

II Réduction algébrique

$\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ et E un $\mathbb{K}$ -espace vectoriel.

6.1 Polynômes en un endomorphisme

6.1.1 Valeur d'un polynôme en un endomorphisme

Définition

On appelle valeur d'un polynôme $P = \sum_{k=0}^N a_k X^k \in \mathbb{K}[X]$ en un endomorphisme $u \in \mathcal{L}(E)$ l'application

$$\tilde{P}(u) \stackrel{\text{def}}{=} \sum_{k=0}^N a_k u^k \in \mathcal{L}(E)$$

Exemple La valeur de $P = X^3$ en u est $P(u) = u^3$.

La valeur de $P = X^3 + 2X - 1$ en u est $P(u) = u^3 + 2u - \text{Id}$.

Attention : La valeur de $P(u)$ en $x \in E$ est notée $P(u)(x)$ à comprendre $[P(u)](x)$.
Ecrire $P(u(x))$ n'a pas de sens.

Théorème

L'application $\varphi_u : \mathbb{K}[X] \rightarrow \mathcal{L}(E)$ définie par $\varphi_u(P) = \tilde{P}(u)$ est un morphisme de $\mathbb{K}$ -algèbres.

dém. :

L'application φ_u est bien définie entre deux $\mathbb{K}$ -algèbres.

$\varphi_u(1) = \text{Id}_E$.

Soit $\lambda, \mu \in \mathbb{K}$ et $P, Q \in \mathbb{K}[X]$.

On peut écrire $P = \sum_{k=0}^N a_k X^k$ et $Q = \sum_{k=0}^M b_k X^k$.

Quitte à adjoindre des coefficients nuls, on peut supposer $M = N$. On a

$$\varphi_u(\lambda P + MQ) = \sum_{k=0}^N (\lambda a_k + M b_k) u^k = \lambda \sum_{k=0}^N a_k u^k + M \sum_{k=0}^N b_k u^k = \lambda \varphi_u(P) + M \varphi_u(Q)$$

Aussi

$$\varphi_u(PQ) = (PQ)(u) = \left(\sum_{k=0}^N a_k X^k Q \right) (u) = \sum_{k=0}^N a_k (X^k Q)(u)$$

la dernière égalité étant justifiée par linéarité de φ_u . Or, pour $k \in \{0, 1, \dots, N\}$, on a

$$(X^k Q)(u) = \sum_{\ell=0}^N b_\ell u^{k+\ell} = u^k \circ Q(u)$$

donc

$$(PQ)(u) = \left(\sum_{k=0}^N a_k X^k Q \right) (u) = \sum_{k=0}^N a_k u^k \circ Q(u)$$

puis

$$\varphi_u(PQ) = (PQ)(u) = P(u) \circ Q(u) = \varphi_u(P) \circ \varphi_u(Q)$$

□

Remarque Par ce morphisme, toute identité polynomiale se transpose aux endomorphismes.

Exemple Puisque

$$X^3 - 2X + 1 = (X - 1)(X^2 + X - 1)$$

on a

$$u^3 - 2u + \text{Id}_E = (u - \text{Id}_E)(u^2 + u - \text{Id}_E)$$

Exemple Soit $P = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{C}[X]$. En notant $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ les racines de P comptées avec multiplicité

$$P = X^n + a_{n-1}X^{n-1} + \dots + a_0 = \prod_{k=1}^n (X - \lambda_k)$$

alors

$$P(u) = \prod_{k=1}^n (u - \lambda_k \text{Id}_E)$$

6.1.2 Polynôme d'endomorphisme

Définition

On dit que $v \in \mathcal{L}(E)$ est un polynôme en $u \in \mathcal{L}(E)$ s'il existe $P \in \mathbb{K}[X]$ tel que $v = P(u)$.
On note $\mathbb{K}[u]$ l'ensemble des polynômes en u :

$$\mathbb{K}[u] \stackrel{\text{def}}{=} \{P(u) / P \in \mathbb{K}[X]\}$$

Exemple $u^3 + 3u + \text{Id}_E$ et $(u - \lambda \text{Id}_E)^\alpha$ sont des polynômes en u .

Théorème

$\mathbb{K}[u]$ est une sous-algèbre commutative de $\mathcal{L}(E)$.

De plus, si A est une sous-algèbre de $\mathcal{L}(E)$,

$$u \in A \Rightarrow \mathbb{K}[u] \subset A$$

Ainsi, $\mathbb{K}[u]$ est la plus petite sous-algèbre de $\mathcal{L}(E)$ contenant u , on l'appelle algèbre engendrée par u .

dém. :

$\mathbb{K}[u] \subset \mathcal{L}(E)$, $\text{Id}_E \in \mathbb{K}[u]$ car pour $P(X) = 1$ on a $P(u) = \text{Id}_E$.

Soit $\lambda, \mu \in \mathbb{K}$ et $v, w \in \mathbb{K}[u]$. Il existe $P, Q \in \mathbb{K}[X]$ tels que $v = P(u)$ et $w = Q(u)$.

On a alors $\lambda v + \mu w = (\lambda P + \mu Q)(u) \in \mathbb{K}[u]$ et $v \circ w = (PQ)(u) \in \mathbb{K}[u]$ donc $\mathbb{K}[u]$ est une sous-algèbre de $\mathcal{L}(E)$.

De plus, $w \circ v = (QP)(u) = (PQ)(u) = v \circ w$ donc $\mathbb{K}[u]$ est une sous-algèbre commutative de $\mathcal{L}(E)$.

