153

POLYNÔMES D'ENDOMORPHISME EN DIMENSION FINIE. APPLICATIONS À LA RÉDUCTION D'UN ENDOMORPHISME EN DIMENSION FINIE

Cadre : K est un corps commutatif, E un K-espace vectoriel de dimension $n<\infty$ et $u \in \mathcal{L}(E)$.

I POLYNÔMES D'ENDOMORPHISME

1 Définition et Structure de $K[u]$

Déf 1 : Polynôme d'endomorphisme, de matrice ([G-Al], 4.2.1)
Si $P = \sum_{i=0}^{p} a_i X^i \in K[X]$,
Pour $u \in \mathcal{L}(E)$, $P(u) = a_0 \mathrm{Id} + a_1 u + \dots + a_p u^p \in \mathcal{L}(E)$
$A \in \mathcal{M}_n(K)$, $P(A) = a_0 I_n + a_1 A + \dots + a_p A^p \in \mathcal{M}_n(K)$

Déf 2 : ([G-Al], 4.2.1)
On définit le morphisme de K-algèbres $\varphi_u : \left| \begin{array}{l} K[X] \to \mathcal{L}(E) \\ P \mapsto P(u) \end{array} \right.$.

L'algèbre des polynômes en u est $K[u] := \mathrm{Im}\, \varphi_u$.

Rq 3 : $\mathrm{Ker}\, P(u)$ et $\mathrm{Im}\, P(u)$ sont stables par u.

Thm 4 : Décomposition des noyaux ([G-Al], 4.2.1).
Soit $u \in \mathcal{L}(E)$ et $P = P_1 \dots P_k \in K[X]$, avec les polynômes P_i premiers entre eux deux à deux.
Alors : $\mathrm{Ker}\, P(f) = \mathrm{Ker}\, P_1(f) \oplus \dots \oplus \mathrm{Ker}\, P_k(f)$.

Ex 5 : On suppose $car(K) \neq 2$.
- Si p est un projecteur non-trivial, alors $E = \mathrm{Ker}\, p \oplus \mathrm{Ker}\,(p - \mathrm{Id})$
- Si s est une symétrie non-trivial, alors $E = \mathrm{Ker}\,(s - \mathrm{Id}) \oplus \mathrm{Ker}\,(s + \mathrm{Id})$.

2 Polynôme minimal.

Déf 6 : ([COG], 5.1)
Le noyau du morphisme φ_u est un idéal de $K[X]$, non-réduit à (0).
Il est engendré par un unique polynôme, appelé polynôme minimal de u, et noté π_u.

Rq 7 : Pour $P \in K[X]$, on en déduit : $P(u) = 0 \Leftrightarrow \pi_u | P$.

Ex 8 :
- Si u est nilpotent d'indice r, alors $\pi_u = X^r$.
- Si u est projecteur $\neq \mathrm{Id}, \neq 0$, alors $\pi_u = X^2 - X$.
- Si u est une symétrie $\neq \pm \mathrm{Id}$, alors $\pi_u = (X-1)(X+1)$.

Prop 9 : ([G-Al], 4.2.1)
Soit $P \in K[X]$, tel que $P(u) = 0$.
Si λ est valeur propre de u, alors $P(\lambda) = 0$.

C-Ex 10 : On n'a pas la réciproque. ([G-Al], 4.2.1)
$P = X(X-1)$ annule Id ; et 0 n'est pas valeur propre de Id.

Prop 11 : ([G-Al], 4.2.2)
Les valeurs propres de u sont les racines de π_u.

Prop 12 : ([COG], rmq 5.1.2).
Deux endomorphismes semblables ont même polynôme minimal.

C-Ex 13 : On n'a pas la réciproque.
$\begin{pmatrix} 1&0&0 \\ 0&2&0 \\ 0&0&2 \end{pmatrix}$ et $\begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&2 \end{pmatrix}$ ne sont pas semblables mais ont même polynôme minimal.

Prop 14 : ([COG], lm 5.1.4)
Soient $F_1, \dots, F_r$ des sev de E stables par u, tels que $E = \bigoplus_{j=1}^{r} F_j$.
On a : $\pi_u = \mathrm{ppcm}\{\pi_{u|_{F_1}}, \dots, \pi_{u|_{F_r}}\}$.

