Équations aux différences linéaires, hypertranscendance et indépendance algébrique

Boris Adamczewski
Travaux communs avec T. Dreyfus, C. Hardouin et M. Wibmer

CNRS, Institut Camille Jordan, Lyon

Une classification géométrico-arithmétique des nombres complexes est donnée par :

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathcal{P} \subset \mathbb{C},$$

où $\mathcal{P}$ désigne l'anneau des périodes au sens de Kontsevich et Zagier.

Les principales caractéristiques de $\mathcal{P}$ sont :

- Cet anneau contient la plupart des constantes mathématiques classiques (comme π, $\log 2$, $\zeta(3)$, $\Gamma(1/3)^3$...)
- $\mathcal{P}$ est dénombrable et ses éléments peuvent être définis par une quantité finie d'information et sont calculables.

La classification suivante, déjà suggérée par Hilbert au début du vingtième siècle, peut être vue comme un analogue fonctionnel de la précédente :

$$\mathrm{Rat} \subset \mathrm{Alg} \subset \mathrm{Hol} \subset \mathrm{Dif} \subset \mathbb{C}[[x]].$$

Remarque. Si le corps de base est $\overline{\mathbb{Q}}$ au lieu de $\mathbb{C}$, les anneaux Hol et Dif ont des caractéristiques semblables à P.

Quelques résultats d'hypertranscendance

Hilbert a également remarqué que certaines fonctions importantes provenant de la théorie des nombres ne sont pas différentiellement algébriques.

• Le premier exemple est dû à Hölder qui a montré que la fonction gamma $\Gamma(x)$ est hypertranscendente.
L'équation fonctionnelle

$$\zeta(x) = 2(2\pi)^{x-1}\Gamma(1-x)\sin\left(\frac{\pi x}{2}\right)\zeta(1-x)$$

implique alors que la fonction zeta de Riemann $\zeta(x)$ est également hypertranscendante.

• Moore, puis Mahler, ont montré l'hypertranscendance de la série

$$\mathfrak{f}_1(x) = \sum_{n \geq 0} x^{2^n} .$$

• Plus récemment, Hardouin and Singer ont montré l'hypertranscendance de certaines séries q-hypergéometriques, comme

$$\mathfrak{f}_2(x) := \sum_{n=0}^{\infty} \frac{(1-a)^2(1-aq)^2\cdots(1-aq^{n-1})^2}{(1-q)^2(1-q^2)^2\cdots(1-q^n)^2} x^n ,$$

où $q \in \mathbb{C}^*$ n'est pas une racine de l'unité, $a \notin q^{\mathbb{Z}}$ et $a^2 \in q^{\mathbb{Z}}$.

La plupart des preuves d'hypertranscendance sont fondées sur le fait que la fonction considérée satisfait à une équation fonctionnelle d'un type différent (*i.e.*, une équation non différentielle).

Par exemple, les trois résultats précédents reposent sur les équation aux différences linéaires suivantes :

$$\Gamma(x+1) = x\Gamma(x)\ ,\ \mathfrak{f}_1(x^2) = \mathfrak{f}_1(x) - x\ ,$$

et

$$\mathfrak{f}_2(q^2x) - \frac{2ax-2}{a^2x-1}\mathfrak{f}_2(qx) + \frac{x-1}{a^2x-1}\mathfrak{f}_2(x) = 0\,.$$

Naît alors de cette expérience l'adage suivant :

(A) *Une solution d'une équation aux différences linéaire devrait être soit rationnelle, soit hypertranscendante.*

Une petite mise en garde

Attention, cet adage doit être considéré *cum grano salis* !

En effet, les fonctions

$$\log(x), \quad \exp(x)$$

et la fonction theta de Jacobi

$$\theta_q(x) = \sum_{n\in\mathbb{Z}} q^{-n(n-1)/2} x^n$$

sont toutes différentiellement algébriques,
bien qu'elle satisfassent à des équations aux différences particulièrement simples :

$$\log(x^p) = p\log x\,, \quad \exp(x+1) = e\exp(x)\,, \quad \theta_q(qx) = qx\theta_q(x)\,.$$

Contexte

On considère des extensions de corps $\mathbb{C} \subset K \subset F$ vérifiant les propriétés suivantes.

- Le corps K est muni d'un automorphisme ρ et d'une dérivation ∂.
- ρ et ∂ s'étendent à F.

