Endomorphismes cycliques

La notion d'endomorphisme cyclique peut être évoquée entre autres dans les leçons sur les anneaux principaux (122), les polynômes d'endomorphisme (153), les sous-espaces stables (154), les formes linéaires et la dualité (159). Pour la leçon sur les 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 utiles pour montrer que l'exponentielle de $\mathrm{SL}_n(\mathbb{C})$ n'est pas surjective (voir [Ro]).

Références : Mansuy et Mneimné, *Algèbre linéaire, Réduction des endomorphismes*, ou Roudier, *Algèbre linéaire*, Francinou, Gianella, Nicolas, *Oraux X-ENS : Algèbre, Tome 2*, ou Gourdon, *Algèbre*.

Soit E un espace vectoriel de dimension finie n sur un corps k. Soient $u \in \mathrm{L}(E)$ un endomorphisme et $x \in E$ un vecteur. Pour $P \in k[X]$, on notera $P(u)$ ou simplement Pu le polynôme d'endomorphisme obtenu en appliquant P à u. On considère les applications linéaires :

$$\begin{array}{ccccc} & & \overset{\mathrm{ev}_{u,x}}{\frown} & & \\ k[X] & \xrightarrow{\mathrm{ev}_u} & \mathrm{L}(E) & \xrightarrow{\mathrm{ev}_x} & E \\ P & \longmapsto & Pu & \longmapsto & (Pu)(x). \end{array}$$

On vérifie sans difficulté que le noyau de ev_u et le noyau de $\mathrm{ev}_{u,x}$ sont des idéaux non nuls de $k[X]$ ([1]). On appelle *polynôme minimal de u* le générateur unitaire du noyau de ev_u et on le note μ_u. On appelle *polynôme minimal ponctuel de u en x* le générateur unitaire du noyau de $\mathrm{ev}_{u,x}$ et on le note $\mu_{u,x}$. On note E_x l'image de $\mathrm{ev}_{u,x}$ i.e. $E_x = \mathrm{Vect}(u^i(x), i \geqslant 0)$.

Définition. On dit que u est *cyclique* s'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 $k[u]$.

Lemme 1. *Pour tout $x \in E$, on a $\mu_x = \mu_{u|E_x}$.*

Preuve : Puisque $(\mu_{u|E_x}(u))(x) = 0$ on a $\mu_x \mid \mu_{u|E_x}$. Enfin, de $(\mu_x u)(x) = 0$ et du fait que $\mu_x u$ commute à tous les u^i, on déduit $(\mu_x u)(u^i(x)) = 0$. En d'autres termes $\mu_x u$ est nul sur E_x, i.e. $\mu_x(u_{|E_x}) = 0$. On en déduit que $\mu_{u|E_x} \mid \mu_x$. Ceci prouve que $\mu_x = \mu_{u|E_x}$. □

Lemme 2. *Il existe $a \in E$ tel que $\mu_a = \mu$.*

1. La raison pour ceci est que $\mathrm{ev}_u : k[X] \to \mathrm{L}(E)$ est un morphisme de k-algèbres et $\mathrm{ev}_x : \mathrm{L}(E) \to E$ est un morphisme de $k[X]$-modules, où les structures de $k[X]$-modules sur $\mathrm{L}(E)$ et sur E sont définies à l'aide de u.

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 $\mathrm{ev}_{u,a}$ induit un isomorphisme $k[X]/(\mu_a) \simeq E_a$. 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 3. *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 $d = \deg(\mu_a) = \deg(\mu)$. Par hypothèse les vecteurs $e_1 = a, e_2 = u(a), \dots, e_d = u^{d-1}(a)$ forment une base de E_a. Complétons-la avec des vecteurs $e_{d+1}, \dots, e_n$ en une base de E et soit $\{e_i^*\}$ la base duale. Considérons le sous-espace :

$$G \overset{\text{déf}}{=} \{\, x \in E,\ u^i(x) \text{ n'a pas de composante sur } e_d, \text{ pour tout } i \geqslant 0 \,\}.$$

Sous forme plus compacte : $G = \bigcap_{i \geqslant 0} \ker(e_d^* \circ u^i)$. Il est clair que G est u-stable. Montrons que $E_a \cap G = \{0\}$. Soit $x = \sum_{i=0}^{d-1} \lambda_i u^i(a)$ un élément de E_a. Si $x \in G$, utilisant la définition de G on voit successivement que $\lambda_{d-1} = 0$ puis $\lambda_{d-2} = 0, \dots, \lambda_0 = 0$, donc $x = 0$. Ainsi E_a et G sont en somme directe. Par ailleurs, comme $u^d, u^{d+1}, \dots$ sont combinaisons linéaires des u^i pour $i \leqslant d-1$, on a $G = \bigcap_{i=0}^{d-1} \ker(e_d^* \circ u^i)$. Ainsi G est intersection de d hyperplans, donc sa dimension est $\geqslant n - d$. Il en découle que $\dim(E_a \oplus G) \geqslant d + (n-d) = n$ donc il y a en fait égalité. On déduit que $E_a \oplus G = E$ et que G est un supplémentaire u-stable de E_a. □

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 il existe un polynôme P tel que $v(x) = (Pu)(x)$. On va montrer que $v = Pu$. Pour cela soit $y \in E = E_x$, il s'écrit $y = (Qu)(x)$ pour un certain polynôme Q. 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 2, $\mu = P_1^{\alpha_1} \dots P_r^{\alpha_r}$, $E_i = \ker(P_i^{\alpha_i} u)$, $a = x_1 + \dots + x_r$ vérifiant $\mu_a = \mu$. D'après le lemme 3 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 $\pi = Pu$ pour un certain polynôme P. On en déduit que $P(u_{|E_a}) = \pi_{|E_a} = 0$, donc $\mu_{u_{|E_a}}$ divise P. Comme d'après le lemme 1 on a $\mu_{u_{|E_a}} = \mu_a = \mu$, on obtient $\pi = Pu = 0$. Ainsi $G = 0$ et $E_a = E$, c'est-à-dire que u est cyclique.

Références

[Gou] Gourdon, *Algèbre, Ellipses.*

[Ro] M. Romagny, *L'exponentielle de* $\mathrm{SL}_n(\mathbb{C})$ *n'est pas surjective*, disponible à l'adresse `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/exp_non_surjective.pdf`.