

Chapitre 6

Polynômes annulateurs et réduction

Dans tout le chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$, et E un $\mathbb{K}$ -espace vectoriel. Sauf mention contraire, on supposera que E est de dimension finie n .

I Polynômes d'endomorphismes, de matrices carrées

1. Définition et propriétés

Définition - Polynôme d'endomorphisme, polynôme de matrice

Soit $P = a_0 + a_1X + \dots + a_dX^d$ un polynôme de $\mathbb{K}[X]$.

- Si $u \in \mathcal{L}(E)$, on définit l'endomorphisme $P(u) \in \mathcal{L}(E)$ par

$$P(u) = a_0 \text{Id}_E + a_1u + \dots + a_du^d.$$

- Si $A \in \mathcal{M}_n(\mathbb{K})$, on définit la matrice $P(A) \in \mathcal{M}_n(\mathbb{K})$ par

$$P(A) = a_0I_n + a_1A + \dots + a_dA^d.$$

On note par ailleurs $\mathbb{K}[u] = \{P(u), P \in \mathbb{K}[X]\}$, et $\mathbb{K}[A] = \{P(A), A \in \mathcal{M}_n(\mathbb{K})\}$.

Exemples.

- Si $P = X^2 - 3X + 2$ et $u \in \mathcal{L}(E)$, alors $P(u) = u^2 - 3u + 2\text{Id}_E$. Si $A \in \mathcal{M}_n(\mathbb{K})$, alors $P(A) = A^2 - 3A + 2I_n$.
- Si $A = \text{diag}(\lambda_1, \dots, \lambda_n) \in \mathcal{M}_n(\mathbb{K})$ et $P \in \mathbb{K}[X]$, alors $P(A) = \text{diag}(P(\lambda_1), \dots, P(\lambda_n))$:

$$\text{si } P = \sum_{k=0}^d a_k X^k, \text{ alors } P(A) = \sum_{k=0}^d a_k \begin{pmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{pmatrix} = \sum_{k=0}^d a_k \begin{pmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{pmatrix} = \begin{pmatrix} P(\lambda_1) & & \\ & \ddots & \\ & & P(\lambda_n) \end{pmatrix}.$$

Remarque. Si $u \in \mathcal{L}(E)$ et $A \in \mathcal{M}_n(\mathbb{K})$, on a alors

$$\mathbb{K}[u] = \text{Vect}\{u^k, k \in \mathbb{N}\}, \quad \text{et} \quad \mathbb{K}[A] = \text{Vect}\{A^k, k \in \mathbb{N}\}.$$

Exemple. Si $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, alors $\mathbb{K}[A] = \text{Vect}(I_2, A)$, car si $k \in \mathbb{N}$, $A^k = \begin{cases} I_2 & \text{si } k \text{ est pair} \\ A & \text{si } k \text{ est impair} \end{cases}$

Théorème

Soit $u \in \mathcal{L}(E)$. L'application $\Psi : P \mapsto P(u)$ est un morphisme de $\mathbb{K}$ -algèbres de $\mathbb{K}[X]$ dans $\mathcal{L}(E)$, qui a pour image $\mathbb{K}[u]$. En particulier,

$$\forall P, Q \in \mathbb{K}[X], (PQ)(u) = P(u) \circ Q(u).$$

Démonstration. On a déjà que $\Psi(1) = \text{Id}_E$, et pour tous $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, $(\lambda P + Q)(u) = \lambda P(u) + Q(u)$.

Par ailleurs, si $P = \sum_{i=0}^d a_i X^i$ et $Q = \sum_{j=0}^d b_j X^j$, alors $PQ = \sum_{i=0}^d \sum_{j=0}^d a_i b_j X^{i+j}$, donc

$$(PQ)(u) = \sum_{i=0}^d \sum_{j=0}^d a_i b_j u^{i+j} = \sum_{i=0}^d \sum_{j=0}^d a_i b_j u^i \circ u^j = \left(\sum_{i=0}^d a_i u^i \right) \circ \left(\sum_{j=0}^d b_j u^j \right) = P(u) \circ Q(u). \quad \square$$

Remarques.

- De même, si $A \in \mathcal{M}_n(\mathbb{K})$, l'application $P \mapsto P(A)$ définit un morphisme de $\mathbb{K}$ -algèbres de $\mathbb{K}[X]$ dans $\mathcal{M}_n(\mathbb{K})$.

- De manière plus générale, si $\mathcal{A}$ est une $\mathbb{K}$ -algèbre, pour tout polynôme $P = a_0 + \dots + a_d X^d$ et tout $x \in \mathcal{A}$, on peut écrire $P(x) = a_0 1_{\mathcal{A}} + \dots + a_d x^d$.

L'application $P \mapsto P(x)$ définit un morphisme d'algèbre de $\mathbb{K}[X]$ dans $\mathcal{A}$. Ceci permet de définir $\mathbb{K}[x]$ comme l'image de ce morphisme.

⚠ Il est crucial d'avoir une structure d'algèbre pour pouvoir écrire $P(x)$. Ainsi, si E est un $\mathbb{K}$ -espace vectoriel quelconque et $x \in E$, $P(x)$ n'a pas de sens.

En particulier, si $u \in \mathcal{L}(E)$ et $x \in E$, alors $P(u)(x)$ a un sens : c'est un vecteur de E car $P(u) \in \mathcal{L}(E)$. Avec les notations précédentes, on a

$$P(u)(x) = a_0 x + a_1 u(x) + \dots + a_d u^d(x).$$

En revanche, si E est un espace vectoriel quelconque, $P(u(x))$ n'a pas de sens !

