Sur les exponentielle-polynômes en plusieurs variables : quelques résultats déjà anciens et bien des questions toujours ouvertes *

by
Alain Yger,
Mathématiques Pures de Bordeaux,
Université de Bordeaux, 33405, Talence, France.

4 avril 2013

1 Trois problèmes classiques pensés de diverses manières

1.1 Le théorème de Lindemann-Weierstrass

Voici la version la plus classique du théorème de Lindemann-Weierstrass :

Assertion LW1. *Soient $\alpha_1, ..., \alpha_s, b_1, ..., b_s$, $2s$ nombres algébriques tels que les b_j soient tous non nuls et les a_j deux à deux distincts ; alors nécessairement*

$$b_1 e^{\alpha_1} + \cdots + b_s e^{\alpha_s} \neq 0 .$$

Cette assertion est équivalente à l'assertion suivante :

Assertion LW2. *Soient $\alpha_1, ..., \alpha_s$ s nombres algébriques linéairement indépendants sur $\mathbb{Q}$; alors leurs exponentielles $e^{\alpha_1}, ..., e^{\alpha_s}$ sont algébriquement indépendantes sur $\overline{\mathbb{Q}}$.*

*Exposé à Angers, 12 Décembre 2001

Preuve de (LW1) $\Longrightarrow$ (LW2) **:** on suppose (LW1) valide et l'on considère s nombres algébriques $\alpha_1, ..., \alpha_s$, $\mathbb{Q}$ -linéairement indépendants ; supposons que

$$Y(X) = \sum_{\underline{m} \in \mathbb{N}^s} Y_{\underline{m}} X^{\underline{m}}\,, \quad r_{\underline{m}} \in \overline{\mathbb{Q}}\,,$$

soit un élément de $\overline{\mathbb{Q}}[X_1, ..., X_s]$ tel que

$$Y(e^{\alpha_1}, ..., e^{\alpha_s}) = \sum_{\underline{m} \in \mathbb{N}^s} r_{\underline{m}} e^{m_1 \alpha_1 + ... + m_s \alpha_s} = 0\,;$$

l'assertion (LW1), couplée avec les fait que tous les $m_1\alpha_1 + \ldots + m_s \alpha_s$, $\underline{m} \in \mathbb{N}^s$, sont distincts (vu la $\mathbb{Q}$-indépendance linéaire des α_j, $j = 1, ..., s$), implique que tous les $r_{\underline{m}}$, $\underline{m} \in \mathbb{N}^s$, sont nuls, donc que $R \equiv 0$; les nombres e^{α_j}, $j = 1, ..., s$, sont donc bien $\mathbb{Q}$-algébriquement indépendants, ce qui prouve l'assertion (LW2).

Preuve de (LW2) $\Longrightarrow$ (LW1) **:** supposons que ω soit un élément primitif de l'extension (de degré d) $\mathbb{Q}(\alpha_1, ..., \alpha_s)$ et qu'il existe une relation non triviale

$$b_1 e^{\alpha_1} + \cdots b_s e^{\alpha_s} = 0$$

avec, pour tout $j = 1, ..., s$, $b_j \neq 0$; pareille relation s'écrit, si

$$\alpha_j = \frac{\sum\limits_{k=0}^{d-1} \nu_{jk} \omega^k}{D}\,, \quad \nu_{jk} \in \mathbb{Z}\,,\ D \in \mathbb{N}^*\,,$$

sous la forme

$$\sum_{\underline{\nu} \in \mathbb{Z}^d} \beta_{\underline{\nu}} X^{\underline{\nu}} = 0\,,$$

avec

$$X = (1, e^{\omega/D}, ..., e^{\omega^{d-1}/D})$$

et $\beta_{\underline{\nu}} = b_j$ si $\nu = (\nu_{jk})_k$, $j = 1, ..., s$, 0 si $\underline{\nu}$ n'est pas de cette forme ; la $\mathbb{Q}$-indépendance linéaire des nombres ω^k/D, $k = 0, ..., d-1$, implique, du fait de l'assertion (LW2), la $\overline{\mathbb{Q}}$-indépendance algébrique de leurs exponentielles ; on en déduit que tous les $\beta_{\underline{\nu}}$ sont nuls, donc en particulier $b_1 = ... = b_s = 0$, ce qui est en contradiction avec le fait que les b_j sont supposés tous non nuls ; l'assertion (LW1) est bien ainsi prouvée.

Les deux assertions (numériques) que sont (LW1) et (LW2) sont en fait équivalentes à deux assertions "fonctionnelles" que nous noterons (PE1) et

(PE2) (PE pour “polynôme exponentiel”). Ces deux assertions sont les suivantes :

Assertion PE1. *Soit F un élément de $\mathbb{Q}[[z]]$ (série formelle en z à coefficients rationnels) telle que F corresponde au développement en zéro d'un polynôme exponentiel (automatiquement à coefficients et fréquences algébriques et noté aussi F) qui s'annule en $z=1$; alors $(z-1)^{-1}F$ est encore un polynôme exponentiel.*

Assertion PE2. *Soient $\alpha_1,...,\alpha_s$, s nombres algébriques distincts et $b_1,...,b_s$ dans $\mathbb{Q}$ tels que le polynôme exponentiel $\sum_{j=1}^{s} b_j e^{\alpha_j z}$ définisse une série formelle à coefficients rationnels ; alors*

$$\sum_{j=1}^{s} b_j e^{\alpha_j} = 0 \Longrightarrow b_1 = \ldots = b_s = 0\,.$$

Preuve de (PE2) $\Longrightarrow$ (LW1) **:** supposons que $\alpha_1,...,\alpha_s$, soient s nombres algébriques distincts et $b_1,...,b_s$ s nombres algébriques non nuls tels que :

$$b_1 e^{\alpha_1} + \cdots + b_s e^{\alpha_s} = 0\,.$$

On introduit le groupe de Galois G de l'extension $[K:\mathbb{Q}]$,

$$K = \mathbb{Q}(\alpha_1,...,\alpha_s,b_1,...,b_s)\,,$$

et le polynôme exponentiel

$$F(z) = \prod_{\sigma\in G}\left(\sum_{j=1}^{s}\sigma(b_j)e^{\sigma(\alpha_j)z}\right).$$

Il s'agit d'une série formelle à coefficients dans $\mathbb{Q}$; ce polynôme exponentiel s'écrit sous la forme

$$F(z) = \sum_{j=1}^{t}\tilde{b}_j e^{\tilde{\alpha}_j z}\,,$$

où

$$\prod_{j=1}^{t}(X-\tilde{\alpha}_j) = X^t - \tilde{a}_1 X^{t-1} - ... - \tilde{a}_t\,,$$

les $\tilde{a}_j$ étant tous rationnels, ainsi que $\tilde{b}_1\tilde{\alpha}_1^n + \ldots + \tilde{b}_t\tilde{\alpha}_j^n$, $n=0,...,t-1$; on peut par conséquent écrire

$$F(z) = \sum_{n=0}^{\infty}\frac{u_n}{n!}z^n\,,$$

où la suite $(u_n)_{n\geq 0}$ se trouve régie par l'équation aux différences

$$u_{n+t} = \tilde{a}_1 u_{n+t-1} + \cdots + \tilde{a}_t u_n \,,\ n \in \mathbb{N}\,,$$

et la donnée des t premiers termes (tous rationnels). Il résulte de (PE2) que F (qui s'annule en $z = 1$) se trouve être (comme polynôme exponentiel, ou comme série formelle, c'est pareil) la série formelle identiquement nulle ; il en résulte, puisque cette série formelle se trouve obtenue en multipliant toutes les séries transformées de

$$\sum_{n\in\mathbb{N}} \frac{\Big(\sum\limits_{j=1}^{s} b_j \alpha_j^n\Big)}{n!} z^n$$

par les divers automorphismes σ du groupe de Galois de l'extension $[K : \mathbb{Q}]$, que

$$\sum_{n\in\mathbb{N}} \frac{\Big(\sum\limits_{j=1}^{s} b_j \alpha_j^n\Big)}{n!} z^n \equiv 0\,,$$

soit encore

$$\sum_{j=1}^{s} b_j e^{\alpha_j z} \equiv 0\,,$$

ce qui implique $b_1 = \ldots = b_s = 0$ puisque les α_j, $j = 1, \ldots, s$, sont supposés distincts. L'assertion (LW1) est donc bien ainsi prouvée.

Preuve de (LW1) $\Longrightarrow$ (EP2) **:** c'est immédiat.

Preuve de (PE1) $\Longrightarrow$ (PE2) **:** on se donne $\alpha_1, \ldots, \alpha_s$ distincts dans $\overline{\mathbb{Q}}$, et un polynôme exponentiel du type

$$F(z) = \sum_{j=1}^{s} b_j e^{\alpha_j z}$$

(avec $b_1, \ldots, b_s$ dans $\overline{\mathbb{Q}}$), tel que $F \in \mathbb{Q}[[z]]$ et que $F(1) = 0$; on peut alors écrire

$$F(z) = (z-1)G(z)\,,$$

où G est un polynôme exponentiel. Il résulte du théorème de Ritt (ou, plus simplement encore, de l'unicité de l'écriture d'une exponentielle polynôme f sous la forme $f_0 + zf_1 + \cdots + z^q f_q$, où les f_l, $l = 0, \ldots, q$, sont des polynômes exponentiels, voir le lemme 3.1.12 dans [8], p. 205) que $F \equiv 0$, c'est à dire $b_1 = ... = b_s = 0$.

Preuve de (PE2) $\Longrightarrow$ (PE1) **:** c'est immédiat car, si F est un polynôme exponentiel dont le développement de Taylor en zéro appartient à $\mathbb{Q}[[z]]$ et qui s'annule en 1, il est automatiquement de la forme

$$F(z) = \sum_{j=1}^{s} b_j e^{\alpha_j z}\,,$$

avec les α_j, $j = 1, ..., s$, deux à deux distincts dans $\overline{\mathbb{Q}}$, et les b_j, $j = 1, ..., s$, aussi dans $\overline{\mathbb{Q}}$; on a donc, du fait de l'assertion (EP2), $b_1 = ... = b_s = 0$, soit $F \equiv 0$, ce qui implique bien sûr (et est même beaucoup plus fort que !) le fait que $(z-1)^{-1}F$ reste un polynôme exponentiel. L'assertion (PE1) est donc valide dès que (PE2) l'est.

La formulation PE1, de nature plus analytique que l'une des assertions PW1 ou PW2, montre la rigidité du cadre arithmétique par rapport au cadre analytique dans une situation très simple ou intervient un probème de division d'un polynôme-exponentiel par un autre ; les contraintes arithmétiques imposent au quotient d'être un polynôme exponentiel, ce qui ne résulte en rien du théorème classique de Ritt. Pour comprendre ce résultat et tenter de le rapprocher de questions concernant les exponentielle-polynômes en plusieurs variables et où des contraintes de type arithmétique impliqueraient le même type de rigidité, nous devons revenir aux outils dont on dispose dans le cadre arithmétique, et non dans le cadre simplement analytique, que sont les notions de hauteur et de taille. Ce sera l'objet de la section 2 de cet exposé. Mais exposons avant les deux autres problèmes.

