Développement: Réduction de Froebenius

Adrien Fontaine

18 novembre 2012

Référence : Gourdon, Annexe B p289 et exercice 3p178 pour la proposition (1).

1 Développement

Soit $u \in \mathcal{L}(E)$ un endomorphisme. On note π_u le polynôme minimal de u et $\mathcal{L}_u = \{P(u), P \in \mathbb{K}[X]\}$.
Si $x \in E$, on note P_x le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X]/P(u)(x) = 0\}$ et $E_x = \{P(u)(x), P \in \mathbb{K}[X]\}$.

Proposition 1

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

Démonstration : Soit $\pi_u = \prod_{i=1}^{k} M_i^{\alpha_i}$ la décomposition de π_u en facteurs irréductibles de $\mathbb{K}[X]$.
Pour tout $i \neq j$, on a $M_i^{\alpha_i} \wedge M_j^{\alpha_j} = 1$, donc d'après le théorème de décomposition des noyaux, on a :

$$E = \bigoplus_{i=1}^{k} Ker(M_i^{\alpha_i}(f))$$

Soit $i_0 \in \{1, ..., k\}$, pour tout $x \in Ker(M_{i_0}^{\alpha_{i_0}}(u))$, on a $M_{i_0}^{\alpha_{i_0}}(u)(x) = 0$, donc $M_{i_0}^{\alpha_{i_0}} \in (P_x)$ donc

$$P_x \mid M_{i_0}^{\alpha_{i_0}} \tag{1}$$

Et comme M_{i_0} est irréductible, il existe $\beta_x \leq \alpha_{i_0}$ tel que $P_x = M_{i_0}^{\beta_x}$.
Montrons par l'absurde qu'il existe $x_{i_0} \in Ker(M_{i_0}^{\alpha_{i_0}}(u))$ tel que $\beta_{x_{i_0}} = \alpha_{i_0}$.
Si $\forall \in Ker(M_{i_0}^{\alpha_{i_0}}(u)), \beta_x < \alpha_{i_0}$, alors

$$\forall x \in Ker(M_{i_0}^{\alpha_{i_0}}(u)), P_x \mid M_{i_0}^{\alpha_{i_0}-1}$$

i.e

$$\forall x \in Ker(M_{i_0}^{\alpha_{i_0}}(u)), M_{i_0}^{\alpha_{i_0}-1}(u)(x) = 0$$

Donc, $Ker(M_{i_0}^{\alpha_{i_0}}(u)) = Ker(M_{i_0}^{\alpha_{i_0}-1}(u))$.
Donc,

$$E = Ker(M_{i_0}^{\alpha_{i_0}-1}(u)) \oplus \left(\bigoplus_{1 \leq i \leq k i \neq i_0} Ker(M_i^{\alpha_i}(u)) \right)$$

Donc, d'après le théorème de décomposition des noyaux,

$$Ker((M_{i_0}^{\alpha_{i_0}-1} \prod_{1 \leq i \leq k i \neq i_0} M_i^{\alpha_i})(u)) = E$$

ou encore,

$$(M_{i_0}^{\alpha_{i_0}-1}\prod_{1\leq i\leq k i\neq i_0} M_i^{\alpha_i})(u) := Q(u) = 0$$

ce qui contredit a minimalité du degré du polynôme minimal π_u car $deg(Q) < deg(\pi_u)$.
Donc, il existe $x_{i_0} \in Ker(M_{i_0}^{\alpha_{i_0}}(u))$ tel que $\beta_{x_{i_0}} = \alpha_{i_0}$, d'où $P_{x_{i_0}} = M_{i_0}^{\alpha_{i_0}}$.
De même pour tous les $1 \leq i \leq k$. Il existe donc, $(x_1, ..., x_k) \in Ker(M_1^{\alpha_1}) \times ... \times Ker(M_k^{\alpha_k})$ tel que $\forall 1 \leq i \leq k, P_{x_i} = M_i^{\alpha_i}$.
Montrons maintenant que $E_{x_1+...+x_k} = E_{x_1} \oplus ... \oplus E_{x_k}$. On montre le résultat pour $k = 2$, la généralisation se faisant facilement par récurrence.
Soient donc x et y tels que $P_x \wedge P_y = 1$ et $z \in E_x \cap E_y$. Il existe $P, Q \in \mathbb{K}[X]$ tels que $z = P(u)(x) = Q(u)(y)$.
Alors,

