Utilisation d'un polynôme annulateur pour calculer les puissances d'un endomorphisme

Fabrice Monfront
Lycée du Parc

Soient E un $\mathbb{K}$ ev et u un endomorphisme de E.
On suppose connu un polynôme annulateur non nul de E.
Soit $n \in \mathbb{N}$.
On suppose que n est supérieur ou égal au degré de p (sinon le calcul ci-dessous n'apporte rien).
On effectue la division euclidienne de X^n par P :
$\exists!(Q_n, R_n) \in \mathbb{K}[X]$ tq $X^n = P(X)Q_n(X) + R_n(X)$ avec le degré de R_n strictement inférieur à celui de P
$u^n = P(u)Q_n(u) + R_n(u) = R_n(u)$

Se pose alors la question de la détermination de R_n.
On va supposer P scindé.
C'est forcément le cas si $\mathbb{K} = \mathbb{C}$. (Si $\mathbb{K} = \mathbb{R}$ et si P n'est pas scindé sur $\mathbb{R}$, il faut passer par les matrices : on sait multiplier une matrice réelle par un complexe, pas un endomorphisme d'un $\mathbb{R}$-espace vectoriel).
Soit $z_1, \dots, z_p$ les racines de P (deux à deux distinctes).
Pour tout k compris entre 1 et p, on note α_i la multiplicité de z_i.
$\displaystyle\sum_{k=1}^{p} \alpha_i = d$ le degré de P.
$\forall k \in [\![1;p]\!]$ $z_k^n = P(z_k)Q_n(z_k) + R_n(z_k) = R_n(z_k)$
Cela fait p équations pour déterminer les d coefficients de R_n.
Le cas le plus simple est donc celui où $p = d$ ie celui où les racines de P sont toutes simples.
Si on note $c_0, \dots, c_{d-1}$ les coefficients de R_n, on a :

$$\begin{cases} c_0 + c_1 z_1 + \cdots + c_{d-1} z_1^{d-1} = z_1^n \\ \vdots \\ c_0 + c_1 z_d + \cdots + c_{d-1} z_d^{d-1} = z_d^n \end{cases}$$

ou encore matriciellement $\begin{pmatrix} 1 & z_1 & \dots & z_1^{d-1} \\ \vdots & & & \\ 1 & z_d & \dots & z_d^{d-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{d-1} \end{pmatrix} = \begin{pmatrix} z_1^n \\ \vdots \\ z_d^n \end{pmatrix}$

On reconnaît une matrice de Vandermonde. Elle est inversible car les z_k sont deux à deux distincts.
Pour des exemples où d est petit, on obtient les coefficients de R_n en résolvant le système par la méthode du pivot.

D'un point de vue plus théorique, on a $\begin{pmatrix} c_0 \\ \vdots \\ c_{d-1} \end{pmatrix} = \begin{pmatrix} 1 & z_1 & \dots & z_1^{d-1} \\ \vdots & & & \\ 1 & z_d & \dots & z_d^{d-1} \end{pmatrix}^{-1} \begin{pmatrix} z_1^n \\ \vdots \\ z_d^n \end{pmatrix}$.

La base canonique n'est pas la seule base de $\mathbb{K}_{d-1}[X]$.

Pour tout $k \in [\![1;d]\!]$, soit $L_k = \dfrac{\displaystyle\prod_{\substack{l=1\\l\neq k}}^{d}(X-z_l)}{\displaystyle\prod_{\substack{l=1\\l\neq k}}^{d}(z_k-z_l)}$.

On a vu dans le cours sur l'interpolation de Lagrange que $(L_1,\ldots,L_d)$ est une base de $\mathbb{K}_{d-1}[X]$ avec :

$\forall Q \in \mathbb{K}_{d-1}[X]\ Q = \displaystyle\sum_{k=1}^{d} Q(z_k)L_k$

On a donc ici :

$R_n(X) = \displaystyle\sum_{k=1}^{d} R_n(z_k)L_k(X) = \sum_{k=1}^{d} z_k^n L_k(X)$

Revenons au cas général.

z_k est racine de multiplicité au moins α_k du polynôme Q_nP donc :