1.2 La conjecture de Schanuel et ses analogues formels

La conjecture de Schanuel, conjecture centrale dans le domaine de la transcendance, et toujours ouverte même dans le cas $s = 2$ (elle impliquerait alors dans ce cas l'indépendance algébrique sur $\mathbb{Q}$ de e et π, ou de $\log 2$, $\log 3$, dont on se sait rien pour l'instant), s'énonce ainsi (dans le cas $s = 1$, c'est le classique théorème de Gelfond-Schneider) :

Conjecture. *Étant donné s nombres complexes $y_1, ..., y_s$ $\overline{\mathbb{Q}}$-linéairement indépendants, le degré de transcendance de l'extension $\overline{\mathbb{Q}}[y_1, ..., y_s, e^{y_1}, ..., e^{y_s}]$ est au moins égal à s.*

Si cette conjecture, sauf dans le cas $n = 1$, reste inaccessible, sa version formelle est elle vraie, comme l'ont prouvé J. Ax ([6, 18], pour un point de vue plus récent, voir aussi [12]), suivant les idées de C. Chabauty [15] et E. Kolchin [26]. En voici une version :

Un énonçé du type Schanuel "formel". *Soient $y_1, ..., y_s$ s séries formelles de $\mathbb{C}[[t_1, ..., t_k]]$ avec $k \geq 1$ et un idéal $\mathcal{I}$ de $\mathbb{C}[X_1, ..., X_s, Y_1, ..., Y_s]$ de dimension au plus s tel que*

$$\forall P \in \mathcal{I}\,, \quad P(y_1(t), ..., y_s(t), e^{y_1(t)}, ..., e^{y_s(t)}) \equiv 0\,.$$

Alors, il existe $r_1, ..., r_s \in \mathbb{Q}$ et $\alpha \in \mathbb{C}$ tels que

$$\sum_{j=1}^{s} r_j y_j(t) \equiv \alpha\,. \tag{1.1}$$

Une conséquence importante de cette conjecture est la proposition suivante (voir [10], proposition 6.4 et corollaire 6.7) :

Corollaire. *Soient $P_1, ..., P_m$ m-polynômes en $2n$ variables*

$$(X_1, ..., X_n, Y_1, ..., Y_n)$$

définissant dans $\mathbb{C}^{2n}$ une variété algébrique $V(P)$ et W le sous-ensemble de $\mathbb{C}^n$ défini par

$$X^{(0)} \notin W \Longrightarrow \dim[V(P)] \cap \{X = X^{(0)}\} \leq 0\,.$$

Alors, toute composante de dimension strictement positive de la variété analytique définie par les exponentielle-polynômes

$$F_j(z) := P_j(z_1, ..., z_n, e^{z_1}, ..., e^{z_n})$$

est automatiquement incluse dans la fermeture de W dans $\mathbb{C}^n$. En particulier, si $m \geq n$, toute composante de dimension strictement positive de la variété analytique définie par les F_j est automatiquement incluse dans l'adhérence de tout sous-ensemble W' de $\mathbb{C}^n$ tel que

$$X \notin W' \Longrightarrow \mathrm{rang}\Big[\frac{\partial P_j(X,Y)}{\partial Y_k}\Big]_{j,k} = n \quad \forall Y\,.$$

Les idées soutendant la preuve de Schanuel "formel" se retrouvent aussi dans la possibilité d'apporter des précisions au théorème de Ritt en plusieurs variables tel qu'il est énoncé par C. A. Berenstein et A. Dostal [7] (voir aussi [5]) : si F et G sont deux exponentielle-polynômes telles que le quotient F/G soit une fonction entière, alors, il existe une exponentielle-polynôme H et un polynôme P tels que

$$\forall z \in \mathbb{C}^n\,, \quad \frac{F(z)}{G(z)} = \frac{H(z)}{P(z)}\,.$$

Notons que c'est déjà ce même théorème de Ritt (voir [33] et [37] pour le cadre d'une variable complexe, ou aussi [8] pour un panorama de synthèse sur les théorèmes de factorisation dans l'anneau des exponentielle-polynômes en une variable, palliant de fait la non noethériannité de cet anneau) que nous avons évoqué à propos de notre interprétation "analytique" (PE1) du théorème de Lindeman-Weierstrass dans la première partie de cette introduction.

Revenant au cadre de plusieurs variables, on peut montrer que les idées soutendant la preuve du théorème de Ax peuvent être exploitées aux fins de prouver la proposition suivante, dont un pan constitue un raffinement du théorème de Ritt (voir [10], section 7, cette proposition est aussi reprise aussi dans le livre de Ronkin [34]) :

Proposition. *Soit Λ un sous-ensemble fini de $\mathbb{C}^n$; si l'exponentielle-polynôme de n variables*

$$\sum_{\omega\in\Lambda} a_\omega(z) e^{i\langle \omega\,, z\,\rangle}\,, \quad a_\omega \in \mathbb{C}[X_1, ..., X_n]\,,$$

est identiquement nulle sur une sous-variété algébrique de $\mathbb{C}^n$ de dimension 1, cette variété est soit incluse dans un sous-espace affine du type

$$\langle \omega_1 - \omega_2\,, z\,\rangle = \alpha\,, \tag{1.2}$$

avec $\omega_1 \neq \omega_2 \in \Lambda$ et $\alpha \in \mathbb{C}$, soit telle que tous les coefficients a_ω s'annulent identiquement dessus ; de la même manière, si un polynôme irréductible P divise (dans l'anneau des fonctions entières) une telle exponentielle-polynôme sans en diviser tous les coefficients, il est automatiquement de la forme

$$\langle \omega_1 - \omega_2\,, z\,\rangle - \alpha\,. \tag{1.3}$$

Notons que ni dans la formulation de la version formelle de la conjecture de Schanuel, ni dans ses conséquences, tel le raffinement du théorème de Ritt ci-dessus, on ne peut préciser cette constante α intervenant dans (1.1), (1.2) ou (1.3). La seule information de nature arithmétique que l'on pourrait tirer concernant un tel coefficient α est donnée par des énoncés tels le suivant (Proposition 6.3 de [10]), lui aussi fortement inspiré du cheminement formel conduisant à la solution de la conjecture de Schanuel formelle ; il s'agit de fait de la transcription au cadre des exponentielle-polynômes d'un outil omniprésent dans les problèmes d'effectivité en algèbre commutative, le lemme de normalisation de E. Noether :

Proposition. *Soient $P_1, ..., P_m$ n polynômes en les variables*

$$X_1, ..., X_k, Y_1, ..., Y_n ,$$

avec $k \leq n$, à coefficients dans un sous-corps K de $\mathbb{C}$, définissant une variété algébrique de $\mathbb{C}^{n+k}$ de dimension au plus n ; il existe une hypersurface algébrique W dans $\mathbb{C}^n$ (ne dépendant que de la donnée des P_j), définie par une équation $\{q(z_1, ..., z_k) = 0\}$ avec $q \in K[X_1, ..., X_k]$, telle que toute composante de dimension strictement positive de la variété cette fois analytique

$$\{z \in \mathbb{C}^n \,;\, P_j(z_1, ..., z_k, e^{iz_1}, ..., e^{iz_n}) = 0 \,,\, j = 1, ..., m\}$$

soit incluse dans W.

Concernant le manque de précisions relativement à α, il est à noter que l'on retrouvera des problèmes de nature semblable avec les questions relatives à la factorisation en formes affines du polynôme de Bernstein sur laquelle nous reviendrons.

1.3 Une conjecture d'Ehrenpreis et Montgomery

Dans son livre [22] (pages 321-322) L. Ehrenpreis formule la conjecture suivante :

Conjecture *Soit f une exponentielle-polynôme de la forme*

$$f(z) = \sum_{j=1}^{s} b_j(z) e^{\alpha_j z} ,$$

où $\alpha_1, ..., \alpha_s$ sont des nombres algébriques et les b_j, $j = 1, ..., s$, sont des éléments de $\overline{\mathbb{Q}}[X]$; il existe des constantes $c > 0$ et $C \geq 0$, un entier $m \in \mathbb{N}$, *tels que, si ξ_1 et ξ_2 sont deux zéros distincts de f, alors*

$$|\xi_1 - \xi_2| \geq c \frac{e^{-C\|\mathrm{Re}\,\xi_1\|}}{(1+|\xi_1|)^m} . \tag{1.4}$$

Remarque. En fait, la conjecture a été formulée pour une somme d'exponentielles

$$f(z) = \sum_{j=1}^{s} b_j e^{\alpha_j z}$$

et sans l'hypothèse d'algébricité sur les b_j pourtant indispensable, comme on le verra sur les exemples décrits plus loin.

L'exemple

$$f(z) = \sin z \sin(az) ,$$

où a aurait d'excellentes approximations rationnelles (par exemple a de Liouville) montre qu'une contrainte portant sur les fréquences de la somme d'exponentielles est assurément indispensable. On trouvera dans [9] des exemples simples (une différence de deux sinus à fréquences algébriques par exemple) pour lesquels l'on voit qu'une condition portant sur les coefficients est aussi nécessaire pour espérer montrer que l'ensemble des zéros est *à étranglement lent* comme on le conjecture dans ce cas.

Pour l'instant, le premier cas connu (et facile) pour lequel la conjecture d'Ehrenpreis-Montgomery est vérifiée est le cas où f est une somme d'exponentielles à coefficients algébriques et fréquences dans un sous-groupe $\mathbb{Z}\oplus\omega_1\mathbb{Z}$ de rang 2 ; dans ce cas, le fait que la courbe analytique de $\mathbb{C}^2$

$$t \to (e^t, e^{\omega_1 t})$$

ne puisse s'approcher asymptotiquement d'un sous-ensemble fini de $\overline{\mathbb{Q}}^2$ se trouve quantifié par le classique théorème d'A. Baker concernant les minorations de combinaisons linéaires de logarithmes de nombres algébriques à coefficients algébriques : si $\alpha, \beta \in \overline{\mathbb{Q}}, \omega_1 \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ satisfont

$$\log\alpha - \omega_1 \log\beta + 2\pi(k_1 + k_2\omega_1) \neq 0$$

pour un certain couple $(k_1, k_2) \in \mathbb{Z}^2$, alors

$$|\log\alpha - \omega_1 \log\beta + 2\pi(k_1 + k_2\omega_1)| \geq \gamma(\alpha,\beta,\omega_1)(1 + |k_1| + |k_2|)^{-C(\alpha,\beta,\omega_1)} ,$$

les constantes γ et C ne dépendant que de α, β, ω_1.

En revanche, l'étape suivante (passer d'un groupe des fréquences de rang 2 à un groupe de rang 3) demande cette fois à quantifier le fait que la courbe analytique de $\mathbb{C}^3$

$$t \to (e^t, e^{\omega_1 t}, e^{\omega_2 t}) \in \mathbb{C}^3$$

ne puisse (si elle ne la rencontre pas) asymptotiquement se rapprocher d'une courbe algébrique Γ de $\mathbb{C}^3$ définie sur $\overline{\mathbb{Q}}$, en l'occurence la courbe d'équations

$$P(\zeta_1, \zeta_2, \zeta_3) = Q(\zeta_1, \zeta_2, \zeta_3)\,,$$

où P et Q sont définis par

$$f(z) = P(e^z, e^{\omega_1 z}, e^{\omega_2 z})\,, \quad f'(z) = Q(e^z, e^{\omega_1 z}, e^{\omega_2 z})\,.$$

Il est significatif de remarquer que la seule très mince avancée concernant le problème d'Ehrenpreis-Montgomery dans le cas du rang 3 concerne le cas où ω_1 est un irrationnel cubique et $\omega_2 = \omega_1^2$; grâce au fait que dès qu'un entier est supérieur à $3/2$, il est supérieur à 2, le degré de transcendance sur $\overline{\mathbb{Q}}$ de $\overline{\mathbb{Q}}(z, z^\omega, z^{\omega_2})$ est au moins égal à 2 ($z \neq 1$), ce que les méthodes fines de transcendance (basées surtout sur la formule d'interpolation d'Hermite) permettent de quantifier au plus juste (sans qu'il soit possible de les améliorer de manière significative) ; c'est un résultat de D. Brownawell, exploité dans [9], qui permet de montrer que si f est une somme d'exponentielles de fréquences dans $\mathbb{Z} + \omega\mathbb{Z} + \omega^2\mathbb{Z}$, il existe, pour tout $\epsilon > 0$, une constante $c(\epsilon, f) > 0$ telle que, si ξ_1 et ξ_2 sont deux zéros distincts de f,

$$|\xi_1 - \xi_2| \geq c(\epsilon, f) \exp(-|\xi_1|^{4+\epsilon})\,;$$

on est bien loin de la minoration conjecturée, mais c'est un premier cas, il semble même que l'on sache aujourd'hui, grâce aux méthodes développées par l'équipe stéphanoise autour de Diaz, remplacer $4 + \epsilon$ par $1 + \epsilon$.

