Algèbre, groupes et géométrie

[Référence Gourdon Les maths en tête Ellipses]

Leçon n° 4 Polynômes d'endomorphismes

$\mathbb{K}$ désigne un corps commutatif (pour nous $\mathbb{R}$ ou $\mathbb{C}$) et E un $\mathbb{K}$-espace vectoriel de dimension n.

I Généralités

Notation : Soit $P = a_0 + a_1 X + \dots + a_p X^p \in \mathbb{K}[X]$

- pour $u \in \mathcal{L}(E)$, on note
$$P(u) = a_0 Id_E + a_1 u + \dots + a_p u^p \in \mathcal{L}(E),$$
où $u^2 = u \circ u$, $\dots$, $u^p = \underbrace{u \circ \dots \circ u}_{p \text{ facteurs}}$,

- pour $A \in \mathcal{M}_n(\mathbb{K})$, on note
$$P(A) = a_0 I_n + a_1 A + \dots + a_p A^p \in \mathcal{M}_n(\mathbb{K}).$$

On dit que $P(u)$ est un "polynôme de l'endomorphisme u" et $P(A)$ un "polynôme de la matrice A".

Dans ce qui suit nous exprimerons le plus souvent les résultats en termes de polynômes d'endomorphismes. Les résultats en termes matriciels sont analogues.

Remarques 1) Si $u \in \mathcal{L}(E)$, $\lambda \in \mathbb{K}$, $P, Q \in \mathbb{K}[X]$, alors
$$\lambda \cdot (P(u)) = (\lambda P)(u)$$
$$P(u) + Q(u) = (P+Q)(u)$$
$$P(u) \circ Q(u) = (PQ)(u).$$
On en déduit que $\{P(u) ; P \in \mathbb{K}[X]\}$, muni de la même définition, est stable pour $+$, $\cdot$ et $\circ$. C'est donc un sous-espace vectoriel et un sous-anneau de $\mathcal{L}(E)$.

2) Avec les mêmes notations, comme on a
$$P(u) \circ Q(u) = (PQ)(u) = (QP)(u) = Q(u) \circ P(u),$$

L'anneau $(\{P(u) ; P \in \mathbb{K}[X]\}, +, \circ)$ est un sous-anneau commutatif de $\mathcal{L}(E)$ (alors qu'en dim ≥ 2, $\mathcal{L}(E)$ n'est pas commutatif : cf feuille I).

Autrement dit, deux polynômes d'un même endomorphisme commutent.

Exemple : si $M = \begin{pmatrix} a_1 & & \\ & a_2 & \\ 0 & & \ddots \\ & & & a_n \end{pmatrix}$ est triangulaire supérieure et $P \in \mathbb{K}[X]$, alors

$P(M) = \begin{pmatrix} P(a_1) & & \\ & \ddots & \\ 0 & & P(a_n) \end{pmatrix}$ et les v.p. de $P(u)$ sont les images par P des valeurs propres de M (exo à faire tout seul !).

Proposition : Soit $u \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$, tel que $P(u) = 0$. Si λ est une v.p. de u, alors $P(\lambda) = 0$.

Dem : Soit x un vecteur propre de u associé à λ.
On a $u(x) = \lambda x$, d'où, en notant $P(X) = a_0 + \dots + a_p X^p$,

$$0 = P(u)(x) = a_0 x + a_1 u(x) + \dots + a_p u^p(x)$$
$$= a_0 x + a_1 \lambda x + \dots + a_p \lambda^p x$$
$$= P(\lambda) \cdot x.$$

Mais $x \neq \vec{0}$, donc $P(\lambda) = 0$. ∎

Remarque attention, écrire $P(u)(x)$, mais pas $P(u(x))$, qui n'a pas de sens !!

Théorème de décomposition des noyaux (souvent appelé "lemme des noyaux").

Soit $u \in \mathcal{L}(E)$ et $P = P_1 \dots P_{ss} \in \mathbb{K}[X]$, les polynômes P_i étant premiers entre eux 2à 2.

Alors $\ker P(u) = \ker P_1(u) \oplus \dots \oplus \ker P_{ss}(u)$.

Dem : par récurrence sur $ss \geq 2$

→ $ss = 2$ P_1 et P_2 étant premiers entre eux, on écrit par le théorème de Bézout $U, V \in \mathbb{K}[X]$ tq

$$UP_1 + VP_2 = 1.$$

- Soit $x \in \ker P_1(u) \cap \ker P_2(u)$.

On a $\left[(UP_1 + VP_2)(u)\right](x) = Id_E(x) = x$,

mais aussi du coup $x = \left[U(u) \circ P_1(u) + V(u) \circ P_2(u)\right] x$

$= U(u)\left(\underbrace{P_2(u)(x)}_{0}\right) + V(u)\left(\underbrace{P_2(u)(x)}_{0}\right) = 0$,

et $x = 0$, ce qui montre que $\ker P_1(u) + \ker P_2(u)$ est une somme directe.

- Soit $x \in \ker P(u)$.

On a $x = \left[UP_1(u)\right](x) + \left[VP_2(u)\right](x)$ (*).

Or $\left[P_2(u)\right]\left[UP_1(u)(x)\right] = \left[U \underbrace{P_1 P_2}_{P}(u)\right](x) = 0$

et $\left[UP_1(u)\right](x) \in \ker P_2(u)$.

