L'algèbre de la décomposition de Chevalley-Dunford

Jean-François Burnol, 28 (et 29 et 30) avril 2017

Table des matières

1 Présentation

Soit $\mathbf{K}$ un corps et A un endomorphisme d'un $\mathbf{K}$-espace vectoriel W de dimension finie. On note P le polynôme minimal de A. Ainsi l'algèbre des polynômes d'endomorphismes $T(A)$, $T \in \mathbf{K}[X]$ est isomorphe à $\mathcal{A} := \mathbf{K}[X]/(P)$. Nous nous intéressons à la question suivante :

> *Caractériser (de manière effective) les $T \in \mathbf{K}[X]$ tels que $T(A) \in \mathrm{End}_{\mathbf{K}}(W)$ est semi-simple, i.e. diagonalisable après extension des scalaires à une clôture algébrique $\overline{\mathbf{K}}$.*

Je vais présenter une analyse qui donne entre autres choses la réponse à cette question, en toute caractéristique. Puis, je donnerai une démonstration directe plus simple

en caractéristique nulle d'une partie des résultats. Il est possible de passer directement à cette dernière partie, peut-être tout de même après avoir lu la section de rappels qui suit.

La partie centrale du texte porte sur une discussion approfondie de la décomposition de Chevalley-Dunford de A en $A = D + N$ avec $DN = ND$, N nilpotent, et D diagonalisable sur $\overline{\mathbf{K}}$. Comme l'on verra dans le texte, en caractéristique nulle la décomposition est définie sur $\mathbf{K}$ mais pas nécessairement en caractéristique positive. Elle l'est si et seulement si le $\overline{\mathbf{K}}$-radical Q de P est défini sur $\mathbf{K}$.

Ce qui est toujours le cas si $\mathbf{K}$ est un corps parfait, en particulier si $\mathbf{K}$ est fini (cf. page 19). 29/04/17

Après extension éventuelle de $\mathbf{K}$ (si la caractéristique est positive) de sorte que Q est défini sur $\mathbf{K}$, nous donnons un système linéaire défini sur $\mathbf{K}$ caractérisant D comme son unique solution. Et ceci donne donc un algorithme effectif pour l'obtention explicite de D comme polynôme en A, en toute caractéristique.

Ce texte est indépendant de mes notes précédentes, mais en est une évolution, résultant en particulier de la volonté de développer complètement la théorie en toute caractéristique.

— http://jf.burnol.free.fr/agreg170406Dunford_NewAlgo.pdf
— http://jf.burnol.free.fr/agreg170408NewDun.pdf
— http://jf.burnol.free.fr/agreg170410NewtonSchroederDunford.pdf
— http://jf.burnol.free.fr/agreg170413DunfordLineaire.pdf
— http://jf.burnol.free.fr/agreg170414DunfordExplicite.pdf

Je remercie Lorenzo Ramero pour quelques échanges sur ce sujet.

2 Rappels sur les endomorphismes semi-simples

Je commence par quelques rappels :

— On dit qu'une matrice carrée M à coefficients dans $\mathbf{K}$ est semi-simple si elle est diagonalisable sur $\overline{\mathbf{K}}$,

— Si A est un endomorphisme d'un $\mathbf{K}$-espace vectoriel W de dimension finie, on dit que A est semi-simple si sa matrice dans une base quelconque l'est ; c'est indépendant de la base. Si l'on sait ce que veut dire $\overline{W} = W \otimes_{\mathbf{K}} \overline{\mathbf{K}}$, cela est donc simplement la diagonalisabilité de l'extension de A à $\overline{W}$.

— Le polynôme minimal unitaire Q d'une matrice carrée M à coefficients dans un corps $\mathbf{K}$ est aussi le polynôme minimal sur la clôture algébrique $\overline{\mathbf{K}}$: en effet si $d = \deg Q$, alors Id, M, …, M^{d-1} sont linéairement indépendantes sur $\mathbf{K}$ donc aussi sur $\overline{\mathbf{K}}$ (avec la $\mathbf{K}$-base canonique de l'espace des matrices, l'indépendance se lit sur la non-annulation d'un au moins parmi certains déterminants de co-

efficients, et cela ne dépend pas du corps de base), donc le polynôme minimal sur une extension ne peut pas avoir un degré inférieur et comme il doit être un diviseur, il ne peut en fait pas changer.

— La matrice M est diagonalisable sur $\overline{\mathbf{K}}$ si et seulement si son polynôme minimal sur $\overline{\mathbf{K}}$ est à racines simples.

— D'où il découle : un $\mathbf{K}$ endomorphisme B est diagonalisable sur la clôture algébrique $\overline{\mathbf{K}}$ si et seulement si il existe un polynôme $Q \in \mathbf{K}[X]$ avec $Q(B) = 0$ et Q n'a que des racines simples dans $\overline{\mathbf{K}}$.

Donc :

Lemme 1. *Si $B \in \mathrm{End}_{\mathbf{K}}(W)$ est de la forme $T(A)$, avec A un endomorphisme de polynôme minimal P, alors B est semi-simple (comme W-endomorphisme) si et seulement si la multiplication f_T par T sur $\mathcal{A}$ est semi-simple (comme $\mathcal{A}$-endomorphisme).*

Preuve. Si $B = T(A)$ est semi-simple il existe un polynôme $Z \in \mathbf{K}[X]$, à racines simples dans $\overline{\mathbf{K}}$ avec $Z(T(A)) = 0$ comme W-endomorphisme. Mais $Z(T(A)) = Z(T)(A)$ et donc cela signifie que P divise $Z(T)$. Et ainsi $Z(T \bmod P) \equiv 0 \bmod P$. Et donc $Z(f_T)$, qui est aussi $f_{Z(T)}$, est nul, et ainsi f_T est semi-simple.

Réciproquement si $Z(f_T)$ est nul, alors $Z(T) = Z(f_T)(1) \bmod P$ est nul, et donc $Z(T(A))$ est nul, et $B = T(A)$ sera semi-simple si on peut prendre Z à racines simples dans $\overline{\mathbf{K}}$. □

Je signale aussi cette caractérisation :

Lemme 2. *Soit $\mathbf{K}$ un corps de caractéristique nulle ou un corps parfait de caractéristique p et W un $\mathbf{K}$-espace vectoriel de dimension finie. L'endomorphisme $B \in \mathrm{End}_{\mathbf{K}}(W)$ est semi-simple si et seulement si l'algèbre $\mathbf{K}[B]$ est réduite, c'est-à-dire sans nilpotents non nuls.*

Preuve. Si B est semi-simple tout élément $T(B)$ de $K[B]$ est diagonalisable sur $\overline{\mathbf{K}}$ donc s'il est nilpotent il est nul. Réciproquement soit P le polynôme minimal unitaire de B, donc $\mathbf{K}[B] \simeq \mathbf{K}[X]/(P)$. Soit Q le $\overline{\mathbf{K}}$-radical de P (voir la section suivante et page 19 pour une discussion détaillée), il appartient à $\mathbf{K}[X]$, donc $Q(B)$ est dans $\mathbf{K}[B]$, et est nilpotent. Il est donc nul. Ainsi en fait $Q = P$ et B est semi-simple. *On verra plus loin un contre-exemple en caractéristique p avec un corps $\mathbf{K}$ non parfait.* □

Dorénavant nous oublions l'espace vectoriel d'origine W et l'endomorphisme A pour ne plus travailler qu'avec une algèbre $\mathbf{K}[X]/(P)$.

3 Théorie générale : $\mathbf{K}[X]/(P)$ comme algèbre $\mathbf{K}[D,N]$

3.1 Factorisation d'un polynôme à la façon « intégrale de Lebesgue »

Soit $\mathbf{K}$ un corps et P un polynôme unitaire de $\mathbf{K}[X]$. Sur une clôture algébrique $\overline{\mathbf{K}}$, $P = \prod (X-\lambda_i)^{m_i}$, $1 \leqslant i \leqslant k$, $1 \leqslant m_i$.

Soit $Q_0 = \prod (X-\lambda_i)$ le polynôme réduit (a priori dans $\overline{\mathbf{K}}[X]$, mais voir plus loin). Puis, Q_1 le polynôme réduit de P/Q_0, Q_2 le polynôme réduit de $P/(Q_0Q_1)$, etc… Explicitement :

$$Q_k = \prod_{i, m_i \geqslant k+1} (X-\lambda_i)$$

et

$$P = Q_0 Q_1 \cdots Q_{m-1} \qquad m := \max\{m_i\}$$

avec $Q_{k+1} \mid Q_k$ pour tout k et $Q_{m-1} \neq 1$.

En caractéristique zéro, $Q_0 = P/\mathrm{pgcd}(P,P')$, et il est donc défini sur $\mathbf{K}$. Par récurrence, $Q_1, \ldots, Q_{m-1}$ sont aussi définis sur $\mathbf{K}$.