Cas S. On choisit $K = \mathbb{C}(x)$, $F = \mathbb{C}((x^{-1}))$,

$$\rho(f(x)) = f(x+h), \quad h \in \mathbb{C}^*$$

et $\partial = \frac{d}{dx}$.

Cas Q. On choisit $K = \bigcup_{j \geq 1} \mathbb{C}(x^{1/j}) =: \mathbb{C}(x^{1/*})$, $F = \mathbb{C}((x^{1/*}))$ le corps des séries de puiseux,

$$\rho(f(x)) = f(qx), \quad \partial = x\frac{d}{dx},$$

où $q \in \mathbb{C}^*$ n'est pas une racine de l'unité.

Cas M. On choisit $K = \mathbb{C}(x^{1/*})$, $F = \mathbb{C}((x^{1/*}))$, $\rho(f(x)) = f(x^p)$, $p \geq 2$ entier, et $\partial = x\frac{d}{dx}$.

Résultat principal

Théorème (A., Dreyfus, Hardouin)

Soient K, F et ρ définis comme dans les cas $\boldsymbol{S}$, $\boldsymbol{Q}$ *ou* $\boldsymbol{M}$, *et n un entier. Si $f \in F$ est solution d'une ρ-équation linéaire d'ordre n*

$$\rho^n(y) + a_{n-1}\rho^{n-1}(y) + \cdots + a_1\rho(y) + a_0 y = 0\,,$$

où $a_0, \ldots, a_{n-1} \in K$, alors soit $f \in K$, soit f est hypertranscendante sur K.

Les résultats obtenus jusqu'ici étaient de trois types.

- Ceux concernant les équations inhomogènes d'ordre 1 ($\rho(y) = ay + b$). Hölder, Moore, Mahler, Randé, Ishisaki, Hardouin-Singer, Nguyen...
- Ceux concernant les équations dont le groupe de Galois est gros (simple, semisimple...). Ces résultats ont en particulier des conséquences sur les équations d'ordre 2. Hardouin-Singer, Dreyfus-Hardouin-Roques, Arreche-Singer, Arreche-Dreyfus-Roques.
- Ceux traitant des équations générales, mais limités à la non holonomie. Ramis, Bézivin, Bézivin-Grammain, Schäfke-Singer.

Résultat principal suite

La même stratégie de preuve permet de considérer le cas de deux opérateurs aux différences suffisamment indépendants
(deux opérateurs de décalage avec $h_1/h_2 \notin \mathbb{Q}$, deux opérateurs aux q-différences multiplicativement indépendants $\log q_1/\log q_2 \notin \mathbb{Q}$ ou deux opérateurs mahlériens multiplicativement indépendants $\log p_1/\log p_2 \notin \mathbb{Q}$).

Les résultats prennent une forme un peu différente, dont voici une illustration qui confirme une conjecture de Loxton et van der Poorten de 1987.

Théorème (A., Dreyfus, Hardouin, Wibmer)

On suppose $\log p_1/\log p_2 \notin \mathbb{Q}$. Soient $f \in \mathbb{C}[[x]]$ une série formelle p_1-mahlérienne irrationnelle et $g \in \mathbb{C}[[x]]$ une série formelle p_2-mahlérienne irrationnelle, alors f et g sont algébriquement indépendantes sur $\mathbb{C}(x)$.

Le théorème de Cobham sur les ensembles automatiques se reformule ainsi : une série formelle p_1- et p_2-automatique est rationnelle.

A. et Bell (redémontré par Schäfke et Singer) : une série formelle p_1- et p_2-mahlérienne est rationnelle,
c'est-à-dire $f \neq g$.

On considère un système de la forme

$$\rho(Y) = AY, \text{ with } A \in \mathrm{GL}_n(K). \tag{1}$$

Attention. On ne considèrera que des extensions de Picard-Vessiot qui sont des corps. Cela est possible car nous pouvons toujours remplacer un système par un système itéré.

Une *extension de Picard-Vessiot* $\mathcal{Q}$ pour (1) sur K est une ρ-extension de corps de K telle que :

(1) Il existe une matrice fondamentale $U \in \mathrm{GL}_n(\mathcal{Q})$, c'est-à-dire telle que $\rho(U) = AU$.

(2) $\mathcal{Q}$ est la plus petite ρ-extension de corps de K contenant U.

(3) $\mathcal{Q}^\rho = K^\rho = \mathbb{C}$.