Exemple. Revenons sur l'exemple précédent. Comme $P = X^2 - 3X + 2 = (X - 1)(X - 2)$, on peut écrire

$$P(u) = (u - \text{Id}_E) \circ (u - 2\text{Id}_E).$$

On a aussi $P(A) = (A - I_n)(A - 2I_n)$.

Théorème

Soient $u, v \in \mathcal{L}(E)$ et $P, Q \in \mathbb{K}[X]$.

- Les endomorphismes $P(u)$ et $Q(u)$ commutent : $P(u) \circ Q(u) = Q(u) \circ P(u)$.
- Si u et v commutent, alors $P(u)$ et $Q(v)$ commutent.

Démonstration.

- On a $P(u) \circ Q(u) = (PQ)(u) = (QP)(u) = Q(u) \circ P(u)$.
- Si $P = \sum_{i=0}^{+\infty} a_i X^i$ et $Q = \sum_{j=0}^{+\infty} b_j X^j$, alors $P(u) \circ Q(u) = \sum_i \sum_j a_i b_j u^i \circ v^j = \sum_i \sum_j a_i b_j v^j \circ u^i = Q(u) \circ P(u)$. □

On retiendra que deux polynômes du même endomorphisme commutent toujours.

Corollaire - Stabilité de $\ker(P(u))$ et $\text{Im}(P(u))$ par u

Si $u \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$, alors $\text{Ker}(P(u))$ et $\text{Im}(P(u))$ sont stables par u .

Démonstration. u et $P(u)$ commutent, et on sait que si u et v commutent alors $\text{Ker } v$ et $\text{Im } v$ sont stables par u . □

Remarque. Plus généralement, si $u, v \in \mathcal{L}(E)$ commutent et $P, Q \in \mathbb{K}[X]$, alors $\text{Ker}(P(u))$ et $\text{Im}(P(u))$ sont stables par $Q(v)$.

Corollaire - L'algèbre $\mathbb{K}[u]$

Si $u \in \mathcal{L}(E)$, alors $\mathbb{K}[u]$ a une structure de $\mathbb{K}$ -algèbre commutative.

Démonstration. Comme image de la $\mathbb{K}$ -algèbre $(\mathbb{K}[X], +, \cdot, \times)$ par un morphisme de $\mathbb{K}$ -algèbre, $\mathbb{K}[u]$ est une sous-algèbre de $(\mathcal{L}(E), +, \cdot, \circ)$. L'algèbre $\mathbb{K}[u]$ est par ailleurs commutative par le théorème précédent. □

Remarque. En d'autres termes, $(\mathbb{K}[u], +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel, $(\mathbb{K}[u], +, \circ)$ est un anneau commutatif, et on a par ailleurs : $\forall \lambda \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X], (\lambda P(u)) \circ Q(u) = P(u) \circ (\lambda Q(u)) = \lambda P(u) \circ Q(u)$.

Théorème

Soient $u \in \mathcal{L}(E)$ et $\mathcal{B}$ une base de E . Pour tout $P \in \mathbb{K}[X]$, on a

$$\text{Mat}_{\mathcal{B}}(P(u)) = P(A), \quad \text{où } A = \text{Mat}_{\mathcal{B}}(u).$$

Démonstration. Si $P = \sum_{k=0}^d a_k X^k$, $\text{Mat}_{\mathcal{B}}(P(u)) = \text{Mat}_{\mathcal{B}}\left(\sum_{k=0}^d a_k u^k\right) = \sum_{k=0}^d a_k \text{Mat}_{\mathcal{B}}(u^k) = \sum_{k=0}^d a_k \text{Mat}_{\mathcal{B}}(u)^k$. $\square$

Théorème

Si $A, B \in \mathcal{M}_n(\mathbb{K})$ sont deux matrices semblables et $P \in \mathbb{K}[X]$, alors $P(A)$ et $P(B)$ sont semblables.

Démonstration. Soit $Q \in \text{GL}_n(\mathbb{K})$ telle que $B = QAQ^{-1}$. Si on note $P = a_0 + \dots + a_d X^d$, alors

$$P(B) = \sum_{k=0}^d a_k (QAQ^{-1})^k = \sum_{k=0}^d a_k QA^k Q^{-1} = Q \left(\sum_{k=0}^d a_k A^k \right) Q^{-1} = QP(A)Q^{-1}. \quad \square$$

2. Polynômes annulateurs, polynôme minimal

Définition - Polynôme annulateur

Soit $P \in \mathbb{K}[X]$.

- Soit $u \in \mathcal{L}(E)$. On dit que P est un polynôme annulateur de u si $P(u) = 0_{\mathcal{L}(E)}$.
- Soit $A \in \mathcal{M}_n(\mathbb{K})$. On dit que P est un polynôme annulateur de A si $P(A) = 0_{n,n}$.

Exemple. Si u est un projecteur de E , alors $u^2 = u$, et $P = X^2 - X$ est un polynôme annulateur de u .

Remarques.

- Si $P \in \mathbb{K}[X]$ est un polynôme annulateur de $u \in \mathcal{L}(E)$, alors tout multiple de P est annulateur de u : si $Q = AP$ où $A \in \mathbb{K}[X]$, alors $Q(u) = A(u) \circ P(u) = 0_{\mathcal{L}(E)}$.
- De même, si $P \in \mathbb{K}[X]$ est un polynôme annulateur de $A \in \mathcal{M}_n(\mathbb{K})$, tous ses multiples le sont également.

