L'ALGÈBRE DES SUITES RÉCURRENTES LINÉAIRES

JEAN-FRANÇOIS BURNOL ET OLIVIER SERMAN

Résumé. On aborde (en toute caractéristique) la théorie de l'équation récurrente linéaire sur un corps du point de vue de la théorie des endomorphismes : dualité, lemme des noyaux, endomorphismes cycliques...

Table des matières

1. Introduction

Soit K un corps.

Soit r un entier strictement positif, $(a_0,\dots,a_{r-1}) \in \mathrm{K}^r$ ainsi que $a_r \in \mathrm{K}\setminus\{0\}$, et considérons les conditions suivantes portant sur une suite $(u_i) \in \mathcal{S} = \mathrm{K}^{\mathbb{N}}$:

$$(\mathrm{E}_n) \qquad a_r u_{n+r} = a_{r-1}u_{n+r-1} + \cdots + a_1 u_{n+1} + a_0 u_n$$

Ce sont des conditions linéaires. On peut en divisant par a_r toujours se ramener au cas $a_r = 1$. Dorénavant nous considérons que cette réduction a été faite et donc que $a_r = 1$.

Le sous-ensemble $\mathrm{V} \subset \mathcal{S}$ des suites (u_i) qui vérifient toutes les E_n, $n \in \mathbb{N}$, est un sous-espace vectoriel de $\mathcal{S}$.

Le premier résultat important est évidemment :

Théorème 1. *Le morphisme* $\psi : \mathrm{V} \to \mathrm{K}^r$ *défini par* $\psi((u_i)) = (u_0, u_1, \dots, u_{r-1})$ *est un isomorphisme et par conséquent* V *est de dimension finie égale à* r.

Dans ce texte nous en donnerons deux démonstrations différentes :

(1) par un Théorème de structure 2 qui fait intervenir d'emblée la notion de dualité et qui est le résultat principal du point de vue algébrique,

(2) par l'approche plus usuelle via le principe de récurrence pour expliquer que chaque « condition initiale » $(u_0, u_1, \dots, u_{r-1})$ détermine une et une seule solution.

Nous présentons en premier le théorème de structure, puis re-débutons à zéro en établissant le Théorème 1 avec une preuve utilisant le principe de récurrence de manière attendue.

Date: 28 octobre 2019.

2. Théorème de structure principal

On associe aux coefficients de la récurrence le polynôme

$$P = a_r X^r - a_{r-1} X^{r-1} - \cdots - a_1 X - a_0 \,. \tag{1}$$

Comme $a_r = 1$ a été fixé à la valeur 1, il s'agit donc d'un polynôme unitaire.

Son introduction à ce stade n'est pas encore motivée, si ce n'est peut-être par l'observation (dont il faut avoir l'idée) qu'une suite (λ^n) est solution des (E_n), $n \in \mathbb{N}$, si et seulement si $P(\lambda) = 0$. On notera ici et par la suite $V(P) \subset \mathcal{S}$ l'espace vectoriel des suites vérifiant les récurrences (E_n) associées aux coeffficients du polynôme (unitaire) P.

Théorème 2 (Théorème principal)**.** *Soit* P *unitaire de degré r.*

Pour toute forme linéaire f sur K[X] *la suite $\theta(f) = (u_n)_{n\in\mathbb{N}}$ définie par les formules*

$$u_n = f(X^n) \tag{2}$$

est dans V(P) *si et seulement si f s'annule identiquement sur l'idéal* (P).

Toute suite x de V(P) *(i.e. $x \in \mathcal{S}$ est solution de la récurrence associée à* P*) est de la forme $x = \theta(f)$ pour une forme linéaire sur* K[X] *s'annulant sur l'idéal* (P) *et qui est unique.*

Les formules (2)*, avec cette fois-ci $f \in (K[X]/(P))^*$ établissent un isomorphisme du dual de* K[X]/(P) *vers* V(P).

Preuve. La première remarque à faire est que l'espace vectoriel $K[X]^*$ dual de K[X] est canoniquement isomorphe avec l'espace des suites $\mathcal{S}$ via l'association à tout $f \in K[X]^*$ de la suite $\theta(f) = (f(X^n))$.

En effet $f \in K[X]^*$ est déterminée par les $u_n = f(X^n)$ et il n'y a aucune contrainte sur les u_n : pour chaque suite (u_n) il existe une et une seule forme linéaire f sur K[X] telle que $\forall n, f(X^n) = u_n$. Si l'on veut vraiment la formule : $f(\sum_j b_j X^j) = \sum_j b_j u_j$.

Autrement dit l'espace des suites $\mathcal{S}$ est canoniquement le dual de l'espace vectoriel K[X].