Une approche alternative vers la conjecture d'Ehrenpreis-Montgomery serait celle consistant à étudier, si P et Q sont deux polynômes à coefficients dans $\overline{\mathbb{Q}}$ en n variables $X_1, ..., X_n$, le prolongement méromorphe de l'application de $\mathbb{C}^{n+1}$ à valeurs dans $\mathcal{D}'(\mathbb{C}^n)$:

$$\begin{aligned}(s_1, ..., s_{n-1}, t_1, t_2) \to \left(\prod_{j=1}^{n-1} |\zeta_{j+1} - \omega_j \zeta_1|^{s_j} \right) \\ \times \Big[P(e^{\zeta_1}, ..., e^{\zeta_n})\Big]^{t_1} \Big[Q(e^{\zeta_1}, ..., e^{\zeta_n})\Big]^{t_2}\end{aligned} \qquad (1.5)$$

les formules de Mellin inverse (voir (6.2) dans la section 6) permettent de relier à cette étude celle du prolongement analytique de la fonction

$$s \in \mathbb{C} \to \left(\sum_{j=1}^{n-1} |\zeta_{j+1} - \omega_j \zeta_1|^2 + |P(e^{\zeta_1}, ..., e^{\zeta_n})|^2 + |Q(e^{\zeta_1}, ..., e^{\zeta_n})|^2 \right)^s \quad (1.6)$$

et en particulier si

$$\zeta \to \sum_{j=1}^{n-1} |\zeta_{j+1} - \omega_j \zeta_1|^2 + |P(e^{\zeta_1}, ..., e^{\zeta_n})|^2 + |Q(e^{\zeta_1}, ..., e^{\zeta_n})|^2$$

ne s'annule pas dans $\mathbb{C}$, à celle de la minoration sur $\mathbb{C}$ de cette fonction (on atteint pour la fonction donnée en (1.6) la valeur en $s = -1$ artificiellement par le jeu d'intégrations par parties déduites de l'étude du prolongement méromorphe de (1.5)).

Le point serait d'établir dans pareille situation que les contraintes de nature arithmétique (algébricité des ω_i, $i = 1, ..., n-1$, et des coefficients de P et Q) permettent d'assurer via des équations fonctionnelles du type de celles de Bernstein

$$\mathcal{Q}(X, d/dX, s)[F^{s+1}] = b(s) F^s$$

le contrôle du prolongement analytique de (1.5) ; notons qu'il existe un analogue multivariables du résultat (malheureusement local !) de Bernstein et que l'on sait, comme l'a établi C. Sabbah [36] que le polynôme jouant le rôle de b s'écrit :

$$\prod_{\substack{\alpha \in \mathbb{N}^{n-1}, \beta \in \mathbb{N}^2 \\ \gamma}} (\alpha_1 s_1 + \cdots + \alpha_{n-1} s_{n-1} + \beta_1 t_1 + \beta_2 t_2 - \gamma) \ ;$$

en particulier, les contraintes de nature arithmétique se répercutent-t'elles sur les coefficients constants γ sur lesquels on ne dispose à ce jour d'aucune information ?

Les méthodes inspirées de l'analyse p-adique et de la théorie des G-objets pourraient donner ici des outils (comment en particulier faire intervenir le contrôle par la taille ?) susceptibles d'éclairer cette démarche alternative. En ce sens, la rigidité introduite dans le théorème de division de Ritt dans la preuve alternative du théorème de Lindemann-Weierstrass présentée dans [13] et [4], ou la transposition au cadre arithmétique des résultats de Ramis-Malgrange concernant l'étude des équations différentielles dans le cadre Gevrey [3] mériteraient d'être reliées à des questions telles que celles que soulève la conjecture d'Ehrenpreis-Montgomery.

2 Quelques concepts issus du point de vue p-adique

2.1 Places et formule du produit

Soit K un corps de nombres et B l'anneau des entiers de K ; l'extension K admet un élément primitif ω, solution d'un polynôme unitaire irréductible f de $\mathbb{Q}[X]$ (de degré d), de telle sorte que

$$K = \mathbb{Q} + \omega\mathbb{Q} + \cdots + \omega^{d-1}\mathbb{Q} \simeq \frac{\mathbb{Q}[X]}{f\mathbb{Q}[X]}\,.$$

La présentation des diverses notions introduites ici suit celle de [1].

1. Places infinies

À chaque racine ω_i, $i = 1, ..., d$, du polynôme f, on peut associer le $\mathbb{Q}$-homomorphisme (de corps) p_i de K dans $\mathbb{C}$ tel que $p_i(\overline{X}) = \omega_i$; à cet homomorphisme, on associe une valeur absolue sur K induisant sur $\mathbb{Q}$ la topologie usuelle de $\mathbb{C}$, soit

$$|x|_{\infty,i} := |p_i(x)|\,, \quad i = 1, ..., d\,.$$

Si les d racines de f sont triées de manière à ce que les d' premières soient réelles et que deux des d'' qui suivent ne soient pas conjuguées, on peut montrer que toute valeur absolue v sur K induisant sur $\mathbb{Q}$ la topologie usuelle est équivalente à l'une de ces valeurs absolues $|\cdot|_{\infty,i}$, avec $i = i(v) \in \{1, ..., d'+d''\}$ (ce qui signifie que v et $|\cdot|_{\infty,i}$ définissent la même topologie sur K, ou encore qu'il existe une constante strictement positive $\delta_{i(v)}$ telle que $v(x) = |x|_{\infty,i(v)}^{\delta_{i(v)}}$) ; de plus, les deux valeurs absolues $|\cdot|_{\infty,i}$ et $|\cdot|_{\infty,j}$ ne sont pas équivalentes si $i \neq j$. On peut donc classer ainsi toutes les valeurs absolues archimédiennes sur K (celles qui induisent sur $\mathbb{Q}$ la topologie usuelle) ; ces valeurs absolues se trouvent ainsi réparties en $d' + d''$ classes (que l'on appellera les *places infinies*.

2. Places finies

Si B désigne l'anneau des entiers de K, c'est à dire

$$B = \mathbb{Z} \oplus \omega\mathbb{Z} + \cdots + \omega^{d-1}\mathbb{Z}$$

ω désignant un élément primitif de l'extension $[K : \mathbb{Q}]$ (B est noethérien), on note $\mathcal{P}(K)$ la liste des idéaux premiers de l'anneau B ; si x est un élément quelconque de K, xB définit un *idéal fractionnaire* du corps de nombres K (c'est à dire un B-module M tel qu'il existe $b \in B$, avec $bM \subset B$) ; cet idéal fractionnaire admet une unique décomposition

$$xB = \prod_{\mathcal{B} \in \mathcal{P}(K)} \mathcal{B}^{\nu_x(\mathcal{B})} ,$$

où les nombres $\nu_{\mathcal{B}}(x)$, $\mathcal{B} \in \mathcal{P}(K)$ sont des entiers relatifs presque tous nuls. Chaque idéal premier $\mathcal{B}$ de B définit une valeur absolue $|\cdot|_{\mathcal{B}}$ (non archimédienne) sur K, via la règle

$$|x|_{\mathcal{B}} := N(\mathcal{B})^{-\nu_{\mathcal{B}}(x)} \tag{2.1}$$

(la *norme* $N(\mathcal{B})$ est par définition le cardinal de $B/\mathcal{B}$).

Exemple. Dans le cas particulier où $K = \mathbb{Q}$ et $B = \mathbb{Z}$, il y a correspondance entre les nombres premiers p et les idéaux premiers $\mathcal{B}$ de $\mathbb{Z}$; la norme de l'idéal $p\mathbb{Z}$ est le cardinal du groupe fini $\mathbb{Z}/p\mathbb{Z}$, soit p, et la norme $|x|_{\mathcal{B}}$, lorsque $\mathcal{B} = p\mathbb{Z}$, est exactement la valeur absolue p-adique sur $\mathbb{Q}$.

Nous avons ainsi su définir une collection de valeurs absolues non archimédiennes sur K, indexée par la collection des idéaux premiers de l'anneau des entiers de K. Toute valeur absolue v sur K induisant sur $\mathbb{Q}$ une topologie p-adique, avec p premier, est équivalente à l'une (et une seule) des valeurs absolues $|\cdot|_{\mathcal{B}}$, où $\mathcal{B}$ parcourt la famille des idéaux premiers de B. Le nombre premier $p = p_{\mathcal{B}}$ ainsi attaché à un idéal premier $\mathcal{B}$ de B est unique ; on retrouve ainsi le fait que la norme de l'idéal premier $\mathcal{B}$ correspondant à $|\cdot|_{\mathcal{B}}$ se doit d'être une puissance de $p_{\mathcal{B}}$, l'exposant étant le degré de l'extension $[B/\mathcal{B} : \mathbb{Z}_{p_{\mathcal{B}}}]$; l'entier $[B/\mathcal{B} : \mathbb{Z}_{p_{\mathcal{B}}}]$ est appelé *degré résiduel* et noté $f_{\mathcal{B}}$ (en effet, cet entier ne dépend que de $\mathcal{B}$ puisque $p_{\mathcal{B}}$ est imposé dès que $\mathcal{B}$ l'est). D'autre part, si $\mathcal{B}$ est un ideal premier de B tel que $|x|_{\mathcal{B}}$ induise la topologie $p_{\mathcal{B}}$-adique sur $\mathbb{Q}$, l'entier $\nu_{p_{\mathcal{B}}}(\mathcal{B})$ est appelé *indice de ramification* de $\mathcal{B}$ au dessus de $p_{\mathcal{B}}$ (on note cet indice $e_{\mathcal{B}}$, car ce n'est pas utile de faire apparaître la dépendance en $p_{\mathcal{B}}$, $p_{\mathcal{B}}$ étant imposé par $\mathcal{B}$). Ainsi l'on peut donc affirmer, en combinant avec (2.1), que

$$|p|_{\mathcal{B}} = p^{-f_{\mathcal{B}}\nu_{p_{\mathcal{B}}}(\mathcal{B})} = p^{-e_{\mathcal{B}} f_{\mathcal{B}}}$$

si la valeur absolue $|\cdot|_{\mathcal{B}}$ attachée à $\mathcal{B}$ induit la topologie $p = p_{\mathcal{B}}$-adique sur $\mathbb{Q}$.

3. Bilan

Nous pouvons donc faire un bilan de la situation avec la définition suivante :

Définition. *Les places de K sont par définition les classes d'équivalence partitionnant l'ensemble des valeurs absolues sur K suivant la relation d'équivalence (deux valeurs absolues sont équivalentes si et seulement si elles définissent la même topologie). On distingue les places finies (en correspondance avec les idéaux premiers de $\mathcal{B}$) qui partitionnent l'ensemble des valeurs absolues induisant une valeur absolue p-adique sur $\mathbb{Q}$, et les places infinies, partitionnant l'ensemble des valeurs absolues induisant la métrique usuelle sur $\mathbb{Q}$.*

4. Comment normaliser ?

Nous distinguerons pour convenir de la normalisation des places K les cas archimédien et non archimédien.

- Soit v une place archimédienne de K (extension de degré d) ; la place v correspond donc à l'un des zéros $\omega_{i(v)}$, $1 \leq i(v) \leq d' + d''$, de la liste ordonnée des zéros du polynôme irréductible unitaire f) ; on convient alors de normaliser la valeur absolue en posant, si $x \in K$,

$$|x|_v = |x|_{\infty,i(v)}^{d_v/d}$$

  où d_v vaut 1 si $i(v)$ correspond à l'un des indices $1, ..., d'$, c'est à dire à une racine réelle du polynôme f tel que $K = \mathbb{Q}[X]/f\mathbb{Q}[X]$, ou 2 si $i(v)$ correspond à une racine complexe non réelle ($i = d', ..., d' + d''$) du polynôme f. L'entier d_v est le degré de l'extension $[K_v : \mathbb{Q}_v]$, où K_v et $\mathbb{Q}_v$ désignent les complétés respectifs de K et $\mathbb{Q}$ pour la valeur absolue archimédienne $|\cdot|_{\infty,i(v)}$; si $i(v) \in \{1, ..., d'\}$ (c'est à dire si $\omega_{i(v)}$ est une racine réelle de f) alors K_v, comme $\mathbb{Q}_v$ est isomorphe (en temps que corps) à $\mathbb{R}$, ce qui explique $d_v = 1$ dans ce cas ; si $i(v) \in \{d' + 1, ..., d' + d''\}$, $\mathbb{Q}_v = \mathbb{R}$ tandis que K_v se trouve dans ce cas isomorphe à $\mathbb{C}$; ceci explique $d_v = 2$ dans ce cas.
- Si v est une place finie (correspondant à un idéal premier $\mathcal{B}_v$ de B), on convient de normaliser la place en posant :

$$|x|_v := (|x|_{\mathcal{B}})^{1/d} = \Big((p(v))^{-\nu_x(\mathcal{B})/e_{\mathcal{B}}}\Big)^{e_{\mathcal{B}} f_{\mathcal{B}}/d}.$$

  En fait, on a encore $e_{\mathcal{B}} f_{\mathcal{B}} = d_v = [K_v : \mathbb{Q}_v]$ si $v = v_{\mathcal{B}}$ (on admettra ici ce point), ce qui rend la définition de $|\cdot|_v$ dans le cas des places finies cohérente avec celle proposée dans le cas des places infinies.