$$\begin{aligned} 0 &= P(u) \circ P_x(u)(x) \\ &= (PP_x)(u)(x) \\ &= P_x(u) \circ P(u)(x) \\ &= P_x(u)(z) \\ &= (P_xQ)(u)(y) \end{aligned}$$

Par le même raisonnement que pour (1), on a : $P_y \mid P_xQ$, or $P_y \wedge P_x = 1$ donc (Gauss) $P_y \mid Q$ donc $z = Q(u)(y) = 0$.
Donc, $E_x \cap E_y = \{0\}$.
Comme $P_{x+y}(u)(x + y) = 0$, on a

$$\underbrace{P_{x+y}(u)(x)}_{\in E_x} = -\underbrace{P_{x+y}(u)(y)}_{\in E_y}$$

Donc, $P_x \mid P_{x+y}$ et $P_y \mid P_{x+y}$.
Donc, $ppcm(P_x, P_y) \mid P_{x+y}$
Or, $P_x \mid ppcm(P_x, P_y)$ donc $ppcm(P_x, P_y)(u)(x) = 0$.
De même, $ppcm(P_x, P_y)(u)(y) = 0$.
Donc, $ppcm(P_x, P_y)(u)(x + y) = 0$
Donc, $P_{x+y} \mid ppcm(P_x, P_y)$
Donc, $P_{x+y} = ppcm(P_x, P_y)P_xP_y$.
D'où, $dim(E_{x+y}) = dim(E_x) + dim(E_y)$ et donc $E_{x+y} = E_x \oplus E_y$.
Ainsi, $E_{x_1+...+x_k} = E_{x_1} \oplus ... \oplus E_{x_k}$.
D'où, par le même raisonnement que pour montrer que $P_{x+y} = P_xP_y$, on a

$$P_{x_1+...+x_k} = P_{x_1}...P_{x_k} = \pi_u$$

D'où le résultat. ■

Théorème 1

Soit $u \in \mathcal{L}(E)$. Il existe une suite $F_1, ..., F_r$ de sev de E, tous stables par u, telle que :

1. *$E = F_1 \oplus ... \oplus F_r$*
2. *pour tout $i \in \{1, ..., r\}$, la restriction $u_i = u_{|F_i}$ de l'endomorphisme u au sev F_i est un endomorphisme de F_i cyclique.*
3. *Si P_i désigne le polynôme minimal de u_i, on a $P_{i+1} \mid P_i$ pour tout $i \in \{1, ..., r-1\}$. La suite de polynômes $P_1, ..., P_r$ ne dépend que de u, et non du choix de la décomposition.*

On l'appelle suite des invariants de similitude de u.

Démonstration : Existence :

Soit $k = deg(\pi_u)$ et soit $x \in E$ tel que $P_x = \pi_f$ (un tel x existe d'après la proposition (1)). Alors E_x est un sev de E de dimension k, stable par u par définition de E_x et dont une base est $(x, ..., u^{k-1}(x))$. Complétons cette base en une base $(e_1, ...e_n)$ de E.
Le sous espace E_x vérifie toutes les propriétés que l'on attend des sous-espaces $F_1, ...F_r$. L'idée est de trouver un supplémentaire G de E_x dans E tel que G soit stable par u et que le polynôme minimal de $u_{|G}$ divise le polynôme minimal de $u_{|E_x}$.
En désignant par $(e_1^*, ..., e_n^*)$ la base duale associée, on note

$$G = \Gamma^\circ \text{ où } \Gamma = \{e_k^* \circ u^i, i \in \mathbb{N}\}$$

et où Γ° désigne l'orthogonal vis à vis du dual de Γ. En d'autres termes, G est l'ensemble des $x \in E$ tels que la k-ième coordonnée de $u^i(x)$ dans la base $(e_1, ..., e_n)$ soit nulle pour tout i. Alors, on vérifie facilement que G est un sev de E stable par u.
Montrons que $E = E_x \oplus G$.