Pour $x \in \mathcal{S}$ et f la forme linéaire qui lui correspond l'équation (E_n) est simplement $f(X^n P) = 0$. Donc $x \in V(P)$ si et seulement si f s'annule sur l'idéal (P).

Ce qui signifie qu'en posant $W(P) = \{f \in K[X]^*, f \text{ nulle sur } (P)\}$ la restriction de θ à W(P) établit un isomorphisme de W(P) vers V(P) (on sait que θ donc $\theta\big|_{W(P)}$ est injective et on a identifié son image).

Le passage au dual de la surjection canonique $K[X] \to K[X]/(P)$ donne une injection canonique $\imath : (K[X]/(P))^* \to K[X]^*$ dont l'image est précisément W(P). Par abus de notation (restriction de l'image) on dit donc que $\imath$ est un isomorphisme de $(K[X]/(P))^*$ avec W(P).

On obtient donc par les formules (2) l'isomorphisme de $(K[X]/(P))^*$ avec V(P) annoncé par l'énoncé. □

Corollaire 3 (c'est le Théorème 1)**.** *L'espace vectoriel* V(P) *est de dimension* deg P *et l'application $\psi : V(P) \to K^r$ qui ne retient que les r premiers coefficients est un isomorphisme.*

Preuve. Les monômes $(1, X, \ldots, X^{r-1})$ forment une base de l'espace quotient K[X]/(P) donc le morphisme de son dual vers K^r défini par $\phi(L) = (L(1), L(X), \ldots, L(X^{r-1}))$ est un isomorphisme.

On constate (on utilise les notations de la preuve précédente) que $\phi = \psi \circ \theta\big|_{W(P)} \circ \imath$ et tous les morphismes dans cette identité sauf peut-être ψ étant des isomorphismes, il en résulte que ψ est un isomorphisme. □

3. Approche via l'étude des polynômes d'endomorphisme en le décalage

On va recommencer à zéro, par une approche plus terre-à-terre.

Preuve directe du Théorème 1. Soit $(u_0, u_1, \dots, u_{r-1}) \in \mathrm{K}^r$ donné. On va montrer par récurrence sur $j \geqslant 0$ l'assertion $\mathcal{H}_j$ suivante : *il existe un choix unique de u_k pour $r \leqslant k < r + j$ tel que les équations (E_k) sont vraies pour $k < j$.*

$\mathcal{H}_0$ est vraie. Supposons $\mathcal{H}_j$ et montrons $\mathcal{H}_{j+1}$. On cherche u_r, u_{r+1}, …, u_{r+j} tels que (E_k) est vrai pour $k \leqslant j$. Par l'hypothèse de récurrence c'est possible de manière unique en ce qui concerne le choix de u_r, u_{r+1}, …, u_{r+j-1}. Il ne reste qu'à imposer que (E_j) soit vraie, ce qui est possible et de manière unique en prenant

$$u_{j+r} = a_{r-1} u_{j+r-1} + \cdots + a_1 u_{j+1} + a_0 u_j \ .$$

Donc $\mathcal{H}_{j+1}$ est vrai.

Les j-uplets $(u_r, \dots, u_{r+j-1})$ fournis par les $\mathcal{H}_j$ sont, par unicité, les tronçons successifs d'une même suite $(u_r, u_{r+1}, \dots)$ et la suite complète $(u_k)_{k \in \mathbb{N}}$ vérifie toutes les récurrences (E_j), $j \in \mathbb{N}$. De plus par $\mathcal{H}_j$, u_{r+j} est uniquement déterminé pour tout $j \geqslant 0$. Et ainsi ψ est surjectif et injectif. □

Nous définissons sur l'espace des suites $\mathcal{S}$ un endomorphisme S :

$$\mathrm{S}((u_n)) = (u_{n+1})_{n \in \mathbb{N}} \tag{3}$$

Les itérés S^k de S agissent par $\mathrm{S}^k((u_n)) = (u_{n+k})$.

Nous associons à la récurrence le morphisme

$$a_r \mathrm{S}^r - a_{r-1} \mathrm{S}^{r-1} - \cdots - a_1 \mathrm{S} - a_0 \,\mathrm{Id}$$

qui envoie la suite (u_n) sur la suite (v_n) avec

$$\forall n \in \mathbb{N} \quad v_n = a_r u_{n+r} - a_{r-1} u_{n+r-1} - \cdots - a_1 u_{n+1} - a_0 u_n \ .$$

Ainsi l'espace vectoriel V des solutions de la récurrence linéaire est simplement le noyau de ce morphisme.

