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

1. Notation. Dans cette leçon, on considère un corps K et un K-espace vectoriel E de dimension $n \geqslant 1$. Soient $u \in \mathscr{L}(E)$ un endomorphisme et $A \in \mathscr{M}_n(K)$ une matrice.

1. Polynômes d'endomorphisme

1.1. Polynômes et lemme des noyaux

2. Définition. Soit $P := a_d X^d + \cdots + a_1 X + a_0 \in K[X]$ un polynôme. On définit l'endomorphisme

$$P(u) := a_d u^d + \cdots + a_1 u + a_0 \operatorname{Id}_E \in \mathscr{L}(E)$$

et la matrice

$$P(A) := a_d A^d + \cdots + a_1 A + a_0 I_n \in \mathscr{M}_n(K).$$

3. Remarque. Pour tous scalaires $a_1, \dots, a_n \in K$ et tout polynôme $P \in K[X]$, on peut écrire

$$P\begin{pmatrix} a_1 & & * \\ & \ddots & \\ & & a_n \end{pmatrix} = \begin{pmatrix} P(a_1) & & * \\ & \ddots & \\ & & P(a_n) \end{pmatrix}.$$

4. Proposition. Soient $A \in \mathscr{M}_n(K)$, $Q \in \mathrm{GL}_n(K)$ et $P \in K[X]$. Alors

$$QP(A)Q^{-1} = P(QAQ^{-1}).$$

5. Proposition. L'application

$$\varphi \colon \left| \begin{array}{rcl} K[X] & \longrightarrow & \mathscr{L}(E), \\ P & \longmapsto & P(u) \end{array} \right.$$

est un morphisme de K-algèbres. En particulier, son image est une sous-K-algèbre commutative de $\mathscr{L}(E)$ que l'on note $K[u]$. On définit de même la K-algèbre $K[A]$ pour une matrice $A \in \mathscr{M}_n(K)$.

6. Exemple. La K-algèbre $K[\operatorname{Id}_E]$ est l'ensemble des homothéties de E.

7. Proposition. Soit $P \in K[X]$ un polynôme vérifiant $P(u) = 0$. Alors toute valeur propre $\lambda \in K$ de l'endomorphisme u satisfait $P(\lambda) = 0$.

8. Contre-exemple. La réciproque est fausse : le polynôme $X(X-1)$ annule l'identité Id_E, mais cette dernière n'admet pas 0 comme valeur propre.

9. Théorème *(lemme des noyaux)*. Soient $P_1, \dots, P_k \in K[X]$ des polynômes deux à deux premiers entre eux. Notons $P := P_1 \cdots P_k$. Alors

$$\operatorname{Ker} P(u) = \operatorname{Ker} P_1(u) \oplus \cdots \oplus \operatorname{Ker} P_k(u).$$

De plus, les projections sur chacun des sous-espaces $\operatorname{Ker} P_i(u)$ associés à cette décomposition sont des polynômes en l'endomorphisme u.

1.2. Le polynôme minimal

10. Définition. Un polynôme $P \in K[X]$ *annule* l'endomorphisme u si $P(u) = 0$.

11. Proposition. L'ensemble

$$\operatorname{Ker} \varphi = \{P \in K[X] \mid P(u) = 0\} \subset K[X]$$

est un idéal propre non nul de l'anneau principal $K[X]$. En particulier, il est engendré par un unique polynôme unitaire non constant $\pi_u \in K[X]$, appelé le *polynôme minimal* de l'endomorphisme u. On définit de même le polynôme minimal d'une matrice.

12. Corollaire. Alors les K-algèbres $K[u]$ et $K[X]/(\pi_u)$ sont isomorphes. En particulier, la dimension du K-espace vectoriel $K[u]$ est le degré du polynôme π_u.

13. Exemple. Le polynôme minimal de l'identité est le polynôme $X - 1$. Celui d'un endomorphisme nilpotent est de la forme X^k où l'entier $k \geqslant 1$ est son indice de nilpotence.

