

DM 14 - Décomposition de Frobenius

On désigne par E un espace vectoriel de dimension finie $n \in \mathbb{N}^*$ sur un corps $\mathbb{K}$ et par u un endomorphisme de E . On rappelle que u^0 désigne id_E . Pour tout $P = \sum_{k=0}^d a_k X^k \in \mathbb{K}[X]$, on note $P(u)$ l'endomorphisme

de E défini par $P(u) = \sum_{k=0}^d a_k u^k$.

On vérifie aisément que l'application $P \in \mathbb{K}[X] \mapsto P(u) \in \mathcal{L}(E)$ est une application linéaire et un morphisme d'anneaux. En particulier, $\forall (P, Q) \in \mathbb{K}[X]^2$, $(PQ)(u) = P(u) \circ Q(u) = Q(u) \circ P(u)$.

1 Sous-espaces cycliques

Soit $x \in E \setminus \{0\}$.

1. (a) Montrer que la famille $(x, u(x), \dots, u^n(x))$ est liée. Justifier l'existence de l'entier

$$n_x = \max \left\{ k \in \mathbb{N}^* \mid (x, u(x), \dots, u^{k-1}(x)) \text{ est libre} \right\}.$$

- (b) Montrer qu'il existe $a_0, \dots, a_{n_x-1} \in \mathbb{K}$ tels que

$$u^{n_x}(x) = a_{n_x-1} u^{n_x-1}(x) + \dots + a_1 u(x) + a_0 x.$$

- (c) Montrer que pour tout $k \geq n_x$, $u^k(x) \in \text{Vect}(x, u(x), \dots, u^{n_x-1}(x))$.

On note $E_x = \text{Vect}(x, u(x), \dots, u^{n_x-1}(x))$. C'est le *sous-espace cyclique* engendré par x .

2. (a) Déterminer la dimension de E_x .
 (b) Montrer que $E_x = \text{Vect}(\{u^k(x), k \in \mathbb{N}\}) = \{P(u)(x), P \in \mathbb{K}[X]\}$.
 (c) Montrer que E_x est stable par u .

3. L'exemple des projecteurs.

- (a) On suppose que u est un projecteur. Que vaut E_x ?
 (b) Exprimer la dimension de E_x en fonction de x et des sous-espaces $\text{Ker } u$ et $\text{Im } u$.

4. On reprend les notations de la question 1.(b). Montrer que

$$\forall y \in E_x, u^{n_x}(y) = a_{n_x-1} u^{n_x-1}(y) + \dots + a_1 u(y) + a_0 y.$$

Le but du problème est de montrer qu'il existe $x_1, \dots, x_r \in E - \{0\}$ tels que $E = \bigoplus_{i=1}^r E_{x_i}$.

C'est une *décomposition de Frobenius* de u .

2 Vecteur u -maximum

5. Soit $P \in \mathbb{K}[X]$. Montrer que $\text{Ker}(P(u))$ est stable par u .

6. **Polynôme minimal.**

- (a) Montrer qu'il existe un polynôme $P \in \mathbb{K}[X]$ non nul tel que $P(u) = 0$.
- (b) Montrer qu'il existe un unique polynôme unitaire $\Pi_u \in \mathbb{K}[X]$ tel que:

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

Ce polynôme Π_u est le *polynôme minimal* de u .

- (c) On suppose u nilpotent d'indice p : $u^p = 0$, mais $u^{p-1} \neq 0$.
Déterminer le polynôme minimal de u .

7. **Lemme des noyaux.**

- (a) Soient $P, Q \in \mathbb{K}[X]$ premiers entre eux. Montrer que:

$$\text{Ker}((PQ)(u)) = \text{Ker}(P(u)) \oplus \text{Ker}(Q(u)).$$

- (b) Soient $P_1, \dots, P_r \in \mathbb{K}[X]$ premiers entre eux deux à deux. Montrer que:

$$\text{Ker}((P_1 \dots P_r)(u)) = \bigoplus_{i=1}^r \text{Ker}(P_i(u)).$$

8. On écrit $\Pi_u = P_1^{m_1} \dots P_r^{m_r}$ pour la décomposition en produit d'irréductibles unitaires deux à deux distincts de Π_u . Déterminer r sous-espaces vectoriels non nuls $E_1, \dots, E_r$ stables par u , distincts de $\{0\}$ et tels que $E = \bigoplus_{i=1}^r E_i$.

9. **Polynôme minimal ponctuel.**

- (a) Soit $x \in E - \{0\}$. Considérons $\mathcal{J}_x = \{P \in \mathbb{K}[X] \mid P(u)(x) = 0_E\}$.
Montrer qu'il existe un unique polynôme unitaire non nul $\Pi_{u,x}$ tel que $\mathcal{J}_x = \Pi_{u,x} \mathbb{K}[X]$.
- (b) On reprend les notations de la partie 1 : soit n_x défini comme dans la question 1 et $a_0, \dots, a_{n_x-1} \in \mathbb{K}$ tels que $u^{n_x}(x) = a_{n_x-1} u^{n_x-1}(x) + \dots + a_1 u(x) + a_0 x$. Que vaut $\Pi_{u,x}$?
- (c) Montrer que $\Pi_{u,x}$ divise Π_u .

On cherche à démontrer qu'il existe $x \in E$ tel que $\Pi_{u,x} = \Pi_u$. Un tel x est un vecteur *u -maximum*.

- 10. On suppose dans cette question que $\Pi_u = P^m$, avec P irréductible et $m \in \mathbb{N}^*$. Soit $(e_1, \dots, e_n)$ une base de E .
 - (a) Montrer que pour tout $i \in \llbracket 1, n \rrbracket$, il existe $m_i \in \mathbb{N}^*$ tel que $m_i \leq m$ et $\Pi_{u,e_i} = P^{m_i}$.
 - (b) En déduire qu'il existe $i \in \llbracket 1, n \rrbracket$ tel que $\Pi_{u,e_i} = \Pi_u$.
- 11. On suppose que la décomposition en produit d'irréductibles de Π_u s'écrit $\Pi_u = P_1^{m_1} \dots P_r^{m_r}$. Montrer qu'il existe $x \in E - \{0\}$ tel que $\Pi_{u,x} = \Pi_u$.

3 Décomposition de Frobenius

On peut donc trouver $x \in E - \{0\}$ tel que $\Pi_{u,x} = \Pi_u$. On note $p = n_x = \deg \Pi_{u,x}$.

12. Montrer qu'il existe $\varphi \in E^*$ telle que $\varphi(u^{p-1}(x)) = 1$ et $\forall i \in \llbracket 0, p-2 \rrbracket, \varphi(u^i(x)) = 0$.

On pose $F = \bigcap_{i=0}^{p-1} \text{Ker}(\varphi \circ u^i)$.

13. Montrer que F est un supplémentaire de E_x .

14. Montrer que F est stable par u .

15. En déduire qu'il existe $x_1, \dots, x_r \in E - \{0\}$ tels que $E = \bigoplus_{i=1}^r E_{x_i}$ et $\forall i \in \llbracket 1, r-1 \rrbracket, \Pi_{u,x_{i+1}} \mid \Pi_{u,x_i}^1$.

¹On peut montrer que les polynômes ainsi construits ne dépendent pas du choix des x_i . Ce sont les *facteurs invariants* de u ; ils jouent un rôle important dans les questions de réduction des endomorphismes.