

Espaces monogènes, endomorphismes cycliques

Définitions et notations

Dans tout le problème, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, E un $\mathbb{K}$ -espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $u \in \mathcal{L}(E)$.

Pour tout $x \in E$ on note $E_u(x) = \{P(u)(x) / P \in \mathbb{K}[X]\}$ et on dit que u est cyclique si $\exists x \in E$ tel que $E_u(x) = E$.

Première partie

Espaces monogènes

- 1: Soit $x \in E$. Montrer que $E_u(x)$ est le plus petit sous-espace de E qui contient x et stable par u . $E_u(x)$ s'appelle le sous-espace u -monogène engendré par x .
- 2: Soit $x \in E \setminus \{0\}$ et $\mathcal{I}_x = \{P \in \mathbb{K}[X] / P(u)(x) = 0\}$.
- 2 - 1: Montrer que $\exists \mu_x \in \mathbb{K}[X]$ unitaire tel que $\mathcal{I}_x = \mu_x \mathbb{K}[X]$.
- 2 - 2: Donner une condition nécessaire et suffisante sur x pour que $\deg \mu_x = 1$.
- 2 - 3: Montrer que $\mu_x | \pi_u$ et déduire que l'ensemble $\{\mu_x / x \in E \setminus \{0\}\}$ est fini.
- 2 - 4: Montrer que $\exists e \in E \setminus \{0\}$ tel que $E = \ker \mu_e(u)$.
- 2 - 5: En déduire que $\mu_e = \pi_u$.
- 3: Soient $x, y \in E \setminus \{0\}$ tels que $\mu_x \wedge \mu_y = 1$. Montrer que $x + y \neq 0$ et $\mu_{x+y} = \mu_x \mu_y$.
- 4: Soit $\pi_u = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition de π_u en facteurs unitaires et irréductibles.
- 4 - 1: Soit $i \in \{1, \dots, r\}$ et $Q \in \mathbb{K}[X]$ tel que $\pi_u = Q P_i^{\alpha_i}$. Montrer que $\exists x_i \in E$ tel que $(Q P_i^{\alpha_i - 1})(u)(x_i) \neq 0$.
- 4 - 2: Soit $y_i = Q(u)(x_i)$. Montrer que $y_i \neq 0$ et $\mu_{y_i} = P_i^{\alpha_i}$.
- 4 - 3: Retrouver le résultat de la question 2-5.
- 5: Soit $x \in E \setminus \{0\}$, u_x l'endomorphisme de $E_u(x)$ induit par u et $k = \deg \mu_x$. On pose $\mu_x = X^k - a_{k-1}X^{k-1} - \dots - a_1X - a_0$.
- 5 - 1: Montrer que $\mathcal{B}_x = (x, u(x), \dots, u^{k-1}(x))$ est une base de $E_u(x)$. En déduire la dimension de $E_u(x)$.
- 5 - 2: Déterminer la matrice de u_x dans la base $\mathcal{B}_x$.
- 5 - 3: Montrer que le polynôme minimale de u_x est μ_x .

Correction du problème

Première partie Espaces monogènes

1:

- Soit $\varphi : \mathbb{K}[X] \rightarrow E$ définie par $\forall P \in \mathbb{K}[X], \varphi(P) = P(u)(x)$.
On a $\forall P, Q \in \mathbb{K}[X], \forall \alpha, \beta \in \mathbb{K}, \varphi(\alpha P + \beta Q) = (\alpha P + \beta Q)(u)(x) = (\alpha P(u) + \beta Q(u))(x) = \alpha P(u)(x) + \beta Q(u)(x) = \alpha \varphi(P) + \beta \varphi(Q)$ donc φ est linéaire d'où $E_u(x) = \text{Im} \varphi$ est un sous-espace vectoriel de E .
- Pour $P = 1$, on a $P(u) = \text{id}_E$ donc $P(u)(x) = x$ d'où $x \in E_u(x)$.
- Soit $P \in \mathbb{K}[X]$ donc $u(P(u)(x)) = (uP(u))(x) = (XP)(u)(x) \in E_u(x)$ d'où $E_u(x)$ est stable par u .
- Soit F un sous-espace vectoriel de E stable par u qui contient x . Montrons d'abord que $\forall k \in \mathbb{N}, u^k(x) \in E$:
 1. On a $u^0(x) = \text{id}_E(x) = x \in F$ donc $u^0(x) \in F$. La relation est alors vraie pour $k = 0$.
 2. Soit $k \in \mathbb{N}$ et supposons que $u^k(x) \in F$. On a F stable par u donc $u^{k+1}(x) = u(u^k(x)) \in F$.