En caractéristique positive, *je fais l'hypothèse supplémentaire* quitte à remplacer $\mathbf{K}$ par une extension *que Q_0 est défini sur* $\mathbf{K}$. Par le Lemme qui suit $Q_1, \ldots, Q_{m-1}$ sont alors aussi définis sur $\mathbf{K}$.

cf. page 19 pour la preuve que Q_0 est toujours défini sur $\mathbf{K}$ si ce dernier est un corps parfait. 29/04/17

Lemme 3. *Soit K un corps, de clôture algébrique $\overline{\mathbf{K}}$. Soit P unitaire dans $\mathbf{K}[X]$ se factorisant sur $\overline{\mathbf{K}}$ en $\prod (X-\lambda_i)^{m_i}$, $1 \leqslant i \leqslant k$, $1 \leqslant m_i$. Soit $Q_0 = \prod (X-\lambda_i)$ le polynôme réduit. Si Q_0 est à coefficients dans $\mathbf{K}$, alors le polynôme réduit Q_1 de P/Q_0 est également à coefficients dans $\mathbf{K}$, et donc aussi le polynôme réduit Q_2 de $P/(Q_0Q_1)$, etc…*

Preuve. Compte tenu des factorisations sur $\overline{\mathbf{K}}$:

$$Q_0 = \prod (X-\lambda_i)$$

$$P/Q_0 = \prod_{i, m_i \geqslant 2} (X-\lambda_i)^{m_i-1}$$

on obtient

$$\mathrm{pgcd}(Q_0, P/Q_0) = \prod_{i, m_i \geqslant 2} (X-\lambda_i)^{\min(1, m_i-1)} = \prod_{i, m_i \geqslant 2} (X-\lambda_i) = Q_1$$

Or, comme Q_0 est dans $\mathbf{K}[X]$, c'est le cas également de P/Q_0, et donc de $\mathrm{pgcd}(Q_0, P/Q_0)$ (qu'on peut obtenir par l'algorithme d'Euclide qui se déroule entièrement dans $\mathbf{K}[X]$). Ainsi $Q_1 = \mathrm{pgcd}(Q_0, P/Q_0) \in \mathbf{K}[X]$. Par récurrence les autres Q_j sont également dans $\mathbf{K}[X]$. D'ailleurs on voit que $Q_{k+1} = \mathrm{pgcd}(Q_0, P/(Q_0 \ldots Q_k)) = \mathrm{pgcd}(Q_k, P/(Q_0 \ldots Q_k))$, ce qui donne un algorithme pour les obtenir une fois connu Q_0. □

L'exemple standard montrant qu'en caractéristique positive Q_0 n'est pas toujours défini sur $\mathbf{K}$ est obtenu avec $\mathbf{K} = \mathbf{F}_p(T)$, $P = X^p - T$, et donc $Q_0 = X - T^{1/p}$, avec $T^{1/p}$ l'unique solution de l'équation $x^p = T$ dans $\overline{\mathbf{K}}$. Dans ce cas $P = Q_0^p$, et $Q_0 = Q_1 = \cdots = Q_{p-1} = X - T^{1/p}$.

On va approfondir cet exemple. Montrons que $X^p - T$ est premier dans $\mathbf{K}[X]$. Si $fg = X^p - T$, alors $f(T^{1/p})g(T^{1/p}) = 0$ dans $\overline{\mathbf{K}}$, donc l'un des deux s'annule, par exemple $f(T^{1/p})$. Donc f n'est pas une constante (sinon elle serait nulle), et ainsi $f = c_0 + c_1 X + \cdots + c_n X^n$, $c_n \neq 0$, $n \geqslant 1$. De plus f divise $X^p - T$ donc $n \leqslant p$. On veut montrer $n = p$ car alors g est nécessairement une constante et on aura établi que $X^p - T$ est premier. Donc par l'absurde on suppose $1 \leqslant n < p$. Quitte à multiplier f par un élément non nul de $\mathbf{F}_p[T] \subset \mathbf{K}$, on peut supposer que les coefficients $c_0, \ldots, c_n$ sont également dans $\mathbf{F}_p[T]$. On a alors $f^p = c_0^p + c_1^p X^p + \cdots + c_n^p X^{pn}$, et en substituant $X = T^{1/p}$ on obtient $c_0^p + c_1^p T + \cdots + c_n^p T^n = 0$ dans $\mathbf{F}_p[T]$. Or les c_j^p sont en fait des polynômes en T^p. Comme $n < p$, pour un $0 \leqslant j < p$ donné, les monômes en T^{kp+j} provenant des polynômes $c_0^p, c_1^p T, \ldots, c_n^p T^n$ viennent tous du seul facteur $c_j^p T^j$. Comme la somme est nulle, chaque facteur est nul, et en particulier $c_n = 0$ ce qui est une contradiction.

Ainsi $\mathbf{K}[X]/(X^p - T)$ est une algèbre intègre, et donc a fortiori réduite. Mieux, comme c'est un $\mathbf{K}$-espace vectoriel de dimension finie, c'est en fait un corps. L'endomorphisme A de multiplication par X n'est cependant pas semi-simple puisque son polynôme minimal $X^p - T$ n'est pas à racines simples dans $\overline{\mathbf{K}}$, $X^p - T = (X - T^{1/p})^p$.

via le Frobenius $x \mapsto x^p$, ce corps est isomorphe au corps $\mathbf{F}_p(T)$ vu comme une algèbre sur le corps $\mathbf{F}_p(T^p)$. Le seul automorphisme sur le corps de base est l'identité. 29/04/17

On peut montrer que les éléments semi-simples dans cette algèbre sont exactement les scalaires $x \in \mathbf{K}$: tous les autres ont un polynôme minimal du type $X^p - f$, $f \notin \mathbf{K}^p$. 29/04/17

On a ici le phénomène que des nilpotents apparaissent *après* extension des scalaires, ce qui ne peut pas arriver pour une algèbre $\mathbf{K}[X]/(P)$ en caractéristique nulle comme on l'a vu déjà.

3.2 Coefficients de Taylor en toutes caractéristiques

Soit $T^{[j]}$ pour $T \in \mathbf{K}[X]$ et $j \in \mathbf{N}$ défini par la formule $\frac{1}{j!} T^{(j)}$ en caractéristique zéro, et en caractéristique positive par linéarité à partir de $(X^k)^{[j]} := \binom{k}{j} X^{k-j}$ pour $j \leqslant k$, 0 si $j > k$.

En toute caractéristique on a l'expansion de Taylor :

$$T(X + Y) = \sum_{j \geqslant 0} T^{[j]}(X) Y^j$$

Par linéarité en $T \in \mathbf{K}[X]$ il suffit de le vérifier pour $T = X^n$, et en effet $(X + Y)^n = \sum_{j \geqslant 0} \binom{n}{j} X^{n-j} Y^j = \sum_{j \geqslant 0} (X^n)^{[j]} Y^j = \sum_{j \geqslant 0} T^{[j]} Y^j$.

Et on a la formule de Leibniz :

$$(TU)^{[k]} = \sum_{i+j=k} T^{[i]} U^{[j]}$$

Ici encore par linéarité en T et en U il suffit de le vérifier pour $T = X^n$, $U = X^m$, et cette vérification peut se faire dans $\mathbf{Q}[X]$, et revient à la formule de Leibniz standard avec les coefficients du binôme. Ou encore on utilise le résultat précédent pour $(TU)(X+Y) = T(X+Y)U(X+Y)$, ce qui d'ailleurs est l'une des façons de démontrer la formule de Leibniz même en caractéristique nulle.

3.3 Isomorphisme avec une algèbre graduée

Je définis $\mathcal{A} = \mathbf{K}[X]/(P)$.

Soit maintenant $\mathcal{B}$ la $\mathbf{K}$-algèbre qui *comme espace vectoriel* est la somme directe

$$\mathcal{B} = \mathbf{K}[X]/(Q_0) \oplus \mathbf{K}[X]/(Q_1) \oplus \cdots \oplus \mathbf{K}[X]/(Q_{m-1})$$

Je mets une structure de $\mathbf{K}$-algèbre sur $\mathcal{B}$ via la règle :

$$(t_0, t_1, \ldots, t_{m-1}) \cdot (u_0, u_1, \ldots, u_{m-1}) \coloneqq (t_0u_0, t_0u_1 + t_1u_0, t_0u_2 + t_1u_1 + t_2u_0, \ldots)$$

Ceci est bien défini, car par exemple pour l'expression

$$t_0u_k + t_1u_{k-1} + \cdots + t_ku_0 \pmod{Q_k}$$

je rappelle que $Q_k \mid Q_{k-1} \mid \cdots \mid Q_0$, et donc les t_i, u_j intervenant dans la formule sont bien définis modulo Q_k.

