Développement. Théorème de réduction de Frobenius

On considère un corps $\mathbf{K}$ et un $\mathbf{K}$-espace vectoriel E de dimension finie $n \in \mathbf{N}^*$. Soit $f \in \mathscr{L}(E)$ un endomorphisme. Soit $\pi \in \mathbf{K}[X]$ son polynôme minimal. Pour tout vecteur $x \in E$, on considère le générateur unitaire $\pi_x \in \mathbf{K}[X]$ de l'idéal

$$\{P \in \mathbf{K}[X] \mid P(f)(x) = 0\} \subset \mathbf{K}[X]$$

Lemme 1. Il existe un vecteur $x \in E$ tel que $\pi = \pi_x$.

Preuve • *Un cas particulier.* On suppose qu'on peut écrire le polynôme minimal sous la forme $\pi = P^r$ pour un polynôme irréductible $P \in \mathbf{K}[X]$. Alors pour tout vecteur $x \in E$, comme $\pi_x \mid \pi$, il existe un entier $r_x \leqslant r$ tel que $\pi_x = P^{r_x}$. Montrons qu'il existe un vecteur $x \in E$ tel que $r = r_x$. Raisonnons par l'absurde et supposons le contraire. Pour tout vecteur $x \in E$, cela implique que $\pi_x \mid P^{r-1}$, donc $P^{r-1}(f)(x) = 0$, donc $P^{r-1}(f) = 0$ ce qui est impossible par minimalité du polynôme minimal.

• *Cas général.* On décompose le polynôme π en produit $P_1^{r_1} \cdots P_s^{r_s}$ de polynômes irréductibles. Le lemme des noyaux donne alors

$$E = E_1 \oplus \cdots \oplus E_s \quad \text{avec} \quad E_i \coloneqq \operatorname{Ker} P_i^{r_i}(f). \tag{1}$$

Soit $i \in [\![1, s]\!]$. Alors le polynôme minimal de l'endomorphisme induit $f|_{E_i}$ est le polynôme $\pi_i \coloneqq P_i^{r_i}$ qui s'écrit donc sous la forme π_{i,x_i} avec $x_i \in E_i$ d'après le cas particulier. Posons $x \coloneqq x_1 + \cdots + x_s$. Montrons que $\pi = \pi_x$. Comme $\pi_x \mid \pi$, il suffit de montrer que $\pi \mid \pi_x$. On peut écrire

$$0 = \pi_x(f)(x) = \pi_x(f)(x_1) + \cdots + \pi_x(f)(x_s).$$

Grâce à la décomposition (1), pour tout indice $i \in [\![1, s]\!]$, on obtient $\pi_x(f)(x_i) = 0$, donc $\pi_{i,x_i} \mid \pi_x$. Or $\pi_{i,x_i} = \pi_i = P_i^{r_i}$, donc $P_i^{r_i} \mid \pi_x$. Comme les polynômes P_i sont premiers entre eux, on en déduit $\pi \mid \pi_x$ ce qui conclut. ◁

Théorème 2. Il existe des sous-espaces vectoriels $F_1, \ldots, F_r \in E$ tels que

(i) on ait $E = F_1 \oplus \cdots \oplus F_r$;
(ii) pour tout indice $i \in [\![1, r]\!]$, le sous-espace vectoriel F_i soit stable par l'endomorphisme f et l'endomorphisme induit $f|_{F_i} \colon F_i \longrightarrow F_i$ soit cyclique de polynôme minimal $P_i \in \mathbf{K}[X]$.
(iii) on ait $P_r \mid \cdots \mid P_1$.

Preuve Montrons l'existence. On note $k \coloneqq \deg \pi$. D'après le lemme, il existe un vecteur $x \in E$ tel que $\pi = \pi_x$. Le sous-espace vectoriel $F \coloneqq \{P(f)(x) \mid P \in \mathbf{K}[X]\}$ est stable par l'endomorphisme f dont une base est la famille $(x, f(x), \ldots, f^{k-1}(x))$ puisque $k = \deg \pi_x$. Complétons cette famille $(e_1, \ldots, e_n)$ en une base de l'espace E. Considérons le sous-espace vectoriel $G \coloneqq \Gamma^\circ$ avec $\Gamma \coloneqq \{e_k^* \circ f^i \mid i \in \mathbf{N}\} \subset E^*$ qui est stable par l'endomorphisme f. On souhaite montrer que $E = F \oplus G$.