Théorème - Existence de polynômes annulateurs non triviaux en dimension finie

En dimension finie, tout endomorphisme $u \in \mathcal{L}(E)$ admet un polynôme annulateur non nul.

Démonstration. On note $d = n^2$. La famille $(\text{Id}_E, u, \dots, u^d)$ est de cardinal $d + 1$. Comme $\dim \mathcal{L}(E) = d$, cette dernière famille est liée, ce qui donne l'existence de $a_0, \dots, a_d \in \mathbb{K}$ non tous nuls tels que $a_0 \text{Id}_E + \dots + a_d u^d = 0_{\mathcal{L}(E)}$. Ainsi, le polynôme non nul $a_0 + \dots + a_d X^d$ est annulateur de u . $\square$

! En dimension infinie, le résultat devient faux. Par exemple, si $E = \mathcal{C}^\infty(\mathbb{R})$, l'endomorphisme $u : f \mapsto f'$ n'admet pas de polynôme annulateur non nul (exercice : le montrer).

Remarques.

- Comme précédemment, le résultat tient également pour les matrices : toute matrice $A \in \mathcal{M}_n(\mathbb{K})$ admet un polynôme annulateur non nul.
- Nous avons donc montré que si $\dim E = n$, tout endomorphisme $u \in \mathcal{L}(E)$ a un polynôme annulateur de degré inférieur à n^2 . Nous verrons plus loin qu'il existe toujours un polynôme annulateur de degré au plus n .

Théorème et définition - Polynôme minimal

Soit $u \in \mathcal{L}(E)$. Il existe un unique polynôme unitaire qui divise tous les polynômes annulateurs de u . On l'appelle le *polynôme minimal* de u , et on le note μ_u .

Démonstration. Existence. On note $d = \min \{\deg(P), P \in \mathbb{K}[X] \setminus \{0\}, P(u) = 0_{\mathcal{L}(E)}\}$. L'existence de d comme minimum d'une partie non vide de $\mathbb{N}$ est assurée par le résultat précédent.

On considère alors $P \in \mathbb{K}[X]$ tel que $\deg P = d$ et $P(u) = 0_{\mathcal{L}(E)}$. Quitte à diviser P par son coefficient dominant, on peut supposer P unitaire.

Considérons un polynôme annulateur $\tilde{P}$ de u , et notons $\tilde{P} = PQ + R$ la division euclidienne de $\tilde{P}$ par P . Alors

$$R(u) = \tilde{P}(u) - (PQ)(u) = 0_{\mathcal{L}(E)}, \quad \text{car} \quad (PQ)(u) = Q(u) \circ P(u) = 0_{\mathcal{L}(E)}.$$

Ainsi, R est annulateur de u et $\deg R < \deg P$. Ceci entraîne que R est nul par minimalité de $\deg P$, donc $P \mid \tilde{P}$.

Unicité. Si $\tilde{P}$ est polynôme annulateur unitaire de u qui divise tous ses polynômes annulateurs, alors $P \mid \tilde{P}$ et $\tilde{P} \mid P$, donc $P = \tilde{P}$ car P et $\tilde{P}$ sont unitaires. $\square$

Remarques.

- De même, si $A \in \mathcal{M}_n(\mathbb{K})$, il existe un unique polynôme unitaire qui divise tous les polynômes annulateurs de A , appelé polynôme minimal de A , et noté μ_A .
- Si $E \neq \{0_E\}$, le polynôme minimal de tout endomorphisme de E est au moins de degré 1, car $1(u) \neq 0_{\mathcal{L}(E)}$.

Exemples. On suppose que $E \neq \{0_E\}$.

- Si $u = \lambda \text{Id}_E$ avec $\lambda \in \mathbb{K}$, alors $\mu_u = X - \lambda$. Réciproquement, les seuls endomorphismes ayant un polynôme minimal de degré 1 sont les homothéties de E .
- Si u est un projecteur non trivial ($u \neq \text{Id}_E$ et $u \neq 0_{\mathcal{L}(E)}$) de E , alors $\mu_u = X^2 - X$.

En effet, $X^2 - X = X(X - 1)$ annule u donc $\mu_u \mid X^2 - X$. Or X et $X - 1$ n'annulent pas u car $u \notin \{0_{\mathcal{L}(E)}, \text{Id}_E\}$, donc $\mu_u = X^2 - X$.

- Si u est nilpotent d'indice p , alors $\mu_u = X^p$.

En effet, X^p est annulateur de u , donc $\mu_u \mid X^p$. On en déduit que μ_u est de la forme X^k , où $k \leq p$. Si $k < p$, on a $u^k \neq 0_{\mathcal{L}(E)}$ donc X^k n'annule pas u . Ainsi, $\mu_u = X^p$.

- Si $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, alors $A^2 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, et on remarque que $A^2 + I_3 = 2A$, donc $P = X^2 - 2X + 1$ annule A .

On en déduit que $\mu_A \mid P$, c'est-à-dire que $\mu_A \mid (X - 1)^2$. Par conséquent, $\mu_A \in \{X - 1, (X - 1)^2\}$. On ne peut avoir $\mu_A = X - 1$, sinon on aurait $A - I_3 = 0$. Finalement, $\mu_A = (X - 1)^2$.

Remarque. Si $u \in \mathcal{L}(E)$ et si F est un sous-espace vectoriel de E stable par u , alors le polynôme minimal de l'endomorphisme u_F induit par u sur F divise le polynôme minimal de u .

