## I.C Réduction de Frobenius

**Lemme 3: Noyaux itérés**

Soit $u$ un endomorphisme. La suite $\left(\ker(P^k(u))\right)_k$ est strictement croissante puis stationnaire.

*Démonstration.* Soit $k$ le premier entier tel que $\ker(P^k(u)) = \ker(P^{k+1}(u))$ (un tel cas existe car on est en dimension finie).
Montrons par récurrence que la suite stationne à partir de ce rang.

<u>*Initialisation :*</u> pour $n = 1$ c'est l'hypothèse

<u>*Hérédité :*</u> Soit $n \geqslant 1$, supposons la propriété vraie au rang $n$, c'est-à-dire : $\ker(P^k(u)) = \ker(P^{k+n}(u))$. Soit $x \in \ker(P^{k+n+1}(u))$. Alors $P^{k+n+1}(u)(x) = P^{k+n}(P(u)(x))$. Donc $P(u)(x) \in \ker(P^{k+n}(u)) = \ker(P^k(u))$ c'est-à-dire $u \in \ker(P^{k+1}(u)) = \ker(P^k(u))$. On a donc :

$$\ker(P^k(u)) \subset \ker(P^{k+n+1}(u)) \subset \ker(P^k(u))$$

et ceci conclut la preuve du lemme. ■

**Proposition 4**

Soit $u$ un endomorphisme. Alors il existe $x \in E$ tel que $\mu_{u,x} = \mu_u$.

*Démonstration.* On écrit $\mu_u = \prod_{k=1}^r P_k^{\alpha_k}$ comme produit d'irréductibles distincts et on prend $x_k \in \ker(P_k^{\alpha_k}) \backslash \ker(P_k^{\alpha_k - 1})$. On notera que $x_k$ est bien défini par minimalié de $\mu_u$. Alors en prenant $x = x_1 + \cdots + x_r$, on obtient : $\mu_{u,x} = \prod_{k=1}^r P_k^{\alpha_k} = \mu_u$. ■

**Lemme 5:**

Soit $u \in \mathcal{L}(E)$. Soit $x \in E$ tel que $\mu_{u,x} = \mu_u$, alors $E_{u,x} := \{P(u)(x) \ / \ P \in \mathbb{K}[X]\}$ (le plus petit sous-espace stable par $u$ contenant $x$) admet un supplémentaire stable

*Démonstration.* Notons $p$ la dimension de $E_{u,x}$.
On pose :

$$e_1 = x, e_2 = u(x), \ldots, e_p = u^{p-1}(x).$$

Alors $(e_1, \ldots, e_p)$ forme une base de $E_{u,x}$ car $\deg(\mu_{u,x}) = \deg(\mu_u) = p$ et la famille ainsi créée est stable par $u$.

On complète $(e_1, \ldots, e_p)$ en une base $(e_1, \ldots, e_n)$ de $E$ et on considère la base duale $(e_1^*, \ldots, e_n^*)$. On définit $F = \cap_{j=0}^{+\infty} \ker(e_p^* \circ u^j)$. On a immédiatement que $F$ est stable par $u$.

Montrons $F \oplus E_{u,x} = E$ :

— $F \cap E_{u,x} = \{0\}$ :
Si $y \in F \cap E_{u,x}$, alors il s'écrit :

$$y = \sum_{j=0}^{p-1} a_j e_{j+1} = \sum_{j=0}^{p-1} a_j u^j(x) \in E_{u,x}$$

De plus $y \in F$ donc pour tout $j$ :

$$e_p^* \circ u^j(y) = 0 \quad \Longleftrightarrow \quad \sum_{k=0}^{p-1} a_j e_p^* \left(u^{k+j}(x)\right) = 0$$

Pour $j = 0$ on obtient donc $a_{p-1} = 0$, puis pour $j = 1$ on a $a_{p-2} = 0$, etc et finalement $y = 0$.

— $\dim F + \dim G = n$ :
On a $\dim(E_{u,x}) = \deg(\mu_{u,x}) = \deg(\mu_u) = p$. Donc $F = \cap_{j=0}^{p-1} \ker(e_p^* \circ u^j)$. La famille $(e_p^* \circ u^0, \dots, e_p^* \circ u^{p-1}$ est libre car si :

$$\sum_{j=0}^{p-1} a_j e_p^* \circ u^j = 0_{E*}$$

alors en évaluant sur la famille $\big(x, u(x), \dots, u^{p-1}(x)\big)$, on obtient $a_j = 0$ pour tout $j$, puis la famille est libre.
On a donc que $F$ est intersection de $p$ hyperplans associés à des formes linéaires indépendantes.
On a donc que $F$ est de codimension $p$.

Par argument de dimension on a donc finalement :

$$E_{u,x} \oplus F = E.$$

Et $E_{u,x}$ admet donc un supplémentaire stable. ■

**Théorème 6: Réduction de Frobenius**

Soit $E$ un $\mathbb{K}$-espace vectoriel de dimension finie $n$.
Soit $u \in \mathcal{L}(E)$.
Alors il existe une unique suite finie $(P_1, \dots, P_r)$ de polynômes unitaires et une unique décomposition $E = \bigoplus_{i=1}^{r} E_i$ telle que $\forall i \in [\![1, \dots, r-1]\!] \quad P_{i+1}|P_i$ et $\forall i \in [\![1, \dots, r-1]\!] \quad u_{|E_i}$ est un endomorphisme cyclique de polynôme minimal de $P_i$.

