# Cours de mathématiques P.S.I.*

D'après les cours de M. Guillaumie

Henriet Quentin

*LibreOffice 3.3*

# Polynômes d'endomorphismes et de matrices

Dans ce chapitre, $E$ désigne un $\mathbb{K}$-ev, $u\in\mathscr{L}(E)$, $A\in\mathscr{M}_n(\mathbb{K})$ $(n\geqslant 1)$.

## I. Idéaux de $\mathbb{K}[X]$

***Définition :***

Soit $I$ une partie de $\mathbb{K}[X]$. On dit que $I$ est un idéal de $\mathbb{K}[X]$ si :

1. $0\in\mathbb{K}$
2. $I$ est stable par $+$
3. $\forall P\in I,\ \forall Q\in\mathbb{K}[X],\ PQ\in I$ (on dit que $I$ est absorbant).

*Exemple :*

Soit $A\in\mathbb{K}[X]$. On note $A\mathbb{K}[X]$ ou $\langle A\rangle$ l'ensemble des multiples de $A$.

$A\mathbb{K}[X]=\{P\in\mathbb{K}[X] \text{ tel que } A|P\}=\{P\in\mathbb{K}[X] \text{ tel que } \exists Q\in\mathbb{K}[X] \text{ tel que } P=AQ\}$.

$A\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$ : $0\in A\mathbb{K}[X]$, si $A|P_1$ et $A|P_2$, alors $A|P_1+P_2$, et si $A|P$, $\forall B\in\mathbb{K}[X]$, $A|PB$.

***Définition :***

L'idéal $A\mathbb{K}[X]$ est appelé idéal principal de $\mathbb{K}[X]$ engendré par $A$.

On dit que $A$ est un générateur de $A\mathbb{K}[X]$. Si $A=0$, alors $0\mathbb{K}[X]=\{0\}$ est appelé idéal nul de $\mathbb{K}[X]$.

***Propriétés :***

Soit $A$ un générateur de $I$, $I$ idéal principal non nul.

1. $A\neq 0$
2. $\forall P\in I,\ A|P$
3. Soit $B$ un autre générateur de $I$. $B|A$ et $A|B$, $\exists\alpha\neq 0$ tel que $B=\alpha A$. $A$ et $B$ sont dits associés
4. Il existe un unique générateur de $I$ unitaire.

***Théorème :***

Dans $\mathbb{K}[X]$, tous les idéaux sont principaux.

*Preuve :*

Soit $I$ un idéal de $\mathbb{K}[X]$. On veut montrer que $\exists A\in\mathbb{K}[X]$ tel que $I=A\mathbb{K}[X]$.

- $I=\{0\}$ : $A=0$ convient.
- $I\neq\{0\}$ : On considère $\mathcal{C}=\{\deg(P) \text{ tel que } P\in I\setminus\{0\}\}$. $\mathcal{C}\neq 0$, et $\mathcal{C}\subset\mathbb{N}$. $\mathcal{C}$ admet un plus petit élément $d$.
  Soit $A\in I$ tel que $\deg(A)=d$.
  - $\supset$ : Soit $P\in A\mathbb{K}[X]\Rightarrow\exists Q\in\mathbb{K}[X]$ tel que $P=AQ$. $A\in I$ et $I$ étant un idéal, $P\in I$. Donc $A\mathbb{K}[X]\subset I$.
  - $\subset$ : Soit $P\in I$, on effectue la division euclidienne de $P$ par $A$ : $\exists(Q,R)\in\mathbb{K}[X]^2$ tel que $P=AQ+R$ et $\deg(R)<\deg(A)$. $AQ\in I$, et $P\in I$, donc $R\in I$.
    Si $\deg(R)\neq 0$, $\deg(R)\in\mathcal{C}$, or $\deg(R)<\deg(A)=d=\text{ppe}(\mathcal{C})$ : impossible, donc $R=0$.
    Ainsi $P=AQ\in A\mathbb{K}[X]\Rightarrow I\subset A\mathbb{K}[X]$.