La notion de polynôme d'endomorphisme est utile dans ce contexte : le morphisme ci-dessus est P(S) avec $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ le polynôme associé aux coefficients de la récurrence.

$$\mathrm{P} = a_r \mathrm{X}^r - a_{r-1} \mathrm{X}^{r-1} - \cdots - a_1 \mathrm{X} - a_0 \ . \tag{4}$$

Et ainsi :

$$\boxed{\mathrm{V} = \mathrm{Ker}\,\mathrm{P(S)}} \tag{5}$$

Soit donc P unitaire et $\mathrm{V} = \mathrm{Ker}\,\mathrm{P(S)}$. On a $\mathrm{S(V)} \subset \mathrm{V}$ (car S commute avec P(S)...). Notons T la restriction de S à V.

Par ailleurs on note $\mathrm{L}_j \in \mathcal{S}^*$ les formes linéaires $\mathrm{L}_j((u_n)) = u_j$, et, pour éviter des confusions, ℓ_j leurs restrictions à $\mathrm{V} = \mathrm{Ker}\,\mathrm{P(S)}$, qui sont donc des éléments du dual de V.

On a bien sûr $\mathrm{L}_0(\mathrm{S}^n(x)) = \mathrm{L}_n(x)$, soit encore $\mathrm{L}_n = (\mathrm{S}^*)^n \mathrm{L}_0$, puis par restriction $\boxed{\ell_n = (\mathrm{T}^*)^n \ell_0}$.

Théorème 4. *Les r formes linéaires $\ell_0, \ell_1, \dots, \ell_{r-1}$ forment une base de* V^*.

Preuve. On a l'isomorphisme $\psi : \mathrm{V} \to \mathrm{K}^r$ qui envoie la suite $x = (u_n)$ sur le r-uplet $(u_0, \dots, u_{r-1})$. Notons $(e_0, \dots, e_{r-1})$ la base canonique de K^n et $(f_0, \dots, f_{r-1})$ la base duale de $(\mathrm{K}^n)^*$. Par définition de ces bases $\psi^*(f_j) = \ell_j$ pour $j = 0, \dots, r-1$. Or ψ^* est aussi un isomorphisme d'où l'énoncé. □

Nous écrivons maintenant la matrice de T^* dans cette base. Pour cela il nous faut calculer $T^*(\ell_{r-1}) = \ell_r$. Mais pour tout $x = (u_n)$ dans V on a par définition

$$u_r = a_{r-1}u_{r-1} + \cdots + a_1u_1 + a_0u_0$$

ce qui s'écrit aussi

$$\ell_r(x) = a_{r-1}\ell_{r-1}(x) + \cdots + a_0\ell_0(x)$$

Comme $x \in V$ est arbitraire cela donne la relation recherchée et la matrice $\mathcal{C}$ de l'action de T^* exprimée dans la base $(\ell_0, \ell_1, \ldots, \ell_{r-1})$:

$$\mathcal{C} = \begin{pmatrix} 0 & 0 & 0 & \ldots & \ldots & a_0 \\ 1 & 0 & 0 & \ldots & \ldots & a_1 \\ 0 & 1 & 0 & \ldots & \ldots & a_2 \\ 0 & \ddots & \ddots & \ddots & \ldots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 & a_{r-2} \\ 0 & 0 & \ldots & 0 & 1 & a_{r-1} \end{pmatrix} \tag{6}$$

Nous reconnaissons la matrice « compagnon » du polynôme unitaire $P = X^r - a_{r-1}X^{r-1} - \cdots - a_0$, c'est-à-dire la matrice de la multiplication par X sur K[X]/(P) dans la base canonique $(1, X, X^2, \ldots, X^{r-1})$ des monômes.

À ce stade nous avons découvert que le *dual* de V(P) = Ker P(S) (muni de l'endomorphisme T) est isomorphe à l'espace quotient K[X]/(P) (muni de la multiplication par X). Il n'est pas encore très clair en quoi cet isomorphisme est intrinsèque puisque nous avons pour l'obtenir utilisé une base spécifique $(\ell_0, \ell_1, \ldots, \ell_{r-1})$ de $V(P)^*$ et une base spécifique $(1, X, \ldots, X^{r-1})$ de K[X]/(P).

En dualisant (théorème du double-dual en dimension finie) nous obtenons l'existence d'un isomorphisme de V(P) avec le *dual* de K[X]/(P). C'est ce que disait déjà le Théorème 2, mais lui de manière intrinsèque, sans faire appel à des bases particulières (sinon l'énoncé est juste une égalité de dimensions).

La suite du texte poursuit l'étude de V(P) muni de l'action de T jusqu'à obtenir (lorsque P est scindé) une base remarquable de solutions particulières de la récurrence définie par P. En cherchant à mieux comprendre leur structure nous finirons avec beaucoup de retard à l'allumage par trouver à nouveau que V(P) = Ker P(S) est intrinsèquement le dual de K[X]/(P).