Remarque. Le fait que le corps des constantes $\mathbb{C}$ est un corps algébriquement clos de caractéristique zéro garantit l'existence et l'unicité de telles extensions.

Soit $\mathcal{Q}$ une extension de Picard-Vessiot de K. Le *Groupe de Galois aux différences* $\mathrm{Gal}(\mathcal{Q}/K)$ du système (1) sur K est défini comme le groupe des K-automorphismes de $\mathcal{Q}$ qui commutent avec ρ :

$$\mathrm{Gal}(\mathcal{Q}/K) := \{\sigma \in \mathrm{Aut}(\mathcal{Q}/K) \mid \rho \circ \sigma = \sigma \circ \rho\}.$$

Si $U \in \mathrm{GL}_n(\mathcal{Q})$ est une matrice fondamentale, alors

$$U^{-1}\sigma(U) \in \mathrm{GL}_n(\mathbb{C})$$

pour tout $\sigma \in \mathrm{Gal}(\mathcal{Q}/K)$.

On obtient une représentation fidèle

$$\begin{array}{ccc} \mathrm{Gal}(\mathcal{Q}/K) & \rightarrow & \mathrm{GL}_n(\mathbb{C}) \\ \sigma & \mapsto & U^{-1}\sigma(U) \end{array}$$

qui permet d'identifier $\mathrm{Gal}(\mathcal{Q}/K)$ à un groupe algébrique linéaire inclut dans $\mathrm{GL}_n(\mathbb{C})$.

(ρ, δ)-trucs : structures compatibles avec l'action de ρ et de δ.

On veut faire la même chose que précédemment, mais au lieu d'un corps de constantes $\mathbb{C}$ algébriquement clos, on doit travailler avec un corps de constantes $\widetilde{\mathbb{C}}$ différentiellement clos.

Un corps différentiel (L, δ) est *differentiellement clos* si tout système d'équations δ-polynomiales a une solution dans une δ-extension de corps de L si et seulement si il a une solution dans L.

On note $\widetilde{K}$ le corps obtenu à partir de K par extension des scalaires de $\mathbb{C}$ à $\widetilde{\mathbb{C}}$. (Si $K = \mathbb{C}(x)$ alors $\widetilde{K} = \widetilde{\mathbb{C}}(x)$).

Remarque. Dans le cas **M**, il y a une petite subtilité car on veut que ρ et δ commutent !

On considère un système de la forme

$$\rho(Y) = AY, \text{ with } A \in \mathrm{GL}_n(\widetilde{K}). \tag{2}$$

Attention. Là encore on ne considèrera que des (ρ, δ)-extensions de Picard-Vessiot qui sont des corps.

Une *(ρ, δ)-extension de Picard-Vessiot* $\widetilde{\mathcal{Q}}$ pour (2) sur $\widetilde{K}$ est une (ρ, δ)-extension de corps de $\widetilde{K}$ telle que :

(1) Il existe une matrice fondamentale $U \in \mathrm{GL}_n(\widetilde{\mathcal{Q}})$, c'est-à-dire telle que $\rho(U) = AU$.

(2) $\widetilde{\mathcal{Q}}$ est la plus petite ρ-extension de corps de $\widetilde{K}$ contenant U.

(3) $\widetilde{\mathcal{Q}}^{\rho} = \widetilde{K}^{\rho} = \widetilde{\mathbb{C}}$.

Remarque. Le fait que le corps des constantes $\widetilde{\mathbb{C}}$ est différentiellement clos garantit l'existence et l'unicité de telles extensions.

Soit $\widetilde{\mathcal{Q}}$ une (ρ, δ)-extension de Picard-Vessiot de $\widetilde{K}$. Le *Groupe de Galois paramétré* $\mathrm{Gal}^{\delta}(\widetilde{\mathcal{Q}}/\widetilde{K})$ du système (2) sur $\widetilde{K}$ est défini comme le groupe des $\widetilde{K}$-automorphismes de $\mathcal{Q}$ qui commutent avec ρ et δ :

$$\mathrm{Gal}^{\delta}(\widetilde{\mathcal{Q}}/\widetilde{K}) := \left\{ \sigma \in \mathrm{Aut}(\widetilde{\mathcal{Q}}/\widetilde{K}) \middle| \; \rho \circ \sigma = \sigma \circ \rho \text{ et } \delta \circ \sigma = \sigma \circ \delta \right\}.$$

On peut identifier $\mathrm{Gal}^{\delta}(\widetilde{\mathcal{Q}}/\widetilde{K})$ à un groupe algébrique différentiel linéaire inclut dans $\mathrm{GL}_n(\widetilde{\mathbb{C}})$.