On déduit, d'après le procédé de récurrence, que $\forall k \in \mathbb{N}, u^k(x) \in F$.

Soit $P = \sum_{k=0}^d a_k X^k \in \mathbb{K}[X]$ donc $P(u)(x) = \sum_{k=0}^d a_k u^k(x) \in F$ car $\forall k \in \{0, \dots, d\}, u^k(x) \in F$ et F un sous-espace vectoriel d'où $P(u)(x) \in F$.

On a $E_u(x) = \{P(u)(x) / P \in \mathbb{K}[X]\}$ et $\forall P \in \mathbb{K}[X], P(u)(x) \in F$ donc $E_u(x) \subset F$ d'où $E_u(x)$ est le plus petit sous-espace de E qui contient x et stable par u .

2:

2 - 1: On a $\pi_u \in \mathbb{K}[X]$ et $\pi_u(u)(x) = 0$ car $\pi_u(u) = 0$ donc $\pi_u \in \mathcal{I}_x$ d'où $\mathcal{I}_x \neq \emptyset$. Or $\pi_u \neq 0$ car unitaire donc $\mathcal{I}_x$ est non nul. Soient $P, Q \in \mathcal{I}_x$ et $R \in \mathbb{K}[X]$. On a :

- $(P - Q)(u)(x) = P(u)(x) - Q(u)(x) = 0 - 0 = 0$ donc $P - Q \in \mathcal{I}_x$.
- $(RP)(u)(x) = (R(u) \circ P(u))(x) = R(u)(P(u)(x)) = R(u)(0) = 0$ donc $RP \in \mathcal{I}_x$.

On déduit que $\mathcal{I}_x$ est un idéal non nul de l'anneau principal $\mathbb{K}[X]$ donc $\exists \mu_x$ unitaire tel que $\mathcal{I}_x$ soit engendré par μ_x . Autrement dit, $\mathcal{I}_x = \mu_x \mathbb{K}[X]$.

2 - 2:

- **Condition nécessaire :** On a μ_x unitaire et $\deg \mu_x = 1$ donc $\exists \alpha \in \mathbb{K}$ tel que $\mu_x = X - \alpha$.
D'autre part, on a $\mu_x \in \mathcal{I}_x$ donc $0 = \mu_x(u)(x) = (X - \alpha)(u)(x) = (u - \alpha \text{id}_E)(x) = u(x) - \alpha x$ d'où $u(x) = \alpha x$.
On a $u(x) = \alpha x$ et $x \neq 0$ donc x est un vecteur propre de u .
- **Condition suffisante :** Supposons que x est un vecteur propre de u donc $\exists \alpha \in \mathbb{K}$ tel que $u(x) = \alpha x$.
Soit $P = X - \alpha$ donc $P(u)(x) = (X - \alpha)(u)(x) = (u - \alpha \text{id}_E)(x) = u(x) - \alpha x = 0$ d'où $P \in \mathcal{I}_x$. Or $\mathcal{I}_x = \mu_x \mathbb{K}[X]$ donc $\mu_x | P$ d'où $\mu_x = 1$ ou $\mu_x = P$ car μ_x est unitaire.
Si $\mu_x = 1$ alors $0 = \mu_x(u)(x) = 1(u)(x) = \text{id}_E(x) = x$. Absurde, car $x \neq 0$ donc $\mu_x = P$ d'où $\deg \mu_x = \deg P = 1$.

On déduit que $\deg \mu_x = 1$ si, et seulement si, x est un vecteur propre de u .

2 - 3: On a déjà montré (question 1-2) que $\pi_u \in \mathcal{I}_x$ et puisque $\mathcal{I}_x = \mu_x \mathbb{K}[X]$ donc $\mu_x | \pi_u$.

Soit $\pi_u = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition de π_u en facteurs unitaires et irréductibles donc $\forall P \in \mathbb{K}[X]$ unitaire, $P | Q \iff \forall i \in \{1, \dots, r\}, \exists \beta_i \in \{0, \dots, \alpha_i\}$ tel que $P = P_1^{\beta_1} \dots P_r^{\beta_r}$ d'où l'ensemble $\mathcal{D}(\pi_u)$ des diviseurs unitaires de π_u est $\mathcal{D}(\pi_u) = \{P_1^{\beta_1} \dots P_r^{\beta_r} / \forall i \in \{1, \dots, r\}, \beta_i \in \{0, \dots, \alpha_i\}\}$. En particulier $\mathcal{D}(\pi_u)$ est finie.