Si A est une sous-algèbre de $\mathcal{L}(E)$ contenant u alors par récurrence

$$\forall n \in \mathbb{N}, u^n \in A$$

puis

$$\mathbb{K}[u] = \text{Vect} \{u^k / k \in \mathbb{N}\} \subset A$$

□

Exemple Si $P \in \mathbb{K}[X]$ alors $\text{Im} P(u)$ et $\ker P(u)$ sont stables par u .

En effet, les $P(u)$ et u commutent. On retrouve en particulier que les sous-espaces propres de u sont stables par u .

6.1.3 Polynôme annulateur

Définition

On appelle polynôme annulateur de $u \in \mathcal{L}(E)$ tout polynôme $P \in \mathbb{K}[X]$ vérifiant $P(u) = \tilde{0}$.

Exemple Le polynôme nul annule tout endomorphisme.

Exemple Le polynôme $X - \lambda$ annule l'endomorphisme λId_E .

Exemple Le polynôme $X^2 - X$ est annulateur des projections vectorielles.

Théorème

L'ensemble des polynômes annulateurs de $u \in \mathcal{L}(E)$ est un sous-espace vectoriel et un idéal de $\mathbb{K}[X]$.

dém. :

Notons $I = \{P \in \mathbb{K}[X] / P(u) = \tilde{0}\}$ l'ensemble des polynômes annulateurs de u .

I est le noyau du morphisme d'algèbres φ_u , c'est donc un sous-espace vectoriel et un idéal de $\mathbb{K}[X]$.

Cor : Si P annule u et si $P \mid Q$ alors Q annule u .

□

6.1.4 Polynôme annulateur et valeur propre

Lemme

Si λ est valeur propre de $u \in \mathcal{L}(E)$ alors, pour tout $P \in \mathbb{K}[X]$, $P(\lambda)$ est valeur propre de $P(u)$.

dém. :

Soit λ une valeur propre de u . Il existe $x \neq 0_E$ tel que $u(x) = \lambda x$.

On a $u^2(x) = u(\lambda x) = \lambda^2 x, \dots, u^n(x) = \lambda^n x$.

Soit $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{K}[X]$.

On a $P(u)(x) = (a_n u^n + \dots + a_1 u + a_0 \text{Id})(x) = (a_n \lambda^n x + \dots + a_1 \lambda x + a_0 x) = P(\lambda)x$ avec $x \neq 0_E$ donc $P(\lambda)$ est valeur propre de $P(u)$.

□

Théorème

Les valeurs propres de $u \in \mathcal{L}(E)$ figurent parmi les racines des polynômes annulateurs de u .

dém. :

Soit $P(X)$ un polynôme annulateur de u et λ une valeur propre de u .

On a $P(\lambda)$ valeur propre de $P(u) = \tilde{0}$ donc $P(\lambda) = 0$.

□

Attention : Des racines d'un polynôme annulateur peuvent ne pas être valeur propre.

Exemple Si p est une projection vectorielle alors $X^2 - X = X(X - 1)$ est annulateur de p et donc $\text{Sp} p \subset \{0, 1\}$.

Exemple 0 est la seule valeur propre d'un endomorphisme nilpotent.

En effet, Soit $u \in \mathcal{L}(E)$ nilpotent.

Il existe $p \in \mathbb{N}^*$ tel que $u^p = \tilde{0}$.

Le polynôme X^p est annulateur de u et donc $\text{Sp} u \subset \{0\}$.

L'endomorphisme u ne peut être injectif (car u^p ne l'est pas) et donc $0 \in \text{Sp} u$.

6.2 Polynôme d'une matrice

6.2.1 Valeur d'un polynôme en une matrice carrée

Définition

On appelle valeur de $P = \sum_{k=0}^N a_k X^k \in \mathbb{K}[X]$ en $M \in \mathcal{M}_n(\mathbb{K})$ la matrice

$$P(M) \stackrel{\text{def}}{=} \sum_{k=0}^N a_k M^k \in \mathcal{M}_n(\mathbb{K})$$

Exemple La valeur de $P = X^3 - 3X + 1$ en $M \in \mathcal{M}_n(\mathbb{K})$ est $P(M) = M^3 - 3M + I_n$.

Exemple Soit $u \in \mathcal{L}(E)$ et $e = (e_1, \dots, e_n)$ une base de E .
Si $M = \text{Mat}_e u$ alors $\forall P \in \mathbb{K}[X]$, $P(M) = \text{Mat}_e P(u)$

Exemple Calcul de $P(M)$ pour

$$M = \begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix}$$

On vérifie par récurrence

$$\forall k \in \mathbb{N}, M^k = \begin{pmatrix} \lambda_1^k & & (0) \\ & \ddots & \\ (0) & & \lambda_n^k \end{pmatrix}$$

puis par linéarité

$$\forall P \in \mathbb{K}[X], P(M) = \begin{pmatrix} P(\lambda_1) & & (0) \\ & \ddots & \\ (0) & & P(\lambda_n) \end{pmatrix}$$

Exemple Expression de $P(M)$ pour

$$M = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix}$$

On vérifie par récurrence

$$\forall k \in \mathbb{N}, M^k = \begin{pmatrix} \lambda_1^k & & * \\ & \ddots & \\ (0) & & \lambda_n^k \end{pmatrix}$$

puis par linéarité

$$\forall P \in \mathbb{K}[X], P(M) = \begin{pmatrix} P(\lambda_1) & * \\ (0) & P(\lambda_n) \end{pmatrix}$$

