Polynômes annulateurs

1) Polynômes d'endomorphismes et de matrices

a) *Définitions et notations*

Soient $P = \sum_{k=0}^{n} a_k X^k \in K[X]$, $u \in \mathcal{L}(E)$ où E est un K-espace vectoriel, $A \in \mathcal{M}_p(K)$.

On pose $P(u) = \sum_{k=0}^{n} a_k u^k \in \mathcal{L}(E)$, où $u^0 = \mathrm{Id}_E$ et de façon générale, u^k désigne la composée k fois de u.

De même, $P(A) = \sum_{k=0}^{n} a_k A^k = a_0 I_p + a_1 A + a_2 A^2 + ... + a_n A^n \in \mathcal{M}_p(K)$.

Exemple : Avec $P = X^2 - X = X(X-1) = (X-1)X$, on a $P(u) = u^2 - u = u \circ (u - \mathrm{Id}) = (u - \mathrm{Id}) \circ u$

b) *Propriétés algébriques*

On a : $(\lambda P + \mu Q)(u) = \lambda P(u) + \mu Q(u)$, et $\boxed{(PQ)(u) = P(u) \circ Q(u) = Q(u) \circ P(u)}$.

Donc $\operatorname{Ker} P(u)$ et $\operatorname{Ker} Q(u)$ sont inclus dans $\operatorname{Ker}(PQ)(u)$. Donc $\boxed{\operatorname{Ker} P(u) + \operatorname{Ker} Q(u) \subset \operatorname{Ker}(PQ)(u)}$.

Remarque culturelle : *Lemme des noyaux* (hors-programme :
Si $\operatorname{pgcd}(P, Q) = 1$, alors $\operatorname{Ker} P(u) \oplus \operatorname{Ker} Q(u) = \operatorname{Ker}(PQ)(u)$.

c) *Sous-espaces vectoriels stables*

Pour tout polynôme $P \in K[X]$, les endomorphismes u et $P(u)$ commutent.
Donc les sev $\operatorname{Ker} P(u)$ et $\operatorname{Im} P(u)$ sont stables par u.

Exemple : Avec $P = X - \lambda$, $\operatorname{Ker} P(u) = \operatorname{Ker}(u - \lambda \mathrm{Id})$ est le sev propre E_λ, qui est stable par u.

d) *Polynômes d'une matrice diagonale*

Si $A = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}$, alors $P(A) = \begin{pmatrix} P(\lambda_1) & & & \\ & P(\lambda_2) & & \\ & & \ddots & \\ & & & P(\lambda_n) \end{pmatrix}$.

Remarque : Si les λ_j sont distincts, il résulte de l'interpolation de Lagrange que toute matrice diagonale s'écrit sous la forme $P(A)$, c'est-à-dire est un polynôme en A.

e) *Polynômes de matrices semblables*

Prop : Si A et B sont semblables, alors $P(A)$ et $P(B)$ sont semblables, avec la même matrice de passage.

Preuve : Si $A = QBQ^{-1}$, alors $A^n = QB^nQ^{-1}$ pour tout $n \in \mathbb{N}$.

La propriété se comprend aussi en utilisant un endomorphisme : Si $A = \operatorname{Mat}_{\mathcal{B}} u$, alors $P(A) = \operatorname{Mat}_{\mathcal{B}} P(u)$.

IMPORTANT : Supposons A diagonalisable et semblable à $B = \operatorname{Diag}(\lambda_1, ..., \lambda_n)$.
Pour $P \in K[X]$ la matrice $P(A)$ est semblable à $\operatorname{Diag}(P(\lambda_1), ..., P(\lambda_n))$, avec la même matrice de passage.

Remarque : Si $\lambda_1, ..., \lambda_n$ sont distincts, $\operatorname{Diag}(P(\lambda_1), ..., P(\lambda_n))$ décrit l'ensemble des matrices diagonales lorsque P décrit le sev des polynômes de degré $\leq n-1$ (cf polynômes d'interpolation de Lagrange).

2) Polynômes annulateurs

a) *Définition*

Def : Soient $P \in K[X]$ et $u \in \mathcal{L}(E)$.
On dit que P est un polynôme annulateur de u ssi $P(u) = 0$ (endomorphisme nul).

Exemple : $u^2 = u$ ssi le polynôme $X^2 - X$ annule u.

Exemple : $X-\lambda$ annule l'homothétie vectorielle $\lambda\,\mathrm{Id}$.

