Théorème de Frobenius

Lemme 1. Soit $u \in \mathcal{L}(E)$. Notons π_u^x le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X],\ P(u)(x) = 0\}$. Il existe $x \in E$ tel que $\pi_u^x = \pi_u$.

Démonstration. Supposons dans un premier temps π_u de la forme P^α, avec P irréductible. Si, par l'absurde, pour tout $x \in E$, il existe $n < \alpha$ tel que $P^n(u)(x) = 0$, alors $P^{\alpha-1}(u) = 0$, ce qui contredit la minimalité de π_u.
Écrivons maintenant $\pi_u = \Pi P_i^{\alpha_i}$. Par lemme des noyaux :

$$E = \bigoplus_{i=1}^{r} \ker(P_i^{\alpha_i}(u)) := \bigoplus_{i=1}^{r} E_i.$$

Par ce qui précède, pour $i \in \{1, \dots, r\}$, il existe $x_i \in E \subset E$ tel que $\pi_{uE_i} = \pi_{uE_i}^{x_i}$. Posons $x = x_1 + \cdots + x_r$.

$$0 = \pi_u^x(u)(x) = \sum_{i=1}^{r} \pi_u^x(u)(x_i) \in \bigoplus_{i=1}^{r} E_i$$

car les espaces E_i sont u-stables. Donc $\pi_u^x(u)(x_i) = 0$. Par minimalité, $\pi_{uE_i} = \pi_{uE_i}^{x_i}$ divise π_u^x. En particulier, $\pi_u^x(u)$ est nul sur chaque E_i, donc sur E. Ainsi π_u divise π_u^x, puis $\pi_u = \pi_u^x$. □

Théorème 2. Soit $u \in \mathcal{L}(E)$. Il existe des espaces $F_1, \dots, F_r$ u-stables tels que :

(i) $E = F_1 \oplus \cdots \oplus F_r$,

(ii) $\forall i \in \{1, \dots, r\},\ u_i = u_{F_i}$ est cyclique,

(iii) $\pi_{u_{i+1}} | \pi_{u_i}$.

De plus, la suite de polynômes (π_{u_i}) ne dépend que de u.

Démonstration. Soit $x \in E$ tel que $\pi_u^x = \pi_u$. Soit $F = \{P(u)(x),\ P \in \mathbb{K}[X]\}$, de dimension $d = \deg \pi_u$. La famille $(e_i = u^i(x))_{0 \le i \le d-1}$ forme une base de F, que l'on complète en $(e_0, \dots, e_{n-1})$ base de E. Posons (e_i^*) la base duale associée et $G = \Gamma^o = \{x \in E,\ \forall i \in \mathbb{N},\ e_{d-1}^* \circ u^i(x) = 0\}$, avec $\Gamma = \{e_{d-1}^* \circ u^i,\ i \in \mathbb{N}\}$.

Fait. L'espace E est somme directe de F et G ci-dessus.

Soit $y = a_0 e_0 + \cdots + a_p e_p \in F \cap G \backslash \{0\}$ avec $a_p \neq 0$ et $p \le d-1$.

$$a_p = e_{d-1}^* \circ u^{d-1-p}(y) = 0$$

ce qui est absurde, donc $F \cap G = \{0\}$. Posons maintenant $\varphi : P(u) \in \mathbb{K}[u] \mapsto e_{d-1}^* \circ P(u) \in Vect\Gamma$, bien définie et surjective. De plus, pour $v = a_0 e_0 + \cdots + a_p e_p \in \ker \varphi$, alors $a_p = e_{d-1}^* \circ v(u^{d-1-p}(x)) = 0$, ce qui assure que φ est injective. Ainsi, $\dim Vect\Gamma = d$, donc $E = F \oplus G$.
De plus, F et G sont u-stables et $\pi_u = \pi_u^x = \pi_{u_F}$ par définition, et $\pi_{u_G} | \pi_u = \pi_{u_F}$. Si $F = E$, c'est terminé, sinon on itère le raisonnement sur G.
Si $(F_1, \dots, F_r)$ et $(G_1, \dots, G_s)$ conviennent, notons $P_i = \pi_{u_{F_i}}$ et $Q_j = \pi_{u_{G_j}}$. Par la chaîne de divisibilité, $P_1 = \pi_u = Q_1$.

Notons k le premier indice tel que $P_k \neq Q_k$. Puisque $P_k(u) = 0$ sur F_l pour $l \ge k$, par décomposition de E,

$$P_k(u)(E) = P_k(u)(F_1) \oplus \cdots \oplus P_k(u)(F_{k-1}) = P_k(u)(G_1) \oplus \cdots \oplus P_k(u)(G_s).$$

En exploitant $P_i = Q_i$ pour $1 \le i \le k-1$,

$$\dim P_k(u)(F_i) = rg(P_k[C(P_i)]) = rg(P_k[C(Q_i)]) = \dim P_k(u)(G_i).$$

De là, $\dim P_k(u)(G_i) = 0$ pour $i \ge k$, ce qui entraîne en particulier $Q_k | P_k$. Par symétrie des rôles, on obtient $P_k = Q_k$, ce qui est absurde. D'où l'unicité. □