14. Proposition. Deux matrices semblables ont le même polynôme minimal.

15. Contre-exemple. La réciproque est fausse : les matrices $\operatorname{diag}(0,0,1)$ et $\operatorname{diag}(0,1,1)$ ont le même polynôme minimal et elles ne sont pas semblables.

16. Proposition. Les valeurs propres d'un endomorphisme sont exactement les racines de son polynôme minimal.

17. Application. Soit $u \in \mathrm{GL}(E)$ un isomorphisme. Alors son polynôme minimal est de la forme $\pi_u = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ avec $a_0 \neq 0$. En particulier, on a

$$u^{-1} = -a_0^{-1}[a_d u^{d-1} + \cdots + a_1 \operatorname{Id}_E] \in K[u].$$

18. Corollaire. Soit $u \in \mathscr{L}(E)$ un endomorphisme. Alors

$$K[u]^\times = K[u] \cap \mathrm{GL}(E).$$

19. Proposition. On suppose que le polynôme minimal π_u s'écrit sous la forme

$$\pi_u = \prod_{i=1}^{d} (X - \lambda_i)^{\alpha_i}$$

avec $\lambda_i \in K$ et $\alpha_i \in \mathbf{N}^*$. Alors

$$E = \bigoplus_{i=1}^{d} \operatorname{Ker}[(u - \lambda_i \operatorname{Id}_E)^{\alpha_i}].$$

20. Proposition. Soit $F \subset E$ un sous-espace vectoriel stable par l'endomorphisme u. Notons $v \in \mathscr{L}(F)$ l'endomorphisme induit. Alors $\pi_v \mid \pi_u$.

21. Proposition. Soient $F, G \subset E$ deux sous-espaces vectoriels stable par l'endomorphisme u vérifiant $E = F \oplus G$. Notons $v, w \in \mathscr{L}(E)$ les deux endomorphismes induits. Alors $\pi_u = \operatorname{ppcm}(\pi_v, \pi_w)$

1.3. Le polynôme caractéristique

22. Définition. Le *polynôme caractéristique* d'une matrice $A \in \mathscr{M}_n(K)$ est

$$\chi_A := \det(XI_n - A) \in K[X].$$

23. Proposition. Deux matrices semblables ont le même polynôme caractéristique.

24. Contre-exemple. La réciproque est fausse : la matrice nulle et la matrice

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathscr{M}_2(K)$$

ont le même polynôme caractéristique bien qu'elles ne soient pas semblables.

25. DÉFINITION. Le polynôme caractéristique de l'endomorphisme u est le polynôme caractéristique de sa matrice dans une base quelconque. Ce dernier ne dépend pas de la base choisie et on le note χ_u.
26. PROPOSITION. Soit $u \in \mathscr{L}(E)$ un endomorphisme. Alors son polynôme caractéristique est de la forme $\chi_u = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ avec
$$a_{n-1} = -\operatorname{tr} u \qquad \text{et} \qquad a_0 = (-1)^n \det u.$$
27. EXEMPLE. Pour $a, b, c, d \in K$, le polynôme caractéristique de la matrice
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
est le polynôme
$$\begin{vmatrix} X-a & -b \\ -c & X-d \end{vmatrix} = X^2 - (a+d)X + ad - bc.$$
28. PROPOSITION. Les valeurs propres d'un endomorphisme sont exactement les racines de son polynôme caractéristique.
29. REMARQUE. Dans toutes extensions, le polynôme minimal et le polynôme caractéristique ont les mêmes racines et, en particulier, les mêmes facteurs irréductibles.
30. COROLLAIRE. Si le corps K est algébriquement clos, alors tout endomorphisme admet une valeur propre.
31. THÉORÈME *(Cayley-Hamilton)*. Le polynôme minimal π_u de l'endomorphisme u divise son polynôme caractéristique χ_u, c'est-à-dire $\chi_u(u) = 0$.
32. EXEMPLE. Un endomorphisme $u \in \mathscr{L}(E)$ est nilpotent si et seulement si $\chi_u = X^n$.
33. COROLLAIRE. Alors $\deg \pi_u \leqslant n$.
34. APPLICATION. Soit L/K une extension finie et $\alpha \in L$ un élément algébrique. Considérons l'endomorphisme K-linéaire
$$u \colon \left| \begin{array}{l} L \longrightarrow L, \\ x \longmapsto \alpha x. \end{array} \right.$$
Alors $\chi_u(\alpha) = 0$.