Remarque Si $K = \mathbb{Q}$ ou $K = \mathbb{Q}[\sqrt{-a}]$, avec $a \in \mathbb{N}^*$, il y a exactement une et une seule place infinie ; cette remarque sera importante dans le contexte des résultats de Bézivin-Robba.

5. Formule du produit (version normalisée)

La formule clef est la formule du produit, qui nous assure, si $\Sigma(K)$ désigne l'ensemble des places (normalisées) de K, que

$$\prod_{v \in \Sigma(K)} |x|_v = 1\,.$$

Dans le cas de $\mathbb{Q}$, cette formule est une évidence : on écrit la décomposition en facteurs premiers d'un nombre rationnel x, soit

$$x = \prod_{p \ \text{premier}} p^{v_p(x)}\,,$$

puis on prend la valeur absolue des deux membres, soit alors

$$|x| = |x|_\infty = \frac{1}{\prod_{p \ \text{premier}} \|x\|_p}\,,$$

d'où la formule. Dans le cas général, on a la

Formule du produit. *Soit K un corps de nombres, $\Sigma(K)$ l'ensemble des places de K (finies ou infinies) ; pour tout $x \in K^*$, on a :*

$$\prod_{v \in \Sigma(K)} |x|_v = 1 \tag{2.2}$$

Preuve. Les entiers $\nu_{\mathcal{B}}(x)$ sont définis par

$$xB = \prod_{\mathcal{B} \ \text{premier de} \ B} \mathcal{B}^{\nu_{\mathcal{B}}(x)}\,.$$

La définition de la norme s'étend à l'ensemble des idéaux fractionnaires non nuls de K (cet ensemble forme un groupe multiplicatif) ; l'extension se fait en exploitant le fait que tout idéal fractionnaire de K se décompose de manière unique comme un produit d'idéaux $\mathcal{B}^{\nu_{\mathcal{B}}}$, $\mathcal{B}$ parcourant la famille des idéaux premiers de B. Cette extension faite, on en déduit ici

$$N(xB) = \prod_{\mathcal{B} \ \text{premier de} \ B} N(\mathcal{B})^{\nu_{\mathcal{B}}(x)}\,.$$

En fait, on a $N(xB) = N_{K/\mathbb{Q}}(x)$, où $N_{K/\mathbb{Q}}$ désigne la norme de l'opérateur de multiplication par x dans le $\mathbb{Q}$-espace vectoriel K (on n'utilisera pas pour l'instant cette propriété mais c'est une remarque importante pour expliquer que

$$|N(xB)|_p = \prod_{\substack{\mathcal{B} \text{ premier} \\ p_{\mathcal{B}}=p}} |x|_{\mathcal{B}} \,).$$

En organisant l'écriture de $N(xB)$, on voit que

$$N(xB) = \prod_{p \text{ premier}} \left(\prod_{\substack{\mathcal{B} \text{ premier} \\ p_{\mathcal{B}}=p}} p^{-\nu_x(\mathcal{B})\, f_{\mathcal{B}}} \right);$$

Il en résulte que

$$|N(xB)|_p = p^{-\sum\limits_{\mathcal{B}\,;p_{\mathcal{B}}=p} \nu_x(\mathcal{B})\, f_{\mathcal{B}}}$$

et donc que

$$|N(xB)|_p = \left(\prod_{\substack{v\in\Sigma(K) \\ p(v)=p}} |x|_v \right)^d.$$

D'autre part, on a, compte tenu de l'identité admise $N(xB) = N_{K/\mathbb{Q}}(x)$,

$$|N(xB)|_\infty^{1/d} = \prod_{j=1}^{d} |p_j(x)|^{1/d},$$

si les $\zeta_j(x)$ sont les conjugués de x ; on a donc

$$|N(xB)|_\infty^{1/d} = \prod_{v \text{ place infinie de } K} |x|_v \,.$$

La formule du produit dans $\mathbb{Q}$ (appliquée à $N(xB)$, puis élevée à la puissance $1/d$, implique donc la formule du produit voulue dans K. $\diamondsuit$

2.2 Hauteur (d'un nombre algébrique, d'un élément de $K[X]$, de $K[[X]]$, de $M_{\mu,\nu}(K)[[X]]$)

Cette section s'inspire directement de l'ouvrage d'Yves André [2].

1. Hauteur d'un nombre algébrique.

Étant donné un corps de nombres K et un élément ζ de K, la <u>*hauteur*</u> de ζ est par définition la quantité :

$$h(\zeta) := \sum_{v \in \Sigma(K)} \log^+ |\zeta|_v \,.$$

Cette définition ne dépend de fait que de ζ (et non de K). En effet, soit

$$P(X) = a_0(X - \zeta_1) \cdots (X - \zeta_n) \in \mathbb{Z}[X]$$

le polynôme minimal de ζ sur $\mathbb{Z}$; d'après la formule de Jensen,

$$\int_0^1 \log |P(e^{2i\pi\theta}|d\theta = |a_0| \prod_{j=1}^{n} \max(1, |\zeta_j|) \,.$$

Comme a_0 représente un dénominateur de ζ, et que par conséquent $a_0\zeta$ est un élément de B, on en déduit que, pour toute place finie v de $\Sigma(K)$, on a $\nu_{a_0\zeta}(\mathcal{B}) \geq 0$ pour tout idéal premier $\mathcal{B}$ de B ; ceci nous assure que pour toute place finie v de K,

$$\log^+ |a_0\zeta|_v = 0 \,.$$

D'autre part, d'après la formule du produit (dans $\mathbb{Q}$),

$$\log |1/a_0| + \sum_{p \text{ premier}} \log |1/a_0|_p = 0 \,.$$

D'autre part

$$\begin{aligned} h(\zeta) &= \frac{1}{n} \sum_{i=1}^{n} \log(\max(1, |\zeta_i|) + \frac{1}{n} \sum_{p \text{ premier}} \log |1/a_0|_p \\ &= \frac{1}{n} \log \left[|a_0| \prod_{j=1}^{n} \max(1, |\zeta_j|) \right] , \end{aligned}$$

d'où la formule

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] h(\zeta) = \int_0^1 \log |P(e^{2i\pi\theta}|d\theta \,, \tag{2.3}$$

où l'on voit la hauteur ne dépendre explicitement que de ζ (et bien sûr de son polynôme minimal).

<u>2. Extension à $M_{\mu,\nu}(K)[X]$ et $M_{\mu,\nu}(K)[[X]]$.</u>

La notion de hauteur s'étend aux polynômes (en une variable) à coefficients dans l'anneau $M_{\mu,\nu}(K)$ ($\mu, \nu \in \mathbb{N}^*$) des matrices à μ lignes et ν colonnes à coefficients dans K ; si

$$Y = \sum_{l=0}^{N} Y_p X^p\,, \quad Y_p \in M_{\mu,\nu}(K)\,,$$

est un tel polynôme, on définit sa hauteur via la formule

$$h(Y) := \frac{1}{N+1}\Big(\sum_{v\in\Sigma(K)} \log^+ \max_{0\le p\le N} \|Y_p\|_v\Big)$$

avec $\|Y_p\|_v := \max_{k,l} |y_{k,l}^{(p)}|_v$ si $Y_p = [y_{k,l}^{(p)}]$, $k = 0, ..., \mu - 1$, $l = 0, ..., \nu - 1$, $p = 0, ..., N$.

Ensuite, on peut définir naturellement la hauteur d'une série formelle (à coefficients dans $M_{\mu,\nu}(K)$),

$$h\left(\sum_{p=0}^{\infty} Y_p X^p\right) := \limsup_{N\to+\infty} \left[h\left(\sum_{p=0}^{N} Y_p X^p\right)\right].$$

On aura aussi besoin d'introduire la notion de hauteur pour une série de Laurent à coefficients dans $M_{\mu,\nu}(K)$, c'est à dire d'un objet du type

$$Y = \sum_{p=-N_0}^{+\infty} Y_p X^p\,, \quad Y_p \in M_{\mu,\nu}(K)\,;$$

la hauteur $h(Y)$ est alors définie comme

$$h(Y) := \begin{cases} 0 \text{ si } Y \text{ est tronquée à droite} \\ h(X^{N_0}Y) \text{ sinon}\,. \end{cases}$$

On peut vérifier que

$$h(Y) = \limsup_{N\to+\infty} \sum_{v\in\Sigma(K)} h_{v,N}(Y)\,,$$

où

$$h_{v,N}(Y) = \frac{1}{N} \max_{\substack{k,l \\ -N_0\le p\le N}} \log^+(|y_{k,l}^{(p)}|_v)\,.$$

2.3 Notion de taille pour un $X\,d/dX$-module

On peut aussi définir une notion de taille pour les $X\,d/dX$-modules au dessus $K(X)$, où K est un corps de nombres ; un tel module $\mathcal{M}$ est par définition un $K(X)\,[X\,d/dX]$-module unitaire tel que le $K(X)$-module induit soit un module libre et de type fini ; ce module peut donc rapporté à une base $\Upsilon := \{m_0, ..., m_{\mu-1}\}$, l'action de $X\frac{d}{dX}$ se trouvant représentée dans la base Υ par une matrice G de type (μ, μ) :

$$X\frac{d}{dX}[m_i] = \sum_{j=0}^{\mu-1} G_{i,j} m_j\ ,\ \ i = 0, ..., \mu - 1\,.$$

Remarque On peut de manière plus générale remplacer $K(X)$ par une K-algèbre unitaire A contenant $K[X]$, par exemple $K[[X]]$, et définir ainsi la notion de $X\frac{d}{dX}$-module de type fini au dessus de $K[[X]]$; on retrouve ici la notion de *connexion à singularité logarithmique* au dessus de l'origine.

Exemple. Si G désigne une matrice (μ, μ) à coefficients dans $K(X)$, le système différentiel

$$\Big(X\,\frac{d}{dX}\Big)[Y] = GY$$

induit naturellement une structure de $X\,d/dX$-module sur $K(X)^\mu$, ce qui nous donne bien une structure de $X\,d/dX$-module au dessus de $K(X)$. équipé de sa base canonique.

Étant donné un tel $X\,d/dX$-module sur $K(X)$, supposé rapporté à une base Υ dans laquelle l'action de $X\frac{d}{dX}$ est représentée par la matrice G, on introduit la suite des matrices $G^{(p)}$, $p = 0, 1, ...$, définie de manière à ce que, si Y vérifie formellement

$$\Big(X\,\frac{d}{dX}\Big)[Y] = GY\,,$$

alors

$$\forall p \in \mathbb{N}\,, \Big(X^p\Big(\frac{d}{dX}\Big)^p\Big)[Y] = G^{[p]}Y\,.$$

Ces matrices $G^{[p]}$ sont définies suivant la récurrence :

$$G^{(0)} = I, \quad G^{(p+1)} = \partial G^{(p)} + G^{(p)}(G - pI_\mu)\,.$$

On associe au $X\,d/dX$-module (et au choix de la base) la série de Laurent en $\mathcal{X}$ (à coefficients dans $M_{\mu,\mu}(K(X))$)

$$\sum_{p\geq 0} \frac{G^{(p)}}{p!}\mathcal{X}^p\,.$$

Or toute valeur absolue sur K s'étend naturellement à $K[X]$, donc à $K(X)$, selon les principes

$$\Big|\sum_{p=0}^{N} a_p X^p\Big|_v = \max_p |a_p|_v\,, \quad |P(X)/Q(X)|_v = |P(X)|_v/|Q(X)|_v\,;$$

ceci nous permet de définir la taille du module M relativement au choix de la base Υ en nous inspirant de la manière dont nous avons défini la hauteur d'une série formelle, mais en ne retenant cette fois que les places finies de K (soit $v \in \Sigma_f(K)$). On pose donc

$$\sigma_\Upsilon(M) := \limsup_{N\to\infty} \frac{1}{N} \sum_{v\in\Sigma_f(K)} \log^+ \max_{0\le p\le N} \|\frac{G^{(p)}(X)}{p!}\|_v\,.$$

De fait, la définition de la taille d'un $X\,d/dX$-module au dessus de $K(X)$ est indépendante du choix de la base Υ.