$\forall l \in [\![0;\alpha_k-1]\!]\ (Q_nP)^{(l)}(z_k) = 0$

et on a :

$\forall l \in [\![0;\alpha_k-1]\!]\ n(n-1)\ldots(n-l+1)z_k^{n-l} = R_n^{(l)}(z_k)$

Si on note $c_0,\ldots,c_{d-1}$ les coefficients de R_n, on a :

$$\begin{cases} c_0 + c_1z_1 + \cdots + c_{d-1}z_1^{d-1} = z_1^n \\ \vdots \\ c_{\alpha_1}\alpha_1! + \cdots + c_{d-1}(d-1)\ldots(d-1-\alpha_1+1)z_1d-1-\alpha_1 = n\ldots(n-\alpha_1+1)z_1^{n-\alpha_1} \\ \vdots \\ c_0 + c_1z_p + \cdots + c_{d-1}z_p^{d-1} = z_p^n \\ \vdots \\ c_{\alpha_1}\alpha_1! + \cdots + c_{d-1}(d-1)\ldots(d-1-\alpha_p+1)z_pd-1-\alpha_p = n\ldots(n-\alpha_p+1)z_p^{n-\alpha_p} \end{cases}$$

ou encore matriciellement :

$$\begin{pmatrix} 1 & z_1 & \ldots & \ldots & \ldots & z_1^{d-1} \\ \vdots & & & & & \\ 0 & \ldots & 0 & \alpha_1! & \ldots & (d-1)\ldots(d-1-\alpha_1+1)z_1^{d-1-\alpha_1} \\ \vdots & & & & & \\ 1 & z_p & \ldots & \ldots & \ldots & z_p^{d-1} \\ \vdots & & & & & \\ 0 & \ldots & 0 & \alpha_p! & \ldots & (d-1)\ldots(d-1-\alpha_p+1)z_p^{d-1-\alpha_p} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ c_{d-1} \end{pmatrix} = \begin{pmatrix} z_1^n \\ \vdots \\ n\ldots(n-\alpha_1+1)z_1^{n-\alpha_1+1} \\ \vdots \\ z_p^n \\ \vdots \\ n\ldots(n-\alpha_p+1)z_p^{n-\alpha_p} \end{pmatrix}$$

La matrice carrée, notée A, est inversible :

Soit $Y = \begin{pmatrix} c_0 \\ \vdots \\ c_{d-1} \end{pmatrix} \in \mathcal{M}_{d-1,1}(\mathbb{K})$ tq $AY = 0$.

Soit $Q = \displaystyle\sum_{l=0}^{d-1} c_lX^l$.

Pour tout $k \in [\![1;p]\!]$, z_k est racine de multiplicité supérieure ou égale à α_k de Q.

On a donc au moins $\sum_{k=1}^{p} \alpha_k = d$ racines de Q de degré inférieur ou égal à $d-1$. On en déduit que Q est le polynôme nul. Ses coefficients sont donc tous nuls et X est nulle.
Pour des exemples où d est petit, on obtient les coefficients de R_n en résolvant le système par la méthode du pivot.
D'un point de vue plus théorique, on a :

$$\begin{pmatrix} c_0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ c_{d-1} \end{pmatrix} = \begin{pmatrix} 1 & z_1 & \dots & \dots & \dots & z_1^{d-1} \\ \vdots & & & & & \\ 0 & \dots & 0 & \alpha_1! & \dots & (d-1)\dots(d-1-\alpha_1+1)z_1^{d-1-\alpha_1} \\ \vdots & & & & & \\ 1 & z_p & \dots & \dots & \dots & z_p^{d-1} \\ \vdots & & & & & \\ 0 & \dots & 0 & \alpha_p! & \dots & (d-1)\dots(d-1-\alpha_p+1)z_p^{d-1-\alpha_p} \end{pmatrix}^{-1} \begin{pmatrix} z_1^n \\ \vdots \\ n\dots(n-\alpha_1+1)z_1^{n-\alpha_1+1} \\ \vdots \\ z_p^n \\ \vdots \\ n\dots(n-\alpha_p+1)z_p^{n-\alpha_p} \end{pmatrix}$$