Ainsi $\mathcal{B}$ est une $\mathbf{K}$-algèbre, je noterai

$$1 = (1, 0, \ldots, 0)$$
$$\eta = (X, 0, \ldots, 0)$$
$$\epsilon = (0, 1, \ldots, 0)$$

où les $\bmod Q_0$ et $\bmod Q_1$ sont sous-entendus.

On voit que $\epsilon^2 = (0, 0, 1, \ldots, 0), \ldots, \epsilon^{m-1} = (0, 0, \ldots, 1)$. Par ailleurs pour tout polynôme T on a $T(\eta) = (T \bmod Q_0, 0, \ldots, 0)$ et $T(\eta)\epsilon^k = (0, \ldots, 0, T \bmod Q_k, 0, \ldots, 0)$, avec le $T \bmod Q_k$ en k^{e} position (celle correspondant à $\mathbf{K}[X]/(Q_k)$).

Théorème 1. *L'application $\phi : \mathbf{K}[X] \to \mathcal{B}$:*

$$T \mapsto \phi(T) = (T \bmod Q_0, T^{[1]} \bmod Q_1, \ldots, T^{[m-1]} \bmod Q_{m-1})$$

est un morphisme de $\mathbf{K}$-algèbres et passe au quotient en un isomorphisme *:*

$$\psi : \mathcal{A} \simeq \mathcal{B}$$

Preuve. Le fait que ϕ soit un morphisme de $\mathbf{K}$-algèbre est conséquence de la loi de Leibniz vue précédemment.

Il nous reste à montrer que son noyau est l'idéal (P). Montrons $\phi(P) = 0$. Certainement Q_j^{j+1} divise $P = Q_0 Q_1 \dots Q_{m-1}$. Soit λ une des racines de Q_j. Donc $Z = (X-\lambda)^{j+1}$ divise P dans $\overline{\mathbf{K}}[X]$. Or on peut montrer que $Z^{[j]}$ vaut $(j+1)(X-\lambda)$ car il suffit de regarder le coefficient de Y^j dans $(X-\lambda+Y)^{j+1}$. Plus généralement on voit de même que $Z^{[i]}(\lambda) = 0$ pour $0 \leqslant i \leqslant j$. Donc par la formule de Leibniz $P^{[j]}(\lambda) = 0$. Autrement dit $X-\lambda$ divise $P^{[j]}$, et donc Q_j divise $P^{[j]}$ dans $\overline{\mathbf{K}}[X]$ donc dans $\mathbf{K}[X]$. Ceci prouve $\phi(P) = 0$.

Ainsi ϕ se factorise en $\psi : \mathcal{A} \to \mathcal{B}$. Les deux $\mathbf{K}$ espaces vectoriels ont la même dimension et il suffit maintenant de montrer que ψ est injective.

On va le faire par récurrence sur m. Pour $m = 1$ c'est immédiat, $\mathcal{A} = \mathcal{B}$. Soit $T \in \mathcal{A}$ dans le noyau, par l'hypothèse de récurrence on sait que $T = P_{m-1} Z$ avec $P_{m-1} = P/Q_{m-1}$. Dans la formule de Leibniz pour $T^{[m-1]}$, les $P_{m-1}^{[j]}$ sont nuls modulo Q_j pour $j < m-1$, donc aussi modulo Q_{m-1}. Ainsi $T^{[m-1]} \bmod Q_{m-1} = P_{m-1}^{[m-1]} Z \bmod Q_{m-1}$. Soit λ une racine de Q_{m-1}. C'est donc une racine d'ordre exactement $m-1$ de P_{m-1} et par conséquent ce n'est *pas* une racine de $P_{m-1}^{[m-1]}$. De $\psi(T) = 0$ résulte $T^{[m-1]}(\lambda) = 0$, et donc $Z(\lambda) = 0$. Donc Q_{m-1} (qui est à racines simples dans $\overline{\mathbf{K}}$) divise Z. Mais alors $P = P_{m-1} Q_{m-1}$ divise T, c.q.f.d. □

Théorème 2. *Soit dans $\mathcal{B}$, $\mathcal{I}_k$ le sous-espace vectoriel dont les éléments $t = (t_0, \dots, t_{m-1})$ vérifient $t_0 = \dots = t_{k-1} = 0$. Alors $\mathcal{I}_k$ est un idéal et $\mathcal{I}_k = \mathcal{I}_1^k$ pour $k \geqslant 1$. De plus $\mathcal{I}_1$ est le radical de $\mathcal{B}$, c'est-à-dire l'idéal des éléments nilpotents.*

Preuve. Soit $t = (t_0, \dots, t_{m-1})$ avec seulement t_j non nul, $j \geqslant 1$. Soit T_j in $\mathbf{K}[X]/(Q_0)$ avec $T_j \equiv t_j \bmod Q_j$. On a déjà vu la formule $t = T_j(\eta)\epsilon^j$, donc t est dans l'idéal engendré par ϵ^j, et donc dans l'idéal (ϵ^k) pour tout $k \leqslant j$. Par conséquent, $\mathcal{I}_k$ est dans l'idéal engendré par ϵ^k, qui est inclus dans l'idéal $\mathcal{I}_1^k$. La réciproque est également immédiate puisqu'on vérifie aisément $\mathcal{I}_i \cdot \mathcal{I}_j \subset \mathcal{I}_{i+j}$.

Si t est nilpotent, alors t_0 aussi puisque la projection sur la première coordonnée est un morphisme d'algèbre. Mais $\mathbf{K}[X]/(Q_0)$ n'a pas d'élèments nilpotents non nuls (si $T^k \equiv 0 \bmod Q_0$ alors $T(\lambda) = 0$ pour toutes les racines de Q_0 et donc T est divisible par Q_0, les racines étant simples). Donc $t_0 = 0$ et $t \in \mathcal{I}_1$. □

On voit donc que $\mathcal{B}$ est isomorphe à l'algèbre graduée associée à la filtration $\mathcal{I}_1$-adique de $\mathcal{A}$ par son radical $\mathcal{I}_1 = \mathcal{N}$ des éléments nilpotents. Et qu'il se trouve que $\mathcal{A}$ est isomorphe *comme algèbre* avec cette algèbre graduée, ce qui n'était pas évident a priori : déjà pour commencer il n'y a pas en général, de morphisme d'anneau naturel

Je veux dire bien sûr, à part la projection $A \to A/I$ sur la première composante… 29/04/17

$f : A \to \mathrm{Gr}_I(A) = A/I \oplus I/I^2 \oplus I^2/I^3 \oplus ..$ d'un anneau commutatif A vers son gradué I-adique, lorsque $I \subset A$ est un idéal. Et pas non plus dans le cas particulier avec $I = \mathrm{rad}(A)$ l'idéal des éléments nilpotents. Car que serait par exemple l'application envoyant A vers I/I^2 ? On sait faire $A \to A/I$, mais pas $A \to I/I^2$. Attention au piège ici que $a \mapsto f_1(a) \coloneqq f(a)_1 \in I/I^2$ ne peut *pas* être un morphisme de A-modules, car cela imposerait $f_1(a) = f_1(a.1) = af_1(1) \pmod{I^2}$, mais $f(1)$ doit être l'unité $(1, 0, 0, \dots)$ de $\mathrm{Gr}_I(A)$, donc $f_1(1) = f(1)_1 = 0$. Et la seule possibilité est alors que f_1 soit le morphisme nul.

Il se trouve qu'ici pour une algèbre polynomiale avec un générateur, nous avons prouvé *en utilisant tacitement des dérivées via les coefficients de* Taylor l'existence d'un tel morphisme $\mathcal{A} \to \mathcal{A}/\mathcal{N} \oplus \mathcal{N}/\mathcal{N}^2 \oplus \mathcal{N}^2/\mathcal{N}^3 \oplus ..$, mais il nous reste à en expliciter la formule, lorsque l'agèbre graduée est présentée sous cette forme. En effet à ce stade nous ne voyons pas encore bien en particulier quel peut être le morphisme de $\mathbf{K}$-espace vectoriel de $\mathcal{A}$ vers $\mathcal{N}/\mathcal{N}^2$ par exemple.

En ce qui concerne le radical $\mathcal{N}$, c'est bien sûr l'idéal (Q_0) de $\mathcal{A}$, comme on voit directement, où qu'on retrouve en disant que T est dans $\mathcal{N} = \mathcal{I}_1$ si son image dans $\mathcal{B}$ par ψ a sa première composante nulle, or celle-ci est $T \bmod Q_0$.

