Leçon 124 : Polynômes d'endomorphisme en dimension finie ; applications à la réduction d'un endomorphisme en dimension finie.

k désigne un corps (commutatif) et E un k-ev de dimension finie $n \geq 1$

I - L'algèbre $k[u]$

1 - Définitions

Déf 1. Soit $u \in \mathcal{L}(E)$, on pose $\varphi_u : \begin{array}{l} k[X] \to \mathcal{L}(E) \\ P \mapsto P(u) \end{array}$ morphisme d'algèbre. On définit $k[u] = \operatorname{Im} \varphi_u$ l'algèbre des polynômes en u.

Déf-prop 2. $\operatorname{Ker} \varphi_u$ est un idéal non nul de $k[X]$ principal, donc il existe un unique polynôme unitaire Π_u tel que $\operatorname{ker} \varphi_u = (\Pi_u)$. Π_u est appelé polynôme minimal de u

2 - Structure de $k[u]$

Prop 3 $\Pi_u = P_1 \dots P_m$ décomposition en facteurs premiers entre eux deux à deux. On a
$$k[u] \simeq k[X]/(\Pi_u) \simeq k[X]/(P_1) \times \dots \times k[X]/(P_m)$$

Cor 4 • $k[u]$ est un corps ssi Π_u est irréductible
• Si $d = \deg(\Pi_u)$, $\dim(k[u]) = d$ et $(1, \dots, u^{d-1})$ est une base de $k[u]$.

Prop 5 u inversible ssi le coefficient constant de Π_u est inversible. Dans ce cas $u^{-1} \in k[u]$

Exemples • $u = \lambda \mathrm{Id}$ $\Pi_u = X - \lambda$ • $u^2 = u$ et $u \neq \mathrm{Id}, 0$ $\Pi_u = X(X-1)$ • u nilpotent d'indice k $\Pi_u = X^k$

Rem Si $A \in M_n(k)$, $\Pi_A \overset{\text{déf}}{=} \Pi_u$ où $u : \begin{array}{l} k^n \to k^n \\ x \mapsto Ax \end{array}$ et dans ce cas, si $\mathcal{B}$ base de E alors $\Pi_u = \Pi_{\mathrm{Mat}_{\mathcal{B}} u}$.

Prop 6 Soit $h \in GL(E)$ et $P \in k[X]$ alors pour tout $u \in \mathcal{L}(E)$
$P(h^{-1} u h) = h^{-1} P(u) h$

Cor 7 - Deux endomorphismes conjugués ont même polynôme minimal
- Deux matrices semblables ont même polynôme minimal

Rq En général $\Pi_{uv} \neq \Pi_{vu}$ $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Prop 8 F sev stable par u alors $\Pi_{u|F} \mid \Pi_u$

3 - Polynômes et valeurs propres

a - Polynômes annulateurs

Prop 9 Si $u \in \mathcal{L}(E)$ et $\lambda \in \operatorname{Spec}(u)$ alors $\forall P \in k[X]$, $P(\lambda) \in \operatorname{Spec}(P(u))$ et $\operatorname{Ker}(u - \lambda \mathrm{Id}) \subseteq \operatorname{Ker}(P(u) - P(\lambda)\mathrm{Id})$

Cor 10 • Si P annule u alors $\operatorname{Spec}(u) \subseteq \operatorname{Racines}(P)$
• $\operatorname{Spec}(u) = \operatorname{Racines}(\Pi_u)$

b - Polynôme caractéristique

Déf 11 $u \in \mathcal{L}(E)$ on définit $\chi_u = \det(u - X\mathrm{Id})$ le polynôme caractéristique de u.

Prop 12 $\chi_u(\lambda) = 0 \iff u - \lambda \mathrm{Id}$ non injective $\iff \operatorname{Ker}(u - \lambda \mathrm{Id}) \neq \{0\} \iff \lambda \in \operatorname{Spec}(u)$.

Prop 13 - $\deg(\chi_u) = n$ - $\forall h \in GL(E), \forall u \in \mathcal{L}(E)$ $\chi_{h^{-1}uh} = \chi_u$
- $\forall u, v \in \mathcal{L}(E)$, $\chi_{uv} = \chi_{vu}$

Thm 14 (Cayley-Hamilton) $\forall u \in \mathcal{L}(E)$, $\chi_u(u) = 0$

Rq : Équivalent à $\Pi_u \mid \chi_u$.