De même $\left[VP_2(u)\right](x) \in \ker P_1(u)$.

Donc, via (*), $x \in \ker P_1(u) + \ker P_2(u)$,

et $\ker P(u) \subset \ker P_1(u) + \ker P_2(u)$.

L'inclusion réciproque est immédiate, et finalement $\ker P(u) = \ker P_1(u) \oplus \ker P_2(u)$.

→ On suppose le résultat vrai au rang k et on le montre au rang $k+1$: avec $P = P_1 \dots P_{k+1}$, on a $P = Q_1 Q_2$ avec $Q_1 = P_1 \dots P_k$ et $Q_2 = P_{k+1}$.

Alors Q_1 et Q_2 sont premiers entre eux et on applique le cas $k=2$, puis l'hypothèse de récurrence à Q_1, d'où le résultat. ∎

Théorème Soit $u \in \mathcal{L}(E)$. L'endomorphisme u est diagonalisable ssi il existe $P \in K[X]$ scindé sur K ayant toutes ses racines simples et tel que $P(u) = 0$

dem CN : Soient $\lambda_1, \dots, \lambda_k$ les vp $\neq 2$ à 2 de u, et $E_{\lambda_1}, \dots, E_{\lambda_k}$ les sev propres associés. Soit $P = (X-\lambda_1)\dots(X-\lambda_k) \in K[X]$. Le polynôme P est scindé et a toutes ses racines simples. Comme les $X-\lambda_i$ sont premiers entre eux, $\ker P(u) = \bigoplus_i \ker(u - \lambda_i \mathrm{Id}_E) = \bigoplus_{i=1}^{k} E_{\lambda_i}$.

Mais comme u est diagonalisable, on a $\bigoplus E_{\lambda_i} = E$, qui montre que $\ker P(u) = E$, i.e $P(u) = 0$.

CS Ecrivons $P = \alpha (X-\lambda_1)\dots(X-\lambda_k)$ avec les $\lambda_i \in K$ $\neq$ à 2 à 2 et $\alpha \neq 0$.

Comme les λ_i sont $\neq$ 2 à 2, les $(X-\lambda_i)$ sont premiers entre eux, et d'après le lemme des noyaux, $\ker P(u) = E = \bigoplus \ker(u - \lambda_i \mathrm{Id}_E)$.

Soit $I = \{i ; \ker(u - \lambda_i \mathrm{Id}_E) \} \neq \{\vec{0}\}$.

Pour tout $i \in I$, λ_i est vp de u et on a $E = \bigoplus_{i \in I} \ker(u - \lambda_i \mathrm{Id}_E)$, qui montre que u est diagonalisable. ∎

Remarque : nous pouvons maintenant montrer que si $u \in \mathcal{L}(E)$ est diagonalisable et F est un sev de E stable par u, alors $u_{/F}$ est aussi diagonalisable. En effet, soit $P \in K[X]$ scindé sur K à racines simples tel que $P(u) = 0$. Alors $P(u_{/F}) = 0$, donc $u_{/F}$ est diagonalisable.

II Polynôme minimal

Soit $u \in \mathcal{L}(E)$, et $\mathcal{J} = \{ P \in K[X] ; P(u) = 0 \}$.

→ Montrons que $\mathcal{J} \neq \{0\}$:
Comme $\dim \mathcal{L}(E) = n^2$, la famille $Id_E, u, u^2, \dots, u^{n^2}$ est liée. Autrement dit, il existe $(a_0, \dots, a_{n^2}) \neq (0, \dots, 0)$ tel que $a_0 Id_E + a_1 u + \dots + a_{n^2} u^{n^2} = 0$, ce qui montre que le polynôme $P(X) = a_0 + a_1 X + \dots + a_{n^2} X^{n^2}$ vérifie $P(u) = 0$.

→ $\mathcal{J}$ est un idéal de $K[X]$ (...), qui est un anneau principal. Il existe donc un unique polynôme unitaire Π_u tel que $\mathcal{J} = (\Pi_u)$
$= \{ P \Pi_u ; P \in K[X] \}$.
On l'appelle polynôme minimal de u.

Remarques : 1) Π_u est le polynôme unitaire de plus bas degré annulateur de u, et si $Q(u) = 0$, alors $\Pi_u \mid Q$. 2) Si F est un sev stable par u, alors $v = u_{/F}$ vérifie $\Pi_v \mid \Pi_u$ car $\Pi_u(v) = 0$.

On déduit du théorème précédent :

Théorème : $u \in \mathcal{L}(E)$ est diagonalisable ssi son polynôme minimal est scindé à racines simples

(démonstration orale...)

Proposition Soit $u \in \mathcal{L}(E)$. Un scalaire λ est vp de u si et seulement si λ est racine de son polynôme minimal.

dem **CN** On a vu que $P(u) = 0$ entraîne pour λ vp que $P(\lambda) = 0$.
On conclut donc avec $\Pi_u(u) = 0$.

CS Soit λ racine du polynôme minimal Π_u, posons $\Pi_u = (X-\lambda)P$.
On a $P(u) \neq 0$ car $d^\circ P < d^\circ \Pi_u$.
Or $\Pi_u(u) = 0 = (u - \lambda Id)\circ P(u) = 0$.
On en déduit que $u - \lambda Id_E$ est non injectif : cqfd.

□