Démonstration. Comme μ_u est un polynôme annulateur de u , μ_u annule également u_F : si $x \in F$, alors $\mu_u(u_F)(x) = \mu_u(u)(x) = 0_E$. On en déduit que $\mu_{u_F} \mid \mu_u$. $\square$

Théorème

Soient $u \in \mathcal{L}(E)$ et $A = \text{Mat}_{\mathcal{B}}(u)$, où $\mathcal{B}$ est une base de E . On a $\mu_A = \mu_u$.

Démonstration. Nous avons vu que $P(A) = \text{Mat}_{\mathcal{B}}(P(u))$, donc $P(A) = 0_{n,n} \Leftrightarrow P(u) = 0_{\mathcal{L}(E)}$. Autrement dit, A et u ont les mêmes polynômes annulateurs, et ont donc même polynôme minimal. $\square$

Théorème - Polynôme minimal et similitude

Si deux matrices A et B de $\mathcal{M}_n(\mathbb{K})$ sont semblables, alors $\mu_A = \mu_B$.

Démonstration. Nous avons vu plus haut que si $B = Q^{-1}AQ$, où $Q \in \text{GL}_n(\mathbb{K})$, alors pour tout polynôme $P \in \mathbb{K}[X]$, $P(B) = Q^{-1}P(A)Q$. Ainsi, A et B ont les mêmes polynômes annulateurs, ce qui conclut. $\square$

Théorème - Polynôme minimal d'une matrice diagonalisable

Si $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable, alors $\mu_A = \prod_{\lambda \in \text{Sp}(A)} (X - \lambda)$.

Démonstration. En effet, si on note $\lambda_1, \dots, \lambda_k$ les valeurs propres de A , on sait que A est semblable à une matrice diagonale de la forme $D = \text{diag}(\lambda_1, \dots, \lambda_1, \dots, \lambda_k, \dots, \lambda_k)$.

Or on a vu que si $P \in \mathbb{K}[X]$, alors $P(D) = \text{diag}(P(\lambda_1), \dots, P(\lambda_1), \dots, P(\lambda_k), \dots, P(\lambda_k))$. Ainsi,

$$P(D) = 0 \Leftrightarrow \forall \lambda \in \text{Sp}(A), P(\lambda) = 0 \Leftrightarrow \prod_{\lambda \in \text{Sp}(A)} (X - \lambda) \mid P.$$

Ceci montre bien que $\mu_A = \prod_{\lambda \in \text{Sp}(A)} (X - \lambda)$. $\square$

Théorème - Base de $\mathbb{K}[u]$

Soient $u \in \mathcal{L}(E)$ et $d = \deg \mu_u$. La famille $(\text{Id}_E, u, \dots, u^{d-1})$ est une base de $\mathbb{K}[u]$.

Démonstration.

- Soit $P \in \mathbb{K}[X]$. On note $P = Q\mu_u + R$ la division euclidienne de P par μ_u , de sorte que $\deg R < \deg \mu_u = d$. On a alors

$$P(u) = Q(u) \circ \mu_u(u) + R(u) = R(u) \in \text{Vect}(\text{Id}_E, u, \dots, u^{d-1}).$$

Ainsi, $\mathbb{K}[u] = \{P(u), P \in \mathbb{K}[X]\} \subset \text{Vect}(\text{Id}_E, u, \dots, u^{d-1})$, et même $\mathbb{K}[u] = \text{Vect}(\text{Id}_E, u, \dots, u^{d-1})$.

- Montrons que $(\text{Id}_E, u, \dots, u^{d-1})$ est libre : si $a_0, \dots, a_{d-1} \in \mathbb{K}$ sont tels que $a_0 \text{Id}_E + \dots + a_{d-1} u^{d-1} = 0_{\mathcal{L}(E)}$, alors $a_0 = \dots = a_{d-1} = 0$ car sinon on a obtenu un polynôme annulateur non nul de u de plus bas degré que μ_u .

La famille $(\text{Id}_E, u, \dots, u^{d-1})$ est donc libre et génératrice de $\mathbb{K}[u]$, ce qui conclut. $\square$

3. Polynômes annulateurs et valeurs propres

Dans la suite, on note $Z(P)$ l'ensemble des racines d'un polynôme. On précisera si besoin $Z_{\mathbb{K}}(P)$ pour désigner l'ensemble des racines dans le corps $\mathbb{K}$.

Théorème - Polynômes annulateurs et valeurs propres

Si P est un polynôme annulateur de $u \in \mathcal{L}(E)$, alors toute valeur propre de u est racine de P : $\text{Sp}(u) \subset Z(P)$.

Démonstration. Soient $P = a_0 + a_1 X + \dots + a_d X^d \in \mathbb{K}[X]$ un polynôme annulateur de u et $\lambda \in \text{Sp}(u)$. Il existe alors $x \in E \setminus \{0_E\}$ tel que $u(x) = \lambda x$. Ainsi, $P(u)(x) = a_0 x + a_1 u(x) + \dots + a_d u^d(x) = a_0 x + a_1 \lambda x + \dots + a_d \lambda^d x = P(\lambda)x$. On en déduit que $P(\lambda)x = 0_E$, puis $P(\lambda) = 0$ car x est non nul. $\square$

Remarque. Ce résultat peut s'avérer utile dans la pratique : lorsqu'on dispose d'un polynôme annulateur dont on connaît les racines, on sait que les valeurs propres sont parmi ces racines.

⚠ Les valeurs propres de u sont toutes racines d'un polynôme annulateur, mais les racines d'un polynôme annulateur ne sont pas toujours des valeurs propres de u . Pour s'en convaincre, il suffit de se souvenir que si P annule u , alors PQ annule u pour tout polynôme $Q \in \mathbb{K}[X]$.