***Remarque :***

Si $I\neq\{0\}$, et $I=A\mathbb{K}[X]$, $A$ est un polynôme de $I$ non nul de degré minimal.

## 2. Polynômes d'endomorphismes et de matrices

***Définition :***

Soient $P=\sum_{k=0}^{d} a_k X^k$ un polynôme de $\mathbb{K}[X]$, $u\in\mathscr{L}(E)$, $A\in\mathscr{M}_n(\mathbb{K})$.

On note $P(u)=\sum_{k=0}^{d} a_k u^k$, et $P(A)=\sum_{k=0}^{d} a_k A^k$.

On dit que $P(u)$ est un polynôme de $u$, et $P(A)$ un polynôme de $A$.

***Remarques :***

Attention aux objets manipulés ! $P(u)$ est un polynôme, et $P(A)$ est une matrice.

$1(u)=\mathrm{Id}_E$, $1(A)=I_n$.

## 3. Propriétés algébriques

***Définition :***

On note $\mathbb{K}[u]$ l'ensemble des polynômes de $u$, et $\mathbb{K}[A]$ l'ensemble des polynômes de $A$.

$\mathbb{K}[u]=\{P(u),\ P\in\mathbb{K}[X]\}$, et $\mathbb{K}[A]=\{P(A),\ P\in\mathbb{K}[X]\}$.

***Proposition :***

Soit $(P,Q)\in\mathbb{K}[X]^2$. $\forall(\alpha,\beta)\in\mathbb{K}^2$ :

1. $(\alpha P+\beta Q)(u)=\alpha P(u)+\beta Q(u)$, et $(\alpha P+\beta Q)(A)=\alpha P(A)+\beta Q(A)$.
2. $(PQ)(u)=(P(u))\circ(Q(u))$, et $(PQ)(A)=(P(A))\times(Q(A))$.

*Preuve (2) :*

Soient $P=\sum_{k=0}^{d} a_k X^k$, $Q=\sum_{k=0}^{s} b_k X^k$. $PQ=\sum_{k=0}^{d+s}\left(\sum_{q=0}^{k} a_q b_{k-q}\right)X^k=\sum_{k=0}^{d+s}\left(\sum_{q+r=k} a_q b_r\right)$

Or $P(u)\circ Q(u)=\left(\sum_{q=0}^{d} a_q u^q\right)\circ\left(\sum_{r=0}^{s} b_r u^r\right)=\sum_{q=0}^{d}\sum_{r=0}^{s} a_q b_r u^{q+r}=\sum_{k=0}^{d+s}\left(\sum_{q+r=k} a_q b_r\right)u^k=(PQ)(u)$.

$PQ=QP$ dans $\mathbb{K}[X]$, donc $P(u)\circ Q(u)=Q(u)\circ P(u)$. Deux polynômes en $u$ commutent .

***Corollaire :***

$\mathbb{K}[u]$ et $\mathbb{K}[A]$ sont des sous-algèbres commutatives de $\mathscr{L}(E)$ et de $\mathscr{M}_n(\mathbb{K})$ respectivement.

***Propriétés :***

Soit $u\in\mathscr{L}(E)$, on pose $\phi$ : $\begin{array}{ccc}\mathbb{K}[X] & \to & \mathscr{L}(E)\\ P & \mapsto & P(u)\end{array}$. On a alors les propriétés suivantes :

1. $\forall(P,Q)\in\mathbb{K}[X]^2$, $\forall(\alpha,\beta)\in\mathbb{K}^2$, $\phi(\alpha P+\beta Q)=\alpha\phi(P)+\beta\phi(Q)$
2. $\forall(P,Q)\in\mathbb{K}[X]^2$, $\phi(PQ)=\phi(P)\circ\phi(Q)$
3. $\phi(1)=\mathrm{Id}_E$.
4. $\phi$ est un morphisme d'algèbre et $\mathrm{Im}(\phi)=\mathbb{K}[u]$.

***Proposition :***

$\forall P\in\mathbb{K}[X]$, $\mathrm{Ker}(P(u))$ est stable par $u$.