Remarque : Tout multiple d'un polynôme annulateur est aussi un polynôme annulateur.

Important : Si $P(u)=0$ et $P=QR$, alors $\mathrm{Im}\,Q(u)\subset\mathrm{Ker}\,R(u)$, car $R(u)\circ Q(u)=0$.

Remarque : En dimension finie, tout endomorphisme $u\in\mathcal{L}(E)$ admet un polynôme annulateur non nul. En effet, comme $\dim\mathcal{L}(E)=n^2$, avec $n=\dim E$, la famille $(\mathrm{Id},u,u^2,...,u^{(n^2)})$ est liée. En fait, on a mieux :

b) *Théorème de Cayley-Hamilton* (admis)

Théorème de Cayley-Hamilton : Le polynôme caractéristique est un polynôme annulateur.

Exemple : Pour toute matrice $A=\begin{pmatrix} a & c \\ b & d \end{pmatrix}\in\mathcal{M}_2(K)$, on a $A^2-(a+d)A+(ad-bc)I_2=O_2$.

c) *Cas de l'inverse d'une matrice inversible*

Prop :

Si A admet un polynôme annulateur P vérifiant $P(0)\neq 0$, alors $A\in GL_n(K)$ et A^{-1} est un polynôme en A.

Preuve : On suppose $a_0I+a_1A+...+a_nA^n=0$. On a par hypothèse $a_0\neq 0$.
Donc $AB=BA=I$, avec $B=-\dfrac{1}{a_0}(a_1I+a_2A+...+a_nA^{n-1})$. Donc $A\in GL_n(K)$ et $A^{-1}=B$.

3) Valeurs propres et polynôme annulateur

a) *Lemme fondamental* : Soit $P\in K[X]$. $\boxed{\text{Si } u(x)=\lambda x, \text{ alors } P(u)(x)=P(\lambda)x}$.

En particulier :

- Tout vecteur propre de u est vecteur propre de $P(u)$.
- $\boxed{\text{Si } \lambda \text{ est valeur propre de } u, \text{ alors } P(\lambda) \text{ est valeur propre de } P(u)}$.

Remarque : Il se peut que $P(u)$ admette d'autres valeurs propres que les $P(\lambda)$, où λ est valeur propre de u. Par exemple, si u est la rotation d'angle $\frac{\pi}{2}$ dans $\mathbb{R}^2$, u n' a pas de valeur propre réelle, alors que $u^2=-\mathrm{Id}$ admet -1 comme valeur propre.
En revanche, dans $\mathcal{M}_n(\mathbb{C})$, comme toute matrice A est trigonalisable, les valeurs propres de $P(A)$ sont exactement les $P(\lambda)$, où λ est une valeur propre de A.

b) *Prop* : $\boxed{\text{Soit } P \text{ un polynôme annulateur de } u. \text{ Alors les valeurs propres de } u \text{ sont DES racines de } P}$.
Ainsi, le spectre de u, ensemble des valeurs propres de u, est inclus dans l'ensemble des racines de P.

Preuve : Si $u(x)=\lambda x$ et $x\neq 0$, alors $P(u)(x)=P(\lambda)x$, et comme $P(u)=0$, alors $P(\lambda)=0$.

Remarque : Pour le polynôme caractéristique, les racines sont LES valeurs propres de u.

4) Exemples

Exemple : Soit $A\in\mathcal{M}_n(\mathbb{R})$ tel que $A^3-I=O_n$. Alors $\mathrm{tr}\,A\in\mathbb{Z}$.
On considère A comme matrice de $\mathcal{M}_n(\mathbb{C})$.
La matrice A est annulée par le polynôme $P=X^3-1=X(X-j)(X-j^2)$.
Donc A est tridiagonalisable dans $\mathcal{M}_n(\mathbb{C})$ et ses valeurs propres appartiennent à $\{1,j,\overline{j}\}$.

Ici, p,q,r sont les ordres de multiplicité de 1, j et $\overline{j}=j^2$.

En particulier, le polynôme caractéristique de B est $\chi_B(x)=(x-1)^p(x-j)^q(x-\overline{j})^r$.

Or, A et B étant semblables, on a $\chi_A=\chi_B$.