Le (ρ, δ)-corps $\widetilde{\mathcal{Q}}$ contient une extension de Picard-Vessiot $\mathcal{Q}$ sur $\widetilde{K}$, ce qui permet de voir $\mathrm{Gal}^{\delta}(\widetilde{\mathcal{Q}}/\widetilde{K})$ comme un sous-groupe de $\mathrm{Gal}(\mathcal{Q}/\widetilde{K})$.

Théorème

Le groupe de Galois paramétré $\mathrm{Gal}^{\delta}(\widetilde{\mathcal{Q}}/\widetilde{K})$ *est Zariski-dense dans* $\mathrm{Gal}(\mathcal{Q}/\widetilde{K})$.

Principe de la démonstration

Elle se décompose en trois étapes.

• On démontre le résultat pour les équations inhomogène d'ordre 1 (déjà connu).

• On démontre le résultat sous l'hypothèse que le groupe de Galois est connexe et irréductible (et que le système associé est de taille au moins 2). L'idée est de se ramener aux résultats connus concernant le cas des groupes semi-simples.

• On démontre le résultat général par récurrence sur l'ordre de l'équation.

Le cas irréductible et connexe

Supposons que le groupe de Galois $\mathrm{Gal}(\mathcal{Q}/K)$ du système sur K est connexe et irréductible.
On considère alors le groupe de Galois $G = \mathrm{Gal}(\mathcal{Q}/\widetilde{K})$ du système sur $\widetilde{K}$, où l'extension de Picard-Vessiot $\mathcal{Q}$ est contenue dans l'extension de Picard-Vessiot paramétrée $\widetilde{\mathcal{Q}}$.

Alors G est irréductible et, d'après le théorème de Lie-Kolchin, G n'est pas résoluble.
Comme G est aussi connexe, le quotient $H := G/R(G)$ est un groupe non-trivial qui est semi-simple.

Comme H est un quotient du groupe de Galois G, la correspondance de Galois assure l'existence d'un système $\rho(Y) = A_1 Y$ qui admet H comme groupe de Galois et qui a une extension de Picard-Vessiot $\mathcal{Q}_1$ dans $\widetilde{\mathcal{Q}}$.

Remarque. A priori A_1 est à coefficients dans $\widetilde{K}$, mais on peut montrer que ces derniers sont en fait dans K.

Comme H est semi-simple, un résultat de Arreche et Singer garantit que

$$\mathrm{Gal}(\mathcal{Q}_1/\widetilde{K}) = \mathrm{Gal}^{\delta}(\widetilde{\mathcal{Q}_1}/\widetilde{K})$$

Maintenant si f est δ-algébrique, alors les coordonnées du vecteur solution $(f, \rho(f), \dots, \rho^{n-1}(f))$ sont toutes δ-algébriques.

Donc l'espace des solutions δ-algébriques n'est pas trivial et il est d'autre part invariant par le groupe de Galois paramétré. Ce dernier est irréductible car dense dans un groupe irréductible.

Cette espace invariant doit donc avoir une dimension maximale, ce qui implique que le δ-degré de transcendance de $\widetilde{\mathcal{Q}}$ est nul. On obtient donc une contradiction. $\square$

Conclusion. Si le groupe de Galois d'un système sur K (de taille au moins 2) est connexe et irréductible, alors la (ρ, δ)-extension de Picard-Vessiot associée $\widetilde{\mathcal{Q}}$ ne contient aucun vecteur solution dont toutes les coordonnées sont δ-algébrique sur $\widetilde{K}$.

(H_n) Pour tout entier k et tout $f \in F$ solution d'une ρ^k-équation linéaire d'ordre au plus n à coefficients dans K, on a soit f est hypertranscendante, soit $f \in K$.

(H_1) est déjà connu. Soit $n \geq 2$ et supposons que (H_{n-1}) est vérifiée.

Soit $f \in F$ une solution d'une ρ^k-équation lineéaire d'ordre n. Quitte à itérer le système associé à f et à changer ρ, on peut se ramener à la situation suivante :

(a) $(f, \ldots, \rho^{n-1}(f))^\top$ est solution du système $\rho(Y) = AY$, où $A \in \mathrm{GL}_n(K)$.

