X] & \to & E\\ P & \mapsto & P(f)(x)\end{array}\right.$, le même raisonnement prouve la deuxième partie de la proposition. □

Théorème 3. *Il existe $x\in E$ tel que $P_x=\pi_f$.*

On trouve une démonstration de ce résultat dans le Gourdon, page 178. Elle est un peu trop longue pour être faite à l'oral avec le théorème de Frobenius, mais il est bon d'avoir une idée de la preuve, qui repose essentiellement sur l'utilisation du lemme des noyaux.

Définition 4. *On dit que f est cyclique s'il existe $x\in E$ tel que $E_x=E$. D'après ce qui précède, ceci équivaut à dire que $k=\deg(\pi_f)=n$, ou encore que $\pi_f=(-1)^n\chi_f$, où χ_f désigne le polynôme caractéristique de f.*

Définition 5. *Soit* $P = X^p + a_{p-1} X^{p-1} + \cdots + a_0$ *un polynôme unitaire de* $\mathbb{K}[X]$*. On appelle matrice compagnon de* P *la matrice*

$$\mathcal{C}(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \cdots & 0 & 1 & -a_{p-1} \end{pmatrix}.$$

Proposition 6. *Le polynôme caractéristique* $\chi_{\mathcal{C}(P)}$ *de* $\mathcal{C}(P)$ *vérifie* $\chi_{\mathcal{C}(P)} = (-1)^p P$*.*

Démonstration. On développe par rapport à la dernière colone le déterminant $\det(\mathcal{C}(P) - X I_p)$. Il vient

$$\begin{aligned} \chi_{\mathcal{C}(P)} &= (-1)^p\, a_0 \begin{vmatrix} 1 & -X & & (0) \\ & \ddots & \ddots & \\ (0) & & 1 & -X \end{vmatrix} + (-1)^{p+1}\, a_1 \begin{vmatrix} -X & & & & (0) \\ 0 & 1 & -X & & \\ & \ddots & \ddots & \ddots & \\ (0) & & 0 & 1 & -X \end{vmatrix} + \cdots - (X + a_{p-1}) \begin{vmatrix} -X & 0 & \cdots & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & -X & 0 \\ (0) & & 1 & -X \end{vmatrix} \\ &= (-1)^p (a_0 + a_1 X + \cdots + a_{p-1} X^{p-1} + X^p) \\ &= (-1)^p P, \end{aligned}$$

où les déterminants masqués dans la première ligne se calculs de même puisqu'ils sont triangulaires par blocs. $\square$

Théorème 7.

Soit $f \in \mathcal{L}(E)$ *un endomorphisme cyclique. Il existe une base de* E *dans laquelle la matrice de* f *soit égale à* $\mathcal{C}(\pi_f)$*.*

Démonstration. Comme f est cyclique, il existe $x \in E$ tel que $E_x = E$. La proposition 2 affirme alors que $(x, f(x), \ldots, f^{n-1}(x))$ est une base de E, et dans cette base, on montre que la matrice de f est $\mathcal{C}(\pi_f)$. $\square$

Le théorème principal du développement est le suivant.

Théorème 8. *(Invariants de similitude)*

Soit $f \in \mathcal{L}(E)$*. Il existe une suite finie* $F_1, \ldots, F_r$ *de sous-espaces vectoriels de* E*, tous stables par* f*, telle que*

1. $E = \bigoplus_{i=1}^{r} F_i$,
2. *pour tout* $i \in [\![1, r]\!]$, $f_{|F_i}$ *est un endomorphisme cyclique,*
3. *si* $P_i = \pi_{f_i}$*, on a* $P_{i+1} | P_i$ *pour tout* $i \in [\![1, r-1]\!]$*.*

La suite $P_1, \ldots, P_r$ *ne dépend que de* f *et non du choix de la décomposition. On l'appelle suite des invariants de similitude de* f*.*

Démonstration.

$\boxed{\exists}$ **Etape 1 :** on trouve deux sous-espaces stables par f qui conviennent.

On note $k=\deg(\pi_f)$ et on se donne $x\in E$ tel que $P_x=\pi_f$, qui existe bien d'après le théorème 3.

Le sous-espace $F:=E_x$ est de dimension k et il est stable par f. Comme $\deg(P_x)=k$, la famille $(e_1,\dots,e_k)$ avec $e_i=f^{i-1}(x)$ est une base de F, que l'on complète en une base $(e_1,\dots,e_n)$ de E.

En désignant par $(e_1^*,\dots,e_n^*)$ la base duale associée, on pose

$$\Gamma=\{e_k^*\circ f^i\ :\ i\in\mathbb{N}\}\ \text{ et }\ G=\Gamma^\circ,$$

où l'orthogonal est vu au sens de la dualité, de sorte que $G=\{x\in E\ :\ \forall i\in\mathbb{N}\quad e_k^*(f^i(x))=0\}$. Il est clair que G est un sous-espace de E qui est également stable par l'endomorphisme f.

L'objectif est de démontrer que $E=F\oplus G$, de sorte que si l'on note P_1 le polynôme minimal de $f_{|F}$ et P_2 celui de $f_{|G}$, on a $P_1=P_x=\pi_f$ et $P_2(f_{|G})=\pi_f(f_{|G})=0$ donc $\pi_f|P_2$, donc $P_1|P_2$. Le résultat suit alors par récurrence sur $n=\dim(E)$.

Etape 2 : on montre que $G\cap F=\{0\}$.