Exemple Expression de $P(M)$ pour

$$M = \begin{pmatrix} A & * \\ O & B \end{pmatrix} \text{ (avec } A, B \text{ matrices carrées)}$$

Comme au dessus, on obtient

$$\forall P \in \mathbb{K}[X], P(M) = \begin{pmatrix} P(A) & * \\ O & P(B) \end{pmatrix}$$

Exemple On a

$$\forall P \in \mathbb{K}[X], P({}^t M) = {}^t P(M)$$

En effet

$$\forall k \in \mathbb{N}, ({}^t M)^k = {}^t (M^k)$$

puis on conclut par linéarité

$$\begin{pmatrix} (0) & & & \\ & \ddots & & \\ & & \ddots & \\ & & & (0) \end{pmatrix} = I_n$$

Théorème

L'application $\varphi_M : \mathbb{K}[X] \rightarrow \mathcal{M}_n(\mathbb{K})$ définie par $\varphi_M(P) = P(M)$ est un morphisme de $\mathbb{K}$ -algèbres.

6.2.2 Polynôme en une matrice carrée

Définition

On dit que $A \in \mathcal{M}_n(\mathbb{K})$ est un polynôme en $M \in \mathcal{M}_n(\mathbb{K})$ s'il existe $P \in \mathbb{K}[X]$ tel que $A = P(M)$. On note

$$\mathbb{K}[M]_{\text{def}} = \{P(M) / P \in \mathbb{K}[X]\}$$

l'ensemble des polynômes en M

Théorème

$\mathbb{K}[M]$ est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$ incluse dans toute sous-algèbre de $\mathcal{M}_n(\mathbb{K})$ contenant M ; on l'appelle algèbre engendrée par M .

6.2.3 Polynôme annulateur

Définition

On appelle polynôme annulateur de $M \in \mathcal{M}_n(\mathbb{K})$ tout polynôme $P \in \mathbb{K}[X]$ vérifiant $P(M) = O_n$.

Exemple Si $M = \text{Mat}_e u$ alors les polynômes annulateurs de M et de u se correspondent.

Exemple Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$.

On vérifie par le calcul que $P = X^2 - (a+d)X + (ad-bc)$ est annulateur de M .

Exemple $P = (X - \lambda_1) \dots (X - \lambda_n)$ est annulateur de

$$D = \begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$$

En effet

$$P(D) = \begin{pmatrix} P(\lambda_1) & & (0) \\ & \ddots & \\ (0) & & P(\lambda_n) \end{pmatrix} = O_n$$

Remarque Si A est diagonalisable semblable à D alors P est aussi annulateur de A . Plus généralement :

Proposition

Si $A, B \in \mathcal{M}_n(\mathbb{K})$ sont semblables alors A et B ont les mêmes polynômes annulateurs.

dém. :

Par le calcul à partir de la relation de similitude $B = Q^{-1}AQ$ ou simplement parce que les matrices A et B représentent le même endomorphisme.

□

Théorème

L'ensemble des polynômes annulateurs de $M \in \mathcal{M}_n(\mathbb{K})$ est un sous-espace vectoriel et un idéal de $\mathbb{K}[X]$.

Corollaire

Si P annule M et si $P \mid Q$ alors Q annule M .

6.2.4 Valeurs propres et polynômes annulateurs

Théorème

Les valeurs propres de $M \in \mathcal{M}_n(\mathbb{K})$ figurent parmi les racines des polynômes annulateurs de M .

Exemple Soit $A \in \mathcal{M}_3(\mathbb{R})$ vérifiant $A^3 = I_n$.

a) Valeurs propres réelles.

b) Valeurs propres complexes.

Le polynôme $X^3 - 1$ est annulateur de A .

Dans $\mathbb{R}$, $X^3 - 1 = (X - 1)(X^2 + X + 1)$ donc $\text{Sp}_{\mathbb{R}} A \subset \{1\}$.

Or A est une matrice réelle de taille impaire donc $\text{Sp}_{\mathbb{R}} A \neq \emptyset$ puis

$$\text{Sp}_{\mathbb{R}} A = \{1\}$$

Dans $\mathbb{C}$, $X^3 - 1 = (X - 1)(X - j)(X - j^2)$ donc $\text{Sp}_{\mathbb{C}} A \subset \{1, j, j^2\}$.

Puisque 1 est valeur propre et puisque les valeurs propres de A sont deux à deux conjuguées

$$\text{Sp}_{\mathbb{C}} A = \{1\} \text{ ou } \text{Sp}_{\mathbb{C}} A = \{1, j, j^2\}$$

On en déduit $\text{tr}(A) = 3$ ou $\text{tr}(A) = 0$ et $\det A = 1$ (car χ_A est scindé et donc A trigonalisable)

6.3 Polynômes annulateurs en dimension finie

E désigne un $\mathbb{K}$ -espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

6.3.1 Théorème de Cayley Hamilton

Théorème

Le polynôme caractéristique χ_u de $u \in \mathcal{L}(E)$ est annulateur de u .

Cet énoncé se transpose aux matrices $A \in \mathcal{M}_n(\mathbb{K})$.

Exemple Pour $A \in \mathcal{M}_2(\mathbb{K})$, le polynôme $\chi_A = X^2 - \text{tr}(A)X + \det(A)$ est annulateur de A .