Comme A est une matrice à coefficients réels, le polynôme caractéristique χ_A est à coefficients réels. Donc les racines complexes de χ_A sont deux à deux conjuguées (avec multiplicité).
On en déduit que les ordres de multiplicité de j et $\overline{j}$ dans χ_B sont égaux, c'est-à-dire $q = r$.
On en conclut que $\operatorname{tr} A = \operatorname{tr} B = p + q(j + \overline{j}) = p - q \in \mathbb{Z}$.

5) Condition nécessaire et suffisante de diagonalisabilité

a) *Théorème* : $\boxed{u \text{ est diagonalisable ssi il est annulé par un polynôme scindé à racines simples}}$.

Plus précisement : - si u est diagonaisable, alors $P(X) = \prod_{\lambda \in \mathrm{Sp}(u)} (X - \lambda)$ annule u.
- si $P(X) = (X - \lambda_1)...(X - \lambda_p)$ scindé à racines simples annule u, alors u est diagonalisable et ses valeurs propres appartiennent à l'ensemble $\{\lambda_1, ..., \lambda_p\}$.

Preuve : - Supposons que u est diagonalisable de valeurs propres $\lambda_1, ..., \lambda_p$.
Alors les E_{λ_i} sont stables par les $(u - \lambda_j \operatorname{Id})$ et $(u - \lambda_i \operatorname{Id})$ est nul sur E_{λ_i}.
Donc $\pi(u) = \prod_{i=1}^{p} (u - \lambda_i \operatorname{Id})$ s'annule sur tous les E_{λ_i}, donc sur $E = \oplus_{i=1}^{p} E_{\lambda_i}$.

- Supposons que $P(X) = (X - \lambda_1)...(X - \lambda_p)$ annule u.
En notant L_i les polynômes d eLagrange associés aux λ_i, on a $1 = \sum_{i=1}^{p} L_i(X)$.
Donc $x = \sum_{i=1}^{p} L_i(u)(x)$. Comme $P(X)$ divise $(X - \lambda_i) L_i(X)$, alors $L_i(u)(x) \in \operatorname{Ker}(u - \lambda_i \operatorname{Id}) = E_{\lambda_i}$.
Ainsi, $E_{\lambda_1} + ... + E_{\lambda_p} = E$, d'où on conclut u diaognalisable (on sait que la somme est directe).

Exemple : Supposons $(u - \lambda \operatorname{Id}) \circ (v - \mu \operatorname{Id}) = 0$, avec $\lambda \neq \mu$.
On a $x = \dfrac{u(x) - \mu x}{\lambda - \mu} + \dfrac{u(x) - \lambda x}{\mu - \lambda} \in E_\lambda \oplus E_\mu$.
Exemple fondamental : $X(X - 1)$ annule $u \in \mathcal{L}(E)$ ssi u est un projecteur. On a alors $E = E_0 \oplus E_1$.

b) *Corollaire fondamental* : Si u est diagonalisable et F sev stable par u, alors $u_{|F}$ est diagonalisable.

Preuve : Tout polynôme (scindé à racines simples) annulant u annule aussi $u_{|F}$.

Remarque : Supposons $u \in \mathcal{L}(E)$ diagonalisable. On a $E_{\lambda_1} \oplus E_{\lambda_2} \oplus ... \oplus E_{\lambda_p} = E$.
On en déduit que les seuls sev stables par u sont les $F_1 \oplus ... \oplus F_p$, où F_λ est un sev de E_{λ_j}.

Projections et symétries

1) Définitions et caractérisations des projections

a) *Prop* : Soit $u \in \mathcal{L}(E)$. Les assertions suivantes sont équivalentes :

(i) u **est une projection** : il existe $E = F \oplus G$tels que p projection sur F parallélèment à G
Autrement dit, on a $\forall x = y + z$, avec $(y, z) \in F \times G$, $p(x) = y$

(ii) $u \circ u = u$

(iii) $\boxed{u \text{ est diagonalisable et } \mathrm{Sp}(u) \subset \{0, 1\} : \text{ Autrement dit, } E_0 \oplus E_1 = E}$.

Dans ce cas, u est la projection sur $E_1 = \operatorname{Ker}(u - \operatorname{Id}) = \operatorname{Im} u$ parallèlement à $E_0 = \operatorname{Ker} u$.

Preuve : Seule l'implication (ii) $\Rightarrow$ (iii) n'est pas immédiate.
Supposons $u^2 = u$. Il s'agit de prouver que $E_0 \oplus E_1 = E$.
Comme on sait que E_0 et E_1 sont en somme directe, il suffit de prouver $E_0 + E_1 = E$.

