Décomposition de Dunford par la méthode de Newton

Les lignes qui suivent visent à donner une preuve effective de la décomposition de Dunford. Cette preuve utilise la formule de Taylor dans un anneau euclidien (cela est suffisant).

Lemma 1 (Formule de Taylor) *Soient R un anneau euclidien, $P \in R[Y]$ et $c \in R$. On a :*

$$P = \sum_{k \geq 0} \alpha_k(P, c)(Y - c)^k,$$

où $\alpha_k(P, c) \in R$ vérifie $P^{(k)}(c) = \alpha_k(P, c)k!$.

Proof: Par translation, il suffit de faire la preuve dans le cas où $c = 0$. Nous pouvons écrire :

$$P = \sum_{k \geq 0} a_k Y^k.$$

En calculant les dérivées successives, nous trouvons : $P^{(k)}(0) = a_k k!$. Cela achève la preuve. $\square$

Le lemme qui suit est le résultat crucial.

Lemma 2 *Soient R un anneau euclidien, $P \in R[Y]$ et $a \in R$. Supposons qu'il existe $x_0 \in R$ tel que*

$$P(x_0) = 0 \mod a$$

et que $P'(x_0)$ soit premier avec a.
Alors, pour tout $n \in \mathbb{N}$, il existe $x_n \in R$ vérifiant :

$$P(x_n) = 0 \mod a^{2^n}$$

et

$$x_n = x_0 \mod a^{2^n}.$$

Proof: Nous prouvons ce résultat par récurrence sur n. Pour $n = 0$, il n'y a rien à faire. Soit $n \geq 0$; supposons que :

$$P(x_n) = 0 \mod a^{2^n},$$

$$x_n = x_0 \mod a^{2^n}$$

et cherchons à construire x_{n+1}. Écrivons $x_{n+1} = x_n + ka^{2^n}$ et trouvons $k \in R$ de sorte que :

$$P(x_{n+1}) = 0 \mod a^{2^{n+1}}.$$

La formule de Taylor nous donne :

$$P(x_n + ka^{2^n}) = P(x_n) + P'(x_n)ka^{2^n} \mod a^{2^{n+1}}.$$

Nous voulons donc trouver k tel que :

$$P'(x_n)ka^{2^n} = -P(x_n) \mod a^{2^{n+1}}.$$

Nous pouvons écrire par hypothèse de récurrence : $P(x_n) = a^{2^n}r$ avec $r \in R$. Ainsi, nous sommes réduits à trouver k tel que :

$$P'(x_n)k = -r \mod a,$$

ce qui est loisible puisque $P'(x_n) = P'(x_0) \mod a$ et que $P'(x_0)$ est inversible modulo a. En d'autres termes, nous avons trouvé x_{n+1} :

$$x_{n+1} = x_n - P(x_n)P'(x_n)^{-1},$$

où nous convenons que $P'(x_n)^{-1}$ désigne un représentant dans R de l'inverse de $P'(x_n)$ modulo a. □

Nous sommes désormais armés pour prouver la décomposition de Dunford en deux coups de cuillère à pot !
Soit A une matrice à coefficients dans $\mathbb{C}$. Soit Q un polynôme annulateur de A. Posons $P = Q/PGCD(Q, Q')$ de sorte que P est scindé à racines simples (ou encore $PGCD(P, P') = 1$).
Appliquons le lemme avec $R = \mathbb{C}[X]$, $a = P(X)$, $x_0 = X$ et $P = P(Y) \in R[Y]$. Il est clair qu'il existe N tel que $P^N(A) = 0$, d'où l'on déduit : $P(x_N(A)) = 0$, ce qui prouve que $x_N(A)$ est diagonalisable. Par ailleurs, on a aussi :

$$x_N(A) = A + PK(A),$$

pour un certain polynôme K. Il est par ailleurs évident que $(PK)^N(A) = 0$ et que $x_N(A)$ et $PK(A)$ commutent !