6.3.2 Polynôme minimal

Théorème

Pour tout $u \in \mathcal{L}(E)$, il existe un unique polynôme Π_u vérifiant :

- 1) Π_u est annulateur de u ;
- 2) Π_u est unitaire ;
- 3) $\forall P \in \mathbb{K}[X], P(u) = \bar{0} \Rightarrow \Pi_u \mid P$.

Ce polynôme Π_u est appelé polynôme minimal de l'endomorphisme u .

Cet énoncé se transpose aux matrices $A \in \mathcal{M}_n(\mathbb{K})$ ce qui définit le polynôme minimal Π_A

dém. :

Existence :

Considérons $I = \{P \in \mathbb{K}[X] / P(u) = \bar{0}\}$.

Puisque I est un idéal de $\mathbb{K}[X]$, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $I = Q \cdot \mathbb{K}[X]$.

Puisque $\chi_u \in I$, l'idéal I est non nul et donc $Q \neq 0$.

Notons λ le coefficient dominant de u et considérons $\Pi_u = Q/\lambda$. Le polynôme Π_u est unitaire et vérifie $I = \Pi_u \cdot \mathbb{K}[X]$.

Unicité :

Supposons Π_u et $\tilde{\Pi}_u$ solutions.

Puisque $\tilde{\Pi}_u(u) = \bar{0}$, $\Pi_u \mid \tilde{\Pi}_u$. De façon symétrique, $\tilde{\Pi}_u \mid \Pi_u$ et donc Π_u et $\tilde{\Pi}_u$ sont associés.

Or ils sont tous deux unitaires donc égaux.

□

Remarque Le polynôme Π_u est non constant.

Exemple Polynôme minimal de $u = \lambda \text{Id}_E$.

$X - \lambda$ annule u et donc $\Pi_u \mid X - \lambda$.

Puisque Π_u est unitaire non constant, on obtient

$$\Pi_u = X - \lambda$$

Exemple Polynôme minimal de p projection autre que $\tilde{0}$ et Id_E .

On a $p^2 = p$ donne $\Pi_p \mid X(X-1)$.

Puisque Π_p est unitaire non constant

$$\Pi_p = X, X-1 \text{ ou } \Pi_p = X(X-1)$$

Puisque $p \neq \tilde{0}$ et $p \neq \text{Id}_E$, les cas $\Pi_p = X$ et $\Pi_p = X-1$ sont à exclure.

Il reste

$$\Pi_p = X(X-1)$$

Exemple Polynôme minimal de $A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

$\chi_A = X^2 - 5X + 6 = (X-2)(X-3)$ est annulateur de A donc $\Pi_A \mid \chi_A$.

Par conséquent

$$\Pi_A = X-1, X-2 \text{ ou } (X-2)(X-3)$$

Les cas $\Pi_A = X-1$ ou $X-2$ sont à exclure et il reste

$$\Pi_A = (X-2)(X-3)$$

Exemple Polynôme minimal de $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$.

Cette fois-ci

$$\chi_D = (X-1)^2(X-2) \text{ et } \Pi_D = (X-1)(X-2)$$

6.3.3 Polynôme minimal et valeurs propres

Théorème

Les valeurs propres de $u \in \mathcal{L}(E)$ sont exactement les racines de son polynôme minimal.
Ce résultat se transpose aux matrices carrées.

dém. :

On sait déjà que les valeurs propres de u sont racines de Π_u car Π_u est annulateur.

Inversement, si λ est racine de Π_u alors λ est aussi racine de χ_u donc λ est valeur propre de u .

□

Exemple Le polynôme $\prod_{\lambda \in \text{Sp}u} (X - \lambda)$ divise Π_u .

6.3.4 Application : calcul des puissances d'un endomorphisme

Soit $u \in \mathcal{L}(E)$. On introduit son polynôme minimal Π_u de degré d (avec $d \leq \dim E$ car Π_u divise χ_u).

On écrit

$$\Pi_u = X^d - (a_{d-1}X^{d-1} + \dots + a_1X + a_0)$$

6.3. POLYNÔMES ANNULATEURS EN DIMENSION FINIE

et alors

$$u^d = a_0 \text{Id}_E + a_1 u + \dots + a_{d-1} u^{d-1}$$

Puisque $u^{d+1} = u \circ u^d$

$$u^{d+1} = a_0 u + a_1 u^2 + \dots + a_{d-1} u^d$$

et en exploitant la relation au dessus, on obtient une expression

$$u^{d+1} = a'_0 \text{Id}_E + a'_1 u + \dots + a'_{d-1} u^{d-1}$$

On peut répéter ce processus... Plus généralement :

Théorème

Si $d = \deg \Pi_u$ alors la famille $(u^k)_{0 \leq k \leq d-1}$ est une base $\mathbb{K}[u]$.
Ce résultat se transpose aux matrices carrées.

dém. :

Commençons par montrer $\mathbb{K}[u] = \text{Vect}(\text{Id}_E, u, \dots, u^{d-1})$

On a déjà l'inclusion $\text{Vect}(\text{Id}_E, u, \dots, u^{d-1}) \subset \mathbb{K}[u]$.

Inversement, soit $P \in \mathbb{K}[X]$.

Par division euclidienne, on peut écrire $P = Q\Pi_u + R$ avec $\deg R < d$.

On a alors

$$P(u) = Q(u) \circ \Pi_u(u) + R(u) = R(u) \in \text{Vect}(\text{Id}_E, u, \dots, u^{d-1})$$

Ainsi $\mathbb{K}[u] \subset \text{Vect}(\text{Id}_E, u, \dots, u^{d-1})$ puis l'égalité.

