Université de Bordeaux
Mathématiques

Préparation à l'agrégation
2015–2016

Décomposition de Dunford-Jordan

Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Il vous est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury demande que la discussion soit accompagnée d'exemples traités sur ordinateur. Il est souhaitable que vous organisiez votre présentation comme si le jury n'avait pas connaissance du texte. Le jury aura néanmoins le texte sous les yeux pendant votre exposé.

1. Lemme de Hensel

Le texte est motivé par le résultat suivant, appelé « Lemme de Hensel » :

Lemme 1.1 (Hensel)**.** *Soit P un polynôme de $\mathbb{Z}[X]$ et p un nombre premier. Soit n un entier supérieur ou égal à 1. On suppose que l'on dispose d'un entier x tel que*

$$P(x) \equiv 0 \pmod{p^n} \quad \textit{et} \quad P'(x) \not\equiv 0 \pmod{p}.$$

Alors il existe un entier y dans $\mathbb{Z}$ tel que

$$y \equiv x \pmod{p^n} \quad \textit{et} \quad P(y) \equiv 0 \pmod{p^{2n}}.$$

De plus, cet entier est unique modulo p^{2n}. On peut le prendre égal à $x - P(x)s$, où s est tel que $sP'(x) \equiv 1 \pmod{p^n}$.

Remarque 1.2. On reconnaît ici une version algébrique de la méthode de Newton, qui s'écrirait $y = x - P(x)P'(x)^{-1}$.

Preuve. On cherche l'entier y sous la forme $x + tp^n$; ce sera un antécédent "bien choisi" de x par la surjection canonique $\mathbb{Z}/p^{2n}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$. On écrit la formule de Taylor à l'ordre 1

$$P(x + tp^n) = P(x) + tp^n P'(x) + t^2 p^{2n} R(x),$$

où $R \in \mathbb{Z}[X]$. Ainsi,

$$P(x + tp^n) \equiv P(x) + tp^n P'(x) \pmod{p^{2n}}.$$

Posons $P(x) = p^n P_0$, où $P_0 \in \mathbb{Z}$. Alors $P(x + tp^n) \equiv 0 \pmod{p^{2n}}$ si et seulement si

$$t \equiv -P'(x)^{-1} P_0 \pmod{p^n},$$

où $P'(x)^{-1}$ est l'inverse de $P'(x)$ modulo p^n, qui existe d'après les hypothèses. □

2. Décomposition de Dunford en caractéristique 0

Nous allons adapter ce résultat, en remplaçant $\mathbb{Z}$ par l'anneau euclidien $K[X]$, où K désigne un corps (commutatif). On suppose dans un premier temps que K est de caractéristique 0.

Théorème 2.1. *Soit K un corps de caractéristique 0. Soit A une matrice carrée à coefficients dans K. Alors il existe un couple unique de matrices D et N, telles que $A = D + N$ et*

(1) *D et N commutent,*
(2) *D est diagonalisable dans une extension finie de K,*
(3) *N est nilpotente.*

De plus, il existe f_D et f_N dans $K[X]$ tels que $D = f_D(A)$ et $N = f_N(A)$.

Démontrer l'unicité n'est pas difficile : si $A = D' + N'$ est une décomposition vérifiant les propriétés du théorème 2.1, alors D' et N' commutent avec A, donc avec D et N ; il suit que $N - N'$ est nilpotente, et $D' - D$ est diagonalisable. On en déduit que $D' - D = N - N' = 0$.

Nous allons donner une preuve constructive de l'existence. On utilisera pour cela le lemme suivant.

Lemme 2.2. *Soit K un corps de caractéristique 0, et soit $A \in M_n(K)$. Alors il existe $P \in K[X]$ sans facteur carré tel que $P(A)^n = 0$.*

Preuve. Soit χ_A le polynôme caractéristique de A. Alors $P = \chi_A/(\chi_A, \chi_A')$ convient. □

Preuve du théorème 2.1 (existence). On utilise une méthode de relèvement de Hensel, dans les quotients $K[X]/(P)^k$. On a bien sûr $P(X) \equiv 0 \pmod{P}$; on pose $x_0 = X$. On va relever cette racine modulo P en une suite de racines x_k modulo P^{2^k}. Comme P est sans facteur carrés, il existe deux polynômes U et V dans $K[X]$ tels que

$$UP' + VP = 1.$$

Lemme 2.3. *Soit $k \geqslant 0$ un entier. On suppose qu'il existe $x_k \in K[X]$ tel que $P(x_k) \equiv 0 \pmod{P^{2^k}}$. Alors il existe $x_{k+1} \in K[X]$ tel que $P(x_{k+1}) \equiv 0 \pmod{P^{2^{k+1}}}$.*

Preuve. On cherche x_{k+1} sous la forme $x_{k+1} = x_k + P(x_k)R$, où $R \in K[X]$. La formule de Taylor donne

$$P(x_k + P(x_k)R) \equiv P(x_k)(1 + P'(x_k)R) \pmod{P(x_k)^2}.$$

Or, $P(x_k) \equiv 0 \pmod{P^{2^k}}$, donc

$$P(x_{k+1}) \equiv P(x_k)(1 + P'(x_k)R) \pmod{P^{2^{k+1}}}.$$

On pose maintenant $R := -U(x_k) \in K[X]$. Alors $1 + P'(x_k)R = P(x_k)V(x_k)$ est divisible par P^{2^k}. Donc $P(x_{k+1}) \equiv 0 \pmod{P^{2^{k+1}}}$. □

