Théorème de Frobenius

Lemme . Soit $u \in \mathscr{L}(E)$ avec E un espace vectoriel de dimension finie. On note Π_u le polynôme minimal de u et Π_u^x le polynôme unitaire qui engendre l'idéal

$$\{P \in \mathbb{K}[X] \ ; \ P(u)(x) = 0\}.$$

Alors il existe $x \in E$ tel que $\Pi_u^x = \Pi_u$.

Preuve :
On commence par traiter le cas où $\Pi_u = P^\alpha$ avec P un polynôme irréductible. On a

$$\forall x \in E, \exists n \in [\![0, \alpha]\!], \ P^n(u)(x) = 0,$$

et on cherche $x \in E$ tel que $P^n(u)(x) \neq 0$ pour $n < \alpha$. Supposons par l'absurde que pour tout $x \in E$, il existe $n < \alpha$ tel que $P^n(u)(x) = 0$. Alors $P^{\alpha-1}(u) = 0$, c'est-à-dire Π_u divise $P^{\alpha-1}$ ce qui est absurde.

Dans le cas général, on considère $\Pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$ la décomposition en facteurs irréductibles de Π_u dans $\mathbb{K}[X]$. D'après le lemme des noyaux, on a

$$E = \bigoplus_{i=1}^{r} \mathrm{Ker}\Big(P_i^{\alpha_i}(u)\Big).$$

On note $E_i := \mathrm{Ker}\Big(P_i^{\alpha_i}(u)\Big)$. On sait par ce qui précède que pour tout $i \in [\![1, r]\!]$, il existe $x_i \in E_i$ tel que $\Pi_{u_{E_i}}^{x_i} = \Pi_{u_{E_i}}$. On pose $x = x_1 + \ldots + x_r$ et on montre que $\Pi_u^x = \Pi_u$.
Comme Π_u^x divise Π_u, il suffit de montrer que Π_u divise Π_u^x, c'est-à-dire que Π_u^x est un polynôme annulateur de u. On a

$$0 = \Pi_u^x(u)(x) = \sum_{i=1}^{r} \Pi_u^x(u)(x_i).$$

Comme les E_i sont en somme directe et stable par u, on en déduit que $\Pi_u^x(u)(x_i) = 0$ pour tout i. Donc

$$\Pi_{u_{E_i}}^{x_i} = \Pi_{u_{E_i}} \text{ divise } \Pi_u^x.$$

Ainsi $\Pi_u^x(u)$ est nul sur chaque E_i et donc sur E, d'où le résultat.

□

Théorème . Soit $u \in \mathscr{L}(E)$ avec E un espace vectoriel de dimension finie n. Alors il existe une suite $F_1, \ldots, F_r$ de sous-espaces vectoriels de E stables par u telle que

- $E = F_1 \oplus \ldots \oplus F_r$.
- Pour tout $i \in [\![1, r]\!]$, $u_i := u|_{F_i}$ est un endomorphisme cyclique de F_i.
- En notant P_i le polynôme minimal de u_i, on a $P_{i+1} | P_i$ pour tout $i \in [\![1, r-1]\!]$.

La suite de polynôme $(P_i)_i$ ne dépend que de u et non du choix de la décomposition. On

appelle cette suite les invariants de similitude de u.

Preuve :
On commence par étudier l'existence de la décomposition annoncée. Pour cela, on construit une décomposition de l'espace, à l'aide de la dualité, pour descendre la dimension et raisonner par récurrence. On note $d = \deg(\Pi_u)$ et soit $x \in E$ tel que $\Pi_u^x = \Pi_u$. On pose

$$F := \{\ P(u)(x)\ ;\ P \in \mathbb{K}[X]\ \},$$

qui est de dimension d car $F \simeq {}^{\mathbb{K}[X]}/_{(\Pi_u^x)}$. La famille $e_i := u^i(x)$ pour $i \in [\![0, d-1]\!]$ forme une base de F. On peut la compléter en une base $(e_0, \dots, e_{n-1})$ de E et on note $(e_0^*, \dots, e_{n-1}^*)$ sa base duale associée. On pose alors

$$G := \Big\{x \in E\ ;\ \forall i \in \mathbb{N}, \Big(e_{d-1}^* \circ u^i\Big)(x) = 0\Big\},$$

et on montre que $E = F \oplus G$.