Montrons maintenant que la famille $(\text{Id}_E, u, \dots, u^{d-1})$ est libre.

Supposons

$$a_0 \text{Id}_E + a_1 u + \dots + a_{d-1} u^{d-1} = \vec{0}$$

Pour $P = a_0 + a_1 X + \dots + a_{d-1} X^{d-1}$, on a $P(u) = \vec{0}$.

Or $\deg P < \deg \Pi_u$ donc $P = 0$ puis $a_0 = a_1 = \dots = a_{d-1} = 0$.

Ainsi, la famille $(\text{Id}_E, u, \dots, u^{d-1})$ est libre et c'est donc une base de $\mathbb{K}[u]$.

□

Corollaire

$$\dim \mathbb{K}[u] \leq \dim E \text{ et } \dim \mathbb{K}[A] \leq n.$$

dém. :

Car le polynôme minimal est diviseur du polynôme caractéristique donc de degré inférieur à n .

□

Exemple Calculons les puissances de $A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

On sait $\Pi_A = (X - 2)(X - 3)$.

Par division euclidienne

$$X^n = \Pi_A(X)Q(X) + \alpha X + \beta \quad (1)$$

En évaluant la relation (1) en 2 et en 3, on obtient

$$\begin{cases} 2\alpha + \beta = 2^n \\ 3\alpha + \beta = 3^n \end{cases} \text{ donc } \begin{cases} \alpha = 3^n - 2^n \\ \beta = 3 \cdot 2^n - 2 \cdot 3^n \end{cases}$$

En évaluant la relation (1) en A , on obtient

$$A^n = (3^n - 2^n)A + (3 \cdot 2^n - 2 \cdot 3^n)I_2$$

6.4 Réduction et polynômes annulateurs

E désigne un $\mathbb{K}$ -espace vectoriel non nul

6.4.1 Lemme de décomposition des noyaux

Théorème

Soit $P, Q \in \mathbb{K}[X]$ et $u \in \mathcal{L}(E)$.

Si P et Q sont premiers entre eux alors

$$\ker(PQ)(u) = \ker P(u) \oplus \ker Q(u)$$

dém. :

Puisque $P \wedge Q = 1$, il existe des polynômes V et W tel que $VP + WQ = 1$.

On a alors $\text{Id} = V(u) \circ P(u) + W(u) \circ Q(u)$.

Soit $x \in \ker P(u) \cap \ker Q(u)$

On a

$$x = (V(u) \circ P(u))(x) + (W(u) \circ Q(u))(x) = 0$$

donc $\ker P(u)$ et $\ker Q(u)$ sont en somme directe.

Montrons $\ker P(u) \oplus \ker Q(u) \subset \ker(PQ)(u)$

Puisque $(PQ)(u) = Q(u) \circ P(u)$ on a $\ker P(u) \subset \ker(PQ)(u)$.

De même $\ker Q(u) \subset \ker(PQ)(u)$ et donc $\ker P(u) \oplus \ker Q(u) \subset \ker(PQ)(u)$.

Inversement

Soit $x \in \ker(PQ)(u)$. On a

$$x = (W(u) \circ Q(u))(x) + (V(u) \circ P(u))(x) = a + b$$

avec $a = (W(u) \circ Q(u))(x)$ et $b = (V(u) \circ P(u))(x)$.

Or

$$P(u)(a) = (P(u) \circ W(u) \circ Q(u))(x) = (W(u) \circ (PQ)(u))(x) = 0$$

et de même $Q(u)(b) = 0$. Ainsi $a \in \ker P(u)$ et $b \in \ker Q(u)$ puis

$$\ker(PQ)(u) \subset \ker P(u) \oplus \ker Q(u)$$

et enfin l'égalité.

□

Corollaire

Si $P_1, \dots, P_m \in \mathbb{K}[X]$ sont deux à deux premiers entre eux alors :

$$\ker \left(\prod_{k=1}^m P_k \right) (u) = \bigoplus_{k=1}^m \ker P_k(u)$$

Ce résultat se transpose aux matrices carrées

$$\ker \left(\prod_{k=1}^m P_k \right) (A) = \bigoplus_{k=1}^m \ker P_k(A)$$

dém. :

On raisonne par récurrence en exploitant

$$(P_1 \dots P_m) \wedge P_{m+1} = 1 \Rightarrow \ker \left(\prod_{k=1}^{m+1} P_k \right) (u) = \ker \left(\prod_{k=1}^m P_k \right) (u) \oplus \ker P_{m+1}(u)$$

□

Rappel :

Si $a \neq b$ alors $(X - a) \wedge (X - b) = 1$.

Plus généralement, $(X - a)^\alpha \wedge (X - b)^\beta = 1$ pour tout $\alpha, \beta \in \mathbb{N}$.

Encore plus généralement, deux polynômes de $\mathbb{K}[X]$ sont premiers entre eux si, et seulement si, ils n'ont pas de racines complexes en commun.

Exemple On appelle projecteur de E tout $p \in \mathcal{L}(E)$ vérifiant $p^2 = p$.

Les espaces $F = \ker(p - \text{Id})$ et $G = \ker p$ sont supplémentaires et

$$\forall x \in F, p(x) = x \text{ et } \forall x \in G, p(x) = 0_E$$

En effet $p^2 - p = \tilde{0}$ donc $E = \ker(p^2 - p)$.

Or $X^2 - X = (X - 1)X$ avec $(X - 1) \wedge X = 1$

donc $E = \ker(p^2 - p) = \ker(p - \text{Id}) \oplus \ker p$.

on reconnaît que p est la projection sur F parallèlement à G .