2. Réduction des endomorphismes et polynômes

2.1. Diagonalisation

35. DÉFINITION. Un endomorphisme est *diagonalisable* s'il existe une base formée de vecteurs propres de cet endomorphisme, c'est-à-dire dans laquelle l'endomorphisme a une matrice diagonale.
36. PROPOSITION. Un endomorphisme dont le polynôme caractéristique est scindé simple est diagonalisable.
37. EXEMPLE. La matrice
$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$$
est diagonalisable puisque son polynôme caractéristique est $(X-1)(X-3)$.
38. CONTRE-EXEMPLE. La réciproque est fausse puisque l'identité est diagonalisable et son polynôme caractéristique vaut $(X-1)^n$.
39. THÉORÈME. Soit $u \in \mathscr{L}(E)$. Alors les points suivants sont équivalents :
- l'endomorphisme u est diagonalisable ;
- l'endomorphisme u admet un polynôme annulateur scindé simple ;
- son polynôme minimal π_u est scindé simple ;
- son polynôme caractéristique χ_u est scindé et, pour toute racine $\lambda \in K$ du polynôme χ_u de multiplicité m, on a $m = \dim \operatorname{Ker}(u - \lambda \operatorname{Id}_E)$;
- il existe des valeurs propres $\lambda_1, \dots, \lambda_p \in K$ deux à deux distinctes de l'endomorphisme u telles que
$$E = \operatorname{Ker}(u - \lambda_1 \operatorname{Id}_E) \oplus \cdots \oplus \operatorname{Ker}(u - \lambda_p \operatorname{Id}_E).$$

40. EXEMPLE. Tout projecteur $p \in \mathscr{L}(E)$ vérifie $p^2 = p$, donc il est annulé par le polynôme scindé simple $X(X-1)$, donc il est diagonalisable.
41. COROLLAIRE. Soit $F \subset E$ un sous-espace vectoriel stable par un endomorphisme diagonalisable $u \in \mathscr{L}(E)$. Alors l'endomorphisme $u|_F \in \mathscr{L}(F)$ est diagonalisable.
42. PROPOSITION. Soient $\mathbf{F}_q$ un corps fini à q éléments et E un $\mathbf{F}_q$-espace vectoriel de dimension finie. Alors un endomorphisme de E est diagonalisable si et seulement s'il est annulé par le polynôme $X^q - X$.
43. THÉORÈME. Le nombre de matrices diagonalisables dans $\mathrm{GL}_n(\mathbf{F}_q)$ vaut
$$\sum_{\substack{(n_1, \dots, n_{q-1}) \in \mathbf{N}^{q-1} \\ n_1 + \cdots + n_{q-1} = n}} \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbf{F}_q)| \cdots |\mathrm{GL}_{n_{q-1}}(\mathbf{F}_q)|}.$$
44. THÉORÈME *(spectral)*. Tout endomorphisme symétrique d'un espace euclidien est diagonalisable en base orthonormée.

2.2. Trigonalisation et réduction simultanée

45. DÉFINITION. Un endomorphisme est *trigonalisable* s'il existe une base dans laquelle sa matrice est triangulaire supérieure.
46. THÉORÈME. Soit $u \in \mathscr{L}(E)$. Alors les points suivants sont équivalents :
- l'endomorphisme u est trigonalisable ;
- l'endomorphisme u admet un polynôme annulateur scindé ;
- son polynôme minimal π_u est scindé ;
- son polynôme caractéristique χ_u est scindé.