*Preuve :*

Soit $x\in\mathrm{Ker}(P(u))$. $(P(u))(x)\times u(x)=(P(u)\circ u)(x)=(u\circ P(u))(x)=u((P(u))(x))=u(0_E)=0$.

# 4. Polynôme annulateur

***Définition :***
Soit $P\in\mathbb{K}[X]$. On dit que $P$ est annulateur de $u$ (respectivement de $A$) si $P(u)=0$, (respectivement $P(A)=0$).

***Définition :***
On note $\mathscr{I}_u$ (respectivement $\mathscr{I}_A$) l'ensemble des polynômes annulateurs de $u$ (respectivement de $A$).

***Remarque :***
$\forall\alpha\in\mathbb{K}$, $\alpha(u)=\alpha\,\mathrm{Id}_E$, donc $\alpha(u)=0 \Leftrightarrow \alpha=0$. Il n'existe donc pas de polynôme annulateur de degré $0$.

*Exemples :*

1. Si $u=\alpha\,\mathrm{Id}_E$, $X-\alpha$ est annulateur de $u$.
2. Si $p$ est un projecteur de $E$, $X^2-X$ est annulateur de $p$.
3. Si $s$ est une symétrie de $E$, $X^2-1$ est annulateur de $s$.

*Exemple :*

Soit $A=\begin{pmatrix} a & b & \dots & b \\ b & \ddots & & \vdots \\ \vdots & & \ddots & b \\ b & \dots & b & a \end{pmatrix}\in\mathscr{M}_n(\mathbb{K})$, $b\neq0$. Soit $J=\begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{pmatrix}$, $J^2=nJ$.

$A=(a-b)I_n+bJ \Rightarrow (A-(a-b)I_n)^2=b^2J^2=b^2nJ=nb(A-(a-b)I_n) \Rightarrow (A-(a-b)I_n)(A-(a-b)I_n-nbI_n)=0$
$\Rightarrow (X-(a-b))(X-(a+(n-1)b))$ est annulateur de $A$.

*Exemple : Matrice de rang 1 :*

Toute matrice carrée $A$ de rang $1$ peut s'écrire sous la forme $A=U\,{}^tV$, où $U=\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, et $V=\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$, $U\neq0$ et $V\neq0$.

$A^2=U\,{}^tV\,U\,{}^tV=U\underbrace{({}^tV\,U)}_{\in\mathbb{K}}{}^tV=({}^tV\,U)\,U\,{}^tV=({}^tU\,V)A$, or ${}^tU\,V=\sum_{i=1}^{n}u_iv_i=\mathrm{tr}(A)$.

Ainsi $A^2=\mathrm{tr}(A)A \Rightarrow X^2-\mathrm{tr}(A)X$ est annulateur de $A$.

***Théorème :***

| Tout endomorphisme d'un espace vectoriel de dimension finie admet au moins un polynôme annulateur non nul. |
|---|

*Preuve :*

On note $n=\dim(E)$, ainsi $\dim(\mathscr{L}(E))=n^2$. Alors la famille $(\mathrm{id}_E,u,u^2,\dots,u^{n^2})$ est une famille de $\mathscr{L}(E)$ formée de $n^2+1$ éléments de $\mathscr{L}(E)$, il s'agit donc d'une famille liée dans $\mathscr{L}(E)$ : $\exists(a_0,\dots,a_{n^2})\in\mathbb{K}^{n^2+1}\setminus\{(0,\dots,0)\}$ tel que $\sum_{k=0}^{n^2}a_ku^k=0$. Ainsi $P=\sum_{k=0}^{n^2}a_kX^k$ est annulateur de $u$, et $P\neq0$.

***Remarque :***
Toute matrice carrée admet donc un polynôme annulateur non nul.

***Remarque :***
La preuve du théorème donne l'existence d'un polynôme annulateur de degré inférieur à $n^2$, où $n=\dim(E)$.
On verra qu'en dimension $n$, il existe des polynômes annulateurs non nuls de degré inférieur à $n$.

