P. Maurer
ENS Rennes

Leçon 153. Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

Devs :

- Réduction de Frobenius
- Décomposition de Dunford

Références :

1. Gourdon, Algèbre
2. Objectif Agrégation
3. Zavidovique, Un max de maths
4. FGN, Oraux X-ENS Algèbre 2

Dans ce qui suit, K désigne un corps commutatif et E est un espace vectoriel sur K, de dimension finie $n \in \mathbb{N}^*$.

1 Polynômes d'endomorphismes

1.1 L'algèbre $K[f]$

Définition 1. *Soit $P = a_n X^n + \cdots + a_0 \in K[X]$. Pour $f \in \mathcal{L}(E)$ et $A \in \mathcal{M}_n(K)$, on définit*

- $P(f) = a_n f^n + \cdots + a_0 \operatorname{Id}_E$,
- $P(A) = a_n A^n + \cdots + a_0 I_n$.

Proposition 2.

L'application $\varphi_f \colon \begin{cases} (K[X], +, \times) & \to & (\mathcal{L}(E), +, \circ) \\ P & \mapsto & P(f) \end{cases}$ *est un morphisme de k-algèbre.*

L'ensemble $K[f] := \{P(f) \mid P \in k[X]\}$ est alors une sous-algèbre commutative de $\mathcal{L}(E)$.

Exemple 3. Si $M = \operatorname{diag}(\alpha_1, \dots, \alpha_n)$, alors $P(M) = \operatorname{diag}(P(\alpha_1), \dots, P(\alpha_n))$.

Proposition 4. *Soit $f \in \mathcal{L}(E)$ et $P \in K[X]$ tel que $P(f) = 0$. Si λ est une valeur propre de f, alors $P(\lambda) = 0$.*

Théorème 5. *(Lemme des noyaux)*

Soit $f \in \mathcal{L}(E)$ et $P = P_1 \cdots P_r \in K[X]$, les polynômes P_i étant premiers entre eux deux à deux. Alors

$$\operatorname{Ker} P(f) = \operatorname{Ker} P_1(f) \oplus \cdots \oplus \operatorname{Ker} P_r(f).$$

1.2 Polynôme minimal

On se donne $f \in \mathcal{L}(E)$.

Proposition 6. *Le noyau $\operatorname{Ker} \varphi_f$ de l'application définie en proposition 2 est un idéal non nul de $K[X]$ appelé idéal des polynômes annulateurs.*

Proposition 7. *Il existe un unique polynôme unitaire $\pi_f \in K[X]$ qui engendre $\operatorname{Ker} \varphi_f$. On l'appelle le polynôme minimal de f.*

Exemple 8. Si f est un projecteur, $\pi_f = X(X+1)$. Si f est une symétrie non triviale et $\operatorname{car}(k) \neq 2$, on a $\pi_f = (X+1)(X-1)$. Si f est nilpotente d'ordre r, on a $\pi_f = X^r$.

Proposition 9. *Soit $\lambda \in k$. Alors $\lambda \in \operatorname{Sp}(f) \Longleftrightarrow \pi_f(\lambda) = 0$.*

Proposition 10. *π_f est invariant par similitude : pour tout $p \in \operatorname{GL}(E)$, $\pi_{pfp^{-1}} = \pi_f$.*

Corollaire 11. *On a l'isomorphisme de K-algèbres $K[f] \simeq K[X]/(\pi_f)$, et si $\pi_u = P_1 \cdots P_r$ avec $P_1, \dots, P_r$ premiers entre eux deux-à-deux, $K[f] \simeq K[X]/(P_1) \times \cdots \times K[X]/(P_r)$.*

Proposition 12. *Si $k = \deg(\pi_f)$, alors $K[f]$ est de dimension k, et une base est donnée par $(\operatorname{Id}_E, f, \dots, f^{k-1})$.*