47. COROLLAIRE. Si le corps Kest algébriquement clos, alors tout endomorphisme est trigonalisable.
48. THÉORÈME. Soit $(u_i)_{i \in I}$ une famille d'endomorphismes diagonalisables (resp. trigonalisables) de E qui commutent deux à deux. Alors il existe une base de E dans laquelle tous les endomorphismes u_i ont une matrice diagonale (resp. triangulaire supérieure).
49. APPLICATION. La somme de deux endomorphismes diagonalisables qui commutent est diagonalisable.

2.3. La réduction de Frobenius

50. DÉFINITION. Un endomorphisme $u \in \mathscr{L}(E)$ est *cyclique* s'il existe un vecteur $x \in E$ tel que la famille $(x, u(x), \dots, u^{n-1}(x))$ soit une base de E.

51. Proposition. On note $C_P \in \mathscr{M}_d(K)$ la matrice compagnon d'un polynôme unitaire $P \in K[X]$ de degré d. Alors $\chi_{C_P} = P$.
52. Lemme. Soit $u \in \mathscr{L}(E)$ un endomorphisme. Pour un vecteur $x \in E$, on considère l'unique polynôme unitaire $\pi_{u,x} \in K[X]$ engendrant l'idéal
$$\{P \in K[X] \mid P(u)(x) = 0\} \subset K[X].$$
Alors il existe un vecteur $x \in E$ tel que $\pi_{u,x} = \pi_u$.
53. Proposition. Les points suivants sont équivalents :
- l'endomorphisme u est cyclique ;
- $\pi_u = \chi_u$;
- il existe une base dans laquelle sa matrice est une matrice compagnon.

54. Théorème *(réduction de Frobenius)*. Soit $u \in \mathscr{L}(E)$. Alors il existe un unique entier $r \geqslant 1$, des uniques polynômes unitaires non constants $P_1, \dots, P_r \in K[X]$ et des sous-espaces vectoriels $E_1, \dots, E_r \subset E$ stables par l'endomorphisme u tels que
- $E = E_1 \oplus \cdots \oplus E_r$;
- $P_r \mid \cdots \mid P_1$;
- pour tout entier $i \in [\![1, r]\!]$, l'endomorphisme $u|_{E_i}$ induit sur le sous-espace vectoriel E_i est cyclique de polynôme minimal P_i.

La suite $(P_1, \dots P_r)$ sont les *invariants de similitude* de l'endomorphisme u.
55. Corollaire. Avec les mêmes hypothèses et notations, il existe une base de E dans laquelle l'endomorphisme u ait pour matrice
$$\operatorname{diag}(C_{P_1}, \dots, C_{P_r}).$$
De plus, on a $P_1 = \pi_u$ et $P_1 \cdots P_r = \chi_u$.
56. Corollaire. Deux endomorphismes de E sont conjugués si et seulement s'ils ont les mêmes invariants de similitude.