***Remarque :***
Le résultat de ce théorème est faux en dimension infinie.

*Exemple :*

Soit $E=\mathbb{K}[X]$, $u : P\in E \mapsto XP(X) \in \mathscr{L}(E)$. $\forall P\in E$, $\forall k\in\mathbb{N}$, $u^k(P)=X^pP$.

Soit alors $Q=\sum_{k=0}^{d} a_k X^k$, et $P\in E$. Alors $(Q(u))(P)=\sum_{k=0}^{d} a_k u^k(P)=\left(\sum_{k=0}^{d} a_k X^k\right)P=QP$.

Si $Q$ est annulateur de $u$, alors $Q(u)=0$ donc $\forall P\in E$, $(Q(u))(P)=0$. Ainsi $\forall P\in E$, $QP=0$.

En particulier pour $P=1$ : $Q=0$.

***Proposition :***

Si $u\in\mathscr{L}(E)$, alors $\mathscr{I}_u$ est un idéal de $\mathbb{K}[X]$. Si $A\in\mathscr{M}_n(\mathbb{K})$, alors $\mathscr{I}_A$ est un idéal de $\mathbb{K}[X]$.

*Preuve :*

- $0\in\mathscr{I}_u$ $(0(u)=0)$
- Soient $P$ et $Q\in\mathscr{I}$. Alors $(P+Q)(u)=P(u)+Q(u)=0 \Rightarrow P+Q\in\mathscr{I}$.
- Soit $P\in\mathscr{I}_u$ et $Q\in\mathbb{K}[X]$. Alors $(PQ)(u)=P(u)\circ Q(u)=0 \Rightarrow PQ\in\mathscr{I}_u$.

***Remarque :***

$\mathscr{I}_u$ est donc un idéal principal de $\mathbb{K}[X]$.

Si $\mathscr{I}_u\neq\{0\}$, il existe alors un unique polynôme unitaire noté $\pi_u$ qui engendre $\mathscr{I}_u$.

$\pi_u$ est appelé polynôme minimal de $u$.

***Propriétés du polynôme minimal (hors programme) :***

1. $\pi_u$ est annulateur de $u$
2. Tout polynôme annulateur $P$ de $u$ est un multiple de $\pi_u$ : $\pi_u | P$
3. $\pi_u$ est un polynôme annulateur de degré minimal au moins 1.

# 5. Premières applications

## 5.1. Calcul de l'inverse d'une matrice

Soit $A\in\mathscr{M}_n(\mathbb{K})$. On suppose connu un polynôme annulateur $P=\sum_{k=0}^{d} a_k X^k$ de $A$ tel que $P(0)\neq 0$.

Alors $A$ est inversible et on peut obtenir $A^{-1}$ de la façon suivante :

$$P(A)=0 \Leftrightarrow \sum_{k=0}^{d} a_k A^k \Leftrightarrow \sum_{k=1}^{d} a_k A^k=-a_0 I_n \Leftrightarrow \left(\sum_{k=1}^{d} a_k A^{k-1}\right)A=-a_0 I_n$$

$A$ est donc bien inversible et $A^{-1}=-\frac{1}{a_0}\sum_{k=1}^{d} a_k A^{k-1}=Q(A)$, et $Q(X)=\frac{-P(X)+P(0)}{P(0)X}$.

## 5.2. Calcul des puissances successives d'une matrice carrée

Soit $A\in\mathscr{M}_n(\mathbb{K})$. On suppose connu un polynôme annulateur de $\pi\neq 0$.

Pour trouver $A^p$ on effectue la division euclidienne de $X^p$ par $\pi$ : $\exists(Q,R)\in\mathbb{K}[X]^2$ tel que $X^p=\pi Q+R$,

avec $\deg(P)<\deg(\pi)$. On applique alors ces polynômes en $A$ : $A^p=(\pi Q+R)(A)=\pi(A)Q(A)+R(A)=R(A)$.

Il suffit de déterminer $R$, reste dans la division euclidienne de $X^p$ par $\pi$. Pour cela, on évalue en les racines de $\pi$.

* * * * *