Exemple On appelle symétrie de E tout $s \in \mathcal{L}(E)$ vérifiant $s^2 = \text{Id}_E$.

Les espaces $F = \ker(s - \text{Id})$ et $G = \ker(s + \text{Id})$ sont supplémentaires et

$$\forall x \in F, s(x) = x \text{ et } \forall x \in G, s(x) = -x$$

En effet, $s^2 - \text{Id}_E = \tilde{0}$ donc $E = \ker(s^2 - \text{Id}_E)$.

Or $X^2 - 1 = (X - 1)(X + 1)$ avec $(X - 1) \wedge (X + 1) = 1$ donc $E = \ker(s - \text{Id}) \oplus \ker(s + \text{Id})$.

Posons $\Pi = \prod_{i=1}^m (X - \lambda_i)$ scindé à racines simples. Puisque les racines de Π sont exactement les racines de χ_u , on peut écrire

Exemple Soit $\lambda_1, \dots, \lambda_m$ les valeurs propres deux à deux distinctes de $u \in \mathcal{L}(E)$.

Les polynômes $X - \lambda_k$ étant deux à deux premiers entre eux, on retrouve que les sous-espaces propres d'un endomorphisme sont en somme directe.

6.4.2 Diagonalisabilité

Théorème

On a équivalence entre :

- (i) u est diagonalisable ;
- (ii) u annule un polynôme scindé à racines simples ;
- (iii) le polynôme minimal de u est scindé à racines simples.

De plus, le polynôme minimal de u est alors

$$\Pi_u = \prod_{\lambda \in \text{Sp} u} (X - \lambda)$$

Ce résultat se transpose aux matrices carrées.

dém. :

Notons $\lambda_1, \dots, \lambda_m$ les valeurs propres de u . $\prod_{k=1}^m (X - \lambda_k) \mid P(u)$

(i) $\Rightarrow$ (ii) Supposons u diagonalisable. On a

$$E = \bigoplus_{k=1}^m E_{\lambda_k}(u)$$

Dans une base adaptée à cette décomposition la matrice de u est de la forme

$$\begin{pmatrix} \lambda_1 I_{\alpha_1} & & (0) \\ & \ddots & \\ (0) & & \lambda_m I_{\alpha_m} \end{pmatrix} \text{ avec } \alpha_k = \dim E_{\lambda_k}(u)$$

Considérons le polynôme

$$P = \prod_{k=1}^m (X - \lambda_k)$$

Dans la base précédente, la matrice de $P(u)$ est

$$\begin{pmatrix} P(\lambda_1) I_{\alpha_1} & & (0) \\ & \ddots & \\ (0) & & P(\lambda_m) I_{\alpha_m} \end{pmatrix}$$

u annule le polynôme P qui est scindé à racines simples.

(ii) $\Rightarrow$ (iii) Si u annule un polynôme scindé à racines simples alors Π_u le divise et est donc lui-même scindé à racines simples.

(iii) $\Rightarrow$ (i) Supposons Π_u scindé à racines simples. Puisque les racines de Π_u sont exactement les valeurs propres de u , on peut écrire

$$\Pi_u = \prod_{k=1}^m (X - \lambda_k)$$

Or les facteurs $(X - \lambda_k)$ étant premiers entre eux, le lemme de décomposition des noyaux donne

$$E = \ker \Pi_u(u) = \bigoplus_{k=1}^m \ker(u - \lambda_k \text{Id}_E) = \bigoplus_{k=1}^m E_{\lambda_k}(u)$$

□

Définition

On dit qu'un polynôme de $\mathbb{K}[X]$ est scindé simple lorsqu'il est scindé dans $\mathbb{K}[X]$ à racines simples

Exemple Diagonalisation de $T : \mathcal{M}_n(\mathbb{R}) \rightarrow \mathcal{M}_n(\mathbb{R})$ définie par $T(M) = {}^t M$.

On a $T^2 = \text{Id}$ donc $X^2 - 1$ annule T .

Puisque le polynôme $X^2 - 1$ est scindé simple, l'endomorphisme T est diagonalisable.

De plus

$$\text{Sp} T \subset \{1, -1\}, E_1(T) = \ker(T - \text{Id}) = \mathcal{S}_n(\mathbb{R}) \text{ et } E_{-1}(T) = \ker(T + \text{Id}) = \mathcal{A}_n(\mathbb{R})$$

On en déduit $\text{tr} T = \dim \mathcal{S}_n(\mathbb{R}) - \dim \mathcal{A}_n(\mathbb{R}) = n$ et $\det T = (-1)^{\dim \mathcal{A}_n(\mathbb{R})} = (-1)^{n(n-1)/2}$.

En fait, l'endomorphisme T est la symétrie vectorielle par rapport à $\mathcal{S}_n(\mathbb{R})$ et parallèlement à $\mathcal{A}_n(\mathbb{R})$.

6.4. RÉDUCTION ET POLYNÔMES ANNULATEURS

Exemple Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A^2 + I = 0$.

Montrons que n est pair et calculons $\det A$ et $\text{tr} A$.

A annule $X^2 + 1 = (X - i)(X + i)$ scindé simple donc A est diagonalisable dans $\mathcal{M}_n(\mathbb{C})$.

