Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

D. Ferrand

Une méthode effective pour la décomposition de Dunford

(Version révisée)

Daniel Ferrand
Février 2003

Introduction

À un candidat qui avait donné la démonstration usuelle, sur $\mathbb{C}$, de la décomposition de Dunford,

$$f = f_s + f_n,$$

un membre du jury a posé, sans succès, la question suivante :

Peut-on calculer f_s et f_n sans connaître les valeurs propres de f ?

Il s'avère que oui ! En fait, une adaptation de la vénérable méthode de Newton pour l'approximation des racines 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 et $A = K[x] = K[X]/(p)$ une K-algèbre monogène de dimension finie. On suppose que p est scindé, *ou* que K est de caractéristique nulle. Alors, il existe $u, v \in K[x]$ tels que

1. $x = u + v$;
2. Le polynôme minimal de u est à racines simples (dans une clôture algébrique de K) ;
3. 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. Montrons comment cet énoncé entraîne la décomposition de Dunford : soit donc 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 ; alors f_n est nilpotent, comme v, et f_s est diagonalisable puisqu'il est annulé par un polynôme à racines simples (si p n'est pas scindé, le terme « 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_s en une application diagonale). Enfin, ces deux endomorphismes commutent puisque u et v commutent.
3. L'hypothèse (p scindé ou $\mathrm{car}(K) = 0$) 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 une hypothèse en vertu du contre-exemple usuel suivant : $K = \mathbb{F}_p(T)$, $A = K[X]/(X^p - T)$ et $f : A \to A, a \mapsto ax$; cet endomorphisme f est bijectif (A est un corps), mais il n'est pas diagonalisable parce que son polynôme caractéristique, $X^p - T$, a une seule racine (de multiplicité p) dans une clôture algébrique de K, et que f n'est pas une homothétie ; d'autre part, un endomorphisme non nul de A de la forme $F(f)$, où F est un polynôme, est simplement l'application $a \mapsto F(x)a$; comme A est un corps, un tel endomorphisme ne peut être nilpotent.

4. Pour ceux qui connaissent un peu le langage algébrique moderne, signalons que cet énoncé est un cas très particulier de la *propriété de relèvement des algèbres étales*. En effet, 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 sous l'hypothèse du théorème, ou celle, plus générale, 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. Cette interprétation est inutile pour la suite et n'a, évidement, pas à être évoquée à l'oral. Mais il fallait rappeler qu'une idée profonde, ici la méthode d'approximation due à Isaac Newton, peut être féconde pendant plusieurs siècles !

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 il existe un entier r tel que p divise q^r. 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.

Notons que, sous les hypothèses du théorème, les polynômes q' et p sont étrangers. En effet, les facteurs irréductibles de p ont leur dérivée non nulle : p_i ne divise donc pas p_i', ni, par suite, q'.

En caractéristique nulle, la démonstration proposée est *effective* car on peut calculer q sans connaître les p_i (qui ne sont pas, en général, calculables). En effet, un pgcd est - facilement - calculable, et on a

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

(Car, en dérivant l'égalité $p = p_i^{m(i)}.u$, on trouve $p' = (m(i)p_i'.u + p_i.u')p_i^{m(i)-1}$; en caractéristique nulle, le polynôme $m(i)p_i'$ est (non nul donc) premier à p_i ; la multiplicité de

p_i dans p' est donc exactement $m(i)-1$).

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 $q(x)^r = 0$; 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 $q(x_n) \in q(x)^{2^n}A$, 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 (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

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

comme on le constate sur un monôme :

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

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 $q(x_n) + yq'(x_n) = 0$; 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 $x - u = x_0 - x_n$, qui est donc nilpotent dans A.

Il reste à vérifier que le polynôme minimal de u est *égal* à $q(X)$. Or, comme $q(u) = 0$, on a un morphisme de $K-$algèbres

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

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