Théorème 5. *Pour tout* P *unitaire,* P *est le polynôme caractéristique* $\det(X\,\mathrm{Id} - T)$ *de la restriction* T *de* S *à* Ker P(S).

Preuve. En effet T a même polynôme caractéristique que son dual T^* et c'est un fait connu que nous ne redémontrons pas que le polynôme caractéristique d'une matrice compagnon est le polynôme unitaire associé à la matrice. □

On désignera donc P comme étant le « polynôme caractéristique » de la récurrence linéaire.

4. Polynôme caractéristique scindé

Nous allons maintenant faire l'hypothèse suivante :

Le polynôme caractéristique $P \in K[X]$ *est* K-*scindé.*

Ce qui incite à évoquer de suite le fameux :

Théorème 6 (Lemme des noyaux)**.** *Soit* E *un espace vectoriel sur un corps* K*,* f *un endomorphisme de* E*,* $P = P_1 \ldots P_d$ *un produit de polynômes de* K[X] *deux-à-deux premiers entre eux. Alors* Ker P(f) *est la somme directe des* Ker $P_i(f)$*. De plus la projection* *de* $\operatorname{Ker} P(f)$ *sur* $\operatorname{Ker} P_i(f)$ *parallèlement à la somme des* $\operatorname{Ker} P_j(f)$, $j \neq i$ *est un polynôme d'endomorphisme en la restriction de* f *à* $\operatorname{Ker} P(f)$.

Remarque 1. Aucun des espaces vectoriels considérés dans la proposition précédente n'est supposé de dimension finie.

Preuve. La preuve est laissée au lecteur comme énoncé extrêmement classique qu'il faut savoir démontrer. **Et** qu'il faut savoir appliquer concrètement ce qui nécessite de savoir exploiter les outils de sa démonstration.

Toute cette discussion est très liée au théorème des restes chinois et aussi par exemple à la décomposition des fractions rationnelles en éléments simples. □

Nous appliquons le Lemme des noyaux à notre espace des suites $\mathcal{S}$ et à son endomorphisme S.

Corollaire 7. *Soit* $P \in K[X]$ *polynôme unitaire, produit de polynômes unitaires* $P_1, \dots, P_d$, *qui sont deux-à-deux premiers entre eux. Alors l'espace vectoriel* $V(P)$ *de dimension* $\deg P$ *des solutions de la récurrence définie par* P *est la somme directe des espaces de dimensions* $\deg P_i$ *associés respectivement aux récurrences définies par les* P_i.

Remarque 2. Dans la première rédaction de ce texte l'isomorphisme entre $V(P)^*$ et $K[X]/(P)$ n'était évoqué qu'après. Comme ici nous l'avons déjà mentionné, nous pourrions nous contenter du théorème des restes chinois pour $K[X]/(P)$, mais au prix de devoir dualiser encore à la fin. Donc on ne s'est pas compliqué la tâche et on a recouru directement au Lemme des noyaux (qui de toute façon est généralement prouvé assez directement comme conséquence du mécanisme sous-jacent au théorème des restes chinois).

Soit donc pour P scindé $\lambda_1, \dots, \lambda_p$ les racines de P et $m_1, \dots, m_p$ leurs multiplicités. L'espace $V(P) = \operatorname{Ker} P(S)$ est, par le lemme des noyaux, la somme directe des espaces $V_i = \operatorname{Ker}(S - \lambda_i \operatorname{Id})^{m_i}$.

Choisissons une valeur propre λ_i particulière. Nous savons que $\dim V_i = m_i$ et que $\operatorname{Ker}(S - \lambda_i \operatorname{Id})^{m_i - 1}$ est de dimension $m_i - 1$. Donc la restriction T_i de S à V_i est telle que $T_i - \lambda_i \operatorname{Id}$ est nilpotent d'ordre exactement m_i. C'est donc aussi le cas de l'adjoint $T_i^* - \lambda_i \operatorname{Id}$ agissant sur V_i^*.

Remarque 3. Plus précisément nous savons par la discussion de la matrice compagnon que cette action est isomorphe à la multiplication par $X - \lambda_i$ sur l'espace quotient $K[X]/(X - \lambda_i)^{m_i}$. En utilisant la base $((X - \lambda_i)^{m_i - 1}, (X - \lambda_i)^{m_i - 2}, \dots, X - \lambda_i, 1)$, on constate que la matrice du morphisme de multiplication par $X - \lambda_i$ est un unique bloc de Jordan (supérieur) de taille $m_i \times m_i$.