Thm 15 : Structure de $K[u]$ ([COG], prop 5.1.1)
- φ_u induit l'isomorphisme de K-algèbres : $K[u] \simeq K[X]/(\pi_u)$.
- $K[u]$ est un K-ev de dimension $\deg(\pi_u)$.
- $(u^j)_{0 \leq j \leq \deg(\pi_u)-1}$ est une base du Kev $K[u]$.

Rq 16 : Si $\pi_u = P_1 \dots P_r$, avec $P_1, \dots, P_r$ premiers entre eux deux à deux,
Alors le théorème chinois fournit : $K[u] \simeq K[X]/(P_1) \times \dots \times K[X]/(P_r)$.

3 Polynôme caractéristique.

Déf 17 : Polynôme caractéristique d'une matrice ([COG], 5.3.1)
Soit $A \in \mathcal{M}_n(K)$; on pose $\chi_A = \det(X I_n - A)$

Prop 18 : ([COG], 5.3.1)
Deux matrices semblables ont même polynôme caractéristique.
Ceci permet de définir le polynôme caractéristique χ_u de u comme celui de sa matrice dans n'importe quelle base.

Ex 19 :
- Si u est nilpotent, alors $\chi_u = X^n$.
- Si u est un projecteur, alors $\chi_u = X^p (1-X)^{n-p}$ où $p := \dim \mathrm{Ker}\, u$.

Prop 20 : ([COG], prop. 5.3.1)
Les valeurs propres de u sont les racines de χ_u.

App 21 : Si K est algébriquement clos, alors $Sp(u) \neq \emptyset$. ([COG], prop 5.3.4)

C-Ex 22 : C'est faux en dimension
Si $K = \mathbb{C}$, $E = \mathbb{C}[X]$, $u : \left| \begin{array}{l} E \to E \\ P \mapsto XP \end{array} \right.$. $Sp(u) = \emptyset$ ([COG], rq 5.3.1)

Prop 23 : ([COG], prop 5.3.3)
Soit F un sev stable par u.
Alors $\chi_{u|_F} | \chi_u$.

Thm 24: Cayley-Hamilton ([G-A], 4.2.3)

On a : $\chi_u(u) = 0$.

Rq 25. On en déduit $\pi_u | \chi_u$ et $\deg \pi_u \leq n$.

App 26: Si $\chi_u(0) \neq 0$, alors u est inversible et $u^{-1} \in K[u]$ ([G-A], exo 4.2.4.1)

II UN OUTIL POUR LA RÉDUCTION

1 Critères de diagonalisabilité.

Thm 27: ([OA], thm 4.41)

S'équivalent : 1) u est diagonalisable

2) il existe un polynôme annulateur de u scindé à racines simples.

3) π_u est scindé à racines simples

4) χ_u est scindé et pour toute valeur propre λ, la dimension du sous-espace propre E_λ est égale à la multiplicité de λ dans χ_u.

Ex 28: ([OA], ex 4.42-43)

- Les projecteurs sont diagonalisables.
- Si car$(K) \neq 2$, alors les symétries sont diagonalisables.

↳ $\left| \begin{array}{l} \mathcal{M}_n(K) \to \mathcal{M}_n(K) \\ A \mapsto {}^tA \end{array} \right.$ est diagonalisable.

App 29: Si $K = \mathbb{F}_q$, alors u est diagonalisable $\Leftrightarrow u^q - u = 0$ ([OA], ex 4.44)

App 30: Théorème de Burnside. ([XENS-Al2], exo 3.8)

Soit G un sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini,

ie : $\exists N \in \mathbb{N}^*, \forall A \in G, A^N = I_n$.

Alors $\#G < \infty$.

DÉVELOPPEMENT N°1

App 31: ([OA], app 4.45)

Si u est diagonalisable et F un sev de E stable par u,

Alors $u_{|F}$ est diagonalisable.

2 Critères de trigonalisabilité

Thm 32: ([OA], thm 4.46)

S'équivalent : 1) u est trigonalisable.

2) il existe un polynôme annulateur de u scindé.

3) π_u est scindé

4) χ_u est scindé.

Rq 33: Si K est algébriquement clos, u est trigonalisable ([OA], ex 4.47)

App 34: $\forall A \in \mathcal{M}_n(\mathbb{C})$, $\exp(\mathrm{tr}(A)) = \det(\exp(A))$.