Ex - $u = \lambda \mathrm{Id}$ $\chi_u = (X - \lambda)^n (-1)^n$
- u projecteur de rang r (e.g. $u^2 = u$) $\chi_u = (-1)^n (X-1)^r X^{n-r}$

4 - Décomposition des noyaux

Thm 15 - $u \in \mathcal{L}(E)$ $P = P_1 \dots P_m$ $P_i \wedge P_j = 1$ $(i \neq j)$

$$\ker P(u) = \bigoplus_{i=1}^{m} \ker P_i(u)$$

- Si $P(u) = 0$ alors $E = \bigoplus_{i=1}^{m} \ker P_i(u)$ et les projecteurs Π_i sur $\ker P_i(u)$ appartiennent à $k[u]$

Calcul des Π_i [ROUD p420]

(i) On pose $Q_i = \frac{P}{P_i}$

(ii) Les Q_i sont premiers entre eux dans leur ensemble, il existe donc des $U_i \in k[X]$ tels que $\sum_i U_i Q_i = 1$

(iii) On a $\Pi_i = U_i Q_i(u)$

Exemple $Car(k) \neq 2$ $P = (X-1)(X+1)$ et $P(u) = 0$ alors $E = \ker(u - Id) \oplus \ker(u + Id)$. $Q_1 = X+1$ $Q_2 = X-1$. $U_1 = \frac{1}{2}$, $U_2 = -\frac{1}{2}$ et $\Pi_1 = \frac{1}{2}(u + Id)$, $\Pi_2 = -\frac{1}{2}(u - Id)$.

Rq • $P = \chi_u$ donne la décomposition en sous-espaces caractéristiques • On peut choisir $P = \Pi_u$.

II - Théorèmes de réduction associés aux polynômes d'endomorphisme.

1 - Critères de diagonalisabilité

Thm 16 • u est diagonalisable ssi Π_u est scindé à racines simples

• u est diagonalisable ssi $\exists P$ scindé à racines simples tel que $P(u) = 0$

Applications : • $k = \mathbb{F}_q$, u diagonalisable $\Leftrightarrow u^q = u$

• Théorème de Burnside : G ss-groupe de $GL_n(\mathbb{C})$, G est fini ssi G est d'exposant fini

dvp ↕

2 - Critères de trigonalisabilité

Thm 17 • u est trigonalisable ssi Π_u est scindé

• u est trigonalisable ssi $\exists P$ scindé tel que $P(u) = 0$

• u est trigonalisable ssi χ_u est scindé.

Application : si k est algébriquement clos, alors u est trigonalisable.

3 - Invariants de similitude

DEF 18 u est cyclique s'il existe $x \in E$ tel que $x, u(x), \dots, u^{n-1}(x)$ est une base.

Prop 19 On a l'équivalence : (i) u cyclique (ii) $\deg(\Pi_u) = n$ (iii) $\Pi_u = \chi_u$ (iv) $\dim(k[u]) = n$

Prop 20 Si u est cyclique, il existe $\mathcal{B}$ base de u tel que $Mat_{\mathcal{B}}(u) = \begin{pmatrix} 0 & & 0 & a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \\ 0 & & 1 & a_{n-1} \end{pmatrix} = C_P$ matrice compagnon du polynôme $P = X^n - a_{n-1}X^{n-1} - \dots - a_0$.

Thm 21 (décomposition en sous-espaces cycliques)

$u \in \mathcal{L}(E)$, il existe $F_1, \dots, F_r$ stables par u tels que

i) $E = F_1 \oplus \dots \oplus F_r$ ii) $u_{|F_i}$ cyclique $\Pi_{u_{|F_i}} = P_i$

tels que $P_i | P_{i+1}$. La suite (P_i) ne dépend que de u et est appelée invariants de similitude de u. (P_i unitaires)

Prop 22 $P_1 = \Pi_u$ et $\chi_u = P_1 \dots P_r$

Prop 23 (Réduction de Frobenius) $P_1, \dots, P_r$ invariants de similitude de $u \in \mathcal{L}(E)$. Il existe $\mathcal{B}$ base de E tq :

$$Mat_{\mathcal{B}}(u) = \begin{pmatrix} \boxed{C_{P_1}} & & \\ & \ddots & \\ & & \boxed{C_{P_r}} \end{pmatrix}$$ avec C_{P_i} matrice compagnon de P_i.