Par abus de notation les ℓ_n désigneront dans la discussion de ce paragraphe et du suivant les restrictions des formes linéaires L_n de $\mathcal{S}$ à l'espace V_i considéré. Ainsi $\ell_n = (T_i^*)^n \ell_0$.

On en arrive au calcul fondamental, qui utilise l'opérateur nilpotent $T_i^* - \lambda_i \operatorname{Id}$ que nous notons N_i^*.

$$\ell_n = (T_i^*)^n(\ell_0) = (\lambda_i \operatorname{Id} + N_i^*)^n \ell_0 = \sum_{k < m_i, k \leqslant n} \binom{n}{k} \lambda_i^{n-k} (N_i^*)^k (\ell_0) \tag{7}$$

Considérons maintenant les éléments $x(\lambda, k) = (x_n(\lambda, k))_{n \in \mathbb{N}}$ définis par les formules suivantes :

$$x_n(\lambda, k) = \begin{cases} 0 & n < k \\ \binom{n}{k} \lambda^{n-k} & n \geqslant k \end{cases} \tag{8}$$

En appliquant l'équation (7) à un $x_i \in V_i$ quelconque, et en rappelant que $x_i = (\ell_n(x_i))_{n\in\mathbb{N}}$, on obtient, pour certains éléments $\alpha_k(x_i) = (N_i^*)^k(\ell_0)(x_i)$ de K dépendant linéairement de $x_i \in V_i$:

$$x_i = \alpha_0(x_i)\cdot x(\lambda_i, 0) + \alpha_1(x_i)\cdot x(\lambda_i, 1) + \cdots + \alpha_{m_i-1}(x_i)\cdot x(\lambda_i, m_i-1)\,. \tag{9}$$

Par conséquent nous obtenons l'inclusion de K-espaces vectoriels :

$$V_i \subset W_i = \mathrm{Vect}_K(x(\lambda_i,0), x(\lambda_i,1), \dots, x(\lambda_i, m_i-1)) \tag{10}$$

Mais V_i est de dimension m_i et W_i est de dimension au plus m_i. Donc en fait $V_i = W_i$, et il résulte (cela n'avait pas encore été établi !) que les $x(\lambda_i, k) \in \mathcal{S}, k < m_i$ sont en fait dans V_i ; et aussi qu'ils en forment une base.

Remarque 4. Une fois que l'on sait que les suites $x(\lambda_i, k)$, $0 \leqslant k < m_i$, sont dans V_i, le fait qu'elles forment une base se voit aussi sur le fait que la matrice de leurs m_i premiers coefficients est triangulaire supérieure à diagonale unité.

Ces dernières conclusions sont suffisamment remarquables pour qu'on les énonce explicitement à nouveau :

Théorème 8. *La suite $x(\lambda, k)$ (pour $\lambda \in K$, $k \in \mathbb{N}$) définie par les coefficients $x_n(\lambda, k) = \binom{n}{k}\lambda^{n-k}$ (avec par convention $\binom{n}{k}\lambda^{n-k} = 0$ pour $n < k$, même si $\lambda = 0$) vérifie la récurrence linéaire d'ordre $k+1$ associée au polynôme $(X-\lambda)^{k+1}$. Plus précisément $x(\lambda, k)$ vérifie la récurrence associée à $(X-\lambda)^q$ si et seulement si $q \geqslant k+1$.*

Si l'on prend plusieurs telles suites associées à des λ et/ou à des k différents, elles sont linéairement indépendantes.

Lorsque le polynôme caractéristique P d'une récurrence linéaire est scindé, l'espace $V(P) = \mathrm{Ker}\,P(S)$ des solutions de la récurrence a une base dont les éléments sont les $x(\lambda, k)$ avec λ parcourant les racines de P et k prenant les valeurs positives entières strictement inférieures à la multiplicité associée à λ.

Preuve. Tout a été essentiellement prouvé déjà. On sait déjà que $(x(\lambda,0), x(\lambda,1), \dots, x(\lambda, k-1))$ est une base de l'espace $\mathrm{Ker}(S-\lambda\,\mathrm{Id})^k$ et cela permet d'obtenir sans calcul les assertions du premier paragraphe de l'énoncé ; le lemme du noyau donne alors celle du second paragraphe. □

Remarque 5. Précisons que pour $\lambda = 0$, le seul élément non nul de la suite $x(0,k)$ est $u_k = 1$, autrement dit $x_n(0,k) = \delta_{n,k}$.

À ce stade nous avons trouvé une certaine base explicite de $V(P) = \mathrm{Ker}\,P(S)$. Nous avons aussi vu qu'il y a un isomorphisme du dual $V(P)^*$ avec $K[X]/(P)$.