(b) Il existe une (ρ, δ)-Picard-Vessiot extension $\widetilde{\mathcal{Q}}$ pour $\rho(Y) = AY$ sur $\widetilde{K}$, telle que le vecteur $(f, \ldots, \rho^{n-1}(f))^\top$ est la première colonne d'une matrice fondamentale $U \in \mathrm{GL}_n(\widetilde{\mathcal{Q}})$.

(c) Le groupe de Galois G du système $\rho(Y) = AY$ sur K est connexe.

Si G est irréductible, on a déjà montré que f est hypertranscendante.
On suppose donc que G est réductible et que f est ∂-algebrique sur K et il reste à montrer que $f \in K$.

Comme G est réductible, il existe $T = (t_{i,j}) \in \mathrm{GL}_n(K)$ telle que

$$\rho(T)AT^{-1} = \begin{pmatrix} A_1 & A_{1,2} \\ 0 & A_2 \end{pmatrix},$$

où $A_i \in \mathrm{GL}_{n_i}(K)$, $n_1 + n_2 = n$ et $n_2 < n$. On choisit n_1 minimal.

Posons

$$(g_i)_{i \leq n}^{\top} := T(\rho^{i-1}(f))_{i \leq n}^{\top} \in F^n .$$

Le vecteur $(g_i)_{n_1+1 \leq i \leq n}^{\top} \in F^{n_2}$ est solution du système $\rho(Y) = A_2 Y$.
De plus, comme f est ∂-algebrique sur K, les g_i le sont également. D'après (H_{n_2}), on a

$$(g_i)_{n_1+1 \leq i \leq n}^{\top} \in K^{n_2} .$$

Si $g_1, \ldots, g_{n_1} \in K$, alors $f \in K$ et c'est fini.

On suppose donc que l'un des g_i n'est pas dans $K = F \cap \widetilde{K}$.
Soit G_1 le groupe de Galois associé au système $\rho(Y) = A_1 Y$ sur K. Alors, G_1 est connexe (car G l'est) et irréductible (par minimalité de n_1).

Montrons que $n_1 = 1$.

Soit H le groupe de Galois paramétré de $\rho(Y) = AY$ sur $\widetilde{K}$. Par hypothèse, au moins l'un des g_i n'appartient pas à $\widetilde{K}$. D'autre part, les g_i, comme les f_i sont dans $\widetilde{\mathcal{Q}}$.

La correspondance de Galois assure l'existence de $\sigma \in H$ tel que

$$(\sigma(g_i))_{i\leq n}^{\top} \neq (g_i)_{i\leq n}^{\top},$$

tandis que $\sigma(g_i) = g_i$ pour $n_1 + 1 \leq i \leq n$.

Posons

$$u_1 := (g_i)_{i\leq \mathbf{n_1}}^{\top}, \quad u_2 := (g_i)_{\mathbf{n_1+1}\leq i\leq n}^{\top} \text{ et } v_1 := (\sigma(g_i))_{i\leq \mathbf{n_1}}^{\top}.$$

Ainsi $w := u_1 - v_1 \neq 0$. Les coordonnées de w sont δ-algébriques sur $\widetilde{K}$.

De plus, u_1 et v_1 sont deux vecteurs solutions du système

$$\rho(Y) = A_1 Y + A_{1,2} u_2,$$

de sorte que

$$\rho(w) = A_1 w. \quad \square$$

Montrons que $(g_1, \ldots, g_n) \in K^n$.
Posons

$$u_2 := (g_i)^{\top}_{2 \leq i \leq n}\,.$$

On a déjà montré que $u_2 \in K^{n-1}$. Ainsi

$$A_{1,2}u_2 \in K\,.$$

D'autre part, $g_1 \in F$ est solution de l'équation inhomogène d'ordre un :

$$\rho(Y) = A_1 Y + A_{1,2}u_2\,.$$

Comme g_1 est ∂-algebrique sur K, on obtient que $g_1 \in K$ et donc $(g_1, \ldots, g_n) \in K^n$.

Comme

$$(f, \ldots, \rho^{n-1}(f))^{\top} = T^{-1}(g_1, \ldots, g_n)^{\top}$$

et que les coefficients de T sont dans K, on obtient bien que $f \in K$, comme voulu. $\square$