3.4 L'idéal des relations entre D et N

Théorème 3. *Soit $\theta : \mathbf{K}[V, W] \to \mathcal{B}$ le morphisme d'algèbre qui envoie V sur η et W sur ϵ. Alors θ est surjectif et son noyau est l'idéal*

$$\mathcal{J} \coloneqq (Q_0(V), Q_1(V)W, Q_2(V)W^2, \dots, Q_{m-1}(V)W^{m-1}, W^m)$$

Autrement dit $\mathcal{B}$ est la $\mathbf{K}$-algèbre engendrée par η et ϵ modulo les relations $Q_0(\eta) = Q_1(\eta)\epsilon = Q_2(\eta)\epsilon^2 = \cdots = Q_{m-1}(\eta)\epsilon^{m-1} = \epsilon^m = 0$.

Preuve. La surjectivité découle de remarques déjà faites, ainsi que le fait que l'idéal $\mathcal{J}$ soit dans le noyau de θ. Il suffit de montrer que $\mathbf{K}[V, W]/\mathcal{J}$ et $\mathcal{B}$ ont la même dimension comme $\mathbf{K}$ espaces vectoriels.

Mais il est immédiat qu'un système générateur de $\mathbf{K}[V, W]/\mathcal{J}$ comme $\mathbf{K}$ espace vectoriel est donné par les $V^a W^b$, $0 \leqslant b < m$, $0 \leqslant a < \deg Q_b$. La dimension de $\mathbf{K}[V, W]/\mathcal{J}$ est donc au plus $\sum_b \deg Q_b = \dim \mathcal{B}$. Par la surjectivité, la dimension ne peut pas être strictement inférieure. Elle est donc égale à celle de $\mathcal{B}$ et $\mathbf{K}[V, W]/\mathcal{J} \simeq \mathcal{B}$. On voit au passage que le système générateur est une base. □

On déduit de ce qui précède :

Théorème 4. *Soit $D = \psi^{-1}(\eta)$ et $N = \psi^{-1}(\epsilon)$. La* **K** *algèbre $\mathcal{A} = \mathbf{K}[X]/(P)$ est engendrée par D et N (on remarque d'ailleurs que $X \bmod P = D + N$) et l'idéal de leurs relations est engendré par :*

$$Q_0(D) = Q_1(D)N = Q_2(D)N^2 = \cdots = Q_{m-1}(D)N^{m-1} = N^m = 0$$

3.5 Les projecteurs de la décomposition faisant de $\mathcal{A}$ une algèbre graduée

Et nous pouvons maintenant répondre à nos interrogations métaphysiques sur le mystérieux morphisme d'algèbres $\mathcal{A} \to \mathrm{Gr}_{\mathcal{N}}(A) = \mathcal{A}/\mathcal{N} \oplus \mathcal{N}/\mathcal{N}^2 \oplus \mathcal{N}^2/\mathcal{N}^3 \oplus \ldots$

Soit $T \in \mathcal{A}$. Au risque de créer des confusions considérons la formule de Taylor :

$$T = T(D+N) = T(D) + T'(D)N + T^{[2]}(D)N^2 + \cdots + T^{[m-1]}(D)N^{m-1}$$

Tout d'abord cela-a-t-il un sens ? Nous avons relevé T, D, et N en des éléments de $\mathbf{K}[X]$ et substitué D et N dans la formule de Taylor pour $T(X+Y)$ qui va jusqu'à $Y^{\deg T}$. Puis nous avons à nouveau réduit modulo P (ce qui a supprimé d'office certains termes puisque $N^m \equiv 0 \bmod P$). Le résultat est-il indépendant du choix des représentants ? Fixons ceux de D et N et modifions T par un terme PZ. Il nous faut donc :

Lemme 4. *Quels que soient les représentants D et N dans* $\mathbf{K}[X]$*, et le polynôme Z, on a dans* $\mathbf{K}[X]$ *:*

$$0 \leqslant j < m \implies (PZ)^{[j]}(D)N^j \equiv 0 \pmod{P}$$

Preuve. Il suffit de vérifier que $\phi((PZ)^{[j]}(D)N^j)$ est nul dans $\mathcal{B}$, puisque (P) est le noyau de ϕ. Or ϕ est un morphisme d'algèbres donc

$$\phi((PZ)^{[j]}(D)N^j) = (PZ)^{[j]}(\eta)\epsilon^j = ((PZ)^{[j]} \bmod Q_j)(\eta)\epsilon^j$$

Donc il suffit de s'assurer que $(PZ)^{[j]} \equiv 0 \bmod Q_j$. Mais cela a déjà été établi lorsque nous avons montré que $\phi(PZ) \in \mathcal{B}$ était nul. □

Donc chaque $T^{[j]}(D)N^j$ ne dépend pas modulo (P) du choix de $T \in \mathbf{K}[X]$, et bien sûr ne dépend pas non plus modulo (P) du choix de D ou N dans $\mathbf{K}[X]$.

Autrement dit nous avons des morphismes de **K**-espaces vectoriels :

$$\begin{aligned} f_j : \mathcal{A} = \mathbf{K}[X]/(P) &\to \mathbf{K}[X]/(P) \\ T &\mapsto T^{[j]}(D)N^j \end{aligned}$$

qui sont correctement définis. Par exemple, dans le cas le plus simple, $f_0(T) = T(D)$ a un sens car $Q_0(D)$ donc a fortiori $P(D)$ est nul (dans $\mathcal{A}$).

En appliquant à

$$T = T(D+N) = T(D) + T'(D)N + T^{[2]}(D)N^2 + \cdots + T^{[m-1]}(D)N^{m-1}$$

le morphisme d'algèbres $\psi : \mathcal{A} \to \mathcal{B}$ on obtient

$$\psi(T) = T(\eta) + T'(\eta)\epsilon + \cdots + T^{[m-1]}(\eta)\epsilon^{m-1}$$

où chaque terme $T^{[j]}(\eta)\epsilon^j$ appartient au sous-espace vectoriel $\mathbf{K}[X]/(Q_j)$ de l'algèbre $\mathcal{B}$. Ceci nous permet d'affirmer que $T^{[j]}(D)N^j$ est le morceau de T correspondant à la partie $\mathcal{N}^j/\mathcal{N}^{j+1}$ dans la décomposition de $\mathcal{A}$ en somme directe déduite de l'isomorphisme avec $\mathrm{Gr}_{\mathcal{N}}(A)$. De plus $T^{[j]}(D)N^j$ et $T^{[j]}(X)N^j$ sont égaux modulo N^{j+1} puisque $D \equiv X \pmod{N}$. Ainsi la projection de $\mathcal{A}$ sur $\mathcal{N}/\mathcal{N}^2$ est donnée par la formule :

$$T \mapsto T'N \bmod \mathcal{N}^2$$

et que celle sur $\mathcal{N}^2/\mathcal{N}^3$ est donnée par la formule :

$$T \mapsto T^{[2]}N^2 \bmod \mathcal{N}^3$$

et ainsi de suite.

Plus précisément la décomposition canonique de $\mathcal{A}$ en somme directe d'espaces vectoriels est donnée par les $f_j \in \mathrm{End}_{\mathbf{K}}(\mathcal{A})$ suivants :

$$f_j(T) = T^{[j]}(D)N^j$$

Ce sont donc des idempotents !

$$f_j \circ f_j = f_j, \qquad j \neq k \implies f_j \circ f_k = 0, \qquad \mathrm{Id} = \sum_j f_j$$

D'où des formules amusantes dont la plus simple est $T(D)(D) = T(D)$.

Au risque d'achever mon lecteur, considérons les cas particuliers $T = D$ et $T = N$. En effet de :

$$N = N(D) + N'(D)N + N^{[2]}(D)N^2 + \cdots + N^{[m-1]}(D)N^{m-1}$$

et compte tenu du fait qu'il ne peut y avoir qu'une seule écriture correspondant à la somme directe nous pouvons affirmer que les égalités suivantes valent dans $\mathcal{A}$:

$$N(D) = 0, \quad N'(D)N = N, \quad N^{[2]}(D)N^2 = 0, \quad \ldots, \quad N^{[m-1]}(D)N^{m-1} = 0$$

Et l'on peut rappeler également les formules qui traduisent simplement que $\psi(N) = (0,1,0,\dots)$:

$$N \equiv 0 \bmod Q_0, \quad N' \equiv 1 \bmod Q_1, \quad N^{[2]} \equiv 0 \bmod Q_2, \quad \dots$$

De même on a :

$$D = D(D) + D'(D)N + D^{[2]}(D)N^2 + \cdots + D^{[m-1]}(D)N^{m-1}$$

ce qui impose :

$$D = D(D), \quad D'(D)N = 0, \quad D^{[2]}(D)N^2 = 0, \quad \dots, \quad D^{[m-1]}(D)N^{m-1} = 0$$

Confusionné ? Pas de ma faute !

