Al5 : Polynômes de matrices et d'endomorphismes

I Polynôme d'un élément d'une algèbre

On note $(\mathscr{A}, +, \times, .)$ une algèbre sur le corps commutatif $\mathbf{K}$ (ou $\mathbf{K}$-algèbre). Cette algèbre est unitaire, on notera e son élément neutre.

Rappelons que cela signifie simplement que
$(\mathscr{A}, +, .)$ est un $\mathbf{K}$-espace vectoriel et
$(\mathscr{A}, +, \times)$ est un anneau, e étant l'élément neutre pour $\times$.
Avec la propriété supplémentaire

$$\forall (x, y) \in \mathscr{A}^2 \quad \forall \lambda \in \mathbf{K} \qquad (\lambda.x) \times y = x \times (\lambda.y) = \lambda.(x \times y)$$

Définition

Si $P = \sum_{k=0}^{+\infty} p_k X^k = p_d X^d + \ldots + p_1 X + p_0 \in \mathbf{K}[X]$, et si $a \in \mathscr{A}$, on note

$$P(a) = \sum_{k=0}^{+\infty} p_k a^k = p_d a^d + \ldots + p_1 a + p_0 e$$

et on définit bien ainsi un élément de $\mathscr{A}$.

Cas particulier des polynômes d'endomorphismes

Ainsi, si u est un endomorphisme d'un $\mathbf{K}$-espace vectoriel E et si $P = \sum_{k=0}^{+\infty} p_k X^k = p_d X^d + \ldots + p_1 X + p_0 \in \mathbf{K}[X]$, on définit le polynôme d'endomorphisme

$$P(u) = \sum_{k=0}^{+\infty} p_k u^k = p_d u^d + \ldots + p_1 u + p_0 \operatorname{Id}_E$$

(on est dans l'algèbre $\left(\mathscr{L}(E),+,\circ,.\right)$)

Cas particulier des polynômes de matrices

Et, si A est une matrice dans $\mathscr{M}_n(\mathbf{K})$ et
$P=\sum_{k=0}^{+\infty} p_k X^k = p_d X^d + \ldots + p_1 X + p_0 \in \mathbf{K}[X]$, on définit

$$P(A)=\sum_{k=0}^{+\infty} p_k A^k = p_d A^d + \ldots + p_1 A + p_0\, I_n$$

(on est dans l'algèbre $\left(\mathscr{M}_n(\mathbf{K}),+,\times,.\right)$).

Remarque Cette définition est d'une grande simplicité. Notons néanmoins que si $P=X^2-1$ et si A est une matrice, $P(A)$ n'est pas $A^2-1\ldots$.
Il n'est pas question ici de fonction polynôme associée : $P(A)$ ne se note pas $\widetilde{P}(A)$.

Polynômes de polynômes

On fait la même chose lorsque P et Q sont deux polynômes dans $\mathbf{K}[X]$: si $P=p_n X^n+\ldots+p_1X+p_0$, on définit

$$P(Q)=p_nQ^n+\ldots+p_1Q+p_0$$

(dans l'algèbre $\left(\mathbf{K}[X],+,\times,.\right)$, cette fois). Ce qui justifie la remarque habituelle « P ou $P(X)$, c'est la même chose ».

Remarque Dans ce dernier cas l'algèbre est commutative, mais en général elle ne l'est pas (puisqu'en pratique, les objets sont des matrices ou des endomorphismes).

II Sous-algèbre engendrée par un endomorphisme ou une matrice

II.1 Définition de $\mathbf{K}[a]$

On note encore $(\mathscr{A}, +, \times, .)$ une algèbre sur le corps commutatif $\mathbf{K}$.

Définition

Soit $a \in \mathscr{A}$. On note

$$\mathbf{K}[a] = \{P(a)\ ;\ P \in \mathbf{K}[X]\} = \mathrm{Vect}\big((a^n)_{n\in\mathbf{N}}\big)$$

On voit facilement que $\mathbf{K}[a]$ est la plus petite sous-algèbre de $(\mathscr{A}, +, \times, .)$ contenant a. Autrement dit, c'est la sous-algèbre de $(\mathscr{A}, +, \times, .)$ engendrée par a.