3 G-objets et rigidité arithmétique

On trouvera dans [2] ou dans [20] une présentation beaucoup plus complète des diverses notions introduites ici.

3.1 G-fonctions

Étant donnée une suite $(a_n)_{n\ge 0}$ de nombres algébriques, dire qu'elle satisfait la condition **(G)** revient à dire qu'il existe une constante $C > 0$ telle que :

- d'une part, la "maison" de chaque a_n (c'est à dire le maximum des modules des conjugués de a_n) est, pour tout $n \in \mathbb{N}$, bornée par C^n (cette clause est dite $(\mathbf{G})_{\text{conj}}$) ;
- d'autre part, pour tout $N \in \mathbb{N}$, $a_0, ..., a_N$ admettent un dénominateur commun $D_N \in \mathbb{N}^*$ inférieur à C^N (cette clause est dite $(\mathbf{G})_{\text{den}}$).

Étant donnée une telle suite $(a_n)_{n\ge 0}$, nous pouvons lui associer la série entière (de rayon de convergence non nul)

$$f(z) = \sum_{n\ge 0} a_n z^n$$

(le rayon de convergence est ici au moins égal à $1/C$).

Nous dirons d'autre part qu'une suite $(a_n)_{n\geq 0}$ de nombres algébriques vérifie la condition **(H)** si et seulement cette suite se plie à une équation aux différences à coefficients polynomiaux

$$P_0(n)a_n + P_1(n+1)a_{n+1} + \cdots + P_\mu(n+\mu)a_{n+\mu} = 0\,, \quad n \in \mathbb{N}\,,$$

où $\mu \in \mathbb{N}^*$, les P_j, $j = 0, ..., \mu$, étant des polynômes à coefficients algébriques; si la suite $(a_n)_{n\geq 0}$ vérifie aussi la condition (**G**), alors le fait qu'elle vérifie également (**H**) équivaut au fait que la fonction

$$f(z) = \sum_{n\geq 0} a_n z^n \tag{3.1}$$

(holomorphe au voisinage de l'origine) soit solution d'une équation différentielle linéaire homogène à coefficients dans $\overline{\mathbb{Q}}[X]$ (comme les deux fonctions classiques $z \mapsto e^z$ ou $z \mapsto \log(1-z)$ impliquées dans l'étude des exponentielle-polynômes).

Une fonction f associée selon (3.1) à une suite $(a_n)_{n\geq 0}$ de nombres algébriques vérifiant à la fois les conditions **(G)** et **(H)** est appelée <u>*G-fonction*</u> (on dit aussi, ce qui serait plus correct, qu'il s'agit d'une <u>*série du type G*</u> car c'est le point de vue "séries formelles" qui est ici constamment privilégié).

On a la proposition importante suivante (facile, il s'agit juste d'une re-interprétation des contraintes arithmétiques en termes de hauteur) :

Proposition. *Un élément Y de $\overline{\mathbb{Q}}[[X]]$ définit une G-fonction si et seulement si :*

- *d'une part, il existe un opérateur différentiel dans $\overline{\mathbb{Q}}[X, \frac{d}{dX}]$ ayant Y dans son noyau;*
- *d'autre part, $h(Y) < \infty$ (la hauteur étant définie comme la hauteur d'une série formelle à coefficients dans $\overline{\mathbb{Q}}$).*

3.2 $\mathcal{G}$-systèmes

Soit M un $K(X)$-module de rang μ rapporté à une base Υ, et $(G^{(p)})_{p\geq 0}$ la suite de matrices (μ, μ) à coefficients dans $K(X)$ qui lui est associée. On note $d_G(X)$ un dénominateur (dans $B(X)$, B étant l'anneau des entiers de K) de la matrice G (matrice de l'opérateur $X\,d/dX$ dans la base Υ).

Définition. *On dit que le module $\mathcal{M}$ obéit à la* <u>*condition de Galochkin*</u> *(ou encore est un $\mathcal{G}$-système) si et seulement si $\sigma(M) < +\infty$, ou encore, ce qui est équivalent, si et seulement si l'une ou l'autre des conditions suivantes est remplie :*

- *il existe une constante $C > 0$ telle que dénominateur commun d_N des coefficients de toutes les matrices $[d_G(X)^p]G^{(p)}/p!$, $p = 0, ..., N$ est borné par C^N (c'est la caractérisation $\mathcal{G}'$) ;*
- *il existe une constante $C > 0$ telle que, pour tout $N \in \mathbb{N}$,*

$$\prod_{\substack{v \in \Sigma(K) \\ \sigma \text{finie}}} \max_{0 \leq p \leq N} \| \frac{d_G(X)^p G^{(p)}(X)}{p!} \|_v \leq C^N$$

(c'est la caractérisation $(\mathcal{G}'')$).

Remarque. On note que seules les places finies interviennent dans la caractérisation $(\mathcal{G}'')$ de la condition de Galochkin.

3.3 Singularités d'un système differentiel

<u>1. Singularités irrégulières ; exemples.</u>

Soit

$$L = \sum_{j=0}^{q} A_q(z) D^q$$

un opérateur différentiel (resp. un système différentiel $\mathcal{L}$) à coefficients polynomiaux (les coefficients sont dans $\mathbb{C}[X]$, resp. dans l'anneau $M_{n,n}(\mathbb{C}[X])$ s'il s'agit d'un système différentiel à coefficients polynomiaux).

On dit que $a \in \mathbb{C} \cup \{\infty\}$ est un <u>*point singulier totalement irrégulier*</u> si et seulement si

$$\text{val}_a A_0 < \min_{j \geq 1} [\text{val}_a(A_j) - j] \,.$$

Les deux exemples typiques (et liés à la preuve de l'assertion (LW1)) sont, d'une part, celui de l'opérateur différentiel

$$L = z^2 D + (z-1) I$$

(l'origine est point singulier totalement irrégulier) ou du système (ici $n = 2$)

$$\mathcal{L}_f := \begin{pmatrix} z^2 & 0 \\ 0 & z^2 \end{pmatrix} D + \begin{pmatrix} z-1 & f \\ 0 & 0 \end{pmatrix} ,$$

où f désigne une fraction rationnelle (il importe d'en chasser les dénominateurs). Plus généralement, si Q désigne un polynôme (non constant) à coefficients complexes, on voit que l'origine est toujours une singularité totalement irrégulière de l'opérateur

$$L_Q := zQ(zD+1) - 1$$

(le cas $Q(X) = X$ donnant précisément l'opérateur L introduit ci-dessus). On remarque que dire que g est une solution de l'équation avec second membre $Lg = f$ (où $f \in \mathbb{C}(z)$) équivaut à dire que le vecteur

$$\mathbf{g} := \begin{pmatrix} g \\ 1 \end{pmatrix}$$

est solution de l'équation homogène

$$\mathcal{L}_f[\mathbf{g}] = 0\,.$$

<u>2. Singularités régulières ; systèmes fuschiens.</u>

Soit $\mathcal{L}$ est un système différentiel

$$\mathcal{L} = \sum_{j=0}^{q} A_j(z) D^q\,,$$

où $A_j \in M_{n,n}(\mathbb{C}[X])$; un élément $a \in \mathbb{C} \cup \{\infty\}$ est dit <u>*singularité régulière*</u> du système lorsque l'on a

$$\min_{j<q}[\mathrm{val}_a(A_j) - j] \geq \mathrm{val}_a(A_q) - q\,.$$

Un système différentiel dont toutes les singularités sont des singularités régulières est appelé <u>*système fuschien*</u>.

3.4 Critères de rationalité (Bézivin-Robba, Chudnovsky+Katz)

La rigidité arithmétique qu'impose la formule du produit se matérialise souvent dans des énonçés de critères de rationnalité. Nous donnerons ici deux scénarios : l'un directement d'inspiration p-adique, le second basé sur les concepts de G-objets et la finitude de la taille.

1. Le critère de rationalité de Bézivin-Robba

Le premier critère de rationalité évoqué ici est un résultat de Bézivin-Robba [BR] inspiré des méthodes p-adiques (formule du produit et critère de rationnalité de Polya-Bertrandias) ; il s'agit du critère suivant :

Critère de Bézivin-Robba. *Soit L un opérateur de $K[X][D]$, où $K = \mathbb{Q}$ ou bien $K = \mathbb{Q}(\sqrt{-d})$ ($d \in \mathbb{N}^*$) et g une série formelle de $K[[z]]$ de rayon de convergence non nul; si l'origine est une singularité totalement irrégulière de L et si Lg est une fraction rationnelle f (ou encore $\mathcal{L}_f[\mathbf{g}] = 0$), alors g correspond aussi au développement en 0 d'une fraction rationnelle.*

2. La combinaison des théorèmes de Chudnovsky et Katz.

Le second crière repose d'abord sur un résultat intéressant de rigidité ; il s'agit d'un résultat de Chudnovsky, qui sera exploité couplé avec le théorème de Katz (comme dans [2] ou [3]) pour obtenir un second critère de rationnalité.

Théorème de Chudnovsky. [16, 17] *Soit K un corps de nombres, Γ une matrice (μ, μ) à coefficients dans $K(X)$ et Y une solution dans $(K[[X]])^\mu$ du système différentiel*

$$(D - \Gamma)[Y] = 0\,. \tag{3.2}$$

Supposons qu'une solution dans $(K[[X]])^\mu$ de ce système ait des composantes $K(X)$ linéairement indépendantes. Si M désigne la structure de $X\,d/dX$-module au dessus de $K(X)$ induite par l'équation (3.2), on a

$$\sigma(M) \leq C(\Gamma)h(Y)\ ;$$

si en particulier, les composantes de Y sont des G-fonctions, alors M satisfait la condition de Galochkin et est donc un $\mathcal{G}$-système.

Ce résultat de Chudnovsky (on trouvera une preuve détaillée dans [20], chapitre 8) s'utilise couplé avec un théorème fondamental de Katz, révélant ce que la rigidité arithmétique impose de contraintes.

Théorème de Katz. [28] *Tout $X\frac{d}{dX}$-module M au dessus de $K(X)$ tel que $\sigma(M) < \infty$ (c'est à dire tout $\mathcal{G}$-système) est fuschien.*

On trouvera une preuve du résultat de Katz (dans cette formulation) dans [20], pages 98-99.

Remarque. Notons que les résultats de Chudnovsky et Katz viennent d'être étendus au cadre multi-variables par L. Di Vizio [19] ; si $\mathcal{Y}$ est un K-schéma lisse, de dimension relative

d, de type fini et géométriquement connexe (de corps de fractions rationnelles $K(\mathcal{Y})$) et si (M, ∇) est un $K(\mathcal{Y})/K$-module différentiel libre de rang μ équipé d'une connexion ∇ intégrable, on peut définir, comme dans le cas $d = 1$, la taille de (M, ∇) relativement au choix d'une base, montrer ensuite que cette notion ne dépend pas en fait de la base et dire que (M, ∇) satisfait la condition de Galochkin si et seulement si il est de taille finie (définition 2.2 de [19]). En un point fermé ξ de $\mathcal{Y}$, on peut définir la notion de G-fonction. Si le module (M, ∇) admet une solution injective φ, c'est-à-dire un morphisme injectif de modules à connexion

$$\varphi \in \mathrm{Hom}_{\nabla}(M, \mathrm{Frac}(\widehat{\mathcal{O}}_{\mathcal{Y},\xi}))$$

tel que, pour une base particulière $m_1, ..., m_\mu$ de M sur $K(\mathcal{Y})$, $\varphi(m_j)$ soit une G-fonction en ξ, alors (M, Δ) satisfait la condition de Galochkin (théorème 4.1 de [19]) et, à condition que soit définie correctement la notion de point singulier-régulier, le module (M, ∇) est à singularités régulières (corollaire 2.5 de [19]).