4 Quels sont les $T \in \mathbf{K}[X]/(P)$ semi-simples ?

On dira que $T \in \mathcal{A}$ est semi-simple si l'endomorphisme f_T de multiplication par T sur l'espace-vectoriel $\mathcal{A} = \mathbf{K}[X]/(P)$ est diagonalisable sur $\overline{\mathbf{K}}$. Comme l'on sait, cela revient à dire que le polynôme minimal de f_T (qui est le même sur $\mathbf{K}$ ou sur la clôture algébrique $\overline{\mathbf{K}}$) est à racines simples dans $\overline{\mathbf{K}}$.

Théorème 5. *Les conditions suivantes sur $T \in \mathcal{A}$ sont équivalentes :*

1. *T est semi-simple,*
2. *$T = T(D)$,*
3. *T est un polynôme en D,*
4. *$T' \equiv 0 \bmod Q_1$, $T^{[2]} \equiv 0 \bmod Q_2$, …, $T^{[m-1]} \equiv 0 \bmod Q_{m-1}$.*

Preuve. Nous commençons par remarquer que $Q_0(D) = 0$ puisque $\psi(Q_0(D)) = Q_0(\eta) = 0$. Donc D est semi-simple, et on voit que Q_0 est son polynôme minimal. On étend les scalaires à $\overline{\mathbf{K}}$ pour $\mathbf{K}[X]/(P)$ afin de décomposer $V = \overline{\mathbf{K}}[X]/(P)$ comme une somme directe d'espaces propres V_λ indicés par les racines de Q_0. Comme la multiplication f_X par X commute avec f_D, X respecte V_λ et comme $X = D + N$ avec N nilpotent, on peut trouver une base donnant une représentation triangulaire de f_X, qui aura comme diagonale la représentation de f_D. On en déduit que $D(\lambda) = \lambda$, ce que l'on voit d'ailleurs déjà sur la congruence $D \equiv X \pmod{Q_0}$.

Soit alors $T \in \mathcal{A}$ tel que le polynôme d'endomorphisme $f_T = T(f_X)$ est diagonalisable sur $\overline{\mathbf{K}}$. Dans la base précédente de V, f_T est donné par des blocs triangulaires, avec

des $T(\lambda)$ sur la diagonale. Ainsi V_λ est respecté par f_T et f_T y possède une unique valeur propre. La diagonalisabilité sur V implique celle sur V_λ et donc que f_T y est une homothétie, autrement dit y agit comme $f_{T(D)}$. En conclusion $f_T = f_{T(D)}$ et $T = T(D)$.

Note : $T(D)$ a bien un sens pour $T \in \mathcal{A} = \mathbf{K}[X]/(P)$ car on a indiqué que le polynôme minimal de D était Q_0, qui est un diviseur de P.

Comme ψ est un morphisme d'algèbre, de $T = Z(D)$ on déduit $\psi(T) = Z(\eta) = (Z \bmod Q_1, 0, 0, 0, \ldots, 0)$. Mais cela signifie $T' \equiv 0 \bmod Q_1$, $T^{[2]} \equiv 0 \bmod Q_2$, …, $T^{[m-1]} \equiv 0 \bmod Q_{m-1}$.

Finalement, si cela est le cas c'est que $\psi(T) = T(\eta) = \psi(T(D))$ et donc que $T = T(D)$ dans $\mathcal{A}$. Comme D est semi-simple il en est de même de $T(D)$ et donc de T. □

On notera la conséquence amusante $\boxed{D = D(D)}$ déjà signalée précédemment !

Théorème 6. *Si le corps* **K** *est de caractéristique nulle, $T \in \mathcal{A}$ est semi-simple si et seulement si $T' \equiv 0 \bmod \operatorname{pgcd}(P, P')$.*

Preuve. En caractéristique nulle, $\operatorname{pgcd}(P, P') = P/Q_0$. Les conditions $T' \equiv 0 \bmod Q_1$, $T^{[2]} \equiv 0 \bmod Q_2$, …, $T^{[m-1]} \equiv 0 \bmod Q_{m-1}$ équivalent en caractéristique nulle à $T' \equiv 0 \bmod Q_1$, $(T')^{[1]} \equiv 0 \bmod Q_2$, …, $(T')^{[m-2]} \equiv 0 \bmod Q_{m-1}$, dont nous savons qu'elles équivalent à $T' \equiv 0 \bmod Q_1 Q_2 \ldots Q_{m-1}$, c'est-à-dire à $T' \equiv 0 \bmod \operatorname{pgcd}(P, P')$. □

Remarque : comme $(nX^{n-1})^{[j-1]} = j(X^n)^{[j]}$, et donc pour tout T, $(T')^{[j-1]} = jT^{[j]}$, en toute caractéristique il est vrai que si $T \in \mathcal{A}$ est semi-simple alors $T' \equiv 0 \pmod{P/Q_0}$. Mais cette condition nécessaire n'est pas suffisante, si $m >$ caract.**K**. Prenons comme exemple le plus simple $\mathcal{A} = K[X]/(X^3)$ en caractéristique 2. La condition nécessaire et suffisante pour que $T = a + bX + cX^2$ soit semi-simple est que $T' = b + 2cX = b \equiv 0 \bmod X$, donc $b = 0$ et $T^{[2]} = c \equiv 0 \bmod X$, donc $c = 0$, soit simplement au total que $T \equiv a \bmod X^3$. Mais cela diffère de la condition $T' \equiv 0 \bmod X^2$ qui signifie simplement $b = 0$ mais n'impose pas de condition sur c.

5 La graduation est-elle invariante par automorphisme ?

Soit donc $\mathcal{A}_{ss} = \mathbf{K}[D]$ la partie de $\mathcal{A}$ comportant les éléments semi-simples. C'est une sous-algèbre. Nous pouvons alors exprimer la décomposition correspondant à l'isomorphisme $\mathcal{A} \simeq \mathcal{B}$ sous la forme :

$$\mathcal{A} = \mathcal{A}_{ss} \oplus \mathcal{A}_{ss}N \oplus \mathcal{A}_{ss}N^2 \oplus \cdots \oplus \mathcal{A}_{ss}N^{m-1}$$

La question se pose de savoir si cette décomposition ne dépend réellement d'aucun choix : est-elle invariante par les automorphismes de $\mathcal{A}$?

Si l'on voit $\mathcal{A}$ comme un $\mathcal{A}_{ss} \simeq \mathbf{K}[X]/(Q_0)$ module, cela donne une décomposition (faisant jouer un rôle particulier à N venant de $\mathcal{A} = \mathcal{A}_{ss} \oplus \mathcal{N}$, $X = D + N$) en somme directe $\mathcal{A}_{ss} \oplus \mathcal{A}_{ss}/(Q_{m-1}) \oplus \cdots \oplus \mathcal{A}_{ss}/(Q_1)$ avec des « facteurs invariants » $Q_{m-1} | \ldots | Q_1$. L'anneau $\mathcal{A}_{ss}$ est principal mais pas en général intègre (s'il l'est $\mathcal{A}_{ss}$ est un corps et les $Q_j = Q_0$ sont nuls dans $\mathcal{A}_{ss}$.) 29/04/17

C'est certainement le cas pour le premier bloc, car $\mathcal{A}_{ss}$ est caractérisé intrinsèquement. Le complément direct donné par la somme des autres blocs est la partie nilpotente, le radical $\mathcal{N}$ de $\mathcal{A}$ qui est aussi caractérisé intrinsèquement.

Donc pour trouver un contre-exemple il faut prendre m au moins égal à 3. Et en effet :

Théorème 7. *Si $m \geqslant 3$, l'algèbre $\mathcal{A}$ admet des automorphismes Ψ tel que*

$$\Psi(N) \notin \mathcal{A}_{ss}N$$

En particulier il existe un (unique) automorphisme Ψ vérifiant $\Psi(D) = D$ et $\Psi(N) = N+N^2$.

Plus généralement pour tout $U \in \mathcal{A}$ il existe un automorphisme Ψ_U de $\mathcal{A}$ vérifiant $\Psi_U(D) = D$ et $\Psi_U(N) = N + N^2U$. Il est caractérisé par $\Psi_U(X) = X + N^2U$.

Si $N^2U \neq 0$, la décomposition de $\mathcal{A}$ en somme directe $\oplus_j \mathcal{A}_{ss}N^j$ n'est donc pas invariante *par ce Ψ_U.*

Preuve. Considérons le morphisme de $\mathbf{K}$-algèbres $\Theta : \mathbf{K}[V, W] \to \mathcal{A}$ défini par $\Theta(V) = D$ et $\Theta(W) = N + N^2U$. Il est clair que $Q_j(V)W^j$ est dans l'idéal noyau, autrement dit que $Q_j(D)\cdot(N+N^2U)^j = 0$ dans $\mathcal{A}$ puisque $Q_j(D)N^j = 0$ et $(N+N^2U)^j = N^j(1+NU)^j$. Donc Θ passe au quotient et définit un morphisme d'algèbre

$$\Psi : \mathbf{K}[V, W]/(Q_0(V), Q_1(V)W, \ldots, W^m) \simeq \mathcal{A} \to \mathcal{A}$$

qui vérifie donc $\Psi(D) = D$ et $\Psi(N) = N + N^2U$.