Proposition 13. *Si F est un sous-espace vectoriel de E stable par f, alors $\pi_{f_{|F}} | \pi_f$. Si $E = F_1 \oplus F_2$ avec F_1 et F_2 des sous-espaces vectoriels de E stables par f, alors $\pi_f = \operatorname{ppcm}(\pi_{f_{|F_1}}, \pi_{f_{|F_2}})$.*

Proposition 14. *Soit P et Q deux polynômes unitaires tels que $\pi_f = PQ$, et $F = \operatorname{Ker} P(u)$. Alors $\pi_{u_{|F}} = P$.*

1.3 Polynôme caractéristique

Définition 15. *On appelle polynôme caractéristique de A (resp. de f) le polynôme de $k[X]$ défini par $\chi_A(X) = \det(A - X I_n)$ (resp. $\chi_f(X) = \det(f - X \operatorname{Id})$).*

Proposition 16. *Le polynôme caractéristique est stable par transposition : $\chi_{A^T} = \chi_A$.*

Proposition 17. *χ_A est un polynôme de degré n. Si $\chi_A = (-1)^n \sum_{k=0}^{n} a_k X^k$, alors on a $a_n = 1$, $a_{n-1} = -\operatorname{Tr}(A)$ et $a_0 = (-1)^n \det(A)$.*

Exemple 18. (Calcul pratique de χ_A)

Si $n=2$, $\chi_A(X)=X^2-\mathrm{Tr}(A)\,X+\det(A)$.

Si $n=3$, $\chi_A(X)=-X^3+\mathrm{Tr}(A)\,X^2-\frac{1}{2}(\mathrm{Tr}(A)^2-\mathrm{Tr}(A^2))\,X+\det(A)$.

Ces formules permettent le calcul efficace du polynôme caractéristique en petite dimension. En grande dimension (en général, à partir de $n=4$) on leur préfère l'algorithme du pivot de Gauss pour le déterminant.

Exemple 19. Si f est nilpotent, $\chi_f(X)=(-1)^n X^n$.

Théorème 20. *(Cayley-Hamilton)*

On a $\chi_f(f)=0$. Autrement dit, $\mu_f|\chi_f$.

Corollaire 21. *Les valeurs propres de f sont racines de son polynôme caractéristique (en fait, ce sont les seules).*

2 Application à la réduction des endomorphismes

2.1 Diagonalisation

Définition 22. *On dit que f est diagonalisable s'il existe une base de vecteurs propres de f. On dit que A est diagonalisable si elle est semblable à une matrice diagonale.*

Proposition 23. *(Condition suffisante de diagonalisabilité)*

Si χ_f est scindé à racines simples, alors f est diagonalisable.

Théorème 24. *Les propositions suivantes sont équivalents :*

- *f est diagonalisable.*
- *π_f est scindé à racines simples dans k.*
- *χ_f est scindé dans k et $\dim(E_\lambda)=v_\lambda$, où v_λ désigne la multiplicité de λ en tant que racine de χ_f.*
- *$E=\bigoplus_{\lambda\in\mathrm{Sp}(f)} E_\lambda$.*

Corollaire 25. *Si f possède n valeurs propres distinctes, alors f est diagonalisable.*

Exemple 26. Les projecteurs et les symétries sont toujours diagonalisables (sauf si $\mathrm{car}(k)=2$).

Les endomorphismes nilpotents non nuls ne sont jamais diagonalisables.

Exemple 27. Les matrices de rotation de $\mathbb{R}^2$ (d'angle non congru à π modulo $\mathbb{Z}$) ne sont pas diagonalisables dans $\mathcal{M}_2(\mathbb{R})$, mais elles le sont dans $\mathcal{M}_2(\mathbb{C})$.

Théorème 28. *Si $k=\mathbb{F}_q$ est fini avec $q=p^n$, f est diagonalisable si et seulement si $F(f)=0$, où $F(X)=X^q-X$.*

Proposition 29. *Soit $f,g\in\mathcal{L}(E)$ tels que $f\circ g=g\circ f$. Alors :*

i. Tout sous-espace propre de f est stable par g (en particulier $\mathrm{Ker}\, f$).

ii. $\mathrm{Im}\, f$ est stable par g.