Soit $y\in G\cap F$. Supposons par l'absurde que y est non nul. Alors on peut écrire $y=y_1\,x+y_2\,f(x)+\cdots+y_p\,f^{p-1}(x)$ avec $p\leq k$ et $y_p\neq 0$. En appliquant $e_k^*\circ f^{k-p}$ à y, il vient

$$\begin{aligned} e_k^*(f^{k-p}(x)) &= e_k^*(y_1\,f^{k-p+1}(x)+\cdots+y_p\,f^{k-1}(x)) \\ &= y_p. \end{aligned}$$

Comme on a $x\in G$, il vient $y_p=0$, ce qui est une contradiction. Ainsi, on a $G\cap F=\{0\}$.

Etape 3 : on montre que $\dim(G)+\dim(F)=\dim(E)$.

Il s'agit de montrer que $\dim(G)=n-k$. Comme $G=(\mathrm{Vect}(\Gamma))^\circ$, on a $\dim(G)=n-\dim(\mathrm{Vect}(\Gamma))$, donc il suffit de prouver que $\mathrm{Vect}(\Gamma)$ est de dimension k.

On considère pour cela l'application linéaire $\varphi\colon\begin{cases}\mathcal{L}_f & \to & \mathrm{Vect}(\Gamma)\\ g & \mapsto & e_k^*(g)\end{cases}$. Alors φ est surjective par définition. De plus, pour $g\in\operatorname{Ker}\varphi$, on a $e_k^*(g)=0$. Supposons par l'absurde que $g\neq 0$: on peut alors décomposer g dans la base $(\mathrm{Id}_E,f,\dots,f^{k-1})$ de $\mathcal{L}_f$. Il existe donc $p\leq k$ tel que

$$g\ =\ g_0\,\mathrm{Id}_E+g_1\,f+\cdots+g_p\,f^{p-1}\quad\text{avec } g_p\neq 0.$$

En appliquant $e_k^*\circ f^{k-p}$ à cette égalité, on en déduit que $g_p=0$, ce qui est une contradiction.

Ainsi, φ est un isomorphisme entre $\mathrm{Vect}(\Gamma)$ et $\mathcal{L}_f$. Comme $\mathcal{L}_f$ est de dimension k, on en déduit le résultat souhaité.

$\boxed{!}$ On suppose qu'il existe deux suites de sous-espaces $F_1,\dots,F_r$ et $G_1,\dots,G_s$ tous stables par f, et qui vérifient les conditions 1, 2 et 3 du théorème. Notons P_i et Q_j les polynôme minimaux respectifs de $f_{|F_i}$ et de $f_{|G_j}$ pour $i\in[\![1,r]\!]$ et $j\in[\![1,s]\!]$.

Pour tout $x_i\in F_i$, $P_i|P_1$ donc il existe $Q\in\mathbb{K}[X]$ tel que $P_1(f)(x_i)=P_i\,(f_{|F_i})(x_i)\times Q\,(f)(x)=0$. On en déduit que $P_1(f)=0$ sur E, donc $\pi|P_1$, et comme P_1 est le polynôme minimal de $f_{|E_1}$, c'est que $P_1|\pi$. Donc $\pi=P_1$. (1) On montre de même que $Q_1=\pi$, donc $P_1=Q_1$.

Supposons $(P_1,\dots,P_r)\neq(Q_1,\dots,Q_s)$ et notons j le premier indice tel que $P_j\neq Q_j$. Cet indice j existe bien même si $r\neq s$, puisque l'on a $\sum_{i=1}^{r}\deg P_i=\sum_{i=1}^{s}\deg Q_i=n$.

Alors par le même argument que (1), on a $P_j(f)(E_k)=0$ pour tout $k \geq j$. On en déduit que

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

Et on a également

$$P_j(f)(E)=P_j(f)(G_1)\oplus\cdots\oplus P_j(f)(G_{j-1})\oplus P_j(f)(G_j)\oplus+\cdots+\oplus P_j(f)(G_s). \quad (\wedge)$$

Par ailleurs, pour tout $i\in[\![1,j-1]\!]$, on a $\dim P_j(f)(F_i)=\dim P_j(f)(G_i)$. En effet, comme $f_{|F_i}$ et $f_{|G_i}$ sont cycliques sur F_i et G_i, il existe une base $\mathcal{B}$ de F_i et une base $\mathcal{B}'$ de G_i telles que

$$\mathrm{mat}_{\mathcal{B}}(f_{|F_i})=\mathcal{C}(P_i)=\mathcal{C}(Q_i)=\mathrm{mat}_{\mathcal{B}'}(f_{|G_i}).$$

On en déduit que $\dim(f(F_i))=\mathrm{rg}(\mathcal{C}(P_i))=\mathrm{rg}(\mathcal{C}(Q_i))=\dim(f(G_i))$, et de fait, $\dim P_j(f)(F_i)=\dim P_j(f)(G_i)$. En prenant les dimensions dans les égalités $(\star)$ et $(\wedge)$, il vient

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

En particulier, $P_j(f)$ est nul sur G_j donc $Q_j|P_j$. Par symétrie des rôles de Q_j et P_j, on a aussi $P_j|Q_j$, donc $P_j=Q_j$, ce qui contredit l'hypothèse de départ. Aussi, il faut que $r=s$ et $P_i=Q_i$ pour tout i. □

Application 9. (réduction de Frobenius)

Soit $f\in\mathcal{L}(E)$ et $P_1,\dots,P_r$ la suite des invariants de similitude de f. Alors il existe une base $\mathcal{B}$ de E dans laquelle

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

On a $P_1=\pi_f$ et $P_1\cdots P_r$ est le polynôme caractéristique de f, à un facteur $(-1)^n$ près.

Application 10.

Deux endomorphismes f et g de $\mathcal{L}(E)$ sont semblables si et seulement si ils ont les mêmes invariants de similitude.