Le couplage des théorèmes de Chudnovsky et Katz conduit au critère de rationalité suivant :

Corollaire (second critère de rationalité). Si l'opérateur $D - \Gamma$, $\Gamma \in M_{\mu,\mu}(K(X))$ admet à la fois une singularité irrégulière (en un point de $\mathbb{C}$ ou à l'infini) et une solution dans $K[[X]]^\mu$ dont les composantes sont des G-fonctions, ces composantes sont $K(X)$-liées.

Exemple. L'exemple typique sera celui de l'opérateur $\mathcal{L}_f$ introduit plus haut ; ce second critère sera (appliqué précisément sur cet exemple) le moteur de la rigidité qu'introduisent les hypothèses de type arithmétique dans le théorème de factorisation de Ritt.

Ce sont des résultats de ce type que nous aimerions invoquer concernant l'existence éventuelle de relations de Bernstein pour f^λ ou $f_1^{\lambda_1} \cdots f_q^{\lambda_q}$, où $f_1, ..., f_q$ sont des exponentielle-polynômes en n variables à coefficients et à fréquences dans un corps de nombres K.

4 Lindemann-Weierstrass revisité

Comme on l'a vu dans la section 1.1, on peut, pour démontrer le théorème de Lindemann-Weierstrass, montrer que si F est un polynôme exponentiel à coefficients et fréquences algébriques s'annulant en 1 et admettant un développement en série de Taylor à l'origine à coefficients rationnels, alors $F \equiv 0$. En fait, on peut se ramener à supposer, si

$$F(z) = \sum_{j=1}^{s} b_j e^{\alpha_j z} ,$$

que l'ensemble des couples $\{(b_j,\alpha_j)\,;\, j=1,...,s\}$ est globalement invariant sous l'action du groupe de Galois de l'extension $[\mathbb{Q}(b_1,...,b_s,\alpha_1,...,\alpha_s):\mathbb{Q}]$; cette hypothèse suffit à affirmer que le développement de Taylor de F en 0 est bien à coefficients rationnels, on le verra un peu plus loin. Si l'on part d'un polynôme exponentiel quelconque à coefficients et fréquences dans $\mathbb{Q}(\omega)$, $\omega\in\overline{\mathbb{Q}}$,

$$f(z)=b_1'e^{\alpha_1' z}+\cdots+b_s'e^{\alpha_s' z}\,,$$

c'est bien à un tel polynôme exponentiel F que l'on aboutit en posant

$$F(z)=\prod_{\sigma\in G_\omega}\Big(\sum_{j=1}^{s}\sigma(b_j)e^{\sigma(\alpha_j)z}\Big)\,,$$

G_ω désignant le groupe de Galois de l'extension $[\mathbb{Q}(\omega):\mathbb{Q}]$.

Considérons donc un tel polynôme exponentiel F, de développement de Taylor en 0

$$F(z)=\sum_{n=0}^{+\infty}\frac{u_n}{n!}z^n\,,$$

où

$$u_n=b_1\alpha_1^n+\cdots+b_s\alpha_s^n\,,\quad n=0,1,...$$

si $F(z)=b_1e^{\alpha_1 z}+\cdots+b_se^{\alpha_s z}$. On suppose que l'ensemble des couples

$$\{(b_j,\alpha_j)\,;\, j=1,...,s\}$$

est globalement stable sous l'action du groupe de Galois de l'extension

$$[\mathbb{Q}(b_1,...,b_s,\alpha_1,...,\alpha_s):\mathbb{Q}]\,.$$

La suite $(u_n)_{n\geq 0}$ se trouve régie par une équation aux différences

$$u_{n+s}=a_1u_{n+s-1}+\cdots+a_su_s\,,\quad n=0,1,...,$$

où les a_j, $j=1,...,s$ sont les coefficients du polynôme

$$\prod_{j=1}^{s}(X-\alpha_j)=X^s-a_1X^{s-1}-\cdots-a_s\,.$$

Comme l'ensemble des couples $\{(b_j,\alpha_j)\,,\, j=1,...,s\}$ est supposé ici globalement stable sous l'action du groupe de Galois de l'extension

$$[\mathbb{Q}(b_1,...,b_s,\alpha_1,...,\alpha_s):\mathbb{Q}]\,,$$

les nombres a_j, $j = 1, ..., s$, sont rationnels ; comme les nombres $b_1\alpha_1^k + \cdots + b_s\alpha_s^k = F^{(k)}(0)$, $k = 0, ..., s-1$, le sont aussi (pour les mêmes raisons), on retrouve bien ici (par induction sur n) que tous les $(u_n)_{n\geq 0}$ sont rationnels.

Comme fonction de type exponentiel (de fonction indicatrice de Lindelöf l'enveloppe convexe du support de l'ensemble des fréquences $\{\alpha_1, ..., \alpha_q\}$), on peut associer à F sa transformée de Laplace ($\mathrm{Lap}\,[F]$) définie dans le demi-plan $\{\zeta \in \mathbb{C}\,;\,, \mathrm{Re}\,\zeta > \max_j \mathrm{Re}\,\alpha_j\}$ par

$$\mathrm{Lap}\,[F](z) = \int_0^{+\infty} F(t)e^{-zt}dt = \sum_{j=1}^{s} \frac{b_j}{z - \alpha_j}\,.$$

La série formelle

$$\sum_{n=0}^{+\infty} u_n z^n$$

s'identifie au développement en $z = 0$ de

$$\frac{1}{z}\mathrm{Lap}\,[F](1/z) = \mathcal{T}[F](z)\,.$$

On introduit (ici un peu artificiellement) la série formelle

$$V(z) = \sum_{n=0}^{+\infty} v_n z^n\,,$$

où

$$v_n := n! \sum_{k=0}^{n} \frac{u_k}{k!}\,.$$

Comme l'on a

$$\frac{v_n}{n!} - \frac{v_{n-1}}{(n-1)!} = \frac{u_n}{n!}\,,$$

on a

$$\sum_{n=0}^{+\infty} (v_n - nv_{n-1})z^n \equiv \sum_{n=0}^{+\infty} u_n z^n\,.$$

Si l'on introduit l'opération de dérivation des séries formelles, on a donc, si

$$V(z) = \sum_{n\geq 0} v_n z^n\,,$$

$$V - [X\frac{d}{dX}][zV] = (1-z)V - z[X\frac{d}{dX}][V] = \sum_{n\geq 0} u_n z^n\,.$$

On a donc, L désignant l'opérateur introduit dans la section 3.3,

$$L[V] = -\sum_{n=0}^{+\infty} u_n z^n\,.$$

On remarque alors que

$$\mathcal{L}_f \begin{pmatrix} V \\ 1 \end{pmatrix} = 0\,,$$

où

$$f(X) = \sum_{j=1}^{s} \frac{b_j}{1-\alpha_j X}\,,$$

le système différentiel étant posé avec inconnues dans $(K[[X]])^2$, où

$$K = \mathbb{Q}(b_1,...,b_s,\alpha_1,...,\alpha_s)\,,$$

et considéré comme un système à coefficients dans $K(X)$.

La suite $(v_n)_{n\geq 0}$ vérifie une équation aux différences à coefficients polynomiaux, puisque c'est le cas de la suite $(u_n)_{n\geq 0}$ et que les deux suites sont liées par la relation

$$v_n - nv_{n-1} = u_n\,,\quad n\in\mathbb{N}^*\,;$$

la série formelle V vérifie donc la condition d'holonomicité (**H**) introduite dans la section 3.1.

Si D est un dénominateur commun des a_j, $j=1,...,s$, D^n est un dénominateur commun des nombres $u_0,...,u_n$. Ceci montre (via les relations $v_n - nv_{n-1} = u_n$ et une induction immédiate) que D^n est aussi un dénominateur pour $v_0,...,v_n$. Enfin, les coefficients u_n s'estiment en

$$|u_n| \leq c_1 A^n\,,\quad n\in\mathbb{N}\,,$$

tandis que les coefficients v_n s'estiment en

$$|v_n| \leq cA^{n+1}\,,\quad n\in\mathbb{N}\,,$$

où

$$A := \max_{1\leq j\leq s}(1,|\alpha_j|)\,,$$

ce qui prouve que V est une G-fonction ; c'est <u>ici</u> que l'on utilise $F(1)=0$ car c'est précisément cette condition qui nous permet d'écrire :

$$|v_n| = n!\Big|\sum_{l=n+1}^{+\infty}\frac{u_l}{l!}\Big| \leq \frac{c_1}{n+1}\sum_{l=n+1}^{+\infty}\frac{A^l}{(l-n-1)!} \leq c_1 e^A \frac{A^{n+1}}{(n+1)}\,.$$

4.1 Fin de preuve utilisant Chudnovsky+Katz

À ce stade, nous pouvons conclure de manière "savante" en invoquant les théorèmes de Katz et Chudnovsky combinés comme expliqé dans la section 3.4 [4]. L'opérateur différentiel $\mathcal{L}_f$ présentant une singularité irrégulière et V et 1 étant des G-fonctions, ces fonctions doivent être liées sur $K(X)$, ce qui implique que V corresponde au développement en 0 d'une fraction rationnelle (notée encore V). Mais l'on remarque que

$$\sum_{n=0}^{+\infty} \frac{v_n}{n!} z^n = [1/z\mathrm{Lap}]^{-1}(V)(z) = \mathcal{T}^{-1}[V](z) \frac{F(z)}{1-z} \,.$$

On déduit de ceci que $F(z)/(1-z)$ a pour image le développement d'une fraction rationnelle via la transformation $\mathcal{T}$; c'est donc, puisque cette transformation échange fractions rationnelles et polynômes exponentiels, un polynôme exponentiel. On déduit de cela (comme dans la preuve de l'implication (EP1)$\Longrightarrow$(EP2)) que $F \equiv 0$.

4.2 Fin de preuve élémentaire [13]

Une manière plus élémentaire de conclure avait été proposée par Beukers-Bézivin-Robba en 1990 [13]. On introduit pour cela les séries formelles

$$V_k(z) = \sum_{n=0}^{+\infty} v_{k,n} z^n$$

définies par :

$$V_k(z) = (1 - a_1 z - \cdots - a_s z^s)^k V(z) \,.$$

Pour tout $k \geq 0$, la suite $(v_{k,n})_{n \geq 0}$ vérifie une équation récurrente à coefficients polynomiaux ; c'est vrai si $k = 0$ et cela résulte ensuite du fait que

$$v_{k+1,n} = v_{k,n-1} - a_1 v_{k,n-1} - \cdots - a_s v_{k,n-s} \,, \quad k \geq 0,\, n \geq s \,; \tag{4.1}$$

la série formelle V_k vérifie donc la condition d'holonomicité ($\mathbf{H}$), comme $V = V_0$. On montre immédiatement par induction sur k que, si $n \geq ks$,

$$|v_{k,n}| \leq c A^{n+1} C^k \,,\ k \geq 0 \,, n \geq 0 \,,$$

où $C = 1 + |a_1| + \cdots + |a_s|$, $c > 0$ (il suffit d'utiliser (4.1) pour conduire l'induction). On montre aussi que $k!$ divise $D^n v_{k,n}$ (toujours si $n \geq ks$). Ceci est un peu plus compliqué : on écrit, si $k > 0$ et $n \geq kt$,

$$v_n = u_n + n u_n + \cdots + n(n-1)\cdots(n-k+2) u_{n-k+1} + w_n \,,$$

avec

$$w_n = n! \sum_{l=0}^{n-k} \frac{u_l}{l!} \, ;$$

on a $D^{n-k} w_n \in \mathbb{Z}$ et $k! \,|D^{n-k} w_n$; si l'on note W la série formelle associée à la suite $(w_n)_{n\geq 0}$, on a

$$\begin{aligned} V(z) - W(z) &= \sum_{l=0}^{k-1} \left(\sum_{n=0}^{\infty} n(n-1)\cdots(n-l+1) u_{n-r} z^n \right) \\ &= \sum_{l=0}^{k-1} \frac{P_l(z)}{(1 - a_1 z - \cdots - a_s z^s)^{l+1}} \, , \end{aligned}$$

où P_l est un polynôme de degré au plus $(l+1)s$. On a donc

$$V(z) - W(z) = \frac{P(z)}{(1 - a_1 z - \cdots - a_s z^s)^k} \, ,$$

où P est un polynôme de degré au plus ks. Ainsi donc $v_{k,n} = w_{k,n}$ si $n \geq ks$, où les $(w_{k,n})_{n\geq 0}$ sont définis comme les $(v_{k,n})_{n\geq 0}$, c'est à dire via les relations

$$\sum_{n=0}^{+\infty} w_{k,n} z^n = (1 - a_1 z - \cdots - a_s z^s)^k \Big(\sum_{n=0}^{+\infty} w_n z^n \Big) \, , \; k \geq 0 \, .$$

Il est clair que $k!$ divise $D^{n-k} w_n$, ce qui implique que $k!$ divise aussi $D^n w_{k,n}$; ainsi, si $n \geq ks$, $k!$ divise $w_{k,n}$, donc aussi $v_{k,n} = w_{k,n}$.