*Démonstration.* La forme matricielle obtenue se déduit immédiatement du lemme.

— ***Existence*** : On procède par récurrence sur la dimension de $E$.

*Initialisation :* si $\dim(E) = 1$ alors il n'y a rien à faire.

*Hérédité :* soit $n \in \mathbb{N}^*$. Soit $E$ un espace vectoriel de dimension $n+1$. Supposons la proposition vraie jusqu'au rang $n$.
Soit $x \in E$ tel que $\mu_u = \mu_{u,x}$.
On pose $E_1 = E_{u,x}$. Alors $u$ est cyclique sur $E_1$. Soit $F$ un supplémentaire de $E_1$ stable par $u$.
On a $\mu_1 = \mu_{u,x} = P_1$.

Par hypothèse de récurrence, il existe alors $P2, \dots, P_r$ telle que $F = \bigoplus_{i=2}^{r} E_i$ et $P_{i+1}|P_i$ pour tout $i \in [\![2, r-1]\!]$ et $P_2|\mu_u$ car comme $\mu_u(u_{|F}) = 0$ alors $\mu_{u_{|F}}|\mu_u$.

On a alors que la décomposition : $E = \bigoplus_{i=1}^{r} E_i$ vérifie les conditions.

— ***Unicité*** : soient $(P_1, \dots, P_r)$ et $(Q_1, \dots, Q_s)$ deux familles de polynômes associées à deux décompositions $E = \bigoplus_{i=1}^{r} E_i$ et $E = \bigoplus_{i=1}^{s} F_i$.
Par construction on a $P_1 = Q_1 = \mu_u$ et

$$\sum_{i=1}^{r} \deg(P_i) = \sum_{i=1}^{r} \dim(E_i) = \dim(E) = \sum_{i=1}^{s} \deg(F_i) = \sum_{i=1}^{s} \deg(Q_i)$$

La première et la dernière égalités proviennent de la cyclicité de $u$ sur chacun des sous-espaces.

Supposons que ces deux réductions soient distinctes. On remarquera que lon ne peut pas avoir l'égalité de tous les polynômes mais $r \neq s$.
On note $j$ l'indice minimal tel que $P_i \neq Q_i$.

Pour tout $i \geqslant j$, on a $P_i | P_j$ et $Q_i | Q_j$ et on a donc $P_j(u_{|E_i}) = 0$.
Puis $P_j(u)(E) = \bigoplus_{i=1}^{r} P_j(u)(E_i) = \bigoplus_{i=1}^{j-1} P_j(u)(E_i)$. Or

$$P_j(u)(E) = \bigoplus_{i=1}^{r} P_j(u)(F_i) = \bigoplus_{i=1}^{r} P_j(u)(E_i).$$

Donc en regardant les dimensions, on obtient :

$$\forall j \leqslant i \leqslant s \qquad \dim(P_j(u)(F_i)) = 0.$$

En effet, on a :

$$\forall i < j \qquad \dim\left(P_j(u)(E_i)\right) = \mathrm{rg}(P_j(u_{E_i})) = \mathrm{rg}(P_j(u_{F_i})) = \dim\left(P_j(u)(F_i)\right)$$

car les deux endomorphismes sont cycliques et de même polynôme minimal par minimalité de $j$.
Cela entraîne :

$$\forall j \leqslant i \leqslant s \quad P_j(u_{|F_i}) = 0$$

D'où :

$$P_j(u_{|F_j}) = 0$$

On obtient alors que $P_j$ annule $u_{|F_j}$ et donc $\mu_{u_{|F_j}} = Q_j | P_j$.

Par symétrie des rôles de $P$ et $Q$, on a $P_j | Q_j$. Ils sont donc associés et comme ils sont unitaires, ils sont égaux. C'est absurde.

■

**Détails supplémentaires**

**Remarque 7**

Si $p = \deg(\mu_u)$, alors $\mathbb{K}[u] := \{P(u) \mid P \in \mathbb{K}[X]\}$ est un sev de $\mathcal{L}(E)$ de dimension $p$, dont une base est $(\mathrm{Id}_E, u, \dots, u^{k-1})$.

Si $l = \deg(P_x)$ (polynôme minimal local en $x$) alors $E_x$ est un sev de $E$ de dimension $l$, dont une base est $(x, \dots, u^{l-1}(x))$.

*Démonstration.*

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow \mathcal{L}(E) \\ P &\longmapsto P(u) \end{aligned}$$

est linéaire, $\mathrm{Im}\,\varphi = \mathcal{L}_u$.

$$\ker \varphi = \{P \in \mathbb{K}[X] \ / \ P(u) = 0\} = (\pi_u)$$

Donc

$$\mathcal{L}_u \cong \mathbb{K}[X]/(\pi_u)$$

dont une base est $(1, X, \dots, X^{k-1})$

Idem avec

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow E \\ P &\longmapsto P(u)(x) \end{aligned}$$

■