Or, pour tout $x \in E$, on a $x = (x - u(x)) + u(x)$.
Et $x - u(x) \in E_0$, car $u(x - u(x)) = u(x) - u^2(x) = 0$. Et $u(x) \in E_1$, car $u(u(x)) = u(x)$.

Remarque culturelle : De façon générale, pour tout endomorphisme diagonalisable u, on a

$$\operatorname{Ker} u \oplus \operatorname{Im} u = E \text{ et } \operatorname{Im} u = \oplus_{\lambda \neq 0} E_\lambda$$

Ici, la somme $\oplus_{\lambda \neq 0} E_\lambda$ se limite à E_1 car 1 seule valeur propre non nulle).

b) *Prop* : Soit $A \in \mathcal{M}_n(K)$. Les assertions suivantes sont équivalentes :

(i) $A^2 = A$
(ii) A est semblable à $\left(\begin{array}{c|c} I_r & O \\ \hline O & O \end{array}\right)$, où $r = \operatorname{rg} A$.

2) Définitions et caractérisations des symétries

a) *Prop* : Soit $u \in \mathcal{L}(E)$. Les assertions suivantes sont équivalentes :

(i) u est une symétrie : il existe $E = F \oplus G$tels que u symétrie par rapport à F parallèlement à G
(ii) $u \circ u = \mathrm{Id}$
(iii) u est diagolisable et $\operatorname{Sp}(u) \subset \{-1, 1\}$: Autrement dit, $E_1 \oplus E_{-1} = E$.
Alors u est la symétrie par rapport à $E_1 = \operatorname{Ker}(u - \mathrm{Id}) = \operatorname{Im} u$ parallèlement à $E_1 = \operatorname{Ker}(u + \mathrm{Id})$.

Preuve : p est la projection sur F parallélèment à G ssi $s = 2p - \mathrm{Id}$ est la symétrie sur F par rapport à G. Ainsi, u est une symétrie ssi $\frac{1}{2}(u + \mathrm{Id})$ est une projection. On déduit alors la porpriété de 1).

b) *Corollaire* : Soit $A \in \mathcal{M}_n(K)$. Les assertions suivantes sont équivalentes :

(i) $A^2 = I_n$
(ii) A est semblable à une matrice diagonale $\left(\begin{array}{c|c} I_p & O \\ \hline O & -I_q \end{array}\right)$.

3) Codiagonalisation de projecteurs commutants

Prop : Soient p et q projections vérifiant $p \circ q = q \circ p$. Alors p et q sont codiagonalisables.

Preuve : Notons E_0 et E_1 les sev propres de p.
Alors E_0 et E_1 sont stables par q. Notons q_0 et q_1 les restrictions de q à E_0 et E_1.
Comme $q^2 = q$, alors $q_0^2 = q_0$, donc q_0 est une projection. De même, q_1 est une projection.
Dans une base adaptée à $(\operatorname{Ker} q_0 \oplus \operatorname{Im} q_0) \oplus (\operatorname{Ker} q_1 \oplus \operatorname{Im} q_1)$, on a :

$$\operatorname{Mat}_{\mathcal{B}} p = \begin{pmatrix} O & & & \\ & O & & \\ & & I & \\ & & & I \end{pmatrix} \textit{ et } \operatorname{Mat}_{\mathcal{B}} p = \begin{pmatrix} O & & & \\ & I & & \\ & & O & \\ & & & I \end{pmatrix}.$$

Remarque importante : De façon générale, on a :

Prop : **Toute famille d'endomorphismes diagonalisables commutant sont codiagonalisables.**

Preuve : On raisonne par récurrence sur $n = \dim E$.
Si tous les endomorphismes sont des homothéties, la propriété est immédiate.
Sinon, l'un des endomorphismes u n'est pas une homothétie. Tout sev propre E_λ de u est stable par les autres, et leurs restrictions à E_λ sont aussi diagonalisables et commutent. Par récurrence (car $\dim \mu E_\lambda < n$), il existe donc une base de E_λ composée de vecteurs propres communs à tous les endomorphismes. On conclut en concaténant les bases obtenues pour tous les E_λ.

Calculs des puissances d'une matrice

1) Exemple

Considérons $A = \begin{pmatrix} \lambda & \omega \\ 0 & \mu \end{pmatrix} \in \mathcal{M}_2(K)$. On souhaite calculer A^n pour tout $n \in \mathbb{N}$.