On a $\forall x \in E \setminus \{0\}, \mu_x$ est unitaire et $\mu_x | \pi_u$ donc $\{\mu_x / x \in E \setminus \{0\}\} \subset \mathcal{D}(\pi_u)$ d'où l'ensemble $\{\mu_x / x \in E \setminus \{0\}\}$ est fini.

2 - 4: L'ensemble $\{\mu_x / x \in E \setminus \{0\}\}$ est fini donc $\exists x_1, \dots, x_p \in E$ tels que $\{\mu_x / x \in E \setminus \{0\}\} = \{\mu_{x_1}, \dots, \mu_{x_p}\}$.

Soit $x \in E$. Si $x = 0$ alors $\mu_{x_1}(u)(x) = 0$, sinon, $\exists k \in \{1, \dots, p\}$ tel que $\mu_x = \mu_{x_k}$ donc $\mu_{x_k}(u)(x) = \mu_x(u)(x) = 0$.

On déduit que $\forall x \in E, \exists k \in \{1, \dots, p\}, \mu_{x_k}(u)(x) = 0$ donc $\forall x \in E, \exists k \in \{1, \dots, p\}, x \in \ker \mu_{x_k}(u)$ d'où $E = \bigcup_{k=1}^p \ker \mu_{x_k}(u)$.

$\{\ker \mu_{x_k}(u) / k \in \{1, \dots, p\}\}$ est une famille de sous-espaces vectoriels de E dont l'union est E qui est un espace vectoriel donc $\exists k \in \{1, \dots, p\}$ tel que $\forall l \in \{1, \dots, p\}, \ker \mu_{x_l}(u) \subset \ker \mu_{x_k}(u)$ d'où $\ker \mu_{x_k}(u) = E$.

Pour $e = x_k$ on a $e \neq 0$ et $E = \ker \mu_e(u)$.

2 - 5: On a $E = \ker \mu_e(u)$ donc $\mu_e(u) = 0$ d'où $\pi_u | \mu_e$. Or, d'après la question 2-3, $\mu_e | \pi_u$ donc $\mu_e = \pi_u$ car μ_e et π_u sont unitaires.

3:

- Supposons que $x + y = 0$ donc $0 = \pi_x(u)(x) = \pi_x(u)(-y) = -\pi_x(u)(y)$ d'où $\pi_x(u)(y) = 0$. On déduit que $\pi_x \in \mathcal{I}_y$ donc $\pi_y \mid \pi_x$. Or $\pi_x \wedge \pi_y = 1$ donc $\pi_x = 1$ d'où $0 = \pi_x(u)(x) = 1(u)(x) = \text{id}_E(x) = x$. Absurde, car $x \neq 0$.
- 1. On a $(\mu_x \mu_y)(u)(x + y) = (\mu_x(u) \mu_y(u))(x + y) = \mu_x(u)(\mu_y(u)(x + y)) = \mu_x(u)(\mu_y(u)(x) + \mu_y(u)(y)) = \mu_x(u)(\mu_y(u)(x)) + \mu_x(u)(\mu_y(u)(y)) = (\mu_x(u) \mu_y(u))(x) = (\mu_y(u) \mu_x(u))(x) = \mu_y(u)(\mu_x(u)(x)) = 0$ donc $\mu_x \mu_y \in \mathcal{I}_{x+y}$ d'où $\mu_{x+y} \mid \mu_x \mu_y$.
- 2. On a $0 = \mu_{x+y}(u)(\mu_x(u)(x)) = (\mu_{x+y}(u) \mu_x(u))(x) = (\mu_x(u) \mu_{x+y}(u))(x) = \mu_x(u)(\mu_{x+y}(u)(x)) = \mu_x(u)(\mu_{x+y}(u)(x + y - y)) = \mu_x(u)(\mu_{x+y}(u)(x + y) - \mu_{x+y}(u)(y)) = -\mu_x(u)(\mu_{x+y}(u)(y)) = -(\mu_x(u) \mu_{x+y}(u))(y) = (\mu_x \mu_{x+y})(u)(y)$ donc $\mu_x \mu_{x+y} \in \mathcal{I}_y$ d'où $\mu_y \mid \mu_x \mu_{x+y}$. Or $\mu_x \wedge \mu_y = 1$ donc $\mu_y \mid \mu_{x+y}$. De même, on a $0 = \mu_{x+y}(u)(\mu_y(u)(y)) = (\mu_{x+y}(u) \mu_y(u))(y) = (\mu_y(u) \mu_{x+y}(u))(y) = \mu_y(u)(\mu_{x+y}(u)(y)) = \mu_y(u)(\mu_{x+y}(u)(x + y - x)) = \mu_y(u)(\mu_{x+y}(u)(x + y) - \mu_{x+y}(u)(x)) = -\mu_y(u)(\mu_{x+y}(u)(x)) = -(\mu_y(u) \mu_{x+y}(u))(x) = (\mu_y \mu_{x+y})(u)(x)$ donc $\mu_y \mu_{x+y} \in \mathcal{I}_x$ d'où $\mu_x \mid \mu_y \mu_{x+y}$. Or $\mu_x \wedge \mu_y = 1$ donc $\mu_x \mid \mu_{x+y}$. On a $\mu_x \mid \mu_{x+y}$, $\mu_y \mid \mu_{x+y}$ et $\mu_x \wedge \mu_y = 1$ donc $\mu_x \mu_y \mid \mu_{x+y}$. On a $\mu_{x+y} \mid \mu_x \mu_y$, $\mu_x \mu_y \mid \mu_{x+y}$ et μ_x, μ_y, μ_{x+y} unitaires donc $\mu_{x+y} = \mu_x \mu_y$.