Exemples.

- Si u est un projecteur de E , on a vu que $X^2 - X$ est annulateur de u . On en déduit que $\text{Sp}(u) \subset \{0, 1\}$.

⚠ Il n'y a pas toujours égalité : par exemple, Id_E est un projecteur, dont la seule valeur propre est 1.

- Si u est un endomorphisme nilpotent d'indice p , alors X^p est annulateur de u . On retrouve alors que 0 est la seule valeur propre de u .
- Si $A \in \mathcal{M}_n(\mathbb{K})$ est donnée par :

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix},$$

alors $A^2 = nA$, donc $X^2 - nX$ annule A , ce qui entraîne $\text{Sp}(A) \subset \{0, n\}$.

- ◊ Si $n \geq 2$, A n'est pas inversible donc 0 est valeurs propre, et $(1 \dots 1)^T$ est vecteur propre associée à la valeur propre n donc $\text{Sp}(A) = \{0, n\}$.
- ◊ Si $n = 1$, alors 0 n'est pas valeur propre, et $\text{Sp}(A) = \{1\}$.

4. Théorème de Cayley-Hamilton**Théorème - Cayley-Hamilton**

Soit $u \in \mathcal{L}(E)$. Le polynôme caractéristique χ_u est un polynôme annulateur de u . En d'autres termes,

$$\mu_u \mid \chi_u.$$

Démonstration. *Non exigible.* Il s'agit de montrer que pour tout $x \in E$, $\chi_u(u)(x) = 0_E$. Si $x = 0_E$, c'est évident, et sinon, on considère $m = \min\{k \in \mathbb{N}, (x, u(x), \dots, u^m(x)) \text{ est liée}\}$. Comme $x \neq 0_E$, on a $m \in \mathbb{N}^*$. La famille $\mathcal{B} = (x, u(x), \dots, u^{m-1}(x))$ étant libre, elle forme une base du sous-espace vectoriel $F = \text{Vect}(x, u(x), \dots, u^{m-1}(x))$. Comme $(x, u(x), \dots, u^{m-1}(x))$ est libre et $(x, u(x), \dots, u^m(x))$ est liée, il existe $a_1, \dots, a_{m-1} \in \mathbb{K}$ tels que $u^m(x) = a_0x + \dots + a_{m-1}u^{m-1}(x) \in F$.

Ainsi, $u(F) = \text{Vect}(u(x), \dots, u^m(x)) \subset F$, et F est stable par u , de sorte qu'on peut considérer l'endomorphisme u_F induit par u sur F . La matrice de u_F dans la base $\mathcal{B}$ de F est donnée par

$$\text{Mat}_{\mathcal{B}}(u_F) = \begin{pmatrix} 0 & & & a_0 \\ 1 & \ddots & & a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \dots & 1 & a_{m-1} \end{pmatrix}, \quad \text{donc} \quad \chi_{u_F} = X^m - \sum_{k=0}^{m-1} a_k X^k$$

car on reconnaît une matrice compagnon¹. Ceci entraîne que $\chi_{u_F}(u)(x) = u^m(x) - \sum_{k=0}^{m-1} a_k u^k(x) = 0_E$.

Par ailleurs, comme on a vu que χ_{u_F} divise χ_u , il existe $P \in \mathbb{K}[X]$ tel que $\chi_u = P\chi_{u_F}$. On en déduit alors que $\chi_u(u)(x) = P(u) \circ \chi_{u_F}(u)(x) = 0_E$. Finalement, pour tout $x \in E$, on a $\chi_u(u)(x) = 0_E$, ce qui conclut. $\square$

Remarques.

- On a le même résultat pour les matrices : si $A \in \mathcal{M}_n(\mathbb{K})$, alors $\chi_A(A) = 0$.
- On obtient une preuve plus simple du résultat démontré dans le chapitre RÉDUCTION DES ENDOMORPHISMES : une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est nilpotente si et seulement si $\chi_A = X^n$.

Démonstration. Si A est nilpotente d'indice p , alors X^p est annulateur de A , donc A a pour seule valeur propre 0, et son polynôme caractéristique est donc X^n .

Si $\chi_A = X^n$, alors $\chi_A(A) = 0$, c'est-à-dire $A^n = 0_{n,n}$, et A est nilpotente. $\square$

Corollaire – Racines du polynôme minimal et valeurs propres

Soit $u \in \mathcal{L}(E)$. Les racines du polynôme minimal μ_u sont exactement les valeurs propres de u : $Z(\mu_u) = \text{Sp}(u)$.

Démonstration. Comme μ_u est annulateur de u , on a $\text{Sp}(u) \subset Z(\mu_u)$. Par ailleurs, d'après Cayley-Hamilton, $\mu_u \mid \chi_u$, donc $Z(\mu_u) \subset Z(\chi_u) = \text{Sp}(u)$. Ceci donne par double inclusion $Z(\mu_u) = \text{Sp}(u)$. $\square$

Remarque. Si $u \in \mathcal{L}(E)$ et χ_u est scindé : $\chi_u = \prod_{i=1}^k (X - \lambda_i)^{m_i}$, alors μ_u s'écrit $\mu_u = \prod_{i=1}^k (X - \lambda_i)^{r_i}$, où $r_i \in \llbracket 1, m_i \rrbracket$ pour tout $i \in \llbracket 1, k \rrbracket$.

Exemple. Le polynôme minimal de $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est $(X - 1)^2$.

