Endomorphismes cycliques

La notion d'endomorphisme cyclique peut être évoquée entre autres dans les leçons :

Exemples d'applications des idéaux d'un anneau commutatif unitaire.
Anneaux principaux.
Sous-espaces stables d'un endom. d'un espace vectoriel de dim. finie. Applications.
Polynômes d'endomorphismes. Applications.
Formes linéaires et hyperplans en dimension finie. Exemples et applications.

Pour la leçon sur les idéaux et celle sur les anneaux principaux, on parlera de μ et μ_x, générateurs d'idéaux de $k[X]$ ayant une signification géométrique. Pour la leçon sur les formes linéaires, on parlera du lemme 2 ci-dessous. Les endomorphismes cycliques sont aussi un peu présents dans la leçon sur l'exponentielle de matrices, si on évoque la non surjectivité de l'exponentielle de $\mathfrak{sl}_n(\mathbb{C})$ (cf le développement correspondant).

$\therefore$

Soit E un espace vectoriel de dimension finie sur un corps k. Pour $u \in \mathrm{L}(E)$ et $P \in k[X]$ on notera parfois simplement Pu au lieu de $P(u)$. On considère le morphisme d'algèbres

$$\begin{array}{rcl} \varphi\colon k[X] & \to & \mathrm{L}(E) \\ P & \mapsto & Pu \end{array}$$

Étant donné en plus un $x \in E$ on peut considérer le morphisme de k-espaces vectoriels

$$\begin{array}{rcl} \varphi_x\colon k[X] & \to & E \\ P & \mapsto & Pu(x) \end{array}$$

On note μ resp. μ_x le générateur unitaire du noyau de φ, resp. φ_x. On note $k[u]$ resp. E_x l'image de φ, resp. de φ_x. Il est clair que pour tout $x \in E$, on a $\mu_x | \mu$.

Définition : u est *cyclique* ssi il existe $x \in E$ tel que $E_x = E$.

Théorème : *Soit $u \in \mathrm{L}(E)$, μ son polynôme minimal, χ son polynôme caractéristique. Les conditions suivantes sont équivalentes :*

(1) *u est cyclique.*
(2) *$\mu = \chi$.*
(3) *l'ensemble des endomorphismes qui commutent avec u est égal à $k[u]$.*

L'ensemble des endomorphismes qui commutent avec u est appelé *commutant* de u et noté parfois $Z(u)$. Il contient toujours $k[u]$. On montrera (1)$\Leftrightarrow$(2) après d'un premier lemme et (1)$\Leftrightarrow$(3) après un second. Dans le lemme 2 on exhibe un certain sous-espace vectoriel stable qui a un supplémentaire stable : notez le lien avec la semi-simplicité, où le phénomène étudié est précisément l'existence de supplémentaires stables. Si on ne démontre pas tout, on peut admettre le lemme 1, mais pas le lemme 2 qui est le cœur de la preuve !

Lemme 1 : *Il existe $a \in E$ tel que $\mu_a = \mu$.*

Preuve : Soit $\mu = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition en facteurs irréductibles, et $E_i = \ker(P_i^{\alpha_i} u)$. Choisissons $x_i \in E_i$ tel que $P_i^{\alpha_i - 1} u(x) \neq 0$, il est alors clair que $\mu_{x_i} = P_i^{\alpha_i}$. Posons $a = x_1 + \dots + x_r$, alors par définition de μ_a on a

$$0 = \mu_a u(a) = \underbrace{\mu_a u(x_1)}_{\in E_1} + \dots + \underbrace{\mu_a u(x_r)}_{\in E_r}$$

Comme les E_i sont en somme directe il vient $\mu_a u(x_i) = 0$ pour tout i. Par définition de μ_{x_i} on obtient $\mu_{x_i} | \mu_a$ et comme les μ_{x_i} sont premiers entre eux deux à deux, leur produit divise μ_a. Ceci montre que $\mu | \mu_a$, et comme $\mu_a | \mu$ on a fini. □

Cela suffit à montrer que (1)⇔(2). En effet par définition de μ_a et de E_a, l'application φ_a donne un isomorphisme $k[X]/(\mu_a) \simeq E_a$. Donc si on choisit a comme dans le lemme, $\mu = \chi$ équivaut à $\mu_a = \chi$, ou encore $\deg(\mu_a) = n$, i.e. $\dim(E_a) = n$.

