Une méthode effective pour la décomposition de Dunford

Daniel Ferrand
Février 2003

Introduction

La démonstration usuelle, sur $\mathbf{C}$, de la décomposition de Dunford,

$$f \;=\; f_s + f_n,$$

utilise les valeurs propres de f ; en fait, on peut calculer f_s et f_n sans les connaître, grâce une adaptation de la vénérable méthode de Newton pour l'approximation des racines ; cela conduit à une démonstration à la fois élémentaire et effective (i.e. transformable, si on y tient, en un algorithme).

Énoncé et commentaires

Théorème *Soient K un corps de caractéristique nulle et $A = K[x] = K[X]/(p)$ une K-algèbre monogène de dimension finie. Alors, il existe $u, v \in K[x]$ tels que*
i) $x = u + v$;
ii) le polynôme minimal de u est à racines simples (dans une clôture algébrique de K) ;
iii) v est nilpotent.

Remarques

1) Comme tout élément de $K[x]$, u et v s'expriment comme des polynômes en x, polynômes que la démonstration produira effectivement.

2) Cet énoncé entraîne la décomposition de Dunford. En effet, soit f un endomorphisme d'un $K-$espace vectoriel de dimension finie V ; si on désigne par p le polynôme caractéristique de f, le théorème de Hamilton-Cayley donne un morphisme de $K-$algèbres

$$K[X]/(p) \;\longrightarrow\; \mathrm{End}_K(V)$$

pour lequel l'image de la classe x de X est f ; notons f_s et f_n les images respectivement des éléments u et v du théorème ; ces deux endomorphismes commutent puisque u et v commutent ; f_n est nilpotent puisque v l'est, et f_s est diagonalisable puisqu'il est annulé par un polynôme à racines simples (si K n'est pas algébriquement clos, « diagonalisable » doit être entendu au sens faible suivant : il existe un changement de base (i.e une matrice inversible) *éventuellement à coefficients dans un surcorps de K*, qui transforme f en une application diagonale).

3) L'hypothèse que K est de caractéristique nulle peut être remplacée par la suivante : les racines de p dans une clôture algébrique de K sont « séparables sur K », ou encore par l'hypothèse équivalente : les facteurs irréductibles de p dans $K[X]$ ont leur dérivée non nulle (ce qui est bien le cas s'ils sont de degré 1, c'est-à-dire si p est scindé, ou bien si la caractéristique de K est nulle !).

Il faut bien ajouter une hypothèse en vertu du contre-exemple usuel suivant : soit q un nombre premier ; considérons le corps $K = \mathbb{F}_q(T)$, et la K-algèbre $A = K[X]/(X^q - T)$; comme c'est un corps (critère d'Eisenstein), le seul élément nilpotent de A est 0, mais le

polynôme minimal de x à savoir $X^q - T$, a une seule racine, de multiplicité q, dans une clôture algébrique de K, puisque, déjà dans $A[X]$, on a $X^q - T = (X - x)^q$.

4) Dans le langage algébrique moderne, signalons que cet énoncé est un cas très particulier de la *propriété de relèvement des algèbres étales*. En effet, avec les notations du théorème, soit A/I le plus grand quotient réduit de A (l'idéal I est donc formé des éléments nilpotents de A) ; A/I est un produit fini de corps extensions finies de K, et si K est de caractéristique nulle, ou sous l'hypothèse évoquée en 3., ces extensions finies sont séparables au sens usuel ; bref, A/I est alors une $K-$algèbre « étale ». La « propriété de relèvement » dit que le morphisme $\pi : A \longrightarrow A/I$ admet une section, c'est-à-dire qu'il existe un morphisme de $K-$algèbres $j : A/I \longrightarrow A$ tel que $\pi \circ j = \mathrm{Id}$. Si on pose $B = \mathrm{Im}(j)$, on a donc $A = B \oplus I$, où B est une $K-$algèbre « étale », et où I est un idéal nilpotent. Dans le cas envisagé, on a $B = K[u]$ et $I = Av$. Cette interprétation déborde de l'esprit de cette note, et elle est inutile pour la suite. Mais elle rappelle qu'une idée profonde, ici la méthode d'approximation due à Isaac Newton, peut rester longtemps féconde, surtout lorsqu'elle est utilisée et réinterprétée par des mathématiciens comme K. Hensel (1861-1941) ou A. Grothendieck !