En effet, on a $\chi_A = (X - 1)^2$, donc on déduit que le polynôme minimal vaut $(X - 1)^2$ ou $X - 1$. Or $X - 1$ n'annule pas A car $A \neq I_2$. Ainsi, on a bien $\mu_A = (X - 1)^2$.

II Polynômes annulateurs et réduction

1. Lemme de décomposition des noyaux

Théorème – Lemme des noyaux

Soient E un K -espace vectoriel de dimension quelconque, $u \in \mathcal{L}(E)$ et $P_1, \dots, P_k \in \mathbb{K}[X]$ des polynômes premiers entre eux deux à deux et $P = P_1 \dots P_k$. Alors

$$\text{Ker}(P(u)) = \bigoplus_{i=1}^k \text{Ker}(P_i(u)).$$

En particulier, si P annule u , alors $E = \bigoplus_{i=1}^k \text{Ker}(P_i(u))$.

1. Voir le TD du Chapitre RÉDUCTION DES ENDOMORPHISMES.

Démonstration. On se contente de démontrer le cas $k = 2$, le cas général s'en déduisant par récurrence en remarquant que si $P_1, \dots, P_k$ sont premiers entre eux deux à deux, alors $P_1 \dots P_{k-1}$ et P_k sont premiers entre eux.

Cas $k = 2$. Comme P_1 et P_2 sont premiers entre eux, on peut écrire une relation de Bézout : il existe $A, B \in \mathbb{K}[X]$ tels que $AP_1 + BP_2 = 1$. Ainsi, comme $A(u) \circ P_1(u) + B(u) \circ P_2(u) = \text{Id}_E$, on a :

$$\forall x \in E, A(u) \circ P_1(u)(x) + B(u) \circ P_2(u)(x) = x. \quad (1)$$

- Si $x \in \text{Ker}(P_1(u)) \cap \text{Ker}(P_2(u))$, alors $x = A(u)(P_1(u)(x)) + B(u)(P_2(u)(x)) = 0_E$, donc $\text{Ker}(P_1(u))$ et $\text{Ker}(P_2(u))$ sont en somme directe.
- Montrons que $\text{Ker}(P(u)) = \text{Ker}(P_1(u)) + \text{Ker}(P_2(u))$.

- ◊ On a $\text{Ker}(P_1(u)) \subset \text{Ker}(P(u))$: si $x \in \text{Ker}(P_1(u))$, alors $P(u)(x) = (P_1 P_2)(u)(x) = P_2(u) \circ P_1(u)(x) = 0_E$. De même, $\text{Ker}(P_2(u)) \subset \text{Ker}(P(u))$, donc $\text{Ker}(P_1(u)) + \text{Ker}(P_2(u)) \subset \text{Ker}(P(u))$.
- ◊ Montrons l'autre inclusion : si $x \in \text{Ker}(P(u))$, on peut écrire $x = x_1 + x_2$, où $x_1 = B(u) \circ P_2(u)(x)$ et $x_2 = A(u) \circ P_1(u)(x)$, d'après (1). Or comme $(P_1 P_2)(u)(x) = P(u)(x) = 0_E$, on a

$$P_1(u)(x_1) = P_1(u) \circ B(u) \circ P_2(u)(x) = B(u) \circ (P_1 P_2)(u)(x) = 0_E$$

car les polynômes en u commutent. De même, on a $P_2(u)(x_2) = A(u) \circ (P_2 P_1)(u)(x_2) = 0_E$. Par conséquent, $x_1 \in \text{Ker}(P_1(u))$ et $x_2 \in \text{Ker}(P_2(u))$, et $x \in \text{Ker}(P_1(u)) + \text{Ker}(P_2(u))$.

Finalement, on a bien $\text{Ker}(P(u)) = \text{Ker}(P_1(u)) \oplus \text{Ker}(P_2(u))$. □

Remarque. On retrouve alors le résultat suivant : si E est un espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$ et χ_u est scindé à racines simples, alors u est diagonalisable.

En effet, on note $\chi_u = (X - \lambda_1) \dots (X - \lambda_k)$, où $\lambda_1, \dots, \lambda_k$ sont distincts. En notant $P_i = X - \lambda_i$ pour $i \in \llbracket 1, k \rrbracket$, les polynômes P_i sont premiers entre eux deux à deux. Or par Cayley-Hamilton, χ_u est annulateur de u , donc le lemme des noyaux donne

$$E = \bigoplus_{i=1}^k \text{Ker}(u - \lambda_i \text{Id}_E).$$

donc u est diagonalisable.

Notons par ailleurs qu'on a seulement utilisé le fait que χ_u est annulateur de u . Par conséquent, comme on le reverra dans la suite, le résultat est valable pour tout polynôme annulateur scindé à racines simples.

Exemple. Trouvons toutes les solutions $y \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ de l'équation différentielle $(\mathcal{E}) : y^{(3)} = -y'' - y' - y$.

On note $E = \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ et on introduit $u \in \mathcal{L}(E)$ défini par $u : y \mapsto y'$. En notant $P = X^3 + X^2 + X + 1$, on constate que si $y \in E$, alors $P(u)(y) = y^{(3)} + y'' + y' + y$. Ainsi, y est solution de $(\mathcal{E})$ si et seulement si $y \in \text{Ker } P(u)$.

Par ailleurs², on a $P = (X + 1)(X^2 + 1)$. Comme $X + 1$ et $X^2 + 1$ sont premiers entre eux, le lemme des noyaux donne $\text{Ker } P(u) = \text{Ker}(u + \text{Id}_E) \oplus \text{Ker}(u^2 + \text{Id}_E)$.