Première méthode : On prouve par récurrence : $A^n = \begin{pmatrix} \lambda^n & r_n \\ 0 & \mu^n \end{pmatrix}$, avec $r_n = \omega \sum_{k=0}^{n-1} \lambda^k \mu^{n-1-k}$.

Seconde méthode (conseillée) :

- *Premier cas* : $\lambda = \mu$. On a $A = \lambda I_2 + N$, avec $N = \begin{pmatrix} 0 & \omega \\ 0 & 0 \end{pmatrix}$ nilpotent d'ordre 2.

Par la formule du binôme (valable car I_n et N commutent), on a $A^n = \lambda^n I_2 + n\lambda^{n-1}N = \begin{pmatrix} \lambda^n & n\omega\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix}$.

- *Second cas* : $\lambda \neq \mu$. La matrice A est diagonalisable et il existe P tel que $A = P \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} P^{-1}$.

Donc $A^n = P \begin{pmatrix} \lambda^n & 0 \\ 0 & \mu^n \end{pmatrix} P^{-1}$, donc A^n est de la forme $\lambda^n R + \mu^n S$, avec R et S matrices de $\mathcal{M}_2(K)$.

On détermine R et S en résolvant $\begin{cases} R + S = I_2 \\ \lambda R + \mu S = A \end{cases}$.

En fait, on sait déjà que A^n est de la forme $\begin{pmatrix} \lambda^n & r_n \\ 0 & \lambda^n \end{pmatrix}$ comme puissance d'une matrice triangulaire.

Il existe donc $(\alpha, \beta) \in K^2$ tel que $\forall n \in \mathbb{N}$, $r_n = \alpha\lambda^n + \beta\mu^n$, et $\begin{cases} \alpha + \beta = 0 \\ \alpha\lambda + \beta\mu = \omega \end{cases}$.

On obtient donc $r_n = \omega \dfrac{\lambda^n - \mu^n}{\lambda - \mu}$.

Troisième méthode : Dans le cas $\lambda \neq \mu$, on peut aussi effectuer une diagonalisation explicite.

On a $E_\lambda = K \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. En résolvant $AX = \mu X$, on obtient $E_\mu = K \begin{pmatrix} \beta \\ 1 \end{pmatrix}$, où $\beta = \dfrac{\omega}{\mu - \lambda}$.

On considère donc $P = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$. On a donc $A = P \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} P^{-1}$.

Donc $A^n = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda^n & 0 \\ 0 & \mu^n \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix}$. On retrouve $r_n = \omega \dfrac{\lambda^n - \mu^n}{\lambda - \mu}$.

2) Calculs des puissances d'une matrice de la forme $\lambda I + N$, où N est nilpotente

Supposons $A = \lambda I + N \in \mathcal{M}_p(K)$, avec N nilpotente. On a donc $N^p = O_p$.

Par le binôme (tronqué), on a $\forall n \in \mathbb{N}$, $(\lambda I + N)^n = \sum_{k=0}^{n-1} \binom{n}{k} \lambda^{n-k} N^k = \lambda^n I + \lambda^{n-1} N + ... + \lambda^{n-p+1} \binom{n}{p-1} N^{p-1}$.

Remarque : Dans la cas général d'une matrice triangulaire, on a bien $A = D + N$, avec D diagonale et N nilpotente, mais D et N ne commutent pas en général, donc on ne peut pas appliquer la formule du binôme.

Exemple : $A = \begin{pmatrix} \lambda & 1 \\ 0 & \mu \end{pmatrix} = D + N$, avec $D = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ et $N = \begin{pmatrix} 0 & \omega \\ 0 & 0 \end{pmatrix}$.

En développant $(D + N)^n$, on obtient 2^n termes.

Mais on a ici $DN = \lambda N$ et $ND = \mu N$.

Comme $N^2 = O$, on obtient finalement $(D + N)^n = D^n + \sum_{k=0}^{n-1} D^k N D^{n-1-k} = D^n + \sum_{k=0}^{n-1} \lambda^k \mu^{n-1-k} N$.

3) Projecteurs spectraux et calcul des puissances d'une matrice diagonalisable

a) *Projecteurs spectraux d'un endomorphisme diagonalisable*

Soit $u \in \mathcal{L}(E)$ diagonalisable de valeurs propres distinctes $\lambda_1, \ldots, \lambda_r$, avec $r \geq 1$.