Il reste à montrer que Ψ est un automorphisme, et pour cela il suffit de montrer qu'il est un isomorphisme d'espaces vectoriels, et donc il suffit de montrer qu'il est surjectif, et pour cela il suffit de montrer que N est dans son image, puisque $\mathcal{A}$ est engendré par $X = D + N$, et que l'image est une algèbre qui contient déjà D.

Posons $N_1 = N + N^2U$, et écrivons le sous la forme

$$N_1 = N + U_2N^2 + U_3N^3 + \cdots + U_{m-1}N^{m-1}$$

avec les U_j dans $\mathcal{A}_{ss}$, donc dans l'image de Ψ_U. Soit $N_2 = N_1 - U_2N_1^2$. Il est dans l'image de Ψ_U et de la forme

$$N_2 = N + U_{3,2}N^3 + \cdots + U_{m-1,2}N^{m-1}$$

avec de nouveaux éléments $U_{j,2} \in \mathcal{A}_{ss}$. On pose alors $N_3 = N_2 - U_{3,2}N_2^3$ qui est à nouveau dans l'image de Ψ_U. Et ainsi de suite. Au final on obtient $N_{m-1} = N$ et donc on a établi $N \in \mathrm{Im}(\Psi_U)$.

Il ne reste plus qu'à montrer que Ψ_U est caractérisé par $\Psi_U(X) = X + N^2U$. Supposons que $\Psi : \mathcal{A} \to \mathcal{A}$ est un morphisme d'algèbre vérifiant $\Psi(X) = X + N^2U$. Soit

$Y = X + N^2U$. Ainsi $Y = \Psi(D) + \Psi(N)$. Comme $\Psi(D)$ annule Q_0, c'est un élément semi-simple. Et $\Psi(N)$ est nilpotent. Nous savons que $\mathcal{A}_{ss}$ et $\mathcal{N}$ sont en somme directe dans $\mathcal{A}$. Donc Y a une seule décomposition de ce type. Or $Y = D + N + N^2U$ en est une autre, donc $D = \Psi(D)$, $N + N^2U = \Psi(N)$ et $\Psi = \Psi_U$. □

Remarque : il résulte de ce qui a été établi que $X + N^2U$ a le même polynôme minimal que X dans $\mathcal{A} = \mathbf{K}[X]/(P)$, à savoir P. Et réciproquement si l'on montre que le polynôme minimal de $X + N^2U$ est P, on en déduit qu'il existe un automorphisme de $\mathcal{A}$ envoyant X sur $X + N^2U$: le fait que $P(X + N^2U) = 0$ suffit à montrer qu'un morphisme d'algèbre existe, et le fait de savoir que P est minimal montre que la dimension comme $\mathbf{K}$ espace vectoriel de l'image est $\deg P$, donc le morphisme est un automorphisme.

Une autre démonstration serait donc de montrer directement que le polynôme minimal de l'endomorphisme de multiplication par $X + N^2U$ sur $\mathbf{K}[X]/(P)$ est P. On peut d'ailleurs remplacer N par le radical Q_0 de P car on a déjà indiqué que (Q_0) et (N) étaient tous deux le même idéal $\mathcal{N}$ des nilpotents de $\mathcal{A}$. Ceci donne donc un énoncé qui ne nécessite pas d'avoir fait la théorie de la décomposition de X en $D + N$:

Lemme 5. *Soit $P \in \mathbf{K}[X]$ unitaire dont le radical Q_0 dans $\overline{\mathbf{K}}$ est aussi dans $\mathbf{K}[X]$. Alors dans l'anneau quotient $\mathcal{A} = \mathbf{K}[X]/(P)$, tout élément T qui est congru à X modulo Q_0^2 possède également P comme polynôme minimal.*

Preuve. Écrivons $T = X + Q_0^2U$. La preuve se fait très facilement après extension des scalaires à $\overline{\mathbf{K}}$ en utilisant la décomposition primaire (la somme directe est ici une somme d'algèbres) :

$$\overline{\mathcal{A}} = \overline{\mathbf{K}}[X]/(P) \simeq \oplus_i \overline{\mathbf{K}}[X]/((X - \lambda_i)^{m_i})$$

En effet, avec $V_i = (Q_0/(X - \lambda_i))^2 U$:

$$(X + Q_0^2U - \lambda_i)^{m_i - 1} = (X - \lambda_i)^{m_i - 1}(1 + (X - \lambda_i)V_i)^{m_i - 1} \equiv (X - \lambda_i)^{m_i - 1} \pmod{(X - \lambda_i)^{m_i}}$$
$$(X + Q_0^2U - \lambda_i)^{m_i} \equiv 0 \pmod{(X - \lambda_i)^{m_i}}$$

donc $P(X + Q_0^2U) = 0$ dans $\mathcal{A}$. Et par contre aucun des $(P/(X - \lambda_i))(X + Q_0^2U)$ n'est nul dans $\overline{\mathcal{A}}$: pour chaque $j \neq i$, $(X + Q_0^2U - \lambda_j)^{m_j}$ est premier avec $X - \lambda_i$ (il ne s'annule pas en λ_i) et par conséquent un inversible modulo $(X - \lambda_i)^{m_i}$, et nous avons vu que $(X + Q_0^2U - \lambda_i)^{m_i - 1}$ était non nul modulo $(X - \lambda_i)^{m_i}$. Ceci prouve que P est le polynôme minimal de $X + Q_0^2U$ dans $\overline{\mathcal{A}}$, donc dans $\mathcal{A}$. □

Comme signalé précédemment il résulte du lemme qu'il existe un automorphisme de $\mathcal{A}$ qui envoie X sur $T = X + Q_0^2U$.

6 Un groupe d'automorphismes de l'algèbre $\mathbf{K}[X]/(P)$

Il y a des cas d'automorphismes qui respectent la graduation, par exemple celui donné par $X \mapsto b + a - X$ dans $\mathbf{K}[X]/((X-a)^m(X-b)^m)$, car il agit par $D \mapsto b + a - D$, $N \mapsto -N$. [1]

Et bien sûr l'existence même de la graduation se traduit par l'existence d'un groupe d'automorphismes particuliers : on peut en effet faire agir le groupe multiplicatif $\mathbf{G}_m$ sur la composante $\mathcal{A}_{ss}N^j$ de $\mathcal{A}$ par son caractère x^j. Autrement dit :

$$T \in \mathcal{A}_{ss}N^j \implies x \cdot T := x^j T$$

et cela donne des *automorphismes de la* $\mathbf{K}$*-algèbre* graduée $\mathcal{A}$. L'automorphisme g_x est caractérisé par

$$g_x(X) = D + xN \qquad \text{ou par } g_x(D) = D \qquad g_x(N) = xN$$

On peut aussi se convaincre que cela marche en constatant que le couple (D, xN) vérifie les mêmes relations $Q_j(D)(xN)^j = 0$ que le couple (D, N). On va formuler un peu différemment :

Théorème 8. *Soit $P \in \mathbf{K}[X]$ unitaire et $\prod_{1\leqslant i\leqslant k}(X-\lambda_i)^{m_i}$ sa décomposition sur la clôture algébrique $\overline{\mathbf{K}}$. Soit $\mathcal{A} = \mathbf{K}[X]/(P)$ et $\overline{\mathcal{A}} = \overline{\mathbf{K}}[X]/(P) \simeq \oplus_i \overline{\mathbf{K}}[X]/((X-\lambda_i)^{m_i})$.*

On peut définir une action du groupe multiplicatif $\mathbf{G}_m(\mathbf{K})$ par des automorphismes g_x de $\overline{\mathcal{A}}$ via les congruences suivantes :

$$\forall T \in \overline{\mathcal{A}} \qquad \forall 1 \leqslant i \leqslant k \qquad g_x(T) \equiv T(xX + (1-x)\lambda_i) \pmod{(X-\lambda_i)^{m_i}}$$

Si le radical Q_0 de P est défini sur $\mathbf{K}$ alors les automorphismes g_x, $x \in \mathbf{K}^*$, de $\overline{\mathcal{A}}$ sont déjà des automorphismes de la $\mathbf{K}$-algèbre $\mathcal{A}$. C'est toujours le cas en caractéristique nulle.