- ◊ $\text{Ker}(u + \text{Id}_E) = \{y \in E, y' = -y\} = \{x \mapsto a e^{-x}, a \in \mathbb{R}\}$.
- ◊ $\text{Ker}(u^2 + \text{Id}_E) = \{y \in E, y'' = -y\} = \{x \mapsto b \cos x + c \sin x\}$

Ainsi, les solutions de $(\mathcal{E})$ sont les fonctions de la forme $y : x \mapsto a e^{-x} + b \cos x + c \sin x$, où $a, b, c \in \mathbb{R}$.

2. Polynômes annulateurs et diagonalisabilité

Nous allons déduire de ce qui précède une nouvelle condition nécessaire et suffisante de diagonalisabilité, algébrique cette fois, qui repose sur l'utilisation de polynômes annulateurs.

Théorème - Condition nécessaire et suffisante de diagonalisabilité

Soit $u \in \mathcal{L}(E)$. Les assertions suivantes sont équivalentes.

- i. u est diagonalisable.
- ii. Il existe un polynôme scindé à racines simples annulateur de u .

2. Par exemple en se souvenant que $X^4 - 1 = (X - 1)(X^3 + X^2 + X + 1)$, donc $(X^3 + X^2 + X + 1) = (X + 1)(X + i)(X - i)$.

iii. Le polynôme minimal de u est scindé à racines simples.

Démonstration.

- i. $\Rightarrow$ ii. Comme nous l'avons vu plus haut, si u est diagonalisable, alors $\mu_u = \prod_{\lambda \in \text{Sp}(u)} (X - \lambda)$, donc μ_u est un polynôme annulateur de u scindé à racines simples.
- ii. $\Rightarrow$ iii. Si P est un polynôme scindé à racines simples annulateur de u , alors μ_u divise P , donc μ_u est également scindé à racines simples.
- iii. $\Rightarrow$ i. Si μ_u est scindé à racines simples, données par $\lambda_1, \dots, \lambda_k$, alors $\mu_u = \prod_{i=1}^k (X - \lambda_i)$ est annulateur de u , et par le lemme des noyaux,

$$E = \bigoplus_{i=1}^k \text{Ker}(u - \lambda_i \text{Id}_E), \quad \text{donc } u \text{ est diagonalisable.} \quad \square$$

Remarques.

- Si un polynôme P est scindé à racines simples, on dit parfois aussi que P est simplement scindé.
- Pour montrer qu'un endomorphisme (ou une matrice) est diagonalisable, il suffit donc de trouver un polynôme scindé à racines simples qui l'annule (pas nécessairement le polynôme minimal).

Exemples.

- On retrouve la diagonalisabilité des projecteurs et symétries de E :
 - ◊ Si p est un projecteur, $X^2 - X = X(X - 1)$ est annulateur de p et simplement scindé.
 - ◊ Si s est une symétrie, $X^2 - 1 = (X - 1)(X + 1)$ est annulateur de s et simplement scindé.

Dans les deux cas, le polynôme annulateur obtenu n'est pas nécessairement le polynôme minimal, mais ça ne change pas la conclusion.

- Si $A \in \mathcal{M}_n(\mathbb{K})$ est une matrice nilpotente d'indice p , on a vu que $\mu_A = X^p$. Ainsi, A est diagonalisable si et seulement si $p = 1$, c'est-à-dire A est nulle. Ainsi, toute matrice nilpotente non nulle n'est pas diagonalisable.

Corollaire - Diagonalisabilité d'un endomorphisme induit

Si $u \in \mathcal{L}(E)$ est un endomorphisme diagonalisable et F un sous-espace vectoriel de E non nul et stable par u , alors l'endomorphisme u_F induit par u sur F est diagonalisable.

Démonstration. Nous avons vu que μ_{u_F} divise μ_u . Comme u est diagonalisable, μ_u est simplement scindé, donc μ_{u_F} l'est également, ce qui assure que u_F est diagonalisable. $\square$

Exercice 1. Soient $u, v \in \mathcal{L}(E)$ deux endomorphismes diagonalisables qui commutent. Alors il existe une base $\mathcal{B}$ de vecteurs propres communs à u et v . Autrement dit, les matrices de u et v sont toutes deux diagonales dans la base $\mathcal{B}$.

3. Réduction des endomorphismes à polynôme annulateur scindé

Théorème - Endomorphismes à polynôme annulateur scindé

Soit $u \in \mathcal{L}(E)$. Les trois assertions suivantes sont équivalentes.

- i. Le polynôme caractéristique χ_u est scindé.
- ii. u admet un polynôme annulateur scindé.
- iii. Le polynôme minimal μ_u est scindé.

Démonstration.

- i. $\Rightarrow$ ii. Par Cayley-Hamilton, χ_u est annulateur de u , ce qui conclut.
- ii. $\Rightarrow$ iii. Si u admet un polynôme annulateur scindé P , on sait que μ_u divise P , donc μ_u est scindé également.

- iii. $\Rightarrow$ i. Supposons que μ_u est scindé. Si $\mathbb{K} = \mathbb{C}$, χ_u est bien sûr scindé. Si $\mathbb{K} = \mathbb{R}$ et χ_u n'est pas scindé alors χ_u admet une racine qui n'est pas réelle, ce qui est impossible car χ_u et μ_u ont les mêmes racines complexes, qui sont les valeurs propres complexes de u . $\square$

Corollaire - Condition nécessaire et suffisante de trigonalisabilité

Si $u \in \mathcal{L}(E)$, alors u est trigonalisable si et seulement si u admet un polynôme annulateur scindé.