- $E_x \cap G = \{0\}$:
  Soit $y \in E_x \cap G$, si $y \neq 0$, on peut écrire

  $$y = a_1 e_1 + ... + a_p e_p \text{ avec } p \leq k \text{ et } a_p \neq 0$$

  En composant par $e_k^* \circ u^{k-p}$, on obtient

  $$\begin{aligned} \underbrace{0}_{y \in G} &= e_k^*(u^{k-p}(a_1 e_1 + ... + a_p e_p)) \\ &= e_k^*(a_1 e_{k-p+1} + ... + a_p e_k) \\ &= a_p \end{aligned}$$

  Absurde. Donc, $E_x \cap G = \{0\}$.
- $E_x + G = E$:
  Pour cela, on va montrer que $dim(G) = n - dim(E_x) = n - k$. Comme $G = (Vect(\Gamma))^\circ$, il suffit de prouver $dim(Vect(\Gamma) = k$. Pour cela, on considère l'application linéaire

  $$\begin{array}{rccc} \varphi & : & \mathcal{L}_u & \to & Vect(\Gamma) \\ & & g & \mapsto & e_k^* \circ g \end{array}$$

  Par définition de $Vect(\Gamma)$, φ est surjective. De plus, φ est injective. En effet, si $e_k^* \circ g = 0$ avec $g \neq 0$, on peut écrire $g = a_1 Id_E + ... + a_p u^{p-1} \in \mathcal{L}_u$ avec $p \leq k$ et $a_p \neq 0$, et

  $$\begin{aligned} 0 &= e_k^* \circ g(u^{k-p}(x)) \\ &= e_k^*(a_1 u^{k-p}(x) + ... + a_p u^{k-1}(x)) \\ &= e_k^*(a_1 e_{k-p+1} + ... + a_p e_k) \\ &= a_p \end{aligned}$$

  Ce qui est absurde ? Finalement, φ est un isomorphisme et donc $dim(Vect(\Gamma)) = dim(\mathcal{L}_u) = k$.

Résumons. Nous avons trouvé un sous-espace G stable par u tel que $E_x \oplus G = E$. Notons P_1 le polynôme minimal de $u_{|E_x}$ (qui est le polynôme minimal de u car $P_1 = P_x = \pi_u$), et P_2 le polynôme minimal de $u_{|G}$. Comme G est stable par u, $P_2 \mid P_1$. On applique alors ce qui précède à $u_{|G}$, et au bout d'un nombre fini d'étapes, on obtient la décomposition voulue.

Unicité :
Supposons l'existence de deux suites de sous-espaces $F_1, ..., F_r$ et $G_1, ..., G_s$ tous stables par u, et vérifiant les trois conditions du théorème. Notons $P_i = \pi_{u_{|F_i}}$ et $Q_j = \pi_{u_{|G_j}}$.
Comme $E = F_1 \oplus ... \oplus F_r$ et $P_r \mid P_{r-1} \mid ... \mid P_1$, on a :

$$P_1 = \pi_u = Q_1$$

Supposons la liste $(P_1, ..., P_r)$ différente de $(Q_1, ..., Q_s)$ et notons j le premier indice tel que $P_j \neq Q_j$ (un tel indice existe toujours même si $r \neq s$ car $\sum deg(P_i) = n = \sum deg(Q_j)$). L'égalité $E = F_1 \oplus ... \oplus F_r$ avec les F_i stables par u, et la propriété $P_j(u)(F_k) = 0$ pour $k \geq j$, entraînent :

$$P_j(u)(E) = P_j(u)(F_1) \oplus ... \oplus P_j(f)(F_{j-1}) \tag{2}$$

Et par ailleurs l'égalité, $E = G_1 \oplus ... \oplus G_s$ avec les G_j stables par u, entraîne,

$$P_j(u)(E) = P_j(u)(G_1) \oplus ... \oplus P_j(u)(G_{j-1}) \oplus P_j(u)(G_j) \oplus ... \oplus P_j(u)(G_s) \tag{3}$$