Le polynôme $M(X) = (X - \lambda_1)...(X - \lambda_r)$ annule u.

On note L_j les polynômes de Lagrange associés aux $\lambda_1, \ldots, \lambda_r$. Autrement dit, $L_j(X) = \prod_{i\neq j} \dfrac{X - a_i}{a_j - a_i}$.

On sait que $1 = \sum_{j=1}^r L_j$, donc $\mathrm{Id} = \sum_{j=1}^r L_j(u)$.

$\boxed{\text{L'endomorphisme } \pi_j = L_j(u) \text{ est le projecteur sur } E_{\lambda_j} \text{ parallèlement à } \oplus_{i\neq j} E_{\lambda_i}}$.

En effet, $x = \sum_{j=1}^r L_j(u)(x)$ et $L_j(u)(x) \in E_{\lambda_j}$, car $(X - \lambda_j)L_i(X)$ annule u.

Comme $u(\pi_j) = \lambda_j u$, on a donc $u = \sum_{j=1}^r \lambda_j L_j(u)$, et plus généralement $u^n = \sum_{j=1}^r \lambda_j^n L_j(u)$.

b) *Calcul des puissances d'une matrice diagonalisable*

Soit A une matrice diagonalisable de valeurs propres distinctes $\lambda_1, \ldots, \lambda_r$, avec $r \geq 1$.
Alors $\forall n \in \mathbb{N}$, $A^n = \sum_{j=1}^r \lambda_j^n R_j$, où R_j est la matrice $L_j(A)$.

Remarque : Les R_j pourraient aussi être obtenus en résolvant le système de Van der Monde :

$$\forall n \in \{0, 1, \ldots, r-1\}, \quad A^n = \sum_{j=1}^r \lambda_j^n R_j$$

Si on considère P telle que $A = PDP^{-1}$, on a $A^n = PD^nP^{-1}$, et $D^n = \sum_{j=1}^r \lambda_j^n Q_j$ matrice diagonale de projections.
On retrouve donc $A^n = \sum_{j=1}^r \lambda_j^n R_j$, avec $R_j = PQ_jP^{-1}$.

4) Calcul des puissances d'une matrice dont on connaît un polynôme annulateur

Considérons $A \in \mathcal{M}_p(K)$ admettant un polynôme annulateur M.

a) *Principe fondamental*

Soit $P \in K[X]$. On considère, la division euclidienne $P = MQ + R$.
D'où $P(A) = M(A)Q(A) + R(A)$. Comme $M(A) = O_n$, on a $P(A) = R(A)$.

Remarque : On a $\deg R_n \leq r - 1$, où $r = \deg M$.
Ainsi, toute matrice A^n, et plus généralement toute matrice $P(A)$ appartient à $\mathrm{Vect}(I, A, A^2, \ldots, A^{r-1})$.

Ainsi, en prenant $P(X) = X^n$, on obtient la propriété suivante :

b) *Prop* : $A^n = R_n(A)$, où R_n est le reste de la division euclidienne de X^n par M.

Remarque : On peut toujours trouver M de degré $r \leq p$, donc a fortiori A^n s'écrit comme combinaison linéaire de $I_p, A, A^2, \ldots, A^{p-1}$, et les coefficients (fonctions de n) sont les coefficients du reste R_n de la division euclidienne de X^n par M.

Exemple : Considérons $A \in \mathcal{M}_p(K)$ admettant un polynôme annulateur $M = (X - \lambda)(X - \mu)$.
Pour $n \in \mathbb{N}$, notons $R_n = a_n + b_n X$ le reste de la division euclidienne de X^n par M.
On a alors $A^n = a_n I_p + b_n A$. Il reste à calculer a_n et b_n.
Si $\lambda \neq \mu$, on obtient (a_n, b_n) en résolvant le système de Van der Monde $\begin{cases} R_n(\lambda) = \lambda^n \\ R_n(\mu) = \mu^n \end{cases}$ $\begin{cases} a_n + b_n\lambda = \lambda^n \\ a_n + b_n\mu = \mu^n \end{cases}$

Si $\lambda = \mu$, on obtient (a_n, b_n) en utilisant le système de Taylor $\begin{cases} R_n(\lambda) = \lambda^n \\ R_n'(\lambda) = n\lambda^{n-1} \end{cases}$