4:

4 - 1: On a $P_i^{\alpha_i-1}Q$ non nul et $\deg(P_i^{\alpha_i-1}Q) < \pi_u$ donc $P_i^{\alpha_i-1}Q$ n'est pas annulateur de u donc $(P_i^{\alpha_i-1}Q)(u) \neq 0$ d'où $\exists x_i \in E$ tel que $(P_i^{\alpha_i-1}Q)(u)(x_i) \neq 0$.

4 - 2:

- On a $P_i^{\alpha_i-1}(u)(y_i) = P_i^{\alpha_i-1}(u)(Q(u)(x_i)) = (P_i^{\alpha_i-1}(u)Q(u))(x_i) = (P_i^{\alpha_i-1}Q)(u)(x_i) \neq 0$ donc $y_i \neq 0$.
- On a $P_i^{\alpha_i}(u)(y_i) = (P_i^{\alpha_i}Q)(u)(x_i) = \pi_u(u)(x_i) = 0$ donc $P_i^{\alpha_i} \in \mathcal{I}_{y_i}$ d'où $\pi_{y_i} \mid P_i^{\alpha_i}$. Or P_i est irréductible dans $\mathbb{K}[X]$ donc $\exists k \in \{1, \dots, \alpha_i\}$, $\pi_{y_i} = P_i^k$. On a $P_i^{\alpha_i-1}(u)(y_i) \neq 0$ donc $P_i^{\alpha_i-1} \notin \mathcal{I}_{y_i}$ donc $P_i^k = \pi_{y_i} \nmid P_i^{\alpha_i-1}$ d'où $k > \alpha_i - 1$ d'où $k = \alpha_i$ car $k \in \{1, \dots, \alpha_i\}$. On déduit que $\pi_{y_i} = P_i^{\alpha_i}$.

4 - 3: D'après la question précédente, $\forall i \in \{1, \dots, r\}$, $\exists e_i \in E \setminus \{0\}$ tel que $P_i^{\alpha_i} = \pi_{e_i}$ et soit $e = e_1 + \dots + e_r$.

Montrons que $\forall k \in \{1, \dots, r\}$, $e_1 + \dots + e_k \neq 0$ et $\mu_{e_1+\dots+e_k} = P_1^{\alpha_1} \dots P_k^{\alpha_k}$:

- On a $e_1 \neq 0$ et $\mu_{e_1} = P_1^{\alpha_1}$ donc la relation est vraie pour $k = 1$.
- Soit $k \in \{1, \dots, r-1\}$ et supposons que $e_1 + \dots + e_k \neq 0$ et $\mu_{e_1+\dots+e_k} = P_1^{\alpha_1} \dots P_k^{\alpha_k}$. On a $\mu_{e_1+\dots+e_k} \wedge \mu_{e_{k+1}} = (P_1^{\alpha_1} \dots P_k^{\alpha_k}) \wedge P_{k+1}^{\alpha_{k+1}} = 1$ car les $P_i, i \in \{1, \dots, k+1\}$ sont deux à deux premiers entre eux donc, d'après la question 3, $e_1 + \dots + e_{k+1} \neq 0$ et $\mu_{e_1+\dots+e_{k+1}} = \mu_{e_1+\dots+e_k} \mu_{e_{k+1}} = P_1^{\alpha_1} \dots P_{k+1}^{\alpha_{k+1}}$. La relation est alors vraie pour $k+1$.

On déduit, d'après le procédé de récurrence, que $\forall k \in \{1, \dots, r\}$, $e_1 + \dots + e_k \neq 0$ et $\mu_{e_1+\dots+e_k} = P_1^{\alpha_1} \dots P_k^{\alpha_k}$. En particulier, pour $k = r$, $e = e_1 + \dots + e_r \neq 0$ et $\mu_e = \mu_{e_1+\dots+e_r} = P_1^{\alpha_1} \dots P_r^{\alpha_r} = \pi_u$.