App 35: Si u est trigonalisable et F un sev de E stable par u,

Alors $u_{|F}$ est trigonalisable.

3 Décomposition de Dunford.

Lem 36: ([G-A], prop 4.4.1)

Soit $F \in K[X]$ un polynôme annulateur de u,

$F = M_1^{\alpha_1} \dots M_s^{\alpha_s}$ une décomposition en facteurs irréductibles de $K[X]$.

Pour $i \in [\![1, s]\!]$, on note : $N_i = \mathrm{Ker}\, M_i^{\alpha_i}(f)$.

Alors : • $E = N_1 \oplus \dots \oplus N_s$.

• $\forall i \in [\![1, s]\!]$, la projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en u.

Thm 37: Décomposition de Dunford ([G-A], thm 4.4.3)

On suppose que χ_u soit scindé sur K.

Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que :

- d est diagonalisable, n est nilpotent
- $u = d + n$ et $d \circ n = n \circ d$.

De plus, $(d, n) \in K[u]^2$.

DÉVELOPPEMENT N°2.

App 38: ([COG], exo 5.6.2)

L'exponentielle est une application surjective de $\mathcal{M}_n(\mathbb{C})$ dans $GL_n(\mathbb{C})$.

App 39:

Si χ_u est scindé, alors u diagonalisable $\Leftrightarrow \exp(u)$ diagonalisable

4 Décomposition de Frobenius. ([G-A], Anx B)

Déf 40.

Pour $x \in E$, on pose $\varphi_x : \left| \begin{array}{l} K[X] \to E \\ P \mapsto P(u)(x) \end{array} \right.$, application linéaire.

On note $E_x := \mathrm{Im}\, \varphi_x$ et $\pi_{u,x}$ le générateur unitaire de l'idéal $\mathrm{Ker}\, \varphi_x$.

Rq 41. Si $d = \deg(\pi_{u,x})$, alors $(x, \dots, u^{d-1}(x))$ est une base de E_x.

Lem 42:

Il existe $x \in E$ tel que $\pi_{u,x} = \pi_u$.

Déf 43: Endomorphisme cyclique.

On dit que u est cyclique si il existe $x \in E$ tel que $E_x = E$.

Cela équivaut à $\deg(\pi_u) = n$ ou encore $\pi_u = \chi_u$.

Déf 44: Matrice compagnon.

À $P = X^p + a_{p-1} X^{p-1} + \dots + a_0 \in K[X]$, on associe la matrice

$$\mathcal{C}_P = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{p-2} \\ 0 & \cdots & 1 & -a_{p-1} \end{pmatrix} \in \mathcal{M}_p(K), \text{ appelée matrice compagnon de } P$$

Prop 45:
Soit $P \in K[X]$, unitaire ; on a : $\chi_{\mathcal{C}_P} = P = \pi_{\mathcal{C}_P}$.

Prop 46:
Soit $u \in \mathcal{L}(E)$; on a :
u est cyclique $\Leftrightarrow$ il existe une base $\mathcal{B}$ de E telle que $\mathcal{M}at_{\mathcal{B}}\, u$ soit une matrice compagnon.

Thm 47: Invariants de similitude.
Soit $u \in \mathcal{L}(E)$, il existe $F_1, \dots, F_r$ sev u-stables de E tels que :
1) $E = F_1 \oplus \dots \oplus F_r$
2) $\forall i \in [\![1, r]\!]$, $u_{|F_i}$ est cyclique
3) $\forall i \in [\![1, r-1]\!]$, $\pi_{u_{|F_{i+1}}} \mid \pi_{u_{|F_i}}$

La suite $\pi_{u_{|F_1}}, \dots, \pi_{u_{|F_r}}$ ne dépend que de u : on l'appelle suite des invariants de similitude de u.

Thm 48: Réduction de Frobenius.
On note $P_1, \dots, P_r$ la suite des invariants de similitude de u.
Alors, il existe une base $\mathcal{B}$ de E, telle que : $\mathcal{M}at_{\mathcal{B}}(u) = \begin{pmatrix} \mathcal{C}_{P_1} & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}_{P_r} \end{pmatrix}$

App 49:
- Soient $f, g \in \mathcal{L}(E)$. f et g sont semblables $\Leftrightarrow$ ils ont mêmes invariants de similitude.
- Dans $\mathcal{M}_n(\mathbb{R})$ ($n = 2$ ou 3), deux matrices sont semblables $\Leftrightarrow$ elles ont mêmes polynômes minimal et caractéristique.
- Soit L/K une extension de corps, $A, B \in \mathcal{M}_n(K)$.
Si A et B sont semblables sur $\mathcal{M}_n(L)$, alors elles sont semblables sur $\mathcal{M}_n(K)$.
- Si les seuls endomorphismes commutant avec u sont dans $K[u]$, Alors u est cyclique.