Montrons que $F \cap G = \{0\}$. Soit $y \in F \cap G$. Comme $y \in F$, on peut l'écrire sous la forme $y = y_0 x + \cdots + y_{k-1} f^{k-1}(x)$ avec $y_i \in \mathbf{K}$. Comme $y \in G$, on a $e_k^*(y) = 0$, c'est-à-dire $y_{k-1} = 0$. De même, comme $e_k^* \circ f(y) = 0$, on trouve $y_{k-2} = 0$. Ainsi de suite, on montre que le vecteur y est nul.

Montrons que $\dim F + \dim G = \dim E$. Comme $\dim G + \dim(\operatorname{Vect} \Gamma) = \dim E$, il suffit de montrer que $\dim(\operatorname{Vect} \Gamma) = k$. Considérons l'application linéaire

$$\begin{vmatrix} \mathbf{K}[f] \longrightarrow \operatorname{Vect} \Gamma, \\ g \longmapsto e_k^* \circ g \end{vmatrix}$$

et montrons qu'elle est un isomorphisme. Par définition de l'ensemble Γ, elle est surjective. Pour l'injectivité, avec le même argument que précédemment et le fait que la famille $(\mathrm{Id}_E, f, \ldots, f^{k-1})$ est une base de l'algèbre $\mathbf{K}[f]$ puisque $k = \deg \pi$, son noyau est nul. Cette isomorphie permet d'écrire que le sous-espace vectoriel $\operatorname{Vect} \Gamma$ est de dimension $k = \dim \mathbf{K}[f]$.

Finalement, on a trouvé un sous-espace vectoriel G qui est stable par l'endomorphisme f et qui vérifie $E = F \oplus G$. Soient $P_1, P_2 \in \mathbf{K}[X]$ les polynômes minimaux des endomorphismes induits $f|_F$ et $f|_G$. La construction ainsi faite assure $P_1 = \pi_x = \pi$ et la stabilité du sous-espace vectoriel G donne $P_2 \mid \pi$, donc $P_2 \mid P_1$. Pour conclure, on raisonne par récurrence sur la dimension de l'espace E en appliquant l'hypothèse de récurrence à l'endomorphisme $f|_G$.

Montrons l'unicité. Soient $G_1, \ldots, G_s \subset E$ des sous-espaces vectoriels vérifiant le théorème associés aux polynômes $Q_1, \ldots, Q_s \in \mathbf{K}[X]$. La construction donne $P_1 = Q_1$. Raisonnons par l'absurde et supposons que $(P_1, \ldots, P_r) \neq (Q_1, \ldots, Q_s)$. Considérons le plus petit indice $j \in [\![1, \min(r, s)]\!]$ tel que $P_j \neq Q_j$. Ce dernier existe puisque, comme les polynômes minimal et caractéristique d'un endomorphisme cyclique sont égaux, on trouve $\sum_{i=1}^r \deg P_i = n = \sum_{i=1}^s Q_i$. Comme $E = F_1 \oplus \cdots \oplus F_r$ et $P_j(f)(F_k) = \{0\}$ lorsque $k \geqslant j$ puisque $P_k \mid P_j$, on obtient

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

Comme $E = G_1 \oplus \ldots G_s$, on a aussi

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

Pour tout indice $i \in [\![1, j-1]\!]$, il existe deux bases dans lesquelles les matrices des endomorphismes cycliques $f|_{F_i}$ et $f|_{G_i}$ sont les compagnes du polynôme $P_i = Q_i$, donc ces deux endomorphismes sont semblables ce qui montre

$$\dim P_j(f)(F_i) = \dim P_j(f)(G_i), \qquad i \in [\![1, j-1]\!].$$

Avec les égalités (2) et (3), pour tout indice $i \in [\![j, s]\!]$, on en déduit $\dim P_j(f)(G_i) = 0$, c'est-à-dire $P_j(f)(G_i) = \{0\}$ ce qui montre $Q_j \mid P_j$. Par symétrie, on trouve $P_j = Q_j$ ce qui contredit la définition de l'indice j. D'où $(P_1, \ldots, P_r) = (Q_1, \ldots, Q_s)$. ◁

[1] Xavier Gourdon. *Algèbre.* 2e édition. Ellipses, 2009.