Soit $y \in F \cap G$. Si y est non nul, alors on peut l'écrire $y = a_0 e_0 + \ldots + a_p e_p$ dans la base de F avec $a_p \neq 0$ et $p \leq d-1$. On compose alors par $e_{d-1}^* \circ u^{d-1-p}$ ce qui donne

$$a_p = e_{d-1}^*\Big(a_0 e_{d-1-p} + \ldots + a_p e_{d-1}\Big) = 0.$$

C'est absurde, donc F est G sont en somme directe.
On a défini G comme l'orthogonal de $\Gamma := \{e_{d-1}^* \circ u^i\ ;\ i \in \mathbb{N}\}$, il suffit donc de montrer que $\dim(\mathrm{Vect}(\Gamma)) = d$ pour conclure. On pose

$$\begin{array}{rccc} \varphi : & \mathbb{K}[u] & \to & \mathrm{Vect}(\Gamma) \\ & P(u) & \mapsto & e_{d-1}^* \circ P(u) \end{array},$$

qui est bien définie et surjective. Elle est de plus injective. En effet, si $e_{d-1}^* \circ v = 0$ avec $v \neq 0$, alors on peut l'écrire $v = a_0 Id_E + a_1 u + \ldots + a_p u^p$ avec $p \leq d-1$ et $a_p \neq 0$. On a alors

$$a_p = e_{d-1}^*\Big(a_0 e_{d-1-p} + \ldots + a_p e_{d-1}\Big) = \Big(e_{d-1}^* \circ v\Big)(u^{d-1-p}(x)) = 0$$

en composant par $e_{d-1}^* \circ v$, ce qui est absurde. On en déduit que φ est bijective, et donc que $\dim(\mathrm{Vect}(\Gamma)) = d$.

On a alors $E = F \oplus G$ avec F et G stable par u. De plus, le polynôme minimal de $u|_F$ est le même que u, et G étant stable par u on a aussi $\Pi_{u|_G} \Big| \Pi_u = \Pi_{u|_F}$. Si $F = E$, on a le résultat, sinon en appliquant le même raisonnement à $u|_G$, on obtient la décomposition voulue par récurrence car E est de dimension finie.

Pour l'unicité, on considère deux suites $F_1, \dots, F_r$ et $G_1, \dots, G_s$ qui vérifient les conditions du théorème et on note $P_i = \Pi_{u|_{F_i}}$ et $Q_i = \Pi_{u|_{G_i}}$. On sait que $P_1 = \Pi_u = Q_1$. Soit j le premier indice tel que $P_j \neq Q_j$, qui existe toujours car $n = \sum_{i=1}^{r} \deg(P_i) = \sum_{i=1}^{s} \deg(Q_i)$.
Comme $E = F_1 \oplus \ldots \oplus F_r = G_1 \oplus \ldots \oplus G_s$, on a

$$P_j(u)(E) = P_j(u)(F_1) \oplus \ldots \oplus P_j(u)(F_{j-1}),$$

car $P_j(u)$ est nul sur F_i pour $i \geq j$, et

$$P_j(u)(E) = P_j(u)(G_1) \oplus \ldots \oplus P_j(u)(G_j) \oplus \ldots \oplus P_j(u)(G_s).$$

Or $P_i = Q_i$ pour $1 \leq i \leq j-1$ donc on a, en passant par les matrices compagnons dans des bonnes bases,

$$\dim\Big(P_j(u)(F_i)\Big) = \mathrm{rg}\Big(P_j(C(P_i))\Big) = \mathrm{rg}\Big(P_j(C(Q_i))\Big) = \dim\Big(P_j(u)(G_i)\Big),$$

ce qui donne en passant au dimension dans l'égalité précédente $\dim\Big(P_j(u)(G_i)\Big) = 0$ pour $i \geq j$, ie $Q_i | P_j$. En particulier, on a $Q_j | P_j$. On peut faire le même raisonnement en inversant P et Q, donc $Q_j = P_j$, ce qui est absurde. Donc $r = s$ et $(P_1, \ldots, P_r) = (Q_1, \ldots, Q_r)$.

□