Vocabulaire

On dit que l'endomorphisme v est un polynôme de l'endomorphisme u lorsque $v \in \mathbf{K}[u]$, i.e. lorsqu'il existe P polynôme tel que $v = P(u)$.
On dit que la matrice B est un polynôme de A lorsqu'il existe P polynôme tel que $B = P(A)$, i.e. lorsque $B \in \mathbf{K}[A]$.

II.2 Calcul dans $\mathbf{K}[a]$

Proposition : Soit a un élément de $\mathscr{A}$. L'application

$$\begin{array}{rccc} \phi_a : & \mathbf{K}[X] & \longrightarrow & \mathscr{A} \\ & P & \longmapsto & P(a) \end{array}$$

est un morphisme d'algèbres, ce qui signifie que c'est à la fois
• un morphisme de l'anneau $(\mathbf{K}[X], +, \times)$ dans l'anneau $(\mathscr{A}, +, \times)$
• une application linéaire de l'espace vectoriel $(\mathbf{K}[X], +, .)$ dans l'espace vectoriel $(\mathscr{A}, +, .)$

Signification dans le cas des polynômes d'endomorphismes :

Si P, Q sont des polynômes, si u est un endomorphisme, si $\lambda \in \mathbf{K}$:

$$(\lambda P + \mu Q)(u) = \lambda P(u) + \mu Q(u)$$
$$(PQ)(u) = P(u) \circ Q(u) = Q(u) \circ P(u)$$
$$1(u) = \mathrm{Id}_E$$

Signification dans le cas des polynômes de matrices :

Si P, Q sont des polynômes, si A est une matrice, si $\lambda \in \mathbf{K}$:

$$(\lambda P + \mu Q)(A) = \lambda P(A) + \mu Q(A)$$
$$(PQ)(A) = P(A)\ Q(A) = Q(A)\ P(A)$$
$$1(A) = I_n$$

On doit donc faire un petit peu plus attention au cas des endomorphismes, la multiplication des polynômes se traduit par une composition, alors que pour les matrices tout est de la multiplication, on ne voit donc pas de difficulté.

Remarque $\mathrm{Im}(\phi_a) = \mathbf{K}[a]$, on retrouve le fait que $\mathbf{K}[a]$ est une sous-algèbre de $\mathscr{A}$.

Remarque L'algèbre $\mathbf{K}[a], +, \times, .)$ est commutative (contrairement à $\mathscr{A}$ dans les deux cas qui nous intéressent).

Remarque

Attention aux contresens : $\mathbf{K}[a]$ est bien la plus petite sous-algèbre de $\mathscr{A}$ contenant a.

Ce n'est pas le plus petit sous-espace vectoriel de $(\mathscr{A}, +, .)$ contenant a (qui est ...

Ce n'est pas le plus petit sous-anneau de $(\mathscr{A}, +, \times)$ contenant a (qui est

...

...moins évident !)

C'est la plus petite partie de A contenant a qui soit à la fois un sous-espace vectoriel et un sous-anneau de $(\mathscr{A}, +, \times, .)$.

III Polynômes annulateurs, polynôme minimal

III.1 Définitions

Soit $(\mathscr{A},+,\times,.)$ une $\mathbf{K}$-algèbre unitaire, $a \in \mathscr{A}$.

Proposition - Définition

On suppose que l'algèbre $\mathscr{A}$ est de dimension finie ; le morphisme

$$\begin{array}{rccc} \phi_a : & \mathbf{K}[X] & \longrightarrow & \mathscr{A} \\ & P & \longmapsto & P(a) \end{array}$$

ne peut alors pas être injectif.
$\text{Ker}(\phi_a) = \{P\ ;\ P(a) = 0_{\mathscr{A}}\}$ est un idéal non nul de l'anneau $(\mathbf{K}[X],+,\times)$.
On dit que $\text{Ker}(\phi_a)$ est l'idéal des polynômes annulateurs de a.
Il existe un unique polynôme unitaire π_a tel que

$$\text{Ker}(\phi_a) = \left(\pi_a\right) = \{\pi_a\, Q\ ;\ Q \in \mathbf{K}[X]\}$$