Lemme 2 : *Soit $a \in E$ tel que $\mu_a = \mu$. Alors E_a est un sous-espace u-stable pour lequel il existe un supplémentaire u-stable.*

Preuve : Soit $k = \deg(\mu_a) = \deg(\mu)$. Par hypothèse les vecteurs $e_1 = a$, $e_2 = u(a)$,... $e_k = u^{k-1}(a)$ forment une base de E_a. Complétons-la avec des vecteurs $e_{k+1}, \dots, e_n$ en une base de E et soit $\{e_i^*\}$ la base duale. Considérons le sous-espace

$$\begin{aligned} G = & \{ x \in E,\ u^i(x) \text{ n'a pas de composante sur } e_k, \text{ pour tout } i \geq 0 \} \\ = & \bigcap_{i \geq 0} \ker(e_k^* \circ u^i) \\ = & \bigcap_{i=0}^{k-1} \ker(e_k^* \circ u^i) \quad \text{car } u^k \text{ est combinaison linéaire des } u^i \text{ pour } i \leq k-1. \end{aligned}$$

Il est clair que G est u-stable et que $E_a \cap G = \{0\}$. Si on montre que $\dim(G) = n - k$ on aura $E = E_a \oplus G$ et ce sera terminé. Pour cela montrons que les k équations d'hyperplans qui définissent G sont linéairement indépendantes :

$$\begin{aligned} \textstyle\sum_{j=0}^{k-1} \lambda_j (e_k^* \circ u^j) = 0 \ &\Rightarrow \ \textstyle\sum_{j=0}^{k-1} \lambda_j (e_k^* \circ u^{j+i}) = 0 \ (\forall i) \\ &\Rightarrow \ e_k^*(u^i(P(u)) = 0 \ (\forall i) \text{ où } P(X) = \textstyle\sum \lambda_j X^j \\ &\Rightarrow \ P(u)(a) \in G \end{aligned}$$

Comme par ailleurs $P(u)(a) \in E_a$ par définition, on obtient $P(u)(a) = 0$. Il en découle que $\mu_a | P$, et comme P est de degré au plus $k-1$ il doit être nul. Donc tous les λ_i sont nuls, ce qui montre que les équations sont linéairement indépendantes comme on le voulait. En conséquence, $\dim(G) = n - k$ et on a le résultat attendu. □

Il reste à montrer (1)⇔(3). Pour le sens direct, il suffit de montrer qu'un endomorphisme v qui commute avec u est un polynôme en u. Or par hypothèse il existe x tel que $E_x = E$, en particulier $v(x) = Pu(x)$ pour un certain polynôme P. On va montrer que $v = Pu$. Pour cela soit $y \in E = E_x$, il s'écrit $y = Qu(x)$. Comme v commute avec u il commute avec tout polynôme en u, donc

$$v(y) = v(Qu(x)) = Qu(v(x)) = Qu(Pu(x)) = Pu(Qu(x)) = Pu(y)$$

Pour (3)⇒(1) on reprend les notations de la preuve du lemme 1, $\mu = P_1^{\alpha_1} \dots P_r^{\alpha_r}$, $E_i = \ker(P_i^{\alpha_i} u)$, $a = x_1 + \cdots + x_r$ vérifiant $\mu_a = \mu$. On a une décomposition $E = E_a \oplus G$ en sous-espaces stables. Soit π le projecteur sur G parallèlement à E_a. Comme E_a et G sont u-stables, π commute avec u, donc par hypothèse, on a $\pi = P(u)$ pour un certain polynôme P. On en déduit que $P(u_{|E_a}) = \pi_{|E_a} = 0$, donc $\mu_u = \mu_{u_{|E_a}}$ divise P, donc $\pi = P(u) = 0$. Ainsi $G = 0$ et $E_a = E$, c'est-à-dire, u est cyclique.

Bibliographie :

[Gou] GOURDON, Les Maths en tête, Mathématiques pour M', *Ellipses*.