Théorème 30. *(Diagonalisation simultannée).*

Si f et $g\in\mathcal{L}(E)$ sont des endomorphismes diagonalisables qui commutent, alors ils sont diagonalisables dans une même base de vecteurs propres : on dit qu'ils sont codiagonalisables.

2.2 Trigonalisation et applications

Définition 31. *Un endomorphisme $f\in\mathcal{L}(E)$ est dit trigonalisable s'il existe une base B de E dans laquelle la matrice de f soit triangulaire supérieure. On dit que B trigonalise f.*

Une matrice $A\in\mathcal{M}_n(K)$ est dite trigonalisable si A est semblable à une matrice triangulaire supérieure.

Théorème 32. *Un endomorphisme $f\in\mathcal{L}(E)$ est trigonalisable si et seulement si son polynôme caractéristique χ_f est scindé sur K.*

Théorème 33. *(Trigonalisation simultanée). Si f et g sont trigonalisables et commutent, alors ils sont trigonalisables dans une même base de E.*

Développement 1 :

Proposition 34. *Soit $P=P_1\cdots P_r$ un polynôme annulateur de f avec $P_1,\dots,P_r$ premiers entre eux deux à deux. On a $E=\mathrm{Ker}\,P_1(f)\oplus\cdots\oplus\mathrm{Ker}\,P_r(f)$, et la projection sur $\mathrm{Ker}\,P_i(f)$ parallèlement à $\bigoplus_{j\neq i}\mathrm{Ker}\,P_j(f)$ est un polynôme en f.*

Théorème 35. *(Décomposition de Jordan-Chevalley)*

On suppose que χ_f est scindé sur k. Alors il existe un unique couple (d,n) d'endomorphismes de $\mathcal{L}(E)$ tels que :

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

De plus, d et n sont des polynômes en f.

Application 36. Les morphismes continus de $\mathbb{U}$ vers $\mathrm{GL}_n(\mathbb{R})$ sont de la forme :

$$\varphi\colon e^{it}\mapsto Q\begin{pmatrix} R_{tk_1} & & & & & \\ & \ddots & & & (0) & \\ & & R_{tk_r} & & & \\ & & & 1 & & \\ & (0) & & & \ddots & \\ & & & & & 1 \end{pmatrix}Q^{-1}$$

Où $Q\in\mathrm{GL}_n(\mathbb{R})$, $r\in\mathbb{N}$, $k_1,\dots,k_r\in\mathbb{Z}^*$ et $R_\theta=\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}$ pour tout $\theta\in\mathbb{R}$.

2.3 Invariants de similitude

Notation 37. *Si $x \in E$, on note P_x le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X] : P(f)(x) = 0\}$, et E_x l'ensemble $\{P(f)(x) : P \in \mathbb{K}[X]\}$.*

Dans la suite, on notera k le degré de π_f et ℓ_x le degré de P_x pour $x \in E$.

Proposition 38. *L'ensemble E_x est un sous-espace vectoriel de E de dimension ℓ_x, dont une base est $(x, \ldots, f^{\ell_x - 1}(x))$.*

Théorème 39. *Il existe $x \in E$ tel que $P_x = \pi_f$.*

Définition 40. *On dit que f est cyclique s'il existe $x \in E$ tel que $E_x = E$. D'après ce qui précède, ceci équivaut à dire que $k = \deg(\pi_f) = n$, ou encore que $\pi_f = (-1)^n \chi_f$, où χ_f désigne le polynôme caractéristique de f.*

Définition 41. *Soit $P = X^p + a_{p-1} X^{p-1} + \cdots + a_0$ un polynôme unitaire de $\mathbb{K}[X]$. On appelle matrice compagnon de P la matrice $\mathcal{C}(P)$ (voire annexe).*