De plus,

$$\text{Sp} A \subset \{i, -i\}$$

Or $\text{Sp} A \neq \emptyset$ et les valeurs propres de A sont conjuguées car $A \in \mathcal{M}_n(\mathbb{R})$ donc

$$\text{Sp} A = \{i, -i\}$$

Enfin, les multiplicités des valeurs propres conjuguées sont égales car $\chi_A \in \mathbb{R}[X]$ donc

$$\dim E_i(A) = \dim E_{-i}(A).$$

En posant p cette valeur commune, on peut affirmer que A est semblable dans $\mathcal{M}_n(\mathbb{C})$ à

$$\begin{pmatrix} iI_p & 0 \\ 0 & -iI_p \end{pmatrix}$$

On en déduit $n = 2p$, $\det A = 1$ et $\text{tr} A = 0$.

6.4.3 Réduction d'un endomorphisme induit par un endomorphisme diagonalisable

Lemme

Si F est un sous-espace vectoriel stable par $u \in \mathcal{L}(E)$ alors F est stable par tout polynôme en u et

$$\forall P \in \mathbb{K}[X], P(u)_F = P(u_F)$$

dém. :

Puisque F est stable par u , il l'est aussi par $u^2, \dots, u^n, \dots$ et

$$\forall n \in \mathbb{N}, (u_F)^n = (u^n)_F$$

Par combinaison linéaire, F est encore stable par les polynômes en u et

$$\forall P \in \mathbb{K}[X], P(u)_F = P(u_F)$$

Si u est diagonalisable alors u annule un polynôme scindé simple P et alors $P(u_F) = (P(u))_F = \tilde{0}$ donc u_F annule un polynôme scindé simple et est donc diagonalisable.

Proposition

Si F est stable par $u \in \mathcal{L}(E)$ alors le polynôme minimal de u_F divise le polynôme minimal de u .

dém. :

Le polynôme minimal de u est annulateur de u_F .

Théorème

Si $u \in \mathcal{L}(E)$ est diagonalisable et si F est un sous-espace vectoriel stable par u alors u_F est diagonalisable.

dém. :

Π_n est scindé à racines simples dont $\Pi_{n,p}$ l'est aussi.

□

Corollaire

Soit $u \in \mathcal{L}(E)$ diagonalisable.

Les sous-espaces vectoriels stables par u sont ceux admettant une base de vecteurs propres.

dém. :

Si F est stable par u alors $u|_F$ est diagonalisable donc F admet une base de vecteurs propres de $u|_F$. Ceux-ci sont aussi vecteurs propres de u .

Inversement, si $(e_1, \dots, e_p)$ est une base de F formée de vecteurs propres alors pour tout $j \in \{1, \dots, p\}$, $u(e_j) \in \text{Vect}(e_j) \subset F$ et donc F est stable par u .

□

Exemple Soit u et $v \in \mathcal{L}(E)$ diagonalisables.

Montrons que si u et v commutent alors il existe une base de E formée de vecteurs propres communs à u et v .

Puisque u est diagonalisable, $E = \bigoplus_{\lambda \in \text{Sp}(u)} E_\lambda(u)$.

Pour $\lambda \in \text{Sp}(u)$, $E_\lambda(u)$ est stable par v , or $v|_{E_\lambda(u)}$ est diagonalisable donc $v|_{E_\lambda(u)}$ l'est aussi. Ainsi, il existe une base B_λ de $E_\lambda(u)$ formée de vecteurs propres de v . Cette base est a fortiori formée de vecteurs propres de u . En accolant les bases B_λ , on forme une base de E formée de vecteurs propres communs à u et v .

Matriciellement, on a obtenu que si $A, B \in \mathcal{M}_n(\mathbb{K})$ sont diagonalisables et commutent alors il existe $P \in \text{GL}_n(\mathbb{K})$ vérifiant $P^{-1}AP$ et $P^{-1}BP$ diagonales.

6.4.4 Trigonalisabilité

Théorème

On a équivalence entre :

- (i) u est trigonalisable ;
- (ii) u annule un polynôme scindé dans $\mathbb{K}[X]$;
- (iii) le polynôme minimal de u est scindé dans $\mathbb{K}[X]$.

De plus, l'espace E est alors la somme directe de sous-espaces stables par u sur chacun desquels u induit la somme d'une homothétie et d'un endomorphisme nilpotent.

dém. :

(i) $\Rightarrow$ (ii) Car si u est trigonalisable alors u annule son polynôme caractéristique qui est scindé dans $\mathbb{K}[X]$.

(ii) $\Rightarrow$ (iii) Car le polynôme minimal divise un polynôme scindé.

(iii) $\Rightarrow$ (i) Supposons le polynôme minimal Π_u de u scindé dans $\mathbb{K}[X]$. On peut écrire

$$\Pi_u = \prod_{k=1}^m (X - \lambda_k)^{\alpha_k}$$

avec $\lambda_1, \dots, \lambda_m$ les valeurs propres distinctes de u . Par le lemme de décomposition des noyaux

$$E = \bigoplus_{k=1}^m \ker(u - \lambda_k \text{Id}_E)^{\alpha_k}$$

Étudions $F = \ker(u - \lambda_k \text{Id}_E)^{\alpha_k}$. L'espace F est stable par u car u et $(u - \lambda_k \text{Id}_E)^{\alpha_k}$ commutent. On peut introduire $n_k = u|_F - \lambda_k \text{Id}_F \in \mathcal{L}(F)$ et on a $n_k^{\alpha_k} = 0$ car $F = \ker(u - \lambda_k \text{Id}_E)^{\alpha_k}$. Ainsi $u|_F = \lambda_k \text{Id}_F + n_k$

avec n_k nilpotent. Enfin, puisque n_k est nilpotent, il existe une base F_k dans laquelle la matrice de n_k est triangulaire supérieure. En accolant ces bases, on obtient une base de E dans laquelle la matrice de u est triangulaire supérieure.