Terminons la preuve du théorème : on pose $x_0 = X$ et on calcule de proche en proche $x_1, \dots, x_k \in K[X]$, en s'arrêtant quand $2^k \geqslant n$, la taille de A. On pose alors $f_D := x_k$, $D = f_D(A)$, et $N = A - D$. Comme $P^n \mid P(x_k)$, on a $P(D) = 0$; D étant annulée par le polynôme sans facteur carré P, elle est diagonalisable dans le corps de décomposition de P. Quant à N, on utilise que $x_k \equiv x_0 \pmod{P}$. Ainsi,

$$f_D - X \equiv 0 \pmod{P},$$

et donc $P^n \mid (f_D - X)^n$. On en déduit que $N^n = 0$. □

3. Caractéristique $p > 0$; polynômes séparables et corps parfaits

Que se passe-t-il si l'on ne suppose plus K de caractéristique nulle ? Le point crucial de la preuve tient dans le Lemme 2.2 : il existe P premier avec sa dérivée tel que $P^n(A) = 0$.

3.1. **Contre-exemple.** En caractéristique $p > 0$, ce lemme 2.2 est faux : voir sur $K = \mathbb{F}_p(T)$ le cas où $\chi_A = X^p - T$. Mais dans ce cas, la décomposition de Dunford elle-même n'existe pas. En effet, la K-algèbre $K[A] \simeq K[X]/(\chi_A)$ est un corps, puisque χ_A est irréductible sur K (polynôme d'Eisenstein en T), et donc elle ne contient pas d'élément nilpotent, hors 0 ! Ainsi, si la décomposition existe, elle s'écrit $A = D + 0$, et donc A est diagonalisable dans une clôture algébrique K^c de K. Mais c'est absurde puisque le polynôme minimal χ_A de A n'est pas sans facteur carré sur K^c.

3.2. **Corps parfaits.** Pour corriger le théorème 2.1, nous avons besoin d'introduire la notion de corps parfait :

Définition 3.1. Soit K un corps.

(1) Un polynôme *irréductible* P est dit séparable si les racines de P dans un corps de décomposition sont simples. Sinon, il est dit inséparable.
(2) Un polynôme est dit séparable si chacun de ses facteurs irréductibles l'est.
(3) On dit que K est parfait si tout polynôme non nul de $K[X]$ est séparable.

Il est facile de décider si un polynôme irréductible est séparable :

Proposition 3.2. *$P \in K[X]$ irréductible est séparable si et seulement si* $\operatorname{pgcd}(P, P') = 1$.

Corollaire 3.3. *Si K est un corps de caractéristique 0 ou un corps fini, alors K est parfait.*

Preuve. Soit P un polynôme irréductible de $K[X]$ (donc non constant) ; montrons qu'il est séparable. Le cas où $P' \neq 0$ (qui inclut le cas de la caractéritique 0) est immédiat : on a $\operatorname{pgcd}(P, P') = 1$.

Supposons maintenant que K est fini, de caractéristique $p > 0$ et $P' = 0$. Alors il existe $Q \in K[X]$ tel que $P = Q(X^p)$. Mais $Q(X^p)$ est une puissance p-ème, et n'est donc pas irréductible ; ce cas est donc impossible. □

En fait, on peut montrer le résultat suivant.

Lemme 3.4. *Un corps K de caractéristique $p > 0$ est parfait si et seulement si $x \mapsto x^p$ est surjective.*

Preuve. Si K est parfait de caractéristique p, alors $X^p - y \in K[X]$ n'est pas irréductible, puisqu'il a une racine multiple α dans une extension L de K. Tout facteur irréductible sur $K[X]$, décomposé dans $L[X]$ s'écrit (à multiplication près par un élément de K^*) sous la forme $(X-\alpha)^k$ où $0 < k < p$. Donc α^k et α^p appartiennent à K. En utilisant une relation de Bézout entre p et k, on en déduit que $\alpha \in K$, et donc que $y \in K^p$.

Réciproquement, si l'on suppose que $x \mapsto x^p$ est surjective, on en déduit comme dans le corollaire 3.3 que K est parfait. □

3.3. **Dunford-Jordan en caractéristique p.** On suppose K parfait de caractéristique $p > 0$. Soit P un polynôme sur $K[X]$ de degré n, et soit

$$P = \prod_{i=1}^{r} f_i^{e_i}$$

sa décomposition en un produit de facteurs irréductibles ; alors $\prod_{i=1}^{r} f_i$ est séparable, ce qui permet de démontrer le Lemme 2.2 dans ce nouveau cadre, et donc le théorème de Dunford-Jordan. D'un point de vue constructif, on vérifie que

$$Q = \frac{P}{(P, P')} = \prod_{p \nmid e_i} f_i \quad \text{et} \quad R = \frac{P}{(P, Q^n)} = \prod_{p \mid e_i} f_i^{e_i}.$$

Le polynôme R est la puissance $p^{\text{ème}}$ d'un polynôme S de $K[X]$. On peut ensuite appliquer le même algorithme à S ; ce qui permet d'obtenir $\prod_{i=1}^{r} f_i$.