Chaque $x(\lambda,k)$ ($P(\lambda) = 0$, $k < m_\lambda$) est un élément de $V(P)$ et définit donc une forme linéaire sur son dual $V(P)^*$, donc sur $K[X]/(P)$, donc aussi une forme linéaire sur $K[X]$ nulle sur l'idéal (P). Peut-on démêler l'écheveau et identifier concrètement cette forme linéaire $f_{\lambda,k}$ sur $K[X]$?

Tout d'abord, il y a une subtilité : il faut noter à ce stade $f_{\lambda,k,P}$ car ne sait pas encore avant de regarder de plus près si $f_{\lambda,k,P}$ dépend ou non du choix de P ayant λ comme racine de multiplicité au moins $k+1$.

Commençons par énoncer quelques propriétés de la forme linéaire $f_{\lambda,k,P}$ sur $K[X]$:

(1) $f_{\lambda,k,P}(X^i) = 0$ pour $i < k$,

(2) $f_{\lambda,k,P}(X^i) = \binom{i}{k}\lambda^{i-k}$ pour $k \leqslant i < \deg P$,

(3) $f_{\lambda,k,P}(A) = 0$ si P divise A.

Le point (3) est par définition de $f_{\lambda,k,P}$ qui est défini comme le « lift » d'une forme linéaire, notons-là L, sur $K[X]/(P)$.

Vérifions (1) et (2). Il faut donc calculer les $L(X^i)$ pour $0 \leqslant i < r = \deg P$. Rappelons que notre isomorphisme de $V(P)^*$ avec $K[X]/(P)$ est celui qui identifie la base $(\ell_0, \dots, \ell_{r-1})$ du premier avec la base $(1, X, \dots, X^{r-1})$ du second. En passant au dual, cela signifie que la contrainte est que $\ell_i(x(\lambda,k))$ est égal à $L(X^i)$ pour $0 \leqslant i < r$. D'où les formules (1) et (2).

Ces conditions déterminent $f_{\lambda,k,P}$ uniquement puisque tout polynôme U est par division euclidienne la somme d'un polynôme PQ et d'un reste V qui est une somme de monômes de degrés strictement inférieurs à celui de P.

Théorème 9. *Soit $\lambda \in K$ quelconque. Considérons les formes linéaires sur $K[X]$ définies par le développement suivant, valable (et fini...) pour tout polynôme A :*

$$A(\lambda + X) = f_{\lambda,0}(A) + f_{\lambda,1}(A)X + f_{\lambda,2}(A)X^2 + f_{\lambda,3}(A)X^3 + \dots . \tag{11}$$

Ainsi $f_{\lambda,0}(A) = A(\lambda)$, $f_{\lambda,1}(A) = A'(\lambda)$, $f_{\lambda,2}(A) = \frac{1}{2}A''(\lambda)$ en caractéristique distincte de 2, $f_{\lambda,3}(A) = \frac{1}{6}A'''(\lambda)$ en caractéristique distincte de 2 et de 3, etc...

Alors pour tout polynôme (unitaire) P divisible par $(X-\lambda)^{k+1}$, on a $f_{\lambda,k,P} = f_{\lambda,k}$.

Preuve. Nous allons montrer que $f_{\lambda,k}$ vérifie les trois conditions suivantes qui sont plus strictes que celles contraignant $f_{\lambda,k,P}$.

(1) $f_{\lambda,k}(X^i) = 0$ pour $i < k$,

(2) $f_{\lambda,k}(X^i) = \binom{i}{k}\lambda^{i-k}$ pour $k \leqslant i$,

(3) $f_{\lambda,k}(A) = 0$ si $(X-\lambda)^{k+1}$ divise A.

En effet par définition $f_{\lambda,k}(X^i)$ est le coefficient de X^k dans le développement de $(\lambda + X)^i$. Ce coefficient est donc nul pour $k > i$ et égal à $\binom{i}{k}\lambda^{i-k}$ pour $k \leqslant i$. Cela établit (1) et (2). Si $(X-\lambda)^{k+1}$ divise A alors X^{k+1} divise $A(\lambda+X)$ et donc le coefficient de X^k dans le développement de $A(\lambda + X)$ est nul. Ce qui établit (3). □

Nous avons identifié intrinsèquement nos formes linéaires, et même très explicitement en caractéristique nulle via les dérivées itérées divisées par des factorielles. Pour avoir un formalisme concret qui marche bien en toute caractéristique, on va faire appel à la notion de résidu.