Pour k convenable, on montre que V_k correspond au développement d'une fraction rationnelle ; pour $n \geq ks$, on a, si $v_{k,n} \neq 0$,

$$k! \leq |D^n v_{k,n}| \leq cA(AD)^n C^k \, .$$

Ainsi, si $k! \geq cA(AD)^n C^k$ et $n \geq ks$, $v_{k,n} = 0$. On choisit k_0 assez grand pour que, pour tout $k \geq k_0$, $k! \geq cA(AD)^{10ks} C^k$ (c'est évidemment possible au vu des croissances comparées des deux membres) ; on a alors, pour tout $k \geq k_0$, pour tout n entre ks et $10ks$, $v_{k,n} = 0$; il en résulte (via les relations récurrentes (4.1) qui régissent le tableau des $(v_{k,n})_{k,n}$) que les nombres $v_{k,n}$ sont tous nuls lorsque (k,n) appartient au secteur conique $\{(k,n) \, ; \, k_0 \leq k \leq n/(10s)\}$, d'où il résulte que $v_{k_0,n} = 0$ pour tout $n \geq k_0 s$, ce qui prouve que V_{k_0} et donc V, correspond au développement en 0 d'une fraction rationnelle, ce que l'on voulait pour conclure. On peut d'ailleurs ici conclure sans utiliser le recours à la transformation de Laplace, en remarquant que l'identité (entre fractions rationnelles cette fois)

$$L[V](z) = [(z-1) + z\partial][V](z) \equiv -\sum_{j=1}^{s} \frac{b_j}{1-\alpha_j z}$$

implique que les pôles non nuls de $L[V]$ doivent avoir un ordre au moins égal à 2, ce qui est en contradiction avec le fait que, du fait de l'identité ci-dessus, ces pôles sont d'ordre un.

5 Des substituts pour l'équation fonctionnelle de Bernstein ?

Les méthodes évoquées à propos de la conjecture d'Ehrenpreis-Montgomery et fondées sur la recherche de substituts pour une équation de Bernstein globale n'intègrent sans doute à ce jour pas assez les contraintes de rigidité arithmétique présentées (par exemple dans le cadre de la théorie des G-objets présentée et utilisée dans les sections 3 et 4) ; on souhaiterait en particulier introduire, parallèlement au concept de *filtration par le degré* (classique dans la théorie algébrique des $\mathcal{D}$-modules) un concept de filtration par la taille. C'est là la raison qui nous a poussé à présenter ici ces points de vue récents concernant le théorème de Lindemann-Weierstrass en même temps que nous faisions le bilan (bien peu consistant) des résultats connus à ce jour en direction d'un problème comme celui d'Ehrenpreis-Montgomery.

Nous rappellerons brièvement dans cette section les résultats auxquels conduit la stratégie qui consiste à reprendre les idées de base conduisant à la preuve de l'existence d'une relation de Bernstein dans le cadre algébrique global. Les méthodes présentées ici (ainsi que les résultats cités) sont toutes issues de [11].

Pour étudier dans toute leur généralité les problèmes relatifs à l'existence de substituts pour l'équation fonctionnelle de Bernstein, nous considérerons les variantes suivantes de l'algèbre de Weyl $K\langle X_1, ..., X_n, d/dX_1, ..., d/dX_n\rangle$: soient n un entier strictement positif, $m_1, ..., m_n$ des éléments de $\mathbb{N}^*$, $(\alpha_{i,l})$, $i = 1, ..., n, j = 1, ..., m_i$, des éléments de K, chaque famille $\alpha_i = (\alpha_{i,l})_l$ étant constituée soit d'éléments tous nuls, soit d'éléments de K linéairement indépendants sur $\mathbb{Q}$, $\beta_1, ..., \beta_n$ des éléments de $\{0, 1\}$; on note

$$K_\alpha(\lambda_1, ..., \lambda_q)\langle X_1, ..., X_n \,;\, Y_{1,1}, ..., Y_{1,m_1}, ..., Y_{n,1}, ..., Y_{n,m_n} \,;\, D_1, ..., D_n\rangle$$

l'algèbre (non commutative) engendrée sur $K(\lambda_1, ..., \lambda_q)$ (extension du corps de nombres K avec les q paramètres transcendants algébriquement indépendants que sont $\lambda_1, ..., \lambda_q$) par les opérateurs

$$X_1, ..., X_n, D_1, ..., D_n, Y_{i,l}\,, \quad i = 1, ..., n, j = 1, ..., m_i\,,$$

suivant les règles de commutation suivantes :

– les X_i et les $Y_{j,l}$ constituent une famille d'opérateurs commutant entre eux deux à deux ;
– on a $[D_i, X_j] = -\beta_i \delta_{i,j}$, $i, j \in \{1, ..., n\}$;
– on a $[D_i, Y_{j,l}] = -\alpha_{i,l}\delta_{i,j}Y_{j,l}$, $l = 1, ..., m_j$.

Si l'on considère q exponentielle-polynômes

$$F_j(z) := P_j(z_1, ..., z_n, e^{\alpha_{1,1}z_1}, ..., e^{\alpha_{1,m_1}z_1}, ..., e^{\alpha_{n,1}z_1}, ..., e^{\alpha_{n,m_n}z_n})$$

on peut considérer l'objet formel

$$\mathcal{F}^\lambda := F_1^{\lambda_1} \cdots F_q^{\lambda_q}$$

et le $K_{\alpha,\beta}(\lambda)\langle X, Y, D\rangle$ module

$$K_{\alpha,\beta}(\lambda)\langle X, Y, D\rangle[\frac{1}{P_1}, ..., \frac{1}{P_q}]\,\mathcal{F}^\lambda.$$

La dimension de ce module, comme d'ailleurs du module obtenu comme sommme directe de q copies de ce module, est au plus $n + m_1 + \cdots + m_n$. Dans deux cas particuliers au moins, on peut affirmer que cette dimension est au plus $n + 1$ (première étape lorsque l'on essaye de généraliser l'algèbre de Weyl) ; ces deux cas particuliers sont les suivants :

• $\beta_1 = \cdots = \beta_n = 1$, $m_1 = 1$, $\alpha_2 = \cdots = \alpha_n = 0$, $\alpha_{1,1} = 1$;
• $\beta_1 = 0$, $\beta_2 = \cdots = \beta_n = 1$, $\alpha_2 = \cdots = \alpha_n = 0$, $m_1 = 2$, $\alpha_{1,1} = 1$, $\alpha_{1,2} = \omega \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$.

Dans ces deux cas, le fait que tout entier supérieur ou égal à $n + (1/2)$ soit automatiquement supérieur à $n+1$ nous permet d'affirmer, en reprenant mot pour mot la preuve que propose F. Ehlers [21] pour l'existence de l'équation fonctionnelle de Bernstein dans le cadre algébrique et celle que donne B. Lichtin et C. Sabbah [31, 36] pour passer du cadre d'un paramètre ($q = 1$) au cadre de q paramètres, qu'il existe dans ces deux cas deux polynômes A et B en $q+1$ variables et $2k$ opérateurs $\mathcal{R}_k, \mathcal{S}_k$, $k = 1, ..., q$, dans $K[\lambda]\langle X, Y, D\rangle$ tels que

$$\begin{array}{rcl} A(\lambda, X_1)\mathcal{F}^\lambda & = & \mathcal{R}_k[F_k\mathcal{F}^\lambda]\,, \quad k = 1, ..., q \\ B(\lambda, Y_1)\mathcal{F}^\lambda & = & \mathcal{S}_k[F_k\mathcal{F}^\lambda]\,, \quad k = 1, ..., q \end{array}$$

ou

$$\begin{array}{rcl} A(\lambda, Y_{1,1})\mathcal{F}^\lambda & = & \mathcal{R}_k[F_k\mathcal{F}^\lambda]\,, \quad k = 1, ..., q \\ B(\lambda, Y_{1,2})\mathcal{F}^\lambda & = & \mathcal{S}_k[F_k\mathcal{F}^\lambda]\,, \quad k = 1, ..., q\,. \end{array}$$

dans le second cas.

6 Questions autour des systèmes d'équations aux différence-différentielles

Soient $L_1, ..., L_q$ q opérateurs différence-différenntiels dans $\mathbb{R}^n$.
Leurs transformées de Fourier F_j, $j = 1, ..., q$, constituent q exponentielle-polynômes en n-variables, à "fréquences" dans un sous-groupe de type fini de $i\mathbb{R}^n$; ce sont des éléments de l'algèbre de Paley-Wiener, engendrant un idéal dans cette algèbre de fonctions holomorphes. Mais ce sont aussi des exponentielle-polynômes. Plusieurs questions naturelles se posent :

Question 1. L'idéal $I_{\rm loc}$ (des éléments de l'algèbre de Paley-Wiener appartenant localement à I en tout point) est-il égal à la fermeture de l'idéal I dans cette même algèbre de Paley-Wiener ? Cette question pose la question de la synthèse spectrale (par dualité) : une solution C^∞ du système d'équation différence-différentielles s'approche-t-elle (pour la topologie de $C^\infty(\mathbb{R}^n)$ de la convergence uniforme sur tout compact des fonctions et de toutes leurs dérivées) par une suite d'exponentielle-polynômes solutions, autrement dit le célèbre résultat d'Euler concernant les équations différentielles à une variable à coefficients constants reste-t-il valable dans ce cadre ? Cette question est de loin la plus difficile car on a peu d'outils pour rendre compte de l'égalité $\overline{I} = I_{\rm loc}$ (on en a plus, à savoir l'artillerie "algébrique" des mécanismes de division ou les résultats du type Hörmander autorisant la correction de la division C^∞ en holomorphe via la résolution du $\overline{\partial}$) pour attaquer le problème de savoir si I est fermé. Notons que, si l'on sait que la synthèse spectrale est en défaut pour les systèmes d'équation de convolution [27], on ne connait aucune classe générale d'exemples où elle pour lesquels elle serait valide, hors du cadre algébrique des systèmes d'équations aux dérivées partielles à coefficients constants.

Question 2. L'idéal I est-il fermé dans l'algèbre de Paley-Wiener ? Ceci est vrai dans le cadre algébrique (où les F_j sont des polynômes) d'après le principe du passage du local au global. En fait, ici encore, plutôt que de répondre à cette question, on s'en pose une autre (question 3) pour laquelle une réponse positive impliquerait ce résultat. Avant de poser cette question, signalons qu'un cas cependant est accessible : c'est le cas où $V(F)$ est de dimension zéro et où l'on connait un critère suffisant pour que la synthèse spectrale soit remplie : une version "faible" de ce critère est la suivante :

Critère [10] *Il existe $\epsilon > 0$ tel que, pour tout caractère $\rho \ : \Lambda \mapsto \mathbb{C}^*$ de Λ ϵ-proche de* Id*, les exponentielle-polynômes $F_{\rho,j}$, $j = 1, ..., q$, obtenues à partir des F_j en remplaçant chaque monôme exponentiel $z^{\underline{m}} \exp(i\langle\gamma, z\rangle)$ par $z^{\underline{m}}\rho(\gamma)\exp(i\langle\gamma, z\rangle)$ définissent un ensemble discret dans $\mathbb{C}^n$.*

Signalons ici que les développements récents centrés autour de la notion d'amibe (introduite par I.N. Gelfand) lorsqu'elle est transcrite du cadre des séries de Laurent à celui des sommes d'exponentielles à fréquences réelles, amènent naturellement à considérer l'amibe d'une somme d'exponentielles

$$\sum_\gamma b_\gamma e^{\langle\gamma,(\cdot)\rangle}$$

comme le sous-ensemble fermé de $\mathbb{R}^n$ défini comme

$$\mathcal{A}_f := \{x \in \mathbb{R}^n \, ; \, \exists \rho \in \mathrm{Hom}\,(\mathbb{R}^n, S^1)\,, \ f_\rho(x) = 0\}\,;$$

comme l'a montré J. Silipo [38], les composantes connexes du complémentaire de cette amibe sont convexes, comme c'est le cas pour celles du complémentaire de l'amibe d'un polynôme de Laurent. Développer la théorie des amibes dans le contexte des sommes d'exponentielles, suivant la démarche engagée par Forsberg-Passare-Tsikh [24], Passare-Rullgard [32] ou A. Enriques [23] semble indispensable pour mieux comprendre du point de vue géométrique les méthodes introduites dans [10]. Signalons aussi les travaux dans cette direction de Kazarnovskii [29, 30] et de Ronkin [35].