Ce polynôme est appelé polynôme minimal de a.
On remarque que π_a est le polynôme unitaire de plus petit degré qui annule a.
Et on a

$$Q(a) = 0_{\mathscr{A}} \iff \pi_a | Q$$

Cette définition générale n'est pas au programme. Sont au programme les deux déclinaisons suivantes :

Proposition - Définition

Soit $n \geq 1$, $A \in M_n(\mathbf{K})$. Le morphisme

$$\begin{array}{rccc} \phi_A : & \mathbf{K}[X] & \longrightarrow & M_n(\mathbf{K}) \\ & P & \longmapsto & P(A) \end{array}$$

n'est pas injectif.
$\text{Ker}(\phi_A) = \{P\ ;\ P(A) = (0)\}$ est un idéal non nul de l'anneau $(\mathbf{K}[X],+,\times)$.
On dit que $\text{Ker}(\phi_A)$ est l'idéal des polynômes annulateurs de A.

Il existe un unique polynôme unitaire π_A tel que

$$\mathrm{Ker}(\phi_A) = \left(\pi_A\right) = \{\pi_A\, Q\ ;\ Q \in \mathbf{K}[X]\}$$

Ce polynôme est appelé polynôme minimal de A.
On remarque que π_A est le polynôme unitaire de plus petit degré qui annule A.
Et on a

$$Q(A) = (0) \iff \pi_A | Q$$

Proposition - Définition

Soit E un $\mathbf{K}$-espace vectoriel de dimension finie, $u \in L(E)$. Le morphisme

$$\begin{array}{rccc} \phi_u : & \mathbf{K}[X] & \longrightarrow & L(E) \\ & P & \longmapsto & P(u) \end{array}$$

n'est pas injectif.
$\mathrm{Ker}(\phi_u) = \{P\ ;\ P(u) = \Theta\}$ est un idéal non nul de l'anneau $(\mathbf{K}[X], +, \times)$.
On dit que $\mathrm{Ker}(\phi_u)$ est l'idéal des polynômes annulateurs de u.
Il existe un unique polynôme unitaire π_u tel que

$$\mathrm{Ker}(\phi_u) = \left(\pi_u\right) = \{\pi_u\, Q\ ;\ Q \in \mathbf{K}[X]\}$$

Ce polynôme est appelé polynôme minimal de u.
On remarque que π_u est le polynôme unitaire de plus petit degré qui annule u.
Et on a

$$Q(u) = \Theta \iff \pi_u | Q$$

Un endomorphisme en dimension non finie n'a pas nécessairement un polynôme minimal. Il peut en avoir un, ou ne pas en avoir.

Attention ! contrairement à ce qui se passe pour les nombres algébriques, le polynôme minimal d'un endomorphisme ou d'une matrice n'est pas en général irréductible. Cela est dû à la non intégrité des algèbres $\left(\mathscr{L}(E), +, \circ, .\right)$ *et* $\left(\mathscr{M}_n(\mathbf{K}), +, \times, .\right)$.

III.2 Quelques exemples

Dans ces trois premiers exemples, on donne $\mathscr{A}$ et a. Déterminer le polynôme minimal de a.

(1) $\mathscr{A} = \mathscr{L}(E)$ (E un $\mathbf{K}$-espace vectoriel), $a = \lambda \mathrm{Id}_E$

(2) $\mathscr{A} = \mathscr{L}(E)$ (E un $\mathbf{K}$-espace vectoriel), a un projecteur. Trois polynômes minimaux sont envisageables (dont deux « rares »).

(3) $\mathscr{A} = \mathscr{L}(E)$ (E un $\mathbf{K}$-espace vectoriel), a une symétrie (ou : involution vectorielle). On envisage aussi trois cas.

(4) $\mathscr{A} = \mathscr{M}_n(\mathbf{K})$, $a = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ \vdots & & & & 0 & 1 \\ 0 & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$.