Preuve. Si $T \in \overline{\mathbf{K}}[X]$ est divisible par $(X-\lambda_i)^{m_i}$ alors $T(xX + (1-x)\lambda_i)$ est divisible par $(xX + (1-x)\lambda_i - \lambda_i)^{m_i} = x^{m_i}(X-\lambda_i)^{m_i}$, donc l'automorphisme $g_i(x)$ sur $\overline{\mathbf{K}}[X]$ de substitution $X \leftarrow xX + (1-x)\lambda_i$ passe au quotient. Par ailleurs, si l'on conjugue par l'automorphisme θ_i de $\overline{\mathbf{K}}[X]$ qui fait la substitution $X \leftarrow X - \lambda_i$, g_i devient simplement la substitution $X \leftarrow xX$, et donc certainement $g_i(xy) = g_i(x)g_i(y)$, d'abord sur $\overline{\mathbf{K}}[X]$ puis sur l'algèbre quotient $\overline{\mathbf{K}}[X]/((X-\lambda_i)^{m_i})$.

Comme l'algèbre $\overline{\mathcal{A}}$ est le produit de ces algèbres on aboutit aux automorphismes g_x définis dans l'énoncé, et au fait que $g_{xy} = g_x g_y$.

1. Ici a et b ne sont pas supposés rationnels ($a+b$ l'est), et à propos, il y a de jolies formules pour D et N lorsque le polynôme minimal P est de ce type à deux racines (multiples) dans $\overline{\mathbf{K}}$.

Si maintenant on considère l'unique $D \in \overline{\mathcal{A}}$ qui vérifie $D \equiv \lambda_i \pmod{(X-\lambda_i)^{m_i}}$ pour tout i, il est clair que D est laissé fixe par les g_x et que $X - D = N$ qui est congru à $X - \lambda_i$ modulo $(X-\lambda_i)^{m_i}$ pour chaque i est transformé par g_x en $g_x(N) = xN$.

Nous savons lorsque $Q_0 \in \mathbf{K}[X]$ qu'en fait le D et le N que nous venons de définir sont dans $\mathcal{A}$: car $Q_0(D) = 0$ donc D est semi-simple, N est nilpotent et $X = D + N$, donc ces D et N sont ceux obtenus précédemment. Nos g_x en effet sont donc des automorphismes de $\mathcal{A}$ (qui est engendré par D et N) et ce sont ceux de l'action du groupe multiplicatif correspondant à la graduation $\mathcal{A} = \mathbf{K}[D] \oplus \mathbf{K}[D]N \oplus \mathbf{K}[D]N^2 \oplus \dots$. □

7 Quand la décomposition de Chevalley-Dunford est-elle définie sur K ?

Revenons provisoirement à un endomorphisme A d'un $\mathbf{K}$-espace vectoriel V de dimension finie. Soit $P \in \mathbf{K}[X]$ le polynôme minimal (unitaire) de A et $Q \in \overline{\mathbf{K}}[X]$ son radical. On a vu que lorsque $Q \in \mathbf{K}[X]$ on obtient une décomposition $A = D + N$ avec D un polynôme en A (à coefficients dans $\mathbf{K}$), N nilpotent, et D semi-simple (vérifiant d'ailleurs $Q(D) = 0$).

Réciproquement supposons $A = D + N$ avec $DN = ND$, D semi-simple, N nilpotent. Notons Q le polynôme minimal de D. Il appartient à $\mathbf{K}[X]$ et est à racines simples dans $\overline{\mathbf{K}}$. Par la formule de Taylor

$$Q(A) = \overbrace{Q(D)}^{0} + Q'(D)N + Q^{[2]}(D)N^2 + \dots$$

est nilpotent. Ainsi le polynôme minimal P de A divise une puissance Q^m. Par ailleurs

$$P(D) = P(A - N) = \overbrace{P(A)}^{0} - P'(A)N + \dots$$

est nilpotent. Mais il est diagonalisable sur $\overline{\mathbf{K}}$ puisque D l'est. Il est donc identiquement nul, et par conséquent Q divise P. Ainsi le radical de P (calculé dans $\overline{\mathbf{K}}[X]$) est Q. Or ce dernier est par définition dans $\mathbf{K}[X]$.

Nous avons établi :

Théorème 9. *Le D de la décomposition de* Chevalley-Dunford *est défini sur $\mathbf{K}$ si et seulement si le radical calculé dans $\overline{\mathbf{K}}[X]$ du polynôme minimal de A est défini sur $\mathbf{K}$. C'est toujours le cas en caractéristique nulle (ou sur un corps parfait cf. page 19).*

8 Une approche simplifiée en caractéristique nulle

Je reprends l'étude de $\mathcal{A} = \mathbf{K}[X]/(P)$ en caractéristique nulle.

Comme il a déjà été dit, le polynôme réduit $Q \in \overline{\mathbf{K}}[X]$ est alors défini sur $\mathbf{K}$ automatiquement car donné par la formule $Q = P/S$ avec $S \coloneqq \text{pgcd}(P, P')$.

Théorème 10. *Le morphisme de* $\mathbf{K}$*-espaces vectoriels* $\psi : \mathcal{A} \mapsto \mathbf{K}[X]/(Q) \oplus \mathbf{K}[X]/(S)$ *qui envoie* T *sur* $(T \bmod Q, T' \bmod S)$ *est bien défini et est un isomorphisme (de* $\mathbf{K}$*-esp. vect.).*

Preuve. Si $T \in \mathbf{K}[X]$ est divisible par P, $T = PZ$, alors $T' = P'Z + PZ'$ est divisible par $\text{pgcd}(P, P')$, donc ψ est bien défini.

C'est un morphisme entre deux espaces vectoriels de la même dimension. Montrons qu'il est injectif donc un isomorphisme.

Si $\psi(T)$ est nul, alors $T(\lambda) = 0$ pour chaque racine λ de P (car ce sont les racines de Q). Notons j la multiplicité de λ comme racine de T, alors $j-1$ est sa multiplicité comme racine de T'. Mais S divise T', donc $j-1$ est au moins $m-1$ avec m la multiplicité de λ comme racine de P. Donc $j \geqslant m$. Par conséquent T est un multiple dans $\overline{\mathbf{K}}[X]$ de $(X-\lambda)^m$. Ainsi P divise T, dans $\overline{\mathbf{K}}$ donc dans $\mathbf{K}$. C.Q.F.D. □

Théorème 11. *Soit* $D = \psi^{-1}(X, 0)$*, et* $N = \psi^{-1}(0, 1)$*. Alors* $X = D + N$ *dans* $\mathcal{A}$*,* $DN = ND$*,* D *est semi-simple et* N *est nilpotent. L'algèbre engendrée par* D *est l'espace vectoriel* $\psi^{-1}(\mathbf{K}[X]/(Q) \oplus \{0\})$*. L'idéal des éléments nilpotents de* $\mathcal{A}$ *est* $\psi^{-1}(\{0\} \oplus \mathbf{K}[X]/(S))$*.*

Preuve. Tout d'abord il est clair que $\psi(X) = (X \bmod Q, 1 \bmod S)$ et donc $X = D + N$.

Comme $D' \equiv 0 \bmod S$, certainement $(D^k)' \equiv 0 \bmod S$ pour tout $k \geqslant 1$. Et ça marche aussi pour $k = 0$! Donc, pour tout polynôme T, on a $\psi(T(D)) = (T(D) \bmod Q, 0) = (T(X) \bmod Q, 0) = (T \bmod Q, 0)$. Cela prouve que l'algèbre engendrée par D est exactement $\psi^{-1}(\mathbf{K}[X]/(Q) \oplus \{0\})$.

Par construction $Q(D) = 0$ donc D est semi-simple. Évidemment $DN = ND$ puisque $\mathcal{A}$ est une algèbre commutative. Il reste à montrer que N est nilpotent.

Par construction $N \equiv 0 \bmod Q$. Donc $N(\lambda) = 0$ pour toute racine de P dans $\overline{\mathbf{K}}$. Notons m le maximum des multiplicités des racines de P, et considérons N^m. Il possède en λ une racine d'ordre au moins m donc sa dérivée (pour que cela n'ait pas d'ambiguïté on a fixé un représentant de N dans $\mathbf{K}[X]$) s'y annule au moins à l'ordre $m-1$, c'est-à-dire au moins autant que S. Donc S divise la dérivée de N^m, et cela prouve que $\psi(N^m) = 0$. Donc $N^m = 0$ dans $\mathcal{A}$. *Avec m choisi de sorte que P divise* Q^m*. (édité 29/04/17)*

Plus généralement, la même preuve montre que tout élément de $\psi^{-1}(\{0\} \oplus \mathbf{K}[X]/(S))$ est nilpotent dans $\mathcal{A}$. La réciproque est vraie, puisque $\mathbf{K}[X]/(Q)$ n'a pas d'éléments nilpotents non nuls. □

On note A l'endomorphisme de multiplication par X sur $\mathcal{A}$.