III Exemples et applications

1) Décomposition de Dunford [GOU]

Thm 24 Soit $u \in \mathcal{L}(E)$ tq χ_u est scindé sur k alors il existe un unique couple (d,n) tel que d est diagonalisable, n nilpotent vérifiant

(i) $u = d + n$ (ii) $d \circ n = n \circ d$

On a de plus $d \in k[u]$ et $n \in k[u]$.

dvp

Rq La méthode de Newton permet un calcul effectif de (d,n) sans connaître les valeurs propres de u.

2) Calcul de puissances

- **Méthode par division euclidienne**

Soit $P \in k[X]$ tel que $P(u) = 0$ $\exists ! (Q,R) \in k[X]$ et $\deg(R) < \deg(P)$ tel que $X^k = PQ + R$ et on a : $u^k = P(u)Q(u) + R(u) = R(u)$. Il suffit donc de connaître les premières puissances de u.

Cas particulier si $P = \Pi_u$ alors on obtient la décomposition de u^k sur la base $(1, \dots, u^{d-1})$

- **Utilisation des projecteurs de la décomposition par Π_u**

$\Pi_u = P_1 \dots P_m$ $P_i \wedge P_j = 1$ $(i \neq j)$ $E = \bigoplus_{i=1}^{m} \ker P_i(u)$

Soient $\Pi_1, \dots, \Pi_m$ les projecteurs associés $(\ker \dots)$.

$x = \sum_i \Pi_i(x) \Rightarrow u^k(x) = \sum_i u^k(\Pi_i(x))$ puis on calcule $u^k(\Pi_i(x))$ en faisant la division euclidienne de X^k par P_i. Avantage : $\deg(P_i)$ petit.

Cas particulier : u diagonalisable, $\deg(P_i) = 1$ et $u(\Pi_i(x)) = \lambda \Pi_i(x)$. $u^k = \sum_i \lambda_i^k \Pi_i$.

3) Calcul de l'inverse de u

- Soit $u \in GL(E)$, $\Pi_u = a_0 + a_1 X + \dots + X^k$ $a_0 \neq 0$

$\Pi_u(u) = a_0 Id + a_1 u + \dots + u^k = 0$ d'où

$$u^{-1} = -\frac{a_1}{a_0} u - \dots - \frac{1}{a_0} u^{k-1}$$

- Cas diagonalisable : vp $\lambda_i \neq 0$ $u^{-1} = \sum_i \frac{1}{\lambda_i} \Pi_i$

4) Exponentielle de u ($k = \mathbb{R}$ ou $\mathbb{C}$)

$$\exp(u) = \sum_{k=0}^{+\infty} \frac{1}{k!} u^k \in k[u]$$

- Méthode 1 : utilisation de la décomposition de Dunford :

$\exp(u) = \exp(n + d) = \exp(d)\exp(n)$

- Méthode 2 : utilisation de polynômes annulateurs

Cas diagonalisable : $u^k = \sum_i \lambda_i^k \Pi_i$ d'où

$\exp(u) = \sum_{i=1}^{m} \exp(\lambda_i) \Pi_i$

Ex Soit u annulé par $(X-1)(X+1)$ alors

$E = \ker(u - Id) \oplus \ker(u + Id)$ $\Pi_1 = \frac{1}{2}(u + Id)$

$\Pi_2 = -\frac{1}{2}(u - Id)$

$\Rightarrow \exp(u) = \frac{e}{2}(u + Id) - \frac{1}{2e}(u - Id)$.

5) Commutant d'un endomorphisme

Déf 25 Soit $u \in \mathcal{L}(E)$ on définit $Com(u) = \{v \in \mathcal{L}(E) \mid u \circ v = v \circ u\}$.

Prop 26 Si $\deg(\Pi_u) = n$ alors $Com(u) = k[u]$.

Références

- [GOU] Gourdon, analyse 2e éd (Annexe sur Frobenius)
- [ROUD] Roudier, Algèbre linéaire (Chap 18 et 19)
- Goblot
- Objectif agreg