Proposition 10. *La forme linéaire $f_{\lambda,k} \in K[X]^*$ associée à $x(\lambda,k) \in \mathcal{S}$ vérifie la formule*

$$\forall A \in K[X] \quad f_{\lambda,k}(A) = \operatorname{Res}_\lambda \frac{A}{(X-\lambda)^{k+1}} \tag{12}$$

Preuve. En effet, l'équation 11 est aussi de manière équivalente (somme finie !) :

$$A = f_{\lambda,0}(A) + f_{\lambda,1}(A)(X-\lambda) + f_{\lambda,2}(A)(X-\lambda)^2 + f_{\lambda,3}(A)(X-\lambda)^3 + \dots \tag{13}$$

et le résultat en découle par définition (et/ou) propriétés de $\operatorname{Res}_\lambda$. □

Nous voyons que nos suites $x(\lambda,k)$ donnant les solutions fondamentales aux récurrences linéaires sont aussi obtenues par ces formules relativement inquiétantes :

$$x(\lambda,k) = (\operatorname{Res}_\lambda \frac{X^n}{(X-\lambda)^{k+1}})_{n\in\mathbb{N}} \tag{14}$$

Bien qu'elles soient inquiétantes ces formules ont néanmoins la structure générale annoncée par le Théorème 2. Si on ne l'avait pas déjà fait on pourrait donc découvrir ici l'énoncé Théorème 2 et en faire la démonstration.

Nous avons choisi d'énoncer le Théorème 2 dès le début, mais de ne pas l'utiliser. Ceci afin d'expliquer comment on peut le découvrir comme un développement logique de la théorie algébrique des suites récurrentes linéaires, même sans posséder le don de divination. Par la suite le Théorème 2 est supposé acquis.

5. Récurrence régulière

La récurrence associée aux coefficients de $P \in K[X]$ (unitaire) est dite régulière si $P(0) \neq 0$.

Théorème 11. *Les conditions suivantes sur* P *unitaire de degré* r *sont équivalentes :*

(1) la récurrence de polynôme caractéristique P *est régulière,*

(2) pour tout entier j*, le morphisme* $\psi_j((u_n)) = (u_j, \dots, u_{j+r-1})$ *est un isomorphisme de* $\operatorname{Ker} P(S)$ *avec* K^r*.*

(3) le morphisme $\psi_1((u_n)) = (u_1, \dots, u_r)$ *est un isomorphisme de* $\operatorname{Ker} P(S)$ *avec* K^r*.*

(4) la restriction T *de* S *à* $\operatorname{Ker} P(S)$ *est un isomorphisme.*

Preuve. Supposons $P(0) \neq 0$. On sait que ψ_0 est un isomorphisme. Soit $j \geqslant 1$ tel que ψ_j n'est pas injectif. Alors il existe un élément $(u_n) \in V = \operatorname{Ker} P(S)$ non nul tel que $u_j = \dots = u_{j+r-1} = 0$. Comme $\psi_0(S^j((u_n))) = 0$ on a $S^j((u_n)) = 0$, c'est-à-dire $u_k = 0$ pour $k \geqslant j$. Comme (u_n) n'est pas la suite nulle, il existe un plus grand indice k tel que $u_k \neq 0$. En utilisant l'équation (E_k) et le fait que $P(0) \neq 0$ on obtient la contradiction $u_k = 0$. Donc ψ_j est injectif et par conséquent un isomorphisme en comparant les dimensions.

Donc (1) $\implies$ (2). (2) $\implies$ (3) est trivial, montrons (3) $\implies$ (1). On montre la contraposée : supposons $P(0) = 0$. La suite $x = (1, 0, 0, \dots)$ est automatiquement dans $\operatorname{Ker} P(S)$. Mais $\psi_1(x) = 0$ et ψ_1 par conséquent n'est pas un isomorphisme.

Finalement (4) équivaut à ce que 0 ne soit pas dans le spectre de T, soit encore à $\det T \neq 0$ mais $\det T = P(0)$. Donc (4) $\iff$ (1). □

6. Caractéristique nulle

Pour le moment la caractéristique reste générale.

Considérons les opérateurs différentiels $D_n = X^n (\frac{d}{dX})^n$, agissant sur $K[X]$. On va commencer par le lemme suivant :

Proposition 12. *Il existe des entiers* $t(n, j)$, $1 \leqslant j \leqslant n$ *tels que*

$$D_1^n = t(n,n) D_n + t(n, n-1) D_{n-1} + t(n, n-2) D_{n-2} + \dots + t(n, 1) X \frac{d}{dX} \tag{15}$$

et de plus $t(n,n) = t(n,1) = 1$.