□

Remarque Les espaces $\ker(u - \lambda_k \text{Id}_E)^{\alpha_k}$ s'appellent espaces caractéristiques de l'endomorphisme u .

Corollaire

Si $A \in \mathcal{M}_n(\mathbb{K})$ est trigonalisable alors A est semblable à une matrice diagonale par blocs où chaque bloc diagonal est de la forme

$$\lambda I_n + N$$

avec N une matrice nilpotente.

Remarque Ce résultat s'applique automatiquement lorsque $\mathbb{K} = \mathbb{C}$ et l'on retrouve que toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable.

Corollaire

Si $u \in \mathcal{L}(E)$ est trigonalisable et si F est un sous-espace vectoriel stable par u alors u_F est trigonalisable.

dém. :

Π_u est scindé donc Π_{u_F} l'est aussi.

□

Exercice : décomposition de Dunford

Soit $u \in \mathcal{L}(E)$ avec Π_u scindé dans $\mathbb{K}[X]$.

On peut écrire $u = d + n$ avec d diagonalisable, n nilpotent et $d \circ n = n \circ d$.

dém. :

On introduit $\lambda_1, \dots, \lambda_m$ les valeurs propres deux à deux distincts de u .

$$\Pi_u = \prod_{k=1}^m (X - \lambda_k)^{\mu_k} \text{ et } E = \bigoplus_{k=1}^m \ker(u - \lambda_k \text{Id}_E)^{\mu_k}$$

Posons d l'endomorphisme déterminé par

$$\forall 1 \leq k \leq m, \forall x \in \ker(u - \lambda_k \text{Id}_E)^{\mu_k}, d(x) = \lambda_k x$$

L'endomorphisme d est évidemment diagonalisable, ses sous-espaces propres sont les espaces caractéristiques.

Posons n l'endomorphisme donné par $n = u - d$.

$$\forall 1 \leq k \leq m, \forall x \in \ker(u - \lambda_k \text{Id}_E)^{\mu_k}, n^{\mu_k}(x) = 0_E$$

Pour $N = \max(\mu_1, \dots, \mu_m)$, on obtient

$$\forall 1 \leq k \leq m, \forall x \in \ker(u - \lambda_k \text{Id}_E)^{\mu_k}, n^N(x) = 0_E$$

L'endomorphisme n est donc nilpotent.

Enfin

$$\forall 1 \leq k \leq m, \forall x \in \ker(u - \lambda_k \text{Id}_E)^{n_k}, (n \circ d)(x) = \lambda_k n(x) = (d \circ n)(x)$$

et donc les endomorphismes d et n commutent.

On peut aussi montrer qu'il y a unicité des endomorphismes d et n de cette décomposition.

Supposons d et n solutions.

d commute avec n donc aussi avec $u = d + n$.

L'espace caractéristique $F = \ker(u - \lambda \text{Id}_E)^n$ est alors stable par d .

L'endomorphisme induit par d sur F est diagonalisable.

Soit μ une valeur propre de celui-ci et $G \subset F$ l'espace propre associé.

G est stable par u et donc aussi par $n = u - d$ et l'on a

$$u_G = \mu \text{Id}_G + n_G$$

Puisque n_G est nilpotent, on peut calculer χ_{u_G} dans une base trigonalisant n_G et affirmer que μ est alors valeur propre de u_G donc de u_F . Or λ est la seule valeur propre de u_F et donc $\mu = \lambda$. On en déduit que λ est la seule valeur propre de l'endomorphisme diagonalisable d_F et ainsi

$$\forall x \in F, d(x) = \lambda x$$

L'endomorphisme d est alors déterminé de façon unique sur les espaces caractéristiques de u .

L'endomorphisme $n = u - d$ est alors aussi unique.

□

Remarque La décomposition de Dunford est utile pour calculer les puissances de u car la formule du binôme peut lui être appliquée.

6.4.2. Misculation : décomposition de Dunford

Théorème

Soit $u \in \mathcal{L}(E)$ avec II_u scindé dans $\mathbb{C}[X]$.
On peut écrire $u = d + n$ avec d diagonalisable et n nilpotent et d, n commutent.

$$\text{II}_u = \prod_{i=1}^m (X - \lambda_i)^{n_i} \quad \text{avec } \lambda_i \in \mathbb{C} \text{ et } n_i \in \mathbb{N}^*$$

Posez $\lambda = \max\{\lambda_i \mid 1 \leq i \leq m\}$.

$$\forall 1 \leq k \leq m, \forall x \in \ker(u - \lambda_k \text{Id}_E)^{n_k}, (n \circ d)(x) = \lambda_k n(x) = (d \circ n)(x)$$

L'endomorphisme n est donc nilpotent et d commute avec n .

On pose $u = d + n$ et on a d, n commutent.

$$\forall 1 \leq k \leq m, \forall x \in \ker(u - \lambda_k \text{Id}_E)^{n_k}, (n \circ d)(x) = \lambda_k n(x) = (d \circ n)(x)$$

Posez $\lambda = \max\{\lambda_i \mid 1 \leq i \leq m\}$.

$$\forall 1 \leq k \leq m, \forall x \in \ker(u - \lambda_k \text{Id}_E)^{n_k}, (n \circ d)(x) = \lambda_k n(x) = (d \circ n)(x)$$