3. Du calculs pour les endomorphismes

3.1. L'exponentielle matricielle

57. Notation. On considère ici le corps K des réels ou des complexes.
58. Définition. L'*exponentielle* d'une matrice $A \in \mathscr{M}_n(K)$ est la matrice
$$\exp A \coloneqq \sum_{k=0}^{+\infty} \frac{A^k}{k!} \in \mathscr{M}_n(K).$$
59. Remarque. Pour toute matrice inversible $P \in \mathrm{GL}_n(K)$, on a
$$\exp(PAP^{-1}) = P(\exp A)P^{-1}.$$
Si deux matrices $A, B \in \mathscr{M}_n(K)$ commutent, alors $\exp(A + B) = \exp A \exp B$.
60. Proposition. Pour toute matrice $A \in \mathscr{M}_n(K)$, on a
$$\exp A \in K[A]^\times \qquad \text{et} \qquad \det(\exp A) = e^{\operatorname{Tr} A}.$$
61. Lemme. Soit $A \in \mathscr{M}_n(\mathbf{C})$ une matrice à coefficients complexes. Alors le groupe topologique $\mathbf{C}[A]^\times$ est un ouvert connexe de $\mathbf{C}[A]$. — D1 —
62. Proposition. Soit $A \in \mathscr{M}_n(\mathbf{C})$ une matrice à coefficients complexes. Alors l'exponentielle matricielle complexe induit une surjection
$$\exp \colon \mathbf{C}[A] \longrightarrow \mathbf{C}[A]^\times.$$
63. Théorème. L'exponentielle matricielle complexe réalise un surjection — D1 —
$$\exp \colon \mathscr{M}_n(\mathbf{C}) \longrightarrow \mathrm{GL}_n(\mathbf{C}).$$
64. Contre-exemple. Le théorème est faux lorsqu'on se place sur le corps $\mathbf{R}$: la matrice $\operatorname{diag}(1, -1)$ n'est pas dans l'image de l'exponentielle.
65. Corollaire. L'image de l'exponentielle matricielle réelle est l'ensemble
$$\exp \mathscr{M}_n(\mathbf{R}) = \mathrm{GL}_n(\mathbf{R})^{\times 2} \coloneqq \{A^2 \mid A \in \mathrm{GL}_n(\mathbf{R})\}.$$

3.2. La décomposition de Dunford et une application

66. Théorème *(Dunford)*. Soit $u \in \mathscr{L}(E)$ un endomorphisme dont le polynôme caractéristique χ_u est scindé sur K. Alors il existe un unique couple $(d, n) \in \mathscr{L}(E)^2$ tel que
- $u = d + n$;
- les endomorphismes d et n commutent ;
- ils sont respectivement diagonalisable et nilpotent.

De plus, les endomorphismes d et n appartiennent à l'algèbre $K[u]$. L'écriture $u = d+n$ est la *décomposition de Dunford* de l'endomorphisme u.
67. Exemple. Attention, la décomposition de Dunford de la matrice
$$A \coloneqq \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$
n'est pas
$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
mais $A = A + 0$.
68. Application. Une matrice $A \in \mathscr{M}_n(\mathbf{C})$ est diagonalisable si et seulement si son exponentielle $\exp A$ l'est.
69. Théorème. On suppose que le corps K est de caractéristique nulle et que le polynôme χ_u est scindé sur K. On considère le polynôme — D2 —
$$P \coloneqq \frac{\chi_u}{\operatorname{pgcd}(\chi_u, \chi_u')}$$
et la suite $(u_r)_{r \in \mathbf{N}}$ d'endomorphismes vérifiant
$$\begin{aligned} u_0 &= u, \\ u_{r+1} &= u_r - P(u_r)P'(u_r)^{-1}, \qquad r \geqslant 1. \end{aligned}$$
Notons $u = d + n$ la décomposition de Dunford de l'endomorphisme u. Alors la suite $(u_r)_{r \in \mathbf{N}}$ est bien définie, elle est stationnaire et elle converge vers l'endomorphisme d au bout d'au plus $\log_2 n$ itérations.

[1] Vincent Beck, Jérôme Malick et Gabriel Peyré. *Objectif Agrégation.* 2e édition. H&K, 2005.
[2] Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries.* T. Tome premier. Calvage & Mounet, 2013.
[3] Serge Francinou, Hervé Gianella et Serge Nicolas. *Algèbre 1.* Cassini, 2001.
[4] Xavier Gourdon. *Algèbre.* 2e édition. Ellipses, 2009.
[5] Maxime Zavidovique. *Un Max de Math.* Calvage & Mounet, 2013.