Démonstration. On sait que u est trigonalisable si et seulement si χ_u est scindé, donc le théorème conclut. $\square$

Dans le cas où l'endomorphisme u est annulé par un polynôme scindé, nous allons voir qu'on peut trouver une base dans laquelle la matrice de u est diagonale par blocs, avec des blocs triangulaires dont les coefficients diagonaux sont les valeurs propres.

Définition-théorème - Sous-espaces caractéristiques

Soit $u \in \mathcal{L}(E)$ de polynôme caractéristique χ_u scindé. On note $\lambda_1, \dots, \lambda_k$ les valeurs propres de u et $m_1, \dots, m_k$ leurs multiplicités respectives. Alors

$$E = \bigoplus_{i=1}^k \text{Ker}(u - \lambda_i \text{Id}_E)^{m_i} \quad (2)$$

On appelle *sous-espaces caractéristiques* de u les espaces $\text{Ker}(u - \lambda_i \text{Id}_E)^{m_i}$. Dans la suite, on notera $F_\lambda(u)$ le sous-espace caractéristique $\text{Ker}(u - \lambda_i \text{Id}_E)^{m_i}$ associé à la valeur propre λ de u .

Démonstration. Par le théorème de Cayley-Hamilton, on sait que le polynôme $\chi_u = \prod_{i=1}^k (X - \lambda_i)^{m_i}$ est annulateur de u et les polynômes $P_i = (X - \lambda_i)^{m_i}$ sont premiers entre eux deux à deux, donc

$$E = \text{Ker } \chi_u(u) = \bigoplus_{i=1}^k \text{Ker}(P_i(u)) = \bigoplus_{i=1}^k \text{Ker}(u - \lambda_i \text{Id}_E)^{m_i}$$

par le lemme de décomposition des noyaux. $\square$

Remarques.

- Les sous-espaces caractéristiques de u sont stables par u , comme noyaux de polynômes en u . On peut donc considérer l'endomorphisme u_i induit par u sur $F_{\lambda_i}(u)$.
- L'endomorphisme $u_i - \lambda_i \text{Id}_E$ est nilpotent sur $F_{\lambda_i}(u)$: pour tout $x \in F_{\lambda_i}(u)$, $(u_i - \lambda_i \text{Id}_E)^{m_i}(x) = 0_E$.

Théorème - Dimension des sous-espaces caractéristiques

Soient $u \in \mathcal{L}(E)$ de polynôme caractéristique scindé, et $\lambda_1, \dots, \lambda_k$ ses valeurs propres, de multiplicités respectives $m_1, \dots, m_k$. Pour tout $i \in \llbracket 1, k \rrbracket$,

$$\dim \text{Ker}(u - \lambda_i \text{Id}_E)^{m_i} = m_i.$$

Démonstration. Pour $i \in \llbracket 1, k \rrbracket$, on considère l'endomorphisme u_i induit par u sur $F_{\lambda_i}(u) = \text{Ker}(u - \lambda_i \text{Id}_E)^{m_i}$. Comme $(X - \lambda_i)^{m_i}$ est un polynôme annulateur de u_i , on en déduit que λ_i est la seule valeur propre de u_i , donc son polynôme caractéristique est $\chi_{u_i} = (X - \lambda_i)^{d_i}$, où $d_i = \dim F_{\lambda_i}(u)$. Comme χ_{u_i} divise χ_u , on a $d_i \leq m_i$.

Ainsi, $\sum_{i=1}^k d_i \leq \sum_{i=1}^k m_i = n$. Or par (2), $\sum_{i=1}^k d_i = n$, ce qui entraîne que $\sum_{i=1}^k \underbrace{(m_i - d_i)}_{\geq 0} = 0$, donc $\forall i \in \llbracket 1, k \rrbracket$, $d_i = m_i$. $\square$

Remarque. On déduit de ce qui précède que pour tout $i \in \llbracket 1, k \rrbracket$, avec les mêmes notations, $\chi_{u_i} = (X - \lambda_i)^{m_i}$.

Théorème - Réduction des endomorphismes à polynôme annulateur scindé

Soit $u \in \mathcal{L}(E)$ de polynôme caractéristique scindé, ayant pour valeurs propres $\lambda_1, \dots, \lambda_k$ de multiplicités respec-

tives $m_1, \dots, m_k$. Il existe une base dans laquelle la matrice de u est diagonale par blocs de la forme :

$$A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}, \quad \text{où pour tout } i \in \llbracket 1, k \rrbracket, \quad A_i = \begin{bmatrix} \lambda_i & \star & \dots & \star \\ & \ddots & \ddots & \vdots \\ & & \ddots & \star \\ & & & \lambda_i \end{bmatrix} \in \mathcal{M}_{m_i}(\mathbb{K}).$$

Démonstration. Pour tout i , on note u_i l'endomorphisme induit par u sur $F_{\lambda_i}(u) = \text{Ker}(u - \lambda_i \text{Id}_E)^{m_i}$. Comme vu plus haut, $\chi_{u_i} = (X - \lambda_i)^{m_i}$, et λ_i est la seule valeur propre de u_i . Ainsi, il existe une base $\mathcal{B}_i$ de $F_{\lambda_i}(u)$ dans laquelle la matrice de u_i est triangulaire, et a tous ses coefficients diagonaux égaux à λ_i .

En concaténant les bases $\mathcal{B}_1, \dots, \mathcal{B}_k$, on obtient une base $\mathcal{B}$ de E , dans laquelle la matrice de u a l'a forme souhaitée. $\square$