Théorème 12. *L'endomorphisme $T(A)$ est semi-simple si et seulement si T' est divisible par $S = \operatorname{pgcd}(P, P')$. Cela est le cas si et seulement si $T \bmod P$ est un polynôme en D.*

Preuve. Si T' est divisible par S, alors $T \bmod P$ est dans l'algèbre engendrée par D d'après le théorème précédent. Comme D est semi-simple, c'est le cas de $T(A)$ également.

Si $T(A)$ est semi-simple, il existe un polynôme Z à racines simples dans $\overline{\mathbf{K}}$ avec $Z(f_T)$ nul, f_T étant une autre notation pour $T(A)$, c'est-à-dire la multiplication par T dans $\mathcal{A}$. Mais $Z(f_T) = f_{Z(T)}$, donc $Z(T)$ est nul dans $\mathcal{A}$. Si on prend un représentant de T, cela veut dire que $Z(T)$ est divisible par P. Donc la dérivée $Z'(T)T'$ est divisible par S. Mais il y a une identité de Bézout $UZ + VZ' = 1$, et en substituant T cela donne que $V(T)Z'(T) \equiv 1 \mod P$ et donc a fortiori modulo S. Par conséquent S divise T', ce qu'il fallait démontrer. □

9 Conclusion (?)

D'après ce qui a été vu dans la section plus détaillée, on peut aussi reconnaître que $T(A)$ est semi-simple à la congruence $T \equiv T(D) \bmod P$, qui s'écrit de manière plus suggestive :

$$T = T(X) \equiv T(D+N) \overset{?}{\equiv} T(D) \pmod{P}$$

Mais « P divise $T(X) - T(D)$ » nécessite la connaissance de D. Par contre le critère (en caractéristique nulle)

$$T' \overset{?}{\equiv} 0 \bmod S$$

lui ne nécessite pas le calcul préalable de D. Et nous avons donné les congruences à utiliser pour la caractéristique positive.

Pour l'obtention concrète en caractéristique zéro de D par la résolution du système

$$D \equiv X \pmod{Q}$$
$$D' \equiv 0 \pmod{S}$$

voir mon article précédent :

http://jf.burnol.free.fr/agreg170414DunfordExplicite.pdf

En caractéristique positive nous avons donc également réussi dans le présent article à réduire le problème de la construction du D de Chevalley-Dunford à un système

linéaire défini sur $\mathbf{K}$ si Q_0 l'est :

$$\begin{aligned} D &\equiv X \pmod{Q_0} \\ D' &\equiv 0 \pmod{Q_1} \\ D^{[2]} &\equiv 0 \pmod{Q_2} \\ &\cdots\cdots \\ D^{[m-1]} &\equiv 0 \pmod{Q_{m-1}} \end{aligned}$$

Une fois connu Q_0 on a vu comment obtenir les Q_j par des calculs de pgcd. En caractéristique nulle, Q_0 s'obtient directement par $P/\mathrm{pgcd}(P,P')$.

On peut aussi remplacer tous les Q_i par Q_0 ce qui revient à travailler modulo Q_0^m, puis réduire à la fin modulo P.

On peut également examiner le système triangulaire rattachant les puissances de Q_0 avec celles de N afin d'écrire N « Q_0-adiquement », voir

http://jf.burnol.free.fr/agreg170413DunfordLineaire.pdf

mais je pense que je vais m'arrêter là.

29 avril 2017. Ben non, encore une petite chose à dire en caractéristique p. Je veux expliquer comment trouver algorithmiquement le radical Q d'un $P \in \mathbf{K}[X]$ unitaire, et une extension $\mathbf{K}'$ de $\mathbf{K}$ sur laquelle il est défini. En particulier nous allons voir que si $\mathbf{K}$ est *parfait*, c'est-à-dire si tout $x \in \mathbf{K}$ peut s'écrire y^p avec $y \in \mathbf{K}$ (c'est le cas pour les corps finis en particulier), alors Q est défini sur $\mathbf{K}$ comme c'est le cas en caractéristique nulle.

Considérons $P = \prod_i (X-\lambda_i)^{m_i}$. Il est clair que $S = \mathrm{pgcd}(P,P') = \prod_{i,p\nmid m_i}(X-\lambda_i)^{m_i-1}\prod_{i,p\mid m_i}(X-\lambda_i)^{m_i}$. Donc, le quotient $P_0 = P/S = \prod_{i,p\nmid m_i}(X-\lambda_i)$ est rationnel. Maintenant on peut (par exemple) calculer $\mathrm{pgcd}(P_0^N, S)$ avec N suffisamment grand (disons $N = \deg S$) et cela fournit le polynôme $R_0 = \prod_{i,p\nmid m_i}(X-\lambda_i)^{m_i-1}$ qui est donc lui aussi rationnel, et on a $P = P_0R_0T_1$ avec $T_1 \in \mathbf{K}[X]$, premier avec P_0, et qui est une puissance p-ième dans $\overline{\mathbf{K}}[X]$, donc est en fait dans $\mathbf{K}[X^p]$. Étendons si nécessaire $\mathbf{K}$ par les racines p-ièmes des coefficients de T_1 en un corps $\mathbf{K}_1$. Alors on peut écrire $T_1 = U_1^p$ avec $U_1 \in \mathbf{K}_1[X]$ et $\mathbf{K}_1^p \subset \mathbf{K}$. On recommence la procédure avec U_1, etc… En un nombre fini d'étapes on obtient un corps $\mathbf{K}_n$ et une factorisation $P = P_0R_0P_1^pR_1^pP_2^{p^2}R_2^{p^2}\dots P_n^{p^n}R_n^{p^n}$. Les P_j sont premiers deux à deux, à racines simples, et chaque R_j divise une puissance de P_j. Le radical Q de P est $P_0P_1\dots P_n$, et il est défini sur le corps $\mathbf{K}_n$ avec $\mathbf{K}_n^{p^n} \subset \mathbf{K}$. Notons que chaque $P_j^{p^j}$ et $R_j^{p^j}$ est en fait défini sur $\mathbf{K}$. Le produit $P_j^{p^j}R_j^{p^j}$ est la partie correspondant aux racines avec multiplicités m_i divisibles par p^j mais pas par p^{j+1}.

En particulier si $\mathbf{K}$ est parfait, l'algorithme prouve que le radical Q de P est défini sur $\mathbf{K}$ et donne un moyen effectif de l'obtenir. Il y a peut-être plus efficace, je n'y ai pas vraiment réfléchi et je voulais juste indiquer ce moyen de procéder algorithmiquement et la conséquence pour les corps parfaits. Une fois $Q_0 = Q$ obtenu, il ne faut pas recommencer toute la procédure avec P/Q_0, mais directement calculer Q_1 par la formule $\mathrm{pgcd}(Q_0, P/Q_0)$, puis Q_2 par $\mathrm{pgcd}(Q_1, P/(Q_0Q_1))$, etc… hmm en fait il faut faire ce genre de choses avec chaque morceau P_jR_j bien sûr et réunir l'information à la fin. (t.s.v.p.)

Voici une autre approche pour un corps fini $\mathbf{K} = \mathbf{F}_q$, $q = p^a$. On peut commencer par calculer tous les $Z_k = \mathrm{pgcd}(P, X^{q^k} - X)$, pour $1 \leqslant k \leqslant \deg P$. Ce sont des polynômes dans $\mathbf{K}[X]$ à racines simples dans $\overline{\mathbf{K}}$, et toute racine de P est racine d'un au moins des Z_k (car $\mathbf{K}$ a une unique extension de degré k, et elle consiste en les x avec $x^{q^k} = x$…). Donc le radical est donné par la formule $Q = \mathrm{ppcm}(Z_1, Z_2, \ldots, Z_{\deg P})$ (il est idiot de laisser Z_1 si on a Z_2, et Z_2 si on a Z_4 ou Z_6, etc…, mais après ça devient un peu compliqué de toute façon). Je suppose qu'il me suffirait d'ouvrir un livre sur les corps finis pour voir comment les gens qui ont réfléchi procèdent. Car cette formule me semble totalement, absolument, inefficace en comparaison avec l'autre algorithme, mais ça donne au moins un argument théorique assez simple pour la rationalité de Q. En fait cette méthode n'est pas bien différente en esprit de celle qui consisterait à tester tous les λ raisonnables et de voir si ce sont des racines… donc ça dépend un peu déjà de comment $\mathbf{K}$ est réalisé concrètement.

Une autre approche générale, un peu semblable, s'applique comme corrélat de tout algorithme trouvant les composantes irréductibles de P sur $\mathbf{K}$. Car cela ramène alors la question à P irréductible et à regarder s'il est un polynôme en X^p.