Preuve. Par récurrence. L'énoncé est vrai pour $n = 1$, supposons-le vrai pour n et dérivons, pour tout polynôme A donné, l'identité de l'hypothèse de récurrence, en appliquant la règle de Leibniz :

$$\begin{aligned}
D_1^n(A) &= X^n A^{(n)} + t(n, n-1) X^{n-1} A^{(n-1)} + t(n, n-2) X^{n-2} A^{(n-2)} + \dots + XA' \\
D_1^{n+1}(A) &= X^{n+1} A^{(n+1)} + n X^n A^{(n)} + t(n, n-1) X^n A^{(n)} + t(n, n-1)(n-1) X^{n-1} A^{(n-1)} \\
&\quad + t(n, n-2) X^{n-1} A^{(n-1)} + t(n, n-2)(n-2) X^{n-2} A^{(n-2)} + \dots + X^2 A'' + XA' \\
D_1^{n+1}(A) &= X^{n+1} A^{(n+1)} + (n + t(n, n-1)) X^n A^{(n)} \\
&\quad + (t(n, n-1)(n-1) + t(n, n-2)) X^{n-1} A^{(n-1)} + \dots + XA'
\end{aligned}$$

d'où le résultat. □

On a donc un système triangulaire à coefficients entiers, avec diagonale identité pour passer des $X^j (\frac{d}{dX})^j$, $n \geqslant j \geqslant 1$, aux $(X \frac{d}{dX})^j$, $n \geqslant j \geqslant 1$, et vice versa. D'où :

Corollaire 13. *Soit* $\lambda \in K$*. Les formes linéaires sur* $K[X]$ *définies par les formules* $A \mapsto D_1^j(A)(\lambda)$, $1 \leqslant j \leqslant n$*, engendrent le même espace vectoriel que les formes linéaires* $A \mapsto \lambda^j A^{(j)}(\lambda)$, $1 \leqslant j \leqslant n$*.*

Supposons dorénavant que K est de caractéristique nulle. Dans ce cas les formes linéaires $f_{\lambda,k} \in \mathrm{K}[\mathrm{X}]^*$ considérées précédemment dans le Théorème 9 (et qui correspondent aux $x(\lambda,k) \in \mathcal{S}$ par l'isomorphisme $\theta : \mathrm{K}[\mathrm{X}]^* \to \mathcal{S}$) sont simplement

$$\mathrm{A} \mapsto f_{\lambda,k} = \mathrm{A}^{(k)}(\lambda)/k!$$

Elles engendrent donc par le corollaire qui précède, pour $1 \leqslant k < m$ *et lorsque* λ *est non nul*, le même espace vectoriel que les formes linéaires $g(\lambda,k)(\mathrm{A}) = \mathrm{D}_1^k(\mathrm{A})(\lambda)$, $1 \leqslant k < m$.

La suite $y(\lambda,k) = (y_n(\lambda,k))_{n\in\mathbb{N}}$ associée à la forme linéaire $g(\lambda,k)$ est donnée par les formules :

$$y_n(\lambda,k) = g(\lambda,k)(\mathrm{X}^n) = \mathrm{D}_1^k(\mathrm{X}^n)(\lambda) = n^k\lambda^n \tag{16}$$

Les suites $y(\lambda,k)$, $1 \leqslant k < m$ engendrent par ce qui précède le même espace vectoriel que les suites $x(\lambda,k)$, $1 \leqslant k < m$. Cela reste évidemment vrai en incluant aussi $k = 0$, en définissant $y(\lambda,0) = x(\lambda,0) = (\lambda^n)_{n\in\mathbb{N}}$.

Nous pouvons donc terminer par l'énoncé classique :

Théorème 14. *Soit* K *un corps* de caractéristique nulle *et* $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ *un polynôme unitaire scindé sur* K, *vérifiant* $\mathrm{P}(0) \neq 0$. *L'espace vectoriel* $\mathrm{V}(\mathrm{P}) = \operatorname{Ker}\mathrm{P}(\mathrm{S})$ *des suites solutions de la récurrence régulière définie par* P *a une base composée des solutions particulières*

$$y(\lambda,k) = (n^k\lambda^n)_{n\in\mathbb{N}}$$

associées aux couples (λ,k) *tels que* $\mathrm{P}(\lambda) = 0$ *et* $0 \leqslant k < m_\lambda(\mathrm{P})$.

Donnez un exemple pour illustrer que cet énoncé serait faux en caractéristique $p > 0$! (pensez au petit Théorème de Fermat).

Bien sûr une fois qu'on dispose de l'énoncé de ce Théorème 14 on peut en donner d'autres démonstrations.

Quoi qu'il en soit, en ce qui concerne le point de vue algébrique le Théorème 2 qui identifie V(P) au dual de K[X]/(P) est certainement plus important que le Théorème 14, puisqu'il l'admet comme corollaire quasi immédiat et que ce dernier ne s'applique que pour P scindé et est limité à la caractéristique nulle.