5: Soit $x \in E \setminus \{0\}$, u_x l'endomorphisme de $E_u(x)$ induit par u et $k = \deg \mu_x$. On pose $\mu_x = X^k - a_{k-1}X^{k-1} - \dots - a_1X - a_0$.

5 - 1: Remarquons d'abord que $x, u(x), \dots, u^{k-1}(x) \in E_u(x)$.

- Soient $\alpha_0, \dots, \alpha_{k-1} \in \mathbb{K}$ tels que $\alpha_0 x + \dots + \alpha_{k-1} u^{k-1}(x) = 0$ donc $(\alpha_0 \text{id}_E + \dots + \alpha_{k-1} u^{k-1})(x) = 0$ d'où $(\alpha_0 + \dots + \alpha_{k-1} X^{k-1})(u)(x) = 0$. On déduit que $\alpha_0 + \dots + \alpha_{k-1} X^{k-1} \in \mathcal{I}_x$ donc $\mu_x \mid \alpha_0 + \dots + \alpha_{k-1} X^{k-1}$. Or $\deg(\alpha_0 + \dots + \alpha_{k-1} X^{k-1}) < k = \deg \mu_x$ donc $\alpha_0 + \dots + \alpha_{k-1} X^{k-1} = 0$ d'où $\alpha_0 = \dots = \alpha_{k-1} = 0$. On déduit que la famille $\{x, u(x), \dots, u^{k-1}(x)\}$ est libre.
- Soit $P \in \mathbb{K}[X]$ et $P = Q\mu_x + R$ la division euclidienne de P par μ_x donc $P(u)(x) = (Q\mu_x + R)(u)(x) = (Q\mu_x)(u)(x) + R(u)(x) = R(u)(x)$ car $(Q\mu_x)(u)(x) = 0$ puisque $Q\mu_x \in \mu_x \mathbb{K}[X] = \mathcal{I}_x$. On déduit que $P(u)(x) = R(u)(x) \in \text{Vect}\{x, u(x), \dots, u^{k-1}(x)\}$ car $\deg R \leq \deg \mu_x - 1 = k - 1$. On déduit que la famille $\{x, u(x), \dots, u^{k-1}(x)\}$ est génératrice dans $E_u(x)$.

La famille $\{x, u(x), \dots, u^{k-1}(x)\}$ est libre et génératrice donc $\mathcal{B}_x$ est une base de $E_u(x)$ et, en particulier, $\dim E_u(x) = \text{card}(\{x, u(x), \dots, u^{k-1}(x)\}) = k = \deg \mu_x$.

5 - 2: On a $\forall p \in \{1, \dots, k-2\}$, $u_x(u^p(x)) = u(u^p(x)) = u^{p+1}(x)$.

D'autre part, on a $\mu_x = X^k - a_{k-1}X^{k-1} - \dots - a_1X - a_0$ donc $0 = \mu_x(u)(x) = (u^k - a_{k-1}u^{k-1} - \dots - a_1u - a_0 \text{id}_E)(x) = u^k(x) - a_{k-1}u^{k-1}(x) - \dots - a_1u(x) - a_0x$ donc $u^k(x) = a_{k-1}u^{k-1}(x) + \dots + a_1u(x) + a_0x$. On déduit que $u_x(u^{k-1}(x)) = u^k(x) = a_{k-1}u^{k-1}(x) + \dots + a_1u(x) + a_0x$.

La matrice de u_x dans la base $\mathcal{B}_x$ est alors :

$$\begin{pmatrix} 0 & \dots & \dots & 0 & a_0 \\ 1 & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{k-2} \\ 0 & \dots & 0 & 1 & a_{k-1} \end{pmatrix}$$

5 - 3: Soit π_x le polynôme minimal de u_x donc $\pi_x(u_x) = 0$ d'où $0 = \pi_x(u_x)(x) = \pi_x(u)(x)$. On déduit que $\pi_x \in \mathcal{I}_x$ donc $\mu_x \mid \pi_x$. En particulier, $\deg \mu_x \leq \deg \pi_x$.

D'autre part, $\deg \pi_x \leq \dim E_u(x) = \deg \mu_x$ donc $\deg \mu_x = \deg \pi_x$.

On a $\mu_x \mid \pi_x$, $\deg \mu_x = \deg \pi_x$ et μ_x, π_x unitaires donc $\pi_x = \mu_x$.