III APPLICATIONS

1 Calculs de puissances et d'inverses

App 50: Calcul de puissances positives. ([METH], 5.9)
Soit P un polynôme annulateur de $A \in \mathcal{M}_n(K)$, soit $s \in \mathbb{N}^*$.
On écrit la division euclidienne : $X^s = P(X).Q_s(X) + R_s(X)$.
On obtient donc $A^s = R_s(A)$ où $\deg R_s < \deg P$.

App 51: Prolongement de l'application 50. ([METH], 5.9)
Supposons que P soit scindé à racines simples.
Notons $\lambda_1, \dots, \lambda_p$ ses racines, où $p = \deg P$.
Alors $R_s(X) = \alpha_{p-1}^{(s)} X^{p-1} + \dots + \alpha_0^{(s)}$
Les coefficients de R_s sont donnés en résolvant le système linéaire :
$$\begin{cases} \lambda_1^s = \alpha_{p-1}^{(s)} \lambda_1^{p-1} + \dots + \alpha_0^{(s)} \\ \vdots \\ \lambda_p^s = \alpha_{p-1}^{(s)} \lambda_p^{p-1} + \dots + \alpha_0^{(s)} \end{cases}$$

App 52: Calcul d'inverse. ([METH], 5.15)
Soit $P \in K[X]$, tel que $P(A) = 0$, et $P(0) \neq 0$
On dispose donc d'une relation du type :
$$A^p + \alpha_{p-1} A^{p-1} + \dots + \alpha_0 I_n = 0$$
Qu'on transforme alors en : $A\left(-\frac{1}{\alpha_0} A^{p-1} - \frac{\alpha_{p-1}}{\alpha_0} A^{p-2} - \dots - \frac{\alpha_1}{\alpha_0} I_n\right) = I_n$
Ainsi A est inversible et on peut calculer son inverse.

2 Calcul d'exponentielles.

Prop 53: ([METH], 12.1)
Soit $A \in \mathcal{M}_n(K)$.
La série $\sum_{p \geq 0} \frac{A^p}{p!}$ converge. On note $\exp(A)$.

Prop 54: ([METH], 12.2)
$\exp(A) \in K[A]$

Prop 55: Décomposition de Dunford de l'exponentielle ([METH], 12.9)
Si $A = D + N$ est la décomposition de Dunford de $A \in \mathcal{M}_n(K)$,
Alors $\exp(A) = \exp(D) + \exp(D).[\exp(N) - I_n]$ est celle de $\exp(A)$.

App 56: Calcul de $\exp(A)$ ([METH], 12.9)
Plus simplement, si $A = D + N$ est la décomposition de Dunford de A,
Alors $\exp(A) = \exp(D).\exp(N)$ permet de calculer simplement $\exp(A)$.

Rq 57: Il n'est pas simple d'obtenir la décomposition de Dunford de A en général.

App 58: ([G-An], prop 6.2.2)
Soit $A \in \mathcal{M}_n(\mathbb{R})$, $V_0 \in \mathbb{R}^n$.
L'ensemble des solutions de $Y' = AY$ a ses solutions maximales définies sur $\mathbb{R}$ par $t \mapsto e^{tA} V_0$.

Références :

[G-Al] : X. Gourdon – Les maths en tête : Algèbre, 2e éd., 2009

[G-An] : X. Gourdon – Les maths en tête : Analyse, 2e éd., 2008

[COG] : M. Cognet – Algèbre linéaire, 1e éd, 2000

[OA] : V. Beck, J. Malick, G. Peyré – Objectif Agrégation, 2e éd, 2005.

[XENS-Al2] : S. Francinou, H. Gianella, S. Nicolas – Oraux X-ENS Algèbre 2, 2e éd, 2009.

[METH] : X. Merlin – Méthodix Algèbre, 1e éd, 1998.