On a $dim(P_j(u)(F_i)) = dim(P_j(u)(G_i))$ pour $1 \leq i \leq j-1$ (en effet, il existe une base B_i de F_i et une base B_i' de G_i telle que la matrice de $u_{|F_i}$ soit la matrice compagnon $\mathcal{C}_{P_i}$ et la matrice de $u_{|G_i}$ soit la matrice compagnon $\mathcal{C}_{Q_i}$, or ces deux polynômes sont égaux par définition de j).
En prenant les dimensions dans (2) et (3), on en déduit $0 = dim(P_j(u)(G_j)) = ... = dim(P_j(u)(G_s))$, ce qui prouve que $Q_j \mid P_j$ (P_j est un polynôme annulateur de u sur G_j). Par symétrie, on a aussi $P_j \mid Q_j$, et donc $P_j = Q_j$. Absurde. Finalement on doit avoir $r = s$ et $P_i = Q_i$ pour tout i. ■

Théorème 2

Si $P_1, ..., P_r$ désigne la suite des invariants de similitude de $u \in \mathcal{L}(E)$, il existe une base B de E telle que :

$$[u]_B = \begin{bmatrix} \mathcal{C}(P_1) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(P_r) \end{bmatrix}$$

On a d'ailleurs $P_1 = \pi_u$ et $P_1...P_r$ est le polynôme caractéristique de u (au facteur $(-1)^n$ près).

Démonstration : Il suffit pour tout i de considérer une base B_i de F_i dans laquelle la matrice de u_i est $\mathcal{C}_{P_i}$. (ce qui est possible d'après le théorème (3), puis d'écrire la matrice de u dans la base $(B_1, ..., B_r)$). ■

2 Rappels

2.1 Sur les endomorphismes cycliques

Référence : Objectif Agrégation, p174

Définition 1

Soit $P = X^p + a_{p-1}x^{p-1} + ... + a_0 \in \mathbb{K}[X]$. On appelle matrice compagnon de P la matrice

$$\mathcal{C}_P = \begin{bmatrix} 0 & ... & 0 & -a_0 \\ 01 & \ddots & \vdots & \vdots \\ & \ddots & 0 & -a_{p-2} \\ & (0) & 1 & -a_{p-1} \end{bmatrix} \in M_p(\mathbb{K})$$

Le polynôme caractéristique de $\mathcal{C}_P$ est $(-1)^p P$.

Définition 2

Soient E un $\mathbb{K}$-espace vectoriel de dimension n et $u \in \mathcal{L}(E)$. On dit que u est cyclique s'il existe $x \in E$ tel que

$$(x, u(x), ..., u^{n-1}(x)) \text{ est une base de } E$$

Théorème 3

Soient E un $\mathbb{K}$-espace vectoriel de dimension n et $u \in \mathcal{L}(E)$. Les propriétés suivantes sont équivalentes :

1. *u est cyclique.*
2. *$(-1)^n P_u = \pi_u$*
3. *π_u est de degré n.*
4. *Il existe une base de E dans laquelle la matrice de E est une matrice compagnon.*
5. *$dim(\mathbb{K}[u]) = n$.*

Démonstration : Objectif Agrégation, proposition 4.64p175 ■

2.2 Sur l'orthogonalité dans le dual

Référence : Gourdon, page 128

Définition 3

Si $B \subset E^*$, on note $B^\circ = \{x \in E / \forall \varphi \in B, \varphi(x) = 0\}$. L'ensemble B° est un sev de E appelé orthogonal de B.

Théorème 4

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Alors si G est un sev de E^*, on a :

$$dim(G) + dim(G^\circ = dim(E)$$