Proposition 42. *Le polynôme caractéristique $\chi_{\mathcal{C}(P)}$ de $\mathcal{C}(P)$ vérifie $\chi_{\mathcal{C}(P)} = (-1)^p P$.*

Développement 2 :

Théorème 43. *(Invariants de similitude)*

Soit $f \in \mathcal{L}(E)$. Il existe une suite finie $F_1, \ldots, F_r$ de sous-espaces vectoriels de E, tous stables par f, telle que

1. *$E = \bigoplus_{i=1}^r F_i$,*
2. *pour tout $i \in [\![1, r]\!]$, $f_{|F_i}$ est un endomorphisme cyclique,*
3. *si $P_i = \pi_{f_i}$, on a $P_{i+1} | P_i$ pour tout $i \in [\![1, r-1]\!]$.*

La suite $P_1, \ldots, P_r$ ne dépend que de f et non du choix de la décomposition. On l'appelle suite des invariants de similitude de f.

Application 44. (réduction de Frobenius)

Soit $f \in \mathcal{L}(E)$ et $P_1, \ldots, P_r$ la suite des invariants de similitude de f. Alors il existe une base $\mathcal{B}$ de E dans laquelle $\mathrm{mat}_{\mathcal{B}}(f) = \mathrm{diag}(\mathcal{C}(P_1), \ldots, \mathcal{C}(P_r))$. On a $P_1 = \pi_f$ et $P_1 \cdots P_r$ est le polynôme caractéristique de f, à un facteur $(-1)^n$ près.

3 Autres applications

3.1 Calcul de puissances et d'inverse

Proposition 45. *Si $A \in \mathcal{M}_n(K)$ et $P \in K[X]$ est un polynôme annulateur de A, alors écrivant $X^k = P(X)Q(X) + R(X)$ la division euclidienne de X^k par P, on a $A^k = R(A)$ avec $\deg(R) < \deg(\pi_A)$.*

Exemple 46. Si $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, alors $A^k = \frac{2^k + (-1)^{k-1}}{3} A + \frac{2^k + 2(-1)^k}{3} I_n$.

Proposition 47. *Si $A \in \mathrm{GL}_n(K)$, alors $A^{-1} \in K[A]$.*

Corollaire 48. *Pour tout $A \in \mathcal{M}_n(K)$, on a $K[A]^\times = K[A] \cap \mathrm{GL}_n(K)$.*

3.2 Exponentielle de matrice

Proposition 49. *On considère une norme d'algèbre $\|.\|$ sur $\mathcal{M}_n(k)$, par exemple la norme d'opérateur. On rappelle que $(\mathcal{M}_n(k), \|.\|)$ est alors un espace de Banach. La série $\sum_{k \in \mathbb{N}} \frac{A^k}{k!}$ est normalement convergente, donc convergente.*

Définition 50. *On note $\exp(A) = \sum_{n=0}^{+\infty} \frac{A^n}{n!}$.*

Proposition 51. *Si $P \in \mathrm{GL}_n(k)$, on a $\exp(PAP^{-1}) = P \exp(A) P^{-1}$.*

Proposition 52. *Si $A = D + N$ avec D diagonalisable et N nilpotente, alors :*

$$\exp(A) = \exp(D)\exp(N)$$

Remarque 53. Si χ_A est scindé sur k, la réduction de Jordan-Chevalley donne alors une méthode simple pour calculer $\exp(A)$. En effet, $\exp(D)$ se calcule facilement par la proposition 50, et le calcul de $\exp(N)$ est immédiat puisque $N^n = 0$ implique que $\exp(N) = \sum_{k=0}^{n-1} \frac{N^k}{k!}$.

Théorème 54. *Pour tout $A \in \mathcal{M}_n(\mathbb{C})$, on a $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.*

Corollaire 55. *L'exponentielle de matrices $\exp\colon \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.*

4 Annexe

Matrice compagnon (définition 41).

$$\mathcal{C}(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \cdots & 0 & 1 & -a_{p-1} \end{pmatrix}.$$