Question 3. Existe-il un processus explicite pour exprimer une fonction C^∞ solution du système d'équations différence-différentielles comme un "empilement" d'exponentielle-polynômes solutions ? Dans le cas algébrique, ceci est vrai, c'est ce que l'on appelle le principe fondamental d'Ehrenpreis-Palamodov. Dans le cas où $q \leq n$ et $F_1, ..., F_q$ définissent une suite régulière dans l'anneau des fonctions entières, on dispose de la possibilité d'écrire des formules explicites de division avec reste ; ces formules génèrent, s'il est possible de l'écrire, une formule de représentation du type

$$f(x) : \left\langle \bigwedge_{j=1}^{q} \overline{\partial}\left(\frac{1}{F_j(\zeta)}\right), \omega(x,\zeta) \wedge \bigwedge_{j=1}^{q} G_j(x,\zeta) \right\rangle,$$

où les formes

$$G_j(z,\zeta) := \sum_{k=1}^{n} G_{jk}(z,\zeta) d\zeta_k, \qquad j = 1, ..., q,$$

sont liées à un système de diviseurs de Hefer $(G_{jk})_k$, système de fonctions dans l'algèbre de Paley-Wiener de $\mathbb{R}^{2n}$ telles que

$$F_j(\zeta) - F_j(z) = \sum_{k=1}^{n} G_{jk}(z,\zeta)(\zeta_k - z_k), \quad j = 1, ..., q.$$

Le fait que le courant résiduel de Coleff-Herrera puisse s'exprimer comme la valeur en $\lambda = 0$ (pour $\underline{t} := (t_1, ..., t_q) \in (\mathbb{R}^{+*})^q$) générique) de

$$\bigwedge_{j=1}^{q} \overline{\partial}\left(\frac{|F_j|^{2\lambda t_j}}{F_j}\right)$$

implique que l'existence de pseudo-équations de Bernstein permet dans ce cas la de conclure ; tel est le cas si

$$F_j(z) = P_j(z_1, z_2, ..., z_n, e^{iz_1}), \quad j = 1, ..., q,$$

ou

$$F_j(z) = P_j(e^{iz_1}, e^{i\omega z_1}, z_2, ..., z_n), \quad j = 1, ..., q$$

avec $\omega \in \overline{\mathbb{Q}}$ et P_j à coefficients algébriques (voir la section précédente).

Question 4. Existe-il une version du Nullstellensatz de Hilbert relative à l'idéal I ? Plus précisément, existe-t'il un entier $N = N(I)$ tel que, pour tout élément de g de $\widehat{\mathcal{E}}'(\mathbb{R}^n)$ s'annulant sur $V(F)$, on ait $g^{N(I)} \in I$? Cette question se ramène à l'existence de pseudo-relations de Bernstein modulo le recours aux formules de Mellin inverse : si $t_1, ..., t_q > 0$ et si $P \in \mathbb{C}[\lambda_1, ..., \lambda_q]$, alors, pour tout nombre complexe β de partie réelle strictement supérieure à 1,

$$\frac{P(\lambda) t_1^{\lambda_1} \cdots t_q^{\lambda_q}}{(t_1 + \cdots + t_q)^{\beta}} = \frac{1}{(2i\pi)^{q-1}\Gamma(\beta)} \times$$
$$\times \int_{\gamma_1 - i\mathbb{R}}^{\gamma_1 + i\mathbb{R}} \cdots \int_{\gamma_{q-1} - i\mathbb{R}}^{\gamma_{q-1} + i\mathbb{R}} \Big(\prod_{j=1}^{q-1} \Gamma(s_j) \Big) \Gamma\Big(\beta - \sum_{j=1}^{q-1} s_j \Big) P(\widetilde{\lambda}_{\lambda,s}) t^{\widetilde{\lambda}(\lambda,s)} ds_1 \cdots ds_{q-1} \,, \tag{6.2}$$

avec

$$\widetilde{\lambda}_{\lambda,s} := (\lambda_1 - s_1, ..., \lambda_{q-1} - s_{q-1}, \lambda_q + \beta - s_1 - \cdots - s_{q-1}) \,.$$

De fait, les formules d'analyse montrent que dans les deux cas particuliers envisagés plutôt, la clôture intégrale locale de I, élevée à la puissance $2\inf(q, n+1)$ est incluse dans l'idéal I ; ceci est une version imparfaite du résultat optimum dans le cadre algébrique [25] : si Q est un polynôme appartenant à la clôture intégrale locale de $I_{\mathrm{loc}}(P_1, ..., P_q)$, avec $\deg P_1 \geq \cdots \geq \deg P_q$, alors

$$Q^n = \sum_{j=1}^{q} A_j P_j \,,$$

avec

$$\deg A_j \leq n \deg Q + \prod_{j=1}^{\inf(q,n)} \deg P_j \,.$$

On voit que le nombre d'exemples où l'on peut pour l'instant avoir une réponse positive à l'une de ces questions est très réduit. On conjecture qu'une réponse positive à la question 1, ainsi sans doute qu'aux questions suivantes, pourrait être apportée dans le cas où les L_j, $j = 1, ..., q$, sont à coefficients algébriques et à retards dans $\mathbb{Q}^n$. Une réponse positive à la question d'Ehrenpreis-Montgomery apparaîtrait comme une conséquence de tels résultats.

Références

[1] Y. Amice, *Les nombres p-adiques*, PUF, 1975.

[2] Y. André, *G-Functions and Geometry*, Aspects of Mathematics, Vieweg, 1989.

[3] Y. André, Séries Gevrey de type arithmétique, I. Théorèmes de pureté et de dualité, Annals of Mathematics 151 (2000), 705-740.

[4] Y. André, Séries Gevrey de type arithmétique, II. Transcendance sans transcendance, Annals of Mathematics 151 (2000), 741-756.

[5] V. Avanissian, R. Gay, Sur les fonctions entières arithmétiques de type exponentiel et le quotient d'exponentielle-polynômes de plusieurs variables, C. R. Acad. Sci. Paris Sér. A 279 (1974), 161–164.

[6] J. Ax, On Schanuel's conjectures, Ann. of Math. 93 (1971), 252-268.

[7] C. A. Berenstein, A. Dostal, The Ritt theorem in several variables, Ark. Math. 12 (1974), 267-280.

[8] C. A. Berenstein, R. Gay, *Complex analysis and special topics in harmonic analysis*, Springer-Verlag, New York, 1995.

[9] C. A. Berenstein, A. Yger, On Lojasiewicz type inequalities for exponential polynomials, J. Math. Anal. Appl. 129 (1988), 166-195.

[10] C. A. Berenstein, A. Yger, Ideals generated by exponential polynomials, Advances in Mathematics 60 (1986), 1-80.

[11] C. A. Berenstein, A. Yger, Exponential polynomials and $\mathcal{D}$-modules, Compositio Mathematica 95 (1995), 131-181.

[12] D. Bertrand, On André's proof of the Siegel-Shidlovsky theorem. Colloque Franco-Japonais : Théorie des Nombres Transcendants (Tokyo, 1998), 51-63, Sem. Math. Sci., 27, Keio Univ., Yokohama, 1999.

[13] F. Beukers, J. P. Bézivin, P. Robba, An alternative proof of the Lindemann-Weierstrass theorem, American Monthly 97,3 (1990), 193-197.

[14] J. P. Bézivin, P. Robba, A new p-adic method for proving irrationality and transcendence results, Annals of Mathematics 129 (1989) 151-160.

[15] C. Chabauty, Sur les équations diophantiennes liées aux unités d'un corps de nombres algébrique fini, Ann. Math. Pura Appl. 17, 138, 127-168.

[16] D. Chudnovsky, G. Chudnovsky, Applications of Padé approximations to diophantine inequalities in values of G-functions, Lecture Notes in Math. 1135, Springer-Verlag, Berlin (1985), 9-51.

[17] D. Chudnovsky, G. Chudnovsky, Applications of Padé approximation to the Grothendieck conjecture on linear differential equations, Lecture Notes in Math. 1135, Springer-Verlag, Berlin (1985) 52-100.

[18] R. Coleman, A generalization of the Ax-Schanuel theorem, Amer. J. Math. 102 (1980) 595-624.

[19] L. di Vizio, Sur la théorie géométrique des G-fonctions, le théorème de Chudnovsky à plusieurs variables, Math. Ann. 319 (2001), 181-213.

[20] B. Dwork, G. Gerotto, F. J. Sullivan, *An introduction to G-functions*, Annals of Mathematics Studies 133, Princeton University Press, 1994.

[21] F. Ehlers, dans *Operations on algebraic $\mathcal{D}$-modules*, A. Borel (editor), Academic Press, Boston, 1987.

[22] L. Ehrenpreis, *Fourier Analysis in several complex variables*, Wiley Interscience, 1970.

[23] A. Enriques, An analogue of convexity for complements of amoebas ov varieties of higher codimension, *preprint.*

[24] M. Forsberg, M. Passare, A. Tsikh, Laurent determinants and arrangements of hyperplane amoebas, Adv. in Maths. 151 (2000), 45-70.

[25] M. Hickel, Solution d'une conjecture de C. A. Berenstein et A. Yger, Ann. Institut Fourier 51(3) (2001), 707-744.2001.

[26] E. Kolchin, Algebraic groups and algebraic dependence, Amer. J. Math. 90, 1968, 1151-1164.

[27] D. Gurevich, Closed ideals with zero dimensional root set in certain rings of holomorphic functions, J. Soviet Math. 9 (1978), 172-182.

[28] N. Katz, Algebraic solutions of Differential Equations (p-curvature and the Hodge filtration), Invent. Math. 18 (1972), 1-118.

[29] B. Ya. Kazarnovskii, On zeros of exponential sums, Dokl. Akad. Nauk SSSR, 257, 4 (1981), 804-808.

[30] B. Ya. Kazarnovskii, Exponential analytic sets, Functional Analysis and its applications, 31, 2 (1997) 86-94.

[31] B. Lichtin, Generalized Dirichlet series and B-functions, Compositio Math. 65 (1988), 81-120.

[32] M. Passare, H. Rullgard, Amoebas, Monge-Ampère measures and triangulations of the Newton polytope, *preprint*, Stockholm, 2002.

[33] J. F. Ritt, A factorization theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i x}$, Trans. Amer. Math. Soc. 29 (1927), no. 3, 584–596.

[34] L. I. Ronkin, *Functions of completely regular growth*, Mathematics and its Applications (Soviet Series), 81. Kluwer Academic Publishers Group, Dordrecht, 1992.

[35] L. I. Ronkin, On zeros of almost periodic functions generated by holomorphic functions in multicircular domain, in *Complex Analysis in Modern Mathematics*, Fazis, Moscow, 2001, 243-256.

[36] C. Sabbah, Proximité évanescente II. Équations fonctionnelles pour plusieurs fonctions analytiques, Compositio Math 64 (1987), 213-241.

[37] A. Shields, On quotients of exponential polynomials. Comm. Pure Appl. Math. 16 (1963) 27-31.

[38] J. Silipo, L'amibe d'une somme d'exponentielles à support réel, *thèse en cours*, Bordeaux.