(5) Ici, $\mathscr{A} = \mathscr{L}(\mathbf{K}[X])$, $a : P \longmapsto P'$. Montrer que a n'admet pas de polynôme minimal.

III.3 Dimension de $\mathbf{K}[a]$ et degré du polynôme minimal

Dans l'énoncé qui suit, a est un élément d'une $\mathbf{K}$-algèbre unitaire $(\mathscr{A}, +, \times, .)$ qui en pratique est une algèbre $(M_n(\mathbf{K}), +, \times, .)$ ou une algèbre $(L(E), +, \times, .)$

Théorème

L'algèbre $\mathbf{K}[a] = \{P(a)\ ;\ P \in \mathbf{K}[X]\}$ est de dimension finie si et seulement si a a un polynôme minimal (i.e. si et seulement si ϕ_a n'est pas injectif). Et dans ce cas

$$\dim\big(\mathbf{K}[a]\big) = \deg(\pi_a)$$

Plus précisément, si $d = \deg(\pi_a)$, $(a^n)_{0 \leq n \leq d-1}$ est une base de $\mathbf{K}[a]$. et l'espace vectoriel $(\mathbf{K}[a], +, .)$ est isomorphe à l'espace vectoriel $(\mathbf{K}_d[X], +, .)$. On a alors trois manières également intéressantes d'écrire $\mathbf{K}[a]$:

$$\mathbf{K}[a] = \{P(a)\ ;\ P \in \mathbf{K}_{d-1}[X]\}$$

$$\mathbf{K}[a] = \mathrm{Vect}\left(\left(a^n\right)_{n \geq 0}\right)$$

$$\mathbf{K}[a] = \mathrm{Vect}\left(\left(a^n\right)_{0 \leq n \leq d-1}\right)$$

Si ϕ_a est injectif, a n'a pas de polynôme minimal, et l'algèbre $(\mathbf{K}[a], +, ., \times)$ est isomorphe à l'algèbre $(\mathbf{K}[X], +, ., \times)$.

Remarque Ce dernier cas (ϕ_a injectif) ne peut pas se produire si $\mathscr{A}$ est de dimension finie : si $a \in \mathscr{M}_n(\mathbf{K})$, ou si $a \in L(E)$ avec $\dim(E) < +\infty$, alors a a un polynôme minimal.

Proposition

Soit $A \in M_n(\mathbf{K})$. Alors $d = \deg(\pi_A)$ est caractérisé par :
La famille $(I_n, \ldots, A^{d-1})$ est , et la famille $(I_n, \ldots, A^d)$ est
Soit $u \in L(E)$, E espace vectoriel de dimension finie. Alors $d = \deg(\pi_u)$ est caractérisé par :
La famille $(\mathrm{Id}_E, \ldots, u^{d-1})$ est , et la famille $(\mathrm{Id}_E, \ldots, u^d)$ est

Exemple : Si $\mathscr{A} = \mathscr{L}(E)$ (E un $\mathbf{K}$-espace vectoriel), et si a est un projecteur, supposé différent de Θ et de Id_E, décrire $\mathbf{K}[a]$.

IV Polynôme d'un endomorphisme, polynôme de sa matrice

Exercice : Soit $u \in L(E)$ où E est un espace vectoriel de dimension finie. Soit B une base de E. Montrer

$$\forall P \in \mathbf{K}[X] \qquad M_B\left(P(u)\right) = P\left(M_B(u)\right)$$

Exercice : Soit $D = \mathrm{diag}(d_1, \ldots, d_n) \in M_n(\mathbf{K})$ une matrice diagonale. Soit $P \in \mathbf{K}[X]$. Calculer $P(D)$.

Un exercice d'oral : Soit $u \in L(E)$ où E est un espace vectoriel de dimension $n \geq 1$. On suppose diagonalisable. Si $\lambda \in \mathrm{Sp}(u)$, on note p_λ la projection sur $E_\lambda(u)$ parallèlement à $\displaystyle\bigoplus_{\mu \in \mathrm{Sp}(u) \setminus \{\lambda\}} E_\mu(u)$. Montrer que $p_\lambda \in \mathbf{K}[u]$.

Table des matières