Préliminaires sur les polynômes

Soit $p(X)$ un polynôme unitaire à coefficients dans un corps K, et

$$p = p_1^{m(1)}.p_2^{m(2)}\dots.p_s^{m(s)}$$

sa décomposition en facteurs irréductibles unitaires. Posons

$$q = p_1.p_2\dots p_s.$$

C'est un diviseur de p, et p divise q^r dès que l'entier r est supérieur à tous les exposants $m(i)$, par exemple si $r = \deg(p)$. En termes d'anneaux, on a un morphisme surjectif

$$\pi : K[X]/(p) \longrightarrow K[X]/(q)$$

dont le noyau est un idéal nilpotent (c'est l'idéal engendré par q, et p divise q^r). Le théorème chinois montre que $K[X]/(q)$ est un produit de corps.
En caractéristique nulle, on peut définir q, effectivement, par l'égalité

$$p \;=\; \mathrm{pgcd}(p, p').q.$$

(En effet, si on dérive une égalité de la forme $p = p_i^{m(i)}.w$, où p_i ne divise pas w, on trouve $p' = (m(i)p_i'.w + p_i.w')p_i^{m(i)-1}$; en caractéristique nulle, le polynôme $m(i)p_i'$ est non nul et donc premier à p_i puisque $\deg(m(i)p_i') < \deg(p_i)$; ainsi la multiplicité de p_i dans p' est exactement $m(i) - 1$).
Par ailleurs, toujours en caractéristique nulle, q' et p sont étrangers puisque chaque diviseur premier p_i de p divise q, et donc ne peut diviser q'.

Démonstration

Pour la démonstration on se place dans la $K-$algèbre A (du point de vue algorithmique, les égalités sont donc à prendre « modulo p ») ; en particulier, on a donc $q(x)^r = 0$, disons avec $r = \deg(p)$; par ailleurs, $q'(x)$ est un élément inversible de A en vertu d'une relation de Bézout entre q' et p.

On pose, suivant ce cher Isaac,

$$x_0 = x, \qquad\qquad x_{n+1} = x_n \ - \ \frac{q(x_n)}{q'(x_n)}.$$

On va montrer, par récurrence, d'une part que cela a bien un sens, c'est-à-dire que pour tout n, $q'(x_n)$ est inversible dans A, et d'autre part, que

$$(*) \qquad\qquad q(x_n) \in q(x)^{2^n} A,$$

ce qui impliquera que les $q(x_n)$ sont nilpotents dans A.

Ces deux propriétés sont vraies au cran 0, c'est-à-dire pour x ; supposons qu'elles soient vérifiées au cran n. On a $q'(x_{n+1}) - q'(x_n) \in (x_{n+1} - x_n)A$, simplement parce que q' est un polynôme, et on a l'inclusion $(x_{n+1} - x_n)A \subset q(x_n)A$, par définition de x_{n+1} ; or, $q(x_n)$ est nilpotent dans A d'après l'hypothèse de récurrence, donc $q'(x_{n+1})$ est inversible (puisque dans un anneau commutatif la somme d'un inversible et d'un nilpotent est un élément inversible). Par ailleurs, pour tout polynôme $q(X)$, il existe un polynôme $\tilde{q}(X, Y)$ tel que

$$q(X + Y) = q(X) + Y q'(X) + Y^2 \tilde{q}(X, Y),$$

comme on le constate sur un monôme :

$$(X + Y)^m = X^m + Y m X^{m-1} + Y^2(\ldots).$$

On en tire l'inclusion $q(x_{n+1}) = q(x_n + y) \in q(x_n)^2 A$, puisque le terme y a été exactement choisi pour que $q(x_n) + y q'(x_n) = 0$; elle entraîne la deuxième propriété (*) au cran $n + 1$.

Comme $q(x_n) \in q(x)^{2^n} A$, et que $q(x)^r = 0$, on voit que la suite (x_n) est stationnaire à partir de l'indice n tel que $2^n \geq r$, et que, notant u cet élément final, on a $q(u) = 0$; enfin, comme chaque $q(x_n)$ est un multiple de $q(x)$, il en est de même, par addition, de $x - u = x_0 - x_n = (x_0 - x_1) + (x_1 - x_2) + \cdots + (x_{n-1} - x_n)$, qui est donc nilpotent dans A.

Il reste à constater que le polynôme minimal de u est à racines simples. Or, il divise q puisque $q(u) = 0$. En fait, ce polynôme minimal est même *égal* à $q(X)$: en effet, comme $q(u) = 0$, on a un morphisme de $K-$algèbres

$$j : K[X]/(q) \longrightarrow K[X]/(p) = A,$$
$$\text{classe } X \quad \longmapsto \quad u$$

L'inclusion $x - u \in q(x)A$ se traduit par $\pi(u) = \bar{x} \in K[X]/(q)$, où

$$\pi : K[X]/(p) \longrightarrow K[X]/(q)$$

est le morphisme de passage au quotient, déja évoqué ; on a donc $\pi \circ j = \mathrm{Id}$. Cela implique, entre autre, que j est injectif, donc que q est bien le polynôme minimal de u.